WORKING PAPER · NO. 2018-21

Some simple Bitcoin Economics

Linda Schilling and Harald Uhlig

MAY 2019

Becker Friedman Institute
FOR ECONOMICS AT UCHICAGO

5757 S. University Ave.
Chicago, IL 60637
Main: 773.702.5599
bfi.uchicago.edu

Some simple Bitcoin Economics

Linda Schilling* and Harald Uhlig†

This revision: May 10, 2019

Abstract

In a novel model of an endowment economy, we analyze coexistence and competition between traditional fiat money (Dollar) and another intrinsically worthless medium of exchange, not controlled by a central bank, such as Bitcoin. Agents can trade consumption goods in either currency or hold on to currency for speculative purposes. A central bank ensures a Dollar inflation target, while Bitcoin mining is decentralized via proof-of-work. We analyze Bitcoin price evolution and interaction between the Bitcoin price and monetary policy which targets the Dollar. We obtain a fundamental pricing equation, which in its simplest form implies that Bitcoin prices form a martingale. We derive conditions, under which Bitcoin speculation cannot happen, and the fundamental pricing equation must hold. We show that the block rewards are not a tax on Bitcoin holders: they are financed by Dollar taxes imposed by the Dollar central bank. We discuss monetary policy implications and characterize the range of equilibria.

Keywords: Cryptocurrency, Bitcoin, exchange rates, currency competition
JEL codes: D50, E42, E40, E50

*Address: Linda Schilling, École Polytechnique CREST, 5 Avenue Le Chatelier, 91120, Palaiseau, France. email: linda.schilling@polytechnique.edu. This work was conducted in the framework of the ECODEC laboratory of excellence, bearing the reference ANR-11-LABX-0047.

†Address: Harald Uhlig, Kenneth C. Griffin Department of Economics, University of Chicago, 1126 East 59th Street, Chicago, IL 60637, U.S.A, email: huhlig@uchicago.edu. I have an ongoing consulting relationship with a Federal Reserve Bank, the Bundesbank and the ECB. We thank our discussants Aleksander Berentsen, Alex Cukierman, Pablo Kurlat, Aleh Tsivinski and Randy Wright. We thank Pierpaolo Benigno, Bruno Biais, Gur Huberman, Todd Keister, Ricardo Reis and many participants in conferences and seminars for many insightful comments.

1 Introduction

In December 2018, the total market capitalization of cryptocurrencies reached nearly 400 Billion U.S. Dollars, equivalent to 11% of U.S. base money or M1.[1] One fundamental use case of currency is that it serves as a store of value. The apparent price volatility of cryptocurrencies, however, suggests a lack of this fundamental feature of currencies and has exposed cryptocurrencies to criticism.

Traditional quantity theory of money suggests that central banks can control the price level (inflation) of their fiat currencies through variation in the total currency supply. Cryptocurrencies, however, are not controlled by central banks. Their prices fluctuate freely according to supply and demand while the total cryptocurrency supply may only increase over time. What determines the price of cryptocurrencies, how can their fluctuations arise and what are the consequences for the monetary policy of central bank controlled currencies, given the competition to cryptocurrencies? This paper sheds light on these questions.

For our analysis, we construct a novel yet simple model, where a cryptocurrency competes with traditional fiat money for usage. We assume that there are two types of infinitely-lived agents, who alternate in the periods, in which they produce and in which they wish to consume a perishable good. This lack of the double-coincidence of wants provides a role for a medium of exchange. We assume that there are two types of intrinsically worthlessmonies: Bitcoins and Dollars. A central bank targets a stochastic Dollar inflation via appropriate monetary injections, while Bitcoin production is decentralized via proof-of-work, and is determined by the individual incentives of agents to mine them. In particular, the central bank controls the inflation of a traditional fiat money while the value of the cryptocurrency is uncontrolled and its supply can only increase over time. Both monies can be used for transactions. In essence, we imagine a future world, where a cryptocurrency such as Bitcoin has become widely accepted as a means of payments, and where technical issues, such as safety of the payments system or concerns about attacks on the system, have been resolved. We view such a future world as entirely within the plausible realms of possibilities, thus calling upon academics to think through the key issues ahead of time. We establish properties of the Bitcoin price expressed in Dollars, construct equilibria

[1]Source: coincodex.com. Base money or M1 were both approximately at 3600 Billion U.S. Dollars as of July 2018

and examine the consequences for monetary policy and welfare. Due to currency competition, the increase in the stock of Bitcoin or "block rewards" are not a tax on Bitcoin holders, they are financed by Dollar taxes imposed by the Dollar central bank.

While we denote the cryptocurrency as Bitcoin, our analysis applies more broadly. Instead of Bitcoin one may imagine any other cryptocurrency or intrinsically worthless object, which is storable, pays no dividend, whose price is not stabilized by some institution and which may be used as a medium of exchange. Therefore, our analysis applies just as much to certain cryptocurrencies such as Litecoin as it applies to objects such as pebbles, seashells, notwithstanding the caveats raised by Goldberg (2005). The analysis does not apply to gold, sugar, utility tokens such as ether and binance coin, equity tokens or stablecoins.

Our key results are propositions 1, 2 and theorem 1 in section 3. Proposition 1 provides what we call a fundamental pricing equation[2], which has to hold in the fundamental case, where both currencies are simultaneously in use. In its most simple form, this equation says that the Bitcoin price expressed in Dollar follows a martingale, i.e., that the expected future Bitcoin price equals its current price. Proposition 2, on the other hand, shows that in expectation the Bitcoin price has to rise if not all Bitcoins are spent on transactions. Under this speculative condition, agents hold back Bitcoins now in the hope to spend them later at an appreciated value, expecting Bitcoins to earn a real interest. Under the assumption 3, theorem 1 shows that this speculative condition cannot hold and that therefore the fundamental pricing equation has to apply. The paper, therefore, deepens the discussion on how, when and why expected appreciation of Bitcoins and speculation in cryptocurrencies can arise.

Section 4 provides a further characterization of the equilibrium. We rewrite the fundamental pricing equation to decompose today's Bitcoin price into the expected price of tomorrow plus a correction term for risk-aversion which captures the correlation between the future Bitcoin price and a pricing kernel. This formula shows, why constructing equilibria is not straightforward: since fiat currencies have zero dividends, the involved covariances cannot be constructed from more primitive as-

[2]In asset pricing, one often distinguishes between a fundamental component and a bubble component, where the fundamental component arises from discounting future dividends, and the bubble component is paid for the zero-dividend portion. The two monies here are intrinsically worthless: thus, our paper, including the fundamental pricing equation, is entirely about that bubble component. We assume that this does not create a source of confusion.

sumptions about covariances between the pricing kernel and dividends. Proposition 6 therefore reduces the challenge of equilibrium construction to the task of constructing a pricing kernel and a price path for the two currencies, satisfying some suitable conditions. We provide the construction of such sequences in the proof, thereby demonstrating existence. We subsequently provide some explicit examples, demonstrating the possibilities for Bitcoin prices to be supermartingales, submartingales as well as alternating periods of expected decreases and increases in value. Under some conditions, and if the stock of Bitcoins is bounded, we state that the real value of the entire stock of Bitcoins shrinks to zero when inflation is strictly above unity. Furthermore, we show that at any point in time the real Bitcoin price is bounded.

Section 5 finally discusses the implications for monetary policy. Our starting point is the market clearing equation arising per theorem 1, that all monies are spent every period and sum to the total nominal value of consumption. As a consequence, the market clearing condition imposes a direct equilibrium interaction between the Bitcoin price and the Dollar supply set by the central bank policy. It then follows that the increase in the quantity of Bitcoin or block rewards is not a tax on Bitcoin holders. The rewards are financed by Dollar taxes imposed by the Dollar central bank, see theorem 2. Armed with these insights, we then examine two scenarios. In the conventional scenario, the Bitcoin price evolves exogenously, thereby driving the Dollar injections needed by the Central Bank to achieve its inflation target. In the unconventional scenario, we suppose that the inflation target is achieved for a range of monetary injections, which then, however, influence the price of Bitcoins.

The first part of the paper focuses on the agent's decision to trade Bitcoin, and we treat the additional Bitcoins arriving each period in the form of block rewards as a lump sum payment to all agents. In section 6, we extend the analysis by assuming that it takes effort to "mine" these additional coins. We show an irrelevance theorem. Any equilibrium of the first part of the paper is also an equilibrium when it takes effort to mine coins: the only difference is the provision of effort. Intuitively, since the total Bitcoin stock increases deterministically and independent of the total hash rate of the network, then for every equilibrium in the effortless Bitcoin production setting, there exists an effort level in the Bitcoin production setting which supports the same equilibrium outcome. We further discuss the taxation of Bitcoin production and discuss welfare implications. In section 7 we discuss random, free entry of cryptocurrencies and its implications for our results. Appendix A provides some background regarding Bitcoin and further discussion of the literature. Appendix B contains proofs. In appendix C, we demonstrate existence, characterize equilibria, and construct examples. We generalize our key no-speculation theorem in appendix D, while E discusses additional monetary policy implications.

1.1 Literature

Our analysis is related to a substantial body of the literature. The idea of the "denationalisation of money" goes back to Hayek (1976). Our model can be thought of as a simplified version of the Bewley model (1977), the turnpike model of money as in Townsend (1980) or the new monetarist view of money as a medium of exchange as in Kiyotaki-Wright (1989) or Lagos-Wright (2005). With these models as well as with Samuelson (1958), we share the perspective that money is an intrinsically worthless asset, useful for executing trades between people who do not share a double-coincidence of wants. Our aim here is decidedly not to provide a new micro foundation for the use of money, but to provide a simple starting point for our analysis.

The key perspective for much of the analysis is the celebrated exchange-rate indeterminacy result in Kareken-Wallace (1981) and its stochastic counterpart in Manuelli-Peck (1990). Our fundamental pricing equation in proposition 1 as well as the indeterminacy of the Bitcoin price in the first period, see proposition 6, can perhaps be best thought of as a modern restatement of these classic result. Similar to Manuelli-Peck (1990), we consider a stochastic endowment economy with competing currencies. There are three key differences from Manuelli-Peck (1990). First, in our analysis, agents are infinitely lived. Therefore, the agent's incentive for currency speculation competes with her incentive to use currency for trade. Second, we explicitly allow the money supply for both Bitcoin and the Dollar to change over time, by this deriving novel results: we analyze how the Bitcoin price evolution impacts the monetary policy of the Dollar central bank under currency competition. Further, we show how the central bank can exploit its flexibility in providing currency and the fact that Bitcoin is supplied in a deterministic way with an upper bound: novel to the literature, the central bank can crowd out Bitcoin by printing Dollars. Third, in an extension, we analyze Bitcoin production by this deviating from a standard endowment economy.

A closely related contribution in the literature to our paper is Garratt-Wallace (2017). Like us, they adopt the Kareken-Wallace (1981) perspective to study the behavior of the Bitcoin-to-Dollar exchange rate. However, there are a number of differences. They utilize a two-period OLG model: the speculative price bound does not arise there. They focus on fixed stocks of Bitcoins and Dollar (or "government issued monies"), while we allow for Bitcoin production and monetary policy. Production is random here and constant there. There is a carrying cost for Dollars, which we do not feature here. They focus on particular processes for the Bitcoin price. The analysis and key results are very different from ours.

The literature on bitcoin, cryptocurrencies and blockchain is currently growing quickly. We provide a more in-depth review of the background and discussion of the literature in the appendix section A, listing only a few of the contributions here. Velde (2013), Brito and Castillo (2013) and Berentsen and Schär (2017, 2018) provide excellent primers on Bitcoin and related topics. Related in spirit to our exercise here, Fernández-Villaverde and Sanches (2016) examine the scope of currency competition in an extended Lagos-Wright model and argue that there can be equilibria with price stability as well as a continuum of equilibrium trajectories with the property that the value of private currencies monotonically converges to zero. Relatedly, Zhu and Hendry (2018) study optimal monetary policy in a Lagos and Wright type of model where privately issued e-money competes with central bank issued fiat money. Athey et al. (2016) develop a model of user adoption and use of virtual currency such as Bitcoin in order to analyze how market fundamentals determine the exchange rate of fiat currency to Bitcoin, focussing their attention on an eventual steady state expected exchange rate. By contrast, our model generally does not imply such a steady state. Huberman, Leshno and Moallemi (2017) examine congestion effects in Bitcoin transactions and their resulting impediments to a Bitcoin-based payments system. Prat and Walter (2018) predict the computing power of the Bitcoin network using the Bitcoin-Dollar exchange rate. Chiu and Koeppl (2017) study the optimal design of a blockchain based cryptocurrency system in a general equilibrium monetary model. They and Budish (2018) argue that the blockchain protocol underlying Bitcoin is vulnerable to attack. Likewise, Abadi and Brunnermeier (2017) examine potential blockchain instability. Sockin and Xiong (2018) price cryptocurrencies which yield membership of a platform on which households can trade goods. This generates complementarity in households' participation in the platform. In our paper, in contrast, fiat money and cryptocurrency are perfect substitutes and goods can be paid for with either currency without incurring frictions. Griffin and Shams (2018) argue that cryptocurrencies are manipulated. By contrast, we imagine a future world here, where such impediments, instabilities, and manipulation issues are resolved or are of sufficiently minor concern for the payment systems both for Dollars and the cryptocurrency. Makarov and Schoar (2018) find large and recurrent arbitrage opportunities in cryptocurrency markets across the U.S., Japan, and Korea. Liu and Tsyvinksi (2018) examine the risks and returns of cryptocurrencies and find them uncorrelated to typical asset pricing factors. We view our paper as providing a theoretical framework for understanding their empirical finding.

2 The model

Time is discrete, $t = 0, 1, \ldots$. In each period, a publicly observable, aggregate random shock $\theta_t \in \Theta \subset \mathbf{R}$ is realized. All random variables in period t are assumed to be functions of the history $\theta^t = (\theta_0, \ldots, \theta_t)$ of these shocks, i.e. measurable with respect to the filtration generated by the stochastic sequence $(\theta_t)_{t \in \{0,1,\ldots\}}$ and thus known to all participants at the beginning of the period. Note that the length of the vector θ^t encodes the period t: therefore, functions of θ^t are allowed to be deterministic functions of t.

There is a consumption good which is not storable across periods. There is a continuum of mass 2 of two types of agents. We shall call the first type of agents "red", and the other type "green". Both types of agents j enjoy utility from consumption $c_{t,j} \geq 0$ at time t per $u(c_{t,j})$, as well as loathe providing effort $e_{t,j} \geq 0$, where effort may be necessary to produce Bitcoins, see in particular section 6. The consumption-utility function $u(\cdot)$ is strictly increasing and concave. The utility-loss-from-effort function $h(\cdot)$ is strictly increasing and weakly convex. We assume that both functions are twice differentiable.

Red and green agents alternate in consuming and producing the consumption good, see figure 1: We assume that red agents only enjoy consuming the good in odd periods, while green agents only enjoy consuming in even periods. Red agents $j \in [0, 1)$ inelastically produce (or: are endowed with) y_t units of the consumption good in even periods t, while green agents $j \in [1, 2]$ do so in odd periods. This creates the absence of the double-coincidence of wants, and thereby reasons to trade.

We assume that $y_t = y(\theta^t)$ is stochastic with support $y_t \in [\underline{y}, \bar{y}]$, where $0 < \underline{y} \leq \bar{y}$. As a special case, we consider the case, where y_t is constant, $\underline{y} = \bar{y}$ and $y_t \equiv \bar{y}$ for all t. We impose a discount rate of $0 < \beta < 1$ to yield life-time utility

$$U = E\left[\sum_{t=0}^{\infty} \beta^t \left(\xi_{t,j} u(c_{t,j}) - h(e_{t,j})\right)\right]. \tag{1}$$

Formally, we impose alternation of utility from consumption per $\xi_{t,j} = 1_{t \text{ is odd}}$ for $j \in [0, 1)$ and $\xi_{t,j} = 1_{t \text{ is even}}$ for $j \in [1, 2]$.

