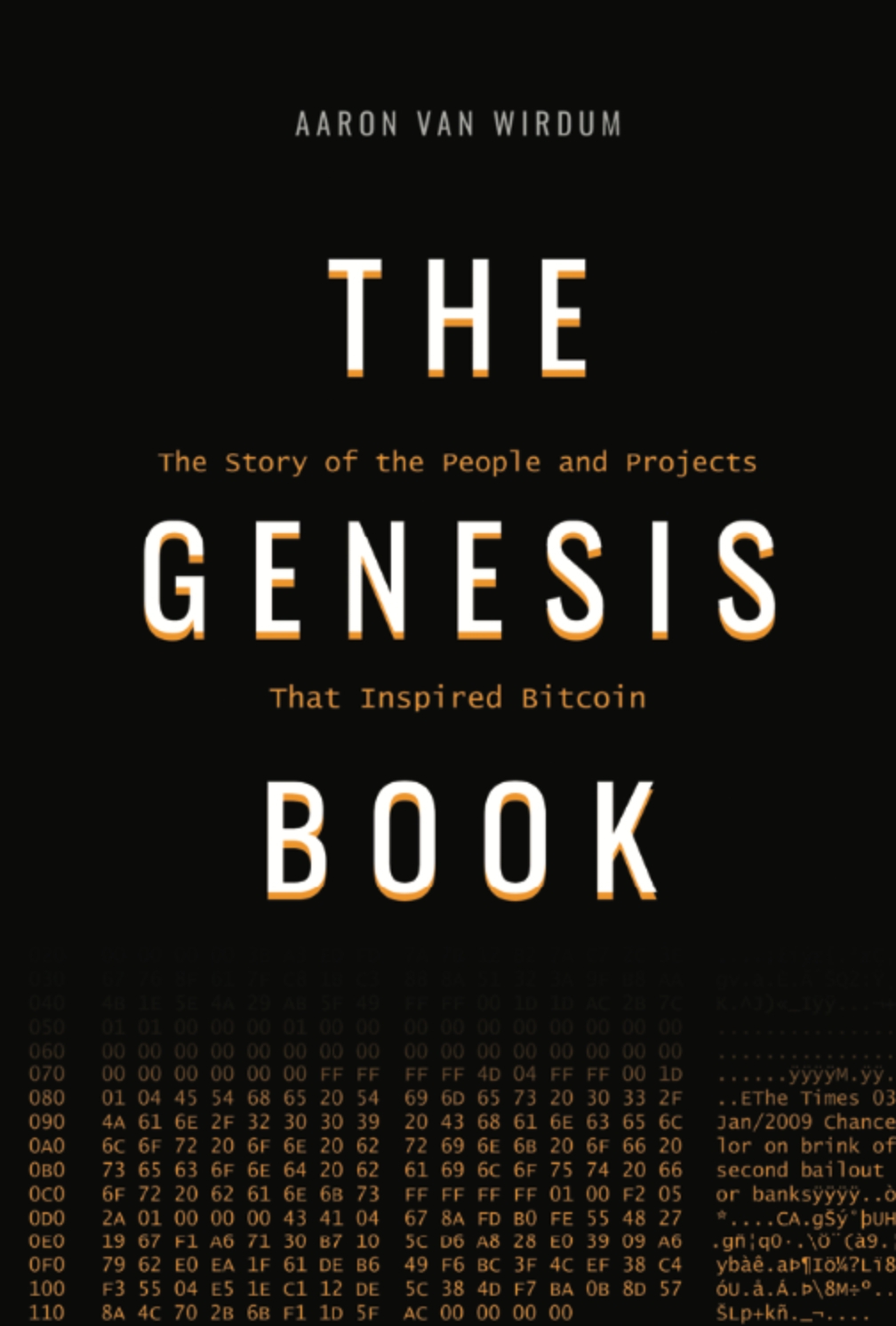
The Genesis Book: The Story of the People and Projects That Inspired Bitcoin

van Wirdum, Aaron

2024-01-15



## Endnotes

[[1]](../part0006.xhtml#a3AV)​Lawrence H. White, “The Troubling Suppression of Competition from Alternative Monies: The Cases of the Liberty Dollar and e-gold,” Cato Journal, 34, No. 2 (2014): 281–301.

[[2]](../part0006.xhtml#a324)​House of Representatives, “Deleting Commercial Pornography Sites From the Internet: The U.S. Financial Industry’s Efforts to Combat This Problem,” Hearing Before the Subcommittee on Oversight and Investigations of the Committee on Energy and Commerce, One Hundred Ninth Congress, Second Session, September 21, 2006, [https://www.govinfo.gov/content/pkg/CHRG-109hhrg31467/html/CHRG-109hhrg31467.htm.](https://www.govinfo.gov/content/pkg/CHRG-109hhrg31467/html/CHRG-109hhrg31467.htm)

[[3]](../part0006.xhtml#a33B)​White, “Troubling Suppression,” 289.

[[4]](../part0006.xhtml#a2PD)​e-gold, “e-gold News,” December 1999, accessed via [https://web.archive.org/web/20001209053900fw\_/http://www.e-gold.com/news.html.](https://web.archive.org/web/20001209053900fw_/http:/www.e-gold.com/news.html)

[[5]](../part0006.xhtml#a34Y)​e-gold, “e-gold® Welcomes US Government Review of its Status as a Privately Issued Currency,” January 20, 2006, accessed via [https://web.archive.org/web/20060304203618if\_/http://www.e-gold.com:80/letter2.html.](https://web.archive.org/web/20060304203618if_/http:/www.e-gold.com:80/letter2.html)

[[6]](../part0006.xhtml#a2TN)​US Department of Justice, “Digital Currency Business e-gold Pleads Guilty to Money Laundering and Illegal Money Transmitting Charges,” July 21, 2008, [https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html.](https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html)

[[7]](../part0006.xhtml#a2UA)​e-gold “Transcript of sentence before the honorable Rosemary M. Collyer United States District Judge,” 114, November 20, 2008, <https://legalupdate.e-gold.com/2008/11/transcript-of-sentence-before-the-honorable-rosemary-m-collyer-united-states-district-judge.html>

[[8]](../part0008.xhtml#a3CJ)​Deirdre N. McCloskey, How to be Human\*– \*Though an Economist (Ann Arbor: The University of Michigan Press, 2000), 33.

[[9]](../part0008.xhtml#a3DM)​Lawrence H. Officer, “Exchange Rates Between the United States Dollar and Forty-one Currencies,” MeasuringWorth, 2023.

[[10]](../part0008.xhtml#a370)​Eamonn Butler, Hayek: His Contribution to the Political and Economic Thought of Our Time (New York: Universe Books, 2010).

[[11]](../part0008.xhtml#a2Y4)​Bruce Caldwell and Hansjoerg Klausinger, Hayek: A Life, 1899–1950 (Chicago: University of Chicago Press, 2022), Chs. 6–9.

[[12]](../part0008.xhtml#a3GE)​Ludwig von Mises, The Historical Setting of the Austrian School of Economics (New Rochelle, NY: Arlington House, 1969), 12.

[[13]](../part0008.xhtml#a3GZ)​Mises, Historical Setting, 12–13, 19–20.

[[14]](../part0008.xhtml#a39Y)​Ludwig von Mises, Human Action: A Treatise on Economics, The Scholar’s Edition (Auburn, AL: Ludwig von Mises Institute, 1998), 21, 38–54.

[[15]](../part0008.xhtml#a3D8)​Carl Menger, Untersuchungen über die Methode der Sozialwissenschaften und der Politischen Oekonomie insbesondere (Leipzig: Dunker und Humblot, 1883).

[[16]](../part0008.xhtml#a39E)​Mises, Historical Setting, 3–19.

[[17]](../part0008.xhtml#a2TW)​Ludwig von Mises, Economic Calculation in the Socialist Commonwealth (Auburn, AL: Ludwig von Mises Institute, 2012).

[[18]](../part0008.xhtml#a3F4)​Although this argument has indeed been made in the context of consumer goods (as it has been in this text), a more precise articulation of this argument—as fleshed out over subsequent economic debates—is that this applies especially to capital goods.

[[19]](../part0008.xhtml#a3CK)​Mises, Economic Calculation, 18.

[[20]](../part0008.xhtml#a3CA) Friedrich A. Hayek, Prices and Production (New York: Augustus M. Kelly, Publishers, 1967).

[[21]](../part0008.xhtml#a3GF) Friedrich A. Hayek, “The Use of Knowledge in Society,” American Economic Review. XXXV, No. 4 (1945): 526–27.

[[22]](../part0008.xhtml#a2S2)​If person A deposits $100 into the bank, and the bank loans out $90 of this $100 to person B, person A will still think he or she has $100 while person B will have $90, for a total of $190. What’s more, if person B deposits the $90 in the bank again (or perhaps a different bank), and the bank loans out $81 of these $90 to person C, three people will think they own a combined $271. This can go on and on, seemingly bringing more and more money into circulation. This concept is referred to as the “money multiplier.” And in actuality, the money multiplier can be even more aggressive than this conventional fractional reserve example suggests, because banks don’t need to first receive deposits before they can issue loans; they can issue loans simply by creating it as credit in customers’ bank accounts.

