The Value of Bitcoin in the Year 2141

(And Beyond!)

Joshua R. Hendrickson* William J. Luther†

May 14, 2021

Abstract

The emergence of bitcoin poses an important question for monetary theorists: can bitcoin compete with or even replace existing fiat monies? To answer this question, one must be able to determine what gives intrinsically useless monies their value, what determines the coexistence of alternative monies, and under what conditions economic agents would prefer to hold one money relative to another. We attempt to answer these questions in light of the emergence of bitcoin. In particular, we outline a theoretical model in which an intrinsically useless money is essential.

JEL Codes: E40, E41, E42, G2, H1, N1, N2

Keywords: bitcoin, cryptocurrency, currency, demand for money, fiat money

*University of Mississippi, Department of Economics, 306 Odom Hall, University, MS, 38677 jrhendr1@olemiss.edu

†Department of Economics, Florida Atlantic University, Boca Raton, FL 33431. E-mail: wluther@fau.edu.

Bitcoin launched in January 2009 with an e-mail sent by the pseudonymous Satoshi Nakamoto to the Cryptography Mailing List. He had circulated a white paper describing its technical details a few months earlier (Nakamoto 2008). In the time since, demand for bitcoin has grown markedly. The price of bitcoin rose from around $\$0.50$ in November 2010 to $\$19,167$ in December 2017. Today, one bitcoin exchanges for roughly $\$54,619$ and its market capitalization exceeds that of many national currencies (Hazlett and Luther 2020). A host of alternative cryptocurrencies, or alt-coins, resembling bitcoin have been issued as well (White 2015).

The emergence of bitcoin poses an important question for monetary theorists: can bitcoin (or some alt-coin) compete with or even replace existing fiat monies? To answer this question, one must be able to determine what gives intrinsically useless monies their value, what determines the coexistence of alternative monies, and under what conditions economic agents would prefer to hold one money relative to another. We attempt to answer these questions in light of the emergence of bitcoin. In particular, we outline a theoretical model in which an intrinsically useless money is essential.[1]

Given the characteristics of a central bank-managed fiat currency and bitcoin in the year 2141 and beyond, when the supply is capped and miners processing transactions rely exclusively on fees, we use the model to determine the conditions under which economic agents will hold bitcoin in conjunction with or as an alternative to currency. Specifically, we demonstrate that, for a given rate of currency growth, the fee associated with processing bitcoin transactions determines whether it is held in equilibrium. If the fee is sufficiently high, economic agents will only hold currency. If the fee is suf-

[1]A money is deemed essential if it expands the set of feasible allocations (Hahn 1987, Kocherlakota 1998, Lagos and Wright 2008, Luther 2016b).

ficiently low, economic agents will only hold bitcoin. We also describe the conditions under which both currency and bitcoin are held in equilibrium. Finally, we discuss the implications of the model and potential extensions.

1 Bitcoin

Bitcoin is a peer-to-peer digital alternative to traditional central bank-managed fiat monies.[2] It is irredeemable (i.e., a bitcoin user does not hold a claim to some underlying asset) and intrinsically useless (i.e., a bitcoin has no non-monetary use).[3] One can only spend bitcoin if someone else is willing to accept it. Moreover, bitcoin differs from other payment mechanisms in that it is neither centralized (e.g., an electronic funds transfer) nor decentralized (e.g., cash). It is a distributed payment mechanism, with transactions processed by the system of users running the bitcoin protocol (Luther and Stein Smith 2020).

At its core, bitcoin is a shared ledger and a protocol for updating that ledger. Transactions are secured by asymmetric cryptography. When a transaction is made, it is bundled together with other unconfirmed transactions waiting to be processed. Computers running the bitcoin protocol compete to be the first to update the block of transactions to the shared ledger, or blockchain. Specifically, they race to produce a SHA-256 hash of the block's header that is less than or equal to the existing target.

[2]Selgin (2015) classifies bitcoin as a synthetic commodity money and explains how it differs from traditional commodity and fiat monies.

[3]Graf (2013) discusses potential non-monetary uses for bitcoin. Luther (2018) suggests bitcoin is best thought of as being intrinsically useless and argues that efforts to show bitcoin has some non-monetary use do not generally get around the problems inherent to intrinsically useless monies. Luther (2019) considers how bitcoin launched with these issues in mind.

Once successful, the block of transactions is added to the existing blockchain, thereby updating the ledger against which future transactions must be confirmed.

Hashing a block is easy. One need only input the block header into a hash function, which scrambles the data and returns a unique fixed-length result. The output of a SHA-256 hash is essentially a random number between 0 and the maximum value of a 256-bit number. The problem is made computationally difficult, however, by requiring the output be less than or equal to the existing target. This constraint effectively turns the race to confirm a block of transactions into a lottery. Those running the protocol produce hash after hash until a winning number is found.