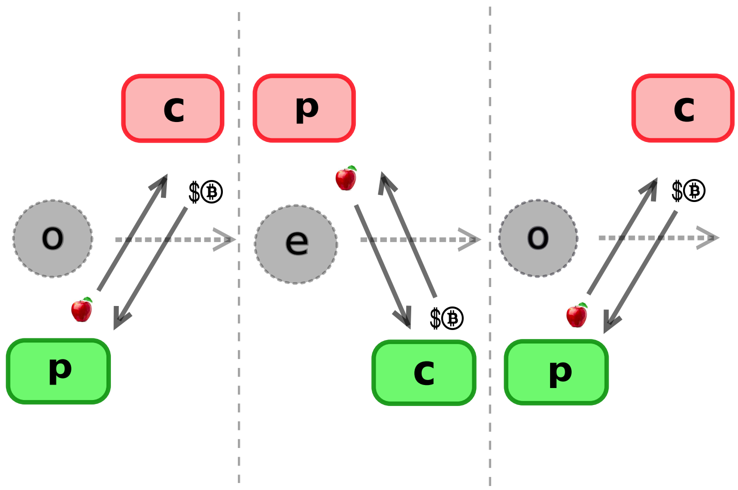

Figure 1: Alternation of production and consumption. In odd periods , green agents produce and red agents consume. In even periods, red agents produce and green agents consume. Alternation and the fact that the consumption good is perishable gives rise to the necessity to trade using fiat money.

Trade is carried out using money. More precisely, we assume that there are two forms of money. The first shall be called Bitcoins and its aggregate stock at time t shall be denoted with B_t. The second shall be called Dollar and its aggregate stock at time t shall be denoted with D_t. These labels are surely suggestive, but hopefully not overly so, given our further assumptions. In particular, we shall assume that there is a central bank, which governs the aggregate stock of Dollars D_t, while Bitcoins can be produced privately.

The sequence of events in each period is as follows. First, θ_t is drawn. Next, given the information on θ^t, the central bank issues or withdraws Dollars, per "helicopter drops" or lump-sum transfers and taxes on the agents ready to consume in that particular period. The central bank can produce Dollars at zero cost. Consider a green agent entering an even period t, holding some Dollar amount $\tilde{D}_{t,j}$ from the previous period. The agent will receive a Dollar transfer $\tau_t = \tau(\theta^t)$ from the central bank, resulting in

$$D_{t,j} = \tilde{D}_{t,j} + \tau_t. \tag{2}$$

We allow τ_t to be negative, while we shall insist, that $D_{t,j} \geq 0$: we, therefore, have to make sure in the analysis below, that the central bank chooses wisely enough so as not to withdraw more money than any particular green agent has at hand in even periods. Red agents do not receive (or pay) τ_t in even period. Conversely, the receive transfers (or pay taxes) in odd periods, while green agents do not. The aggregate stock of Dollars changes to

$$D_t = D_{t-1} + \tau_t. \tag{3}$$

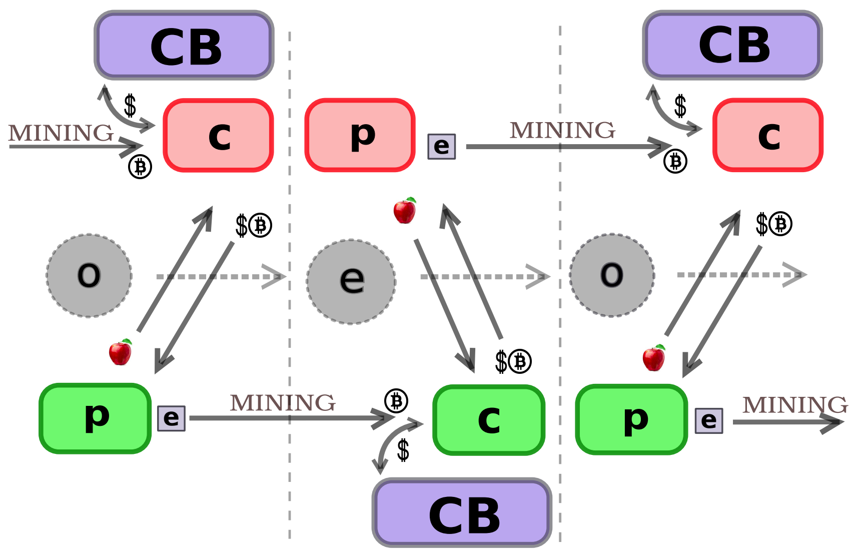

Figure 2: Transfers: In each period, a central bank injects to or withdraws Dollars from agents, before they consume, to target a certain Dollar inflation level. By this, the Dollar supply may increase or decrease. Across periods, agents can put effort to mine Bitcoins. By this, the Bitcoin supply can only increase.

The green agent then enters the consumption good market holding $B_{t,j}$ Bitcoins from the previous period and $D_{t,j}$ Dollars, after the helicopter drop. The green agent will seek to purchase the consumption good from red agents. As is conventional, let $P_t = P(\theta^t)$ be the price of the consumption good in terms of Dollars and let

$$\pi_t = \frac{P_t}{P_{t-1}}$$

denote the resulting inflation. We could likewise express the price of goods in terms of Bitcoins, but it will turn out to be more intuitive (at the price of some initial asymmetry) as well as in line with the practice of Bitcoin pricing to let $Q_t = Q(\theta^t)$ denote the price of Bitcoins in terms of Dollars. The price of one unit of the good in terms of Bitcoins is then P_t/Q_t. Let $b_{t,j}$ be the amount of the consumption good purchased with Bitcoins and $d_{t,j}$ be the amount of the consumption good purchased with Dollars. The green agent cannot spend more of each money than she owns but may choose not to spend all of it. This implies the constraints

$$\begin{aligned} 0 \leq \frac{P_t}{Q_t} b_{t,j} &\leq B_{t,j}, & (4) \\ 0 \leq P_t d_{t,j} &\leq D_{t,j}. & (5) \end{aligned}$$

The green agent then consumes

$$c_{t,j} = b_{t,j} + d_{t,j}, \tag{6}$$

and leaves the even period, carrying

$$\begin{aligned} B_{t+1,j} &= B_{t,j} - \frac{P_t}{Q_t} b_{t,j} \geq 0, & (7) \\ D_{t+1,j} &= D_{t,j} - P_t d_{t,j} \geq 0 & (8) \end{aligned}$$

Bitcoins and Dollars into the next and odd period $t+1$.

At the beginning of that odd period $t+1$, the aggregate shock θ_{t+1} is drawn and added to the history θ^{t+1}. The green agent produces y_{t+1} units of the consumption good.

Green agents produce $A_{t+1,j} \geq 0$ additional Bitcoins per agent, which they can spend in the subsequent period. For the baseline version of the model, we assume that the production of these additional Bitcoins takes the form of an endowment and is the same for all agents of the same type, $A_{t+1,j} = A_{t+1}$, and that no effort is involved, $e_{t,j} \equiv 0$. In section 6, we examine the case, where nonzero effort is required to receive or "mine" Bitcoins, and provide more comparison to the actual practice of mining Bitcoins. In both cases, we assume that the aggregate quantity $A_{t+1} \geq 0$ of additional Bitcoins (or: "Bitcoin block rewards")is a deterministic function of time. Thus, the aggregate stock of Bitcoin B_t is a deterministic and weakly increasing function of time. We will occasionally impose that the Bitcoin quantity is bounded from above, $B_t \leq \bar{B}$ for all t: this is a feature of Bitcoin in practice.

In odd periods, only green agents may produce Bitcoins, while only red agents get to produce Bitcoins in even periods.

The green agent sells the consumption goods to red agents. Given market prices Q_{t+1} and P_{t+1}, he decides on the amount of output $x_{t+1,j} \geq 0$ sold for Bitcoins and $z_{t+1,j} \geq 0$ sold for Dollars, where

$$x_{t+1,j} + z_{t+1,j} = y_{t+1},$$

as the green agent has no other use for the good. After these transactions, the green agent holds

$$\tilde{D}_{t+2,j} = D_{t+1,j} + P_{t+1} z_{t+1,j}$$

Dollars, which then may be augmented per central bank lump-sum transfers at the beginning of the next period $t+2$ as described above. As for the Bitcoins, the green agent carries the total of

$$B_{t+2,j} = A_{t+1,j} + B_{t+1,j} + \frac{P_{t+1}}{Q_{t+1}} x_{t+1,j}$$

to the next period.

The aggregate stock of Bitcoins has increased to

$$B_{t+2} = B_{t+1} + \int_{j=0}^{2} A_{t+1,j} dj,$$

noting that red agents do not produce Bitcoins in even periods.

The role of red agents and their budget constraints is entirely symmetric to green agents, per merely swapping the role of even and odd periods. There is one difference, though, and it concerns the initial endowments with money. Since green agents are first in period $t = 0$ to purchase goods from red agents, we assume that green agents initially have all the Dollars and all the Bitcoins and red agents have none.

While there is a single and central consumption good market in each period, payments can be made with the two different monies. We therefore get the two market clearing conditions

$$\int_{j=0}^{2} b_{t,j} dj = \int_{j=0}^{2} x_{t,j} dj, \quad (9)$$

$$\int_{j=0}^{2} d_{t,j} dj = \int_{j=0}^{2} z_{t,j} dj, \quad (10)$$

where we adopt the convention that $x_{t,j} = z_{t,j} = 0$ for green agents in even periods and red agents in odd periods as well as $b_{t,j} = d_{t,j} = 0$ for red agents in even periods and green agents in odd periods.

The central bank picks transfer payments τ_t, which are itself a function of the publicly observable random shock history θ^t, and thus already known to all agents at the beginning of the period t. In particular, the transfers do not additionally reveal information otherwise only available to the central bank. For the definition of the equilibrium, we do not a priori impose that central bank transfers τ_t, Bitcoin prices Q_t or inflation π_t are exogenous. Our analysis is consistent with a number of views here. For example, one may wish to impose that π_t is exogenous and reflecting a random inflation target, which the central bank, in turn, can implement perfectly using its transfers. Alternatively, one may fix a (possibly stochastic) money growth rule per imposing an exogenous stochastic process for τ_t and solve for the resulting Q_t and π_t. Generally, one may want to think of the central bank as targeting some Dollar inflation and using the transfers as its policy tool, while there is no corresponding institution worrying about the Bitcoin price Q_t. The case of deterministic inflation or a constant Dollar price level $P_t \equiv 1$ arise as special cases. These issues require a more profound discussion and analysis, which we provide in section 5.

So far, we have allowed individual green agents and individual red agents to make different choices. We shall restrict attention to symmetric equilibria, in which all agents of the same type end up making the same choice. Thus, instead of subscript j and with a slight abuse of notation, we shall use subscript g to indicate a choice by a green agent and r to indicate a choice by a red agent. With these caveats and remarks, we arrive at the following definition.

Definition 1. *An* **equilibrium** *is a stochastic sequence*

$$(A_t, A_{t,r}, A_{t,g}, B_t, B_{t,r}, B_{t,g}, D_t, D_{t,r}, D_{t,g}, \tau_t, P_t, Q_t, b_t, c_t, d_t, e_t, \bar{e}_t, x_t, y_t, z_t)_{t \in \{0,1,2,\ldots\}}$$

which is measurable[3] with respect to the filtration generated by $(\theta_t)_{t\in\{0,1,\dots\}}$, such that

1. **Green agents** *optimize: given aggregate money quantities (B_t, D_t, τ_t), production y_t, prices (P_t, Q_t) and initial money holdings $B_{0,g} = B_0$ and $D_{0,g} = D_0$, a green agent $j \in [1, 2]$ chooses nonnegative consumption quantities b_t, c_t, d_t in even periods and x_t, z_t, nonnegative effort e_t and Bitcoin production $A_{t,g}$ in odd periods as well as individual money holdings $B_{t,g}$, $D_{t,g}$, all non-negative, so as to maximize*

$$U_g = E\left[\sum_{t=0}^{\infty} \beta^t \left(\xi_{t,g} u(c_t) - h(e_t)\right)\right] \tag{11}$$

where $\xi_{t,g} = 1$ in even periods, $\xi_{t,g} = 0$ in odd periods, subject to the budget constraints

$$\begin{aligned} 0 \leq \frac{P_t}{Q_t} b_t &\leq B_{t,g}, &(12)\\ 0 \leq P_t d_t &\leq D_{t,g}, &(13)\\ c_t &= b_t + d_t, &(14)\\ B_{t+1,g} &= B_{t,g} - \frac{P_t}{Q_t} b_t, &(15)\\ D_{t+1,g} &= D_{t,g} - P_t d_t, &(16)\end{aligned}$$

in even periods t and

$$\begin{aligned} e_t &= 0 \ and A_{t,g} = A_t, &(17)\\ y_t &= x_t + z_t, &(18)\\ B_{t+1,g} &= A_{t,g} + B_{t,g} + \frac{P_t}{Q_t} x_t, &(19)\\ D_{t+1,g} &= D_{t,g} + P_t z_t + \tau_{t+1}, &(20)\end{aligned}$$

in odd periods t.

2. **Red agents** *optimize: given aggregate money quantities (B_t, D_t, τ_t), production y_t, prices (P_t, Q_t) and initial money holdings $B_{0,r} = 0$ and $D_{0,r} = 0$, a red agent $j \in [0, 1)$ chooses nonnegative consumption quantities b_t, c_t, d_t in odd periods and x_t, z_t, nonnegative effort e_t and Bitcoin production A_t in even periods as*

[3] More precisely, $B_t, B_{t,g}$ and $B_{t,r}$ are "predetermined", i.e. are measurable with respect to the $\sigma-$-algebra generated by θ^{t-1}

well as individual money holdings $B_{t,r}$, $D_{t,r}$, all non-negative, so as to maximize

$$U_r = E\left[\sum_{t=0}^{\infty} \beta^t \left(\xi_{t,r} u(c_t) - h(e_t)\right)\right] \tag{21}$$

where $\xi_{t,r} = 1$ in odd periods, $\xi_{t,r} = 0$ in even periods, subject to the budget constraints

$$\begin{aligned}
D_{t,r} &= D_{t-1,r} + \tau_t, & (22)\\
0 \leq \frac{P_t}{Q_t} b_t &\leq B_{t,r}, & (23)\\
0 \leq P_t d_t &\leq D_{t,r}, & (24)\\
c_t &= b_t + d_t, & (25)\\
B_{t+1,r} &= B_{t,r} - \frac{P_t}{Q_t} b_t, & (26)\\
D_{t+1,r} &= D_{t,r} - P_t d_t, & (27)
\end{aligned}$$

in odd periods t and

$$\begin{aligned}
e_t &= 0 \text{ and[4] } A_{t,r} = A_t, & (28)\\
y_t &= x_t + z_t, & (29)\\
B_{t+1,r} &= A_{t,r} + B_{t,r} + \frac{P_t}{Q_t} x_t, & (30)\\
D_{t+1,r} &= D_{t,r} + P_t z_t + \tau_{t+1}, & (31)
\end{aligned}$$

in even periods t.

3. *The* **central bank** *supplies Dollar transfers τ_t to achieve $\frac{P_t}{P_{t-1}} = \pi_t$, where π_t and P_0 are exogenous*

4. **Markets clear***:*

$$\begin{aligned}
\textit{Bitcoin market:} \quad B_t &= B_{t,r} + B_{t,g}, & (32)\\
\textit{Dollar market:} \quad D_t &= D_{t,r} + D_{t,g}, & (33)\\
\textit{Bitcoin denom. cons. market:} \quad b_t &= x_t, & (34)\\
\textit{Dollar denom. cons. market:} \quad d_t &= z_t, & (35)\\
\textit{Aggregate effort:} \quad e_t &= \bar{e}_t. & (36)
\end{aligned}$$

The equilibrium condition (17) is later replaced by equation (65) in section 6 as soon as agents can put effort to mine Bitcoin.

3 Analysis

For the analysis, proofs not included in the main text can be found in appendix B. The equilibrium definition implies that $c_t = y_t$, that $B_{t+1} = B_t + A_t$ and that $D_t = D_{t-1} + \tau_t$. Bitcoin production is analyzed in appendix 6. We restrict attention to equilibria, where Dollar prices are strictly above zero and below infinity, and where inflation is always larger than unity

Assumption A. 1. $0 < P_t < \infty$ *for all* t *and*

$$\pi_t = \frac{P_t}{P_{t-1}} \geq 1. \tag{37}$$

For example, if inflation is exogenous, this is a restriction on that exogenous process. If inflation is endogenous, restrictions elsewhere are needed to ensure this outcome.

