Some simple Bitcoin Economics

Linda Schilling* and Harald Uhlig†

This revision: December 14, 2018

Abstract

In an endowment economy, we analyze coexistence and competition between traditional fiat money (Dollar) and cryptocurrency (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 explicitly construct examples for 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, and Aleh Tsivinski. 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

Cryptocurrencies, in particular Bitcoin, have received a large amount of attention as of late. In a white paper, 'Satoshi Nakamoto' (2008), the developer of Bitcoin, describes Bitcoin as a 'version of electronic cash to allow online payments' to be sent directly from one party to another. The question of whether cryptocurrencies can become a widely accepted means of payment, alternative or parallel to traditional fiat monies such as the Dollar or Euro, concerns researchers, policymakers, and financial institutions alike. The total market capitalization of cryptocurrencies reached nearly 400 Billion U.S. Dollars in December 2018, according to coincodex.com. This is a sizeable amount compared to U.S. base money or M1, which both reached approximately 3600 Billion U.S. Dollars as of July 2018. In the Financial Times on June 18th, 2018, the Bank of International Settlements (BIS) addresses 'unstable value' as one major challenge for cryptocurrencies for becoming a major currency in the long run. The price fluctuations are substantial indeed, see figure 1. The BIS further relates this instability back to the lack of a cryptocurrency central bank. What, indeed, determines the price of cryptocurrencies such as the Bitcoin, how can their fluctuations arise and what are the consequences for monetary policy?

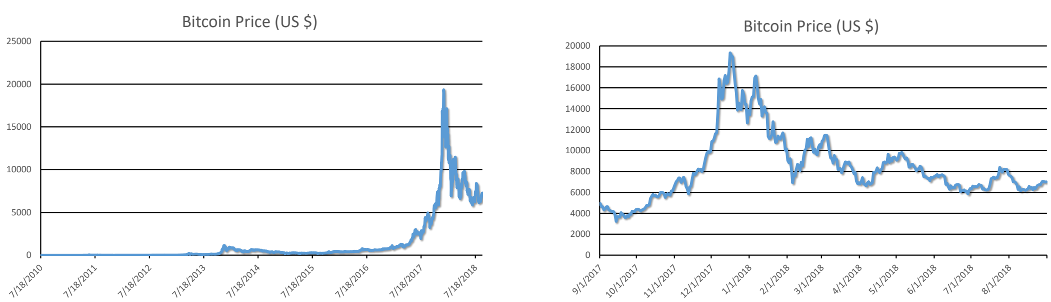

Figure 1: The Bitcoin Price since 2010-07-18 and "zooming in" on one year 2017-09-01 to 2018-08-31. Data per coindesk.com.

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. Our setting, in particular, captures the feature that a central bank controls inflation of traditional fiat money while the value of the cryptocurrency is uncontrolled and its supply can only increase over time. 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 then provides a role for a medium of exchange. We assume that there are two types of intrinsically worthless[1] monies: 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. 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 and examine the consequences for monetary policy and welfare.

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, in case not all Bitcoins are spent on transactions. In 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

[1]This perhaps distinguishes our analysis from a world of Gold competing with Dollars, as Gold in the form of jewelry provides utility to agents on its own.

[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.

dividends, these covariances cannot be constructed from more primitive assumptions about covariances between the pricing kernel and dividends. Proposition 4 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.

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. Armed with that equation, 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. 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. We analyze welfare and optimal monetary policy and examine robustness. Section 6 concludes. Bitcoin production or "mining" is analyzed in appendix B.

Our analysis is related to a substantial body of the literature. 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 4, can perhaps be best thought of as a modern restatement of these classic result. The speculative price bound provided in proposition 2 is a novel feature and does not arise in their analysis, however, as we allow agents to live for infinitely many periods rather than two. As a consequence, in our model, an agent's incentive for currency speculation competes with her incentive to use currency for trade.

The most 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 the 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, 2018a) 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. Budish (2018) argues that the blockchain protocol underlying Bitcoin is vulnerable to attack. 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. 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 is put to produce Bitcoins, see below. The consumption-utility function $u(\cdot)$ is strictly increasing and concave. The utility-loss-from-effort function $h(\cdot)$ is strictly increasing and convex. We assume that both functions are twice differentiable.

Red and green agents alternate in consuming and producing the consumption good, see figure 2: 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 $j \in [1,2]$.

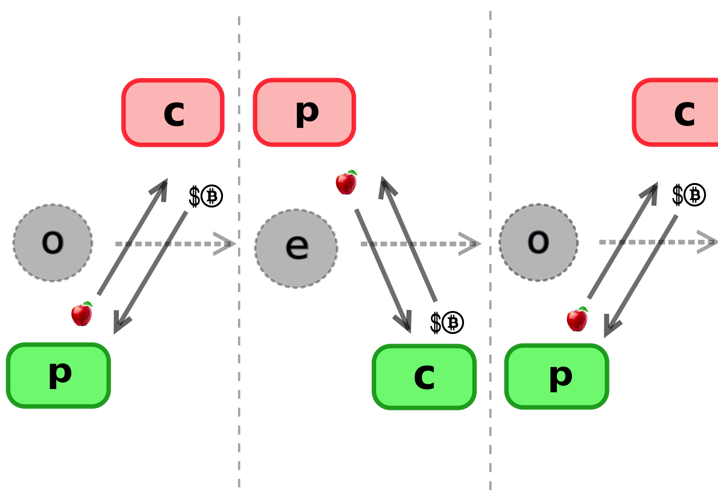

Figure 2: Alternation of production and consumption. In odd periods , green agents produce and red agents consume. In even periods, red agents produce and green agents consume. Alternation and the fact that the consumption good is perishable gives rise to the necessity to trade using fiat money.

