Bitcoin 1, Bitcoin 2, ... : An experiment in privately issued outside monies*

Rodney Garratt
University of California Santa Barbara, R3
garratt@ucsb.edu

and

Neil Wallace
Penn State University
nxw9@psu.edu

October 2016

Abstract

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 sovereign currency. Some aspects of the indeterminacy we describe would no longer hold if Bitcoin were an interesting-bearing object.

JEL Codes: D50, E42
Keywords: Virtual Currency, Bitcoin, Indeterminancy, Exchange Rates

In a 1981 paper [11], John Kareken and Neil Wallace 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 mislabelled Bitcoin 1, Bitcoin 2,.... in order to indicate that there could be many of them – do seem to

*We are grateful to Charles Kahn for helpful comments.

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.

1 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 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 3-D 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,

[1] See, for example, the discussions in Hellwig [8] and Wallace [15].

[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.

[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.

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 done with German marks during the 1922-23 hyperinflation.

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.[4] We do so against the background of a very simple model introduced to most economists by Samuelson in a 1958 paper [14]. 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.[5]

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 sovereign 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

[4]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 sovereign currencies. These included its price volatility and the deflation implied by its fixed supply. We add price indeterminacy to the list.

[5]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.

other aspects of competing outside monies, such as the payment of interest.

1.1 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. [1], the consumer seeks to make remittance 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 [5], 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 [2]. 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.

A recent paper by Bolt and van Oordt [3] combines 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 [6] evaluate the role of competing (possibly virtual) private currencies by adding currency-providing entrepreneurs to the Lagos and Wright [13] 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 [12]. 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.

2 One good, one money (Bitcoin)

Time is discrete and extends into the indefinite future with dates labelled t=1,2,.... 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 labelled 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 $u(c^{young}, c^{old})$, 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 $\ln c^{young} + .9 \ln c^{old}$ and $(c^{young})^{1/2} + .8(c^{old})^{1/2}$.) Under uncertainty, people maximize expected utility.

There is a fixed stock of money, denoted B. As opposed to the good, money is durable in the sense that it can be stored costlessly from 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.[6]

2.1 Private-ownership, price-taking equilibrium

Everything is owned by someone, including the fixed stock of money, B. In particular, each member of generation t for $t \geq 1$ owns the same income stream, denoted (w^{young}, w^{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 $N(w^{young} + w^{old}) = W$. Each member of generation 0, the initial old at $t = 1$, owns w^{old} amount of the date-1 good and M/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^B_t. 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*.

[6] See Kandori [10] for a discussion of the role of money in OLG models.

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.

2.2 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 positive until some known date and then zero thereafter? (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?

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:

$$c_t^{young} = w^{young} - p_t^B b_t \equiv w^{young} - s_t^B \tag{1}$$

$$c_t^{old} = w^{old} + p_{t+1} b_t \equiv w^{old} + \frac{p_{t+1}^B}{p_t^B} s_t^B \tag{2}$$

In the second equation in (1), s_t^B, a mnemonic for saving in Bitcoin, is a convenient shorthand for $p_t^B b_t$. The second equation in (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 (1) and (2) into the utility function so that we end up expressing utility in terms of s_t^B; namely, as

$$u[w^{young} - s_t^B, w^{old} + \frac{p_{t+1}^B}{p_t^B} s_t^B] \equiv f(s_t^B; \frac{p_{t+1}^B}{p_t^B}). \tag{3}$$

We can answer question (i) by setting $(p_{t+1}^B / p_t^B) = 1$ 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 positive and constant magnitude of p_t^B, denoted p^B, by solving $s^{B*} = p^B(M/N)$.

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 $(p^B_{t+1}/p^B_t) = 1$. In part (a), the utility function and the income stream are such that there is a positive s^{B*}, while in part (b) a positive s^{B*}does not exist.

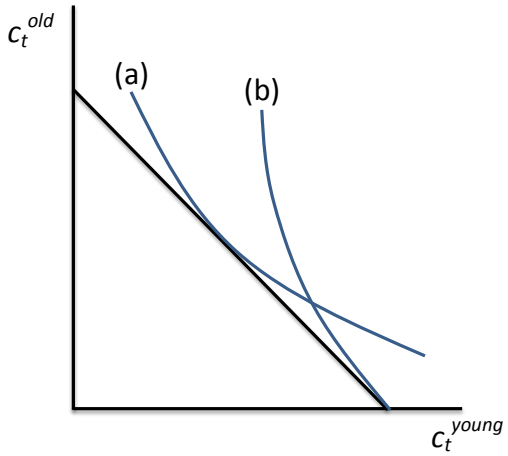

Figure 1: Alternative preference specifications.

