The Equilibrium Value of Bitcoin

Radwanski, Juliusz

Humboldt University of Berlin

18 November 2021

The Equilibrium Value of Bitcoin*

Juliusz F. Radwański

juliusz.radwanski@hu-berlin.de

November 18, 2021

Preliminary. Comments welcome.

Abstract Can the value of a cryptocurrency be uniquely determined by the fundamentals, such as the rule for money growth implicit in the design of the protocol? To answer this question, we construct a recursive asset-pricing model for a single fiat cryptocurrency, similar to actual Bitcoin. We think of our model as an ideal laboratory, in which *equilibria* correspond to model solutions that can generate actual data. Our approach stresses the role of the value function as an object of rational choice and hence rests on solid micro-foundations. By imposing enough economically motivated restrictions on that choice, we are able to pin down unique equilibrium and hence demonstrate that the value of our cryptocurrency is immune to self-fulfilling expectations. This result depends only on the design of the cryptocurrency protocol.

Keywords: Bitcoin, cryptocurrency, equilibrium, expectations, money, sunspots.

JEL Classification Numbers: E40, E50, G12.

*Wirtschaftswissenschaftliche Fakultät, Humboldt-Universität zu Berlin, Dorotheenstr. 1, 10099 Berlin, Germany. I would like to thank Anna Almosova, Hermann Elendner, Ingolf Pernice, and participants of the workshop Cryptocurrencies – Markets and Pricing (Weizenbaum Institut, Berlin).

1 Introduction

Can the value of a cryptocurrency be uniquely determined by the fundamentals, such as the rule for money growth implicit in the design of the protocol? To the best of our knowledge, none of existing monetary models applied to cryptocurrencies is able to rule out (so-called) multiple equilibria, including the one in which money is permanently worthless. From a purist's point of view, there is no complete asset-pricing theory applicable to cryptocurrencies. As a consequence, some economists even believe that cryptocurrencies are merely speculative bubbles.

We construct a recursive asset-pricing model for a single fiat cryptocurrency, which we call Bitcoin. We think of our model as an ideal laboratory, in which *equilibria* correspond to model solutions that can generate actual data. Our approach stresses the role of the value function as an object of rational choice and hence rests on solid micro-foundations. By imposing enough economically motivated restrictions on that choice, we are able to pin down unique equilibrium and hence demonstrate that the value of our cryptocurrency is immune to self-fulfilling expectations. This result depends only on the design of the protocol.

Since our focus is on *valuation*, we work with a maximally tractable environment. The economy is populated with symmetric, indefinitely-lived, competitive, and knowledgeable households. Each household owns a growing Lucas tree of specialized endowment. Money is *potentially* useful due to the existence of proportional costs of various forms of non-monetary exchange. Barter is costly due to spatial separation combined with imperfect portability of goods. Paying with promises of forward delivery is costly due to limited commitment. There is no public record of past actions under which monetary exchange could be replaced by gifts.[1]

Each household is composed of a producer who stays at home and a consumer who can travel. There is a proof-of-work blockchain technology allowing house-

[1]The results do not depend on a particular set of real-world frictions giving rise to the assumed cost structure.

holds to accumulate intrinsically useless net worth and make secure transfers to other households from any location. The time lag between sending a transfer and receiving funds is fixed technologically. A consumer using the blockchain technology can interact with many producers without the need to carry goods. We abstract from the costs of search and matching, which allows to define the competitive value of Bitcoin, uniform across the locations.[2]

We impose rigor by carefully specifying the sequence of events. At the beginning of each period, before the market opens, the households observe the state variables, form expectations of prices and aggregate quantities, and choose their value functions. The value functions guide optimal decisions throughout the period. Having interacted in the market, the households decide on mining and consumption. The difficulty of mining is automatically adjusted by the protocol in order to keep the money growth consistent with a given rule. The protocol allows to mine marginal Bitcoins for free when aggregate mining is zero.

We assume that the households are sufficiently informed to form correct (maximally precise) expectations of aggregate variables, and that the market value of Bitcoin coincides with expectations formed before trade. Although there is no explicit price setting in the model, this simple price mechanism is consistent with the situation in which producers *set* their prices to not deviate from (correctly formed) expectations of the competitive market value of Bitcoin.[3]

We posit that the actions of any subset of agents cannot depend on time as the independent variable. We assume that the number of households is finite, and that each household can generate at most finitely many information signals. We allow for a finite number of state variables unrelated to the fundamentals (sunspots) on which the households might condition their expectations. Under these assump-

[2]We abstract from whether the blockchain technology provides anonymity. The economics of valuation should not depend on the interpretation of the network of (potential) users.

[3]We note that this removes any 'creative' role from the Walrasian auctioneer, who is neither needed in the model, nor exists in reality.

tions, the environment has a convenient recursive structure which allows to study equilibria as collections of functions (Lucas, 1978).

We restrict attention to value functions reflecting lifetime utility, maximized at choices consistent with aggregate identities and feasibility. Any collection of functions representing expectations and a value function restricted in this way is called *pre-equilibrium*. The conditions for a pre-equilibrium are not sufficient to establish that the market value of Bitcoin must be unique, or even positive. We impose further restrictions on the value function, motivated by the general observation that rational households should be allowed to form private valuations based on their knowledge of the whole *set* of pre-equilibria, treated as economically justified, and hence a-priori possible market outcomes.[4]

In particular, we postulate that the value function should be strictly increasing in Bitcoin net worth, at given state variables, if there exists a pre-equilibrium with a positive value of Bitcoin. Otherwise, a household would be ignoring the *possibility* that owning more Bitcoins can increase consumption via the market.

Similarly, suppose that there exists a pre-equilibrium in which selling a marginal unit of endowment for Bitcoin (or spending a Bitcoin to buy consumption) yields a risk-adjusted return strictly exceeding the utility of consuming that unit (holding unspent Bitcoin until the next period), while all other pre-equilibria are characterized by indifference between these options. We postulate that this is enough to induce the households, before trade, to form private valuations under which the marginal trade (of either type) is strictly preferred. Otherwise, a household would be ignoring the possibility that it might benefit from selling *more* endowment for Bitcoin (spending *more* Bitcoins) at the margin, in some pre-equilibria.

Our equilibrium conditions (iii)-(iv) restrict the value function in a way consis-

[4]Our notion of pre-equilibrium (essentially) coincides with the definition of equilibrium in Lucas (1978). As already mentioned, we prefer to reserve the term *equilibria* for model solutions which have some probability of generating *observed* data, which is not necessarily true of every pre-equilibrium.

tent with the motivation above (see section 3 for additional discussion). Together with pre-equilibrium conditions (i)-(ii), they constitute our generalized definition of equilibrium. We show that the model has only one equilibrium as long as the rule for money growth implicit in the design of the protocol satisfies two sufficient conditions, formulated as assumption 10. The role of these conditions is to guarantee that there *exists* a pre-equilibrium in which all Bitcoins are spent and all endowment is sold. This pre-equilibrium is then selected as the unique equilibrium of the model, and the value of Bitcoin is characterized by the equation of exchange (Fisher, 1911). We offer examples in which the protocol can be designed to guarantee this outcome.

1.1 Related Literature

Some economists have suggested that cryptocurrencies are purely speculative assets with zero fundamental values. For example, Garratt and Wallace (2018) argue that the value of Bitcoin depends upon self-fulfilling beliefs that are hard to pin down, either in the case where Bitcoin is the only form of money, or with multiple Bitcoin clones and/or a competing fiat currency. Cheah and Fry (2015) find empirical evidence that Bitcoin price is a speculative bubble with the fundamental value of zero. Fry (2018) constructs a model of a bubble with a probability of complete collapse, and finds that it fits well to the data on Bitcoin and Ethereum.