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

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

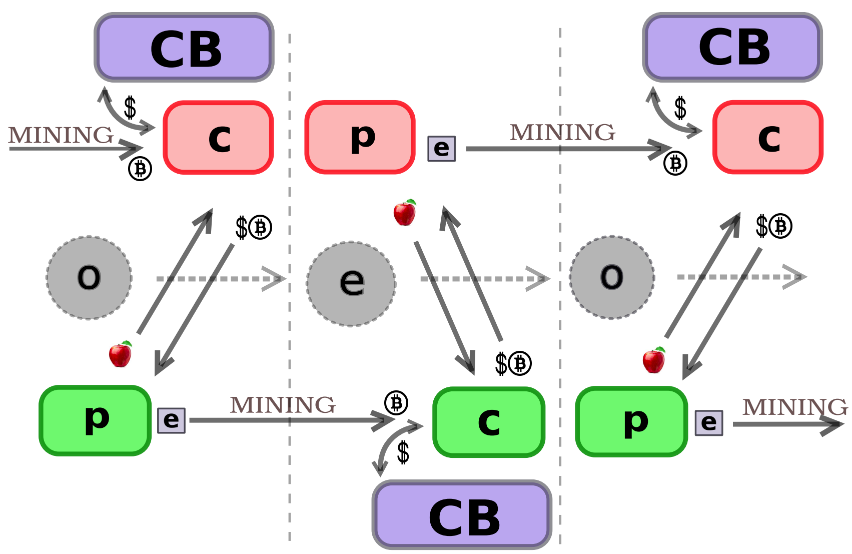

Figure 3: Transfers: In each period, a central bank injects to or withdraws Dollars from agents, before they consume, to target a certain Dollar inflation level. By this, the Dollar supply may increase or decrease. Across periods, agents can put effort to mine Bitcoins. By this, the Bitcoin supply can 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

$$0 \leq \frac{P_t}{Q_t} b_{t,j} \leq B_{t,j} \tag{4}$$

$$0 \leq P_t d_{t,j} \leq D_{t,j} \tag{5}$$

The green agent then consumes

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

and leaves the even period, carrying

$$B_{t+1,j} = B_{t,j} - \frac{P_t}{Q_t} b_{t,j} \geq 0 \tag{7}$$

$$D_{t+1,j} = D_{t,j} - P_t d_{t,j} \geq 0 \tag{8}$$

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. Define the aggregate effort level of one agent group for mining Bitcoin at time t,

$$\bar{e}_t = \int_{j \in [0,1]} e_{t,j} \, dj \tag{9}$$

Then, an individual agent expands effort $e_{t+1,j} \geq 0$ to produce additional Bitcoins according to the production function

$$A_{t+1,j} = f(B_{t+1})\frac{e_{t+1,j}}{\bar{e}_{t+1}} \tag{10}$$

where, as a result, the total number of newly minted coins per period

$$A_{t+1} = \int_{j\in[0,1]} A_{t+1,j}\,dj = f(B_{t+1}) \tag{11}$$

is deterministic, and independent of the aggregate effort level. This modeling choice captures the idea, that in real world, by expanding more effort an individual miner can only increase the likelihood with which she wins the proof-of-work competition. In the aggregate, however, the number of mined blocks increases in deterministic time increments no matter how much hash power (effort) the network provides.[3] Note further, the fraction $\frac{e_{t+1,j}}{\int_{j\in[0,1]} e_{t+1,j}}$ is a probability. Thus, $A_{t+1,j}$ takes the form of an expected value which can be interpreted as individual agents mining in a pool which captures 100% of market share and thus wins the proof-of work competition for sure while individual miners obtain a fraction of the block reward according to their individually excerted effort level, see the appendix in detail.[4]

Further, we assume that the effort productivity function $f(\cdot)$ is nonnegative and decreasing. This specification captures the idea that individual agents can produce Bitcoins at a cost or per "proof-of-work", given by the utility loss $h(e_{t+1,j})$, and that it gets increasingly more difficult to produce additional Bitcoins, as the entire stock of Bitcoins increases. This captures the feature that in the real world, the block reward declines over time. An example is the function

$$f(B) = \max(\bar{B} - B; 0)$$

implying an upper bound for Bitcoin production. An extreme, but convenient case is $B_0 = \bar{B}$, so that no further Bitcoin production takes place. We discuss Bitcoin production further in appendix B. 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 fraction $x_{t+1,j} \geq 0$ sold for Bitcoins and $z_{t+1,j} \geq 0$

[3]This is achieved by regular adaption of the difficulty level of the proof of work competition.
[4]See also Cong, He, and Li (2018).

