

The Rhetoric of Bitcoin:  
Money, Politics, and the Construction of Blockchain Communities

Matthew Bellinger

A dissertation  
submitted in partial fulfillment of the  
requirements for the degree of

Doctor of Philosophy

University of Washington

2018

Reading Committee:

Christine Harold, Chair

Leah Ceccarelli

Gina Neff

Program Authorized to Offer Degree:

Communication

© Copyright 2018

Matthew Bellinger

University of Washington

**Abstract**

The Rhetoric of Bitcoin: Money, Politics, and the Construction of Blockchain Communities

Matthew Bellinger

Chair of the Supervisory Committee:

Christine Harold

Department of Communication

The rise of Bitcoin and related digital currencies has been accompanied by a proliferation of discourse about these technologies, including debates about their value and status as forms of money. This dissertation examines digital currency discourse from a rhetorical perspective, and traces the development and impact of a key trope of early Bitcoin discourse—the application of commodity money rhetoric to Bitcoin—to understand the rhetorical construction of Bitcoin. It argues that early attempts to establish Bitcoin as a form of money, which figured Bitcoin as a “natural” entity beyond the reach of community politics, produced an unanticipated rhetorical fallout: the displacement of the politics of the Bitcoin community onto the development of Bitcoin as a technology. It further argues that this early displacement continues to influence the rhetorical dynamics of Bitcoin and its heirs by shaping subsequent debates over digital currency governance and valuation.

## Acknowledgments

This project was made possible by the aid of many people. First and foremost among those deserving of thanks are my dissertation advisor, Christine Harold, and the members of my dissertation committee: Leah Ceccarelli, Gina Neff, and Candice Rai. I am deeply grateful for their mentorship throughout my time at the University of Washington. Also worthy of recognition, for the intellectual stimulation and academic commiseration that they provided, are Will Mari, Ruth Moon Mari, Bob Hodges, and Allen Baros. I hope that I always have the fortune to work alongside such gracious colleagues. The Walter Chapin Simpson Center for the Humanities, in concert with the Andrew K. Mellon Foundation, provided support for early stages of this dissertation, and the encouragement of Steve and Jeanne Bellinger, long an integral part of my academic journey, was an invaluable aid in bringing the project to completion. For their years of support, I am truly thankful. And finally, to the love and unending patience of Shannon Liudahl, I am forever indebted.

*Everyone has to make up their mind if money is money or money isn't money and sooner or later they always do decide that money is money.*

Gertrude Stein

## Table of Contents

Introduction .....	1
Nine years later .....	3
The discourse of Bitcoin .....	8
From discourse to rhetoric .....	14
The rhetoric of Bitcoin .....	18
Chapter One: Tearing the Veil: Money and Discourse between Economics and Sociology ...	22
Weaving a “neutral veil”: Money and the <i>Methodenstreiten</i> .....	29
The “rediscovery” of money .....	39
The influence of the performative turn .....	47
Bitcoin and the rhetoric of money .....	58
Chapter Two: Constructing a Collective: Digital Metallism and the Procedural Rhetoric of Bitcoin .....	61
The rhetorical problem of establishing money .....	62
From commodity to code .....	67
Procedural rhetoric and rhetorical ecologies .....	73
Locating Bitcoin’s procedural rhetoric .....	77
Bitcoin’s rationale .....	80
Digital signatures .....	83
Cryptographic hash functions .....	86
Defining an electronic coin .....	87
The double spend problem and proof of work .....	90
Interpreting the protocol .....	97
Chapter Three: Contesting Development: Ethics, Politics, and Expertise in the Bitcoin Community .....	102
The Satoshi affair .....	106
The rhetorical significance of Nakamoto .....	111
The ethics and politics of protocol development .....	118
The block size crisis .....	130
What would Satoshi do? .....	136
Nakamoto and the politics of development .....	145
Chapter Four: Rewriting History: On Blockchain Forks and Cryptocurrency Identity .....	149
Ethereum, smart contracts, and decentralized autonomous organizations .....	152
The DAO attack .....	161
Blockchain forks .....	166
Responses to the attack on The DAO .....	170
The rhetoric of blockchain forks .....	181
Conclusion: The Future of Cryptocurrencies .....	186
Bibliography .....	191

## Introduction

It began like something from a cyberpunk novel. On November 1<sup>st</sup>, 2008, an individual or group using the pseudonym “Satoshi Nakamoto” emailed a cryptography mailing list:

I’ve been working on a new electronic cash system that’s fully peer-to-peer, with no trusted third party.

The paper is available at: <http://www.bitcoin.org/bitcoin.pdf><sup>1</sup>

The linked paper—nine pages of dense, technical writing—described Bitcoin,<sup>2</sup> a new technology for sending payments across the Internet.<sup>3</sup> The paper both explicitly and implicitly situated Bitcoin within a multi-decade history of proposals for cash-like online payment systems, but offered a new combination of cryptographic protocols and economic incentives.<sup>4</sup> Unlike past proposals in a similar vein, Bitcoin did not require the use of

---

<sup>1</sup> Satoshi Nakamoto, “Bitcoin P2P E-Cash Paper,” November 1, 2008, <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>.

<sup>2</sup> The term “Bitcoin” can refer to both the payment system and to the units of account tracked by this system (i.e., to both the means of transferring currency and the currency itself) precisely because the technology erases the distinction between the two. For the sake of clarity, this study uses capitalization to distinguish Bitcoin (the monetary technology) from bitcoins (tokens or units of account), following the convention of Pedro Franco, *Understanding Bitcoin: Cryptography, Engineering, and Economics* (Chichester, UK: John Wiley & Sons, 2015). Quantities of bitcoins are indicated by the abbreviation “BTC.”

<sup>3</sup> Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008, <https://bitcoin.org/bitcoin.pdf>.

<sup>4</sup> Explicitly named precursors include Wei Dai, “B-Money,” 1998, <http://www.weidai.com/bmoney.txt>; and Adam Back, “Hashcash - A Denial of Service Counter-Measure,” August 1, 2002, <http://www.hashcash.org/papers/hashcash.pdf>; for the listserv’s cryptographic audience, the paper also clearly builds on David Chaum, “Blind

intermediaries—such as a bank or a payments processor—to keep participants in its payment network honest. Instead, it utilized a decentralized network, analogous to that of the file-sharing protocol BitTorrent, with no centralized clearinghouse necessary to validate transactions. The end result was a “digital currency”—a monetary form native to the Internet and inseparable from it. Like more familiar online payment systems (e.g., Visa, PayPal), Bitcoin could be used to make purchases and exchange funds via the Internet. But in contrast to these older forms of payment, Bitcoin promised the privacy, independence, and decentralization of cash.

The initial response on the mailing list was skeptical. “We very, very much need such a system,” one list subscriber replied, “but the way I understand your proposal, it does not seem to scale to the required size.”<sup>5</sup> Another subscriber responded with an economic critique: “[T]he real issue with this system is the market for bitcoins.”<sup>6</sup> Bitcoin could not function as a currency in market exchange, the respondent argued, because Bitcoin’s computational foundations “have no intrinsic value.”<sup>7</sup> Cryptographer Hal Finney, who would later collaborate with Nakamoto in developing the early versions of Bitcoin’s

---

Signatures for Untraceable Payments” (Santa Barbara, CA: University of California, 1982); and David Chaum, Amos Fiat, and Moni Naor, “Untraceable Electronic Cash,” in *Advances in Cryptology -- CRYPTO '88*, Lecture Notes in Computer Science (Springer, 1988), 319–27, [https://doi.org/10.1007/0-387-34799-2\\_25](https://doi.org/10.1007/0-387-34799-2_25); for a popular history of the relevant cryptographic community (i.e., “cypherpunks”), see Andy Greenberg, *This Machine Kills Secrets: How WikiLeaks, Cypherpunks, and Hactivists Aim to Free the World's Information* (New York: Dutton, 2012).

<sup>5</sup> James A. Donald, “Re: Bitcoin P2P e-Cash Paper,” November 2, 2008, <https://www.mail-archive.com/cryptography@metzdowd.com/msg09963.html>.

<sup>6</sup> Ray Dillinger, “Re: Bitcoin P2P e-Cash Paper,” November 7, 2008, <https://www.mail-archive.com/cryptography@metzdowd.com/msg09970.html>.

<sup>7</sup> Ibid.

software, was more optimistic. “Bitcoin seems to be a very promising idea,” Finney wrote. “It is a very modern notion that exploits the power of the long tail. When Wikipedia started I never thought it would work, but it has proven to be a great success for some of the same reasons.”<sup>8</sup>

Despite this mixed reception, only a few months later, on January 3<sup>rd</sup>, 2009, Nakamoto released the first Bitcoin software. The same day, Finney downloaded the software, and received the world’s first Bitcoin transaction: 10 BTC sent by Nakamoto. The Bitcoin network was live, and Nakamoto’s white paper found its first instantiation. Bitcoin was born.

### *Nine years later*

Much has changed since then. Over the course of the last nine years, Bitcoin has grown from an obscure proposal on an esoteric mailing list to a formidable economic force. As of January 18<sup>th</sup>, 2018, hundreds of thousands of Bitcoin transactions regularly occur each day,<sup>9</sup> one Bitcoin is valued at roughly \$11,300 USD<sup>10</sup>—down from a peak price just shy of \$20,000 USD—and the Bitcoin market capitalization sits at \$190 billion USD.<sup>11</sup> Bitcoins

---

<sup>8</sup> Hal Finney, “Re: Bitcoin P2P e-Cash Paper,” November 8, 2008, <https://www.mail-archive.com/cryptography@metzdowd.com/msg09975.html>.

<sup>9</sup> “Number of Transactions per Day,” Blockchain.info, accessed January 18, 2018, <https://blockchain.info/charts/n-transactions>.

<sup>10</sup> “Market Price (USD),” Blockchain.info, accessed January 18, 2018, <https://blockchain.info/charts/market-price>.

<sup>11</sup> “Market Capitalization,” Blockchain.info, accessed January 18, 2018, <https://blockchain.info/charts/market-cap>.

are traded on several currency exchanges,<sup>12</sup> and they are accepted by a variety of online merchants, including the web-hosting platform Wordpress.com and the retailer Overstock.com. Bitcoin is also accepted by a growing number of brick and mortar stores, and with the support of new ecosystems of apps and associated technologies (e.g., currency conversion ATMs), Bitcoin consumer transactions are increasingly approaching the everyday experience of using a credit or debit card. In contrast to the convoluted technical process involved in the Nakamoto's first transaction with Finney, today a typical Bitcoin transaction at a brick and mortar store looks something like this: A customer walks into a shop that accepts Bitcoin, and selects whatever item the customer wants to purchase. At the register, instead of paying with cash or card, the shopkeeper scans a QR code generated by an app on the customer's smartphone. The app then broadcasts the transaction with the shopkeeper to the Bitcoin network, and the customer is free to leave the store with his or her purchase. Today, paying with Bitcoin is not much more complicated than paying with a card or cash.<sup>13</sup>

The Bitcoin community has changed as well. The person or persons behind the pseudonym of Satoshi Nakamoto—whose real identity or identities remain unproven,

---

<sup>12</sup> "Bitstamp," Bitstamp, accessed January 19, 2018, <https://www.bitstamp.net/>; "Bitfinex," Bitfinex, accessed January 19, 2018, <https://www.bitfinex.com/>; "Coinbase," Coinbase, accessed January 19, 2018, <https://www.coinbase.com/>; "Kraken," Kraken, accessed January 19, 2018, <https://www.kraken.com/>; "BTCChina," BTCChina, accessed January 19, 2018, <https://www.btcchina.com/>.

<sup>13</sup> In the final months of drafting this dissertation, one significant complication to the everyday use of Bitcoin did in fact develop: high transaction fees associated with the difficulties of scaling Bitcoin to accommodate larger numbers of users. The increase in transaction costs and the Bitcoin community's response to it are notable and worthy of study in their own right, but because these developments emerged beyond the time frame covered by this project I leave this issue to be covered in future work.

despite multiple high-profile, journalistic “unmaskings”<sup>14</sup>—has withdrawn from engagement with Bitcoin, and the development and maintenance of the free and open-source technology now rests with the community of Bitcoin supporters. Importantly, this community now exists within a much broader network of digital currency enthusiasts, advocates, and experts: Bitcoin has inspired hundreds of additional digital currencies, and now discussions of Bitcoin’s development and future take place alongside similar discussions of second and third generation “altcoins” (alternative coins).<sup>15</sup> Though Bitcoin is still by far the most well-known and prominent digital currency, it increasingly seems that the Bitcoin community is one among many—an influential subset of a much larger social formation.

But perhaps the most dramatic development for Bitcoin is its increasing visibility to the general public. Bitcoin now regularly draws coverage from *The New York Times* and

---

<sup>14</sup> Nakamoto claimed to be a Japanese man in his thirties. However, there is no conclusive evidence indicating that Nakamoto was Japanese, male, of such an age, or even an individual person rather than a group. Widely discussed—though not necessarily widely accepted—candidates for Nakamoto’s real identity include computer scientist Nick Szabo, who proposed a Bitcoin precursor called “bit gold”; and computer scientist Craig Steven Wright, who claimed to be Nakamoto and provided disputed cryptographic evidence to support his claim. See, respectively, Nathaniel Popper, “Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin,” *The New York Times*, May 15, 2015, <https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html>; and Andrew O’Hagan, “The Satoshi Affair,” *London Review of Books*, June 30, 2016, <https://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair>. In light of the uncertainty about Nakamoto’s identity, this study adopts the convention of referring to Nakamoto in terms consistent with the pseudonymous identity (i.e., the masculine singular pronoun).

<sup>15</sup> Over 800 cryptocurrencies now exist, and the total market capitalization of these currencies exceeds \$100 billion USD. However, the large majority of this value is tied to a handful of prominent currencies, such as Bitcoin, Litecoin, and Ethereum. In contrast to these big players in the cryptocurrency market, most currencies trade at less than \$0.01 USD. See “CryptoCurrency Market Capitalizations,” CoinMarketCap, accessed July 3, 2017, <http://coinmarketcap.com/currencies/views/all/>.

similarly prominent media outlets—in addition to coverage provided by new, digital currency-focused media platforms, such as *CoinDesk*<sup>16</sup>—and the currency has attracted the attention, interest, and investment of a host of individuals and groups, ranging from technologists to financiers, from regulators to artists. Admittedly, substantial portions of this attention has been negative: Bitcoin’s public perception has suffered from its association with Dark Web markets (e.g., Ross Ulbricht’s infamous Silk Road),<sup>17</sup> its use as the currency of choice for major ransomware attacks (e.g., the May 2017 WannaCry attack),<sup>18</sup> and its employment in a variety of Ponzi schemes and related forms of fraud<sup>19</sup>—not to mention condemnation by influential figures in finance and economics, who lambast the currency as economically unsound at best and fraudulent at worst.<sup>20</sup> But even these negative associations have served to bring the terms “Bitcoin” and “digital currency” to the vocabulary of those far removed from arcane discussions on cryptography listservs.

---

<sup>16</sup> “CoinDesk,” CoinDesk, accessed October 4, 2017, <https://www.coindesk.com/>.

<sup>17</sup> See Joshua Bearman, “Silk Road: The Untold Story,” *Wired*, May 23, 2015, <https://www.wired.com/2015/05/silk-road-untold-story/>.

<sup>18</sup> For example, Brian Fung, “What You Need to Know about Bitcoin after the WannaCry Ransomware Attack,” *Washington Post*, May 15, 2017, <https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack/>.

<sup>19</sup> It is worth noting that Bitcoin is far from unique in this respect; prior digital currencies have been favored as vehicles for money laundering and investment scams. See P. Carl Mullan, *A History of Digital Currency in the United States: New Technology in an Unregulated Market* (New York: Palgrave Macmillan, 2016).

<sup>20</sup> For example, see Paul Krugman, “Bitcoin Is Evil,” *The New York Times*, December 28, 2013, <http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/>; and David Henry and Anna Irrera, “JPMorgan’s Dimon Says Bitcoin ‘Is a Fraud,’” *Reuters*, September 13, 2017, <https://www.reuters.com/article/legal-us-usa-banks-conference-jpmorgan/jpmorgans-dimon-says-bitcoin-is-a-fraud-idUSKCN1BN2PN>.

Yet all of these changes over the last nine years—Bitcoin’s meteoric economic growth, the development and expansion of the digital currency community, and the increasing prominence of such currencies in the public eye—have only served to raise additional and increasingly pressing questions about Bitcoin’s economic, social, and political significance. Bitcoin is hardly the first electronic cash system, but it is the first to reach such a level of success, and this has spurred a tremendous amount of discourse *about* Bitcoin.<sup>21</sup> The range of people praising, condemning, or otherwise offering analyses of the technology is considerable, and includes software developers, venture capitalists, engineers, law enforcement officers, bankers, lawyers, politicians, journalists, financial regulators, and academics from multiple disciplines—in addition to the commentary from the average Bitcoin user. Their conversations and debates are spread across a broad range of media—including books (both scholarly and popular), message boards, white papers, MOOCs, peer-reviewed journal articles, newspaper columns, chat rooms, podcasts, documentary films, and more—and they address a wide range of questions, many of which cut to the heart of contemporary assumptions about money, economics, and society. What exactly are the economics of this new payment system? Is it a bubble? Is Bitcoin best understood as a currency—or as a commodity, or as a security, or as an entirely new economic object? Is it really money? (And what, after all, *is* money?) What should its regulatory status be? *Can* it be regulated? How should the technology be developed further? What is the role of the community that supports it? Will Bitcoin eventually challenge the hegemony of the US dollar—or will it remain a monetary novelty? There is

---

<sup>21</sup> For an account of Bitcoin’s precursors, see Mullan, *A History of Digital Currency in the United States*.

even considerable debate over basic terminological matters: Should Bitcoin be called a “digital currency,” a “cryptocurrency,” a “virtual currency,” or perhaps something else?

### *The discourse of Bitcoin*

As intriguing as these individual questions may be, this proliferation of discourse itself points to two key dimensions of Bitcoin. First, while the sheer volume of discourse about Bitcoin certainly indicates growth of attention and interest in the currency, it also evidences Bitcoin’s interpretive flexibility over the last nine years.<sup>22</sup> Bitcoin discourse has been dominated by Bitcoin *debates*, and the fact that such foundational questions as “Is Bitcoin a currency or a commodity?” still generate a multitude of responses nearly a decade since the technology’s introduction shows that the social construction of Bitcoin is in its early stages, far from closure. Second, all of this commentary, analysis, and critique—all of the responses to variations of *How did this all happen? What does it all mean?* and *What will happen next?*—is not divorced from its object. To the contrary, the myriad attempts to address the questions of Bitcoin’s economic, social, and political significance—from top-of-the-head message board musings to rigorously argued academic articles—are themselves *participants in Bitcoin’s development* as both a technology and as a form of money.<sup>23</sup> And

---

<sup>22</sup> Trevor J. Pinch and Wiebe E. Bijker, “The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit from Each Other,” *Social Studies of Science* 14, no. 3 (1984): 399–441; Wiebe E. Bijker, *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change* (Cambridge, MA: MIT Press, 1995).

<sup>23</sup> As Mallard et al. write in their study of expert discourse on Bitcoin, the proliferation of Bitcoin discourse “is a witness to how the Bitcoin debates do not merely spread, communicate and diffuse representation of this currency, but are closely intertwined with the practice of the money itself.” Alexandre Mallard, Cécile Méandel, and Francesca Musiani, “The Paradoxes of Distributed Trust: Peer-to-Peer Architectures and User

while the precise nature of this participation is far from self-evident—a point to which I return for a more detailed consideration in chapter one—the Bitcoin community nevertheless features a wealth of examples suggesting that discourse plays some significant role in Bitcoin’s development. Discussions of Bitcoin’s value, for instance, influence and are influenced by market activity: “True believers” in Bitcoin’s “intrinsic” value readily endorse the purchase of bitcoins in the midst of price crashes, and in doing so contribute to the liquidity of Bitcoin exchanges. Similarly, discussions of Bitcoin’s technological design (e.g., Bitcoin improvement proposals)<sup>24</sup> are not only integral to the processes of Bitcoin’s development as open source software, but also have implications for Bitcoin’s broader acceptance by those outside the Bitcoin community (e.g., the feasibility of increasing the capacity of the Bitcoin network to accommodate more users).<sup>25</sup> In short, Bitcoin’s spectacular rise and its attendant uncertainties seem to be intimately bound with communication about that rise and those uncertainties. Bitcoin cannot be understood simply as an economic or technological phenomenon; it is a *discursive* phenomenon, too. And if Bitcoin is at least in part a matter of discourse, then making sense of the developments of the last nine years entails not only the study of Bitcoin as software or as an economic system, but also the study of Bitcoin discourse.

---

Confidence in Bitcoin,” *Journal of Peer Production* 4 (2014), <http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust/>.

<sup>24</sup> The Bitcoin improvement proposal (BIP) system is the Bitcoin development community’s protocol for proposing modifications to the underlying Bitcoin software. See “BIP Purpose and Guidelines,” GitHub, August 19, 2011, <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki>.

<sup>25</sup> Andrew Marshall, “Bitcoin Scaling Problem, Explained,” CoinTelegraph, March 2, 2017, <https://cointelegraph.com/explained/bitcoin-scaling-problem-explained>.

Of course, given that the study of technologies and discourse in periods of uncertainty has a long history within science and technology studies (STS) and its disciplinary relatives, the conclusion that Bitcoin discourse warrants investigation is hardly radical.<sup>26</sup> But Bitcoin moves beyond the well-worn path of the typical STS case study in one crucial dimension: Bitcoin is a *monetary* technology. This places Bitcoin's study squarely within much broader debates concerning the nature of money, markets, finance, and contemporary capitalism—debates that range across economics, sociology, anthropology, and related disciplines. Because Bitcoin is a monetary technology, the study of the discursive construction of Bitcoin—the work of following the path from Nakamoto's first email to the multi-thousand dollar valuation of today—necessarily involves the reexamination of deep assumptions within the social sciences and humanities about both money as an object of study (including, not the least of all, which disciplines can and should study it) and money as a key conceptual tool for the analysis and explanation of social, political, and economic systems.<sup>27</sup> And by reexamining such assumptions about money, new lines of inquiry are opened: For instance, if our understanding of *money* changes in light of Bitcoin, how does this change alter analyses and explanations of markets, exchange, the nation state, or capitalism more generally? Simply put, as a technology in the process of

---

<sup>26</sup> For example, Wiebe E. Bijker, Thomas P. Hughes, and Trevor J. Pinch, eds., *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology* (Cambridge, MA: The MIT Press, 1987).

<sup>27</sup> That is to say, reexamining money leads to reexamining the ways that explanations of social and economic phenomena depend on particular conceptions of money. In his review of the anthropological study of money, for example, Bill Maurer notes that “[t]he difficulty in reviewing the anthropology of money is compounded by the reliance of much anthropological research on theories of meaning and symbol that derived analytical precision through monetary metaphors.” Bill Maurer, “The Anthropology of Money,” *Annual Review of Anthropology* 35 (2006): 16, <https://doi.org/10.1146/annurev.anthro.35.081705.123127>.

becoming (or reconfiguring) money, Bitcoin affords far more than the chance to analyze the early, uncertain, and contested development of a new technology; it also presents the opportunity to contribute to a much broader research agenda that intersects with concerns across the social sciences and humanities.

Admittedly, this opportunity also presents a bit of a self-reflexive trap: As was noted above, the analysis of Bitcoin discourse necessarily contributes to its object of study. To some degree this dynamic is unavoidable, but there is a useful distinction to be drawn between the study of Bitcoin discourse *qua* discourse and the majority of the contributions to that body of discourse. For the former, the point is not to *resolve* the uncertainties threaded throughout Bitcoin discourse—to settle the question of Bitcoin’s valuation, for instance, or to offer policy suggestions to regulators. Instead, the point is to show how particular discursive practices both respond to and construct Bitcoin as a new object within social, political, and economic life—even if analysis of these practices does, ultimately, contribute in some way to the processes under examination. The key here is the line of questioning provoked by such an approach: It generates questions that focus on the relationship between Bitcoin as a monetary technology and Bitcoin as a body of discourse. How do Bitcoin commentators, for example, attempt to construct Bitcoin as a form of money through their discursive interventions? (Put differently, how do these actors self-consciously attempt to produce the *social* through *individual* action?) What barriers do these discursive attempts face, and how do individuals and groups opposed to the construction of Bitcoin-as-money respond? And what are the consequences of these discursive choices? How do early characterizations of Bitcoin enable or constrain subsequent discursive action?

These questions are not well represented within the burgeoning literature of digital currency studies. While a growing number of studies reference some aspect of “Bitcoin discourse” in the course of sociological, political, or cultural analysis, these references tend either to be high-level surveys of community sentiments (often tied to price analyses) or to function more as summaries of a given scholar’s impressions of the Bitcoin community, as opposed to detailed analyses of specific texts.<sup>28</sup> In short, these veins of scholarship treat Bitcoin discourse as evidence to be marshaled in the explanation of some other phenomenon under investigation (e.g., Bitcoin prices, the political ideology of the Bitcoin community, the role of algorithms in contemporary culture), rather than as an object itself requiring explanation.

There is, however, a thread of scholarship that *has* begun exploration of the questions above, primarily by focusing on the communicative strategies utilized by participants in the Bitcoin community to establish the digital currency as an economic object. That is to say, these studies have focused on how Bitcoin enthusiasts attempt to convince others (and themselves) that Bitcoin—despite all its differences from the everyday experience of contemporary, state-produced, fiat currencies—really is a form of *money*. In particular, two studies are key for this area of research. First, Maurer, Nelms, and

---

<sup>28</sup> For example, see Henrik Karlstrøm, “Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin,” *Distinktion: Scandinavian Journal of Social Theory* 15, no. 1 (2014): 23–36, <https://doi.org/10.1080/1600910X.2013.870083>; Vasilis Kostakis and Chris Giotitsas, “The (a)Political Economy of Bitcoin,” *TripleC* 12, no. 2 (2014): 431–40; David Golumbia, *The Politics of Bitcoin: Software as Right-Wing Extremism* (Minneapolis, MN: University of Minnesota Press, 2016); Ed Finn, *What Algorithms Want: Imagination in the Age of Computing* (Cambridge, MA: MIT Press, 2017); and to a lesser extent, Mallard, Méandel, and Musiani, “The Paradoxes of Distributed Trust”; and Lana Swartz, “Blockchain Dreams: Imagining Techno-Economic Alternatives after Bitcoin,” in *Another Economy Is Possible: Culture and Economy in a Time of Crisis*, ed. Manuel Castells (Malden, MA: Polity, 2017), 82–105.

Swartz, writing from an anthropological perspective, have studied the social semiotics of Bitcoin.<sup>29</sup> In their foundational essay, Maurer et al. argued that early discourse about Bitcoin's value was constructed in a manner analogous to that of commodity-backed monies insofar as "[t]he discursive politics of Bitcoin involves a similar foregrounding of materiality and backgrounding of credit relations."<sup>30</sup> However, instead of guaranteeing value through reference to silver or gold, Maurer et al. found that Bitcoin was represented by members of the Bitcoin community as being "backed" by Bitcoin's code. In essence, the software itself served as the semiotic guarantee for claims about Bitcoin's value—a strategy that Maurer et al. name "digital metallism." This analysis has been borne out by the second important contribution to studies of Bitcoin discourse: Lynette Shaw's examination of Bitcoin message boards.<sup>31</sup> Using automated content analysis, Shaw showed the prevalence of digital metallist discourse throughout the Bitcoin community, though she also noted a shift in recent years *away* from digital metallist discourse and towards discourse more focused on "blockchain," one of the key technological elements underpinning both Bitcoin and its currency heirs.

In sum, this burgeoning area of scholarship has made important strides toward understanding the role of Bitcoin discourse in the social construction of the currency by

---

<sup>29</sup> Bill Maurer, Taylor C. Nelms, and Lana Swartz, "When Perhaps the Real Problem Is Money Itself!': The Practical Materiality of Bitcoin," *Social Semiotics* 23, no. 2 (2013): 261–77, <https://doi.org/10.1080/10350330.2013.777594>; also see Deja Elana Swartz, "Tokens, Ledgers, and Rails: The Communication of Money" (Ph.d. diss., University of Southern California, 2015).

<sup>30</sup> Maurer, Nelms, and Swartz, "When Perhaps the Real Problem Is Money Itself!," 262.

<sup>31</sup> Lynette Shaw, "The Meanings of New Money: Social Constructions of Value in the Rise of Digital Currencies" (Ph.D. diss., University of Washington, 2016).

examining a key trope (digital metallism) and by highlighting the extent to which such social construction is tied to particular strategies of *persuasion*. To be sure, this is a valuable contribution to the study of Bitcoin and to the study of money more broadly. However, while the identification of this trope in Bitcoin discourse is a helpful initial step, there is still a need to study how digital metallism is *used* in specific instances. There is also a need to examine, especially in light of Shaw's findings about the changing prevalence of digital metallist discourse, the way that the use and influence of such tropes have evolved over time. A trope employed to resolve a persuasive challenge early in the history of Bitcoin, for instance, may not function in the same manner at a later point—when the currency is more established, when the membership of the Bitcoin community has changed, when Bitcoin is one among many similar digital currencies, etc. Indeed, changes in Bitcoin's context might even render such tropes discursive liabilities rather than resolutions to discursive problems. The naming of digital metallism is an important first step, but more work is needed.

#### *From discourse to rhetoric*

Given this need for further examination and analysis of Bitcoin tropes—and the need to better account for the relationship between money, technology, and discourse more broadly—the present study conducts a rhetorical analysis of several key persuasive moments in the history of Bitcoin and its heirs to advance understanding of how the discourse and technology of Bitcoin interact and develop over time. My aim is to contribute to the burgeoning analysis of Bitcoin as a discursive object—with an eye towards advancing the broader scholarly project of understanding the social, political, and

economic dimensions of digital currencies—and my choice of a rhetorical perspective is meant as a direct complement to the initial analyses of Maurer et al. and Shaw.

Consequently, it is worth spending a moment to elucidate exactly what such a perspective entails, and how it serves as a methodological and analytical complement to prior studies.

Four points inform my choice of a rhetorical perspective. First, the discursive act of attempting to *persuade*—previously identified in the case of digital metallism—is rhetoric in the most traditional sense, so the object of study is already well suited for rhetorical investigation. Second, the key limitation of rhetorical analysis, the inability to generalize beyond the specifics of a text, has already been addressed by prior work, particularly in Shaw’s content analysis; indeed, now the need is precisely for analyses that focus on *specific* rhetorical instances, rather than on general discursive trends. Third, the defining feature of rhetorical analysis—the feature that sets the rhetorical tradition apart from, for instance, the parallel tradition of literary analysis—is its long emphasis on attending to the relationship between text and context.<sup>32</sup> Attending to this dynamic allows rhetorical critics to see, for example, how the repeated invocation of a particular rhetorical trope alters its significance in each new instance, precisely because prior texts shape subsequent contexts. In other words, the persistence of a particular trope necessarily changes its rhetorical significance—a point relevant to the analysis of Bitcoin discourse, and crucially, one for which content analysis (e.g., Shaw’s study) cannot account. And finally, given that Bitcoin is

---

<sup>32</sup> To put it somewhat reductively: In rhetorical studies, New Criticism never happened. See Herman Cohen, *The History of Speech Communication: The Emergence of a Discipline, 1914-1945* (Washington, DC: National Communication Association, 1994); Pat J. Gehrke, *The Ethics and Politics of Speech: Communication and Rhetoric in the Twentieth Century* (Carbondale, IL: Southern Illinois University Press, 2009); and Steven Mailloux, *Disciplinary Identities: Rhetorical Paths of English, Speech, and Composition* (New York: Modern Language Association, 2006).

both a matter of software and of discourse, the recently developed analytical tools of digital rhetoric are particularly relevant for understanding the ways in which the procedural rhetoric of Bitcoin as a protocol and as software may work within a broader rhetorical ecology—that is, in concert *or* in opposition to Bitcoin discourse.<sup>33</sup>

For these reasons, I believe that the tools of the rhetorical tradition offer a useful complement to prior analyses of Bitcoin discourse. That said, the very features of Bitcoin discourse that make it so intriguing—its rapid proliferation and its range of contested perspectives—raise a significant challenge to the application of rhetorical analysis to the case of Bitcoin. Simply put, given the constantly growing archive of Bitcoin discourse, how can one possibly choose specific texts for analysis? For this project, I have assembled and examined an archive of hundreds of texts (news articles, white papers, books, etc.), and while my chronological constraints do offer something of a useful limit—for example, relatively few books on Bitcoin were published in the first few years of its existence—the challenges of selecting texts and justifying these selections remain.

My response to these challenges is informed by both theoretical and practical concerns. First, following the work of Michael McGee, I see the work of the rhetorical scholar as intertwined with the production of the object of study from rhetorical

---

<sup>33</sup> Though I discuss these tools more extensively in the chapters that follow, here it is worth noting particularly relevant methodological guides for this kind of analysis: Ian Bogost, *Persuasive Games: The Expressive Power of Videogames* (Cambridge, MA: MIT Press, 2007); James J. Brown Jr., *Ethical Programs: Hospitality and the Rhetorics of Software* (Ann Arbor, MI: University of Michigan Press, 2015); and Douglas Eyman, *Digital Rhetoric: Theory, Method, Practice* (Ann Arbor, MI: University of Michigan Press, 2015).

fragments,<sup>34</sup> and I take this assembly to be all the more necessary in the analysis of artifacts of digital culture.<sup>35</sup> This assembly is not, however, an arbitrary or capricious process; instead, my identification of relevant rhetorical fragments is guided by Maurer et al. and Shaw's prior work, and I frame my investigation by tracing the rhetorical implications, so to speak, of a key trope (i.e., digital metallism) that prior scholars have identified. Second, I focus my analytical attention on episodes of "punctuated crisis" within the Bitcoin community.<sup>36</sup> Focusing on moments of controversy and contestation has the triple benefit of constraining my archive of materials (since key texts are identified and cited by participants *within* the archive), of highlighting points of rhetorical uncertainty (i.e., the still "in development" and "flexible" portions of Bitcoin discourse), and of implicitly figuring the rhetorical and conceptual norms against which such controversies take place (i.e., by demonstrating both what is and what is *not* up for debate).<sup>37</sup> And finally, because a key

---

<sup>34</sup> Michael Calvin McGee, "Text, Context, and the Fragmentation of Contemporary Culture," *Western Journal of Speech Communication* 54, no. 3 (1990): 274–89, <https://doi.org/10.1080/10570319009374343>.

<sup>35</sup> Though McGee's call for the assembly of rhetorical fragments was written with a media environment quite different from that of the present in mind, the move to self-conscious production of the critical text prefigures important developments in contemporary studies of digital culture. The assembly of rhetorical fragments, by rejecting an understanding of the text as self-evidently delineated, turns attention to rhetorical process rather than rhetorical product—a move echoed by more recent the turn in the digital humanities to "algorithmic reading," which "take[s] the culture machine itself as the object of study, rather than just its cultural outputs." Finn, *What Algorithms Want*, 53.

<sup>36</sup> I borrow this term from Gabriella Coleman's study of the Debian development community. Her focus on moments of crisis as key to understanding the dynamics of free and open source software (F/OSS) communities offers a helpful model for the analysis Bitcoin, which also functions along F/OSS lines. See E. Gabriella Coleman, *Coding Freedom: The Ethics and Aesthetics of Hacking* (Princeton: Princeton University Press, 2013).

<sup>37</sup> On this last point, I am heavily indebted to studies of digital culture that see errors, glitches, and failures—in short, moments when technology and discourse seem to go

feature of my study is the focus on processes of rhetorical legitimation—that is, the management of politics within the Bitcoin community—I pay special attention to texts that attempt to reinforce their own legitimation through their choice of publication platform. That is to say, I pay close attention to white papers, technical documentation, and the like, not because these *are* definitive instances of Bitcoin rhetoric, but because the choice of platform or medium (e.g., white paper versus message board post) suggests that they are *meant* as such. This is not to say that I have avoided more ephemeral rhetorical interventions, but rather that the nature of my analysis has demanded that I pay special attention to more formal genres and modes of publishing.

### *The rhetoric of Bitcoin*

Ultimately, my rhetorical analysis of Bitcoin leads me to argue three key claims. First, rhetorical choices made early in Bitcoin's history—specifically, the embrace of digital metallism as a trope of monetary legitimation—resulted in a shift of the space of political contest in the Bitcoin community from the *economic production and utilization* of Bitcoin as a form of money to the *development* of Bitcoin as software. Second, this rhetorical shift from a politics of money to a politics of development introduced an apparently unanticipated rhetorical dynamic into the Bitcoin community: Collapsing decisions about development and decisions about the community's future meant that those able to perform

---

*wrong*—not as anomalies to be dismissed, but rather as opportunities to analyze otherwise overlooked processes. For example, see Finn Brunton, *Spam: A Shadow History of the Internet*, Infrastructures 4 (Cambridge, MA: MIT Press, 2013); Jussi Parikka and Tony D. Sampson, eds., *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture*, Communication Alternatives (Cresskill, NJ: Hampton Press, 2009); and Mark Nunes, ed., *Error: Glitch, Noise, and Jam in New Media Cultures* (New York: Continuum, 2011).

relevant technical expertise had more rhetorical “say” in the politics of the community, and left those *without* such expertise rhetorically constrained in their efforts to advocate for a particular vision of Bitcoin’s future. In turn, these rhetorical constraints prompted the development of rhetorical alternatives to technical expertise, including a kind of Bitcoin conservatism that used the person and writings of Bitcoin inventor Satoshi Nakamoto—in particular, Nakamoto’s “original vision” for Bitcoin—as a means of intervening in debates over Bitcoin’s development. Third, this displacement of politics—and the attendant heightening of the political stakes of development—persists beyond Bitcoin to influence Bitcoin’s technological and economic heirs, even in cases where the trope of digital metallism is not explicitly invoked, and this produces a dynamic in which the *rhetorical identity* of a given cryptocurrency plays a key role in maintaining economic value and stability. Ultimately, this suggests that the future of cryptocurrencies like Bitcoin will not simply be a matter of their economic or technological development, but will also depend on the extent to which the communities of such currencies are able to maintain a stable, cohesive identity that can compete with the identities underpinning other currencies (e.g., in the case of fiat currencies, national or regional identity). In short, valuation is at least in part dependent on the rhetorical performance of a single and consistent identity, which is something of a paradoxical challenge for Bitcoin and its heirs given the digital currency community’s early and persistent valorization of decentralization.

To advance these arguments, I proceed in four steps—each corresponding to a chapter of this dissertation—grouped into two sections: The first pair of chapters establish the study’s theoretical backdrop and introduce the key rhetorical dynamic of Bitcoin, while

the second pair traces the implications of this dynamic. In the first section, my initial point of departure is the key question that Bitcoin has faced since its inception, a question to which the trope of digital metallism implicitly responds: “Is Bitcoin money?” But because answering this question—and appreciating the implications of *attempts* to answer it—depends on understanding exactly what money *is*, in the first chapter I review the interdisciplinary literature on money as a social phenomenon, and show how the discursive dimensions of Bitcoin relate to key debates about the nature of money—primarily those situated at the border of economics and sociology—and how these debates offer an opening for rhetorical study to contribute to the study of money. With this theoretical backdrop established, in the second chapter I examine Nakamoto’s original white paper announcing Bitcoin. Here I offer an introduction to Bitcoin’s technical underpinnings while simultaneously reading the procedural rhetoric of Bitcoin—that is, the rhetoric of Bitcoin *as a protocol*—against Nakamoto’s own characterization of Bitcoin as a form of money. In doing so, I highlight the extent to which the key dynamic in Bitcoin’s procedural rhetoric is not so much monetary, but rather is a means of producing what I term an “individualist collective”: a shared sociality and shared history that, in keeping with the trope of digital metallism, nevertheless forecloses the political contestation inherent in the construction of both the social and the historical.

The second half of this dissertation traces the rhetorical fallout of this foreclosure of politics. In the third chapter, I turn to the strange case of pseudo-religious rhetoric centering on the person and writings of Satoshi Nakamoto—particularly as they relate to controversies over Nakamoto’s identity—and show how this figuring of Nakamoto served to enable participants to intervene, *contra* the technical expertise privileged by Bitcoin’s

development community, in the development (and by extension, the politics) of Bitcoin. Next, in the fourth chapter I move beyond the specific case of Bitcoin to examine the influence of this rhetorical dynamic on subsequent digital currencies. I examine the case of The DAO, a decentralized autonomous organization hosted on the Ethereum platform—a successor to Bitcoin—and show how a prominent theft from The DAO and the rhetorical response to this theft were influenced by the rhetorical dynamic introduced by the combination of digital metallism and Bitcoin’s procedural rhetoric. Finally, in the conclusion, I consider the implications of my analysis for digital currencies in the future, and for the interdisciplinary study of money more broadly.

## Chapter One

### Tearing the Veil: Money and Discourse between Economics and Sociology

Is Bitcoin money? Debate over the question actually predates Bitcoin's technical implementation; the email thread generated by Nakamoto's initial announcement took up the issue months before the first launch of Bitcoin software, and the matter has dogged Bitcoin ever since.<sup>1</sup> The question persists in newspapers,<sup>2</sup> in court rulings,<sup>3</sup> in regulatory guidelines<sup>4</sup>—not to mention the online discussions of the Bitcoin community—and it has provoked responses from computer scientists, economists, lawyers, artists, and more. And in one sense, it is hardly surprising that the question has sustained debate for so long, among such diverse participants, precisely because the stakes are so high. Responses to the question of “Is Bitcoin money?”—regardless of whether they ultimately deliver a “yes,” “no,” or “kind of”—are more than a matter of intellectual amusement. Rather, such responses articulate the manner and extent to which this new technology can and should be integrated into the social, political, cultural, and economic processes that cluster under the term “money.” Viewed from this perspective, the question of “Is Bitcoin money?” and its responses are legible as the negotiated attempt to fit a new phenomenon (Bitcoin) into

---

<sup>1</sup> Dillinger, “Re: Bitcoin P2P e-Cash Paper.”

<sup>2</sup> For example, Paul Krugman, “Golden Cyberfettters,” *The New York Times*, September 7, 2011, <http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfettters/>.

<sup>3</sup> For example, U.S. v. Murgio et al, U.S. District Court, Southern District of New York, No. 15-cr-00769

<sup>4</sup> For example, “IRS Virtual Currency Guidance,” Internal Revenue Service, March 25, 2014, <https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>.

relation with an already established social fact (money). It is not just a matter of constructing something new; it is a matter of constructing something new that fits recognizably with the old.

Yet viewed from another perspective, the persistence of this debate cannot help but appear somewhat surprising, since it seems that the steps necessary for *resolving* the question of “Is Bitcoin money?” are more or less clear. Presumably, the ambiguous part of the question lies in the word “Bitcoin.” It is Bitcoin, after all, which presents novelty; money is old and familiar. Bitcoin, despite its growth, is still relatively esoteric; money, by contrast, plays a quotidian role in the lives of billions. Presumably, then, if one is to construct a convincing answer to the question of “Is Bitcoin money?” one should compare the new, unsettled phenomenon (Bitcoin) to the well-worn concept (money). And presumably this comparison is a matter of *economic* analysis, since the comparison is between Bitcoin and a self-evidently economic concept, money.<sup>5</sup> Indeed, the argumentative sequence implied by this bundle of presumptions is familiar enough in the burgeoning field of digital currency studies: Begin with an economic definition of money (usually articulated in terms of money’s “features” or “functions”) and examine the extent to which Bitcoin meets this definition.<sup>6</sup> Compare and contrast. Spot the differences.

---

<sup>5</sup> The standards of evaluation might differ in other domains—for example, in legal analysis—but these still presume an economic foundation. In other words, even if the legal question of “Is Bitcoin money?” hinges on criteria (i.e., laws) different from those at play in economic analysis, the legal criteria are themselves attempts to grasp the underlying economic phenomenon.