[[23]](../part0008.xhtml#a3EW) Gary Richardson and Tim Sablik, “Banking Panics of the Gilded Age: 1863–1913,” Federal Reserve History, December 4, 2015, [https://www.federalreservehistory.org/essays/banking-panics-of-the-gilded-age.](https://www.federalreservehistory.org/essays/banking-panics-of-the-gilded-age)

[[24]](../part0008.xhtml#a37K)​Friedrich A. Hayek, “Monetary Policy in the United States after the Recovery from the Crisis of 1920,” in The Collected Works of F.A. Hayek, Good Money: part I, ed. Stephen Kresge (Indianapolis, IN: Liberty Fund, 2009), 145.

[[25]](../part0008.xhtml#a39G)​Hayek, “Monetary Policy,” 146.

[[26]](../part0008.xhtml#a3DA) Stephen Kresge, The Collected Works of F.A. Hayek, Good Money: part I (Indianapolis, IN: Liberty Fund, 2009), 13.

[[27]](../part0008.xhtml#a36V)​Most expansively (though not exclusively) outlined in John Maynard Keynes, The General Theory of Employment, Interest and Money (London: Palgrave Macmillan, 1936).

[[28]](../part0008.xhtml#a34H)​George Selgin, “The New Deal and Recovery, Part 15: The Keynesian Myth,” Cato Institute, March 16, 2022, [https://www.cato.org/blog/new-deal-recovery-part-15-keynesian-myth.](https://www.cato.org/blog/new-deal-recovery-part-15-keynesian-myth)

[[29]](../part0008.xhtml#a3AR)​Friedrich A. Hayek, “The Gold Problem,” in The Collected Works of F.A. Hayek, Good Money: part I, ed. Stephen Kresge (Indianapolis, IN: Liberty Fund, 2009), 184.

[[30]](../part0009.xhtml#a39B) Richard Stallman, “Richard Stallman: High School Misfit, Symbol of Free Software, MacArthur-Certified Genius.” Interview by Michael Gross, mgross.com, 1999, [https://www.mgross.com/writing/books/my-generation/bonus-chapters/richard-stallman-high-school-misfit-symbol-of-free-software-macarthur-certified-genius/.](https://www.mgross.com/writing/books/my-generation/bonus-chapters/richard-stallman-high-school-misfit-symbol-of-free-software-macarthur-certified-genius/)

[[31]](../part0009.xhtml#a2RA)​This section (as well as some other parts of this chapter) is largely based on Steven Levy, Hackers: Heroes of the Computer Revolution (Sebastopol, CA: O’Reilly, 2010).

[[32]](../part0009.xhtml#a32X)​Richard Stallman, “Talking to the Mailman,” Interview by Rob Lucas, New Left Review, Sept–Oct 2018, [https://newleftreview.org/issues/ii113/articles/richard-stallman-talking-to-the-mailman.](https://newleftreview.org/issues/ii113/articles/richard-stallman-talking-to-the-mailman)

[[33]](../part0009.xhtml#a2WT)​Richard Stallman, “RMS Berättar,” Linköping University, [http://www.lysator.liu.se/history/garb/txt/87-2-rms.txt.](http://www.lysator.liu.se/history/garb/txt/87-2-rms.txt)

[[34]](../part0009.xhtml#a33K)​Stallman, “Talking to the Mailman.”

[[35]](../part0009.xhtml#a2P8)​Levy, Hackers, 448.

[[36]](../part0009.xhtml#a3F1)​Levy, Hackers, 472.

[[37]](../part0009.xhtml#a2W3)​Stallman, “High School Misfit.”

[[38]](../part0009.xhtml#a34P)​Stallman, “RMS Berättar.”

[[39]](../part0009.xhtml#a2RP)​Steven Levy, Hackers, 441–42.

[[40]](../part0009.xhtml#a37V)​Angela Watercutter, “Why Free Software Is More Important Now Than Ever Before,” Wired, September 20, 2013, [https://www.wired.com/2013/09/why-free-software-is-more-important-now-than-ever-before/.](https://www.wired.com/2013/09/why-free-software-is-more-important-now-than-ever-before/)

[[41]](../part0009.xhtml#a3EP)​For the sake of accuracy, it should be noted that this part of the argument technically only came to prominence when Stallman launched the GNU project a year-or-so later; it hadn’t yet been part of his original motivation to start the project in the first place. This minor anachronism was left in the text for the purpose of readability.

[[42]](../part0009.xhtml#a2Y5)​Richard Stallman, “Free Software Is Even More Important Now,” gnu.org, [https://www.gnu.org/philosophy/free-software-even-more-important.en.html.](https://www.gnu.org/philosophy/free-software-even-more-important.en.html)

[[43]](../part0009.xhtml#a3CD)​GNU Operating System, “What is Free Software?” [https://www.gnu.org/philosophy/free-sw.html.](https://www.gnu.org/philosophy/free-sw.html)

[[44]](../part0009.xhtml#a2Z0) ​Actually, freedom 0 was only explicitly added in the 1990s; before that, Stallman thought that it was an automatic legal consequence of the original three freedoms.

[[45]](../part0009.xhtml#a2T4)​GNO Operating System, “What is Free Software?”

[[46]](../part0009.xhtml#a32K)​Richard Stallman, “Free Unix!” September 27, 1983, [https://www.gnu.org/gnu/initial-announcement.en.html.](https://www.gnu.org/gnu/initial-announcement.en.html)

[[47]](../part0009.xhtml#a3BB)​GNU Operating System, “The GNU Manifesto,” 1985,​[https://www.gnu.org/gnu/manifesto.html.en.](https://www.gnu.org/gnu/manifesto.html.en)

[[48]](../part0009.xhtml#a37U) ​To emphasize the project’s heavy reliance on GNU, some (including Richard Stallman) prefer to call it “GNU/Linux.”

[[49]](../part0009.xhtml#a2P3)​Eric S. Raymond, The Cathedral & The Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary (Sebastopol, CA: O’Reilly, 2001).

[[50]](../part0009.xhtml#a2WV)​Richard Stallman is not a fan of this terminology either. If a term to include both sides of the schism must be used, he prefers “Free/Libre and Open Source Software” because it more clearly conveys that the “free” part is about “freedom.”

[[51]](../part0009.xhtml#a2X4)​Raymond, The Cathedral & The Bazaar, 52.

[[52]](../part0009.xhtml#a2ZC)​Raymond, The Cathedral & The Bazaar, 52.

[[53]](../part0009.xhtml#a342)​Raymond, The Cathedral & The Bazaar, 52.

[[54]](../part0010.xhtml#a309) ​Ludwig von Mises, The Theory of Money and Credit, trans. J.E. Batson (New Haven, CT: Yale University Press, 1953).

[[55]](../part0010.xhtml#a36G)​This is sometimes considered “intrinsic value,” which is a common expression in economics to signify that a good has economic use value apart from its monetary role. Austrians generally reject the idea that products actually have intrinsic value at all, however: value is always subjective.

[[56]](../part0010.xhtml#a3CG)​More recent archeological research published in David Graeber’s Debt: The First 5,000 Years (New York: Melville House, 2011), suggests that there was never a pure barter economy as described in the regression theorem. Instead, the oldest human civilizations used debt as their first currency. However, debt only works as currency in high-trust, reputation-based environments. In low-trust environments, gold was often the currency of choice, and it’s entirely feasible that the precious metal garnered this status over time through a process resembling what is described in the regression theorem.

[[57]](../part0010.xhtml#a3EF)​Nicholas Dimsdale, “British Monetary Policy and the Exchange Rate 1920-1938,” Oxford Economic Papers 33, New Series (Jul. 1981): 307–49.

[[58]](../part0010.xhtml#a3GJ)​Irving Fisher, The Purchasing Power of Money (New York: The Macmillan Company, 1920).

[[59]](../part0010.xhtml#a32J)​John Maynard Keynes, A Tract on Monetary Reform (London: Macmillan and Co, 1923), 173.

[[60]](../part0010.xhtml#a3DY)​Friedrich A. Hayek, “Intertemporal Price Equilibrium and Movements in the Value of Money,” in The Collected Works of F.A. Hayek, Good Money: part I, ed. Stephen Kresge (Indianapolis, IN: Liberty Fund, 2009), 195.

[[61]](../part0010.xhtml#a2ZJ)​Hayek, “Intertemporal Price Equilibrium,” 207.

[[62]](../part0010.xhtml#a38F)​Hayek, “Intertemporal Price Equilibrium,” 190.

[[63]](../part0010.xhtml#a3D4)​Hayek, “Intertemporal Price Equilibrium,” 214.

[[64]](../part0010.xhtml#a31G)​Keynes, Tract, 164.

[[65]](../part0010.xhtml#a2NV)​Friedrich A. Hayek, “Monetary Nationalism and International Stability,” in The Collected Works of F.A. Hayek, Good Money: part II, ed. Stephen Kresge (Indianapolis, IN: Liberty Fund, 2009): 55.

[[66]](../part0010.xhtml#a323)​Hayek, “Monetary Nationalism,” 55–56.

