WORKING PAPERS

N° 973

November 2021

"Equilibrium Bitcoin Pricing"

Bruno Biais, Christophe Bisière, Matthieu Bouvard, Catherine Casamatta and Albert J. Menkveld

Toulouse School of Economics

Equilibrium Bitcoin Pricing

Bruno Biais* Christophe Bisière† Matthieu Bouvard‡
Catherine Casamatta§ Albert J. Menkveld¶

November 9, 2021

Abstract

We offer a general equilibrium analysis of cryptocurrency pricing. The fundamental value of the cryptocurrency is its stream of net transactional benefits, which depend on its future prices. This implies that, in addition to fundamentals, equilibrium prices reflect sunspots. This, in turn, implies there are multiple equilibria and extrinsic volatility, i.e., cryptocurrency prices fluctuate even when fundamentals are constant. To match our model to the data, we construct indices measuring the net transactional benefits of bitcoin. In our calibration, a fraction of the variations in bitcoin returns reflects changes in net transactional benefits, but a larger fraction reflects extrinsic volatility.

*HEC Paris
†Toulouse School of Economics, Université Toulouse Capitole (TSM-Research)
‡Toulouse School of Economics, Université Toulouse Capitole (TSM-Research)
§Toulouse School of Economics, Université Toulouse Capitole (TSM-Research)
¶Vrije Universiteit Amsterdam

‖Many thanks for helpful comments to the editor, Stefan Nagel, the Associate Editor, two referees, as well as Will Cong, Patrick Fève, René Garcia, Co-Pier Georg, Alexander Guembel, Zhiguo He, Michael Kumhof, Nour Meddahi, Eric Mengus, Julien Prat, George Tauchen, Harald Uhlig, Boris Vallée, Stefan Voigt, Yu Wang and conference and seminar participants in the 2018 BIS Research Network meeting, the 2018 Becker Friedman Institute Conference on Blockchains and Cryptocurrencies, the 2018 Ridge Forum, the 2018 EuroFIT Conference at UCL, the 2019 WEF Davos, the 2019 Toronto FinTech Conference, the 2019 Tokenomics Conference, the 2019 Sustainable Finance Center Conference and Financial Econometrics Conference at TSE, the 2019 ESSFM in Gerzensee, the 2019 CEBRA Annual Meeting, the 2019 EFA Meeting, the 2020 AFA meeting, the 2021 AFFI meeting, Autorité des Marchés Financiers, Banque Centrale du Luxembourg, Banque de France, Cambridge University, CEIBS Shanghai, Central European University, Fudan University, HEC Paris, HEC Liège, Imperial College, Said Business School, University of Chile FEB, University of New South Wales, University Paris Dauphine, University of Technology Sydney and University of Vienna. We gratefully acknowledge support from the Jean-Jacques Laffont Digital Chair, the Norwegian Finance Initiative (NFI), the Netherlands Organization for Scientific Research (NWO Vici grant), the ANR (grant ANR-17-EURE-0010), EconPol Europe, and the European Research Council (grant 882375, WIDE).

1 Introduction

What is the fundamental value of cryptocurrencies? Do high market valuations reflect fundamentals or speculation? Does high volatility reflect investors' irrationality? We offer a framework to address these issues. In our framework, the fundamentals of a cryptocurrency are the net transactional benefits it is expected to provide.[1] Yet, in addition to changes in fundamentals, variation in equilibrium cryptocurrency prices reflects sunspot-driven extrinsic volatility. The contribution of this paper is thus to offer a theoretical formalisation and empirical quantification of the relationship between cryptocurrency prices, fundamentals, and extrinsic volatility.

Our theoretical model involves overlapping generations of agents, with stochastic endowments, who can trade standard fiat money (such as dollar) and a cryptocurrency (such as bitcoin). While both can be used to purchase consumption goods, the cryptocurrency can provide transactional benefits that standard money cannot. For example, citizens of Venezuela or Zimbabwe can use bitcoins to conduct transactions even when their national currencies and banking systems are in disarray. Also, cryptocurrencies can be used for cross-borders transfers when high costs or government controls hinder transfers via traditional financial institutions. Along with these transactional benefits, cryptocurrencies come with costs: limited convertibility into traditional currencies, transaction costs on exchanges, fees that agents must pay to have their transactions mined, and the risk of a crash of the cryptocurrency.

In our model, investors rationally choose their demand for cryptocurrency based on their beliefs about future prices and transactional benefits net of costs. This yields an Euler equation relating the current price of the cryptocurrency to the expectation of the stochastic discount factor multiplied by the sum of the future price and net transactional benefit. This highlights that transactional benefits are to cryptocurrencies what dividends are to stocks. There is, however, a major difference. In perfect markets, dividends, which do not depend on stock prices, provide a real anchor for stock valuations. In contrast, the transactional benefits provided by a cryptocurrency depend on its price: The higher the price of the cryptocurrency, the stronger its purchasing power relative to the standard currency, and

[1] Thus, when it becomes more likely that a cryptocurrency will facilitate transactions, its price should go up. For example, this is consistent with the rise in bitcoin price, following announcements that firms such as Paypal, MasterCard or Visa would integrate bitcoin in their payment architecture.

consequently the higher the transactional benefits it delivers via the purchase of goods. Because cryptocurrency prices reflect beliefs about future prices rather than real variables independent of prices, equilibrium can reflect exogenous sunspots.[2] This major difference between cryptocurrencies and stocks precludes a standard Campbell and Shiller (1988b) decomposition, but, as explained below, we propose an alternative decomposition.

Characterising equilibrium currency price processes is challenging. One of our contributions is to offer a new characterisation of two classes of equilibria: First, we consider "constant price equilibria" in which, at each period, there can be a sunspot leading to a crash in which the cryptocurrency price permanently drops to zero, while the standard currency price remains positive. Before and after the crash, however, prices of both currencies are constant. We show there are multiple constant price equilibria, one for each possible constant value of the crash probability. Second, we characterise "volatile price equilibria," in which sunspots can trigger price changes at each period. To do so, we consider an arbitrary horizon of N periods. From period N onwards, the continuation equilibrium falls in the class of "constant price equilibria." There are different continuation constant price equilibria, one for each value of the crash probability prevailing from period N onwards. These different crash probabilities determine the state of the sunspot at that time, and the corresponding equilibrium price.[3] By backward induction we then obtain the equilibrium cryptocurrency price at period $N-1$, as a function of the state of the sunspot at $N-1$, the transition probabilities from that state to the period N state, and the corresponding possible values of the cryptocurrency price at period N. Iterating, backward induction yields the sequence of equilibrium cryptocurrency prices at all periods before $N-1$.

There is equilibrium multiplicity since there exists an equilibrium for each possible *distribution* of the trajectory of the sunspot variable. Moreover, within each equilibrium (i.e., for each distribution of the sunspot), there is extrinsic volatility, since cryptocurrency prices change, in response to the random evolution of the sunspot variable, even when fundamental variables remain constant. While related, equilibrium multiplicity and extrinsic volatility are different concepts. On the one hand, there are multiple constant price equilibria, in each of which, except at the time of the crash, there is no volatility. On the other hand, within

[2]This is less of an issue for official currencies, such as the dollar or the euro, whose fundamental value reflects that they can be used to pay taxes (see, e.g., Starr, 1974).

[3]Precisely, the state of the sunspot includes whether a crash occurred, and what is the belief about a crash occurring in the current period.

a given volatile price equilibrium, there is volatility, as the sunspot and consequently the prices vary randomly *on the equilibrium path*.[4]

For isoelastic utilities, we can further identify the economic determinants of equilibrium cryptocurrency prices. The price of the cryptocurrency increases with its transactional benefits and decreases with its crash risk. Moreover, risk averse investors require a risk premium to hold the cryptocurrency in spite of its crash risk.

To confront our theory to the data, we compile data from 20 major exchanges to construct a time series of bitcoin prices from July 2010 to December 2018. We also construct three time series that proxy for the transactional costs and benefits of bitcoin. First, we collect the time series of the transaction fees paid by bitcoin users to miners entering transactions in the blockchain. These fees are high when the number of trades in bitcoin is very high, leading to congestion in the blockchain. Thus, high transaction fees are not only costly by themselves but also signal other costs of bitcoin associated with delays and congestion. For the two other time series, we browse the web archives to collect information on events likely to affect the costs and benefits of transacting in bitcoin. We categorise these events into two subsets. The first subset captures further information on the transaction costs of bitcoin. More specifically, it contains events indicative of the ease with which bitcoins can be exchanged against other currencies, such as a new currency becoming tradable against bitcoin or the shutdown of a large platform. The second subset captures information on transactional benefits: it contains events affecting the ease with which bitcoin can be used to purchase goods and services, such as merchants starting or ceasing to accept bitcoin as means of payment. Based on these two subsets of events, we construct two indices proxying for transactional costs and transactional benefits, respectively. Finally, we collect data about bitcoin thefts and hacks, to obtain a measure of the corresponding losses.

Using these data, we calibrate our model. For simplicity, in the calibration, we focus on

[4]Equilibrium multiplicity was previously obtained for stocks by Spiegel (1998), Watanabe (2008), Biais, Bossaerts and Spatt (2010), and Bacchetta, Tille and van Wincoop (2012). Both in these models and the present one, multiplicity arises because of overlapping generations. One difference between these models and the present one is that, while they assume investors born at time t maximise the expected utility of their time $t+1$ consumption and the risk free rate is constant, we take a general equilibrium approach in which investors maximise the expected utility of their current and future consumption and all rates of return are endogenous. So, in our analysis, required returns reflect the marginal rates of substitution between current consumption and future consumption in the different possible states. Excess volatility also obtains in Spiegel (1998) but it is driven by random stock supplies, unlike in the present paper, in which excess volatility is driven by sunspots.

the special case in which investors are risk neutral. Empirically, risk neutrality is likely to be an admissible shortcut, because Liu and Tsyvinski (2021) find that, for our sample period, cryptocurrency returns are not significantly correlated with consumption or production growth. Theoretically, our analysis of the risk averse case shows that cryptocurrency price changes do not affect much standard currency prices, and investors' consumption, as long as the bitcoin capitalisation is small relative to that of GDP. Current bitcoin market capitalisation represents 1.3% of world GDP, which suggests that risk neutrality is a reasonable approximation. In the risk neutral case, we obtain an expression for cryptocurrency required returns that holds across all possible equilibria.[5] While we calibrate the exact (nonlinear) form of this restriction, its linearisation is useful to give intuition, as it states that the expected return must equal the sum of the probability of a crash and the transactions and hacks costs, minus the expected transactional benefits of the cryptocurrency.

For the calibration, we specify transactional costs and benefits as linear functions of the empirical variables whose construction is described above. The coefficients of these linear functions are set to minimise the root mean squared difference between the required returns implied by our calibrated model and the realised returns. This yields coefficients with signs in line with economic intuition, as they imply required returns that increase in transactional costs and decrease in transactional benefits. That said, we do not claim statistical significance or estimation of population parameters. This is precluded by the relatively short size of our sample and the fact that our variables (in particular transactional costs and benefits) are likely to be non-stationary.

We find that required bitcoin weekly returns start at a high level (between 8% and 18% per week) in 2010 and 2011, remain between 2% and 8% for the next couple of years, and drop below 2% during the rest of the sample period, except in the last months of 2017. In the calibration, crash risk explains around 11 percentage points of the required return during the first two years of the sample period. Then, as time goes by, the probability of a crash and its contribution to required returns decrease to close to zero, reflecting that no crash occurred during the sample period. The costs associated with the mining fees and delays and congestion on the blockchain are negligible throughout the sample except for 2017. During 2017 they spike up, especially towards the end of the year, at which point they explain up to 10 percentage points of the calibrated required return. The index proxying for the

[5] In the risk neutral case, as in the risk averse case, there is equilibrium multiplicity and extrinsic volatility.

difficulty to exchange bitcoin against standard currency adds almost 10 percentage points to the calibrated required return at the beginning of the sample. Within a year, however, its contribution to the calibrated required return drops to around eight percentage points. It then remains around that level throughout the rest of the sample period. The contribution of hack risk is relatively small, as it amounts to only four basis points. Against these costs, the calibrated transactional benefit component starts around zero at the beginning of the sample but increases until 2015. From that point on the calibrated transactional benefit, which underlies the fundamental value of the cryptocurrency, is around 8%. This is admittedly high, and maybe implausible. It is useful, however, to compare this magnitude to that of the cost of cross border fund transfers, which cryptocurrencies can help avoid. For example data from the World Bank suggests that remittance costs are around 6%.[6]

While our calibration quantifies the effect of fundamentals on required expected returns, it also shows that changes in fundamentals only explain a small share (around 5%) of the variance of bitcoin returns. Under the hypothesis that our model is well specified and our proxies accurate, this implies that the lion's share of bitcoin fluctuations reflects another feature of the equilibria we characterise, extrinsic volatility unrelated to fundamentals.

Literature: Our theoretical analysis is in line with the classic overlapping generations models of money (Samuelson, 1958, Wallace, 1980, and Tirole, 1985), which have also been extended to cryptocurrencies by Saleh (2020) and Garratt and Wallace (2018). In a one-currency model, Saleh (2020) compares equilibrium prices and welfare in two protocols: proof-of-burn and proof-of-work. Garratt and Wallace (2018) use the Kareken and Wallace (1981) model of several currencies to analyse the joint determination of the prices of a cryptocurrency (say bitcoin) and a standard currency (say dollar). An important ingredient in their analysis is that at each period, there can be a sunspot leading to a crash in which the cryptocurrency price permanently drops to zero. This gives rise to the "constant price equilibria" we also analyse. The incremental contribution of our theoretical analysis, relative to that of Garratt and Wallace (2018), is twofold.[7] First, for "constant price equilibria" we complement Garratt and Wallace (2018) by solving explicitly for the cryptocurrency price in

[6]See "The World Bank, Remittance Prices Worldwide," available at `http://remittanceprices.worldbank.org`.

[7]While we confront our theoretical model to the data, the analysis in Garratt and Wallace (2018) is purely theoretical.

the isoelastic case. This enables us to conduct comparative statics analysis of the economic drivers of the cryptocurrency price. Second, in addition to "constant price equilibria", we characterise a new class of equilibria: "volatile price equilibria", in which sunspots trigger cryptocurrency price changes at each period, resulting in volatile equilibrium cryptocurrency price paths, even when fundamentals remain constant.[8]

Schilling and Uhlig (2019) study the interaction between bitcoin and dollars in a model in which agents live forever, but alternate between consumption and production. This alternation generates non double coincidence of wants so that money plays a role in facilitating exchanges, similar to the role it plays in the overlapping generations model. Schilling and Uhlig (2019) show that, if consumption and the price of dollar are independent from the price of bitcoin, then the latter follows a martingale. This is similar to the condition we obtain in the risk neutral case, except that the pricing equation in Schilling and Uhlig (2019) does not feature the transactional costs and benefits of the cryptocurrency, which play a central role in our analysis. Instead, Schilling and Uhlig (2019) focus on the public policy implications of the introduction of a cryptocurrency, which we do not analyse.[9] Benigno, Schilling and Uhlig (2019) develop this line of research further by showing how a global cryptocurrency may enforce a synchronisation of interest rates across countries.

Also in relation with the monetary theory literature, Chiu and Koeppl (2021), Hendry and Zhu (2019), Fernández-Villaverde and Sanches (2019), Pagnotta (2021), and Auer, Monnet and Shin (2021) extend the Lagos and Wright (2005) model to the case of cryptocurrencies. An important feature of the models studied by Chiu and Koeppl (2021) and Pagnotta (2021) is the risk of an attack on the network, which decreases with the hashpower that miners dedicate to the network. In Pagnotta (2021) there are multiple equilibria: If the cryptocurrency is expected to be safe, its price is high. This induces many agents to engage in mining,[10] thus making the cryptocurrency safe. But there is also a rational expectations equilibrium in which the cryptocurrency is expected to be risky, its price is low, and there is little mining. The multiplicity of equilibria in Pagnotta (2021) differs from that arising in our model. In Pagnotta (2021) equilibrium multiplicity reflects the loop between prices and mining, in our

[8]Zimmerman (2020) proposes a different model in which the volatility of cryptocurrency prices arises from the blockchain transaction validation process.

[9]Hendry and Zhu (2019) also study monetary policy implications of the existence of cryptocurrencies.

[10]Relatedly, Prat and Walter (2021) analyse theoretically and empirically how increases in bitcoin prices induce miners' entry.

paper it reflects that investors can coordinate on different beliefs about the likelihood of a crash. Fernández-Villaverde and Sanches (2019) and Choi and Rocheteau (2020) analyse models in which agents can create private monies at a cost, and show there exist equilibria in which the value of private monies eventually vanishes. Choi and Rocheteau (2020) characterise the set of all deterministic perfect foresight equilibria, which differs from our focus on stochastic equilibrium price paths. The focus of Fernández-Villaverde and Sanches (2019) on the consequences of the shape of the entrepreneurs' cost function and the quantity of money differs from our focus on the transactional benefits and costs of the cryptocurrency and the agents' beliefs on the risk of a crash. Auer, Monnet and Shin (2021) jointly analyse the use of cryptocurrencies in a Lagos-Wright framework and the strategic contribution of validators to the validation of trades conducted on the blockchain. Their emphasis on the optimal design of the validation mechanism differs from our emphasis on the dynamics of cryptocurrency prices in general equilibrium.

Another interesting strand of the literature to which our paper is related focuses on platforms within which agents can use cryptocurrencies to reap gains from trade. In Athey et al. (2016), the platform is used by the agents to transfer funds abroad, for example to their family, as in remittances. An important ingredient in this model is the risk of a fatal flaw making the platform vulnerable to a successful attack. As time goes by, if there is no crash, Bayesian learning leads to a decrease in the probability of platform disruption, and more and more people adopt the platform. Similarly, in our model, there is a risk that the cryptocurrency crashes. Our model encompasses the case in which a crash could be triggered by a real event, as in Athey et al. (2016), and the case in which the crash is triggered by a sunspot. It is the latter aspect of our analysis, which is not present in Athey et al. (2016), which enables us to construct volatile price equilibria, in which bitcoin price variation reflects extrinsic volatility unrelated to fundamentals. Cong, Li and Wang (2021) also consider a platform, in which agents can use cryptocurrency tokens to conduct peer to peer transactions, and thus benefit from transactional benefits. An important ingredient in Cong, Li and Wang (2021) is that there are network externalities: The larger the number of platform users, the larger the transactional benefits each gets. This implies there can be equilibrium multiplicity. But the source of multiplicity in Cong, Li and Wang (2021): network externalities, differs from that in our paper: sunspots. Another important feature of the model analysed by Cong, Li and Wang (2021) is that transactional benefits are increasing in the platform productivity,

which evolves randomly. Network externalities amplify the impact of productivity shocks on token prices. The corresponding "excess volatility" of cryptocurrency prices differs from the extrinsic volatility in our analysis: In Cong, Li and Wang (2021) excess volatility reflects changes in fundamentals, in our analysis extrinsic volatility is unrelated to fundamentals. Sockin and Xiong (2020) also offer a model of cryptocurrency valuation in the presence of positive network externalities. They show that by delegating control to users, tokenization creates commitment not to exploit users.