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 yes – that we have the situation depicted in part (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 $p^B_{t+1} = 0$. Then, each young person chooses $b = 0$ at time t at any $p^B_t > 0$. (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 $p^B_t = 0$ for all t.

Now we can quickly answer question (iii): Is there an equilibrium in which $p^B_t > 0$ for all $t < T$ and $p^B_t = 0$ for all $t \geq T$ for some known 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 $T-1$. 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,

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

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

Now, assume heads have appeared at dates $1, 2, ..., t$. A young person at t maximizes

$$\pi u[c_t^{young}, c_t^{old}(head)] + (1 - \pi)u[c_t^{young}, c_t^{old}(tail)], \tag{5}$$

where

$$c_t^{young} = w^{young} - s_t^B, \tag{6}$$

$$c_t^{old}(head) = w^{old} + \frac{p_{t+1}^B}{p_t^B} s_t^B \text{ and } c_t^{old}(tail) = w^{old} \tag{7}$$

Here, a young person at t faces uncertainty about the outcome of the lottery at the next date. The outcome could be head or it could be tail and we have labelled 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 $c_t^{old}(head)$, and one for $c_t^{old}(tail)$. We can, however, easily use calculus. Let us substitute from (6) and (7) into (5) and call the result $g(s_t^B; p_{t+1}^B/p_t^B, \pi)$. 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 $\pi = .99$, that we are living at date 68, that heads have been experienced at all earlier dates, but that a tail 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 *head-tail* 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 [3]. 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. However, there is another interpretation of the same mathematical model in which 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. Or, we could imagine that at every date t there is an exogenous probability $1-\pi$ that there is a disruption of the Bitcoin system (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 (other than a zero price).

3 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 sovereign issued money, M that coexists alongside the fixed stock of Bitcoin, B. Both monies are durable, however we will consider the case where the fiat money holding m_t of a young generation-t individual has a storage cost $v(m_t)$, where $v(0)=0$ and $v' \geq 0$. Bitcoin, in contrast, can be costlessly stored.[7] Let p_t^B and p_t^M denote the period t prices of Bitcoin and sovereign 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 section 2, let b_t and m_t denote a young generation-t's purchases of Bitcoin and sovereign money, respectively, and let s_t^B and s_t^M denote the corresponding savings in terms of Bitcoin and sovereign money, where $s_t^B = p_t^B b_t$ and $s_t^M = p_t^M m_t$. 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

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

where

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

[7] 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 [9].

$$c_t^{old} = w^{old} + \frac{p_{t+1}^M}{p_t^M} s_t^M + \frac{p_{t+1}^B}{p_t^B} s_t^B \tag{10}$$

and

$$m_t = \frac{s_t^M}{p_t^M} \tag{11}$$

We maintain our standard assumptions on u.

3.1 Zero Storage Costs: $v(m_t) \equiv 0$

In this case the two monies are perfect substitutes. There exists a constant price equilibrium (type (i) in section 2) in which saving is done through all of one money or the other or both.

To see this, set $\frac{p_{t+1}^M}{p_t^M} = \frac{p_{t+1}^B}{p_t^B} = 1$. Then all that matters in the utility maximization problem is the choice of total savings $s_t = s_t^B + s_t^M$. A unique, positive constant solution s^* exists under the conditions provided in section 2. Given the stocks of money we simply require price levels to satisfy

$$s^* = p^B \frac{B}{N} + p^M \frac{M}{N}. \tag{12}$$

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.[8] We could think of the fraction α as the Libertarians. Then we would require

$$s^* = p^B \frac{B}{\alpha N} = p^M \frac{M}{(1-\alpha)N}, \tag{13}$$

implying

$$p^B = \frac{\alpha N s}{B}, \text{ and } p^M = \frac{(1-\alpha)Ns}{M}. \tag{14}$$

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 $u(c_t^{young}, c_t^{old}) = ln(c_t^{young}) + .9ln(c_t^{old})$ and set $\frac{p_{t+1}^M}{p_t^M} = \frac{p_{t+1}^B}{p_t^B} = 1$. Given constant prices we look for a solution with constant money savings s^M and s^B. Substituting (9) and (10) into (8) gives us the unconstrained utility maximization problem of the young consumer:

$$\max_{s^B, s^M} \; ln(w^{young} - s^B - s^M) + .9ln(w^{old} + s^M + s^B). \tag{15}$$

[8] 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.

The first-order necessary condition for an optimum solution is

$$-\frac{1}{w^{young}-s}+.9\frac{1}{w^{old}+s}=0 \tag{16}$$

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

$$s^*=\frac{.9w^{young}-w^{old}}{1.9} \tag{17}$$

Hence a constant price-taking equilibrium exists so long as $.9w^{young}>w^{old}$. Moreover, if we pin things down by assuming α of each generation only wishes to hold M, then equilibrium money prices are

$$p^M=\frac{\alpha N(.9w^{young}-w^{old})}{1.9M} \text{ and } p^B=\frac{(1-\alpha)N(.9w^{young}-w^{old})}{1.9B}. \tag{18}$$

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 (14) are unlikely to be stable.