It will be convenient to bound the degree of consumption fluctuations. The following somewhat restrictive assumption will turn out to simplify the analysis of the Dollar holdings.

Assumption A. 2. *For all* t*,*

$$u'(y_t) - \beta^2 E_t[u'(y_{t+2})] > 0. \tag{38}$$

The assumption says that no matter how many units of the consumption good an agent consumes today she will always prefer consuming an additional marginal unit of the consumption good now as opposed to consuming it at the next opportunity two periods later. The assumption captures the agent's degree of impatience.

3.1 Equilibrium Conditions for Simultaneous Currency Trade

The following proposition is a consequence of a central bank policy aimed at price stability, inducing an opportunity cost for holding money. This is in contrast to the literature concerning the implementation of the Friedman rule, where that opportunity cost is absent: we return to the welfare consequences in section 5. Note that assumption (38) holds.

Lemma 1. (All Dollars are spent:) *Agents will always spend all Dollars. Thus,* $D_t = D_{t,g}$ *and* $D_{t,r} = 0$ *in even periods and* $D_t = D_{t,r}$ *and* $D_{t,g} = 0$ *in odd periods.*

Lemma 2. (Dollar Injections:) *In equilibrium, the post-transfer amount of total Dollars is*

$$D_t = P_t \, z_t,$$

and the transfers are

$$\tau_t = P_t \, z_t - P_{t-1} \, z_{t-1}. \tag{39}$$

The following proposition establishes properties of the Bitcoin price Q_t in the "fundamental" case, where Bitcoins are used in transactions.

Proposition 1. (Fundamental pricing equation[5]:)
Suppose that sales happen both in the Bitcoin-denominated consumption market as well as the Dollar-denominated consumption market at time t *as well as at time* $t+1$, *i.e. suppose that* $x_t > 0$, $z_t > 0$, $x_{t+1} > 0$ *and* $z_{t+1} > 0$. *Then*

$$E_t \left[u'(c_{t+1}) \, \frac{P_t}{P_{t+1}} \right] = E_t \left[u'(c_{t+1}) \frac{(Q_{t+1}/P_{t+1})}{(Q_t/P_t)} \right]. \tag{40}$$

In particular, if consumption and production is constant at $t+1$, $c_{t+1} = y_{t+1} \equiv \bar{y} = \underline{y}$, *or agents are risk-neutral, then*

$$Q_t = \mathbb{E}_t \left[\frac{Q_{t+1}}{\pi_{t+1}} \right] \cdot \mathbb{E}_t \left[\frac{1}{\pi_{t+1}} \right]^{-1}. \tag{41}$$

If further Q_{t+1} *and* $\frac{1}{\pi_{t+1}}$ *are uncorrelated conditional on time-t information, then the stochastic Bitcoin price process* $\{Q_t\}_{t \geq 0}$ *is a martingale*

$$Q_t = \mathbb{E}_t \left[Q_{t+1} \right]. \tag{42}$$

If zero Bitcoins are traded, the fundamental pricing equation becomes an inequality, see lemma 3 in the appendix.

[5] The proof for this proposition as well as most other results are in the appendix section B.

The logic for the fundamental pricing equation is as follows. The risk-adjusted real return on Bitcoin has to equal the risk-adjusted real return on the Dollar. Otherwise, agents would hold back either of the currencies.

The result can be understood as an updated version of the celebrated result in Kareken-Wallace (1981). These authors did not consider stochastic fluctuations. Our martingale result then reduces to a constant Bitcoin price, $Q_t = Q_{t+1}$, and thus their "exchange rate indeterminacy result" for time $t = 0$, that any Q_0 is consistent with some equilibrium, provided the Bitcoin price stays constant afterwards. Our result here reveals that this indeterminacy result amounts to a potentially risk-adjusted martingale condition, which the Bitcoin price needs to satisfy over time while keeping Q_0 undetermined.

Our result furthermore corresponds to equation (14') in Manuelli-Peck (1990) who provide a stochastic generalization of the 2-period OLG model in Kareken-Wallace (1981). Aside from various differences in the model, note that Manuelli-Peck (1990) derive their results from considering intertemporal savings decisions, which then, in turn, imply the indifference between currencies. While we agree with the latter, we do not insist on the former. Indeed, it may be empirically problematic to base currency demand on savings decisions without considering interest-bearing assets. By contrast, we obtain the indifference condition directly.

Equation (40) can be understood from a standard asset pricing perspective. The goods seller will sell against the currency which offers a higher risk-preference adjusted return. Due to the currency competition, sales against both Bitcoins and Dollars implies seller indifference. The risk-adjusted returns, therefore, have to be the same.

Finally, our result relates to the literature on uncovered interest parity. In that literature, it is assumed that agents trade safe bonds, denominated in either currency. That literature derives the uncovered interest parity condition, which states that the expected exchange rate change equals the return differences on the two nominal bonds. This result is reminiscent of our equation above. Note, however, that we do not consider bond trading here: rates of returns, therefore, do not feature in our results. Instead, they are driven entirely by cash use considerations.

3.2 Equilibrium Conditions for (no) Speculation

The next proposition establishes properties of the Bitcoin price Q_t, if potential goods buyers prefer to keep some or all of their Bitcoins in possession, rather than using them in a transaction, effectively speculating on lower Bitcoin goods prices or, equivalently, higher Dollar prices for a Bitcoin in the future. This condition establishes an essential difference to Kareken and Wallace (1981). In their model, agents live for two periods and thus splurge all their cash in their final period. Here instead, since agents are infinitely lived, the opportunity of currency speculation arises which allows us to analyze currency competition and asset pricing implications simultaneously.

Proposition 2. (Speculative price bound:)
Suppose that $B_t > 0$, $Q_t > 0$, $z_t > 0$ and that not all Bitcoins are spent in t, $b_t < (Q_t/P_t)B_t$. Then,

$$u'(c_t) \leq \beta^2 E_t \left[u'(c_{t+2}) \frac{(Q_{t+2}/P_{t+2})}{(Q_t/P_t)} \right], \tag{43}$$

where this equation furthermore holds with equality, if $x_t > 0$ and $x_{t+2} > 0$.

A few remarks regarding that last proposition and the equilibrium pricing equation Proposition (1) are in order. To understand the logical reasoning applied here, it is good to remember that we impose market clearing. Consider a (possibly off-equilibrium) case instead, where sellers do not wish to sell for Bitcoin, i.e., $x_t = 0$, because the real Bitcoin price Q_t/P_t is too high, but where buyers do not wish to hold on to all their Bitcoin, and instead offering them in trades. This is a non-market clearing situation: demand for consumption goods exceeds supply in the Bitcoin-denominated market at the stated price. Thus, that price cannot be an equilibrium price. Heuristically, the pressure from buyers seeking to purchase goods with Bitcoins should drive the Bitcoin price down until either sellers are willing to sell or potential buyers are willing to hold. One can, of course, make the converse case too. Suppose that potential goods buyers prefer to hold on to their Bitcoins rather than use them in goods transactions, and thus demand $b_t = 0$ at the current price. Suppose, though, that sellers wish to sell goods at that price. Again, this would be a non-market clearing situation, and the price pressure from the sellers would force the Bitcoin price upwards.

Considering the right-hand side of equations (40) as well as (43): these are expected utilities of the next usage possibility for Bitcoins only if transactions actually happen at that date for that price. However, as equation (43) shows, Bitcoins may be more valuable than indicated by the right-hand side of (40) states, if Bitcoins are then entirely kept for speculative reasons. These considerations can be turned into more general versions of (40) as well as (43), which take into account the stopping time of the first future date with positive transactions on the Bitcoin-denominated goods market. The interplay of the various scenarios and inequalities in the preceding two propositions gives rise to potentially rich dynamics, which we explore and illustrate further in the next section.

If consumption and production are constant at $t, t+1$ and $t+2$, $c_t = c_{t+1} = c_{t+2} \equiv \bar{y} = \underline{y}$, and if Q_{t+1} and $\frac{1}{\pi_{t+1}}$ are uncorrelated conditional on time-t information, absence of goods transactions against Bitcoins $x_t = 0$ at t requires

$$E_t\left[Q_{t+1}\right] \leq Q_t \leq \beta^2 E_t\left[Q_{t+2}\,\frac{1}{\pi_{t+2}\,\pi_{t+1}}\right] \tag{44}$$

per propositions 2 and Lemma 3. We next show that this can never be the case. Indeed, even with non-constant consumption, all Bitcoins are always spent, provided we impose a slightly sharper version of assumption 2.

Assumption A. 3. (Global Impatience:) *For all t,*

$$u'(y_t) - \beta E_t[u'(y_{t+1})] > 0. \tag{45}$$

Global impatience together with the law of iterated expectations imply assumption 2. If assumption 2 holds, then (45) cannot be violated two periods in a row. Since consumption alternates between the green and the red agent group across time, equation (45) compares marginal utilities across agent groups. We discuss this issue further in appendix D.

Theorem 1. (No-Bitcoin-Speculation:) *Suppose that $B_t > 0$ and $Q_t > 0$ for all t. Impose assumption 3. Then in every period, all Bitcoins are spent.*

One way of reading this result is, that under assumption 3, the model endogenously reduces to a two period overlapping generations model.[6]

[6]In two-period OLG models, agents die after two time periods and thus consume their entire endowment and savings at the end of their life. Here, agents do so endogenously. Thus, the time

Proof. [Theorem 1] Since all Dollars are spent in all periods, we have $z_t > 0$ in all periods. Observe that then either inequality (77) holds, in case no Bitcoins are spent at date t, or equation (40) holds, if some Bitcoins are spent. Since equation (40) implies inequality (77), (77) holds for all t. Calculate that

$$\begin{aligned}
\beta^2 \mathbb{E}_t[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}] &= \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}\right]\right] && \text{(law of iterated expectation)}\\
&\le \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{P_{t+1}}{P_{t+2}}\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per equ. (77) at } t+1)\\
&\le \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 1)}\\
&< \beta \mathbb{E}_t\left[u'(c_{t+1})\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 3 in t+1)}\\
&\le \beta \mathbb{E}_t\left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right]\,\frac{Q_t}{P_t} && \text{(per equ. (77) at } t)\\
&\le \beta \mathbb{E}_t\left[u'(c_{t+1})\right]\,\frac{Q_t}{P_t} && \text{(per ass. 1)}\\
&< u'(c_t)\,\frac{Q_t}{P_t} && \text{(per ass. 3 in t).}
\end{aligned}$$

which contradicts the speculative price bound (43) in t. Consequently, $b_t = \frac{Q_t}{P_t} B_t$, i.e. all Bitcoins are spent in t. Since t is arbitrary, all Bitcoins are spent in every period. $\square$

4 Equilibrium: Price Properties and Construction

Since our equilibrium construction draws on a covariance characterization of the Bitcoin price, we first show the characterization and then discuss equilibrium construction.

period at which an agent earns her stochastic endowment can be interpreted as the agents birth, since she carries no wealth from previous time periods.

4.1 Equilibrium Pricing

The No-Bitcoin-Speculation Theorem 1 implies that the fundamental pricing equation holds at each point in time. Next, we discuss Bitcoin pricing implications.

Define the nominal pricing kernel m_t per

$$m_t = \frac{u'(c_t)}{P_t} \tag{46}$$

We can then equivalently rewrite equation (40) as

$$Q_t = \mathbb{E}_t[Q_{t+1}] + \frac{\mathrm{cov}_t(Q_{t+1}, m_{t+1})}{\mathbb{E}_t[m_{t+1}]}. \tag{47}$$

Note that one could equivalently replace the pricing kernel m_{t+1} in this formula with the nominal stochastic discount factor of a red agent or a green agent, given by $M_{t+1} := \beta^2(u'(c_{t+1})/u'(c_{t-1}))/(P_{t+1}/P_{t-1})$. For deterministic inflation $\pi_{t+1} \geq 1$,

$$Q_t = \mathbb{E}_t[Q_{t+1}] + \frac{\mathrm{cov}_t(Q_{t+1}, u'(c_{t+1}))}{\mathbb{E}_t[u'(c_{t+1})]}. \tag{48}$$

With that, we obtain the following corollary to theorem 1 which fundamentally characterizes the Bitcoin price evolution

Corollary 1. (Equilibrium Bitcoin Pricing Formula:)
Suppose that $B_t > 0$ and $Q_t > 0$ for all t. Impose assumption 3. In equilibrium, the Dollar-denominated Bitcoin price satisfies

$$Q_t = E_t[Q_{t+1}] + \kappa_t \cdot corr_t\left(m_{t+1}, Q_{t+1}\right), \tag{49}$$

where

$$\kappa_t = \frac{\sigma_{m_{t+1}|t} \cdot \sigma_{Q_{t+1}|t}}{\mathbb{E}_t[m_{t+1}]} > 0, \tag{50}$$

where $\sigma_{m_{t+1}|t}$ is the standard deviation of the pricing kernel, $\sigma_{Q_{t+1}|t}$ is the standard deviation of the Bitcoin price and $corr_t\left(m_{t+1}, Q_{t+1}\right)$ is the correlation between the Bitcoin price and the pricing kernel, all conditional on time t information.

One immediate implication of corollary 1 is that the Dollar denominated Bitcoin price process is a supermartingale (falls in expectation) if and only if in equilibrium the pricing kernel and the Bitcoin price are positively correlated for all $t+1$ conditional on time t-information. Likewise, under negative correlation, the Bitcoin price process is a submartingale and increases in expectation. In the special case that in equilibrium the pricing kernel is uncorrelated with the Bitcoin price, the Bitcoin price process is a martingale.

If the Bitcoin price is a martingale, today's price is the best forecast of tomorrow's price. There cannot exist long up- or downwards trends in the Bitcoin price since the mean of the price is constant over time. If Bitcoin prices and the pricing kernel are, however, positively correlated, then Bitcoins depreciate over time. Essentially, holding Bitcoins offers insurance against the consumption fluctuations, for which the agents are willing to pay an insurance premium in the form of Bitcoin depreciation. Conversely, for a negative correlation of Bitcoin prices and the pricing kernel, a risk premium in the form of expected Bitcoin appreciation induces the agents to hold them.

One implication of our pricing formula is that the equilibrium evolution of the Bitcoin price can be completely detached from the central bank's inflation level. Consider $P_t \equiv 1$ across time. Then the Bitcoin price can be all, a super- or a submartingale, depending on its correlation with marginal utility of consumption. That is, the price evolution across time may differ substantially although inflation is held constant.

If on the other hand agents are risk-neutral, then the distribution of the Dollar price level and its correlation with Bitcoin determines the Bitcoin price path, see (41).

The following result is specific to cryptocurrencies which have an upper limit on their quantity, i.e., in particular, Bitcoin. Independently of whether all, some or no Bitcoins are spent,

Proposition 3. (Real Bitcoin Disappearance:)
Suppose that the quantity of Bitcoin is bounded above, $B_t \leq \bar{B}$ and let $\pi_t \geq \underline{\pi}$ for all $t \geq 0$ and some $\underline{\pi} > 1$. If marginal consumption is positively correlated or uncorrelated with the exchange rate $\frac{Q_{t+1}}{P_{t+1}}$, $cov_t(u'(c_{t+1}), \frac{Q_{t+1}}{P_{t+1}}) \geq 0$, then

$$E_0\left[\frac{Q_t}{P_t}B_t\right] \to 0, \quad as\ t \to \infty. \tag{51}$$

In words, the purchasing power of the entire stock of Bitcoin shrinks to zero over time, if inflation is bounded below by a number strictly above one.

The assumption on the covariance is in particular satisfied when agents are risk-neutral, or for constant output $c_t \equiv y_t \equiv \bar{y} = \underline{y}$. Note also, that we then have

$$\frac{Q_t}{P_t} = \mathbb{E}_t\left[\frac{Q_{t+1}}{P_{t+1}}\right] \cdot \mathbb{E}_t\left[\frac{1}{\pi_{t+1}}\right]^{-1} \geq \mathbb{E}_t\left[\frac{Q_{t+1}}{P_{t+1}}\right], \tag{52}$$

that is, the real value of Bitcoin falls in expectation (is a supermartingale) by equation (41).

