

- accumulators 225–6
 - witness 225
- addresses 12–13, 17, 73–5
 - Base58 74–5
 - Base64 75 and note
 - Exodus 202
 - public key 74
 - script 74
 - tampering 124
 - unlocked 204
 - validation 213–14
 - vanity 137–9
- Advanced Encryption Standard (AES) 125–6
- AES *see* Advanced Encryption Standard
- alternative coins (alt-coins)
 - advantages/disadvantages 178–81
 - description 171
 - market capitalization 181
 - multipools 171
 - pre-mining 171
 - types 172–8
- AML *see* Anti-Money Laundering
- Anoncoin 178
- anonymous electronic cash 165–7
- anonymous electronic payments *see* ecash
- Anti-Money Laundering (AML) 38, 39
- Aphroditecoin 177
- Application Programming Interface (API) 10
- Application-Specific Integrated Circuit (ASIC) 145, 147, 148–9, 172
- ASIC *see* Application-Specific Integrated Circuit
- asset swaps 197
- assurance contract 189
- asynchronous multisignature escrow 200
- ATMs 48
- atomic cross-chain trading 232–3
- attacks, attackers 17 and note
 - access to private keys 17
 - block withholding 153–4
 - blockchain 15
 - central database 12
 - decentralized systems 5–6
 - denial of service 88, 91, 101, 102, 116, 121n, 155, 184, 193, 201
 - double-spend 6, 8 and note, 17 and note, 113–16
 - existential forgery attack 61
 - Finney 116
 - length extension 99
 - Man-in-the-Middle 53–5
 - quantum computing 244
 - race 115
 - stealth addresses 217–19
 - Sybil 165n
 - wallets 17–18, 44
 - ZeroCoin 228
- AUR *see* Auroracoin
- Auroracoin (AUR) 175
- Austrian School 21–2, 30
- autonomous agents 10, 187–8, 200
- b-money 164–5
- Back, Adam 163–4
- Bank Secrecy Act 37
- BIP 70 124, 141–2
- bit gold 164–5
- Bitcoin
 - advantages 25–6, 30–1
 - anonymous 9
 - applications 39–48
 - creation 3–4
 - creator/s 168–9
 - criticism 24
 - decentralized 4–6, 13–15, 188
 - different meanings 18–19
 - disadvantages 26–7, 31–2
 - distributed database 8–9
 - economics 21–38
 - effect on financial industry/monetary policy 35–7
 - features 4
 - hedging volatility 145
 - investment aspect 4, 29–32
 - media coverage/misconceptions 3
 - network 4
 - open-source code 4, 6–8

