

# Getting off the ground: the case of bitcoin

WILLIAM J. LUTHER\*

Department of Economics, Florida Atlantic University, Boca Raton, FL 33431

**Abstract.** By declaring an item legal tender or making it publicly receivable, governments might generate sufficient demand to determine the medium of exchange. How do private actors launch a new money? There are two views in the literature. The first requires offering an item with a use value to some agents that is distinct from its role as a medium of exchange. The second suggests that agents might coordinate on an intrinsically useless item. With these views in mind, I survey the logs from the original bitcoin forum, bitcoin-list. I find that early participants in the bitcoin community understood the importance of coordination and took steps to coordinate users.

When it comes to launching a new money, governments have a distinct advantage. They can require their citizens pay taxes with and accept payments from the government in a particular money. They can declare it legal tender, requiring their citizens to accept it when extinguishing debt contracts. And they can impose penalties on those using alternatives. By relying on coercion of some sort or another, a government of sufficient size can determine the medium of exchange (Aiyagari and Wallace 1997; Forstater 2006; Goldberg 2012; Hendrickson and Luther 2017a; Hendrickson *et al.* 2016; Li and Wright 1998; Salter and Luther 2014).<sup>1</sup>

How might a money get off the ground in the absence of sovereign support? There are essentially two views on the prerequisites for launching a new private money. The first view, which I call the *use-value view*, insists that a private money must have some non-monetary use in order to gain acceptance as a medium of exchange. The second view, which I call the *coordination view*, maintains that no non-monetary use is necessary; agents might agree to use a money if they believe others will.

In what follows, I express the value of a particular money to a representative agent in order to present these two views more precisely. Then, I consider the case

\*Email: [wluther@fau.edu](mailto:wluther@fau.edu)

<sup>1</sup> Luther and White (2016) suggest that, in addition to coercing private agents to use a particular medium of exchange, a government might also serve as a coordination device. See also: Luther (2016b). The *state theory of money*, which dates back to Knapp (1924), usually holds that government is necessary for launching a new money.

of bitcoin to determine which of these two views more accurately describes its launch. Surveying the transcripts from the original bitcoin forum, bitcoin-list, I find that early participants in the bitcoin community understood the importance of coordination and took steps to coordinate users. This matters for two reasons. First, it suggests that those working in the use-value tradition have paid too little attention to coordination. Second, it goes beyond the mere assumption that coordination is possible by explaining how, in this particular case, coordination was actually achieved.

## 1 The value of money

Consider a world with  $N$  infinitely lived money-using agents. One can express the utility a representative agent derives from using a particular item as money from time  $T$  onwards as:

$$u(T) = (an + b) \int_T^\infty e^{-r(t-T)} dt = (an + b)/r,$$

where  $a$  and  $b$  are fixed parameters,  $r$  is the discount rate,  $n \equiv \ln(\theta N)$ , and  $0 \leq \theta \leq 1$  is the proportion of agents using the item as money.<sup>2</sup>

The first term in the value function,  $an/r$ , represents the item's *monetary value*. It denotes the benefits the agent enjoys from using the item as a medium of exchange. Note that the monetary value depends on the number of other agents using the item as money.<sup>3</sup> Intuitively, an agent derives no benefits from employing the item as a medium of exchange if no one else accepts it; the more people that employ the item as a medium of exchange, the more useful it is as a medium of exchange; and the marginal value of an additional user is greater for a medium of exchange with a small network of users than a large network of users. Hence,  $an = 0$  when  $\theta N = 1$  and  $n$  increases with  $\theta N$  but at a diminishing rate. Finally, the parameter  $a$  captures the characteristics of the item that make it more or less suitable for use as a money.

The second term in the value function,  $b/r$ , represents the item's *non-monetary value*. It denotes any other benefits the agent enjoys from the item – that is, any benefits other than those stemming from its use as a medium of exchange. Unlike the monetary value, it does not depend on the number of other agents using the money.

2 Following Dowd and Greenaway (1993), Luther (2016b) uses a similar value function in considering the prospect of adopting a cryptocurrency like bitcoin. Hendrickson and Luther (2017c) employ a more rigorous search model to demonstrate the conditions where bitcoin has a positive value. See also: Fernández-Villaverde and Sanches (2016), Hendrickson and Luther (2017b).

3 Networks tend to be local, and density and quality often matter more than the total number of participants. However, focusing exclusively on network size preserves the friction while removing much of the complexity. For a survey of the relevant literature, see Shy (2011). On the social dimensions of networks, see Fafchamps *et al.* (2010).

To illustrate, consider China's 100-yuan note. With roughly 1.4 billion users, the 100-yuan note has a very large network ( $n > 0$ ). It is durable, portable, and uniform; and it can be divided by exchanging it for lower denomination notes ( $a > 0$ ). Hence, users enjoy some benefits from employing the item as a medium of exchange. Its monetary value is positive ( $an/r > 0$ ).

Although it is often useful to model fiat monies like the yuan as intrinsically worthless items ( $b = 0$ ), there is no denying that some users derive benefits from the physical notes' aesthetics.<sup>4</sup> The front of the note depicts the Shenzhou nine-man spacecraft docking with the Tiangong-1 space station, in addition to the Chang'e 1 lunar-orbiting spacecraft, the Dongfanghong I satellite, and a coat of arms. The back of the note portrays the evolution of flight, from bird to Chang'e 1, and a brilliant color fade from green to blue. Indeed, the 100-yuan note is so stunning that it was one of 20 notes nominated for the 2015 Banknote of the Year award by members of the International Banknote Society. These members (and perhaps others) enjoy some benefits from the 100-yuan note in and of itself – that is, beyond its role as a medium of exchange. Hence, its non-monetary value is positive ( $b/r > 0$ ).<sup>5</sup>

## 2 On launching a new private currency

Broadly speaking, two views dominate the debate on launching a new private currency. The use-value view maintains that a potential money must have some use to some agents apart from its role as a medium of exchange. The coordination view suggests that agents might coordinate on an intrinsically worthless item. In what follows, I consider these two views with the aforementioned value function in mind.