<sup>6</sup> For example, Jan A. Bergstra and Peter Weijland, “Bitcoin: A Money-like Informational Commodity,” 2014, <https://arxiv.org/abs/1402.4778>; Konrad S. Graf, “Commodity, Scarcity, and Monetary Value Theory in Light of Bitcoin,” *Prices & Markets* 3, no. 3 (2015): 52–69; Brian P. Hanley, “The False Premises and Promises of Bitcoin,” 2013, <https://arxiv.org/abs/1312.2048>; Milhaela Iavorschi, “The Bitcoin Project and the Free

Crucially, this kind of analysis implies a particular relationship between Bitcoin, money, and discourse—a relationship that leaves little room for studying communication *about* Bitcoin. More precisely, if responses to the question of “Is Bitcoin money?” are understood in terms of *comparison*, in terms of holding a phenomenon against the standard of an economic concept, then discourse itself is epiphenomenal. From this perspective, Bitcoin discourse may (and perhaps even should) be evaluated in terms of accuracy of representation, of clarity of analysis, and so on—but ultimately Bitcoin relates, in something ranging from total identity to total exclusion, to the *economic* concept of money, and no amount of discourse can alter this. At best, then, discourse can clarify this relationship; at worst, it can obscure it. There is, in other words, a very old view of language and persuasion baked into the purely economic analysis of “Is Bitcoin money?”: From such a perspective, the only relevant discursive analysis is the analysis of style.<sup>7</sup>

Thus, how one understands money as a concept has a great deal of influence on how one understands the symbolic action of persuading others that something is or is not

---

Market,” *Center for European Studies Working Papers* 5, no. 4 (2013): 529–34; Stephanie Lo and J. Christina Wang, “Bitcoin as Money?,” *Current Policy Perspectives* (Boston, MA: Federal Reserve Bank of Boston, 2014); William J. Luther and Josiah Olson, “Bitcoin Is Memory,” *The Journal of Prices & Markets* 3, no. 3 (2015); Malovic Marko, “Demystifying Bitcoin: Sleight of Hand or Major Global Currency Alternative?,” *Economic Analysis* 47, no. 1–2 (2014): 32–41; Ísak Andri Ólafsson, “Is Bitcoin Money? An Analysis from the Austrian School of Economic Thought” (Master’s thesis, University of Iceland, 2014); George Selgin, “Synthetic Commodity Money,” *Journal of Financial Stability* 17 (April 2015): 92–99, <https://doi.org/10.1016/j.jfs.2014.07.002>; Peter Šurda, “Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold?” (Vienna University of Economics and Business, 2012); Beat Weber, “Can Bitcoin Compete with Money?,” *The Journal of Peer Production* 4 (2014), <http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoin-compete-with-money/>.

<sup>7</sup> Walter J. Ong, *Ramus, Method, and the Decay of Dialogue: From the Art of Discourse to the Art of Reason* (Chicago: University of Chicago Press, 2004).

money (e.g., responses to the question of “Is Bitcoin money?”). If the above presumptions hold, if “money” is taken as settled, fixed concept, then analysis of responses to the question of “Is Bitcoin money?”—including those of the “Yes, and here’s why you should exchange some currency or commodity or service for it...” variety—necessarily focuses on the ways that Bitcoin is represented as corresponding (or not) to this concept of money. But what if these foundational presumptions are reexamined? What if money, as a concept, is itself found to be unstable and uncertain? What then is the role of discourse in the study of Bitcoin?

A brief selection of quotations from the interdisciplinary scholarship on money serves to show that these questions are far from idle. Consider, for instance, economist Carl Menger’s dissatisfied assessment of the study of money, penned more than a century ago: “The enigmatic phenomenon of money is even at this day without an explanation that satisfies,” he complained. “[N]or is there yet agreement on the most fundamental questions of its nature and functions. Even at this day we have no satisfactory theory of money.”<sup>8</sup> Notwithstanding Menger’s efforts to remedy the matter in the remainder of his essay, decades later economist Joseph Schumpeter lamented the same lack of clarity and consensus: “There is no denying that views on money are as difficult to describe as are shifting clouds.”<sup>9</sup> And half a century beyond Schumpeter’s posthumously published lament, scholars of money still bemoaned the trouble provoked by their object of study. Sociologist Nigel Dodd, for instance, declared money studies to be a “muddle” because “there is no common view of what counts as ‘money’ in a more general sense”; in fact, “[t]here never

---

<sup>8</sup> Carl Menger, “On the Origin of Money,” *Economic Journal* 2, no. 6 (1892): 239.

<sup>9</sup> Joseph A. Schumpeter, *History of Economic Analysis*, ed. Elizabeth Boody Schumpeter (New York: Taylor & Francis, 2006), 276.

has been a consensus about this: the extant literature on money is replete with debates over competing definitions.”<sup>10</sup> Similarly, in his introduction to an interdisciplinary collection of essays on money, sociologist Geoffrey Ingham writes:

It is one of money’s many puzzles and paradoxes that there is such widespread disagreement on the essential nature of something that has been a commonplace, constituent element of human society for such a long time. The question of the ‘moneyness’ of money continues to produce a range of quite different answers.<sup>11</sup>

It is telling that Ingham immediately follows this assessment with academic folk stories *about the problem itself*:

Keynes is reputed to have said that he knew of only three people who really understood money: a professor at another university; one of his students; and a rather junior clerk at the Bank of England [...] The financier Baron Rothschild had made a similar observation a century earlier, but also added that unfortunately they disagreed.<sup>12</sup>

That such jokes can be told at all signals the extent to which, after more than a century of complaints about the puzzles of money, the gesture of decrying the confusion of money is itself a recognizable trope within the literature, a standard refrain required of any survey of the relevant scholarship.<sup>13</sup>

---

<sup>10</sup> Nigel Dodd, “Laundering ‘Money’: On the Need for Conceptual Clarity within the Sociology of Money,” *European Journal of Sociology* 46, no. 03 (December 2005): 387, <https://doi.org/10.1017/S0003975605000159>.

<sup>11</sup> Geoffrey Ingham, “Introduction,” in *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, ed. Geoffrey K. Ingham, Critical Studies in Economic Institutions 8 (Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005), xi.

<sup>12</sup> Ibid.

<sup>13</sup> As one economist complains, “The discussion of money is plagued with the question of what is money.” Malcolm Sawyer, “Money and the State,” in *Financial Crises and the Nature*

This trope should give pause to any purely economic analysis of the kind noted above, and the “muddle” that it marks goes some way towards explaining the persistence of debate over the question of Bitcoin and money. While the preceding quotations are far from an exhaustive survey of the literature on money, they do suggest that the underlying assumption of a purely economic approach to Bitcoin and money (i.e., that money is a clear, stable point of reference) is unwarranted.<sup>14</sup> To be sure, a lack of clarity and consensus about money does not rule out the possibility that, equipped with the proper conception of money, such an analysis could be fruitful, but this still begs the conceptual question—that is to say, the whole enterprise depends on having the “correct” concept of money. In any case, if money is something other than a stable reference point for economic analysis, then the relationship between Bitcoin, money, and discourse becomes significantly more complex, and it becomes much more difficult to equate the analysis of Bitcoin discourse with the analysis of style. If money is a “muddle,” then it seems that, in the midst of all the debate over whether Bitcoin is or is not a form of money, discourse is *doing something*, something more than glossing the surfaces of economic arguments—but what exactly?

Answering this question will set the stage for my analyses of Bitcoin discourse in the chapters to come. So with this end goal in mind, the remainder of this chapter engages the interdisciplinary literature of money as a social phenomenon to develop a theoretical

---

*of Capitalist Money: Mutual Developments from the Work of Geoffrey Ingham*, ed. Jocelyn Pixley and G. C. Harcourt (Basingstoke: Palgrave Macmillan, 2013), 162.

<sup>14</sup> Neither is this presumption warranted by the everyday experience of money, in which we treat discrete objects, practices, and institutions as bearing “family resemblances” to a polymorphous “money” concept. See H.M.J.J. Snelders et al., “The Polymorphous Concept of Money,” *Journal of Economic Psychology* 13, no. 1 (March 1992): 71–92, [https://doi.org/10.1016/0167-4870\(92\)90053-A](https://doi.org/10.1016/0167-4870(92)90053-A).

account of the relationship between money and discourse—that is, to clarify how exactly we should understand the discursive action at work in questions like “Is Bitcoin money?” and responses to them (e.g., digital metallism). As I explain below, this body of literature is somewhat unusual in that it emerges from and still contends with something of an historical accident in the development of the social sciences’ disciplinary divisions. Indeed, the story of this literature on money is in large part the story of the disciplinary clashes, truces, and rapprochements between economics and its disciplinary siblings (particularly sociology) over the last century—a story that, if told in detail, would take me far beyond the scope of the present study. Consequently, in this chapter I trace both the origins of the money “muddle” and subsequent scholarly attempts to overcome it, not to exhaustively account for all studies of money, but rather to highlight the manner in which evolving accounts of money also entailed changes in the role and relevance of *discourse* in the study of money. In turn, attending to the evolving role of discourse in studies of money allows me not only to situate the study of Bitcoin within a broader interdisciplinary literature, but also shows how this literature opens space specifically for the discursive analysis of digital currencies. Sketching this interdisciplinary history will not only clarify the stakes of analyzing Bitcoin discourse, but will also justify a communicative approach—more specifically, a *rhetorical* approach—to an apparently purely economic phenomenon.

To this end, I begin by reviewing the relationship between theories of money and the separation of economics and sociology into modern disciplines, and I show how this separation, and the resultant emergence of the theory of money as a “neutral veil,” led to the omission of discursive analysis from the study of money for much of the last century. Next, I examine economic sociology’s “rediscovery” of money at the turn of the 21<sup>st</sup> century.

I review two theoretical outgrowths of this rediscovery—namely, “constructionist” and “embeddedness” approaches to money—and consider the ways that these developments reintroduced, in a limited manner, the study of discourse to the study of money. From here, I turn to the “performative turn” in economic sociology, and show how this broader theoretical development heightened the significance of discourse to money scholarship, and made possible the integration of scholarship on money with rhetorical scholarship. Finally, in light of this review of the evolving relationship between money and discourse in the literature, I return to and reevaluate the opening question of this chapter: Is Bitcoin money?

*Weaving a “neutral veil”: Money and the Methodenstreiten*

According to scholar of money Geoffrey Ingham, the “puzzle” in the literature on money has its origins in the years before the divisions between economics, sociology, and related disciplines solidified.<sup>15</sup> In this period, many of the founding figures of modern social science turned their attention to money as a facet of social life—and crucially, at this point money was *not* the exclusive domain of economics. Money figures prominently in the work of both pre- and post-marginalist revolution economists, of course, but also in that of the founders of sociology—for example, in Marx's *Capital*,<sup>16</sup> in Simmel's *The Philosophy of*

---

<sup>15</sup> Ingham's reading of the history of money scholarship in the space between the disciplines of economics and sociology—a reading to which I am heavily indebted—is articulated in a number of articles and monographs. The most developed version of his argument can be found in Geoffrey Ingham, *The Nature of Money* (Malden, MA: Polity, 2004); for a more succinct account, see Geoffrey Ingham, “On the Underdevelopment of the ‘Sociology of Money,’” *Acta Sociologica* 41, no. 1 (1998): 3–18.

<sup>16</sup> Karl Marx, *Capital: A Critique of Political Economy*, trans. Ben Fowkes, vol. 1 (New York: Penguin, 1990).

*Money*,<sup>17</sup> and in Weber's *Economy and Society*.<sup>18</sup> There was no sense of money “belonging” to any particular branch of the academy, at least in part because the boundaries between disciplines were themselves so fluid.

From this early state of affairs there emerged two key developments that—according Ingham’s account of the money “puzzle”—profoundly shaped the study of money for the better part of a century. First, the fluid boundaries between disciplines began to grow firm and rigid. Through debate and institutionalization, the intellectual labor of the social sciences was divvied up, and formerly wide-ranging paths of research were tethered to specific disciplines. Of particular note for its influence on studies of money is the distinction that developed between economics and sociology, a distinction that was, according to economic sociologist Heiner Ganßmann, “so simple that it appears to be irresistible”: “Economics is to deal with man-matter-, sociology with man-man-relations.”<sup>19</sup> This clarification of the respective territories of economics and sociology—regardless of how much later scholars, such as Ganßmann, might contest such distinctions—established where the study of money belonged and who should study it; accordingly, sociology largely

---

<sup>17</sup> Georg Simmel, *The Philosophy of Money*, ed. David Frisby, trans. Tom Bottomore, David Frisby, and Kaethe Mengelberg, 3rd ed. (New York: Routledge, 2011).

<sup>18</sup> Max Weber, *Economy and Society: An Outline of Interpretive Sociology*, ed. Guenther Roth and Claus Wittich (Berkeley, CA: University of California Press, 1978).

<sup>19</sup> This distinction was proposed by turn of the century German sociologist and economist Leopold von Wiese; accordingly, Ganßmann terms the distinction—for its role in impeding money studies—“von Wiese’s curse.” Heiner Ganßmann, “Money—A Symbolically Generalized Medium of Communication?,” *Economy & Society* 17, no. 3 (1988): 286, <https://doi.org/10.1080/03085148800000013>.

ceded the “matter” of money to economics.<sup>20</sup> Indeed, this division of labor eventually became so self-evident to sociologists—notwithstanding the examples of Marx, Simmel, and Weber—that for a good portion of the 20th century money ceased to be recognized as a meaningfully *social* object of study at all. Even when sociology did try to address the place of money in social life, money was a means to some other analytical end rather than an object of study—as, for example, in Parsons’ account of money as a theoretical parallel to political power.<sup>21</sup> In and of itself, money was of little interest to sociology; as Randall Collins remarked in an often-quoted essay, sociologists ignored money “as if it were not sociological enough.”<sup>22</sup>

Crucially, the ceding of money by sociology to economics meant that any dominant theory of money in economics would be taken as *the* theory of money across the social

---

<sup>20</sup> Anthropology established a somewhat parallel distinction, albeit with the dividing line drawn between anthropology’s “primitive,” pre-industrial, non-Western money (notably subject to social constraints) and the contemporary money of economics. As Keith Hart writes, “Most anthropologists don’t like money and they don’t have much of it. It symbolises the world they have rejected for something more authentic elsewhere. It lines them up with the have-nots and against the erosion of cultural diversity by globalisation. Anthropologists have, as a result, not had much of theoretical interest to say about money. Rather, they have been limited to discussing whether primitive valuables are money or not.” Keith Hart, “Notes towards an Anthropology of Money,” *Kritikos* 2 (2005): n.p., <http://intertheory.org/hart.htm>; for an introduction to the anthropological debates over “primitive” money, see Jonathan Parry and Maurice Bloch, eds., *Money and the Morality of Exchange* (Cambridge, UK: Cambridge University Press, 1989); for an overview of the anthropology of money, see Maurer, “The Anthropology of Money”; and Keith Hart, “Money Is Always Personal and Impersonal,” *Anthropology Today* 23, no. 5 (October 2007): 12–16, <https://doi.org/10.1111/j.1467-8322.2007.00536.x>.

<sup>21</sup> Talcott Parsons, “On the Concept of Political Power,” in *Sociological Theory and Modern Society* (New York: The Free Press, 1967), 297–354; for an overview and critique, see Ganßmann, “Money.”

<sup>22</sup> Randall Collins, “*The Bankers*. By Martin Mayer,” *American Journal of Sociology* 85, no. 1 (July 1979): 190, <https://doi.org/10.1086/226983>.

sciences. And this brings us to the second key development in the study of money: the theory of money that dominated economics after the split from sociology. Again, processes of disciplinary formation are central to the story here, as the origins of both this theory and its dominance in economic thought lie not in studies of money per se, but rather in the turn of the century *Methodenstreiten* (methodological disputes) that helped to shape economics as a modern discipline.<sup>23</sup> Through a somewhat circuitous route, these early debates led to a set of metatheoretical commitments in economics, which in turn left the discipline particularly well disposed to theorize money in functionalist terms.

More specifically, this circuitous route begins with the late 19<sup>th</sup> century debates in economics (i.e., the *Methodenstreiten*) regarding “the relative merits of formal deductive logic and explanation by means of general laws (*Naturwissenschaften*) as opposed to a more interpretive and empirical procedure (*Kulturwissenschaften*)”—in short, the question of exactly how “hard” or “soft” economics should be as a social science.<sup>24</sup> As Ingham explains, the success of the positivistic, *Naturwissenschaften* view (and its attendant drive to abstraction) helped to commit economics to a particular metatheoretical conception of the economy as an object of study:

The former natural science model [i.e., *Naturwissenschaften*] increasingly dominated economic theory, which took on an even more marked positivist complexion with the development of ‘marginal utility’ theory, based on axioms of individual rational choice and the associated equilibrium model of the perfectly competitive market. The metatheory of the ‘economy’ underlying these abstractions involves the conceptualization of a system comprising exchange ratios between commodities expressed in money terms (object-object relations), established as the result of

---

<sup>23</sup> Ingham, “On the Underdevelopment of the ‘Sociology of Money.’”

<sup>24</sup> *Ibid.*, 4.

individual acts of utility calculation (individual agent-object relations). These relations—object-object and agent-object—comprise the ‘real’ economy.<sup>25</sup>

In turn, the adoption of the metatheory of the “real” economy—that is, an economy that is ultimately a kind of fundamental barter, a matter of ratios between objects and agents—produced a somewhat paradoxical result with respect to the study of money: “After the *Methodenstreit*,” Ingham recounts, “economic thought became dominated by the idea that money was epiphenomenal—that is to say, it was treated as a neutral ‘veil’ over the underlying ‘real’ natural economy.”<sup>26</sup> In other words, the development of this metatheory of the “real” economy led economics away from the study of money by suggesting that money obscured—*albeit in an analytically insignificant manner*—the “reality” of the economy. Indeed, the neutral veil and the real economy were two sides of the same coin: The veil of money was neutral precisely because it masked but did not meaningfully affect the real economy, and the real economy could be conceptually separated from such a veil precisely because the veil was neutral.

Consequently, instead of seeing money as an economic phenomenon to be studied closely, economists increasingly saw money as theoretically inconsequential, a thing to be explained *away* rather than explained. Schumpeter, for example, provides a summary of this view in his *History of Economic Analysis*:

Real Analysis [*sic*] proceeds from the principle that all the essential phenomena of economic life are capable of being described in terms of goods and services, of decisions about them, and of relations between them. Money enters the picture only in the modest role of a technical device that has been adopted in order to facilitate

---

<sup>25</sup> Ibid.

<sup>26</sup> Ibid.

transactions. This device can no doubt get out of order, and if it does it will indeed produce phenomena that are specifically attributable to its *modus operandi*. But so long as it functions normally, it does not affect the economic process, which behaves in the same way as it would in a barter economy: this is essentially what the concept of Neutral Money implies. Thus, money has been called a ‘garb’ or ‘veil’ of the things that really matter, both to households or firms in their everyday practice and to the analyst who observes them.<sup>27</sup>

Here money is explained away as a “technical device”—a convenience for exchange in everyday life, but not an analytically significant one; money is simply a glass through which economists must see, albeit not darkly. Yet for Schumpeter, this view of money as a veil has significant analytical implications. The theory of neutral money does not simply *allow* economic analysis to ignore “normal” money—a normative distinction to which we will return in a moment—but in fact *forecloses* investigation of money in a “properly” functioning money economy:

Not only *can* [money] be discarded whenever we are analyzing the fundamental features of the economic process but it *must* be discarded just as a veil must be drawn aside if we are to see the face behind it. Accordingly, money prices must give way to the exchange ratios between the commodities that are the really important thing ‘behind’ money prices; income formation must be looked upon as an exchange of, say, labor and physical means of subsistence; saving and investment must be interpreted to mean saving of some real factors of production and their conversion into real capital goods, such as buildings, machines, raw materials; and, though ‘in the form of money,’ it is these physical capital goods that are ‘really’ lent when an industrial borrower arranges for a loan.<sup>28</sup>

So what are the implications of this “real” economy metatheory and the neutral veil theory for the study of money? The first consequence of these intellectual developments verges on comedy, or at least historical irony: The discipline claiming money did not see fit to spend

---

<sup>27</sup> Schumpeter, *History of Economic Analysis*, 264.

<sup>28</sup> *Ibid.*, 264–65.

much time studying money per se.<sup>29</sup> Even though the turn of the century disputes left money squarely in the domain of economics, and even though sociology's own approach to money largely respected this division of intellectual labor, the metatheoretical commitment to the notion of the "real" economy, in which properly functioning money was analytically irrelevant, meant that economists generally did not study *money itself*, and instead approached money obliquely (e.g., through the study of monetary policy).<sup>30</sup> Indeed, exceptions to this trend—for example, Keynes's *Treatise*—are notable precisely as exceptions.<sup>31</sup>

The second consequence of this metatheory/theory pair is economic thought's conceptual emphasis of money's abstracted *functions*. Here we can see the significance of

---

<sup>29</sup> As Ganßmann points out, "The conviction that money is a mere means to facilitate transactions that can just as well take place in the absence of money implies that the use of money can only seriously modify the allocation of resources if something goes wrong. In other words, most economists think about money in an asymmetric way: If all goes well, money is not important." Heiner Ganßmann, *Doing Money: Elementary Monetary Theory from a Sociological Standpoint* (New York: Routledge, 2012), 14.

<sup>30</sup> It is worth noting that while the *critique* of this oversight emerges most forcefully from outside the discipline (i.e., from sociology), it is leveled against economics by economists, too. Economist John Smithin, for example, writes that "orthodox economic theory [...] has had a persistent tendency to deny the importance of money and monetary factors in determining economic outcomes, despite the apparent evidence of our senses. [...] The essence of the economic thought of the classical economists [...] was their indignation at what they perceived to be the errors of their mercantilist predecessors, including the idea 'that wealth consists in ... gold and silver,' or in other words, the money of the day. And this attitude has persisted to the present day. [...] [E]very economist is familiar with the catchphrases and slogans which express this point of view, such as 'money is neutral' or 'money is a veil'. Underlying this perspective is the view that economics deals fundamentally with the so-called 'real' exchange of goods and services, as opposed to the accumulation of financial resources." John N. Smithin, "What Is Money? Introduction," in *What Is Money?*, ed. John N. Smithin, Routledge International Studies in Money and Banking 6 (London ; New York: Routledge, 2000), 1.

<sup>31</sup> John Maynard Keynes, *A Treatise on Money* (New York: AMS Press, 1976).

Schumpeter's distinction between "normally functioning" and malfunctioning money: If money is epiphenomenal, if it is a mere "technical device," then what makes something money is the extent to which it fulfills the *technical functions* of money without disturbing the underlying "real" economy—that is, without straying from the epiphenomenal.<sup>32</sup> And since, in this view, money is a matter of functions, economics was able to rely on—and *still* relies on, as is evidenced by contemporary economics textbooks<sup>33</sup>—a 19th century conceptualization of money in terms of three functions:

1. Money is a *medium of exchange*. Instead of trading commodity for commodity, money functions as a commodity substitute in market exchange, and in doing so, solves the "double coincidence of wants" problem.<sup>34</sup>
2. Money is a *unit of account*. Instead of denominating exchange rates of a given commodity for every other possible commodity (e.g., *A* bushels of wheat for *B* chickens, but *C* bushels of wheat for *D* cords of wood), money allows for the use of a single denomination for all commodity exchanges.

---

<sup>32</sup> Notably, this view of money is as much at home in Marxian scholarship as it is in classical and neoclassical economics: "Both Smithian and Marxian classical political economy work with a functionalist conception of money, which ultimately derives from the commodity theory of money. Money, including capitalist forms of credit-money, is seen as a simple unmediated response to the needs of an expanding economy whose dynamic lies elsewhere in 'real' material or social factors: technology; the division of labour; or the means and social relations of production etc." Geoffrey Ingham, "Capitalism, Money and Banking: A Critique of Recent Historical Sociology," *The British Journal of Sociology* 50, no. 1 (March 1999): 78, <https://doi.org/10.1111/j.1468-4446.1999.00076.x>.

<sup>33</sup> For example, see the discussion of money in N. Gregory Mankiw, *Principles of Economics*, 4th ed. (Mason, OH: Thomson South-Western, 2007), 642–43.

<sup>34</sup> William Stanley Jevons, *Money and the Mechanism of Exchange* (New York: D. Appleton & Co., 1875), 3–5.

3. Money is a *store of value*. The rates of exchange for money are stable enough over time to facilitate exchange.<sup>35</sup>

The point here, of course, is not the specific virtues or failings of these particular money functions; as conceptual tools, they have been well tested and shown to be analytically useful for certain investigations. Rather, the point is the *kinds of inquiry* such a functionalist definition of money facilitates. By adopting a perspective in which “money is as money does,”<sup>36</sup> economics promoted some lines of inquiry and discouraged others: If one begins with a definition of money in terms of *functions*, then it is quite natural to investigate an apparent money phenomenon through a process of comparison—that is, the method previously noted to be well-represented within Bitcoin scholarship.<sup>37</sup> By contrast, many money-related social phenomena (spending habits, earmarking, taboos, etc.) are very difficult to meaningfully connect to a functionalist definition of money. After all, if some social or communicative practice has a significant impact on the functioning of a monetary form, then the money in question is decidedly *not* a neutral veil, *cannot* be analytically separated into *only* money’s three functions, and therefore, is not *really* money.

---

<sup>35</sup> Early formulations of this functionalist definition included a fourth “function,” namely that money is a *settlement of debts*; see Jevons, *Money and the Mechanism of Exchange*. While all four features are still occasionally referenced today, contemporary scholarship generally views the settlement of debts as subsidiary to the medium of exchange function, and consequently collapses this fourth function into the first.

<sup>36</sup> Ingham, “On the Underdevelopment of the ‘Sociology of Money,’” 3.

<sup>37</sup> A classic example of this kind of analysis is the functional analysis of the use of cigarettes and other rations as money in World War II prisoner of war camps. See R.A. Radford, “The Economic Organization of a P.O.W. Camp,” in *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, ed. Geoffrey K. Ingham, Critical Studies in Economic Institutions 8 (Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005), 20–32.

With these three pieces established—the split of economics and sociology, the dominance of the neutral veil theory, and the functionalist definition of money—we can see the roots of the “puzzle” of the literature on money. The development of economics and sociology into modern academic disciplines left the study of money as a social phenomenon curiously “underdeveloped” as an area of research: The neutral veil theory and attendant functionalist definitions of money discouraged investigation in economics, and economics’ claim of intellectual ownership discouraged research in sociology. Since money belonged to the domain of economics, across the social sciences money was understood as a matter of its functions.<sup>38</sup> And given this functionalist conceptualization, the social and discursive aspects of money were either irrelevant or a matter of self-contradiction; the moment that discourse about money actually mattered, the object of study in question was no longer money. Accordingly, the functionalist view of money left—and to the extent that this view persists in money scholarship, still leaves—little room for discursive analysis in the study of money.

---

<sup>38</sup> It is worth noting that the integration of the functionalist view of money into other disciplines was facilitated by the extent to which scholarship predating the development of sharp disciplinary divisions itself relied on functionalist definitions. In his study of Simmel and money, for example, Gianfranco Poggi clearly identifies this functionalist element in the *Philosophy of Money*: “While [...] Simmel does not formally define money, the closest he comes to a purely conceptual presentation of it is a passage which considers it as a link, an element intervening in interindividual exchanges. Given a situation involving two parties A and B, if A wants an object *b* which B has, but cannot induce him to hand over *b* because B does not want that *a* which A can supply, it is useful for some *X* to exist into which A can convert *a* at any time and which B can be assumed to want, because he can exchange it in turn. [...] Whatever functions as *X* in this example constitutes money; and the point of money's existence is ultimately to convey, by being expended and received, the individuals' valuations of objects intrinsically apt to satisfy their desires, while money itself cannot do this directly, for money possesses no value of its own.” Gianfranco Poggi, *Money and the Modern Mind: Georg Simmel's Philosophy of Money* (Berkeley, CA: University of California Press, 1993), 135–36.

*The “rediscovery” of money*

There are, however, important exceptions to the story of underdevelopment told above—exceptions that drove the reinvigoration of money scholarship near the turn of the 21<sup>st</sup> century as economic sociologists “rediscovered” money as an object of study. These exceptions generally fall into one of two categories: Scholars who focused on the social *construction* of money, and scholars whose attention rested on the social *embeddedness* of money. In their own ways, both threads of scholarship served to complicate the economic orthodoxy of neutral money, and both opened new, albeit limited, possibilities for integrating the study of discourse into the study of money.

The first of these exceptions has its roots in Keynesian monetary theory and related schools of economic thought situated beyond the neoclassical mainstream, including chartalism and monetary circuit theory. While detailed discussions of each of these goes beyond the scope of the present chapter, it is sufficient to note that while such avenues of scholarship do not contest the *functions* captured by the traditional, threefold definition of money—chartalists do not, for example, dispute that money is a medium of exchange—it is the *origins* of these functions that loom large in these monetary theories. Methodologically individualist economic models have attempted to show, admittedly with some difficulty, that the use of money could—and presumably did, though the empirical confirmation of this purely logical investigation is left aside—arise out of barter between rational individuals. (This problem of accounting for the emergence of money within a general

equilibrium model is known as “Hahn’s problem,” after economist Frank Hahn.)<sup>39</sup> By contrast, heterodox scholars have viewed money as *beginning* with social relations (e.g., between creditors and debtors) rather than with the exchange of commodities between individuals, though there exists disagreement between the various schools about which entities (e.g., the state, private banks) occupy the respective roles in money’s social foundation. These disputes over money’s origins have significant policy implications, of course, since they have bearing on the appropriate manipulation of the money supply—and consequently, this is a facet of monetary study for which the economic scholarship is quite robust.<sup>40</sup>

For the present chapter’s purposes, however, it is sociology’s adoption of this concern with money’s origins that is noteworthy, and the work of Geoffrey Ingham, on which I have already drawn to sketch the history above, is the preeminent example of this line of research. Across multiple monographs, edited collections, and numerous essays, Ingham has focused on the sociological implications of the debates over money’s origins, and sides decisively against the neoclassical attempt to reduce the emergence of money to

---

<sup>39</sup> See Frank H. Hahn, “The Foundations of Monetary Theory,” in *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, ed. Geoffrey K. Ingham, Critical Studies in Economic Institutions 8 (Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005), 52–74.

<sup>40</sup> It should be noted that the word *appropriate* is key here, as this normative distinction is what allows these policy disputes to remain fully in line with the metatheory of the real economy (e.g., through a monetary policy aimed at guaranteeing the “normal” neutrality of money). This is not to say that a monetary policy cannot affect economic phenomenon; the point of something like quantitative easing is to do precisely that. Rather, this merely highlights the extent to which the appropriate “reality” of the economy is itself a contested matter.

individual, rational actors.<sup>41</sup> For instance, in a response to economist Frank Hahn's analysis of the emergence of money, in which Hahn concludes that it is "advantageous for any given agent to mediate his transactions by money provided that all other agents do likewise,"<sup>42</sup>

Ingham insists that such an individualist orientation fundamentally misses the point:

[I]t is not so much a question of whether it is advantageous to use money if others do, but rather that agents cannot use money unless others do likewise. To state the obvious: the advantage of money presupposes a monetary system. We have here [i.e., Hahn's analysis] a typical example of the way in which the rational choice explanations of neoclassical economics soon become locked into slightly absurd circularities. Money is an advantage to the individual only if others use it; but, according to the theory, they can only rationally use it if it can be shown to be an individual advantage.<sup>43</sup>

For Ingham, the way out of these "absurd circularities" is to accept that money is deeply social from the start—that is, to accept that "money [is] not only produced socially, but actually constituted by a social relation of credit-debt denominated in an abstract money of account."<sup>44</sup> More specifically, for Ingham the constitution of money begins when "issuers promise to accept in payment of any debt owed to them, denominated in their declared money of account, the form of money that they have emitted and described by the same

---

<sup>41</sup> Geoffrey Ingham, "Money Is a Social Relation," *Review of Social Economy* 54, no. 4 (December 1996): 507–29, <https://doi.org/10.1080/00346769600000031>; Ingham, "On the Underdevelopment of the 'Sociology of Money'"; Ingham, "Capitalism, Money and Banking"; Ingham, *The Nature of Money*; Geoffrey Ingham, "The Emergence of Capitalist Credit Money," in *Credit and State Theory of Money*, ed. L. Randall Wray (Cheltenham, UK: Edward Elgar, 2004), 173–222; Ingham, "Introduction"; and Geoffrey Ingham, "Further Reflections on the Ontology of Money: Responses to Lapavistas and Dodd," *Economy and Society* 35, no. 2 (May 2006): 259–78, <https://doi.org/10.1080/03085140600635730>.

<sup>42</sup> Hahn, "The Foundations of Monetary Theory," 57.

<sup>43</sup> Ingham, "Money Is a Social Relation," 514–15.

<sup>44</sup> Ingham, "Further Reflections on the Ontology of Money," 261.

money of account”—a process which implies that “money (as opposed to mere tradable commodities) cannot be created without the creation of debt.”<sup>45</sup> For the purposes of the present chapter, the equation of money with credit/debt is significant here not so much for its policy implications, but rather for the way it makes the origins of money a thoroughly sociological matter. If money is ultimately a matter of credit and debt, then all of the social dimensions relevant to credit-debtor relations (e.g., power, authority, legitimacy) are relevant to money, too. And in turn, this introduction of the social into money’s origins has implications for the role of discourse in the study of money: By emphasizing that money, as a relation of credit and debt, *needs to be established* by someone or something—and by extension, money needs to be *legitimated*—Ingham highlights the ways that the production of money, far from being a natural outgrowth of “real” economic action (i.e., barter), actually involves social action—and by extension, *symbolic* action. Indeed, the point that Ingham’s account of money emphasizes again and again—that the original and most fundamental function of money is the quantification of credit/debt in a unit of account—is entirely symbolic in nature; for Ingham, the emergence of money is the emergence of a *symbol* for credit and debt.

The second of the exceptions to the broader trend of “underdevelopment” in the study of money is scholarship that focuses explicitly on the social embeddedness of money and monetary practices. A significant though far from solitary influence on this line of research is the work of Karl Polanyi, insofar as his study of the boundary between the economic and the social opened the door to considering the ways in which money itself might be subject to the contest between market and society: If money was in fact subject to

---

<sup>45</sup> Ibid.

social constraints during historical periods assumed to have “normally functioning” money, then the functionalist account of money—and its presupposition that proper money is neutral money—would necessarily be inadequate.<sup>46</sup> The possibilities for research along these lines were amplified by the Granovetterian reinvention of economic sociology,<sup>47</sup> and by the late 1980s and early 1990s, against the backdrop of economic sociology’s turn to studying the embeddedness of economic phenomena, scholars began to articulate the need for a research program centered on the social embeddedness of money.<sup>48</sup> Sociologists joined with anthropologists to challenge longstanding assumptions about the social life of money by demonstrating that money, too, was embedded in social contexts: Studies of earmarking, for example, showed that despite money’s supposed quantification and alienation of social relations—side effects of money’s abstracted functions—in practice the use of money was socially constrained (e.g., “gift” money might be allocated only to “fun” purchases, as opposed to “needs”).<sup>49</sup> In contrast to the simplistic story told by the “neutral

---

<sup>46</sup> Karl Polanyi, *The Great Transformation: The Political and Economic Origins of Our Time*, 2nd ed. (Boston, MA: Beacon Press, 2001).

<sup>47</sup> Granovetter’s link to Polanyi was explicit from the start: “The embeddedness position is associated with the ‘substantivist’ school in anthropology, identified especially with Karl Polanyi...” Mark Granovetter, “Economic Action and Social Structure: The Problem of Embeddedness,” *American Journal of Sociology* 91, no. 3 (November 1985): 482, <https://doi.org/10.1086/228311>; for a distilled account of the shift, see Mark Granovetter, “The Old and New Economic Sociology: A History and an Agenda,” in *Beyond the Marketplace: Rethinking Economy and Society*, ed. Roger Friedland and A. F. Robertson (Berlin: Aldine de Gruyter, 1990), 53–88; for an a broader overview, see Richard Swedberg, *Principles of Economic Sociology* (Princeton, NJ: Princeton University Press, 2003).

<sup>48</sup> For example, Ganßmann, “Money”; Nigel Dodd, *The Sociology of Money: Economics, Reason & Contemporary Society* (New York: Continuum, 1994); and Viviana Zelizer, *The Social Meaning of Money: Pin Money, Paychecks, Poor Relief and Other Currencies* (New York: Basic Books, 1994).

<sup>49</sup> Zelizer, *The Social Meaning of Money*, 1994.

veil” theory, money was increasingly recognized as a complex and multifaceted object of study—and as an object not belonging exclusively to economists.

Examining the social embeddedness of money also led to a significant and decidedly non-functionalist reconceptualization of money. Viviana Zelizer, for instance, whose work is perhaps the foremost representative of the embeddedness approach to money studies, conceptualizes money not as a thing or as a set of functions, but rather as continuum of social abstraction:

Money is an abstraction that observers make from social interactions. *It is a matter of degree*; to the extent that interactions transfer rights to goods and services by means of tokens that could also serve transfers of other such rights, we can call those tokens money. The more generalizable across social locations, varieties of goods and services, interaction partners, types of rights, and physical forms of the token itself is that capacity to facilitate transfer of rights, the more readily people recognize the token involved as monetary. International currencies, nationally issued legal tenders, electronic monies, bank accounts, and other highly liquid tokens of transferable rights represent one extreme of a continuum running from such generalized forms to the narrowly limited circuits of such other monies as credits in baby-sitting pools, casino chips, or investment diamonds.<sup>50</sup>

And crucially, this redefinition of money, by undermining both the assumption of money’s singularity and the assumption of money’s separation from social context, draws attention to the significance not only of what money *does* (i.e., the focus of the functionalist account, in which money is as money does) but also of what money *means*. As Zelizer explains:

Impressed by the fungible, impersonal characteristics of money, traditional social thinkers emphasized its instrumental rationality and apparently unlimited capacity to transform products, relationships, and sometimes even emotions into an abstract and objective numerical equivalent. But money is neither culturally neutral nor morally invulnerable. It may well “corrupt” values into numbers, but values and

---

<sup>50</sup> Viviana Zelizer, “Fine Tuning the Zelizer View,” *Economy and Society* 29, no. 3 (January 2000): 384–85, <https://doi.org/10.1080/03085140050084570>. Italics added.

sentiment reciprocally corrupt money by investing it with moral, social, and religious meaning. *We need to examine more carefully how cultural and social structural factors influences the uses, meaning, and even quantity of money.* What is the relationship of money as a medium of exchange and measure of utility to money as a symbol of social value?<sup>51</sup>

It is worth pausing here to note the contrast between both Ingham's and Zelizer's respective visions of the study of money and the vision implied by a purely functionalist definition of money.<sup>52</sup> In the functionalist view, discourse is by definition irrelevant; the moment discourse starts to matter to the study of money, the object of study morphs to become some strange aberration, a kind of pseudo-money. By contrast, in both the constructionist and embeddedness perspectives, money is imbued with social meaning—in the former, at the point of monetary construction, and in the latter, in the everyday assessment of object's "moneyness"—and therefore the study of money in fact necessitates the *interpretation* of at least some aspects of money (e.g., construction, earmarking). These approaches to the study of money, far from foreclosing the role of discourse, actually make discourse integral to money as a concept; money *means* something, this meaning is

---

<sup>51</sup> Viviana Zelizer, "The Social Meaning of Money: 'Special Monies,'" in *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, ed. Geoffrey K. Ingham, Critical Studies in Economic Institutions 8 (Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005), 580–81. Italics added.

<sup>52</sup> This is not to say that Ingham and Zelizer are in complete agreement on all points in the study of money; to the contrary, both have been involved in significant disputes within the subfield. See, for example, the extended debate between Ben Fine and Costas Lapavitsas, "Markets and Money in Social Theory: What Role for Economics?," *Economy and Society* 29, no. 3 (January 2000): 357–82, <https://doi.org/10.1080/03085140050084561>; Zelizer, "Fine Tuning the Zelizer View"; Geoffrey Ingham, "Fundamentals of a Theory of Money: Untangling Fine, Lapavitsas and Zelizer," *Economy and Society* 30, no. 3 (January 2001): 304–23, <https://doi.org/10.1080/03085140120071215>; Costas Lapavitsas, "The Social Relations of Money as Universal Equivalent: A Response to Ingham," *Economy and Society* 34, no. 3 (August 2005): 389–403, <https://doi.org/10.1080/03085140500112137>; Dodd, "Laundering 'Money'"; and Ingham, "Further Reflections on the Ontology of Money."

constructed and contested, and far from being epiphenomenal, this meaning has some bearing on the apparently “separate” sphere of money as an economic phenomenon.

Yet these theoretical developments in the study of money require their caveats. While both the constructionist and embeddedness approaches highlighted the importance of discourse to some aspects of money as a social phenomenon, and while the emergence of these lines of research helped to broaden the study of money beyond the limits of the neutral veil theory, these new approaches to money came with their own conceptual constraints. The crux of these constraints is that, for both the constructionist and embeddedness approaches, discourse reenters the study of money through the collapse of the division between the social and the economic. Indeed, both approaches are premised on this collapse: Though Ingham and Zelizer focus on different aspects of money’s social existence (i.e., credit/debt, earmarking), both try to demonstrate that the orthodox, functionalist account of money is a misleading abstraction, a representation that sidesteps the messy complexities of the social—and in doing so, presents a fatally inadequate view of human behavior and experience.<sup>53</sup> For both Ingham and Zelizer, the study of money needs the study of discourse precisely to counteract this deceptive abstraction. But crucially, this intellectual goal implies a role for discourse that, while certainly more significant than the space allotted by the neutral veil theory, is nevertheless limited in scope: As a means to demonstrate the inadequacy of a purely “economic” account of money, discourse is either a predicate or a supplement to other, relatively independent sociological processes. In Ingham’s account of the production of money, for example, discourse enters the scene in

---

<sup>53</sup> This is perhaps easier to see in the embeddedness research, but Ingham’s insistence on the circularity of rational-individualist responses to Hahn’s problem is a variant of the same point. See Ingham, “Money Is a Social Relation.”

the founding of the creditor/debtor relationship, but has little bearing *after* credit/debt is established. In Zelizer's account of earmarking practices, the reverse is the case; discourse about money is one of the many means by which the dull abstraction of money is burnished with nuance. To draw an example from Zelizer's study of domestic earmarking: A household's discussion about the proper and improper division of money between husband, wife, and children is evidence of underlying sociological complexity, a complexity that exists, in some form, regardless of whether it is actually *discussed* at the dinner table (or in magazines, etc.).<sup>54</sup> In short, in both constructionist and embeddedness approaches to money, discourse remains a bit of an afterthought—something that adds color to other, more fundamental processes, but does not play a critical role throughout the entirety of the money phenomenon. Again, this is still a far cry from the strictures of the neutral veil theory, but it shows the extent to which economic sociology's rediscovery of money came with its own constraints.

#### *The influence of the performative turn*

It was broader developments in the economic sociology of markets, rather than any innovation internal to the scholarship on money, that challenged this still-constrained role of discourse and further expanded the possibilities for the discursive study of money. More specifically, the work of Michel Callon and his colleagues—a research agenda that eventually clustered under the heading of the “performativity of economics”—opened the way for discourse to be understood as more than a simple predicate or supplement to

---

<sup>54</sup> See the second chapter of Zelizer, *The Social Meaning of Money*, 1994.

sociological processes.<sup>55</sup> But to fully appreciate the significance of this research agenda, it is worth taking a moment to review the intellectual currents against which the performative turn was a reaction.

The text that served as the performative turn's point of departure, a collection of essays edited by Callon,<sup>56</sup> was published at a moment when much of economic sociology positioned itself in opposition to the core tenets of classical and neoclassical economics.<sup>57</sup> These tenets led economists to conceptualize economic phenomena in a methodologically individualist manner, placing the rational, self-interested, preference-having and

---

<sup>55</sup> The inaugural text is Michel Callon, ed., *The Laws of the Markets* (Malden, MA: Blackwell, 1998); also see Andrew Barry and Don Slater, eds., *The Technological Economy* (London ; New York: Routledge, 2005); Donald A. MacKenzie, *An Engine, Not a Camera: How Financial Models Shape Markets*, Inside Technology (Cambridge, Mass: MIT Press, 2006); Michel Callon, Yuval Millo, and Fabian Muniesa, eds., *Market Devices* (Malden, MA: Blackwell, 2007); Donald A. MacKenzie, Fabian Muniesa, and Lucia Siu, eds., *Do Economists Make Markets? On the Performativity of Economics* (Princeton: Princeton University Press, 2007); Donald A. MacKenzie, *Material Markets: How Economic Agents Are Constructed*, Clarendon Lectures in Management Studies (Oxford ; New York: Oxford University Press, 2009); Fabian Muniesa, *The Provoked Economy: Economic Reality and the Performative Turn*, Culture, Economy and the Social (London: Routledge, 2014); and Ivan Boldyrev and Ekaterina Svetlova, eds., *Enacting Dismal Science: New Perspectives on the Performativity of Economics*, Perspectives from Social Economics (New York: Palgrave Macmillan, 2016).

<sup>56</sup> Callon, *The Laws of the Markets*.

<sup>57</sup> Admittedly, there is a certain arbitrariness in identifying this text with an intellectual "break." As one of Callon's collaborators writes, "The expression 'performative turn in the social sciences' is perhaps a bit misleading. First, the notion of performativity (or the idea of the performative) has been used in a variety of ways which are often unrelated and perhaps even contradictory, in reference to speech, theatre, efficacy, and so forth. [...] Second, identifying an intellectual turn requires situating a relevant shift in a particular time and place, which is unlikely in cases such as the one to be examined here. It is a well-known fact that novelty in the social sciences is almost systematically accompanied by the rediscovery of old precursors. So the performative turn [...] is not a clear-cut epochal shift, nor a complete intellectual revolution, nor a coherent, self-conscious endorsement of a unique doctrine." Muniesa, *The Provoked Economy*, 7. That said, given that *The Laws of Markets* is identified *within* the literature as a key moment of transition, I have framed my own account accordingly.

preference-knowing *homo economicus* at the center of economic theory; social factors (e.g., networks of relationships) could be ignored to the extent that they exceeded the categories of economic analysis (e.g., individual preferences). By contrast, economic sociology, in a move that still echoed the split of sociology and economics, rejected this as overly reductionist; sociology took economic phenomena to be much more complex objects of study, hardly reducible to individuals, and certainly not expressive of any consistent rationality. The task for sociology, then, was to account for the nuance passed over by economics. In cases of apparently cold-blooded, profit-maximizing rationality, the sociologist would endeavor to uncover irrational attachments, moral impediments, institutional pressures, and the like. The sociologist would aim at showing how economic phenomena, rather than being separate from the social, are actually embedded in it.