While some empirical studies found significant bubble components in prices of cryptocurrencies (Corbet et al., 2018), others have documented relatively tight empirical links between these prices and measurable factors which could be interpreted as fundamentals. For example, Aoyagi and Hattori (2019) find evidence that the price of Bitcoin and its total hash rate are determined simultaneously in the long-run, and that the hash rate (Granger) causes the Bitcoin price in the short-run. Similarly, Bhambhwani et al. (2019) find a strong relationship between the price, hashrate, and the number of active users for five major cryptocurrencies. The latter authors interpret the two latter variables as proxies for the trustwor-

thiness of the network (Pagnotta and Buraschi, 2018) and its transaction benefits (Biais et al., 2020), respectively.

It is difficult to interpret this evidence partly because most cryptocurrencies are not (yet) commonly used as media of exchange (Bariviera et al., 2017). Nevertheless, it is reasonable to ask if their values would be uniquely determined under a set of idealized conditions, which is the main question asked here. Our approach extends the asset-pricing framework of Lucas (1978) to a single unbacked and intrinsically useless cryptocurrency, without relying on the cash-in-advance constraint (Lucas, 1980) or other modeling shortcuts. Our work can be seen as an integration of the theory of cryptocurrencies with asset pricing, offering a framework in which the value of a cryptocurrency is uniquely determined in equilibrium by economic forces derived from rational behavior.

Existing theoretical studies of cryptocurrencies usually apply off-the-shelf monetary theories. Biais et al. (2020) use the overlapping generations (OLG) model (Samuelson, 1958; Wallace, 1980; Tirole, 1985) to argue that the value of a cryptocurrency depends on future prices, which implies that returns can exhibit large volatility unrelated to the fundamentals. At the same time, they show empirically that a statistically significant fraction of Bitcoin returns is explained by estimated transactional benefits, which suggests an important role for the fundamentals in practice. Other studies using the OLG model include Garratt and Wallace (2018) and Saleh (2019). On the other hand, Schilling and Uhlig (2019) employ a turnpike model of Townsend (1980) to study the coexistence of a cryptocurrency with a fiat currency. These studies find, or at least mention, the possibility of multiple equilibria consistent with rational expectations, which is a direct consequence of the same property of the underlying frameworks. While we do not deny the usefulness of these studies for understanding a variety of important issues, models allowing for multiple equilibria cannot be considered complete theories of *valuation*.

A separate strand of monetary literature is built around the assumption that

money provides a flow of utility or liquidity services, following the suggestion of Hicks (1935) and subsequent contributions by Patinkin (1965); Sidrauski (1967); Brock (1974). For example, Benigno et al. (2019) use such model to study restrictions on domestic monetary policy implied by the presence of a global cryptocurrency. This modeling shortcut is methodologically invalid if one's objective is to understand the economics behind the adoption and valuation of a (fiat) cryptocurrency. Moreover, as with traditional monetary models, this approach is plagued with problems of equilibrium non-uniqueness, as observed by Hahn (1965). The basic reason is that money *is* a purely speculative asset under this approach.

By focusing on the microfoundations while retaining the analytical convenience of an asset pricing model with symmetric agents, this paper offers an alternative to the literature often classified under the name New Monetarism (see Williamson and Wright (2010); Lagos et al. (2017) for surveys). These studies highlight the importance of explicit frictions under which there is an essential role for a medium of exchange, and predominantly rely on the modeling device of random search and matching, following Kiyotaki and Wright (1989). In the context of cryptocurrencies, Choi and Rocheteau (2021) adopt the model of Shi (1995) and Trejos and Wright (1995) with indivisible money and limited money holdings, extended to include a mining technology allowing for endogenous choice of mining. Choi and Rocheteau (2020) study a continuous time version of Lagos and Wright (2005) model in which money is divisible. Both studies find that, apart from the unique steady-state equilibrium, there exists a continuum of equilibria in which the value of the cryptocurrency first grows and then bursts gradually over time. Other studies employing New Monetarist models to study cryptocurrencies include Zhu and Hendry (2018); Fernández-Villaverde and Sanches (2019); Lotz and Vasselin (2019); Kang and Lee (2019); Yu (2021).

While our paper does offer a stylized environment designed to at least partly justify the assumed cost structure, the main focus is on the *microfoundations* understood as rules of rational decision making in the context of valuation. We

contribute to the methodology of monetary economics by arguing that these rules should be explicit in monetary models, even though they can be safely ignored in models where money would necessarily be worthless, in particular in economies with complete markets.[5]

A closely related study is Radwanski (2021), who studies equilibrium valuation of fiat money issued by a generic institutional authority in a similar economic setup. His model differs from ours in two main respects. First, the operation of the payment system does not require mining costs, which makes the analysis simpler. Second, the authority in his model operates a market for risk-free loans in which it sets the interest rate. In contrast, the market for risk-free loans is missing from our model, and hence equilibrium cannot be characterized by the usual first-order condition in that market. His definition of equilibrium is therefore less general than ours, although sufficient under his assumptions.

2 Model

2.1 Time and Information

Time is divided into periods $[t, t+1)$, $t \in \{0, 1, \dots\}$. Information is generated and observed at the beginning of each period. The structure of information is restricted by the following assumption:

Assumption 1 *The environment admits at most a finite number of state variables. The state vector can be partitioned into (x_t, s_t), where $s_t \in \mathcal{S}$ is a stationary and ergodic Markov process with transition density $F(s, s')$, having a stationary distribution Φ, and x_t is valued in a Cartesian product of (subsets of) real lines.*

[5] Arguably, rules of rational valuation should rank higher among the microfoundations than stylized assumptions about the environment. Some simple environments designed to explain the use of fiat money have been criticized for lacking realism, e.g., the assumption of finite lives (with no inter-generational links) in OLG models (Tobin, 1980). Instead of attempting to explain frictions (and potentially assuming too much), we take their existence as given.

There is a continuous[6] *function* $g(x, s, s')$ *such that*

$$x_{t+1} = g(x_t, s_t, s_{t+1}). \tag{1}$$

Intuitively, only a finite number of state variables can be generated by the economy at any point in time. These variables must follow time-invariant laws and summarize everything that can be known about the economy at t. Not all state variables in x_t need to be named. The variables in x_t with no interpretation will be collected in $u_t \in \mathcal{U}$, and assumed to obey a joint law $g_u(x, s, s')$.[7]

The following property of the environment is imposed for technical reasons.

Assumption 2 *For every continuous and* φ*-bounded function* $f(x, s)$ *(see definition 3 in the appendix), the function* $(Tf)(x, s) \equiv \int_S f(x', s')dF(s, s')$*,* $x' = g(x, s, s')$*, is continuous.*

2.2 Households and Endowment

There is a finite number of competitive, symmetric, and indefinitely-lived households. The households occupy distinct locations. The distance between any two locations is normalized to one. A household is composed of a producer who stays at home and a consumer who can travel, carry goods, and consume at any location. In what follows, all aggregate quantities are expressed per household.

Preferences of a household at t are represented by the functional

$$V_t = E_t \left\{ \sum_{s=0}^{\infty} \beta^s u(c_{t+s}) \right\}, \tag{2}$$

[6] In what follows, the term *continuous* will denote *joint* continuity (the inverse image of every open set is open in the usual product topology on the domain).

[7] We believe that it is important to keep track of these variables in the notation, in order to explicitly allow the agents to condition expectations on *any* available source of information, including *sunspots*. At the same time, it makes little sense to explicitly name all potential sunspots.

where $0 < \beta < 1$, $u(c) = c^{1-\gamma}/(1-\gamma)$ if $\gamma \in (0,1) \cup (1,\infty)$, or $u(c) = \log(c)$. The constant $1/\gamma$ is the elasticity of inter-temporal substitution (EIS), which in the presence of risk also controls the relative risk aversion.[8]

Each household receives perishable endowment $e_t > 0$, growing at the rate

$$e_{t+1}/e_t = 1 + \lambda(s_t, s_{t+1}). \tag{3}$$

The function $\lambda(s, s')$ is continuous and valued in a compact interval covering 0 and bounded away from -1. Endowment can either be consumed or given to a member of another household.