The computational difficulty of processing a block of transactions makes it unlikely that one confirms her own transactions and, hence, limits the potential for illegitimate ledger entries. Moreover, the consensus to recognize the longest blockchain as legitimate further undermines the black hat's efforts: she would not only have to confirm her own illegitimate transaction, but also continue to confirm transactions at a rate faster than the rest of the system in order to prevent her illegitimate transaction from being reversed by a longer blockchain that excludes her illegitimate transaction. Given that winning the hash race is essentially random, with her odds reflecting her share of the system's computing power, it is incredibly unlikely that she would be able to maintain the longest blockchain unless she holds a majority of the computing power on the system.[4]

Of course, individuals will only run their computers to process transactions if the

[4]As Luther (2016c, 2020) explains, system norms and the risk of devaluing one's own bitcoin holdings discourages miners and mining pools from securing more than fifty percent of the computational power on the system.

benefits are greater than or equal to the cost. These costs include electricity, as well as the wear and tear on their machines. As for the benefits, the bitcoin system offers two forms of compensation: new bitcoin and transaction fees.

When a block of transactions is processed, new bitcoin is created and rewarded to the winning computer. For this reason, those running the bitcoin protocol are typically described as "mining bitcoin." The block reward a successful miner receives, which was initially set at 50 bitcoin, is cut in half every $210,000$ blocks. It halved from 12.5 to 6.25 in May 2020.

The target value for the SHA-256 hash is routinely (and automatically) adjusted to ensure that roughly one block of transactions gets processed every ten minutes. When computational power picks up and blocks are processed too quickly, the target value is reduced to slow the speed of block creation. Likewise, when the computational power falls and blocks are processed too slowly, the target value is increased to speed up block creation. This feature, combined with the predetermined reward structure, results in the predetermined supply schedule for bitcoin presented in Figure 1.

Given the speed of block creation and routine halving of the block reward, the supply of bitcoin is expected to reach its apex of $20,999,999.9769$—commonly rounded to 21 million—around May 7, 2140.[5] No new bitcoin will be created after the reward for block $6,929,999$ is distributed. However, since the block reward is very small for a long time before actually reaching zero, the supply will be nearly fixed much earlier. For example, at block $1,680,000$, which should be reached around April 12, 2039, roughly

[5]While the block reward asymptotically approaches zero, it falls to 1 satoshi—or, 0.00000001 bitcoin—at block $6,720,000$. Since a satoshi is the smallest unit recognized on the bitcoin system, the halving at block $6,930,000$ reduces the block reward to zero.

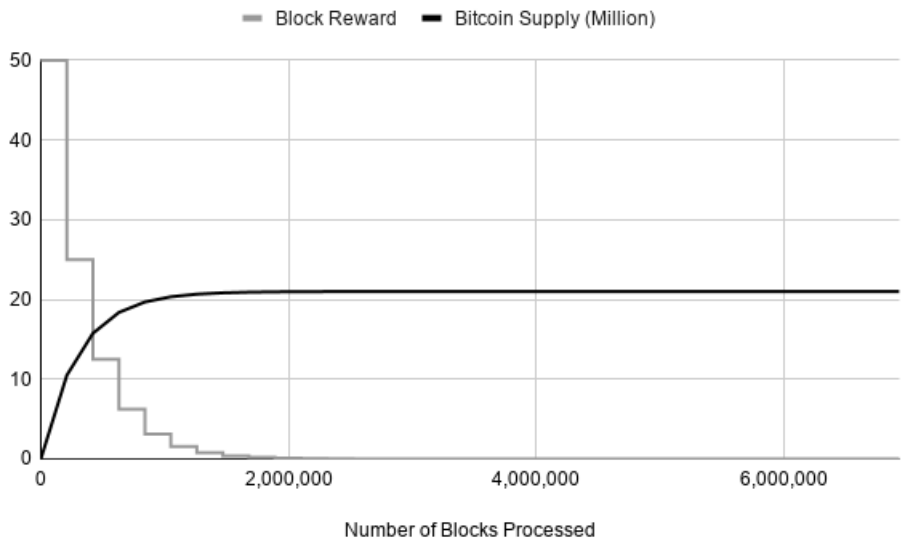

Figure 1: Bitcoin's supply schedule

$20,917,968.75$ bitcoin (99.6 percent) will have been issued and the block reward will be just 0.19531250 bitcoin. As of May 2021, a little more than 18.7 million bitcoin (89 percent) have been issued.

As the block reward falls to zero, the bitcoin system will increasingly rely on transaction fees to encourage miners to process transactions. Users can choose to include a transaction fee when transferring funds. The fee is then distributed to the first miner who processing a block including that transaction.

Strictly speaking, the inclusion of a transaction fee is optional. However, miners can choose whether to include a given transaction in the block being processed. This exclusion option is especially relevant when the network is congested. Each block is limited to 1 MB. When the number of transactions awaiting confirmation is sufficiently large, those sending funds can either include a sufficiently large transaction fee to ensure