But scholars contributing to the performative turn took this mode of analysis and turned it on its head. Instead of inquiring about how economic phenomena (e.g., markets) are embedded in the social, Callon and his colleagues asked: How is it that we get to the abstraction, the quantification, the “calculative-ness” of *disembedded* economic phenomena in the first place?<sup>58</sup> In other words, what are the conditions that make something like *homo economicus*—the individual cut free from social bonds, relentlessly pursuing rational calculation—possible?

It is important to note that this line of questioning, at least in its initial articulation, was a departure from contemporary work in economic sociology, and Callon and his colleagues drew criticism for their apparent reification of economic theory; after all,

---

<sup>58</sup> Michel Callon and Fabian Muniesa, “Peripheral Vision: Economic Markets as Calculative Collective Devices,” *Organization Studies* 26, no. 8 (August 2005): 1229–50, <https://doi.org/10.1177/0170840605056393>.

Callon's questions seemed to affirm that *homo economicus* really *did* exist and was not, as it was viewed from other corners of the social sciences, simply a fiction of economists overly preoccupied with elegant equations. But it is equally important to note that these critiques generally failed to account for the theoretical commitments that informed the initial development of this line of research—more specifically, Callon's collaboration with Bruno Latour in the development of actor-network theory (ANT).<sup>59</sup> Given ANT's emphasis on analyses and explanations that avoid reducing the social to individual actors but instead seeks to describe social phenomena in terms of assemblages or arrangements of entities (in Callon's terms, *agencements*)<sup>60</sup> that execute agency, Callon's affirmation of *homo economicus* should not be understood as a claim that rational, preference-following, profit-maximizing *individuals* exist on their own; instead, it should be understood as an acknowledgement that particular *assemblages* in particular empirical settings can make *homo economicus* possible.

So how does this lead back to the performativity of economics? The key here is the way an assemblage perspective reformulates economic phenomena as objects of study. If the task of sociological inquiry shifts away from uncovering the latent social in the apparently separate sphere of the economic, and towards the description and analysis of the assemblages that make that separation possible, then it is necessary to consider the

---

<sup>59</sup> Michel Callon and Bruno Latour, "Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So," in *Advances in Social Theory and Methodology: Toward an Integration of Micro-and Macro-Sociologies*, ed. Katherine Knorr-Cetina and Aaron Victor Cicourel (Routledge, 1981), 277–303.

<sup>60</sup> Michel Callon, "Economic Markets and the Rise of Interactive *Agencements*: From Prosthetic Agencies to Habilitated Agencies," in *Living in a Material World: Economic Sociology Meets Science and Technology Studies*, ed. Trevor Pinch and Richard Swedberg, Inside Technology (Cambridge, Mass: MIT Press, 2008), 29–56.

role played in those assemblages by *economics* itself—that is, economics in the broadest sense, inclusive of the academic discipline, but also of the lay theories, practices, etc. of bankers, analysts, government officials, accountants, and anyone else who might have some role in conceptualizing or acting in a given assemblage. In a sense, this is a pragmatist refiguring of the relationship between economics and its object: While both orthodox economic thought and sociology's traditional critique of it understand "economics" in *representational* terms—the dispute between the two primarily concerns the representation's accuracy—an assemblage perspective rejects the privileging of represented over representation. Since the point is not to explain the economic in terms of the social (or vice versa), but rather to account for the *conditions of possibility* underlying assemblages "made economic," representations of economic phenomena should be understood as potentially just as important to a given assemblage as other elements (e.g., institutions, infrastructures).

With this possibility made conceptually accessible by an assemblage perspective, Callon and his colleagues turned to cases in which economics (in the broad sense, inclusive of the academic discipline) played a crucial role in the *construction* of economic phenomena (e.g., markets), not simply in their description. For example, the construction of strawberry markets in France and derivatives markets in America are favorite cases for their pointed attempts to implement, socially and materially, neoclassical economic theory.<sup>61</sup> In these

---

<sup>61</sup> See, respectively, Marie-France Garcia, "La Construction Sociale d'un Marché Parfait: Le Marché Au Cadran de Fontaines-En-Sologne," *Actes de La Recherche En Sciences Sociales* 65 (1986): 2–13; Donald MacKenzie and Yuval Millo, "Constructing a Market, Performing Theory: The Historical Sociology of a Financial Derivatives Exchange," *American Journal of Sociology* 109, no. 1 (July 2003): 107–45, <https://doi.org/10.1086/374404>; and MacKenzie, *An Engine, Not a Camera*.

cases, economics in some sense *performs* (or, to use Fabian Muniesa's more evocative term, *provokes*)<sup>62</sup> its object of study—though precisely in what sense this occurs is a contested matter within the performativity literature—and in so doing, plays a key part in bringing the abstraction of *homo economicus* into real, material and social existence. In short, the performative turn repeats a move already familiar to the STS literature, and it turns an analytical lens, previously applied to the natural sciences, on the social sciences as well. In this view, the work of economics in economic assemblages is analogous to the work of the physics or biology in the assemblages of scientific experiment: Both contribute to the production of their objects of study.<sup>63</sup>

This core thesis of the performative turn was extended and developed by subsequent scholarship—perhaps most notably by Donald MacKenzie, who added clarity and nuance to the performativity debates by introducing a typology of *degrees* of performativity<sup>64</sup>—but for the purposes of the present chapter, this basic sketch of the turn is sufficient to introduce four key implications for the study of money and for the relationship between money and discourse. First, the connection to STS and ANT created an explicit link between the study of technology and the study of economic sociology. For Callon, “It is impossible to think of markets and their dynamics without taking into account the materiality of markets and the role of technological devices,” and thus “[t]he

---

<sup>62</sup> Muniesa, *The Provoked Economy*.

<sup>63</sup> As Callon succinctly writes, “My thesis is that both the natural and life sciences, along with the social sciences, contribute toward enacting the realities that they describe.” Michel Callon, “What Does It Mean to Say That Economics Is Performative?,” in *Do Economists Make Markets? On the Performativity of Economics*, ed. Donald A. MacKenzie, Fabian Muniesa, and Lucia Siu (Princeton: Princeton University Press, 2007), 315.

<sup>64</sup> See MacKenzie, *An Engine, Not a Camera*.

anthropology of technology might be very helpful if we want to understand better how markets are stabilised and organised.”<sup>65</sup> For scholarship on money, this connection came a crucial historical moment: The performative turn directed attention towards the role of assemblages of material, technological artifacts in producing and maintaining economic phenomena even as the advent of the Internet and related communications technologies began both to substantially alter the everyday experience of money—to a degree not experienced since the widespread adoption of paper notes—and to erase the intuitive, if misguided, distinction between monetary technologies and communication technologies.<sup>66</sup> By making the study of technological assemblages integral to the study of economic assemblages—and more generally, by adopting the language and theoretical concerns of STS to economic sociology—the performative turn made new cross-disciplinary engagement possible, and opened avenues for the integration of hitherto parallel scholarship on communication technologies into the study of money.<sup>67</sup> Even though the

---

<sup>65</sup> Michel Callon, Andrew Barry, and Don Slater, “Technology, Politics, and the Market: An Interview with Michel Callon,” in *The Technological Economy*, ed. Andrew Barry and Don Slater (London ; New York: Routledge, 2005), 101–21; also see Trevor Pinch and Richard Swedberg, eds., *Living in a Material World: Economic Sociology Meets Science and Technology Studies*, Inside Technology (Cambridge, Mass: MIT Press, 2008).

<sup>66</sup> For early discussions of this point, see Supriya Singh, “Electronic Commerce and the Sociology of Money,” *Sociological Research Online* 4, no. 4 (2000), <http://www.socresonline.org.uk/4/4/singh.html>; and Keith Hart, “Money in an Unequal World,” *Anthropological Theory* 1, no. 3 (September 2001): 307–30, <https://doi.org/10.1177/14634990122228755>.

<sup>67</sup> For example, the chapter on money in Marshall McLuhan, *Understanding Media: The Extensions of Man* (New York: Signet, 1966); for an example of later scholarship inspired by this connection, see Josh Lauer, “Money as Mass Communication: U.S. Paper Currency and the Iconography of Nationalism,” *The Communication Review* 11, no. 2 (2008): 109–32, <https://doi.org/10.1080/10714420802068359>; Bill Maurer, “Mobile Money: Communication, Consumption and Change in the Payments Space,” *Journal of Development Studies* 48, no. 5 (2012): 589–604, <https://doi.org/10.1080/00220388.2011.621944>; Bill

primary concern of early work in the performative turn was markets in general, rather than money specifically, the turn's reliance on STS and ANT became something of an intellectual bridge between disciplines studying economic phenomena and those studying technological phenomena, and thus provided a context in which parallel lines of scholarship on money and monetary technologies could be mutually intelligible.

The second of impact of the performative turn on the study of money is tied to the notion of economic assemblages: This new emphasis on the conditions that make economic phenomena (e.g., markets) possible opened a path to conceptualizing *money itself* as an assemblage. In this view, money is not so much a single phenomenon or artifact; rather, it is a kind of conceptual marker for the *intersection* of a myriad of processes, procedures, artifacts, behaviors, and beliefs, all of which add some dimension to money but none of which capture any sort of monetary essence. Nigel Dodd's *The Social Life of Money* is a good example of this approach: Rather than focusing only on the contributions of his own discipline (sociology), Dodd embraces the perspectives of economics, philosophy, anthropology, literary theory, and finance.<sup>68</sup> The result is a multifaceted view of money—money as barter, money as tribute, money as quantification, money as mana, money as language, and money as violence—that accounts for money from a diverse range of perspectives; in other words, rather than trying to pin down a single definition or conception of money, Dodd embraces a pragmatist, pluralist, and transdisciplinary

---

Maurer, Taylor C. Nelms, and Stephen C. Rea, "Bridges to Cash': Channelling Agency in Mobile Money," *Journal of the Royal Anthropological Institute* 19, no. 1 (2013): 52–74, <https://doi.org/10.1111/1467-9655.12003> and; Swartz, "Tokens, Ledgers, and Rails."

<sup>68</sup> Nigel Dodd, *The Social Life of Money* (Princeton, NJ: Princeton University Press, 2014); this is somewhat of a break from his earlier work in Dodd, *The Sociology of Money*.

approach that integrates multiple views on money.<sup>69</sup> And crucially, this approach to money represents a dramatic elevation of the role of discourse in money studies, insofar as discourse is no longer a mere predicate or supplement to other, more fundamental social processes, but is instead an equal member of the “money” assemblage. To be sure, money’s “functions” (e.g., medium of exchange) are an important part of this assemblage, as are the productive relations of creditor and debtor (Ingham), and the everyday practices of earmarking (Zelizer), but an understanding of money as an assemblage places all of these elements on the same conceptual level as discourse. All are participants in this thing called “money,” and none are intrinsically preeminent.

This view of money as an assemblage or conceptual marker brings us to the third key impact of the performative turn on money scholarship: The refiguring of money scholarship itself in performative terms. Prior to the performative turn, theories of money could be understood as competing attempts to account for some phenomenon “out there” in the world; even though such theories might diverge in their explanations of money, they shared a metatheoretical commitment to the division between object and the theory attempting to account for that object. For example, even though the functionalist definition of money and Zelizer’s continuum of “moneyness” are in opposition as *theories*, both share an assumption of money’s independence from their accounts of it. But the performative turn and a view of money-as-assemblage collapses this distinction, not in the sense that

---

<sup>69</sup> For a similar though less comprehensive approach to money, see Massimo Amato, Luigi Doria, and Luca Fantacci, eds., *Money and Calculation: Economic and Sociological Perspectives*, Bocconi on Management Series (Hampshire ; New York: Palgrave Macmillan, 2010); also see Zelizer’s engagement with the performative turn in Viviana Zelizer, “Pasts and Futures of Economic Sociology,” *American Behavioral Scientist* 50, no. 8 (April 2007): 1056–69, <https://doi.org/10.1177/0002764207299353>.

theories of money are understood as creating their object out of thin air, independent of other processes, but rather in the sense that scholarship on money is itself understood as one element involved in the framing (to use Callon's term) of money. In other words, viewing money as an assemblage, as a conceptual marker indicating the intersection of a variety of phenomena, refigures the seemingly endless debates over "what money is" as *participants in the construction of money*, rather than as attempts to accurately represent some separate phenomenon "out there" in the world.

At this point, it is necessary to address the obvious objection: Is it not the case that this conceptual pluralism—in which functionalist, embeddedness, etc. accounts of money, not to mention wildly inaccurate lay theories of money ("It's backed by gold at Fort Knox!"), are all held as conceptually equal—leads to a dead end of relativism? Don't we end up with an infinitely expandable, and therefore analytically useless, view of money? Surely if everything can be money then nothing is *really* money. The response to this objection brings us to the final—and for the purposes of this chapter, most significant—implication of the performative turn for money scholarship. Simply put, the claim that money is an assemblage does *not* imply that all elements in that assemblage are *equally* significant. With respect to discourse in particular, the claim that discourse—including money scholarship—is a part of the construction of money does not imply that every bit of money discourse has a relevant impact on that construction. To the contrary, it is both possible and necessary to assess the significance of a given discursive element to the assemblage of money *by examining its impact and influence on other parts of the assemblage*.

Indeed, some of the strongest contributions to the literature on the performativity of economics do precisely this. Donald MacKenzie's account of the development of

derivative trading in the U.S. hinges on the expressly *rhetorical* work of convincing regulators to allow the creation of derivatives markets; that is to say, MacKenzie shows how discursive interventions (specifically, academic arguments justifying derivatives, and personal conversations between regulators and those interested in establishing derivatives trading) in the assemblage of U.S. markets impacted the boundaries of those markets (i.e., the activity of trading expanded to include derivatives).<sup>70</sup> Similarly, Alex Preda's account of the origins of the stock ticker shows how the introduction of the ticker helped to construct markets by literally *producing new kinds of discourse* about them (i.e., more frequent and systematic price updates).<sup>71</sup> New forms of price data allowed for new forms of representation (e.g., more detailed price charts), which enabled the development of new forms of interpretation (e.g., technical analysis), which in turn guided market action (e.g., investment).

In other words, taking seriously the performative turn in the context of money studies necessitates something like *rhetorical analysis*—the analysis of discursive *effects* in the construction of money.<sup>72</sup> If a theory of money (e.g., the long-dominant functionalist

---

<sup>70</sup> MacKenzie, *An Engine, Not a Camera*.

<sup>71</sup> Alex Preda, *Framing Finance: The Boundaries of Markets and Modern Capitalism* (Chicago: The University of Chicago Press, 2009).

<sup>72</sup> In this way, the influence of the performative turn comes full circle: One of Callon's initial influences was Deidre McCloskey's work on the rhetoric of economics, and while the explicitly rhetorical dimension of performativity largely fell to the background as the literature developed (with important exceptions; see Svetlova), the basic point that discourse about economic life takes the form of argument and persuasion still stands. See Deirdre N. McCloskey, *The Rhetoric of Economics*, 2nd ed. (Madison, WI: University of Wisconsin Press, 1998); and Ekaterina Svetlova, "Performativity and Emergence of Institutions," in *Enacting Dismal Science: New Perspectives on the Performativity of Economics*, ed. Ivan Boldyrev and Ekaterina Svetlova, *Perspectives from Social Economics* (New York: Palgrave Macmillan, 2016), 183–200; for Callon's explicit discussion of the

account) can be shown to impact other parts of the money assemblage (e.g., the behavior of central banks), then what is demonstrated is precisely the *rhetorical* significance of that discourse; by contrast, if a discursive intervention *cannot* be shown to influence other parts of the money assemblage, then it may be safely set aside. Thus, the pluralist approach to money is not tantamount to relativism, but it does necessitate a pragmatic, rhetorical orientation: What makes the study of discourse important to the study of money is the potential (but not the inevitability) of discourse shaping money itself.

### *Bitcoin and the rhetoric of money*

At this point, it is possible to return to this chapter's opening question: When someone asks (or responds to) the question of "Is Bitcoin money?" what exactly is the question (or answer) *doing*? The threads of literature reviewed in this chapter each suggest a distinct answer. From the perspective of the functionalist definition of money, discourse is merely a more or less adequate facilitator of more fundamental economic analysis; the question "Is Bitcoin money?" is a matter of comparison, and the only role for discourse is to present this comparison clearly and accurately. Curiously enough, the constructionist approach to money would understand both the question and responses to it in a manner similar to the functionalist approach, precisely because the only role for discourse in the constructionist account is at the founding of money—and subsequently, answering the question of "Is *X* money?" is a matter of comparison to the original dynamic of credit and debt. From the embeddedness perspective, however, the question appears somewhat

---

rhetorical tradition, see Callon, "What Does It Mean to Say That Economics Is Performative?," 316.

differently. Here the question may be understood as an attempt to situate Bitcoin along a spectrum of money-like objects; that is to say, as discursive elements, both the question and its responses are attempts to embed Bitcoin in the social, to integrate this new technology into preexisting understandings of money. And finally, from a more performative perspective, the question of “Is Bitcoin money?” becomes legible not only as an attempt to construct Bitcoin, but also as an attempt to construct money itself, too.

So is there a “correct” way to understand the question of “Is Bitcoin money?” It is worth emphasizing that the point of this theoretical review is not to settle on a single definition or conception of money. Though the various perspectives on money that this chapter has covered have proceeded in a more or less historical sequence, this ordering is not meant to suggest that the embeddedness perspective, for instance, definitively supersedes the abstraction of the functionalist approach. Rather, it is the *plurality* of implied relationships between the study of money and the study of discourse that is significant here, because the very fact of this plurality suggests that “Is Bitcoin money?” may be understood as *more* than a process of comparison—though clearly it *is* a process of comparison, too—and therefore studies of Bitcoin need not foreclose the study of discourse. That said, a research agenda that takes this plurality as its point of departure—as the present study does—will necessarily be guided by the conception of economic phenomena provided by the performative turn. Again, this is not to say that the “pure” economic analysis of Bitcoin, framed in terms of the “real” economy, is not useful, or that it should not be undertaken; the point is that such an analysis is not the *only* lens available for viewing the emergence of Bitcoin, and that there exist equally valid approaches to studying

economic phenomena that do in fact place discourse—and in particular, rhetoric—at the center of inquiry.

And given the massive proliferation of discourse about Bitcoin over the last nine years, it seems that research informed by a view of economic phenomena as at least in part *rhetorically constructed* would be a welcome complement to studies of Bitcoin along more traditional economic or sociological lines. If so many people have spent so much time, money, and effort *talking* about this new monetary technology, and if there exists a conceptual framework to support the investigation of this talk as part of the construction of Bitcoin as a technological and economic object, then it seems that Bitcoin scholarship would be remiss to pass over discourse without trying to account for the role that it has played in making Bitcoin what it is today. Simply put, to begin to make sense of Bitcoin's astounding rise, it is necessary to examine the rhetorical dynamics at work in this strange new "money."

## Chapter Two

### Constructing a Collective: Digital Metallism and the Procedural Rhetoric of Bitcoin

The previous chapter's review of theories of money and discourse presented a justification for the rhetorical study of money and Bitcoin. If the last nine years of Bitcoin discourse—the books and blog posts and white papers and op-eds—are understood not as a mass of attempts to elucidate or occlude some deeper economic reality (e.g., that Bitcoin is or is not a form of money), but rather as a series of performative interventions in the construction of Bitcoin as an assemblage, then making sense of Bitcoin's development entails analysis of the rhetorical dynamics at work in this assemblage. From this perspective, the tropes of Bitcoin discourse, the controversies and conflicts that have prompted commentary and debate, the personae adopted by participants in these debates—all of this becomes legible not only as responses to the emergence of a new monetary technology, but also as integral elements of that monetary technology's construction.

And with this theoretical foundation established, it is possible to return to this study's central task, a task that will occupy this chapter and the two that follow—namely, identifying and explicating the key rhetorical currents in the construction of Bitcoin. Accordingly, this chapter develops a reading of what I argue is Bitcoin's central rhetorical dynamic: The shifting of the space of politics from the production and use of Bitcoin as a form of money to the development of Bitcoin as software. To this end, I proceed in three steps. First, I engage the burgeoning scholarly literature on Bitcoin discourse, a literature that has thus far focused on the problem of *establishing* Bitcoin as a new form of money. I

show how “digital metallism,” identified in prior studies of Bitcoin discourse as a key trope in representations of Bitcoin’s value, responds to a performative contradiction in the establishment of new forms of money, and I highlight the way that this contradiction hinges on the transition of valuation from individual conviction to social fact. Second, I consider the limitations of digital metallism as a means of understanding Bitcoin rhetoric, and I show that fully accounting for the rhetorical implications of this trope requires situating digital metallism in relation to Bitcoin’s own rhetoric as a monetary protocol—that is, in relation to Bitcoin’s procedural rhetoric. Third, I advance a reading of Nakamoto’s original Bitcoin whitepaper as a means of addressing Bitcoin as a procedural object, and I show how the procedural rhetoric of Bitcoin complicates the rhetoric of digital metallism by figuring digital metallism not as a foreclosure of politics—as the trope purports to be—but as a shifting of the political space from the use of Bitcoin as a form of money to the development of Bitcoin as software.

### *The rhetorical problem of establishing money*

New currencies are a tough sell, rhetorically speaking. The trouble starts with money’s curious place in social life: “Money works best,” write sociologists Bruce Carruthers and Sarah Babb in their study of postbellum monetary rhetoric, “when it can be taken for granted, when its value, negotiability, and neutrality can simply be assumed.”<sup>1</sup> In other words, as a mediator of exchange and as a facilitator of economic relations, the success of a currency is measured by the extent to which it remains out of mind. It is only

---

<sup>1</sup> Bruce G. Carruthers and Sarah Babb, “The Color of Money and the Nature of Value: Greenbacks and Gold in Postbellum America,” *American Journal of Sociology* 101, no. 6 (May 1996): 1556, <https://doi.org/10.1086/230867>.

when something goes awry—counterfeiting or rapid inflation or sudden shifts in exchange rates—that a particular currency draws attention to itself *as a monetary form*, with all of its specific legal, political, cultural, and material limitations. Simply put, a socially effective currency is one that avoids highlighting its own social construction; it simply appears to *be* money.

Consequently, the introduction of a *new* currency, such as Bitcoin, presents its advocates with something of a rhetorical contradiction. On one hand, the efficacy of a given form of money is tied to the extent to which it remains unexamined. On the other hand, new currencies cannot rely on historical precedent for their social efficacy; instead, new forms of money necessitate arguments about why *this* currency should be treated as money. But arguments for a particular monetary form work directly against the very thing that makes a currency effective: its unexamined and unquestioned presence in social life. In this way, the introduction of a new currency requires rhetorical labor on two fronts at once: Arguments in favor of a new currency must simultaneously argue for the legitimacy of the new monetary form even as these arguments occlude their own presence as arguments.

In other words, the establishment of money faces the challenge of transitioning from individual conviction to social fact. Here we return to Hahn's argument about the origins of money—that it is “advantageous for any given agent to mediate his transactions by money provided that all other agents do likewise”<sup>2</sup>—and Ingham's critique of it: The problem of money's origins cannot be reduced to individual action precisely because there exists a gap between the individual and the social—that is to say, because the establishment of money

---

<sup>2</sup> Hahn, “The Foundations of Monetary Theory,” 57.

depends not only on the beliefs of an individual, but also on the individual's beliefs *about others' beliefs*.<sup>3</sup> This means that the demonstration of equivalence between some object and money—for example, the comparison of Bitcoin to the classic functions of money—is not rhetorically sufficient to establish that object as money for an individual, insofar as the demonstration is itself legible as *rhetorical act targeting the individual*. What needs to be demonstrated is not that the object fits some conception of money, but rather that everyone else will behave as if it does—in short, that the demonstration is already a *fait accompli*, and therefore not a rhetorical intervention at all.

This seems to be an impossible, contradictory task. And yet new forms of money *are* established. The rhetorical feat of producing collective belief, even as the production is itself obscured, *can* be accomplished. So how does this happen? We have already hinted at one potential answer in the previous chapter's review of the constructionist approach to money: Institutional *authority* can be wielded to establish money. The rhetorical strategy is this: When a state or a bank establishes money, it draws on its preexisting rhetorical assets—ranging from legitimacy to the threat of violence—and individual belief in the “money-ness” of the new currency is cultivated through association with the preexisting beliefs about the authority of the state or bank. Crucially, these preexisting beliefs about the institution are not exactly the individual's (i.e., belonging to the audience for this rhetorical appeal); rather, they are reflexive, meta-beliefs—beliefs about the institution that the individual believes *others* to believe. This structure of meta-belief allows the institution to sidestep the task of persuading *individuals* to accept the new money and to move directly to persuading a collective audience: If an individual believes that others

---

<sup>3</sup> Ingham, “Money Is a Social Relation.”

believe that the state or bank is authoritative, the state or bank can legitimate the new money *by acting as if no legitimation is needed* (e.g., by accepting the new money as payment for taxes).<sup>4</sup> In other words, this rhetorical strategy is one that ostensibly targets the generalized Other rather than the individual, but it is effective at the individual level precisely to the extent that the individual believes that the generalized Other believes as well. This is not to say that such strategies are always effective; the rhetorical resources of the state or bank may not be sufficient to establish a new form of money, or they may only be sufficient to establish the new money as an inferior alternative to prior currencies. But when such strategies *are* effective, the rhetorical feat is accomplished by leveraging the institution's ability to address the Other rather than the individual.

And this point brings us to the limit of such a strategy: Establishing money in this way depends on the rhetorical resources of the state or bank—specifically, the ability to authoritatively address the generalized Other—and consequently it is not applicable to forms of money not associated with an institution.<sup>5</sup> But the appeal to authority is not the only way of dealing with the rhetorical problem of establishing money. Another way out of this rhetorical contradiction—a path well-trod, as Carruthers and Babb show, by 19<sup>th</sup> century commodity theorists of money, and still employed today by some on the libertarian

---

<sup>4</sup> However, this lack of legitimation still needs to be *enacted* (e.g., by declaring a creditor/debtor relationship), as Ingham argues in Ingham, *The Nature of Money*.

<sup>5</sup> For this reason, Ingham objects to understanding alternative monies (e.g., local exchange trading systems) *as money*; in Ingham's view, money requires that this initial rhetorical move be made by an authoritative institution. See Geoffrey Ingham, "The Specificity of Money," *European Journal of Sociology* 48, no. 02 (August 2007), <https://doi.org/10.1017/S0003975607000367>.

right—is a strategy of naturalization.<sup>6</sup> This strategy, which may very well serve as a complement to the institution-oriented strategy just discussed, attempts to legitimate a form of money through appeals to its “natural” value.<sup>7</sup> For example, in the case of commodity-based currencies, such as gold or silver, it is claimed that the intrinsic utility and natural scarcity of the particular commodity gives money its value, and thus assures the currency’s firm foundation as the unexamined and unquestioned backdrop of exchange. In the case of paper currencies tied to commodity stores (e.g., the “gold standard”), this process is mediated through a token, but the essential dynamic remains the same: Echoing the metatheory of the “real” economy, the currency is understood as a representation of a deeper, more “natural” economic substrate. Crucially, instead of grounding money’s value in the *politics* of a community (i.e., the communal agreement that *X* is money, or that institution *Y* has the authority to determine that *X* is money), this rhetorical strategy has “the ideological effect of naturalizing, and thereby concealing, the social relation of credit that underpin[s] the monetary promise to pay.”<sup>8</sup> In other words, the strategy of naturalization employs the age-old rhetorical feint of denying rhetoric altogether: While the strategy of appealing to institutional authority grounds money in the political—and by extension, the self-evidently artificial—the rhetoric of commodity currencies, grounded in the supposed economic reality of “intrinsic value,” simply “tells it like it is.” In commodity

---

<sup>6</sup> Carruthers and Babb, “The Color of Money and the Nature of Value.”

<sup>7</sup> For a historical overview and critique of this strategy, see the first chapter of Ingham, *The Nature of Money*.

<sup>8</sup> Ingham, “The Emergence of Capitalist Credit Money,” 179.

rhetoric, the currency is money not because it is embedded in a *polis*, but precisely the opposite—that is, because it is beyond the reach of the political.

*From commodity to code*

Here we can return to Bitcoin. Suspect as the appeals to naturally self-evident value may be, they *are* rhetorically productive, and given Bitcoin's lack of a central institution capable of addressing the generalized Other of the Bitcoin community, commodity money rhetorics present an appealing path for establishing Bitcoin as a form of money. But the adaptation of commodity rhetoric to Bitcoin is not a straightforward process, in part because Bitcoin faces the significant challenge of lacking any association with a "natural" commodity. There is no precious metal sitting at the base of Bitcoin's valuation; nor, for that matter, is there any looming threat of state power, the "backing" typically identified as the support of fiat currencies when commodity rhetoric is transposed to contemporary monetary forms. Without such support, Bitcoin advocates seem fated to fall back into the same rhetorical dilemma faced by all new monetary forms: How do you get people to believe that this thing is money without drawing too much attention to your attempt to do so?

Bitcoin's solution—or more properly, the solution employed by early Bitcoin advocates—is the object of study of the first substantial examination of Bitcoin discourse: Maurer, Nelms, and Swartz's "When perhaps the real problem is money itself!: The practical materiality of Bitcoin."<sup>9</sup> Though this essay is guided by a social semiotic perspective rather than an explicitly rhetorical orientation, Maurer et al. nevertheless

---

<sup>9</sup> Maurer, Nelms, and Swartz, "When Perhaps the Real Problem Is Money Itself!"

explicate a rhetorically significant dimension of Bitcoin discourse, which they term “digital metallism.” Here they build on Geoffrey Ingham’s term, “practical metallism”—which Ingham uses to describe the naturalizing function of the rhetoric of commodity theories of money—by drawing attention to the similarity between commodity theories of money and certain arguments for Bitcoin’s value.<sup>10</sup> Maurer et al.’s key insight is that naturalization arguments about Bitcoin’s value draw on the framework of commodity theories of money, but in the case of Bitcoin, the object that justifies this naturalization shifts from a precious commodity (e.g., gold, silver) to the *technology* of Bitcoin. This shift is visible in the “potent discursive investment by Bitcoin users in the determinist mechanics of Bitcoin’s code.”<sup>11</sup> For example, typical responses to the question of “What backs Bitcoin?”—a question frequently posed on the message boards, chat rooms, and email listservs of the Bitcoin community—clearly demonstrate this discursive investment: In contrast to commodity-backed currencies or state-backed fiat currencies, Bitcoin is said to be “backed by cryptography and decentralization,”<sup>12</sup> or “by the most powerful and secure decentralized distributed computational network on the planet,”<sup>13</sup> or “by math, miners, and the

---

<sup>10</sup> In turn, Ingham borrows the term from Joseph Schumpeter, who distinguishes between “theoretical” and “practical” metallists—that is, between true believers in the intrinsic value of commodity money, and those who “understood that this form of money-stuff would be trusted more readily than a mere promise to pay.” Geoffrey Ingham, “‘Babylonian Madness’: On the Historical and Sociological Origins of Money,” in *What Is Money?*, ed. John N. Smithin, Routledge International Studies in Money and Banking 6 (London ; New York: Routledge, 2000), 31; also see Ingham, “The Emergence of Capitalist Credit Money.”

<sup>11</sup> Maurer, Nelms, and Swartz, “When Perhaps the Real Problem Is Money Itself!,” 2.

<sup>12</sup> anon13488, “I Believe in Bitcoin,” *Reddit*, November 29, 2013, [https://www.reddit.com/r/Bitcoin/comments/1rq8ua/i\\_believe\\_in\\_bitcoin/](https://www.reddit.com/r/Bitcoin/comments/1rq8ua/i_believe_in_bitcoin/).

<sup>13</sup> HermanLeon, “Here Is an Answer When Somebody Says: ‘Bitcoin Is Backed by Nothing!’,” *Reddit*, December 12, 2014,

protocol.”<sup>14</sup> The key point here is not the specifics of each response, but rather the way that all hew to a common pattern of explanation that *figures the technological underpinnings of Bitcoin as a “natural” object*—an object beyond the reach any community influence or coercion, and one that consequently *forecloses the political*. As Bitcoin entrepreneur Erik Voorhees puts it, “the government, no matter how many guns they draw, cannot change a mathematical problem”—that is, no central authority can change the technological basis of Bitcoin.<sup>15</sup> This is the crux of digital metallism as a rhetorical strategy: By treating the technology of Bitcoin as a source of value located beyond the influence of political intervention, the rhetorical structure of commodity arguments is maintained, but the commodity base is replaced with code.

Maurer et al.’s analysis of digital metallism is a valuable first step in the study of Bitcoin discourse, and the significance of the trope has been borne out by subsequent research: Lynette Shaw’s automated content analysis of Bitcoin message boards, which offers a big data approach to the analysis Bitcoin discourse, has demonstrated the prevalence of digital metallism as an discursive pattern throughout the broader Bitcoin community.<sup>16</sup> However, this initial work raises two further questions about the rhetorical dimensions of digital metallism. First, while the identification of digital metallism as a trope

---

[https://www.reddit.com/r/Bitcoin/comments/2p4yfy/here\\_is\\_an\\_answer\\_when\\_somebody\\_says\\_bitcoin\\_is/](https://www.reddit.com/r/Bitcoin/comments/2p4yfy/here_is_an_answer_when_somebody_says_bitcoin_is/).

<sup>14</sup> “Should Bitcoin Be Backed by Something like Bullion? Gold, Silver, Oil, Platinum?,” Bitcoin FAQ, January 31, 2013, <http://bitcoin-faq.com/should-bitcoin-be-backed-by-something-like-bullion-gold-silver-oil-platinum/>.

<sup>15</sup> Nicholas Mross, *The Rise and Rise of Bitcoin*, Documentary (Gravitas Ventures, 2014).

<sup>16</sup> Shaw, “The Meanings of New Money.”

is a useful starting point for analysis, there is still a need to explain its rhetorical force—that is, to explain why *this* trope in particular proliferated throughout the Bitcoin community and played a noticeable role in the economic assemblage of Bitcoin. This question can be addressed to some extent by pointing to the ideological inclinations of early members of the Bitcoin community: As a number of political analyses of Bitcoin have noted, the politics of the early Bitcoin community drew heavily from right-wing political thought—particularly from strains of cyberlibertarianism and anarcho-capitalism, traditions for which commodity money rhetoric is a familiar companion—and if early Bitcoin supporters were already politically inclined to accept commodity money arguments, then digital metallism can be understood as a rhetorically appropriate response to the community in which it emerged.<sup>17</sup> The early prevalence of digital metallism can also be attributed, at least in part, to the terminology introduced in Nakamoto's white paper (e.g., "mining" Bitcoins)<sup>18</sup>—a terminology that was itself influenced, via earlier cyberlibertarian attempts to build "digital gold," by commodity theories of money.<sup>19</sup> But given that the Bitcoin community grew beyond these early, cyberlibertarian adopters to include individuals and institutions adamantly opposed to commodity money theories and rhetorics, it is difficult to connect this early rhetorical success to the "mainstreaming" of

---

<sup>17</sup> See Karlstrøm, "Do Libertarians Dream of Electric Coins?"; and Golumbia, *The Politics of Bitcoin*; and for an introduction to the political tradition that inspired early Bitcoin advocates, see Peter Ludlow, ed., *Crypto Anarchy, Cyberstates, and Pirate Utopias* (Cambridge, MA: MIT Press, 2001); particularly Eric Hughes, "A Cypherpunk's Manifesto," in *Crypto Anarchy, Cyberstates, and Pirate Utopias*, ed. Peter Ludlow (Cambridge, MA: MIT Press, 2001), 81–83.

<sup>18</sup> Nakamoto, "Bitcoin," 4.

<sup>19</sup> Karlstrøm, "Do Libertarians Dream of Electric Coins?"; and Swartz, "Tokens, Ledgers, and Rails," 182–92.

Bitcoin. After all, to those not ideologically predisposed to accept a foundation of money in “intrinsic value,” the rhetoric of digital metallism seems to present a blatant contradiction: a “natural” grounding in the artifice of technology. So what made the figuring of Bitcoin as a form of “digital gold” an attractive and apparently successful rhetorical strategy?

Second, the studies of Maurer et al. and Shaw both demonstrate a crucial conceptual limitation: They both treat the process of Bitcoin representation as beginning with talk *about* the currency, and omit consideration of the ways that Bitcoin, as a technology, is itself engaged in the work of representation. That is to say, viewing digital metallism as a supplement to an apparently semiotically neutral technology implicitly buys into the characterization of the technology of Bitcoin developed by the adaptation of commodity arguments to digital currencies—a characterization of Bitcoin’s technology as a “natural” ground of value situated beyond the influence of the political, and as a non-participant in the currency’s own representation. In short, digital metallism, as a concept, effectively brackets the rhetorical force of Bitcoin as a technology. This is not to suggest that digital metallism is useless or fatally flawed as a concept; rather, it is merely a limited tool for rhetorical analysis—and quite understandably so, given that neither Maurer et al. nor Shaw adopted an explicitly rhetorical aim. Digital metallism focuses attention on one aspect of Bitcoin discourse and omits consideration of other aspects, including Bitcoin’s technological foundation, but from a rhetorical perspective this is an especially significant omission, given the possibility that the technology of Bitcoin may or may not perform rhetorical work complementary to the discourse *about* Bitcoin. So how should the rhetoric of digital metallism be understood in relation to Bitcoin’s technology?

To account for both of these questions, and to contribute to this dissertation's overall goal of understanding Bitcoin as a performative assemblage, the remainder of this chapter presents an analysis of Bitcoin's procedural rhetoric—that is, the rhetoric of Bitcoin as a computational process and protocol—as a counterpart to the rhetoric of digital metallism. To this end, I first briefly review the literature on procedural rhetoric, and explain its special relevance to the rhetorical ecologies of digital objects such as Bitcoin. Next, I discuss the difficulties in identifying the specific procedural basis of Bitcoin given the currency's continual technical development. My solution to this difficulty engages the rest of the chapter: By reading the original Bitcoin white paper—the first public description of Bitcoin's technical foundation by Bitcoin inventor Satoshi Nakamoto—against Nakamoto's own characterization of the technology, it is possible to analyze the ways in which the protocol of Bitcoin exerts a rhetorical force of its own, independent of discourse *about* Bitcoin. Ultimately, I argue that the procedural rhetoric of Bitcoin produces what I term an “individualist collective”—that is, a state of consensus among individuals without the integration of those individuals into any broader social structure. Crucially, this individualist collective *seems* to accomplish the very thing that the rhetoric of digital metallism aspires to achieve—that is, the foreclosure of politics in the domain of money—and it is this apparent achievement, I argue, that reinforces the rhetoric of digital metallism, and helps to explain the strength of this trope. However, I show that this achievement is only apparent, insofar as the protocol actually shifts the space of political contest outside of itself—that is to say, within the Bitcoin protocol, politics are foreclosed, but this merely makes the *construction of the protocol* a key point of political contest. In other words, while digital metallism and the procedural rhetoric of Bitcoin are rhetorically effective because

together they seem to enact a foreclosure of politics, both must be understood instead as a *displacement* of politics, a politics that returns in contests over the very rules of the game—that is, over how the protocol itself should be constructed.

### *Procedural rhetoric and rhetorical ecologies*

To begin this chapter's analysis of Bitcoin as a computational artifact, it is necessary to take a brief detour through one of the most significant contributions to the study of digital rhetoric in recent years: Ian Bogost's *Persuasive Games*.<sup>20</sup> Bogost's contribution begins with a critique of prior scholarship in digital rhetoric: "Digital rhetoric tends to focus on the presentation of traditional materials—especially text and images," he claims, "without accounting for the computational underpinnings of that presentation."<sup>21</sup> What is needed, Bogost argues, is an approach to digital objects that "address[es] the role of procedurality, the unique representational property of the computer."<sup>22</sup> In short, rhetorical scholars cannot assume that the analytical tools developed for one medium (e.g., writing) can grasp all of the rhetorical complexities of another (i.e., the computer); new tools are needed for the analysis of digital rhetoric.

With this need in mind, Bogost introduces his concept of *procedural rhetoric*. Procedural rhetoric, Bogost explains, is a "type of persuasion [...] tied to the core affordances of the computer," and is defined as "the art of persuasion through rule-based representations and interactions rather than with the spoken word, writing, images, or

---

<sup>20</sup> Bogost, *Persuasive Games*.

<sup>21</sup> *Ibid.*, 28.

<sup>22</sup> *Ibid.*

moving pictures.”<sup>23</sup> In contrast to conceptions of digital rhetoric that focus exclusively on the content or style of digital objects, procedural rhetoric, as a tool for rhetorical analysis, points to the ways that digital objects may exert a persuasive force in the very structure of their rules, protocols, and procedures.<sup>24</sup>

Bogost’s analysis of *The McDonald’s Videogame*, a game designed as a critique of fast food corporations, offers a helpful example of this kind of rhetoric:

*The McDonald’s Videogame* is a critique of McDonald’s business practices by Italian social critic collective Molleindustria. [...] The player controls four separate aspects of the McDonald’s production environment, each of which he has to manage simultaneously: the third-world pasture where cattle are raised as cheaply as possible; the slaughterhouse where cattle are fattened for slaughter; the restaurant where burgers are sold; and the corporate offices where lobbying, public relations, and marketing are managed.<sup>25</sup>

Each section of the game requires the game’s player to make challenging business decisions, and to weigh these decisions against moral considerations. For example, “in the pasture, the player must create enough cattle-grazing land and soy crops to produce the meat required to run the business,”<sup>26</sup> but given the limited supply of land, the player is forced to choose between “brib[ing] the local governor for rights to convert his people’s crops into corporate ones,” or “bulldoz[ing] rainforest,” or even “dismantle[ing] indigenous

---

<sup>23</sup> Ibid., ix.

<sup>24</sup> It is worth noting that there is substantial overlap between Bogost’s concept of procedure and Alexander Galloway’s notion of protocol. However, procedural rhetoric is distinct in its explicitly rhetorical orientation. See Alexander R. Galloway, *Protocol: How Control Exists after Decentralization* (Cambridge, MA: MIT Press, 2004).

<sup>25</sup> Bogost, *Persuasive Games*, 29.

<sup>26</sup> Ibid.

settlements to clear space for grazing.”<sup>27</sup> By representing the business practices of McDonald’s through these particular sets of rule-governed choices, *The McDonald’s Videogame* “mounts a procedural rhetoric about the necessity of corruption in the global fast food business.”<sup>28</sup>

Though Bogost is primarily interested in the specific computational form of the videogame, and dedicates the majority of *Persuasive Games* to artifacts in this vein, he is careful to point out that the rhetorical force of rule-based, procedural systems should not be understood as restricted to games,<sup>29</sup> and it is this broader introduction of *procedure* to rhetorical scholarship that has served as a much needed corrective to previous trends in the subfield of digital rhetoric. But the introduction of this new concept and tool for analysis also raises an additional conceptual problem: What is the relationship between the procedures of a digital object and its content—that is, the more traditional rhetorical matters of text, image, and sound? Bogost seems to suggest that procedural rhetoric often works in concert with more traditional rhetorical elements, but it is unclear if this is always the case. Indeed, it seems that the very conceptual division between procedure and content (e.g., text, images) must allow for a divergence between the two, but Bogost does not address such cases in detail. The question, in other words, is one of procedural rhetoric’s

---

<sup>27</sup> Ibid., 29–30.

<sup>28</sup> Ibid., 31.

<sup>29</sup> “Despite my preference for videogames,” Bogost writes, “I should stress that I intend the reader to see *procedural rhetoric* as a domain much broader than that of videogames, encompassing any medium—computational or not—that accomplishes its inscription via processes.” Ibid., 46.

place in a broader rhetorical ecology.<sup>30</sup> Yes, it is important to study the rhetoric of procedures, but how does *that* rhetoric interact with the multiple, multivalent, and potentially contradictory *rhetorics* of a given digital object?

James J. Brown's *Ethical Programs* helpfully builds on Bogost's work to address this question.<sup>31</sup> More specifically, Brown "offer[s] three rhetorics of software—arguing *about* software, arguing *with* software, and arguing *in* software—as a way of productively expanding digital rhetoric beyond procedural rhetoric."<sup>32</sup> In brief, arguing *about* software is the domain most familiar to rhetorical scholars: Located here are the metaphors, tropes, narratives, and arguments used to describe digital objects. Arguing *with* software is the domain of procedural rhetoric: the ways in which digital objects, in their rules and protocols, perform rhetorical labor. And finally, arguing *in* software highlights the ways in which the very developmental processes of software may themselves be understood as rhetorical. For example, software developers, in their production of digital artifacts, choose particular patterns and procedural schemas that in turn influence subsequent patterns of development—and this is a rhetorical process, albeit one not visible in discourse *about* the software or argued through a user's interaction with a set of procedures.<sup>33</sup> The utility of

---

<sup>30</sup> Jenny Edbauer, "Unframing Models of Public Distribution: From Rhetorical Situation to Rhetorical Ecologies," *Rhetoric Society Quarterly* 35, no. 4 (September 2005): 5–24, <https://doi.org/10.1080/02773940509391320>.