Assumption 3 *The growth rate of endowment satisfies*

$$\begin{aligned} &0 < \underline{w} \leq w(s, s') \leq \bar{w} < 1, \\ &w(s, s') \equiv \beta[1 + \lambda(s, s')]^{1-\gamma}. \end{aligned} \tag{4}$$

This implies that there exists a number δ such that

$$\int_S w(s, s') dF(s, s') \leq \delta < 1. \tag{5}$$

2.3 Inefficiency of non-Monetary Exchange

The following assumptions introduce proportional costs of consuming own endowment, and of two forms of non-monetary exchange.

Assumption 4 *Consuming own endowment results in a proportional waste* $\kappa_s \in (0, 1]$.

Assumption 5 *Carrying endowment over a unit of distance results in a proportional waste* $\kappa_p \in (0, 1]$.

[8] This is the standard CRRA utility function, assumed for convenience.

Assumption 6 *Accepting a promise of future delivery from another household reduces the expected discounted present value of the promised flow by* $\kappa_e \in (0, 1]$*, under the appropriate consumption-based stochastic discount factor.*

As shown by Kocherlakota (1998), money could still be worthless in our environment if there existed a public record of past actions on which the households could condition gifts. We, therefore, need to impose:

Assumption 7 *There does not exist a public record of past actions.*

While these assumptions are important to restrict the efficiency of various forms of non-monetary exchange, the following one is only for convenience, as it allows to ignore barter and promises in the analysis, without affecting the main results.[9]

Assumption 8 *The cost parameters of assumptions (4)-(6) satisfy*

$$\kappa \equiv \min\{\kappa_s, \kappa_p, \kappa_e\} = \kappa_s.$$

The parameter κ will be referred to as the inefficiency of non-monetary exchange.

2.4 Bitcoin Protocol

Starting from the initial date $t = 0$, the environment features a distributed ledger keeping track of individual net worth at the beginning of each period, $H_t \geq 0$, measured in units called Bitcoins. The initial net worth satisfies $H_0 > 0$.

Using the ledger is costless, and consumers can send secure Bitcoin transfers from any location. The transfers are confirmed by a well-functioning proof-of-work algorithm as long as some real resources are spent on mining.

Assumption 9 *There is a frictionless spot market in which Bitcoin transfers can*

[9]Otherwise, one would need to allow the households to consider all ways of non-monetary exchange before showing that only the one with the lowest proportional cost could ever be used as the alternative to monetary exchange. The analysis is particularly easy when consumption of own endowment is this alternative.

be exchanged for goods in a quid-pro-quo fashion.

We denote the market value of a Bitcoin by $(1/P)_t \geq 0$. This way, we do not rule out the possibility that $(1/P)_t = 0$ before studying the equilibrium.

Bitcoin net worth (at the beginning of the period) evolves according to

$$H_{t+1} = H_t - M_t + Y_t + G_{t+1}, \tag{6}$$

where $M_t \geq 0$ is the sum of transfers sent to other households, $Y_t \geq 0$ the sum of transfers received from other households (called income), and $G_t \geq 0$ mining profit. The income and mining profit arrive after a time lag, fixed by the design of the protocol, for convenience set to the length of one period.[10]

The sum of transfers sent by a household is restricted by the budget constraint

$$M_t \leq H_t. \tag{7}$$

The choice of income is restricted by the resource constraint

$$Y_t(1/P)_t \leq e_t. \tag{8}$$

Since nominal spending and income are identical in the aggregate, we impose

$$M_t = Y_t \tag{9}$$

as an equilibrium condition, although individual households can choose these variables separately. Under the assumptions so far, $H_t > 0$ for all $t \geq 0$.

Let $W_t = H_t - M_t + Y_t$ denote Bitcoin net worth at the end of the period, and Z_t its aggregate counterpart. We have $W_t > 0$, and hence $Z_t > 0$ for all $t > 0$.[11]

[10] All these variables can be defined irrespective of whether the household actually uses the blockchain technology, or ignores its existence.

[11] One must distinguish W_t from Z_t in the notation, since a household can di-

Mining requires real resources $q_t \geq 0$. The mining profit of a household satisfies

$$G_{t+1} D_{t+1} = q_t, \tag{10}$$

with D_{t+1} being the difficulty of mining, set ex-post by the protocol according to

$$D_{t+1} = \frac{q_t^a}{Z_t} \frac{1}{\alpha(s_t, s_{t+1})}, \tag{11}$$

where q_t^a is the aggregate mining activity, and $\alpha(s, s')$ a strictly positive continuous function called the design function (of the protocol). We impose

$$q_t^a = q_t \tag{12}$$

as an equilibrium condition.[12] If $q_t > 0$ and hence $q_t^a > 0$ in equilibrium, since $Z_{t+1} = Z_t + G_{t+1}$, the aggregate Bitcoin net worth grows according to

$$\frac{Z_{t+1}}{Z_t} = 1 + \alpha(s_t, s_{t+1}). \tag{13}$$

If $q_t^a = 0$, the protocol still sets $G_{t+1} = \alpha(s_t, s_{t+1}) Z_t$, such that equation (13) holds. A household expecting $q_t^a = 0$ believes to have the opportunity to mine Bitcoin for free at the margin, in addition to already expected mining profit.[13]

We require $q_t / e_t \in [0, \kappa]$ in equilibrium. The upper bound cannot be exceeded, since otherwise a household would optimally consume its endowment at t and delay the decision to use the blockchain technology.

The following assumption is central to our results.

Assumption 10 *The design function $\alpha(s, s')$ is chosen such that*

rectly control W_t but takes the evolution of Z_t as given. The analogous distinction for individual and aggregate endowment is not needed, since both are exogenous.

[12] The individual and aggregate mining activities must be separated for the same reason as explained in footnote 11.

[13] The actual Bitcoin protocol halves the money growth rate periodically and allows for fees for the miners. We assume these features away for simplicity.

(a) There is a unique solution $\xi(s) \in (0, \kappa)$ to the functional equation

$$\xi(s) = \beta \int_S [1 + \lambda(s, s')]^{1-\gamma} \left[\frac{1 - \xi(s')}{1 - \xi(s)}\right]^{-\gamma} \frac{\alpha(s, s')}{1 + \alpha(s, s')} dF(s, s'). \tag{14}$$

(b) The functions α and ξ jointly satisfy

$$1 - \kappa < \beta \int_S [1 + \lambda(s, s')]^{1-\gamma} \left[\frac{1 - \xi(s')}{1 - \xi(s)}\right]^{-\gamma} \frac{1}{1 + \alpha(s, s')} dF(s, s') < 1. \tag{15}$$

Whether a given function α satisfies these conditions depends on the details of the environment, such as the stochastic properties of endowment and/or parameter values. Section 4 offers some examples.

2.5 Expectations

Consistent with the Markovian structure of the economy, expectations are given by time-invariant functions of the state variables.

Prior to trade, a household expects that the market value of Bitcoin will be

$$(1/P)_t = \frac{e_t}{Z_t} \eta(Z_t, e_t, u_t, s_t), \tag{16}$$

where $\eta(z, e, u, s)$ is a continuous function called price function. This function must be bounded (almost surely), since otherwise a household would expect to attain consumption exceeding any given value at some state variables.[14]

We assume that the expectations of the evolution of aggregate state variables are correct. This corresponds to the situation in which the households either know the structure of the economy, or are sufficiently experienced. In particular, the households know the evolution of aggregate Bitcoin net worth (13).

[14]Factoring e/Z is without loss of generality.

The expectations of aggregate mining activity are formed according to the model

$$q_t^a = e_t \zeta(Z_t, e_t, u_t, s_t), \tag{17}$$

where $\zeta(z, e, u, s) \in [0, 1]$ is a continuous function. We note that the equilibrium condition $q < e$ is equivalent to $\zeta < 1$ (since $q = q^a$), and condition $q > 0$ (discussed later) to $\zeta > 0$.