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

$$\int_{j=0}^{2} b_{t,j} dj = \int_{j=0}^{2} x_{t,j} dj \qquad (12)$$

$$\int_{j=0}^{2} d_{t,j} dj = \int_{j=0}^{2} z_{t,j} dj \qquad (13)$$

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*

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

which is measurable[5] *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 consumption quantities* b_t, c_t, d_t *in even periods and* x_t, z_t, *effort* e_t *and Bitcoin production* A_t *in odd periods as well as individual*

[5] 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}

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

$$U_g = E\left[\sum_{t=0}^{\infty} \beta^t \left(\xi_{t,g} u(c_t) - h(e_t)\right)\right] \tag{14}$$

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

$$\begin{aligned} 0 \leq \frac{P_t}{Q_t} b_t &\leq B_{t,g} && (15)\\ 0 \leq P_t d_t &\leq D_{t,g} && (16)\\ c_t &= b_t + d_t && (17)\\ B_{t+1,g} &= B_{t,g} - \frac{P_t}{Q_t} b_t && (18)\\ D_{t+1,g} &= D_{t,g} - P_t d_t && (19)\end{aligned}$$

in even periods t and

$$\begin{aligned} A_t &= f(B_t)\frac{e_t}{\bar{e}_t}, \text{ with } e_t \geq 0 && (20)\\ y_t &= x_t + z_t && (21)\\ B_{t+1,g} &= A_t + B_{t,g} + \frac{P_t}{Q_t} x_t && (22)\\ D_{t+1,g} &= D_{t,g} + P_t z_t + \tau_{t+1} && (23)\end{aligned}$$

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 consumption quantities b_t, c_t, d_t in odd periods and x_t, z_t, effort e_t and Bitcoin production A_t in even periods as well as individual money holdings $B_{t,r}$, $D_{t,r}$, all non-negative, so as to maximize*

$$U_r = E\left[\sum_{t=0}^{\infty} \beta^t \left(\xi_{t,r} u(c_t) - h(e_t)\right)\right] \tag{24}$$

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

$$
\begin{aligned}
D_{t,r} &= D_{t-1,r} + \tau_t && (25)\\
0 \le \frac{P_t}{Q_t} b_t &\le B_{t,r} && (26)\\
0 \le P_t d_t &\le D_{t,r} && (27)\\
c_t &= b_t + d_t && (28)\\
B_{t+1,r} &= B_{t,r} - \frac{P_t}{Q_t} b_t && (29)\\
D_{t+1,r} &= D_{t,r} - P_t d_t && (30)
\end{aligned}
$$

in odd periods t and

$$
\begin{aligned}
A_t &= f(B_t)\frac{e_t}{\bar{e}_t}, \; \textit{with } e_t \ge 0 && (31)\\
y_t &= x_t + z_t && (32)\\
B_{t+1,r} &= A_t + B_{t,r} + \frac{P_t}{Q_t} x_t && (33)\\
D_{t+1,r} &= D_{t,r} + P_t z_t + \tau_{t+1} && (34)
\end{aligned}
$$

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***:*

$$
\begin{aligned}
\textit{Bitcoin market:} \quad B_t &= B_{t,r} + B_{t,g} && (35)\\
\textit{Dollar market:} \quad D_t &= D_{t,r} + D_{t,g} && (36)\\
\textit{Bitcoin denom. cons. market:} \quad b_t &= x_t && (37)\\
\textit{Dollar denom. cons. market:} \quad d_t &= z_t && (38)\\
\textit{Aggregate effort:} \quad e_t &= \bar{e}_t && (39)
\end{aligned}
$$

3 Analysis

For the analysis, proofs not included in the main text can be found in appendix C. The equilibrium definition quickly generates the following accounting identities. The aggregate, deterministic evolution for the stock of Bitcoins follows from the Bitcoin market clearing condition and the bitcoin production budget constraint,

$$B_{t+1} = B_t + f(B_t) \tag{40}$$

Bitcoin production is analyzed in appendix B. The aggregate evolution for the stock of Dollars follows from the Dollar market clearing constraint and the beginning-of-period transfer of Dollar budget constraint for the agents,

$$D_t = D_{t-1} + \tau_t \tag{41}$$

The two consumption markets as well as the production budget constraint

$$y_t = x_t + z_t$$

delivers that consumption is equal to production[6]

$$c_t = y_t \tag{42}$$

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*

$$\pi_t = \frac{P_t}{P_{t-1}} \geq 1 \tag{43}$$

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.

[6]Note that the analysis here abstracts from price rigidities and unemployment equilibria, which are the hallmarks of Keynesian analysis, and which could be interesting to consider in extensions of the analysis presented here.

Assumption A. 2. *For all t,*

$$u'(y_t) - \beta^2 E_t[u'(y_{t+2})] > 0 \tag{44}$$

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.

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 further, that the across-time insurance motives present in models of the Bewley-Huggett-Aiyagari variety are absent here, see Bewley (1977), Huggett (1993), Aiyagari (1994) and may be tangential to the core issue of Bitcoin pricing.

Note that assumption (44) 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

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

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:)
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

$$E_t\left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right] = E_t\left[u'(c_{t+1})\frac{(Q_{t+1}/P_{t+1})}{(Q_t/P_t)}\right] \tag{45}$$

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*

$$Q_t = \mathbb{E}_t\left[\frac{Q_{t+1}}{\pi_{t+1}}\right] \cdot \mathbb{E}_t\left[\frac{1}{\pi_{t+1}}\right]^{-1} \tag{46}$$

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*

$$Q_t = \mathbb{E}_t\left[Q_{t+1}\right] \tag{47}$$

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

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 empricially problematic to base currency demand on savings decisions without considering interest bearing assets. By contrast, we obtain the indifference condition directly.