On the empirical side, Makarov and Schoar (2020), Borri and Shakhnov (2019), and Hautsch, Scheuch, and Voigt (2020) document mispricings and arbitrage opportunities across exchanges for bitcoin. Rather than on differences in prices at the same point in time, our work focuses on the dynamics of equilibrium cryptocurrency prices. This relates our paper to Liu and Tsyvinski (2021), Liu, Tsyvinski and Wu (2021), Bianchi (2020), and Bhambhwani, Delikouras and Korniotis (2019). Liu and Tsyvinski (2021) document that cryptocurrency returns are not significantly correlated with consumption or production growth, but are exposed to cryptocurrency network factors. Liu, Tsyvinski and Wu (2021) show that three factors: cryptocurrency market, size, and momentum, capture the cross section of cryptocurrencies' expected returns. In contrast with that literature, our empirical focus is on i) measuring the costs and benefits of bitcoin and ii) using these measures to calibrate our theoretical model. Our indices measuring the ease and cost of using bitcoins are in the same line as the index constructed by Auer and Claessens (2018) to measure the extent to which regulation is favourable to cryptocurrencies. Both Auer and Claessens (2018) and the present paper study how the evolution of such indices relates to the evolution of cryptocurrency prices. Differences between Auer and Claessens (2018) and our paper include Auer and Claessens (2018)'s focus on regulatory events and our reliance on a theoretical model.

2 Model

Time is discrete and divided into periods and the horizon is infinite. There is one consumption good and three assets: a cryptocurrency (e.g., bitcoin), in supply X_t at period t, a standard currency (e.g., dollar) in fixed supply m, and a risk-free asset in zero net supply.

There are investors, miners and hackers. All are competitive and take prices as given. We consider miners and hackers in order to introduce two important features of the cryptocur-

rency: the creation of new coins and the risk of hacks. In our model their actions are very simple: they perform their activity and then sell their cryptocurrency holdings and consume. In contrast, we analyse in detail the consumption and savings decisions of investors, which, combined with market clearing, pin down equilibrium pricing.

At each period t a new generation of miners is born. Miners born at period t mine until $t+1$, at which point they get rewarded by newly created coins, $X_{t+1} - X_t$, and transaction fees. At period $t+1$ they sell their coins against consumption goods, which they consume (along with the fees they received) before exiting the market. Denote by c^m_{t+1} the consumption of miners at period $t+1$.

Similarly, at each period t, a new generation of hackers is born. They try to steal some cryptocurrency, for example by hacking a cryptocurrency exchange (like Bitfinex in 2016) or a decentralized autonomous organization (like the DAO built on top of Ethereum, also in 2016).[11] The fraction they manage to steal is a random variable living in $[0, 1]$, which we denote by h_{t+1}. The index $t+1$ reflects the fact that the fraction stolen is not known by investors at t, and is only discovered at $t+1$. At period $t+1$, hackers sell their stolen coins against consumption goods, which they consume before exiting the market. Their consumption is denoted by c^h_{t+1}.

Finally, a mass one continuum of investors are born at each period. They live and consume during two periods, have separable additive utility $u(.)$, with $u' > 0$ and $u'' \leq 0$, and discount factor β. At each period, their utility is defined over positive consumption and the transactional benefits of using cryptocurrencies. To simplify the analysis, we assume that consumption and transactional benefits enter additively in the utility function. To initialise the model, at date 1 there is also a generation of old investors, miners and hackers, who hold the supply of cryptocurrencies X_1 and standard currency m.

At period t, each young investor is endowed with e_t units of consumption good, can buy q_t units of cryptocurrency, or coins, at unit price p_t, $\hat{q}_t$ units of standard currency at unit price $\hat{p}_t$, and can save s_t. For notational simplicity, the consumption good is the numeraire. That is, p_t (resp. $\hat{p}_t$) is the number of units of consumption good that can be purchased

[11] There could also be security breaches resulting in thefts for the standard currency. For instance, hackers used the SWIFT system to steal reserves of the Central Bank of Bangladesh at the New York Fed (see "The billion-dollar bank job" by J. Hammer published in the NYtimes on May, 3, 2018.) However, because cryptocurrency ownership is defined outside the legal system, it is more vulnerable to such thefts. To capture this, we set $h_t \geq 0$ for the cryptocurrency only.

with one unit of cryptocurrency (resp. standard currency) at period t.

When buying cryptocurrency, each investor incurs a linear cost $\varphi_t q_t p_t$, with $\varphi_t \geq 0$. Thus, the young investor's budget constraint is:

$$c_t^y = e_t - s_t - q_t p_t - \hat{q}_t \hat{p}_t - \varphi_t q_t p_t. \tag{1}$$

The cost term $\varphi_t q_t p_t$ reflects the cost of having a wallet, going through crypto-exchanges, transactions fees, etc. It is indexed by t to capture the notion that this cost can change with time. We assume that this cost is paid when buying the cryptocurrency, and thus depends on the cryptocurrency price at period t.[12]

When old, in period $t+1$, each investor consumes savings, plus proceeds from sale of currencies. For the standard currency these proceeds are $\hat{q}_t \hat{p}_{t+1}$. For the cryptocurrency, proceeds are $(1-h_{t+1})q_t p_{t+1}$, where, as mentioned above, h_{t+1} is the fraction of cryptocurrency holdings that is stolen by hackers, between t and $t+1$. Thus, old investors consume

$$c_{t+1}^o = s_t(1+r_t) + (1-h_{t+1})q_t p_{t+1} + \hat{q}_t \hat{p}_{t+1}. \tag{2}$$

We assume that old investors also receive transactional benefits $(1-h_{t+1})\theta_{t+1} q_t p_{t+1}$ generated by cryptocurrencies. For example, those benefits can stem from the ability to send money, possibly to another country, without using the banking system, and without being controlled by the government. Another example is that cryptocurrencies can enable agents holding them to use more easily smart contracts and tokenized assets. Since the agent uses cryptocurrency to buy consumption at period $t+1$ the transactional benefits reflect the period $t+1$ price. We denote $\hat{c}_{t+1}^o = c_{t+1}^o + (1-h_{t+1})\theta_{t+1} q_t p_{t+1}$ the sum of the consumption and transactional benefits that enters into the utility function of old investors.

We assume that $\theta_{t+1} \geq -1$.[13] Equation (2) then implies that old agents sell all their holdings of cryptocurrency $(1-h_{t+1})q_t$ to increase their consumption. Note that, in our theoretical and our empirical analyses, we assume $\{X_t\}_{t>0}$, $\{\theta_t\}_{t>0}$ and $\{\varphi_t\}_{t>0}$ are exogenous processes, independent from the actions of the agents in the market.

[12] The analysis remains largely unchanged if we include a cost when selling the cryptocurrency at $t+1$ as well.

[13] If $\theta_{t+1} < -1$, then old agents would be better off not selling their holdings if p_{t+1} was strictly positive. Market clearing would then imply $p_{t+1} = 0$. Assuming $\theta_{t+1} \geq -1$ rules out this degenerate case.

Finally the budget constraints of miners and hackers born at period t are

$$c_{t+1}^m = (X_{t+1} - X_t)p_{t+1} + \varphi_{t+1}q_{t+1}p_{t+1} \tag{3}$$

and

$$c_{t+1}^h = h_{t+1}q_t p_{t+1}, \tag{4}$$

respectively.

As in Garratt and Wallace (2018), we allow for the possibility that, at the end of each period t, with probability π_t, there is a crash, and the cryptocurrency price permanently drops to 0, i.e., $p_{t+s} = 0$, for all $s > 0$. As discussed in Garratt and Wallace (2018), the occurrence of a crash can be due to a sunspot (see Cass and Shell, 1983). In that interpretation, the crash is a purely extrinsic random variable. It does not reflect any change in the fundamentals but an extrinsic change in beliefs, triggered by a sunspot, independent from all the other variables, e.g., θ_t, φ_t or p_t.

A crash occurs all agents believe the cryptocurrency is worthless. Hence they reject payment in the cryptocurrency, which thus becomes worthless. So the agents' belief is self-fulfilling. An alternative interpretation of the crash is that it is triggered by a real event, such as the discovery of a flaw in the protocol, a successful attack on the blockchain (for example a 51% attack), or a sudden change in the political and legal environment making it impossible to use the cryptocurrency.

In our model, the standard currency price could also go to zero. As shown in Starr (1974), however, this can be prevented when the government levies taxes which must be paid in that currency: Even if agents anticipate the others not to accept the standard currency, as long as they know the government will accept it for the payment of taxes, the demand for the standard currency is strictly positive at prices bounded away from zero.[14] So, in our analyses, we focus on equilibria in which the price of the standard currency is strictly positive at all times.

The sequence of events at each period is summarised in Figure 1. As can be seen in Figure 1, the probability π_t of a crash during period t is determined at the beginning of period t. In the sunspot interpretation of crashes, π_t is the realisation of a random variable independent from all other variables in the information set of agents at the beginning of period t. Whether

[14]For a recent analysis of these issues see Gaballo and Mengus (2021).

there is a crash in period t or not is determined by the realisation of a random variable at the end of period t. In the sunspot interpretation of crashes, the distribution of this random variable depends only on π_t and is independent from all the other variables in the information set of the agents period t.

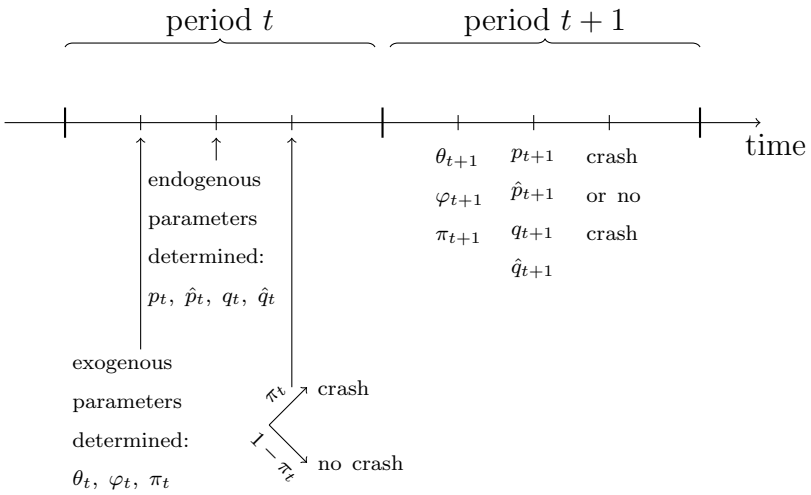


Figure 1: Sequence of events.

3 Equilibria

3.1 The general case

A rational expectation equilibrium is defined by prices $\{p_t, \hat{p}_t, r_t\}_{t>0}$ and portfolio decisions $\{q_t, \hat{q}_t, s_t\}_{t>0}$ such that

(i) $\{q_t, \hat{q}_t, s_t\}$ maximises generation t investors' expected utility, given prices and subject to the budget constraints (1) and (2), and to consumptions being positive, while the consumptions of the miners and hackers are set by (3), and (4), respectively,

(ii) at each period t, the markets for the cryptocurrency, the standard currency and the risk-free asset clear: $q_t = X_t$, $\hat{q}_t = m$, and $s_t = 0$.[15]

[15]By Walras's law, the market for the consumption good also clears, that is: $c_t^y + c_t^o + c_t^h + c_t^m = e_t$.

A young investor at period t solves

$$\begin{aligned} &\max_{q_t, s_t, \hat{q}_t} u(c_t^y) + \beta E_t u(\hat{c}_{t+1}^o) \\ \text{s.t.} \quad &c_t^y \geq 0, \ (1), \ (2) \end{aligned}$$

where E_t is the expectation conditional on the information set of the agents at the beginning of period t, which includes, in particular, θ_t, φ_t, and π_t (see Figure 1). Assume first that the positive consumption constraint does not bind. The first order optimality condition with respect to q_t yields

$$p_t = \beta E_t \left[\frac{u'(\hat{c}_{t+1}^o)}{u'(c_t^y)} (1 - h_{t+1}) \frac{1 + \theta_{t+1}}{1 + \varphi_t} p_{t+1} \right], \tag{5}$$

or equivalently,

$$p_t = \beta (1 - \pi_t) \ E_t \left[\frac{u'(\hat{c}_{t+1}^o)}{u'(c_t^y)} (1 - h_{t+1}) \frac{1 + \theta_{t+1}}{1 + \varphi_t} p_{t+1} \middle| \text{no crash} \right]. \tag{6}$$

The first order condition with respect to s_t is

$$\beta = \frac{1}{1 + r_t} \frac{u'(c_t^y)}{E_t \left[u'(c_{t+1}^o) \right]}. \tag{7}$$

On the equilibrium path, at period t old investors cannot borrow or lend, since they won't be present in the market at period $t + 1$. Hence, in equilibrium $s_t = 0$. So the interest rate must adjust so that (7) holds when evaluated at $s_t = 0$.

Denote

$$1 + \mathcal{T}_{t+1} = \frac{1 + \theta_{t+1}}{1 + \varphi_t}. \tag{8}$$

$\mathcal{T}_{t+1}$ can be interpreted as the net transactional benefit per unit of the cryptocurrency, reflecting its transactional benefits (θ_{t+1}) net of its transactions costs (φ_t). Using (7) to replace β into (5), we obtain our first proposition.

Proposition 1 *The equilibrium price of the cryptocurrency at period t is such that*

$$p_t = \frac{1}{1 + r_t} E_t \left(\frac{u'(\hat{c}_{t+1}^o)}{E_t \left[u'(\hat{c}_{t+1}^o) \right]} (1 - h_{t+1}) \left(p_{t+1} + \mathcal{T}_{t+1} p_{t+1} \right) \right), \tag{9}$$

or, equivalently, for an arbitrary $K > 1$,

$$p_t = E_t \left(\sum_{k=1}^{K} \left(\prod_{j=1}^{k} \frac{1 - h_{t+j}}{1 + r_{t+j-1}} \frac{u'(c^o_{t+j})}{E_t \left[u'(c^o_{t+j}) \right]} \mathcal{T}_{t+k} p_{t+k} \right) + \left(\prod_{j=1}^{K} \frac{1 - h_{t+j}}{1 + r_{t+j-1}} \frac{u'(c^o_{t+j})}{E_t \left[u'(c^o_{t+j}) \right]} \right) p_{t+K} \right) \tag{10}$$

In Appendix 1, we complete the proof of Proposition 1 by showing that (9) also holds when the constraint that consumption is positive binds.

Fundamental value, price and transactional benefit. Equation (9) states that the price of the cryptocurrency at period t is equal to the present value of the expectation of the product of three terms: i) The first term is the pricing kernel, capturing the correlation between the marginal utility of consumption and the cryptocurrency price. ii) The second term reflects the risk of hacks. iii) The third term is the sum of the price of the cryptocurrency at period $t + 1$ and its net transactional benefit.

(10) rewrites (9) to show that the equilibrium price p_t is the sum of the discounted expected transactional benefits brought by the cryptocurrency $\mathcal{T}_{t+k} p_{t+k}$, which correspond to its fundamental value. (10) is similar to its counterpart for stocks, except that instead of stemming from the transactional benefits $\mathcal{T}_{t+k} p_{t+k}$, the fundamental value would stem from the firm's dividend. This points to an essential difference between the fundamental value of a currency and that of a stock. For stocks, in perfect markets, current valuation reflects the expectation of future dividends, which do not depend on future stock prices. Thus, valuation is anchored by a fundamental variable independent of future prices. In contrast, for currencies, there is no such anchor, since endogenous future prices determine transactional benefits. This lack of exogenous anchor raises the possibility of equilibrium multiplicity and extrinsic volatility, as explained below.[16] Equation (10) further shows that, for the cryptocurrency price to be strictly positive at time t, its net transactional benefit τ_{t+k} must be positive for some k. Equation (10), however, does not rule out the possibility that, in the short term, net transactional benefits could be negative, as long as they would be expected to become sufficiently positive in the long term.

[16] As will be clarified below, such equilibrium multiplicity goes far beyond the possibility that, when there exists an equilibrium with $p_t > 0$, there also exists another equilibrium with $p_t = 0$.

3.2 Constant price equilibria with risk averse agents

It is difficult, in our stochastic infinite horizon setting, to explicitly solve for equilibrium prices when agents are risk averse. There is one relatively simple case, however, in which we can further characterise equilibrium prices: equilibria in which prices are constant until there is a crash, bringing the cryptocurrency price down to zero. In this subsection the crash probability is constant, and denoted by π.[17] By a slight abuse of language, we refer to these equilibria as "constant price equilibria", although, of course, at the time of the crash they involve a sharp change in prices. Admittedly, these constant price equilibria are not very plausible, because they do not allow for volatility except at the time of the crash. But they offer a simple laboratory in which to develop intuition about the economics of currency pricing. They also serve as a building block, which we use below to characterise more general and plausible equilibria, with volatile prices.

To study constant price equilibria, for simplicity we assume that endowments, cryptocurrency supply, costs, and benefits are constant, i.e. $e_t = e$, $X_t = X$, $\varphi_t = \varphi$, $\theta_t = \theta$ et $h_t = h$. In the event of a crash, the cryptocurrency price goes to 0. We also assume $(1-h)(1+\theta) > 1+\varphi$ so that the net transactional benefit of the cryptocurrency is positive, which is necessary for the cryptocurrency to have a positive price. Finally, we assume that $u'' < 0$, so we can analyse the consequences of investors' risk aversion on currency pricing.

3.2.1 General preferences

Denote by p and $\hat{p}$, respectively, the prices of the cryptocurrency and the standard currency, which remain constant as long as there is no crash. The equilibrium condition for the cryptocurrency (6) is

$$u'(e - X(1+\varphi)p - m\hat{p})p = \beta(1-\pi)(1-h)\frac{1+\theta}{1+\varphi}u'((1-h)Xp(1+\theta) + m\hat{p})p. \qquad (11)$$

The left-hand side of (11) is the period t price of the cryptocurrency, evaluated at the marginal utility of young investors at that time, while the right-hand side is the present value of the period $t+1$ price of the cryptocurrency when there is no crash, evaluated at the

[17] In the next subsection we extend the analysis to the case in which the probability of a crash evolves stochastically.

marginal utility of old investors at that time. We focus on strictly positive prices.[18] So (11) simplifies to

$$u'(e - X(1+\varphi)p - m\hat{p}) = \beta(1-\pi)(1-h)\frac{1+\theta}{1+\varphi}u'((1-h)Xp(1+\theta) + m\hat{p}). \tag{12}$$

The equilibrium condition for the standard currency is

$$u'(e - X(1+\varphi)p - m\hat{p})\hat{p} = \beta\left[(1-\pi)u'((1-h)Xp(1+\theta) + m\hat{p})\hat{p} + \pi u'(m\hat{p}_c)\hat{p}_c\right], \tag{13}$$

where $\hat{p}_c$ is the price of the standard currency after the crash of the cryptocurrency. Finally, the equilibrium condition for the risk-free asset is

$$u'(e - X(1+\varphi)p - m\hat{p}) = \beta(1+r)\left[(1-\pi)u'((1-h)Xp(1+\theta) + m\hat{p}) + \pi u'(m\hat{p}_c)\right]. \tag{14}$$

Substituting the right-hand side of (12) into the left-hand side of (13), the equilibrium condition for the standard currency becomes

$$(1-\pi)\left(\frac{(1-h)(1+\theta)}{1+\varphi} - 1\right)u'((1-h)Xp(1+\theta) + m\hat{p})\hat{p} = \pi u'(m\hat{p}_c)\hat{p}_c. \tag{15}$$

Finally, $\hat{p}_c$ is pinned down by the equilibrium condition for a constant price on the continuation equilibrium path after a crash:

$$u'(e - m\hat{p}_c) = \beta u'(m\hat{p}_c).$$

With $u'' < 0$, there exists a unique solution $\hat{p}_c$ to that equation.