### *The use-value view*

According to the use-value view, an item must have some non-monetary value in order to gain acceptance as a medium of exchange through the private interactions of agents. The argument is straightforward. Initially, no one accepts the item as a medium of exchange. An agent choosing to accept the item would increase its network size to one. However, the monetary benefits  $an = 0$  when the network size  $\theta N = 1$ , regardless of the characteristics of the item that make it more or less suitable for use as a money ( $a$ ). No one has an incentive to give up valuable goods or services in exchange for a money that no one else yet uses unless they derive some non-monetary benefits from the item ( $b > 0$ ). For

4 On the efficiency of non-price competition for paper monies, see: Sumner (1993, 2000), White (1987), White and Boudreaux (1998, 2000).

5 Most economists will no doubt find it odd to claim that government-issued paper money has some non-monetary use value. However, Goldberg (2005) finds no conclusive evidence that an intrinsically worthless money has ever existed. Luther (2018) considers whether bitcoin is intrinsically worthless. See also: Graf (2013).

this reason, proponents of the use-value view maintain that a positive use-value is necessary for an item to serve as a medium of exchange in purely private orderings.

The traditional account of money emerging out of barter relationships is wholly consistent with the use-value view. Menger (1892), for example, explains a process where an agent accepts a good that he does not wish to consume because it is more saleable – that is, more widely accepted – than the good he offers in exchange. In doing so, the agent increases the network size of the good in question, making it even more saleable. According to Menger (1892: 243):

*The theory of money necessarily presupposes a theory of the saleableness of goods. If we grasp this, we shall be able to understand how the almost unlimited saleableness of money is only a special case, – presenting only a difference of degree – of a generic phenomenon of economic life – namely, the difference in the saleableness of commodities in general.*

Hence, in Menger’s account, the emergence of money begins with an item possessing some non-monetary value. It is, at first, just a commodity – a good that someone consumes. Given the positive network size resulting from those willing to accept it for consumption, others might then employ it as a medium of exchange. And, if enough others join the network, the item will possess sufficient salability to warrant the label money.

Whereas Menger limited his attention to commodity monies, Mises (1934) argued that all monies – that is, commodity and fiat monies – must have some initial non-monetary use value.<sup>6</sup> According to Mises (1934: 131), agents will only be able to estimate the value of money if there is a preexisting market exchange ratio between the item functioning as money and other goods. Consequently, “it follows that an object cannot be used as money unless, at the moment when its use as money begins, it already possesses an objective exchange value based on some other use.” Mises (1934: 132) explains the historical origins of fiat monies as redeemable banknotes.<sup>7</sup> Although these notes were ultimately “deprived of their character as claims,” they continued to circulate at a positive value since “money that already functions as such may remain valuable even when the original source of its exchange value has ceased to exist.”<sup>8</sup> Hence, all monies must have some initial non-monetary use; and only once the link with its original

<sup>6</sup> Selgin (2015) offers a third classification, “synthetic commodity monies,” to describe intrinsically worthless items with a positive and increasing marginal cost of production.

<sup>7</sup> Selgin and White (1987) extend the traditional Mengerian account by describing the emergence of inside money. See also: Selgin and White (1994).

<sup>8</sup> Selgin (2003: 147) uses an adaptive learning algorithm to provide a theoretical account of the “historically-observed tendency for fiat monetary standards to emerge only following the prior appearance of commodity money and the widespread employment of redeemable banknotes.”

use is broken is the value of money “based entirely on its function as a common medium of exchange.”<sup>9</sup>

### *The coordination view*

In contrast to the use-value view, the coordination view maintains that an item might gain acceptance as a medium of exchange despite lacking a positive non-monetary value *if agents can coordinate their actions*. The coordination view recognizes that an agent need not enter a monetary network alone. Instead, one might coordinate to enter the network at the same time as others. In that case, an agent might exchange valuable resources for the item in the expectation that  $\theta N > 1$  and  $n > 0$ , even if  $b/r \leq 0$ .

Early advocates of the coordination view were, perhaps, unaware of the assumption of coordination implicit in their models. Nonetheless, they were quite clear in stating that no initial non-monetary use was required for an item to enter circulation. In constructing a hypothetical market to explore the quantity theory, for example, Nicholson (1895: 57) employs a cash-in-advance constraint and notes that the “money is to be regarded as of no use whatever except to effect exchanges.”<sup>10</sup> Likewise, Patinkin (1965) makes it clear that his “utility of money” is not “intended to denote the utility of the money commodity; indeed, we continue to assume a fiat paper money precisely in order to avoid any ambiguity on this score.”<sup>11</sup> In other words, they limit their consideration to intrinsically worthless items ( $b = 0$ ). As Selgin (1994: 815) explains:

Patinkin (like Nicholson) can be accused of assuming that, because something may potentially serve as a generally accepted medium of exchange, it will be accepted and valued in accordance with this potential.

Patinkin thus overlooks the tenuous “bootstrap” nature of an equilibrium involving positive real balances of fiat money.

Later advocates have been clearer about the coordination required for intrinsically worthless items to function as money. Hahn (1965), for example, demonstrates the existence of non-monetary equilibria in Patinkin’s model. Building on Hahn, Gale (1982: 292) laments that the standard Walrasian

<sup>9</sup> The use-value view suggests prerequisites for government-issued monies as well. Specifically, a “new fiat money must at first be linked to an established money through a fixed rate of exchange. Otherwise would-be users of the new money will have no means of assigning any future purchasing power to it – stable or otherwise – and no basis for demanding definite quantities of it” (Selgin 1994: 811). Only after the new money gains widespread acceptance can the fixed exchange rate be removed without damaging the item’s acceptability as money.

