Economic Inquiry

BITCOIN 1, BITCOIN 2, ...: AN EXPERIMENT IN PRIVATELY ISSUED OUTSIDE MONIES

RODNEY GARRATT and NEIL WALLACE*

The value of bitcoin depends upon self-fulfilling beliefs that are hard to pin down. We demonstrate this for the case where bitcoin is the only form of money in the economy and then generalize the message to the case of multiple bitcoin clones and/or a competing fiat currency. Some aspects of the indeterminacy we describe would no longer hold if bitcoin were an interest-bearing object. (*JEL* D50, E42)

I. INTRODUCTION

Kareken and Wallace (1981) set out some sufficient conditions for the relative values of two fiat currencies to be indeterminate—sufficient conditions for exchange rate indeterminacy. Many would say that their sufficient conditions are not met by the currencies issued by countries. For example, they did not assume that the taxes levied by a country have to be paid in the form of that country's currency or that some prices denominated in the currency of a country are fixed or sticky. What about bitcoin? Bitcoin and its actual and potential rivals—in the title intentionally mislabeled bitcoin 1, bitcoin 2, … in order to indicate that there could be many of them—do seem to satisfy all the assumptions that Kareken and Wallace made to get exchange-rate indeterminacy. In other words, the best theory of the value of bitcoin is that it rests on what are called self-fulfilling beliefs and that the set of beliefs that can be self-fulfilling is huge. Put still differently, little can be said about the future value of bitcoin.

II. HOW SHOULD WE VIEW BITCOIN?

Most economists distinguish between inside and outside money. Inside money is *inside* the economy in the sense that each unit is someone's asset and someone else's liability. That is, inside money disappears if there is sufficient consolidation across the balance sheets of agents in the economy. Examples of inside money are checking accounts and grocery-store coupons. Outside money, in contrast, does not disappear when balance sheets are consolidated. Examples are gold coins under a gold standard and Federal Reserve notes since August 15, 1971 when Nixon closed the gold window. In terms of that dichotomy, bitcoin is best viewed as an outside money. In particular, the issuer of bitcoin makes no promise to redeem it for any other object. As regards competition, while there is nothing strange about competition among different inside monies, competition among different outside monies is problematic.[1] In particular, an outside money does not satisfy the notion of goods to which Adam Smith's invisible-hand proposition applies.

An issuer of outside money must deal with two concerns on the part of those who potentially accept it: additional issues of it and counterfeiting of it. Most would agree that the initial issuer (and inventor) of bitcoin successfully alleviated both concerns. We can assume that the initial stock of bitcoin was fixed at the outset forever and that there is no possibility of counterfeiting it.[2] Any weakening of these assumptions will only make it easier to reach the conclusion that little can be said about the future value of bitcoin.

One other assumption is crucial; namely, that people give up other things to get bitcoin only because they think that others in the future will

*We are grateful to Charles Kahn and an anonymous referee for helpful comments.

Garratt: Professor, Department of Economics, University of California Santa Barbara, Santa Barbara, CA 93106. Phone 805-893-2849, E-mail garratt@ucsb.edu

Wallace: Distinguished Professor, Department of Economics, Pennsylvania State University, University Park, PA 16802. Phone 814-863-3805, E-mail nxw9@psu.edu

1. See, for example, the discussions in Hellwig (1985) and Wallace (1979).

2. We are aware of the fact that the total stock of bitcoin increases over time up to a total of 21 million bitcoins, but this detail is not crucial to what we have to say.

Economic Inquiry
(ISSN 0095-2583)
Vol. 56, No. 3, July 2018, 1887–1897

doi:10.1111/ecin.12569
Online Early publication March 9, 2018

do the same. In other words, ownership of bitcoin does not yield utility as might ownership of a Picasso, and is not an input into the production of other things as is farmland, a factory, or a 3D printer. Nor does such ownership entitle the owner to a dividend stream of other valuable objects.[3]

Everything we have to say follows from the above assumptions: namely, that there is a fixed stock that is valuable today only because it is believed that others will treat it as valuable in the future. In particular, the electronic (*virtual*) feature of bitcoin and its purported use in illegal activity play no role. After all, even those who acquire bitcoin through illegal activity accept it only because they think others will accept it in the future.

The above assumptions about bitcoin are classic assumptions about outside monies. Indeed, David Hume and other founders of the quantity theory of money made those assumptions at a time when the objects used as money were commodities—gold and silver. They found it useful to ignore the commodity value of the objects used as money when making predictions about how the total value of money would vary with its quantity. When it comes to bitcoin, there is no commodity value to ignore. You cannot even use it as wall paper—as some stories suggest was performed with German marks during the 1922–1923 hyperinflation.[4]

Although we are interested in drawing conclusions about the value of bitcoin in terms of other assets like Federal Reserve notes, it is convenient and informative to start by demonstrating that the problem of multiple equilibria occurs even when bitcoin is the only asset.[5] We do so against the background of a very simple model introduced to most economists by Samuelson (1958). And, in keeping with the goal of keeping the exposition accessible, we use the simplest version of such a model—a version of identical two-period lived overlapping generations with one good per date.[6]

After exploring the problems of pinning down money prices in the one-money model, we expand our analysis to include a competing outside (fiat) money. Absent any distinguishing features of the fiat money, such as special treatment by the government, its addition adds to the indeterminacy problem by introducing a coordination problem. People must decide which money to use, or, if both are used, in what proportions. If bitcoin and the fiat currency are perfect substitutes as stores of wealth, then their coexistence magnifies the indeterminacy problems already present in the one-money economy. However, it is reasonable to assume that fiat money is at a disadvantage as a store of value due to its physical nature. When we add a storage cost to fiat money, the equilibrium set changes. There is no longer an equilibrium in which both monies co-exist with constant prices; however, there is an equilibrium in which both currencies co-exist for an indeterminate period of time until bitcoin becomes valueless. This equilibrium requires that peoples' beliefs over bitcoin prices include the possibility of a collapse. These beliefs can be entirely baseless or they can reflect uncertainty about some fundamental aspect of the bitcoin technology or other external forces that may prohibit the use of bitcoin (i.e., legal restrictions).

