No. 13-17
September 2013

# WORKING PAPER

## CRYPTOCURRENCIES, NETWORK EFFECTS, AND SWITCHING COSTS

by William J. Luther

MERCATUS CENTER
George Mason University

## About the Author

William J. Luther
Kenyon College
Department of Economics
lutherw@kenyon.edu

## Abstract

Cryptocurrencies are digital alternatives to traditional government-issued paper monies. Given the current state of technology and skepticism regarding the future purchasing power of existing monies, why have cryptocurrencies failed to gain widespread acceptance? I offer an explanation based on network effects and switching costs. In order to articulate the problem that agents considering cryptocurrencies face, I employ a simple model developed by Dowd and Greenaway (1993). The model demonstrates that agents may fail to adopt an alternative currency when network effects and switching costs are present, even when all agents agree that the prevailing currency is inferior. The limited success of Bitcoin—almost certainly the most popular cryptocurrency to date—serves to illustrate. After briefly surveying episodes of successful monetary transition, I conclude that cryptocurrencies like Bitcoin are unlikely to generate widespread acceptance in the absence of either significant monetary instability or government support.

***JEL* codes:** E40, E41, E42, E49

**Keywords:** Bitcoin, cryptocurrency, currency competition, lock-in, medium of exchange, monetary standard, money, network effects, path dependence, spontaneous switching, standardization

**Cryptocurrencies, Network Effects, and Switching Costs**

William J. Luther

> Just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions.
>
> —*Timothy May,* The Crypto Anarchist Manifesto*, 1992*

Recent technological advances have significantly lowered the cost of processing electronic payments. Electronic banking and digital wallets (also called e-wallets) allow individuals to transfer funds securely. Whereas these services were used almost exclusively for remote transactions in the past, the widespread adoption of smartphones has made it easier to make and receive payments in person with electronic bank accounts and digital wallets. More recently, the development of inexpensive card-reading devices has enabled virtually anyone to accept electronic payments.[1] With a simple click, tap, or swipe, individuals can now transact without having to handle physical cash or write checks.

At the same time, there has been a growing concern over the safety and stability of some of the most widely used currencies. Successive rounds of quantitative easing in the United States have been met with opposition, as some users of the dollar fear the currency will be worth significantly less in the future. Similarly, instability in Europe prompts fears of the devaluation or outright collapse of the euro. Although many continue to put their trust in dollars and euros, uncertainty abounds.

In this context, a small but vocal minority has turned to cryptocurrencies. Cryptocurrencies are digital alternatives to traditional government-issued paper monies.

[1] Square—a company that processes electronic payments via smartphones, iPads, and computers—sends its users a complimentary card-reading device. There are no upfront costs to Square users. Square charges a per-transaction rate equal to 2.75 percent of the balance transferred. PayPal offers a similar product—PayPal Here—while charging just 2.7 percent.

Cryptography is used to ensure that transactions are secure, to prevent users from spending the same balance more than once, and to govern the supply of digital notes in circulation. Some cryptocurrencies are decentralized, enabling quasi-anonymous transactions and making it difficult for governments to regulate them. Moreover, the electronic nature of cryptocurrencies means they are relatively easy to use across international borders.

Given the current state of technology and skepticism regarding the future purchasing power of existing monies, why have cryptocurrencies failed to gain widespread acceptance? I offer a simple explanation based on network effects and switching costs. In order to articulate the problem that agents considering cryptocurrencies face, I employ a simple model developed by Dowd and Greenaway (1993). The model demonstrates that agents may fail to adopt an alternative currency when network effects and switching costs are present, even when all agents agree that the prevailing currency is inferior. The limited success of Bitcoin—almost certainly the most popular cryptocurrency to date—serves to illustrate. After briefly surveying episodes of successful monetary transition, I conclude that cryptocurrencies like Bitcoin are unlikely to generate widespread acceptance in the absence of either significant monetary instability or government support.

## I. A Model of Currency Acceptance with Network Effects and Switching Costs

In order to explore currency competition, monetary unionization, and currency substitution, Dowd and Greenaway (1993) develop a simple model of currency acceptance. Their approach differs from earlier models in two important respects. First, they assume money is subject to a

network effect.[2] In other words, the value conferred to a user of a particular currency depends, at least in part, on the number of other users willing to transact with that currency. Second, they include a cost of switching from one currency to another. Switching costs might arise from the need to retool vending and automatic teller machines, update menus and transaction records, or learn to think and calculate in terms of a new unit of account. With these two features—network effects and switching costs—the authors are able to articulate a model where agents might either switch or continue to accept currencies suboptimally.

### *A. The Core Model*

There are $N$ money-using agents in the model space. Each agent lives forever and uses a particular currency. Initially, the agents have no choice about which money to use and expect to use it forever. The utility an agent derives using the money from time $T$ onwards can be written as $u(T) = (a + bn) \int_T^\infty e^{-r(t-T)}dt = (a + bn)/r$, where $a$ and $b$ are fixed parameters, $r$ is the discount rate, and $n \equiv ln(N)$.[3] The network effect is captured by $n$, which increases with $N$ but at a diminishing rate. The term $bn$ denotes the network-related benefits from using the same money as $N - 1$ other agents. Notice that, when $N = 1$, $bn = 0$. In other words, an agent derives no network-related benefits when no one else uses the money. Assuming $b > 0$ implies network-related benefits are positively related to the size of the network. Any benefits independent of

[2] Network effects were originally modeled in the context of competing technological standards (e.g., Katz and Shapiro 1985, 1986; Farrell and Saloner 1986; Arthur 1989). See also David (1985) and Liebowitz and Margolis (1990, 1994, 1995).

[3] The discount rate $r$ is assumed to be fixed. It can be thought of as the real interest rate.

network size are represented by $a$. Hence, the net present value of using the same money as $N-1$ other agents over the period $(T,\infty)$ can be expressed as $(a+bn)/r$.[4]

To analyze currency acceptance when alternatives are present, suppose a new money unexpectedly becomes available at time $T=T^*$. The new money is assumed to be at least as good as the old money, irrespective of network size. Since agents are limited to using just one currency, each agent must decide whether to continue using the old money or incur a one-time fixed cost $s$ to switch to the potentially superior alternative. If $N$ agents choose to use the new money, they each earn utility $v(T)=\left[(c+dn)\int_T^\infty e^{-r(t-T)}dt\right]-s=(c+dn)/r-s$, $T\geq T^*$, where $c$ and $dn$ respectively denote the network-independent and network-related benefits from using the new money.[5]

Switching to the potentially superior money at time $T=T^*$ increases aggregate welfare if and only if $Nu(T)_N<Nv(T)_A$, where $u(T)_N$ is the utility of a representative agent continuing to use the old money when no other agents switch and $v(T)_A$ is the utility of the representative agent switching to the new money when all other agents switch.[6] Substitution yields $N(a+bn)/r<N[(c+dn)/r-s]$. Hence, it is socially optimal to switch when $s<[c-a+(d-b)n]/r$—that is, when the representative agent finds that the cost of switching is less than the net gain in utility from switching.

Next, consider the conditions under which it is in an individual agent's interest to switch to the new money at time $T=T^*$. An agent will switch regardless of whether other agents switch if $u(T)_N<v(T)_N$, where $v(T)_N$ is the utility of the representative agent switching to the new

[4] A more realistic model might discount a nontrading partner's participation in one's network. However, this increases complexity without adding much value for the application considered herein.
[5] The assumption that the new money is at least as good as the old money, irrespective of network size, can be expressed as $c\geq a$, $d\geq b$.
[6] Since agents are homogeneous and both monies are subject to network effects, maximizing aggregate welfare in this simple model requires that all agents employ the same currency.

money when no other agents switch. An agent who switches when no one else does forgoes network-related benefits, receiving only the net present value of the non-network benefits of the new currency, minus the cost of switching. Hence, $v(T)_N = c/r - s$. It follows, then, that an agent will switch to the new money when $s < c - a - bn)/r$ (i.e., when the cost of switching is sufficiently low).

Conversely, it is in an agent's interest to continue transacting with the old money at time $T = T^*$ regardless of whether other agents switch if $u(T)_A > v(T)_A$, where $u(T)_A$ is the utility of the representative agent continuing to use the old money when all other agents switch to the new money. Again, an agent comprising the entire network receives only the net present value of non-network benefits. Hence, $u(T)_A = a/r$ and an agent will continue using the old money when $s > (c - a + dn)/r$ (i.e., when the cost of switching is sufficiently high).