<sup>31</sup> Brown, *Ethical Programs*.

<sup>32</sup> *Ibid.*, 173.

<sup>33</sup> The aestheticization of coding, for instance, is a unique intersection of arguments *about* software and arguments *in* software: Aestheticization marks the development of discourse *about* arguments *in* software. For example, see Andrew Oram and Greg Wilson, eds., *Beautiful Code: Leading Programmers Explain How They Think* (Sebastapol, CA: O'Reilly, 2007).

these three levels, as Brown points out, is that each may advance a rhetoric independent of the others, and in doing so, each may respond to or have its rhetorical force altered by the rhetorics existing at other levels. In this way, “all of the interesting rhetorics of software participate in complex rhetorical ecologies.”<sup>34</sup> And it is this ecological aspect that is key to understanding the rhetorical workings of digital objects. To return to the earlier example of *The McDonald’s Videogame*: The game certainly advances an argument about corruption and fast food business at the level of the game’s rules, but the full force of the argument equally depends upon the representational content of the game (e.g., the name “McDonald’s”). A game with the same rules but different content would simply not advance the same argument, and thus the *interactions* between different facets of the game’s rhetorical ecology must be taken into account to properly assess its overall rhetorical functioning.

### *Locating Bitcoin’s procedural rhetoric*

With Brown’s threefold division of digital rhetoric and the ecological implications of this division in mind, it is possible to return to Bitcoin. Patterns of discourse, such as digital metallism, clearly operate at the level of arguments *about* Bitcoin. Here we find the metaphors, narratives, arguments, and tropes that are used to characterize Bitcoin as a technology and as a currency. But this is not the only level of rhetoric engaged by Bitcoin. Both Bitcoin’s procedures—that is, the rules of Bitcoin as a protocol designed to process payment transactions—and the patterns of their development contribute to Bitcoin as a rhetorical object. Consequently, to more fully account for Bitcoin beyond the limits of

---

<sup>34</sup> Brown, *Ethical Programs*, 173.

digital metallism, it is necessary to examine Brown's levels as they relate to the rhetoric of Bitcoin. The present chapter addresses arguments *with* Bitcoin; subsequent chapters more directly address arguments *about* and *in* Bitcoin.

However, any attempt to study Bitcoin's procedural rhetoric—that is, arguments *with* Bitcoin, embedded in Bitcoin's protocol—immediately confronts a problem: *Where* are the procedures to be located? Given that Bitcoin is ultimately an elaborate system for tracking transactions—that is, a system for maintaining a record of who gave what to whom—the foundation of Bitcoin, the core of what makes it a notable technological development, is a rule-based representation of monetary transactions. But where does this protocol exist? As an open-source project, the software underlying Bitcoin is perpetually under development, and thus every concrete instantiation of Bitcoin is, by definition, incomplete. This perpetually incomplete status means that it is impossible to point to one configuration of Bitcoin software as the key representation of Bitcoin's protocol; every example of the protocol is seen through a software build. Furthermore, the boundaries of the protocol are themselves somewhat indistinct, as supplementary software and procedures can change the context in which the protocol operates, thereby altering its interactions within a given rhetorical ecology. So how can the protocol be identified and properly bounded for critical assessment?

To be sure, these problems are not necessarily insurmountable, and an analysis of Bitcoin procedural rhetoric could simply choose a particular build of Bitcoin software as a means of accessing Bitcoin's procedurality and delineating the boundaries of those procedures. There is, however, an alternative to this arbitrary selection, an alternative that corresponds to the present chapter's focus on Bitcoin's origins: Instead of locating the

protocol in any particular build of Bitcoin software, it is possible to return to Bitcoin's moment of origin, before the protocol actually existed as software, and extract the core of Bitcoin's procedural rhetoric from Nakamoto's original whitepaper.<sup>35</sup> Given that the purpose of Nakamoto's paper was to articulate the essential features of Bitcoin as a protocol, the paper makes possible the analysis of the protocol, even if this structure is not directly accessible *as* protocol. In other words, even though the white paper is not a procedural artifact, its description of Bitcoin *as a set of procedures* makes possible the study and the critical delineation of Bitcoin's procedural rhetoric.

Accessing Bitcoin's protocol in this manner, however, does present two additional challenges. First, given that Nakamoto makes reference to a variety of cryptographic and other technical concepts to explain Bitcoin as a protocol, analysis of Bitcoin's procedural rhetoric will necessitate explanations of these concepts, and will consequently entail reference to other technical literatures. It is essential here, however, not to let explanations of these technical concepts overwhelm the rhetorical impact of their *functioning* in Bitcoin's protocol. References to additional technical sources are a kind of necessary evil of explanation, and must be separated as much as possible from the procedures themselves. The second challenge is similar to the first, but originates from Nakamoto's own language. The very terms that Nakamoto uses to characterize elements of his protocol (e.g., mining) engage in significant rhetorical work—they are, in short, arguments *about* Bitcoin—and such rhetorical work occurs from the very first sentence of the paper's abstract. To avoid being unduly influenced by Nakamoto's arguments *about* Bitcoin, it is necessary to read the Bitcoin protocol *against* Nakamoto's own explanation of it. By bracketing the question of

---

<sup>35</sup> Nakamoto, "Bitcoin."

what the protocol *means* in Nakamoto's account, and by instead focusing on what the proposed protocol *does*, it is possible to analyze the protocol's procedural rhetoric, to ask how the protocol represents itself and its users, and to examine the ways that Bitcoin's protocol interfaces with other elements of Bitcoin's rhetorical ecology.

### *Bitcoin's rationale*

Nakamoto begins his white paper by explaining the rationale for his proposal. Contemporary Internet commerce, Nakamoto claims, "still suffers from the inherent weaknesses of the trust based model"—that is to say, such commerce relies on trusted third parties, such as financial institutions, to process payments.<sup>36</sup> This reliance on third parties, Nakamoto explains, means that completely non-reversible transactions, like those achievable with cash, are impossible in an online context, and this consequently raises the transaction costs associated with online commerce (i.e., payment processors have to account for chargebacks in their overhead).<sup>37</sup> To move past these problems, Nakamoto calls for "an electronic payment system based on cryptographic proof instead of trust," which will allow for the disintermediation of online commerce.<sup>38</sup> In other words, Nakamoto sees a need for a digital payments system that functions less like a debit card processor and more like cold, hard cash.

And in this, Nakamoto is far from alone. The idea of an entirely digital, cash-like currency hardly begins with Nakamoto; cryptography researchers have proposed a variety

---

<sup>36</sup> Ibid., 1.

<sup>37</sup> Ibid.

<sup>38</sup> Ibid.

of such currencies since the 1980s,<sup>39</sup> and the 1990s saw commercial implementation of some of these ideas with limited success.<sup>40</sup> But these precursors to Bitcoin all stumbled on the two key problems faced by all digital currencies:

1. *How can users trust that their money is authentic and not counterfeit?*<sup>41</sup>

Paper bills, for example, solve this problem through a variety of anti-counterfeit protections (e.g., special ink), but any entirely digital currency cannot rely on physical countermeasures.<sup>42</sup> It is also much easier to duplicate digital objects than physical ones, so digital currencies face additional challenges in this regard.

2. *How can users be sure that no one else can claim ownership of their money?*<sup>43</sup>

Again, paper bills solve this problem through physical means: Since the same bill

---

<sup>39</sup> For example, Chaum, “Blind Signatures”; Chaum, Fiat, and Naor, “Untraceable Electronic Cash”; Dai, “B-Money”; and Nick Szabo, “Bit Gold,” *Unenumerated: An Unending Variety of Topics* (blog), December 27, 2008, <http://unenumerated.blogspot.com/2005/12/bit-gold.html>.

<sup>40</sup> For example, cryptographer David Chaum founded the online payment processor DigiCash in 1989. Despite a promising beginning, the company declared bankruptcy nine years later. See Julie Pitta, “Requiem for a Bright Idea,” *Forbes*, November 1, 1999, <http://www.forbes.com/forbes/1999/1101/6411390a.html>.

<sup>41</sup> Andreas M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies* (Sebastopol, CA: O’Reilly Media, 2015), 2.

<sup>42</sup> Here it is not necessary to endorse the erroneous opposition, all too common to studies of digital rhetoric, between the digital and the material. Digital currencies *do* have a material presence. The catch, of course, is that this material presence (e.g., electrons trapped in wells) is largely beyond the scope of direct human observation. It is a problem of scale—not the supposed immateriality of digital objects—that renders physical countermeasures inapplicable to digital currencies such as Bitcoin. For an analysis of Bitcoin’s materiality, see Finn Brunton, “Heat Exchanges,” in *MoneyLab Reader: An Intervention in Digital Economy*, ed. Geert Lovink, Nathaniel Tkacz, and Patricia de Vries (Amsterdam: Institute of Network Cultures, 2015), 158–72.

<sup>43</sup> The ability for the same digital object to be sent to multiple parties as payment is referred to as the “double-spend problem.” See Antonopoulos, *Mastering Bitcoin*, 2.

cannot be in two places at once, simple material presence registers ownership of a bill. But digital currencies lack an easily identifiable material presence—and furthermore, they are easily and potentially infinitely duplicable—so they cannot rely on physical scarcity to indicate ownership.

Ultimately, Bitcoin's precursors resolved these challenges by resorting to centralization—that is, by becoming more like a debit card than like cash.<sup>44</sup> But the introductory section of the Bitcoin white paper makes clear that Nakamoto finds this solution unsatisfactory. With centralization, digital currencies simply repeat the same structural problem of contemporary Internet commerce: There is still a trusted middle party in every transaction, and that middle party is a potential point of failure or of increased costs.

In this way, the white paper's introduction establishes the problem that Nakamoto is trying to solve with his Bitcoin proposal. There is also a hint—visible in the initial introduction of concepts that are central to Bitcoin's protocol (e.g., cryptographic proof)—of the shape of Nakamoto's ultimate solution to the problems faced by digital currencies, but it is only in the second section of the paper that Nakamoto begins to describe the various portions of his protocol in detail. This description begins with a key definition in a technically dense paragraph:

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.<sup>45</sup>

---

<sup>44</sup> Mullan, *A History of Digital Currency in the United States*.

<sup>45</sup> Nakamoto, "Bitcoin," 2.

These few sentences do much to construct the foundation of Bitcoin's protocol, but explaining the full significance of this definitional work faces two challenges: First, this paragraph makes implicit reference to a range of Bitcoin precursors and cryptographic literatures; and second, the paragraph also explicitly uses terminology that associates portions of the Bitcoin protocol (e.g., "a chain of digital signatures") with particular monetary concepts (e.g., "an electronic coin"). Consequently, to explicate this section of the white paper, it is necessary to bracket momentarily the rhetorical move of equating protocol components with monetary concepts, and to explain the range of cryptographic references. I begin by explaining two key cryptographic concepts: *digital signatures* and *cryptographic hash functions*.

### *Digital signatures*

Digital signatures are a specific application of a more general category of cryptography—namely, public key cryptography—and so to adequately account for the role of digital signatures in Bitcoin, it is necessary to briefly overview this domain. In cryptography, the term "key" refers to the information needed to encrypt and/or decrypt a message. For example, a very simple encryption algorithm might make use of the "key" of converting letters of the alphabet to numbers based on a given letter's order in the alphabet. In this case, A becomes 1, B becomes 2, C becomes 3, and so on, with the end result that a message such as "H E L L O" becomes "8 5 12 12 15."<sup>46</sup> Note that in this example, the method for encrypting the message and decrypting the message are the

---

<sup>46</sup> This simple cipher is known as "Caesar's cipher," due to its alleged use by Julius Caesar. See Franco, *Understanding Bitcoin*, 52.

same—that is, they use the same key—and as a consequence, this form of encryption is known as *symmetric key cryptography*. But symmetric encryption has an important weakness. As digital currency researcher Pedro Franco explains in *Understanding Bitcoin*,

When two people use symmetric encryption, they must ensure beforehand that they both share the same symmetric key: they must interchange the keys through a secure channel before using the symmetric encryption system. However, there are many situations where it is not possible to interchange the symmetric key through a secure channel, such as e-commerce. The internet is an insecure channel: traffic can be eavesdropped and even modified in transit. Therefore it is impossible to establish a secure connection through the internet using only symmetric encryption.<sup>47</sup>

Public key cryptography solves the problem faced by symmetric key cryptography by utilizing two different keys: one for encryption and another for decryption. Franco explains this via a helpful analogy:

An analogy for symmetric key encryption is that of a safe with one key. This (symmetric) key can be used both to lock the safe (encrypt) and to unlock the safe (decrypt). A similar analogy for public key encryption is that of a safe with a pair of keys. One of the keys, the public key, can only be used to lock the safe, while the other key, the private key, can only be used to unlock the safe.<sup>48</sup>

In practice, both keys are large numbers generated using an algorithm (called a “key generation algorithm”) that guarantees each public key is mathematically linked to its corresponding private key without allowing the deduction of the private key from the public key.<sup>49</sup> The important point here, however, is not the mathematics of key generation, but rather how the different keys are used in the encryption and decryption process: While

---

<sup>47</sup> Ibid., 53.

<sup>48</sup> Ibid.

<sup>49</sup> Ibid.

the private key is to be kept secret (i.e., known only to one individual), the public key is to be published (i.e., known to anyone and everyone). This means that anyone can encrypt a message using the public key, but *only the individual possessing the private key* can decrypt the message. In fact, this system is used as the basis of many email encryption systems: First, Person A makes their public key accessible to the public (e.g., by posting it on their webpage); next, Person B encrypts an email using this public key and sends the email to Person A; and finally, Person A uses their private key to decrypt Person B's message. Throughout all of this, the encryption process guarantees that only someone in possession of the private key can read the message encrypted with the corresponding public key.

Digital signatures are an alternative application of public key cryptography, one that hinges on the mathematical links between public and private keys. In this case, instead of using a public-private pair of keys to hide messages, a key pair is used to guarantee that a publicly accessible message originated from a particular source. In brief, the process of digitally signing a message is as follows: First, Person A generates a public-private key pair and sends the public key to Person B through a communication channel; second, Person A uses an algorithm which employs Person A's private key to "sign" a message; and third, Person A sends the signed message to Person B, who can use a verification algorithm in combination with Person A's public key to authenticate the message.<sup>50</sup> In this way, Person B is able to be mathematically certain that a given message was signed by someone possessing Person A's private key. Consequently, as long as Person A maintains the security of their private key, the signature system is secure.

---

<sup>50</sup> Ibid., 57.

*Cryptographic hash functions*

With digital signatures explained, it is possible to turn to hash functions. In brief, hash functions are special mathematical functions that have the useful property of taking data of arbitrary length as input—this could be anything from a single email to the entirety of Wikipedia—and outputting a fixed length (e.g., 256 bits).<sup>51</sup> Given the nature of these hash functions, even a very small change to the input—one character, for instance—will produce a change in the hash output. For example, the SHA-256 function converts the input “This is message #1” to:

15d49403466b47ee9b8ef2f783cdce03c7d06f26310619a6dc41f0fd71a3d67e<sup>52</sup>

But simply changing “1” to “2” in this string of text dramatically changes the hash output. The input “This is message #2” generates:

dc980599bc3513462b0624c5ccce2de7817c3cf3ba7d18a65703372958201fd3

And yet even very large inputs produce an output of the exact same length. Here is the hash of the entirety of Alexander Pope’s translation of the *Iliad*, generated from Project Gutenberg’s copy of the text:

7836d2c48ac1fbca4e164d63acc04adc47ad653524b406bb7b46c0016abd0ba8<sup>53</sup>

---

<sup>51</sup> Ibid., 95.

<sup>52</sup> This and the following hashes were generated with Chris Veness, “SHA-256 Cryptographic Hash Algorithm,” Movable Type Scripts, 2015, <http://www.movable-type.co.uk/scripts/sha256.html>.

*Cryptographic* hash functions have two additional properties. First, they have “one-wayness”: If an individual has the input data, calculating the hash output is relatively easy, but if an individual only has access to the hash output, “it must be computationally infeasible to find out the input data.”<sup>54</sup> In short, “one-wayness” means that it must be infeasible to “work backwards” from the output, even though it is a simple matter to generate the output from the input (e.g., to confirm that a particular input corresponds to a particular output). Second, cryptographic hash functions are “collision-free,” which means that it is highly unlikely that two different inputs would create the same output.<sup>55</sup> For Bitcoin’s purposes, the key point is that cryptographic hash functions enable both 1) the secure recording of nearly infinite amounts of information within a relatively small space, and 2) a recording system in which it is impractical for an adversary to “work backwards” from an output to discover the system’s input.

### *Defining an electronic coin*

With digital signatures and cryptographic hash functions explained, it is possible to return to Nakamoto’s key definitional move:

---

<sup>53</sup> Generated from Homer, *The Iliad of Homer*, trans. Alexander Pope (Project Gutenberg, 2006), <https://www.gutenberg.org/files/6130/6130-h/6130-h.html>.

<sup>54</sup> Franco, *Understanding Bitcoin*, 96.

<sup>55</sup> *Ibid.* It is not, strictly speaking, *impossible* that two inputs for a function would create the same output; in fact, given that potential inputs are infinite and that potential outputs are fixed in length, no hash functions can truly be collision-free. Consequently, this hash function property is sometimes discussed in terms of “collision resistance,” which can vary in strength (i.e., the likelihood of two inputs producing the same output).

We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.<sup>56</sup>

Here Nakamoto proposes a combination of two technologies—digital signatures and cryptographic hash functions—to create a form of database entries that are “chained” together. This combination takes advantage of the properties of both digital signatures and hash functions to securely store transaction records: By “nesting” multiple hash functions—that is, by hashing some data that itself includes other data that has already been hashed—it is possible to cryptographically guarantee a link between the two hash outputs, and by *digitally signing* each step of this nested structure of hash functions, it is possible to guarantee the pairing of particular hashes with a particular identity over time.

And this guarantee is what makes it possible to define an electronic coin, which needs a secure record of ownership, in terms of a chain of digital signatures. If a record of a given electronic coin transaction (i.e., a digitally signed message detailing what payment goes to who from whom) is combined with the hash of previous transactions, and then *that* combined data is hashed, then a permanent link is established between the two: If an individual tries to go back and alter one of the previous transactions, it will alter *all subsequent hashes*, thus proving that the record has been tampered with. And since Nakamoto has defined electronic coins as a record of “signed” ownership transfers, securing that record is a key step towards solving the two digital currency problems outlined above: A secure record of who gave what to whom is a means of guaranteeing that

---

<sup>56</sup> Nakamoto, “Bitcoin,” 2.

a given amount of legitimate coins was sent to one particular person, giving that person ownership of that amount. Given Bitcoin's reliance on cryptographic hash signatures, this record of who gave what to whom cannot be altered after the fact without disrupting all subsequent transactions—and by extension, marking the entire record as illegitimate.

It is worth stepping back for a moment to note the rhetorical import of this definition of an electronic coin as a chain of hashed digital signatures. In this short definitional paragraph, Nakamoto lays out the initial components of Bitcoin's procedural rhetoric: Within Bitcoin's protocol, digital signatures (i.e., public/private key pairs) are the sole markers of identity—though within this schema, one person (i.e., a human making use of Bitcoin) may very well possess several identities (i.e., several different key pairs). These identities (in the conventional Bitcoin terminology, “addresses”), are each associated with particular amounts of tokens (i.e., bitcoins), and the ability to sign a transaction with a signature cryptographically linked to a particular address—which depends on possession of a private key linked to that address—is the sole means of “owning” those tokens. In addition, through a process discussed further in the following sections, Bitcoin's protocol records the relationship of digitally signed messages as they develop over time, and by storing signed and hashed versions of these messages, the interactions between these messages are fixed in an unalterable database—or rather, a database that cannot be altered without altering all subsequent entries.

Importantly, neither of these key elements of the Bitcoin protocol yet require the introduction of any monetary concepts. Electronic coins are defined as a chain of digital signatures, but one might just as well say, “The data structure that I am about describe consists of a chain of digital signatures.” Despite Nakamoto's equation of a chain of hashed

digital signatures to an electronic coin, it is the hashed chain of signatures that is primary here; in Brown's terms, "electronic coin" is an argument *about* Bitcoin, not an argument *with* Bitcoin (i.e., a procedure that establishes rules for identity, action, temporal relations, etc.). There is nothing in the outlined protocol thus far that necessitates the terminology of "coin."

*The double spend problem and proof of work*

Defining electronic coins as chains of hashed digital signatures does much to establish the basic components of Bitcoin's procedural rhetoric, but this definition does raise an additional problem. As Nakamoto notes, even though "a payee can verify the signatures to verify the chain of ownership" of a coin, "the payee can't verify that one of the owners did not double-spend the coin"—that is, sign a message delivering the same coin to more than one recipient.<sup>57</sup> This is essentially a problem of ordering: If the transfer of a coin's ownership is accomplished through the sending of (digitally signed) messages, then establishing the temporal sequence of messages is crucial in situations where two or more messages transfer ownership of the same coin to multiple owners. This is the problem, Nakamoto points out, that previously drove other digital currencies toward centralization: "A common solution is to introduce a trusted central authority, or mint, that checks every transaction for double spending."<sup>58</sup> But again, this solution generates a problem of its own, insofar as it produces a single point of failure for the currency as a whole. What is needed, then, is "a way for the payee to know that the previous owners [of a coin] did not sign any

---

<sup>57</sup> Ibid.

<sup>58</sup> Ibid.

earlier transactions”—that is, they did not double spend the coin—and “the only way to confirm the absence of a transaction is to be aware of all transactions.”<sup>59</sup>

And the only way to ensure that every participant in the Bitcoin protocol is aware of all transactions without relying on centralization, Nakamoto argues, is to *publicly announce* all transactions.<sup>60</sup> If every Bitcoin user broadcasts every transaction they initiate to all other users—which does not, it should be noted necessarily entail announcing any details of one’s offline identity, since “identity” in this context is simply a Bitcoin address—then all users should be capable of assessing the legitimacy of a particular coin (i.e., the chain of digital signatures). But here again it seems necessary to move to centralization: If all users are broadcasting all transactions all the time, how could users possibly agree on the broader transaction history of the Bitcoin network? It seems that there needs to be some kind of “system for participants to agree on a single history of the order in which [coins] were received.”<sup>61</sup> In other words, even if Bitcoin possesses *internal* cryptographic security—that is, every transaction hash is cryptographically linked to the transactions prior to it and ownership guaranteed by digital signatures—this does not guarantee that every participant in the Bitcoin network possesses the *same* copy of transactions. So how is it possible to ensure that all participants in the Bitcoin network are referencing the same record of transactions?

---

<sup>59</sup> Ibid.

<sup>60</sup> Here Nakamoto’s argument follows (and cites) Dai, “B-Money.”

<sup>61</sup> Nakamoto, “Bitcoin,” 2.

This puzzle is a specific instance of a more general problem in computing, known as the “Byzantine Generals Problem.” The problem takes its name from an imagined scenario in which

several generals have to agree on the strategy for a battle and, due to their physical separation, they must communicate using messages. However, the messages can be corrupt and there can be traitors among the generals. The (loyal) generals must solve the problem of how to arrive at a common strategy in the face of faulty messages and traitors.<sup>62</sup>

Applied to the case of Bitcoin, the generals are participants in the Bitcoin network and the messages sent between generals are copies of the chain of transactions, so “the problem is how the network can agree on the state of the distributed database [i.e., the chain of transactions] when both messages between the nodes can be corrupted and there might be attackers trying to subvert the distributed database.”<sup>63</sup>

In the following sections of his white paper, Nakamoto solves the Byzantine Generals Problem by relying on one additional feature of cryptographic hash functions: that such hash functions require computational power to calculate. In other words, it takes *work* to compute the hash of a Bitcoin transaction and to add that hash to a chain of previous transactions. Furthermore, the difficulty of this work can be increased by procedurally designating a desired hash “target”—for example, a hash output that begins with a particular number of zeros. Consider the previously referenced hash of the *Iliad*:

7836d2c48ac1fbca4e164d63acc04adc47ad653524b406bb7b46c0016abd0ba8<sup>64</sup>

---

<sup>62</sup> Franco, *Understanding Bitcoin*, 165.

<sup>63</sup> Ibid.

<sup>64</sup> Generated from Homer, *The Iliad of Homer*.

And consider the result if a single character is added to the poem—for instance, if the poem’s famous opening lines entreat the muse to “singe” rather than to “sing”:

929bdf99bfc9a3f1cdc368b144a5304e61337f26517c42bd21e76bda7f035604

If a goal is set to reach a hash output that has a particular beginning—for example, a zero rather than a seven or a nine—there is no alternative but to modify the input text by adding random data to the input (in this example, an additional letter to “sing”), calculate the hash, and check the result. So we can cycle through “singq,” “singw,” “sine,” etc., none of which generate a hash that begins with a zero, until finally attempting “singl,” which yields a hash matching the desired output:

034b007f205bee7d4475d8ea42f12556ca37f451419d60f979fb0b7ebb1ded94

Notably, increases in the length of the “target” (e.g., a hash that begins with 000 rather than just 0) correspond to a considerable increase in the work required to generate an appropriate hash. This means that hash calculations can be made *intentionally difficult*—that is, intentionally requiring more resources to compute. It also means that the very existence of a particular hash function represents a kind of proof not only of the hashed data, but also of a particular amount of computational work—a “proof of work.”

Nakamoto’s paper proposes using this proof of work—that is, this form of intentionally difficult computation—to limit the ability of individuals to modify the chain of Bitcoin transactions.<sup>65</sup> This is accomplished through two levels of hashing: First, there is

---

<sup>65</sup> Nakamoto, “Bitcoin,” 3.

the previously discussed chain of hashed signatures that track the transfer of ownership of bitcoins; and second, these individual hashed transactions are clustered into sequential “blocks” of data, which are in turn hashed. Each hashed block of transactions includes a hash of the previous block of transactions, creating a “chain” of blocks—hence the name “blockchain” is used for this data structure. This work involved in creating the blockchain is crucial to Bitcoin’s protocol: If the mass of Bitcoin users (or rather, their computers) constantly perform the computational work of 1) verifying the validity of transactions, 2) calculating hashes of blocks of valid transactions, and 3) adding these hashes to the blockchain, then any single modification of the chain of transactions must be weighted against the *total computational power of the Bitcoin network*.<sup>66</sup> In other words, while it is possible to retroactively change an earlier section in the chain of transactions, doing so would also require calculating the hashes for *every subsequent transaction in the chain*. As Franco explains, this means that

an attacker wishing to change the [chain of transactions] would have to apply a computational power equivalent to all of the computational power spent from that point in time to the present. Furthermore, the attacker would have to outrun the legitimate Bitcoin network, which keeps adding entries to the distributed database. In other words, it would have to catch up, computationally speaking, with the legitimate network to change the information in the database.<sup>67</sup>

---

<sup>66</sup> The work required for any given block is continually adjusted according to the Bitcoin protocol: “To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they’re generated too fast, the difficulty increases.” *Ibid.*

<sup>67</sup> Franco, *Understanding Bitcoin*, 95.

But here it is possible to raise an objection: If participants in the Bitcoin network are calculating blocks of the blockchain in a decentralized manner, there will inevitably arise competing versions of the blockchain—that is, one network participant might calculate and link blocks *X*, *Y*, and *Z* while another might chain together *X*, *Y*, and *Q*. So which blockchain is correct? This question brings us back to the white paper, in which Nakamoto proposes an elegant solution to the Byzantine Generals' problem, the problem of determining a single transaction history for the entire Bitcoin network: The Bitcoin protocol simply mandates that participants in the Bitcoin network reach consensus about the Bitcoin transaction history by treating the *longest available chain of blocks* (i.e., the version including the most blocks) as the “true” copy of this transaction history.<sup>68</sup> In other words, the “true” chain of transactions is the one that has required the greatest amount of computational work to create. Consequently, any malicious attacker would need to possess over half of the computing resources dedicated to the Bitcoin network—a scenario that is less likely as the network grows in size—and the security of the chain of transactions increases with every subsequent addition to the chain.<sup>69</sup> The problem of defining a single transaction history is simply sidestepped through radical relativism: The true transaction history is the one supported by the majority of the computational labor of the Bitcoin network.

And at this point, we have addressed nearly all of the pieces necessary to make sense of the summary of the Bitcoin network protocol that Nakamoto provides in the fifth section of his paper:

---

<sup>68</sup> Nakamoto, “Bitcoin,” 3.

<sup>69</sup> An attack on the integrity of the chain of transactions that utilizes over half of the network's computing power is consequently termed a “51% attack.” Franco, *Understanding Bitcoin*, 113.

1. New transactions are broadcast to all nodes [i.e., participants in the Bitcoin network].
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.<sup>70</sup>

But two key pieces of the Bitcoin protocol are still missing from this overview: First, how do participants in the Bitcoin network obtain the tokens (i.e., bitcoins) to transfer in the first place? And second, if the security of the blockchain depends on the work necessary to form it, and if that work has real world costs (e.g., electricity), why should participants in the Bitcoin network spend resources in contributing to the blockchain? Nakamoto solves both problems by rewarding contributors to the blockchain *within* the blockchain:

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.<sup>71</sup>

---

<sup>70</sup> Nakamoto, "Bitcoin," 3.

<sup>71</sup> Ibid., 4. Notably, "[t]he incentive can also be funded with transaction fees"; that is, those conducting Bitcoin transactions can, within a given transaction, designate a payment to the particular node processing the block in which the transaction appears.

Thus, the computational work required for Bitcoin's functioning is rewarded with bitcoins. (And though metaphor should not be confused with procedure here, it is worth noting that Nakamoto's mining analogy gives Bitcoin its terminology for this process: the computation work is known as "mining," and those who perform this work for the network are known as "miners.") Furthermore, this means that those who have the greatest ability to damage the Bitcoin network (e.g., by retroactively altering the blockchain with massive amounts of computational work), also have the greatest incentive to preserve the perceived value of the tokens they can earn through computation—that is, by not disrupting the blockchain. In short, such a potential attacker "ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth."<sup>72</sup>

### *Interpreting the protocol*

So what exactly does this protocol, this set of procedures, *do*? Notably, if we set aside Nakamoto's own characterization of the technology, there is not much *in the protocol* that is framed in terms of money per se. There are tokens (i.e., bitcoins), the system tracks ownership of these tokens in relation to cryptographic addresses, and the security of this tracking system is tied to the perceived value of these tokens (i.e., to encourage miners to expend resources on building the blockchain)—but the key pieces of this system could be conceptualized in terms of a commodity just as well as a currency. And this conceptual ambiguity actually helps to highlight the real procedural feat of Bitcoin: Whether Bitcoin

---

<sup>72</sup> Ibid.

tokens are understood as a currency or as a commodity, the protocol does in fact accomplish the secure, distributed production of a *history of ownership* of those tokens.

And crucially, this is a history that *does not take the form of a narrative*—that is to say, this is a non-representational history. The blockchain, as a system of hashed transactions, certainly condenses Bitcoin transactions into a form apparently distinct from the transactions themselves, but it is a mistake to conceptualize the relationship between transactions and blockchain, mediated through hashes, as a matter of representation. There is no ambiguity of interpretation here, none of the minimal gap between represented and representation that characterizes history conveyed in language; the slightest change to input data produces, with mathematical certainty, a corresponding alteration of the output. As a history generated and stored by the rule-based affordances of the computer—that is, through code—this is a history that is *executed*, not written.<sup>73</sup> Within the Bitcoin protocol, there is no ambiguity of ownership of bitcoins, no necessity of interpreting influence or rights; either one controls bitcoins through possession of a particular private key, or one does not. To be sure, this does not eliminate the possibility that a user might misunderstand the shared history of the blockchain—for example, by accidentally losing a private key and thereby losing ownership of what the user perceives to “still own.”<sup>74</sup> But

---

<sup>73</sup> As Alexander Galloway succinctly puts this distinction: “Code is the only language that is executable.” Galloway, *Protocol*, 165.

<sup>74</sup> Humanistic analyses of computation often introduce an unwarranted homocentrism when engaging this point, and miss the importance of distinguishing between human *interpretation* of computational processes and the *execution* of those processes. In his study of Bitcoin’s cryptography, for instance, information scientist Quinn DuPont refers repeatedly to “algorithmic representation” and to the fact that such representation presupposes elements that are discrete, disjointed, and modular. And while it is true that Bitcoin’s underlying cryptographic processes *can* be understood from the standpoint of human interpretation—in which case they *are* representational—this overlooks the more

such misinterpretations are irrelevant to the blockchain itself. Here is a history that is not told, not interpreted; it simply is.

So if the procedural rhetoric of Bitcoin produces a non-representational history, what does this history say about the participants in it? That is to say, what manner of community corresponds to this history? A strange one at that—a community that exists as a collective, since its history is shared, but a community that cannot engage itself as such. The only possible intervention in this community—that is, the only way, within the Bitcoin protocol, to modify the history that is the blockchain—is intervention at the level of the *individual* transaction. What the Bitcoin protocol produces, then, through the production of the history of the blockchain, is a strange kind of “individualist collective”—a shared history, a shared sociality, but one that nonetheless cannot be shaped through shared action.<sup>75</sup>

The production of this individualist collective has significant rhetorical implications, and understanding this procedural achievement is critical to understanding the rhetorical force of digital metallism. Without the context of the procedure—that is, without placing digital metallism in a rhetorical ecology alongside Bitcoin’s protocol—digital metallism

---

significant point that such processes can *execute*, even in the absence of human interpretation. In other words, representational aspects of cryptography and other algorithmic processes are secondary, not primary. See Quinn DuPont, “The Politics of Cryptography: Bitcoin and the Ordering Machines,” *Journal of Peer Production* 4 (2013), <http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/>.

<sup>75</sup> In this way, Bitcoin participates in a long tradition of replacing community governance with technological mechanisms (e.g., implementing copyright protections in software). See Galloway, *Protocol*; and Lawrence Lessig, *Code: Version 2.0* (New York: Basic Books, 2006). Bitcoin extends this tradition by technologically regulating the past as well as action in the present.

appears simply as a repetition of the commodity money rhetoric, albeit with the additional rhetorical wrinkle of figuring the artifice of code as a “natural” object. As I noted above, while such rhetoric might be persuasive to those already ideologically primed to accept a new form of commodity money (e.g., early, cyberlibertarian Bitcoin supporters), it is difficult to see how digital metallism alone could account for Bitcoin’s expansion beyond this already-receptive audience. But the trope of digital metallism becomes more forceful when it is paired with the technology of Bitcoin, precisely because the procedural rhetoric of Bitcoin seems to accomplish exactly the thing to which the rhetoric of digital metallism aspires: the foreclosure of the political from a particular community. And it is this interaction, this apparent complement of digital metallism and procedural rhetoric, which helps to explain why digital metallism has been such a pervasive and persuasive trope within the Bitcoin community. Digital metallism not only resonated with the ideologies of early Bitcoin supporters; it also accurately described *what the technology of Bitcoin seemed to do*—that is, produce a collective of individuals “unburdened” by the intervention of the political, a community without the communal.

Yet there is one very significant catch to this individualist collective, a catch that, as I will argue over the next two chapters, significantly shapes the rhetorical dynamics of both Bitcoin and its technological heirs. It is true that within the Bitcoin protocol, there is no room for negotiation, for alteration of the money, etc.—in short, no room for any intervention of community, no room for politics—and it is true that this sets the political dynamics of Bitcoin, as a form of money, apart from the forms of money covered thus far in this dissertation. Unlike other currencies, the economic production and use of Bitcoins are matters apparently not accessible to political intervention. But crucially, this is only true

*within the protocol*. And this protocol, the procedural glue that binds this individualist collective together is itself modifiable, malleable, and subject to community intervention. New forms of the protocol are developed, and participants in the Bitcoin community—in the extra-protocol sense—can be persuaded to adopt these new protocols, or to stick to the old. Unexpected functions of the protocol (i.e., bugs) are discovered, and the community must respond with alterations of the protocol or acceptance of the bug. It is a simple point with far reaching implications for the politics and rhetoric of Bitcoin: The procedurality of Bitcoin is itself a constructed thing, *built* in software, so even if politics is foreclosed *within* the Bitcoin protocol, this only serves to heighten the political stakes of choices made in the development of Bitcoin as a procedural object.<sup>76</sup> In other words, what Bitcoin accomplishes is a shift of the space of political from the use and production of Bitcoin as a form of money to the production of Bitcoin as a protocol. And to fully appreciate the rhetorical impact of digital metallism and Bitcoin's procedural rhetoric, it is vital to understand this dynamic: Bitcoin's banishment of politics from money is not a foreclosure, but a *displacement* of politics. As the remainder of this dissertation will demonstrate, this shift of the space of the political does much to explain both the types of discourse present in cryptocurrency communities, and the role that these communities play in processes in valuation.

---

<sup>76</sup> To put it in terms of the performative turn, the foreclosure of politics is a *frame* that produces the *overflow* of heightened political stakes in the development of Bitcoin as a technology. See Michel Callon, "An Essay on Framing and Overflowing: Economic Externalities Revisited by Sociology," *The Sociological Review* 46, no. 1 (May 1998): 244–69, <https://doi.org/10.1111/j.1467-954X.1998.tb03477.x>.

## Chapter Three

### Contesting Development: Ethics, Politics, and Expertise in the Bitcoin Community

In the previous chapter, I established a key rhetorical dynamic of Bitcoin: I argued that Bitcoin's procedural rhetoric (i.e., rhetoric *with* Bitcoin) seems to accomplish the production of an individualist collective—a *polis* without the political—and that this apparent accomplishment reinforces digital metallist rhetoric *about* Bitcoin that figures the currency as grounded in “natural” value. However, this accomplishment is only apparent, insofar as Bitcoin's procedural rhetoric actually functions not as a foreclosure of politics but as a displacement of the political into the sphere of Bitcoin's development as a protocol. As I noted in the previous chapter, this complement of procedural and commodity rhetorics goes some way towards explaining the appeal of Bitcoin among early enthusiasts, and by extension, contributes to understanding the processes of adoption and valuation in the early Bitcoin community. Yet it is important not to overstate this contribution, which is limited in significant ways—not only because valuation, while involving rhetorical processes, is not reducible to them, but also because, as a technology still in the early stages of its social construction, the long-term significance of other factors in the mainstream adoption and valuation of Bitcoin (e.g., new regulatory frameworks for digital currencies, the integration of Bitcoin into existing payment infrastructures) may not yet be apparent. In other words, while the procedural rhetoric of Bitcoin certainly plays a role in Bitcoin's establishment as an economic assemblage, this role cannot be understood as an exclusive one.

What the connection of digital metallism and Bitcoin's procedural rhetoric *can* do, however, is provide context for interpreting the rhetorical significance of other discourses (e.g., rhetoric *about* Bitcoin) within the assemblage of Bitcoin, and for understanding the role that these discourses play in the construction of Bitcoin as a monetary technology. That is to say, identifying the displacement of Bitcoin politics provides a new context in which to assess Bitcoin as a monetary *polis* in which the distribution and use of political power is subject to rhetorical influence. This is especially significant given that previous treatments of "the politics of Bitcoin," if they avoid the trap of accepting "apolitical" digital metallism at face value, generally consider the subject either from a perspective external to the currency's monetary community (e.g., by tracing Bitcoin's ideological origins in the cypherpunk movement, or by assessing the affinities between Bitcoin and right-wing monetary policy)<sup>1</sup> or from a perspective that notes but does not substantially engage the political processes of *constructing* the Bitcoin protocol (e.g., by noting that a few members of the Bitcoin community seem to exhibit outsized influence on the community, either due to amassing Bitcoins early in the currency's history or due to involvement in Bitcoin's development).<sup>2</sup> To some extent, this focus is understandable—if Bitcoin's advocates claim that the currency is apolitical, then the obvious starting point for Bitcoin scholarship is to interrogate this claim—but a nuanced account of the politics of Bitcoin needs not only to

---

<sup>1</sup> For example, Golumbia, *The Politics of Bitcoin*.

<sup>2</sup> For example, Sarah Jeong, "The Bitcoin Protocol as Law, and the Politics of a Stateless Currency," 2013; and Vasilis Kostakis and Chris Giotitsas, "The (a)Political Economy of Bitcoin," *TripleC* 12, no. 2 (2014): 431–40. The former, for example, notes that "[w]here Bitcoin goes and what it becomes largely depends on what kind of political inclinations win out in the community," which is certainly the case, but this leaves aside the question of *how* differing political inclinations are articulated and contested.

point out that Bitcoin is, in fact, political; it also needs to explore the workings of this politics. And this is precisely the kind of exploration that approaching Bitcoin's politics from a rhetorical perspective enables: Identifying the displacement of politics at work in Bitcoin's procedural rhetoric makes other elements of Bitcoin discourse—even the seemingly strange and inconsequential—legible as *political* responses to this displacement. In other words, this perspective enables the recognition of additional, rhetorically significant discourses within the assemblage of Bitcoin—that is, dimensions of Bitcoin rhetoric that have been significant thus far for Bitcoin's social construction as a form of money, and will likely warrant further attention in the future as Bitcoin and related digital currencies evolve.

This chapter, and the one that follows, will trace the rhetorical implications of Bitcoin's political displacement as a means of uncovering these additional rhetorical dynamics, and of identifying dimensions of the assemblage of Bitcoin that will likely remain rhetorically significant in the currency's future. To this end, the present chapter focuses on the developmental processes instituted by the Bitcoin community to manage alterations of the Bitcoin protocol, and shows how the limitations of these processes prompt the creation of new rhetorics meant to intervene in the politics of Bitcoin. More specifically, I examine the Bitcoin community's use of Satoshi Nakamoto, the mysterious creator of Bitcoin, and I show how the strangely pseudo-religious valorization (and in some instances, the explicit deification) of Nakamoto is leveraged by some members of the Bitcoin community to contest rhetorics of expertise at work in the development of Bitcoin's protocol—and by extension, to intervene in the broader organization of Bitcoin's monetary *polis*.

To advance this argument, I proceed in three steps. I begin by reviewing the case of Australian computer scientist Craig Steven Wright, one of the few suspected candidates for Nakamoto's real identity who actually claimed to be Nakamoto rather than denying any connection to the Bitcoin creator. This case leads me to consider the curious tension between the Bitcoin community's fascination, even obsession, with Nakamoto's identity, and its emphasis on "natural" and "trustless" cryptography as the ultimate foundation of Bitcoin. In short, the puzzle is this: If Bitcoin is, for its community members, so much a matter of mathematics and technology rather than people and personalities—as the rhetoric of digital metallism suggests—how should the community's focus on Nakamoto be understood? Answering this question brings me to the next step, in which I analyze the ethics and politics of Bitcoin development. Here I argue that, because Bitcoin politics are displaced onto development, the ethical privileging of rhetorics of expertise in Bitcoin's development process becomes a political problem for the Bitcoin community as a whole—that is, in the domain of development, technical expertise bears an oversized role in the politics of Bitcoin. Next, I examine the limitations of this political configuration by analyzing the debate over a technical matter with significant implications for the Bitcoin community: the size of the blocks in the Bitcoin blockchain. Specifically, I show how participants in this debate contested rhetorics of expertise through appeals to Nakamoto's "original vision" for Bitcoin. This use of Nakamoto as an alternative to rhetorics of expertise, I argue, helps to explain both the extreme forms of valorization of Nakamoto in the Bitcoin community *and* the potential disruption of Bitcoin's politics that a true "return" of Satoshi Nakamoto would initiate. In turn, the case of Nakamoto points to a broader rhetorical dynamic in digital currencies modeled on Bitcoin's apparent foreclosure of the political: Shifting the politics of

a currency into the technical sphere of protocol development prompts the creation of decidedly non-technical rhetorics meant to challenge the legitimacy of the currency's developers and developmental processes, and suggests that the question of *who may participate* in the development of the protocol will remain a crucial rhetorical arena for digital currencies in the years to come.

### *The Satoshi affair*

On December 8<sup>th</sup>, 2015, the technology magazine *Wired* published an article claiming to have uncovered the true identity of Satoshi Nakamoto, the pseudonymous creator of Bitcoin.<sup>3</sup> The probable person behind the Nakamoto pseudonym, reporters Andy Greenberg and Gwern Branwen claimed, was an Australian computer scientist and businessman, little known even within the cryptocurrency community, who described himself as a “former academic who does research that no one ever hears about”: Craig Steven Wright.<sup>4</sup> “In the last weeks, *WIRED* has obtained the strongest evidence yet of Satoshi Nakamoto’s true identity,” Greenberg and Branwen wrote.<sup>5</sup> This evidence pointed to “a man who never even made it onto any Nakamoto hunters’ public list of candidates, yet fits the cryptocurrency creator’s profile in nearly every detail.”<sup>6</sup> Later that same day,

---

<sup>3</sup> Andy Greenberg and Gwern Branwen, “Bitcoin’s Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius,” *Wired*, December 8, 2015, <https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/>.