Equation (45) can be understood from a standard asset pricing perspective. As a slight and temporary detour for illuminating that connection, consider some extension of the current model, in which the selling agent enjoys date t consumption with utility $v(c_t)$. The agent would have to give up current consumption, marginally valued at $v'(c_t)$ to obtain an asset, yielding a real return R_{t+1} at date $t+1$ for a real unit of consumption invested at date t. Consumption at date $t+1$ is evaluated at the margin with $u'(c_{t+1})$ and discounted back to t with β. The well-known Lucas asset pricing equation then implies that

$$1 = E_t \left[\beta \frac{u'(c_{t+1})}{v'(c_t)} R_{t+1} \right] \tag{48}$$

One such asset are Dollars. They yield the random return of $R_{D,t+1} = \frac{1}{P_{t+1}}$ units of the consumption good in $t+1$ and require an investment of $\frac{1}{P_t}$ consumption goods at t. The asset pricing equation (48) then yields

$$1 = E_t \left[\beta \frac{u'(c_{t+1})}{v'(c_t)} \frac{P_t}{P_{t+1}} \right] \tag{49}$$

Likewise, Bitcoins provide the real return $R_{B,t+1} = \frac{(Q_{t+1}/P_{t+1})}{(Q_t/P_t)}$, resulting in the asset pricing equation

$$1 = E_t \left[\beta \; \frac{u'(c_{t+1})}{v'(c_t)} \frac{(Q_{t+1}/P_{t+1})}{(Q_t/P_t)} \right] \tag{50}$$

One can now solve (50) for $v'(c_t)$ and substitute it into (50), giving rise to equation (45). The difference to the model at hand is the absence of the marginal disutility $v'(c_t)$.

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.

The next proposition establishes properties of the Bitcoin price Q_t, if potential good 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. 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,*

$$u'(c_t) \leq \beta^2 E_t \left[u'(c_{t+2}) \frac{(Q_{t+2}/P_{t+2})}{(Q_t/P_t)} \right] \tag{51}$$

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 good 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.

We also wish to point out the subtlety of the right hand side of equations (45) as well as (51): 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 (51) shows, Bitcoins may be more valuable than indicated by the right hand side of (45) states, if Bitcoins are then entirely kept for speculative reasons. These considerations can be turned into more general versions of (45) as well as (51), 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 three 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

$$E_t\left[Q_{t+1}\right] \leq Q_t \leq \beta^2 E_t\left[Q_{t+2}\,\frac{1}{\pi_{t+2}\,\pi_{t+1}}\right] \tag{52}$$

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,*

$$u'(y_t) - \beta E_t[u'(y_{t+1})] > 0 \tag{53}$$

Note, global impatience is always satisfied for risk-neutral agents if $\beta < 1$. With the law of iterated expectations, it is easy to see that assumption 3 implies assumption 2. Further, assumption 2 implies that (53) cannot be violated two periods in a row.

Note that equation (53) 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 (53) 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 a generalization of assumption 3, resulting from distinct welfare weights. Indeed, the proof of 1 works with such a suitable generalization as well: we analyze this further in the technical 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.[7]

Proof. [Theorem 1] Since all Dollars are spent in all periods, we have $z_t > 0$ in all periods. Observe that then either inequality (88) holds, in case no Bitcoins are spent at date t, or equation (45) holds, if some Bitcoins are spent. Since equation (45) implies inequality (88), (88) holds for all t. Calculate that

$$\begin{aligned}
\beta^2 \mathbb{E}_t[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}] &= \beta^2 \mathbb{E}_t \left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}\right]\right] && \text{(law of iterated expectation)} \\
&\leq \beta^2 \mathbb{E}_t \left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{P_{t+1}}{P_{t+2}}\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per equ. (88) at } t+1\text{)} \\
&\leq \beta^2 \mathbb{E}_t \left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 1)} \\
&< \beta \mathbb{E}_t \left[u'(c_{t+1})\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 3 in t+1)} \\
&\leq \beta \mathbb{E}_t \left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right]\,\frac{Q_t}{P_t} && \text{(per equ. (88) at } t\text{)} \\
&\leq \beta \mathbb{E}_t \left[u'(c_{t+1})\right]\,\frac{Q_t}{P_t} && \text{(per ass. 1)} \\
&< u'(c_t)\,\frac{Q_t}{P_t} && \text{(per ass. 3 in t)}
\end{aligned}$$

which contradicts the speculative price bound (51) 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. □

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.

[7] 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 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. We discuss next Bitcoin pricing implications.

Define the pricing kernel m_t per

$$m_t = \frac{u'(c_t)}{P_t} \tag{54}$$

We can then equivalently rewrite equation (45) as

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

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 $\pi_{t+1} \geq 1$,

$$Q_t = \mathbb{E}_t[Q_{t+1}] + \frac{\mathrm{cov}_t(Q_{t+1}, u'(c_{t+1}))}{\mathbb{E}_t[u'(c_{t+1})]} \tag{56}$$

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

$$Q_t = E_t[Q_{t+1}] + \kappa_t \cdot corr_t\left(\frac{u'(c_{t+1})}{P_{t+1}}, Q_{t+1}\right) \tag{57}$$

where

$$\kappa_t = \frac{\sigma_{\frac{u'(c_{t+1})}{P_{t+1}}|t} \cdot \sigma_{Q_{t+1}|t}}{\mathbb{E}_t[\frac{u'(c_{t+1})}{P_{t+1}}]} > 0 \tag{58}$$

where $\sigma_{\frac{u'(c_{t+1})}{P_{t+1}}|t}$ is the standard deviation of the pricing kernel, $\sigma_{Q_{t+1}|t}$ is the standard deviation of the Bitcoin price and $corr_t(\frac{u'(c_{t+1})}{P_{t+1}}, Q_{t+1})$ is the correlation between the Bitcoin price and the pricing kernel, all conditional on time t information.