<sup>10</sup> Indeed, money in Nicholson’s model consists of “counters of a certain size made of the bones of the dodo” (p. 57). According to Anderson (1917: 132), “Nicholson chose the illustration to throw into the sharpest relief the absence of any value from a non-monetary employment. Nobody has any use for them as dodo-bones.” See also: Scott (1897).

<sup>11</sup> Patinkin (1965: 79) refers to the problem addressed by Mises and discussed above as the “sham ‘circularity’ issue which never should have arisen in the first place.”

approach taken by Patinkin and others “gives some indication of the outcome of a market game without ever specifying [...] what the process of coalition formation looks like.” Likewise, Ostroy and Starr (1990: 6) discuss Hahn’s “existence problem” before considering the extent to which money is Pareto-improving or, to use the more modern term, essential. And these works form the backdrop for the more recent search-theoretic approach pioneered by Kiyotaki and Wright (1989, 1991, 1993) and exemplified by Lagos and Wright (2005).<sup>12</sup> In general, these works consider the conditions rendering money essential while acknowledging the potential for non-monetary equilibria.<sup>13</sup>

It is important to acknowledge the limits of the coordination view – limits that, as suggested above, have not always been acknowledged by those holding what I have described as the coordination view. In brief, recognizing that agents might coordinate does not eliminate the fundamental network effects problem that would-be currencies face. All else being equal, an item possessing non-monetary value is more likely to get off the ground than an item that does not. The coordination view merely provides an exception: if the costs of coordination are sufficiently low, agents might overcome the network effects problem without the assistance of non-monetary value (Luther 2016b).<sup>14</sup>

### 3 A brief history of Bitcoin

Bitcoin was introduced to the world with little fanfare in an e-mail sent to the Cryptography Mailing List on January 8, 2009.<sup>15</sup> The e-mail’s author, the pseudonymous Satoshi Nakamoto, had circulated a white paper explaining the technical details a few months earlier. It was little known outside a core group of coders at the time. Today, it is used to make transactions all over the world. Although one can certainly debate whether its user base is sufficiently large to warrant the label money, there is no denying that bitcoin has *gotten off the ground* in the sense described above.<sup>16</sup>

12 Experimental (Duffy 2001; Duffy and Ochs 1999, 2002; Duffy and Puzzello 2014) and agent-based computational (Başçı 1999; Giansante 2006; Hasker and Tahmilci 2008; Kawagoe 2007; Marimon *et al.* 1990; Staudinger 1998) approaches in the search-theoretic environment have considered coordination most explicitly. See also: Aliprantis *et al.* (2006, 2007a, 2007b), Araujo (2004), Araujo *et al.* (2012), Lagos and Wright (2008)

13 Luther (2016c) offers a brief survey of the modern search-theoretic approach. See also: Rupert *et al.* (2000).

14 In many cases, the costs of coordination seem to be sufficiently high to preclude switching to otherwise desirable alternatives (King 2004; Luther 2013; Luther and White 2016).

15 For a more complete history of bitcoin’s early days, see Popper (2015). Weber (2014, 2015a, 2015b, 2016) and Fung *et al.* (2017) offer several conjectures regarding the future of bitcoin based on historical experience. See also: Fung and Halaburda (2014), Gans and Halaburda (2013, 2014), Luther and Olson (2015), and White (2015).

16 Yermack (2013) discusses whether bitcoin warrants the label money. On the legal status of bitcoin, see: Grinberg (2012) and Luther (forthcoming).

The initial reactions were positive and congratulatory. But they soon jumped straight to the heart of the matter. As California-based computer scientist Hal Finney made clear in a January 11, 2009 post to the bitcoin-list,

[o]ne immediate problem with any new currency is how to value it. Even ignoring the practical problem that virtually no one will accept it at first, there is still a difficulty in coming up with a reasonable argument in favor of a particular non-zero value for the coins.<sup>17</sup>

In other words, the question of bitcoin's value – the primary issue considered herein – was front and center at the outset.

For nearly nine months after its launch, bitcoin was effectively (if not precisely) worthless. Transactions were executed, to be sure. But they were limited to test spends by coders working out the bugs in the protocol. The first transaction, for example, was confirmed on January 12, 2009, when Nakamoto sent 50 bitcoin to two addresses owned by Finney.<sup>18</sup> There were no market exchange rates with existing monies and no known transactions of bitcoin for goods or services.

The first known exchange rate for bitcoin was posted on October 5, 2009. A user going by the moniker New Liberty Standard estimated that it cost roughly \$1 to produce 1,309.03 bitcoin. Seven days later, he sent \$5.05 via PayPal to Martti Malmi in exchange for 5,050 bitcoin. Hence, in the first known currency exchange, one bitcoin was valued at just \$0.0010. In the months that followed, currency exchanges were made *ad hoc*. Then, on February 6, 2010, the user *dwdollar* launched The Bitcoin Market to make exchanging bitcoin and dollars more convenient. Initially, users were credited with play balances of dollars and bitcoin to test out the platform. Actual exchanges were not permitted until March 16, 2010. The real first bid, posted by *dwdollar*, valued bitcoin at \$0.0067.

The new exchange made it easier to buy and sell bitcoin with dollars and, soon after, users would begin spending their bitcoin to acquire goods and services in the real world. The first known purchase took place on May 22, 2010. Four days prior, a Jacksonville, FL-based programmer named Laszlo Hanyecz offered to purchase two pizzas for 10,000 bitcoin on the BitcoinTalk forum. Initially, there were no takers, despite a favorable exchange rate. The Bitcoin Market valued 10,000 bitcoin at around \$41 at the time. "I just think it would be interesting if I could say that I paid for a pizza in bitcoins," Hanyecz posted on May 21. Then, the following day, he confirmed a successful transaction with photos of two large Papa John's pizzas. A user named *jercos* had facilitated the transaction, demonstrating that bitcoin could be used to acquire goods and services in the real world.

<sup>17</sup> A full transcript of bitcoin-list is available from the author upon request.