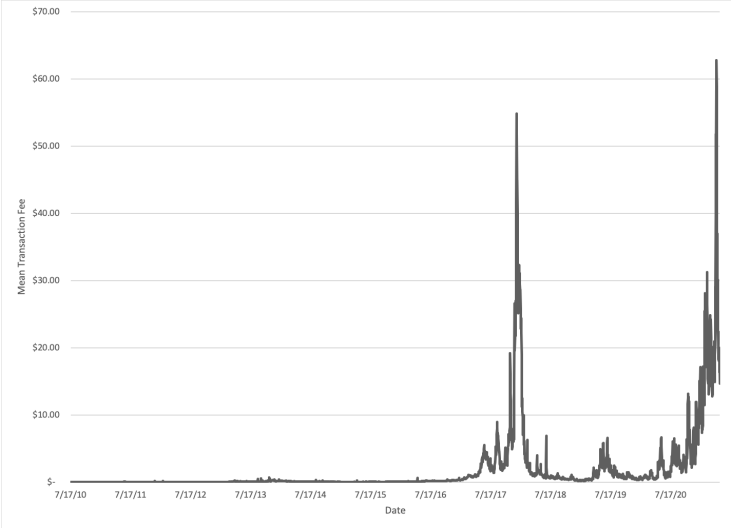

Figure 2: Mean transaction fee over time

miners include their transaction in the next block being processed or risk having their transaction excluded until those transactions associated with higher fees are confirmed.[6]

The daily mean transaction fee over time, as reported by Glassnode (2020), is presented in Figure 2. Transaction fees averaged just $0.06 from July 2010 to July 2016. It grew from $0.18 in July 2016 to $1.77 in July 2017 and then peaked at $55.83 in December 2017, as a surge in price led to extreme congestion. It then declined, averaging $1.09 from July 2018 to July 2020. For the seven-day period ending July 16, 2020, the mean transaction fee was $1.41. More recently, the mean transaction fee has risen. Transaction fees averaged $4.86 from August 2020 to January 2021 and $20.00 from January 2021 to May 2021. For the seven-day period ending May 12, 2021, the mean transaction fee averaged $18.03.

Since its launch, bitcoin has been positioned as an alternative to central bank-

[6]Bitcoin wallet services typically recommend (and some require) a transaction fee amount to ensure the transfer is processed in a timely manner.

managed fiat monies. "The root problem with conventional currency is all the trust that's required to make it work." the pseudonymous Satoshi Nakamoto (2009) wrote. "The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."

Others echoed the sentiment. "At first," early adopter Roger Ver noted, "almost everyone who got involved did so for philosophical reasons. We saw bitcoin as a great idea, as a way to separate money from the state" (Feuer 2013). Tech writer Timothy Lee (2013) similarly claimed that "the cryptocurrency's most enthusiastic advocates tend to subscribe to a hard-money, end-the-Fed worldview that is unpopular among elites."[7] Even today, with inflation averaging well below 2 percent in the U.S. since the Federal Reserve explicitly adopted the target in 2012, it is not uncommon to see bitcoin lauded as a much-needed check on money printing (Co 2020, Huang 2020).

In summary, bitcoin is a digital alternative to traditional central bank-managed fiat monies. Although those processing bitcoin transactions are currently rewarded with new bitcoin, the supply is scheduled to become fixed before 2141. At that time, the system will rely entirely on transaction fees to encourage users to process transactions. With these features in mind, we model bitcoin in the year 2141 and beyond and consider the conditions whereby it is employed in lieu of or alongside central bank-managed fiat monies. We offer a formal model in Section 2. Readers less interested in the technical details of our analysis might skip to Section 3, where we discuss the implications of the model.

[7]Yelowitz and Wilson (2015) finds that, at least between January 2011 and July 2013, users tended to be computer programmers and criminals, not libertarians.

2 Model

We modify the monetary search framework of Lagos and Wright (2005). Time is discrete and continues forever. Each period is divided into two subperiods. In the first subperiod, agents are matched pairwise in a decentralized market (DM) and negotiate the terms of trade. In the second subperiod, agents meet in a centralized, Walrasian market (CM). A unique good is produced and traded in each market. There is a continuum of agents with unit mass whose preferences are given as

$$\sum_{t=0}^{\infty} \beta^t [u(q_t) - c(q_t) - h_t + x_t]$$

where $0 < \beta < 1$ is the discount factor, h_t is labor that is used to produce the CM good one-for-one, x_t is the consumption of CM good, $u(q)$ is the utility generated from the consumption of a quantity of the DM good, q, where $u' > 0$, $u'' < 0$, $u'(0) = \infty$, $u'(\infty) = 0$, and $-c(q)$ measures the disutility associated with producing the DM good, where $c' > 0$, $c'' \geq 0$, and $c(0) = 0$.

When agents enter the DM, they receive a preference shock. With probability σ agents are buyers who are matched pairwise with a seller. With probability σ agents are seller who are matched pairwise with a buyer. With probability $1 - 2\sigma$ agents are unmatched. After they are matched, buyers and sellers negotiate the terms of trade. Buyers want to consume in the DM, but can only produce in the CM. Sellers can produce, but do not want to consume in the DM. As a result, there is an absence of double coincidence of wants problem in the DM. In addition, it is assumed that all matches in the DM are anonymous. As a result, credit is infeasible and money is

essential.

There are two types of money in the model. The first is a central bank-managed fiat currency. For simplicity, it is assumed that the supply of currency grows at a constant rate μ. In addition, it is assumed that the central bank takes steps to make the currency more recognizable to discourage counterfeiting. In particular, it is assumed that there is a fixed cost associated with counterfeiting currency and that this cost is a policy variable for the central bank.