A graphical representation of the model is presented in figure 1. The cost of switching to the new money is measured along the horizontal axis. The percentage of the population the model predicts will switch—given the parameters $a, b, c, d, n, r, s$—is tracked along the vertical axis. Recall that, when the cost of switching is less than the net gain in utility from switching (i.e., $s < [c - a + (d - b)n]/r$), it is socially optimal for all agents to switch to the new money. If, on the other hand, $s > [c - a + (d - b)n]/r$, it is socially optimal for no agents to switch to the new money—that is, all agents would be best served if they all continued transacting with the old money.

**Figure 1. Network Effects, Switching Costs, and the Percentage of the Population Switching to a New Money**

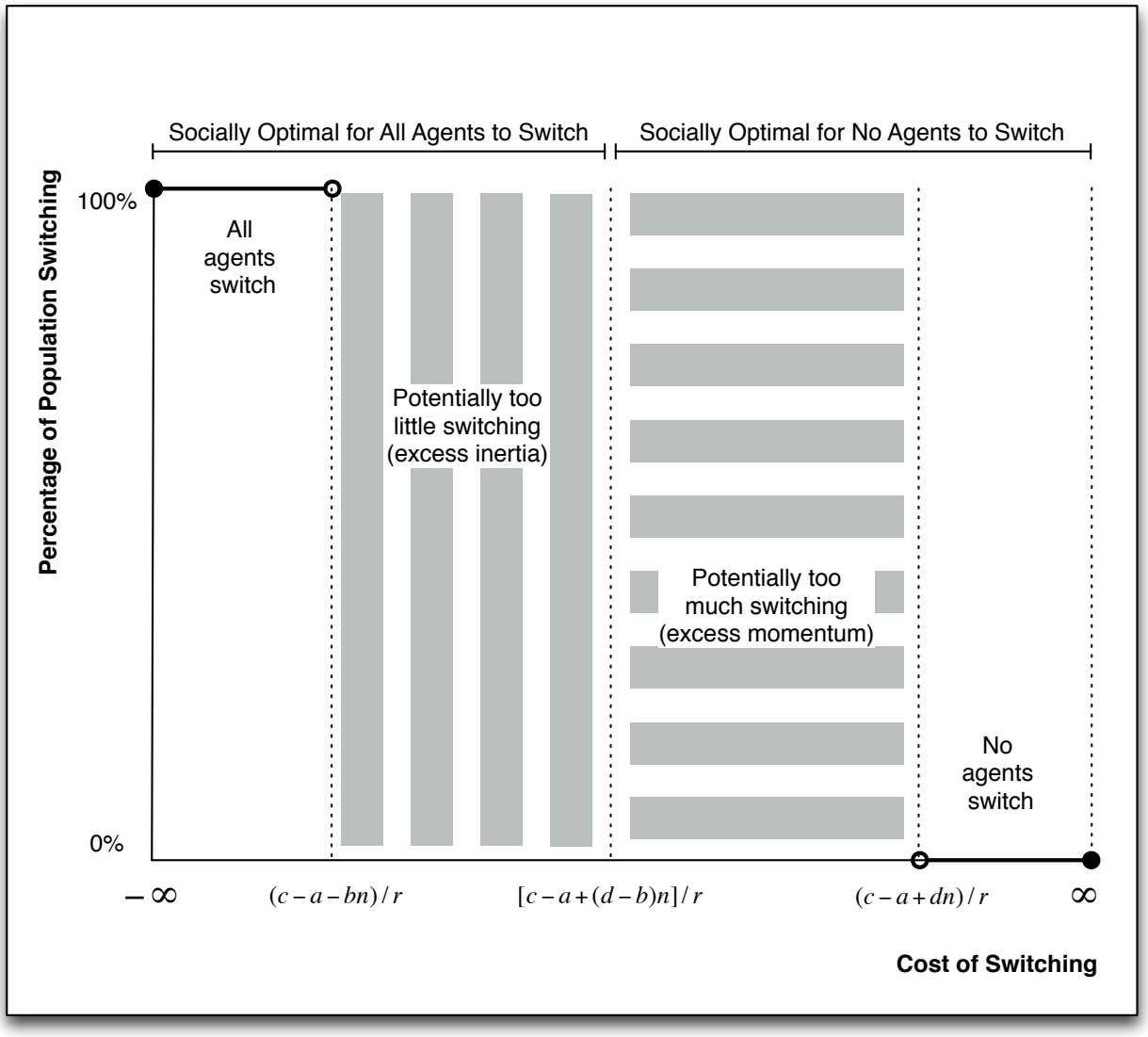



Figure 1 illustrates that, for some parameterizations, decentralized decision-making may fail to maximize aggregate welfare. Since agents are homogeneous, the model predicts that all agents will switch if switching costs are sufficiently low and that no agents will switch if switching costs are sufficiently high. However, the model is ambiguous regarding whether any or all agents will switch to the new money between these two boundary cases—that is, for

switching costs $(c - a - bn)/r \geq s \geq (c - a + dn)/r$. There is the potential (1) that some agents will continue to use the old money when maximizing social welfare requires all agents to switch to the new money, and (2) that some agents will switch to the new money when maximizing social welfare requires all agents to continue to use the old money. In another context, Farrell and Saloner (1986) refer to these cases as demonstrating *excess inertia* and *excess momentum*, respectively. Both are suboptimal.

The potential for excess inertia and excess momentum arises because, with network effects, an agent's expected utility from switching (and refraining from switching) depends crucially on whether other agents are expected to switch. If many agents are expected to switch to the new money, the expected network-related benefits of the new money are large and the utility expected from employing the new money is more likely to warrant the cost of switching. Similarly, if few agents are expected to switch to the new money, the expected network-related benefits of the new money are small and the utility expected from employing the new money is less likely to warrant the cost of switching. In other words, the existence of network effects means expectations matter; but the model, as stated, provides no basis for agents to coordinate expectations.

### *B. The Case against Excess Momentum*

The Dowd and Greenaway (1993) model described above can be used to explain both too little and too much switching. It is my view, however, that—at least in terms of currency acceptance—excess momentum is unlikely. To justify this position, I move beyond the core model to discuss the process through which expectations are formed and how the process might limit the set of expectations human subjects are able to hold. I argue that adaptive learning deters agents from spontaneously adopting an alternative currency. As demonstrated below, this

position is consistent with the available historical and experimental evidence; it is also a standard assumption in agent-based computational models of currency acceptance.

Agents face a serious problem in the model described above. Consider a representative agent. In order to make an informed decision and maximize his own welfare, he must know which money other agents will decide to use. If this information is unavailable, as assumed in the model above, he must form an expectation about the decisions of all other agents. Of course, their decisions also rely on expectations. So, for our representative agent to form an expectation about the decisions others will make, he must form an expectation about their expectations—their expectations of his expectation, their expectations of his expectation of their expectations, and so on. In short, every agent is simultaneously trying to guess what every other agent will do based on what every other agent knows, what every other agent knows every agent knows, and so on. How might this problem be resolved?

Some may be tempted to eliminate this problem by assuming the agents in the model are hyperrational. The term hyperrational denotes that agents have (1) unbiased beliefs and (2) the cognitive capacity to derive their optimal behavior contingent on these beliefs. If all agents know from the outset what all other agents will do, the ambiguity discussed above disappears; without epistemic limitations, they can coordinate on the superior equilibrium, thereby maximizing social welfare. Voilà! All is right with the world.

Unfortunately, the hyperrational solution offers little help when considering the decisions of human agents. Human agents are almost certainly not endowed with the information required by the hyperrational solution. Instead, they must learn through a process of social interaction as time unfolds. They must expend valuable resources in order to coordinate economic activity with

others. And, when the costs of coordinating are too high, they must rely on existing social institutions or historical experience.

