

How Cypherpunks Paved the Way for Satoshi's Bitcoin:

The Evolution of Decentralized Ideals and the Birth of Bitcoin (1992– 2009)

Neal de Hoop

14622106

[19th of June 2024]

Histories of Digital Culture

Dr. Steve Jankowski

"I affirm that this assignment was written by me, in accordance with the rules and regulations governing fraud and plagiarism for UvA students."

Introduction: The Path to Bitcoin, Decentralization and the Cypherpunk Vision

In the late 20th century, a group known as cypherpunks emerged. These individuals, In the late 20th century, fueled by a confluence of technological advancements and a strong ideological vision, a group known as cypherpunks emerged. They envisioned a radical transformation in how information and value could be exchanged securely and privately (Jarvis 2022). Their vision, rooted in decentralization, cyberlibertarianism, and cryptography, aimed to empower individuals and safeguard personal freedoms within our increasingly interconnected world. Today, the term "crypto" often conjures immediate images of cryptocurrencies like Bitcoin. But how are these digital currencies linked to the cypherpunks, and how much influence did these early digital activists have?

This paper delves into this very question: what conditions did the cypherpunk movement (from 1992 to 2009) create for the development of decentralized and cryptographic ideas, and how did these pave the way for Bitcoin? I will explore the Cypherpunk email list, a crucial online forum established by Timothy C. May and E. Hughes, which served as a platform for early digital activists and technologists to exchange ideas on cryptography, privacy, and decentralization. This archived resource from [Cryptoanarchy.wiki](https://cryptoanarchy.wiki) documents the foundational discussions that shaped the cypherpunk movement's philosophy and technical advancements. Similarly, the Bitcoin white paper, authored by the pseudonymous Satoshi Nakamoto and available through the Wayback Machines digital archive, outlines the design of the first decentralized cryptocurrency. These resources provide essential primary sources for understanding the evolution of decentralized digital technologies and the intellectual context that birthed Bitcoin.

I argue that Satoshi's creation of Bitcoin can be seen as a logical progression from the groundwork laid by the cypherpunk movement. Bitcoin embodies and realizes the cypherpunks' ideals. The cultural and technological conditions fostered by this movement made Bitcoin's emergence not only possible but almost inevitable.

The paper will delve deeper into the concept of cyberlibertarianism, drawing on the work of Fred Turner (2006). We will also explore the principles of hacker culture, as outlined by Haigh (2021). We will then examine how these principles align with the cypherpunk ideals of individual freedom and a healthy skepticism towards centralized authority (Coleman 2017).

Decentralization is a key concept for both cypherpunks and cryptology. Emerging in the 1990s, cypherpunks believed power, information, and financial transactions should be spread out, not concentrated in the hands of a few (Jarvis 2022). They envisioned a world where individuals control their own data and conduct transactions without needing oversight from authorities.

By focusing on sources up to 2009, this research acknowledges the time frame limitations and underscores the pivotal role cypherpunk culture played in shaping Bitcoin's genesis (1992-2009). The following section will analyze these concepts in greater detail and explore the broader cultural context of the cypherpunks.

Change and continuity: Cyberlibertarianism and Hacker Culture

The broader cultural position of the Cypherpunk movement can be found within hacker culture. A culture that was established through hacker practices. "Hackers were not simply highly individualistic and innovative engineers. They were cultural rebels -- and their computers were the new tools of utopian cultural change" (Turner 2006, 11). This quote by Turner indicates that hackers used computers as tools to develop and change the world to their likings, following their ideals.

The hacker ethic, which embodies their ideals and beliefs, emphasizes information freedom, mistrust of authority, not being judged by criteria such as degrees, age, race, sex or position, that beauty and art can be created on computers, and that computers can change your life for the better (Haigh 2021, 21). Within the context of cryptology and Cypherpunks, the ideals of mistrusting authority and “information should be free” are most relevant. “[...] source code is the most material of the five components of Free Software; it is both an expressive medium, like writing or speech, and a tool that performs concrete actions” (Kelty 2008, 118). In other words, hackers use source code to convey their ideas and beliefs. Although Hacker culture is one part of Cypherpunks, politics also play a big role in the movement (Jarvis 2022, 327).