Proof. With theorem 1, the fundamental pricing equation, i.e. proposition 1 and equation (45) always applies in equilibrium. Equation (45) implies equation (55), which in turn implies (57). $\square$

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 (46).

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*

$$E_0\left[\frac{Q_t}{P_t}B_t\right] \to 0, \quad as\ t \to \infty \tag{59}$$

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

$$\frac{Q_t}{P_t} = \mathbb{E}_t\left[\frac{Q_{t+1}}{P_{t+1}}\right] \cdot \mathbb{E}_t\left[\frac{1}{\pi_{t+1}}\right]^{-1} \geq \mathbb{E}_t\left[\frac{Q_{t+1}}{P_{t+1}}\right] \tag{60}$$

that is, the real value of Bitcoin falls in expectation (is a supermartingale) by equation (46).

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

$$E_t\left[\frac{v_{t+1}}{v_t}\right] = -\frac{\text{cov}_t\left(u'(c_{t+1}), \frac{v_{t+1}}{v_t}\right)}{E_t[u'(c_{t+1})]} + \frac{1}{\pi} \tag{61}$$

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 (61) 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[8]. Should those terms cancel, then the real value of the stock of Bitcoins remains unchanged in expectation.

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* $\frac{Q_t}{P_t} \in (0, \frac{\bar{y}}{B_0})$.

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

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

$$\frac{Q_t}{P_t} = \frac{b_t}{B_t} \leq \frac{b_t}{B_0} \leq \frac{\bar{y}}{B_0} = \bar{Q} \tag{62}$$

$\square$

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.[9]

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 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

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

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 4. (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 (55) and*

$$m_t - \beta E_t \left[m_{t+1} \frac{P_{t+1}}{P_t} \right] > 0 \qquad \textit{for all } t \tag{63}$$

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 (55) and (63) 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* $m_t = u'(c_t)/P_t$.

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 (63) 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[10] $\epsilon_t = \epsilon(\theta^t)$, 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 $0 < \zeta, \tilde{\zeta} < \infty$,

$$\sum_{t=0}^{\infty} \mid \epsilon_t \mid \leq \zeta \text{ a.s.} \tag{64}$$

$$\sum_{t=0}^{\infty} \sigma_{\epsilon_t} \leq \tilde{\zeta} \tag{65}$$

Pick an initial Bitcoin price Q_0 satisfying

$$Q_0 > \zeta + \sum_{t=0}^{\infty} \frac{\text{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} \tag{66}$$

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 (66) is smaller than infinity. Therefore, a finite Q_0 satisfying (66) can always be found. Recursively calculate the sequence Q_t per

$$Q_{t+1} = Q_t + \epsilon_{t+1} - \frac{\text{cov}_t(\epsilon_{t+1}, m_{t+1})}{\mathbb{E}_t[m_{t+1}]} \tag{67}$$

The initial condition (66) implies that $Q_t > 0$ for all t. With Lemma 4, and iterating

[10] 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.

backwards via (67) we have

$$\begin{aligned} Q_t &= Q_0 + \sum_{s=1}^{t} \epsilon_s + \sum_{s=1}^{t} \frac{\text{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} && (68) \\ &< Q_0 + \sum_{s=1}^{\infty} \mid \epsilon_s \mid + \sum_{s=1}^{\infty} \mid \frac{\text{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} \mid < \infty && (69) \end{aligned}$$

By Lemma 4 and (64). 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 (55) 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 (55) and (63) such that the sequences Q_t/P_t and $P_t m_t$ are bounded. Part 2(b) of proposition 4 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

$$\epsilon_t = Q_t - E_{t-1}[Q_t] \tag{70}$$

be the one-step ahead prediction error for the Bitcoin price Q_t. Then, equation (55) is equivalent to equation (67). The restrictions above concern just the various boundedness properties, which we imposed.

4.3 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 (63) 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

$$\frac{\mathrm{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} = 2^{-(t+1)} \frac{u'(c_L) - u'(c_H)}{u'(c_L) + u'(c_H)} \iota_t \tag{71}$$

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

$$\frac{\mathrm{cov}_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} = 2^{-(t+1)} \frac{\frac{1}{\pi_L} - \frac{1}{\pi_H}}{\frac{1}{\pi_L} + \frac{1}{\pi_H}} \iota_t \tag{72}$$

which is positive for $\iota_t = 1$ and $\pi_L < \pi_H$ but negative for $\iota_t = -1$. With equation (66), 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 (67) and the resulting equilibrium with proposition 4. 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 (71) respectively (72) into equation

$$E_t[Q_{t+1}] = Q_t + E_t[\epsilon_{t+1}] - \frac{cov(\epsilon_{t+1}, m_{t+1})}{E_t[m_{t+1}]} \tag{73}$$

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. Sample paths of these price processes are unlikely to look like the saw tooth pattern shown in figure 1, however. 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 (55). 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.

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

$$y_t = \frac{D_t}{P_t} \tag{74}$$

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

$$y_t = \frac{D_t}{P_t} + \frac{Q_t}{P_t} B_t \tag{75}$$

That is, there are now two endogenous variables, the Dollar quantity and the Bitcoin price. To understand their 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 $B_t = 0$, equation (74) implies the classic relationship between the quantity of money and the price level. There, policy via the choice of the Dollar quantity D_t can pick a desired level of prices P_t. 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 (75),

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

These two lines are shown in the left panel of figure 4. 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 a large 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 4, 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 (75) 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.