- Bitcoin (*continued*)
 - origins 161–9
 - peer-to-peer network 5, 6, 144
 - personal information/transparency 9
 - as Ponzi scheme 4
 - pseudonymity 14, 26
 - start-up 29–30
 - technology 9–10, 11–19
 - transaction fees 39
 - volatility 33–5
- Bitcoin Core 19, 74n, 137, 143n, 227
- Bitcoin Core Server (bitcoind) 19
- Bitcoin Core Wallet (bitcoin-qt) 19, 78n, 125–6
 - key pool 126
- bitcoin (currency)
 - as bubble 4
 - creation 4
 - dormant accounts 28
 - hoarding 28–9
- Bitcoin Improvement Proposals (BIPs) 90
- Bitcoin Pooled Mining (BPM) 153
- bitcoind *see* Bitcoin Core Server
- BitLicense 37n
- BitTorrent 12–13
- blind signature 71–2
- block ciphers 125
- block reward 16, 39, 105–6, 107–8
- blockchain 15–17, 27, 74n, 95
 - alternative chains 237
 - archival mode 122
 - block difficulty 105, 107
 - block height 108
 - bootstrapping 112
 - coinbase 106–7
 - currency generation algorithm 108
 - data insertion 192–4
 - decentralized asset register 183–4
 - empty blocks 107
 - finite 122
 - fork 108–9
 - genesis block 108
 - hash functions 95–9, 107
 - head 108
 - length 109
 - Merkle trees 117–20
 - miners 105
 - mining 107
 - on-blockchain/off-blockchain 194
 - orphan block 108
 - parent block 108
 - proof-of-work 101–5
 - scalability 120–2
 - time-stamp 99–101
 - transfer value 237
 - ultimate compression 121–2
 - unconfirmed transactions 110
- bloom filters 44n, 140 and note
- botnet 102, 145
- bottleneck for scalability 121
 - computational power 121
 - network 121
 - storage 121–2
- bounded error quantum polynomial time (BQP) 243n
- BPM *see* Bitcoin Pooled Mining
- BQP *see* bounded error quantum polynomial time
- brain wallets 132
- business applications 39
 - ATMs 48
 - exchange sector 40–3
 - mining industry 46–8
 - money transfer cost advantages 39–40
 - multisignature escrow services 45–6
 - payment processors 43
 - web wallets 43–5
- Byzantine Generals' problem 6n, 165
- CA *see* Certificate Authority
- Caesar's cipher 51–2
- CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) 102–3 and note
- central database 11–13, 15
- Central Processing Unit (CPUs) 146–7 and note, 148–9
- Certificate Authority (CA) 55
- CFDs *see* Contract for Differences
- chain-trade script 232
- charge-back fraud 25
- Chaum, David 162–3, 241n
- ChromaWallet 197
- ciphertext 51
- cloud wallets 131
- Coase, Ronald 10
- coin control 78n
- coin-days 28–9
- coinbase 106–7 and note
- CoinJoin 214–15
- CoinPrism 197
- CoinSwap 215–17
- cold storage 18, 126
- Colored Coins 196–7
 - genesis transaction 196
 - issuing address 196
 - multi-colored transactions 197
 - transfer transaction 196–7
- commitment scheme 221
- committed transaction 220
- computational complexity theory 221–3
- Contract for Differences (CFDs) 190–1, 203
- contracts 183
 - assurance 189
 - autonomous agents 187–8
 - CFDs 190–1

- crowdfunding 189
- deposits 191–2
- digital assets 183–5
- distributed exchange 191
- dominant assurance 189
- external state contract 190
- inserting data into blockchain 192–4
- meta-coins 194–207
- micropayments 186–7
- potential applications 188
- Ricardian 240–2
- savings addresses 192
- smart 9
- smart property 185–6
- costs 26, 39
- Counterparty 197–8
 - protocol 199
 - transaction data output 198
 - XCPs 197–8
- Counterparty message
 - bet 198
 - broadcast 198
 - burn 198
 - dividend 198
 - issue 198
 - order 198
 - send 198
- CPUs *see* Central Processing Unit
- credit 26
- crowd-funding 189
- cryptocurrencies 7, 31
 - anonymity/decentralization 161
 - development 161–9
 - government bans on 32
 - increase resilience of economy 37
 - legal tender status 31
 - substitutes 31
- cryptographic hash functions 96–7
 - compression function 97
 - Merkle-Damgård construction 97–9
 - one-wayness (preimage resistance) 96
 - strong collision resistance 96
 - weak collision resistance 96
- cryptographic key 13–14
- cryptology
 - blind signature 71–2
 - definition/description 51
 - hash functions 52
 - Shamir secret sharing 72–3
 - symmetric ciphers 51–2
 - zero knowledge 58 and note
 - see also* public key cryptography; symmetric-key cryptography
- cryptolegder 183 and note
- CryptoNote 178
- Cunicula 236
- CureCoin 178
- currency 19
 - self-stabilizing 202
- currency generation algorithm 108
- cypherpunk movement 161–2
- DACs (or DAOs) *see* Decentralized Autonomous Corporations (Decentralized Autonomous Organizations or Distributed Autonomous Corporations)
- DAG *see* directed acyclic graph
- DarkCoin 178
- data insertion 192–4
 - in the coinbase 192–3
 - digital notaries 194
 - fake Bitcoin address 193
 - multisignature transaction 193
 - OP_RETURN controversy 193
- data storage 200
- data stream registration 203
- DDoS *see* Distributed Denial of Service
- Decentralized Autonomous Corporations (Decentralized Autonomous Organizations or Distributed Autonomous Corporations) (DACs or DAOs) 187–8
- decentralized system 4–6, 187
- deflation 30, 32–3
- demurrage 177
- denial of service (DoS) 88, 91, 101, 102, 116, 121n, 155, 184, 193, 201
- deposit insurance 32
- deposits 191–2
- derivatives 200
- deterministic wallets 132
 - advantages 132–3
 - hierarchical 135–6
 - master password 133
 - Message Authentication Code (MAC) 134–5
 - type-1 133
 - type-2 133–4
- Devcoin 178
- DHT *see* Distributed Hash Table
- Diffie-Hellman key exchange protocol 217–18
- digital assets 183–5, 200, 203
 - blockchain 183–5
 - creation 184
 - issuer 185
 - storage 185
 - transfer 26
- digital notary 100, 194
- digital payment system, creating 11–13
- Digital Signature Algorithm (DSA) 59
- digital signatures
 - description/process 56–8
 - DSA 59
 - Elgamal 59