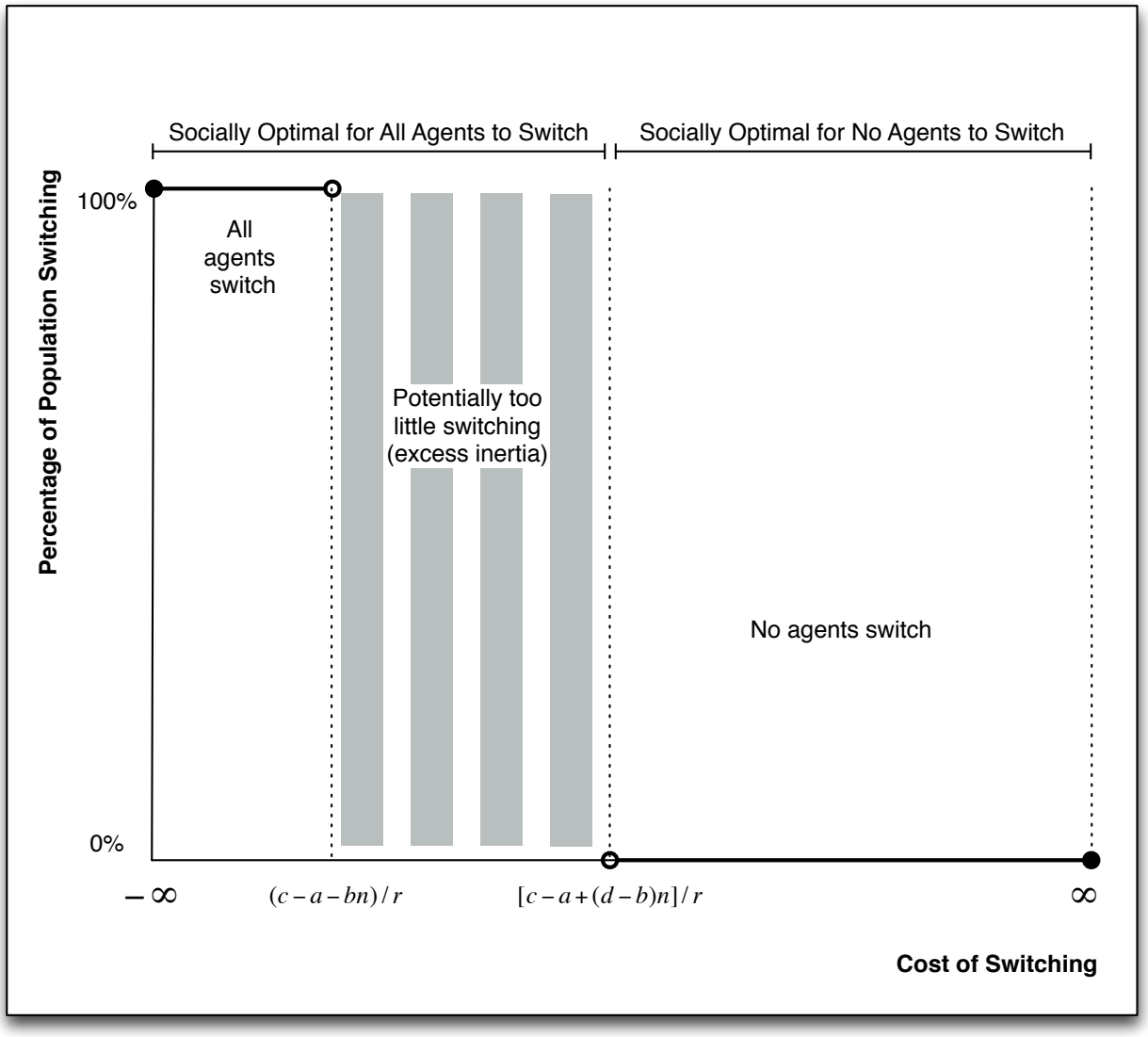
Along these lines, Selgin (2003) employs Elison and Fudenberg's (1993) "rule of thumb" learning algorithm to consider whether fiat money can emerge naturally in economies starting with barter or commodity money. Expectations in Selgin's (2003, 153) model are "'static' and 'adaptive' rather than 'rational' in so far as the rule of thumb on which they are based itself remains uninfluenced by experience." Requiring that agents update beliefs adaptively does not preclude the emergence of commodity monies from barter. Since some individuals are willing to accept the commodity ultimately employed as money from the outset, the less-than-hyperrational agents in Selgin's model are capable of learning beliefs consistent with commodity money equilibria. In contrast, Selgin demonstrates that these agents cannot learn the beliefs consistent with fiat money equilibria on their own because no agent accepts an intrinsically worthless item at the outset and, therefore, has no basis to believe anyone will ever accept it. Selgin claims this result is consistent with the historical record. Where fiat monies exist, they are the product of governments—either directly, as when a government introduces the money, or indirectly, as when it fails to enforce the contractual obligation to redeem paper banknotes for the underlying commodity. By limiting beliefs to those consistent with an adaptive learning algorithm, Selgin is able to articulate the significance of social institutions for the existence of fiat monies.

In considering how a government might launch a new fiat money, Selgin (1994) expresses a similar backward-looking view and discusses intellectual antecedents. Whereas the model presented herein demonstrates that the superiority of an alternative money is not a sufficient condition for successful transition, he considers whether a necessary condition

exists. Specifically, Selgin (1994, 823) argues that "a new fiat money must be operationally linked to some established money if it is to achieve a positive value," and he finds no evidence of successful currency reforms inconsistent with his view. I take it for granted that the alternative money is potentially superior, and therefore has a plausible prospect of achieving widespread acceptance, in order to explore whether, in fact, it will. Nonetheless, our approaches are similar: we both assume agents are less than hyperrational and stress the importance of historical acceptance.

Adaptive learning as put forth formally by Selgin (2003) is a rather strong modeling assumption. In the model presented herein, his conception of adaptive learning would preclude switching in all cases except where the cost of switching, $s$, is less than $(c - a - bn)/r$ and it is in an agent's interest to switch even if no other agent is willing to do so. In contrast, one might accept a weaker notion of adaptive learning where historical acceptance is one of many factors potentially affecting belief acquisition. According to this view, agents find themselves in a sort of coordination game—trying to guess whether others will switch and relying on focal points to coordinate behavior. Insofar as it is an experience shared by all agents, historical acceptance would seem to be a particularly salient focal point in this environment. With historical acceptance, the incumbent money functions as a default option. Absent another more salient focal point favoring the alternative money, the incumbent money has a tendency to persist.

**Figure 2. Percentage of Population Switching to a New Money When Historical Acceptance Serves as Dominant Focal Point**




As shown in figure 2, historical experience eliminates one set of suboptimal outcomes—those associated with excess momentum—when it serves as the dominant focal point. So long as no one tries to coordinate a transition to the new money, everyone will continue using the old

money. And, since $S > [c - a + (d - b)n]/r$, no agent is willing to bear a non-negative cost to establish a new dominant focal point.[7] As a result, everyone continues to use the old money.

The available evidence from experiments with human subjects is consistent with the view presented herein. Brown (1996) and Duffy and Ochs (1999, 2002) demonstrate that many agents do not employ equilibrium-consistent strategies from the outset in commodity and fiat money environments. However, agents usually get better as play evolves and the subjects gain experience.[8] Duffy (2001) goes even further, using artificial agents to anchor the beliefs of human subjects under parameterizations where equilibrium requires that agents employ nonsalient trading strategies. He finds that anchoring beliefs in this manner increases the speed of learning.

Similar results have been found using agent-based computational models, where it is standard practice to assume agents employ adaptive learning algorithms (e.g., Marimon, McGrattan, and Sargent 1990; Staudinger 1998; Başçi 1999; Giansante 2006; Kawagoe 2007; and Hasker and Tahmilci 2008).[9] In general, these authors find strong convergence to optimal behavior under many (but not all) parameterizations.[10] Exploring parameterizations similar to those found in Duffy (2001), where agents would do best by employing a nonsalient trading strategy, Başçi (1999) finds that allowing agents to learn by imitating the successful strategies of other agents (in addition to their own experience) increases the degree of equilibrium-consistent behavior.

[7] A representative agent's maximum willingness to pay to establish a new focal point is determined by the net gain in utility from switching less the cost of switching. Over the range considered, $[c - a + (d - b)n]/r - s < 0$.
[8] In their studies, improvements are properly signed, if not always statistically significantly.
[9] See also Yasutomi (1995, 2003) and Shinohara and Gunji (2001).
[10] For example, Kawagoe (2007) finds that artificial agents are reluctant to employ a perishable good as money, even under parameterizations where accepting such an item would result in greater utility.

### *C. Excess Inertia and the Cost of Coordination*

While historical acceptance reduces the set of suboptimal outcomes when it is the dominant focal point, it does not preclude agents from failing to adopt a superior alternative. The potential for excess inertia remains. Indeed, historical acceptance may exacerbate the problem. If the shared experience of accepting a particular money provides an especially strong focal point, agents will not be easily persuaded that others will stop using the money when it is socially optimal to do so. As a result, they may be even more reluctant to switch than they would be in the absence of a historically determined focal point.