<sup>18</sup> The transaction can be found in Block #170. No transactions were possible prior to Block #101, since it takes 100 blocks to confirm newly created bitcoin.

The bitcoin economy gradually progressed throughout the rest of 2010. A July 11 Slashdot article introduced bitcoin to a host of new users. The exchange rate increased from \$0.008 on July 12 to \$0.080 on July 17. Jed McCaleb launched the popular exchange site MtGox on July 18. By November 6, the \$0.50 exchange rate on MtGox meant that the bitcoin in circulation were worth more than \$1 million. Further developments, like the first mobile-to-mobile transaction on December 8, demonstrated bitcoin's promise for the future. But by the end of 2010, bitcoin had clearly gotten off the ground.<sup>19</sup>

#### 4 Analyzing bitcoin-list

In the previous section, I presented a general history of the early days of bitcoin. Next, I consider how bitcoin got off the ground. Specifically, I analyze posts to the bitcoin forum, bitcoin-list, paying special attention to instances where the use-value or coordination views are expressed by early participants in the bitcoin community. In general, I find that members understood the importance of coordination and took steps to coordinate users.

The forum launched in December 2008, less than one month before bitcoin.exe v0.1.0 was announced, with a welcome message from Nakamoto. There were 23 posts in total over the course of the year. Nakamoto was the most active, with 11 posts (47.83%). Finney contributed three posts (13.04%). Nicholas Bohm, general counsel for the UK-based Foundation for Information Policy Research, and the pseudonymous Liberty Standard each made two posts (8.7%). Others, including Tyler Gillies, Mike Hearn, Jeff Kane, Eugen Leitl, and Martti Malm, also posted to the forum. The original forum ended on December 17, 2009 when Nakamoto announced a new forum hosted on bitcoin.org. A list of all posts to bitcoin-list, including subject, author, date, and time, is presented in [Table 1](#).

There are several problems with relying exclusively on posts to bitcoin-list. For one, it is a limited window into the conversations surrounding bitcoin at the time. Recall that the initial white paper and release were announced on a separate forum, the Cryptography Mailing List. A similar message to the initial release was not sent to bitcoin-list by Nakamoto until four days after the initial announcement. In the meantime, Finney had already downloaded and attempted to run bitcoin.exe v0.1.0, posting a crash report when the program failed; and Nakamoto had made v0.1.2 available. Likewise, Finney's congratulatory note, dated January 11, 2009, was in reply to the January 8 announcement on the Cryptography Mailing List.<sup>20</sup> Furthermore, Nakamoto frequently requested that users e-mail him directly. For example, in response to a technical problem raised

<sup>19</sup> Nair and Cachanosky (2017) discuss later developments to encourage bitcoin use. See also: Luther and White (2014), Luther (2016a), Luther and Salter (2017)

<sup>20</sup> Several messages seem to be in response to posts on other forums. For example, Nakamoto's January 16, 2009 post references a message from Dustin D. Trammell. The original message from Trammell does not appear on bitcoin-list.



Table 1. Posts to bitcoin-list, 2008–2009

Subject	From	Date	Time
Welcome	Satoshi Nakamoto <satoshi@vi...>	December 10, 2008	5:00:23 p.m.
Crash in bitcoin 0.1.0	Hal Finney <hal.finney@gm...>	January 10, 2009	7:13:18 p.m.
Re: Bitcoin v0.1 released	<hal@fi...>	January 11, 2009	3:16:43 a.m.
Bitcoin v0.1.2 now available	Satoshi Nakamoto <satoshi@vi...>	January 11, 2009	10:32:18 p.m.
Bitcoin v0.1 Alpha release notes	Satoshi Nakamoto <satoshi@vi...>	January 12, 2009	8:20:47 p.m.
Bitcoin v0.1.3	Satoshi Nakamoto <satoshi@vi...>	January 12, 2009	10:48:23 p.m.
Re: Bitcoin v0.1 released	Satoshi Nakamoto <satoshi@vi...>	January 16, 2009	6:35:32 p.m.
Problems	Nicholas Bohm <nbohm@er...>	January 25, 2009	10:17:52 a.m.
Re: Problems	Satoshi Nakamoto <satoshi@vi...>	January 25, 2009	4:45:25 p.m.
Bitcoin works with Wine/Ubuntu	Jeff Kane <kanegs@gm...>	January 30, 2009	2:39:29 a.m.
Bitcoin v0.1.5 released	Satoshi Nakamoto <satoshi@vi...>	February 4, 2009	7:46:04 p.m.
Bitcoin v0.1.5 released	Nicholas Bohm <nbohm@er...>	February 18, 2009	2:55:50 p.m.
Re: Bitcoin v0.1.5 released	Satoshi Nakamoto <satoshi@vi...>	February 22, 2009	5:47:52 p.m.
Re: Bitcoin v0.1.5 released	Hal Finney <hal.finney@gm...>	February 27, 2009	8:00:12 p.m.
Re: Bitcoin v0.1.5 released	Satoshi Nakamoto <satoshi@vi...>	March 4, 2009	4:59:12 p.m.
Bitcoin website update	<mmalmi@cc...>	June 13, 2009	6:41:12 a.m.
new user	tyler gillies <tjgillies@gm...>	August 15, 2009	11:33:44 a.m.
Does Bitcoin Crash in Windows?	Liberty Standard <newlibertystandard@gm...>	October 23, 2009	11:50:10 a.m.
Website Down	Liberty Standard <newlibertystandard@gm...>	October 23, 2009	11:59:34 a.m.
Re: Does Bitcoin Crash in Windows?	Satoshi Nakamoto <satoshin@gm...>	October 23, 2009	11:57:51 p.m.
Re: Does Bitcoin Crash in Windows?	Mike Hearn <mike@pl...>	October 24, 2009	3:05:07 p.m.
Re: Does Bitcoin Crash in Windows?	Eugen Leitl <eugen@le...>	October 26, 2009	12:46:27 p.m.
Bitcoin 0.2 released	Satoshi Nakamoto <satoshin@gm...>	December 17, 2009	6:52:09 a.m.

by Nicholas Bohm on January 25, 2009, Nakamoto recommended sending the debug.log file directly, noting that it is “best not to send attachments to the list.” Similarly, Nakamoto advised Liberty Standard to “e-mail me and I may be able to figure out what happened” if “you get another crash in Wine and it prints anything on the terminal.” Finally, on June 13, 2009, Martti Malmi wrote to bitcoin-list to note that a “new Bitcoin website/portal is up at bitcoin.sourceforge.net.” The new website included a separate forum and Malmi encouraged bitcoin-list users to join the discussion taking place there. With these thoughts in mind, it seems reasonable to suspect that a fair amount of communication was taking place through other channels from the outset.