- digital signatures (*continued*)
 - message length 58
 - public key families 58
 - RSA 58
 - schemes 58–9
 - Schnorr 58–9
- directed acyclic graph (DAG) 209
- discrete logarithm (DL) 58
- dispute mediation 45–6
- distributed database 15–17
- Distributed Denial of Service (DDoS) 102
- distributed exchange 191
- Distributed Hash Table (DHT) 193
- DL *see* discrete logarithm
- DOGE *see* Dogecoin
- Dogecoin (DOGE) 176–7
- Domain Name System (DNS) 174 and note, 175
- dominant assurance contract 189
- DoS *see* denial of service
- double-spend 12
 - 51% attack 17, 113–15
 - attacks 6, 8 and note, 17 and note
 - Finney attack 116
 - race attack 115
 - transaction spamming 116–17
- DRM schemes 188
- DSA *see* Digital Signature Algorithm
- dust transaction 80
- e-gold 12
- EC *see* elliptic curve
- ecash 162–3
- ECDH *see* Elliptic Curve Diffie-Hellman
- ECDSA *see* elliptic curve digital signature algorithm
- economics
 - Austrian School 21–2
 - business cycles 22
 - deflation 21–2
 - inflation 21, 22
 - mediums of exchange 21
- EFTs *see* Exchange Traded Funds
- Elgamal signature 59
- Elliptic Curve Diffie-Hellman (ECDH) key exchange 218–19
- elliptic curve digital signature algorithm (ECDSA) 70–1, 178, 204 and note
- elliptic curve (EC) 58, 62, 243
 - abelian group 66
 - cyclic group 66
 - discrete logarithm 66, 67n
 - double-and-add algorithm 67 and note
 - ephemeral random number 70–1
 - group operation/addition 64–6
 - nonce 70
 - point in infinity 66
 - point multiplication 66
 - summary 63–4
 - theory 64–71
- ephemeral random number 70–1
- escrow services *see* multisignature escrow
- Ethereum 192, 194n, 199–202
 - blocks 199–200
 - contracts 199
 - description 199
 - halting problem 201
 - hash function 201 and note
 - loops 201 and note
 - mining proposals 201–2
 - native currency 201
 - proposed applications 200
 - transaction fees 200–1
 - Turing-complete nature 199
- Ethereum Virtual Machine (EVM) 199
- EVM *see* Ethereum Virtual Machine
- Exchange Traded Funds (ETFs) 38
- exchanges 40–3
 - counterparty risk 42
 - decentralized 200
 - derivatives 42
 - limit orders 40
 - off-blockchain/third party model 42
 - spot contracts 41
 - web wallets 42
- existential forgery attack 61
- Exodus address 202
- external state contract (oracle contract) 190
- fees 25
 - base fees 26
 - Ethereum 200
- FHE *see* fully homomorphic encryption
- fiat money 5, 26, 30
- Field-Programmable Gate Array (FPGAs) 147
- Financial Crimes Enforcement Network (FinCEN) 37–8
- FinCEN *see* Financial Crimes Enforcement Network
- Finney attack 116
- Finney, Hal 167–8
- floating fees 156
- floating point operations per second (FLOPs) 149n
- FLOPs *see* floating point operations per second
- forks, forking 8, 108–9 and note
- FPGAs *see* Field-Programmable Gate Array
- fractional reserve banking 22 and note, 35–6 and note
- fragmented backups 73
- FRC *see* Freicoin
- Freicoin (FRC) 177
- fully homomorphic encryption (FHE) 245
- generation signature 204
- GHOST (Greedy Heaviest-Observed Sub-Tree) 115