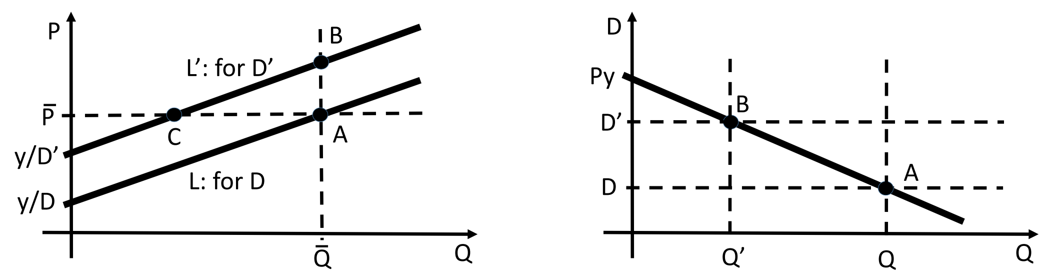

Figure 4: Examining equation (75), $y = \frac{D}{P} + \frac{Q}{P}B$, taking y and B as given.

5.1 Conventional Scenario

The most conventional causality one may impose is, assume that Bitcoin prices move independently of central bank policies. Then, we can explicitly characterize the impact of the Bitcoin price on policy.

Corollary 3. (Conventional Monetary Policy:)
The equilibrium Dollar quantity is given as

$$D_t = y_t P_t - Q_t B_t \tag{76}$$

The central bank's transfers are

$$\tau_t = y_t P_t - Q_t\, B_t - P_{t-1} z_{t-1} \tag{77}$$

The corollary follows since by equation (75) and Lemma 2, $\tau_t = P_t z_t - P_{t-1} z_{t-1} = D_t - P_{t-1} z_{t-1}$. Corollary 3 and the fundamental pricing equation provide a straightforward receipt for forecasting the dollar supply.

Application 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

A less conventional view to read equation (75) is as follows. Assume the central bank can maintain the inflation level π_t independently of the transfers she sets. Further, assume that she sets transfers independently of production.[11] The market clearing condition implies that

Corollary 4. (Policy-driven Bitcoin price:) *The equilibrium Bitcoin price satisfies*

$$Q_t = \frac{y_t P_t - D_t}{B_t} \tag{78}$$

Intuitively, the causality is in reverse compared to scenario 1: now central bank policy drives Bitcoin prices. However, the process for the Dollar stock cannot be arbitrary. To see this, suppose that $y_t \equiv \bar{y}$ and $\pi_t \equiv \bar{\pi}$ are constant. We already know that Q_t must then be a martingale per equation (47). Suppose B_t is constant as well. Equation (78) now implies that D_t must be a martingale too. Intuitively, the

[11] This may surely appear to be an unconventional perspective. The key here is, however, that these assumptions are not inconsistent with our definition of an equilibrium. The analysis would then be incomplete without the consideration of such an unconvential perspective.

central bank has been freed from concerns regarding the price level, and is capable to steer the Bitcoin price this way or that, per equation (78). But in doing so, the equilibrium asset pricing conditions imply that the central bank is constrained in its policy choice.

Under the unconventional scenario various applications are possible.

Application 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

$$G_{t|t-1,D_t}(s) = \mathbb{P}(Q_t \leq s | t-1, D_t) = F(\frac{B_t\, s + D_t}{P_t}). \tag{79}$$

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.

Application 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.

5.3 Optimal Monetary Policy and Welfare

Analyzing welfare in this model is straightforward. 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. 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 (14) and (24). 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. The absence of Bitcoin production is welfare optimal and feasible. Any production of Bitcoin is wasteful in terms of welfare. This result should not surprise in this model. Anything that can possibly 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 then, all equilibria, in which no Bitcoin production takes place, are welfare optimal and minimize GNP. Needless to say, these results are unlikely to remain true in generalizations of our model.

5.4 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

$$Q_t \geq E_t[Q_{t+1}] + \kappa_t \cdot \text{corr}_t\left(\frac{u'(c_{t+1})}{P_{t+1}}, Q_{t+1}\right) \tag{80}$$

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 Conclusions

This paper has analyzed the evolution of cryptocurrency prices and the consequences for monetary policy in a model, in which a cryptocurrency (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 have derived 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. We have provided a "speculative price bound" when Bitcoins are held back in transactions in the hope of a Bitcoin price appreciation. We have provided conditions, under which no speculation in Bitcoins arises. We have provided 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 have studied 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.

The simple model environment considered here already gives rise to a rich set of insights and results. Future research may examine the robustness of the results obtained here as well as their general applicability to the market of digital currencies.

References

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

[2] Aiyagari, Rao (1994) "Uninsured Idiosyncratic Risk and Aggregate Saving," *Quarterly Journal of Economics*, 109, 659-684.

[3] Aoyagi, Jun and Adachi, Daisuke (2018), "Fundamental Values of Cryptocurrencies and Blockchain Technology", SSRN.

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

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

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

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

[8] 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.

[9] Berentsen, Aleksander and Fabian Schär (2018b), "The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies," Federal Reserve Bank of St. Louis Review, Second Quarter 2018, 100 (2), pp. 97-106.

[10] Bewley, Truman (1977), "The permanent income hypothesis: a theoretical formulation," Journal of Economic Theory, vol. 16, no. 2, pp. 252292.

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

[12] 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.

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

[14] 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.