Further variations of the model, including a single fiat money and multiple versions of bitcoin, are discussed but not fully explored. Finally, we discuss other aspects of competing outside monies, such as the payment of interest.

A. *Existing Literature*

Most of the existing papers that model the bitcoin/dollar exchange rate do so for the purpose of empirical estimation. These papers specify models where consumers trade off the benefits of using bitcoin versus the fiat currency to achieve some spending objective. In Athey et al. (2016), the consumer seeks to make remittance

3. In this regard, it is important to distinguish between dividends in the form of other valuable objects and dividends that consist of more bitcoins. It is well known that additional quantities of bitcoin can be earned by devoting computer time to verifying transactions. That resembles a scheme in which additional issues of the common stock of a company are given as rewards for costly activities. Such dividends are consistent with everything assumed here. In particular, unlike dividends paid in the form of other valuable objects, such dividends do not make the rate of return on bitcoins rise as the value of bitcoins fall.

4. While bitcoins are intrinsically worthless, there is value associated with the underlying protocol. The term "colored coins" is often used to describe methods for representing ownership of physical assets (e.g., land, stocks, movie tickets) on the bitcoin blockchain. This is distinct from the idea of having multiple versions of bitcoin, as suggested in our title.

5. Paul Krugman in his blog "Bitcoin Is Evil" and Charlie Stross in his blog "Why I Want Bitcoin to Die in a Fire" raised several concerns regarding the viability of bitcoin as a replacement for fiat currencies. These included its price volatility and the deflation implied by its fixed supply. We add price indeterminacy to the list.

6. This assumption limits us in some ways when we turn to competing currencies as one could imagine that some currencies are more suitable for the purchase of some goods.

payments. In contrast to the fiat currency, bitcoin has no fee, but there is a time cost of usage and there is a chance that bitcoin may "break" at any moment and become valueless. Likewise in Ciaian, Rajcaniova, and Kancs (2016), bitcoin demand relative to dollar demand is based on exogenous factors (velocity, size of the bitcoin economy, general price level) which are linked together through an adaption of the quantity equation specified in Barro (1979). These papers specify demand and supply equations that have a unique equilibrium and, hence, provide testable models of the bitcoin/dollar exchange rate. These models capture bitcoin price movements with varying success, but they are not adequate for the purposes of understanding the range of equilibrium possibilities. There are no goods in these models, just currencies and assumed demand for their usage. These models are inconsistent with the multiple equilibria that we contend any reasonable model of the value of bitcoin should display. In particular, there is no equilibrium in which bitcoin exists, but has zero value.

Bolt and van Oordt (2016) combine a quantity theory model of the virtual currency price with a speculative demand model. Speculative demand is determined by investors that maximize mean–variance utility over future wealth: future wealth is a random variable that depends on the choice of holdings of the virtual currency and an exogenous random variable that determines its uncertain future value. Thus, the price of the virtual currency is determined by two equations: the Fisher quantity equation and the first-order condition for the optimal investment choice. As in the empirical work mentioned above, there are no goods in this model and, hence, the value of the virtual currency is pinned down by assumptions on the direct utility consumers and merchants get from using it to transact.

Fernández-Villaverde and Sanches (2016) evaluate the role of competing (possibly virtual) private currencies by adding currency-providing entrepreneurs to the Lagos and Wright (2005) model. There, money is needed to facilitate trade across the centralized and decentralized markets, since goods are perishable and traders are anonymous, and the money supply is determined from the profit maximization motive of the entrepreneurs. They obtain similar qualitative results to ours: indeterminacy of money prices and the existence of a zero-price equilibrium. They also share the indeterminacy of supply by individual suppliers that was identified by Klein (1974). These authors go on to consider the competing role of government-supplied money when the government has the ability to impose taxes and when entrepreneurs have access to productive capital. The existence of productive capital provides a fundamental value for the entrepreneur's currency-issuing business and eliminates equilibrium paths that converge to worthless money. In fact, it is well known that adding a positive real dividend to money, no matter how small, eliminates worthless money and eliminates equilibrium paths that converge to worthless money in any model. Therefore, as discussed in the section on interest payments, this is necessarily true in our model as well.

III. ONE GOOD, ONE MONEY (BITCOIN)

Time is discrete and extends into the indefinite future with dates labeled $t = 1, 2, \ldots$. There is one perishable good per date, the total amount of which is constant over time and denoted W. At each date t, a new generation of N identical two-period lived people appears. The generation that appears at t is labeled generation t and is young at t and old at $t+1$.

Each member of generation t for $t \geq 1$ is selfish and cares about his or her own life-time profile of consumption according to a utility function, denoted $u(c_t^{\text{young}}, c_t^{\text{old}})$, where, as indicated, the first argument is consumption when young and the second argument is consumption when old. The function $u : \mathbb{R}_{++}^2 \to \mathbb{R}$ is strictly increasing, strictly concave, and continuously differentiable (examples include $\ln c_t^{\text{young}} + 0.9 \ln c_t^{\text{old}}$ and $(c_t^{\text{young}})^{1/2} + 0.8(c_t^{\text{old}})^{1/2}$.) Under uncertainty, people maximize expected utility.

There is a fixed stock of money, denoted B (for bitcoin).[7] As opposed to the good, money is durable in the sense that it can be stored costlessly from one date to the next. Finally, if we want to make this a model in which the existence of this stock of money helps achieve outcomes that would otherwise not be achievable, then we should assume that generation t does not know what generation $t-1$ did when they were young.[8]

7. The actual supply of bitcoins increases over time (at a decreasing rate) until the year 2140, at which point a total supply of 21 million coins will have been distributed. Our assumption of an initial fixed stock is, of course, a simplification. The essential aspect is that total stock of bitcoins at any point in time, present or future, is known.