- GNU Public License (GPL) 7
- GPG (Gnu Privacy Guard) computer program 55
 - and note
- GPU *see* Graphics Processing Unit
- graph 3-colorability problem 222–3
 - cut-and-choose 223
 - NP-complete 223
- Graphics Processing Unit (GPU) 147, 148
- graphs *see under* network analysis
- greenlisting (address validation) 213–14
- Gresham's Law 33
- Grover's algorithm 244

- hardware wallets 130–1
- hash functions 52, 58 and note
 - cryptographic 96
 - description 95–9
 - hash value 95
 - meat grinder analogy 96n
 - memory-hard 99
 - password hashing 98
 - solution to hash inversion 105–6
- hash rate 107
- hash tree *see* Merkle trees
- hash type 88 and note
- Hash-based Message Authentication Code (HMAC) 135
- Hashcash 163–4
 - counter 104
 - date 104
 - header 104–5
 - nonce 104
 - preimage 104
 - recipient email address 104
 - version 104
- hashlocked transactions 215–16
 - linked 216–17
- HD wallets *see* Hierarchical Deterministic wallets
- HDM wallets *see* Hierarchical Deterministic Multisignature wallets
- HFE^v 244
- Hierarchical Deterministic Multisignature wallets (HDM wallets) 137
- Hierarchical Deterministic wallets (HD wallets) 135
 - child number 135–6
 - private child derivation 135
 - private nodes 135
 - public child derivation 135
 - public nodes 135
- HMAC *see* hash-based Message Authentication Code
- hoarding 28
- homomorphic encryption 188, 244–5
- hosted wallets 131
- hot wallet 126

- integer factorization 58
- Internal Revenue Service (IRS) 38
- investment 29–30
- Invisible Internet Project (I2P) 178
- IRS *see* Internal Revenue Service

- Java Virtual Machine 199

- Kerckhoff's Principle 51 and note
- key stretching 132
- key-derivation function 99
 - bcrypt 99
 - memory-hard hash functions 99
 - PBKDF2 99
- Know Your Customer (KYC) 38
- KYC *see* Know Your Customer

- Lamport signatures 244
- lattice-based system 244
- laundry services (mixing services) 212–13
- length extension attacks 99
- Liberty Reserve 12
- liquidity 179
- Litecoin (LTC) 172–3
- LTC *see* Litecoin
- Lucifer (blind signature) 241n

- m-of-n multisignature transactions 84–5
- MaaS *see* mining as a service
- MAC *see* Message Authentication Code
- McEliece code-based encryption 244
- machine-learning fraud-detecting algorithms 45
- Man-in-the-Middle attack (MitM) 53–5
- Mastercoin
 - creating digital assets 202–3
 - creating “rate-limited” addresses 203
 - creating “savings” addresses 203
 - currency (mastercoin) (MSC) 202
 - description 202
 - Exodus address 202
 - guardian address 203
 - paying dividends to digital assets 203
 - protocol 203
 - purchasing mastercoins 202
 - registering data streams 203
 - sending mastercoins/other digital assets 202
 - submitting/executing bets/CFDs 203
 - submitting/executing buy/sell orders 203
- mastercoin (currency) (MSC) 202
- medium of exchange 21, 22–4
 - advantages 26–7
 - critical mass 23–4
 - drawbacks 25–6
- mempool 110 and note
- Meni 236
- merge avoidance 219–20