The second type of money is bitcoin. As noted above, the supply of bitcoin is capped at 21 million and, once it reaches the cap, miners are rewarded for verifying transactions exclusively with transaction fees. Since the emphasis below is carried out over an infinite horizon, we specify that the growth rate of bitcoin is zero. The cost of exchanging bitcoin therefore includes a transaction fee paid to miners and any additional costs incurred to prevent fraud. For example, it is possible to imagine a virus that transfers bitcoin from an infected machine to another bitcoin account. For simplicity, we assume there is some fixed cost associated with preventing this type of theft.

The subsequent analysis proceeds by starting in the CM and working backward through the DM.

2.1 Centralized Market

Let $\phi_{1,t}$ and $\phi_{2,t}$ denote the price of currency and the price of bitcoin, respectively, in terms of the CM good. The budget constraint for agents entering the CM is given as

$$\phi_{1,t}m_{1,t+1} + \phi_{2,t}m_{2,t+1} = \phi_{1,t}m_{1,t} + \phi_{2,t}m_{2,t} + h_t - x_t \tag{1}$$

where $m_{1,t}$ is the quantity of money held in the form of currency and $m_{2,t}$ is quantity of money held in the form of bitcoin.

Let $W_t(m_{1,t}, m_{2,t})$ and $V_t(m_{1,t}, m_{2,t})$ be the value functions for agents holding currency $m_{1,t}$ and bitcoin $m_{2,t}$ entering the centralized and decentralized markets at time t, respectively. The value function for those entering the centralized market is given as:

$$W_t(m_{1,t}, m_{2,t}) = \max_{h_t, x_t, m_{1,t+1}, m_{2,t+1}} [-h_t + x_t + \beta E_t V_{t+1}(m_{1,t+1}, m_{2,t+1})]$$

where E_t is the mathematical expectations operator.

Assuming an interior solution in the CM, equation (1) can be substituted into the value function such that

$$W_t(m_{1,t}, m_{2,t}) = \phi_{1,t}m_{1,t} + \phi_{2,t}m_{2,t} + \max_{m_{1,t+1}, m_{2,t+1}} [-\phi_{1,t}m_{1,t+1} - \phi_{2,t}m_{2,t+1} + \beta E_t V_{t+1}(m_{1,t+1}, m_{2,t+1})] \tag{2}$$

2.2 Decentralized Market

The value function for agents entering the decentralized market is given as

$$V_t(m_{1,t}, m_{2,t}) = \sigma[u(q_t)+W_t(m_{1,t}-d_{1,t}, m_{2,t}-d_{2,t})]+\sigma[-c(q_t)+W_t(m_{1,t}+d_{1,t}, m_{2,t}+d_{2,t})]$$

$$+ (1-2\sigma)W_t(m_{1,t}, m_{2,t}) \tag{3}$$

After buyers and sellers are matched, they negotiate the terms of trade. For simplicity, it is assumed that buyers make take-it-or-leave-it offers to sellers. Since trade in the DM is anonymous, buyers must offer currency, bitcoin, or some combination thereof in exchange for the desired quantity of the DM good. Consistent with the description of bitcoin above, buyers who offer bitcoin in exchange for goods must pay a transaction fee, τ. In addition, as described above, sellers face the threat of fraud with respect to each form of money. Specifically, it is assumed there is a fixed cost, κ, associated with counterfeiting currency. Also, there is a fixed cost, δ, associated with fraudulently obtaining bitcoin.

For a buyer's offer to the seller to be incentive feasible, the offer must satisfy five conditions. First, the buyer must offer enough to compensate the seller for the disutility of production. Second, the value of the currency that is offered must be less than or equal to the cost of counterfeiting. Third, the value of bitcoin offered to the seller cannot exceed the cost associated with bitcoin fraud. The final two conditions are that the buyer cannot offer more currency or bitcoin than what the buyer is holding in the

DM. In the context of the model, these respective conditions can be written as

$$\phi_{1,t}d_{1,t} + (1-\tau)\phi_{2,t}d_{2,t} \geq c(q_t) \tag{4}$$

$$\phi_{1,t}d_{1,t} \leq \kappa \tag{5}$$

$$\phi_{2,t}d_{2,t} \leq \delta \tag{6}$$

$$d_{1,t} \leq m_{1,t} \tag{7}$$

$$d_{2,t} \leq m_{2,t} \tag{8}$$

where d_1 and d_2 are the nominal amounts of currency and bitcoin offered to the seller, respectively. Also, given the buyers objective to maximize utility, they will never offer more than the least that is necessary to get sellers to accept the trade. This implies that equation (4) will always hold with equality.

Given the linearity of W_t, equation (3) can be re-written as

$$V_t(m_{1,t}, m_{2,t}) = \sigma[u(q_t) - c(q_t)] + W_t(m_{1,t}, m_{2,t})$$

Iterating forward and substituting this expression into (2), the objective of agents is to maximize the bracketed expression in (2) subject to (5), (6), (7), (8), $m_{1,t} \geq 0$, and $m_{2,t} \geq 0$. Formally, this maximization problem can be written as

$$\max_{m_{1,t+1}, m_{2,t+1}, d_{1,t+1}, d_{2,t+1}} \left\{ -\phi_{1,t}m_{1,t+1} - \phi_{2,t}m_{2,t+1} + \beta E_t \left[\sigma[u(q_{t+1}) - c(q_{t+1})] + \phi_{1,t+1}m_{1,t+1} + \phi_{2,t+1}m_{2,t+1} \right] \right.$$

$$+\lambda_1(\kappa-\phi_{1,t+1}d_{1,t+1})+\lambda_2(\delta-\phi_{2,t+1}d_{2,t+1})+\lambda_3\phi_{1,t+1}(m_{1,t+1}-d_{1,t+1})+\lambda_4\phi_{2,t+1}(m_{2,t+1}-d_{2,t+1})\Big\} \tag{9}$$

where, from equation (4), q_{t+1} can be expressed as an implicit function of $d_{1,t+1}$ and $d_{2,t+1}$.