[[67]](../part0010.xhtml#a39J)​Hayek, “Intertemporal Price Equilibrium,” 212.

[[68]](../part0010.xhtml#a2YA)​Hayek, “Intertemporal Price Equilibrium,” 217.

[[69]](../part0010.xhtml#a3E6)​Hayek, “Monetary Nationalism,” 87.

[[70]](../part0010.xhtml#a3E9)​Nicholas Wapshott, Keynes Hayek: The Clash That Defined Modern Economics (New York: Norton, 2011): 159.

[[71]](../part0010.xhtml#a31S)​Franklin D. Roosevelt, “Relating to the Hoarding, Export, and Earmarking of Gold Coin, Bullion, or Currency and to Transactions in Foreign Exchange,” August 28, 1993, available via The American Presidency Project.

[[72]](../part0010.xhtml#a3DV) ​James Rickards, Currency Wars: The Making of the Next Global Crisis (New York: Portfolio 2012), 56–77.

[[73]](../part0011.xhtml#a396) ​Much of this chapter is based on Steven Levy’s Crypto: How the Code Rebels Beat the Government–Saving Privacy in the Digital Age (New York: Viking, 2001).

[[74]](../part0011.xhtml#a2ZT) Whitfield Diffie and Martin E. Hellman, “Multiuser Cryptographic Techniques,” AFIPS '76: Proceedings of the June 7-10, 1976, national computer conference and exposition (June 1976): 109–112.

[[75]](../part0011.xhtml#a2Z2)​Levy, Crypto, 76.

[[76]](../part0011.xhtml#a2SX)​Whitfield Diffie and Martin E. Hellman, “New Directions in Cryptography,” IEEE Transactions On Information Theory, vol. IT-22, no. 6 (November 1976): 644.

[[77]](../part0011.xhtml#a3CB) Steven Levy, “E-Money (That’s What I Want),” Wired, December 1, 1994, [https://www.wired.com/1994/12/emoney/.](https://www.wired.com/1994/12/emoney/)

[[78]](../part0011.xhtml#a3FS) David Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms,” Communications of the ACM 24, 2 (February 1981): 84–90.

[[79]](../part0012.xhtml#a384)​Edward S. Mason and Robert E. Asher, The World Bank Since Bretton Woods: The Origins, Policies, Operations and Impact of the International Bank for Reconstruction (Washington, DC: Brookings Institution, 1973), 29.

[[80]](../part0012.xhtml#a2XN)​Andrew F. Brimmer, “Remembering William McChesney Martin Jr.,” Federal Reserve Bank of Minneapolis, September 1, 1998, [https://www.minneapolisfed.org/article/1998/remembering-william-mcchesney-martin-jr.](https://www.minneapolisfed.org/article/1998/remembering-william-mcchesney-martin-jr)

[[81]](../part0012.xhtml#a341)​Wapshott, Keynes Hayek, 242.

[[82]](../part0012.xhtml#a2WB)​Wapshott, Keynes Hayek, 242.

[[83]](../part0012.xhtml#a3AZ)​Richard Nixon, “Address to the Nation Outlining a New Economic Policy: ‘The Challenge of Peace’,” August 15, 1971.

[[84]](../part0012.xhtml#a39D)​Michael J. Graetz and Olivia Briffault, “A ‘Barbarous Relic’: The French, Gold, and the Demise of Bretton Woods,” in The Bretton Woods Agreements, eds. Naomi Lamoreaux and Ian Shapiro (New Haven: Yale University Press, 2019): 121–142.

[[85]](../part0012.xhtml#a2S5) Federal Reserve Economic Data, “Consumer Price Index for All Urban Consumers,” available via [https://fred.stlouisfed.org/series/CPIAUCSL.](https://fred.stlouisfed.org/series/CPIAUCSL)

[[86]](../part0012.xhtml#a2VH)​Friedrich A. Hayek, “Can We Still Avoid Inflation?” in The Austrian Theory of the Trade Cycle and Other Essays, ed. Richard M. Ebeling (New York: Center for Libertarian Studies, 1978): 101.

[[87]](../part0012.xhtml#a3A4)​Mark Blaug, Economic Theory in Retrospect, 4th edition (Cambridge: Cambridge University Press, 1985), 20–23.

[[88]](../part0012.xhtml#a37B)​Hayek, Prices and Production, 203.

[[89]](../part0012.xhtml#a3ES)​Hayek, “Can We Still Avoid Inflation?” 108.

[[90]](../part0012.xhtml#a2US) Friedrich A. Hayek, Denationalisation of Money (London: The Institute of Economic Affairs, 1976), 89.

[[91]](../part0012.xhtml#a322)​Hayek, Denationalisation of Money, 91.

[[92]](../part0012.xhtml#a2PX)​Friedrich A. Hayek, Denationalisation of Money: The Argument Refined (London: The Institute of Economic Affairs, 1990), 13.

[[93]](../part0012.xhtml#a34X)​Republished in Friedrich A. Hayek, Choice in Currency: A Way to Stop Inflation (London: The Institute of Economic Affairs, 1976).

[[94]](../part0012.xhtml#a2WH)​Hayek, The Argument Refined, 78.

[[95]](../part0012.xhtml#a2Z6)​Hayek, The Argument Refined, 83.

[[96]](../part0012.xhtml#a2SK)​Hayek, The Argument Refined, 109.

[[97]](../part0012.xhtml#a3C7)​Hayek, The Argument Refined, 77.

[[98]](../part0012.xhtml#a34T)​Hayek,The Argument Refined, 133.

[[99]](../part0012.xhtml#a38A)​Hayek, The Argument Refined, 93.

[[100]](../part0012.xhtml#a3DF) Hayek, The Argument Refined, 134.

[[101]](../part0013.xhtml#a2X0) David Chaum, “Security Without Identification: Transaction Systems to Make Big Brother Obsolete,” Communications of the ACM 28, no. 10 (October 1985): 1030–1044.

[[102]](../part0013.xhtml#a2U7) David Chaum, “Achieving Electronic Privacy,” Scientific American 267, 2 (August 1992): 96–101.

[[103]](../part0013.xhtml#a3BF) David Chaum, “Blind Signatures for Untraceable Payments,” Advances in Cryptology: Proceedings of Crypto 82 (Boston: Springer, 1983): 199–203.

[[104]](../part0013.xhtml#a38U) Chaum would later also propose a solution where double-spending could de-anonymize the perpetrator, somewhat limiting the need to immediately check each incoming payment against the bank’s records since the perpetrator of a double-spend attack can be identified.

[[105]](../part0013.xhtml#a2Z9) As a nifty extra detail, the system also embeds a type of fraud prevention check—albeit one that comes at the expense of privacy if and when users would opt to use it. If Carol would falsely claim that she’d never been paid, Bob could choose to reveal the nonce to Alice Bank, proving that he created the digital dollars that Carol deposited, proving that he paid them to her.

[[106]](../part0013.xhtml#a3DS) That said, there are some other, perhaps more drastic measures that Alice Bank could have taken. Besides refusing to issue digital dollars to Bob in the first place, she could have also blocked all electronic cash payments. Similarly, she could block particular users from accepting payments; even if payments can’t be traced, some users can still be excluded from participation in the system.

[[107]](../part0013.xhtml#a36Y) It can (and has) been argued that Chaum did use a rather loose definition of “cash,” as cash typically has more distinguishing properties. Chaum’s form of digital cash for example offered limited person-to-person transferability—a feature that physical cash does have, as it can freely be passed around. Regardless, Chaum invented a form of digital money that at least offered a similar level of privacy as physical cash, which was his main objective.

[[108]](../part0013.xhtml#a39C) David Chaum, “Security Without Identification.”

[[109]](../part0013.xhtml#a37Y) In the end, the toll project was not adopted: the idea proved to be too controversial in the Netherlands. However, the technology would later be licensed under the name “DyniCash” to a Dallas-based company that specialized in microwave-frequency communication for trains.