- merged mining 237–8
- Merkle trees 166–7
 - binary tree 117
 - block header 117–18 and note
 - description 117
 - Merkle branch 118
 - root hash/Merkle root 117
 - transaction malleability 119–20
 - Zerocash 229
- Merkle-Damgård construction 97–9
- Message Authentication Code (MAC) 134–5
- meta-coins 185, 194–5
 - description 194
 - on-blockchain/off-blockchain 194–5
 - open-source code 196
 - types 196–207
- metahashes 152
- Metcalfe's law 179
- micropayment channel 231
- micropayments (microtransactions) 26, 186–7, 231–2
- miners
 - block rewards 105–8
 - blockchains 105, 107–8
 - committed transaction 220
 - definition/description 16
 - forks 108–9
 - hash rate 107
 - hash solution 107
 - incentive to cheat 152
 - inserting data into blockchain 192–3
 - metahashes 152
 - revenue 24–5
 - shares 152
 - transaction fees 154–6
- mining
 - advantages 144–5
 - business models 46
 - cashflow analysis 47–8
 - datacenters 46
 - definition/description 143–5
 - equipment 16–17, 46–7
 - Ethereum proposals 201–2
 - hosted mining/cloud mining 46
 - merged 237–8
 - mining pool operators 46
 - nodes 111–12
 - pooled 149–54
 - revenues 46
 - selfish 156–8
 - technology 146–9
 - transaction fees 154–6
- mining pool 150–3
 - Bitcoin Pooled Mining 153
 - block withholding attack 153–4
 - incentive to cheat 152
 - P2Pool 153
 - pay-per-last-N-shares 153
 - pay-per-share 153
 - protocols 153–4
- mining as a service (MaaS) 46
- Mises' regression theorem 22
- MitM *see* Man-in-the-Middle attack
- mixing services (laundry services) 212–13
- money
 - functions 21
 - medium of exchange 21
 - multiplier 35n
 - store of value 21
 - transfer 39–40
 - transmitters 37–8
 - unit of account 21
- MSC *see* mastercoin (currency)
- multi-PPS 158
- Multilinear Jigsaw Puzzles 246
- multisignature escrow 45–6, 200
- multisignature voting pools 242
- multisignature wallets 44, 45, 136–7
- multivariate-quadratic system 244
- Nakamoto, Satoshi 3, 168–9
- Namecoin (NMC) 174–5, 200
- network 18
 - externalities 178
 - hash rate 107
 - network analysis
 - closure under signing operation 210
 - cluster analysis 211
 - directed acyclic graph (DAG) 209
 - flow/temporal analysis 211–12
 - graph isomorphism with other social networks 212
 - graph isomorphism problem 212
 - integrate IP traffic 211
 - integrate off-network information 211
 - network topology 211
 - transaction graph 209
 - user graph 210–12
 - network effect 178–9
 - direct 178
 - indirect 178
 - liquidity 179
 - nHashType 88n
 - NMC *see* Namecoin
 - nodes 110–11
 - mining 111
 - passive 111
 - non-interactive zero-knowledge proof (NIZKP)
 - 224–5, 228, 229
 - non-outsourcable puzzles 157–8
 - nonce 63, 70, 98, 103, 104, 105, 107, 143 and note, 201, 202, 217n
 - nondeterministic polynomial time 222
 - NTRU 244