The Kuhn-Tucker conditions are given as

$$-\frac{\phi_{1,t}}{\phi_{1,t+1}}+\beta+\lambda_3\leq 0 \tag{10}$$

$$\beta\sigma\left[\frac{u'(q_{t+1})}{c'(q_{t+1})}-1\right]-\lambda_1-\lambda_3\leq 0 \tag{11}$$

$$-\frac{\phi_{2,t}}{\phi_{2,t+1}}+\beta+\lambda_4\leq 0 \tag{12}$$

$$\beta\sigma(1-\tau)\left[\frac{u'(q_{t+1})}{c'(q_{t+1})}-1\right]-\lambda_2-\lambda_4\leq 0 \tag{13}$$

where we have used the result from the implicit function theorem and equation (4) that $\partial q_t/\partial d_{1,t}=\phi_{1,t}/c'(q_t)$ and $\partial q_t/\partial d_{2,t}=[(1-\tau)\phi_{2,t}]/c'(q_t)$. These conditions hold with equality if $m_{1,t+1}>0$, $d_{1,t+1}>0$, $m_{2,t+1}>0$, $d_{1,t+1}>0$, $d_{2,t+1}>0$, respectively.

2.3 Equilibrium

A stationary equilibrium consists of quantities of currency, $m_1, d_1 \geq 0$, and bitcoin, $m_2, d_2 \geq 0$, and fixed costs (κ, δ) that solve (9) such that

1. $m_{1,t}=m_1=M_1$, where M_1 is the aggregate supply of currency.

2. $m_{2,t}=m_2=M_2$, where M_2 is the aggregate supply of bitcoin.

3. Currency is neutral: $\phi_{1,t}M_{1,t} = \phi_{1,t+1}M_{1,t+1}$

4. Bitcoin is neutral: $\phi_{2,t}M_{2,t} = \phi_{2,t+1}M_{2,t+1}$

5. $M_{1,t+1} = \mu M_{1,t}$; $M_{1,0} = \bar{M}_1$

6. $M_{2,t+1} = M_{2,t} = M_{2,0} = \bar{M}_2$

7. $\mu \geq \beta$

8. The CM market clears: $x_t = X_t = y_t = Y_t$, where Y_t is the aggregate production in the CM.

9. The DM market clears: $\phi_{1,t}d_{1,t} + (1-\tau)\phi_{2,t}d_{2,t} \geq c(q_t)$

Given this definition, there are three possible equilibria to consider: an equilibrium in which both bitcoin and currency circulate, an equilibrium in which only currency circulates, and an equilibrium in which only bitcoin circulates. The assumption that $\mu \geq \beta$ guarantees that $d_{1,t} = m_{1,t}$ and the fact that the supply of bitcoin is fixed guarantees that $d_{2,t} = m_{2,t}$. So, $\lambda_3, \lambda_4 > 0$. In addition, assume that κ and δ are sufficiently high such that the fraud constraints are non-binding. This implies that $\lambda_1 = \lambda_2 = 0$.[8]

2.3.1 The Coexistence of Currency and Bitcoin

Consider the case in which both currency and bitcoin are held in equilibrium. Under this scenario, equations (10) - (13) hold with equality. Combining these equations yields

[8]The simplifying assumption that fraud constraints are non-binding does not affect the conclusions that follow.

the following stationary equilibrium conditions:

$$\mu = \beta\left\{\sigma\left[\frac{u'(q)}{c'(q)} - 1\right] + 1\right\} \tag{14}$$

$$1 = \beta\left\{\sigma(1-\tau)\left[\frac{u'(q)}{c'(q)} - 1\right] + 1\right\} \tag{15}$$

As a result, for currency and bitcoin to coexist, it must be true that

$$\tau = \frac{\mu - 1}{\mu - \beta}$$

This conditions implies that, for a given rate of money growth, there is a particular transaction fee that enables both currency and bitcoin to circulate. Or alternatively, given the fee associated with processing bitcoin transactions, there is a particular level of money growth that allows for both currency and bitcoin to circulate. In addition, it is important to note that the rate of money growth associated with dual circulation is increasing in the transaction fee associated with processing bitcoin transactions.

What this condition reveals, however, is that there are conditions under which bitcoin will never circulate. For example, if $\beta < \mu < 1$, then the transaction fee must be negative for bitcoin to circulate. Since the transaction fee associated with processing bitcoin transactions is greater than zero, it follows that nobody will use bitcoin in equilibrium when $\beta < \mu < 1$.