Cyberlibertarianism is introduced by Turner (2006) as a belief of Hackers to “[...] identify the social work that has gone into aligning emerging digital technologies with libertarian political ideals” (Turner 2006, 3). This quote emphasizes the importance of understanding the historical context and social processes that have shaped cyberlibertarianism as an ideology aligning hacker culture with libertarian principles.

The Cypherpunks also made a distinctive contribution to the history of decentralized and cryptographically secure technology by introducing the concept of resilience not only as architectural decentralization of digital infrastructure but also as political decentralization of control (Nabben 2021). The cypherpunks helped shape our internet. Beltramini comments they were, “perhaps the single most effective grassroots organization in history dedicated to protecting freedom in cyberspace” (Beltramini 2020, p. 1). United as “privacy activists,” this diverse group of individuals, including cryptographers, hippies, computer programmers, hackers, activists, and philosophers, shared a common belief in safeguarding freedom from state interference in private matters through digital encryption technology (Beltramini 2020). Cryptography emerged as their

primary tool against the threats of corporate and government surveillance (Coleman & Golub 2008; Beltramini 2020; Hughes 1992). The term "cryptology", or short "crypto", which involves encrypting information to make it unreadable to anyone except the intended recipients. As stated by the Helengren (2017, 286), "The term crypto is short for cryptography, which refers to the practice of encrypting, i.e. rendering information illegible to anyone but its intended recipient(s)". This definition highlights the core purpose of cryptography, which is to ensure the confidentiality and security of communication by making it inaccessible to unauthorized parties.

Timothy C. May, one of the creators of the Cypherpunk email list, took the foundational principles of resilience advocated by David Chaum to an extreme political stance, aiming to reshape the social, economic, and political order (Chaum 1985). He championed the concept of digital cash as a means to diminish the coercive power of governments in taxation, thereby advancing his vision of a more liberated society. Through works like the "Crypto-anarchist Manifesto" and the "Cyphernomicon", May articulated cypherpunk ideals, portraying cryptography and decentralization as tools to combat government surveillance. In his interpretation of political decentralization, May envisioned an anarchic system characterized by decentralized organization, devoid of central leadership, and driven by individual actions and market dynamics (May 1992; 1994). The pursuit of digital cash epitomized their quest to realize this vision.

It is also worth mentioning that there is a distinction between cypherpunks and crypto-anarchists in their approaches to digital privacy and security. Computer scientist Arvind Narayanan (2013) explains this difference by stating, "For cypherpunks, crypto was at the core of a vision of how technology would cause sweeping social and political change, weakening the power of governments and established institutions. A closely related term is crypto-anarchism, a

political philosophy that, in its idealized form, recognizes no laws except those that can be described by math and enforced by code". This quote elucidates that while cypherpunks focus on utilizing cryptography for societal transformation and reducing governmental influence, crypto-anarchists advocate for a governance model based solely on mathematical laws enforced through code, rejecting traditional legal structures.

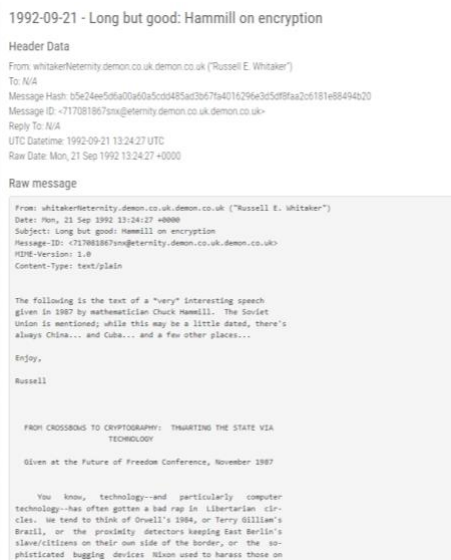


Figure 1. First post on the Cypherpunk email list by Russell E. Whitaker on the 21st of September 2021. Archived by Cryptoanarchy.wiki.

The Cypherpunk Movement

To delve into the historical artifacts within this paper, there will be looked at the first ten emails within the Cypherpunk email list (see Figure 1 for example of an email). These emails origin from June 1992 to Mon, 15 July 1996 and are the expressions of the Cypherpunk ideals and beliefs in a collective space. The mail list contains over 98.000 posts from at least a thousand contributors (Jarvis 2022, 317). The list was organized by “threads”, which were derived from email subject lines. Once a user posted to the mail list all subscribers would receive a message.