<sup>4</sup> Quoted in *ibid.*

<sup>5</sup> *Ibid.*

<sup>6</sup> *Ibid.*

technology website *Gizmodo* published a similar but separately sourced story, claiming that Wright and his deceased friend, Dave Kleiman, shared the Nakamoto pseudonym.<sup>7</sup> Yet both stories came with significant caveats, and their sources admittedly pointed just as much to a potential hoax as they did a dramatic revelation of Nakamoto's secret identity. "[D]espite a massive trove of evidence, we still can't say with absolute certainty that the mystery is solved," Greenberg and Branwen wrote. "But two possibilities outweigh all others: Either Wright invented bitcoin, or he's a brilliant hoaxer who very badly wants us to believe he did."<sup>8</sup>

As the stories broke, Wright was fleeing Australia to avoid tax authorities—and the press.<sup>9</sup> During his escape, he closed email accounts and deleted his social media presence, partly in an attempt to erase what he later characterized as his online "rants," and partly to cut himself off from journalistic contact.<sup>10</sup> In the absence of a detailed response to the stories from Wright, the attention generated by the *Wired* and *Gizmodo* stories quickly turned even more skeptical. Follow-up reporting pointed to inconsistencies in the cryptographic evidence linking Wright to Nakamoto, as well as in Wright's self-presented personal history.<sup>11</sup> (Wright's LinkedIn profile, for instance, listed two PhDs from Charles

---

<sup>7</sup> Sam Biddle and Andy Cush, "This Australian Says He and His Dead Friend Invented Bitcoin," *Gizmodo*, December 8, 2015, <https://gizmodo.com/this-australian-says-he-and-his-dead-friend-invented-bi-1746958692>.

<sup>8</sup> Greenberg and Branwen, "Bitcoin's Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius."

<sup>9</sup> O'Hagan, "The Satoshi Affair."

<sup>10</sup> *Ibid.*

<sup>11</sup> Andy Greenberg, "New Clues Suggest Craig Wright, Suspected Bitcoin Creator, May Be a Hoaxer," *WIRED*, December 11, 2015, <https://www.wired.com/2015/12/new-clues->

Stuart University, but when contacted by journalists, the university denied having ever awarded Wright those degrees.)<sup>12</sup> In the course of only a few days, the dominant media characterization of Wright shifted decisively from “reclusive genius” to “elaborate hoaxer.”

There were good reasons to be skeptical. First, debate over Nakamoto’s identity had been a favorite parlor game in the Bitcoin community for nearly the entirety of the community’s existence, and by 2015, the lack of biographical details in Nakamoto’s communications (aside from his name and his claims to be male, living in Japan, and in his thirties) had already prompted elaborate analyses of Nakamoto’s emails and message board posts. The hope was that these texts, which largely focus on Bitcoin and its technical development, might offer an indirect clue to Nakamoto’s identity: Some commentators, for example, interpreted Nakamoto’s flawless English and his occasional use of British spellings and expressions as evidence that he lived or studied in the Commonwealth, while others tracked the timestamp patterns of Nakamoto’s posts to try to determine the time zone in which he was likely to live (i.e., by deducing his sleep patterns through periods of message board inactivity).<sup>13</sup> But though these analytical efforts pointed to a number of

---

suggest-satoshi-suspect-craig-wright-may-be-a-hoaxer/; Sarah Jeong, “Satoshi’s PGP Keys Are Probably Backdated and Point to a Hoax,” Motherboard, December 9, 2015, [https://motherboard.vice.com/en\\_us/article/jpgq3y/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax](https://motherboard.vice.com/en_us/article/jpgq3y/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax); and Thomas Fox-Brewster, “Time to Call a Hoax? Inconsistencies on ‘probable’ Bitcoin Creator’s PhD and Supercomputers Revealed,” Forbes, December 11, 2015, <https://www.forbes.com/sites/thomasbrewster/2015/12/11/bitcoin-creator-satoshi-craig-wright-lies-hoax/#5739ede06794>.

<sup>12</sup> Fox-Brewster, “Time to Call a Hoax?”

<sup>13</sup> See Nathaniel Popper, *Digital Gold: Bitcoin and the inside Story of the Misfits and Millionaires Trying to Reinvent Money* (New York: HarperCollins, 2015); and Andy Greenberg, “Nakamoto’s Neighbor: My Hunt for Bitcoin’s Creator Led to a Paralyzed Crypto Genius,” Forbes, March 25, 2014,

possible candidates, including cryptographers Nick Szabo and Hal Finney, all denied being Nakamoto, and no case was ever conclusively proven. Furthermore, in 2015, the memory of the previous “unmasking” of Nakamoto by a media outlet was still fresh in the minds of the Bitcoin community: The previous year, *Newsweek* claimed that Dorian Nakamoto, an engineer living in California, was the true identity of Satoshi.<sup>14</sup> Dorian Nakamoto initially seemed to confirm this report, but the story unraveled as Dorian later denied being Satoshi, and said he had misunderstood the questions asked by the *Newsweek* reporter. In short, when the Wright stories broke, there was already a long list of potential Nakamotos, and an equally long list of denials.

But Wright’s case differed from these others in one significant way: He did, in fact, *intend* to claim to be Nakamoto—though not, apparently, in the venues that the stories first appeared. In the months before the *Wired* and *Gizmodo* stories broke, Wright sold his life story rights to Canadian money transfer firm nTrust as part of a broader deal that transferred ownership of some of Wright’s intellectual properties to the firm, and both parties planned to unveil Wright’s identity as Nakamoto to promote their deal and associated research ventures.<sup>15</sup> As part of a carefully orchestrated revelation, writer Andrew O’Hagan, who had previously drawn the attention of technology circles for his coverage of Wikileaks founder Julian Assange, was invited to shadow Wright and to publish an account of the Australian’s story—and eventually O’Hagan did, in the form of a 35,000

---

<https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/>.

<sup>14</sup> Leah McGrath Goodman, “The Face behind Bitcoin,” *Newsweek*, March 6, 2014, <http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html>.

<sup>15</sup> O’Hagan, “The Satoshi Affair.”

word essay in the *London Review of Books*.<sup>16</sup> However, the unexpected publication of the *Wired* and *Gizmodo* stories threw a substantial wrench into this plan by prematurely revealing the Wright-Nakamoto connection.

For the next several months, the Bitcoin community debated Wright's links to the Nakamoto pseudonym. Then, on May 2<sup>nd</sup>, 2016, four documents were posted online: First, a blog post from Wright, in which he publicly claimed to be Nakamoto;<sup>17</sup> second, a blog post from Gavin Andresen, Bitcoin developer and widely respected member of the Bitcoin community, which related Andresen's experience as an in-person witness of Wright's possession of cryptographic keys known to have belonged to Nakamoto;<sup>18</sup> and third and fourth, articles from the *BBC* and *The Economist*, each documenting a similar demonstration, in which Wright used Nakamoto's keys to digitally sign a message.<sup>19</sup> All four posts immediately faced heavy criticism, with notable figures in the Bitcoin community arguing that Wright's cryptographic demonstrations were not what they seemed, that Andresen and other witnesses had been duped by Wright, and that Wright should settle the matter once and for all by publicly using Nakamoto's keys (e.g., by moving bitcoins that were known to have been mined by Nakamoto early in the blockchain's history, before any

---

<sup>16</sup> Ibid.

<sup>17</sup> Original deleted. Archived at Craig Wright, "Jean-Paul Sartre, Signing and Significance," Dr. Craig Wright Blog, May 2, 2016, <http://archive.is/m5euI>.

<sup>18</sup> Gavin Andresen, "Satoshi," Gavin Andresen, May 2, 2016, <http://gavinandresen.ninja/satoshi>.

<sup>19</sup> "Australian Craig Wright Claims to Be Bitcoin Creator," BBC News, May 2, 2016, <http://www.bbc.com/news/technology-36168863>; and "Craig Steven Wright Claims to Be Satoshi Nakamoto. Is He?," *The Economist*, May 2, 2016, <https://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin>.

other users possessed bitcoins).<sup>20</sup> In a subsequent blog post, Wright promised to do so.<sup>21</sup> The following day, he deleted all of his posts, replacing them with a message stating that he “[did] not have the courage” to follow through on his promise, and apologizing to those, such as Andresen, whose credibility his actions had undermined.<sup>22</sup> Since then, Wright has actively participated in the cryptocurrency community, but he has not substantiated his claim to be the “real” Satoshi Nakamoto.

### *The rhetorical significance of Nakamoto*

The “Satoshi affair,” as O’Hagan’s account titled it, is a compelling tale in its own right, and Wright remains an enigmatic figure. But from a rhetorical perspective, the most intriguing element of this episode is not Wright, his somewhat shadowy connections, or the flurry of media coverage that both inspired; instead, the most notable feature of the affair is the response of the Bitcoin community. To be sure, many members of the community followed and commented upon the story with hopes that Nakamoto might be at last revealed, but others expressed a surprisingly different, even oppositional, view. For example, in response to the May 2<sup>nd</sup> stories about Wright’s purported use of Nakamoto’s keys, Bitcoin advocate Andreas Antonopoulos—a figure of significant standing in the

---

<sup>20</sup> For example, Dan Kaminsky, “Validating Satoshi (Or Not),” *Dan Kaminsky’s Blog* (blog), May 2, 2016, <https://dankaminsky.com/2016/05/02/validating-satoshi-or-not/>.

<sup>21</sup> Original deleted. Archived at Craig Wright, “Extraordinary Claims Require Extraordinary Proof,” Dr. Craig Wright Blog, May 4, 2016, <https://web.archive.org/web/20160504045648/http://www.drcraigwright.net/extraordinary-claims-require-extraordinary-proof/>.

<sup>22</sup> Original deleted. Archived at Craig Wright, “I’m Sorry,” Dr. Craig Wright Blog, May 7, 2016, <https://web.archive.org/web/20160507165900/http://www.drcraigwright.net/>.

Bitcoin community, well known for his books and lectures on Bitcoin and related technologies<sup>23</sup>—posted a message on the discussion forum Reddit, in which Antonopoulos claimed to have been offered—and declined—the opportunity to verify the identity of Nakamoto:

About two weeks ago I was contacted and asked to offer security advice for a project. I was asked to sign an NDA in order to discuss the project itself, something I am reluctant to do, in general. Once I received the NDA however, it became obvious that the project was related to verifying the identity of Satoshi Nakamoto. I immediately declined the offer, declined to participate and declined to sign the NDA.<sup>24</sup>

Notably, Antonopoulos goes on to justify his decision, not in terms of an objection to the NDA per se, but rather in terms of an objection to the social *trust* that such an arrangement would entail:

I'm sure many people will think I was wrong to decline the “opportunity” to verify [Nakamoto]’s identity. From my perspective, the request for me to verify his/her/their identity is in itself an appeal to authority. It is replacing public cryptographic proof with endorsement by a third party. If [Nakamoto] wants to “prove” their identity, they don't need an “authority” to do so. They can do it in a public, open manner. To ask people in the space who have a reputation to stake that reputation and vouch for [Nakamoto]'s identity raises many red flags in my mind.<sup>25</sup>

---

<sup>23</sup> For example, Antonopoulos, *Mastering Bitcoin*; and Andreas M Antonopoulos, *The Internet of Money: A Collection of Talks* (Merkle Bloom, 2016).

<sup>24</sup> andreasma, “Why I Declined to ‘Verify’ SN’s Identity Two Weeks Ago,” *Reddit*, May 2, 2016, [https://www.reddit.com/r/Bitcoin/comments/4hj1xu/why\\_i\\_declined\\_to\\_verify\\_sns\\_identity\\_two\\_weeks/](https://www.reddit.com/r/Bitcoin/comments/4hj1xu/why_i_declined_to_verify_sns_identity_two_weeks/).

<sup>25</sup> *Ibid.*

Here Antonopoulos sets up an opposition between trust and proof—an opposition that repeats digital metallism’s key rhetorical move of rejecting the social in favor of the “natural.” For Antonopoulos, appeals to authority are suspect precisely because they belong to the domains of the social and the political; they are explicitly rhetorical, a matter of persuasion, of interpretation—and consequently, of uncertainty. Cryptography, by contrast, is a “natural” and “trustless” object here, just as gold is figured as a source of “natural” and “trustless” (i.e., requiring no social validation) form of money in commodity money rhetorics. For Antonopoulos, the mathematical proof of cryptography, situated beyond the constraints of the *polis*, is the only appropriate ground on which the question of Nakamoto’s identity may be resolved—and crucially, in the following paragraph Antonopoulos takes this opposition between trust and proof to its logical conclusion. If the foundation of Bitcoin is the “nature” of cryptography, rather than (social) trust in some authority, then the question of Nakamoto’s identity itself becomes irrelevant: “I don’t know if Craig Wright is [Nakamoto],” Antonopoulos writes. “I don’t care and I don’t want to know.”<sup>26</sup>

Yet even as Antonopoulos declares his adherence to the supposedly firm foundation of cryptography, this declaration betrays an unresolved contradiction: If Antonopoulos does not *care* about Nakamoto’s identity—if the whole question is irrelevant to the “natural” domain of Bitcoin—why does he desire *not to know* Nakamoto’s true identity? It seems that Antonopoulos is trying to have his cryptographic cake and eat it, too: Nakamoto’s identity is both irrelevant to the cryptographic world of Bitcoin *and* the

---

<sup>26</sup> Ibid.

debates over Nakamoto's identity should be kept separate from this world. This contradiction is developed further in the next paragraph of Antonopoulos's message:

As I have expressed many times in the past, I think the identity of Satoshi Nakamoto does not matter. More importantly I think it serves to distract from the fact that bitcoin is not controlled by anyone and is not a system of Appeal-to-Authority. Identifying the creator only serves to feed the appeal-to-authority crowd, as if [Nakamoto] is some kind of infallible prophet, or has any say over bitcoin's future.<sup>27</sup>

Again, Antonopoulos attempts to assert two points at once: Nakamoto's identity "does not matter," and yet it *does* matter insofar as it serves to "distract" the Bitcoin community. As he states later in his message, Bitcoin "works because it doesn't depend on any authority"<sup>28</sup>—and yet somehow the potential existence of an authority, such as Nakamoto, threatens the workings of this system to such a degree that Antonopoulos feels it must be actively (and very publicly) rejected rather than simply ignored.

Admittedly, Antonopoulos's statement is one among many responses to the "Satoshi affair," and even when taking into account Antonopoulos's stature in the Bitcoin community—and the fact that Wright's short-lived promise of "proof" was framed directly in response to Antonopoulos's post<sup>29</sup>—it would be unfair to place too much weight on a single Reddit post composed in the midst of controversy. Nevertheless, Antonopoulos's statement offers a useful window into a much more extensive tension in how the Bitcoin community relates to the person and persona of Satoshi Nakamoto. On one hand, the digital metallism and Bitcoin's procedural rhetoric establish the monetary technology as natural,

---

<sup>27</sup> Ibid.

<sup>28</sup> Ibid.

<sup>29</sup> Wright, "Extraordinary Claims Require Extraordinary Proof."

as divorced from the influence of the social and the political, both in terms of its monetary value and in terms of how the technology operates. On the other hand, it is indisputable that Satoshi Nakamoto continually draws the attention and energies of the Bitcoin community. So how should these two be reconciled? If Bitcoin is understood as a “neutral framework,” to use Antonopoulos’s term, why is Nakamoto so important? How should the rhetorical tension between the protocol of Bitcoin and the person of Nakamoto be understood?

Perhaps the most obvious reading of this tension is one that focuses on Nakamoto’s role in the founding mythology of Bitcoin. As Bitcoin developer Gavin Andresen notes in an interview for O’Hagan’s coverage of the Wright story, “having a mysterious founder is a great creation myth. People love a creation myth.”<sup>30</sup> The *mystery* of Nakamoto’s identity is compelling in its own right, and it is not a far stretch to interpret the parlor game speculation over the “real” Nakamoto—including speculation spurred by dramatic episodes, such as the *Newsweek* story on Dorian Nakamoto, or the Craig Wright case—as a kind of communal ritual. From this perspective, the rhetorical role of Satoshi Nakamoto is to bind the Bitcoin community together, to serve as a cultural reference point, albeit one that *supplements* the more foundational, “natural” bonds of the blockchain. In this reading, Antonopoulos’s apparently contradictory emphasis on both Nakamoto’s irrelevance and his potential to distract the community should be understood as a matter of prioritization: The technology is foundational, and Nakamoto is a distraction insofar as he replaces this foundation. The proper role for Nakamoto, then, is as a mythic supplement to the community, a quaint figure from days gone by, but *not* as a factor that intervenes in the

---

<sup>30</sup> O’Hagan, “The Satoshi Affair.”

technology of the present moment or in the technology's future. As Antonopoulos writes, it is a mistake to think of Nakamoto as having "any say over bitcoin's future."<sup>31</sup>

This reading is convincing to an extent, but there are elements of the Bitcoin community's treatment of Nakamoto that are difficult to integrate into it. First, if Nakamoto's rhetorical function is understood as one of community binding, as a supplement to the technology of Bitcoin, statements like Antonopoulos's expressed desire *not* to learn Nakamoto's identity seem out of place. Why not embrace the apparently widely shared desire to solve the mystery of Nakamoto's identity *and* remind the community of the irrelevance of this identity to Bitcoin, rather than simply denying the allure of the mystery? Second, this interpretation has difficulty accounting for treatments of Nakamoto in the Bitcoin community that do the *exact opposite* of what Antonopoulos recommends—that is, valorizing, even venerating, Nakamoto as the foundation of all that is Bitcoin, and treating him as "some kind of infallible prophet."<sup>32</sup> The most extreme form of this veneration is the figurative *deification* of Nakamoto as a "cryptocurrency god"<sup>33</sup>—a joking characterization that, in accordance with Poe's Law,<sup>34</sup> has actually spawned a 503(c)3

---

<sup>31</sup> andreasma, "Why I Declined to 'Verify' SN's Identity Two Weeks Ago."

<sup>32</sup> Ibid.

<sup>33</sup> For example, chsados, "The One True God: Satoshi Nakamoto," Bitcointalk.org, October 22, 2013, <https://bitcointalk.org/index.php?topic=315953.0>; and Alissa, "Satoshi Nakamoto - The God of Crypto," CryptoCurrency Times, November 2, 2017, <http://cryptotimes.org/cryptocurrency/satoshi-nakamoto-god-crypto/>.

<sup>34</sup> Poe's law is an "internet axiom" premised on the difficulty of distinguishing between ironic and earnest endorsements of extremism online—in this case, the difficulty of distinguishing ironically religious treatments of Satoshi and genuine reverence. See Ryan M. Milner, "Hacking the Social: Internet Memes, Identity Antagonism, and the Logic of Lulz," *The Fibreculture Journal*, no. 22 (2013): 62–92.

registered “Church of Bitcoin,” which holds Nakamoto’s original white paper to be its holy text.<sup>35</sup> But even less extreme forms of veneration still figure Nakamoto as a crucial element of Bitcoin’s foundation, not simply as a historical or mythological figure, but as someone worth consulting for the concerns of the present. For example, in the introduction of *The Book of Satoshi*, a print edition of Nakamoto’s collected emails, message board posts, and other writings, editor Phil Champagne explains that he has collected Nakamoto’s writings so that readers can learn “about the thought processes of [Bitcoin’s] creator.”<sup>36</sup> Even though Champagne acknowledges that “[Nakamoto’s] identity is irrelevant to the well-being of Bitcoin,” he still sees value for the *present moment* in “gaining an understanding of the mindset of the mysterious person (or group of persons) behind this marvelous new technology.”<sup>37</sup> While certainly not as extreme a treatment of Nakamoto as the Church of Satoshi, this is still a far cry from actively desiring ignorance about him. In any case, it seems that treatments of Nakamoto within the Bitcoin community are far from monolithic, and are even to some degree contradictory—which suggests that it is misguided to understand Nakamoto’s rhetorical function solely in terms of some kind of mythological facilitator of community solidarity. If anything, the range of responses to and uses of Nakamoto suggest that he serves less as a tool for binding the community together and more as a point of contestation.

---

<sup>35</sup> “Church of Bitcoin,” August 7, 2017, <https://www.churchofbitcoin.org/>.

<sup>36</sup> Satoshi Nakamoto, *The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*, ed. Phil Champagne (e53 Publishing, 2014), xv; a similar archive is maintained at the “Satoshi Nakamoto Institute,” accessed April 17, 2018, <http://satoshi.nakamotoinstitute.org/>.

<sup>37</sup> Nakamoto, *The Book of Satoshi*, 3.

So what then is the rhetorical significance of Satoshi Nakamoto in the Bitcoin community? In the remainder of this chapter, I pursue this question by placing the Bitcoin community's contradictory treatment of Nakamoto in relation to the shift of Bitcoin politics to the development of Bitcoin's protocol that I introduced in the previous chapter. In doing so, I show how the community's treatment of Nakamoto should be understood not simply as engagement with a common cultural referent, but also as an intervention into the politics of Bitcoin development prompted by the limitations of the structures managing the development process. To this end, I first review the site to which Bitcoin politics are displaced by digital metallism and Bitcoin's procedural rhetoric—the processes of Bitcoin's development—and show how the politics of development are constrained by a reliance on rhetorics of expertise. Next, I examine a case—the debate over the size of blocks in the Bitcoin blockchain—in which such rhetorics were not sufficient to build consensus in the Bitcoin community, and I show how the person of Nakamoto was used as a rhetorical tool in response to the political limitations of Bitcoin's processes of development.

### *The ethics and politics of protocol development*

In her study of the software development community supporting Debian, a FOSS (free and open-source software) operating system, anthropologist Gabriella Coleman identifies two key forms of “everyday micropractices” that serve to structure participation and decorum in FOSS development communities: enculturation and punctuated crisis.<sup>38</sup> The former refers to “a process of relatively conflict-free socialization,” which includes “learning the tacit and explicit knowledge (including technical, moral, or procedural

---

<sup>38</sup> Coleman, *Coding Freedom*, 124.

knowledge) needed to effectively interact with other project members as well as acquiring trust, learning appropriate social behavior, and establishing best practices.”<sup>39</sup> By contrast, punctuated crises are episodes of conflict within a development community, affectively intense and often spread across multiple platforms of communication, which provoke “instances of assessment, in which people turn their attentive, ethical beings toward an unfolding situation and engage in difficult questions.”<sup>40</sup> Such crises “can be evaluated as moments of ethical production in terms of not only their functional outcomes but also their ability to move people to reflexively articulate their ideals.”<sup>41</sup> In other words, practices of enculturation involve integrating new members into a development community’s established ethics—teaching members how they should behave, communicate, and relate to one another—whereas moments of crisis trigger reflection upon and possible modification of those ethical expectations.

Coleman’s study is explicit in its ethical orientation. She is concerned with understanding how development communities form, how participants negotiate patterns of behavior and communication to facilitate the distributed labor of FOSS software development, and how the norms and expectations of these communities are assessed and modified by participants over time. But enculturation and crises are not merely ethical matters; insofar as the socialization and periodic reorganization of development communities engages questions of *who decides* whether a particular change to the developed software is implemented or not, the stakes of FOSS development are political,

---

<sup>39</sup> Ibid., 124–25.

<sup>40</sup> Ibid., 125.

<sup>41</sup> Ibid.

too. As Nicolas Ducheneaut writes in his study of the community developing the programming language Python, “open source software (OSS) development is politics by other means.”<sup>42</sup> Because socialization in FOSS development communities is not only about how participants should behave, but also about how those behaviors serve as prerequisites for exerting influence within the community, any attempt to understand the political dynamics of a FOSS development community necessarily entails engagement with the community’s integration of new participants into a particular ethical framework. And insofar as the politics of Bitcoin as a whole are shifted to the development of Bitcoin—the argument of the previous chapter—Coleman’s concepts of enculturation and punctuated crisis are helpful for explicating the political dynamics of Bitcoin as a whole. Examining how the Bitcoin development community manages standards of appropriate behavior *within* that community is a means of accessing the political dynamics of Bitcoin development more generally.

So how exactly does the Bitcoin development community exhibit these everyday micropractices? Though Bitcoin began as Nakamoto’s personal project, soon after his initial email announcement Nakamoto began collaborating with others (e.g., Hal Finney) in the development of the Bitcoin protocol and its reference implementation, and since Nakamoto’s disappearance from the Bitcoin community in 2010, development of Bitcoin has been managed in a manner explicitly modeled on other large FOSS projects. Most notably, the Bitcoin development community has instituted the Bitcoin Improvement Proposal (BIP) system, a Request for Comments-type protocol modeled on (and in some

---

<sup>42</sup> Nicolas Ducheneaut, “Socialization in an Open Source Software Community: A Socio-Technical Analysis,” *Computer Supported Cooperative Work* 14, no. 4 (August 2005): 353, <https://doi.org/10.1007/s10606-005-9000-1>.

cases, directly copied from) the Python Enhancement Proposal (PEP) system that underlies the development of the Python programming language.<sup>43</sup> As the BIP guidelines explain, a BIP “is a design document providing information to the Bitcoin community, or describing a new feature for Bitcoin or its processes or environment.”<sup>44</sup> These proposals are meant “to be the primary mechanisms for proposing new features, for collecting community input on an issue, and for documenting the design decisions that have gone into Bitcoin.”<sup>45</sup> In other words, the BIP system *both* documents how the Bitcoin community should engage itself to propose, debate, and build consensus on changes to the Bitcoin protocol, *and* it is the means of executing these changes.<sup>46</sup> Thus, the BIP system is a site of enculturation, a resource for new members of the development community to learn the ropes of Bitcoin’s development decorum, but also the mechanism through which modifications to the protocol are communicated to the broader Bitcoin community.

This system follows a particular workflow—that is, a process by which a potential change to Bitcoin is developed into a BIP. As the BIP guidelines explain, “the BIP process

---

<sup>43</sup> Amir Taaki, “BIP 1: BIP Purpose and Guidelines,” GitHub, August 19, 2011, <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki>; for an overview of the the PEP system as a political structure, see Ducheneaut, “Socialization in an Open Source Software Community.”

<sup>44</sup> The BIP guidelines are codified in the first two BIPs, BIP 1 and BIP 2. See Taaki, “BIP 1”; the first BIP was revised and superseded by Luke Dashjr, “BIP 2: BIP Process, Revised,” GitHub, February 3, 2016, <https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki>.

<sup>45</sup> Dashjr, “BIP 2.”

<sup>46</sup> It should be noted that these changes are changes to the Bitcoin protocol, not to implementations of the protocol in particular software. The relationship between the BIP process and software implementations is analogous to the relationship, addressed in the previous chapter, of Satoshi’s white paper and its software implementations.

begins with a new idea for Bitcoin,” and this idea must be developed by a specific person: “Each potential BIP must have a *champion*—someone who writes the BIP using the style and format described below, shepherds the discussions in the appropriate forums, and attempts to build community consensus around the idea.”<sup>47</sup> The champion’s first step in advancing his or her idea is “to ascertain whether the idea is BIP-able”—that is, to review past BIPS to determine if the new proposal has been proposed before, to consider whether the new proposal is of an appropriate scale for the BIP process,<sup>48</sup> and to consult the Bitcoin development mailing list to solicit feedback from other developers about the idea.<sup>49</sup> Next, the champion creates a draft BIP document, and presents this document to other developers via the mailing list. Drafts must be composed in a very specific style and format: They are required to contain a particular header, a brief abstract, copyright information, technical specifications, sections discussing the motivation and rationale for the BIP, and a section addressing the BIP’s backwards compatibility.<sup>50</sup> Once the BIP champion has presented a draft of the BIP to the developer mailing list and has responded to and documented the ensuing discussion, the champion submits the draft to an online repository managed by the BIP editor. The BIP editor, who oversees the BIP submission process,

---

<sup>47</sup> Dashjr, “BIP 2.” Italics added.

<sup>48</sup> As the guidelines explain, “Small enhancements or patches to a particular piece of software often don’t require standardisation between multiple projects; these don’t need a BIP and should be injected into the relevant project-specific development workflow with a patch submission to the applicable issue tracker.” Ibid.

<sup>49</sup> Ibid.

<sup>50</sup> Ibid.

assigns a draft BIP a number (e.g., BIP 123)<sup>51</sup> and a label that describes the BIP's status within the BIP system workflow. Notably, the editor has some latitude to reject BIPs, though not "unreasonably" so: BIPs may be rejected due to "duplication of effort, disregard for formatting rules, being too unfocused or too broad, being technically unsound, not providing proper motivation or addressing backwards compatibility, or not in keeping with the Bitcoin philosophy."<sup>52</sup> Furthermore, acceptance of a draft BIP by the editor does not guarantee the proposal's implementation in the "real world" of Bitcoin's functioning protocol; this is determined by the extent to which users operating Bitcoin software adopt new software versions that actually implement the proposed changes to the protocol.<sup>53</sup> Consequently, part of the BIP editor's responsibility is to monitor the implementation of a BIP (e.g., by assessing the percentage of the Bitcoin network that has adopted a particular BIP), and document a BIP's implementation status when certain criteria are met.

Because this community self-engagement is formalized into a particular protocol for communication (i.e., managing how proposals are presented, commented upon, etc.), the guidelines for the BIP system are a key site for enculturation in the Bitcoin development community: The first two BIPs are explicitly a guide for how participants should engage the community of developers and how they should demonstrate their eligibility to do so (i.e.,

---

<sup>51</sup> BIP numbers are not strictly sequential. For example, BIP 11 was created on October 18, 2011, whereas BIP 2 was created on February 3, 2016. See Gavin Andresen, "BIP 11: M-of-N Standard Transactions," GitHub, October 18, 2011, <https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki>; and Dashjr, "BIP 2."

<sup>52</sup> Dashjr, "BIP 2."

<sup>53</sup> In other words, a BIP serves as a prerequisite to coordinated implementation, in software, of a particular change to the Bitcoin protocol. A BIP acceptance is a necessary condition, but not sufficient one, for coordinated software development across the Bitcoin network.

by appropriately navigating the BIP process). And significantly, this enculturation is formed quite literally from a set of rhetorical guidelines—that is, instructions for *how to present an argument* for a particular change to the Bitcoin protocol. At stake here is a whole range of rhetorical considerations: The BIP process outlines the process of invention (e.g., consulting prior BIPs), dictates a particular style and arrangement (e.g., the header, abstract, copyright information), requires certain practices of memory (e.g., documenting comments on the BIP), specifies a sequence of delivery (e.g., iterative submissions to the development mailing list), and even indicates the appropriate persona a champion should present to the community (e.g., someone who is concerned with soliciting and documenting the feedback of others). Indeed, the very fact that BIPs are “championed” by specific individuals—even if a BIP is ultimately the product of collective labor—points to the importance of a champion’s persona in the BIP process.

Importantly, as a site of enculturation, the BIP process privileges particular rhetorical expressions, and some forms of communication are more appropriate and more readily integrated into the BIP process than others. This is most evident in the BIP guidelines’ explanation of BIP rejections: BIPs may be rejected not only due to stylistic or formatting issues (“disregard for formatting rules”), but also for “being technically unsound”—as judged by the BIP editor, who must ensure that BIPs “make technical sense, even if they don’t seem likely to be accepted [by the broader Bitcoin community].”<sup>54</sup> In other words, the BIP guidelines place great weight on the ability to formulate arguments for a particular change to the Bitcoin protocol in terms of what Coleman calls “technical rhetoric”: When proposing changes to the protocol, BIP champions must articulate their

---

<sup>54</sup> Dashjr, “BIP 2.”

proposals within the technical idioms of computer science and cryptography.<sup>55</sup> Crucially, the requirement here is not merely that BIP champions *possess* some specialized technical knowledge, but that they *demonstrate* this knowledge in the course of developing a BIP. This requirement can be seen most clearly in the guidelines for the BIP comment process: The guidelines state that “participants should freely refrain from commenting outside of their area of knowledge or expertise,” but this statement is immediately followed by the caveat that comments outside of one’s area of expertise are not actually censored (e.g., by the BIP editor).<sup>56</sup> Consequently, the pressure on commenting participants is enforced entirely through persuasive means: Both the BIP author and commenters participating in the BIP feedback process must demonstrate, through their discursive interventions, their own eligibility to claim a particular area of knowledge. In other words, the judgment of a BIP’s technical validity is intimately connected not only to the content of a given BIP, but also to the BIP champion’s *performance of technical expertise*.<sup>57</sup> To be enculturated into the Bitcoin development community is to conform to the BIPs process, and successful conformity to this process hinges on the successful performance of technical expertise.

It is worth emphasizing that the role of expertise here is not simply a matter of possessing a set of coding skills or a particular technical background; to the contrary, it is

---

<sup>55</sup> Coleman, *Coding Freedom*, 140.

<sup>56</sup> Dashjr, “BIP 2.”

<sup>57</sup> It is worth noting that this performance is at work in a BIP’s stylistic elements, too. Appropriately documenting a BIP’s backward compatibility, for example, is as much a matter of demonstrating a champion’s facility with a particular technical idiom as it is a matter of documenting the technical compatibility between BIPs.

the legitimization of a particular BIP through a deeply rhetorical performance that is crucial.

As Johanna Hartleius explains in *The Rhetoric of Expertise*:

Expertise is not simply about one person's skills being different from another's. It is also grounded in a fierce struggle over ownership and legitimacy. To be an expert is to claim a piece of the world, to define yourself in relation to certain insights into human experience. Expertise constitutes a special relationship between subject matter, a public, and one who masters and manipulates the former for the latter's benefit or need. The crux of the expertise issue is that being recognized as an expert generates not only status and power but considerable influence. [...] To be an expert, in short, is to rhetorically gain sanctioned rights to a specific topic or mode of knowledge.<sup>58</sup>

In the case of the BIP process, a champion's rhetorical performance is a prerequisite to "gain[ing] sanctioned rights" to the modification of the Bitcoin protocol; a champion must establish a particular relationship between the champion, the portion of the Bitcoin protocol addressed by the BIP, and the public of other Bitcoin developers.<sup>59</sup> A draft BIP may in fact be technically sound, but if this soundness is not demonstrated by the champion throughout the BIP process (e.g., in email interactions with other developers on the Bitcoin development mailing list), then the draft BIP's ultimate technical legitimacy will not be recognized, and the BIP will not advance throughout the workflow.

And yet premising participation in the BIP process on the successful performance of technical expertise is not simply an ethical matter. Because the BIP system is the means of collectively modifying the Bitcoin protocol, this participatory prerequisite of technical expertise significantly influences the *political* dynamics of Bitcoin, and it introduces the

---

<sup>58</sup> E. Johanna Hartleius, *The Rhetoric of Expertise* (Lanham, MD: Lexington Books, 2010), 1.

<sup>59</sup> This dynamic is reinforced by the BIP process's reliance on "champions": A champion who has already advocated for several BIPs will be able to draw on that history as part of his or her performance of expertise.

same political problem to the Bitcoin community that expertise does in liberal democratic polities more generally.<sup>60</sup> Simply put, this problem is this: Rhetorics of expertise hinge on the expert's political intervention *counting for more* than that of the non-expert. As Stephen Turner puts it in his study of the politics of expertise, "In the face of expertise, something has to give: either the idea of government by generally intelligible discussion, or the idea that there is a genuine knowledge that is known to a few, but not generally intelligible."<sup>61</sup> The abandonment of "government by generally intelligible discussion"—that is, the accessibility of politics by the broader community—may not seem to be a significant issue for a FOSS development community; after all, the development of network protocols *is* a technical matter requiring specialized knowledge and skills, and such development *does* draw on "genuine knowledge that is known to a few, but not generally intelligible."<sup>62</sup> But the Bitcoin protocol—and by extension, the BIP process that manages modifications to that protocol—bears much more significant political weight than simple software development does. As the previous chapter demonstrated, Bitcoin's commodity and procedural rhetorics displace the political as such onto the development of the Bitcoin protocol, which means that any barrier to participation in the development of the protocol is in fact a barrier to participation in the politics of the Bitcoin community. That is to say, a development process premised on the performance of technical expertise, combined with the rhetorical dynamic explored in the previous chapter, produces a community in which political participation as

---

<sup>60</sup> Stephen P. Turner, *Liberal Democracy 3.0: Civil Society in an Age of Experts*, Theory, Culture & Society (London ; Thousand Oaks, Calif: SAGE Publications, 2003).

<sup>61</sup> *Ibid.*, 5.

<sup>62</sup> *Ibid.*

such is *also* premised on the rhetorical performance of expertise. In short, the politics of an individualist collective end up looking a lot like technocracy.

This immediately raises the question of how the Bitcoin community, which rhetorically privileges the individual to the extent of entirely doing away with the communal, responds to a dynamic in which individuals are apparently required to submit to community experts. The means of reconciling this apparent contradiction is this: While the BIP process manages and organizes the development of the Bitcoin protocol, because the project is FOSS, adherence to the BIPs system is not a requirement for merely modifying software implementations of the protocol—or even proposing, outside of the BIP system, changes to Bitcoin’s protocol. Simply put, anyone is able to build new software that implements a new protocol that is in some way derivative of Bitcoin—and indeed, many of the altcoins within the broader cryptocurrency community began as modifications of Bitcoin’s protocol (e.g., Litecoin). The catch, however, lies in the interoperability of the new protocol with the rest of the Bitcoin network. Since the network exists only to the extent that network participants are connected *through a common protocol*, any changes to the protocol not sanctioned by participants in the Bitcoin network cannot be integrated into that network—and the BIP system, of course, is the community’s means of collectively coordinating such sanctions. In other words, to create a new protocol is to create a new monetary network, *albeit one that does not benefit from the network effects of engaging a large number of participants*; modifying the protocol in this way creates a new currency, but this currency is separated from any community willing to accept it as money. Indeed, the entire point of codifying the BIP system is to preserve Bitcoin as a monetary network in the midst of alterations to the rules of that network; the BIP process addresses the

collective action problem presented by the modification of a decentralized system. Thus, while it is technically true that the Bitcoin protocol may be modified outside of the BIPs system, and it is technically true that anyone is welcome to do so, these points offer an escape from BIP politics only in the most limited sense, precisely because the value and functionality of Bitcoin, like any other monetary technology, is dependent on others making use of the same technology. In practice, any workaround of the BIP system entails cutting oneself free of the entire Bitcoin network, and entirely restarting, from scratch, the difficult rhetorical work of constructing a new form of money.

Furthermore, problems of unequal access to and participation in the politics of Bitcoin are not the only side effects of an enculturation that privileges rhetorics of expertise: By privileging such rhetorical performances, the BIP process effectively constrains the range of issues that can be addressed by the Bitcoin community as a collective. In other words, while the displacement of Bitcoin's politics into the sphere of development means that all political matters for the currency are expressed through technical means (i.e., by modifying the protocol), not all political matters are reducible to technical disputes. The manner in which Bitcoin's proof-of-work function is constructed, for example, has far-reaching effects in the Bitcoin community, with implications for the kinds of hardware necessary to make Bitcoin mining economically profitable, for who is able to participate in Bitcoin mining, and for Bitcoin's ecological impact.<sup>63</sup> But the choice between different proof-of-work functions, insofar as they express these outcomes for the Bitcoin community, is not merely a technical question; it is a matter of values, of

---

<sup>63</sup> See Brunton, "Heat Exchanges."

convictions about what the community and currency *should* be.<sup>64</sup> In other words, the BIP system can only work as long as the development community maintains some degree of consensus about what is “in keeping with the Bitcoin philosophy”—to borrow a particularly telling phrase from BIP 2.<sup>65</sup> And when that consensus breaks down, when the BIP process is insufficient as both a political and ethical system, the second of Coleman’s FOSS terms rears its head: crisis.

### *The block size crisis*

What became known as the “block size debate” or the “Bitcoin scaling problem” began as a technical problem. As I explained in the previous chapter, Bitcoin records transactions of bitcoins—that is, digitally signed and hashed messages authorizing the movement of a particular amount of bitcoins from one address to another—in a sequence of hashed “blocks” of transactions, which are cryptographically linked into a “chain”—hence, the term blockchain. Importantly, these blocks are limited in size by the Bitcoin protocol: Each block can only contain up to a certain amount of transaction data, though blocks need not be “full” to be added to the blockchain.<sup>66</sup> Though the origins of this limit are sparsely documented, it seems that early in Bitcoin’s development Nakamoto recognized

---

<sup>64</sup> O’Hagan aptly captures the limits of such technical debates: “Coders call one another liars,” he writes, “when all they really mean is that they disagree about how software should work.” O’Hagan, “The Satoshi Affair.”

<sup>65</sup> Dashjr, “BIP 2.”

<sup>66</sup> In 2015, the default setting for the standard Bitcoin client filled blocks to roughly 75% of capacity. See Grace Caffyn, “What Is the Bitcoin Block Size Debate and Why Does It Matter?,” CoinDesk, August 21, 2015, <https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/>.

that large blocks could expose the Bitcoin network to denial-of-service (DoS) attacks—that is, malicious actors could spam the Bitcoin network with large, computationally intensive, and fraudulent blocks—and he instituted a 1 MB block size cap to prevent such attacks.<sup>67</sup> With a clearly defined and relatively small block size cap, any large, fraudulent blocks sent as part of a DoS attack could be rejected *before* the Bitcoin network devoted its computational resources to such blocks.

This smaller block size solved the problem of the moment, but it did lead to additional problems down the line. In the years after Nakamoto implemented the block size limit, Bitcoin's exposure, community, and perceived value grew—and consequently, the number of Bitcoin transactions occurring at any given time also grew. In fact, the number of transactions increased so much that the 1 MB blocks began to “fill up” every so often, which meant that the number of transactions that users were attempting to push through the Bitcoin network was periodically exceeding the number of transactions the Bitcoin network could readily support.<sup>68</sup> In turn, this excess resulted in delayed transaction processing times, since any transactions that could not fit into a “full” block would need to wait for the next block—making it more likely for the next block to fill, and so on.

According to a report by Bitcoin trading firm Tradeblock, by mid-2015 the Bitcoin network was hitting the 1 MB block size limit an average of four times per day.<sup>69</sup> At this point, it was

---

<sup>67</sup> David Dinkins, “Satoshi’s Best Kept Secret: Why Is There a 1 MB Limit to Bitcoin Block Size,” CoinTelegraph, September 19, 2017, <https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size>.

<sup>68</sup> Caffyn, “What Is the Bitcoin Block Size Debate and Why Does It Matter?”

<sup>69</sup> “Bitcoin Network Capacity Analysis – Part 1: Macro Block Trends,” TradeBlock, July 3, 2015, <https://tradeblock.com/blog/bitcoin-network-capacity-analysis-part-1-macro-block-trends>.

clear that Bitcoin was becoming a bit of a victim of its own success: Growing interest in the currency translated into an increased number of transactions, but this increase strained the ability of the network to process transactions in a timely manner, and thereby threatened to undercut the mainstream adoption of Bitcoin.

This development did not come as a surprise to the Bitcoin community; when the block size limit was first implemented, it was apparent that as the network grew, the block size limit would eventually have to be adjusted.<sup>70</sup> But as the network began to exhibit the effects of being “clogged,” the community paid more and more attention to constructing a number of solutions to this problem, each of which can be sorted into one of three general categories. First, a number of Bitcoin developers advocated for simply increasing the block size (e.g., from 1 MB to 2 MB, or from 1 MB to 8 MB).<sup>71</sup> Doing so would immediately alleviate pressure on the Bitcoin network, and would ensure that growing attention from outside the Bitcoin community would remain unsullied by reports of slow transaction speeds. However, advocates of this position had to contend with the fact that this solution seemed merely to kick the can down the road—if the network continued to grow, a larger block size would eventually fill, too—and that any increase in the block size would require full-scale adoption by the network, as larger blocks would not be compatible with the variant protocol versions sticking to smaller-sized blocks. Furthermore, since larger blocks are more computationally intensive to process (i.e., to validate and add to the blockchain), increasing the block size could potentially further restrict the work of Bitcoin mining to

---

<sup>70</sup> Nakamoto apparently thought that adjusting the block size would be trivial, and did not anticipate the controversy that doing so would inspire. See Dinkins, “Satoshi’s Best Kept Secret.”

<sup>71</sup> Caffyn, “What Is the Bitcoin Block Size Debate and Why Does It Matter?”

fewer participants in the network, thereby moving a decentralized network closer to centralization. Second, some Bitcoin developers argued for changing the size of transactions—that is, reducing the amount of data required for each transaction.<sup>72</sup> This proposal, named Segregated Witness (SegWit) for its separation of components of Bitcoin transaction data, was often compared to block size increases through a “checks in a box” analogy: If individual Bitcoin transactions are imagined to be paper checks in a box, and the box is imagined to be a block in the blockchain, then advocates of increasing the block size wanted a bigger box that could hold more checks, whereas SegWit advocates proposed introducing new, smaller checks, more of which could be stuffed into a small box.<sup>73</sup> Notably, and in contrast to the proposals for increasing the block size, SegWit would ensure compatibility with non-SegWit variants of the protocol, since the SegWit did not dramatically increase the block size. And finally, some Bitcoin developers advocated doing nothing at all.<sup>74</sup> These developers saw the block size issue as a problem that would solve itself: Since miners could be paid additional transaction fees to incentivize them to include a particular transaction in a block, as transactions moved more slowly, market mechanisms would respond to ensure that those most willing to pay for a transaction would see their transactions go through, while those unwilling or unable to pay would experience longer delays.

---

<sup>72</sup> “What Is SegWit?,” CoinDesk, February 22, 2018, <https://www.coindesk.com/information/what-is-segwit/>.