To understand this point, define the liquidity premium for holding an asset as

$$\ell(q) = \sigma\left[\frac{u'(q)}{c'(q)} - 1\right]$$

The liquidity premium therefore measures the marginal value of holding an additional unit of money, which is measured here by the size of the surplus from trade in the DM multiplied by the probability of being matched. Marginal analysis implies that the marginal cost of holding money should be equal to the marginal benefit, in this case, the liquidity premium. It follows from (14) and (15) that for both assets to be held it must be true that

$$\mu - \beta = \beta \ell(q) = \frac{1-\beta}{1-\tau}$$

Solving this expression for τ gives us the condition for the coexistence equilibrium shown above.

2.3.2 Currency Equilibrium

Given the condition described above, it follows that agents will hold currency, but not bitcoin, if the marginal cost of holding currency is less than the marginal cost of holding bitcoin. Using the condition above, this implies that

$$\mu - \beta < \frac{1-\beta}{1-\tau}$$

Solving this expression for μ yields

$$\mu < \frac{1-\tau\beta}{1-\tau} \tag{16}$$

What this suggests is that, for a given transaction cost associated with using bitcoin, sufficiently low currency growth can preclude bitcoin from circulation.

2.3.3 Bitcoin Equilibrium

The final equilibrium is one in which bitcoin circulates and currency does not. For bitcoin to circulate on its own, it must be the case that the marginal cost associated with bitcoin is lower than the marginal cost associated with using currency. This implies that

$$\mu - \beta > \frac{1-\beta}{1-\tau}$$

Solving for τ yields

$$\tau < \frac{\mu - 1}{\mu - \beta} \tag{17}$$

So, for a given rate of currency growth, if the transaction cost associated with processing bitcoin transactions is sufficiently low, then everyone will use bitcoin, and no one will use currency, in equilibrium.

3 Discussion

The formal model presented in Section 2 allows us to consider the conditions necessary for bitcoin to be used as a medium of exchange (i.e., circulate) in the future. We have shown that, so long as there is a desirable role for money, there are three possible outcomes:

1. Only bitcoin circulates;
2. Only currency circulates;
3. Both bitcoin and currency circulate.

In other words, bitcoin *might* be employed as a medium of exchange in the future (exclusively or alongside currency), but that result is not inevitable. It depends on the characteristics of bitcoin and currency.

What conditions improve the odds that bitcoin will circulate? We have paid special attention to the relationship between the growth rate of currency and the fee associated with processing bitcoin transactions. As the growth rate of currency increases, the rate of return on currency falls. If the rate of return on currency is sufficiently low, individuals will prefer to use bitcoin to make transactions. This suggests that bitcoin is more likely to be adopted in countries where there is a greater risk of sufficiently high money growth. Historically, some countries, like Argentina, Venezuela, and Zimbabwe, have been more inclined to monetize their existing debts or create money to cover temporary fiscal imbalances than others. Those transacting in these countries might reasonably fear the government might resort to excessive money creation again. As a result, they might be more inclined to use bitcoin, which protects them from the risk of high money growth.

Correspondingly, bitcoin stands a better chance of circulating as the fee associated with processing bitcoin transactions declines. If the transaction fee is sufficiently low, individuals will prefer to use bitcoin to make transactions. There are several ways to think about this implication. For starters, recall that the cost of processing transactions is endogenous. The computational cost of hashing a block of transactions is very low. The cost of processing transactions is made more difficult, however, because the bitcoin protocol requires the output of the SHA-256 hash to be greater than the existing target. And the target is routinely adjusted to ensure that one block of transactions is

confirmed every ten minutes. Suppose that the existing target is sufficiently high that no one is willing to incur the requisite transaction fee. In that case, no transactions will be processed. Since less than one transaction is processed every ten minutes, the bitcoin protocol will lower the existing target, making it less costly to process transactions. And, in general, this process will continue until the transaction fee is sufficiently low. There are two caveats, however. First, the transaction fee cannot be less than or equal to zero. It will always require some resources to process transactions. If the rate of currency growth is sufficiently low to require a non-positive transaction fee for bitcoin to circulate, bitcoin will not circulate. Second, some believe that the bitcoin protocol is not sufficiently robust to attack when transaction fees are very low. If the requisite transaction fee falls below the threshold transaction fee required to secure the bitcoin protocol, sellers might refuse to accept bitcoin on the grounds that they cannot trust the system to secure the funds once received.

Another way to think about the implication that transaction fees must be sufficiently low for bitcoin to circulate requires specifying whether these fees are flat-rate fees or proportional to transaction size. In the case of flat-rate transaction fees, there is some minimum transaction size below which it is too costly to use bitcoin. Hence, it is more likely that bitcoin will circulate for large payments if transaction fees are flat-rate, since the effective proportional fee is lower for larger transactions.

The implication that transaction fees must be sufficiently low for bitcoin to circulate also suggests bitcoin proponents might consider ways to reduce those fees. Increased interest in second layer solutions, like the lightning network, are consistent with this view. In brief, second layer solutions allow one to trade bitcoin or claims to bitcoin

without executing each individual transaction on the bitcoin blockchain. Then, after a series of transactions have been made, the transactions can be netted out, with final settlement resolved on the bitcoin blockchain. By effectively collapsing a great many individual transactions into a few settlement transactions, the implicit cost per individual transaction—which can be calculated by dividing the transaction fees incurred for the settlement transactions by the total number of individual transactions—is greatly reduced. Other potential solutions, like moving from a proof-of-work to a proof-of-stake mechanism come to mind, though the level of coordination required to permit such a change to the bitcoin protocol make these kinds of solutions very unlikely.