Another way to understand this result is to rewrite the fundamental pricing equation for the case of a constant Bitcoin stock $B_t \equiv B$ and a constant inflation $\pi_t \equiv \pi$ as

$$E_t\left[\frac{v_{t+1}}{v_t}\right] = -\frac{\mathrm{cov}_t\left(u'(c_{t+1}), \frac{v_{t+1}}{v_t}\right)}{E_t[u'(c_{t+1})]} + \frac{1}{\pi}, \tag{53}$$

where

$$v_t = \frac{Q_t}{P_t} B_t$$

is the real value of the Bitcoin stock at time t. The left-hand side of (53) is the growth of the real value of the Bitcoin stock. The first term on the right-hand side (including the minus sign) is the risk premium for holding Bitcoins. With a fixed amount of Bitcoins and a fixed inflation rate, the equation says that the expected increase of the real value of the stock of Bitcoins is (approximately) equal to the risk premium minus the inflation rate on Dollars[7]. Should those terms cancel, then the real value of the stock of Bitcoins remains unchanged in expectation.

The following result requires that the total supply of the analyzed cryptocurrency is strictly bounded away from zero.

Corollary 2. (Real Bitcoin price bound:) *Suppose that $B_t > 0$ and $Q_t, P_t > 0$ for all t. The real Bitcoin price is bounded by $\frac{Q_t}{P_t} \in (0, \frac{\bar{y}}{B_0})$.*

Proof. It is clear that $Q_t, P_t \geq 0$. Per theorem 1, all Bitcoins are spent in every periods. Therefore, the Bitcoin price satisfies

$$\frac{Q_t}{P_t} = \frac{b_t}{B_t} \leq \frac{b_t}{B_0} \leq \frac{\bar{y}}{B_0} = \bar{Q}. \tag{54}$$

□

[7] Note that a Taylor expansion yields $1/\pi \approx 1 - (\pi - 1)$ for $\pi \approx 1$, and that $\pi - 1$ is the inflation rate.

The upper bound on the Bitcoin price is established by two traits of the model. First, the Bitcoin supply may only increase implying that B_t (the denominator) cannot go to zero. This is a property only common to uncontrolled cryptocurrencies. Second, by assumption, we bound production fluctuation. However, even if we allow the economy to grow over time, this bound continues to hold.[8]

Obviously, the current Bitcoin price is far from that upper bound. The bound may therefore not seem to matter much in practice. However, it is conceivable that Bitcoin or digital currencies start playing a substantial transaction role in the future. The purpose here is to think ahead towards these potential future times, rather than restrict itself to the rather limited role of digital currencies so far.

Heuristically, assume agents sacrifice consumption today to keep some Bitcoins as an investment in order to increase consumption the day after tomorrow. Tomorrow, these agents produce goods which they will need to sell. Since all Dollars change hands in every period, sellers always weakly prefer receiving Dollars over Bitcoins as payment. The Bitcoin price tomorrow can therefore not be too low. However, with a high Bitcoin price tomorrow, sellers today will weakly prefer receiving Dollars only if the Bitcoin price today is high as well. But at such a high Bitcoin price today, it cannot be worth it for buyers today to hold back Bitcoins for speculative purposes, a contradiction.

4.2 Constructing Equilibria

The challenge in explicitly constructing equilibria (and thereby showing their existence) lies in the zero-dividend properties of currencies. In asset pricing, one usually proceeds from a dividend process D_t. Denoting by Q_t the price of the asset, one usually exploits the asset pricing formula $Q_t = D_t + E_t[M_{t+1}Q_{t+1}]$ and "telescopes" out the right-hand side in order to write Q_t as an infinite sum of future dividends, discounted by stochastic discount factors. Properties of fundamentals such as correlations of dividends D_t with the stochastic discount factor then imply correlation properties of the price Q_t and the stochastic discount factor. This approach will not work here for equilibria with nonzero Bitcoin prices since dividends of fiat currencies are identical to zero.

[8]Assume, we allow the support of production y_t to grow or shrink in t: $y_t \in [\underline{y}, \overline{y}_t]$, then $\frac{Q_t}{P_t} \leq \frac{\overline{y}_t}{B_0}$.

The solution rests in rewriting equation (47) as

$$Q_{t+1} = Q_t + \epsilon_{t+1} - \frac{\text{cov}_t(\epsilon_{t+1}, m_{t+1})}{\mathbb{E}_t[m_{t+1}]}. \tag{55}$$

To sketch the idea, let a sequence of Dollar goods prices P_t and pricing kernels m_t be given, which satisfy the strong impatience assumption, written as

$$\beta E_t \left[\frac{m_{t+1}}{m_t} \frac{P_{t+1}}{P_t} \right] < 1 \qquad \text{for all } t. \tag{56}$$

Pick the initial Bitcoin price Q_0 and pick some sequence ϵ_t with $E_t[\epsilon_{t+1}] = 0$ and some chosen conditional covariance with the pricing kernels. Recursively, construct the sequence Q_{t+1} per (55). In order to arrive at an equilibrium, one needs to ensure that $Q_t > 0$ and $Q_t B_t < P_t y_t$ for all t and all sample paths. Under some mild constraints on the sequence ϵ_t, this will be so for a nonempty interval of initial Bitcoin prices Q_0, thereby delivering a version of the exchange-rate indeterminacy result in Kareken-Wallace (1981) and its stochastic counterpart in Manuelli-Peck (1990), proposition 3.2. For the exact details and explicit examples, we refer the reader to section C in the appendix.

5 Implications for Monetary Policy

Throughout the section, we impose assumption 3. The resulting No-Bitcoin-Speculation Theorem 1 in combination with the equilibrium conditions implies interdependence between the Bitcoin price and monetary policy of the central bank. Since all Dollars and Bitcoins change hands in every period, the velocity of money equals one. In a world with only one money, classical quantity theory yields that depending on the exogenous realization of output, the central bank adjusts the dollar quantity such that the desired Dollar price level realizes, i.e., according to

$$y_t = \frac{D_t}{P_t}. \tag{57}$$

In our model instead, with two monies, equilibrium market clearing imposes

$$y_t = \frac{D_t}{P_t} + \frac{Q_t}{P_t} B_t. \tag{58}$$

That is, there are now two endogenous variables, the Dollar quantity and the Bitcoin price. This already shows a crucial distinction between our two-currency world and a one-currency world. Holding P_t, y_t and Q_t constant, in equilibrium, a deterministic increase in B_t must be compensated by a corresponding decrease in D_t:

Theorem 2. (Bitcoin block rewards are financed by Dollar taxes:) *Any no-speculation equilibrium price sequence (Q_t, P_t) with $Q_t > 0$ for some given path $B_t > 0$ can also be supported as an equilibrium price sequence by an alternative path B'_t, provided that $0 < B'_t < (P_t/Q_t)y_t$, per appropriately adjusting the Dollar quantity D_t. For given Dollar lump-sum transfers τ_t in the original equilibrium, the adjusted Dollar lump-sum transfers τ'_t are given by*

$$\tau'_t = \tau_t - (Q_t - Q_{t-1})(B'_t - B_t) - Q_{t-1}\left((B'_t - B'_{t-1}) - (B_t - B_{t-1})\right) \tag{59}$$

Suppose the economy is deterministic and that the Bitcoin quantity in the original economy is constant $B_t \equiv B$, while the Bitcoin stock in the new economy is increasing period-per-period per the Bitcoin block rewards A'_t, i.e. $B'_{t+1} = A'_t + B'_t$. Theorem 1 with proposition 1 implies that Q_t is constant, $Q_t \equiv Q$. Equation (59) then states that $\tau'_t = \tau_t - Q(B'_t - B'_{t-1})$, i.e. the Dollar lump-sum taxes pay for the block rewards.

This logic applies to (59) generally. The no-speculation equilibrium imposes the fundamental pricing equation to hold for P_t and Q_t. Since this equation imposes no constraints on B_t and D_t, the alternative Bitcoin quantity path B'_t with adjusted Dollar supply D'_t and Dollar lump-sum transfers τ'_t is equally compatible with the equilibrium prices P_t and Q_t. In particular, a change in the path B_t does neither require nor necessarily allow a change in Q_t. Formulated more succinctly: the block rewards to miners, which are provided in our baseline model as lump-sum distribution to agents and which are earned through effort in section 6, are financed not by deflating the Bitcoin currency but by the Dollar central bank, which has to accordingly decrease its Dollar supply, per imposing Dollar lump-sum taxes on the population. The block rewards are not a tax on Bitcoin holders but are financed through Dollar taxes imposed by the Dollar central bank. This may have important consequences for the political debate.

To understand their further relationship, first, consider the price level P_t to be endogenous as well. Think of the Dollar quantity as a policy choice, while keeping $y_t = y$ and $B_t = B$ as exogenously given. Without Bitcoins or with $B_t = 0$, we are back to equation (57) and the classic relationship between the quantity of money and the price level. With $B_t > 0$ and Q_t endogenous, however, matters become a bit more involved. Consider two different Dollar quantities $D_t = D$ and $D_t = D'$. For each Dollar quantity, there is now a set or line of equilibrium values for $P = P_t$ and $Q_t = Q$ satisfying the market clearing equation (58),

$$L = \{(Q, P) \mid P = \frac{D}{y} + Q\frac{B}{y}\},\ L' = \{(Q, P) \mid P = \frac{D'}{y} + Q\frac{B}{y}\}.$$

These two lines are shown in the left panel of figure 3. Suppose we start from the equilibrium at point A for the Dollar quantity D. What happens, as the central bank issues the Dollar quantity D' instead? Without further assumptions, any (Q, P)-pair on line L' may constitute the new equilibrium. Some additional equilibrium selection criterion would be required. One possibility, which we label the "conventional scenario", is to think of the Bitcoin price as moving exogenously: in the figure, we fix it at $Q = \bar{Q}$. In that case, we get a version of the classic relationship in that the increase in the dollar quantity from D to D' leads to a higher price level, moving the equilibrium from point A to point B. Another possibility though, which we label the "unconventional scenario", is to instead fix the price level at some exogenously given level $P = \bar{P}$: now, increasing the Dollar quantity reduces the Bitcoin price, moving the equilibrium from point A to point C. Many other equilibrium selection criteria can be introduced, in principle.

We have side-stepped these equilibrium selection issues per fixing π_t as an exogenous stochastic process along with P_0. There is an extensive literature on the capability of central banks to influence the Dollar price level, and we have nothing new to contribute to that: our assumption about the exogeneity of the price level encodes that literature. The question of interest here is to what degree the central bank can influence the Bitcoin price. The relevant equilibrium relationship is then given by the right panel of figure 3, where we have now fixed the price level P. The "conventional" scenario now amounts to assuming exogenous fluctuations in Q, moving, say, from Q to Q', to which the central bank has to react per moving the Dollar quantity from D to D' in order for (58) to continue to be satisfied. The equilibrium then moves from point A to point B. Conversely, and for the "unconventional" scenario, one may wish to think of the central bank as picking the Dollar quantity as D or D' and thereby picking the Bitcoin price to be Q or Q'. Both (and more) scenarios are consistent with our definition of equilibrium. We proceed to examine the consequences of each in greater detail.

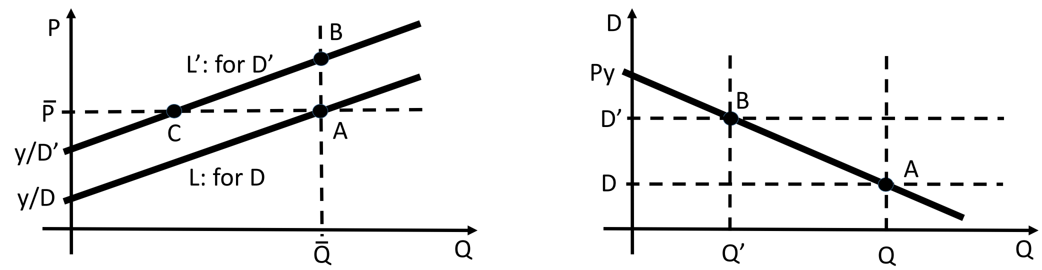

Figure 3: Examining equation (58), $y = \frac{D}{P} + \frac{Q}{P}B$, taking y and B as given.

In order to bring structure to that discussion, it is useful to expand and alter the model slightly. First, let us introduce two new random variables $P_t^* > 0$ and $Q_t^* > 0$, which we call the target outcomes, drawn alongside y_t as a function of the stochastic state history θ^t at the beginning of the period[9]. Second, we introduce a central bank objective via the loss function

$$\mathcal{L}(P_t, Q_t) = -(P_t - P_t^*)^2 - (Q_t - Q_t^*)^2. \tag{60}$$

The loss function can be thought of reflecting a desire by the central bank to stabilize the Dollar price level as well as the Bitcoin price near their target outcomes. The central bank seeks to minimize this loss through suitable choice of the dollar supply D_t, subject to the market clearing equation (58). The two scenarios now differ in what else gets drawn alongside P_t^*, Q_t^*, y_t at the beginning of the period as a function of θ^t. These scenarios have additional implications, which we discuss in appendix E. We discuss welfare implications and optimal monetary policy in section 6.1, once we have introduced effort-driven mining of additional Bitcoins.

5.1 Conventional Scenario

For the conventional scenario, we shall assume that the Bitcoin price Q_t is exogenous.

Assumption A. 4. *(***Conventional Scenario:)** *Assume that Q_t is drawn alongside P_t^*, Q_t^*, y_t at the beginning of the period as a function of θ^t.*

[9]Recall that the Bitcoin quantity B_t is a deterministic function of time.

Corollary 3. (Conventional Monetary Policy:)
Under assumption 4, the loss-minimizing central bank picks the Dollar quantity

$$D_t = y_t P_t^* - Q_t B_t,$$

to uniquely achieve the Dollar price level $P_t = P_t^*$.

Corollary 3 and the fundamental pricing equation provide a straightforward receipt for forecasting the dollar supply.

Implication 1 (Forecasting the Dollar supply)**.** *Since* B_{t+1} *is known at time* t*, using Corollary 3, Corollary 1 and* $B_{t+1} = B_t + A_t$ *we obtain*

$$\begin{aligned}\mathbb{E}_t[D_{t+1}] &= \mathbb{E}_t[y_{t+1}P_{t+1}] - (B_t + A_t)\,(Q_t - \kappa_t \cdot corr_t(\frac{u'(c_{t+1})}{P_{t+1}}, Q_{t+1})) \\ &= \mathbb{E}_t[y_{t+1}P_{t+1}] - B_t\, Q_t - A_t Q_t + \kappa_t\, (B_t + A_t)\, \cdot corr_t(\frac{u'(c_{t+1})}{P_{t+1}}, Q_{t+1}) \\ &= D_t - (y_t P_t - \mathbb{E}_t[y_{t+1}P_{t+1}]) - A_t Q_t + \kappa_t\, (B_t + A_t)\, \cdot corr_t(u'(c_{t+1}), Q_{t+1}),\end{aligned}$$

where κ_t *stems from Corollary 1.*

5.2 Unconventional Scenario

For the unconventional scenario, we shall assume that the Dollar price level P_t is exogenous.

Assumption A. 5. (Unconventional Scenario:) *Assume that* P_t *is drawn alongside* $\bar{P}_t, Q_t^*, y_t$ *at the beginning of the period as a function of* θ^t.

Assumption 5 implies that the central bank can maintain the inflation level π_t independently of the transfers she sets.

Corollary 4. (Policy-driven Bitcoin price:)
Under assumption 5, the loss-minimizing central bank picks the Dollar quantity

$$D_t = y_t P_t - Q_t^* B_t,$$

to uniquely achieve the Bitcoin price $Q_t = Q_t^*$

Intuitively, the causality is in reverse compared to the conventional scenario: now the central bank policy drives Bitcoin prices.

5.3 Robustness

We are next interested in the implications of our model should the No-Speculation Theorem fail. For instance, assume, assumption 3 does not hold. Assume, not all Bitcoins are spent. Then either some Bitcoins are spent, or no Bitcoins are spent. Since all Dollars are spent in each period, by Lemma 1, if some Bitcoins are spent the fundamental pricing equation 1 and therefore Corollary 1 still apply. If no Bitcoins are spent, the fundamental condition holds with inequality, see Lemma 3. As a consequence, the covariance formula in Corollary 1 becomes

$$Q_t \geq E_t[Q_{t+1}] + \kappa_t \cdot \mathrm{corr}_t \left(\frac{u'(c_{t+1})}{P_{t+1}}, Q_{t+1} \right), \tag{61}$$

which implies price bounds. Concerning monetary policy, if not all Bitcoins are spent we have $b_t < (Q_t/P_t)B_t$. Market clearing and other equilibrium conditions yield

$$P_t\, y_t = P_t\,(b_t + z_t) < Q_t\, B_t + D_t,$$

which implies bounds for monetary policy respectively the Bitcoin price.