[[110]](../part0013.xhtml#a3CZ) Peter H. Lewis, “Attention Internet Shoppers: E-Cash Is Here,” The New York Times, October 19, 1994, [https://www.nytimes.com/1994/10/19/business/attention-internet-shoppers-e-cash-is-here.html.](https://www.nytimes.com/1994/10/19/business/attention-internet-shoppers-e-cash-is-here.html)

[[111]](../part0013.xhtml#a2X9) DigiCash, “Bank Austria and Den norske Bank to Issue ecash™ the Electronic Cash for the Internet,” DigiCash, April 14, 1997, accessed via [https://web.archive.org/web/19970605025912/http://www.digicash.com:80/publish/ec\_pres8.html.](https://web.archive.org/web/19970605025912/http:/www.digicash.com:80/publish/ec_pres8.html)

[[112]](../part0013.xhtml#a2PR) DigiCash, “Advance Bank First to Provide DigiCash’s ecash™ System in Australia,” DigiCash, October, 1996, accessed via [https://web.archive.org/web/19961102121407/https://www.digicash.com/publish/ec\_pres6.html.](https://web.archive.org/web/19961102121407/https:/www.digicash.com/publish/ec_pres6.html)

[[113]](../part0013.xhtml#a3AS) DigiCash, “DigiCash’s Ecash™ to be Issued by Deutsche Bank,” DigiCash, May 7, 1996, accessed via [https://web.archive.org/web/19961102121355/https://www.digicash.com/publish/ec\_pres5.html.](https://web.archive.org/web/19961102121355/https:/www.digicash.com/publish/ec_pres5.html)

[[114]](../part0013.xhtml#a3GG) Jeffrey Kutler, “Credit Suisse, Digicash in E-Commerce Test,” American Banker, June 16, 1998, [https://www.americanbanker.com/news/credit-suisse-digicash-in-e-commerce-test.](https://www.americanbanker.com/news/credit-suisse-digicash-in-e-commerce-test)

[[115]](../part0013.xhtml#a2WF) Next! Magazine “Hoe DigiCash alles verknalde,” Next!, January 1999, accessed via [https://web.archive.org/web/19990427142412/https://www.nextmagazine.nl/ecash.htm.](https://web.archive.org/web/19990427142412/https:/www.nextmagazine.nl/ecash.htm)

[[116]](../part0013.xhtml#a3FZ) American Banker, “Digicash Sends Signal by Hiring Visa Veteran,” American Banker, May 6, 1997, [https://www.americanbanker.com/news/digicash-sends-signal-by-hiring-visa-veteran.](https://www.americanbanker.com/news/digicash-sends-signal-by-hiring-visa-veteran)

[[117]](../part0013.xhtml#a3CW) Julie Pitta, “Requiem for a Bright Idea,” Forbes, November 1, 1999, [https://www.forbes.com/forbes/1999/1101/6411390a.html.](https://www.forbes.com/forbes/1999/1101/6411390a.html)

[[118]](../part0013.xhtml#a32P) Hash functions were first proposed by University of Illinois at Urbana–Champaign mathematician George B. Purdy in his paper “A High Security Log-in Procedure,” Communications of the ACM 17, no. 8 (August 1974): 442–445.

[[119]](../part0013.xhtml#a2SF) Scott Stornetta, “The Missing Link between Satoshi & Bitcoin: Cypherpunk Scott Stornetta,” interview by Naomi Brockwell, NBTV, with Naomi Brockwell, YouTube, September 6, 2018, [https://youtu.be/fYr-keVOQ18.](https://youtu.be/fYr-keVOQ18)

[[120]](../part0013.xhtml#a2V8) Stuart Haber and Scott W. Stornetta, “How to Time-Stamp a Digital Document,” Journal of Cryptology 3 (1991): 99–111.

[[121]](../part0013.xhtml#a2V4) Ralph C. Merkle, “A Certified Signature,” Advances in Cryptology—CRYPTO ’89: Proceedings (1989): 218–238. (Although the article was only published in 1989, Markle wrote the paper in 1979.)

[[122]](../part0013.xhtml#a2WN) Dave Bayer, Stuart Haber and Scott W. Stornetta, “Improving the Efficiency and Reliability of Digital Time-Stamping,” Conference Paper, Sequences II: Methods in Communication, Security, and Computer Science (1993): 329–34.

[[123]](../part0013.xhtml#a2UD) Stuart Haber and Scott W. Stornetta, “Secure Names for Bit-strings,” CCS ’97: Proceedings of the 4th ACM Conference on Computer and Communications Security, (April 1997): 28–35.

[[124]](../part0014.xhtml#a35B) Ed Regis, “Meet the Extropians,” Wired, October 1, 1994, [https://www.wired.com/1994/10/extropians/.](https://www.wired.com/1994/10/extropians/)

[[125]](../part0014.xhtml#a2XB) Douglas Martin, “Futurist Known as FM-2030 Is Dead at 69,” The New York Times, July 11, 2000, [https://www.nytimes.com/2000/07/11/us/futurist-known-as-fm-2030-is-dead-at-69.html.](https://www.nytimes.com/2000/07/11/us/futurist-known-as-fm-2030-is-dead-at-69.html)

[[126]](../part0014.xhtml#a3DC) K. Eric Drexler, Engines of Creation (New York: Doubleday, 1986), 146.

[[127]](../part0014.xhtml#a31R) Max More, “Transhumanism: Towards a Futurist Philosophy,” maxmore.com, accessed via [https://web.archive.org/web/20051029125153/http://www.maxmore.com/transhum.htm.](https://web.archive.org/web/20051029125153/http:/www.maxmore.com/transhum.htm)

[[128]](../part0014.xhtml#a2RH) Max More, “The Extropian Principles: A Transhumanist Declaration,” maxmore.com, accessed via [https://web.archive.org/web/20090130143449/https://www.maxmore.com/extprn3.htm.](https://web.archive.org/web/20090130143449/https:/www.maxmore.com/extprn3.htm)

[[129]](../part0014.xhtml#a30E) The American Food and Drug Administration (FDA) was a particularly restrictive example; the federal agency made tinkering with and trying out new types of drugs and medicine all but impossible.

[[130]](../part0014.xhtml#a3C4) More, “Extropian Principles.”

[[131]](../part0014.xhtml#a2X2) Much of this section is based on Finn Brunton’s Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Built Cryptocurrency (Princeton, NJ: Princeton University Press, 2019), 118–134.

[[132]](../part0014.xhtml#a3GV) Max More, “Transhumanism.”

[[133]](../part0014.xhtml#a37F) Don Lavoie, Howard Baetjer, and William Tulloh, “High-Tech Hayekians: Some Possible Research Topics in the Economics of Computation,” Market Process 8 (Spring 1990): 119–146.

[[134]](../part0014.xhtml#a2XU) E.g., Phil Salin, “Costs and Computers,” Release 1.0 (November 25, 1991): 5–18; Phil Salin, “The Ecology of Decisions, or ‘An Inquiry into the Nature and Causes of the Wealth of Kitchens’,” Market Process 8 (Spring 1990): 91–114.

[[135]](../part0014.xhtml#a2VD) Facilities include Alcor and the Cryonics Institute (both in the US), Kriorus (Russia), Tomorrow Bio (Germany), and Yinfeng Biological Group (China).

[[136]](../part0014.xhtml#a2SW) Hal Finney, “Protecting Privacy with Electronic Cash,” Extropy 10 (Winter/Spring 1993): 14.

[[137]](../part0014.xhtml#a327) Mark Grant, “Introduction to Digital Cash,” Extropy 15 (2nd–3d Quarter 1995): 15.

[[138]](../part0014.xhtml#a3ER) Eric Watt Forste, “The Theory of Free Banking (George A. Selgin),” Extropy 15 (2nd–3d Quarter 1995): 53.

[[139]](../part0014.xhtml#a2PK) Lawrence H. White, “Thoughts on the Economics of ‘Digital Currency’.” Extropy 15 (2nd–3d Quarter 1995): 18.

[[140]](../part0014.xhtml#a3CT) Max More, “Hayek’s Denationalisation of Money,” Extropy 15 (2nd–3d Quarter 1995): 20.

[[141]](../part0014.xhtml#a2VS) More, “Hayek’s Denationalisation of Money,” 20.

[[142]](../part0016.xhtml#a2U4) Tim May, “Untraceable Digital Cash, Information Markets, and BlackNet (‘Governmental and Social Implications of Digital Money’ panel at CFP ‘97),” The Computers Freedom & Privacy Conference (1997), accessed via [https://web.archive.org/web/20130501134401/https://osaka.law.miami.edu/~froomkin/articles/tcmay.htm.](https://web.archive.org/web/20130501134401/https:/osaka.law.miami.edu/~froomkin/articles/tcmay.htm)

[[143]](../part0016.xhtml#a345) Tim May, “The Cyphernomicon,” originally distributed through the Cypherpunks mailing list, September 10, 1994, available via [https://nakamotoinstitute.org/static/docs/cyphernomicon.txt.](https://nakamotoinstitute.org/static/docs/cyphernomicon.txt)

[[144]](../part0016.xhtml#a2VE) Hal Finney, “Chaum on the wrong foot?” originally sent to the Cypherpunks mailing list, August 22, 1993 available via [https://cypherpunks.venona.com/date/1993/08/msg00652.html.](https://cypherpunks.venona.com/date/1993/08/msg00652.html)

[[145]](../part0016.xhtml#a350) Eric Hughes, “A Cypherpunk’s Manifesto,” originally sent to the Cypherpunks mailing list, March 17, 1993, available via [https://cypherpunks.venona.com/date/1993/03/msg00392.html.](https://cypherpunks.venona.com/date/1993/03/msg00392.html)

[[146]](../part0016.xhtml#a2ZK) Tim May, “Degrees of Freedom,” originally sent to the Cypherpunks mailing list, February 8, 1996, available via [https://cypherpunks.venona.com/date/1996/02/msg00637.html.](https://cypherpunks.venona.com/date/1996/02/msg00637.html)

[[147]](../part0016.xhtml#a3FR) Tim May, “‘Who shall speak for us?’,” originally sent to the Cypherpunks mailing list, Available via [https://cypherpunks.venona.com/date/1995/09/msg02189.html.](https://cypherpunks.venona.com/date/1995/09/msg02189.html)

[[148]](../part0016.xhtml#a2PN) The title and text was a bit of a parody of Karl Marx’s and Friedrich Engels’s Communist Manifesto, while the term crypto-anarchy is something of a pun referring to crypto-fascism, the secret support for fascism.