Thus we obtain our next proposition:

Proposition 2 *There exists a constant price equilibrium iff there exists a solution $(p, \hat{p})$ to the system of equations*

$$u'((1-h)Xp(1+\theta) + m\hat{p}) = \frac{\hat{p}_c}{\hat{p}}\frac{\pi}{1-\pi}\frac{1+\varphi}{(1-h)(1+\theta) - (1+\varphi)}u'\left(m\hat{p}_c\right), \tag{16}$$

[18] There always exists an equilibrium such that $p_t = 0\ \forall t$. Here we investigate equilibria with strictly positive prices.

$$u'((1-h)Xp(1+\theta)+m\hat{p}) = \frac{1+\varphi}{\beta(1-\pi)(1-h)(1+\theta)}u'(e-X(1+\varphi)p-m\hat{p}), \tag{17}$$

with $\hat{p}_c$ *defined by* $u'(e-m\hat{p}_c) = \beta u'(m\hat{p}_c)$.

(16) stems from (15), the equilibrium condition for the standard currency, while (17) stems from (12) the equilibrium condition for the cryptocurrency. For general preferences it is not easy to prove existence of a solution to this system of equations and to characterise equilibria. As shown below, however, for isoelastic utility functions the problem is more tractable.

3.2.2 Isoelastic utility

For tractability, we assume isoelastic utility, with constant relative risk aversion (CRRA) coefficient denoted by γ: For $\gamma \neq 1$, $u(c) = \frac{c^{1-\gamma}-1}{1-\gamma}$ while for $\gamma = 1$, $u(c) = \ln(c)$. Also, to avoid heavy notations but without qualitatively affecting the results, we assume $h = 0$ and $\varphi = 0$ and we denote $D \equiv \beta(1-\pi)(1+\theta)$. D can be interpreted as a generalised discount factor for the cryptocurrency. In this context, we obtain the following proposition:

Proposition 3 *If investors have power utility, for any crash probability* $\pi \in (0,1)$ *and benefit* θ *such that*

$$\left(\frac{1+D^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\right)^{\gamma-1} > \frac{\pi(1+\theta)}{\theta(1-\pi)^{\frac{1}{\gamma}}(1+\theta)^{\frac{1}{\gamma}}}, \tag{18}$$

there exists a unique equilibrium in which the cryptocurrency price p *is strictly positive and constant until there is a crash and is such that*

$$Xp = \frac{eD^{\frac{1}{\gamma}} - m\hat{p}(1+D^{\frac{1}{\gamma}})}{1+\theta+D^{\frac{1}{\gamma}}}, \tag{19}$$

while the standard currency price until there is a crash is the unique solution $\hat{p}$ *of*

$$\theta(1-\pi)\left(\frac{(1+\theta)D^{\frac{1}{\gamma}}e - \theta D^{\frac{1}{\gamma}}m\hat{p}}{1+\theta+D^{\frac{1}{\gamma}}}\right)^{-\gamma} = \pi(m\hat{p}_c)^{-\gamma}\frac{\hat{p}_c}{\hat{p}}, \tag{20}$$

with

$$\hat{p}_c = \frac{e\beta^{\frac{1}{\gamma}}}{m(1+\beta^{\frac{1}{\gamma}})}. \tag{21}$$

The equilibrium conditions (19) and (20) give the capitalisations of the cryptocurrency and of the standard currency, Xp and $m\hat{p}$, respectively, as a function of the parameters: θ, π, and γ. The equilibrium existence condition (18) defines an upper bound on the crash probability π as stated in the next corollary.

Corollary 1 *Condition (18) is equivalent to*

$$\pi < \overline{\pi} < 1 \tag{22}$$

with $\overline{\pi} \equiv g^{-1}\left((1+\beta^{\frac{1}{\gamma}})^{1-\gamma})\theta(1+\theta)^{\frac{1-\gamma}{\gamma}}\right)$, *and* $g(\pi) = \pi(1-\pi)^{-\frac{1}{\gamma}}(1+D^{\frac{1}{\gamma}})^{1-\gamma}$.

For each value of the crash probability $\pi < \overline{\pi}$, there exists a pair of strictly positive prices such that (19) and (20) hold, i.e., there exists a constant price equilibrium. As π varies, there is a continuum of constant price equilibria. If one interprets crashes in terms of sunspot, different values of π correspond to different beliefs on which investors coordinate. Since there is a continuum of different possible beliefs π, there is a multiplicity of sunspot equilibria.

In any constant price equilibrium, gross of transactional benefit the expected return on the cryptocurrency is negative, since with probability π there is a crash and the return is negative, while with the complementary probability there is no crash and the return is zero. Yet, as stated in the next corollary, the expected return on the cryptocurrency, inclusive of the transactional benefit, is higher than the equilibrium risk free rate.

Corollary 2 *In the equilibrium defined in Proposition 3, the cryptocurrency commands a strictly positive risk premium, i.e.*

$$(1+\theta)(1-\pi) > (1+r). \tag{23}$$

To see why the cryptocurrency commands a risk premium, note that combining the first-order conditions for the cryptocurrency (12) and for the risk-free asset (14) (with $\varphi = h = 0$)

yields

$$(1+\theta)(1-\pi) = (1+r)\left[(1-\pi) + \pi\frac{u'(m\hat{p}_c)}{u'(m\hat{p} + Xp(1+\theta))}\right]. \tag{24}$$

That is, there is a cryptocurrency risk premium if and only if old investors' consumption is lower in the state where the cryptocurrency crashes than in the state where it does not crash, which we show to be true (see the proof of Corollary 2 in Appendix 1). Thus, the cryptocurrency's return is positively correlated with consumption. In contrast, as we will see below, when investors are risk neutral the expected return of the cryptocurrency (inclusive of transactional benefits) is equal to the risk free rate.

The magnitude of the cryptocurrency risk premium is obviously related to the crash probability π. Note that not only the return of cryptocurrency but also the risk-free rate r depend on π (Equation (14)) so that the variation of this risk premium with respect to π is not a priori straightforward. When the crash probability tends to the upper bound $\overline{\pi}$ defined in Corollary 1, the cryptocurrency price tends to zero, and thus its market capitalization Xp becomes small relative to the market capitalization of the standard currency $m\hat{p}$. Old investors' consumption is then less affected by the occurrence of a crash, and the cryptocurrency risk premium tends to 0. This suggests that the risk neutral case we study below can be an approximation of a model with risk aversion when the cryptocurrency has a relatively high crash probability and a low market capitalisation relative to the standard currency.[19]

3.2.3 Logarithmic utility

For the logarithmic utility case ($\gamma = 1$), the equilibrium conditions (18), (19), and (20) simplify and yield an explicit solution for the equilibrium price vector, as stated in the next proposition.

Proposition 4 *If the investors have log utility and*

$$(1+\theta)(1-\pi) > 1, \tag{25}$$

then there exists an equilibrium in which, as long as there is no crash, the capitalisation of

[19] If, in the future, the capitalisation of the cryptocurrency became larger (relative to GDP), then the risk premium could become large.

the cryptocurrency as a percentage of total endowment is

$$\frac{Xp}{e} = \frac{\beta}{1+\beta}(1 - \pi(1 + \frac{1}{\theta})), \tag{26}$$

while the capitalisation of the standard currency is

$$\frac{m\hat{p}}{e} = \frac{\pi(1+\theta)}{\theta}\frac{\beta}{1+\beta}. \tag{27}$$

Consistent with intuition, Equation (26) implies that the cryptocurrency price is decreasing in crash risk (π) and increasing in transactional benefits (θ). In contrast the standard currency price is increasing in the probability of crash, and decreasing in the transactional benefits. The larger π, the more likely it is that the cryptocurrency will crash, resulting in an increase in the standard currency price. Also, the lower θ the less the cryptocurrency can compete with the standard currency, the larger the price of the latter.

More precisely

$$\frac{\partial p}{\partial \pi} = -\frac{e}{X}\frac{\beta}{1+\beta}\frac{1+\theta}{\theta} < 0 \text{ and } \frac{\partial \hat{p}}{\partial \pi} = \frac{e}{m}\frac{\beta}{1+\beta}\frac{1+\theta}{\theta} > 0. \tag{28}$$

The opposite directions of the changes in the standard currency and the cryptocurrency prices when the probability of a crash changes reflect the competition between the two currencies. That competition, however, is muted when the capitalisation of the cryptocurrency is small. To see that note that (28) implies that the elasticity of the standard currency price to the cryptocurrency price is equal to the opposite of the ratio of the capitalisation of the cryptocurrency to the capitalisation of the standard currency:

$$\frac{\frac{\partial \hat{p}}{\partial \pi}/\hat{p}}{\frac{\partial p}{\partial \pi}/p} = -\frac{Xp}{m\hat{p}}.$$

So if $\frac{Xp}{m\hat{p}}$ is close to 0, the percentage change in the standard currency price is small relative to the percentage change in the cryptocurrency price. This is consistent with the stylized fact that, so far, large variations in bitcoin prices had no noticeable effect on dollar price. This however could change, if bitcoin became more widely used and its capitalisation grew

relative to that of the dollar.

Since investors save a constant fraction $\beta/(1+\beta)$ of their endowment, the ratio of cryptocurrency capitalisation to standard currency capitalisation can be seen as a proxy for cryptocurrency adoption. Using equations (26) and (27), this ratio can be written as

$$\frac{Xp}{m\hat{p}} = \frac{(1-\pi)(1+\theta)-1}{1+\theta-(1-\pi)(1+\theta)}.$$

Consider the following comparative statics: increase the crash risk π while adjusting the transaction benefit θ to keep the cryptocurrency expected return inclusive of private benefit $(1-\pi)(1+\theta)$ constant. Since the variance of the cryptocurrency return is $(1-\pi)(1+\theta)^2-((1-\pi)(1+\theta))^2$, this effectively adds a mean-preserving spread of the cryptocurrency return distribution. Then it is apparent from the equation above that $\frac{Xp}{m\hat{p}}$ declines. The interpretation is that extrinsic volatility is a drag on adoption.

3.2.4 Numerical illustration

To illustrate our analysis, we solve numerically for the cryptocurrency and standard currency prices, for $\gamma = .5$, 1 and 3, with π ranging between 3% and 7% and θ ranging between 0 and 10%. Figure 2 plots the capitalisation of the cryptocurrency Xp as a fraction of total endowment e. As θ increases, the capitalisation of the cryptocurrency increases, reflecting that the demand for that currency increases with the transactional benefits it delivers. As π increases, the capitalisation of the cryptocurrency decreases, because the demand for that currency decreases as its crash risk increases. As the investors' risk aversion increases, the capitalisation of the cryptocurrency decreases, because investors demand a larger risk premium to bear crash risk.

The curve depicting the capitalisation of the cryptocurrency starts only for values of θ that are above π. This reflects the condition for existence of an equilibrium with strictly positive cryptocurrency price, (18). When θ is too low relative to π, transactional benefits do not make up for crash risk, so that investors are not willing to buy the cryptocurrency at any positive price.

In the figure, the capitalisation of the cryptocurrency ranges between 0 and 35% of the endowment. Current world GDP is around 84.5 trillion dollars, while the current capitalisation of bitcoin is around 1.1 trillion dollars. So bitcoin capitalisation is currently around

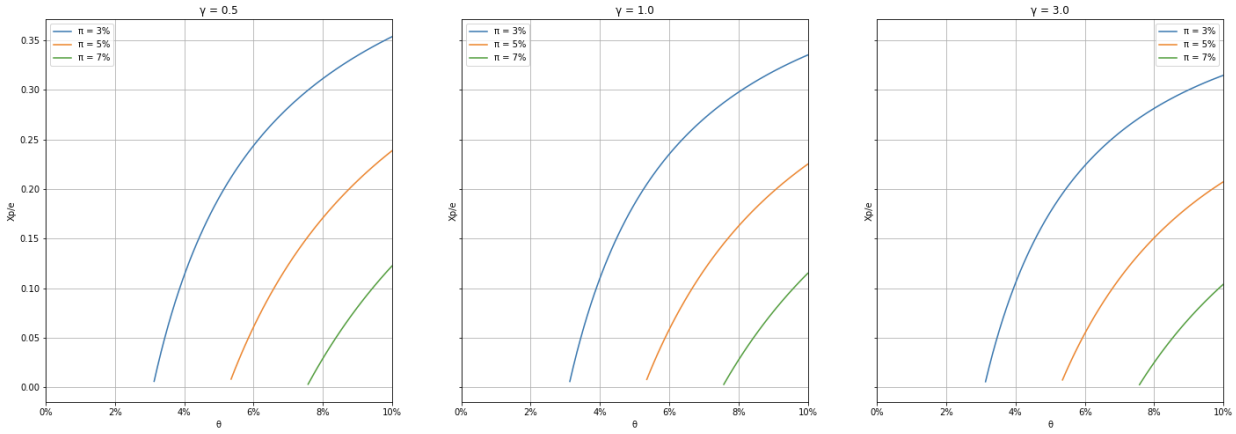


Figure 2: Cryptocurrency market capitalisation as a function of benefit

1.3% of world GDP. When crash risk is low ($\pi = 3\%$) and risk aversion is .5, one obtains this order of magnitude when θ is lower than 4%. When crash risk is larger ($\pi = 7\%$), one obtains this order of magnitude for θ as large as 8%. Of course this back of the enveloppe calculation is to be taken with a generous dose of salt. Constant price equilibria are an extremely simplified representation of reality, in particular because volatility in these equilibria is small relative to its empirical counterpart. Yet, the analysis of constant price equilibria paves the way for the more realistic analysis of the next subsection, in which equilibrium prices change at each period and volatility can be large.

3.3 Volatile price equilibria

Building on the above analysis, we now construct equilibria in which prices can vary at each period. First, with constant relative risk aversion, we consider the case in which the only source of variation is sunspots, so that volatility is purely extrinsic. Second, we turn to the case of risk neutrality, which is tractable enough to yield equilibrium restrictions with both sunspot-driven and fundamental-driven volatility. In both the risk averse and the risk neutral cases, there is sunspot-driven equilibrium multiplicity.

3.3.1 CRRA investors

Consider the case in which crashes are arbitrary, up to "sunspot" beliefs. In this context, we now construct an equilibrium in which, in contrast with the previous section in which the probability of a crash was constant, it changes at each period t until period N. From period N on, the probability of a crash remains constant, and the cryptocurrency and standard currency prices are set as in the constant price equilibrium studied in Section 3.2.2.

To capture the dependence of prices to sunspot-driven crash risk, we define the sunspot at period t as $\omega_t = (\xi_{t-1}, \pi_t)$, where $\xi_{t-1} = c$ in case of a crash at the end of period $t-1$ and $\xi_{t-1} = nc$ otherwise, while π_t is the probability of a crash during period t. The sunspot ω_t is publicly observed at the beginning of period t. Conditional on $(\omega_{t-1}, \xi_{t-1})$, π_t is independent of all the other variables in the information set of the agents at period t. Moreover, the distribution of ξ_t depends only on π_t. An equilibrium is a mapping from ω_t into prices. As before, the price of the standard currency after a crash is given by (21).

The family of equilibria we consider involve two phases. For $t \geq N$, we are in the second phase in which, as long as there is no crash, the probability of a crash remains constant and equal to π_N. Let $p(\pi_N)$ and $\hat{p}(\pi_N)$ denote the prices of the cryptocurrency and the standard currency in the second phase as long as no crash happens, i.e., at all $t \geq N$ such that $\xi_{t-1} = nc$. Similarly to Proposition 3, these prices are determined by the equilibrium conditions, equating current prices, valued at current marginal utility, with discounted expected future prices, valued at future marginal utility:

$$\frac{p(\pi_N)}{(e - Xp(\pi_N) - m\hat{p}(\pi_N))^\gamma} = \frac{D(\pi_N)p(\pi_N)}{(Xp(\pi_N)(1+\theta) + m\hat{p}(\pi_N))^\gamma}, \tag{29}$$

and

$$\frac{\hat{p}(\pi_N)}{(e - Xp(\pi_N) - m\hat{p}(\pi_N))^\gamma} = \frac{\hat{D}(\pi_N)\hat{p}(\pi_N)}{(Xp(\pi_N)(1+\theta) + m\hat{p}(\pi_N))^\gamma} + \frac{\beta\pi_N\hat{p}_c}{(m\hat{p}_c)^\gamma}. \tag{30}$$

where $D(\pi) = \beta(1+\theta)(1-\pi)$ and $\hat{D}(\pi) = \beta(1-\pi)$ can be interpreted as generalised discount factors for the cryptocurrency and the standard currency, respectively.

Now turn to the first phase when $t \leq N-1$. At the beginning of each period $t \leq N-1$, a sunspot determines the current beliefs about the probability of a crash at the end of this period, π_t. Specifically, we consider sunspot-driven beliefs such that, at the beginning of period $t \leq N-1$, with probability x_t, the crash probability goes up to $\pi_t^u \geq \pi_{t-1}$ while, with

probability $1 - x_t$, it decreases to $\pi_t^d \leq \pi_{t-1}$. Figure 3 presents the timing of events.

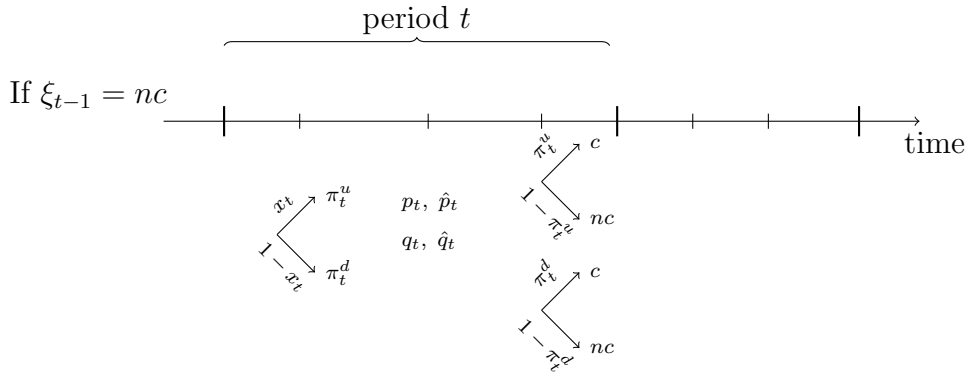


Figure 3: Sequence of events for volatile price equilibria.