6 Bitcoin Production

So far, we have assumed that Bitcoin production takes the form of an exogenous endowment. The purpose of this section is to examine what happens when it takes effort $e_{t,j}$ for agent j to produce or "mine" additional Bitcoins (or: "receive Bitcoin block rewards") $A_{t,j}$. Effort $e_{t,j}$ causes disutility $h(e_{t,j})$, where $h(\cdot)$ is strictly increasing and weakly convex. We have chosen the effort formulation rather than a resource-cost formulation, in order to avoid some tedious terms of reducing overall goods consumption, due to the diversion of output into Bitcoin production. To the degree that the resource costs of producing Bitcoins in practice are still minor compared to global output, this seems appropriate for the analysis. In light of that practice, one may wish to interpret effort $e_{t,j}$ as the individually provided hash rate resulting from consuming electricity or a combination of electricity and the appropriate utilization of hardware. If electricity is the only input and production is viewed as scalable, then it is appropriate to choose $h(\cdot)$ as a linear function with a positive slope. If there is an additional capacity constraint arising from available hardware, then $h(\cdot)$ could be chosen to be piecewise linear, with a low slope up to that constraint and a much higher slope beyond. This leaves aside the issue of hardware acquisition and investment, an issue studied in considerable detail in Prat-Walter(2018).

Define the aggregate effort level for mining Bitcoin at time t per

$$\bar{e}_t = \int_{j \in [0,1]} e_{t,j} \, dj. \tag{62}$$

As before, let A_t be the deterministic quantity of additional Bitcoins added in period t. We assume that an individual agent expanding effort $e_{t,j} \geq 0$ will then receive additional Bitcoins according to the production function

$$A_{t,j} = A_t \frac{e_{t,j}}{\bar{e}_t}. \tag{63}$$

As a consequence of equation (63), the total number of newly mined coins per period indeed satisfies

$$A_t = \int_{j \in [0,1]} A_{t,j} \, dj, \tag{64}$$

and is independent of the aggregate effort level. This modeling choice captures the real-life feature, that the increase in the hash rate has no impact on the total Bitcoin production[10], see Huberman, Leshno and Moallemi (2017). In comparison to the practice of Bitcoin mining, one might wish to interpret $\frac{e_{t+1,j}}{\int_{j \in [0,1]} e_{t+1,j}}$ as the probability for an individual miner to win the proof-of-work competition for the next block reward. Typically, individual miners associate in large mining pools, thereby eliminating the idiosynchratic risk of mining success, see Cong, He, and Li (2018). Thus, $A_{t+1,j}$ becomes a deterministic function of individual and aggregate effort and the deterministic increase in the aggregate stock of Bitcoins.

The equilibrium conditions (17) and (28) for mining in the definition of an equilibrium now need to be replaced by

$$A_{t,g} = A_t \frac{e_t}{\bar{e}_t}, \text{ with } e_t \geq 0, \tag{65}$$

$$A_{t,r} = A_t \frac{e_t}{\bar{e}_t}, \text{ with } e_t \geq 0, \tag{66}$$

$$\tag{67}$$

[10]This is achieved by regular adaption of the difficulty level of the proof-of-work competition.

while the rest of the equilibrium definition remains unchanged.

As for the production of Bitcoins, we obtain the following result.

Proposition 4. (Bitcoin Production Condition:) *Suppose that the aggregate quantity A_t of additionally mined Bitcoins in period t is strictly positive*[11]*. Given the processes*[12] *for $Q_{t+1}, P_{t+1}, y_{t+1}$, the equilibrium Bitcoin production effort $e_{t,j} = \bar{e}_t > 0$ is the unique solution to*

$$h'(\bar{e}_t) = \beta E_t \left[u'(y_{t+1}) \frac{Q_{t+1}}{P_{t+1}} \right] \frac{A_t}{\bar{e}_t}. \tag{68}$$

In particular, the Proposition implies that the equilibrium mining effort $\bar{e}_t$ is always strictly positive provided that the price $Q_{t+1} > 0$ and the aggregate quantity A_t are strictly positive. Intuitivly, this is due to the externality in mining: If other agents put zero mining effort, then an agent can ensure herself the entire new block reward but putting only small effort. Equation (68) further tells us that the individual and therefore also the aggregate mining effort increases as expectations on the real Bitcoin price increase.

We can now show, that introducing Bitcoin production does not otherwise change the equilibrium. This may be a bit of a surprise: one might have thought that costly Bitcoin production should somehow lead to a tax on Bitcoin transactions, for example[13] or alter the outcomes in some other way.

Theorem 3. (Irrelevance of Mining effort:) *Consider an equilibrium of the original economy with exogenous (effort-less) Bitcoin production, and that Bitcoin production is always strictly positive. Then, there exists an equilibrium of the economy with effort needed to produce Bitcoins, where all variables are the same except that $e_t = \bar{e}_t > 0$ is the unique solution to equation (68) rather than $e_t = \bar{e}_t = 0$.*

Proof. Recall that the aggregate Bitcoin production is assumed to be an exogenous and deterministic function of time. Therefore, all equations in the no-effort equilibrium continue to hold, if effort of production is introduced instead. □

[11] Recall that we assumed the aggregate quantity A_t to be deterministic and exogenous.

[12] Recall that we focus on equilibria in which $Q_{t+1} > 0$. If $Q_{t+1} \equiv 0$ instead, then mining effort in t must be zero.

[13] One reads this argument frequently in popular postings on Bitcoins.

6.1 Optimal Monetary Policy and Welfare

Analyzing welfare in the baseline model or in the baseline model extended with effort-driven Bitcoin production is straightforward[14]. Let $0 < \lambda < 1$ be the welfare weight on green agents and $1 - \lambda$ be the welfare weight on red agents, assuming that agents of the same type all receive the same weight, see also appendix D. The overall welfare function is then given by

$$W = \lambda U_g + (1 - \lambda) U_r,$$

where U_g and U_r are given in equations (11) and (21). Welfare is maximized if all output of the consumption good is always consumed and no Bitcoins are ever produced. For this, note that the social planner cannot redistribute consumption goods from even to odd periods, i.e., changing the welfare weight λ does not change the welfare-maximal allocation.

In all our equilibria, all output of the consumption good is always consumed. Therefore, the welfare arising from goods consumption is unaffected by monetary policy or the price path for Bitcoins. This implies that low inflation, as well as high inflation, all achieve the same goods consumption welfare. The only part of utility possibly affected is the disutility from producing Bitcoin.

Any equilibrium in the baseline model, where additional Bitcoins are received as endowment without the supply of effort, is welfare optimal. Any production of Bitcoin requiring effort is wasteful in terms of welfare. This result should not surprise in this model. Anything that can be done with Bitcoin can be done with Dollar. Since Bitcoins are costly to produce, while Dollars can be produced costlessly, Dollars should be used, if otherwise, Bitcoin production is necessary. It is a policy conclusion reached straight from the assumption, that the government is better at doing something than the private sector, and thus not very informative. It may also be interesting to note that the mining of Bitcoins adds to the gross national product since the mined Bitcoins would need to be evaluated at their market price. More Bitcoin production means more GNP, but less welfare. In summary, all equilibria, in which no Bitcoin production takes place or where Bitcoin production takes no effort, are welfare optimal and minimize GNP. Nevertheless, these results are unlikely to remain true in generalizations of our model.

[14]The welfare analysis becomes a bit more involved if we allow for effort-driven Bitcoin production as well as versions of the unconventional scenario and thereby endogeneity of Q_t. We leave that to future research.

6.2 Taxing Bitcoin Production

Could a government capable of imposing a tax on Bitcoin production change the equilibrium outcome and how? As a practical matter, it may be easiest to impose a proportional tax on the energy consumption of miners or, in the language here, on the effort of miners. If one reads $h(e_{t,j})$ as the energy costs of mining effort $e_{t,j}$, these costs will then increase to $h(e_{t,j})/(1-\tau)$, where $\tau \in [0,1)$ is that tax rate. The Bitcoin equilibrium production equation (68) then generalizes to

$$\frac{h'(\bar{e}_t)}{1-\tau} = \beta E_t \left[u'(y_{t+1}) \frac{Q_{t+1}}{P_{t+1}} \right] \frac{A_t}{\bar{e}_t}, \tag{69}$$

per the same logic as in the proof above. Some more analysis reveals the overall consequences of imposing these taxes.

Proposition 5. (Irrelevance of Mining Taxation:) *Consider an equilibrium of the original economy without imposing taxes on Bitcoin production, and that Bitcoin production is always strictly positive. There is then an equilibrium of the economy with imposing taxes $0 < \tau < 1$ on Bitcoin production, where all variables are the same except that $e_t = \bar{e}_t$ is the unique solution to equation (69) rather than (68). Compared to the no-tax equilibrium, effort levels are always strictly lower and welfare is strictly higher.*

The logic of the proposition and the argument in the proof goes through, when imposing the linear tax in some other manner, distributing the proceeds lump-sum to the group of taxed agents[15]. Generally, effort provision is imposing a wasteful externality on all other effort-providing agents in the economy, since the additional quantity of Bitcoins is not affected: it, therefore, should not surprise that welfare can be improved per taxing that activity. Note that this conclusion is likely to change in a setting where the total hash rate provided by the network is relevant for the security of the mining network and thus the cryptocurrency as a whole. Keep in mind that we are assuming in the proposition above, that Bitcoin production can happen right away if this turns out to be profitable. In practice, capacity such as computing farms together with programmers capable of writing the appropriate code may need to build

[15]The results might get altered, if the tax schedule is nonlinear, as one could now introduce, e.g. multiple equilibria. They would also be altered, if, say, the tax receipts collected from green agents are redistributed to red agents, but equilibrium-altering redistributive taxes do not require the taxation of Bitcoin production.

up gradually over time. One could extend the model to allow for such time-to-build of capacity as investigated in Prat and Walter (2018), and it may be interesting to do so.

7 Multiple Private Currencies and Free Entry

So far we have analyzed competition between two fiat currencies without addressing entry of new currencies. This section offers a sketch on how to extend our analysis to that situation. A full development is left to future research.

While the supply of any particular cryptocurrency may evolve deterministically over time and be bounded, the total supply of all cryptocurrencies may be stochastic and unbounded due to entry. One particular property of monetary equilibria is that they are self-eliminating backwards in time. As Kareken and Wallace (1981) already mention in their deterministic setting, if tomorrow's price of a currency is zero, its price today is zero as well. For a fiat currency to enter, the opposite effect must be true. The fundamental pricing equation (40) will hold for any cryptocurrency with a nonzero price at date t. That equation expresses, in particular, the logic that agents accept a currency at some date t at a strictly positive price only because they believe that the currency will have a positive price at the following date $t + 1$ with some nonzero probability. Put differently, if today sufficiently many agents believe that tomorrow sufficiently many agents believe that the currency has value, then its price today is positive indeed. In that sense, monetary equilibria are self-fulfilling, see also Sockin-Xiong (2018). This reasoning applies in particular to the initial sale of a new currency or the initial coin offering. Furthermore, this argument has to work from the perspective of a miner. As in our main model, suppose that the sale of a (new) coin in $t + 1$ takes mining effort in date t. A miner mines the first coin only if her joint belief about the measure of agents who will accept the currency tomorrow as well as the price of the currency justifies her effort level today.

Under free entry, the pricing formula (40) remains correct. If trade in all positively priced currencies happens simultaneously, sellers are marginally indifferent in accepting all of these currencies. This can only be the case if the sellers expect the risk-adjusted returns on all traded currencies to be equal, as expressed in the fundamental pricing equation (40). Under the global impatience assumption 3 and the no-speculation theorem 1, assume that the quantity of any cryptocurrency cannot decrease. Let Q_t^j denote the price of cryptocurrency j at date t. Let n_t the random quantity of distinct cryptocurrencies available for purchase at date t. Denote by $B_{t_0^j}^j \geq 0$ the initial stock of cryptocurrency j, where $t_0^j \geq 0$ is the time of the initial coin offering of currency j. Let B_t^j the stock of that cryptocurrency at date t where $B_t^j = 0$ for $t < t_0^j$ before the ICO. Then, the real price bound of corrolary 2 generalizes to

$$\sum_{j=1}^{n_t} \frac{Q_t^j}{P_t} B_{t_0^j}^j \leq \bar{y}, \tag{70}$$

since we must have $\sum_{j=1}^{n_t} \frac{Q_t^j}{P_t} B_t^j \leq y_t$. The result on Bitcoin disappearance may no longer obtain. If over time new currencies enter faster than established currencies devalue, the total purchasing power of all cryptocurrencies may not vanish and can even increase.

8 Conclusions

This paper analyzes the evolution of cryptocurrency prices and the consequences for monetary policy in a model, in which a cryptocurrency such as Bitcoin coexists and competes with a traditional fiat money (Dollar) for usage. A central bank targets a stochastic inflation level for the Dollar via appropriate monetary injections, while Bitcoin production is decentralized via proof-of-work and Bitcoin supply may only increase over time. Both monies can be used for transactions. We derive a "fundamental pricing equation" for Bitcoin prices when both currencies are simultaneously in use. It implies that Bitcoin prices form a martingale in a special case. Due to currency competition, the block rewards are not a tax on Bitcoin holders. Instead, they are financed by Dollar taxes imposed by the central bank. We also provide a "speculative price bound" when Bitcoins are held back in transactions in the hope of a Bitcoin price appreciation. We provide conditions, under which no speculation in Bitcoins arises. We further provide a general method for constructing equilibria, thereby demonstrating their existence. Specific examples show that the Bitcoin price might appreciate or depreciate in expectation, or a mix thereof. We study the implications for monetary policy under a "conventional" as well as an "unconventional" scenario. In the conventional scenario, the Bitcoin price evolves exogenously, thereby driving the Dollar injections needed by the central bank to achieve its inflation target.

In the unconventional scenario, we suppose that the inflation target is achieved for a range of monetary injections, which then, however, influence the price of Bitcoins. We discuss the taxation of Bitcoin production.

For our analysis, one should think of Bitcoin as a representative of the family of intrinsically worthless, storable, non-dividend paying objects, which are used as a medium of exchange but whose price process is not manipulated or stabilized by a third institution such as a central bank. We abstract from several features which distinguish Bitcoin from for instance Visa, Paypal, and cash such as censorship resistance, transparency, and speed of trading. These characteristics may be important for future research when thinking about Bitcoin speculation.

References

[1] Abadi, Joseph and Brunnermeier, Markus (2018), "Blockchain economics", mimeo Princeton University.

[2] Athey, Susan, Ivo Prashkevov, Vishnu Sarukkai, Jing Xia (2016), "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence", draft, Stanford University.

[3] Badev, Anton and Matthew Chen (2014), "Bitcoin: Technical Background and Data Analysis," Federal Reserve Board, Washington, D.C., Staff Working Paper 2014-104.

[4] Bech, Morten and Rodney Garratt (2017), "Central Bank Cryptocurrencies," BIS Quarterly Review (September), 55-70.

[5] Berentsen, Aleksander and Fabian Schär, *Bitcoin, Blockchain und Kryptoassets: Eine umfassende Einführung.* BoD, Norderstedt, 2017.

[6] Berentsen, Aleksander and Fabian Schär (2018a), "A Short Introduction to the World of Cryptocurrencies," Federal Reserve Bank of St. Louis Review, First Quarter 2018, 100 (1), pp. 1-16.

[7] Bewley, Truman (1977), "The permanent income hypothesis: a theoretical formulation," Journal of Economic Theory, vol. 16, no. 2, pp. 252–292.

[8] Biais, Bruno and Bisiere, Christophe and Bouvard, Matthieu and Casamatta, Catherine (2018), "The blockchain folk theorem".

[9] Böhme, Rainer, Nicolas Christin, Benjaimin Edelman and Tyler Moore (2015), "Bitcoin: Economics, Technology and Governance," Journal of Economic Perspectives (Spring), vol. 29, no. 2, pp. 213-238.

[10] Bolt, Wilko and Maarten R.C. van Oordt (2016), "On the Value of Virtual Currencies," Financial Stability Department, Bank of Canada, draft.