Given M_t, Y_t, and under the assumed expectations, the resources available for consumption and mining (c, q, respectively) are

$$\begin{aligned} c_t + q_t &= M_t(1/P)_t + (1-\kappa)[e_t - Y_t(1/P)_t], \\ &= M_t \frac{e_t}{Z_t}\eta(Z_t, e_t, u_t, s_t) + (1-\kappa)[e_t - Y_t \frac{e_t}{Z_t}\eta(Z_t, e_t, u_t, s_t)]. \end{aligned} \tag{18}$$

2.6 Price Formation

We assume that the price function determines the actual market value of Bitcoin. This reflects two insights. First, the market price is in reality set by the same households who form the expectations, and hence cannot contain information beyond what is known to the households. Second, if a household expects a given market value of Bitcoin, it has no incentive to deviate from it in its own price setting. Although there is no explicit price setting in the model, these observations about reality justify our price mechanism.

2.7 Value Function

A household guides its decisions using a continuous value function $v(h, z, e, u, s)$, with domain denoted by $\mathcal{X}$, where the first argument corresponds to Bitcoin net worth at the beginning of the period.[15] We are only interested in value functions representing maximized utility (2). Since lifetime utility cannot asymptotically

[15]Rational households cannot ignore the existence of Blockchain technology in their environment, hence Bitcoin net worth must appear as one of the arguments.

change faster than $e_t^{1-\gamma}$ (or $\log e_t$, if $\gamma = 1$), any value function must be φ-bounded, according to definition 3 of the appendix.

2.8 A Technical Constraint

The measure of Bitcoins raised by selling endowment is physically limited by the aggregate supply, which could be a binding constraint at a sufficiently low $(1/P)_t$, in particular when $\eta = 0$. However, in a competitive equilibrium, prices must adjust such that a household never experiences aggregate constraints.

To guarantee that the physical limit never binds, we let $\bar{\bar{y}} > 1$ be sufficiently large such that

$$Y_t < \bar{\bar{y}} Z_t. \tag{19}$$

We allow $Y_t \leq \bar{\bar{y}} Z_t$ in the household's problem, in order to make the choice set compact, while the version with strict inequality (19) is imposed as an equilibrium condition.

The constraints (8) and (19) can be combined. Under the assumed expectations, both bind when $\eta(Z_t, e_t, u_t, s_t) = 1/\bar{\bar{y}}$. Hence,

$$Y_t \in [0, \bar{y}(Z_t, e_t, u_t, s_t)], \quad \bar{y}(z, e, u, s) \equiv \begin{cases} \frac{1}{\eta(z,e,u,s)} z & \text{if } \eta(z, e, u, s) \geq 1/\bar{\bar{y}}, \\ \bar{\bar{y}} z & \text{if } \eta(z, e, u, s) < 1/\bar{\bar{y}}. \end{cases} \tag{20}$$

By construction, the function $\bar{y}$ is positive and continuous in the state variables.

The set $\mathcal{C}(H_t, Z_t, e_t, u_t, s_t)$ of feasible choices M_t, Y_t, q_t is non-empty and compact, and the correspondence defined in this way is continuous.

3 Equilibrium

We start with the definition of pre-equilibrium. Let $\mathcal{Y} = \mathcal{R}_+ \times \mathcal{R}_+ \times \mathcal{U} \times \mathcal{S}$.

Definition 1 *A pre-equilibrium is:*

(a) A continuous bounded function $\eta\colon \mathcal{Y} \to \mathcal{R}_+$*, and a continuous function* $\zeta\colon \mathcal{Y} \to [0, \kappa]$*,*

(b) A continuous, φ*-bounded function* $v\colon \mathcal{X} \to \mathcal{R}$*,*

such that:

(i) Given η*,* ζ*, the function* v *solves*

$$v(h,z,e,u,s) = \max_{(m,y,q)} \left\{ u(c) + \beta \int_S v(h',z',e',u',s') dF(s,s') \right\}, \tag{21}$$

$$\text{subj. to:} \quad c = m\frac{e}{z}\eta + (1-\kappa)(e - y\frac{e}{z}\eta) - q, \tag{22}$$

$$(m,y,q) \in \mathcal{C}(h,z,e,u,s), \tag{23}$$

$$h' = h - m + y + g', \quad g'd' = q, \quad d' \equiv \frac{\zeta e}{z}\frac{1}{\alpha(s,s')} \tag{24}$$

$$z' = z(1 + \alpha(s,s')), \tag{25}$$

$$e' = e(1 + \lambda(s,s')), \tag{26}$$

$$u' = g_u(z,e,u,s,s'), \tag{27}$$

(ii) For each z, e, u, s*, the value* $v(z,z,e,u,s)$ *is attained by* m, y, q *such that* $m = y$*,* $q = q^a$*, and* $y < \bar{\bar{y}}z$*.*

Condition (i) requires that the value function represents maximized utility given the expectations η, ζ. The content of condition (ii) is that the maximum is attained by choices consistent with aggregate identities and the feasibility restriction.

The two conditions are sufficient to select unique equilibrium in a model without money (Lucas, 1978). The following observation shows that this is not the case in our monetary model.

Observation 1 *For any function* $\alpha(s,s')$*, whether satisfying assumption 10 or not, there is a pre-equilibrium with* $\eta = \zeta = 0$*, all* z, e, u, s*.*

The reason is that the market value of Bitcoin can stay at zero for ever without

violating (i)-(ii), since the value function can assign no value to Bitcoin net worth, in which case the households never spend any resources on mining, either.

An important property of a pre-equilibrium is that there is exactly one value function consistent with given expectations as long as $\zeta > 0$.[16]

Proposition 1 *Given η, ζ specified as in (a), if $\zeta > 0$ for all z, e, u, s, there is exactly one continuous and φ-bounded function v satisfying conditions (i)-(ii).*

The proof is in the appendix and employs a standard fixed-point theorem.

Proposition 2 *If $\eta > 0$ and $\zeta > 0$ for all z, e, u, s, the value function is differentiable in h at $h = z$, with*

$$\frac{\partial}{\partial h} v(h, z, e, u, s)|_{h=z} = u'(c)\frac{e}{z}\eta(z, e, u, s) = u'(c)(1/P)_t. \tag{28}$$

The proof is in the appendix. Under the conditions of the proposition, the partial derivative of the value function must be tightly linked to the market value of Bitcoin. We will use this result to formulate our equilibrium condition (iv) (below), and to study the problem (21) in terms of the associated first-order conditions.

Proposition 3 *There exists a pre-equilibrium with $\eta > 0$ and $\zeta > 0$.*

The proof is in the appendix, and demonstrates the existence by constructing a pre-equilibrium with $\eta = 1$ and $\zeta \in (0, \kappa)$, under assumption 10.

We now formulate our definition of equilibrium.

Definition 2 *An equilibrium is a collection of functions η, ζ, v satisfying definition 1, such that in addition:*

(iii) If there are functions η^p, ζ^p, v^p satisfying definition 1, with $\eta^p(z, e, u, s) > 0$, then v is strictly increasing in h, at each z, e, u, s.

[16] At $\zeta = 0$ and $\eta > 0$, a household optimally attempts to mine unlimited number of Bitcoins for free, so the problem (21) has no solution. This case will not be relevant for our analysis of equilibrium.

(iv) If for all η^p, ζ^p, v^p satisfying definition 1 and (iii) it is true that

$$1-\kappa \leq \beta \int_S \frac{\frac{\partial}{\partial h} v^p(z', z', e', u', s')}{\frac{\partial}{\partial h} v^p(z, z, e, u, s)} dF(s, s') \leq 1,$$

with strict inequalities for some p, then

$$1-\kappa < \beta \int_S \frac{\frac{\partial}{\partial h} v(z', z', e', u', s')}{\frac{\partial}{\partial h} v(z, z, e, u, s)} dF(s, s') < 1.$$

Conditions (iii)-(iv) formalize the intuition of the introduction. The former requires that if there exists a pre-equilibrium with a positive Bitcoin value (at a given state of the economy), rational households must take this into account when forming their private valuations before trade. Any resulting value function must then assign a positive value to additional Bitcoin net worth.