[[149]](../part0016.xhtml#a33P) Tim May, “The Crypto Anarchist Manifesto,” originally sent to the Cypherpunks mailing list, November 22, 1992, available via [https://cypherpunks.venona.com/date/1992/11/msg00204.html.](https://cypherpunks.venona.com/date/1992/11/msg00204.html)

[[150]](../part0016.xhtml#a2TH) Tim May, “Libertaria in Cyberspace,” originally sent to the Cypherpunks mailing list, August 9, 1993, accessed via [https://cypherpunks.venona.com/date/1993/08/msg00168.html.](https://cypherpunks.venona.com/date/1993/08/msg00168.html)

[[151]](../part0016.xhtml#a3GT) Tim May, “Cyberspace, Crypto Anarchy, and Pushing Limits,” originally sent to the Cypherpunks mailing list, April 3, 1994, accessed via [https://cypherpunks.venona.com/date/1994/04/msg00096.html.](https://cypherpunks.venona.com/date/1994/04/msg00096.html)

[[152]](../part0016.xhtml#a2V0) Tim May, “Hayek (was: Cato Institute conference on Net-regulation),” originally sent to the Cypherpunks mailing list, August 27, 1996, Accessed via [http://cypherpunks.venona.com/date/1996/08/msg02102.html.](http://cypherpunks.venona.com/date/1996/08/msg02102.html) As a funny aside, Tim May concluded a different email with a compliment to one of his fellow Cypherpunks: “I just want to end on a positive note before leaving for the holidays (the birthday of my savior, F. Hayek, of course).” See: Tim May, “Re: The War on Some Money [long],” originally sent to the Cypherpunks mailing list, December 21, 1995, accessed via [https://cypherpunks.venona.com/date/1995/12/msg01044.html.](https://cypherpunks.venona.com/date/1995/12/msg01044.html)

[[153]](../part0016.xhtml#a2UM) Tim May, “‘Stopping Crime’ Necessarily Means Invasiveness,” originally sent to the Cypherpunks mailing list, October 17, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/10/msg01269.html.](https://cypherpunks.venona.com/date/1996/10/msg01269.html)

[[154]](../part0016.xhtml#a36H) Eric Hughes, “No digital coins (was: Chaum on the wrong foot?),” originally sent to the Cypherpunks mailing list, August 24, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00690.html.](https://cypherpunks.venona.com/date/1993/08/msg00690.html)

[[155]](../part0016.xhtml#a3EX) Tim May, “Crypto Activism and Respectability,” originally sent to the Cypherpunks mailing list, April 21, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/04/msg00400.html.](https://cypherpunks.venona.com/date/1993/04/msg00400.html)

[[156]](../part0016.xhtml#a33F) Tim May, “Opportunities in Cyberspace,” originally sent to the Cypherpunks mailing list, September 8, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/09/msg00140.html.](https://cypherpunks.venona.com/date/1993/09/msg00140.html)

[[157]](../part0016.xhtml#a3AF) Michelle Quinn, “The Cypherpunks Who Cracked Netscape,” San Francisco Chronicle, September 20, 1995, [https://people.eecs.berkeley.edu/~daw/press/iang/ian1.html.](https://people.eecs.berkeley.edu/~daw/press/iang/ian1.html)

[[158]](../part0016.xhtml#a38T) Tim May, “Re: Stalling the crypto legislation for 2-3 more years,” originally sent to the Cypherpunks mailing list, July 23, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/07/msg01245.html.](https://cypherpunks.venona.com/date/1994/07/msg01245.html)

[[159]](../part0017.xhtml#a3AG) Tim May, “Scenario for a Ban on Cash Transactions,” originally sent to the Cypherpunks mailing list, November 24, 1992, accessed via: [https://cypherpunks.venona.com/date/1992/11/msg00211.html.](https://cypherpunks.venona.com/date/1992/11/msg00211.html)

[[160]](../part0017.xhtml#a3AH) Tim May, “Scenario for a Ban.”

[[161]](../part0017.xhtml#a38G) Tim May, “Crypto Anarchy, the Government, and the National Information Infrastructure,” originally sent to the Cypherpunks mailing list, November 29, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/11/msg01106.html.](https://cypherpunks.venona.com/date/1993/11/msg01106.html)

[[162]](../part0017.xhtml#a2UF) Tim May, “DigiCash can use whatever currencies are valued,” originally sent to the Cypherpunks mailing list, May 4, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/05/msg00243.html.](https://cypherpunks.venona.com/date/1994/05/msg00243.html)

[[163]](../part0017.xhtml#a34R) Tim May, “Re: Hettinga’s e$yllogism,” originally sent to the Cypherpunks mailing list, June 28, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/06/msg01637.html.](https://cypherpunks.venona.com/date/1997/06/msg01637.html)

[[164]](../part0017.xhtml#a372) Tim May, “‘Stopping Crime’ Necessarily Means Invasiveness,” originally sent to the Cypherpunks mailing list, October 17, 1996, accessed via: [http://cypherpunks.venona.com/date/1996/10/msg01269.html.](http://cypherpunks.venona.com/date/1996/10/msg01269.html)

[[165]](../part0017.xhtml#a3AB) Tim May, “Untraceable Payments, Extortion, and Other Bad Things,” originally sent to the Cypherpunks mailing list, December 21, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/12/msg01468.html.](https://cypherpunks.venona.com/date/1996/12/msg01468.html)

[[166]](../part0017.xhtml#a2RW) Tim May, “‘Stopping Crime’.”

[[167]](../part0017.xhtml#a393) Douglas Barnes, “Re: cypherpunks digicash bank?,” originally sent to the Cypherpunks mailing list, October 8, 1995, accessed via:              [https://cypherpunks.venona.com/date/1995/10/msg00731.html.](https://cypherpunks.venona.com/date/1995/10/msg00731.html)

[[168]](../part0017.xhtml#a34M) Tim May, “Software Patents are Freezing Evolution of Products,” originally sent to the Cypherpunks mailing list, October 7, 1995, accessed via:              [https://cypherpunks.venona.com/date/1995/10/msg00685.html.](https://cypherpunks.venona.com/date/1995/10/msg00685.html)

[[169]](../part0017.xhtml#a37J) Eduard de Jong, “Electronic Money: From Cryptography and Smart Cards to Bitcoin and Beyond,” Fraunhofer SmartCard Workshop 2017 (2017).

[[170]](../part0017.xhtml#a3EA) Laurie Law, Susan Sabett, and Jerry Solinas, “How To Make a Mint: The Cryptography of Anonymous Electronic Cash,” National Security Agency Office of Information Security Research and Technology, Cryptology Division, June 18, 1996,              [https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm.](https://groups.csail.mit.edu/mac/classes/6.805/articles/money/nsamint/nsamint.htm)

[[171]](../part0017.xhtml#a30W) Hadon Nash, “Digital Gold,” originally sent to the Cypherpunks mailing list, August 24, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00698.html.](https://cypherpunks.venona.com/date/1993/08/msg00698.html)

[[172]](../part0017.xhtml#a35X) Hal Finney, “Digital Gold, a bearer instrument?,” originally sent to the Cypherpunks mailing list, August 26, 1993, accessed via: [https://cypherpunks.venona.com/date/1993/08/msg00788.html.](https://cypherpunks.venona.com/date/1993/08/msg00788.html)

[[173]](../part0017.xhtml#a38K) Black Unicorn, “DigiCash Announcement,” originally sent to the Cypherpunks mailing list, May 10, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/05/msg00616.html.](https://cypherpunks.venona.com/date/1994/05/msg00616.html)

[[174]](../part0017.xhtml#a2V6) Pr0duct Cypher, “Magic Money Digicash System,” originally sent to the Cypherpunks mailing list, February 4, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/02/msg00247.html.](https://cypherpunks.venona.com/date/1994/02/msg00247.html)

[[175]](../part0017.xhtml#a2WP) Perry E. Metzger, “Re: Virtual Cash,” originally sent to the Cypherpunks mailing list, May 3, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/05/msg00131.html.](https://cypherpunks.venona.com/date/1994/05/msg00131.html)

[[176]](../part0017.xhtml#a3BT) Robert Hettinga, “Re: digital cc transactions, digital checks vs real digital cash,” originally sent to the Cypherpunks mailing list, May 3, 1997, accessed via: <https://cypherpunks.venona.com/date/1997/05/msg00147.html>

[[177]](../part0017.xhtml#a2TA) Robert Hettinga, “Re: Bypassing the Digicash Patents,” originally sent to the Cypherpunks mailing list, April 29, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/04/msg00811.html.](https://cypherpunks.venona.com/date/1997/04/msg00811.html)

[[178]](../part0017.xhtml#a30C) Tim May, “Re: alternative b-money creation,” originally sent to the Cypherpunks mailing list, December 11, 1998, accessed via: [https://cypherpunks.venona.com/date/1998/12/msg00455.html.](https://cypherpunks.venona.com/date/1998/12/msg00455.html)

[[179]](../part0017.xhtml#a3B3) Tim May, “What backs up digital money?,” originally sent to the Cypherpunks mailing list, March 27, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/03/msg01576.html.](https://cypherpunks.venona.com/date/1996/03/msg01576.html)

[[180]](../part0017.xhtml#a35K) Adam Back, “Re: Bypassing the Digicash Patents,” originally sent to the Cypherpunks mailing list, April 30, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/04/msg00822.html.](https://cypherpunks.venona.com/date/1997/04/msg00822.html)

[[181]](../part0017.xhtml#a2RM) Adam Back, “digital cc transactions, digital checks vs real digital cash,” originally sent to the Cypherpunks mailing list, May 2, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/05/msg00104.html.](https://cypherpunks.venona.com/date/1997/05/msg00104.html)

[[182]](../part0017.xhtml#a305) Adam Back, “Re: Bypassing.”