8. See Kandori (1992) for a discussion of the role of money in overlapping generations models.

A. Private-Ownership, Price-Taking Equilibrium

Everything is owned by someone, including the fixed stock of money, B, which can be freely discarded. In particular, each member of generation t for $t \geq 1$ owns the same income stream, denoted $(w^{\text{young}}, w^{\text{old}})$, where w^{young} denotes the income of a young generation-t person in the form of the perishable date-t good and w^{old} denotes the income of a generation-t person in the form of the perishable date-$t+1$ good. We assume that $N(w^{\text{young}} + w^{\text{old}}) = W$. Each member of generation 0, the initial old at $t = 1$, owns w^{old} amount of the date-1 good and B/N amount of money.

At each date t, people face a non-negative price at which the date-t good can be traded for bitcoin. It is convenient to express this price as a price of bitcoin in terms of the good—the amount of the good that has to be given up to acquire one unit of bitcoin. We denote the date-t price p_t^B. Finally, beliefs are important; if the young at a date give up some of the good for money, it is because they think the next generation will also do that. Throughout, we assume that people in the model have beliefs that are consistent with the model in which they live or, in other words, have what are called *rational expectations*.

Because we want to consider both equilibria under uncertainty and equilibria with some uncertainty, we will not formally define equilibrium at this point. Roughly speaking, an equilibrium is an allocation, possibly random sequences of consumption and money holdings, and a possibly random sequence for p_t^B, such that the allocation is feasible (satisfies market clearing) and such that the individuals are doing the best they can for themselves while facing the possibly random sequence for p_t^B.

B. Four Questions about Equilibria

Rather than try to describe the entire set of equilibria for the above model, we will limit ourselves to addressing the following four questions: (i) Is there an equilibrium in which the value of bitcoin is constant and positive? (ii) Is there an equilibrium in which the value of bitcoin is always zero? (iii) Is there an equilibrium in which the value of bitcoin is zero at some known date T and is positive at some earlier dates? (iv) Is there an equilibrium in which the value of bitcoin is random in the following way: if it has been positive and constant at each date 1, 2, …, $t-1$, then with probability π the value is equal to that constant at t; otherwise, it is zero at t and thereafter.

The first three questions can be answered using the same apparatus. We start by setting out the equations that describe how consumption opportunities of a young generation-t person depend on the quantity of money purchased, an amount denoted b_t:

$$(1) \quad c_t^{\text{young}} = w^{\text{young}} - p_t^B b_t \equiv w^{\text{young}} - s_t^B$$

$$(2) \quad c_t^{\text{old}} = w^{\text{old}} + p_{t+1}^B b_t \equiv w^{\text{old}} + \left(p_{t+1}^B / p_t^B\right) s_t^B.$$

In the second equation in Equation (1), s_t^B, a mnemonic for saving in bitcoin, is a convenient shorthand for $p_t^B b_t$. The second equation in Equation (2) is valid only if p_t^B is positive. The person is not allowed to choose $b_t < 0$, which would correspond to issuing money or borrowing. Hence, the person cannot choose $s_t^B < 0$.

In order to proceed using calculus (of one variable), we insert the second expressions for consumption from Equations (1) and (2) into the utility function so that we end up expressing utility in terms of s_t^B; namely, as

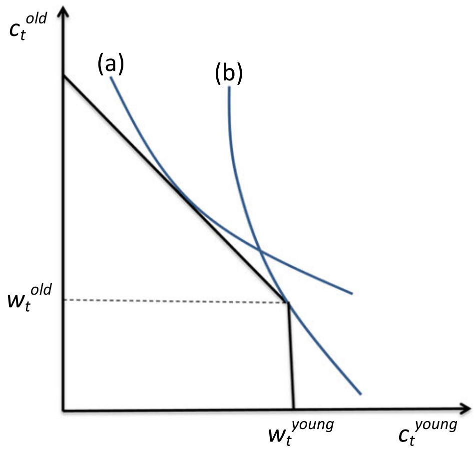
$$(3) \quad u\left[w^{\text{young}} - s_t^B, w^{old} + \left(p_{t+1}^B / p_t^B\right) s_t^B\right] \equiv f\left(s_t^B; p_{t+1}^B / p_t^B\right).$$

We can answer question (i) by setting $\left(p_{t+1}^B / p_t^B\right) = 1$ and determining if there exists a positive and constant s^B that maximizes the function $f(s^B;1)$ for each generation t. (Because the function f is strictly concave and differentiable, a necessary and sufficient condition for the existence of a unique and positive s^B that maximizes the function f is $\partial f(0;1)/\partial s^B > 0$.) If there is such an s^B, let us call it s^{B*}. We then obtain a positive and constant magnitude of p_t^B, denoted p^B, by solving $s^{B*} = p^B(B/N)$.

We can represent the conditions under which there is and is not a positive s^{B*} in a simple and familiar diagram. In Figure 1, we depict two possibilities for the indifference curve implied by the utility function and the trading opportunities implied by $\left(p_{t+1}^B / p_t^B\right) = 1$. In scenario (a), the utility function and the income stream are such that there is a positive s^{B*}, while in scenario (b) a positive s^{B*} does not exist.

Thus, our answer to question (i) is maybe. The environment and the income stream may be such that the answer is yes, but may also be such that the answer is no. Let us proceed under the assumption that the environment and the lifetime income stream are such that the answer is

FIGURE 1
Alternative Preference Specifications



yes—that we have the situation depicted in scenario (a) in Figure 1.

Now we turn to question (ii). The answer is arrived at by examining the first equalities in Equations (1) and (2) and by adopting the usual view that an object is worthless if the demand for it at any positive price falls short of the supply. Suppose at any t, the young at t believe that bitcoin will be worthless at $t+1$; that $p_{t+1}^B = 0$. Then, each young person chooses $b_t = 0$ at time t at any $p_t^B > 0$. (Why give up goods which can be consumed when young in order to acquire an asset that will be worthless when it is sold?) Because this conclusion holds for each t, there is an equilibrium in which $p_t^B = 0$ for all t.