The artifacts will be analyzed based on textual analysis, a methodological approach that involves examining and interpreting texts, such as emails, to uncover underlying meanings, themes, and cultural implications (Phillipinov 2013, 2009). This approach focuses on analyzing the content, structure, and language of texts to gain insights into the experiences, values, and perspectives embedded within them.

The emails from the Cypherpunk community members in the analyzed sample from the email list reflect a strong commitment to privacy, encryption, and resistance against government control over cryptographic technologies. The members express concerns about potential government efforts to restrict strong cryptography and undermine privacy rights. They emphasize the importance of maintaining individual freedoms and resisting attempts to limit encryption capabilities.

In one of the emails, the author (Whitaker) outlines a hypothetical scenario of how strong crypto could be banned in the U.S., involving collaboration with various entities to limit crypto use globally. "I propose a libertarian network spreading the technologies by which we may seize freedom for ourselves" (Whitaker 1992). Whitaker advocates against supporting any plan that grants the government such power and stresses the importance of resisting potential encroachments on privacy and encryption rights.

The emails also touch upon the resistance against government control and the push for encryption technologies that empower individuals. "But here we must be a bit careful. While it is not (at present) illegal to encrypt information when government wants to spy on you, there is no guarantee of what the future may hold" (Whitaker 1992). The Cypherpunks aim to protect privacy and promote freedom through encryption tools, as seen in their efforts to combat potential restrictions on cryptography. Based on these emails, the Cypherpunk ideals of privacy,

encryption, and individual empowerment shine through. The members are dedicated to safeguarding privacy rights, resisting government overreach, and advocating for the use of strong encryption technologies to protect personal freedoms. Their discussions reflect a commitment to upholding civil liberties in the digital age.

The other main primary artifact surrounding cypherpunk was the Cypherpunk Manifesto by Eric Hughes (1993). It underscores the critical role of privacy in an open society within the electronic age. It distinguishes privacy from secrecy, emphasizing the power of selectively revealing oneself to the world. The manifesto advocates for the use of anonymous transaction systems and cryptography to safeguard privacy rights. It highlights the necessity of individuals taking proactive measures to defend their privacy, including the development and utilization of technologies that enable anonymous transactions and secure communication. The manifesto also stresses the importance of a social contract where individuals come together to deploy privacy-enhancing systems for the common good.

The Wired article (see Figure 1) also delves into this topic of privacy advocates, focusing on the emergence of Cypherpunks, civil libertarians, and hackers as key players in the battle for privacy (Levy 1993). The article introduces the Cypherpunks as a group of individuals who are passionate about codes, privacy, and taking action to defend privacy rights in the digital realm. They believe in the power of cryptography to protect anonymity and privacy in an increasingly digitized society.

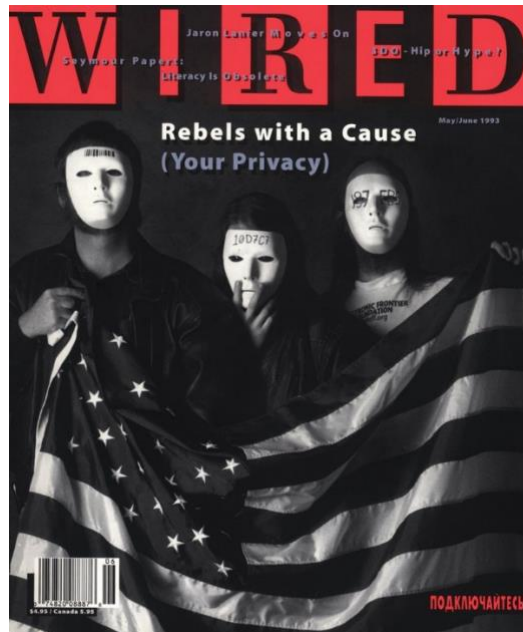


Figure 2. The cover of Wired Magazine 1.02 May/June 1993. The cover features the founders of the Cypherpunks: Timothy C. May, Eric Hughes, and John Gilmore.