- Nxt
 - currency (NXT) 204
 - description 203
 - elliptic curve algorithm 204 and note
 - generation signature 204
 - protocol 204
 - transactions 204
 - transparent forging 204
 - unlocked addresses/active accounts 204
- nyms (pseudonyms) 240
- obfuscation 245–6
 - indistinguishability 246
 - Multilinear Jigsaw Puzzles 246
- off-blockchain 194
- off-chain transaction 187
- offline wallets 126–7
 - devices 129
 - external storage media 127
 - hardware wallets 130–1
 - paper wallets 127–9
- on-blockchain 194
- one-way accumulators 225–6
- online wallet 126
- open source
 - implementation 19
 - replication 31
 - software 4, 6–8
- open source licenses
 - Copyright 7
 - Permissive 7
- Open Transactions (OT) 240–2
 - development 242
 - features 241–2
 - multisignature voting pools/multisig web wallet service 242
 - nyms 240
 - Ricardian contracts 240–1
 - triple-signed receipts 241
- OP_RETURN 193
 - message 198
 - stealth addresses 218–19
- oracle contract (external state contract) 190
- orphan block 108
- P2Pool 153, 157
- paper wallets 127–9
 - hexadecimal format 127
 - mini private key format 127–8
 - passphrase-protected private keys 128
 - physical bitcoin 129
 - Wallet Import Format (WIF) 127
- parent block 108
- password hashing 98
 - key-derivation function 99
 - rainbow tables 98
 - salt 98
- pay-per-last-N-shares (PPLNS) 153
- pay-per-share (PPS) 153
- pay-to-address 82–3, 93
- pay-to-public-key 83–4
- pay-to-script-hash (P2SH) 89–92, 239
- payment processors 43
- Payment Protocol (BIP 70) 124, 141–2
- Pedersen commitment scheme 224
- peer-to-peer gambling 200
- peer-to-peer network 5, 6, 144, 153, 178
- Peercoin (PPC) 173–4, 236
- permissionless innovation 10
- PGP (Pretty Good Privacy) computer program 55
 - and note
- PKI *see* Public Key Infrastructure
- Ponzi scheme 4
- pour transaction 228, 229
- PPC *see* Peercoin
- PPLNS *see* pay-per-last-N-shares
- PPS *see* pay-per-share
- Primecoin (XMP) 175–6
- priority block 155
- privacy 202
 - fully anonymous decentralized currencies 221–9
 - generalizing 213–14
 - laundry services 212–13
 - network analysis 209–12
 - privacy-enhancing technologies 214–20
- private keys
 - cold storage 18
 - encrypted 17
- proof of existence 194
- proof-of-burn 236
 - proposed applications 237
- proof-of-stake 234
 - advantages 234–5
 - disadvantages 235
 - proposed implementations 235–6
- proof-of-work 101–5
 - alternatives 233–7
 - Hashcash 104–5
 - partial hash inversion 103–4
 - protocols 102–3
- protocols 18, 19n, 26
 - Challenge-Response 102–3
 - Diffie-Hellman key exchange protocol 217–18
 - Master 203
 - mining 153–4
 - Nxt 204
 - Payment Protocol (BIP 70) 141–2
 - Ripple 207
 - Solution-Verification 103
- public asset ledger 8–9
- public key cryptography 52, 244
 - Bitcoin addresses 73–5

- public key cryptography (*continued*)
 - blind signatures 71–2
 - Certificate Authority 55
 - development 53
 - digital signatures 56–9
 - elliptic curves 62–71
 - example of use 53–5
 - hash-based 244
 - key distribution 53
 - key generation algorithm 53
 - keyring 55
 - Man-in-the-Middle attack 53–5
 - private key 53
 - public key 53
 - public key distribution 55
 - public–private keypair 53
 - quantum computing 244
 - RSA technology 59–62
 - Shamir secret sharing 72–3
 - web of trust 55
 - see also* cryptography
- public key families
 - discrete logarithm 58
 - elliptic curve 58
 - integer factorization 58
- Public Key Infrastructure (PKI) 55, 124
- push payment system 26

- Qixcoin 178
- QR code 128 and note
- Quantity Theory of Money 36–7
- quantum computing 242–4
- quantum gates 243

- race attack 115
- rate-limited addresses 203
- record keeping 30
- Red Queen Effect 144 and note
- regulation 26, 37–8
- Reusable Proof-Of-Work (RPOW) 167–8
- Ricardian contracts 240–2
- ring signature 178 and note
- Ripple (decentralized financial network)
 - accounts 206
 - consensus 205–6
 - currency (ripples or ripple credits) (XRP) 206
 - description 204–5
 - development 205
 - gateways 206
 - ledger 205
 - ledger chain 205
 - protocol 207
 - unique node list 206
- ripples (or ripple credits) (XRP) 206
- risk score 45
- RPOW *see* Reusable Proof-Of-Work

- RSA encryption scheme 59–60, 243
- RSA signature 58, 60–2

- SAFE network 178
- Safecoin 178
- Sander, Tomas 165–7
- satoshis 19
- saving accounts 200
- savings addresses 192, 203
- scalability 27, 120–1
 - bottlenecks 121–2
- scarcity issue 30
- Schnorr protocol 224
- Schnorr signature 58–9
- script address 91
- scripts 80–2
 - opcodes 81
 - Turing-complete 81
- scrypt 99, 172
- secure hash functions 96–7
- secure sockets layer (SSL) 56
- security 25, 30
- selfish mining 156–8
- Shamir secret sharing 72–3
- share chain 133
- Shor's algorithm 243, 244
- side-chains 238–40
 - 2-way pegging 239
- simplified payment verification (SPV) 44n, 139–41, 197n
 - block depth 140
 - block height 140
 - connection bloom filtering 140 and note
- Slasher 236
- smart contracts 9
- smart fees 156
- smart property 185–6
- SolarCoin 177
- Splash 177
- SPV *see* simplified payment verification
- SSL *see* secure sockets layer
- stealth addresses 217–19
- storage requirements 121–2
- store of value 21
 - advantages 30–1
 - comparison with other assets 31
 - disadvantages 31–2
 - hoarding 28–9
 - risk/reward of investment 29–30
- stream ciphers 125
- Sybil attack 165n
- symmetric ciphers 52
- symmetry-key cryptography 52, 125–6
 - block ciphers 125
 - stream ciphers 125
- Szabo, Nick 164–5