Denote by $p(\pi_t)$ and $\hat{p}(\pi_t)$ the prices of the cryptocurrency and the standard currency in the first phase as long as no crash happens (i.e., as long as $\xi_{t-1} = nc$). If there is no crash up to period t, the prices of the standard currency and the cryptocurrency, $p(\pi_t)$ and $\hat{p}(\pi_t)$, are related to the period $t+1$ prices by the following general equilibrium conditions

$$\frac{p(\pi_t)}{(e - Xp(\pi_t) - m\hat{p}(\pi_t))^\gamma} = \frac{x_{t+1} D(\pi_t) p(\pi_{t+1}^u)}{(Xp(\pi_{t+1}^u)(1+\theta) + m\hat{p}(\pi_{t+1}^u))^\gamma} + \frac{(1 - x_{t+1}) D(\pi_t) p(\pi_{t+1}^d)}{(Xp(\pi_{t+1}^d)(1+\theta) + m\hat{p}(\pi_{t+1}^d))^\gamma}, \tag{31}$$

and

$$\frac{\hat{p}(\pi_t)}{(e - Xp(\pi_t) - m\hat{p}(\pi_t))^\gamma} = \left[\frac{x_{t+1} \hat{D}(\pi_t) \hat{p}(\pi_{t+1}^u)}{(Xp(\pi_{t+1}^u)(1+\theta) + m\hat{p}(\pi_{t+1}^u))^\gamma} + \frac{(1 - x_{t+1}) \hat{D}(\pi_t) \hat{p}(\pi_{t+1}^d)}{(Xp(\pi_{t+1}^d)(1+\theta) + m\hat{p}(\pi_{t+1}^d))^\gamma} \right] + \pi_t \frac{\beta \hat{p}_c}{(m\hat{p}_c)^\gamma}. \tag{32}$$

The left-hand side of (31) is the cryptocurrency price multiplied by the marginal utility of the investor at period t. The first term on the right-hand side is the probability x_{t+1} that crash risk goes up to π_{t+1}^u multiplied by the product of the discounted price of the cryptocurrency and the marginal utility of the investor in that state. The second term on the right-hand side is the corresponding term for the state in which the crash risk goes down to π_{t+1}^d.

Similarly for (32): The left-hand side is the standard currency price multiplied by the marginal utility of the investor at period t. The first two terms on the right-hand side correspond to the cases in which there is no crash at period t and the crash probability moves up or down at the beginning of $t+1$. The last term on the right-hand side of (32) corresponds to the case in which there is a crash at the end of period t.

Equilibrium prices for $t \leq N-1$ are obtained by backward induction. At $t = N-1$, using (31) and (32) one gets $p(\pi_{N-1})$ and $\hat{p}(\pi_{N-1})$, as functions of $p(\pi_N^u)$, $p(\pi_N^d)$, $\hat{p}(\pi_N^u)$, and $\hat{p}(\pi_N^d)$ defined by (29) and (30). Then at $t = N-2$, using again (31) and (32) one gets $p(\pi_{N-2})$ and $\hat{p}(\pi_{N-2})$ as functions of the equilibrium prices $p(\pi_{N-1})$ and $\hat{p}(\pi_{N-1})$ obtaining for the different possible realisations of π_{N-1}. Iterating, one recovers prices in all states from $t = N-1$ to $t = 1$. In Appendix 1, we prove there exists a unique pair of prices, $(p_t(\pi_t), \hat{p}(\pi_t))$ solving (31) and (32), so we can state our next proposition:

Proposition 5 *For any sunspot process such that $\pi_t < \overline{\pi}$ for all $t \leq N$, there exists an equilibrium such that*

(i) for $t < N$, if there is no crash before t, the cryptocurrency price goes down with probability x_t and up with probability $1 - x_t$ while the standard currency price moves in the opposite direction. Both prices are defined by conditions (31) and (32).

(ii) for $t \geq N$, as long as no crash happens, prices are constant and defined by (29) and (30).

(iii) After a crash, the cryptocurrency price is equal to zero and the standard currency price is given by (21).

Proposition 5 shows that, within a given equilibrium, the sunspot (ξ_t, π_t) plays the role of a sequence of coordination variables, generating fluctuations in prices, even when fundamentals endowments (e, transactional benefits θ) remain constant. These fluctuations correspond to extrinsic volatility.[20]

[20]Such within equilibrium volatility is related to our earlier results on equilibrium multiplicity for constant-price equilibria in Proposition 3 and Corollary 1. Indeed, we construct the equilibrium described in Proposition 5 working backward from multiple constant-price continuation equilibria after $t = N$, each corresponding to a particular crash probability π_N.

Moreover, there is a large number of possible distributions of the sunspot, each corresponding to a possible equilibrium. So there is a large multiplicity of equilibria. Thus, Proposition 5 extends the multiplicity results of Proposition 3 to our new class of equilibria, in which prices move in response to sunspots not only when the cryptocurrency crashes but also during arbitrarily many periods before that.

3.3.2 Risk neutral investors with linear transactional benefits

We now turn to the case in which investors are risk neutral. The equilibrium cryptocurrency pricing relation (9) then simplifies to

$$p_t = \frac{1}{1+r} E_t \left[(1 - h_{t+1}) \frac{1+\theta_{t+1}}{1+\varphi_t} p_{t+1} \right], \tag{33}$$

with

$$\beta = \frac{1}{1+r}.$$

Equivalently, to make crash risk explicit, (33) can be rewritten as

$$p_t = \frac{1-\pi_t}{1+r} \, E_t \left[(1 - h_{t+1}) \frac{1+\theta_{t+1}}{1+\varphi_t} p_{t+1} \middle| \text{no crash} \right]. \tag{34}$$

The pricing equation (33) leads to our next proposition.

Proposition 6 *Consider a sequence of prices $\{p_t\}_{t=1,..,\infty}$ satisfying (33). There exists a constant $\lambda > 0$ and a sequence of random variables $\tilde{u}_\tau$, each with unit expectation ($E_{\tau-1}(\tilde{u}_\tau) = 1$) and independent from the investors' information set at period $\tau - 1$, such that the new price sequence*

$$\{\bar{p}_t\}_{t=1,..,\infty} = \left\{ \lambda \left(\prod_{\tau=1}^{t} u_\tau \right) p_t \right\}_{t=1,..,\infty}, \tag{35}$$

also satisfies (33), and therefore also is an equilibrium.

Proposition 6 implies that, for any equilibrium price sequence $\{p_t\}_{t=1,..,\infty}$, one can construct another equilibrium price sequence $\{\bar{p}_t\}_{t=1,..,\infty}$. And, when one has gone from $\{p_t\}_{t=1,..,\infty}$ to $\{\bar{p}_t\}_{t=1,..,\infty}$, one can iterate the process and go from $\{\bar{p}_t\}_{t=1,..,\infty}$ to yet another equilibrium. Iterating, one can generate a continuum of equilibria. Hence, as in the risk averse case, there

exist multiple sunspot-driven equilibria. Also as in the risk-averse case, within each equilibrium there is extrinsic (sunspot) volatility, so that prices can vary even when fundamentals remain constant. In Proposition 6, this extrinsic volatility is the volatility of the random variables $\tilde{u}_t, t = 1, .., \infty$.

To see, intuitively, how Proposition 6 obtains, take the three following steps: First multiply the left-hand side of (33) by $\lambda \left(\prod_{\tau=1}^{t} u_\tau \right)$, which yields $\bar{p}_t$. Second, also multiply the right-hand side of (33) by $\lambda \left(\prod_{\tau=1}^{t} u_\tau \right)$, so that it is equal to $\bar{p}_t$. Third, multiply by $\tilde{u}_{t+1}$ the terms inside the brackets in (33) and note that this does not change the value of the expectation, since $E_t(\tilde{u}_{t+1}) = 1$ and $\tilde{u}_{t+1}$ is independent from the variables in the investors' period t information set.

3.3.3 Risk neutral investors with concave transactional benefits

These three steps take advantage of the linearity in price of (33), which itself stems from the linearity of the utility function and the linearity of transactional benefits. The analysis of Sections 3.1 and 3.2 shows that extrinsic volatility arises also when the utility function is strictly concave. We now show that our results are robust to relaxing the assumption that transactional benefits are linear. For simplicity, we conduct this analysis in the simple case in which parameters are constant through time. Instead of assuming that transactional benefits are equal to $\theta q_t p_t$, where θ is a constant scalar, we assume there exists a twice differentiable function $\theta(.)$ such that transactional benefits are equal to $\theta(q_t p_t)$ and such that $\theta' > 0$, $\theta'' < 0$, and $\theta'(x) \to 0$ when $x \to \infty$. In this case, instead of yielding (33), market clearing and first order conditions yields, for risk neutral investors

$$p_t = \frac{1 - \pi_t}{1 + r} \, E_t \left[(1 - h) \frac{1 + \theta'((1 - h) X p_{t+1})}{1 + \varphi} p_{t+1} \middle| \text{no crash} \right]. \tag{36}$$

Our first step, in this context, is to show there exist constant price equilibria similar to those characterised in Proposition 2. Following the same approach as for Proposition 2, from (36) we have that the constant equilibrium price p is pinned down by

$$1 + \theta'((1 - h) X p) = \frac{1 + r}{1 - \pi} \frac{1 + \varphi}{1 - h}. \tag{37}$$

Since θ' is decreasing, (37) admits a unique solution iff

$$1 - \frac{1+r}{1+\theta'(0)}\frac{1+\varphi}{1-h} > \pi. \tag{38}$$

Denoting that solution by $p(\pi)$, we obtain our next proposition.

Proposition 7 *With linear utility and strictly concave transactional benefits, if*

$$1 > \frac{1+r}{1+\theta'(0)}\frac{1+\varphi}{1-h},$$

there exists a continuum of constant price equilibria $p(\pi)$, corresponding to the different possible values of the sunspot-driven probability of crash $\pi \in [0, 1 - \frac{1+r}{1+\theta'(0)}\frac{1+\varphi}{1-h}]$.

Our second step is to construct volatile price equilibria when transactional benefits are concave. To do so in the simplest possible manner, suppose that i) at the first period the sunspot-driven probability of a crash is π, ii) at the second period it can go up to π^u with probability x or down to π^d with probability $1-x$, and iii) thereafter the probability of a crash remains constant. In this context there are two possible constant price equilibria from period 2 on: $p(\pi^u)$ and $p(\pi^d)$. The equilibrium price at period 1 is

$$p_1 = \frac{1-\pi}{1+r}\frac{1-h}{1+\varphi}\left[x\left[1+\theta'\left((1-h)Xp(\pi^u)\right)\right]p(\pi^u) + (1-x)\left[1+\theta'\left((1-h)Xp(\pi^d)\right)\right]p(\pi^d)\right]. \tag{39}$$

This is a volatile price equilibrium similar to those of Proposition 5 in that prices change, from period 1 to period 2, without any change in fundamental and without the occurrence of a crash. While in the analysis leading to (39) there is only one period at which prices change without any crash or change in fundamentals, one can iterate the argument to construct equilibria in which, as in Proposition 5, prices can vary at each period until N.

Thus, both in the risk averse and the risk neutral cases, and also both for linear and for concave transactional benefits, our theoretical analysis implies the following: In contrast with perfect-markets equilibrium stock prices, which should not be more volatile than fundamentals (Shiller, 1981), equilibrium currency prices can exhibit sunspot-driven extrinsic volatility, unrelated to fundamentals.[21] While stock prices are anchored by real variables

[21] Campbell and Shiller (1988a) emphasise that stock price changes can also stem from changes in discount

such as firms' profits, which, in perfect markets, are not determined by stock prices, currencies have no such real anchors, since their fundamental value directly depends on their future price. Lack of real anchor raises the scope for extrinsic volatility.

4 Data

Our theoretical model yields implications about the relationship between cryptocurrency prices, transactional benefits and costs, and crash probabilities. To confront these theoretical implications to data, we collected data on returns, transactional benefits and costs.

Our dataset starts on July 17, 2010, with the opening of the MtGox bitcoin marketplace, and ends on December 31, 2018. Computing a bitcoin price series over a period of almost 9 years is subject to several caveats: new marketplaces, sometimes short-lived, have been created and shut down at a rather high pace, price volatility is high, and there is large price dispersion between exchanges even when trading volumes are high (see Makarov and Schoar, 2020). To construct a time series of bitcoin prices, we rely on the Kaiko dataset. We use all transaction prices denominated in five currencies from 20 major exchanges.[22] Following Paine and Knottenbelt (2016), pooling all transaction prices in each currency intervals, we split each UTC day in 5-minute. In each interval, we compute the volume weighted median price. To construct a daily price for each currency, we then compute an arithmetic (unweighted) average of these median prices. Using medians reduces the effect of outliers. Using weighted medians prevents small trades from having too much influence. Finally, non-weighted averages give equal weight to the information flowing at different times during a day. To obtain a single daily price series, we convert daily prices in each currency in US dollars using daily USD exchange rates from FRED (Federal Reserve Economic Data)

rates, reflecting changes in risk premia. This differs from the risk created by changes in investors' beliefs, which we analyse.

[22]Precisely, for transactions in euros, we use all transactions from Bitfinex, bitFlyer, Bitstamp, BTC-e, Coinbase-GDAX, CEX.IO, Gatecoin, HitBTC, itBit, Kraken and Quoine. For transactions in US dollars, we use Bitfinex, bitFlyer, Bitstamp, Bittrex, BTC-e, BTCChina, CEX.IO, Coinbase-GDAX, Gatecoin, Gemini, hitBTC, Huobi, itBit, Kraken, MtGox, OKCoin and Quoine. For transactions in British pounds, we use Bitfinex, Coinbase-GDAX, CEX.IO and Kraken. For transactions in Japanese yens, we use Bitfinex, bitFlyer, BTCBox, Kraken, Quoine and Zaif. For transactions in Chinese yuans, we use BTCChina, BTC38, Huobi, OKCoin and Quoine. We also ran the estimation using only transactions between dollars and bitcoins. This did not alter qualitatively our results. In particular it did not change the sign and significance of the coefficient estimates.

and compute an unweighted average daily price. This time series is illustrated in Figure 4.

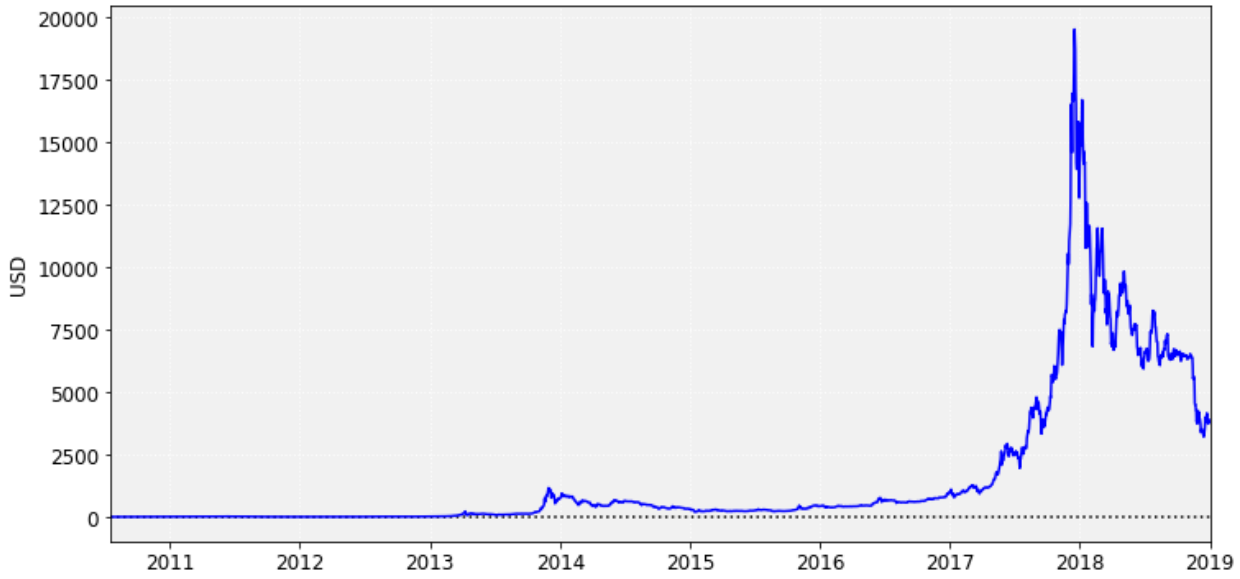


Figure 4: Bitcoin price, in USD

We retrieve bitcoin transaction fees paid to miners (hereafter referred to as miners' fees) from blockchain data using Blocksci, an open-source software platform for blockchain analysis (Kalodner et al., 2017). Then, to compute percentage miners' fees we divide fees by transaction volume. Transaction volume, however, is difficult to measure (see for instance Meiklejohn et al., 2013, or Kalodner et al., 2017). This is because part of the transfers occur among addresses belonging to the same participant. Yet, in a pseudonymous network like Bitcoin, the identity of the participant corresponding to an address cannot be observed. To estimate bitcoin transaction volume we retrieve the on-chain transaction volume, excluding coinbase transactions (that is, transactions that reward miners by the creation of new bitcoins) and transfers from an address to itself.[23] From that value, we further exclude amounts that are likely to result from "self churn" behaviour, that is, transfers among adresses be-

[23]The Bitcoin protocol states that an output of a transaction (that is, an amount payed to a particular bitcoin address), when spent, must be spent in full. Thus, if a bitcoin owner wants to transfer, e.g, 1 BTC to a payee, but owns 20 BTC as a single output of an earlier transaction, she has to create a transaction with one input (the 20 BTC) and two outputs: 1 BTC to an address belonging to the payee, and 19 BTC (abstracting from the fee payed to the miner of the block in which that transaction will be included) to herself. These 19 BTC are change money, and should not be counted as transaction volume.

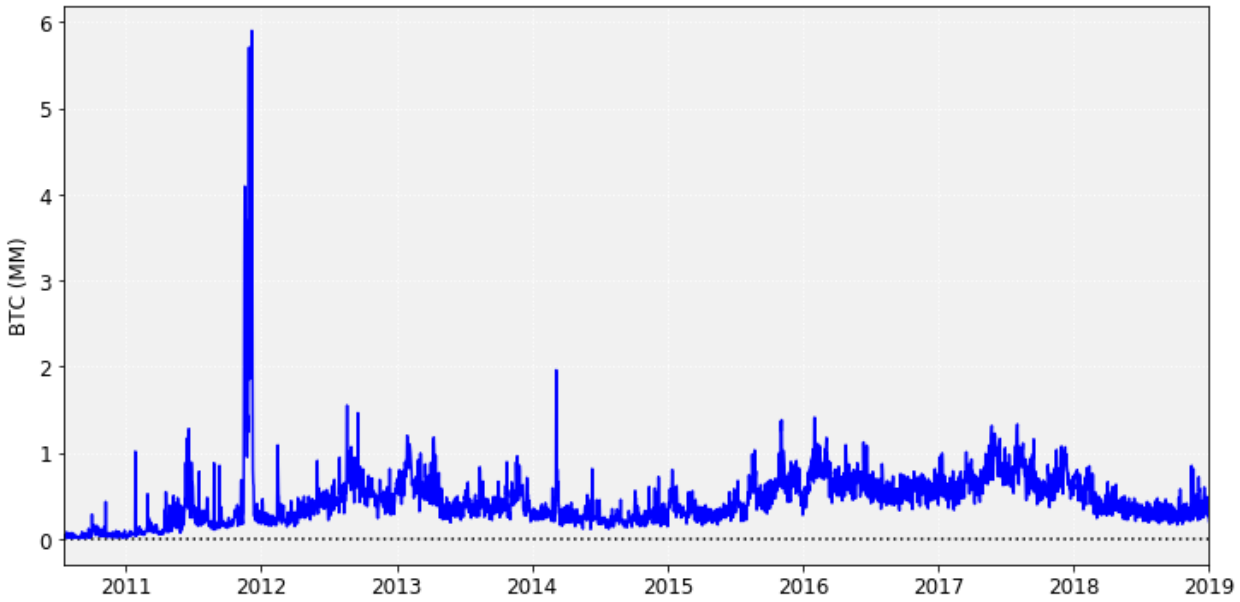


Figure 5: Estimated transaction volume, in millions of BTC

longing to the same participant.[24] The time series of transaction volume is illustrated in Figure 5.[25]

The time series of miners' fees (in percent of transaction volume) is depicted in Figure 6. The figure illustrates that, during most of the sample period, miners' fees are low. Daily fees amount to .0106% of transaction volume, on average. Q1, median, and Q3 are .0038%, .0057% and .0099%, respectively. There are a few spikes, however. The largest one occurs towards the end of 2017, a time at which transaction fees exceeded 0.23%, due to the congestion triggered by the surge in trading volume (see Easley, O'Hara and Basu, 2019, Huberman, Leshno and Moalleni, 2021, or Iyidogan, 2019 for models of blockchain miners' fees).