The Foundation of Bitcoin and Cypherpunk Ideals

By early 2000s, the excitement around both cypherpunk and crypto-anarchy had cooled down (Swartz 2018, 628). John Gilmore, one of the list's founders, declared it dead in 2001 (Rodger 2001). While advances were made in academic and commercial cryptography, little new work was being done in 'crypto for privacy' (Narayanan 2013, p. 75). Then, in 2008, an individual or group using the pseudonym Satoshi Nakamoto posted to a different, largely non-political cryptography email list a whitepaper outlining a new system for digital cash called Bitcoin. Shortly after the publication of the whitepaper, Satoshi and members of the email list began a Free and Open Source software project, a concept that lives up to its very name, to implement the proposed system (Kelty 2008). In 2009, the first Bitcoin client was released, and Satoshi mined the first 'genesis block' of 50 Bitcoins (Swartz 2018, 628). In the spirit of the 1990s Cypherpunks email list, the conversation about the technical and philosophical dimensions

of Bitcoin was spirited. On Bitcoin email lists and forums, veterans and newcomers revived the conversation around cypherpunk and crypto-anarchy.

The Bitcoin whitepaper by Satoshi Nakamoto (2008) completely outlines a system for digital cash that eliminates the need for trusted third parties like banks in online transactions. This is achieved through a peer-to-peer network where users bundle transactions together into blocks, chronologically chaining them using a complex mathematical problem called "proof-of-work" for security. Miners compete to solve these puzzles, adding new blocks to the chain and earning rewards in the process. This approach creates a tamper-proof record of transactions while keeping the system decentralized, transparent, and secure. Users are identified by public keys instead of real names, offering a degree of anonymity, and the system incentivizes honest participation through rewards.

Satoshi (2009) also posted an update on his newly created e-cash system on the P2P (Peer to Peer) foundation forum (see Figure 2). In this posts he recalled the need for cryptographic electronic currencies and secure and effortless transactions. Satoshi comments on someone else's responds on the project with that Bitcoin is based on the old "Chaumian" central stuff. Chaumian referring to David Chaum's vision aimed to make traditional financial intermediaries obsolete by offering a decentralized and anonymous way to conduct transactions.

The beliefs of Cypherpunks, characterized by a strong distrust of centralized authority and a fervent belief in the power of cryptography for individual empowerment, laid the groundwork for the emergence of Bitcoin. This ideological foundation permeated both the Bitcoin whitepaper and Satoshi Nakamoto's forum posts. The whitepaper itself proposed a system that bypassed traditional financial institutions, directly aligning with the Cypherpunks' desire to dismantle reliance on trusted third parties. Satoshi's forum post referencing David Chaum's vision for

anonymous digital cash further reinforces this connection. By explicitly mentioning Chaum, a prominent figure in crypto anarchist circles, Satoshi subtly acknowledges the intellectual heritage of Bitcoin and its alignment with Cypherpunk ideals. In essence, Bitcoin wasn't just a technical innovation; it was a cultural and ideological culmination of the Cypherpunk movement's vision for a more secure, private, and an user-controlled financial future.



Figure 3. Post by Satoshi Nakamoto on February 11 on the Bitcoin open-source implementation of P2P currency. Posted on P2P (Peer-to-peer) foundation forum on February 11, 2009.

Conclusion: Bitcoin Founded in Conditions Created by Cypherpunks

The question I explored was whether the founding of Bitcoin by Satoshi Nakamoto in 2008 can be seen as a progression from conditions that the cypherpunk movement created. The answer to this question is affirmative. The cultural and technological groundwork laid by the cypherpunks not only made Bitcoin's emergence possible but almost inevitable. At its core, the cypherpunk movement was fueled by a deep distrust of centralized authority and a belief in the

power of cryptography to empower individuals. This ideology found voice in online forums like the Cypherpunk mailing list and manifestos like the Cypherpunk Manifesto. These platforms emphasized the importance of privacy, encryption, and freedom from government oversight in the digital age.

The 1990s also witnessed significant advancements in cryptography, paving the way for secure communication channels and, ultimately, digital currencies. Enter Bitcoin, meticulously outlined in a whitepaper by the pseudonymous Satoshi Nakamoto. Bitcoin's design perfectly mirrored the cypherpunk desire for a decentralized system by eliminating the need for trusted third parties like banks in financial transactions. Furthermore, Satoshi Nakamoto's reference to David Chaum, a pioneer in anonymous digital cash, subtly acknowledged the intellectual heritage of Bitcoin and its alignment with cypherpunk ideology. This connection goes beyond mere technology; it represents a shared vision for a more secure, private, and user-controlled financial future.