Successful transition to the superior alternative in the indeterminate area of figure 2 depends crucially on the cost of coordination. If agents have mechanisms to coordinate cheaply, optimal switching is more likely to result. If such mechanisms do not exist, are prohibitively expensive, or are not powerful enough to overcome the historical focal point, too few agents will switch and excess inertia will perpetuate the incumbent money. To see this more clearly, consider whether a representative agent is willing to enter into contracts with others to address the problem. Let $\kappa/N \geq 0$ be the per person cost of establishing a new dominant focal point. Since the net benefit of universally adopting the new money is greater than the cost of switching over the relevant range, the agent is willing to pay a small fee $\varepsilon \leq [c - a + (d - b)n]/r - s > 0$. Under some parameterizations (i.e., when $\varepsilon \geq \kappa/N$), agents might pool their resources to cover the cost of coordination, thereby enabling a transition to the superior money. If the cost of coordination is sufficiently high, however, historical acceptance will continue to serve as the dominant focal point; agents will continue to employ the historically accepted money.

What are the conditions under which agents might coordinate on the superior money? For starters, agents must be able to communicate. They must also have access to a focal point that is

powerful enough to overcome the status quo. If they do not possess a mechanism to contract around the problem, either because they cannot communicate or because they do not have a potential dominant focal point at their disposal, the cost of coordination is effectively infinite. Provided that contracting around the problem is an option, standard game-theoretic analysis suggests coordination is more likely to result in small groups of homogeneous agents with sufficiently low discount rates. Although minor deviations from these characteristics do not preclude coordination outright, they would likely increase the cost $\kappa$. Recall that, for a given cost of switching, the higher $\kappa$ is, the better the alternative money must be to justify the cost of coordination.

## II. Bitcoin

Having articulated a simple model of currency acceptance and the conditions under which a superior alternative might supplant an existing money, I consider why cryptocurrencies have failed to gain widespread acceptance. In doing so, I focus on the case of Bitcoin, which is almost certainly the most successful cryptocurrency to date. After clarifying what Bitcoin is and how it works, I use the model developed above to explain why it has failed to gain widespread acceptance and is unlikely to do so in the future.[11] The model is also used to make sense of Bitcoin's limited success.

### *A. A Brief Overview*

Bitcoin is a peer-to-peer cryptocurrency developed by Satoshi Nakamoto (2008) that was launched in January 2009.[12] The peer-to-peer nature of the Bitcoin system means that there is no central clearinghouse. Instead, transactions are processed in a decentralized manner through the

[11] Grinberg (2012) provides a more thorough review of Bitcoin, its ecosystem, and the surrounding legal issues.
[12] Many believe "Satoshi Nakamoto" is in fact a pseudonym. The developer has not been heard from since April 2011.

simultaneous efforts of contributors. Cryptography is employed to transfer funds securely, while exchange between addresses (as opposed to individuals) enables quasi-anonymous transactions. Bitcoins can be traded for goods and services with other users via a personal computer or smartphone; swapped for traditional currencies on a Bitcoin exchange; donated to a political party, charity, or friend; or mined by successfully verifying the transactions of others. With sufficient maintenance from the Bitcoin community, Barber et al. (2012, 399) maintain that Bitcoin could be "a serious candidate for a long-lived stable currency."

Transacting with bitcoins is a lot like using any other digital payment system, except that the underlying money is not a traditional currency (e.g., dollar, euro, yen, etc.).[13] Users install the open-source Bitcoin client on their computers to manage accounts. In order to accept payments, receivers publish a unique address where senders can transfer bitcoins. Cryptography ensures transfers are secure. Senders encode the payment with the receiver's public key, using their own private keys to authorize the transfer of funds. Receivers then decode the payment with their own private keys, thereby depositing the funds in their accounts. Payments encoded with a public key can only be decoded with the corresponding private key. So long as users keep their private keys secure, unauthorized payments cannot be made from their accounts; nor can payments be intercepted by a third party once they have been sent.

The real innovation of Bitcoin concerns the way in which transactions are processed.[14] In order for a transaction to be completed, it must be added to the official block chain—a public

[13] Selgin (2012) describes Bitcoin as a "synthetic-commodity money" in that it is both intrinsically worthless (i.e., not used for any nonmonetary purpose) and scarce. Other monies falling outside the traditional classification scheme include the Iraqi Swiss dinar (King 2004) and the Somali shilling (Luther and White 2011; Luther 2012a, 2012b, 2013).
[14] Unlike cash balances, which literally change hands during a transaction, digital balances require proper checks to ensure a sender does not spend the same balance more than once. Most electronic payment systems rely on a central clearinghouse to prevent double spending. Consider how a bank processes an electronic check: the sender issues an electronic check to the receiver and the receiver accepts the check. The bank then debits the account of the sender and credits the account of the receiver. In doing so, the bank prevents the sender from spending the transferred funds again.

record of all past transactions—by a Bitcoin miner.[15] Any member of the network can function as a miner, provided that member is willing to hash the block of transactions to be added to the block chain. In doing so, the member checks the existing block chain to make sure that the sender had the requisite funds before the transaction, thereby preventing a sender from spending the same balance more than once. Once hashed, the transaction block is added to the block chain, thereby informing all future transactions.[16]

Hash values must meet strict criteria; therefore, miners must expend costly computing power hashing a new block.[17] Since the Bitcoin protocol recognizes the longest block chain as genuine, this "proof of work" precludes would-be fraudsters from altering the block chain. Undoing a past transaction would require reproducing the entire block chain from the altered transaction forward faster than any other miner can verify the next transaction—a very unlikely event if no one controls the majority of computing power in the system.[18] As a result, hashing means transactions are effectively irreversible.

Since hashing is costly, the Bitcoin protocol provides a built-in incentive for miners during the early adoption phase. The first miner to successfully hash a new block is immediately credited with a small amount of new bitcoins—hence, the name "miners." The number of bitcoins earned from mining declines over time. Between January 2009 and May 2012, miners earned 50 bitcoins per block. The prize fell to 25 bitcoins in 2013. It will continue to fall by half

[15] Kocherlakota and Wallace (1998) and Kocherlakota (1998, 2002) compare money to a recordkeeping device, which they call memory. Luther and Olson (2013) argue that Bitcoin is an application of the money-is-memory view.
[16] Babaioff et al. (2012) worry that the Bitcoin protocol provides no incentive for nodes to broadcast transactions.
[17] In other words, it is not enough to demonstrate that the new transaction fits into the block chain. The hash value must also conform to some given parameters specified by the Bitcoin protocol. As a result, miners may have to hash the block multiple times before producing an acceptable solution.
[18] Cryptography limits the fraudsters to altering only those transactions they are party to (i.e., they cannot reverse transactions between other users).

every four years, as the total supply asymptotically approaches 21 million bitcoins.[19] When the prospect of new bitcoins is insufficient to encourage mining, users can pay a voluntary transaction fee.[20]

From an individual user's perspective, Bitcoin has several desirable properties.[21] As mentioned above, Bitcoin transactions are effectively irreversible. Bitcoins are similar to cash in this regard since, unlike with credit and debit cards, there is no possibility for chargebacks. Hence, vendors need not worry that they could be handing over valuable goods and services only to have the payment returned to the buyer at some future date.[22]

Another potentially desirable property of Bitcoin is that it does not rely on the discretion of a government or central bank. Instead, the supply of bitcoins is governed by a strict rule. The Bitcoin protocol regulates the speed of hashing—and, hence, the mining of new bitcoins—by altering the hash value criteria. If computing power increases, for example, the protocol quickly recognizes that blocks are being hashed too quickly. It responds by making the hash value criteria more stringent, thereby slowing down the production of new bitcoins. As a result, the supply of bitcoins follows a predetermined growth path.

Bitcoin also facilitates very small transactions and precise prices. The subunit, satoshi, is equal to $10^{-8}$ of a bitcoin. In the absence of satoshis, small transactions would most likely rely on barter, bundling, credit, or gifting; prices would have to be rounded in terms of a less precise unit of account.

---

[19] Although the Bitcoin protocol limits the long-run supply of outside money, it does not prohibit the creation of inside money.

[20] At present, transaction fees are almost exclusively offered in complicated transactions where bitcoins are drawn from multiple accounts. Most transactions do not involve a fee.

[21] For a more complete list of the benefits of Bitcoin, see Barber et al. (2012).