3.2 Linear Storage Costs: $v(m_t)=\ell m_t$

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 "head-tails" random variable. Note that we are not explicitly modelling a probabilistic collapse of Bitcoin (as in Athey et al. [1]), 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 sovereign money and make people willing to hold the sovereign currency. In other words, while I may not like paying a storage cost I still hold fiat money if I 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

$$\max_{s_t^M,s_t^B}\pi u(c_t^{young},c_t^{old}(heads))+(1-\pi)u(c_t^{young},c_t^{old}(tails))-\ell m_t$$

where

$$c_t^{young} = w^{young} - s_t^M - s_t^B, \tag{19}$$

$$c_t^{old}(heads) = w^{old} + \frac{p_{t+1}^M(heads)}{p_t^M(heads)} s_t^M + \frac{p_{t+1}^B(heads)}{p_t^B(heads)} s_t^B, \tag{20}$$

$$c_t^{old}(tails) = w^{old} + \frac{p_{t+1}^M(tails)}{p_t^M(heads)} s_t^M, \tag{21}$$

$$c_t^{old,M}(heads) = \frac{p_{t+1}^M(heads)}{p_t^M(heads)} s_t^M, \tag{22}$$

$$c_t^{old,M}(tails) = \frac{p_{t+1}^M(tails)}{p_t^M(heads)} s_t^M. \tag{23}$$

and

$$m_t = \frac{s_t^M}{p_t^M} \tag{24}$$

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:

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

where

$$c_t^{young} = w^{young} - s_t^M, \tag{25}$$

$$c_t^{old} = w^{old} + \frac{p_{t+1}^M}{p_t^M} s_t^M \tag{26}$$

and

$$m_t = \frac{s_t^M}{p_t^M} \tag{27}$$

There is a solution to the proposed privacy-matters model in which sovereign money and Bitcoin have constant positive prices each date up until the occurrence of "tails" and sovereign 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 sovereign money, which we denote by $s^M(after\ tails)$. In this equilibrium the privacy cost of using sovereign currency is counterbalanced by the potential for Bitcoin to become worthless.

Example 2. Once again we let $u(c_t^{young}, c_t^{old}) = ln(c_t^{young}) + .9ln(c_t^{old})$, 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 sovereign 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:

$$\begin{aligned}&\max_{s^M,s^B} \pi[ln(w^{young}-s^M-s^B)+.9ln(w^{old}+s^M+s^B)]\\&+(1-\pi)[ln(w^{young}-s^M-s^B)+.9ln(w^{old}+\tfrac{q^M}{p^M}s^M)]-\ell\tfrac{s^M}{p^M}\end{aligned}$$

which simplifies to

$$\begin{aligned}&\max_{s^M,s^B} ln(w^{young}-s^M-s^B)\\&+\pi[.9ln(w^{old}+s^M+s^B)]+(1-\pi)[.9ln(w^{old}+\tfrac{q^M}{p^M}s^M)]-\ell\tfrac{s^M}{p^M}.\end{aligned}$$

The first-order necessary conditions for an interior solution are

$$-\frac{1}{w^{young}-s^M-s^B}+\frac{.9\pi}{w^{old}+s^M+s^B}+\frac{.9(1-\pi)}{w^{old}+\frac{q^M}{p^M}s^M}\frac{q^M}{p^M}-\frac{\ell}{p^M}=0 \quad (28)$$

and

$$-\frac{1}{w^{young}-s^M-s^B}+\pi\frac{.9}{w^{old}+s^M+s^B}=0 \quad (29)$$

Rewrite (29) as

$$s^B+s^M=\frac{.9\pi w^{young}-w^{old}}{1+.9\pi} \quad (30)$$

and substitute into (28). Solve to get

$$s^M=\frac{.9(1-\pi)p^M}{\ell}-\frac{p^M}{q^M}w^{old} \quad (31)$$

Next consider the utility maximization problem starting in a "tails" state. This is the same problem that leads to equilibrium (i) from Section 2.2 with a slight modification due to the privacy issue.