In conclusion, Bitcoin was not just a new technology; it was the realization of the cypherpunk vision. The cultural and technological ideas and beliefs by this movement were expressed into a revolutionary concept that challenged traditional financial structures and empowered individuals with greater control over their financial lives. Bitcoin stands as a testament to the enduring legacy of the cypherpunks and their belief in the transformative power of cryptography.

Bibliography

- “Index of /~bryan/Irc/Bitcoin-Satoshi.” n.d. Accessed May 30, 2024. <https://diyhpl.us/~bryan/irc/bitcoin-satoshi/>.
- Beltramini, E. 2020. Against Technocratic Authoritarianism: A short intellectual history of the cypherpunk movement. Internet Histories. <https://doi.org/10.1080/24701475.2020.1731249>
- Chaum, D. 1985. ‘Security without Identification, Card Computers to make Big Brother Obsolete’, Communications of the ACM, vol. 28 (10), 1030-1044.
- Coleman, G.E. and Alex Golub. 2008. ‘Hacker practice: Moral genres and the cultural articulation of liberalism’, Anthropological Theory, 8 (3, 2008). <https://doi.org/10.1177/1463499608093814>.
- Coleman, Gabriella. 2017. “From Internet Farming to Weapons of the Geek.” Current Anthropology 58 (S15): S91–102. <https://doi.org/10.1086/688697>
- cryptoanarchy.wiki. n.d. “Cypherpunks Mailing List Archive.” Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. Accessed June 16, 2024. <https://mailing-list-archive.cryptoanarchy.wiki>.
- Dai, W. 1998. “B-Money”. Accessed June 19 2024. <http://www.weidai.com/bmoney.txt>
- Detweiler, L. 1993. “NY TAXES CYBERSPACE, CRAM REACTS.” Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. September 1, 1993. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1993/09/1c08c097e7722b824081c3b9e834a3d0e3b790891237c240be6ac92ded954360/>.
- Ghosh, Rishab Aiyer. 1995. “Re: Exporting Cryptographic Materials, Theory vs. Practice.” Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. January 1, 1995. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1995/01/55bad2eb32ef7a46a8cb496264df63d16f8143569f587a8eaa7105c5840c70f3/>.
- Haigh, Thomas. 2021. “When Hackers Were Heroes.” Communications of the ACM 64 (4): 28–34. <https://doi.org/10.1145/3451227>
- Hellegren, Z. Isadora. 2017. “A History of Crypto-Discourse: Encryption as a Site of Struggles to Define Internet Freedom.” Internet Histories 1 (4): 285–311. <https://doi.org/10.1080/24701475.2017.1387466>
- Hettinga, Robert. 1997. “E-Cash IPO! PCweek Mag!” Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. January 2, 1997. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1997/01/6d1eac01663752cd90613cc3b37c0149ba3044a1087ac007abab11aefec89951/>.

- Hettinga, Robert. 1998. "E-Cash Cost Advantage Acknowledged." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. January 3, 1998. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1998/01/5a0e9ad05fe226e63d96af55a05fb5308b2b11e95f8b1e426e886c5018fd808f/>.
- Hughes, E. 1993. 'A Cypherpunk's Manifesto.' in *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*, John Wiley & Sons, Inc. (1997), 285–87.
- Internet Archive. 2009. "Bitcoin.Org - Research Paper on Peer-to-Peer Electronic Cash." Wayback Machine. January 31, 2009. <https://web.archive.org/web/20090131115053/http://bitcoin.org/>.
- Jarvis, Craig. 2022. "Cypherpunk Ideology: Objectives, Profiles, and Influences (1992–1998)." *Internet Histories* 6 (3): 315–42. <https://doi.org/10.1080/24701475.2021.1935547>.
- Kelty, Christopher. 2008. "Chapter 4: Sharing Source Code." In *Two Bits: The Cultural Significance of Free Software*, 118-142. Durham, Duke University Press Books.
- Levy, Steven. 1993. "Crypto Rebels." *Wired*. Accessed June 16, 2024. <https://www.wired.com/1993/02/crypto-rebels/>.
- Martinson, Yanek. 1993. "CFP'93 Electronic Brochure 1.2 (Fwd)." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. January 1, 1993. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1993/01/0dc76c739f7106ee0198a4e025334614003d73c090f8bc7a8abe6e76052fa7c9/>.
- May, Timothy C. 1992. 'The Crypto Anarchist Manifesto'. Accessed June 17th, 2024. <https://www.activism.net/cypherpunk/crypto-anarchy.html> .
- May, Timothy C. 1992b. 'Libertaria in Cyberspace'. Accessed June 17th, 2024. <https://nakamotoinstitute.org/libertaria-in-cyberspace/> .
- May, Timothy C. 1994. 'The Cyphernomicon'. Accessed June 17th, 2024. <https://nakamotoinstitute.org/static/docs/cyphernomicon.txt> .
- May, Timothy C. 1996. "Free Speech and List Topics." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. September 2, 1996. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1996/09/8267653f7fbdc0c7da8467326259835eaaad88f0fc069618c3dfdbab1c9608e99/>.
- May, Timothy C. 1996b. "How I Would Ban Strong Crypto in the U.S. Arise, You Have Nothing to Lose but Your Barbed Wire Fences!" Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. July 15, 1996. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1996/07/bdc4cf9abea287d6d25bac4b8331106247b923c1e5c3223da9cef7db2e2b02f7/>.