In Section 2, we assumed that the cost of counterfeiting currency and the cost of obtaining bitcoin via theft or fraud are sufficiently high to be rendered inconsequential. However, it is not difficult to relax these assumptions and consider the implications. In general, the lower the cost of counterfeiting currency, the more likely bitcoin is to circulate. A lower cost of counterfeiting makes counterfeiting more likely. If counterfeit currency is indistinguishable from legitimate currency, routine counterfeiting raises the growth rate of money, all else equal. If counterfeit currency is distinguishable from legitimate currency, counterfeiting raises the cost of transacting with currency, as users must be on-guard and employ costly detection strategies to protect themselves from receiving potentially-worthless counterfeits. In either case, the lower cost of counterfeiting currency makes counterfeiting more likely and, hence, bitcoin more attractive relative to currency.

Correspondingly, as the cost of obtaining bitcoin via theft or fraud falls, the likeli-

hood that bitcoin circulates falls, as well.[9] There is effectively no difference to the seller from receiving no money in exchange for goods and services and receiving a money that will be promptly stolen. Users must have a reasonable degree of confidence that their funds will be secure once received. Moreover, the lower the cost of theft or fraud, the more costs one might need to incur to sufficiently protect against such outcomes. Just as counterfeiting currency makes bitcoin more attractive relative to currency, the prospect of losing one's bitcoin due to theft or fraud makes currency more attractive relative to bitcoin.

We have offered a simple model in Section 2, which yields several interesting implications. However, the real world is much more complex than our model. Recognizing this, we might also use this model as a foil: identifying the features of the real world that are absent in our model and then considering the implications of incorporating those features. For example, in our model, currency and bitcoin are assumed to have the same exchange properties. Either can be used to make the available transactions, provided that others accept it, with one being no better at executing the transaction than the other. They are only assumed to differ in terms of how their supplies are managed, the relative transaction fee, and the costs of counterfeiting, theft, and fraud. It seems plausible, however, that bitcoin is better suited for making some transactions, and visa versa.

In a recent paper, Hendrickson and Luther (2021) discuss the financial privacy afforded by cash, digital dollars, and bitcoin. Cash typically offers the most financial privacy, though it typically requires the parties to an exchange be physically present

[9]Similarly, Luther and Salter (2017) find that a greater risk of government expropriation encourages users to consider bitcoin.

and capable of making exact change. Bitcoin typically offers more financial privacy than digital dollars, but—unlike cash—maintains a record of all past transactions between pseudonymous parties; it also does not require the parties to an exchange be physically present. Hence, bitcoin might be more useful than currency (cash or digital dollars) in long-distance transactions where financial privacy is important. Recognizing the unique exchange properties of currency and bitcoin implies that bitcoin might circulate exclusively or as a niche money even if it is dominated in terms of the features considered in Section 2.

Another simplification that might lead to inappropriate conclusions is our limiting the choice to just two monies, currency and bitcoin. In the real world, there are many government-issued currencies and alternative cryptocurrencies (alt-coins) available. Consider the view, which follows directly from our model, that those in places like Argentina, Venezuela, and Zimbabwe might be more inclined to use bitcoin given the historical experiences in those countries with excessive money growth. It is also possible that individuals in these countries would adopt some more stable currency, like the dollar, rather than bitcoin. Likewise, those interested in maintaining financial privacy while conducting long-distance transactions might opt for a privacy-focused alt-coin like zcash or monero instead of bitcoin.

Finally, our model can be used to explore questions other than the likelihood that bitcoin will circulate. For example, early proponents of bitcoin sometimes claimed that it would serve as a check on a government's ability to print money. This view is consistent with our model: for a given bitcoin transaction fee, there exists a growth rate of currency above which only bitcoin will be accepted. If a government is intent

on seeing its own currency circulate, therefore, it must ensure the growth rate of its currency falls below this threshold. Historical experience suggests that the knife-edge equilibrium implied by the model is probably too strong.[10] Nonetheless, the view that competition from alternatives like bitcoin provides some constraint on a government's ability to debase the currency seems plausible.

Of course, controlling the growth rate of currency is not the only way governments facing competition from bitcoin might maintain market share.[11] The random matching models offered by Aiyagari and Wallace (1997) and Li and Wright (1998) suggest a sufficiently large government can determine the medium of exchange by committing to make transactions in its preferred money. Hendrickson et al. (2016) show that this result generally holds when agents choose their trading partners, rather than being matched randomly. And Hendrickson and Luther (2017) go even further, showing that a government of *any* size can ban bitcoin so long as it is willing to mete out sufficiently severe punishments. Whether governments have the desire or the political will to do what is required to prevent bitcoin or other alt-coins from encroaching on their ability to create money remains to be seen. But one should at least recognize the prospect.

4 Conclusion

Over the last twelve years, bitcoin has grown from a little-known open source project to a functioning medium of exchange employed all over the world. But usage remains quite limited. One naturally wonders whether bitcoin (or some alt-coin) can compete

[10] Luther (2013) surveys the debate between Milton Friedman and F.A. Hayek on the question of currency substitution and then explores more recent evidence.