[11] Borgonovo, Emanuele, Stefano Caselli, Alessandra Cillo and Donato Masciandaro (2017), "Beyond Bitcoin and Cash: do we would like a central bank digital currency? A financial and political economics approach," Bocconi WP 65.

[12] Brandvold, Morten, Peter Molnár, Kristian Vagstad, Ole Christian Andreas Valstad, "Price discovery on Bitcoin exchanges," Journal of International Financial Markets, Institutions & Money, vol. 36 (2015), 18-35.

[13] Brito, Jerry and Andrea Castillo (2013), "Bitcoin. A Primer for Policymakers," Mercatus Center, George Mason University, draft.

[14] Budish, Eric (2018), "The Economic Limits of Bitcoin and the Blockchain", National Bureau of Economic Research.

[15] Burnside, Craig, Martin Eichenbaum and Sergio Rebelo (2011), "Carry Trade and Momentum in Currency Market," Annual Review of Financial Economics, vol. 3, pp. 511-535.

[16] Burnside, Craig, Martin Eichenbaum and Sergio Rebelo (2015), "Understanding Booms and Busts in Housing Markets," draft, Northwestern University.

[17] Carstens, Augustin (2018), "Money in the digital age: what role for central banks?", Lecture at the House of Finance, Goethe University Frankfurt February 6th, 2018, available as a draft from BIS.

[18] Catalini, Christian and Joshua S. Gans (2016), "Some Simple Economics of the Blockchain," NBER WP 22952.

[19] Chiu, Jonathan, and Thorsten V. Koeppl (2017) "The economics of cryptocurrencies–Bitcoin and beyond."

[20] Chohan, Usman W. (2017), "A History of Bitcoin," Discussion Paper, University of New South Wales, Canberra.

[21] Cong, Lin William, Zhiguo He, and Jiasun Li (2018), "Decentralized mining in centralized pools," draft, The University of Chicago Booth School of Business.

[22] Cong, Lin William and Zhiguo He (2018), "Blockchain Disruption and Smart Contracts," draft, Booth School of Business, University of Chicago.

[23] Fantazzini, Dean, Erik Nigmatullin, Vera Sukhanovskaya and Sergey Ivliev (2016), "Everything you always wanted to know about Bitcoin modelling but were afraid to ask," draft (in English), Moscow School of Economics, published (in Russian) in Applied Econometrics (2016), vol. 44, 5-24 as part I and Applied Econometrics (2017),vol. 45, pp. 5-28 as part 2.

[24] Fernández-Villaverde, Jesús and Daniel Sanches (2016), "Can Currency Competition Work?", draft, University of Pennsylvania.

[25] Foley, Sean, Jonathan R. Karlsen, Talis J. Putnins (2018), "Sex, drugs, and Bitcoin: how much illegal activity is financed through cryptocurrencies?", draft, University of Sydney.

[26] Gandal, Neil and Hanna Halaburda (2014), "Competition in the Cryptocurrency Market," CEPR DP 10157, CEPR, London.

[27] Garratt, Rodney and Neil Wallace (2017), "Bitcoin 1, Bitcoin 2, ... : An Experiment in Privately Issued Outside Monies," draft, UC Santa Barbara and Penn State University.

[28] Goldberg, Dror (2005), "Famous Myths of 'Fiat Money' ", Journal of Money, Credit and Banking, vol. 37, no. 5, pp. 957-967.

[29] Griffin, John M. and Amin Shams (2018), "Is Bitcoin Really Un-Tethered?", draft, McCombs School of Business, The University of Texas at Austin.

[30] Guerrieri, Veronica and Harald Uhlig (2016), "Housing and Credit Markets: Booms and Busts," chapter 17 in *Handbook of Macroeconomics*, John Taylor and Harald Uhlig, eds., Elsevier, pp. 1427-1496.

[31] Halaburda, H., and M. Sarvary (2015), *Beyond Bitcoin: The Economics of Digital Currencies,* Palgrave Macmillan.

[32] Hayek, Friedrich (1976), *The Denationalization of Money,* Institute of Economic Affairs.

[33] Huberman, Gur and Leshno, Jacob D and Moallemi, Ciamac C (2017), “Monopoly without a monopolist: An economic analysis of the Bitcoin payment system”.

[34] Kareken, John and Neil Wallace (1981), “On the Indeterminacy of Equilibrium Exchange Rates,” The Quarterly Journal of Economics, vol. 96, No. 2 (May), pp. 207-222.

[35] Kiyotaki, Nobuhiro and Randall Wright (1989), “On Money as a Medium of Exchange,” Journal of Political Economy, Vol. 97, No. 4 (August), pp. 927-954.

[36] Lagos, Ricardo and Randall Wright (2005), “A Unified Framework for Monetary Theory and Policy Analysis,” Journal of Political Economy, Vol. 113, No. 3 (June), pp. 463-484.

[37] Lee Kuo Chuen, David, ed. (2015), *Handbook of Digital Currency,* 1st edition, Elsevier.

[38] Liu, Yukun and Tsyvinski, Aleh (2018), “Risks and Returns of Cryptocurrency”, National Bureau of Economic Research Working Paper no. 24877.

[39] Makarov, Igor, and Antoinette Schoar, (2018), “Trading and Arbitrage in Cryptocurrency Markets.”

[40] Manuelli, Rodolfo E., and James Peck. ”Exchange rate volatility in an equilibrium asset pricing model.” International Economic Review (1990): 559-574.

[41] Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller and Steven Goldfeder (2016), *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction,* Princeton University Press.

[42] Nakamoto, Satoshi (2008), “Bitcoin: A Peer-to-Peer Electronic Cash System,” www.Bitcoin.org.

[43] Prat, Julien, and Benjamin Walter (2018), ”An equilibrium model of the market for Bitcoin mining,” draft, CREST, France.

[44] Routledge, Bryan and Zetlin-Jones, Ariel (2018), "Currency Stability Using Blockchain Technology", draft, Carnegie-Mellon.

[45] Samuelson, Paul A. (1958), "An Exact Consumption Loan Model of Interest, With or Without the Social Contrivance of Money," Journal of Political Economy 66(5), pp. 467—482.

[46] Scheinkman, José A. and Wei Xiong (2003), "Overconfidence and speculative bubbles," Journal of Political Economy, vol. 111 no. 6, pp. 1183-1220.

[47] Schnabel, Isabel and Hyun Song Shin (2018), "Money and trust: lessons from the 1620s for money in the digital age," BIS Working Paper no 698.

[48] Sockin, Michael and Xiong, Wei (2018), "A model of cryptocurrencies", draft, Princeton University.

[49] Tirole, Jean (1982), "On the Possibility of Speculation under Rational Expectations," Econometrica, vol. 50, no. 5, pp. 1163-1181.

[50] Townsend, Robert (1980), "Models of Money with Spatially Separated Agents," in *Models of Monetary Economies*, John Kareken and Neil Wallace, eds., Federal Reserve Bank of Minneapolis, pp. 265-303.

[51] Trimborn, Simon and Wolfgang Härdle, "CRIX or evaluating blockchain based currencies," SFB 649 Discussion Paper 2016-021, Humboldt University Berlin.

[52] Velde, Francois R. (2013), "Bitcoin: A primer," Chicago Fed Letter, The Federal Reserve Bank of Chicago, December, no. 317.

[53] Weber, Beat (2013), "Bitcoin and the legitimacy crisis of money,,' Oesterreichische Nationalbank.

[54] Yermack (2015), David, "Is Bitcoin a real currency?" in D. Lee (ed), The Handbook of Digital Currency, Elsevier, pp. 31-44.

[55] Zhu and Hendry (2018), "A framework for analyzing monetary policy in an economy with E-money", Bank of Canada.

ONLINE APPENDIX

A Some background and literature

The original Bitcoin idea and the key elements of its construction and trading system are described by the mysterious author Nakamoto (2008). They can perhaps be summarized and contrasted with traditional central-bank issued money as follows: this will be useful for our analysis. While there are many currencies, each currency is traditionally issued by a single monopolist, the central bank, which is typically a government organization. Most currencies are fiat currencies, i.e. do not have an intrinsic value as a commodity. Central banks conduct their monetary operations typically with the primary objective of maintaining price stability as well as a number of perhaps secondary economic objectives. Private intermediaries can offer inside money such as checking accounts, but in doing so are regulated and constrained by central banks or other bank regulators, and usually need to obtain central bank money to do so. By contrast, Bitcoin is issued in a decentralized manner. A Bitcoin is an entry in an electronic, publicly available ledger or blockchain. Issuing or creating (or "mining") a Bitcoin requires solving a changing mathematical problem. Anyone who solves the problem can broadcast the solution to the Bitcoin-using community. Obtaining a solution is hard and becoming increasingly harder while checking the correctness of the solution is relatively easy. This "proof of work" for creating a Bitcoin thus limits the inflow of new Bitcoins. Bitcoins and fractions of Bitcoins can be transferred from one owner to the next, per broadcasting the transaction to the community and adding that transaction to the ledger information or blockchain. Transaction costs may be charged by the community, which keeps track of these ledgers.

There is an increasing number of surveys or primers on the phenomenon, its technical issues or its regulatory implications, often provided by economists working for central banks or related agencies and intended to inform and educate the public as well as policymakers. Velde (2013), as well as Brito and Castillo (2013) provide early and excellent primers on Bitcoin. Weber (2013) assesses the potential of the Bitcoin system to become a useful payment system, in comparison to current practice. Badev and Chen (2014) provide an in-depth account of the technical background. Digital Currencies have received a handbook treatment by Lee (2015), collecting contributions by authors from various fields and angles, and a textbook treatment in Halaburda-Sarvary (2015) and Narayanan et al (2016). Böhme et al. (2015) provide an introduction to the economics, technology, and governance of Bitcoin in their Journal-of-Economics-Perspective contribution. There is now a journal called Ledger, available per ledgerjournal.org, devoted to publishing papers on cryptocurrencies and blockchain since its inaugural issue in 2016. Bech and Garratt (2017) discuss whether central banks should introduce cryptocurrencies, finding its echo in the lecture by Carstens (2018). Borgonovo et al. (2017) examine this issue from a financial and political economics approach. Chohan (2017) provides a history of Bitcoin.

The phenomenon of virtual currencies such as Bitcoin is increasingly attracting the attention of serious academic study by economists. Rather than an exhaustive literature overview, we shall only provide a sample. Some of the pieces cited above contain data analysis or modeling as well.

Gandal and Halaburda (2014) empirically investigate competition between cryptocurrencies. Yermack (2015), a chapter in the aforementioned handbook, concludes that Bitcoin appears to behave more like a speculative investment than a currency. Brandvold et al. (2015) examine the price discovery on Bitcoin exchanges. Fantazzini et al. (2016, 2017) provide a survey of econometric methods and studies, examining the behavior of Bitcoin prices, and list a number of the publications on the topic so far. Fernández-Villaverde and Sanches (2016) examine the scope of currency competition in an extended Lagos-Wright model and argue that there can be equilibria with price stability as well as a continuum of equilibrium trajectories with the property that the value of private currencies monotonically converges to zero. Bolt and Oordt (2016) examine the value of virtual currencies, predicting that increased adoption will imply that the exchange rate will become less sensitive to the impact of shocks to speculators' beliefs. This accords with Athey et al. (2016), who develop a model of user adoption and use of a virtual currency such as Bitcoin in order to analyze how market fundamentals determine the exchange rate of fiat currency to Bitcoin, focussing their attention on an eventual steady state expected exchange rate. They further analyze its usage empirically, exploiting the fact that all individual transactions get recorded on Bitcoin's public ledgers. They argue that a large share of transactions is related to illegal activities, thus agreeing with Foley et al. (2018), who investigate this issue in additional detail. Trimborn and Härdle (2016) propose an index called CRIX for the overall cryptocurrency market. Catallini and Gans (2016) provide "some simple economics of the blockchain", a key technological component of Bitcoin, but which has much broader usages. Schnabel and Shin (2018) draw lessons from monetary history regarding the role of banks in establishing trust and current debates about cryptocurrencies. Bias et al (2018) as well as Cong and He (2018) examine the role of the blockchain technology, a key component of the Bitcoin technology, for "smart contracts". The most closely related contribution in the literature to our paper is Garratt-Wallace (2017), as we discussed at the end of the introduction.

It is hard not to think of bubbles in the context of Bitcoin. There is a large literature on bubbles, that should prove useful in that regard. In the original analysis of Samuelson (1958), money is a bubble, as it is intrinsically worthless. We share that perspective here for both the Dollar and the Bitcoin. It might be tempting to think that prices for Bitcoin could rise forever, as agents speculate to receive even higher prices in the future. Tirole (1982) has shown that this is ruled out in an economy with infinite-lived, rational agents, a perspective which we share, whereas Burnside-Eichenbaum-Rebelo (2015) have analyzed how bubbles may arise from agents catching the "disease" of being overly optimistic. Our model shares some similarity with the bubbles perspective in Scheinkman-Xiong (2003), where a bubble component for an asset arises due to a sequence of agents, each valuing the asset for intermittent periods. Guerrieri-Uhlig (2016) provides some overview of the bubble literature. The Bitcoin price evolution can also be thought about in the context of currency speculation and carry trades, analyzed e.g. by Burnside-Eichenbaum-Rebelo (2012): the three perspectives given there may well be relevant to thinking about the Bitcoin price evolution, but we have refrained from pursuing that here.

B Proofs

Proof. [Lemma 1] Let $\underline{D}_{\infty,g} = \liminf_{t\to\infty} D_{t,g}$. It is clear, that $\underline{D}_{\infty,g} = 0$. By assumption, it cannot undercut zero. Also, it cannot be strictly positive, since otherwise, a green agent could improve his utility per spending $\underline{D}_{\infty,g}$ on consumption goods in some even period, without adjusting anything else except reducing Dollar holdings subsequently by $\underline{D}_{\infty,g}$ in all periods. Note that Dollar holdings for green agents in odd periods are never higher than the Dollar holdings in the previous even period since at best, they can choose not to spend any Dollars in the even periods. Consider then some odd period, such that $D_{t+1,g} > 0$, i.e. suppose the green agent has not spent all her Dollars in the previous even period t. Given θ^t, the agent can then increase his consumption in t at the cost of reducing his consumption in $t+2$, for a marginal utility gain of

$$\beta^t \left(u'(c_t) - \beta^2 E_t \left[u'(c_{t+2}) \, \frac{P_t}{P_{t+2}} \right] \right) \tag{71}$$

$$= \beta^t \left(u'(c_t) - \beta^2 E_t \left[u'(c_{t+2}) \, \frac{P_t}{P_{t+1}} \frac{P_{t+1}}{P_{t+2}} \right] \right). \tag{72}$$

This gain is strictly positive, since $c_t = y_t$ in all periods, and per assumption 1 and 2. For red agents, this argument likewise works for all even periods $t \geq 2$. □

Proof. [Lemma 2] Assume, $t+1$ is even. The Dollar-denominated consumption market clearing condition implies

$$D_{t+1} = D_{t+1,g} + D_{t+1,r} = D_{t+1,g} = P_t z_t + \tau_{t+1}, \tag{73}$$

where we used $D_{t+1,r} = 0 = D_{t,g}$. If $t+1$ is odd, then analogously $D_{t+1,g} = 0 = D_{t,r}$. The evolution of the amount of Dollar is given as

$$D_{t+1} = D_t + \tau_{t+1}. \tag{74}$$

Comparing (73) and (74), we have

$$D_t = P_t \, z_t. \tag{75}$$

Likewise, $D_{t+1} = P_{t+1} z_{t+1}$. Plugging $D_{t+1} = P_{t+1} \, z_{t+1}$ into (73) and using that equation for t rather than $t+1$ delivers

$$\tau_t = P_t \, z_t - P_{t-1} \, z_{t-1}. \tag{76}$$

□

Proof. [Proposition 1] If $x_t > 0$ and $z_t > 0$, selling agents at time t must be marginally indifferent between accepting Dollars and accepting Bitcoins. If they sell one marginal unit of the consumption good for Dollars, they receive P_t Dollar with which they can buy $\frac{P_t}{P_{t+1}}$ units of the consumption good at date $t+1$ and evaluating the extra consumption at the marginal utility $u'(c_{t+1})$. If they sell one marginal unit of the consumption good for Bitcoin, they receive (P_t/Q_t) Bitcoins and can thus buy $(P_t/Q_t)\cdot(Q_{t+1}/P_{t+1})$ units of the consumption good at date $t+1$, evaluating the extra consumption at the marginal utility $u'(c_{t+1})$. Indifference implies (40). □