Before discussing condition (iv), we note the following fact.

Proposition 4 *If functions η, ζ, v satisfy definition 1, and if the value function v is strictly increasing in h, then $\eta > 0$ and $\zeta > 0$, all z, e, u, s.*

The proof is in the appendix. The proposition shows that condition (iii) could impose $\eta > 0$ and $\zeta > 0$ directly, as long as there exists a pre-equilibrium with a positive Bitcoin value. We prefer our formulation as more directly reflecting the economic intuition that the households optimally *choose* to use value functions that are strictly increasing in Bitcoin net worth.

Propositions 2, 3 and 4 together imply that, in every pre-equilibrium satisfying (iii), the value function must be differentiable in h. Since $h = z$ with symmetric households, equation (28) allows to write the weak inequalities of condition (iv)

$$1-\kappa \leq \beta \int_S \frac{u'(e'(1-\zeta^p(z', e', u', s')))}{u'(e(1-\zeta^p(z, e, u, s)))} \frac{(1/P)^{p'}}{(1/P)^p} dF(s, s') \leq 1,$$

where $(1/P)^p \equiv \frac{e}{z}\eta^p(z, e, u, s)$. It can now be seen that condition (iv) tests whether the consumption-based return on Bitcoin is bounded between $(1-\kappa)$ and 1 across

all pre-equilibria. An equality on the left-hand side would imply indifference between selling a marginal unit of endowment for Bitcoin or consuming that unit inefficiently, at the cost κ. An equality on the right-hand side would imply indifference between spending a marginal Bitcoin on consumption versus holding the unspent Bitcoin until the next period. If there exists at least one pre-equilibrium p in which a representative household strictly prefers to sell all endowment *and* spend all Bitcoins, while all other pre-equilibria are characterized by weak preference towards either of these alternatives, condition (iv) imposes the strict preference on equilibrium value functions. Intuitively, since a household must choose its value function before the market opens to guide its quantity decisions, choosing a value function consistent with indifference might subject a household to the risk of missing a value-improving trade.[17]

We note that choosing a value function according to conditions (iii)-(iv) does not subject a household to any risk in the case of guessing pre-equilibrium incorrectly. If the market value of Bitcoin turns out to be zero, it costs nothing to demand a positive quantity of Bitcoin. Similarly, it costs nothing to perform either of the marginal trades discussed above, since they are at least zero-NPV actions across all pre-equilibria.

Proposition 5 *Under assumption 10, the model has only one equilibrium. In the unique equilibrium, $\eta = 1$, the value of Bitcoin is given by*

$$(1/P)_t = \frac{e_t}{Z_t}, \tag{29}$$

and the mining activity is uniquely determined, with $\zeta = \xi$.

Equation (29) is the usual equation of exchange (Fisher, 1911). In contrast to many studies which impose it ad-hoc or reserve for the 'long run', here it emerges as a necessary implication of equilibrium. Conditions (iii) and (iv) play key roles

[17]Condition (iv) could equivalently be formulated as a requirement of strict positivity of Lagrange multipliers μ and λ, defined in the proof of proposition 3.

in establishing this result. Both can be applied because the Bitcoin protocol is designed according to assumption 10, which guarantees that there *exists* a pre-equilibrium with $\eta > 0$ and $\zeta > 0$, in which case the market value of Bitcoin must be positive, and the households commit to strict preference towards both directions of trade tested by condition (iv).

4 Examples

We offer three examples in which $\alpha(s, s')$ satisfies assumption 10. In all examples, the households consume a constant fraction of endowment, so mining is not used to smooth consumption paths. All exchange is intermediated by the cryptocurrency, so no resources are wasted in non-monetary exchange, although a fraction of endowment must be lost due to mining. In all examples, the protocol can be designed to make the cost of mining arbitrarily small.

4.1 Money Growth Linked to Endowment Growth

In the first example, new money is created in a way to offset random fluctuations in the endowment. Suppose that the inefficiency of non-monetary exchange is large relative to the expected growth in utility-valued endowment (assuming that all endowment could be consumed):[18]

$$\bar{x} \equiv \min_{s} \int_{S} w(s, s') dF(s, s') - 1 + \kappa > 0. \tag{30}$$

Let $\alpha(s, s')$ be chosen such that

$$\frac{\alpha(s, s')}{1 + \alpha(s, s')} = x \left[\beta \left(1 + \lambda(s, s') \right)^{1-\gamma} \right]^{-1}, \tag{31}$$

where x is a constant in $(0, \min\{\underline{w}, \bar{x}\})$. It is easy to verify that the right-hand

[18]Condition (30) takes the simple form $\kappa > 1 - \beta$ if $\gamma = 1$ (log utility), or if there is no endowment growth. In either case, this is likely to be true empirically with β close to one.

side of (31) is in $(0,1)$, as required by the formulation. One can see that $\xi(s) = x$ is a solution to equation (14), with $\xi \in (0, \kappa)$.

To show that it is the only solution, write (14) in the form

$$(1-\xi_t)^{-\gamma} = \frac{x}{\xi_t} \mathrm{E}_t \left[(1-\xi_{t+1})^{-\gamma} \right], \tag{32}$$

where we have used (31), defined $\xi_t = \xi(s_t)$, and denoted the conditional expectation by E_t. If $\xi_t < x$, the process $\tau_t \equiv (1-\xi_t)^{-\gamma}$ is a (strict) super-martingale, assigning a positive probability to the event

$$\tau_{t+1} \leq \frac{1}{\theta_t} \tau_t,$$

where $\theta_t \equiv x/\xi_t > 1$. Since the function $(1-y)^{-\gamma}$ is increasing in y (for $y < 1$), this implies $\xi_{t+1} < \xi_t$, and hence $\theta_{t+1} \equiv x/\xi_{t+1} > \theta_t$. Conditional on this event, the process must then assign a positive probability to

$$\tau_{t+2} \leq \frac{1}{\theta_{t+1}} \tau_{t+1} < \frac{1}{\theta_t^2} \tau_t.$$

Continuing in this fashion, we find that the process must assign a positive probability that $\tau_{t+N} < 1$ for any natural number $N > -\gamma \log(1-\xi_t)/\log(\theta_t)$. Since this implies $\xi_{t+N} < 0$, the solution ultimately fails, with positive probability, to satisfy the lower bound on ξ_t specified in (a) of assumption 10. If instead $\xi_t > x$, implying $\theta_t < 1$, we can apply an analogous reasoning to show that the process must assign a positive probability to $\tau_{t+M} > (1-\kappa)^{-\gamma}$, which is equivalent to $\xi_{t+M} > \kappa$ for all natural numbers $M > \gamma[\log(1-\kappa) - \log(1-\xi_t)]/\log(\theta_t)$.

Under (30), the expression in the middle of (15) evaluates to $\int_S w(s,s')dF(s,s') - x$, which satisfies the strict inequalities required by part (b) of assumption 10.

Hence, the design function of the protocol satisfies assumption 10, and the results of the paper apply. By proposition 5, the unique equilibrium features $\eta = 1$, $\zeta = x$,

and the value function v is determined by proposition 1.

4.2 Log-Utility, Constant Money Growth

Suppose that $u(c) = \log(c)$ ($\gamma = 1$), and that

$$\beta > \kappa > 1 - \beta. \tag{33}$$

Let the design function of the protocol be a constant function $\alpha > 0$.

Under these assumptions, equation (14) becomes

$$\xi(s) = \beta \frac{\alpha}{1+\alpha} \int_S \left[\frac{1-\xi(s')}{1-\xi(s)} \right]^{-\gamma} dF(s, s'), \tag{34}$$

with solution $\xi = \beta \frac{\alpha}{1+\alpha}$. One can use the same reasoning as in the previous example to show that this is the only solution with $\xi \in (0, \kappa)$ as long as $\alpha < \kappa/(\beta - \kappa)$, which is possible to set under the left inequality of (33).