Browsing the web (in particular bitcointalk.org), we collected information about all hacks and other losses on Bitcoin. We identified and collected data on about 53 such events over our sample period.[26] We collected the amounts of the losses and the times at which they were

[24]For that purpose, we eliminate outputs spent within less than 4 blocks, an heuristic proposed by Kalodner et al. (2017).

[25]The spike in trading volume at the end of 2011 was noted by the Bitcoin community and was attributed to consolidation operations by MtGox.

[26]We have been unable to find information about the amount lost for the following three events: the hack

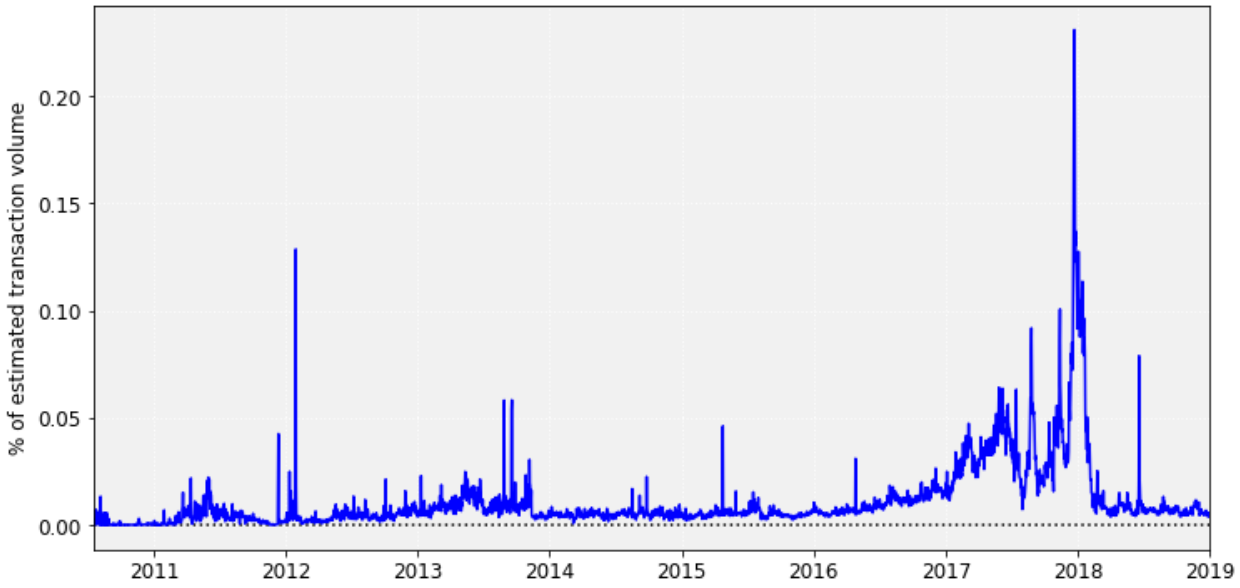


Figure 6: Miners' fees, in percent of estimated transaction volume

reported. To obtain percentage losses (to fit our definition of h), we divide lost amounts by X_t. This time series is illustrated in Figure 7. The corresponding events are listed in Table 2 in the Online Appendix. Most events correspond to hacks of exchange platforms, during which private keys securing access to bitcoins deposited by platform's clients are stolen by attackers. Besides being hacked, exchange platforms may also lose their private keys (Bitomat, July 2011) or accidentally transfer bitcoins to wrong Bitcoin addresses (MtGox, October 2011). The largest loss is due to the collapse of MtGox in February 2014, when 744,408 bitcoins were lost. On average, during the whole sample period, the fraction of bitcoins lost per week is approximately 0.04%.

We also collected information about events likely to affect the costs and benefits of using bitcoins. We distinguished between two types of events, relative to:

- The ease with which bitcoins could be exchanged with currencies such as e.g. euros, Japanese yens, or US dollars.

- The ease to use bitcoins to buy goods or services and thus reap transactional benefits.

of the e-wallet service company Instawallet in April 2013; the hack of the South Korean exchange Bithumb reported in June 2017; the hack of the South Korean exchange Youbit in December 2017.

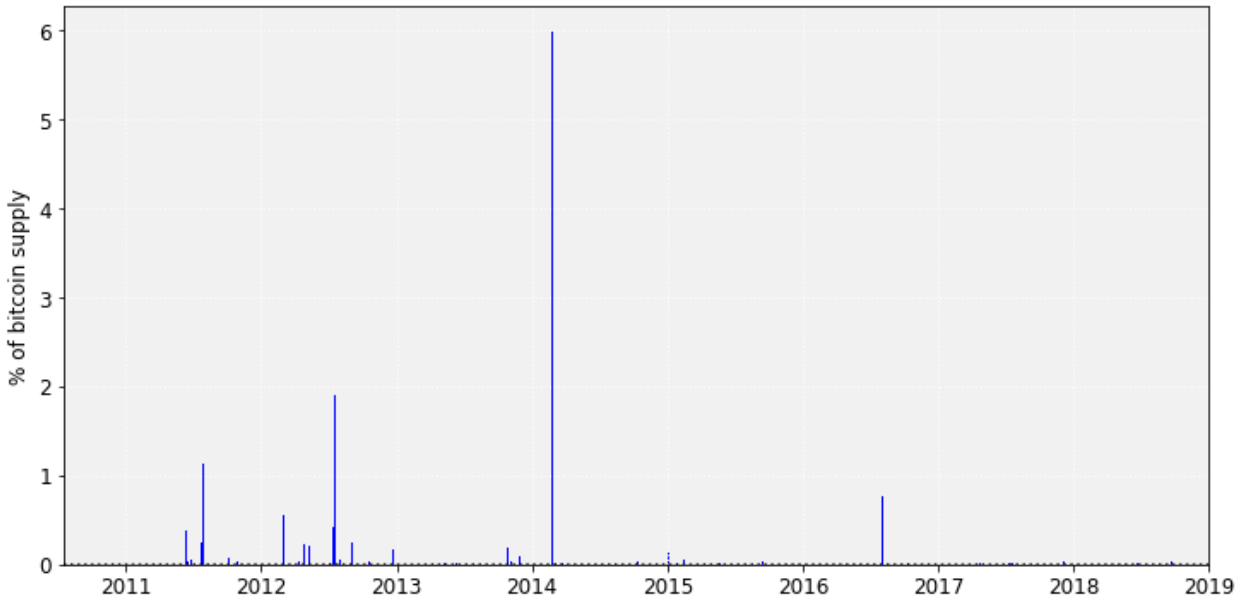


Figure 7: Hacks, thefts and other losses of bitcoins, in percent of bitcoin supply

As explained below, we constructed two indices referred to as *MarketAccess* and *Benefit*, measuring the cumulative impact of those events. To construct *MarketAccess*, we identified 43 events over our sample period (see Table 3 in the Online Appendix). We considered three categories of events. The first category relates to exchange platforms.[27] It includes the creation of the first exchange platform on which a given currency can be traded against bitcoin, or the closure of the last exchange platform on which that currency can be traded. For example, in the case of the Chinese yuan, the first exchange opened on June 13, 2011, while the last one closed on September 30, 2017.[28] The first category of events also includes evolutions of these platforms, for example technological improvements in their payment system (e.g. MtGox eased fund transfers on October 25, 2010) or trading disruptions. The second category relates to regulatory changes that facilitate or impair the trading of bitcoin, for example the ban of bitcoin trading by citizens in China from January 16, 2018. The third

[27]We use the term exchange platform to refer to electronic limit order markets, although such markets are not regulated exchanges.

[28]We consider all currencies for which bitcoin trading is significant, i.e. average trading volume exceeds 100 transactions a day during the lifetime of a given market. For each currency, we select as the event date the first day for which trading data is available in at least one of the following two large-coverage, tick-by-tick datasets: Kaiko and bitcoincharts.com (see `https://bitcoincharts.com/markets/list/`).

category includes miscellaneous but important events, e.g., the opening of the first bitcoin ATM on October 29, 2013, or the start of bitcoin futures trading at the CBOE on December 10, 2017. Positive events are coded by +1 and negative events by −1. To account for the importance of these events, we weight them by the GDP of the country in which they take place, relative to the world GDP.[29] The *MarketAccess* index is the sum of these weighted events: At each point in time, it quantifies how easy it is to buy or sell bitcoins.

To construct *Benefit*, we identified 39 events, listed in Table 4 in the Online Appendix. These events fall in two categories. The first category includes new goods and services available for electronic purchase with bitcoins (e.g. computer hardware or travel agency services or illegal products). For example, on June 11, 2014, Expedia started accepting bitcoins for hotel reservations. An example of illegal activity is the opening of SilkRoad on January 23, 2011. The second category corresponds to new payment facilities (gift cards or payment systems accepting bitcoins). For instance, Paypal accepted bitcoins on January 22, 2015. As before, positive events are coded by +1 and negative events are coded by −1. We do not weight these events because it is hard to define an appropriate weighting scheme. The *Benefit* index is the sum of these events: At each time t it quantifies the variety of goods and services which can be purchased with bitcoins.

The time series of the two indices is illustrated in Figure 8. The *MarketAccess* index increased sharply during the first two years, as new exchange platforms allowing trades between bitcoins and new currencies opened. Two major events triggered a sharp decrease in the index in 2013: MtGox suspended fund transfers on May 14, 2013 and China banned financial institutions from using bitcoins on December 3, 2013. The *Benefit* index remained low in the first years of the sample period, reflecting that it was hard to use bitcoins to purchase goods and services. It started increasing towards the end of 2013 and reached its maximum in 2018. It then decreased somewhat, as some large companies stopped accepting payments in bitcoins.

[29] We retrieve yearly GDP data from the World Bank database.

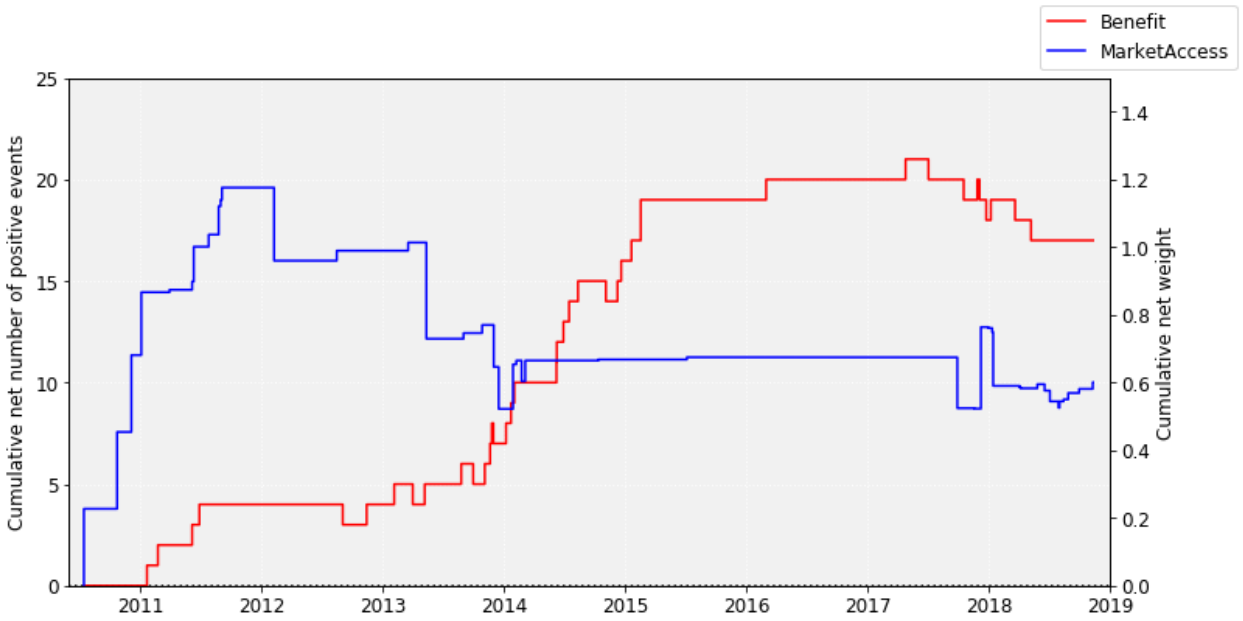


Figure 8: *MarketAccess* and *Benefit* indices

5 Calibration

The goal of this section is to calibrate the model, by evaluating the order of magnitude of the coefficients which offer a relatively good match between the model and the data.[30]

5.1 Calibrated model

We perform our calibration under the assumption that investors are risk neutral. This assumption is likely to be innocuous because, during our sample period (2010-2018), the capitalisation of bitcoin was only a small fraction of aggregate wealth. So variations in bitcoin prices likely did not move marginal consumption a lot. Indeed, Liu and Tsyvinski (2021) find empirically that the correlation of bitcoin returns with durable or non durable consumption growth, industrial production growth and personal income growth is economically and statistically insignificant. In the next paragraphs, we present the model that is calibrated,

[30]Estimating the parameters of the model would be more ambitious, but would be difficult given that the data is likely to be non-stationary. Thus, our calibration approach can be seen as a relatively modest first step towards confronting the model to the data.

the proxies for the model variables h, θ, and ϕ, and the specification of the probability of a crash π_t.

Expected returns. Proceeding as for (33), one obtains the price of the standard currency,

$$\hat{p}_t = \frac{1}{1+r_t} E_t \left(\hat{p}_{t+1} \right). \tag{40}$$

In practice, during our sample period (2010-2018), inflation in the US has been low and not very volatile. Thus, in order to simplify the econometric analysis, we hereafter assume that inflation in the standard currency between period t and period $t+1$ is known at period t.[31] Under this assumption, in (40) $\hat{p}_{t+1}$ is in the information set used to take the expectation.[32] Hence (40) simplifies to

$$\hat{p}_t = \frac{\hat{p}_{t+1}}{1+r_t}. \tag{41}$$

Dividing (33) by (41), the price of the cryptocurrency in terms of standard currency, $\frac{p_t}{\hat{p}_t}$, (e.g., the price of bitcoin in dollars) writes as

$$\frac{p_t}{\hat{p}_t} = E_t \left[(1-h_{t+1}) \frac{1+\theta_{t+1}}{1+\varphi_t} \frac{p_{t+1}}{\hat{p}_{t+1}} \right]. \tag{42}$$

The rate of return on the cryptocurrency price expressed in the standard currency is

$$\rho_{t+1} = \frac{\frac{p_{t+1}}{\hat{p}_{t+1}}}{\frac{p_t}{\hat{p}_t}} - 1.$$

Substituting this expression into (42) we obtain our next proposition.

Proposition 8 *When investors are risk neutral and period $t+1$ inflation in the standard currency is known at period t, the rate of return on the cryptocurrency price expressed in*

[31] As explained below, in our calibration, the length of one period is set to one week, making our assumption that inflation is known from one period to the next quite innocuous.

[32] Because the occurrence of a crash between t and $t+1$ is not in the time t information set, the assumption that $\hat{p}_{t+1}$ is in that information set implies the price of the standard currency cannot be affected by the crash in the cryptocurrency. With risk neutral investors this is consistent with equilibrium, which only requires that the standard currency prices be such that (40) holds. In other words, with risk neutral investors, one can construct equilibria such that the standard currency price does not change following a cryptocurrency crash.

standard currency is such that

$$1 = (1 - \pi_t) E_t \left[(1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) (1 + \rho_{t+1}) | no\ crash \right], \tag{43}$$

Equation (43) reflects that, in equilibrium, investors must be indifferent between using one unit of consumption good to invest in bitcoin (generating transactional benefits as well as costs and hacking risk) and using it to invest in dollars. To see the intuition more clearly, take a first-order Taylor expansion of (43), for ρ_{t+1}, π_t, h_{t+1}, φ_t and θ_{t+1} close to 0,

$$E_t \left[\rho_{t+1} | \text{no crash} \right] \approx \pi_t + \varphi_t + E_t(h_{t+1}) - E_t(\theta_{t+1}). \tag{44}$$

Equation (44) states that the return on the cryptocurrency must compensate investors for crashes, transactions costs and hacks, minus transactional benefits.

Transactional benefits and costs. To calibrate (43), we need to specify θ_{t+1} and φ_t. We assume that the transactional benefit θ_{t+1} is

$$\theta_{t+1} = \alpha_1 Benefit_{t+1}, \tag{45}$$

where α_1 is the parameter to be calibrated, and $Benefit_{t+1}$ is the index described in the previous section. The transactional cost φ_t is

$$\varphi_t = \beta_1 CostMiningFee_t + \beta_2 CostMarketAccess_t, \tag{46}$$

where β_1 and β_2 are to be calibrated and $CostMarketAccess_t$ measures the cost of accessing bitcoin markets:

$$CostMarketAccess_t = \frac{1}{1 + MarketAccess_t}. \tag{47}$$

Note that (47) purposefully lets the cost tend to zero when *MarketAccess* tends to infinity. We further assume that the fraction of bitcoins hacked or lost, h_{t+1}, is constant and we set it to the sample average:

$$h_{t+1} = \bar{h}. \tag{48}$$

Crash probability. Finally, similarly to Athey et al. (2016), we model π_t as the Bayesian update of the probability of a fatal event such as the discovery of a flaw in the protocol, a successful attack of the blockchain, or a sudden change in the political and legal environment making it impossible to use the cryptocurrency.[33] To do so, we assume that there are two states H and L, that the a priori probability of state H is λ_0, and that the probability of a crash is μ in state H and 0 in state L. Afterwards, this probability is updated based on the observation of a crash or no crash. If, at period t, there has been no crash so far, the probability of state H is

$$\lambda_t = \Pr(H| \text{ no crash until } t) = \frac{(1-\mu)^t \lambda_0}{(1-\mu)^t \lambda_0 + (1-\lambda_0)}. \tag{49}$$

This probability goes down as the number of periods with no crash increases. Consequently, the probability of a crash,

$$\pi_t = \lambda_t \mu, \tag{50}$$

also decreases monotonically with the length of time with no crash. We chose this very stylized model for simplicity. For greater realism, one would have to consider a richer model, in which π_t could go up after bad news, even in the absence of a crash. Note that such dynamics would be possible with sunspots.

5.2 Sample

To avoid day-of-the-week effects while keeping a reasonable amount of data, the daily price series is downsampled to a weekly frequency. The final sample used in the calibration contains 432 observations and runs from the week of September 26, 2010, until the week of December 23, 2018.[34] Several forks occurred in our sample period that granted bitcoin owners additional coins in the newly created currency. These coins can be interpreted as a form of dividend and we therefore add them to the $t+1$ bitcoin price when computing the bitcoin return from t to $t+1$. Table 5 in the Online Appendix presents the forks considered and the value of the

[33] In this context, crashes and their probability are not driven by sunspots, but correspond to fundamental uncertainty about the reliability of the technology and its environment.