Now we can quickly answer question (iii): Is there an equilibrium in which $p_T^B = 0$ and $p_t^B > 0$ for some $t < T$? Consider what happens at $T-1$. As in our argument concerning question (ii), no one is willing to give up goods for money at $T-1$. Then, by backward induction, no one gives up goods for money at any $t < T$. Hence, the answer to question (iii) is no.

Finally, we turn to question (iv). We can restate the question as follows: Is there an equilibrium in which at each date t,

$$(4)\quad p_t^B = \begin{cases} p^B > 0 & \text{with prob } \pi \text{ if } p_k^B = p^B \\ & \text{for } k = 1, 2, \ldots, t-1. \\ 0 & \text{otherwise} \end{cases}$$

Before proceeding, let us give one possible interpretation of the events underlying this process for p_t^B. At the beginning of each date, before trade occurs, there is a simple two-outcome public lottery that determines an outcome from the set *{heads, tails}*, where the lottery is such that heads occurs with probability π and tails occurs with probability $1-\pi$. Also, if heads has occurred at dates, 1, 2.....$t-1$, then the same lottery happens at date t. If not, then $p_t^B = 0$. (That is, once tails appears, bitcoin is worthless from then on, an equilibrium we know exists based on our answer to question (ii).) Thus, *otherwise* in Equation (4) includes the appearance of tails at date-t or at any earlier date.

Now, assume heads has appeared at dates 1, 2, …, t. A young person at t maximizes

$$(5)\quad \pi u\left[c_t^{\text{young}}, c_t^{\text{old}}(heads)\right] + (1-\pi)\, u\left[c_t^{\text{young}}, c_t^{\text{old}}(tails)\right]$$

where

$$(6)\quad c_t^{\text{young}} = w^{\text{young}} - s_t^B$$

$$(7)\quad c_t^{\text{old}}(heads) = w^{\text{old}} + \left(p_{t+1}^B / p_t^B\right) s_t^B \quad \text{and } c_t^{\text{old}}(tails) = w^{\text{old}}.$$

Here, a young person at t faces uncertainty about the outcome of the lottery at the next date. The outcome could be heads or it could be tails and we have labeled consumption when old as dependent on that outcome. Now, we cannot easily use a diagram unless you are adept at depicting three dimensions: one dimension for c_t^{young}, one for $c_t^{\text{old}}(heads)$, and one for $c_t^{\text{old}}(tails)$. We can, however, easily use calculus. Let us substitute Equations (6) and (7) into Equation (5) and call the result $g\left(s_t^B; p_{t+1}^B/p_t^B, \pi\right)$. Then we can state two simple results that provide an answer to question (iv): (a) If $\partial g(0; 1, \pi)/\partial s_t^B > 0$, then the answer is yes; (b) if $\partial f(0;1)/\partial s^B > 0$, then there exists $\pi^* < 1$ such that if $\pi \in [\pi^*, 1]$, then the answer is yes. (The proof of (a) is the same as the proof we used to answer question (i). The proof of (b) uses the fact that question (iv) and question (i) are the same question when $\pi = 1$ and the assumption that the function u is continuously differentiable.)

Our answers to questions (iii) and (iv) are an instance of a general phenomenon that depicts the sense in which a collapse in the value of a money is hard to predict. Suppose the answer to question (iv) is positive, that $\pi = 0.99$, that we are living at date 68, that heads has been experienced at all earlier dates, but that tails has occurred at date 68. Someone might be tempted to criticize economists for not having predicted the collapse in the value of money at date 67. At $t = 1$, someone who knows the model and the equilibrium would have said that the probability of a collapse at *some* time in the first 68 periods is $(1-.99^{68}) = 0.495$, almost one-half. However, from the vantage point of date 67, a collapse at date 68 happens only with probability 0.01. In other words, and consistent with our answer to question (iii), although a collapse at some time is likely, predicting when it will occur is not possible.

There are two, substantially different interpretations of the *heads-tails* randomness in the equilibrium described in question (iv). One interpretation is that the uncertainty is purely extrinsic. That is, heads and tails represent the two outcomes of a publicly observed sunspot variable à la Cass and Shell (1983). The appearance of a tails sunspot triggers a change in beliefs that leaves bitcoin valueless. This interpretation is consistent with our message that equilibrium prices depend upon beliefs which may be hard to predict. And, it illustrates a rather interesting aspect of rational expectations equilibria. Under the assumption that storing fiat money is costly and storing bitcoin is not, bitcoin is a strictly superior technology for storing wealth. And yet, the simple fact that people, for whatever reason, have pessimistic beliefs about the future value of bitcoin, means that both bitcoin and fiat money can coexist with positive prices.

The other interpretation of the randomness underlying the equilibrium described in question (iv) is that the heads-tails variable represents intrinsic uncertainty. The appearance of *tails* could represent the appearance of a preferred version of bitcoin, say bitcoin 2, that is started by the young at each date with probability π.[9] Or, we could imagine that at every date t there is an exogenous probability $1-\pi$ that there is a disruption of platform for transacting bitcoin (someone hacks the protocol) or the passage of a law outlawing bitcoin. The addition of intrinsic uncertainty to our model would change some of our conclusions. For instance, there would be no constant price equilibrium in the sense of question (i)—trivially, the price of bitcoin cannot be positive and constant after the platform for transacting bitcoin is rendered obsolete, illegal, or is undermined in some other way.

IV. ONE GOOD, TWO MONIES

Everything is the same as in the one money, one good model except that now there is a fixed stock of fiat money, M that coexists alongside the fixed stock of bitcoin, B. Although both forms of money are durable, there is a storage cost for holding the fiat money. Bitcoin, in contrast, can be costlessly stored.[10] Let p_t^B and p_t^M denote the period t prices of bitcoin and fiat money in terms of the numeraire good, respectively. As before, each member of generation t for $t \geq 1$ is selfish and maximizes life-time utility from consumption net of any disutility from public purchases. More specifically, using the notational conventions of Section III, let b_t and m_t denote a young generation-t's purchases of bitcoin and fiat money, respectively, and let s_t^B and s_t^M denote the corresponding savings in terms of bitcoin and fiat money, where $s_t^B = p_t^B b_t$ and $s_t^M = p_t^M m_t$. Then, the storage cost (in terms of utility) of a young generation-t individual with fiat money holding m_t is determined by the current value of these holdings, denoted above as s_t^M, according to the function $v\left(s_t^M\right)$, where $v(0) = 0$ and $v' \geq 0$.