Under this solution, expression in the middle of (15) becomes $\frac{\beta}{1+\alpha}$, which satisfies both strict inequalities as long as $\alpha < \beta/(1-\kappa) - 1$, which is possible to set under the right inequality of (33).

Proposition 5 shows that there is only one equilibrium. In that equilibrium, $\eta = 1$, $\zeta = \xi$, and the value function v is uniquely determined by proposition 1.

4.3 Constant Endowment Growth and Money Growth

Assume

$$\frac{e_{t+1}}{e_t} = 1 + \lambda,$$

and restrict the parameters such that:

$$\beta(1+\lambda)^{1-\gamma} > \kappa > 1 - \beta(1+\lambda)^{1-\gamma}. \tag{35}$$

Once again, a constant $\xi = \beta(1+\lambda)^{1-\gamma}\alpha/(1+\alpha)$ solves (14), which satisfies the bounds of assumption 10 as long as $\alpha < \kappa/(\beta(1+\lambda)^{1-\gamma} - \kappa)$. It is possible to show that it is the only solution, using the same argument as in example 4.1. Concerning part (b) of assumption 10, both strict inequalities are satisfied when $\alpha < [\beta(1+\lambda)^{1-\gamma} - (1-\kappa)]/(1-\kappa)$. Hence, if α is set according to both requirements, proposition 5 can be applied to show that there is only one equilibrium, in which $\eta = 1$, $\zeta = \xi$, and the value function v is uniquely determined by proposition 1.

5 Conclusion

In this paper, we propose a model designed to answer the question of whether a representative cryptocurrency, similar in many respects to actual Bitcoin, can be uniquely valued in equilibrium under idealized conditions. We show that if the households are allowed to set their private valuations of marginal Bitcoin holdings according to certain rules of rational choice, then the answer is *yes*. It follows that self-fulfilling expectations (sunspots) cannot matter as causal factors affecting the value of our cryptocurrency.

Our solution concept extends in a natural way the notion of recursive competitive equilibrium of Lucas (1978), and collapses to (essentially) his definition in models where fiat money would necessarily be worthless, e.g., under complete markets. Our households do not behave strategically, since their choices depend on the set pre-equilibria, as opposed to the actions of other households. We do not invoke the properties of Pareto-(sub)optimality of alternative pre-equilibria, since the households are only concerned with their own welfare.

Our paper provides a theoretical support to the claim that cryptocurrencies are forms of money. Moreover, it is demonstrated that one does not need a central bank, government, or active policy intervention to *stabilize* the value of our cryptocurrency, if only the protocol can be designed to support unique equilibrium.

The scope of our work is limited in several ways. For example, we only consider

one cryptocurrency, whereas in reality there are many cryptocurrencies competing with national and privately issued currencies. Then, we assume exogenous endowment, while productive capacities of actual monetary economies are co-determined with the value of money. Finally, our model does not take into account a plethora of real-world complications like bounded rationality, costly adoption, price manipulation by strategic agents, etc. Hence, if one would like to argue that the value of actual Bitcoin is too volatile to be consistent with fundamentals, we cannot disagree before seeing a model like ours, but taking all important complications into account. Still, we believe that our paper significantly improves our understanding of the valuation of not just cryptocurrencies, but money in general.

References

Altug, Sumru and Pamela Labadie (2008), *Asset pricing for dynamic economies*. Cambridge University Press.

Aoyagi, Jun and Takahiro Hattori (2019), "The empirical analysis of bitcoin market in the general equilibrium framework." *http://dx.doi.org/10.2139/ssrn.3433833*.

Bariviera, Aurelio F, María José Basgall, Waldo Hasperué, and Marcelo Naiouf (2017), "Some stylized facts of the bitcoin market." *Physica A: Statistical Mechanics and its Applications*, 484, 82–90.

Benigno, Pierpaolo, Linda M Schilling, and Harald Uhlig (2019), "Cryptocurrencies, currency competition, and the impossible trinity." Technical report, National Bureau of Economic Research.

Berge, Claude (1963), *Topological spaces*. Oliver and Boyd.

Bhambhwani, Siddharth, Stefanos Delikouras, and George M. Korniotis (2019), *Do fundamentals drive cryptocurrency prices?*

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, Catherine Casamatta, and Albert J. Menkveld (2020), "Equilibrium bitcoin pricing." *http://dx.doi.org/10.2139/ssrn.3261063*.

Boud, John H. III (1990), "Recursive utility and the ramsey problem." *Journal of Economic Theory*, 50, 326–345.

Brock, William A. (1974), "Money and growth: The case of long run perfect foresight." *International Economic Review*, 750–777.

Cheah, Eng-Tuck and John Fry (2015), "Speculative bubbles in bitcoin markets? an empirical investigation into the fundamental value of bitcoin." *Economics Letters*, 130, 32–36.

Choi, Michael and Guillaume Rocheteau (2020), "More on money mining and price dynamics: Competing and divisible currencies." *http://dx.doi.org/10.2139/ssrn.3632646*.

Choi, Michael and Guillaume Rocheteau (2021), "Money mining and price dynamics." *American Economic Journal: Macroeconomics*, 13, 246–94.

Corbet, Shaen, Brian Lucey, and Larisa Yarovaya (2018), "Datestamping the bitcoin and ethereum bubbles." *Finance Research Letters*, 26, 81–88.

Fernández-Villaverde, Jesús and Daniel Sanches (2019), "Can currency competition work?" *Journal of Monetary Economics*, 106, 1–15.

Fisher, Irving (1911), *The purchasing power of money*. Macmillan. Assisted by H. G. Brown.

Fry, John (2018), "Booms, busts and heavy-tails: The story of bitcoin and cryptocurrency markets?" *Economics Letters*, 171, 225–229.

Garratt, Rodney and Neil Wallace (2018), "Bitcoin 1, bitcoin 2,....: An experiment in privately issued outside monies." *Economic Inquiry*, 56, 1887–1897.

Hahn, Frank H. (1965), *On some problems of proving the existence of an equilibrium in a monetary economy*. Macmillan.

Hicks, John R. (1935), "A suggestion for simplifying the theory of money." *Economica*, 2, 1–19.

Kang, Kee-Youn and Seungduck Lee (2019), "Money, cryptocurrency, and monetary policy." *http://dx.doi.org/10.2139/ssrn.3303595*.

Kiyotaki, Nobuhiro and Randall Wright (1989), "On money as a medium of exchange." *Journal of Political Economy*, 97, 927–954.

Kocherlakota, Narayana R. (1998), "Money is memory." *Journal of Economic Theory*, 81, 232–251.

Lagos, Ricardo, Guillaume Rocheteau, and Randall Wright (2017), "Liquidity: A new monetarist perspective." *Journal of Economic Literature*, 55, 371–440.

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

Lotz, Sébastien and Françoise Vasselin (2019), "A new monetarist model of fiat and e-money." *Economic Inquiry*, 57, 498–514.

Lucas, Robert E. (1978), "Asset prices in an exchange economy." *Econometrica*, 1429–1445.

Lucas, Robert E. (1980), "Equilibrium in a pure currency economy." *Economic Inquiry*, 18, 203–220.

Pagnotta, Emiliano and Andrea Buraschi (2018), "An equilibrium valuation of bitcoin and decentralized network assets." *http://dx.doi.org/10.2139/ssrn.3142022*.

Patinkin, Don (1965), *Money, interest, and prices; an integration of monetary and value theory*.

Radwanski, Juliusz F. (2021), "The purchasing power of money in an exchange economy." *http://dx.doi.org/10.2139/ssrn.3729256*.

Saleh, Fahad (2019), "Volatility and welfare in a crypto economy." *http://dx.doi.org/10.2139/ssrn.3235467*.

Samuelson, Paul A. (1958), "An exact consumption-loan model of interest with or without the social contrivance of money." *Journal of Political Economy*, 66, 467–482.

Schilling, Linda and Harald Uhlig (2019), "Some simple bitcoin economics." *Journal of Monetary Economics*, 106, 16–26.