- Miller, Jim. 1994. "Re: Anonymous Video on Demand." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. January 1, 1994. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1994/01/00aaf58cc01e9fa176888aa29ea6968219f8c8ff8d9332de638b7f3c813b4961/>.
- Nabben, Kelsie. 2021. "Resilience as 'Political Decentralization': An Alternate History of the Cypherpunks Origins of Decentralised Technology." SSRN Scholarly Paper. Rochester, NY. <https://doi.org/10.2139/ssrn.3938626>.
- Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." <https://bitcoin.org/bitcoin.pdf>
- Nakamoto, Satoshi. 2009. "Bitcoin Open Source Implementation of P2P Currency." November 2, 2009. Accessed June 17, 2024. <https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source>.
- Narayanan, A., 2013. What happened to the crypto dream? Part 1. IEEE security & privacy, 11 (2), 75–76.
- Owens, Trevor and Thomas Padilla. 2021. "Digital sources and digital archives: historical evidence in the digital age." *International Journal of Digital Humanities* 1 (3): 325-341. <https://doi.org/10.1007/s42803-020-00028-7>
- Phillipov, Michelle. 2013. "In Defense of Textual Analysis: Resisting Methodological Hegemony in Media and Cultural Studies." *Critical Studies in Media Communication* 30 (3): 209–23.
- Rodger, Will. 2001. "SecurityFocus: R.I.P. Cypherpunks." Wayback Machine. December 10, 2001. <https://web.archive.org/web/20011210025552/http://www.securityfocus.com/news/294>.
- Swartz, Lana. 2018. "What Was Bitcoin, What Will It Be? The Techno-Economic Imaginaries of a New Money Technology." *Cultural Studies* 32 (4): 623-650. <https://doi.org/10.1080/09502386.2017.1416420>
- Szabo, N., 2011. "Bitcoin, what took ye so long?" Accessed June 19 2024. <http://www.unenumerated.blogspot.com/2011/05/bitcoin-what-took-ye-so-long.html>.
- Thaddeus, J. Beier. 1996. "Re: Is This as Insecure... (Really 'Fax Crypto')." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. January 1, 1996. <https://mailing-list-archive.cryptoanarchy.wiki/archive/1996/01/a4ec12c7f83ffa4fab392a9831add893732f3a3a0be515ab32139f8d1a72b3ab/>.
- Turner, Fred. 2006. "How Digital Technology Found Utopian Ideology: Lessons From the First Hackers' Conference." *Critical Cyberculture Studies: Current Terrains, Future Directions*.
- Whitaker, Russell E. 1992. "Hammill on Public Key." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. October 8, 1992. <https://mailing-list->

archive.cryptanarchy.wiki/archive/1992/10/6115ca8faf4522b00345f547f7092e8d3eb00e56e294c4e5b757d2dec8166589/.

Whitaker, Russell E. 1992. "Long but Good: Hammill on Encryption." Cryptoanarchy.Wiki - Cypherpunks Mailing List Archive. September 21, 1992. <https://mailing-list-archive.cryptanarchy.wiki/archive/1992/09/b5e24ee5d6a00a60a5cdd485ad3b67fa4016296e3d5df8faa2c6181e88494b20/>.