[[183]](../part0018.xhtml#a340) Leslie Lamport, Robert Shostak, and Marshall Pease, “The Byzantine Generals Problem,” ACM Transactions on Programming Languages and Systems (July 1982): 382–401.

[[184]](../part0018.xhtml#a377) Adam Back, “Re: ‘why privacy’ revisited,” originally sent to the Cypherpunks mailing list, March 22, 1997, available via: [https://cypherpunks.venona.com/date/1997/03/msg00586.html.](https://cypherpunks.venona.com/date/1997/03/msg00586.html)

[[185]](../part0018.xhtml#a39Z) Adam Back, “The Bitcoin Game #59: Dr. Adam Back,” interview by Rob Mitchell, The Bitcoin Game, YouTube, October 25, 2018, <https://youtu.be/xxYsRjanphA?si=XVdLXPWGUk6oVPXg&t=647> 10:47–11:19.

[[186]](../part0018.xhtml#a3GU) Adam Back, “Re: cypherpunks digicash bank?,” originally sent to the Cypherpunks mailing list, October 8, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/10/msg00734.html.](https://cypherpunks.venona.com/date/1995/10/msg00734.html)

[[187]](../part0018.xhtml#a31U) Adam Back, “cypherpunks digicash bank?,” originally sent to the Cypherpunks mailing list, October 7, 1995, accessed via:              [https://cypherpunks.venona.com/date/1995/10/msg00690.html.](https://cypherpunks.venona.com/date/1995/10/msg00690.html)

[[188]](../part0018.xhtml#a3E4) Barnes, “cypherpunks digicash.”

[[189]](../part0018.xhtml#a2RU) Adam Back, “distributed virtual bank,” originally sent to the Cypherpunks mailing list, August 27, 1997, accessed via: <https://cypherpunks.venona.com/date/1997/08/msg01289.html>.

[[190]](../part0018.xhtml#a2Z3) Tim May, “Re: More on digital postage,” originally sent to the Cypherpunks mailing list, February 15, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/02/msg02295.html.](https://cypherpunks.venona.com/date/1997/02/msg02295.html)

[[191]](../part0018.xhtml#a32T) Adam Back, “Re: bulk postage fine (was Re: non-censorous spam control),” originally sent to the Cypherpunks mailing list, August 3, 1997 accessed via: [https://cypherpunks.venona.com/date/1997/08/msg00070.html.](https://cypherpunks.venona.com/date/1997/08/msg00070.html)

[[192]](../part0018.xhtml#a31A) Adam Back, “no government regulation of the net (was Re: bulk postage fine),” originally sent to the Cypherpunks mailing list, August 3, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/08/msg00087.html.](https://cypherpunks.venona.com/date/1997/08/msg00087.html)

[[193]](../part0018.xhtml#a2XJ) Cynthia Dwork and Moni Naor, “Pricing via Processing or Combatting Junk Mail,” Advances in Cryptology—Crypto ’92 (1992): 139–147.

[[194]](../part0018.xhtml#a3FX) Adam Back, “[ANNOUNCE] hash cash postage implementation,” originally sent to the Cypherpunks mailing list, March 28, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/03/msg00774.html.](https://cypherpunks.venona.com/date/1997/03/msg00774.html)

[[195]](../part0018.xhtml#a37D) Adam Back, “Re: Remailer problem solution?” March 23, 1997, accessed via: [https://cypherpunks.venona.com/date/1997/03/msg00631.html.](https://cypherpunks.venona.com/date/1997/03/msg00631.html)

[[196]](../part0018.xhtml#a2WA) Back, “Re: Bypassing.”

[[197]](../part0018.xhtml#a36M) Back, “Re: Bypassing.”

[[198]](../part0019.xhtml#a2S9) Nick Szabo, “Why Cryptocurrency? Governments Abuse Their Power—Nick Szabo Interview Part 1,” interview by Zulu Republic, Zulu Republic, YouTube, October 25, 2018, [https://youtu.be/LZw4LNLYUgc?si=\_FilNeaFnWxpvv9U.](https://youtu.be/LZw4LNLYUgc?si=_FilNeaFnWxpvv9U)

[[199]](../part0019.xhtml#a39K) Nick Szabo (@NickSzabo4), “Some of the most important books I’ve read,” X, January 31, 2016, [https://twitter.com/NickSzabo4/status/693682157525401601.](https://twitter.com/NickSzabo4/status/693682157525401601)

[[200]](../part0019.xhtml#a3DE) Nick Szabo, “Re: Crypto + Economics + AI = Digital Money Economies,” originally sent to the Cypherpunks mailing list, September 19, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/09/msg01303.html.](https://cypherpunks.venona.com/date/1995/09/msg01303.html)

[[201]](../part0019.xhtml#a33E) Nick Szabo, “Smart Contracts: Building Blocks for Digital Free Markets,” Extropy 16 (1st Quarter of 1996): 50–64.

[[202]](../part0019.xhtml#a2PW) Szabo, “Smart Contracts,” 51.

[[203]](../part0019.xhtml#a39H) Nick Szabo, “Re: Crypto + Economics + AI = Digital Money Economies,” originally sent to the Cypherpunks mailing list, September 19, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/09/msg01303.html.](https://cypherpunks.venona.com/date/1995/09/msg01303.html)

[[204]](../part0019.xhtml#a35V) Nick Szabo, email to author, July 10, 2018.

[[205]](../part0019.xhtml#a3AC) Nick Szabo, “Trusted Third Parties are Security Holes,” Satoshi Nakamoto Institute (2001), [https://nakamotoinstitute.org/trusted-third-parties/.](https://nakamotoinstitute.org/trusted-third-parties/)

[[206]](../part0019.xhtml#a31E) Nick Szabo, “Nick Szabo on Cypherpunks, Money and Bitcoin,” interview by Peter McCormack, What Bitcoin Did, November 1, 2019, [https://www.whatbitcoindid.com/podcast/nick-szabo-on-cypherpunks-money-and-bitcoin.](https://www.whatbitcoindid.com/podcast/nick-szabo-on-cypherpunks-money-and-bitcoin)

[[207]](../part0019.xhtml#a3FT) Nick Szabo, “Bit Gold,” Unenumerated, December 27, 2008, [https://unenumerated.blogspot.com/2005/12/bit-gold.html.](https://unenumerated.blogspot.com/2005/12/bit-gold.html)

[[208]](../part0019.xhtml#a3D9) Richard Dawkins, The Selfish Gene (Oxford: Oxford University Press, 2016), 244.

[[209]](../part0019.xhtml#a35G) Nick Szabo, “Shelling Out: The Origins of Money,” Satoshi Nakamoto Institute (2002), [https://nakamotoinstitute.org/shelling-out/.](https://nakamotoinstitute.org/shelling-out/)

[[210]](../part0019.xhtml#a38S) It is worth noting however that this number—named after primatologist Robin Dunbar—has (more recently) been criticized, and isn’t, in the scientific community today, held with the specificity that it suggests. While there is a limit on the number of stable social relationships people can maintain, the actual number isn’t necessarily (around) 150 for everyone. See for instance Patrick Lindenfors, Andreas Wartel, and Johan Lind, “‘Dunbar’s Number’ Deconstructed,” Biology Letters, May 5, 2021: <https://royalsocietypublishing.org/doi/10.1098/rsbl.2021.0158>

[[211]](../part0019.xhtml#a360) Strictly speaking a “public goods game” is the more precise game theory analogy.

[[212]](../part0019.xhtml#a2TZ) Szabo, “Bit Gold.”

[[213]](../part0019.xhtml#a2TX) In Szabo’s original proposal, Bit Gold would actually use a “secure benchmark function,” which is slightly different from a hash function, but similar enough that referring to the product as a “hash” and the act of producing it as “hashing” is accurate enough for the purpose of understanding Bit Gold’s mechanics (and probably easier to follow).

