Index

Note: Page references in *italics* refer to figures.

ABC Conjecture, 40
Abiodun, Emmanuel, 28, 75–77, 84–85
AIG, 35
AirBnB, 174
Airline frequent flier miles, as currency, 9
Akkoyunlu, A., 50
Alternative currency investment, 121–137
  alternative cryptocurrencies (alt-coins), defined, 88 (*See also* Bitcoin)
  Bitcoin volatility and, 127–129
  exchanges for, 133–135
  growth and, 137
  "Nixon Shock" and, 121–123, 137
  regulation of, 5, 139–148
  60/40 portfolio model and, 123–127, *125, 126*
  valuation and, 129–133, *131, 132, 133*
  vehicles for, 135–137
American Bankers Association, 150
Andreessen, Marc, 6–7
Andreessen Horowitz, 6–7
Andresen, Gavin, 40
Apple, 11
ARPANET (Defense Advanced Research Projects Agency), 150–151
ASIC (application-specific integrated circuit) miners, 21–22, 84–85
ASIC-resistant algorithm, 158
Auroracoin, 141
Austin Global Exchange, 95, 96, 97, 99
Australian, 2
Automobiles, as smart property, 153

Bank for International Settlements, 123
Bank of England, 60–61

Barter system, 63
BCG Matrix, 169–171
Bear Stearns, 34–35, 45
Bernanke, Ben, 35, 65–66
Bitcoin
  Bitcoin and bitcoins, defined, 22–23
  blockchain, defined, 23–24 (*See also* Blockchain)
  as bubble, 1–2, 130–133, *132*
  buying, 3–6, 26–29
  Byzantine Generals' Problem and, 44–45, 52–58
  California gold rush compared to, 19–22
  as currency, 8–10, 13–18
  decentralized financial systems, defined, 63–69, *64, 68*, 73–74
  as disruption to financial services industry, 69–72, *71*
  early sales of, 2, 16
  expectations for, 31–32
  growth of alternative currencies and, 46–47
  inception of, 34–44
  language of, 22–26
  miners' role in, 25–26 (*See also* Miners/mining)
  as peer-to-peer network, 6–8, 10–13, 63–64 (*See also* Peer-to-peer network(s))
  public and private keys, 24–25, 77–78, *78*
  regulation of, 139–148
  timestamp protocol of, 128
  valuation, 129–133, *131, 132, 133*
  value transfer and, 33–34, 39
  volatility and, 127–129
  See also Smart money
Bitcoin Foundation, 40, 42
Bitcoin Investment Trust, 132–133, *133*, 135–137
Bitcoin Magazine, 156
BITCOIN.ORG, 39
"Bitcoin P2P E-Cash Paper" (Nakamoto), 36–37
Bitcoin protocol, 45
Bitcoin-QT, 27
bitcoins
  accepted by merchants, 30–31
  defined, 22–23
  as incentive for mining, 54 (*See also* Miners/mining)
  price fluctuation of, 76
  See also Bitcoin
Bitcointalk (forum), 98
"Bitcoin time," 150
"Bit gold," 40
BitLicense, 144–147
BitPay, 7, 31
Blockchain
  blocks, 12–13, 25–26, 78
  defined, 11–13, 15, 23–24
  international monetary exchange and, 72–73
  security issues of, 11–13, 82
  smart property and, 156–157
Blockchain.info, 27–28
Block halving rate, 83
Bretton Woods Conference, 121–123, 137
Brokers, for bitcoins, 28–29
Bry, Charles, 39
Bubbles (financial), 1–2, 130–133, *132*. *See also* Great Recession
BusinessWeek, 7
Buterin, Vitalik, 155–156
Byrne, Patrick, 30–31
Byzantine Generals' Problem, 44–45, 49–58, 62–63

California gold rush, history of, 19–20, 22
Carlson, Dave, 85, *85*
Cellphones, as smart property, 152