Again letting c_t^{young} and c_t^{old} denote the period t consumption of young and old people, respectively, the young generation-t individual solves

$$\max_{s_t^M, s_t^B} u\left(c_t^{\text{young}}, c_t^{\text{old}}\right) - v\left(s_t^M\right) \tag{8}$$

where

$$c_t^{\text{young}} = w^{\text{young}} - s_t^B - s_t^M \tag{9}$$

and

$$c_t^{\text{old}} = w^{\text{old}} + \left(p_{t+1}^M / p_t^M\right) s_t^M + \left(p_{t+1}^B / p_t^B\right) s_t^B. \tag{10}$$

We maintain our standard assumptions on u.

A. *Zero Storage Costs:* $v\left(s_t^M\right) \equiv 0$

In this case the two monies are perfect substitutes. There exists a constant price equilibrium

9. The August 1, 2017 launch of Bitcoin Cash, a new version of the bitcoin protocol with a larger block size, could have, at least in principle, led to the abandonment of the original bitcoin. Time will tell how this ultimately plays out.

10. An alternative interpretation of this model is that all purchases made with money M are public and all purchases made with money B are private. The storage cost can then be interpreted as disutility from public purchases due to the loss of privacy; see Kahn, McAndrews, and Roberds (2005).

(type (i) in Section III) in which saving is done through all of one money or the other or both.

To see this, set $p^M_{t+1}/p^M_t = p^B_{t+1}/p^B_t = 1$. Then all that matters in the utility maximization problem is the choice of total savings $s_t = s^B_t + s^M_t$. A unique, positive constant solution s^* exists under the conditions provided in Section III. Given the stocks of money we simply require price levels to satisfy

$$s^* = p^B B/N + p^M M/N. \tag{11}$$

But this allows a wide array of constant money price combinations.

We could pin things down if we assumed people had strong preferences over the type of money they used. Suppose a fraction α of each generation only wishes to hold B and a fraction $1-\alpha$ of each generation only wishes to hold M.[11] We could think of the fraction α as the Libertarians. Then we would require

$$s^* = p^B B/(\alpha N) = p^M M/((1-\alpha)N) \tag{12}$$

implying

$$p^B = \alpha Ns/B, \text{ and } p^M = (1-\alpha)Ns/M. \tag{13}$$

So the price of each money is increasing in the fraction of people that prefer to use it and decreasing in the stock of each money.

Example 1. Let $u\left(c^{\text{young}}_t, c^{\text{old}}_t\right) = \ln\left(c^{\text{young}}_t\right) + 0.9\ln\left(c^{\text{old}}_t\right)$ and set $p^M_{t+1}/p^M_t = p^B_{t+1}/p^B_t = 1$. Given constant prices we look for a solution with constant money savings s^M and s^B. Substituting Equations (9) and (10) into Equation (8) gives us the unconstrained utility maximization problem of the young consumer:

$$\max_{s^B, s^M} \ln\left(w^{\text{young}} - s^B - s^M\right) + 0.9\ln\left(w^{\text{old}} + s^M + s^B\right). \tag{14}$$

The first-order necessary condition for an optimum solution is

$$-1/\left(w^{\text{young}} - s\right) + 0.9/\left(w^{\text{old}} + s\right) = 0 \tag{15}$$

where $s = s^B + s^M$. So total savings for each young individual is

$$s^* = \left(0.9w^{\text{young}} - w^{\text{old}}\right)/1.9. \tag{16}$$

Hence a constant price-taking equilibrium exists so long as $0.9w^{\text{young}} > w^{\text{old}}$. Moreover, if we pin things down by assuming α of each generation only wishes to hold M, then equilibrium money prices are

$$p^M = \alpha N\left(0.9w^{\text{young}} - w^{\text{old}}\right)/(1.9M) \text{ and}$$
$$p^B = (1-\alpha)N\left(0.9w^{\text{young}} - w^{\text{old}}\right)/(1.9B). \tag{17}$$

The above analysis applies equally well to the case of two privately issued outside monies: bitcoin 1 and bitcoin 2. Moreover, it extends easily to bitcoin 1, bitcoin 2, …, bitcoin n. The key point is that absent strong preferences over equivalent types of outside money there would be a high degree of price indeterminacy, even in the simplest, constant price equilibrium. To the extent that preferences over various outside money "brands" are fickle and unpredictable, solutions like the one proposed in Equation (13) are unlikely to be stable.

B. Linear Storage Costs: $v\left(s^M_t\right) = \ell s^M_t$

In this case, absent strong non-Libertarian preferences, there is no constant (positive) price equilibrium with both currencies in positive demand as constructed above. However, there are equilibria, analogous to the type (iv) equilibria of the one-money economy, in which the price of bitcoin depends on the outcome of an exogenous "heads-tails" random variable. Note that we are not explicitly modeling a probabilistic collapse of the bitcoin system (as in Athey et al. 2016), although this interpretation of our model is possible. Rather, we are pointing out that "pessimistic" beliefs on bitcoin's future equilibrium price path are sufficient to offset the real financial costs of storing fiat money and make people willing to hold the fiat currency. In other words, while people may not like paying a storage cost they may still hold fiat money if they think that at some point in the future people will lose faith in the alternative (bitcoin) currency.