[22] Buyers, on the other hand, are left without recourse if purchased goods are not delivered. For the system to work, sellers—who are more likely to be fixed entities—must establish reputations that provide buyers with the confidence necessary to warrant exchange.

Perhaps most importantly, Bitcoin enables quasi-anonymous transacting.[23] Although the block chain provides a public record of all past transactions, these transactions take place between addresses—not users—and users do not have to reveal any information that would enable identification. As Nakamoto (2008, 1) explains, "The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone." Moreover, one can create multiple addresses, further obscuring one's true identity. "In fact," Ron and Shamir (2012, 4) note, "it is considered good practice for a user to generate a new address, i.e., public-private key-pair, for every transaction even if this is not necessary." The result is a degree of anonymity not provided by other means of payment.

Despite these benefits, the best available evidence suggests that the network of users transacting with bitcoins (i.e., sending and receiving) is relatively small.[24] For starters, most bitcoins appear to be employed as either a store of value or a speculative bet on the value of bitcoins increasing, as opposed to being held as a medium of exchange. Ron and Shamir (2012, 7) report that 7,019,100 of 9,000,050 bitcoins available as of May 13, 2012, or 77.99 percent, had accumulated in the accounts of 609,270 addresses that receive but never send bitcoins. Three-fourths of these—nearly 60 percent of all bitcoins in the system—were received at least three months before their study. Even after excluding balances stashed before the bitcoin exchange Mt.Gox opened in July 2010, on the grounds that they were accumulated by early users who had since left the system and should therefore be considered "lost" rather than "hoarded,"

[23] Reid and Harrigan (2011) explore the degree of anonymity provided by Bitcoin.

[24] Of course, Bitcoin has undesirable properties as well. For example, it is prone to hacker attacks and is not backed by a sovereign nation. These features may account for its failure to gain widespread acceptance. However, proponents of Bitcoin often take its superiority for granted. I follow that approach here in order to show that *even if* it is superior it might still fail to gain widespread acceptance. For more on the undesirable properties of Bitcoin, see Luther and Olson (2013).

the authors find that more than half of all bitcoins had been dormant for three or more months before the study cutoff date.

The trivial sums received by most users provide another reason to believe the network of Bitcoin transactors is small. Of the 2,460,816 unique users identified by Ron and Shamir (2012, 7), 893,763—or 36.32 percent—had received less than 1 bitcoin in their entire transaction history.[25] Another 389,302 users—or 15.82 percent—received between 1 and 10 bitcoins. Only 40,652 users had received 1,000 or more bitcoins. The distribution and cumulative distribution of the total number of bitcoins received by users and addresses between January 2009 and May 2012 are presented in tables 1 and 2.[26]

Further proof that the network of Bitcoin transactors is small comes from considering the current and maximum balance of bitcoins held by users. As of May 13, 2012, 85.23 percent of users (2,097,245) held less than 0.01 bitcoin in their accounts, and 7.84 percent (192,931) held balances between 0.01 and 0.1 bitcoin. Only 3.06 percent of users (75,244) held 10 or more bitcoins in their account. Moreover, roughly half of all users (1,216,010 or 49.41 percent) had never held 10 or more bitcoins in their accounts. And only 12.18 percent of all users (299,723) had ever held a balance of 100 or more bitcoins. Distributions of the current and maximum balance of bitcoins by users and addresses are presented in tables 3 and 4.

[25] Anonymity and a user's ability to employ multiple addresses make estimating the number of unique users difficult. Ron and Shamir (2012) estimate the number of users by assuming that, when multiple sending addresses are associated with a single transaction, that transaction, and, hence, those addresses, are associated with a single user. Their approach might result in an overestimation of the number of users if some users are not grouping multiple addresses in a single transaction; on the other hand, it might result in an underestimation if users pool their activities into a single transaction. They report that discussions with Bitcoin members led them to worry more about the former than the latter over the period considered.

[26] Ranges listed in tables 1–5 are inclusive of the smallest and exclusive of the largest number. For example, the second row of table 1 shows that 389,302 users and 698,132 addresses have received 1 or more but fewer than 10 bitcoins over their lifetime. The exchange rate employed to calculate an approximate USD equivalent in all tables is the May 13, 2012, closing price, as reported by Mt.Gox. This date corresponds to the study by Ron and Shamir (2012). Of course, the exchange rate has fluctuated significantly in the time since.

## Table 1. Distribution of the Total Number of Bitcoins Received by Users and Addresses between January 2009 and May 2012

| Bitcoins Received over Lifetime | Approximate USD Equivalent | Number of Users | Number of Addresses |
|---|---|---|---|
| < 1 | < 5.27 | 893,763 | 1,497,451 |
| 1 to < 10 | 5.27 to < 52.7 | 389,302 | 698,132 |
| 10 to < 100 | 52.7 to < 527 | 881,273 | 1,206,209 |
| 100 to < 1,000 | 527 to < 5,270 | 255,826 | 285,820 |
| 1,000 to < 10,000 | 5,270 to < 52,700 | 36,713 | 38,484 |
| 10,000 to < 50,000 | 52,700 to < 263,500 | 3,593 | 3,723 |
| 50,000 to < 100,000 | 263,500 to < 527,000 | 181 | 190 |
| 100,000 to < 200,000 | 527,000 to < 1,054,000 | 55 | 50 |
| 200,000 to < 400,000 | 1,054,000 to < 2,108,000 | 30 | 29 |
| 400,000 to < 800,000 | 2,108,000 to < 4,216,000 | 76 | 129 |
| ≥ 800,000 | ≥ 4,216,000 | 4 | 1 |

Source: Ron and Shamir (2012).

## Table 2. Cumulative Distribution of the Total Number of Bitcoins Received by Users and Addresses between January 2009 and May 2012

| Bitcoins Received over Lifetime | Approximate USD Equivalent | Number of Users | Number of Addresses |
|---|---|---|---|
| 0 or More | 0 or More | 2,460,816 | 3,730,218 |
| 1 or More | 5.27 or More | 1,567,053 | 2,232,767 |
| 10 or More | 52.7 or More | 1,177,751 | 1,534,635 |
| 100 or More | 527 or More | 296,478 | 328,426 |
| 1,000 or More | 5,270 or More | 40,652 | 42,606 |
| 10,000 or More | 52,700 or More | 3,939 | 4,122 |
| 50,000 or More | 263,500 or More | 346 | 399 |
| 100,000 or More | 527,000 or More | 165 | 209 |
| 200,000 or More | 1,054,000 or More | 110 | 159 |
| 400,000 or More | 2,108,000 or More | 80 | 130 |
| 800,000 or More | 4,216,000 or More | 4 | 1 |

Source: Ron and Shamir (2012).

## Table 3. Distribution of the Current Balance on May 13th, 2012, of Bitcoins by Users, and Addresses

| Current Balance of Bitcoins | Approximate USD Equivalent | Number of Users | Number of Addresses |
|---|---|---|---|
| < 0.01 | < 0.0527 | 2,097,245 | 3,399,539 |
| 0.01 to < 0.1 | 0.0527 to < 0.527 | 192,931 | 152,890 |
| 0.1 to < 10 | 0.527 to < 52.7 | 95,396 | 101,186 |
| 10 to < 100 | 52.7 to < 527 | 67,579 | 68,907 |
| 100 to < 1,000 | 527 to < 5,270 | 6,746 | 6,778 |
| 1,000 to < 10,000 | 5,270 to < 52,700 | 841 | 848 |
| 10,000 to < 50,000 | 52,700 to < 263,500 | 71 | 65 |
| 50,000 to < 100,000 | 263,500 to < 527,000 | 5 | 3 |
| 100,000 to < 200,000 | 527,000 to < 1,054,000 | 1 | 1 |
| 200,000 to < 400,000 | 1,054,000 to < 2,108,000 | 1 | 1 |
| ≥ 400,000 | ≥ 2,108,000 | 0 | 0 |

Source: Ron and Shamir (2012).