Proof. [Proposition 2] Market clearing implies that demand equals supply in the Bitcoin-denominated consumption market. Therefore, $b_t < (Q_t/P_t)B_t$ implies that buyers choose not to use some of their Bitcoins in purchasing consumption goods. For a (marginal) Bitcoin, they could obtain Q_t/P_t units of the consumption good, evaluated at marginal utility $u'(c_t)$ at time t. Instead, they weakly prefer to hold on to the Bitcoin. The earliest period, at which they can contemplate purchasing goods is $t+2$, where they would then obtain Q_{t+2}/P_{t+2} units of the consumption good, evaluated at marginal utility $u'(c_{t+2})$, discounted with β^2 to time t. As this is the weakly better option, equation (43) results. If good buyers use Bitcoins both for purchases as well as for speculative reasons, both uses of the Bitcoin must generate equal utility, giving rise to equality in (43). □

Lemma 3. (Zero-Bitcoin-Transactions Condition:)
Suppose that $B_t > 0$, $Q_t > 0$, $z_t > 0$ and that there is absence of goods transactions against Bitcoins $x_t = b_t = 0$ at date t. Then

$$E_t\left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right] \geq E_t\left[u'(c_{t+1})\frac{(Q_{t+1}/P_{t+1})}{(Q_t/P_t)}\right]. \tag{77}$$

If consumption and production is constant at t and $t+1$, i.e. if $c_t = c_{t+1} \equiv \bar{y} = \underline{y}$, and if Q_{t+1} and $\frac{1}{\pi_{t+1}}$ are uncorrelated conditional on time-t information, absence of goods transactions against Bitcoins at date t implies

$$Q_t \geq \mathbb{E}_t\left[Q_{t+1}\right]. \tag{78}$$

Proof. If $x_t = b_t = 0$, it must be the case, that sellers do not seek to sell positive amounts of goods against Bitcoin at the current price in Bitcoin Q_t, and at least weakly prefer to sell using Dollars instead. This gives rise to equation (77). □

Proof. [Corrolary 1)] With theorem 1, the fundamental pricing equation, i.e. proposition 1 and equation (40) always applies in equilibrium. Equation (40) implies equation (47), which in turn implies (49). □

Lemma 4. *Suppose ϵ_t satisfies $E_{t-1}[\epsilon_t] = 0$ for all $t \geq 1$ and satisfies equation (93). Suppose that $E_t[m_{t+1}]$ are bounded from below by some strictly positive number and that the conditional variances $\sigma_{m_{t+1}|t}$ are bounded from above. Then,*

$$\psi := \sum_{t=0}^{\infty} \left| \frac{cov_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} \right| < \infty. \tag{79}$$

Proof. By (94), the sum of the conditional standard deviations of ϵ_t is bounded above by some finite $\tilde{\zeta}$,

$$\sum_{t=0}^{\infty} \sigma_{\epsilon_{t+1}|t} \leq \tilde{\zeta}. \tag{80}$$

Let $\underline{m}$ be a lower bound for the sequence $\{E_t[m_{t+1}]\}_{t\geq 0}$ and let $\bar{\sigma}_m$ be an upper bound for the conditional standard deviations of m_t. Note that

$$\begin{aligned} \psi &= \sum_{t=0}^{\infty} \frac{|\text{corr}_t(m_{t+1}, \epsilon_{t+1})|\, \bar{\sigma}_m\, \sigma_{\epsilon_{t+1}}}{|E_t[m_{t+1}]|} \\ &\leq \sum_{t=0}^{\infty} \frac{\bar{\sigma}_m}{\underline{m}} \sigma_{\epsilon_{t+1}|t} \\ &\leq \frac{\bar{\sigma}_m}{\underline{m}} \tilde{\zeta}, \end{aligned}$$

by $\text{corr}_t(m_{t+1}, \epsilon_{t+1}) \in (-1, 1)$ for all t. □

Proof. [Proposition 3] Assume $\pi_t \geq \underline{\pi}$ for all $t \geq 0$ and some $\underline{\pi} > 1$. Assume

$cov_t(u'(c_{t+1}), \frac{Q_{t+1}}{P_{t+1}}) \geq 0$. Then, with equations (40) and (77),

$$\frac{Q_t}{P_t} \geq \frac{E_t[u'(c_{t+1})\,\frac{Q_{t+1}}{P_{t+1}}]}{E_t[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}]} \tag{81}$$

$$\geq \frac{E_t[u'(c_{t+1})\,\frac{Q_{t+1}}{P_{t+1}}]}{E_t[u'(c_{t+1})]\,\frac{1}{\underline{\pi}}} \tag{82}$$

$$= \underline{\pi}\,\frac{cov_t(u'(c_{t+1}), \frac{Q_{t+1}}{P_{t+1}}) + E_t[u'(c_{t+1})]\,E_t[\frac{Q_{t+1}}{P_{t+1}}]}{E_t[u'(c_{t+1})]} \tag{83}$$

$$= \underline{\pi}\,\left(\frac{cov_t(u'(c_{t+1}), \frac{Q_{t+1}}{P_{t+1}})}{E_t[u'(c_{t+1})]} + E_t\left[\frac{Q_{t+1}}{P_{t+1}}\right]\right) \tag{84}$$

$$\geq \underline{\pi}\; E_t\left[\frac{Q_{t+1}}{P_{t+1}}\right]. \tag{85}$$

Writing this equation in $t = 0$ and iterating yields

$$\frac{Q_0}{P_0} \geq \underline{\pi} E_0\left[\frac{Q_1}{P_1}\right] \geq \underline{\pi}^2 E_0\left[E_1\left[\frac{Q_2}{P_2}\right]\right] \geq \cdots \geq \underline{\pi}^t E_0\left[E_1\left[\ldots E_{t-1}\left[\frac{Q_t}{P_t}\right]\right]\right]. \tag{86}$$

By the law of iterated expectations, find

$$E_0\left[\frac{Q_t}{P_t}B_t\right] \leq E_0\left[\frac{Q_t}{P_t}\right]\bar{B} \leq \frac{Q_0}{P_0}\bar{B}\underline{\pi}^{-t} \to 0 \;\text{ for } t \to \infty,$$

demonstrating convergence in mean. □

Proof. [Theorem 2] Per equation (39) in Lemma 2, we have

$$\tau_t = P_t z_t - P_{t-1} z_{t-1} \tag{87}$$

$$\tau'_t = P_t z'_t - P_{t-1} z'_{t-1} \tag{88}$$

Since all Bitcoins are spent,

$$x_t = \frac{Q_t}{P_t} B_t$$

$$x'_t = \frac{Q_t}{P_t} B'_t$$

Use

$$\begin{aligned} z_t &= y_t - x_t \\ z'_t &= y_t - x'_t \end{aligned}$$

and plug the formulas for z_t and z'_t and their lags into the two equations (87) and (88), substituting out $x_t, x'_t, x_{t-1}, x'_{t-1}$. One obtains

$$\begin{aligned} \tau_t &= P_t y_t - Q_t B_t - P_{t-1} y_{t-1} + Q_{t-1} B_{t-1} \\ \tau'_t &= P_t y_t - Q_t B'_t - P_{t-1} y_{t-1} + Q_{t-1} B'_{t-1} \end{aligned}$$

Taking the difference,

$$\begin{aligned} \tau'_t - \tau_t &= -Q_t(B'_t - B_t) + Q_{t-1}(B'_{t-1} - B_{t-1}) \\ &= -(Q_t - Q_{t-1})(B'_t - B_t) - Q_{t-1}(B'_t - B_t) + Q_{t-1}(B'_{t-1} - B_{t-1}) \\ &= -(Q_t - Q_{t-1})(B'_t - B_t) - Q_{t-1}((B'_t - B'_{t-1}) - (B_t - B_{t-1})) \end{aligned}$$

The condition $0 < B'_t < (P_t/Q_t)y_t$ implies that $z_t > 0$, i.e. that the resulting trades remain compatible with a no-speculation equilibrium and spending all Bitcoins every period. □

Proof. [Corollary 3] Per assumption 4, the central bank regards P_t^*, Q_t, Q_t^* in (60) as given. Minimizing the loss over P_t results in $P_t = P_t^*$. This outcome can be achieved per $D_t = y_t P_t - Q_t B_t$, and is the only outcome compatible with that choice for D_t. □

Proof. [Corollary 4] Per assumption 4, the central bank regards P_t^*, P_t, Q_t^* in (60) as given. Minimizing the loss over Q_t results in $Q_t = Q_t^*$. This outcome can be achieved per $D_t = y_t P_t - Q_t^* B_t$, and is the only outcome compatible with that choice for D_t. □

Proof. [Proposition 4] Providing effort causes disutility of $h'(e_t)$ at time t at the margin. Likewise and at the margin, effort generates $A_t/\bar{e}_t$ Bitcoins in t which can be traded in $t+1$. A Bitcoin is worth Q_{t+1}/P_{t+1} units of the consumption good at time $t+1$, to be evaluated at marginal utility $u'(c_{t+1})$. In equilibrium $c_{t+1} = y_{t+1}$ and $e_{t,j} = \bar{e}_t$. Equating equilibrium mining disutility to the equilibrium payoff gives rise to condition (68). Note that the right hand side diverges to infinity, as $\bar{e}_t \to 0$ and converges to zero, as $\bar{e}_t \to \infty$, while $h'(\bar{e}_t)$ is always strictly positive except for perhaps $h'(0) = 0$. Both sides are continuous functions in $\bar{e}_t$. Therefore, a solution always exists and is strictly positive. Since the right hand side is a strictly decreasing function of $\bar{e}_t$, while the left hand side is a weakly increasing function of $\bar{e}_t$, the solution is unique. $\square$

Proof. [Proposition 5] Recall that aggregate Bitcoin production is assumed to be an exogenous and deterministic function of time. Therefore all equations in the no-tax equilibrium continue to hold, if the tax is imposed except for equation (68). Compared to that equation, the left hand side is shifted up in equation (69) and still weakly increasing in $h'(\bar{e}_t)$, while the right hand side is the same and strictly decreasing in $\bar{e}_t$. Therefore, individual effort levels $e_{t,j} = \bar{e}_t$ are strictly lower in the equilibrium with taxation. Welfare is therefore strictly higher, per the analysis in subsection 6.1.

C Equilibrium Construction

C.1 Equilibrium Existence: A Constructive Approach

We seek to show the existence of equilibria and examine numerical examples. The challenge in doing so lies in the zero-dividend properties of currencies. In asset pricing, one usually proceeds from a dividend process D_t, exploits an asset pricing formula $Q_t = D_t + E_t[M_{t+1}Q_{t+1}]$ and "telescopes" out the right hand side in order to write Q_t as an infinite sum of future dividends, discounted by stochastic discount factors. Properties of fundamentals such as correlations of dividends D_t with the stochastic discount factor then imply correlation properties of the price Q_t and the stochastic discount factor. This approach will not work here for equilibria with nonzero Bitcoin prices, since dividends of fiat currencies are identical to zero. Something else must generate the current Bitcoin price and the correlations. We examine this issue as well as demonstrate existence of equilibria per constructing no-Bitcoin-speculation equilibria explicitly. The next proposition reduces the task of constructing no-Bitcoin-speculation equilibra to the task of constructing sequences for (m_t, P_t, Q_t) satisfying particular properties.

Proposition 6. (Equilibrium Existence and Characterization:)

1. *Every equilibrium which satisfies assumptions 1 and 3 generates a stochastic*

sequence $\{(m_t, P_t, Q_t)\}_{t\geq 0}$ *which satisfy equation (47) and*

$$\beta E_t \left[\frac{m_{t+1}}{m_t} \frac{P_{t+1}}{P_t} \right] < 1 \qquad \textit{for all } t. \tag{89}$$

2. *Conversely, let* $0 < \beta < 1$*.*

   (a) *There exists a strictly positive* (θ_t)*-adapted sequence* $\{(m_t, P_t, Q_t)\}_{t\geq 0}$ *satisfying assumption 1 as well as equations (47) and (89) such that the sequences* $\{Q_t/P_t\}_{t\geq 0}$ *and* $\{P_t m_t\}_{t\geq 0}$ *are bounded from above and that* $\{P_t m_t\}_{t\geq 0}$ *is bounded from below by a strictly positive number.*

   (b) *Let* $\{(m_t, P_t, Q_t)\}_{t\geq 0}$ *be a sequence with these properties. Let* $u(\cdot)$ *be an arbitrary utility function satisfying the Inada conditions, i.e. it is twice differentiable, strictly increasing, continuous, strictly concave,* $\lim_{c\to 0} u'(c) = \infty$ *and* $\lim_{c\to\infty} u'(c) = 0$*. Then, there exists* $\bar{b}_0 > 0$*, such that for every initial real value* $b_0 \in [0, \bar{b}_0]$ *of period-0 Bitcoin spending, there exists a no-Bitcoin-speculation equilibrium which generates the stochastic sequence* $\{(m_t, P_t, Q_t)\}_{t\geq 0}$ *and satisfies* $m_t = u'(c_t)/P_t$*.*

Proof. [Proposition 6]

1. For part 1 of the proposition, consider an equilibrium satisfying assumptions 1 and 3. Theorem 1 implies, that there will be no Bitcoin speculation, and that therefore equation (47) holds. Equation (89) follows directly from equation (45), the definition of m_t and the equilibrium condition $c_t = y_t$.

2. (a) This is trivially true for the sequence $(m_t, P_t, Q_t) \equiv (1, 1, 1)$ for all t.

   (b) Fix the sequence $\{(m_t, P_t, Q_t)\}_{t\geq 0}$ with the properties mentioned in (a), that is assumption 1 and equations (47) and (89) hold. Further, there exist bounds $\mu, \upsilon, \Upsilon > 0$ such that $0 < Q_t/P_t < \mu$ and $0 < \upsilon < P_t m_t < \Upsilon$ for all t.

   Let $u(\cdot)$ an arbitrary, twice differentiable, strictly increasing, concave utility function. Pick $\bar{b}_0$ as the solution to the equation

$$u'\left(\frac{P_0}{Q_0}\mu\bar{b}_0\right) = \Upsilon. \tag{90}$$

Note, $\bar{b}_0 > 0$ is well-defined since $u'(\cdot)$ is invertible and since $\frac{P_0}{Q_0}\mu, \Upsilon > 0$. Let $f(\cdot)$ be the unique inverse of u', i.e. $f(u'(c)) = c$ for all $c > 0$. Define the sequence $\{c_t\}_{t\geq 0} \equiv \{y_t\}_{t\geq 0} := \{f(P_t m_t)\}_{t\geq 0}$. Note, the choice of utility function pins down the consumption sequence. Observe that $y_t \in [\underline{y}, \bar{y}]$ for all t, where $\underline{y} = f(\Upsilon)$, $\bar{y} = f(\upsilon)$ since u' and thus f are decreasing. Also, $\{c_t\}$ and $\{y_t\}$ are θ_t-adapted. Since (89) holds by assumption for all t and since we defined $y_t = c_t$ for all t, assumption (3) is satisfied. Given $b_0 \in [0, \bar{b}_0]$, let $B_0 := (P_0/Q_0)b_0$ be the initial quantity of Bitcoins resulting in the real quantity b_0 of spending in Bitcoins, if all Bitcoins are spent. Note that by (90),

$$0 \leq B_0 \leq \underline{y}/\mu. \tag{91}$$

Pick a disutility-of-effort function such that Bitcoins are never produced, see the appendix for details. Therefore, the quantity of Bitcoins B_t stays constant at $B_t \equiv B_0$. Note that by (91), and the existence of the upper bound μ, the real value of Bitcoins is always strictly below the total value of output,

$$(Q_t/P_t)B_t < \mu B_t \leq \underline{y} \leq y_t. \tag{92}$$

Solve for the quantity of dollars $D_t = P_t y_t - Q_t B_t > 0$ and thus the monetary transfers $\tau_t = D_t - D_{t-1}$. The remaining quantities follow from the equilibrium definition in a straightforward manner and by this, it is clear that the resulting sequences constitute an equilibrium. Since assumptions 1 and 3 are satisfied, the no-Bitcoin-speculation property holds per theorem 1.