Another issue concerns the potential power of the evidence contained in the forum. No post to bitcoin-list can adjudicate the central question as to whether bitcoin has some non-monetary use value. The forum cannot tell us whether the value of bitcoin depends exclusively on coordination. And the absence of evidence is, of course, not the evidence of absence – especially considering the limited scope of analysis employed herein. The best one can hope for in surveying the bitcoin-list is some corroboration that users saw some non-monetary value in bitcoin, recognized the importance of coordination, or both.

Despite these limitations, it seems reasonable to sift through the bitcoin forum in search of some evidence for how bitcoin got off the ground. While the potential scope of inquiry is vast, the bitcoin-list provides a convenient boundary within which to focus the analysis. The participants on bitcoin-list were present at the outset. They were considering – and discussing – what it would take for bitcoin to gain acceptance. With this in mind, I maintain that it is worthwhile to consider what they were saying at the time – not that it would be the last word on the matter, but rather that it might provide a useful starting point for meaningful discourse.

In general, the posts to bitcoin-list reveal three recurring themes consistent with the coordination view. First, bitcoin was primarily viewed *as a currency*. To the extent that non-monetary uses are considered, they appear to be an afterthought. Second, the need to coordinate beliefs was widely recognized. Third, a clear strategy to generate coordination was discussed. Specifically, early proponents of bitcoin thought it best to establish a core group of users to get the currency off the ground. Then, they would gradually expand the network to include more and more users. I discuss each of these three themes in turn.

There is little doubt that bitcoin was primarily intended and widely understood to be used as a currency. For example, in the release notes sent out on January 12, 2009, Nakamoto describes “two ways to send money,” where money clearly refers to bitcoin. Hence, even at the earliest stage, bitcoin was thought of as a currency – or, at the very least, a potential currency. And not just by Nakamoto. Other users corroborate this understanding. Tyler Gillies’ succinct post to the forum on August 15, 2009 illustrates the point nicely: “[I] just downloaded bitcoin, epic piece of software. [T]he digital cash age has arrived.”

Other users speculated on the value of bitcoin in the event that it were to succeed as a currency. On January 11, 2009, Finney offered “an amusing thought experiment”:

[I]magine that Bitcoin is successful and becomes the dominant payment system in use throughout the world. Then the total value of the currency should be equal to the total value of all the wealth in the world. Current estimates of total worldwide household wealth that I have found range from \$100 trillion to \$300 trillion. With 20 million coins, that gives each coin a value of about \$10 million.

So the possibility of generating coins today with a few cents of compute time may be quite a good bet, with a payoff of something like 100 million to 1! Even if the odds of Bitcoin succeeding to this degree are slim, are they really 100 million to one against? Something to think about...

Finney’s calculations are questionable. The appropriate value, given his stated view, would be the total value of all currency in circulation or, perhaps, the total value of all currency and checkable deposits – not the total value of household wealth. But what is important for the purposes here is how Finney defined success for bitcoin. Success, according to Finney, would be achieved if bitcoin were to become “the dominant payment system in use throughout the world” – no small feat. And, although he allows for success to some lesser degree, success is always considered in terms of the extent to which bitcoin is employed as a means of payment. Nakamoto concurred, noting that “[i]t might make sense just to get some in case it catches on.”

Recognizing that bitcoin was intended and understood to be used as a currency is not to argue that early advocates did not conceive of alternative, non-monetary applications. There is some evidence of such alternative applications in the original bitcoin forum posts. For example, Finney and Nakamoto discuss timestamping documents to prove that they existed at some specific point in time. But such applications appear as an afterthought and are not considered pressing. “BTW I don’t remember if we talked about this,” Finney wrote when raising the issue. Nakamoto responded by noting the potential use and suggesting he might incorporate it in a future version: “A few lines of code could create a transaction with an extra hash in it of anything that needs to be timestamped. I should add a command to timestamp a file that way.” The alternative use was acknowledged. But it was of secondary importance to bitcoin’s role as a currency.

While bitcoin was intended and understood to be used as a currency, early bitcoin proponents recognized the need to coordinate beliefs in order to achieve that end. As noted above, Finney recognized the valuation problem that alluded earlier monetary economists like Nicholson and Patinkin. Likewise, Nakamoto expressed views remarkably close to those found in the search-theoretic monetary literature today. “If enough people think the same way,” he wrote, “that becomes a self-fulfilling prophecy. Once it gets bootstrapped, there are so many

applications if you could effortlessly pay a few cents to a website as easily as dropping coins in a vending machine.” Again, the goal is for bitcoin to gain widespread acceptance. But, in order for this to happen, early proponents have to get enough people thinking the same way – that is, they must coordinate beliefs.

Coordinating beliefs would be no small task, to be sure. But those on the bitcoin forum discussed a strategy for seeing it through. The idea was to start small. First, establish a core group of users. Prove that the concept works. Then, gradually expand the network.<sup>21</sup> Nakamoto wrote:

It could get started in a narrow niche like reward points, donation tokens, currency for a game or micropayments for adult sites. Initially it can be used in proof-of-work applications for services that could almost be free but not quite. It can already be used for pay-to-send e-mail. [...] Subscription sites that need some extra proof-of-work for their free trial so it doesn't cannibalize subscriptions could charge bitcoins for the trial.