[[214]](../part0019.xhtml#a2T2) Nick Szabo, “Secure Property Titles with Owner Authority,” Satoshi Nakamoto Institute (1998), [https://nakamotoinstitute.org/secure-property-titles/.](https://nakamotoinstitute.org/secure-property-titles/)

[[215]](../part0019.xhtml#a3CU) Nick Szabo, “Nick Szabo—The Quiet Master of Cryptocurrency | Co-Hosted by Naval Ravikant” interview by Tim Ferriss, The Tim Ferriss Show, YouTube, August 12, 2017, <https://youtu.be/3FA3UjA0igY>

[[216]](../part0019.xhtml#a31X) Szabo, “Secure Property Titles.”

[[217]](../part0019.xhtml#a39W) Nick Szabo, “Bit Gold: Towards Trust-Independent Digital Money” (1999), accessed via [https://web.archive.org/web/20140406003811/http://szabo.best.vwh.net/bitgold.html.](https://web.archive.org/web/20140406003811/http:/szabo.best.vwh.net/bitgold.html)

[[218]](../part0019.xhtml#a2YH)Nick Szabo, “Bit Gold Markets,” Unenumerated, December 27, 2008, [https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html.](https://unenumerated.blogspot.com/2008/04/bit-gold-markets.html)

[[219]](../part0019.xhtml#a3EZ) Szabo, “Bit Gold Markets.”

[[220]](../part0019.xhtml#a38C) Szabo, “Bit Gold.”

[[221]](../part0020.xhtml#a3FA) Wei Dai, “Work on Security Instead of Friendliness?” GreaterWrong, July 21, 2012, [https://www.greaterwrong.com/posts/m8FjhuELdg7iv6boW/work-on-security-instead-of-friendliness.](https://www.greaterwrong.com/posts/m8FjhuELdg7iv6boW/work-on-security-instead-of-friendliness)

[[222]](../part0020.xhtml#a35E) Wei Dai, “Law vs Technology,” originally sent to the Cypherpunks mailing list, February 10, 1995, accessed via: [https://cypherpunks.venona.com/date/1995/02/msg00508.html.](https://cypherpunks.venona.com/date/1995/02/msg00508.html)

[[223]](../part0020.xhtml#a2V9) Wei Dai, “PipeNet 1.1 and b-money,” originally sent to the Cypherpunks mailing list, November 26, 1998, accessed via: [https://cypherpunks.venona.com/date/1998/11/msg00941.html.](https://cypherpunks.venona.com/date/1998/11/msg00941.html)

[[224]](../part0020.xhtml#a37T) Wei Dai, untitled b-money description, 1998, accessed via [https://web.archive.org/web/20090415130807/https://www.weidai.com/bmoney.txt.](https://web.archive.org/web/20090415130807/https:/www.weidai.com/bmoney.txt)

[[225]](../part0020.xhtml#a3DW) Dai, untitled b-money description.

[[226]](../part0020.xhtml#a388) Wei Dai, “Re: alternative b-money creation,” originally sent to the Cypherpunks mailing list, December 11, 1998, accessed via: [https://cypherpunks.venona.com/date/1998/12/msg00448.html.](https://cypherpunks.venona.com/date/1998/12/msg00448.html)

[[227]](../part0020.xhtml#a2UP) Wei Dai, comment in the discussion thread “AALWA: Ask any LessWronger anything,” LessWrong, 2014, [https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything.](https://www.lesswrong.com/posts/YdfpDyRpNyypivgdu/aalwa-ask-any-lesswronger-anything)

[[228]](../part0020.xhtml#a307) Dai, comment.

[[229]](../part0020.xhtml#a2YB)Eric Hughes, “Kid Gloves or Megaphones,” originally sent to the Cypherpunks mailing list, March 14, 1996, accessed via: [https://cypherpunks.venona.com/date/1996/03/msg00932.html.](https://cypherpunks.venona.com/date/1996/03/msg00932.html)

[[230]](../part0020.xhtml#a333) Hughes, “Kid Gloves.”

[[231]](../part0020.xhtml#a2NR) Austin Hill, draft document from 2005 shared with author, March 30, 2022.

[[232]](../part0020.xhtml#a39R) Ori Brafman and Rod A. Beckstrom, The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations (New York: Portfolio, 2006), 22–27.

[[233]](../part0020.xhtml#a2TE) Damien Cave, “The Mojo solution,” Salon, October 9, 2000,              [https://www.salon.com/2000/10/09/mojo\_nation/.](https://www.salon.com/2000/10/09/mojo_nation/)

[[234]](../part0020.xhtml#a3BV) As a mildly interesting detail, most Mojo transactions were actually only recorded between two peers at first, each building up credit or debit with the other peer, to only settle the debt using an actual Mojo token when a certain threshold was met.

[[235]](../part0020.xhtml#a3F0) Cave, “The Mojo solution.”

[[236]](../part0020.xhtml#a33W) Daniel A. Nagy, comments in response to “The Mojo Nation Story—Part 2,” Financial Cryptography, October 12, 2005, <https://www.financialcryptography.com/mt/archives/000572.html>

[[237]](../part0020.xhtml#a2Z5) Bryce Wilcox-O’Hearn, “Experiences Deploying A Large-Scale Emergent Network,” Peer-to-Peer Systems (2002): 104–110.

[[238]](../part0020.xhtml#a3BY) Wilcox-O’Hearn, “Large-Scale Emergent Network.”

[[239]](../part0020.xhtml#a386) Liang Wang, “BitTorrent Mainline DHT Measurement,” MLDHT, 2013, accessed via: [https://www.cl.cam.ac.uk/~lw525/MLDHT/.](https://www.cl.cam.ac.uk/~lw525/MLDHT/)

[[240]](../part0020.xhtml#a3GR) BitTorrent, “BitTorrent and µTorrent Software Surpass 150 Million User Milestone; Announce New Consumer Electronics Partnerships,” BitTorrent.com, January 9, 2012, accessed via [https://web.archive.org/web/20140326102305/http://www.bittorrent.com/intl/es/company/about/ces\_2012\_150m\_users.](https://web.archive.org/web/20140326102305/http:/www.bittorrent.com/intl/es/company/about/ces_2012_150m_users)

[[241]](../part0020.xhtml#a31D) Hendrik Schulze and Klaus Mochalski, “Internet Study 2008/2009,” ipoque (2009).

[[242]](../part0021.xhtml#a330) Tim May, “My Departure, Moderation, and ‘Ownership of the List,’ originally sent to the Cypherpunks mailing list, February 2, 1997, accessed via:

https://cypherpunks.venona.com/date/1997/02/msg02898.html

[[243]](../part0021.xhtml#a2ZU)​Mark Frauenfelder, “Homeless Cypherpunks Turn to Usenet,” Wired, February 17, 1997, [https://www.wired.com/1997/02/homeless-cypherpunks-turn-to-usenet/.](https://www.wired.com/1997/02/homeless-cypherpunks-turn-to-usenet/)

[[244]](../part0021.xhtml#a2TS) Declan McCullagh, “Digging Those Digicash Blues,” Wired, June 14, 2001, [https://www.wired.com/2001/06/digging-those-digicash-blues/.](https://www.wired.com/2001/06/digging-those-digicash-blues/)

[[245]](../part0021.xhtml#a36Z) Nicole Weinstock, “Member Profile: Hal Finney,” Cryonics 40, issue 2 (2nd Quarter 2019): 9.

[[246]](../part0021.xhtml#a31Y) Hal Finney, ”Re: Physical to digital cash, and back again,” originally sent to the Cypherpunks mailing list, August 19, 1993, accessed via: <https://cypherpunks.venona.com/date/1993/08/msg00581.html>

[[247]](../part0021.xhtml#a36T) Hal Finney, “Why remailers…,” originally sent to the Cypherpunks mailing list, November 15, 1992, accessed via: [https://cypherpunks.venona.com/date/1992/11/msg00108.html.](https://cypherpunks.venona.com/date/1992/11/msg00108.html)

[[248]](../part0021.xhtml#a3F2) Hal Finney, “Re: Voluntary Governments?” originally sent to the Cypherpunks mailing list, August 4, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/08/msg00239.html.](https://cypherpunks.venona.com/date/1994/08/msg00239.html)

[[249]](../part0021.xhtml#a2SY) Hal Finney, “POLI: Politics vs Technology,” originally sent to the Cypherpunks mailing list, January 2, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/01/msg00014.html.](https://cypherpunks.venona.com/date/1994/01/msg00014.html)

[[250]](../part0021.xhtml#a379) Hal Finney, “Re: Re: re: re: digital cash,” originally sent to the Cypherpunks mailing list, March 16, 1994, accessed via: [https://cypherpunks.venona.com/date/1994/03/msg00694.html.](https://cypherpunks.venona.com/date/1994/03/msg00694.html)

[[251]](../part0021.xhtml#a2YF) Finney, “Re: Re: re: re: digital cash.”

[[252]](../part0021.xhtml#a3C0) Hal Finney, “Reusable Proofs of Work,” RPOW website index page, accessed via: [https://web.archive.org/web/20090217090451/http://rpow.net/index.html.](https://web.archive.org/web/20090217090451/http:/rpow.net/index.html)

[[253]](../part0021.xhtml#a2T8) Hal Finney, “RPOW Theory,” RPOW website theory page, accessed via [https://web.archive.org/web/20040815154951/http://rpow.net/theory.html.](https://web.archive.org/web/20040815154951/http:/rpow.net/theory.html)

[[254]](../part0021.xhtml#a3DN) Hal Finney, “RPOW FAQs,” RPOW website FAQ page, accessed via [https://web.archive.org/web/20090217090439/http://rpow.net/faqs.html#inflation.](https://web.archive.org/web/20090217090439/http:/rpow.net/faqs.html#inflation)

[[255]](../part0021.xhtml#a2XX)Gregory Maxwell, IRC message to author, August 13, 2020.