## Table 4. Distribution of the Maximum Balance of Bitcoins by Users and Addresses between January 2009 and May 2012

| Maximum Balance of Bitcoins | Approximate USD Equivalent | Number of Users | Number of Addresses |
|---|---|---|---|
| < 0.1 | < 0.527 | 547,763 | 1,063,876 |
| 0.1 to < 10 | 0.527 to < 52.7 | 668,247 | 1,160,170 |
| 10 to < 100 | 52.7 to < 527 | 945,083 | 1,188,596 |
| 100 to < 1,000 | 527 to < 5,270 | 259,142 | 276,613 |
| 1,000 to < 10,000 | 5,270 to < 52,700 | 36,769 | 37,087 |
| 10,000 to < 50,000 | 52,700 to < 263,500 | 3,513 | 3,521 |
| 50,000 to < 100,000 | 263,500 to < 527,000 | 163 | 159 |
| 100,000 to < 200,000 | 527,000 to < 1,054,000 | 40 | 41 |
| 200,000 to < 400,000 | 1,054,000 to < 2,108,000 | 26 | 26 |
| 400,000 to < 500,000 | 2,108,000 to < 2,635,000 | 68 | 129 |
| ≥ 500,000 | ≥ 2,635,000 | 2 | 0 |

Source: Ron and Shamir (2012).

Finally, consider the number and size of transactions taking place in bitcoins between January 2009 and May 2012. Most users had completed very few transactions. For example, 557,783 users (22.67 percent) had completed fewer than two transactions, and 2,173,682 users (88.33 percent) had completed fewer than four transactions. Only 64,701 users (2.63 percent) had completed 10 or more transactions. Additionally, the size of transactions completed tended to be small. Of the 7,134,836 transactions tracked by Ron and Shamir (2012), more than half (50.21 percent) involved exchanges of less than 1 bitcoin, and 28.44 percent were of less than 0.1 bitcoin; 381,846 transactions, or 5.35 percent, were of less than 0.001 bitcoin. Distributions of the number and size of transactions by users and addresses between January 2009 and May 2012 are presented in tables 5 and 6.

**Table 5. Distribution of the Number of Transactions by Users and Addresses between January 2009 and May 2012**

| Number of Transactions | Number of Users | Number of Addresses |
|---|---|---|
| < 2 | 557,783 | 495,773 |
| 2 to < 4 | 1,615,899 | 2,197,836 |
| 4 to < 10 | 222,433 | 780,433 |
| 10 to < 100 | 55,875 | 228,275 |
| 100 to < 1,000 | 8,464 | 26,789 |
| 1,000 to < 5,000 | 287 | 1,032 |
| 5,000 to < 10,000 | 35 | 51 |
| 10,000 to < 100,000 | 32 | 24 |
| 100,000 to < 500,000 | 7 | 3 |
| ≥ 500,000 | 1 | 2 |

Source: Ron and Shamir (2012).

**Table 6. Distribution of the Size of Transactions by Users and Addresses between January 2009 and May 2012**

| Size of Transactions | Approximate USD Equivalent | Number of Transactions by Users | Number of Transactions by Addresses |
|---|---|---|---|
| < 0.001 | < 0.00527 | 381,846 | 2,315,582 |
| 0.001 to < 0.1 | 0.00527 to < 0.527 | 1,647,087 | 4,127,192 |
| 0.1 to < 1 | 0.527 to < 5.27 | 1,553,766 | 2,930,867 |
| 1 to < 10 | 5.27 to < 52.7 | 1,628,485 | 2,230,077 |
| 10 to < 50 | 52.7 to < 263.5 | 1,071,199 | 1,219,401 |
| 50 to < 100 | 263.5 to < 527 | 490,392 | 574,003 |
| 100 to < 500 | 527 to < 2,635 | 283,152 | 262,251 |
| 500 to < 5,000 | 2,635 to < 26,350 | 70,427 | 67,338 |
| 5,000 to < 20,000 | 26,350 to < 105,400 | 6,309 | 6,000 |
| 20,000 to < 50,000 | 105,400 to < 263,500 | 1,809 | 1,796 |
| ≥ 50,000 | ≥ 263,500 | 364 | 340 |

Source: Ron and Shamir (2012).

Establishing an estimate for the Bitcoin network size depends crucially on what one views as a reasonable inclusion criterion. For example, if the network size were measured by the number of users that made 10 or more transactions between January 2009 and May 2012, it would total 64,701 users. When limited to those making 100 or more transactions over the period, however, the total number of users in the Bitcoin network falls to 8,826 (see table 5). Given that Bitcoin is a global currency—with users spread all over the world—even the high estimate seems small. Therefore, it seems reasonable to conclude that Bitcoin has failed to gain widespread acceptance.

### *B. Using the Model to Explain the Lack of Widespread Acceptance*

How might one account for Bitcoin's inability to garner widespread acceptance? In this section, I will consider four potential explanations.

1. Bitcoin is no better (and perhaps worse) than incumbent monies, irrespective of network size.
2. The cost of switching to Bitcoin is sufficiently high.
3. Agents do not have access to an alternative dominant focal point.
4. Agents have access to an alternative dominant focal point, but the cost of coordination is too high.

It might be the case that, irrespective of network size, Bitcoin is no better (and perhaps worse) than incumbent monies. One might express this formally in terms of the model developed above. Once again, let $u(T) = (a + bn)/r$ be the representative agent's utility from employing the incumbent money from time $T$ onwards. Let $v(t) = (c + dn)/r - s$ be the representative agent's utility from switching to Bitcoin from time $T$ onwards. The proposition that Bitcoin is no better than the incumbent money can be expressed as $a \geq c$, $b \geq d$. It implies that, for non-negative switching costs, $u(T)_N \geq v(T)_A$; the net benefits from switching to Bitcoin are less than or equal to zero. If this is the case, one should not be surprised that Bitcoin has failed to gain widespread acceptance.

Given the potentially desirable properties of Bitcoin discussed above, one may be reluctant to accept that it is no better than incumbent monies. Instead, one might maintain that, irrespective of network size, Bitcoin is superior (i.e., $c > a$, $d > b$). However, as the model developed herein demonstrates, mere superiority to the incumbent is insufficient to prompt widespread switching; net benefits have to be large enough to warrant switching costs. If

switching costs $s$ are greater than $[c - a + (d - b)n/r]$, agents will not want to switch to Bitcoin.

The cost of switching to an alternative money might seem insurmountable at first glance. Upon further inspection, however, it is not so clear. Many vendors are already equipped to receive digital payments. In the United States, there are hundreds of thousands of Near Field Communication–enabled merchants. Since these "Tap and Go" or "Tap to Pay" machines can be used to process payments from digital wallets, many vendors have the technology in place to accept Bitcoin. Existing records, to the extent that they are already available in a digital format, could be updated at little cost. Even learning to think and calculate in terms of a new unit of account might be easier than expected. The widespread adoption of smartphones means that most consumers could convert prices to and from Bitcoin with minimal effort. Indeed, perhaps as an intermediate step, prices could continue to be quoted in the more familiar money while electronic payments are made in Bitcoin at the current exchange rate. In the United States, for example, the consumer would continue to see dollar prices and the checkout register would continue to ring up the total in dollars, but the actual funds transferred electronically would be bitcoins.[27] If the unfamiliar money functions behind the scenes with infrastructure already in place, the cost of switching would be much smaller than one might initially think.

Even if switching costs are sufficiently low, the existence of network effects might preclude Bitcoin from replacing incumbent monies. In this case, agents find themselves in the indeterminate area of figure 2. Although all agents believe that Bitcoin is superior and would prefer to switch to Bitcoin if they knew everyone else would switch as well, they find it

[27] Most credit cards already process international transactions this way. If you purchase breakfast for 20 S/. in Peru with your dollar-denominated credit card, for example, $7.73 (plus a small transaction fee) will be debited from your account, exchanged into soles, and transferred to the merchant—all before you can say *gracias por el desayuno*.

difficult to coordinate. The shared knowledge of historical acceptance is an especially strong focal point since everyone knows that everyone else has a history of transacting in the incumbent money (and everyone knows that everyone knows). To state the matter somewhat differently, agents do not have access to an alternative focal point powerful enough to overcome the status quo. In this environment, no one wants to be the first mover. As Luther and White (2011, 5) explain in another context, "absent some clear death knell for the [incumbent] money, [the representative agent] has no reason to discontinue acceptance before others do. Inertia carries it forward."

If agents have access to an alternative focal point powerful enough to overcome the status quo, Bitcoin might still fail to catch on. Historical acceptance will continue to serve as the dominant focal point if the cost of coordination is sufficiently high. Given the decentralized nature of economic exchange and the lack of communication across some groups, it seems conceivable that the cost of coordination is high. If so, agents will fail to adopt Bitcoin—even though it is technically possible to organize a transition.