The unconstrained utility maximization problem of the young consumer is:

$$\max_{s^M} \; ln(w^{young}-s^M)+.9ln(w^{old}+s^M)-\ell\frac{s^M}{p^M}. \quad (32)$$

The first-order necessary condition for an interior solution is

$$-\frac{1}{w^{young}-s^M}+\frac{.9}{w^{old}+s^M}-\frac{\ell}{p^M}=0. \quad (33)$$

So total savings for each young individual in the tails state is given by the solution to the quadratic equation[9]

$$-\frac{\ell}{p^M}(s^M)^2+(1.9+\frac{\ell(w^{young}-w^{old})}{p^M})s^M+\frac{\ell w^{young}w^{old}}{p^M}+w^{old}-.9w^{young}=0. \tag{34}$$

Let $s^M(after\ tails)$ denote the solution to (34). Then

$$q^M=\frac{s^M(after\ tails)N}{M}, \tag{35}$$

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

Note that we also have the equations

$$p^M=s^M\frac{N}{M}\text{ and }p^B=s^B\frac{N}{B}, \tag{36}$$

where B is the fixed stock of Bitcoin. Equations (30), (31), (34), (35) and (36) represent the six equations and six unknowns that (for suitable parameter choices that permit interior solutions) describe the equilibrium.

As π approaches 1, s^M approaches 0, but $s^M(after\ tails)$ is not affected. Hence, for sufficiently large π we are assured that $s^M(after\ tails)>s^M$, 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 sovereign money before and after the tails event, respectively. Thus, following a collapse of Bitcoin, there is a discrete drop in the money price of goods.[10]

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 a money in the current period equates to excess supply and supports a price of zero.

4 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 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

[9] A positive real solution exists since the discriminant is positive.

[10] Of course, in reality, this drop would be small since holdings of Bitcoin are negligible relative to sovereign currency holdings in the United States.

latter, because the former has no significance: it is like paying dividends on a stock in the form of additional stock.

We think it best to think about paying interest in the form of other valuable objects as a form of financial intermediation of the following sort. One can imagine someone setting up an intermediary that sells a Bitcoin-type object and uses the proceeds to hold interest bearing securities—the interest on which is used 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. 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 an interesting-bearing object. If d denotes the interest payment (or dividend) and p the constant price, then the yield 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 (i) equilibrium in section 2.2. or the similar zero-price equilibrium in section 3. 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 managing the portfolio and 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.

5 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 [12] emphasizes that the coexistence of competing currencies requires trade at flexible exchange rates. Klein [12, 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 US 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.[11] 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 sovereign 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 sovereign currency than a competing, private outside money.

References

[1] Athey, S., I. Parashkevov, V. Sarukkai and J. Xia (2016): Bitcoin pricing, adoption, and usage: Theory and evidence, mimeo.

[2] Barro, R.J. (1979): Money and the price level under the gold standard, *The Economic Journal* 89, 13-33.

[3] Bolt, W. and M. van Oordt (2015): On the value of virtual currencies, Bank of Canada working paper.

[4] Cass, D. and K. Shell (1983): Do Sunspots Matter? *Journal of Political Economy* 91(2), 193-227.

[5] Ciaian, P., M Rajcaniova and d'A. Kancs. (2016): The economics of BitCoin price formation, *Applied Economics* 48(19) 1799-1815.

[6] Fernández-Villaverde, J., and D. Sanches (2016): Can Currency Competition Work? NBER working paper.

[7] Friedman, M. (1959): A Program for Monetary Stability. New York: Fordam University Press.

[8] Hellwig, M. (1985): What do we know about Currency competition?, Zeitschrift für Wirtschafts-und Sozialwissenschaften 105, 565-588. Reprinted in L. H. White (ed.) Free banking. Volume 3: Modern theory and policy, Elgar Reference collection. International Library of Macroeconomic and Financial History, no. 11. Aldershot, U.K.; 1993 Elgar 1993, 324-47.

[11] The idea is the same as Friedman's [7] contention that indistinguishable competing currencies lead to an infinite price level, since indistinguishability implies a fixed-exchange rate.

[9] Kahn, C, J. McAndrews and W. Roberds (2005) Money is Privacy, *International Economic Review*, 46(2), 377-399.

[10] Kandori, M., Repeated games played by overlapping generations of players, *Review of Economic Studies*, Wiley Blackwell, vol. 59 (1992) 81-92.

[11] Kareken, J., and N. Wallace (1981): On the indeterminacy of equilibrium exchange rates, *The Quarterly Journal of Economics*, 96(2), 207-222.

[12] Klein, B. (1974) The Competitive Supply of Money, *Journal of Money, Credit and Banking*, 6(4), 423-453.

[13] Lagos, R., and R. Wright (2005): A unified framework for monetary theory and policy analysis, *Journal of Political Economy*, 113(3), 463-484.

[14] Samuelson, P. (1958): An exact consumption-loan model of interest with or without the social contrivance of money. *Journal of Political Economy* 66, 467-82.

[15] Wallace, N. (1979): Why markets in foreign exchange are different from other markets, *Quarterly Review*, Federal Reserve Bank of Minneapolis, 3(4).