<sup>73</sup> Jimmy Song, “Understanding Segregated Witness,” SegWit Resources, August 7, 2017, <https://segwit.org/understanding-segregated-witness-905cc712c692>.

<sup>74</sup> Caffyn, “What Is the Bitcoin Block Size Debate and Why Does It Matter?”

The debates over these three categories of proposals played out across the mailing lists, discussion boards, and other media platforms of the Bitcoin community—and crucially, participation in these debates was not limited to regular contributors to other aspects of Bitcoin’s development. The block size problem was a question that truly involved the broader Bitcoin community, precisely because each category of solutions expressed a different vision for what Bitcoin should be, and thus the choice between different block size solutions was a political matter, not simply a technical one. Those who argued for leaving the block size problem to the market, for example, figured Bitcoin more as a store of value than as a medium of exchange: Bitcoin transactions would be slow and expensive, better suited for the occasional transfer of substantial wealth than paying for one’s morning coffee. In contrast, increases to the block size or implementation of SegWit aimed at preserving Bitcoin’s ability to facilitate cheap, quick transactions of the kind suitable for merchant payments or small remittances. And even between these two there is a contrast as well: Each category of proposal places different value on preserving compatibility with variants of the Bitcoin protocol, as well as a different value on maintaining a decentralized network of Bitcoin miners, and thus each expresses a different idea of how the Bitcoin community should be constituted.

To scrutinize these different courses of action, and to build community consensus around a particular choice, developers submitted proposals both for block size increases and for SegWit to the Bitcoin community’s central development institution: the BIP system.<sup>75</sup> These BIPs made their way through the specified cycles of proposal, revision, and

---

<sup>75</sup> See James Hilliard, “BIP 91: Reduced Threshold Segwit MASF,” GitHub, May 22, 2017, <https://github.com/bitcoin/bips/blob/master/bip-0091.mediawiki>; Eric Lombrozo, Johnson Lau, and Pieter Wuille, “BIP 141: Segregated Witness (Consensus Layer),” GitHub,

comment—and ultimately, something of a consensus formed to support SegWit, which was activated in Bitcoin software on August 23, 2017.<sup>76</sup> However, this consensus was a fragile one, and the progression of SegWit through the BIP system only marked the intensification of the block size debate into community crisis, in Coleman’s sense of the term, rather than the resolution of the problem. As SegWit progressed through the BIP system, a minority of the Bitcoin community remained dissatisfied with the proposal, and during the lead up to SegWit’s activation, momentum grew behind an alternate proposal to implement a new change to the protocol *outside* the BIP system—an explicit rejection of the ethical framework formalized in the BIP guidelines, and a sharp break in the previously shared sense of a common “Bitcoin philosophy.” This new protocol, known as Bitcoin Cash, would raise the block size limit to 8 MB—similar to an earlier and largely abandoned protocol alternative, Bitcoin XT<sup>77</sup>—as well as implement a number of changes unrelated to the block

---

December 21, 2015, <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>; Johnson Lau and Pieter Wuille, “BIP 143: Transaction Signature Verification for Version 0 Witness Program,” GitHub, January 3, 2016, <https://github.com/bitcoin/bips/blob/master/bip-0143.mediawiki>; Eric Lombrozo and Pieter Wuille, “BIP 144: Segregated Witness (Peer Services),” GitHub, March 12, 2017, <https://github.com/bitcoin/bips/blob/master/bip-0144.mediawiki>; Luke Dashjr, “BIP 145: Getblocktemplate Updates for Segregated Witness,” GitHub, January 30, 2016, <https://github.com/bitcoin/bips/blob/master/bip-0145.mediawiki>; and Shaolin Fry, “BIP 148: Mandatory Activation of Segwit Deployment,” GitHub, March 12, 2017, <https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki>.

<sup>76</sup> Alyssa Hertig, “SegWit Goes Live: Why Bitcoin’s Big Upgrade Is a Blockchain Game-Changer,” CoinDesk, August 23, 2017, <https://www.coindesk.com/50-blocks-segwit-bitcoins-coming-upgrade-blockchain-game-changer/>.

<sup>77</sup> Alex Hern, “Bitcoin’s Forked: Chief Scientist Launches Alternative Proposal for the Currency,” the Guardian, August 17, 2015, <http://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist>.

size.<sup>78</sup> As I noted above, changes to the protocol outside of the BIP system have always been possible, but are difficult to accomplish in practice due to the importance of network effects; however, the slow crescendo of the block size debate brought substantial attention to Bitcoin Cash and saved it the work of establishing a form of money from scratch. On August 1, 2017 Bitcoin Cash went live, adding a competing solution to the block size problem just weeks before SegWit finalized in the “original” Bitcoin (now referred to as “Bitcoin Core” for the sake of clarity). Thus, even after implementing solutions to the block size problem, the debate did not end: Today, both Bitcoin Cash and Bitcoin Core exist side by side, and supporters of each continue to lay claim to the “best” solution to the block size limit.

#### *What would Satoshi do?*

This is an admittedly abbreviated account of the block size debates, but for the purposes of the present chapter, the key feature of this story is not so much the details of the various proposals, but rather the way that the block size debates—and in particular, the split of Bitcoin Cash from Bitcoin Core—illustrate the intimate connection between the ethics of development (i.e., the formalization of developer communication in the BIP system), the rhetorics privileged by that ethical system (i.e., rhetorics of technical expertise), and the politics of implementing changes to the Bitcoin protocol. And crucially, these connections are thrown into relief by the *failure* of Bitcoin development processes to reach a solution acceptable to all members of the Bitcoin community. Though the block size

---

<sup>78</sup> “What Is Bitcoin Cash?,” CoinDesk, April 16, 2018, <https://www.coindesk.com/information/what-is-bitcoin-cash/>.

debate centered on a technical matter and was submitted to Bitcoin's technical process for modifying the protocol (i.e., the BIP system), technical rhetorics were not sufficient to resolve the matter, precisely because the choice between different block size solutions was a political matter as well as a technical one. In other words, the block size debates demonstrate the inability of developmental processes—designed with the intent to resolve technical matters, and consequently structured to privilege rhetorics of technical expertise—to bear the political weight assigned to them by digital metallism and Bitcoin's procedural rhetoric.

From one perspective, this failure is not surprising at all. Bitcoin's attempt to "get politics out of money" does warrant both a skeptical assessment and the expectation that, sooner or later, the structures supporting this supposed foreclosure of politics will break down. But from another perspective, there is something of a puzzle here: If the block size debate was a technical problem, submitted to a process that privileged technical rhetoric, how were those who rejected the technical consensus (i.e., SegWit) able to articulate an alternative in the first place? In other words, even if the politics of the various solutions to the block size problem were unsatisfactory to various elements of the Bitcoin community, on what rhetorical grounds could an alternative be constructed, if not technical ones? Simply put, from a rhetorical point of view, the notable element of the block size debates is not the proposals themselves, but rather *how the proposals were justified*.

Here at last we can return to the figure of Satoshi Nakamoto. Threaded throughout the block size debates, from their beginning in the mid-2010s to the present, are references to Nakamoto and his work—not just the white paper, but his email and message board exchanges, too. On its own, this point is not terribly compelling—after all, as the creator of

Bitcoin, Nakamoto is sure to be referenced in the course of debates over changes to the technology—but many of these references to Nakamoto go beyond providing historical context for early design decisions, or citation of Bitcoin concepts introduced by Nakamoto. Instead, they tend to cluster around a particularly telling phrase: Participants in the block size debates continually reference Nakamoto’s “original vision” for Bitcoin.

For example, early in the block size debates, in an episode that drew attention throughout the Bitcoin community, a person claiming to be Nakamoto—though widely believed not to be, due to the absence of any cryptographic signature—emailed the Bitcoin development mailing list and castigated the developers behind a particular block size increase implementation: “I have been following the recent block size debates through the mailing list,” the supposed Nakamoto wrote.<sup>79</sup> “The developers of this pretender-Bitcoin [i.e., the implementation of the proposed block size increase] claim to be following my *original vision*, but nothing could be further from the truth.”<sup>80</sup> Instead, the pseudo-Nakamoto claimed, “these developers are violating the ‘original vision’ they claim to honour.”<sup>81</sup>

The phrase is used not only in the first-person by Nakamoto impersonators—in fact, the email is somewhat unusual in this regard—but also in arguments for and explanations of particular block size solutions more generally. Nakamoto’s “original vision” is something of a rallying cry for advocates of Bitcoin Cash, for example, and the currency’s official

---

<sup>79</sup> Satoshi Nakamoto, “[Bitcoin-Dev] Bitcoin XT Fork,” August 15, 2015, <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-August/010238.html>.

<sup>80</sup> Ibid. Italics added.

<sup>81</sup> Ibid.

website justifies the split from Bitcoin Core using this language: Though increasing the block size in the original Bitcoin would be a trivial task, the website explains, “[s]ome of the developers [of Bitcoin Core] did not understand and agree with the *original vision* of peer-to-peer electronic cash that Satoshi Nakamoto had created”—and thus, Bitcoin Cash is needed to preserve this original vision.<sup>82</sup> (As evidence for this claim, the Bitcoin Cash website provides a link to the Bitcoin community’s central text: Nakamoto’s white paper.) Advocates for Bitcoin Cash have even adopted the phrase as the title and theme of a cryptocurrency conference: In March 2018, 400 attendees gathered in Tokyo to discuss “Satoshi’s Vision.”<sup>83</sup>

Furthermore, this reference to Satoshi’s vision for Bitcoin is even explicitly used to link the block size debates and the Bitcoin community’s pseudo-religious veneration of Nakamoto. As one commentator writes:

Within the Bitcoin community, if someone can show Satoshi’s support for his ideas, then he is sure to get widespread acceptance. Likewise, any effort to change one of Satoshi’s fundamental principles—such as the 21 million bitcoins money supply—is sure to be rejected with extreme prejudice. This widespread devotion to Satoshi has been largely beneficial to Bitcoin, *for devotion to Satoshi usually means devotion to his vision*. But like any devotion, it can be misapplied, and what appears to be faithfulness to Satoshi’s ideas can actually become a deviation from them.<sup>84</sup>

A few sentences later, the author explains that “[t]he blocksize [sic] debate is of course the primary arena of this deviation,” and goes on to argue that those committed to preserving

---

<sup>82</sup> “About,” Bitcoin Cash, 2018, <https://www.bitcoincash.org/#about>. Italics added.

<sup>83</sup> “Satoshi’s Vision | Bitcoin Cash Conference | March 23-25 Tokyo Japan,” accessed April 18, 2018, <https://satoshisvisionconference.com/>.

<sup>84</sup> Eric Sammons, “Fulfilling Satoshi’s Vision,” Decentralize Today, April 4, 2016, <https://decentralize.today/fulfilling-satoshi-s-vision-605e80845d0f>. Italics added.

the 1 MB block size, while appearing to adhere to Satoshi's "original vision," actually represent a deviation from it.<sup>85</sup>

Yet not all members of the Bitcoin community are pleased with the term; like Antonopoulos, some find the focus on Nakamoto to be inappropriate for a currency founded on the "nature" of cryptography and computer science. But crucially, even among those unconvinced by appeals to Nakamoto's vision, the phrase is recognized as a pervasive argumentative trope throughout the community.<sup>86</sup> As one community member complains, "I'm quite sick of people [...] using the phrase 'Satoshis [sic] original vision'."<sup>87</sup> "What bothers me most," another adds, "is that people who use "Satoshi's Original Vision" to make a point, do so selectively."<sup>88</sup> Notably, critiques of the "original vision" trope even reflect debate over what exactly counts as part of the Nakamoto "canon," suggesting that the phrase has less to do with Nakamoto's own views than the rhetorical leverage of those views. For example, in a follow-up discussion of the contradiction between a quote from a Nakamoto email and a particular protocol modification proposal framed as faithful to Nakamoto's "original vision," one exasperated user complained that they were "told in some other place that if [a Nakamoto quote is] not in the whitepaper [sic] it's not his vision

---

<sup>85</sup> Ibid.

<sup>86</sup> As one commentator joked, "Satoshi's original vision would be a good name for a horse." Neeraj K. Agrawal, "Satoshi's Original Vision," Tweet, Twitter, April 12, 2018, <https://twitter.com/NeerajKA/status/984606680871833601>.

<sup>87</sup> theonevortex, "Sick of Hearing 'Satoshi's Original Vision,'" *Reddit*, May 6, 2017, [https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick\\_of\\_hearing\\_satoshis\\_original\\_vision/](https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick_of_hearing_satoshis_original_vision/).

<sup>88</sup> SamWouters, "What Bothers Me Most," *Reddit*, May 7, 2017, [https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick\\_of\\_hearing\\_satoshis\\_original\\_vision/dh7jz8m/](https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick_of_hearing_satoshis_original_vision/dh7jz8m/).

but ‘an implementation detail’.”<sup>89</sup> In this way, contradictions between Nakamoto’s writings and his “original vision” can be resolved—though not necessarily convincingly so—by modifying the Nakamoto canon rather than by modifying the vision.

So how should these continual references to Satoshi’s vision—and the debates over the content and boundaries of that vision—be understood from a rhetorical perspective? It seems clear that the figure of Satoshi Nakamoto is invoked as an appeal to authority in the sense that Antonopoulos described above. It also seems clear that, as an appeal, references to Satoshi’s original vision are meant to justify *action* on the part of members of the Bitcoin community—that is, to endorse a particular change to the protocol. But two additional points add crucial nuance to this initial “appeal to authority” assessment.

First, references to Satoshi’s original vision *are not distributed evenly across the Bitcoin community*. They do not regularly appear in technical discussions of the block size, for example; in fact, aside from the previously noted impersonation of Nakamoto, the phrase “original vision” occurs only a handful of times in the voluminous correspondence of the Bitcoin development mailing list, as does “Satoshi’s vision”—and the phrase “Nakamoto’s vision” does not appear at all.<sup>90</sup> Furthermore, *none* of these phrases appear in the BIP archive.<sup>91</sup> And this absence of these phrases from the “primary mechanisms for proposing new features, for collecting community input on an issue, and for documenting

---

<sup>89</sup> SamWouters, “I Was Told in Some Other Place,” *Reddit*, May 7, 2017, [https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick\\_of\\_hearing\\_satoshis\\_original\\_vision/dh8mo6h/](https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick_of_hearing_satoshis_original_vision/dh8mo6h/).

<sup>90</sup> Archived at “Bitcoin-Dev,” accessed April 25, 2018, <https://www.mail-archive.com/bitcoin-dev@lists.linuxfoundation.org/>.

<sup>91</sup> *Bips: Bitcoin Improvement Proposals*, Go (2013; repr., Bitcoin, 2018), <https://github.com/bitcoin/bips>.

the design decisions that have gone into Bitcoin” suggests that the rhetorical function of the “original vision” should be understood as operating separately from the technical discussions of the BIP process.<sup>92</sup> Despite the presence of references to Nakamoto’s vision throughout the broader Bitcoin community’s debates over the block size, within purely technical discussions of the block size problem, Nakamoto’s vision simply is not a factor.

Second, appeals to Nakamoto’s original vision are tied both to a course of political action in the present (e.g., choosing Bitcoin Cash over Bitcoin Core) *and* to a particular understanding of Bitcoin’s political past. More specifically, references to Nakamoto’s original vision figure *the disappearance of Nakamoto from the Bitcoin community* as a key moment in the politics of Bitcoin. In most cases, this understanding of Bitcoin’s past is implicit—calls for adherence to Nakamoto’s original vision are necessary only because Nakamoto is no longer active in the community—but the instances in which this connection between Nakamoto’s vision and his disappearance is made explicit shed light on the deeper significance of Nakamoto’s departure:

With the disappearance of Satoshi, it has been left to lesser individuals to guide the project forward. As Bitcoin continues to grow and be developed, there are unfortunately no new Satoshis around to guide it. Some of those involved might be outstanding technological giants (even more technologically adept than Satoshi himself, perhaps?), and others might be outstanding in the field of economics. However, without Satoshi, it is up to the Bitcoin community to meld the principles of both these fields soundly to keep Bitcoin growing, robust, and in line with Satoshi’s original vision.<sup>93</sup>

---

<sup>92</sup> Dashjr, “BIP 2.”

<sup>93</sup> Sammons, “Fulfilling Satoshi’s Vision.”

Here Nakamoto is not merely an individual possessing exceptional technical skills or a deep understanding of economics; he is qualitatively different from all other members of the Bitcoin community—there are “no new Satoshis”—and as such, he is uniquely capable of “guid[ing] the project.” And crucially, it is only after the disappearance of this singular individual that the Bitcoin community is faced with the task of “soundly” melding technology and economics—that is, of making political decisions about the development of Bitcoin—in accordance with “Satoshi’s original vision.” By extension, the period prior to Nakamoto’s disappearance is figured as *apolitical*, a time in which the community, under the benevolent guidance of Nakamoto, did not need to engage in the work of deciding Bitcoin’s future. From this perspective, then, the invocation of Nakamoto’s vision functions not merely as a justification for a course of action, but as a way of framing contemporary political contests in the Bitcoin community as aberrations—as consequences of a “fall” from a prior state of harmony. In other words, appeals to the “original vision” implicitly draw on a deeply conservative condemnation of the political as such: Debates over how the community should proceed in the development of the Bitcoin protocol are themselves a deviation from Nakamoto’s guidance, since what is ultimately needed is not *debate* about the future of Bitcoin but *adherence* to Nakamoto’s vision. In Nakamoto’s absence, the politics of Bitcoin development is a kind of necessary evil, but it is an evil nonetheless, and one that is perpetually shadowed by the “memory” of an apolitical past. And in this figuring of the political as a barrier to be overcome rather than as an inherent element of every community, appeals to “Satoshi’s original vision” implicitly *repeat the foundational rhetorical move of digital metallism*. Here the problem is not a particular political disagreement; the problem is the existence of the political.

And yet this implicit condemnation of the political exists side-by-side with—though separate from—an elaborately detailed *political process* for determining the future of Bitcoin's protocol (i.e., the BIP system), and this context adds crucial nuance to the rhetorical role of appeals to Nakamoto's original vision. While on one level, both the BIP rhetorics of expertise and rhetorics of the "original vision" can be understood as interventions in the block size debates in the sense of advocating for a particular course of action, on another level, each of these strands of rhetoric also works, in its own way, to challenge the legitimacy of the other. Just as the rules of the BIP system challenge the political legitimacy of those unable or unwilling to articulate proposals to modify Bitcoin in terms of technical expertise (i.e., by excluding "inappropriately" constructed BIP submissions), rhetorics of Satoshi's vision challenge the legitimacy of the BIP process, insofar as that process is avowedly a matter of communal decision-making rather than of disavowing politics in a return to some prelapsarian, apolitical community. That is to say, in a manner analogous to commodity rhetorics, which disguise their own rhetorical presence by "telling it like it is," appeals to Nakamoto's original vision intervene in the politics of Bitcoin by figuring such interventions as apolitical, and thereby challenge the legitimacy of all other interventions. Thus, the "original vision" should be understood not only as one among many rhetorical strategies employed in the block size debates and related arguments; it should also be understood as a means of contesting the constraints of the BIP process, of challenging the privileging of rhetorics of expertise throughout Bitcoin's developmental processes, and *of challenging the legitimacy of Bitcoin's existing political structure*. In other words, appeals to "Satoshi's original vision" not only offer justification for particular changes to the Bitcoin protocol, but also give members of the Bitcoin

community the ability to substantially intervene into the politics of Bitcoin development without relying on rhetorics of expertise.

*Nakamoto and the politics of development*

While the “original vision” trope is certainly not the only use of Satoshi Nakamoto within the broader Bitcoin community, understanding this trope as a competitor to rhetorics of expertise helps to clarify several elements of the Bitcoin community’s treatment of Nakamoto more generally. First, the tension between “trustless” cryptography and the person of Nakamoto becomes legible not simply as a strange contradiction, but as an indicator of digital metallism’s political limitations: The valorization of cryptography and technology as grounds for a “trustless,” apolitical, individualist collective—which implicitly submits the politics of Bitcoin to the processes of protocol development—is what necessitates the parallel valorization of alternative grounds for political action (e.g., Satoshi’s original vision). In other words, for members of the Bitcoin community attempting to limit Bitcoin politics to the BIP system and associated development processes, Nakamoto’s “original vision” *is* a threat—in Antonopoulos’s terms, a “distraction”<sup>94</sup>—precisely because it highlights the fundamental political antagonism obscured by rhetorics of “trustless” cryptography and “natural” value. And for members of the Bitcoin community attempting to circumvent the BIP system and associated development processes, any valorization of Nakamoto—even valorization that tends toward strangely pseudo-religious veneration—serves to strengthen the grounds for political action that does not rely on rhetorics of expertise. As long as Nakamoto is

---

<sup>94</sup> andreasma, “Why I Declined to ‘Verify’ SN’s Identity Two Weeks Ago.”

recognized as important to the broader Bitcoin community, then his “vision” can be leveraged as a rhetorical tool.

Second, if appeals to “Satoshi’s original vision” are understood less in terms of advancing a particular change to the protocol and more in terms of giving a political voice to those unable or unwilling to advocate through the standard development process, then the ambiguity about what exactly counts as part of the Nakamoto canon can be understood not as a rhetorical flaw but as a rhetorical asset, insofar as it allows members of the Bitcoin community to employ the “original vision” as a rhetorical strategy across a broad range of political positions. Indeed, the flexibility of this strategy can be seen in the previously cited comment mocking the distinction between Satoshi’s “true” vision, as articulated in his white paper, and the “implementation details” of his emails and message board posts: Even those opposed to the use of the “original vision” trope can appeal to different conceptualizations of the Nakamoto canon—and by extension, different versions of the “original vision”—to undermine particular uses of the phrase in debates over Bitcoin’s development.<sup>95</sup>

And finally, the use of the “original vision” to contest rhetorics of expertise helps to explain what makes the *actual* return of Nakamoto—or episodes, such as the Wright affair, in which this return seems to be a possibility—such a deeply ambiguous thing in the Bitcoin community. On one hand, the return of Nakamoto certainly could bolster the rhetorical leverage of those advocating for some return to Satoshi’s “original vision”—after all, who in the Bitcoin community could persuasively advocate *against* a cryptocurrency “god”? As one member of the Bitcoin community wistfully mused in the midst of the Wright

---

<sup>95</sup> theonevortex, “Sick of Hearing ‘Satoshi’s Original Vision.’”

affair and the block size debates: “If [Wright] proves [that he is Nakamoto] and he comes at us saying we need to remove the block size limit now will we listen?”<sup>96</sup> From this perspective, Nakamoto’s return is a kind of Bitcoin *parousia*; indeed, in the previously cited thread, one commenter notes that “[h]oping for the return of Satoshi feels a little like hoping for the return of Jesus.”<sup>97</sup> And yet, such a return of Nakamoto to the Bitcoin community could just as well jeopardize the rhetorical flexibility afforded by the “original vision” trope. What if Nakamoto returns—and chooses the “wrong” side of a debate? For at least one community member, the fact that Craig Wright had not leveraged his identity as Nakamoto to intervene early in the block size debate was sufficient evidence *against* Wright’s claim to be Nakamoto: “I’m convinced that Craig Wright is not Satoshi, [sic] He is a strong supporter of big blocks and bitcoin cash, so if he had the power the put Bitcoin in the right direction before the community [split into Bitcoin Core and Bitcoin Cash] he would have done it years ago.”<sup>98</sup> In short, an absent cryptocurrency god might be preferable to one that endorsed the wrong block size solution.

This, then, is the rhetorical significance of Satoshi Nakamoto: In an arena where the politics of a community is filtered through the performance of rhetorics of expertise, Nakamoto functions as a rhetorical resource, as a means of advancing arguments about

---

<sup>96</sup> Edit0r88, “IF Dr. Wright Is Satoshi..,” *Reddit*, December 10, 2015, [https://www.reddit.com/r/bitcoin\\_uncensored/comments/3w5fcg/if\\_dr\\_wright\\_is\\_satoshi/](https://www.reddit.com/r/bitcoin_uncensored/comments/3w5fcg/if_dr_wright_is_satoshi/).

<sup>97</sup> Ibid.

<sup>98</sup> HurlSly, “If Craig Wright Is Satoshi, the Scaling Debate Would Be Settled Years Ago,” *Reddit*, March 1, 2018, [https://www.reddit.com/r/btc/comments/816hri/if\\_craig\\_wright\\_is\\_satoshi\\_the\\_scaling\\_debate/](https://www.reddit.com/r/btc/comments/816hri/if_craig_wright_is_satoshi_the_scaling_debate/).

how the protocol of Bitcoin *should* be constructed without submitting to the performance of expertise. “Satoshi’s vision” is—somewhat paradoxically, given that its key document is a technical white paper—a means of legitimating interventions into the politics of Bitcoin for those lacking or unwilling to perform technical expertise, and of challenging community structures that restrict Bitcoin politics to technical discourses. But crucially, Nakamoto achieves rhetorical relevance in the broader assemblage of Bitcoin *only in relation to Bitcoin’s more fundamental rhetorical dynamic*, produced through the combination of digital metallism and Bitcoin’s procedural rhetoric, in which the politics of Bitcoin is shifted to the politics of protocol development. Thus, the use of Nakamoto as a rhetorical tool is the unanticipated side effect of the displacement of politics into a framework ill suited to dealing with questions that exceed the bounds of technical disputes, and it suggests that any currency sharing a similar rhetorical foundation will need to grapple with—and will see the emergence of rhetorics, even those as apparently disconnected from politics as the veneration of Nakamoto, that attempt to grapple with—the unavoidably political question of “Who has a say in the construction of the currency?”

## Chapter Four

### Rewriting History: On Blockchain Forks and Currency Identity

In the previous chapter, I argued that the displacement of Bitcoin politics onto the development of Bitcoin's protocol produced a political structure that privileges rhetorics of technical expertise, and prompted the creation of rhetorical alternatives to performances of expertise, such as appeals to Nakamoto's original vision. By advancing this argument, I showed how the rhetorical dynamic embraced by early Bitcoin advocates, in which politics itself is figured as a problem to be overcome via the "nature" of Bitcoin's code, continued to influence discursive elements of Bitcoin, even when those elements (e.g., the deification of Nakamoto) are not immediately engaged with questions of monetary value (i.e., the original rhetorical focus of digital metallism). I also showed how a rhetorical perspective can aid the understanding of connections between discourse, technology, and politics by identifying key areas of rhetorical contest (e.g., the politics of protocol development) that have been important for Bitcoin's construction thus far, and will likely remain so in the future.

Yet identifying this chain of rhetorical influences also raises questions about the extent of those influences, particularly as they relate to cryptocurrencies other than Bitcoin. As I noted in the introduction of this dissertation, Bitcoin's meteoric rise over the last decade has been followed by the rise of hundreds of alternatives to Bitcoin ("altcoins"), and as Lynette Shaw's study of Bitcoin message boards suggests, this rise of these altcoins is paralleled by a shift towards "blockchain" as a key term in Bitcoin discourse, and *away*

from discourse focused on digital metallism.<sup>1</sup> These developments do not necessarily mean that the central rhetorical dynamic of digital metallism (i.e., the attempt to foreclose politics) is irrelevant—as the analysis of the last chapter showed, this dynamic impacts more than explicit discussions of value—but they do raise an important question: To what extent does the rhetorical legacy of digital metallism continue to play a role in Bitcoin’s digital currency successors? That is to say, are the rhetorical dynamics explored in the previous chapters unique to Bitcoin, with its attachment to a mysterious creator and its ideological roots in cyberlibertarianism and crypto-anarchism, or do these dynamics extend to other blockchain-based altcoins, too? How does Bitcoin’s combination of commodity money rhetoric and procedural rhetoric change in the context of a new digital currency?

To answer these questions, the remainder of this chapter examines Ethereum, one of the most prominent of Bitcoin’s heirs. More specifically, I examine the case of The DAO, a decentralized autonomous organization constructed using Ethereum, which was the site of a widely publicized theft in June 2016. This theft and the Ethereum community’s response to it, I argue, show that the central rhetorical dynamic of Bitcoin—the displacement of politics onto development—still persists, even in the context of a successor currency, and even in the absence of explicitly digital metallist discourse. Furthermore, I argue that the case of The DAO demonstrates that the persistence of this political displacement plays a crucial role in the valuation of digital currencies more generally, insofar as the rhetorical *identity* of a given currency is a key means of addressing the political problems introduced by the procedural rhetoric of blockchain technology.

---

<sup>1</sup> Shaw, “The Meanings of New Money.”

To advance this argument, I proceed in five steps. First, I introduce Ethereum, and explain how its development arose out of an interest in expanding the capabilities of digital currency-based programming languages. Next, I explain how this expansion enables the development of new legal and organizational technologies—namely, smart contracts and decentralized autonomous organizations—and I show how the goals of these developments are premised on the same conceptual and rhetorical basis as digital metallism. Next, I turn to the case of a specific decentralized autonomous organization, The DAO, and review its development, the theft of its funds, and the solutions to the theft considered by the Ethereum community, including the “forking” of the Ethereum blockchain. After a brief detour into the technical details of blockchain forks, I examine the curious response of The DAO attacker to these proposals, and show both how the attacker justified the theft from The DAO in terms that borrow from the rhetoric of digital metallism, and how this response caught the Ethereum community in a rhetorical contradiction. I then review the fallout of the Ethereum fork, and use this case to identify and explicate another key rhetorical dynamic of blockchain-based procedural rhetoric: Because there is always a potential gap between the procedural constitution of an individualist collective and human understanding of such a collective, blockchain-based currencies cannot rely solely on their protocols to produce a stable and coherent monetary community, and instead must rely on the production of a coherent and stable rhetorical *identity*. Ultimately, then, the influence of digital metallism extends past Bitcoin, and makes the production of a community identity—an identity distinct from the procedural production of a blockchain collective—a key factor in the valuation of cryptocurrencies.

*Ethereum, smart contracts, and decentralized autonomous organizations*

Ethereum is an altcoin project: a technological successor to Bitcoin that adapts and alters Bitcoin's innovations to new ends.<sup>2</sup> As such, Ethereum shares many of Bitcoin's key features. Like Bitcoin, Ethereum's foundation is a blockchain. This blockchain tracks the transfer and control of digitally signed tokens—though in Ethereum's blockchain these tokens are known as “ether” rather than bitcoins—and Ethereum uses computational work to enforce the scarcity of these tokens.<sup>3</sup> Like Bitcoin, Ethereum was initially proposed in a white paper.<sup>4</sup> In contrast to Bitcoin, however, the identity of the Ethereum paper's author, Vitalik Buterin, has always been publicly known, and Buterin continues to be a central player in the ongoing development of Ethereum.<sup>5</sup> This development, like Bitcoin's, is conducted along FOSS lines, and Ethereum features a protocol development process—the Ethereum Improvement Proposal (EIP) system—derived primarily from the Bitcoin Improvement Proposal system discussed in the previous chapter.<sup>6</sup>

The key difference between Bitcoin and Ethereum, and the motivation for Buterin's initial proposal of the project, is Ethereum's programming capabilities.<sup>7</sup> Bitcoin features a

---

<sup>2</sup> “Ethereum Project,” Ethereum, 2018, <https://www.ethereum.org/>.

<sup>3</sup> Henning Diedrich, *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations* (Wildfire Publishing, 2016), 43.

<sup>4</sup> Vitalik Buterin, “Ethereum White Paper,” GitHub, 2013, <https://github.com/ethereum/wiki/wiki/White-Paper>.

<sup>5</sup> “History of Ethereum,” Ethereum Homestead, 2016, <http://www.ethdocs.org/en/latest/introduction/history-of-ethereum.html>.

<sup>6</sup> “EIPs: The Ethereum Improvement Proposal Repository,” GitHub, May 4, 2018, <https://github.com/ethereum/EIPs>.

<sup>7</sup> Buterin, “Ethereum White Paper.”

built-in scripting language (simply named “Script”), which allows the currency to handle certain types of transactions internally. For example, using Bitcoin’s Script, it is possible to implement a simple escrow service, in which bitcoins are “locked” in the blockchain until multiple parties digitally sign a transaction together.<sup>8</sup> But even though “[t]he scripting language in Bitcoin is quite flexible and powerful,” the functionality of this language is intentionally limited.<sup>9</sup> In particular, Script is not “Turing-complete”—that is, it cannot be used to process all types of computational problems.<sup>10</sup> As digital currency researcher Pedro Franco explains, this limitation was implemented for purposes of security:

If the scripting language were Turing-complete an attacker could craft a [script] that never finished, say because it enters an infinite loop. This would cause the nodes in the network that evaluate this script to stall and could bring the network down. For this reason it was decided that the scripting language would not contain loops.<sup>11</sup>

Ethereum, by contrast, rejects these intentional constraints and introduces two technological features to make Ethereum more “programmable” than Bitcoin. First, Ethereum’s programming language, Solidity, *is* Turing-complete, which means that in theory there is no limit to the kinds of computational structures that can be build “on top” of Ethereum—though the practical limits of data storage and computational resources still apply.<sup>12</sup> Second, Ethereum is “stateful,” which means that programs implemented in

---

<sup>8</sup> Franco, *Understanding Bitcoin*, 84–85.

<sup>9</sup> *Ibid.*, 81.

<sup>10</sup> *Ibid.*

<sup>11</sup> *Ibid.*

<sup>12</sup> Diedrich, *Ethereum*, 28.

Ethereum can store and reference past program outputs.<sup>13</sup> Together, these features make Ethereum much more than a technology for processing payments or for storing value, as Bitcoin aims to be; instead, Ethereum functions as “a platform for many different types of decentralized blockchain applications, including but not limited to cryptocurrencies.”<sup>14</sup>

Of course, this raises the obvious question of *why* one would want to expand Ethereum’s capabilities in this way. What is the benefit of moving beyond Bitcoin’s self-imposed limitations, especially given the security concerns that led to the restriction of Script? The answer, simply put, is that pairing a digital currency (ether) with a full-fledged programming language (Solidity) enables the construction of *smart contracts*.<sup>15</sup> As defined by cryptographer Nick Szabo in the essay that coined the term, “[a] smart contract is a set of promises, specified in digital form, including protocols within which the parties perform on these promises.”<sup>16</sup> In essence, such contracts substitute legal documents with computer programs; they aim “to codify a legal agreement in a program and have a computer execute [the agreement’s] terms instead of humans having to interpret and act on it.”<sup>17</sup> This collapse of the distinction between the contract and its execution is key here; what makes a

---

<sup>13</sup> Ibid.

<sup>14</sup> “What Is Ethereum?,” Ethereum Homestead, 2016, <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>.

<sup>15</sup> Buterin, “Ethereum White Paper.”

<sup>16</sup> Nick Szabo, “Smart Contracts: Building Blocks for Digital Markets,” *Extropy*, 1996.

<sup>17</sup> Diedrich, *Ethereum*, 166.

smart contract “smart” is that it requires no third party for the interpretation and enforcement of its terms, since *the terms are their own enforcement*.<sup>18</sup>

This dynamic can be illustrated by the often-cited example of the “low tech” predecessor to smart contracts: the vending machine.<sup>19</sup> Unlike a human cashier, who *interprets* the interpersonal exchange of money and goods in accordance with a set of policies, a vending machine simply waits for a set of conditions to be met (i.e., some amount of money is inserted and an available item is selected) and then responds accordingly (i.e., by dispensing the item) in what is essentially a mechanistic process. In the case of the vending machine, both the terms of the agreement (e.g., insert one dollar, receive one item) and the means of executing this agreement are one and the same; both are “built into” the technology of the vending machine. Of course, as anyone who has used a vending machine can attest, this process may not result in the *customer’s* desired outcome (e.g., the machine may break, items may get caught within the machine). But from the point of view of the vending machine, this is irrelevant; the “contract” of the machine is fulfilled by the execution of the vending process, not by satisfying the customer’s interpretation of that process.

In essence, then, smart contracts are an extension of this vending machine automation to a broader range of contractual relationships. But crucially, this extension depends on the combination of a robust programming language and a digital currency.

---

<sup>18</sup> As the Ethereum white paper points out, “Even without any extensions, the Bitcoin protocol actually does facilitate a weak version of a concept of ‘smart contracts,’” in the sense that the agreement to transfer bitcoins *is* the transfer of those bitcoins. See Buterin, “Ethereum White Paper.”

<sup>19</sup> This comparison was introduced in the same essay that coined the term “smart contract.” See Szabo, “Smart Contracts.”

Prior to the advent of digital currencies, the key limitation in implementing smart contracts was money: Without a cash-like digital currency, a smart contract would be forced to rely on third-party payment processors to execute monetary aspects of a contract. In turn, such third parties would need to be bound by *legal* contractual agreements (as opposed to the code of a smart contract), since such a payment processor would possess the power to alter or block particular transactions (e.g., chargebacks), and thereby alter the execution of the contract in question. But by pairing a digital currency with a Turing-complete and stateful programming language, Ethereum provides a workaround for this reliance on third parties: Ethereum's combination of Solidity and ether enables the construction of "an agreement that is binding, not only in theory but in practice, as it can move information *and* money around based on the concrete terms of the agreement."<sup>20</sup>

But explaining the expansion of Ethereum's programming capabilities by pointing to the ability to build smart contracts simply raises additional questions: Why build smart contracts in the first place? What is the problem that such contracts solve? The answer to these questions can be found in the contrast between the enforcement processes of smart contracts and those of ordinary legal contracts. A "dumb" contract, for example, functions only insofar as its parties share some common social ground—a shared interpretation of the contract, or in cases of disagreement, a shared commitment to resolving contractual disputes within a shared institutional context (e.g., a judicial system). But because such "dumb" contracts are dependent on shared interpretation and shared institutions, there is always the possibility that a contract might not execute according to its terms: Parties might disagree on the interpretation of a contract, for example, and one party might refuse

---

<sup>20</sup> Diedrich, *Ethereum*, 167.

to act according to a particular understanding of the contract's terms; or a court might declare the terms of a contract to be unenforceable; or a party might simply ignore a contract altogether, judging that benefits gained from a breach of the contract outweigh any costs associated with this breach. In turn, these possibilities force "dumb" contracts to rely on what Szabo calls "reactive security": Because contract violations are *possible courses of action* for the parties involved, the terms of a contract are enforced *after* a violation occurs (e.g., by submitting the matter to the judicial system).<sup>21</sup> By contrast, smart contracts preemptively eliminate the possibility of contract violation by making the contract and its execution one and the same; to agree to a smart contract is to execute the contract's terms, with no reactive security (i.e., shared interpretation and shared institutions) required. And in this way, smart contracts reiterate the same conceptual framework used to establish Bitcoin as a form of money. That is to say, the "problem" to which smart contracts respond is *the embeddedness of contracts within social and political contexts*. Just as Bitcoin attempts to foreclose the social and political by producing an asocial and apolitical monetary community, smart contracts attempt to foreclose the possibility of community intervention in contractual relations. Thus, smart contracts are the natural extension of the underlying drive of digital metallism: Money without community intervention becomes the basis for contracts without community intervention.

But smart contracts are not the end point of this extension, and with the ability to build automated contractual relations comes the ability to construct *organizations* on the same basis. To the extent that organizations consist of a set of rules that outline roles of authority and responsibility, that manage intra- and inter-organizational interactions, and

---

<sup>21</sup> Szabo, "Smart Contracts."

that define organizational membership, such organizations can be replicated on Ethereum as complex smart contracts (or as an interlocking set of smart contracts).<sup>22</sup> An employee in a smart contract-based company, for example, might not have his or her job defined in terms of company policies, which necessitate interpretation. Instead, the full extent of the employee's ability to interact with the company could be defined within the smart contract: An employee joining a smart contract-based company might have his or her access to company resources (e.g., ether, company data, Internet of Things-linked assets), ability to direct (or even contact) other members of the company, and terms of compensation all defined by the company smart contract. However, the point of constructing organizations on Ethereum is not simply to replicate already-existing organizations; rather, the point is to leverage the combination of ether and Solidity to create *new types* of organizations, organizations that would be impossible to construct without smart contracts.

The most notable of such new organizational structures are *decentralized autonomous organizations* (DAOs). A DAO is "more than using the blockchain to manage a company: instead, the code *is* the entire company."<sup>23</sup> As a smart contract (or group of smart contracts), a DAO can own digital assets (e.g., ether); it can use those assets to purchase goods or services from "real world" organizations, or from other DAOs; and in turn, it can provide goods or services to any person or organization able to interact with the Ethereum network.<sup>24</sup> And crucially, a DAO can do all of the above without any organizational "leader"

---

<sup>22</sup> As Buterin noted in the Ethereum white paper, to do so "replicates the legal trappings of a traditional company or nonprofit but using only cryptographic blockchain technology for enforcement." Buterin, "Ethereum White Paper."

<sup>23</sup> Diedrich, *Ethereum*, 180.

<sup>24</sup> *Ibid.*, 181–84.

or “owner” in the usual sense; since a DAO requires no interpretation to execute the terms of its smart contract, a DAO need not have any CEO or other figure managing the organization’s adherence to its stated goals. A DAO might have something like “shareholders,” in the sense of (smart) contractual obligations to those who fund the organization, but not in the legal sense of the term, and even if a DAO owned and operated real-world assets, the organization would only “reside” on the Ethereum blockchain, and consequently, it would not necessarily have a legal existence at all—and would then, by default, be a stateless entity.

So what might a DAO look like in the “real world”? A leaderless DAO could “run and own a hotel: hire and fire people by scanning its own Yelp ratings, procure whatever is needed for daily operations using the Ethereum [network] and leverage smart building technology to offer the best possible experience for guests.”<sup>25</sup> Paired with other technologies, such as self-driving vehicle technology, another DAO could operate as an ownerless, employee-less, self-managing transportation service, receiving passenger payments via the Ethereum blockchain, and automatically allocating funds for periodic maintenance of the DAO’s vehicles at a Ethereum-compatible garage.<sup>26</sup> These examples are hypothetical, of course, and depend on the integration of Ethereum with other technologies, but the point here is that the technological foundation for implementing these types of ownerless, leaderless, stateless organizations does in fact exist. The primary barrier to developing a self-owning, self-managing, employee-less, ether-based investment firm, for instance, is the work of designing an appropriate smart contract to control the

---

<sup>25</sup> Ibid., 181.

<sup>26</sup> Ibid., 181–82.

firm's management of ether; the platform on which such a contract could operate (i.e., Ethereum) already exists.

In the following section of this chapter, I will discuss DAO structures in more detail, but for the moment, it is sufficient to note that DAOs are ownerless, leaderless organizations, constructed via smart contracts within the broader individualist collective of Ethereum's blockchain. In this way, DAOs are a repetition of the digital metallist dream of a *polis* without politics, but implemented at a scale different from that of a monetary community: Money without community intervention leads to contracts without community intervention, which leads in turn to organizations without community intervention. This is not to say that Ethereum, its smart contracts, and its DAOs *explicitly* invoke digital metallist rhetoric to justify the value of ether, Ethereum's token; comparisons of ether to digital gold, references to ether's intrinsic value, or even discussions of ether as a commodity are not frequent or significant elements in Ethereum discourse. But although the explicit references to commodity money rhetoric do not carry over from Bitcoin to Ethereum, the entire motivation for Ethereum—providing a platform for contracts and organizations that exist entirely as code—is premised on the *same foreclosure of politics* that Bitcoin attempts in a monetary domain. A contract without interpretation is a contract whose terms cannot be altered under community pressure, and a company with no owner, leader, employees, or legal residence is subject to nothing more than its own rules. In this way, Ethereum is not so much a break with Bitcoin's combination of digital metallism and blockchain procedural rhetoric, but rather an intensification of it—an extension of digital metallism's logic beyond monetary communities to community as such.

*The DAO attack*

With this background on Ethereum, smart contracts, and DAOs established, it is possible to turn to the central case of this chapter: a particular DAO named—quite unhelpfully—*The DAO*.<sup>27</sup> The DAO was designed to be a kind of decentralized, crowd-funded venture capital fund, with a central mission of supporting Ethereum start-up companies, and thereby helping to spur the growth and adoption of Ethereum more generally.<sup>28</sup> The plan for The DAO was this: After an initial twenty-eight day period of funding, in which potential investors in The DAO could scrutinize The DAO’s publicly-accessible code (i.e., the terms of its governing smart contract) and “buy into” The DAO by sending ether to an account controlled by The DAO, the organization would solicit proposals from developers in the Ethereum community. After reviewing these proposals for Ethereum start-ups, “investors would vote for the ideas brought before The DAO with votes weighed by the size of their investment into [T]he DAO” in a “completely automated investing, voting and payout process.”<sup>29</sup> Structurally, the organization resembled a shares-based company in which shareholders directly managed investment decisions, albeit with the important caveat that since The DAO was *a* DAO, no one actually “owned” or “led” the

---

<sup>27</sup> To distinguish between this particular DAO and the more general category of organizations, I refer to the former with a capitalized “The.” Like Bitcoin and Ethereum, The DAO was initially proposed in a white paper; see Christoph Jentzsch, “Decentralized Autonomous Organization to Automate Governance” (Slock.it, 2016), <https://download.slock.it/public/DAO/WhitePaper.pdf>.

<sup>28</sup> Diedrich, *Ethereum*, 286.