[11] Luther and White (2014), Luther (2016a) discusses potential obstacles to widespread bitcoin adoption.

with or even replace existing fiat monies. We have offered a simple model to address this question.

Our model takes as given that bitcoin has a fixed supply schedule and will eventually rely exclusively on fees to process transactions. We show that there are equilibria where (1) only bitcoin circulates, (2) only currency circulates, and (3) both bitcoin and currency circulate. In particular, we show that, for a given growth rate of currency, the fee associated with processing bitcoin transactions determines whether it will circulate. If the fee is sufficiently high, economic agents will only hold currency. If the fee is sufficiently low, economic agents will only hold bitcoin.

The simple model we have offered herein is not intended to serve as the final word on the subject. As with any good model, it is merely intended to provide a framework for exploring the relevant issues. With this in mind, we have discussed several shortcomings of the model and informally considered how relaxing some of the assumptions in the model might affect the results. We hope that others will build on our work in interesting ways to explore the prospects for bitcoin and other cryptocurrencies in the future.

References

S. Rao Aiyagari and Neil Wallace. Government transaction policy, the medium of exchange, and welfare. *Journal of Economic Theory*, 74(1):1–18, 1997.

Mike Co. Bitcoin, monetary expansion, and 'safe Havens'. *Medium*, March 2020.

Alan Feuer. The bitcoin ideology. *The New York Times*, December 2013.

Glassnode. Bitcoin: Fee (mean). Data, 2020. URL https://studio.glassnode.com/metrics?a=BTC&c=usd&m=fees.VolumeMean.

Konrad Graf. On the origins of bitcoin: stages of monetary evolution. 2013.

Frank H. Hahn. The foundations of monetary theory. In *Monetary Theory and Economic Institutions*, pages 21–43. Springer, 1987.

Peter K. Hazlett and William J. Luther. Is bitcoin money? And what that means. *Quarterly Review of Economics and Finance*, 77:144–149, 2020.

Joshua R. Hendrickson and William J. Luther. Banning bitcoin. *Journal of Economic Behavior & Organization*, 141:188–195, 2017.

Joshua R. Hendrickson and William J. Luther. Cash, crime, and cryptocurrencies. *Quarterly Review of Economics and Finance*, 2021.

Joshua R. Hendrickson, Thomas L. Hogan, and William J. Luther. The political economy of bitcoin. *Economic Inquiry*, 54(2):925–939, 2016.

Roger Huang. Bitcoin vs. inflation. *Forbes*, May 2020.

Narayana R. Kocherlakota. Money Is memory. *Journal of Economic Theory*, 81:232–251, 1998.

Ricardo Lagos and Randall Wright. A unified framework for monetary theory and policy analysis. *Journal of Political Economy*, 113(3):463–484, 2005.

Ricardo Lagos and Randall Wright. When is money essential? A comment on Aliprantis, Camera and Puzzello. 2008.

Timothy B. Lee. Four reasons bitcoin is worth studying. *Forbes*, April 2013.

Yiting Li and Randall Wright. Government transaction policy, media of exchange, and prices. *Journal of Economic Theory*, 81(2):290–313, 1998.

William J. Luther. Friedman versus Hayek on Private Outside Monies: New Evidence for the Debate. *Economic Affairs*, 33(1):127–135, 2013.

William J. Luther. Cryptocurrencies, network effects, and switching costs. *Contemporary Economic Policy*, 34(3):553–571, 2016a.

William J. Luther. Mises and the moderns on the inessentiality of money in equilibrium. *Review of Austrian Economics*, 29(1):1–13, 2016b.

William J. Luther. Regulating bitcoin: on what grounds? In Hester Peirce and Benjamin Klutsey, editors, *Reframing Financial Regulation: Enhancing Stability and Protecting Consumers*, pages 391–415. Mercatus Center at George Mason University, Arlington, VA, 2016c.

William J. Luther. Is bitcoin intrinsically worthless? *Journal of Private Enterprise*, 33(1): 31–45, 2018.

William J. Luther. Getting of the ground: the case of bitcoin. *Journal of Institutional Economics*, 15(2):189–205, 2019.

William J. Luther. Regulatory Ambiguity in the Market for Bitcoin. *Review of Austrian Economics*, 2020.

William J. Luther and Alexander W. Salter. Bitcoin and the Bailout. *The Quarterly Review of Economics and Finance*, 66:50–56, 2017.

William J. Luther and Sean Stein Smith. Is bitcoin a decentralized payment mechanism? *Journal of Institutional Economics*, 16(4):433–444, 2020.

William J. Luther and Lawrence H. White. Can Bitcoin Become a Major Currency? *Cayman Financial Review*, 36:78–79, 2014.

Satoshi Nakamoto. Bitcoin: a peer-to-peer electronic cash system. Published: Working paper, 2008.

Satoshi Nakamoto. Bitcoin open source implementation of P2P currency, February 2009. URL https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

George A. Selgin. Synthetic commodity money. *Journal of Financial Stability*, 17:92–99, 2015.

Lawrence H. White. The market for cryptocurrencies. *Cato Journal*, 35(2):383–402, 2015.

Aaron Yelowitz and Matthew Wilson. Characteristics of Bitcoin users: an analysis of Google search data. *Applied Economics Letters*, 22(13):1030–1036, 2015.