If we start the date in a "so far nothing but heads" state and π is the probability of heads tomorrow and $1-\pi$ is the probability of tails tomorrow, then the utility maximization problem is

$$\max_{s^M_t, s^B_t} \pi u\left(c^{\text{young}}_t, c^{\text{old}}_t(\textit{heads})\right) + (1-\pi)u\left(c^{\text{young}}_t, c^{\text{old}}_t(\textit{tails})\right) - \ell s^M_t$$

where

$$c^{\text{young}}_t = w^{\text{young}} - s^M_t - s^B_t \tag{18}$$

11. There are no trade frictions in this economy so old B money lovers can always find young B money lovers to trade with and similarly for M money lovers.

(19)
$$c_t^{\text{old}}(heads) = w^{\text{old}} + \left[p_{t+1}^M(heads)/p_t^M(heads)\right]s_t^M + \left[p_{t+1}^B(heads)/p_t^B(heads)\right]s_t^B$$

(20)
$$c_t^{\text{old}}(tails) = w^{\text{old}} + \left[p_{t+1}^M(tails)/p_t^M(heads)\right]s_t^M$$

(21)
$$c_t^{\text{old},M}(heads) = \left[p_{t+1}^M(heads)/p_t^M(heads)\right]s_t^M$$

and

(22)
$$c_t^{\text{old},M}(tails) = \left[p_{t+1}^M(tails)/p_t^M(heads)\right]s_t^M.$$

Given prices, this problem has a solution under our assumptions, but in order to solve for *equilibrium* prices we need to also consider the problem of a young consumer following the realization of tails. This is necessary to determine market clearing prices that match the young generation's demand for money in the newly arrived at tails state with the old generation's supply.

Following a realization of tails, the value of bitcoin falls to zero and members of the young generation solve:

$$\max_{s_t^M} u\left(c_t^{\text{young}}, c_t^{\text{old}}\right) - \ell s_t^M$$

where

(23)
$$c_t^{\text{young}} = w^{\text{young}} - s_t^M$$

and

(24)
$$c_t^{\text{old}} = w^{\text{old}} + \left(p_{t+1}^M/p_t^M\right)s_t^M.$$

There is a solution to the linear storage costs model in which fiat money and bitcoin have constant positive prices each date up until the occurrence of "tails" and fiat money and bitcoin and have (different) constant prices (the latter being zero) in all dates following the occurrence of tails. The solution has constant money savings s^M and s^B, up to the realization of a tails state. Afterwards, savings in bitcoin is zero and there will be a new level of savings in fiat money, which we denote by $s^M(\textit{after tails})$. In this equilibrium the privacy cost of using fiat currency is counterbalanced by the potential for bitcoin to become worthless.

Example 2. Once again we let $u\left(c_t^{\text{young}}, c_t^{\text{old}}\right) = \ln\left(c_t^{\text{young}}\right) + 0.9\ln\left(c_t^{\text{old}}\right)$, but now we look for a solution where prices depend on the state of nature that is determined by independent coin tosses: each period outcome is heads with probability π and tails with probability $1-\pi$. Money prices start at $p^M > 0$ and $p^B > 0$, for the fiat currency and bitcoin, respectively, and remain this way so long as every outcome of the coin tosses is heads. If the coin ever comes up tails prices switch to q^M and 0, respectively, and remain that way forever, regardless of the outcome of future coin tosses.

Taking these prices as given the consumer solves the following unconstrained utility maximization problem in the "so far nothing but heads" states:

$$\max_{s^M,s^B} \pi\left[\ln\left(w^{\text{young}} - s^M - s^B\right) + 0.9\ln\left(w^{old} + s^M + s^B\right)\right] + (1-\pi)\left[\ln\left(w^{\text{young}} - s^M - s^B\right) + 0.9\ln\left(w^{old} + \left(q^M/p^M\right)s^M\right)\right] - \ell s^M$$

which simplifies to

$$\max_{s^M,s^B} \ln\left(w^{\text{young}} - s^M - s^B\right) + \pi 0.9\ln\left(w^{\text{old}} + s^M + s^B\right) + (1-\pi)\,0.9 \ln\left(w^{\text{old}} + \left(q^M/p^M\right)s^M\right) - \ell s^M.$$

The first-order necessary conditions for an interior solution are

(25)
$$-1/\left(w^{\text{young}} - s^M - s^B\right) + 0.9\pi/\left(w^{\text{old}} + s^M + s^B\right) + \left[0.9(1-\pi)/\left(w^{old} + \left(q^M/p^M\right)s^M\right)\right]\left(q^M/p^M\right) - \ell = 0$$

and

(26)
$$-1/\left(w^{\text{young}} - s^M - s^B\right) + 0.9\pi/\left(w^{\text{old}} + s^M + s^B\right) = 0.$$

Rewrite Equation (26) as

(27)
$$s^B + s^M = \left(0.9\pi w^{\text{young}} - w^{\text{old}}\right)/(1+0.9\pi).$$

Combine Equations (25) and (26) to get

(28)
$$s^M = 0.9(1-\pi)/\ell - \left(p^M/q^M\right)w^{\text{old}}.$$

Next consider the utility maximization problem starting in a "tails" state. This is the same problem that leads to equilibrium (i) from Section III.B with a slight modification due to the storage cost.

The unconstrained utility maximization problem of the young consumer is:

$$\max_{s^M} \ \ln\left(w^{\text{young}} - s^M\right) + 0.9 \ln\left(w^{\text{old}} + s^M\right) - \ell s^M. \tag{29}$$

The first-order necessary condition for an interior solution is

$$-1/\left(w^{\text{young}} - s^M\right) + 0.9/\left(w^{\text{old}} + s^M\right) - \ell = 0. \tag{30}$$

So total savings for each young individual in the tails state is given by the solution to the quadratic equation[12]

$$-\ell\left(s^M\right)^2 + \left(1.9 + \ell\left(w^{\text{young}} - w^{\text{old}}\right)\right)s^M + \ell w^{\text{young}} w^{\text{old}} + w^{\text{old}} - 0.9 w^{\text{young}} = 0. \tag{31}$$

Let $s^M(\textit{after tails})$ denote the solution to Equation (31). Then

$$q^M = s^M(\textit{after tails})\, N/M \tag{32}$$

where N is the number of individuals and M is fixed the stock of fiat money.