To get off the ground, early bitcoin advocates recognized, you do not need to convince everyone to join the network. You just need a small, reliable user base to anchor the currency. Then, others can join on the expectation that the core group is committed to accepting bitcoin. In doing so, the additional users expand the network and, in turn, encourage still others to join. It is that old Mengerian story, with one very important exception: at the outset, it is coordination – not some non-monetary use value – that gets the ball rolling.

The idea that coordination, as opposed to some non-monetary use, played an important role differs to some extent from earlier efforts to account for bitcoin's successful launch. For example, Ron and Shamir (2013) claim many users adopted bitcoin for political and philosophical reasons. Libertarians or crypto-anarchists might assign a positive value to bitcoin, even if it is not useful as money, because it provides a mechanism for signaling their beliefs to others. Likewise, programmers might realize benefits from participating in the bitcoin community by virtue of working to improve the underlying software. To maintain interest in the network, and thereby continue to improve their own human capital, they might be willing to give up valuable goods and services for bitcoin, even if they have no interest in employing bitcoin as a medium of exchange themselves.

In a recent study, Yelowitz and Wilson (2015) use Google Trends to consider the characteristics of those driving interest in bitcoin. Specifically, they track search trends related to libertarians, computer programming enthusiasts, speculative investors, and criminals. The first two categories of users could conceivably be interpreted as use-value users. Although they might be interested

<sup>21</sup> This strategy also allowed them to prioritize issues. For example, in a March 4, 2009 response to Finney, Nakamoto notes that a particular technical issue “doesn't really matter for now, since the network would have to get huge before the bandwidth is anything more than trivial.”

in bitcoin as a medium of exchange, it is at least plausible that they derive some non-monetary benefit from accepting bitcoin. The third category is ambiguous. Speculation is ultimately based on expectations of network demand, but that demand could be driven (or expected to be driven) by monetary or non-monetary uses. The fourth category, criminals, would seem to imply some monetary demand. Presumably, criminals want to employ bitcoin to buy or sell illegal goods and services at a lower risk of detection than traditional payment mechanisms permit. In general, the authors find that computer programming and illegal activity search terms are positively correlated with bitcoin interest, while libertarian and speculative investment terms are not. Hence, there is some evidence of monetary and non-monetary demand in the early days of bitcoin use.

Although there is much support for the coordination view in the bitcoin forum, the use-value view cannot be ruled out. Much of the correspondence is technical in nature, discussing current bugs or potential changes to the bitcoin code. Surely those working on bitcoin code derived some benefit from doing so. However, it is worth noting that technical issues are typically discussed on the bitcoin forum with explicit reference to network size. For example, in a January 11, 2009 message, Nakamoto laments some of the early bugs: “These problems are kind of screwing up the network and will get worse as more users arrive, so please make sure to upgrade.” Similarly, on February 22, 2009, he expresses interest in adding “interfaces to make it really easy to integrate into websites from any server side language.” Again, the idea is to improve the odds of widespread adoption. In terms of the political and philosophical motivations, little support can be found in the bitcoin forum posts. There is widespread recognition that bitcoin does not require a trusted third party, and Liberty Standard’s username suggests a certain affinity to libertarian ideas. But, otherwise, forum posts do not suggest that libertarianism or crypto-anarchism was a primary driver of interest among the earliest users. Hence, the somewhat crude but more open-ended approach taken here ultimately reaches conclusions quite similar to the more precise but also more constrained approach taken by Yelowitz and Wilson (2015). Early interest in bitcoin was technical and focused largely on ways of making transactions that were not possible or costlier with traditional payment mechanisms.

## 5 Conclusion

In a world dominated by government-issued monies little attention has been given to how an item might get off the ground in the absence of sovereign support. Those who have considered the question have generally held one of two views. The use-value view insists that a private money must have some non-monetary use in order to gain acceptance as a medium of exchange. The coordination view maintains that some non-monetary use is unnecessary since agents might agree to use a money if they believe others will.

The recent launch of bitcoin provides a rare opportunity to consider these two views. Although the existence of some non-monetary use at the outset cannot be ruled out, evidence from the original bitcoin forum, bitcoin-list, indicates that bitcoin was initially intended and understood to be used as a currency, the need to coordinate beliefs was widely recognized, and a clear strategy to generate coordination was discussed. At a minimum, the evidence suggests coordination is a more important contributing factor than some scholars have previously thought. At the same time, it provides a clear example for those who are inclined to believe that coordination is possible but, at least historically, have not devoted much effort toward understanding the process whereby coordination is achieved.

### Acknowledgments

Jesus Fernandez-Villaverde, Hanna Halaburda, Gina Pieters, George Selgin, and seminar participants at the American Institute for Economic Research provided valuable comments on an earlier draft of this paper. Any remaining errors should be attributed to the author.