Shi, Shouyong (1995), "Money and prices: A model of search and bargaining." *Journal of Economic Theory*, 67, 467–496.

Sidrauski, Miguel (1967), "Rational choice and patterns of growth in a monetary economy." *American Economic Review*, 57, 534–544.

Tirole, Jean (1985), "Asset bubbles and overlapping generations." *Econometrica*, 1499–1528.

Tobin, James (1980), "Discussion." In *Models of Monetary Economies* (Kareken J. H. and Wallace N., eds.), Federal Reserve Bank of Minneapolis.

Townsend, Robert M. (1980), "Models of money with spatially separated agents." In *Models of Monetary Economies* (Kareken J. H. and Wallace N., eds.), 265–303, Federal Reserve Bank of Minneapolis.

Trejos, Alberto and Randall Wright (1995), "Search, bargaining, money, and prices." *Journal of Political Economy*, 103, 118–141.

Wallace, Neil (1980), "The overlapping generations model of fiat money." In *Models of Monetary Economies* (Kareken J. H. and Wallace N., eds.), 49–82, Federal Reserve Bank of Minneapolis.

Williamson, Stephen and Randall Wright (2010), "New monetarist economics: Models." In *Handbook of Monetary Economics*, volume 3, 25–96, Elsevier.

Yu, Zhixiu (2021), "On the coexistence of cryptocurrency and fiat money." *http://dx.doi.org/10.2139/ssrn.3776097*.

Zhu, Yu and Scott Hendry (2018), "A framework for analyzing monetary policy in an economy with e-money." *http://dx.doi.org/10.2139/ssrn.3318915*.

A Definitions and Proofs

Definition 3 *Let $\mathcal{F}$ be the space of functions $f\colon \mathcal{D} \to \mathcal{R}$, where $\mathcal{D} \subset \mathcal{R}^k$ includes a copy of $\mathcal{R}_+$, with corresponding argument e. Let $\varphi(x_1, \ldots, e, \ldots, x_k) \in \mathcal{F}$ be given by $e^{1-\gamma}/(1-\gamma)$ if $\gamma \in (0,1) \cup (1,\infty)$, or $\log e$ if $\gamma = 1$. For any $g \in \mathcal{F}$ define the norm $\|g\|_\varphi = \sup_{x \in \mathcal{D}} |g(x_1, \ldots, e, \ldots, x_k)/\varphi(x_1, \ldots, e, \ldots, x_k)|$. Functions for which $\|g\|_\varphi < \infty$ will be called φ-bounded.*[19]

Proof of proposition 1.

- Let $\mathcal{V}$ be the Banach space of continuous φ-bounded functions $g\colon \mathcal{X} \to \mathcal{R}$. Let $\mathcal{T}$ be an operator on $\mathcal{V}$ defined such that condition (i) of definition 2 is equivalent to $\mathcal{T}v = v$. If $\zeta > 0$, applying $\mathcal{T}$ involves maximization of a continuous function on a compact set, so the maximum exists. Since the choice set $\mathcal{C}(h, z, e, u, s)$ is given by a continuous correspondence, the maximum is continuous in h, z, e, u, s (theorem of the maximum, Berge (1963)).

- The function $(\mathcal{T}v)(h, z, e, u, s)$ is φ-bounded, since the maximand in (21) is a sum of two φ-bounded functions. Indeed, this is true of $u(c)$ under the assumed CRRA utility, since

$$c \leq (1-\kappa)e + (1/P)m = e\left[(1-\kappa) + \eta(z,e)m/z\right],$$

  and both m/z and η are bounded. For the other part of the maximand,

$$\left|\frac{\beta v(h', z', e', u', s')}{\varphi(e)}\right| = \left|\beta \frac{\varphi(e')}{\varphi(e)} \frac{v(h', z', e', u', s')}{\varphi(e')}\right| \leq$$
$$\beta(1+\lambda)^{1-\gamma}\left|\frac{v(h', z', e', u', s')}{\varphi(e')}\right| \leq \left|\frac{v(h', z', e', u', s')}{\varphi(e')}\right| < \infty,$$

  by assumption 3, and because v is φ-bounded.

- For any $a > 0$ and $f \in \mathcal{V}$, it is easy to check that there exists $\delta \in (0,1)$ such that $\mathcal{T}(f + a\varphi)(z, e, u, s) \leq \mathcal{T}f(z, e, u, s) + \delta a \varphi(e)$. (Set $\delta = \bar{w}$, defined in (3) of the main text). In addition, $f \geq g$ implies $\mathcal{T}f \geq \mathcal{T}g$ for any $f, g \in \mathcal{V}$, and finally $\mathcal{T}0 \in \mathcal{V}$. These are the sufficient conditions of the weighted contraction mapping theorem (Boud, 1990; Altug and Labadie, 2008), and hence $\mathcal{T}$ has a unique fixed point $v = \mathcal{T}v$ in $\mathcal{V}$. In addition, $\lim_{n\to\infty} \mathcal{T}^n f = v$, for every $f \in \mathcal{V}$.

■

Lemma 1 *In a pre-equilibrium, the value function v is (weakly) concave in h, for all z, e, u, s.*

Proof of lemma 1.

Take any concave function $g(h, z, e, u, s) \in \mathcal{V}$. Fix z, e, u, s, let h^0, h^1 be chosen, and let m^i, y^i, q^i, $i \in \{0,1\}$, attain $(\mathcal{T}g)(h^i, z, e, u, s)$. Define $c^i = e[(1-\kappa) + \eta(m^i/z - (1-\kappa)y^i/z)] - q^i$, and $h'^i = h^i - m^i + q^i d$, $i \in \{0,1\}$. For $0 \leq \theta \leq 1$, define $h^\theta \equiv \theta h^0 + (1-\theta)h^1$, $(m^\theta, y^\theta, b^\theta) \equiv (\theta m^0 + (1-\theta)m^1, \ldots, \ldots)$, $c^\theta \equiv$

[19] This definition is standard (Altug and Labadie, 2008, ch. 8).

$\theta c^0 + (1-\theta)c^1$, and $h'^\theta \equiv \theta h'^0 + (1-\theta)h'^1$. Note that $m^\theta, y^\theta, q^\theta$ are feasible at h^θ, and $h'^\theta = h^\theta - m^\theta + q^\theta d$. At h^θ, $\mathcal{T}g$ satisfies

$$\begin{aligned}(\mathcal{T}g)(h^\theta, z, e, u, s) &\geq u(c^\theta) + \beta g(h'^\theta, z', e', u', s') \\ &\geq \theta(\mathcal{T}g)(h^0, z, e, u, s) + (1-\theta)(\mathcal{T}g)(h^1, z, e, u, s),\end{aligned}$$

which proves the concavity of $(\mathcal{T}g)(h, z, e, u, s)$ in h. Since concave functions form a Banach subspace of $\mathcal{V}$, the fixed point $v = \mathcal{T}v$ must also be concave in h.

■

Lemma 2 *If $\eta > 0$ in a pre-equilibrium, then $m > 0$, for all z, e, u, s.*

Proof of lemma 2.

Suppose $m = 0$, which also requires $y = 0$ by condition (ii) of definition 2. Increasing both m and y by a small number is feasible (since $h > 0$ and $\bar{y} > 0$). Since $\eta > 0$, this strictly increases consumption (22), and hence utility, without affecting h'. It follows that $m > 0$ is necessary in a pre-equilibrium with $\eta > 0$.

■

Proof of proposition 2.

- Fix z, e, u, s, and let $f(A) \equiv (\mathcal{T}v)(A, z, e, u, s)$. The maximand in (21) is continuous in m, y, and (since $\zeta > 0$) in q. Let $m(A)$, $y(A)$, $q(A)$ attain $f(A)$. Define $\tilde{u}(m) = u\left(\frac{e}{z}[\eta m + (1-\kappa)(z - \eta y] - q\right)$. Since $\eta > 0$, $\tilde{u}(m)$ is strictly concave in m, and $v(h', z', e', u', s')$ is concave in h' (lemma 1), and hence in m. It follows that the maximand in $(\mathcal{T}v)(A, z, e, u, s)$ is strictly concave in m, and hence $m(A)$, $y(A)$, and $q(A)$ are unique and continuous in A (Berge, 1963).