The latter two explanations are particularly attractive for proponents of Bitcoin since they both assume Bitcoin is superior to incumbent monies—even after accounting for the cost of switching. Hence, Bitcoin's failure to gain widespread acceptance is not necessarily because it was poorly conceived or seriously flawed. Rather, it is because of the nature of currencies in general. Since the usefulness of a medium of exchange depends crucially on the number of users in its network, agents are inclined to continue accepting the incumbent money. In other words, there is a systemic bias against monetary transition.

### *C. Accounting for the Limited Success of Bitcoin*

Based on the model described above, amended to exclude the prospect of excess momentum, it is perhaps unsurprising that Bitcoin has failed to gain widespread acceptance. Indeed, one might be more surprised to find that anyone chooses to use Bitcoin at all. In order to explain the limited success of Bitcoin, I modify the model to account for multiple agent types. I argue that, irrespective of networks, current users of Bitcoin experience greater benefits and face lower costs of switching and coordination than nonusers would if they were to adopt the alternative money.

In developing the model described above, it was assumed that all agents are identical. The easiest way to relax this assumption is to assume, instead, that there are two types of agents. Both type 1 and type 2 agents earn $u(T) = (a + bn) \int_T^\infty e^{-r(t-T)}\, dt = (a + bn)/r$ from using the historically accepted money from time $T$ onwards, where parameters are defined as above. Agents differ, however, with respect to the alternative currency. Type 1 agents earn $v_1(T) = (c_1 + d_1 n) \int_T^\infty e^{-r(t-T)}\, dt - s_1 = (c_1 + d_1 n)/r - s_1$ from switching to the potentially superior alternative, whereas type 2 agents earn $v_2(T) = (c_2 + d_2 n) \int_T^\infty e^{-r(t-T)}\, dt - s_2 = (c_2 + d_2 n)/r - s_2$. Assuming $c_1 \leq c_2$ and $d_1 \leq d_2$ means that, irrespective of network effects, the benefits of employing the alternative money are potentially greater for type 2 agents. Similarly, assuming $s_1 > s_2$ and $\kappa_1 > \kappa_2$ means type 2 agents face lower costs of switching and coordinating.

The implications of modifying the model in this manner are rather straightforward. Except in the case where $v_1(T) = v_2(T)$, type 2 agents face a lower threshold (in terms of switching cost) for optimal switching; and, provided $c_1 \neq c_2$, they face a lower threshold for switching regardless of whether others switch. This is reinforced by the fact that type 2 agents face a lower cost of switching; and, should they find themselves in the indeterminate area of the

model, the lower cost of coordination implies they will be more likely to overcome the saliency of historical acceptance to coordinate on the superior alternative.

To consider whether the modified model can account for the limited success of Bitcoin, we need to compare the likely characteristics of current users to members of the broader population.[28] So, who uses Bitcoin? According to Ron and Shamir (2012, 4), "Many users adopt the Bitcoin payment system for political and philosophical reasons." These users might broadly be classified as *crypto-anarchists*, though casual observations suggest more traditional libertarians are keen to use Bitcoin as well.[29] It seems reasonable to assume these "political and philosophical" factors do not play much of a role in the currency decisions of the average money user, who is primarily interested in a functioning medium of exchange. It follows, then, that the non-network benefit of Bitcoin is greater for current users than it would be for members of the broader population (i.e., $c_1 < c_2$).

Another group of Bitcoin users might be classified as *computer gamers*.[30] Grinberg (2012, 171) explains that Bitcoin "alleviate[s] or eliminate[s]" a number of problems with currencies common in the online gaming world. For these users, then, it would seem reasonable to assume that the network benefits of Bitcoin are higher than it would be for members of the broader population (i.e., $d_1 < d_2$). Moreover, since online games are often equipped with corresponding chat rooms or web forums, these users might find it less costly to coordinate (i.e., $\kappa_1 > \kappa_2$).

[28] Obviously, this will require some speculation about those actually using Bitcoin since, by design, users of Bitcoin can remain anonymous.
[29] Similarly, Grinberg (2012, 172) suggests Bitcoin might be a reasonable alternative for "'gold bugs' and 'perma bears.'"
[30] For a partial list of games where bitcoins can be used, see http://bitcoingamelist.com/.

Along these lines, we might also consider the *tech savvy*, who are naturally inclined to adopt new technologies, already own (and are familiar with) the requisite hardware to transact with and mine for bitcoins, and—since they are often members of virtual communities—can communicate cheaply with other potential users. Their natural inclination suggests they experience greater non-network benefits (i.e., $c_1 < c_2$). Owning the requisite hardware means the cost of switching is probably lower than for members of the broader population (i.e., $s_1 > s_2$). Also, existing channels of communication make it easier to coordinate (i.e., $\kappa_1 > \kappa_2$).

Finally, we might consider those users employing Bitcoin for *black market* transactions. Grinberg (2012, 161) laments how Bitcoin might facilitate "money laundering, tax evasion, and trade in illegal drugs and child pornography." Indeed, Silk Road, an online market where users can swap bitcoins for illegal drugs, was launched in February 2011. More recently, the website Satoshidice was launched to enable users to gamble with bitcoins. Since anonymity is very important in black market transactions, it might be the case that the network-related benefits of Bitcoin are greater for black market transactors than for members of the broader population (i.e., $d_1 < d_2$).

Although some categories of Bitcoin users have been overlooked, the few examples considered suggest that the modified model might plausibly account for Bitcoin's limited success. Simply put, some agents might experience greater network- and non-network-related benefits from Bitcoin, lowering the threshold at which these agents would be willing to switch. Similarly, since some agents already possess the material necessary to use Bitcoin or are linked through strong social networks, it is conceivable that the costs of switching and coordination they face are lower than those of the broader population.

## III. Successful Switching

Despite network effects, one can observe successful monetary transitions in history. These episodes typically involve government support or the existence of hyperinflation or both.

### *A. Government Support*

Most new monies successfully launched in the past 50 years have benefited from the support of government. Recent examples include the South Sudanese pound in July 2011 and the Somaliland shilling in October 1994. These two currencies have much in common. Both were introduced by new governments following a civil war. Both were also linked to an existing money via a fixed exchange rate when introduced: the Somaliland shilling traded for 100 Somali shillings; the South Sudanese pound traded at par with the Sudanese pound. Finally, in the time since they were launched, both have gained widespread acceptance in their respective regions.

The success of these currencies—and of countless other government-issued monies—is consistent with the existing theoretical literature. Aiyagari and Wallace (1997) and Li and Wright (1998) show that a government can determine the medium of exchange if it is involved in a sufficiently large number of transactions. Ritter (1995) stresses the importance of credibly committing to limit the supply of money, but similarly concludes that government can determine which money is used. The model presented above suggests another channel through which government might affect the acceptability of a currency: by anchoring expectations—perhaps by committing to (or refusing to) accept a currency for payment of taxes—a government can effectively determine the medium of exchange.

The welfare consequences of a government action establishing a focal point for a particular medium of exchange are theoretically ambiguous. On the one hand, government

support might remedy the problem of excess inertia by endorsing the superior alternative when the cost of switching is sufficiently low but not so low that all agents will switch without coordination (i.e., $(c - a - bn)/r < s < [c - a + (d - b)n]/r$). On the other hand, it might make matters worse (or at least no better). If the government encourages excess inertia by endorsing the incumbent money, it merely reinforces historical acceptance; agents will continue to transact with the historically accepted money even though they would be better served by switching. However, if the government endorses the alternative money when the cost of switching is sufficiently high but not so high that no agent will switch (i.e., $(c - a + dn)/r > s > [c - a + (d - b)n]/r$), agents might switch to the alternative even though they would be better served by continuing to use the incumbent money. In other words, government support might resurrect the prospect of excess momentum if it creates a focal point strong enough to overcome historical acceptance.

***B. Hyperinflation***

Successful monetary transitions have also been observed during episodes of hyperinflation. Official dollarization, as in the case of Ecuador in 2000, results when a domestic government supports transitioning to a foreign currency. However, some episodes of hyperinflation have prompted unofficial dollarization—that is, spontaneous switching to a superior alternative. Many Bolivians and Peruvians, for example, sought refuge in the dollar while their countries endured hyperinflations during the years 1984–1986 and 1988–1990, respectively.

Why does hyperinflation lead to spontaneous switching? For starters, hyperinflation drastically reduces the benefits associated with the incumbent money. As a result, the likelihood increases that the costs of switching to and coordinating on an alternative are sufficiently low.