[34] Note that this weekly sample starts somewhat later than the daily sample described in Section 4. The reason is that we use a burn-in period for the smoothed series that our calibrated results are benchmarked to (see Figure 11).

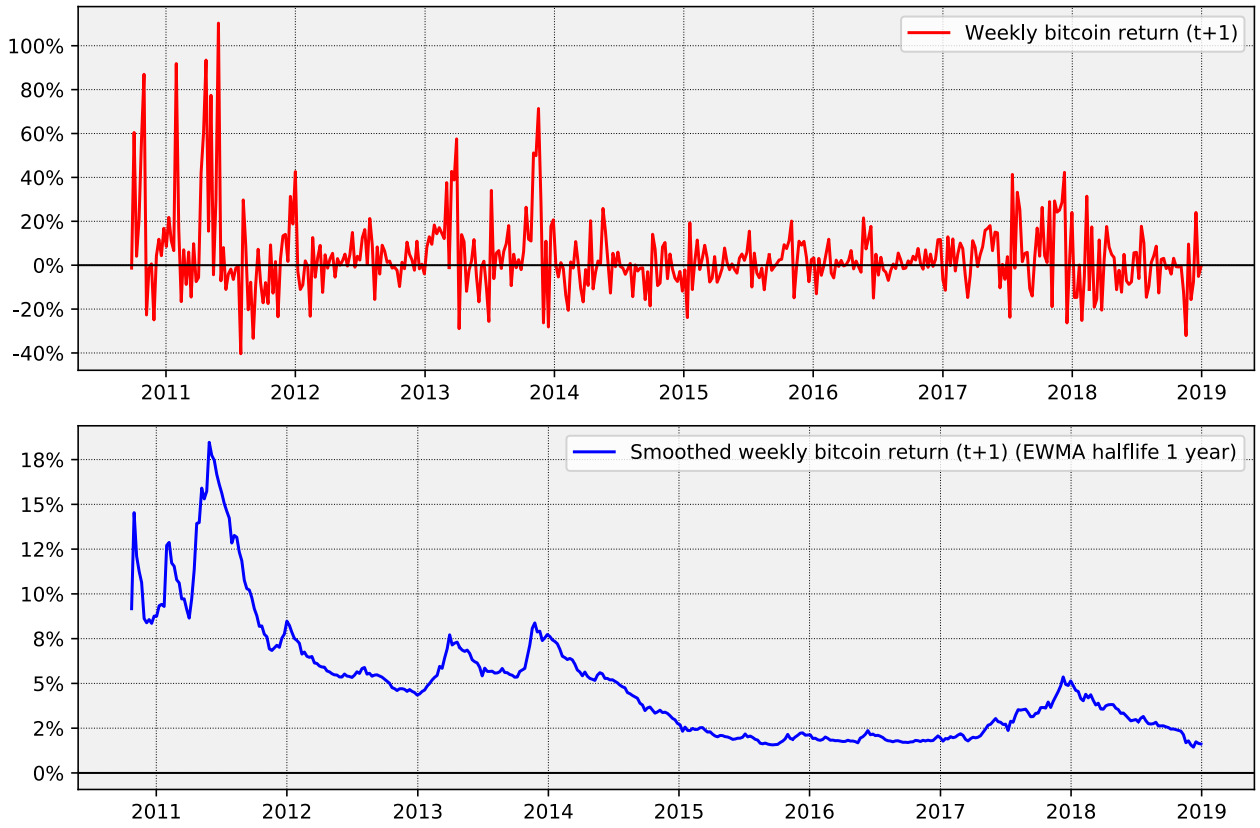


Figure 9: Bitcoin returns. This figure plots weekly bitcoin returns expressed in USD. The top graph plots raw returns. The bottom graph smooths these returns by plotting an exponentially weighted moving average of these returns with a half-life of one year.

new currencies.

The top panel of Figure 9 plots the raw weekly bitcoin return series in USD, net of hacked coins. This is the series for which the equilibrium pricing equation (43) should hold. The bottom panel of the figure plots a smoothed version of the returns series. The raw weekly bitcoin return exhibits substantial variation. Its mean is 3.9% with a standard deviation of 17.3%, a minimum of -40.4%, and a maximum of 110.3%. The smoothed series helps visualise a low-frequency trend of a generally declining return in the course of the sample. We will revisit this plot after the model has been calibrated, overlaying it with the model-implied required expected return to verify model fit.

5.3 Calibration procedure

Calibration proceeds as follows: we replace model variables in (43) by their proxies defined above, and we define the error as the difference between the model-implied bitcoin return in the oncoming period and the realised return. We then perform our calibration by minimising the root mean squared errors (RMSE).

Error definition. Conditional on no-crash in the sample, the model-implied required return for the oncoming period is obtained by inserting (48), (45), and (46) into (43):

$$E_t\left(\frac{(1-\pi_t)\left(1-\bar{h}\right)\left(1+\alpha_1 Benefit_{t+1}\right)}{1+\beta_1 CostMiningFee_t+\beta_2 CostMarketAccess_t}\left(1+\rho_{t+1}\right)\right)=1,$$

where $\pi_t(\lambda_0,\mu)$ is given by (50). One final assumption is needed to define the error that enters the RMSE minimisation. We assume that agents at time t have perfect foresight on the transactional benefit in the oncoming period (θ_{t+1}). This is a relatively innocuous assumption as the proxy for θ_t turns out to be highly persistent.

We define the error as the difference between the model-implied bitcoin return in the oncoming period and the realised return:

$$\varepsilon_{t+1}=\rho_{t+1}-\left(\frac{1+\beta_1 CostMiningFee_t+\beta_2 CostMarketAccess_t}{(1-\pi_t)\left(1-\bar{h}\right)\left(1+\alpha_1 Benefit_{t+1}\right)}-1\right). \tag{51}$$

The model is calibrated by minimising the distance between model-implied returns and realised returns, i.e., the root mean squared error:

$$\min_{\lambda_0\,\mu,\gamma\,\alpha_1\,\beta_1\,\beta_2}\text{RMSE}=\left(\frac{1}{T}\sum_t \varepsilon_t^2\right)^{\frac{1}{2}},$$

where T is the number of observed bitcoin returns and ε_t is defined in (51).

The challenge of optimising a non-linear expression over multiple parameters (the "curse of dimensionality") requires a careful approach. We proceed in two steps:

1. In the first step, we calibrate a linearised version of our multiplicative model. To do

so, we use the Taylor expansion of our model defined in (44) and obtain

$$\varepsilon_{t+1} \approx \rho_{t+1} - \pi_t + \bar{h} - \alpha_1 Benefit_{t+1} + \beta_1 CostMiningFee_t + \quad + \beta_2 CostMarketAccess. \quad (52)$$

The only non-linearity remaining is in π_t, which is a function of (λ_0, μ). The linearisation, therefore, reduces the curse of dimensionality to manageable proportions. RMSE minimisation proceeds through the search over a two-dimensional evenly-spaced grid for $(\lambda_0, \mu) \in [0, 1) \times [0, 1]$.[35] For each point on the grid, the model is linear in the remaining parameters. These are therefore straightforward to calibrate by RMSE minimisation implemented with ordinary least squares. Figure 10 depicts the RMSE corresponding to the different possible values of the parameters.

2. In the second step, the non-linear model of (51) is calibrated by applying a standard steepest-descent algorithm (BFGS). The calibrated parameters of the linearised model serve as starting values in this minimisation. We will report both sets of parameters because the parameters of the linear model serve as a natural "robustness" check.

We want to emphasise that the goal of our calibration exercise is only to study if there exist parameters that provide a good match of the model to the data. We stop short of actually estimating population parameters. Such an estimation would be difficult, given the statistical problems associated with the short size of our sample and the likely non-stationarity of our variables. Solving these problems would go beyond the scope of the present paper and is left for further research.

5.4 Calibration results

Table 1 presents the calibrated parameter values. Consistent with intuition, calibrated bitcoin required expected returns decrease in the proxy for transactional benefits ($\alpha_1 > 0$) and increase in the cost of market access ($\beta_1 > 0$ and $\beta_2 > 0$). Again, given the above mentioned statistical problems, we do not claim statistical significance of α_1, β_1, or β_2.

A natural way to judge model fit is to plot the smoothed realised bitcoin return of Figure 9 and overlay it with the calibrated required expected return implied by (43). Figure 11 shows

[35] Note that $\mu = 1$ is excluded as a sure crash at time zero is not consistent with the sample in which no such crash occurred. The size of the grid is 100×100.

Table 1: Calibrated parameters

This table contains the calibrated values for the model parameters. The calibration minimises the root mean squared error (RMSE), with errors defined as

$$\varepsilon_{t+1} = \rho_{t+1} - \left(\frac{1 + \beta_1 \mathit{CostMiningFee}_t + \beta_2 \mathit{CostMarketAccess}_t}{(1 - \pi_t)\left(1 - \bar{h}\right)\left(1 + \alpha_1 \mathit{Benefit}_{t+1}\right)} - 1 \right).$$

RMSE is minimised with a standard steepest-descent algorithm (BFGS). The starting values in this minimisation are obtained by calibrating a (partially) linearised model with ordinary least squares (OLS).

	μ	λ_0	α_1	β_1	β_2
Starting values (OLS)	0.07	0.9999000000	0.0039	0.69	0.14
Calibrated values	0.11	0.9999992691	0.0037	0.69	0.14

that our required-return series track the time-varying mean of the realised return series reasonably well.

To assess economic significance of the variables that drive the required return, it is useful to decompose this total return across these variables. The linearised version of the model (44) allows us to do so. Figure 12 thus illustrates the decomposition of the calibrated required expected return. The top graph depicts the total required expected return which is the sum of the five components that follow in the five graphs below it. Figure 12 shows that the required weekly bitcoin return starts at a very high level (between 8 and 18%) during the first two years of our sample period, 2010 and 2011. Expected weekly returns remain high, between 2% and 8%, for the next couple of years. Then, expected returns are lower, around 2%, during the rest of the sample period, except towards the end of 2017.

Figure 12 also shows that crash risk explains a large fraction of the required expected return (around 11 percentage points) during the first two years of the sample period. As time goes by, however, and no crash is observed, Bayesian updating leads to decline in the conditional probability of a crash, which converges to 0. Figure 12 also shows that costs associated with mining fees, delays and congestion on the blockchain are negligible, with the notable exception of 2017. Figure 12 shows that towards the end of 2017, the costs of mining fees, delays and congestion contribute to 10 percentage points of bitcoin required

Figure 10: Root mean squared error linearised model

This figure plots the root mean squared error (RMSE) for the (partially) linearised model. RMSE is plotted as a function of the two parameters, λ_0 and μ, that make up the two-dimensional grid over which is being minimized. *Given* a point on this grid, the model is linear in the remaining parameters $(\alpha_1, \beta_1, \beta_2)$:

$$\rho_{t+1} = \pi_t + \bar{h} - \alpha_1 Benefit_{t+1} + \beta_1 CostMiningFee_t + \beta_2 CostMarketAccess_t + \varepsilon_{t+1}.$$

Ordinary least squares (OLS) can therefore be used to find values for the remaining parameters that minimise the RMSE for this point on the grid.

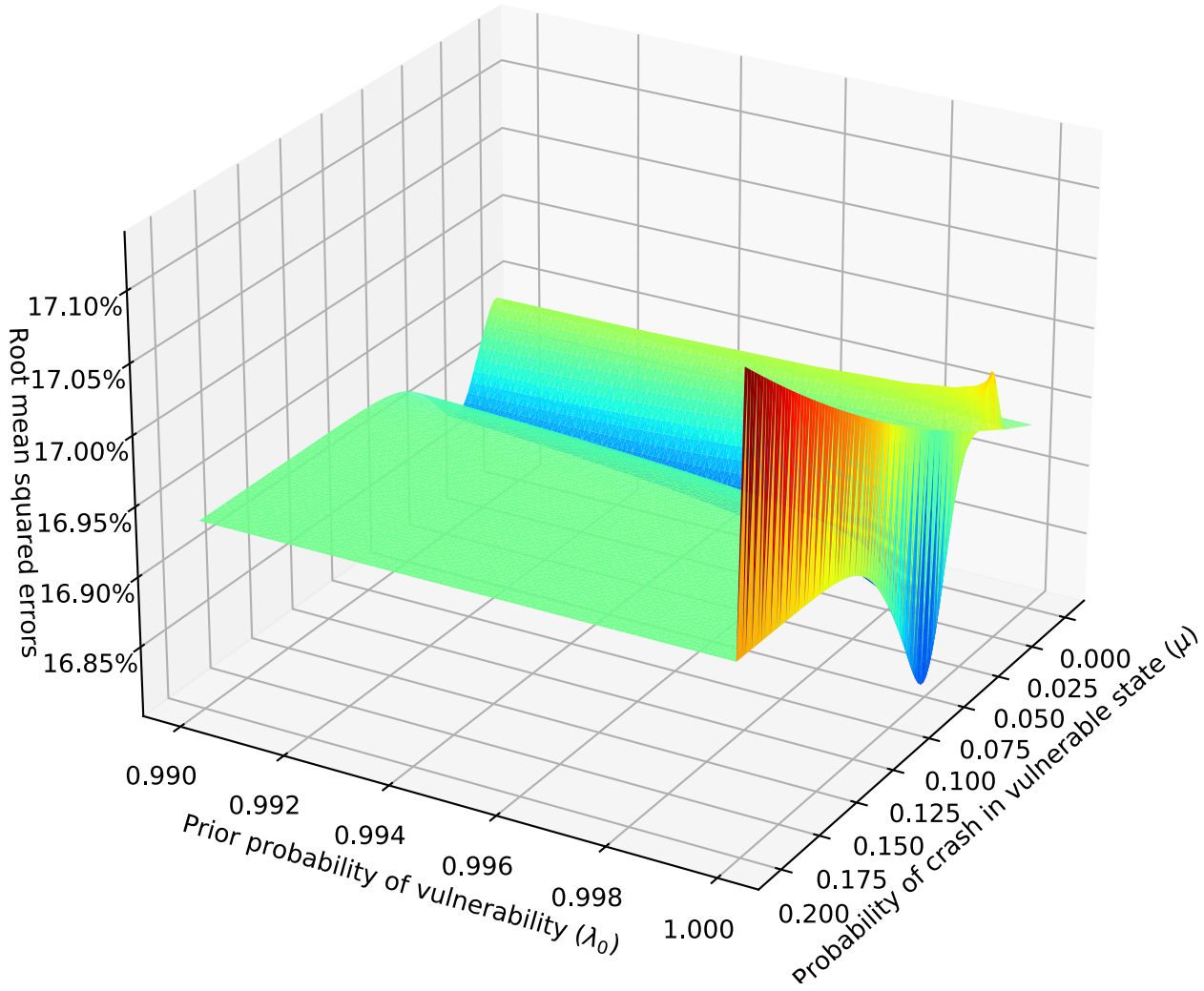
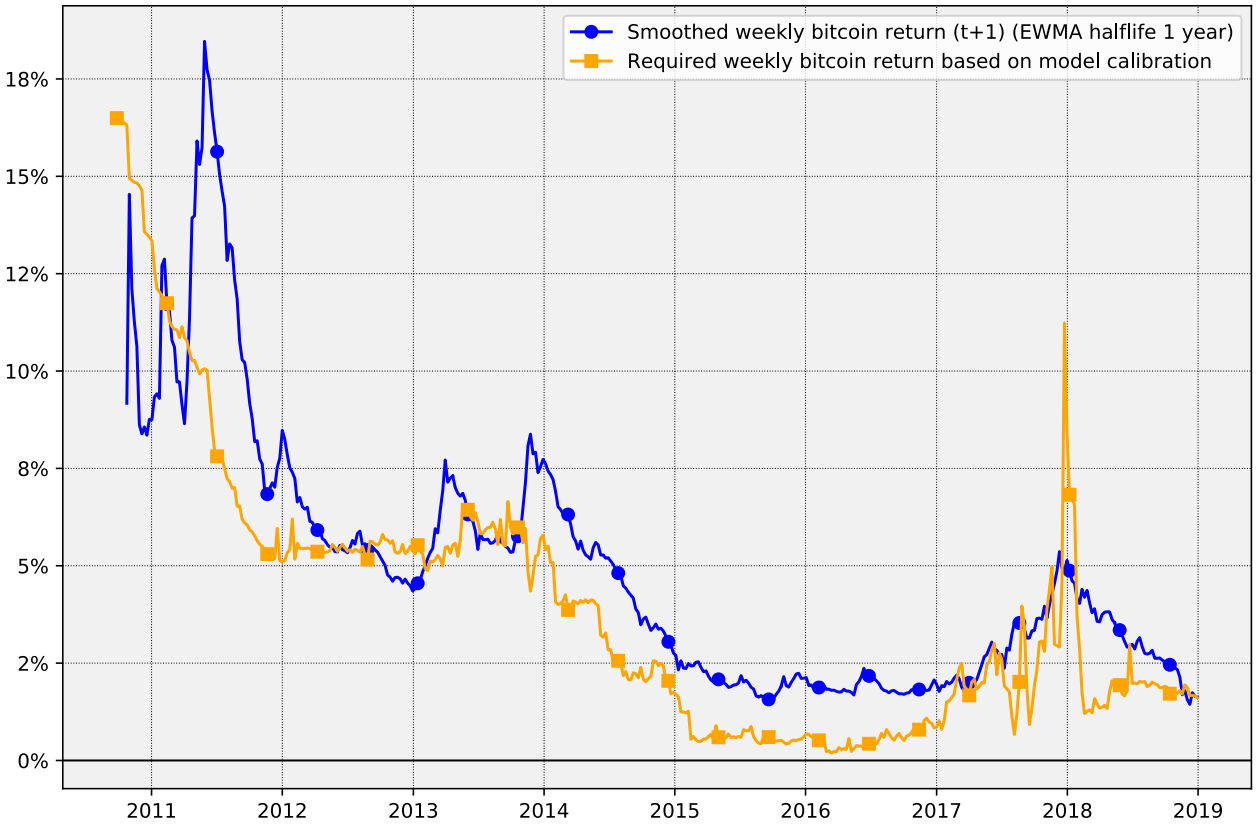


Figure 11: Illustration of model fit
This graph plots the smoothed realised bitcoin return of Figure 9, and overlays it with the required return implied by the calibrated model.



return. Figure 12 also shows that the index proxying for the difficulty to exchange bitcoin against standard currency contributes almost 10 percentage points to the required return at the beginning of the sample, and then around 8 percentage points in the rest of the sample. The contribution of hack risk is relatively small, as it amounts to only 4 basis points.

Against these costs, Figure 12 shows that the transactional benefit component (θ) starts around 0 at the beginning of the sample but increases until 2015. From that point on the calibrated transactional benefit, which underlies the fundamental value of the cryptocurrency, is around 8%. Such large magnitude may be viewed as implausible. It is useful, however, to compare this magnitude to that of, for instance, the cost of cross border fund transfers.

According to World Bank data, the cost of remittances is around 6%.[36] To that amount, one must add, for countries with severe capital controls, the cost of avoiding these controls.