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

[16] 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.

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

[18] 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

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

[20] 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.

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

[22] Chiu, Jonathan, and Thorsten V. Koeppl (2017) ”The economics of cryptocurrenciesbitcoin and beyond.”

[23] Cole, Harold L. and Narayana Kocherlakota (1998), “Zero Nominal Interest Rates: Why They’re Good and How to Get Them,” Federal Reserva Bank of Minneapolis, Quarterly Review (Spring).

[24] Cong, Lin William, Zhiguo He, and Jiasun Li (2018), ”Decentralized mining in centralized pools.”

[25] Chohan, Usman W. (2017), “A History of Bitcoin,” School of Business and Economics, University of New South Wales (draft).

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

[27] 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,vol. 45, pp. 5-28 as part 2.

[28] Financial Times (2018), “Environmental disaster: BIS warns on cryptocurrencies”

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

[30] 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.

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

[32] Gandal, Neil, JT Hamrick, Tyler Moore and Tali Oberman (2017), "Price Manipulation in the Bitcoin Ecosystem," CEPR DP 12061, CEPR, London.

[33] 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.

[34] 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

[35] Hu, Albert and Parlour, Christine A and Rajan, Uday (2018), "Cryptocurrencies: Stylized Facts on a New Investible Instrument".

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

[37] Huggett, Mark, "The Risk-Free Rate in Heterogeneous-Agent Incomplete-Insurance Economies", Journal of Economic Dynamics and Control, 1993, 17, 953-69.

[38] 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.

[39] 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.

[40] 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.

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

[42] Liu, Yukun and Tsyvinski, Aleh (2018), “Risks and Returns of Cryptocurrency”, National Bureau of Economic Research.

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

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

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

[46] Prat, Julien, and Benjamin Walter (2018), ”An equilibrium model of the market for bitcoin mining.”

[47] Routledge, Bryan and Zetlin-Jones, Ariel (2018), “Currency Stability Using Blockchain Technology”, Society for Economic Dynamics 2018 Meeting Papers.

[48] 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. 467482.

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

[50] Schilling, Rene (2017), “Measures, Integrals and Martingales,” Cambridge University Press.

[51] 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.

[52] Sockin, Michael and Xiong, Wei (2018), “A model of cryptocurrencies”, Working paper.

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

[54] 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.

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

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

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

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

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. 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. 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 Bitcoin Production

One interpretation of the Bitcoin production function in equation (11), which is close to the institutional details, is to interpret effort e_t as “energy” or a combination of energy and the appropriate acquisition of hardware. We have chosen the effort 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 are still minor compared to global output, this seems appropriate for the analysis.

Our modeling of individual Bitcoin production $A_{t,j}$ in form of an expected value avoids uneven distribution of Bitcoins across the population per the random outcome of mining. We effectively assume that mining effort is perfectly observable to all and that a mutual insurance contract grants each agent a share of the Bitcoins mined by the entire population in the appropriate proportion of energy or effort expended. One might object to this assumption, that there is no such world-wide insurance across Bitcoin miners. However, if large numbers of Bitcoins are mined each period, then relatively large subgroups of agents, which are nonetheless small compared to the entire population, can enter into such mutual insurance contracts and achieve near-certain Bitcoin-mining outcomes, by the law of large numbers, see also Cong, He, and Li (2018). Such subgroups can be thought of as Bitcoin mining farms, which indeed are in existence now.

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

Proposition 5. (Bitcoin Production Condition:) *Suppose that Dollar sales are nonzero, $z_t > 0$ in period t. Then*

$$h'(e_{t,j}) \geq \beta E_t \left[u'(c_{t+1}) \frac{Q_{t+1}}{P_{t+1}} \right] f(B_t) \frac{1}{\bar{e}_t} \tag{81}$$

This inequality is an equality, if there is positive production $A_t > 0$ of Bitcoins and associated positive effort $e_t > 0$ at time t as well as positive spending of Bitcoins $b_{t+1} > 0$ in $t + 1$.

Proof. This is a standard comparison of costs to benefits and can be derived formally, using the usual Kuhn-Tucker conditions and some tedious calculations. Briefly, providing effort causes disutility of $h'(e_t)$ at time t at the margin. Likewise, at the margin, this effort generates $f(B_t)$ Bitcoins. A Bitcoin buys Q_{t+1}/P_{t+1} units of the consumption good at time $t + 1$, to be evaluated at marginal utility $u'(c_{t+1})$. This gives rise to condition (81) with equality, when Bitcoin production is positive as well as $b_{t+1} > 0$. For that latter condition, note that the agent may value Bitcoins more highly than Q_{t+1}/P_{t+1} at $t + 1$, if she chooses to keep them all, i.e. $b_{t+1} = 0$. □

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 up gradually over time. One could extend the model to allow for such time-to-build of capacity, and it may be interesting to do so.