Moreover, since the event is common knowledge, it has the potential to serve as a salient focal point. If everyone is losing faith in the incumbent money, and everyone knows that everyone is losing faith in the incumbent money, it might be possible to orchestrate a switch.

### *C. Implications for Cryptocurrencies*

Unlike the episodes of successful switching observed in recent years, cryptocurrencies like Bitcoin are intended to replace relatively stable currencies—and without support from the government. This seems an unlikely feat. Even if cryptocurrencies were vastly superior to incumbent monies, network effects might preclude adoption. Hence, in the absence of significant monetary instability—or government support—cryptocurrencies will find it difficult to garner widespread acceptance.

## IV. Concluding Remarks

Despite recent technological advances, cryptocurrencies like Bitcoin have failed to gain widespread acceptance. As demonstrated with a simple model for currency acceptance, this failure does not necessarily imply that existing cryptocurrencies are inferior to incumbent monies. Even if they are superior to the status quo, network effects might keep cryptocurrencies from gaining acceptance.

The lesson to be drawn from this study is not necessarily that proponents of cryptocurrencies should give up—though they may be fighting a losing battle. Rather, it is an understanding of the fundamental problem with replacing an existing money. A successful transition requires widespread coordination to overcome the network effects at play. Moreover, the costs of coordination are likely to increase as the pool of early adopters is exhausted. Whether their efforts will be successful in the long run remains to be seen—but there is certainly room for doubt.

**References**


Aiyagari, S. Rao, and Neil Wallace. 1997. "Government Transaction Policy, the Medium of Exchange, and Welfare." *Journal of Economic Theory* 74: 1–18.

Arthur, Brian W. 1989. "Competing Technologies, Increasing Returns, and Lock-In by Historical Events." *The Economic Journal* 99(394): 116–31.

Babaioff, Moshe, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. 2012. "On Bitcoin and Red Balloons." *Proceedings of the 13th ACM Conference on Electronic Commerce* 56–73.

Barber, Simon, Xavier Boyen, Elaine Shi, and Ersin Uzun. 2012. "Bitter to Better—How to Make Bitcoin a Better Currency." *Financial Cryptography and Data Security* 399–414.

Başçi, Erdem. 1999. "Learning by Imitation." *Journal of Economic Dynamics and Control* 23(9): 1569–85.

Brown, Paul M. 1996. "Experimental Evidence on Money as a Medium of Exchange." *Journal of Economic Dynamics and Control* 20: 583–600.

David, Paul A. 1985. "Clio and the Economics of QWERTY." *American Economic Review* 75(2): 332–37.

Dowd, Kevin, and David Greenaway. 1993. "Currency Competition, Network Externalities, and Switching Costs: Towards an Alternative View of Optimum Currency Areas." *The Economic Journal* 103(420): 1180–89.

Duffy, John. 2001. "Learning to Speculate: Experiments with Artificial and Real Agents." *Journal of Economic Dynamics and Control* 25: 295–319.

Duffy, John, and Jack Ochs. 1999. "Emergence of Money as a Medium of Exchange: An Experimental Study." *American Economic Review* 89: 847–77.

———. 2002. "Intrinsically Worthless Objects as Media of Exchange: Experimental Evidence." *International Economic Review* 43: 637–73.

Elison, Glen, and Drew Fudenberg. 1993. "Rules of Thumb for Social Learning." *Journal of Political Economy* 101(4): 612–43.

Farrell, Joseph, and Garth Saloner. 1986. "Installed Base and Compatibility: Innovation, Product Preannouncements, and Predation." *American Economic Review* 76(5): 940–55.

Giansante, Simone. 2006. "Social Networks and Medium of Exchange." Working paper. Available online: http://andromeda.rutgers.edu/~jmbarr/NYComp/GiasanteEEA.pdf.

Grinberg, Reuben. 2012. "Bitcoin: An Innovative Alternative Digital Currency." *Hastings Science & Technology Law Journal* 4: 159–208.

Hasker, Kevin, and Ahmet Tahmilci. 2008. "The Rise of Money: An Evolutionary Analysis of the Origins of Money." Working paper. Available online: http://www.bilkent.edu.tr /~hasker/Research/Hasker-Tahmilci-evolution-of-money-08-05-15.pdf.

Katz, Michael, and Carl Shapiro. 1985. "Network Externalities, Competition, and Compatibility." *American Economic Review* 75(3): 424–40.

———. 1986. "Technology Adoption in the Presence of Network Externalities." *Journal of Political Economy* 94(4): 822–41.

Kawagoe, Toshiji. 2007. "Learning to Use a Perishable Good as Money." *Multi-Agent-Based Simulation VII* 4442: 96–111.

King, Mervyn. 2004. "The Institutions of Monetary Policy." *American Economic Review* 94(2): 1–13.

Kocherlakota, Narayana. 1998. "Money Is Memory." *Journal of Economic Theory* 81(2): 232–51.

Kocherlakota, Narayana, and Neil Wallace. 1998. "Incomplete Record-Keeping and Optimal Payment Arrangements." *Journal of Economic Theory* 81(2): 272–89.

———. 2002. "The Two-Money Theorem." *International Economic Review* 43(2): 333–46.

Li, Yiting, and Randall Wright. 1998. "Government Transaction Policy, Media of Exchange, and Prices." *Journal of Economic Theory* 81: 290–313.

Liebowitz, Stan J., and Stephen E. Margolis. 1990. "The Fable of the Keys." *Journal of Law and Economics* 33(1): 1–25.

———. 1994. "Network Externality: An Uncommon Tragedy." *Journal of Economic Perspectives* 8(2): 133–50.

———. 1995. "Path Dependence, Lock-In, and History." *Journal of Law, Economics, and Organization* 11(1): 205–26.

Luther, William J. 2012a. "The Monetary Mechanism of Stateless Somalia." Working paper. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2047494.

———. 2012b. "Evaluating the Range of Currency Denominations Circulating in Somalia." Working paper. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract _id=2066090.

———. 2013. "Friedman Versus Hayek on Private Outside Monies: New Evidence for the Debate." *Economic Affairs* 33(1): 127–35.

Luther, William J., and Josiah Olson. 2013. "Bitcoin Is Memory." Working paper. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2275730.

Luther, William J., and Lawrence H. White. 2011. "Positively Valued Fiat Money after the Sovereign Disappears: The Case of Somalia." *GMU Working Paper in Economics No. 11-14*. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1801563.

Marimon, Ramon, Ellen R. McGrattan, and Thomas J. Sargent. 1990. "Money as a Medium of Exchange in an Economy with Artificially Intelligent Agents." *Journal of Economic Dynamics and Control* 14(2): 329–73.

May, Timothy. 1992. *The Crypto Anarchist Manifesto*. http://www.activism.net/cypherpunk/crypto-anarchy.html.

Nakamoto, Satoshi. 2008. "Bitcoin: A Peer-to-Peer Electronic Cash System." Available online: http://bitcoin.org/bitcoin.pdf.

Reid, Fergal, and Martin Harrigan. 2011. "An Analysis of Anonymity in the Bitcoin System." *Privacy, Security, Risk, and Trust* 3: 1318–26.

Ritter, Joseph A. 1995. "The Transition from Barter to Fiat Money." *American Economic Review* 85(1): 134–49.

Ron, Dorit, and Adi Shamir. 2012. "Quantitative Analysis of the Full Bitcoin Transaction Graph." Working paper. Available online: http://fc13.ifca.ai/proc/1-1.pdf.

Selgin, George. 1994. "On Ensuring the Acceptability of a New Fiat Money." *Journal of Money, Credit and Banking* 26(4): 808–26.

———. 2003. "Adaptive Learning and the Transition to Fiat Money." *The Economic Journal* 113(484): 147–65.

———. 2012. "Synthetic Commodity Money." Working paper. Available online: http://papers.ssrn.com/sol3/papers.cfm?abstract-id=2000118.

Shinohara, Shuji, and Yukio P. Gunji. 2001. "Emergence and Collapse of Money through Reciprocity." *Applied Mathematics and Computation* 117(2–3): 131–50.

Staudinger, Sylvia. 1998. "Money as a Medium of Exchange: An Analysis with Genetic Algorithms." Technical University of Vienna working paper.

Yasutomi, Ayumu. 1995. "The emergence and collapse of money." *Physica D: Nonlinear Phenomena* 82(1): 180–94.

Yasutomi, Ayumu. 2003. "Itinerancy of Money." *Chaos* 13(3): 1148–64.