While our calibration quantifies the effect of fundamentals on required expected returns, it also provides information on how much of the time variation in bitcoin return can be attributed to a changing model-implied required expected return. To do so, let us compute an R-squared. The standard deviation of the calibrated model-implied required expected return is 3.9%. The standard deviation of realised returns is much larger, since it is 17.3%. The R-squared therefore is $(3.9\%)^2/(17.3\%)^2 = 5.2\%$. Thus, changes in fundamental variables explain only a small fraction of the variation in bitcoin returns.[37] To interpret the result that fundamentals explain only 5.2% of the variance of bitcoin returns, it is useful to bear in mind that, in our theoretical model, return volatility can reflect extrinsic noise in addition to changes in fundamental variables, as stated in Proposition 6. Thus, in the framework of our model, our empirical results suggest a decomposition of the total variance of bitcoin returns: 5.2% stems from changes in fundamentals, while the remaining 94.8% reflects extrinsic noise.[38]

6 Conclusion

We build an overlapping generations rational expectation equilibrium model relating the price of a cryptocurrency to its fundamentals: transaction costs and benefits. The model shows how these fundamentals should be priced, and highlights the interaction between expected future prices and fundamentals. The model also shows that equilibrium price volatility can be increased by extrinsic volatility unrelated to fundamentals.

We then calibrate the equilibrium pricing equation, relying on a hand-collected dataset of fundamental events that affect the ease for agents to transact in bitcoins. Using these data we construct proxies for the fundamentals of bitcoin: its transaction costs and benefits. We show that these fundamentals are significant determinants of bitcoin returns, and we provide

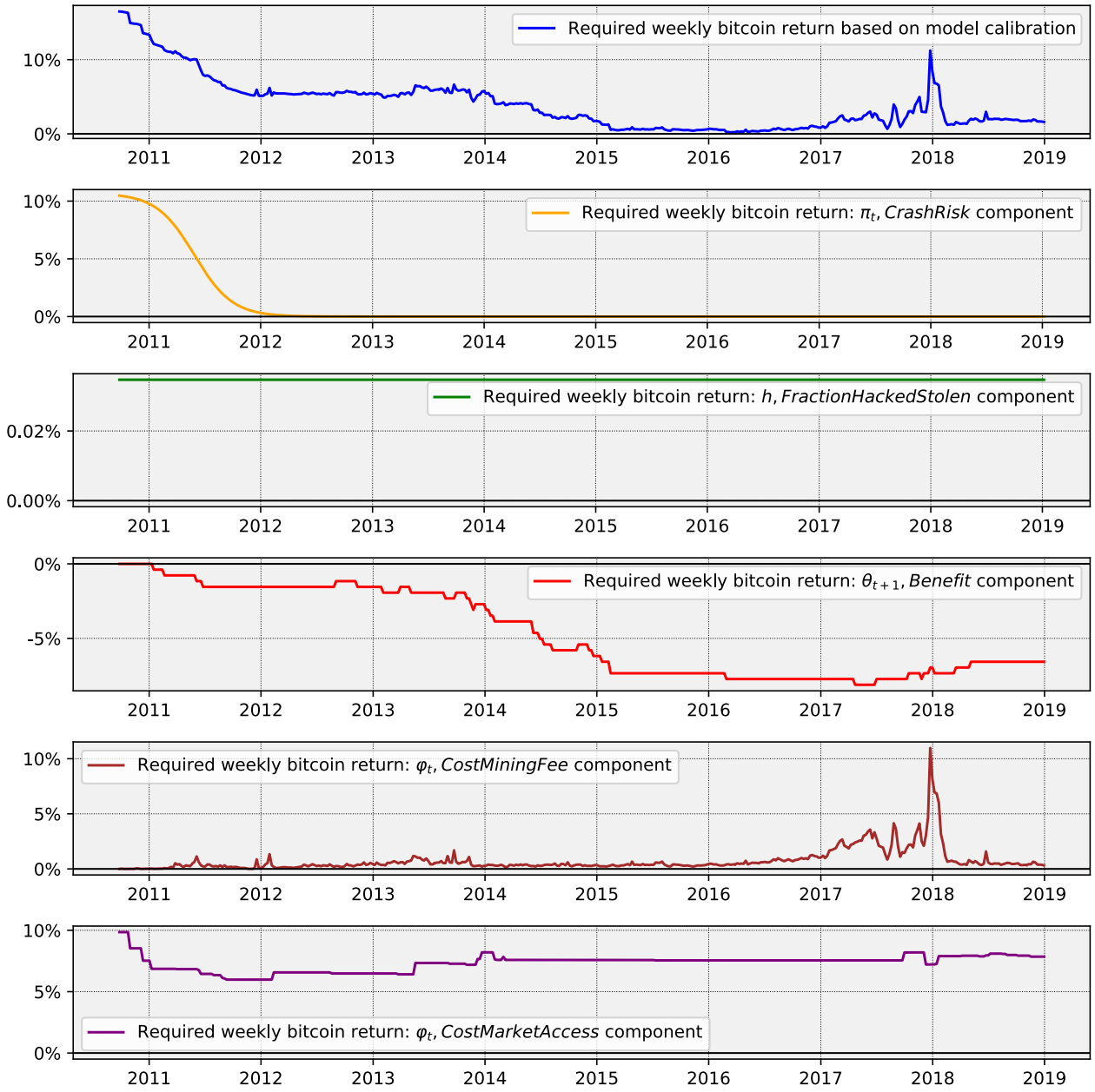
[36] See "The World Bank, Remittance Prices Worldwide," available at http://remittanceprices.worldbank.org.

[37] This is not unlike traditional currencies, for which fundamentals (such as money supply, interest rates or trade balances) also have no predictive power (see Meese and Rogoff, 1983), at least up to a yearly horizon.

[38] If the set of events we used to construct the transactional benefits and market access indices was incomplete, this would reduce the calibrated contribution of fundamentals to bitcoin returns and bias upward our estimate of the share of extrinsic noise in bitcoin fluctuations.

Figure 12: Bitcoin required return components

This figure plots a decomposition of the required bitcoin return across all model variables that contribute to it. The decomposition is based on the linearised model. The top graph plots the total required return and the graphs below it decompose it into five components.



quantitative measures of their relative importance over time. Consistent with our theoretical implication that equilibrium prices can exhibit extrinsic volatility, our calibration also shows that a large part of the variation in prices is not explained by changes in fundamentals.

Reflecting the very large realised bitcoin returns, our calibrated transactional costs and benefits are very large, and arguably implausible. This calls for extensions of our framework that could better rationalise observed returns. Our calibration relies on a simple Bayesian specification of agents' beliefs about crash risk. Richer specifications, possibly allowing for differences in beliefs, or keeping the probability of crash high even after a long period without crash, could help match the data with more plausible parameters.

Appendix 1: Proofs

Proof of Proposition 1: In the main text, we solved for prices and quantities under the assumption that consumption was strictly positive (i.e. the constraint $c_t^y \geq 0$ did not bind). We show here that Equation (9) also holds when considering explicitly the non-negativity constraint on young investors' consumption.

Formally, let μ be the Lagrange multiplier associated with the constraint that young investors' consumption be non-negative, $c_t^y \geq 0$. With that constraint, the young investors' optimisation problem becomes

$$\max_{q_t, s_t, \hat{q}_t} u(c_t^y) + \beta \mathbb{E}_t u(c_{t+1}^o) + \mu c_t^y$$

First-order conditions with respect to q_t, s_t and $\hat{q}_t$ write, respectively

$$-u'(c_t^y)p_t + \beta \mathbb{E}_t \left[u'(c_{t+1}^o)(1-h_{t+1}) \frac{(1+\theta_{t+1})}{1+\varphi'(q_t)} p_{t+1} \right] = \mu p_t \tag{53}$$

$$-u'(c_t^y) + \beta(1+r_t)\mathbb{E}_t \left[u'(c_{t+1}^o) \right] = \mu \tag{54}$$

$$-u'(c_t^y)\hat{p}_t + \beta \mathbb{E}_t \left[u'(c_{t+1}^o)\hat{p}_{t+1} \right] = \mu \hat{p}_t \tag{55}$$

Suppose $\mu > 0$, i.e., the consumption non-negativity constraint binds. Then combining (53) and (54) yields the cryptocurrency pricing equation (9) in Proposition 1.

To write the cryptocurrency price as the present value of its expected discounted transactional benefits, note that (9) implies that the price at period $t+1$ verifies

$$p_{t+1} = E_{t+1} \left[\frac{1-h_{t+2}}{1+r_{t+1}} \frac{u'(c_{t+2}^o)}{E_{t+1}\left[u'(c_{t+2}^o)\right]} (p_{t+2} + \mathcal{T}_{t+2} p_{t+2}) \right]. \tag{56}$$

Substituting (56) into (9) yields

$$p_t = E_t \left[\left(\frac{1-h_{t+1}}{1+r_t} \frac{u'(c_{t+1}^o)}{E_t\left[u'(c_{t+1}^o)\right]} \right) (1+\mathcal{T}_{t+1}) \left(\frac{1-h_{t+2}}{1+r_{t+1}} \frac{u'(c_{t+2}^o)}{E_t\left[u'(c_{t+2}^o)\right]} \right) (1+\mathcal{T}_{t+2}) p_{t+2} \right].$$

Iterating we obtain (10), or equivalently

$$p_t = E_t \left[\left(\prod_{k=1}^{K} (1 - h_{t+k}) \frac{u'(c^o_{t+k})}{E_t \left[u'(c^o_{t+k}) \right]} \frac{(1 + \mathcal{T}_{t+k})}{1 + r_{t+k-1}} \right) p_{t+K} \right]. \tag{57}$$

QED

Proof of Proposition 3: For power utility, the equilibrium condition for the cryptocurrency (17) yields

$$\begin{aligned} & (e - m\hat{p} - Xp) D^{\frac{1}{\gamma}} = m\hat{p} + Xp(1 + \theta) \\ \Leftrightarrow \quad & Xp = \frac{eD^{\frac{1}{\gamma}} - m\hat{p}(1 + D^{\frac{1}{\gamma}})}{1 + \theta + D^{\frac{1}{\gamma}}}. \end{aligned} \tag{58}$$

This is the first equation in Proposition 3. Similarly, the equilibrium condition for the standard currency (16) yields

$$\theta(1 - \pi)(m\hat{p} + Xp(1 + \theta))^{-\gamma} = \pi(m\hat{p}_c)^{-\gamma} \frac{\hat{p}_c}{\hat{p}} \tag{59}$$

Using (58) to substitute Xp in (59) yields

$$\begin{aligned} & \theta(1 - \pi) \left(m\hat{p} + \frac{eD^{\frac{1}{\gamma}} - m\hat{p}(1 + D^{\frac{1}{\gamma}})}{1 + \theta + D^{\frac{1}{\gamma}}} (1 + \theta) \right)^{-\gamma} = \pi(m\hat{p}_c)^{-\gamma} \frac{\hat{p}_c}{\hat{p}} \\ \Leftrightarrow \quad & \theta(1 - \pi) \left(\frac{(1 + \theta) D^{\frac{1}{\gamma}} e - \theta D^{\frac{1}{\gamma}} m\hat{p}}{1 + \theta + D^{\frac{1}{\gamma}}} \right)^{-\gamma} = \pi(m\hat{p}_c)^{-\gamma} \frac{\hat{p}_c}{\hat{p}}. \end{aligned} \tag{60}$$

This is the second equation in Proposition 3. The left-hand side of (60) is increasing in $\hat{p}$. The right-hand side of (60) is decreasing and tends to $+\infty$ when $\hat{p} \to 0$. From (58), $m\hat{p}$

is at most equal to $eD^{\frac{1}{\gamma}}/(1+D^{\frac{1}{\gamma}})$. Therefore (60) has a solution iff

$$\begin{aligned}
& \theta(1-\pi)\left(\frac{D^{\frac{1}{\gamma}}}{1+D^{\frac{1}{\gamma}}}e\right)^{-\gamma} > \pi\left(\frac{\beta^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}e\right)^{-\gamma}\frac{\beta^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\frac{1+D^{\frac{1}{\gamma}}}{D^{\frac{1}{\gamma}}} \\
\Leftrightarrow \quad & \theta(1-\pi)\left(1+D^{\frac{1}{\gamma}}\right)^{\gamma} > \pi\frac{(1+\beta^{\frac{1}{\gamma}})^{\gamma}}{\beta}\frac{\beta^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\left(1+D^{\frac{1}{\gamma}}\right)\frac{D}{D^{\frac{1}{\gamma}}} \\
\Leftrightarrow \quad & \beta\theta\frac{1-\pi}{\pi}\left(\frac{1+D^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\right)^{\gamma} > \beta^{\frac{1}{\gamma}}\frac{1+D^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\frac{D}{D^{\frac{1}{\gamma}}} \\
\Leftrightarrow \quad & \left(\frac{1+D^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\right)^{\gamma-1} > \frac{\pi(1+\theta)}{\theta(1-\pi)^{\frac{1}{\gamma}}(1+\theta)^{\frac{1}{\gamma}}},
\end{aligned} \tag{61}$$

which is the equilibrium condition stated in Proposition 3.

QED

Proof of Corollary 1: Condition (18) can be written

$$\frac{\theta(1+\theta)^{\frac{1-\gamma}{\gamma}}}{(1+\beta^{\frac{1}{\gamma}})^{\gamma-1}} > \frac{\pi}{(1-\pi)^{\frac{1}{\gamma}}(1+(\beta(1-\pi)(1+\theta))^{\frac{1}{\gamma}})^{\gamma-1}}. \tag{62}$$

Define $g(\pi) = \pi(1-\pi)^{-\frac{1}{\gamma}}(1+D^{\frac{1}{\gamma}})^{1-\gamma}$. See that when $\gamma \geq 1$, g is increasing in π, hence (62) is equivalent to $\pi < \overline{\pi}$. When $\gamma < 1$, rewrite g as

$$g(\pi) = \frac{\pi\left((1-\pi)^{-\frac{1}{\gamma}}(\beta(1+\theta))^{\frac{1}{\gamma}}\right)^{1-\gamma}}{1-\pi}. \tag{63}$$

Again, see that g is strictly increasing in π.

QED

Proof of Corollary 2: We first establish that investors require a positive risk premium for the cryptocurrency when their consumption decreases after the crash. In the constant price equilibrium with $\varphi = h = 0$ and constant e, X, and π, the FOCs for the cryptocurrency,

standard currency, and risk-free asset are

$$\begin{aligned} u'(c^y) &= \beta(1-\pi)(1+\theta)u'(c^o_{nc}) && (64)\\ u'(c^y) &= \beta\left[(1-\pi)u'(c^o_{nc}) + \pi u'(c^o_c)\frac{\hat{p}_c}{\hat{p}}\right] && (65)\\ u'(c^y) &= \beta(1+r)\left[(1-\pi)u'(c^o_{nc}) + \pi u'(c^o_c)\right], && (66) \end{aligned}$$

where c^o_{nc} denotes the consumption of old investors if there is no crash, and c^o_c their consumption otherwise. Combining (64) and (66) yields

$$\frac{(1-\pi)(1+\theta)}{1+r} = \frac{(1-\pi)u'(c^o_{nc}) + \pi u'(c^o_c)}{u'(c^o_{nc})}$$

and therefore, the cryptocurrency commands a (strictly positive) risk premium iff

$$u'(c^o_{nc}) < u'(c^o_c) \Leftrightarrow c^o_c < c^o_{nc} \Leftrightarrow \frac{m\hat{p}_c}{m\hat{p} + Xp(1+\theta)} < 1.$$

For power utility, see that (59) implies that $\frac{m\hat{p}_c}{m\hat{p}+Xp(1+\theta)} < 1$ iff

$$\hat{p} > \frac{\pi}{\theta(1-\pi)}\hat{p}_c. \tag{67}$$

We next prove that (67) holds at equilibrium. To do so, we first need to show that the equilibrium condition (18) implies $(1-\pi)(1+\theta) > 1$. There are two cases.

1. $\gamma \geq 1$

   By contradiction: suppose $(1-\pi)(1+\theta) \leq 1$.

   $(1-\pi)(1+\theta) \leq 1$ implies the left-hand side of (18) is smaller than 1. It also implies that $\pi(1+\theta) > \theta$. Therefore (18) implies

   $$\frac{1}{(1-\pi)^{\frac{1}{\gamma}}(1+\theta)^{\frac{1}{\gamma}}} < 1,$$

   a contradiction.

2. $\gamma < 1$

For $\pi > 0$, (18) is equivalent to

$$\left(\frac{\frac{1}{(1-\pi)^{\frac{1}{\gamma}}} + (\beta(1+\theta))^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}} \right)^{\gamma-1} > \frac{\pi(1+\theta)}{\theta(1-\pi)(1+\theta)^{\frac{1}{\gamma}}}. \tag{68}$$

The left-hand side of (68) is strictly decreasing in π while the right-hand side is strictly increasing in π. Note also that if $\pi = \frac{\theta}{1+\theta} \Leftrightarrow (1-\pi)(1+\theta) = 1$, then the left-hand side of (68) is equal to its right-hand side. It follows that

$$\pi < \frac{\theta}{1+\theta} \Leftrightarrow (1-\pi)(1+\theta) > 1.$$

Last, (67) holds in equilibrium iff the left-hand side of (20) is smaller than the right-hand side of (20) when evaluated at

$$\hat{p} = \frac{\pi}{\theta(1-\pi)}\hat{p}_c.$$

This is equivalent to

$$\begin{aligned}
& \frac{\theta(1-\pi)}{D}\left(\frac{(1+\theta)e - \frac{\pi}{1-\pi}m\hat{p}_c}{1+\theta+D^{\frac{1}{\gamma}}}\right)^{-\gamma} < \pi(m\hat{p}_c)^{-\gamma}\frac{\theta(1-\pi)}{\pi} \\
\Leftrightarrow \quad & \frac{1+\theta+D^{\frac{1}{\gamma}}}{(1+\theta)e - \frac{\pi}{1-\pi}m\hat{p}_c} < \frac{D^{\frac{1}{\gamma}}}{m\hat{p}_c} \\
\Leftrightarrow \quad & (1+\theta+D^{\frac{1}{\gamma}})\frac{m\hat{p}_c}{e} < (1+\theta)D^{\frac{1}{\gamma}} - \frac{\pi}{1-\pi}D^{\frac{1}{\gamma}}\frac{m\hat{p}_c}{e} \\
\Leftrightarrow \quad & \left(1+\frac{\pi}{1-\pi}\right)\frac{\beta^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}D^{\frac{1}{\gamma}} < (1+\theta)\left(D^{\frac{1}{\gamma}} - \frac{\beta^{\frac{1}{\gamma}}}{1+\beta^{\frac{1}{\gamma}}}\right) \\
\Leftrightarrow \quad & \frac{1}{1-\pi}\beta^{\frac{1}{\gamma}}D^{\frac{1}{\gamma}} < (1+\theta)\left(D^{\frac{1}{\gamma}}(1+\beta^{\frac{1}{\gamma}}) - \beta^{\frac{1}{\gamma}}\right) \\
\Leftrightarrow \quad & D^{\frac{1}{\gamma}} < (1+\theta)(1-\pi)\left(((1+\theta)(1-\pi))^{\frac{1}{\gamma}}(1+\beta^{\frac{1}{\gamma}}) - 1\right) \\
\Leftrightarrow \quad & 0 < (1+\theta)(1-\pi)[((1+\theta)(1-\pi))^{\frac{1}{\gamma}} - 1] + D^{\frac{1}{\gamma}}[(1+\theta)(1-\pi) - 1]
\end{aligned}$$

which is true since $(1-\pi)(1+\theta) > 1$.

QED

Proof of Proposition 4: Condition $\theta(1-\pi) > \pi$ (which is equivalent to (25)) straightforwardly follows from (18) when $\gamma = 1$.