<sup>29</sup> Ibid. More specifically, investors in The DAO would be issued “DAO tokens” in accordance with the size of their ether investment, so that possession of DAO tokens would be somewhat analogous to ownership of “shares” of The DAO—though not in the legal sense of the term, since The DAO was governed by a smart contract rather than a shareholder agreement.

organization, and The DAO's funds were not controlled by (or legally subject to) these "shareholders," but rather by The DAO itself.

The DAO's funding period commenced on April 30, 2016. Much to the surprise of The DAO's developers, over the next few weeks the organization attracted far more investment than anticipated, and during the first fifteen days of its funding period, The DAO raised an amount of ether equivalent to \$100 million USD.<sup>30</sup> However, even as investors flocked to The DAO, members of the digital currency community began to raise concerns about the organization. Some worried about the legal implications of The DAO's fundraising, especially given the amounts that had been raised, and feared that governments would find The DAO to be in violation of securities regulations.<sup>31</sup> Others turned their attention to the "text" of The DAO's smart contract: Public examination of The DAO's code led to the identification of several potential exploits of the contract, and these security concerns were thought to be so significant that some members of the Ethereum community called for a temporary moratorium on funding The DAO.<sup>32</sup> There were, in short, good reasons to suspect that The DAO might not be the soundest of investments.

---

<sup>30</sup> David Siegel, "Understanding The DAO Attack," CoinDesk, June 25, 2016, <https://www.coindesk.com/understanding-dao-hack-journalists/>.

<sup>31</sup> In the following year, this concern was borne out by the U.S. Securities and Exchange Commission's classification of "shares" of The DAO as securities. See "Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO" (U.S. Securities and Exchange Commission, July 25, 2017), <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

<sup>32</sup> Dino Mark, Vlad Zamfir, and Emin Gün Sirer, "A Call for a Temporary Moratorium on The DAO," Hacking Distributed, May 27, 2016, <http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/>. Notably, these concerns were paired with calls for a moratorium, rather than with calls to alter the code of The DAO, because The DAO, as FOSS software developed in a decentralized manner similar to Bitcoin and Ethereum, could not be unilaterally altered by developers after the code

Nevertheless, investors continued to pour money into The DAO, and by the close of the funding period in late May, the contributions of over 11,000 investors gave The DAO control of a store of ether valued at a little over \$150 million USD.<sup>33</sup> In parallel to this attention from investors, hopeful Ethereum start-up projects flocked to The DAO, and when The DAO's funding period closed, "more than 50 project proposals were waiting for The DAO's token holders to vote on them."<sup>34</sup> Yet despite having a sizeable pool of proposals and a wealth of ether to spend, The DAO's participants agreed that it was necessary to fix the flaws in the smart contract (i.e., those identified during the initial funding period) before moving on to the proposal selection stage; accordingly, developers set to work designing and coordinating the deployment of remedies to these exploits.<sup>35</sup>

However, before these remedies could be implemented, some unknown person or persons began to use these exploits to steal funds from The DAO. On June 17, 2016, this attacker was able to move \$3.6 million ether, the equivalent of about \$50 million USD at the

---

began to execute (i.e., after the April 30<sup>th</sup> launch). That is to say, in the absence of coordinated action from participants in The DAO, the only means of addressing The DAO's security flaws was for individual investors to voluntarily halt the flow of money into the organization.

<sup>33</sup> Nathaniel Popper, "A Venture Fund With Plenty of Virtual Capital, but No Capitalist," *The New York Times*, May 21, 2016, sec. DealBook, <https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html>.

<sup>34</sup> Siegel, "Understanding The DAO Attack."

<sup>35</sup> See Stephan Tual, "No DAO Funds at Risk Following the Ethereum Smart Contract 'Recursive Call' Bug Discovery," Slock.it Blog, June 12, 2016, <https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b#.mbfqikiyo>; and Stephan Tual, "Proposal Framework 1.0, DAO 1.1 Draft!," Slock.it Blog, June 10, 2016, <https://blog.slock.it/proposal-framework-1-0-dao-1-1-draft-427c40ef9ed4#.wkgvffoqx>.

time of the attack, into a “child DAO.” This new child DAO was yet another iteration of *The DAO*, with the same structure, rules, and vulnerabilities as its “parent” smart contract—including, crucially, the twenty-eight day funding period, during which the child DAO’s funds could not be transferred *out* of the contract. But since this child DAO’s sole source of funding came directly from a single transfer (i.e., the theft from *The DAO*) rather than from a myriad of investor contributions, at the end of the child DAO’s twenty-eight day period the attacker would control all of the voting “rights” in the child DAO, and thus, all of the stolen funds.

Since it took place on a blockchain-based platform, this theft was conducted entirely “in public”—that is, the theft was visible to anyone inspecting the Ethereum blockchain—and as such, the attack drew rapid responses from the Ethereum community. On the same day as the attack, Ethereum founder Vitalik Buterin issued a statement in which he explained how the attack was accomplished, and emphasized that “[t]his is an issue that affects the DAO specifically; Ethereum itself is perfectly safe.”<sup>36</sup> Nevertheless, the Ethereum community treated the fortunes of the two as intimately linked, and the theft clearly shook investor confidence in Ethereum. In the wake of the attack, the price of ether on major cryptocurrency exchanges “dropped from over \$20 to under \$13” USD—a loss of more than a third of the currency’s price.<sup>37</sup>

Yet there was something of an odd sense of *time* provoked by this theft, too. The exploit of *The DAO* was immediately recognized by the Ethereum community as a

---

<sup>36</sup> Vitalik Buterin, “CRITICAL UPDATE Re: DAO Vulnerability,” *Ethereum Blog* (blog), June 17, 2016, <https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/>.

<sup>37</sup> Siegel, “Understanding The DAO Attack”; also see “Ethereum (ETH) Historical Data,” CoinMarketCap, 2018, <https://coinmarketcap.com/currencies/ethereum/historical-data/>.

significant crisis—both in the sense of being a substantial theft, and also in the sense of being a publicity nightmare for Ethereum—and it prompted understandably rapid responses from traders and developers. But the fact that the funds had been transferred to a child DAO meant that the attacker could not make use of those funds for nearly a month; that is to say, the stolen funds would remain locked in the child DAO for the child DAO's standard twenty-eight day funding period. Furthermore, because the Ethereum blockchain is public, the entirety of the Ethereum community knew exactly where the stolen money was, and would be able to watch exactly where the money went when the attacker finally move the funds again. In short, even as the Ethereum community sorted out how to respond to such a sizable theft, the stolen money would remain “out in the open” for four weeks, visible to all, but accessible by no one.

This left participants in The DAO, and the Ethereum community more broadly, twenty-eight days to determine an appropriate response to theft. Over the weeks following the attack, the community debated three courses of action: 1) Implement a “soft” change to the Ethereum protocol to restrict the use of the stolen funds; 2) Implement a “hard” change to the protocol to recoup the stolen funds; or 3) Do nothing. I have already discussed one case of protocol change in the previous chapter (i.e., the split of Bitcoin Cash from Bitcoin Core), though for the purposes of that chapter, I did not delve into the technical details of how such splits are implemented. But because these details *are* relevant to the case of The DAO, and because understanding these details is necessary to grasp the contours of the debates over these three possible responses to the attack on The DAO, I now briefly turn to the process of blockchain protocol splitting—that is, blockchain “forking.”

*Blockchain forks*

In this dissertation, I have already discussed the importance of protocol interoperability for Bitcoin, and I have noted that changes to the Bitcoin protocol not sanctioned by participants in the Bitcoin network face significant consequences—namely, they lose the benefits of the network effects that come with having a large number of participants in a single monetary network. But it is not just the protocol that is important in such scenarios; indeed, the protocol is important precisely because it governs another aspect of the digital currency system: the production of the blockchain. As I explained in the second chapter, blockchains consist of hashed “blocks” of transaction data that miners compute and then broadcast to their network. Other miners, in turn, add these newly broadcast blocks to their own copies of the blockchain. However, before each miner adds a newly broadcast block to their copy of the blockchain, the miner checks to both that the hash of the block is legitimate *and* that the block is constructed in accordance with the miner’s version of the Bitcoin protocol.<sup>38</sup> Any blocks *not* compatible with the miner’s protocol will be rejected, and will not be added to that miner’s copy of the blockchain.<sup>39</sup> In other words, if one miner uses a new, changed protocol, but the rest of the network does not, the singular miner’s blocks will be rejected by the network as a whole. The reverse can be the case as well: If the network as a whole upgrades to a new, incompatible version of the protocol, but one miner does not, this miner will not accept any of the new blocks broadcast by the rest of the network.

---

<sup>38</sup> Franco, *Understanding Bitcoin*, 109.

<sup>39</sup> *Ibid.*

But the key point here is not merely that changes to the protocol alter the blockchain; it is that changes to the protocol alter the blockchain *as it lengthens*—that is, moving forward from a particular point in time. Such changes do *not* reach back into the past and alter all of the blockchain, and this means that protocol changes do not establish an *entirely* new chain of blocks.<sup>40</sup> Instead, protocol changes produce something like a break in the sequence of the blockchain: Prior to a protocol change, the blockchain is shared, but after the change, old and new protocols construct different “branches” from this common “trunk” (see Figure 1). In the parlance of cryptocurrencies, each competing path is a *fork* of the blockchain, and to initiate such a split is known as *forking*.<sup>41</sup>

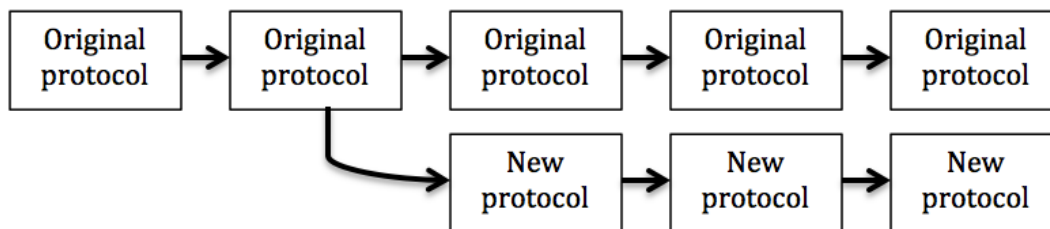


Figure 1: A blockchain fork

It is worth emphasizing that while forking a cryptocurrency can be accomplished by anyone with the technical skills necessary to modify cryptocurrency software—as I noted in the previous chapter, this is the rhetorical cover offered by FOSS development to justify

---

<sup>40</sup> The sole exception to this would be a protocol change that targets the very first block in a blockchain, since all subsequent blocks—that is, all blocks in the chain—would then be altered.

<sup>41</sup> Franco, *Understanding Bitcoin*, 108.

Bitcoin's de facto centralization of development—forking is nevertheless bound up with all of the political concerns introduced by blockchain procedural rhetoric: For Bitcoin, Ethereum, and similar blockchain-based currencies, to implement a blockchain fork is to politically restructure a given currency's individualist collective. Indeed, in this sense blockchain forks are moments of political rupture, momentous events in which one collective becomes two, as the previous chapter's case of Bitcoin Cash demonstrated. But because blockchain forks are not only technological matters, but political matters as well, every fork requires *justification*: If the person implementing a fork wants others to adopt the new branch of the blockchain—that is, if the person implementing the fork wants it to be *useful*—then he or she must argue for the superiority of the new branch over the old branch—and by extension, for the superiority of the new collective over the old one.

As I showed in the last chapter, these arguments can be made on technical grounds, or by appealing to some authority figure (e.g., Nakamoto's vision). For the purposes of the present chapter, however, the point to emphasize is the more foundational rhetorical dynamic that emerges out of such forks: *Old and new branches of a blockchain fork do not encounter the same rhetorical situation.*<sup>42</sup> More specifically, old and new branches each face a different rhetorical exigence. As defined by rhetorical scholar Lloyd Bitzer, a rhetorical exigence is “an imperfection marked by urgency; it is a defect, and obstacle, something waiting to be done, a thing which is other than it should be.”<sup>43</sup> In the context of blockchain forking, the rhetorical “imperfection marked by urgency” is the division of network

---

<sup>42</sup> Lloyd F. Bitzer, “The Rhetorical Situation,” in *Contemporary Rhetorical Theory: A Reader*, ed. John Louis Lucaites, Celeste Michelle Condit, and Sally Caudill (New York: Guilford Press, 1999), 217–25.

<sup>43</sup> *Ibid.*, 221.

participants between different branches of the fork, and this exigence can be addressed by persuading participants to choose one branch over another. But crucially, the work required of participants in selecting a new branch of a blockchain fork is not the same as that which is required by selecting an old branch. Choosing to follow a *new* blockchain fork, for instance, requires an active choice on the part of users of blockchain software. Users must be convinced to update their software in accordance with the new protocol; choosing a new fork is an *opt-in* process. By contrast, sticking with the unchanged protocol (and by extension, the “original” branch of the blockchain) requires no justification at all, precisely because it requires no action; the old branch is simply the status quo. Even though a single fork produces two blockchain branches, it is only the new branch that faces the more rhetorically difficult task of convincing users to take action.

One more point about blockchain forks should be made before returning to the case of The DAO: the distinction between soft and hard forks. Thus far, I have discussed changes to protocol as if all changes result in immediate excommunication from the existing network, but there is a bit more nuance to the matter than this—and this nuance is relevant to the Ethereum community’s response to the attack on The DAO. The forks I have discussed so far, such as the split of Bitcoin Cash from Bitcoin Core, are “hard” forks. These are changes to protocol so substantial that old protocol versions completely reject the blocks that new protocol versions generate; the new blocks are *not* backwards compatible with the old protocol.<sup>44</sup> Hard forks represent total incompatibility between protocols—and as such, such forks are also the most rhetorically and politically interesting, since each

---

<sup>44</sup> Amy Castor, “A Short Guide to Bitcoin Forks,” CoinDesk, March 27, 2017, <https://www.coindesk.com/short-guide-bitcoin-forks-explained/>.

constitutes a new, distinct monetary *polis*. But it is also possible to implement protocol changes that maintain limited backwards compatibility between old and new versions of the protocol. For example, a protocol change that *reduced* block sizes from 1 MB to 500 k would still be compatible with older versions of the protocol, since 500 k is smaller than the cap of 1 MB.<sup>45</sup> However, this compatibility only goes one way, since additional blocks generated by the old protocol may be larger than 500 k, and would thus be rejected by the new protocol. In other words, these new protocols produce blocks that are intelligible to and accepted by the rest of the network, and thus are only “soft” forks, in the sense that *some* protocol change has been implemented, but not one that entirely cuts ties to the old protocol and forms an new collective.

#### *Responses to the attack on The DAO*

With this background established, we can return to the three options considered by the Ethereum community as responses to the attack on The DAO: A soft fork, a hard fork, or nothing. The first of these three proposals was announced by Vitalik Buterin in his initial public response to the attack on The DAO:

A software fork has been proposed, (with NO ROLLBACK; no transactions or blocks will be “reversed”) which will make any transactions that make any calls/callcodes/delegatecalls that reduce the balance of an account with code hash 0x7278d050619a624f84f51987149ddb439cdaadfba5966f7cfaea7ad44340a4ba (i.e. the DAO and children) lead to the transaction (not just the call, the transaction) being invalid, starting from block 1760000 (precise block number subject to change up until the point the code is released), preventing the ether from being withdrawn by the attacker past the 27-day window.<sup>46</sup>

---

<sup>45</sup> Ibid.

<sup>46</sup> Buterin, “CRITICAL UPDATE Re: DAO Vulnerability.”

In less technical terms, this soft fork proposal would essentially blacklist the funds stolen from The DAO. By updating the Ethereum protocol, the Ethereum community could collectively target the funds of the child DAO, and could designate any movement of those funds *after* the child DAO's initial funding period (i.e., after the child DAO's funds "unlocked") as invalid transactions. Implementing this soft fork would not *reverse* the theft from The DAO, and would not permanently alter the functioning of all other ether associated with other accounts throughout the network, but it would ensure that the attacker would never be able to move or make use of the stolen ether. Consequently, advocates of a soft fork justified the proposal not so much as a final remedy to the attack on The DAO, but rather as a temporary fix to buy the community time to debate other solutions. As Buterin argued in his initial statement, implementing the soft fork would "provide plenty of time for discussion of potential further steps including to give token holders the ability to recover their ether."<sup>47</sup>

And as this justification indicates, the Ethereum community was already thinking about steps more drastic than a soft fork, and even as Buterin announced the soft fork proposal, the community began to debate the possibility of hard forking the Ethereum blockchain. This proposal would go a step further than the soft fork: Rather than simply isolating the stolen ether, as a soft fork would do, a hard fork would actually reverse the attacker's transaction of ether from The DAO to the child DAO.<sup>48</sup> In essence, this hard fork

---

<sup>47</sup> Ibid.

<sup>48</sup> Stephan Tual, "A Fork in the Road," *Stephan Tual* (blog), June 18, 2016, <https://medium.com/@stephantual/a-fork-in-the-road-c3c267b9ff31#.czj4ma1q7>.

would begin an alternate timeline of transactions in the Ethereum blockchain, beginning just one block earlier than the transaction that constituted the attacker's theft from The DAO. With funds "returned"—or rather, with those funds not stolen in the first place—participants in The DAO could collectively make use of another, simpler smart contract that would return The DAO's funds to investors.<sup>49</sup> Notably, this hard fork proposal was justified not in terms of pragmatic considerations, but rather in terms of the *rights* of participants in The DAO. As Ethereum developer Stephan Tual argued, implementing a hard fork would mean that "all the funds put in by the DAO Token Holders will make their way back to their *rightful owners*, ready to be used towards new, exciting Ethereum projects."<sup>50</sup>

Both the soft and hard fork proposals spurred debate throughout the Ethereum community, but as I noted previously, such forks were not the only options under consideration, and "do nothing" was treated as an equally valid option by a significant number of those involved in the forking debate. While many in the Ethereum community were supportive of some kind of fork, even if it only served as a precursor to some other solution after the child DAO's initial funding window expired, others worried about the apparent conflict between the purpose of smart contracts and DAOs—which are intended to be subject only to their own code, and thus entirely self-governing—and intervention in a particular smart contract by the broader Ethereum community. "If we fork because of a faulty contract," one user asked in a Reddit thread that served as the locus of the Ethereum community's response to Buterin's soft fork proposal, "how often are we going to fork in

---

<sup>49</sup> Ibid.

<sup>50</sup> Ibid. Italics added.

the future?”<sup>51</sup> Others questioned the fork proposals through comparisons to the “too big to fail” institutions of the 2008 financial crisis:

This exposed one of many DAO flaws and is a lesson learned to greedy investors that there are risks involved. If we bail out stupid investment behavior like we did with big banks taking stupid exposure risks, we risk a moral hazard because we are implicitly [sic] giving insurance to idiotic behavior. [Y]ou don't get to say, we are not governed by a jurisdiction and existing laws and then go back and try to use centralized policies when being decentralized is inconvenient.<sup>52</sup>

Still others, in a conceptually similar but more sarcastic vein, requested their own Ethereum “bailout”: “I made a bad contract in the first days [Ethereum] was online and lost 2K [ether] with it, can I also get it back? Thanks!”<sup>53</sup>

Incredibly, this debate over forking Ethereum even expanded to include participation *from the attacker responsible for the theft*—or at least from someone purporting to be the attacker. The day following the announcement of the soft fork proposal, an individual or group using the pseudonym “The Attacker”<sup>54</sup> posted an open letter, addressed “to the DAO and the Ethereum community,” on the text storage site

---

<sup>51</sup> gergi, “If We Fork Because of a Faulty Contract,” *Reddit*, June 17, 2016, [https://www.reddit.com/r/ethereum/comments/4oiqj7/critical\\_update\\_re\\_dao\\_vulnerability/](https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/).

<sup>52</sup> jedigras, “This Was a Contractually Allowed Result,” *Reddit*, June 18, 2016, [https://www.reddit.com/r/ethereum/comments/4oiqj7/critical\\_update\\_re\\_dao\\_vulnerability/](https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/).

<sup>53</sup> apoefjmqdsfls, “I Made a Bad Contract in the First Days ETH Was Online,” *Reddit*, June 17, 2016, [https://www.reddit.com/r/ethereum/comments/4oiqj7/critical\\_update\\_re\\_dao\\_vulnerability/](https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/).

<sup>54</sup> To distinguish between the persona constructed by this open letter and the person or persons actually responsible for the theft from The DAO, for the remainder of this chapter I capitalize the former (The Attacker) but not the latter (the attacker).

Pastebin.com.<sup>55</sup> The letter opens by explaining and justifying The Attacker's involvement with the DAO:

I have carefully examined the code of The DAO and decided to participate after finding the feature where splitting [i.e., creating a child DAO] is rewarded with additional ether. I have made use of this feature and have rightfully claimed 3,641,694 ether, and would like to thank the DAO for this reward. It is my understanding that the DAO code contains this feature to promote decentralization and encourage the creation of "child DAOs".<sup>56</sup>

Notably, in this message The Attacker characterizes The DAO's flaws in positive terms: The exploit used in the attack is a "feature," and the amount of ether transferred to the child DAO is a "reward" for using this feature. This characterization carries through into the next paragraph, in which The Attacker claims to be "disappointed by those who are characterizing the use of this intentional feature as 'theft.'"<sup>57</sup> Such an interpretation of the ether transfer is unfounded, The Attacker argues, not only because the theft is not recognized as such by any relevant legal jurisdiction—The Attacker claims that "my law firm has advised me that my action is fully compliant with United States criminal and tort law"<sup>58</sup>—but also because The Attacker was only "making use of this explicitly coded feature as per the smart contract terms."<sup>59</sup> To support this claim, The Attacker extensively quotes The DAO's own documentation:

---

<sup>55</sup> The Attacker, "An Open Letter," Pastebin.com, June 18, 2016, <https://pastebin.com/CcGUBgDG>.

<sup>56</sup> Ibid.

<sup>57</sup> Ibid.

<sup>58</sup> Ibid.

<sup>59</sup> Ibid.

The terms of The DAO Creation are set forth in the smart contract code existing on the Ethereum blockchain at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413. Nothing in this explanation of terms or in any other document or communication may modify or add any additional obligations or guarantees beyond those set forth in The DAO's code. *Any and all explanatory terms or descriptions are merely offered for educational purposes and do not supercede or modify the express terms of The DAO's code set forth on the blockchain; to the extent you believe there to be any conflict or discrepancy between the descriptions offered here and the functionality of The DAO's code at 0xbb9bc244d798123fde783fcc1c72d3bb8c189413, The DAO's code controls and sets forth all terms of The DAO Creation.*<sup>60</sup>

In other words, by The DAO's own account, the "real" agreement of The DAO is not found in The DAO's documentation or in explanations of how The DAO is *supposed* to work; rather, *the agreement is the code itself*, inclusive of all "features" that might be construed, even reasonably so, by others to be "bugs." And if this is the case, The Attacker points out, then "[a] soft or hard fork would amount to seizure of [The Attacker's] legitimate and rightful ether, claimed legally through the terms of a smart contract."<sup>61</sup> Furthermore, such a seizure of "legitimate" ether, The Attacker argues, would have drastic consequences:

Such fork would permanently and irrevocably ruin all confidence in not only Ethereum but also the in the field of smart contracts and blockchain technology. Many large Ethereum holders will dump their ether, and developers, researchers, and companies will leave Ethereum. Make no mistake: any fork, soft or hard, will further damage Ethereum and destroy its reputation and appeal.<sup>62</sup>

According to The Attacker, initiating a soft or hard fork would be the *real* theft here, and such a theft should be understood as a significant setback to the development of smart

---

<sup>60</sup> Quoted in *ibid.* Italics added.

<sup>61</sup> *Ibid.*

<sup>62</sup> *Ibid.*

contracts. Following this grim prediction, The Attacker ends with a more pointed threat: In the face of this potential “theft,” The Attacker “reserve[s] all rights to take any and all legal action against any accomplices of illegitimate theft, freezing, or seizure of my legitimate ether.”<sup>63</sup>

This, then, was the argument for the “do nothing” response to the attack on The DAO: If the point of smart contracts, including DAOs, is to substitute the politics of a community with the procedures of software, what grounds did the Ethereum community have to intervene in the contract of The DAO? To be sure, the theft of funds from The DAO showed that nearly all of The DAO’s funders—thousands of individuals in total—interpreted the organization, as a smart contract, in an inaccurate manner. But the point of smart contracts, just like their vending machine predecessors, *is to render such (human) interpretations irrelevant*. Indeed, as far as the terms (i.e., the code) of The DAO are concerned, The Attacker is clearly in the right: The theft of the funds was not a theft at all, since anything that *can* be done with The DAO is by definition part of those terms. Theft, by this definition, is an impossible absurdity.

There are, in other words, two different senses of *rights* at work in this debate. On the one hand, advocates of a hard fork focused on the rights of The DAO’s investors—in Ethereum developer Stephen Tual’s words, these investors are “the rightful owners” of The DAO’s funds<sup>64</sup>—and this sense of “rights” is clearly one grounded in the shared expectations and understanding of The DAO’s community, and of Ethereum community more generally. That is to say, the investors can only be understood as “rightful owners” if

---

<sup>63</sup> Ibid.

<sup>64</sup> Tual, “A Fork in the Road.”

the source of these rights is the *community itself*. But The Attacker also invokes the language of rights (the stolen funds are The Attacker's "legitimate and rightful ether"), though he or she frames these rights in terms of the *code* of The DAO.<sup>65</sup> For The Attacker, "rightful ownership" is determined not by participants in The DAO, or by the Ethereum community at large, but rather by the "text" of The DAO's smart contract. In short, for the former line of argument, rights are the product of an implicitly articulated *social* contract; for the latter, rights are the product of an explicitly articulated "natural" contract, built on the cryptographic foundation of the blockchain, and beyond the reach of the social.

And in this latter argument, we can see the legacy of digital metallism in full force, as a kind of rhetorical trap for the Ethereum community. On one hand, the exploit of The DAO was clearly a theft in the ordinary sense of the term, and was experienced as such by participants in The DAO, and by the broader Ethereum community—after all, if the theft really *was* part of the expected functioning of The DAO, it would hardly draw the same attention, debate, and radical solutions. On the other hand, the point of a blockchain is to create an immutable transaction record, and the point of smart contracts and DAOs is to extend this unalterable history—and the community to which it corresponds—into ever more elaborate yet always "apolitical" structures. To fork the Ethereum blockchain in order to reverse a transaction that resulted from a lack of investor due diligence would represent a complete reversal of this rhetorical inheritance from digital metallism—that is, of the attempt to construct an apolitical *polis*.

This deep opposition between the rhetorical foundation of The DAO and the fork solutions to the attack makes the next development in The DAO's story all the more

---

<sup>65</sup> The Attacker, "An Open Letter."

remarkable: The Ethereum community *did* in fact implement a soft fork (i.e., to ensure that the attacker would not be able to move the stolen ether after the child DAO unlocked)<sup>66</sup> and later, a hard fork as well (i.e., to “undo” the attacker’s initial transaction).<sup>67</sup> Despite the clear contradiction between implementing these forks and the purpose and rhetoric of smart contracts, a majority of the Ethereum community chose to alter the immutable Ethereum blockchain, to save the unwise investors, and to adopt the new protocol introduced by the hard fork. Yet like the case of Bitcoin Cash, community consensus in these forks was not unanimous. Particularly in the context of the hard fork, some members of the Ethereum community continued to use the older versions of the Ethereum protocol, and consequently, they continued the “old” branch of the Ethereum fork—now renamed “Ethereum Classic” to distinguish it from the new Ethereum branch.<sup>68</sup> Today, ether from both branches of the Ethereum hard fork are traded side by side on cryptocurrency exchanges—though crucially, the valuation of the two currencies is not equal, and Ethereum Classic trades at a fraction of the price of the “new” Ethereum.<sup>69</sup> Still, in these

---

<sup>66</sup> Péter Szilágyi, “DAO Wars: Your Voice on the Soft-Fork Dilemma,” *Ethereum Blog* (blog), June 24, 2016, <https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma/>.

<sup>67</sup> Vitalik Buterin, “Hard Fork Completed,” *Ethereum Blog* (blog), July 20, 2016, <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>.

<sup>68</sup> Pete Rizzo, “Ethereum Hard Fork Creates Competing Currencies,” *CoinDesk*, July 24, 2016, <https://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/>; Aaron van Wirdum, “Rejecting Today’s Hard Fork, the Ethereum Classic Project Continues on the Original Chain: Here’s Why,” *Bitcoin Magazine*, July 20, 2016, <https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808/>.

<sup>69</sup> “Top 100 Cryptocurrencies by Market Capitalization,” *CoinMarketCap*, 2018, <https://coinmarketcap.com/>.

competing timelines of transactions, The DAO's funds are *both* returned to investors *and* hoarded by the attacker, and the sanctity of smart contracts is both abandoned and preserved.

Nevertheless, individual members of the Ethereum community had to choose between these two branches: stick with Ethereum Classic, or move on to the new Ethereum. And as with the case of the split of Bitcoin Cash from Bitcoin Core, the rhetorically significant aspect of this choice is not so much the specifics of each particular branch of the fork, but rather the way that each branch *constructs its relationship to the other*. For example, the landing page of the Ethereum Classic website makes clear that, at least for advocates of Ethereum Classic, the choice between Ethereum and Ethereum Classic represents not only a disagreement about the specifics of The DAO case, but also a much deeper disagreement about what blockchain technology should be:

We [i.e., Ethereum Classic] believe the core value proposition of any blockchain is immutability; valid transactions can never be erased or forgotten. Individuals interacting on Ethereum Classic are governed by this reality: Code is Law. [...] By entering into contracts on Ethereum Classic, you can be certain that the network remains neutral. The outcome of transactions will be dictated by code you voluntarily interact with. Unless explicitly defined by the contract code, there are no reversals, no undos, no opt-outs. Transactions are final; applications are unstoppable.<sup>70</sup>

Here can be seen the familiar rhetorical legacy of digital metallism: the value of the blockchain derives from its immutability, from its place beyond the reach of human intervention. This technology then becomes the basis for constructing collectives of individuals, albeit collectives that cannot alter their own terms through collaborative

---

<sup>70</sup> "Ethereum Classic," Ethereum Classic, 2018, <https://ethereumclassic.github.io/>.

effort—and in such collectives, smart contracts, DAOs, and the like are “unstoppable,” freed from any danger of community coercion. In this figuring of blockchain technologies as circumventions of the social and the political, digital metallism persists beyond the explicit commodity money rhetoric of the early Bitcoin community—and crucially, Ethereum Classic draws on this rhetorical legacy to advance an argument about its own relationship to Ethereum, since Classic’s commitment to blockchain immutability stands in contrast to Ethereum’s “mutable” branch of the hard fork.

The website for Ethereum, by contrast, makes absolutely no mention of Ethereum Classic.<sup>71</sup> No justification is offered for why this new branch of the Ethereum protocol should be considered the “true” Ethereum, and no arguments are presented regarding Ethereum’s stance on the immutability—or rather, the occasional mutability—of the blockchain. No attempt is made to respond to or preempt the arguments for Ethereum Classic. The issue simply is not part of the Ethereum website’s discourse.

And at first glance, this contrast may not appear to be terribly significant. After all, the majority of the Ethereum community endorsed the hard fork of the Ethereum blockchain, and only a minority continued mining the Ethereum Classic branch, so why should Ethereum need to justify its own existence? But this contrast becomes a bit more puzzling when viewed in conjunction with a point made earlier in this chapter: namely, *that old and new branches of a blockchain fork do not face the same rhetorical exigence*. Given that old branches are the status quo (an exigence that does not entail persuading users to actively choose a branch) and that new branches require users to actively *opt in*, one would expect the rhetorical efforts of Ethereum and Ethereum Classic to be exactly

---

<sup>71</sup> “Ethereum Project.”

reversed: It should be Ethereum that expends so much effort in justifying its own existence and convincing users to join its branch, while Ethereum Classic, as the blockchain status quo, should not need to make this case. And yet even the *names* of the two branches upend this expectation, since it is the status quo that was renamed “Ethereum Classic,” while the *new* protocol version adopted the *old* name of Ethereum. So how should we make sense of this unexpected rhetorical reversal?

### *The rhetoric of blockchain forks*

To answer this question, it is necessary to return to the theft from The DAO. In the previous chapter, I argued that the attempt to foreclose politics with protocol merely heightens the political stakes of developing the protocol, and to be sure, a similar dynamic is present in The DAO: The entire debate over forking the Ethereum blockchain is the fallout of restricting the space of community politics to the boundaries of a smart contract. But the case of The DAO also sheds light on an *additional* rhetorical side effect of the attempt to foreclose the political: the role that *rhetorical identity* plays in the construction of cryptocurrencies. More specifically, The DAO shows the importance of *how a community understands itself* in relation to a particular protocol or smart contract, and the inevitability of this understanding diverging from the actual functioning of that protocol or contract as that protocol or contract produces an individualist collective. Because every attempt to build an apolitical, individualist collective—at a monetary or contractual or organizational level—still involves humans, who experience such collectives in terms of representation, these attempts are always shadowed by the very slippery, uncertain, and ambiguous processes of representation that they try to escape. As an owner of bitcoins, for example, I

may belong to a community that has procedurally displaced its politics onto the BIP system, but I nevertheless experience the “Bitcoin community” in representational terms—that is, as composed of individuals, groups, discourses, and so on. But the blockchain—and the community that it produces—is *not* representational, and consequently my sense of what the community *means* will always be inadequate to capture the entirety of the blockchain as a non-representational entity. In other words, there is always a minimal gap between the code and human understanding of it, between the blockchain community as it is procedurally constituted and the blockchain community as members imagine it to be. Indeed, this gap is the core of digital metallism’s rhetorical legacy: Despite the certainty that it purports to provide, an individualist collective—whether grounded on gold, cryptography, or smart contracts—always has the potential to misalign with members’ conceptions of it.

That said, even individualist collectives are constructed things, built by humans, so in places where protocol and human understanding of protocol diverge, it is clear that humans will attempt to “correct” the protocol—and the elimination of “bugs” is, of course, a key part of software development. But crucially, such correction is premised on the protocol being “wrong” in some way—that is, some functioning of the protocol is understood to be a bug, flaw, or glitch. Yet precisely because different individuals may experience the gap between protocol and representations of it in different ways, instances of the protocol functioning “incorrectly” *are not self-evident*. As I have argued elsewhere, it takes rhetorical *work* to designate elements of a technology as “errors,” “bugs,” or

“failures”; users must be *persuaded*, either preemptively or after the fact, that some particular technological function was unintended or inappropriate.<sup>72</sup>

This dynamic can be clearly seen in the case of The DAO. Even though the theft was, in one sense, self-evidently an inappropriate transaction—one that the community immediately recognized as such—in another sense quite consistent with the overall project of Ethereum, smart contracts, and The DAO, it was not inappropriate at all. And *this* is the crucial point from a rhetorical perspective: How is it that the transaction was, for the majority of the Ethereum community, self-evident as a theft? Such self-evidence makes no sense from the perspective of The DAO as a smart contract. Indeed, it only makes sense *if members of the Ethereum community already have some sense of Ethereum’s rhetorical identity*—that is, an understanding of Ethereum separate from the technology or the currency, against which the “inappropriate” sequence of transactions can be compared. This identity, apart from any particular individualist collective, is an essential rhetorical component in the characterization of the attack on The DAO as a “theft,” and is a key factor in explaining how the Ethereum community could coordinate the shift of valuation (as indicated by divergent prices) from Ethereum Classic to Ethereum; only by referencing this sense of what The DAO and Ethereum *should* be can we make sense of the responses to what they *were*.

The previous chapter introduced a case in which Bitcoin faced an “external” challenger in the form of Bitcoin Cash: In the split of Bitcoin Cash from Bitcoin Core, the *new* protocol was a break from the rhetorical identity of Bitcoin as a currency, albeit a

---

<sup>72</sup> Matthew Bellinger, “The Rhetoric of Error in Digital Media,” *Computational Culture* 5 (2016), <http://computationalculture.net/article/the-rhetoric-of-error-in-digital-media-2>.

break that was framed in terms of pursuing Nakamoto's original vision. But the case of the Ethereum fork shows that this dynamic can emerge not only from challenges external to a currency—that is, from a competitor who introduces a competing blockchain fork—but can also emerge *internal* to a currency, too. A community can discover that the protocol diverges in significant ways from the community's conception of that protocol, and requires currency forking to maintain this vision. But in such instances, the community's sense of the currency's identity—and in particular, the extent to which this identity is consistent and coherent—plays a vital role in navigating the politics of the fork. Only with a clear sense of what the currency and community *should* be can a currency coordinate the movement of its network—and by extension, maintain its perceived value—along a particular branch of a blockchain fork.

In sum, there is yet another rhetorical dynamic at play in blockchain forks, a dynamic that emerges, like the debates over protocol development covered in the previous chapter, from the pairing of digital metallism with procedural rhetoric of blockchain technology. Even when explicit commodity rhetoric falls by the wayside, the rhetorical legacy of digital metallism persists in the assumption that the social and the political can be circumvented through the production of an individualist collective—and this assumption, I have shown, is integral to applications of blockchain technology beyond Bitcoin. But as the case of The DAO suggests, a blockchain's community exceeds its individualist collective; every collective is ultimately composed of humans, who share understandings of their community and the technology that underpins it. And because these understandings are representational, there is always a potential gap between the non-representation of the blockchain and community representations of that non-representation—yet crucially,

different members of a collective can experience this gap differently. To close these gaps requires altering the foundation of the collective (i.e., the protocol), but since such alterations require *collective* action (e.g., individuals choosing a new protocol version), they can only be executed to the extent that a currency's community maintains a stable, coherent identity, an identity that can be used as a reference point for modifications of the protocol. Thus, the stability of a given cryptocurrency—and by extension, its ability to function as *money*—is tied to the maintenance of a stable, coherent identity that exists *apart* from the currency's procedurally produced individualist collective. In this way, the dream of digital metallism, brought to life in blockchain technology, ends up amplifying the importance the very thing it seeks to escape: the communal.

## Conclusion: The Future of Cryptocurrencies

“Money defines each of us,” writes anthropologist Keith Hart, “by articulating the relationship between individuals and their communities.”<sup>1</sup> Every monetary transaction simultaneously presupposes and reinforces this relationship: To offer a particular currency as payment is to express faith in a monetary community—a belief in the *social* that exceeds the currency’s utility to the individual—and every acceptance of payment presents more evidence to support this belief. And at its strongest and most influential, this strange faith, affirmed and rededicated in countless transactions, appears so unremarkable, so a part of the “natural” order of things, that it fades into the blurry, taken-for-granted backdrop of everyday life. Money defines us, shapes our relationships to our communities, to the extent that it appears to be a certainty, an inevitability, an inescapable mediator between self and society.

And if money defines us, then a new form of money presents the opportunity for redefining ourselves. For early members of the Bitcoin community, this was the promise of a new, digital currency. Bitcoin was a chance to reconfigure the mediation of individual and community, a chance to define money rather than be defined by it. But because money works best when it is unquestioned, self-evident, and taken for granted, fulfillment of this promise presented Bitcoin advocates with a rhetorical puzzle: Constructing new money required obscuring the work of construction. To reconfigure the relationship between

---

<sup>1</sup> Keith Hart, “The Financial Crisis and the End of All-Purpose Money,” *Economic Sociology: The European Electronic Newsletter* 12, no. 2 (2011): 5.

individuals and their communities, Bitcoin needed to be *made* self-evident as a form of money.

To meet this rhetorical challenge, members of the Bitcoin community drew upon a well-established tradition of monetary rhetoric: the grounding of money's value in natural commodities. Though the fit was at times awkward, the early Bitcoin community adopted commodity money rhetoric to Bitcoin by figuring the technology of Bitcoin as the "natural" ground of Bitcoin's value. Crucially, this reworking of commodity money rhetoric, which at its rhetorical core claims to provide an escape from the uncertainties and ambiguities of social and political life, complemented the procedural rhetoric of Bitcoin's protocol. Digital metallism *worked* as a rhetorical strategy not only because it drew from the same intellectual tradition that informed the politics of the early Bitcoin community, but also because it seemed to accurately describe how Bitcoin functioned as a monetary technology. Bitcoin, it seemed, was the digital equivalent of gold: an articulation of the relationship between the individual and the community that placed full weight on the individual, and that consequently offered protection from any communal "interference." Bitcoin, it seemed, was a monetary *polis* without the political.

This productive pairing of digital metallism and Bitcoin's procedural rhetoric, originally formed as a response to the question of Bitcoin's monetary value, had far reaching implications for the construction of Bitcoin and related cryptocurrencies as economic assemblages, and though explicit invocations of digital metallism has subsided over time, the rhetorical core of this trope (i.e., the foreclosure of politics) continues to influence Bitcoin and its heirs. This influence can be seen in two areas. First, there are the heightened stakes of cryptocurrency development—now the key means of cryptocurrency

communities' political self-engagement—and the rhetorically diverse responses to these stakes. Because the procedural rhetoric of blockchain technology produces a collective in which no communal action is possible—or at least, such actions are impossible *within* the blockchain's procedural bounds—the construction of the “rules of the game” takes on paramount political importance for cryptocurrencies, and the processes governing the development of a given cryptocurrency's protocol become the processes governing the cryptocurrency more generally. Furthermore, because these processes (e.g., the BIP system) are themselves constructed to facilitate the development of technology rather than to manage the politics of a monetary community, questions of development inspire not only technical arguments, but also the creation of new rhetorical grounds on which developmental decisions can be made. Tropes such as Nakamoto's “original vision,” which challenge the legitimacy of developmental processes that privilege technical expertise, are the unexpected byproduct of the pairing of digital metallism and the procedural rhetoric of the blockchain.

The second area in which the legacy of digital metallism can be seen is in the execution and coordination of blockchain forks. As a competition between two rival protocol versions, a fork also presents the choice between two competing individualist collectives—and in doing so, such forks highlight the importance of a given cryptocurrency's community as it extends *beyond* the procedural boundaries of protocol. When the protocol itself is insufficient to determine the “rules of the game,” because the choice at hand is between multiple versions of the rules, cryptocurrencies' communal identities come to the fore as a complement to blockchain-produced collectives. In other words, blockchain forks are moments when a community's sense of what a monetary

technology *should be* overrides its procedural constitution. Here again is an unexpected consequence of the attempt to foreclose politics: Making political intervention *within* protocol impossible heightens the political importance of community identity when choosing one protocol version over another. In short, the attempt to escape politics only pushes politics into new arenas, and makes new dimensions of cryptocurrencies rhetorically relevant for their construction as economic assemblages.

Understanding this cascade of consequences throughout the rhetorical ecology of Bitcoin places the digital currency's rise in new light. Tracing the legacy of digital metallism shows that the discussions and debates of the Bitcoin community cannot be understood as separate from the construction of Bitcoin as a monetary technology, and also shows that Bitcoin's attempt to foreclose politics—as self-evidently fruitless as it may appear to skeptical observers—should be taken seriously as a rhetorical component of this construction. Furthermore, it shows that attending to the rhetorical fallout of attempts to *make money* can be fruitful not only for understanding Bitcoin, but also for understanding the growing number of attempts to extend the logic of digital metallism into ever more elaborate configurations (e.g., smart contracts, DAOs).

But this cascade of rhetorical consequences is significant not only for the story of Bitcoin's development; close attention to the legacy of digital metallism also suggests that certain rhetorical dynamics will play a significant role in the future of cryptocurrencies more generally, and that scholars in the burgeoning field of digital currency studies would be wise to attend to these dynamics. The legacy of digital metallism is the dream of escaping the work of maintaining community—the work of political engagement, and the work of shaping communal identity through discourse. But as I have shown in this

dissertation, this dream of escaping politics is not a reality, not even when the dream is supported by complex and ingenious combinations of cryptography, software, and economic incentives. Even individualist collectives ultimately require—though through somewhat indirect means—the work of building, preserving, and sometimes modifying community. The decentralized nature of cryptocurrencies makes this work particularly difficult—for Bitcoin, at least, there is no obvious center from which governing structures or definitive identities may emerge—and the structures currently bearing this political burden (e.g., the BIP system) seem poorly suited to the task. But if cryptocurrencies are to have a future, they will need to develop new structures that purposefully and decisively manage cryptocurrencies' governance and identities. This is not to say that cryptocurrencies will need to replicate the exact same structures that perform this work in the context of fiat currencies (e.g., banks, the state); if anything, the development of cryptocurrencies presents not the opportunity to avoid politics altogether, but rather the chance to construct more robust and accountable institutions of monetary governance. But if cryptocurrency communities do not seize this opportunity, and if the displacement of politics and its ensuing rhetorical consequences are not addressed by these communities directly, then it is difficult to see how these monetary technologies can continue to build on the growth of the last decade. In other words, if Bitcoin—or one of its successors—is to meaningfully rearticulate money's relationship between individuals and their communities, then its advocates will need to recognize and take seriously this point: The construction of money is the construction of community.

### Bibliography

"About." Bitcoin Cash, 2018. <https://www.bitcoincash.org/#about>.

Agrawal, Neeraj K. "Satoshi's Original Vision." Tweet. Twitter, April 12, 2018.

<https://twitter.com/NeerajKA/status/984606680871833601>.

Alissa. "Satoshi Nakamoto - The God of Crypto." *CryptoCurrency Times*, November 2, 2017.