C 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

$$\beta^t \left(u'(c_t) - \beta^2 E_t \left[u'(c_{t+2}) \, \frac{P_t}{P_{t+2}} \right] \right) \tag{82}$$

$$= \beta^t \left(u'(c_t) - \beta^2 E_t \left[u'(c_{t+2}) \, \frac{P_t}{P_{t+1}} \frac{P_{t+1}}{P_{t+2}} \right] \right) \tag{83}$$

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

$$D_{t+1} = D_{t+1,g} + D_{t+1,r} = D_{t+1,g} = P_t z_t + \tau_{t+1} \tag{84}$$

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

$$D_{t+1} = D_t + \tau_{t+1} \tag{85}$$

Comparing (84) and (85), we have

$$D_t = P_t \, z_t \tag{86}$$

Likewise, $D_{t+1} = P_{t+1} z_{t+1}$. Plugging $D_{t+1} = P_{t+1} \, z_{t+1}$ into (84) and using that equation for t rather than $t+1$ delivers

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

$\square$

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 (45). $\square$

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 (51) 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 (51). $\square$

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

$$E_t\left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right] \geq E_t\left[u'(c_{t+1})\frac{(Q_{t+1}/P_{t+1})}{(Q_t/P_t)}\right] \tag{88}$$

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*

$$Q_t \geq \mathbb{E}_t [Q_{t+1}] \tag{89}$$

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 (88). □

Proof. [Proposition 4]

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 (55) holds. Equation (63) follows directly from equation (53), 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 (55) and (63) 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 (63) 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.

$\square$

Lemma 4. *Suppose ϵ_t satisfies $E_{t-1}[\epsilon_t] = 0$ for all $t \geq 1$ and satisfies equation (64). 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,*

$$\psi := \sum_{t=0}^{\infty} \mid \frac{cov_t(m_{t+1}, \epsilon_{t+1})}{E_t[m_{t+1}]} \mid < \infty \tag{93}$$

Proof. By (65), the sum of the conditional standard deviations of ϵ_t is bounded above by some finite $\tilde{\zeta}$,

$$\sum_{t=0}^{\infty} \sigma_{\epsilon_{t+1}|t} \leq \tilde{\zeta} \tag{94}$$

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

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

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

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 (45) and (88),

$$\frac{Q_t}{P_t} \geq \frac{E_t[u'(c_{t+1}) \frac{Q_{t+1}}{P_{t+1}}]}{E_t[u'(c_{t+1}) \frac{P_t}{P_{t+1}}]} \tag{95}$$

$$\geq \frac{E_t[u'(c_{t+1}) \frac{Q_{t+1}}{P_{t+1}}]}{E_t[u'(c_{t+1})] \frac{1}{\underline{\pi}}} \tag{96}$$

$$= \underline{\pi} \, \frac{cov_t(u'(c_{t+1}), \frac{Q_{t+1}}{P_{t+1}}) + E_t[u'(c_{t+1})] \, E_t[\frac{Q_{t+1}}{P_{t+1}}]}{E_t[u'(c_{t+1})]} \tag{97}$$

$$= \underline{\pi} \, \left(\frac{cov_t(u'(c_{t+1}), \frac{Q_{t+1}}{P_{t+1}})}{E_t[u'(c_{t+1})]} + E_t \left[\frac{Q_{t+1}}{P_{t+1}} \right] \right) \tag{98}$$

$$\geq \underline{\pi} \; E_t \left[\frac{Q_{t+1}}{P_{t+1}} \right] \tag{99}$$

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

$$\frac{Q_0}{P_0} \geq \underline{\pi} E_0 \left[\frac{Q_1}{P_1} \right] \geq \underline{\pi}^2 E_0 \left[E_1 \left[\frac{Q_2}{P_2} \right] \right] \geq \cdots \geq \underline{\pi}^t E_0 \left[E_1 \left[\dots E_{t-1} \left[\frac{Q_t}{P_t} \right] \right] \right] \tag{100}$$

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. $\square$

Technical Appendix

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

Consider the following slightly more general version of assumption 3.

Assumption A. 4. *Let $\alpha > 0$. For all even t*

$$u'(y_t) - \alpha\beta E_t[u'(y_{t+1})] > 0 \tag{101}$$

while for all odd t

$$\alpha u'(y_t) - \beta E_t[u'(y_{t+1})] > 0 \tag{102}$$

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 $\lambda = 1/(1+\alpha)$.

Theorem 2. (No-Bitcoin-Speculation Generalized.) *Suppose that $B_t > 0$ and $Q_t > 0$ for all t. Impose assumption 4. Then in every period, all Bitcoins are spent.*

Proof. [Theorem 2] 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 (88) holds, in case no Bitcoins are spent at date t, or equation (45) holds, if some Bitcoins are spent. Since equation (45) implies inequality (88), (88) holds for all t. Suppose first that t is an even period. Then

$$\begin{aligned}
\beta^2 \mathbb{E}_t[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}] &= \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{Q_{t+2}}{P_{t+2}}\right]\right] && \text{(law of iterated expectation)} \\
&\leq \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\,\frac{P_{t+1}}{P_{t+2}}\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per equ. (88) at } t+1) \\
&\leq \beta^2 \mathbb{E}_t\left[\mathbb{E}_{t+1}\left[u'(c_{t+2})\right]\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 1)} \\
&< \alpha\beta \mathbb{E}_t\left[u'(c_{t+1})\,\frac{Q_{t+1}}{P_{t+1}}\right] && \text{(per ass. 4 in t+1)} \\
&\leq \alpha\beta \mathbb{E}_t\left[u'(c_{t+1})\,\frac{P_t}{P_{t+1}}\right]\,\frac{Q_t}{P_t} && \text{(per equ. (88) at } t) \\
&\leq \alpha\beta \mathbb{E}_t\left[u'(c_{t+1})\right]\,\frac{Q_t}{P_t} && \text{(per ass. 1)} \\
&< u'(c_t)\,\frac{Q_t}{P_t} && \text{(per ass. 4 in t)}
\end{aligned}$$

which contradicts the speculative price bound (51) 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. $\square$