Note that we also have the equations

$$p^M = s^M(N/M) \ \text{ and } \ p^B = s^B(N/B) \tag{33}$$

where B is the fixed stock of bitcoin. Equations (27), (28), and (31)–(33) represent the six equations and six unknowns that (for suitable parameter choices that permit interior solutions – see the Appendix) describe the equilibrium.

As π approaches 1, s^M approaches 0, but $s^M(\textit{after tails})$ is not affected. Hence, for sufficiently large π we are assured that $s^M(\textit{after tails}) > s^M$, which implies $q^M > p^M$. The prices p^M and q^M represent the amount of the good that must be given up in order to get one unit of fiat money before and after the tails event, respectively. Thus, following a collapse in the price of bitcoin, there is a discrete drop in the money price of goods.[13]

Equilibria also exist in the two-monies setting in which the prices of either or both monies are zero. If the young hold the belief that the price of any money is zero next period, then they will demand zero units of that money today. Zero demand for money in the current period equates to excess supply and supports a price of zero.

12. A positive real solution exists since the discriminant is positive.

13. Of course, in reality, this drop would be small since holdings of bitcoin are negligible relative to fiat currency holdings in the United States.

V. INTEREST

Bitcoin was founded when the nominal interest rate was near zero, a situation that has continued up until now. Could it survive if the nominal interest rate was positive and substantial? In his insightful discussion of competitive monies, Klein (1974) notes that competitive forces would lead to interest payments on private monies. This leads us to consider whether there could be bitcoin-type monies which pay interest.

At the outset, we have to distinguish between interest payments in the form of the bitcoin object itself and interest payments in the form of other valuable objects, like base money. In this discussion we mean the latter, because the former has no significance: it is like paying dividends on a stock in the form of additional stock.

To think about this against the background of the overlapping generations model, let us reinterpret the currency (or base money) in the two-asset model as net government indebtedness, which includes deposits at the central bank, that pays nominal interest financed by lump-sum taxes. In doing this, we ignore currency, which is done in most applied macroeconomic models, or are considering a world in which the Rogoff (2016) proposal to eliminate currency has been adopted. One way to think about paying interest on a bitcoin-type object in the form of deposits at the central bank is to envisage the issuer as a particular kind of financial intermediary: the bitcoin issuer sells bitcoins for central bank deposits and uses the interest on those deposits to pay interest on the bitcoin-type objects. Certainly, the bitcoin technology would seem to lend itself easily to paying interest on holdings of the bitcoin-type object. However, existing bitcoin and such an interest-bearing version differ in two important respects.

First, the kind of multiplicity pointed out above no longer holds for such an interesting-bearing version of bitcoin. If d denotes the interest payment (or dividend) and p the constant price, both in units of deposits at the central bank, then the yield on bitcoin is d/p, which for a given $d > 0$ goes to infinity as p goes to zero. Therefore, such an interest-bearing version of bitcoin cannot have a zero price, which, in turn, rules out the type (ii) and (iv) equilibria in Section III.B or similar zero-price equilibria in Section IV. Second, this vision of an intermediary with liabilities in the form of a bitcoin-type object that pays interest seems to require a very different governance structure from existing bitcoin. It seems to require a legal structure consistent with assigning responsibility for paying interest on the bitcoin-type object. This differs a lot from the structure of existing bitcoin under which no one carries any kind of obligation aside from the limitations on subsequent issues built into the software.

VI. CONCLUDING REMARKS

Bitcoin currently has value and its value moves around. Admittedly, none of the equilibria described in this paper provide a good description of its value. However, the nature of the randomness described above could be generalized to enlarge the set of equilibria in a way that would make the set include ones that more closely resemble what we have seen. For example, there could be three possible outcomes (with associated probabilities) rather than just two: bitcoin 1 remains the only such money; bitcoin 2 appears and it and bitcoin 1 equally share the demand for such money; bitcoin 2 appears and completely supplants bitcoin 1. Also, there is no reason why π has to be constant. It, itself, could follow a random process as in what are called regime-switching models. And we could go on and on. That is why we said at the outset that the number of equilibria is huge.

Much of the uncertainty in the value of bitcoin comes from the ease of creating perfect substitutes. It is easy to clone bitcoin and the creation of very close substitutes makes the value of bitcoin rest on beliefs that may be hard to pin down.

Klein (1974) emphasizes that the coexistence of competing currencies requires trade at flexible exchange rates. Klein (1974, Section III A) points to historical examples where competing money systems that tried to enforce fixed exchange rates failed. Current versions of competing virtual currencies have flexible exchange rates, but there has been talk of issuing a bitcoin clone, Fedcoin, with a fixed one-to-one exchange rate with the U.S. dollar. The Fedcoin proposal involves two-way convertibility, but the Federal Reserve would control both the creation and destruction of Fedcoin. This aspect is crucial. As Klein points out, if a competing currency were issued by a private supplier, then, under a fixed exchange rate, the private supplier would have incentives to continually increase supply leading to an infinite price level.[14] Under the Fedcoin proposal each dollar of cash surrendered for Fedcoin would be removed from the monetary base and each dollar of Fedcoin surrendered for fiat currency would be removed from the distributed ledger for Fedcoin transactions. So, in fact, the Fedcoin proposal is really more about an alternative "form" of fiat currency than a competing, private outside money.

14. The idea is the same as Friedman's (1959) contention that indistinguishable competing currencies lead to an infinite price level, since indistinguishability implies a fixed-exchange rate.

APPENDIX

Parameter Choices that Permit an Interior Solution

The set of parameters that permit an interior solution will depend upon the functional form of the utility function. Here we provide a characterization of these parameter values for the utility function used in Examples 1 and 2. This analysis gives an indication of the required qualitative relationship between parameter values needed in other cases. In particular, the endowment when old must be sufficiently small relative to the endowment when young to induce saving. This relationship was already identified in Example 1 in Section IV.A. In Example 2, it is a bit more complicated. A condition is also required on the probability π that ensures fiat money, but not only fiat money, is demanded.