<http://cryptotimes.org/cryptocurrency/satoshi-nakamoto-god-crypto/>.

Amato, Massimo, Luigi Doria, and Luca Fantacci, eds. *Money and Calculation: Economic and Sociological Perspectives*. Bocconi on Management Series. Hampshire ; New York: Palgrave Macmillan, 2010.

andreasma. "Why I Declined to 'Verify' SN's Identity Two Weeks Ago." *Reddit*, May 2, 2016.

[https://www.reddit.com/r/Bitcoin/comments/4hj1xu/why\\_i\\_declined\\_to\\_verify\\_sn\\_s\\_identity\\_two\\_weeks/](https://www.reddit.com/r/Bitcoin/comments/4hj1xu/why_i_declined_to_verify_sn_s_identity_two_weeks/).

Andresen, Gavin. "BIP 11: M-of-N Standard Transactions." GitHub, October 18, 2011.

<https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki>.

———. "Satoshi." Gavin Andresen, May 2, 2016. <http://gavinandresen.ninja/satoshi>.

anon13488. "I Believe in Bitcoin." *Reddit*, November 29, 2013.

[https://www.reddit.com/r/Bitcoin/comments/1rq8ua/i\\_believe\\_in\\_bitcoin/](https://www.reddit.com/r/Bitcoin/comments/1rq8ua/i_believe_in_bitcoin/).

Antonopoulos, Andreas M. *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*.

Sebastopol, CA: O'Reilly Media, 2015.

Antonopoulos, Andreas M. *The Internet of Money: A Collection of Talks*. Merkle Bloom, 2016.

apoefjmqdsfls. "I Made a Bad Contract in the First Days ETH Was Online." *Reddit*, June 17, 2016.

- [https://www.reddit.com/r/ethereum/comments/4oiqj7/critical\\_update\\_re\\_dao\\_vulnerability/](https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/).
- “Australian Craig Wright Claims to Be Bitcoin Creator.” BBC News, May 2, 2016.  
<http://www.bbc.com/news/technology-36168863>.
- Back, Adam. “Hashcash - A Denial of Service Counter-Measure,” August 1, 2002.  
<http://www.hashcash.org/papers/hashcash.pdf>.
- Barry, Andrew, and Don Slater, eds. *The Technological Economy*. London ; New York: Routledge, 2005.
- Bearman, Joshua. “Silk Road: The Untold Story.” Wired, May 23, 2015.  
<https://www.wired.com/2015/05/silk-road-untold-story/>.
- Bellinger, Matthew. “The Rhetoric of Error in Digital Media.” *Computational Culture* 5 (2016). <http://computationalculture.net/article/the-rhetoric-of-error-in-digital-media-2>.
- Bergstra, Jan A., and Peter Weijland. “Bitcoin: A Money-like Informational Commodity,” 2014. <https://arxiv.org/abs/1402.4778>.
- Biddle, Sam, and Andy Cush. “This Australian Says He and His Dead Friend Invented Bitcoin.” Gizmodo, December 8, 2015. <https://gizmodo.com/this-australian-says-he-and-his-dead-friend-invented-bi-1746958692>.
- Bijker, Wiebe E. *Of Bicycles, Bakelites, and Bulbs: Toward a Theory of Sociotechnical Change*. Cambridge, MA: MIT Press, 1995.
- Bijker, Wiebe E., Thomas P. Hughes, and Trevor J. Pinch, eds. *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. Cambridge, MA: The MIT Press, 1987.

“BIP Purpose and Guidelines.” GitHub, August 19, 2011.

<https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki>.

*Bips: Bitcoin Improvement Proposals*. Go. 2013. Reprint, Bitcoin, 2018.

<https://github.com/bitcoin/bips>.

“Bitcoin Network Capacity Analysis – Part 1: Macro Block Trends.” TradeBlock, July 3, 2015. <https://tradeblock.com/blog/bitcoin-network-capacity-analysis-part-1-macro-block-trends>.

“Bitcoin-Dev.” Accessed April 25, 2018. <https://www.mail-archive.com/bitcoin-dev@lists.linuxfoundation.org/>.

“Bitfinex.” Bitfinex. Accessed January 19, 2018. <https://www.bitfinex.com/>.

“Bitstamp.” Bitstamp. Accessed January 19, 2018. <https://www.bitstamp.net/>.

Bitzer, Lloyd F. “The Rhetorical Situation.” In *Contemporary Rhetorical Theory: A Reader*, edited by John Louis Lucaites, Celeste Michelle Condit, and Sally Caudill, 217–25. New York: Guilford Press, 1999.

Bogost, Ian. *Persuasive Games: The Expressive Power of Videogames*. Cambridge, MA: MIT Press, 2007.

Boldyrev, Ivan, and Ekaterina Svetlova, eds. *Enacting Dismal Science: New Perspectives on the Performativity of Economics*. Perspectives from Social Economics. New York: Palgrave Macmillan, 2016.

Brown, James J., Jr. *Ethical Programs: Hospitality and the Rhetorics of Software*. Ann Arbor, MI: University of Michigan Press, 2015.

- Brunton, Finn. "Heat Exchanges." In *MoneyLab Reader: An Intervention in Digital Economy*, edited by Geert Lovink, Nathaniel Tkacz, and Patricia de Vries, 158–72. Amsterdam: Institute of Network Cultures, 2015.
- . *Spam: A Shadow History of the Internet*. Infrastructures 4. Cambridge, MA: MIT Press, 2013.
- "BTCChina." BTCChina. Accessed January 19, 2018. <https://www.btcchina.com/>.
- Buterin, Vitalik. "CRITICAL UPDATE Re: DAO Vulnerability." *Ethereum Blog* (blog), June 17, 2016. <https://blog.ethereum.org/2016/06/17/critical-update-re-dao-vulnerability/>.
- . "Ethereum White Paper." GitHub, 2013. <https://github.com/ethereum/wiki/wiki/White-Paper>.
- . "Hard Fork Completed." *Ethereum Blog* (blog), July 20, 2016. <https://blog.ethereum.org/2016/07/20/hard-fork-completed/>.
- Caffyn, Grace. "What Is the Bitcoin Block Size Debate and Why Does It Matter?" CoinDesk, August 21, 2015. <https://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/>.
- Callon, Michel. "An Essay on Framing and Overflowing: Economic Externalities Revisited by Sociology." *The Sociological Review* 46, no. 1 (May 1998): 244–69. <https://doi.org/10.1111/j.1467-954X.1998.tb03477.x>.
- . "Economic Markets and the Rise of Interactive *Agencements*: From Prosthetic Agencies to Habilitated Agencies." In *Living in a Material World: Economic Sociology Meets Science and Technology Studies*, edited by Trevor Pinch and Richard Swedberg, 29–56. Inside Technology. Cambridge, Mass: MIT Press, 2008.

- , ed. *The Laws of the Markets*. Malden, MA: Blackwell, 1998.
- . “What Does It Mean to Say That Economics Is Performative?” In *Do Economists Make Markets? On the Performativity of Economics*, edited by Donald A. MacKenzie, Fabian Muniesa, and Lucia Siu, 311–57. Princeton: Princeton University Press, 2007.
- Callon, Michel, Andrew Barry, and Don Slater. “Technology, Politics, and the Market: An Interview with Michel Callon.” In *The Technological Economy*, edited by Andrew Barry and Don Slater, 101–21. London ; New York: Routledge, 2005.
- Callon, Michel, and Bruno Latour. “Unscrewing the Big Leviathan: How Actors Macro-Structure Reality and How Sociologists Help Them to Do So.” In *Advances in Social Theory and Methodology: Toward an Integration of Micro-and Macro-Sociologies*, edited by Katherine Knorr-Cetina and Aaron Victor Cicourel, 277–303. Routledge, 1981.
- Callon, Michel, Yuval Millo, and Fabian Muniesa, eds. *Market Devices*. Malden, MA: Blackwell, 2007.
- Callon, Michel, and Fabian Muniesa. “Peripheral Vision: Economic Markets as Calculative Collective Devices.” *Organization Studies* 26, no. 8 (August 2005): 1229–50. <https://doi.org/10.1177/0170840605056393>.
- Carruthers, Bruce G., and Sarah Babb. “The Color of Money and the Nature of Value: Greenbacks and Gold in Postbellum America.” *American Journal of Sociology* 101, no. 6 (May 1996): 1556–91. <https://doi.org/10.1086/230867>.
- Castor, Amy. “A Short Guide to Bitcoin Forks.” CoinDesk, March 27, 2017. <https://www.coindesk.com/short-guide-bitcoin-forks-explained/>.

Chaum, David. "Blind Signatures for Untraceable Payments." Santa Barbara, CA: University of California, 1982.

Chaum, David, Amos Fiat, and Moni Naor. "Untraceable Electronic Cash." In *Advances in Cryptology -- CRYPTO '88*, 319–27. Lecture Notes in Computer Science. Springer, 1988. [https://doi.org/10.1007/0-387-34799-2\\_25](https://doi.org/10.1007/0-387-34799-2_25).

chsados. "The One True God: Satoshi Nakamoto." Bitcointalk.org, October 22, 2013. <https://bitcointalk.org/index.php?topic=315953.0>.

"Church of Bitcoin," August 7, 2017. <https://www.churchofbitcoin.org/>.

Cohen, Herman. *The History of Speech Communication: The Emergence of a Discipline, 1914-1945*. Washington, DC: National Communication Association, 1994.

"Coinbase." Coinbase. Accessed January 19, 2018. <https://www.coinbase.com/>.

"CoinDesk." CoinDesk. Accessed October 4, 2017. <https://www.coindesk.com/>.

Coleman, E. Gabriella. *Coding Freedom: The Ethics and Aesthetics of Hacking*. Princeton: Princeton University Press, 2013.

Collins, Randall. "The Bankers. By Martin Mayer." *American Journal of Sociology* 85, no. 1 (July 1979): 190–94. <https://doi.org/10.1086/226983>.

"Craig Steven Wright Claims to Be Satoshi Nakamoto. Is He?" *The Economist*, May 2, 2016. <https://www.economist.com/news/briefings/21698061-craig-steven-wright-claims-be-satoshi-nakamoto-bitcoin>.

"CryptoCurrency Market Capitalizations." CoinMarketCap. Accessed July 3, 2017. <http://coinmarketcap.com/currencies/views/all/>.

Dai, Wei. "B-Money," 1998. <http://www.weidai.com/bmoney.txt>.

Dashjr, Luke. "BIP 2: BIP Process, Revised." GitHub, February 3, 2016.

<https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki>.

———. "BIP 145: Getblocktemplate Updates for Segregated Witness." GitHub, January 30,

2016. <https://github.com/bitcoin/bips/blob/master/bip-0145.mediawiki>.

Diedrich, Henning. *Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations*. Wildfire Publishing, 2016.

Dillinger, Ray. "Re: Bitcoin P2P e-Cash Paper," November 7, 2008. <https://www.mail-archive.com/cryptography@metzdowd.com/msg09970.html>.

Dinkins, David. "Satoshi's Best Kept Secret: Why Is There a 1 MB Limit to Bitcoin Block Size." CoinTelegraph, September 19, 2017.

<https://cointelegraph.com/news/satoshis-best-kept-secret-why-is-there-a-1-mb-limit-to-bitcoin-block-size>.

Dodd, Nigel. "Laundering 'Money': On the Need for Conceptual Clarity within the Sociology of Money." *European Journal of Sociology* 46, no. 03 (December 2005): 387.

<https://doi.org/10.1017/S0003975605000159>.

———. *The Social Life of Money*. Princeton, NJ: Princeton University Press, 2014.

———. *The Sociology of Money: Economics, Reason & Contemporary Society*. New York: Continuum, 1994.

Donald, James A. "Re: Bitcoin P2P e-Cash Paper," November 2, 2008. <https://www.mail-archive.com/cryptography@metzdowd.com/msg09963.html>.

Ducheneaut, Nicolas. "Socialization in an Open Source Software Community: A Socio-

Technical Analysis." *Computer Supported Cooperative Work* 14, no. 4 (August 2005):

323–68. <https://doi.org/10.1007/s10606-005-9000-1>.

DuPont, Quinn. "The Politics of Cryptography: Bitcoin and the Ordering Machines." *Journal of Peer Production* 4 (2013). <http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-politics-of-cryptography-bitcoin-and-the-ordering-machines/>.

Edbauer, Jenny. "Unframing Models of Public Distribution: From Rhetorical Situation to Rhetorical Ecologies." *Rhetoric Society Quarterly* 35, no. 4 (September 2005): 5–24. <https://doi.org/10.1080/02773940509391320>.

Edit0r88. "IF Dr. Wright Is Satoshi.." *Reddit*, December 10, 2015. [https://www.reddit.com/r/bitcoin\\_uncensored/comments/3w5fcg/if\\_dr\\_wright\\_is\\_satoshi/](https://www.reddit.com/r/bitcoin_uncensored/comments/3w5fcg/if_dr_wright_is_satoshi/).

"EIPs: The Ethereum Improvement Proposal Repository." GitHub, May 4, 2018. <https://github.com/ethereum/EIPs>.

"Ethereum Classic." Ethereum Classic, 2018. <https://ethereumclassic.github.io/>.

"Ethereum (ETH) Historical Data." CoinMarketCap, 2018. <https://coinmarketcap.com/currencies/ethereum/historical-data/>.

"Ethereum Project." Ethereum, 2018. <https://www.ethereum.org/>.

Eyman, Douglas. *Digital Rhetoric: Theory, Method, Practice*. Ann Arbor, MI: University of Michigan Press, 2015.

Fine, Ben, and Costas Lapavistas. "Markets and Money in Social Theory: What Role for Economics?" *Economy and Society* 29, no. 3 (January 2000): 357–82. <https://doi.org/10.1080/03085140050084561>.

Finn, Ed. *What Algorithms Want: Imagination in the Age of Computing*. Cambridge, MA: MIT Press, 2017.

- Finney, Hal. "Re: Bitcoin P2P e-Cash Paper," November 8, 2008. <https://www.mail-archive.com/cryptography@metzdowd.com/msg09975.html>.
- Fox-Brewster, Thomas. "Time to Call a Hoax? Inconsistencies on 'probable' Bitcoin Creator's PhD and Supercomputers Revealed." *Forbes*, December 11, 2015. <https://www.forbes.com/sites/thomasbrewster/2015/12/11/bitcoin-creator-satoshi-craig-wright-lies-hoax/#5739ede06794>.
- Franco, Pedro. *Understanding Bitcoin: Cryptography, Engineering, and Economics*. Chichester, UK: John Wiley & Sons, 2015.
- Fry, Shaolin. "BIP 148: Mandatory Activation of Segwit Deployment." GitHub, March 12, 2017. <https://github.com/bitcoin/bips/blob/master/bip-0148.mediawiki>.
- Fung, Brian. "What You Need to Know about Bitcoin after the WannaCry Ransomware Attack." *Washington Post*, May 15, 2017. <https://www.washingtonpost.com/news/the-switch/wp/2017/05/15/what-you-need-to-know-about-bitcoin-after-the-wannacry-ransomware-attack/>.
- Galloway, Alexander R. *Protocol: How Control Exists after Decentralization*. Cambridge, MA: MIT Press, 2004.
- Ganßmann, Heiner. *Doing Money: Elementary Monetary Theory from a Sociological Standpoint*. New York: Routledge, 2012.
- . "Money—A Symbolically Generalized Medium of Communication?" *Economy & Society* 17, no. 3 (1988): 285–316. <https://doi.org/10.1080/03085148800000013>.
- Garcia, Marie-France. "La Construction Sociale d'un Marché Parfait: Le Marché Au Cadran de Fontaines-En-Sologne." *Actes de La Recherche En Sciences Sociales* 65 (1986): 2–13.

Gehrke, Pat J. *The Ethics and Politics of Speech: Communication and Rhetoric in the Twentieth Century*. Carbondale, IL: Southern Illinois University Press, 2009.

gergi. "If We Fork Because of a Faulty Contract." *Reddit*, June 17, 2016.

[https://www.reddit.com/r/ethereum/comments/4oiqj7/critical\\_update\\_re\\_dao\\_vulnerability/](https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/).

Columbia, David. *The Politics of Bitcoin: Software as Right-Wing Extremism*. Minneapolis, MN: University of Minnesota Press, 2016.

Goodman, Leah McGrath. "The Face behind Bitcoin." *Newsweek*, March 6, 2014.

<http://www.newsweek.com/2014/03/14/face-behind-bitcoin-247957.html>.

Graf, Konrad S. "Commodity, Scarcity, and Monetary Value Theory in Light of Bitcoin."

*Prices & Markets* 3, no. 3 (2015): 52–69.

Granovetter, Mark. "Economic Action and Social Structure: The Problem of Embeddedness."

*American Journal of Sociology* 91, no. 3 (November 1985): 481–510.

<https://doi.org/10.1086/228311>.

———. "The Old and New Economic Sociology: A History and an Agenda." In *Beyond the Marketplace: Rethinking Economy and Society*, edited by Roger Friedland and A. F. Robertson, 53–88. Berlin: Aldine de Gruyter, 1990.

Greenberg, Andy. "Nakamoto's Neighbor: My Hunt for Bitcoin's Creator Led to a Paralyzed Crypto Genius." *Forbes*, March 25, 2014.

<https://www.forbes.com/sites/andygreenberg/2014/03/25/satoshi-nakamotos-neighbor-the-bitcoin-ghostwriter-who-wasnt/>.

- . “New Clues Suggest Craig Wright, Suspected Bitcoin Creator, May Be a Hoaxer.” WIRED, December 11, 2015. <https://www.wired.com/2015/12/new-clues-suggest-satoshi-suspect-craig-wright-may-be-a-hoaxer/>.
- . *This Machine Kills Secrets: How WikiLeaks, Cypherpunks, and Hactivists Aim to Free the World's Information*. New York: Dutton, 2012.
- Greenberg, Andy, and Gwern Branwen. “Bitcoin’s Creator Satoshi Nakamoto Is Probably This Unknown Australian Genius.” Wired, December 8, 2015. <https://www.wired.com/2015/12/bitcoins-creator-satoshi-nakamoto-is-probably-this-unknown-australian-genius/>.
- Hahn, Frank H. “The Foundations of Monetary Theory.” In *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, edited by Geoffrey K. Ingham, 52–74. Critical Studies in Economic Institutions 8. Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005.
- Hanley, Brian P. “The False Premises and Promises of Bitcoin,” 2013. <https://arxiv.org/abs/1312.2048>.
- Hart, Keith. “Money in an Unequal World.” *Anthropological Theory* 1, no. 3 (September 2001): 307–30. <https://doi.org/10.1177/14634990122228755>.
- . “Money Is Always Personal and Impersonal.” *Anthropology Today* 23, no. 5 (October 2007): 12–16. <https://doi.org/10.1111/j.1467-8322.2007.00536.x>.
- . “Notes towards an Anthropology of Money.” *Kritikos* 2 (2005). <http://intertheory.org/hart.htm>.
- . “The Financial Crisis and the End of All-Purpose Money.” *Economic Sociology: The European Electronic Newsletter* 12, no. 2 (2011): 4–10.

Hartleius, E. Johanna. *The Rhetoric of Expertise*. Lanham, MD: Lexington Books, 2010.

Henry, David, and Anna Irrera. "JPMorgan's Dimon Says Bitcoin 'Is a Fraud.'" *Reuters*, September 13, 2017. <https://www.reuters.com/article/legal-us-usa-banks-conference-jpmorgan/jpmorgans-dimon-says-bitcoin-is-a-fraud-idUSKCN1BN2PN>.

HermanLeon. "Here Is an Answer When Somebody Says: 'Bitcoin Is Backed by Nothing!'" *Reddit*, December 12, 2014. [https://www.reddit.com/r/Bitcoin/comments/2p4yfy/here\\_is\\_an\\_answer\\_when\\_sombody\\_says\\_bitcoin\\_is/](https://www.reddit.com/r/Bitcoin/comments/2p4yfy/here_is_an_answer_when_sombody_says_bitcoin_is/).

Hern, Alex. "Bitcoin's Forked: Chief Scientist Launches Alternative Proposal for the Currency." *the Guardian*, August 17, 2015. <http://www.theguardian.com/technology/2015/aug/17/bitcoin-xt-alternative-cryptocurrency-chief-scientist>.

Hertig, Alyssa. "SegWit Goes Live: Why Bitcoin's Big Upgrade Is a Blockchain Game-Changer." *CoinDesk*, August 23, 2017. <https://www.coindesk.com/50-blocks-segwit-bitcoins-coming-upgrade-blockchain-game-changer/>.

Hilliard, James. "BIP 91: Reduced Threshold Segwit MASF." *GitHub*, May 22, 2017. <https://github.com/bitcoin/bips/blob/master/bip-0091.mediawiki>.

"History of Ethereum." *Ethereum Homestead*, 2016. <http://www.ethdocs.org/en/latest/introduction/history-of-ethereum.html>.

Homer. *The Iliad of Homer*. Translated by Alexander Pope. Project Gutenberg, 2006. <https://www.gutenberg.org/files/6130/6130-h/6130-h.html>.

Hughes, Eric. "A Cypherpunk's Manifesto." In *Crypto Anarchy, Cyberstates, and Pirate Utopias*, edited by Peter Ludlow, 81–83. Cambridge, MA: MIT Press, 2001.

- HurlSly. "If Craig Wright Is Satoshi, the Scaling Debate Would Be Settled Years Ago." *Reddit*, March 1, 2018.  
[https://www.reddit.com/r/btc/comments/816hri/if\\_craig\\_wright\\_is\\_satoshi\\_the\\_scaling\\_debate/](https://www.reddit.com/r/btc/comments/816hri/if_craig_wright_is_satoshi_the_scaling_debate/).
- Iavorschi, Milhaela. "The Bitcoin Project and the Free Market." *Center for European Studies Working Papers* 5, no. 4 (2013): 529–34.
- Ingham, Geoffrey. "'Babylonian Madness': On the Historical and Sociological Origins of Money." In *What Is Money?*, edited by John N. Smithin, 16–41. Routledge International Studies in Money and Banking 6. London ; New York: Routledge, 2000.
- . "Capitalism, Money and Banking: A Critique of Recent Historical Sociology." *The British Journal of Sociology* 50, no. 1 (March 1999): 76–96.  
<https://doi.org/10.1111/j.1468-4446.1999.00076.x>.
- . "Fundamentals of a Theory of Money: Untangling Fine, Lapavitsas and Zelizer." *Economy and Society* 30, no. 3 (January 2001): 304–23.  
<https://doi.org/10.1080/03085140120071215>.
- . "Further Reflections on the Ontology of Money: Responses to Lapavitsas and Dodd." *Economy and Society* 35, no. 2 (May 2006): 259–78.  
<https://doi.org/10.1080/03085140600635730>.
- . "Introduction." In *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, edited by Geoffrey K. Ingham, xi–xxiv. Critical Studies in Economic Institutions 8. Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005.

- . “Money Is a Social Relation.” *Review of Social Economy* 54, no. 4 (December 1996): 507–29. <https://doi.org/10.1080/00346769600000031>.
- . “On the Underdevelopment of the ‘Sociology of Money.’” *Acta Sociologica* 41, no. 1 (1998): 3–18.
- . “The Emergence of Capitalist Credit Money.” In *Credit and State Theory of Money*, edited by L. Randall Wray, 173–222. Cheltenham, UK: Edward Elgar, 2004.
- . *The Nature of Money*. Malden, MA: Polity, 2004.
- . “The Specificity of Money.” *European Journal of Sociology* 48, no. 02 (August 2007). <https://doi.org/10.1017/S0003975607000367>.
- “IRS Virtual Currency Guidance.” Internal Revenue Service, March 25, 2014. <https://www.irs.gov/uac/Newsroom/IRS-Virtual-Currency-Guidance>.
- jedigras. “This Was a Contractually Allowed Result.” *Reddit*, June 18, 2016. [https://www.reddit.com/r/ethereum/comments/4oiqj7/critical\\_update\\_re\\_dao\\_vulnerability/](https://www.reddit.com/r/ethereum/comments/4oiqj7/critical_update_re_dao_vulnerability/).
- Jentzsch, Christoph. “Decentralized Autonomous Organization to Automate Governance.” Slock.it, 2016. <https://download.slock.it/public/DAO/WhitePaper.pdf>.
- Jeong, Sarah. “Satoshi’s PGP Keys Are Probably Backdated and Point to a Hoax.” Motherboard, December 9, 2015. [https://motherboard.vice.com/en\\_us/article/jpgq3y/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax](https://motherboard.vice.com/en_us/article/jpgq3y/satoshis-pgp-keys-are-probably-backdated-and-point-to-a-hoax).
- . “The Bitcoin Protocol as Law, and the Politics of a Stateless Currency,” 2013. <http://dx.doi.org/10.2139/ssrn.2294124>.

Jevons, William Stanley. *Money and the Mechanism of Exchange*. New York: D. Appleton & Co., 1875.

Kaminsky, Dan. "Validating Satoshi (Or Not)." *Dan Kaminsky's Blog* (blog), May 2, 2016.  
<https://dankaminsky.com/2016/05/02/validating-satoshi-or-not/>.

Karlstrøm, Henrik. "Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin." *Distinktion: Scandinavian Journal of Social Theory* 15, no. 1 (2014): 23–36. <https://doi.org/10.1080/1600910X.2013.870083>.

Keynes, John Maynard. *A Treatise on Money*. New York: AMS Press, 1976.

Kostakis, Vasilis, and Chris Giotitsas. "The (a)Political Economy of Bitcoin." *TripleC* 12, no. 2 (2014): 431–40.

"Kraken." Kraken. Accessed January 19, 2018. <https://www.kraken.com/>.

Krugman, Paul. "Bitcoin Is Evil." *The New York Times*. December 28, 2013.  
<http://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/>.

———. "Golden Cyberfettters." *The New York Times*. September 7, 2011.  
<http://krugman.blogs.nytimes.com/2011/09/07/golden-cyberfettters/>.

Lapavitsas, Costas. "The Social Relations of Money as Universal Equivalent: A Response to Ingham." *Economy and Society* 34, no. 3 (August 2005): 389–403.  
<https://doi.org/10.1080/03085140500112137>.

Lau, Johnson, and Pieter Wuille. "BIP 143: Transaction Signature Verification for Version 0 Witness Program." GitHub, January 3, 2016.  
<https://github.com/bitcoin/bips/blob/master/bip-0143.mediawiki>.

- Lauer, Josh. "Money as Mass Communication: U.S. Paper Currency and the Iconography of Nationalism." *The Communication Review* 11, no. 2 (2008): 109–32.  
<https://doi.org/10.1080/10714420802068359>.
- Lessig, Lawrence. *Code: Version 2.0*. New York: Basic Books, 2006.
- Lo, Stephanie, and J. Christina Wang. "Bitcoin as Money?" Current Policy Perspectives. Boston, MA: Federal Reserve Bank of Boston, 2014.
- Lombrozo, Eric, Johnson Lau, and Pieter Wuille. "BIP 141: Segregated Witness (Consensus Layer)." GitHub, December 21, 2015.  
<https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki>.
- Lombrozo, Eric, and Pieter Wuille. "BIP 144: Segregated Witness (Peer Services)." GitHub, March 12, 2017. <https://github.com/bitcoin/bips/blob/master/bip-0144.mediawiki>.
- Ludlow, Peter, ed. *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge, MA: MIT Press, 2001.
- Luther, William J., and Josiah Olson. "Bitcoin Is Memory." *The Journal of Prices & Markets* 3, no. 3 (2015).
- MacKenzie, Donald A. *An Engine, Not a Camera: How Financial Models Shape Markets*. Inside Technology. Cambridge, Mass: MIT Press, 2006.
- . *Material Markets: How Economic Agents Are Constructed*. Clarendon Lectures in Management Studies. Oxford ; New York: Oxford University Press, 2009.
- MacKenzie, Donald A., Fabian Muniesa, and Lucia Siu, eds. *Do Economists Make Markets? On the Performativity of Economics*. Princeton: Princeton University Press, 2007.

- MacKenzie, Donald, and Yuval Millo. "Constructing a Market, Performing Theory: The Historical Sociology of a Financial Derivatives Exchange." *American Journal of Sociology* 109, no. 1 (July 2003): 107–45. <https://doi.org/10.1086/374404>.
- Mailloux, Steven. *Disciplinary Identities: Rhetorical Paths of English, Speech, and Composition*. New York: Modern Language Association, 2006.
- Mallard, Alexandre, Cécile Méandel, and Francesca Musiani. "The Paradoxes of Distributed Trust: Peer-to-Peer Architectures and User Confidence in Bitcoin." *Journal of Peer Production* 4 (2014). <http://peerproduction.net/issues/issue-4-value-and-currency/peer-reviewed-articles/the-paradoxes-of-distributed-trust/>.
- Mankiw, N. Gregory. *Principles of Economics*. 4th ed. Mason, OH: Thomson South-Western, 2007.
- Mark, Dino, Vlad Zamfir, and Emin Gün Sirer. "A Call for a Temporary Moratorium on The DAO." *Hacking Distributed*, May 27, 2016. <http://hackingdistributed.com/2016/05/27/dao-call-for-moratorium/>.
- "Market Capitalization." *Blockchain.info*. Accessed January 18, 2018. <https://blockchain.info/charts/market-cap>.
- "Market Price (USD)." *Blockchain.info*. Accessed January 18, 2018. <https://blockchain.info/charts/market-price>.
- Marko, Malovic. "Demystifying Bitcoin: Sleight of Hand or Major Global Currency Alternative?" *Economic Analysis* 47, no. 1–2 (2014): 32–41.
- Marshall, Andrew. "Bitcoin Scaling Problem, Explained." *CoinTelegraph*, March 2, 2017. <https://cointelegraph.com/explained/bitcoin-scaling-problem-explained>.

- Marx, Karl. *Capital: A Critique of Political Economy*. Translated by Ben Fowkes. Vol. 1. New York: Penguin, 1990.
- Maurer, Bill. "Mobile Money: Communication, Consumption and Change in the Payments Space." *Journal of Development Studies* 48, no. 5 (2012): 589–604.  
<https://doi.org/10.1080/00220388.2011.621944>.
- . "The Anthropology of Money." *Annual Review of Anthropology* 35 (2006): 15–36.  
<https://doi.org/10.1146/annurev.anthro.35.081705.123127>.
- Maurer, Bill, Taylor C. Nelms, and Stephen C. Rea. "'Bridges to Cash': Channelling Agency in Mobile Money." *Journal of the Royal Anthropological Institute* 19, no. 1 (2013): 52–74. <https://doi.org/10.1111/1467-9655.12003>.
- Maurer, Bill, Taylor C. Nelms, and Lana Swartz. "'When Perhaps the Real Problem Is Money Itself!': The Practical Materiality of Bitcoin." *Social Semiotics* 23, no. 2 (2013): 261–77. <https://doi.org/10.1080/10350330.2013.777594>.
- McCloskey, Deirdre N. *The Rhetoric of Economics*. 2nd ed. Madison, WI: University of Wisconsin Press, 1998.
- McGee, Michael Calvin. "Text, Context, and the Fragmentation of Contemporary Culture." *Western Journal of Speech Communication* 54, no. 3 (1990): 274–89.  
<https://doi.org/10.1080/10570319009374343>.
- McLuhan, Marshall. *Understanding Media: The Extensions of Man*. New York: Signet, 1966.
- Menger, Carl. "On the Origin of Money." *Economic Journal* 2, no. 6 (1892): 239–55.
- Milner, Ryan M. "Hacking the Social: Internet Memes, Identity Antagonism, and the Logic of Lulz." *The Fibreculture Journal*, no. 22 (2013): 62–92.
- Mross, Nicholas. *The Rise and Rise of Bitcoin*. Documentary. Gravitas Ventures, 2014.

Mullan, P. Carl. *A History of Digital Currency in the United States: New Technology in an Unregulated Market*. New York: Palgrave Macmillan, 2016.

Muniesa, Fabian. *The Provoked Economy: Economic Reality and the Performative Turn*. Culture, Economy and the Social. London: Routledge, 2014.

Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.  
<https://bitcoin.org/bitcoin.pdf>.

———. "Bitcoin P2P E-Cash Paper," November 1, 2008. <https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html>.

———. "[Bitcoin-Dev] Bitcoin XT Fork," August 15, 2015.  
<https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2015-August/010238.html>.

———. *The Book of Satoshi: The Collected Writings of Bitcoin Creator Satoshi Nakamoto*. Edited by Phil Champagne. e53 Publishing, 2014.

"Number of Transactions per Day." Blockchain.info. Accessed January 18, 2018.  
<https://blockchain.info/charts/n-transactions>.

Nunes, Mark, ed. *Error: Glitch, Noise, and Jam in New Media Cultures*. New York: Continuum, 2011.

O'Hagan, Andrew. "The Satoshi Affair." London Review of Books, June 30, 2016.  
<https://www.lrb.co.uk/v38/n13/andrew-ohagan/the-satoshi-affair>.

Ólafsson, Ísak Andri. "Is Bitcoin Money? An Analysis from the Austrian School of Economic Thought." Master's thesis, University of Iceland, 2014.

Ong, Walter J. *Ramus, Method, and the Decay of Dialogue: From the Art of Discourse to the Art of Reason*. Chicago: University of Chicago Press, 2004.

Oram, Andrew, and Greg Wilson, eds. *Beautiful Code: Leading Programmers Explain How They Think*. Sebastapol, CA: O'Reilly, 2007.

Parikka, Jussi, and Tony D. Sampson, eds. *The Spam Book: On Viruses, Porn, and Other Anomalies from the Dark Side of Digital Culture*. Communication Alternatives. Cresskill, NJ: Hampton Press, 2009.

Parry, Jonathan, and Maurice Bloch, eds. *Money and the Morality of Exchange*. Cambridge, UK: Cambridge University Press, 1989.

Parsons, Talcott. "On the Concept of Political Power." In *Sociological Theory and Modern Society*, 297–354. New York: The Free Press, 1967.

Pinch, Trevor J., and Wiebe E. Bijker. "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit from Each Other." *Social Studies of Science* 14, no. 3 (1984): 399–441.

Pinch, Trevor, and Richard Swedberg, eds. *Living in a Material World: Economic Sociology Meets Science and Technology Studies*. Inside Technology. Cambridge, Mass: MIT Press, 2008.

Pitta, Julie. "Requiem for a Bright Idea." *Forbes*, November 1, 1999.

<http://www.forbes.com/forbes/1999/1101/6411390a.html>.

Poggi, Gianfranco. *Money and the Modern Mind: Georg Simmel's Philosophy of Money*. Berkeley, CA: University of California Press, 1993.

Polanyi, Karl. *The Great Transformation: The Political and Economic Origins of Our Time*. 2nd ed. Boston, MA: Beacon Press, 2001.

Popper, Nathaniel. "A Venture Fund With Plenty of Virtual Capital, but No Capitalist." *The New York Times*, May 21, 2016, sec. DealBook.

<https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html>.

———. “Decoding the Enigma of Satoshi Nakamoto and the Birth of Bitcoin.” *The New York Times*, May 15, 2015. <https://www.nytimes.com/2015/05/17/business/decoding-the-enigma-of-satoshi-nakamoto-and-the-birth-of-bitcoin.html>.

———. *Digital Gold: Bitcoin and the inside Story of the Misfits and Millionaires Trying to Reinvent Money*. New York: HarperCollins, 2015.

Preda, Alex. *Framing Finance: The Boundaries of Markets and Modern Capitalism*. Chicago: The University of Chicago Press, 2009.

Radford, R.A. “The Economic Organization of a P.O.W. Camp.” In *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, edited by Geoffrey K. Ingham, 20–32. Critical Studies in Economic Institutions 8. Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005.

“Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO.” U.S. Securities and Exchange Commission, July 25, 2017. <https://www.sec.gov/litigation/investreport/34-81207.pdf>.

Rizzo, Pete. “Ethereum Hard Fork Creates Competing Currencies.” CoinDesk, July 24, 2016. <https://www.coindesk.com/ethereum-hard-fork-creates-competing-currencies-support-ethereum-classic-rises/>.

Sammons, Eric. “Fulfilling Satoshi’s Vision.” Decentralize Today, April 4, 2016. <https://decentralize.today/fulfilling-satoshi-s-vision-605e80845d0f>.

SamWouters. "I Was Told in Some Other Place." *Reddit*, May 7, 2017.

[https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick\\_of\\_hearing\\_satoshis\\_original\\_vision/dh8mo6h/](https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick_of_hearing_satoshis_original_vision/dh8mo6h/).

———. "What Bothers Me Most." *Reddit*, May 7, 2017.

[https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick\\_of\\_hearing\\_satoshis\\_original\\_vision/dh7jz8m/](https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick_of_hearing_satoshis_original_vision/dh7jz8m/).

"Satoshi Nakamoto Institute." Accessed April 17, 2018.

<http://satoshi.nakamotoinstitute.org/>.

"Satoshi's Vision | Bitcoin Cash Conference | March 23-25 Tokyo Japan." Accessed April 18, 2018. <https://satoshisvisionconference.com/>.

Sawyer, Malcolm. "Money and the State." In *Financial Crises and the Nature of Capitalist Money: Mutual Developments from the Work of Geoffrey Ingham*, edited by Jocelyn Pixley and G. C. Harcourt, 162–77. Basingstoke: Palgrave Macmillan, 2013.

Schumpeter, Joseph A. *History of Economic Analysis*. Edited by Elizabeth Boody Schumpeter. New York: Taylor & Francis, 2006.

Selgin, George. "Synthetic Commodity Money." *Journal of Financial Stability* 17 (April 2015): 92–99. <https://doi.org/10.1016/j.jfs.2014.07.002>.

Shaw, Lynette. "The Meanings of New Money: Social Constructions of Value in the Rise of Digital Currencies." Ph.D. diss., University of Washington, 2016.

"Should Bitcoin Be Backed by Something like Bullion? Gold, Silver, Oil, Platinum?" Bitcoin FAQ, January 31, 2013. <http://bitcoin-faq.com/should-bitcoin-be-backed-by-something-like-bullion-gold-silver-oil-platinum/>.

- Siegel, David. "Understanding The DAO Attack." CoinDesk, June 25, 2016.  
<https://www.coindesk.com/understanding-dao-hack-journalists/>.
- Simmel, Georg. *The Philosophy of Money*. Edited by David Frisby. Translated by Tom Bottomore, David Frisby, and Kaethe Mengelberg. 3rd ed. New York: Routledge, 2011.
- Singh, Supriya. "Electronic Commerce and the Sociology of Money." *Sociological Research Online* 4, no. 4 (2000). <http://www.socresonline.org.uk/4/4/singh.html>.
- Smithin, John N. "What Is Money? Introduction." In *What Is Money?*, edited by John N. Smithin, 1–15. Routledge International Studies in Money and Banking 6. London ; New York: Routledge, 2000.
- Snelders, H.M.J.J., Gönül Hussein, Stephen E.G. Lea, and Paul Webley. "The Polymorphous Concept of Money." *Journal of Economic Psychology* 13, no. 1 (March 1992): 71–92.  
[https://doi.org/10.1016/0167-4870\(92\)90053-A](https://doi.org/10.1016/0167-4870(92)90053-A).
- Song, Jimmy. "Understanding Segregated Witness." SegWit Resources, August 7, 2017.  
<https://segwit.org/understanding-segregated-witness-905cc712c692>.
- Šurda, Peter. "Economics of Bitcoin: Is Bitcoin an Alternative to Fiat Currencies and Gold?" Thesis, Vienna University of Economics and Business, 2012.
- Svetlova, Ekaterina. "Performativity and Emergence of Institutions." In *Enacting Dismal Science: New Perspectives on the Performativity of Economics*, edited by Ivan Boldyrev and Ekaterina Svetlova, 183–200. Perspectives from Social Economics. New York: Palgrave Macmillan, 2016.
- Swartz, Deja Elana. "Tokens, Ledgers, and Rails: The Communication of Money." Ph.D. diss., University of Southern California, 2015.

Swartz, Lana. "Blockchain Dreams: Imagining Techno-Economic Alternatives after Bitcoin."

In *Another Economy Is Possible: Culture and Economy in a Time of Crisis*, edited by Manuel Castells, 82–105. Malden, MA: Polity, 2017.

Swedberg, Richard. *Principles of Economic Sociology*. Princeton, NJ: Princeton University Press, 2003.

Szabo, Nick. "Bit Gold." *Unenumerated: An Unending Variety of Topics* (blog), December 27, 2008. <http://unenumerated.blogspot.com/2005/12/bit-gold.html>.

———. "Smart Contracts: Building Blocks for Digital Markets." *Extropy*, 1996.

Szilágyi, Péter. "DAO Wars: Your Voice on the Soft-Fork Dilemma." *Ethereum Blog* (blog), June 24, 2016. <https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma/>.

Taaki, Amir. "BIP 1: BIP Purpose and Guidelines." GitHub, August 19, 2011. <https://github.com/bitcoin/bips/blob/master/bip-0001.mediawiki>.

The Attacker. "An Open Letter." Pastebin.com, June 18, 2016. <https://pastebin.com/CcGUBgDG>.

theonevortex. "Sick of Hearing 'Satoshi's Original Vision.'" *Reddit*, May 6, 2017. [https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick\\_of\\_hearing\\_satoshis\\_original\\_vision/](https://www.reddit.com/r/Bitcoin/comments/69l3zk/sick_of_hearing_satoshis_original_vision/).

"Top 100 Cryptocurrencies by Market Capitalization." CoinMarketCap, 2018. <https://coinmarketcap.com/>.

Tual, Stephan. "A Fork in the Road." *Stephan Tual* (blog), June 18, 2016. <https://medium.com/@stephantual/a-fork-in-the-road-c3c267b9ff31#.czj4ma1q7>.

- . “No DAO Funds at Risk Following the Ethereum Smart Contract ‘Recursive Call’ Bug Discovery.” Slock.it Blog, June 12, 2016. <https://blog.slock.it/no-dao-funds-at-risk-following-the-ethereum-smart-contract-recursive-call-bug-discovery-29f482d348b#.mbfqikiyo>.
- . “Proposal Framework 1.0, DAO 1.1 Draft!” Slock.it Blog, June 10, 2016. <https://blog.slock.it/proposal-framework-1-0-dao-1-1-draft-427c40ef9ed4#.wkgvffoqx>.
- Turner, Stephen P. *Liberal Democracy 3.0: Civil Society in an Age of Experts*. Theory, Culture & Society. London ; Thousand Oaks, Calif: SAGE Publications, 2003.
- Veness, Chris. “SHA-256 Cryptographic Hash Algorithm.” Movable Type Scripts, 2015. <http://www.movable-type.co.uk/scripts/sha256.html>.
- Weber, Beat. “Can Bitcoin Compete with Money?” *The Journal of Peer Production* 4 (2014). <http://peerproduction.net/issues/issue-4-value-and-currency/invited-comments/can-bitcoin-compete-with-money/>.
- Weber, Max. *Economy and Society: An Outline of Interpretive Sociology*. Edited by Guenther Roth and Claus Wittich. Berkeley, CA: University of California Press, 1978.
- “What Is Bitcoin Cash?” CoinDesk, April 16, 2018. <https://www.coindesk.com/information/what-is-bitcoin-cash/>.
- “What Is Ethereum?” Ethereum Homestead, 2016. <http://www.ethdocs.org/en/latest/introduction/what-is-ethereum.html>.
- “What Is SegWit?” CoinDesk, February 22, 2018. <https://www.coindesk.com/information/what-is-segwit/>.

Wirdum, Aaron van. "Rejecting Today's Hard Fork, the Ethereum Classic Project Continues on the Original Chain: Here's Why." *Bitcoin Magazine*, July 20, 2016.

<https://bitcoinmagazine.com/articles/rejecting-today-s-hard-fork-the-ethereum-classic-project-continues-on-the-original-chain-here-s-why-1469038808/>.

Wright, Craig. "Extraordinary Claims Require Extraordinary Proof." *Dr. Craig Wright Blog*, May 4, 2016.

<https://web.archive.org/web/20160504045648/http://www.drcaigwright.net/extraordinary-claims-require-extraordinary-proof/>.

———. "I'm Sorry." *Dr. Craig Wright Blog*, May 7, 2016.

<https://web.archive.org/web/20160507165900/http://www.drcaigwright.net/>.

———. "Jean-Paul Sartre, Signing and Significance." *Dr. Craig Wright Blog*, May 2, 2016.

<http://archive.is/m5euI>.

Zelizer, Viviana. "Fine Tuning the Zelizer View." *Economy and Society* 29, no. 3 (January 2000): 383–89. <https://doi.org/10.1080/03085140050084570>.

———. "Pasts and Futures of Economic Sociology." *American Behavioral Scientist* 50, no. 8 (April 2007): 1056–69. <https://doi.org/10.1177/0002764207299353>.

———. *The Social Meaning of Money: Pin Money, Paychecks, Poor Relief and Other Currencies*. New York: Basic Books, 1994.

———. "The Social Meaning of Money: 'Special Monies.'" In *Concepts of Money: Interdisciplinary Perspectives from Economics, Sociology and Political Science*, edited by Geoffrey K. Ingham, 575–610. *Critical Studies in Economic Institutions* 8. Cheltenham, UK ; Northampton, MA: Edward Elgar Pub, 2005.