Central banks
centralized systems, defined, *62*, 62–69, 72–73
history of, 46, 59–61 (*See also* Federal Reserve)
money supply and economic growth, *111*, 111–112
Nautiluscoin Stability Fund as "central bank," 94, 95–100
Challenge, defined, 80
Chile, currency of, 130, *131*
China
Bitcoins banned by, 5
digital currency regulation in, 141
Hong Kong economy and, 67–68
Qing Dynasty monetary system, 60
Clear, Michael, 38
CloudHashing, 75–77
CNBC, 2, 124
Coinbase, 4, 27–28, 28–29
"Coincidence of wants," 62
CoinDesk, 70, *71*
Coingen.io, 95, 96, 97
Cold wallets, 134–135
Collision resistant, defined, 80
Colored Coins, 17, 151–152
Committee on Uniform Securities Identification Procedures (CUSIP), 150
ConAgra, 69
Continental currency, history of, 91–92
Counterfeit, avoiding, 11–12
Credit cards
Bitcoin as competition of, 29, 30
processing fees of, 31, 70
security issues of, 71–72
Crypto 2011, 38
Cryptoequities, 160–161
Cryptography
Bitcoin creation and, 38
Bitcoin mining techniques, 78–82, *81*
cryptographic hash functions, 79–82, *81*, 156
cryptographic key pair, 24–25, 77–78, *78*
defined, 23–24
encryption and, 51–58, 70, 81, *81*, 88
SHA-256 (Secure Hash Algorithm), 53, 81, *81*
See also Cryptonomics
Cryptography Mailing List, 35
Cryptonomics, 163–178
DAOs and, 166–169, 173–174
decentralization and, 163–166
defined, 166–169
Experience Curve and, *171*, 171–172
future of, 176–178
Growth Share Matrix and, 169–170, *170*
sharing economy concept of, 174–176
Three Generic Strategies and, 172–173, *173*
Currency
Bitcoin as, 8–10, 13–18
Bitcoin currency exchanges, 21
fiat currency for bitcoins, 28–29
growth of alternative currencies, 46–47
history of, in U.S., 91–92
pegged currency failures, 91–94
trust in, 8–10, 45
See also Alternative currency investment

Davis, Joshua, 38
Decentralized autonomous organizations (DAOs)
Byzantine Generals' Problem and Bitcoin technology, 57–58
cryptonomics and, 161–162, 163–166, 173–174
DAOs, defined, 18, 86
decentralized financial systems, defined, 63–69, *64, 68*, 73–74
Defense Advanced Research Projects Agency (DARPA), 150–151

Denationalization of Money, The (Hayek), 92–93, 104–105, 108
Denmark, digital currency regulation in, 141–142
Department of Finance (New York), 143–147
DigiByte, 97
DigiShield, 97, 98, 102
Digital Asset Transfer Authority (DATA), 147
Digital signature, 79
Digital wallets, 4, 21, 134. *See also* Wallets
Distributed financial systems, 63–69, *64*
Dividends, programming into transactions, 16–17
Dixon, Chris, 7
Dual encryption, credit cards and, 70
Dutch East India Company, 165

EBay, 4
Ekanadham, K., 50
Electricity, used for mining, 87
Encryption
  Byzantine Generals' Problem and, 51–58
  dual encryption and credit cards, 70
  scrypt, 88
  SHA-256 (Secure Hash Algorithm), 53, 81, *81*, 88
  See also Cryptography
Eshet, Mary, 30
Ethereum, 155–160
Ethereum Virtual Machine (EVM) code, 158
Exchange Rate Mechanism (ERM), 93–94
Exchanges, for digital currency, 28–29, 133–135
Experience Curve, *171*, 171–172

Facebook, 49
Fast Company, 39
Fast Money, 4, 96
Federal Reserve
  Great Recession and, 34–35, 45, 47, 65
  quantitative easing by, 2
  regional Federal Reserve Banks, 66–67
Fees
  credit card processing fees, 31, 70
  miners' revenue and, 82
Fiat currency, for bitcoins, 28–29
Field-programmable gate arrays (FPGAs), *84*, 84–85
51 percent attack, 55–57, 86
Financial Crimes Enforcement Division (FINCEN) (U.S. Treasury), 142–143
Financial services industry
  Bitcoin as disruption to, 69–72, *71*
  centralized systems, *62*, 62–69, 72–73
  decentralized systems, 63–69, *64, 68*, 73–74
  distributed systems, 63–69, *64*
  history of, 59–61
Financial Supervisory Authority (FSA) (Denmark), 141–142
Fitch, Jon, 101–103

Gambling, Bitcoin and, 142
Garzik, Jeff, 41–43
Geithner, Tim, 65
Ghash.io, *86*, 87
Gold
  "gold rush" history, 19–20, 22
  as medium of exchange, 107–108
  Nautiluscoin as alternative to, 115–116, *116*
  "Nixon Shock" and gold standard, 121–123, 137
  stable purchasing power and, 88–89
"Gold Standard, Deflation, and Financial Crisis in the Great Depression, The" (Bernanke), 65–66