### References

- Aiyagari, S. R. and N. Wallace (1997), 'Government Transaction Policy, the Medium of Exchange, and Welfare', *Journal of Economic Theory*, 74(1): 1–18.
- Aliprantis, C. D., G. Camera and D. Puzzello (2006), 'Matching and Anonymity', *Economic Theory*, 29(2): 415–432.
- Aliprantis, C. D., G. Camera and D. Puzzello (2007a), 'Anonymous Markets and Monetary Trading', *Journal of Monetary Economics*, 54(7): 1905–1928.
- Aliprantis, C. D., G. Camera and D. Puzzello (2007b), 'Contagion Equilibria in a Monetary Model', *Econometrica*, 75(1): 277–282.
- Anderson, B. M. (1917), *The Value of Money*. Macmillan.
- Araujo, L. (2004), 'Social Norms and Money', *Journal of Monetary Economics*, 51(2): 241–256.
- Araujo, L., B. Camargo, R. Minetti and D. Puzzello (2012), 'The Essentiality of Money in Environments with Centralized Trade', *Journal of Monetary Economics*, 59(7): 612–621.
- Başçı, E. (1999), 'Learning by Imitation', *Journal of Economic Dynamics and Control*, 23(9): 1569–1585.
- Dowd, K. and D. Greenaway (1993), 'Currency Competition, Network Externalities and Switching Costs: Towards an Alternative View of Optimum Currency Areas', *Economic Journal*, 103(420): 1180–1189.
- Duffy, J. (2001), 'Learning to Speculate: Experiments with Artificial and Real Agents', *Journal of Economic Dynamics and Control*, 25(3): 295–319.
- Duffy, J. and J. Ochs (1999), 'Emergence of Money as a Medium of Exchange: An Experimental Study', *American Economic Review*, 89(4): 847–877.
- Duffy, J. and J. Ochs (2002), 'Intrinsically Worthless Objects as Media of Exchange: Experimental Evidence', *International Economic Review*, 43(3): 637–673.

- Duffy, J. and D. Puzzello (2014), 'Gift Exchange versus Monetary Exchange: Theory and Evidence', *American Economic Review*, **104**(6): 1735–1776.
- Fafchamps, M., M. J. Leij and S. Goyal (2010), 'Matching and Network Effects', *Journal of the European Economic Association*, **8**(1): 203–231.
- Fernández-Villaverde, J. and D. Sanches (2016), 'Can Currency Competition Work?' National Bureau of Economic Research, Working Paper 22157.
- Forstater, M. (2006), 'Tax-driven Money: Additional Evidence from the History of Economic Thought, Economic History and Economic Policy', *Complexity, Endogenous Money and Macroeconomic Theory: Essays in Honour of Basil J. Moore*, pp. 202–220.
- Fung, B. and H. Halaburda (2014), 'Understanding Platform-based Digital Currencies', *Bank of Canada Review* (Spring): 12–20.
- Fung, B., S. Hendry and W. E. Weber (2017), 'Canadian Bank Notes and Dominion Notes: Lessons for Digital Currencies', Bank of Canada Staff Working Paper 2017-4.
- Gale, D. (1982), *Money: In Equilibrium*. Cambridge University Press.
- Gandal, N. and H. Halaburda (2014), 'Competition in the Cryptocurrency Market', Bank of Canada Staff Working Paper 2014–33.
- Gans, J. S. and H. Halaburda (2013), 'Some Economics of Private Digital Currency', Bank of Canada Staff Working Paper 2013–38.
- Giansante, S. (2006), 'Social Networks and Medium of Exchange', Working paper.
- Goldberg, D. (2005), 'Famous Myths of "Fiat Money"', *Journal of Money, Credit and Banking*, **37**(5): 957–967.
- Goldberg, D. (2012), 'The Tax-foundation Theory of Fiat Money', *Economic Theory*, **50**(2): 489–497.
- Graf, K. (2013), 'On the Origins of Bitcoin: Stages of Monetary Evolution', Working paper.
- Grinberg, R. (2012), 'Bitcoin: An Innovative Alternative Digital Currency', *Hastings Science & Technology Law Journal*, **4**: 159–207.
- Hahn, F. H. (1965), 'On Some Problems of Proving the Existence of an Equilibrium in Monetary Economies', *The Theory of Interest Rates*, pp. 126–135.
- Hasker, K. and A. Tahmilci (2008), 'The Rise of Money: An Evolutionary Analysis of the Origins of Money', Working paper, Bilkent University.
- Hendrickson, J. R. and W. J. Luther (2017a), 'Banning Bitcoin', *Journal of Economic Behavior & Organization*, **141**: 188–195.
- Hendrickson, J. R. and W. J. Luther (2017b), 'Cash, Crime, and Cryptocurrency', Working paper.
- Hendrickson, J. R. and W. J. Luther (2017c), 'The Value of Bitcoin in the Year 2141 (and beyond!)', Working paper.
- Hendrickson, J. R., T. L. Hogan and W. J. Luther (2016), 'The Political Economy of Bitcoin', *Economic Inquiry*, **54**(2): 925–939.
- Kawagoe, T. (2007), 'Learning to Use a Perishable Good as Money', *Multi-Agent-Based Simulation VII*, **4442**: 96–111.
- King, M. (2004), 'The Institutions of Monetary Policy', *American Economic Review*, **94**(2): 1–13.
- Kiyotaki, N. and R. Wright (1989), 'On Money as a Medium of Exchange', *Journal of Political Economy*, **97**(4): 927–954.
- Kiyotaki, N. and R. Wright (1991), 'A Contribution to the Pure Theory of Money', *Journal of Economic Theory*, **53**(2): 215–235.
- Kiyotaki, N. and R. Wright (1993), 'A Search-theoretic Approach to Monetary Economics', *American Economic Review*, **83**(1): 63–77.