- 2-way pegging 239
- Ta-Shma, Amnon 165–7
- Tabarrok, Alexander 189
- TAGCoin 178
- target hash 107
- testnet 74 and note
- three-party escrow 85
- threshold scheme 72
- time-stamp 99–101, 194
 - linked 101
- Time-Stamping Authority (TSA) 100–1
- TLS *see* Transport Layer Security
- TPM *see* Trusted Platform Modules
- tragedy of the commons 8
- transaction inputs (TxIn) 77
- transaction malleability 119–20
- transaction outputs (TxOut) 77
- transactions
 - change address 77–8
 - confirmed 110
 - definition/description 77–80
 - denial of service (DoS) 88
 - dust 80, 116
 - fees 77, 154–6
 - hashlocked 215–17
 - lock time 86
 - multisignature (m-of-n) 84–5
 - non-standard 92
 - off-chain 187
 - other types 85–6
 - pay-to-address/pay-to-public-key 82–4, 93
 - pay-to-script-hash (P2SH) 89–92
 - pour 228, 229
 - priority 155
 - scripts 80–2
 - sequence number 86–7
 - signature 86–9
 - standard 923
 - transaction replacement 87
 - unconfirmed 110
 - unfinalized transactions 87–8
 - valid 78–9
- transparent forging 204
- Transport Layer Security (TLS) 56
- Trezor™ hardware wallet 130 and note
- triple-signed receipts 242
- trusted computing 188
- Trusted Platform Modules (TPM) 188
- Trusted Third Party systems 169
- Turing-complete 81 and note, 199
- TxIn *see* transaction inputs
- unconfirmed transactions' memory pool 110
- unit of account 21, 32
- unspent transaction outputs (UTXO) 15–16, 79, 110–11, 122, 139, 199
- unused output tree (UOT) 122
- UOT *see* unused output tree
- UTXO *see* unspent transaction outputs
- valid transaction 78
- vanity addresses 137–9
- volatility 33–5
- Wallet Import Format (WIF) 127
- wallet protection service 85
- wallets 17–18
 - address tampering 124
 - backing-up 124
 - Bitcoin vs physical differences 123
 - brain 132
 - copying 123
 - deterministic 132–6
 - distributed across devices 123
 - full node 18
 - hybrid web wallets 131
 - lightweight 18
 - multisignature 136–7
 - offline 126–31
 - open source 18 and note
 - Payment Protocol 141–2
 - private keys 17–18
 - receive-only 123
 - simplified payment verification 139–41
 - software 123–4
 - symmetric-key cryptography 125–6
 - vanity addresses 137–9
 - web 18, 43–5, 131, 242
- web of trust 55
- Wei Dai 164–5
- WIF *see* Wallet Import Format
- WiFi hotspots 187
- X.509 certificate 141
- XCP 197–8
- XMP *see* Primecoin
- XRP *see* ripples (or ripple credits)
- zero-knowledge 58 and note, 158 and note, 166
- zero-knowledge proofs (ZKP) 221
 - accumulators 225–6
 - discrete logarithm 223–4
 - graph 3-colorability 222–3
 - non-interactive 224–5
 - Pedersen commitment scheme 224
 - Schnorr protocol 224
 - strong RSA assumption 223
 - trapdoor function 223
- Zerocash 167
 - description 228
 - disadvantage 229
 - pour transaction 228, 229

ZeroCash (*continued*)
storage 229
trapdoor 229
ZeroCoin 167, 224
creation 226
criticism 228

description 226
implementing 227
proposals for change 228
spending/redeeming 226–7
ZKP *see* zero-knowledge proofs

<http://www.pbookshop.com>