Goodman, Leah McGrath, 41
Great Depression, 65–66, 177–178
Great Recession
  Bitcoin creation and, 10, 34–35, 45, 47
  centralized financial systems and, 65
  impact on Iceland, 140–141
Growth Share Matrix, 169–170, *170*

Hash value, 80–81
Hayek, Friedrich, 92–93, 104–105, 108
Henderson, Bruce, 169–172
Hong Kong, monetary system of, 67–68
Hot wallets, 134–135
Huber, R. V., 50

Iceland, digital currency regulation in, 140–141
"Idea of Smart Contracts, The" (Szabo), 153–154
Interest rates, purchasing power and, 112–113, *113*
Internal Revenue Service (IRS), 141. *See also* Taxes
International monetary exchange
  central banks and, 72–73
  currency peg failure example, 93–94
  free-floating exchange rates, 122–123
International Monetary Fund (IMF), 119, 121
Internet
  Byzantine Generals' Problem and, 51–52
  inception of, 73, 150–151
IOU enforcement, 8
IrishCentral, 38
ITunes (Apple), 11

Japan, Mt. Gox and, 3
JPMorgan, 34

Kickstarter, 175
Kimoto Gravity Well (KGW), 96
King, Neal, 39
Kinney, Alva, 69

Lamport, Leslie, 44–45, 50
Lawsky, Benjamin, 144
Lawson, Nigel, 93
Ledgers. *See* Blockchain
Lee, Charles, 87
Lehman Brothers, 35
Lerner, Sergio, 42
Litecoin, 87–88, 96
Little, Frank, 69
"Losing positions," 5

Major, John, 93–94
Malkiel, Burton, 124
Markowitz, Harry, 123, 124
Marshall, James, 19
MasterCard, 30
Mastercoin, 17, 151–152
McCaleb, Jed, 39–40
Medici Bank, 60
Medium of exchange, Bitcoin as, 13, 127
Merchants, bitcoins accepted by, 30–31, 130, 132
Merkle, Ralph, 156
Mind Candy, 43–44
Miners/mining, 75–89
  affordability of large mining operations, 157
  ASIC (application-specific integrated circuit) miners, 21–22
  Bitcoin transactions, 77, 77–78
  Byzantine Generals' Problem and, 49–58
  cryptography techniques for, 78–82, *81* (*See also* Cryptography)
  defined, 12–13, 14, 21
  examples of operations, 75–77, *84*, 84–85, *85, 86*, 87
  field-programmable gate arrays (FPGAs), *84*, 84–85

Miners/mining (*Continued*)
impact of, on Nautiluscoin, 98–99, 104
miners as "middlemen," 78
mining pools, 85–88, *86*, 114–115
network difficulty, 82–83, *83*
role of miners, 25–26
stable purchasing power and, 88–89
Mintpal, 99–100
Mobile phones, as smart property, 152
Mochizuki, Shinichi, 40
Modern Portfolio Theory, 123–127, *125, 126*
Money, functions of, 127
Money supply, 5
Money transmitters/money transmission services, 143
MPEx, 142
Mt. Gox
failure of, 14, 15–16
founding of, 39
as largest exchange, 3
security of, 134–135
Musk, Elon, 7

Nakamoto, Dorian S., 41, 43
Nakamoto, Satoshi
Bitcoin inception and, 6, 26
"Bitcoin P2P E-Cash Paper," 36–37
identity of, 3, 20–21, 37–44
Napster, 11
National Banking Acts (1863, 1864), 92
Native Americans, wampum of, 9
Nautiluscoin, 91–105, 107–120
creation of, 94–104
cryptonomic decision-making process and, 167
developing economy of, 107–110
financial market integration of, 117–118
as gold alternative, 115–116, *116*
Hayek's theory and, 92–93, 104–105, 108
Nautiluscoin Stability Fund and, 94, 95–100, 113–114
pegged currency issues and, 91–94
proof-of-stake (PoS), method, 100, 103–104, 110–113, *111, 113*
proof-of-stake (PoS), multipool, 114–115
purchasing power and, 116–117, *117*
Special Drawing Rights (SDRs) and, 119
transparency of, 119–120
Nebraska Consolidated Mills, 69
Network difficulty, 82–83, *83*
Newsweek, 41
New York Department of Finance, 143–147
New Yorker, 38
Nixon, Richard, 122
"Nixon Shock," 121–123, 137
Nodes, 51
Nonce, 81