[[256]](../part0023.xhtml#a3FF) Andrea Wong, “The Untold Story Behind Saudi Arabia’s 41-Year U.S. Debt Secret,” Bloomberg, May 31, 2016, [https://www.bloomberg.com/news/features/2016-05-30/the-untold-story-behind-saudi-arabia-s-41-year-u-s-debt-secret#xj4y7vzkg.](https://www.bloomberg.com/news/features/2016-05-30/the-untold-story-behind-saudi-arabia-s-41-year-u-s-debt-secret#xj4y7vzkg)

[[257]](../part0023.xhtml#a2T0) Energy Exploration & Exploitation, “World Oil Reserves 1948–2001: Annual Statistics and Analysis,” Energy Exploration & Exploitation, vol. 19, no. 2 & 3 (2001), <https://journals.sagepub.com/doi/pdf/10.1260/0144598011492561>

[[258]](../part0023.xhtml#a310) Alex Gladstein, “Uncovering The Hidden Costs of the Petrodollar,” Bitcoin Magazine, April 28, 2021, <https://bitcoinmagazine.com/culture/the-hidden-costs-of-the-petrodollar>

[[259]](../part0023.xhtml#a329) Wapshott, Keynes Hayek, 258–59.

[[260]](../part0023.xhtml#a33C) Wapshott, Keynes Hayek, 261.

[[261]](../part0023.xhtml#a2NT) Wapshott, Keynes Hayek, 211–214.

[[262]](../part0023.xhtml#a30Y) Milton Friedman and Anna Schwartz, A Monetary History of the United States (Princeton, NJ: Princeton University Press, 1963).

[[263]](../part0023.xhtml#a3FM) The Economist, “Why don’t rising house prices count towards inflation?” The Economist, July 29, 2021, [https://www.economist.com/the-economist-explains/2021/07/29/why-dont-rising-house-prices-count-towards-inflation.](https://www.economist.com/the-economist-explains/2021/07/29/why-dont-rising-house-prices-count-towards-inflation)

[[264]](../part0023.xhtml#a312) US Department of the Treasury, “Troubled Asset Relief Program (TARP),” available via: <https://home.treasury.gov/data/troubled-asset-relief-program>; Federico Mor, Bank Rescues of 2007-09: Outcomes and Cost, House of Commons Research Briefing, October 8, 2018, available via: <https://commonslibrary.parliament.uk/research-briefings/sn05748/>

[[265]](../part0023.xhtml#a2RF) Rupal Patel and Jack Meaning, Can’t We Just Print More Money? Economics in Ten Simple Questions, The Bank of England (London: Cornerstone Press, 2022), 238.

[[266]](../part0023.xhtml#a35A) New Keynesians integrated more of the neoclassical (and therefore Hayekian) ideas on free markets, but also assumed more potential market failures, in particular due to an inability of some prices to adjust to new circumstances quickly, justifying government intervention. This most notably includes the price of labor (wages) due to psychological factors.

[[267]](../part0024.xhtml#a3G6) Satoshi Nakamoto and Wei Dai, “Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails,” gwern.net, last modified September 14, 2017, [https://gwern.net/doc/bitcoin/2008-nakamoto.](https://gwern.net/doc/bitcoin/2008-nakamoto)

[[268]](../part0024.xhtml#a34W) Nakamoto and Dai, “Wei Dai/Satoshi Nakamoto 2009 Bitcoin emails.”

[[269]](../part0024.xhtml#a35N) Satoshi Nakamoto, “Bitcoin P2P e-cash paper.” Originally sent to the Cryptography mailing list. October 31, 2008. Accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html.](https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html)

[[270]](../part0024.xhtml#a30V) Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System” (2008), available via: <https://bitcoin.org/bitcoin.pdf>

[[271]](../part0024.xhtml#a3CR) James A. Donald, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 2, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014814.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014814.html)

[[272]](../part0024.xhtml#a3FH) Satoshi Nakamoto, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 2, 2008, accessed via:              [https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014815.html)

[[273]](../part0024.xhtml#a399) James A. Donald, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 3, 2008 accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014819.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014819.html)

[[274]](../part0024.xhtml#a3F9) Satoshi Nakamoto, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 6, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014823.html)

[[275]](../part0024.xhtml#a32E) Ray Dillinger, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 6, 2008, Accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014822.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014822.html)

[[276]](../part0024.xhtml#a30A) Ray Dillinger, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 14, 2008, Accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014857.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014857.html)

[[277]](../part0024.xhtml#a2PY) James A. Donald, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 9, 2008, accessed via: <https://www.metzdowd.com/pipermail/cryptography/2008-November/014837.html>.

[[278]](../part0024.xhtml#a2VU) Ray Dillinger, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 15, 2008, accessed via: <https://www.metzdowd.com/pipermail/cryptography/2008-November/014859.html>.

[[279]](../part0024.xhtml#a32G) James A. Donald, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 9, 2008, accessed via: <https://www.metzdowd.com/pipermail/cryptography/2008-November/014841.html>.

[[280]](../part0024.xhtml#a3EJ) John Levine, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 3, 2008, accessed via: <https://www.metzdowd.com/pipermail/cryptography/2008-November/014817.html>.

[[281]](../part0024.xhtml#a3BW) Hal Finney, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 7, 2008, accessed via: <https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html>.

[[282]](../part0024.xhtml#a354) Hal Finney, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 7, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014827.html)

[[283]](../part0024.xhtml#a3DH) Hal Finney, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 13, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014848.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014848.html)

[[284]](../part0024.xhtml#a2VX) Satoshi Nakamoto, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 14, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014853.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014853.html)

[[285]](../part0024.xhtml#a32B) Satoshi Nakamoto, “Bitcoin P2P e-cash paper,” originally sent to the Cryptography mailing list, November 8, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014832.html)

[[286]](../part0024.xhtml#a3G7) Perry E. Metzger, “ADMIN: end of bitcoin discussion for now,” originally sent to the Cryptography mailing list, November 17, 2008, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2008-November/014867.html.](https://www.metzdowd.com/pipermail/cryptography/2008-November/014867.html)

[[287]](../part0025.xhtml#a374) Friedrich A. Hayek, “F. A. Hayek on Monetary Policy, the Gold Standard, Deficits, Inflation, and John Maynard Keynes,” interview by James U. Blanchard III, re-uploaded by Libertarianism.org on April 19, 2015, [https://youtu.be/EYhEDxFwFRU.](https://youtu.be/EYhEDxFwFRU)

[[288]](../part0025.xhtml#a39T) Hayek, interview.

[[289]](../part0025.xhtml#a2UV) Satoshi Nakamoto, “Bitcoin v0.1 released,” originally sent to the Cryptography mailing list, January 8, 2009, Accessed via: [https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html.](https://www.mail-archive.com/cryptography@metzdowd.com/msg10142.html)

[[290]](../part0025.xhtml#a3BG) Michael J. Casey, “Bitcoin Foundation’s Andresen on Working With Satoshi Nakamoto,” The Wall Street Journal, March 6, 2014, [https://www.wsj.com/articles/BL-MBB-17626.](https://www.wsj.com/articles/BL-MBB-17626)

[[291]](../part0025.xhtml#a2SV) Since Bitcoin was ultimately released on January 8, this would have left the system’s creator with a maximum of six days to comfortably generate coins in absence of any competition—but early block timestamps indicate that he didn’t do this either.

[[292]](../part0025.xhtml#a315) It’s worth noting though that each bitcoin can be divided up to eight decimal points, so in a way there are 2.1 quadrillion currency units. The smallest unit, 0.00000001 bitcoin, is today usually referred to as a “satoshi,” or “sat” for short.

[[293]](../part0025.xhtml#a2UK) Hal Finney, “Bitcoin v0.1 released,” originally sent to the Cryptography mailing list, January 10, 2009, accessed via: <https://www.metzdowd.com/pipermail/cryptography/2009-January/015004.html>

[[294]](../part0025.xhtml#a3A1) Satoshi Nakamoto, “Bitcoin v0.1 released,” originally sent to the Cryptography mailing list, January 16, 2009, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html.](https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html)

[[295]](../part0025.xhtml#a2X5) Satoshi Nakamoto, “Bitcoin v0.1 released,” originally sent to the Cryptography mailing list, January 16, 2009, accessed via: [https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html.](https://www.metzdowd.com/pipermail/cryptography/2009-January/015014.html)

[[296]](../part0025.xhtml#a2PV) This most famously included the 1-megabyte block size limit, preventing the block chain from growing so fast that most regular users wouldn’t be able to run a Bitcoin node on their home computer.

[[297]](../part0025.xhtml#a385) The currently best-known example of such a payment layer is called the Lightning Network.