- Let $h'(A) = A - m(A) + y(A) + q(A)$. We know from lemma (2) that $m(A) > 0$. For small $\epsilon \neq 0$, $m(A) + \epsilon$ is feasible at $A + \epsilon$, and $m(A+\epsilon) - \epsilon$ is feasible at A. These observations, together with the definition of f, imply that

$$\begin{aligned}f(A+\epsilon) &\geq \tilde{u}(m(A)+\epsilon) + \beta \int_S v(h'(A), z', e', u', s') dF(s, s'), \\ &= \tilde{u}(m(A)+\epsilon) - \tilde{u}(m(A)) + f(A). \qquad (36)\end{aligned}$$

$$\begin{aligned}f(A) &\geq \tilde{u}(m(A+\epsilon)-\epsilon) + \beta \int_S v(h'(A+\epsilon), z', e', u', s') dF(s, s'), \\ &= \tilde{u}(m(A+\epsilon)-\epsilon) - \tilde{u}(m(A+\epsilon)) + f(A+\epsilon). \qquad (37)\end{aligned}$$

  Combining these inequalities,

$$\tilde{u}(m(A)+\epsilon) - \tilde{u}(m(A)) \leq f(A+\epsilon) - f(A) \leq \tilde{u}(m(A+\epsilon)) - \tilde{u}(m(A+\epsilon)-\epsilon).$$

  Dividing by ϵ, taking the limit $\epsilon \to 0$, using the continuity of $m(A)$, and the definition of $\tilde{u}(m)$, one finds that $f'(A) = u'(c)\frac{e}{z}\eta(z, e, u, s)$. The partial derivative of v with respect to h coincides with $f'(h)$, since $f = \mathcal{T}v = v$. This

is true in particular at $h = z$, the net worth of a representative household.

■

Proof of proposition 3. We will demonstrate the existence of a pre-equilibrium with $\eta = 1$. The proof will proceed in several steps.

- Since conditions of proposition 2 are met, the optimization problem (21) can be studied using the Lagrangian:

$$\begin{aligned}\mathcal{L} \equiv u\left(m\frac{e}{z}\eta + (1-\kappa)(e - y\frac{e}{z}\eta) - q\right) + \\ + \beta\int_S v(h')dF + \lambda(h-m) + \mu(y-\bar{y}),\end{aligned} \tag{38}$$

  where λ and μ are nonnegative multipliers.[20]

  The first-order conditions associated with m, y, and q are, respectively,

$$u'(c)\frac{e}{z}\eta - \beta\int_S v'(h')dF - \lambda = 0, \;\; \lambda \geq 0, \;\; \lambda(h-m) = 0, \tag{39}$$

$$-u'(c)\frac{e}{z}\eta(1-\kappa) + \beta\int_S v'(h')dF - \mu = 0, \;\; \mu \geq 0, \;\; \mu(\bar{y}-y) = 0, \tag{40}$$

$$-u'(c) + \beta\int_S v'(h')\frac{1}{d'}dF = 0. \tag{41}$$

  Combining (39) and (40) yields

$$u'(c)\frac{e}{z}\eta\kappa = \lambda + \mu. \tag{42}$$

  Multiplying condition (41) by q, using (28), $u'(c) = c^{-\gamma}$, $q/d' = g'$, $g'/z = \alpha$, and $\eta' = 1$, we obtain

$$\frac{q}{e} = \beta\int_S \left(\frac{c'}{c}\right)^{-\gamma}\frac{e'}{e}\frac{\alpha(s,s')}{1+\alpha(s,s')}dF. \tag{43}$$

- We will now show that $\eta = 1$ implies $e = c + q$ in a pre-equilibrium (no resources are wasted on inefficient forms of exchange). We first show that $\eta = 1$ implies $y = z$. The alternative is $y < z$, but then, since $y = m$ and $z = h$, we obtain $m < h$ and hence $\lambda = 0$, by condition (39). This implies $\mu > 0$ by condition (42), since the left-hand side is positive. This in turn requires $y = \bar{y}$, by condition (40). Since $\eta = 1$ and $\bar{\bar{y}} > 1$, $\bar{y}$ is given by the first line of (20), which implies $y = z$, a contradiction. Now, using $y = z$ and $\eta = 1$ in equation (22) results in $e = c + q$.

[20] We have simplified the notation by suppressing functional dependencies on most state variables. We use the prime (') symbol to denote both the derivatives and future values of the state variables. The meaning is uniquely determined by the context.

- Substituting the latter result into (43), using $q = \zeta e$ (pre-equilibrium condition), and (3), we obtain

$$\zeta(s) = \beta \int_S [1 + \lambda(s, s')]^{1-\gamma} \left[\frac{1 - \zeta(s')}{1 - \zeta(s)}\right]^{-\gamma} \frac{\alpha(s, s')}{1 + \alpha(s, s')} dF(s, s'). \tag{44}$$

  Under assumption (10) on the design of the cryptocurrency protocol, this has a (unique) solution $\zeta(s) \in (0, \kappa)$. By proposition (1), we know that there exists (exactly one) value function v consistent with the given η, ζ.

■

Proof of proposition 4. Suppose $\eta = 0$. Since the value function is increasing in h, a household solving the problem (21) optimally sets $m = 0$ and $y = \bar{y}(z, e, u, s) > 0$. Since $m = y$ is necessary by condition (ii), it must be that $\eta > 0$. The same argument applies at each z, e, u, s.

Suppose $\zeta = 0$. Since this implies zero mining difficulty, a household guided by a value function increasing in h optimally sets $q > 0$. Since $q = q^a$ by condition (ii), and since $\zeta = q^a/e$, this leads to a contradiction. Again, the argument is valid at each each z, e, u, s. ■

Proof of proposition 5. The proof uses some results and notation from the proof of proposition 3.

- Since under assumption (10) there exists a pre-equilibrium with $\eta > 0$, as shown in proposition 3, condition (iii) postulates that only those pre-equilibria for which $\eta > 0$ and $\zeta > 0$ can be equilibria. Then, by proposition 2, the associated value functions must be differentiable in h.

- Using the first-order conditions associated with the Lagrangian (38), and applying the formula for the partial derivative of proposition (2), all these pre-equilibria satisfy

$$(1 - \kappa) \leq \beta \int_S \frac{\frac{\partial}{\partial h} v^p(z', ...)}{\frac{\partial}{\partial h} v^p(z, ...)} dF(s, s') \leq 1.$$

  At the same time, the pre-equilibrium with $\eta = 1$, constructed in the proof of proposition 3, satisfies strict versions of these inequalities, which follows directly from the design of the cryptocurrency protocol, part (b) of assumption 10. Hence, by condition (iv) of definition 2,

$$(1 - \kappa) < \beta \int_S \frac{\frac{\partial}{\partial h} v^p(z', ...)}{\frac{\partial}{\partial h} v^p(z, ...)} dF(s, s') < 1$$

  must be true in all equilibria. This is equivalent to $\lambda > 0$ and $\mu > 0$.

- With $\lambda > 0$, the complementary slackness condition (39) implies $h = m$, which then implies $y = z$, by condition (ii) of definition 2. With $\mu > 0$, the complementary slackness condition (40) implies $y = \bar{y}$. Since $y < \bar{\bar{y}} z$ by condition (ii) of definition 2, $\bar{y}$ is determined by the first row of (20), and hence $y = z/\eta$. Combining these two results, $\eta = 1$ is the only possibility in

equilibrium. With $\eta = 1$, (29) follows from (16).

- Given $\eta = 1$, there is exactly one solution for ζ under assumption 10, as shown in the proof of proposition 3. Since that solution satisfies $\zeta > 0$, proposition 1 tells us that there is exactly one associated value function v.

■