Oksman, Vladimir, 39
Open source, digital currencies as, 137
Options Clearing Corporation, 159
Overstock, 30

Parker, Sean, 11
Paulson, Hank, 35, 65
PayPal, 4, 7
Pease, Marshall, 44–45, 50
Peer-to-peer network(s)
Bitcoin as, 6–8, 10–13, 63–64
P2P lending, 154
Western Union as P2P network, 61
Penenberg, Adam, 39
People's Bank of China, 141
Perplex City (Mind Candy), 43–44
Peso (Chile), 130, *131*
Popeil, Ron, 149
Porter, Michael, 172
Pound sterling, currency peg failure and, 93–94

P2P Foundation, 36–37, 43
Profit motive, cryptonomics and, 166–169
Proof-of-stake (PoS) method, 100, 103–104, 110–113, *111, 113*
Proof-of-work (PoW) method, 80
Public/private key pair, 24–25, 77, 77–78

Qing Dynasty, 60
Quantitative easing, 2

Regulation, 5, 139–148
Ripple, 39, 151–152

Satoshi (bitcoin denomination), 153
SatoshiDice, 142
Satoshi (name of Bitcoin inventor). *See* Nakamoto, Satoshi
Scrypt, 88
Search for Extraterrestrial Intelligence (SETI), 159
SecondMarket Inc., 136–137
Securities and Exchange Commission (SEC), 142
Security issues
  of bitcoin purchases, 28–29
  blockchain and, 11–13, 23–24, 82 (*See also* Blockchain)
  Byzantine Generals' Problem and, 44–45, 49–58, 62–63
  credit data and, 71–72
  of hot and cold wallets, 134–135
  regulation and, 5, 139–148
  of revealing personal information, 10
Sharing economy concept, 174–176
SHA-256 (Secure Hash Algorithm), 53, 81, *81*, 88
"Shelling out," 9
Shiller, Robert, 88
Shostak, Robert, 44–45, 50
Silk Road (website), 3
Simple Mail Transfer Protocol (SMTP), 151
60/40 portfolio model, 123–127, *125, 126*
Smart contracts, 17, 40
Smart money, 149–162
  Bitcoin as, 17–18
  cryptoequities and, 160–161
  decentralized autonomous organizations (DAO) and, 161–162
  Ethereum and, 155–160
  generally, 149–151
  protocols, 151–152
  smart contracts and smart property, 150, 152–155
Social networks
  Bitcoin as, 17–18
  Facebook and, 49
Society for Human Resource Management (SHRM), 173
Soros, George, 2, 92
S&P 500, 124
SPAM, deterring, 80
S&P Capital IQ, 150
Special Drawing Rights (SDRs), 119
Steffens, Lincoln, 176
Stone, Oliver, 175–176
Store of value, Bitcoin as, 13, 127
Szabo, Nick, 40, 153–154

TARP, 35
Tate, Jared, 97, 98
Taxes
  IRS and guidance on digital currency, 141
  New York tax-free zones, 146–147
  using digital currency for, 128–129
Thiel, Peter, 7, 156
Thomas, Stefan, 37
Three Generic Strategies, 172–173, *173*
Times of London, 38
Two Generals' Problem, 50–52

United Kingdom, currency peg failure in, 92–94
United States, digital currency regulation in, 141–148
Unit of account, Bitcoin as, 13, 127
University of California–Berkeley, 159
U.S. Department of Commerce, 70
U.S. dollar
  early history of, 91–92
  gold standard and, 121–123, 137
U.S. Treasury, 35

Valuation, of digital currencies, 129–133, *131, 132, 133*
Vault, for bitcoins, 27
Vietnam, digital currency regulation in, 140–141
Volcker, Paul, 45
Voorhees, Erik, 142

Wallets
  digital wallets, 4, 21, 134
  hot and cold wallets, 134–135
  public/private key pair, 24–25, 77–78, *78*
  software wallet and web wallet, defined, 26–29
Wall Street (film), 175–176
Wall Street Journal, 124
Walters, Alan, 93
Wampum, 9
"We Are All Bitcoin" (Garzik), 41–43
Wells Fargo, 21, 30, 61
Western Union, 61, 71
William III (King of England), 60–61
Wilson, Fred, 7
Winkelvoss ETF, 135
World Bank, creation of, 121

ZipCar, 174
Zuckerberg, Mark, 49