Begin by considering the "so far nothing but heads" problem. Our choice of the natural log function ensures the optimal choice will have strictly positive consumption when young and old. It is, in fact, easily verified by subtracting w^{young} from Equation (27) that the difference is negative: that is, $s^B + s^M < w^{\text{young}}$. Likewise, $s^M(\textit{after tails}) < w^{\text{young}}$. Also, from Equation (27) it is immediate that total savings (in terms of both monies) will be positive if

$$0.9\pi w^{\text{young}} > w^{\text{old}}. \tag{A1}$$

We mention in footnote 12 that the discriminant of Equation (31) is positive. This implies that there are two real roots for Equation (31). Moreover, using the quadratic formula for these two roots reveals two useful facts: the first root is always greater than w^{young} and hence is never a valid solution and the second root is always less than w^{young} and hence is a valid solution so long as it is positive. To see these facts let the two real roots be denoted by r_1, r_2 and let $w = w^{\text{young}} + w^{\text{old}}$. Then

$$r_1 - w^{\text{young}} = \left[1.9 - \ell w + \sqrt{(1.9 - \ell w)^2 + 4\ell w}\right] / 2\ell > 0 \tag{A2}$$

and

$$r_2 - w^{\text{young}} = \left[1.9 - \ell w - \sqrt{(1.9 - \ell w)^2 + 4\ell w}\right] / 2\ell < 0. \tag{A3}$$

The condition which ensures the second root is positive is, after some manipulations,

$$3.6\ell w^{\text{young}} - 4\ell w^{\text{old}} - 4\ell^2 w^{\text{young}} w^{\text{old}} > 0. \tag{A4}$$

Assuming this is satisfied we have $s^M(\textit{after tails}) = r_2 > 0$, which implies $q^M > 0$. Given $q^M > 0$ we can substitute the first expression in Equation (33) into Equation (28) to get

$$s^M = 0.9\,(1 - \pi)\,q^M M / \left[\ell\left(q^M M + N w^{old}\right)\right] > 0 \tag{A5}$$

for $\pi < 1$.

Taking stock, so far under the assumptions that Equations (A1) and (A4) hold and $\pi < 1$ we have that $s^M > 0$, $0 < s^M(\textit{after tails}) < w^{\text{young}}$ and $0 < s^M + s^B < w^{\text{young}}$. The only thing remaining is to determine conditions such that $s^B > 0$. Subtracting Equation (A5) from Equation (27) yields a rather unwieldy expression which we require to be strictly positive. That is, we require

$$\text{(A6)} \quad \left(0.9\pi w^{\text{young}} - w^{\text{old}}\right) / (1 + 0.9\pi) - 0.9\,(1 - \pi)\,q^M M \,/\, \left(\ell \left(q^M M + N w^{\text{old}}\right)\right) > 0.$$

This cannot be simplified in a useful way, because q^M depends on the solution to a quadratic equation; however, it is worth noting that given Equation (A1) the first expression is strictly positive and hence our final condition is the intuitive requirement for $s^B > 0$ that π must be sufficiently close to 1.

For the purpose of illustration let $w^{\text{young}} = 100$, $w^{\text{old}} = 20$, $M = N = 100$, and $\ell = 0.001$. Then $s^M(\textit{after tails}) = q^M = 34.96073$ and an interior solution exists with s^M varying from 34.34961 to 0 and s^B varying from 0.64498 to 36.84205 as π increases from 0.94 to 1.

REFERENCES

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia. "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence." Mimeo, 2016.

Barro, R. J. "Money and the Price Level under the Gold Standard." *The Economic Journal*, 89(353), 1979, 13–33.

Bolt, W., and M. van Oordt. "On the Value of Virtual Currencies." Bank of Canada Working Paper No. 2016-42, 2016.

Cass, D., and K. Shell. "Do Sunspots Matter?" *Journal of Political Economy*, 91(2), 1983, 193–227.

Ciaian, P., M. Rajcaniova, and d'A. Kancs. "The Economics of BitCoin Price Formation." *Applied Economics*, 48(19), 2016, 1799–815.

Fernández-Villaverde, J., and D. Sanches. "Can Currency Competition Work?" NBER Working Paper No. 22157, 2016.

Friedman, M. *A Program for Monetary Stability*. New York: Fordam University Press, 1959.

Hellwig, M. "What Do We Know about Currency Competition?" *Zeitschrift für Wirtschafts-und Sozialwissenschaften*, 105, 1985, 565–88 Reprinted in L. H. White (ed.), *Free Banking. Vol. 3: Modern Theory and Policy*, Elgar Reference Collection. International Library of Macroeconomic and Financial History, No. 11. Aldershot, UK: Edward Elgar Publishing, 1993, 324–47.

Kahn, C. M., J. McAndrews, and W. Roberds. "Money Is Privacy." *International Economic Review*, 46(2), 2005, 377–99.

Kandori, M. "Repeated Games Played by Overlapping Generations of Players." *Review of Economic Studies*, 59(1), 1992, 81–92.

Kareken, J., and N. Wallace. "On the Indeterminacy of Equilibrium Exchange Rates." *Quarterly Journal of Economics*, 96(2), 1981, 207–22.

Klein, B. "The Competitive Supply of Money." *Journal of Money, Credit and Banking*, 6(4), 1974, 423–53.

Lagos, R., and R. Wright. "A Unified Framework for Monetary Theory and Policy Analysis." *Journal of Political Economy*, 113(3), 2005, 463–84.

Rogoff, K. *The Curse of Cash*. Princeton, NJ, and Oxford: Princeton University Press, 2016.

Samuelson, P. A. "An Exact Consumption-Loan Model of Interest with or without the Social Contrivance of Money." *Journal of Political Economy*, 66(6), 1958, 467–82.

Wallace, N. "Why Markets in Foreign Exchange Are Different from Other Markets." *Quarterly Review*, 3(4), 1979, 1–7.