- Knapp, G. F. (1924), *The State Theory of Money*. Macmillan.
- Lagos, R. and R. Wright (2005), 'A Unified Framework for Monetary Theory and Policy Analysis', *Journal of Political Economy*, 113(3): 463–484.
- Lagos, R. and R. Wright (2008), 'When is Money Essential? A Comment on Aliprantis, Camera and Puzzello', Working paper.
- Li, Y. and R. Wright (1998), 'Government Transaction Policy, Media of Exchange, and Prices', *Journal of Economic Theory*, 81(2): 290–313.
- Luther, W. J. (2013), 'Friedman versus Hayek on Private Outside Monies: New Evidence for the Debate', *Economic Affairs*, 33(1): 127–135.
- Luther, W. J. (2016a), 'Bitcoin and the Future of Digital Payments', *Independent Review*, 20(3): 397–404.
- Luther, W. J. (2016b), 'Cryptocurrencies, Network Effects, and Switching Costs', *Contemporary Economic Policy*, 34(3): 553–571.
- Luther, W. J. (2016c), 'Mises and the Moderns on the Inessentiality of Money in Equilibrium', *Review of Austrian Economics*, 29(1): 1–13.
- Luther, W. J. (forthcoming), 'Regulating Bitcoin: On What Grounds?' *Journal of New Finance*.
- Luther, W. J. (2018), 'Is Bitcoin Intrinsically Worthless?' *Journal of Private Enterprise*, 33(1): 31–45.
- Luther, W. J. and J. Olson (2015), 'Bitcoin is Memory', *Journal of Prices & Markets*, 3(3): 22–33.
- Luther, W. J. and A. W. Salter (2017), 'Bitcoin and the Bailout', *Quarterly Review of Economics and Finance*, 66: 50–56.
- Luther, W. J. and L. H. White (2014), 'Can Bitcoin Become a Major Currency?' *Cayman Financial Review*, 36: 78–79.
- Luther, W. J. and L. H. White (2016), 'Positively Valued Fiat Money after the Sovereign Disappears: The Case of Somalia', *Review of Behavioral Economics*, 3(3–4): 311–334.
- Marimon, R., E. McGrattan and T. J. Sargent (1990), 'Money as a Medium of Exchange in an Economy with Artificially Intelligent Agents', *Journal of Economic Dynamics and Control*, 14(2): 329–373.
- Menger, C. (1892), 'On the Origin of Money', *Economic Journal*, 2(6): 239–255.
- Mises, L. von (1934), *The Theory of Money and Credit*. Jonathan Cape.
- Nair, M. and N. Cachanosky (2017), 'Bitcoin and Entrepreneurship: Breaking the Network Effect', *Review of Austrian Economics*, 30(3): 263–275.
- Nicholson, J. S. (1895), *A Treatise on Money and Essays on Monetary Problems* (3rd edition), Adam and Charles Black.
- Ostroy, J. M. and R. M. Starr (1990), 'The Transactions Role of Money', *Handbook of Monetary Economics*, 1: 3–62.
- Patinkin, D. (1965), *Money, Interest, and Prices: An Integration of Monetary and Value Theory*. Harper and Row.
- Popper, N. (2015), *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. HarperCollins.
- Ron, D. and A. Shamir (2013), 'Quantitative Analysis of the Full Bitcoin Transaction Graph', *Financial Cryptography and Data Security*, pp. 6–24.
- Rupert, P., M. Schindler, A. Shevchenko and R. Wright (2000), 'The Search-theoretic Approach to Monetary Economics: A Primer', *Economic Review*, 36(4): 10–28.
- Salter, A. W. and W. J. Luther (2014), 'Synthesizing State and Spontaneous Order Theories of Money', *Advances in Austrian Economics*, 18: 161–178.



- Scott, W. A. (1897), 'The Quantity Theory', *Annals of the American Academy of Political and Social Science*, 9(2): 40–58.
- Selgin, G. (2015), 'Synthetic Commodity Money', *Journal of Financial Stability*, 17: 92–99.
- Selgin, G. A. (1994), 'On Ensuring the Acceptability of a New Fiat Money', *Journal of Money, Credit and Banking*, 26(4): 808–826.
- Selgin, G. A. (2003), 'Adaptive Learning and the Transition to Fiat Money', *Economic Journal*, 113(484): 147–165.
- Selgin, G. A. and L. H. White (1987), 'The Evolution of a Free Banking System', *Economic Inquiry*, 25(3): 439–457.
- Selgin, G. A. and L. H. White (1994), 'How Would the Invisible Hand Handle Money?' *Journal of Economic Literature*, 32(4): 1718–1749.
- Shy, O. (2011), 'A Short Survey of Network Economics', *Review of Industrial Organization*, 38(2): 119–149.
- Staudinger, S. (1998), 'Money as Medium of Exchange – An Analysis with Genetic Algorithms', *IFAC Proceedings Volumes*, 31(16): 93–98.
- Sumner, S. (1993), 'Privatizing the Mint', *Journal of Money, Credit and Banking*, 25(1): 13–29.
- Sumner, S. (2000), 'Is Nonprice Competition in Currency Inefficient? A Comment', *Journal of Money, Credit and Banking*, 32(1): 146–149.
- Weber, W. E. (2014), 'The Efficiency of Private E-money-like Systems: the US Experience with State Bank Notes', Bank of Canada Staff Working Paper 2014–15.
- Weber, W. E. (2015a), 'Government and Private E-money-like Systems: Federal Reserve Notes and National Bank Notes', Bank of Canada Staff Working Paper 2015–18.
- Weber, W. E. (2015b), 'The Efficiency of Private E-money-like Systems: the US Experience with National Bank Notes', Bank of Canada Staff Working Paper 2015-3.
- Weber, W. E. (2016), 'A Bitcoin Standard: Lessons from the Gold Standard', Bank of Canada Staff Working Paper 2016-14.
- White, L. H. (1987), 'Accounting for Non-interest-bearing Currency: A Critique of the Legal Restrictions Theory of Money', *Journal of Money, Credit and Banking*, 19(4): 448–456.
- White, L. H. (2015), 'The Market for Cryptocurrencies', *Cato Journal*, 35(2): 383–402.
- White, L. H. and D. J. Boudreaux (1998), 'Is Nonprice Competition in Currency Inefficient?' *Journal of Money, Credit and Banking*, 30(2): 252–260.
- White, L. H. and D. J. Boudreaux (2000), 'Is Nonprice Competition in currency inefficient? A Reply', *Journal of Money, Credit and Banking*, 32(1): 150–153.
- Yelowitz, A. and M. Wilson (2015), 'Characteristics of Bitcoin Users: An Analysis of Google Search Data', *Applied Economics Letters*, 22(13): 1030–1036.
- Yermack, D. (2013), 'Is Bitcoin a Real Currency? An Economic Appraisal', National Bureau of Economic Research, Working Paper 19747.