□

Part 2b of the proposition implies a version of the Kareken-Wallace (1981) result that the initial exchange rate Q_0 between Bitcoin and Dollar is not determined. The proposition furthermore relates to proposition 3.2 in Manuelli-Peck (1990). Part 2b reduces the challenge of constructing equilibria to the task of constructing (θ_t)-adapted sequences $\{(m_t, P_t, Q_t)\}$ satisfying the properties named in 2a. This feature can be exploited for constructing equilibria with further properties as follows. Suppose we are already given strictly positive and (θ_t)-adapted sequences for m_t and P_t, satisfying assumption 1 as well as equation (89) such that $m_t P_t$ is bounded from above and below by strictly positive numbers. Suppose, additionally, that P_t as well as $E_t[m_{t+1}]$ are bounded from below by some strictly positive number and that the conditional variances $\sigma_{m_{t+1}|t}$ are bounded from above. For example, $m_t \equiv 1$ and $P_t \equiv 1$ will work. Then, we can show how to construct a sequence for Q_t such that part 2b of the Proposition applies:

Pick a sequence of random shocks[16] $\epsilon_t = \epsilon(\theta^t)$, such that $E_{t-1}[\epsilon_t] = 0$ and such that both the infinite sum of its absolute values and the sum of its standard deviations are bounded by some real number $0 < \zeta, \tilde{\zeta} < \infty$,

$$\sum_{t=0}^{\infty} \mid \epsilon_t \mid \leq \zeta \text{ a.s.} \tag{93}$$

$$\sum_{t=0}^{\infty} \sigma_{\epsilon_t} \leq \tilde{\zeta}. \tag{94}$$

Pick an initial Bitcoin price Q_0 satisfying

$$Q_0 > \zeta + \sum_{t=0}^{\infty} \frac{\text{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]}. \tag{95}$$

This choice guarantees that the entire price sequence of $\{Q_t\}$ we are about to generate is strictly positive. Lemma 4 in the appendix shows that the right hand side of (95) is smaller than infinity. Therefore, a finite Q_0 satisfying (95) can always be found. Recursively calculate the sequence Q_t per

$$Q_{t+1} = Q_t + \epsilon_{t+1} - \frac{\text{cov}_t(\epsilon_{t+1}, m_{t+1})}{\mathbb{E}_t[m_{t+1}]}. \tag{96}$$

The initial condition (95) implies that $Q_t > 0$ for all t. With Lemma 4, and iterating backwards via (96) we have

$$\begin{aligned} Q_t &= Q_0 + \sum_{s=1}^{t} \epsilon_s + \sum_{s=1}^{t} \frac{\text{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} && (97) \\ &< Q_0 + \sum_{s=1}^{\infty} \mid \epsilon_s \mid + \sum_{s=1}^{\infty} \mid \frac{\text{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} \mid < \infty. && (98) \end{aligned}$$

[16]Note that θ^t encodes the date t per the length of the vector θ^t. Therefore, we are formally allowed to change the distributions of the ϵ_t as a function of the date as well as the past history.

By Lemma 4 and (93). Therefore, Q_t is bounded from above. By assumption, P_t is bounded from below by a strictly positive number. Thus, it follows that Q_t/P_t is bounded from above. Since the conditional covariance of m_{t+1} and ϵ_{t+1} equals the conditional covariance of m_{t+1} and Q_{t+1}, equation (47) is now satisfied by construction. Thus, we arrived at a strictly positive (θ_t)-adapted sequence (m_t, P_t, Q_t) satisfying assumption 1 as well as equations (47) and (89) such that the sequences Q_t/P_t and $P_t m_t$ are bounded. Part 2(b) of proposition 6 shows how to obtain a no-Bitcoin-speculation equilibrium with these sequences.

It is also clear, that this construction is fairly general. In any equilibrium, let

$$\epsilon_t = Q_t - E_{t-1}[Q_t] \tag{99}$$

be the one-step ahead prediction error for the Bitcoin price Q_t. Then, equation (47) is equivalent to equation (96). The restrictions above concern just the various boundedness properties, which we imposed.

C.2 Equilibrium: Examples

For more specific examples, suppose that $\theta_t \in \{L, H\}$, realizing each value with probability 1/2. Pick some utility function $u(\cdot)$ satisfying the Inada conditions. For a first scenario, suppose that inflation is constant $P_t = \bar{\pi} P_{t-1}$ for some $\bar{\pi} \geq 1$ and that consumption is iid, $c(\theta^t) = c_{\theta_t} \in \{c_L, c_H\}$ with $0 < c_L \leq c_H$ and such that $u'(c_H) > \beta(u'(c_L) + u'(c_H))/2$. For a second scenario, suppose that inflation is iid, $P_t/P_{t-1} = \pi_{\theta_t} \in \{\pi_L, \pi_H\}$, with $1 \leq \pi_L \leq \pi_H$ and that consumption is constant $c_t \equiv \bar{c} > 0$. It is easy to check that (89) is satisfied in both scenarios for $m_t = u'(c_t)/P_t$. For both scenarios, consider two cases for $\epsilon(\theta^t) = \epsilon_t(\theta_t)$,

Case A: $\epsilon_t(L) = 2^{-t}$, $\epsilon_t(H) = -2^{-t}$.

Case B: $\epsilon_t(L) = -2^{-t}$, $\epsilon_t(H) = 2^{-t}$.

We assume that the distribution for ϵ_{t+1} is known is one period in advance, i.e., in period t, agents know, whether ϵ_{t+1} is distributed as described in "case A" or as described in "case B". Expressed formally, define an indicator ι_t and let it take the value $\iota_t = 1$, if we are in case A in $t+1$, and $\iota_t = -1$, if we are in case B in $t+1$: we assume that ι_t is adapted to (θ_t). The absolute value of the sum of the ϵ_t is bounded by $\xi = 2$ which holds by exploiting the geometric sum. For the first scenario, calculate

$$\frac{\mathrm{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} = 2^{-(t+1)} \frac{u'(c_L) - u'(c_H)}{u'(c_L) + u'(c_H)} \iota_t \tag{100}$$

which is positive for $\iota_t = 1$ and $c_L < c_H$ but negative for $\iota_t = -1$. For the second scenario, likewise calculate

$$\frac{\mathrm{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} = 2^{-(t+1)} \frac{\frac{1}{\pi_L} - \frac{1}{\pi_H}}{\frac{1}{\pi_L} + \frac{1}{\pi_H}} \iota_t \tag{101}$$

which is positive for $\iota_t = 1$ and $\pi_L < \pi_H$ but negative for $\iota_t = -1$. With equation (95), pick

$$Q_0 > 2 + \frac{u'(c_L) - u'(c_H)}{u'(c_L) + u'(c_H)}$$

for scenario 1 and

$$Q_0 > 2 + \frac{\frac{1}{\pi_L} - \frac{1}{\pi_H}}{\frac{1}{\pi_L} + \frac{1}{\pi_H}}$$

for scenario 2. Consider three constructions,

Always A: Always impose case A, i.e. $\epsilon_t(L) = 2^{-t}$, $\epsilon_t(H) = -2^{-t}$.

Always B: Always impose case B, i.e. $\epsilon_t(L) = -2^{-t}$, $\epsilon_t(H) = 2^{-t}$.

Alternate: In even periods, impose case A, i.e. $\epsilon_t(L) = 2^{-t}$, $\epsilon_t(H) = -2^{-t}$. In odd periods, impose case B, i.e. $\epsilon_t(L) = -2^{-t}$, $\epsilon_t(H) = 2^{-t}$.

For each of these, calculate the Q_t sequence with equation (96) and the resulting equilibrium with proposition 6. As third scenario, if both consumption and inflation are constant, then all three constructions result in a martingale for $Q_t = E_t[Q_{t+1}]$. Suppose that $c_L < c_H$ in scenario 1 or $\pi_L < \pi_H$ in scenario 2, i.e. suppose we have nontrivial randomness of the underlying processes in either scenario. The "Always A" construction results in $Q_t > E_t[Q_{t+1}]$ and Q_t is a supermartingale. This can be seen by plugging in (100) respectively (101) into equation

$$E_t[Q_{t+1}] = Q_t + E_t[\epsilon_{t+1}] - \frac{cov(\epsilon_{t+1}, m_{t+1})}{E_t[m_{t+1}]}, \tag{102}$$

where $E_t[\epsilon_{t+1}] = 0$ by construction. The "Always B" construction results in a submartingale $Q_t < E_t[Q_{t+1}]$. The "Alternate" construction results in a price process that is neither a supermartingale nor a submartingale.

These examples were meant to illustrate the possibility, that supermartingales, submartingales as well as mixed constructions can all arise, starting from the same assumptions about the fundamentals. To get somewhat closer to that, the following construction may help. Once again, let $\theta_t \in \{L, H\}$, but assume now that $P(\theta_t = L) = p < 0.5$. Suppose that $P_t \equiv 1$ and $c_t \equiv \bar{c}$, so that m_t is constant and that Q_t must be a martingale. Pick some $\underline{Q} \geq 0$ as well as some $Q^* > \underline{Q}$. Pick some $Q_0 \in [\underline{Q}, Q^*]$. If $Q_t < Q^*$, let

$$Q_{t+1} = \begin{cases} \frac{Q_t - p\underline{Q}}{1-p} & \text{if } \theta_t = H, \\ \underline{Q} & \text{if } \theta_t = L. \end{cases}$$

If $Q_t \geq Q^*$, let $Q_{t+1} = Q_t$. Therefore Q_t will be a martingale and satisfies (47). If Q_0 is sufficiently far above $\underline{Q}$ and if p is reasonably small, then typical sample paths will feature a reasonably quickly rising Bitcoin price Q_t, which crashes eventually to $\underline{Q}$ and stays there, unless it reaches the upper bound Q^* first. Further modifications of this example can generated generate repeated sequences of rising prices and crashes.

D The No-Bitcoin-Speculation Theorem: A Slight Generalization

Note that equation (45) compares marginal utilities of red agents and green agents. For an interpretation, consider the problem of a social planner, assigning equal welfare weights to both types of agents. Suppose that this social planner is given an additional marginal unit of the consumption good at time t, which she could provide to the agent consuming in period t or to costlessly store this unit for one period and to provide it to the agent consuming in period $t+1$. Condition (45) then says that the social planner would always prefer to provide the additional marginal unit to the agent consuming in period t. This interpretation suggests the following generalization of assumption 3, resulting from distinct welfare weights, implying a slight generalization of our No-Bitcoin-Speculation Theorem.

Assumption A. 6. *Let $\alpha > 0$. For all even t*

$$u'(y_t) - \alpha\beta E_t[u'(y_{t+1})] > 0, \tag{103}$$

while for all odd t

$$\alpha u'(y_t) - \beta E_t[u'(y_{t+1})] > 0. \tag{104}$$

For $\alpha = 1$, one obtains assumption 3. The assumption above arises, when considering welfare weights of λ on green agents and $1-\lambda$ on red agents, where $\lambda = 1/(1+\alpha)$, see also subsection 6.1.

Theorem 4. (No-Bitcoin-Speculation Generalized.) *Suppose that $B_t > 0$ and $Q_t > 0$ for all t. Impose assumption 6. Then in every period, all Bitcoins are spent.*

Proof. [Theorem 4] The proof closely parallels the proof of theorem 1. Since all Dollars are spent in all periods, we have $z_t > 0$ in all periods. Observe that then either inequality (77) holds, in case no Bitcoins are spent at date t, or equation (40) holds, if some Bitcoins are spent. Since equation (40) implies inequality (77), (77) holds for all t. Suppose first that t is an even period. Then

$$\begin{aligned}
\beta^2 \mathbb{E}_t[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}] &= \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}\right]\right] && \text{(law of iterated expectation)}\\
&\leq \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{P_{t+1}}{P_{t+2}}\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per equ. (77) at } t+1)\\
&\leq \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 1)}\\
&< \alpha\beta \mathbb{E}_t\left[u'(c_{t+1})\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 6 in t+1)}\\
&\leq \alpha\beta \mathbb{E}_t\left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right]\,\frac{Q_t}{P_t} && \text{(per equ. (77) at } t)\\
&\leq \alpha\beta \mathbb{E}_t\left[u'(c_{t+1})\right]\,\frac{Q_t}{P_t} && \text{(per ass. 1)}\\
&< u'(c_t)\,\frac{Q_t}{P_t} && \text{(per ass. 6 in t).}
\end{aligned}$$

which contradicts the speculative price bound (43) in t. Consequently, $b_t = \frac{Q_t}{P_t} B_t$, i.e. all Bitcoins are spent in t. The same calculations obtain, if t is an odd period, per replacing α with $1/\alpha$ in the equations above. Since t is either even or odd, all Bitcoins are spent in every period. $\square$

E Implications of the Monetary Policy Scenarios

E.1 Conventional Monetary Policy Scenario

If one were to use a vector autoregression to estimate the impact of monetary policy shocks in this economy (or, more precisely, a linearized version thereof), one might wish to order the observable stochastic variables as (y_t, Q_t, P_t, D_t). The VAR is then a vector of four equations. A Cholesky decomposition of the covariance matrix of the one-step ahead prediction errors would reveal an identity for the forth equation. Put differently, the innovation in the Dollar quantity ordered last is always identical to zero, and would not serve well for identifying the monetary policy shock (unless one wishes to state, that it is always zero indeed). A more fruitful interpretation might be to instead regard $P_t - \bar{P}_t$ as the monetary policy shock, and identify it as the third shock in this Cholesky decomposition.

E.2 Unconventional Monetary Policy Scenario

If one were to use a four-variable VAR (as already described above) to estimate the impact of monetary policy shocks in this economy, one might now wish to order the observable stochastic variables as (y_t, P_t, Q_t, D_t) instead. A Cholesky decomposition of the covariance matrix of the one-step ahead prediction errors would again result in an identity for the forth equation, and one can now entertain a discussion as to whether the monetary policy shock should be the shock to the second equation interpreting the exogenous movements in P_t as a central bank taste shock, or a shock to the third equation, interpreting P_t as truly exogenous. There is no a priori correct choice here. It now depends on where one sees the exogenous variations coming from.'

The unconventional monetary policy scenario delivers some interesting further implications.

Implication 2. (Bitcoin Price Distribution:)
Suppose that production y_t is iid. with distribution function F, $y_t \sim F$. Assume P_t is predetermined with, $P_t = E_{t-1}[P_t]$, i.e. P_t is known at time t. The distribution G_t of the Bitcoin price conditional on time $t-1$ information and conditional on the realization of the Dollar supply D_t is then given by

$$G_{t|t-1,D_t}(s) = \mathbb{P}(Q_t \le s | t-1, D_t) = F(\frac{B_t\, s + D_t}{P_t}). \tag{105}$$

As a consequence, changes in expected production or production volatility translate directly to changes in the expected Bitcoin price or price volatility. If Bitcoin quantity or Dollar quantity is higher, high Bitcoin price realizations are less likely in the sense of first order stochastic dominance. This holds since $F(\frac{B_t s + D_t}{P_t})$ is increasing in both B_t and D_t.

Intuitively, by setting the Dollar quantity, the central bank can control the Bitcoin price. Further, a growing quantity of Bitcoins calms down the Bitcoin price.

Implication 3. (Bitcoin price and Productivity)
Compare two economies which differ only in terms of their productivity distributions, F_1 vs F_2. Say economy 2 is more productive than economy 1, if the productivity distribution of economy 2 first order stochastically dominates the productivity distribution of economy 1. Then, as economies become more productive, the Bitcoin price is higher in expectation. Assume F_2 first-order stochastically dominates F_1. Let $G_{2,t}$ and $G_{1,t}$ be the resulting distributions for Bitcoin prices. Since the Bitcoin price is positive,

$$\begin{aligned}
\mathbb{E}[Q_{t,2}] &= \int_0^\infty x\, dG_{2,t}(x) \\
&= \int_0^\infty (1 - G_{2,t}(x))\, dx \\
&= \int_0^\infty (1 - F_2(\frac{B_t x + D_t}{P_t}))\, dx \\
&\geq \int_0^\infty (1 - F_1(\frac{B_t x + D_t}{P_t}))\, dx \\
&= \mathbb{E}[Q_{t,1}].
\end{aligned}$$

Note, the application only requires second order stochastic dominance which is implied by first order stochastic dominance.

□