Next, Equation (20) with log utility yields

$$\begin{aligned}
&\frac{(1-\pi)\theta}{D}\frac{1+\theta+D}{(1+\theta)e-\theta m\hat{p}} = \pi\frac{1+\beta}{e\beta}\frac{\frac{e\beta}{1+\beta}}{m\hat{p}} \\
\Leftrightarrow\ & m\hat{p}((1-\pi)\theta(1+\theta)+\theta D) = \pi D(1+\theta)e \\
\Leftrightarrow\ & \frac{m\hat{p}}{e} = \frac{\pi(1+\theta)}{\theta}\frac{\beta}{1+\beta}.
\end{aligned} \tag{69}$$

Last, using (27), Equation (26) with log utility yields

$$\begin{aligned}
\frac{Xp}{e} =& \frac{D-\frac{\pi(1+\theta)}{\theta}\frac{\beta}{1+\beta}(1+D)}{1+\theta+D} \\
=& \frac{\theta(1+\beta)D-\pi(1+\theta)\beta(1+D)}{\theta(1+\beta)(1+\theta)(1+\beta(1-\pi))} \\
=& \frac{(1+\beta(1-\pi))\theta(1+\beta)-\theta(1+\beta)-\pi\beta(1+\beta(1-\pi)(1+\theta))}{\theta(1+\beta)(1+\beta(1-\pi))} \\
=& \frac{\beta}{1+\beta}(1-\pi(1+\frac{1}{\theta})).
\end{aligned} \tag{70}$$

QED

Proof of Proposition 5: From Proposition 3, we know that for each realisation of π_N, prices defined by (29) and (30) form a unique continuation equilibrium as long as $\pi_N < \overline{\pi}$.

We now show that given equilibrium prices at N, there exists a unique pair of prices $p(\pi_{N-1})$ and $\hat{p}(\pi_{N-1})$ at $N-1$ solving (31) and (32). That is, for a given probability of a crash π_{N-1}, we study the system of two equations with two unknowns, p and $\hat{p}$:

$$\frac{\beta^{-1}p}{(e-Xp-m\hat{p})^{\gamma}} = (1+\theta)(1-\pi_{N-1})Z, \tag{71}$$

$$\frac{\beta^{-1}\hat{p}}{(e-Xp-m\hat{p})^{\gamma}} = (1-\pi_{N-1})\hat{Z} + \pi_{N-1}\frac{\hat{p}_c}{(m\hat{p}_c)^{\gamma}}, \tag{72}$$

where

$$Z \equiv \left[\frac{x_N p(\pi_N^u)}{(Xp(\pi_N^u)(1+\theta) + m\hat{p}(\pi_N^u))^\gamma} + \frac{(1-x_N)p(\pi_N^d)}{(Xp(\pi_N^d)(1+\theta) + m\hat{p}(\pi_N^d))^\gamma} \right],$$

$$\hat{Z} \equiv \left[\frac{x_N \hat{p}(\pi_N^u)}{(Xp(\pi_N^u)(1+\theta) + m\hat{p}(\pi_N^u))^\gamma} + \frac{(1-x_N)\hat{p}(\pi_N^d)}{(Xp(\pi_N^d)(1+\theta) + m\hat{p}(\pi_N^d))^\gamma} \right].$$

Note that Z, $\hat{Z}$ and therefore the right-hand sides of (71) and (72) are independent from p and $\hat{p}$.

For any $\hat{p} \in (0, \frac{e}{m})$, the left-hand side of (71) is strictly increasing in p for $p \in (0, (e - m\hat{p})/X)$, tends to 0 when p tends to 0 and to $+\infty$ when p tends to $(e - m\hat{p})/X$. Therefore (71) implicitly defines a function $p(\hat{p})$ for $\hat{p} \in (0, \frac{e}{m})$. Furthermore,

$$0 < p(\hat{p}) < (e - m\hat{p})/X, \tag{73}$$

and total differentiation of (71) yields

$$\begin{aligned} & \frac{\partial p}{\partial \hat{p}}(\hat{p})(e - Xp(\hat{p}) - m\hat{p})^{-\gamma} + \gamma p(\hat{p})(e - Xp(\hat{p}) - m\hat{p})^{-\gamma-1}(X\frac{\partial p}{\partial \hat{p}}(\hat{p}) + m) = 0 \\ \Leftrightarrow \quad & \frac{\partial p}{\partial \hat{p}}(\hat{p})(e - Xp(\hat{p}) - m\hat{p}) + \gamma p(\hat{p})(X\frac{\partial p}{\partial \hat{p}}(\hat{p}) + m) = 0. \end{aligned} \tag{74}$$

(74) implies

$$\frac{\partial p}{\partial \hat{p}}(\hat{p}) < 0. \tag{75}$$

Let $g(\hat{p})$ be the left-hand side of (72) where p is the implicit function of $\hat{p}$ we just defined:

$$g(\hat{p}) \equiv \frac{\beta^{-1}\hat{p}}{(e - Xp(\hat{p}) - m\hat{p})^\gamma}. \tag{76}$$

Differentiating,

$$g'(\hat{p}) = \frac{\beta^{-1}}{(e - Xp(\hat{p}) - m\hat{p})^\gamma} + \frac{\gamma\beta^{-1}\hat{p}}{(e - Xp(\hat{p}) - m\hat{p})^{\gamma+1}}(X\frac{\partial p}{\partial \hat{p}}(\hat{p}) + m),$$

that has the sign of

$$e - Xp(\hat{p}) - m\hat{p} + \gamma\hat{p}(X\frac{\partial p}{\partial \hat{p}}(\hat{p}) + m),$$

which, using (74), is equal to

$$e - Xp(\hat{p}) - m\hat{p} - \frac{\partial p}{\partial \hat{p}}(\hat{p})\frac{\hat{p}}{p(\hat{p})}(e - Xp(\hat{p}) - m\hat{p}),$$

which, from (73) and (75), is strictly positive.

Hence, $g(.)$ is strictly increasing and admits the following limits.

- $g(\hat{p}) \to 0$ when $\hat{p} \to 0$.

  From (76), this is true if $\lim_{\hat{p}\to 0} p(\hat{p}) < \frac{e}{X}$. We know from (73) that $p(\hat{p}) < \frac{e}{X}$. Suppose $\lim_{\hat{p}\to 0} p(\hat{p}) = \frac{e}{X}$, then the left-hand side of (71) tends to $+\infty$ when $\hat{p} \to 0$ while the right-hand side is finite, a contradiction (in other words, we cannot have $p = \frac{e}{X}$ as young investors would then prefer to consume and buy less cryptocurrencies).

- $g(\hat{p}) \to +\infty$ when $\hat{p} \to \frac{e}{m}$.

  From (76), this is true if $p(\hat{p}) \to 0$ when $\hat{p} \to \frac{e}{m}$, which is implied by (73).

It follows that there is a unique $\hat{p} \in (0, \frac{e}{m})$ such that $g(\hat{p}) = (1 - \pi_{N-1})\hat{Z} + \pi_{N-1}\frac{\hat{p}_c}{m\hat{p}_c}$. To that unique $\hat{p}$ corresponds a unique $p(\hat{p})$, thus the system $\{(71), (72)\}$ has a unique solution.

Therefore, given prices $p(\pi_N)$ and $\hat{p}(\pi_N)$ at period N, there exists a unique pair of prices $p(\pi_{N-1})$ and $\hat{p}(\pi_{N-1})$ consistent with equilibrium conditions at period $N-1$. Iterating backward, we can find equilibrium prices at $t-1$ as a function of equilibrium prices at t for all $t \leq N-1$.

Proof of Proposition 6: We want to prove that if (33) holds for p_t then it holds for $\bar{p}_t$. Start from the equilibrium condition for p_t

$$p_t = \frac{1}{1+r_t} E_t \left[(1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) p_{t+1} \right].$$

Multiplying both sides by $\lambda \left(\prod_{\tau=1}^{t} u_\tau \right)$, we have

$$\lambda \left(\prod_{\tau=1}^{t} u_\tau \right) p_t = \frac{1}{1+r_t} E_t \left[\lambda \left(\prod_{\tau=1}^{t} u_\tau \right) (1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) p_{t+1} \right].$$

The left-hand side is $\bar{p}_t$. So we have

$$\bar{p}_t = \frac{1}{1+r_t} E_t \left[\lambda \left(\prod_{\tau=1}^{t} u_\tau \right) (1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) p_{t+1} \right].$$

Moreover, since u_{t+1} has unit expectation and is independent from the investors' period t information set, we have

$$\begin{aligned} E_t \left[\lambda \left(\prod_{\tau=1}^{t} u_\tau \right) (1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) p_{t+1} \right] &= E_t \left[\lambda \left(\prod_{\tau=1}^{t+1} u_\tau \right) (1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) p_{t+1} \right] \\ &= E_t \left[(1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) \bar{p}_{t+1} \right]. \end{aligned}$$

So

$$\bar{p}_t = \frac{1}{1+r_t} E_t \left[(1 - h_{t+1}) (1 + \mathcal{T}_{t+1}) \bar{p}_{t+1} \right].$$

QED

References

Athey, S., I. Parashkevov, V. Sarukkai and J. Xia, 2016, "Bitcoin Pricing, Adoption, and Usage: Theory and Evidence", Stanford University Graduate School of Business Research Paper No. 16-42.

Auer, R., and S. Claessens, 2018, "Regulating Cryptocurrencies: Assessing Market Reactions", *BIS Quarterly Review*, pp. 51-65.

Auer, R, C. Monnet and H. S. Shin, 2021, "Permissioned distributed ledgers and the governance of money", BIS Working Papers No 924.

Bacchetta, P., C. Tille, and E. van Wincoop, 2012, "Self-Fulfilling Risk Panics", *American Economic Review* 102(7), pp. 3674-3700.

Benigno, P. L. Schilling and H. Uhlig, 2019, "Cryptocurrencies, Currency Competition, and the Impossible Trinity", University of Chicago, Becker Friedman Institute for Economics Working Paper No. 2019-108.

Bhambhwani, S., S. Delikouras and G. Korniotis, 2019, "Do Fundamentals Drive Cryptocurrency Prices?", CEPR Discussion Paper No. DP13724.

Biais, B., P. Bossaerts, and C. Spatt, 2010, "Equilibrium Asset Pricing and Portfolio Choice Under Asymmetric Information", *The Review of Financial Studies* 23(4), pp. 1503-1543.

Bianchi, D., 2020, "Cryptocurrencies as an Asset Class: an Empirical Assessment", "The Journal of Alternative Investments" 23(2), pp. 162-179.

Borri, N. and K. Shakhnov, 2019, "The Cross-Section of Cryptocurrency Returns", Working paper.

Campbell, J., and R. Shiller, 1988, "Stock Prices, Earnings, and Expected Dividends", *Journal of Finance* 43, pp. 661-676.

Campbell, J., and R. Shiller, 1988, "The Dividend-Price Ratio and Expectations of Future Dividends and Discount Factors", *The Review of Financial Studies* 1(3), pp. 195-228.

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

Chiu, J. and T. Koeppl, 2017, "The Economics of Cryptocurrencies - Bitcoin and Beyond", Working paper, Queen's University.

Choi, Michael, and G. Rocheteau, 2020, "Money Mining and Price Dynamics", forthcoming *American Economic Journal: Macroeconomics*.

Cong, L. W., Y. Li, and N. Wang., 2021, "Tokenomics: Dynamic Adoption and Valuation", *Review of Financial Studies* 34 (3), pp. 1105-1155.

Easley, D., M. O'Hara, and S. Basu, 2019, "From Mining to Markets: The Evolution of Bitcoin Transaction Fees", *Journal of Financial Economics* 134, pp. 91-109.

Fernández-Villaverde, J., and D. Sanchez, 2019, "Can Currency Competition Work?", *Journal of Monetary Economics* 106, pp. 1-15.

Gaballo, G. and E. Mengus, 2021, "Optimal Price Level Determination by Short-Run Redistribution Policies", Working paper, HEC Paris.

Garratt, R. and N. Wallace, 2018, "Bitcoin 1, Bitcoin 2...: an Experiment with Privately Issued Outside Monies", *Economic Inquiry*, 56 (3), pp. 1887-1897.

Hautsch, N., C. Scheuch, and S. Voigt, 2020, "Building Trust Takes Time: Limits to Arbitrage in Blockchain-Based Markets", Working paper.

Hendry, S. and Y. Zhu, 2019, "A Framework for Analyzing Monetary Policy in an Economy with E-money", Bank of Canada Staff Working Paper 2019-1.

Huberman, G., J. Leshno, and C. Moalleni, 2021, "Monopoly without a monopolist: An Economic Analysis of the Bitcoin Payment System", forthcoming *Review of Economic Studies*.

Iyidogan, E., 2019, "An Equilibrium Model of Blockchain-Based Cryptocurrencies", Working paper.

Kalodner, H., S. Goldfeder, A. Chator, M. Möser, and A. Narayanan, 2017, "BlockSci: Design and Applications of a Blockchain Analysis Platform", Working paper, arXiv:1709.02489v1.

Kareken, J. and N. Wallace, 1981, "On the Indeterminacy of Equilibrium Exchange Rates", *Quarterly Journal of Economics* 96(2), pp. 207-222.

Lagos, L. and R. Wright, 2005, "A Unified Framework for Monetary Theory and Policy Analysis ", *Journal of Political Economy* 113, pp. 463-484.

Liu, Y. and A. Tsyvinski, 2021, "Risks and Returns of Cryptocurrency", *The Review of Financial Studies* 34(6), pp. 2689-2727.

Liu, Y., A. Tsyvinski and X. Wu, 2021, "Common Risk Factors in Cryptocurrency", forthcoming *Journal of Finance*.

Makarov, I., and A. Schoar, 2020, "Trading and Arbitrage in Cryptocurrency Markets", *Journal of Financial Economics* 135, pp. 293-319.

Meese R., and K. Rogoff, 1983, "Empirical Exchange Rate Models of the Seventies: Do They Fit Out of Sample?", *Journal of International Economics* 14, pp. 3-24.

Meiklejohn S., M. Pomarole, G. Jordan, K. Levchenko, D. McCoy, G. M. Voelker, and S. Savage, "A Fistful of Bitcoins: Characterizing Payments Among Men With No Names", In Proceedings of the 2013 conference on Internet measurement conference (IMC '13). ACM, New York, NY, USA, pp. 127-140, DOI: `https://doi.org/10.1145/2504730.2504747`.

Paine, A. and W. Knottenbelt, 2016, "Analysis of the CME CF Bitcoin Reference Rate and Real Time Index", Imperial College Centre for Cryptocurrency Research and Engineering, Report.

Pagnotta, E., 2021, "Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security", forthcoming *Review of Financial Studies*.

Prat, J., and B. Walter, 2021, "An Equilibrium Model of the Market for Bitcoin Mining", *Journal of Political Economy* 129(8), pp. 2415-2452.

Saleh, F., 2020, "Volatility and Welfare in a Crypto Economy", Working Paper.

Samuelson, P., 1958, "An Exact Consumption-Loan Model of Interest with or without the Social Contrivance of Money", *Journal of Political Economy* 6, pp. 467-482.

Schilling, L. and H. Uhlig, 2019a, "Some Simple Bitcoin Economics", *Journal of Monetary Economics* 106, pp. 16-26.

Shiller, R, 1981, "Do Stock Prices Move Too Much to Be Justified by Subsequent Changes in Dividends?", *American Economic Review* 71, pp. 421-36.

Sockin, M. and W. Xiong, 2020, "A Model of Cryptocurrencies", NBER Working Paper No. w26816.

Spiegel, M., 1998, "Stock Price Volatility in a Multiple Security Overlapping Generations Model", *The Review of Financial Studies* 11(2), pp. 419-447.

Starr, R. M., 1974, "The Price of Money in a Pure Exchange Monetary Economy with Taxation", *Econometrica* 42, pp. 45-54.

Tirole, J., 1985, "Asset Bubbles and Overlapping Generations", *Econometrica* 53, pp. 1499-1528.

Wallace, N., 1980, "The Overlapping Generations Model of Fiat Money", in Neil Wallace and John H. Kareken, eds., *Models of Monetary Economics,* Minneapolis, MN, Federal Reserve Bank of Minneapolis.

Watanabe, M., 2008, "Price Volatility and Investor Behavior in an Overlapping Generations Model with Information Asymmetry", *The Journal of Finance* 63(1), pp. 229-72.

Zimmerman, P, 2020, "Blockchain and Price Volatility", mimeo Said Business School.

Online Appendix

Table 2: Hacks, thefts and losses events

Date	Amount (BTC)	Description
2011-06-13	25000	User Allinvain hacked
2011-06-19	2000	MtGox theft
2011-06-25	4019	MyBitcoin theft
2011-07-26	17000	Bitomat loss
2011-07-29	78739	MyBitcoin theft
2011-10-06	5000	Bitcoin7 hack
2011-10-28	2609	MtGox loss
2012-03-01	46653	Linode hacks
2012-04-13	3171	Betcoin hack
2012-04-27	20000	Tony76 Silk Road scam
2012-05-11	18547	Bitcoinica hack
2012-07-04	1853	MtGox hack
2012-07-13	40000	Bitcoinica theft
2012-07-17	180819	BST Ponzi scheme
2012-07-31	4500	BTC-e hack
2012-09-04	24086	Bitfloor theft
2012-09-28	9222	User Cdecker hacked
2012-10-17	3500	Trojan horse
2012-12-21	18787	Bitmarket.eu hack
2013-05-10	1454	Vircurex hack
2013-06-10	1300	PicoStocks hack
2013-10-02	29655	FBI seizes Silk Road funds
2013-10-25	144336	FBI seizes Silk Road funds
2013-10-26	22000	GBL scam
2013-11-07	4100	Inputs.io hack
2013-11-12	484	Bitcash.cz hack
2013-11-29	5400	Sheep Marketplace closes
2013-11-29	5896	PicoStocks hack
2014-02-13	4400	Silk Road 2 hacked
2014-02-25	744408	MtGox collapse
2014-03-04	896	Flexcoin hack

Continued on next page

Table 2: Hacks, thefts and losses events

Date	Amount (BTC)	Description
2014-03-04	97	Poloniex hack
2014-03-25	950	CryptoRush hacked
2014-10-14	3894	Mintpal hack
2015-01-05	18886	Bitstamp hack
2015-01-28	1000	796Exchange hack
2015-02-15	7170	BTER hack
2015-02-17	3000	KipCoin hack
2015-05-22	1581	Bitfiniex hack
2015-09-15	5000	Bitpay fishing scam
2016-01-15	11325	Cryptsy hack
2016-04-07	315	ShapeShift hack
2016-04-13	154	ShapeShift hack
2016-05-14	250	Gatecoin hack
2016-08-02	119756	Bitfinex hack
2016-10-13	2300	Bitcurex hack
2017-04-22	3816	Yapizon hack
2017-07-12	1942	AlphaBay admin's assets sized by FBI
2017-07-20	1200	Hansa's funds seized by Dutch police
2017-12-06	4736	NiceHash hacked
2018-06-20	2016	Bithumb hacked
2018-09-20	5966	Zaif hacked
2018-10-28	8	MapleChange hack / scam

Table 3: Market access events

Date	Effect	Regions	Weight	Description
2010-07-17	1	USA	0.2270	MtGox USD/BTC exchange opens
2010-10-25	1	USA	0.2270	MtGox eases fund transfers
2010-12-07	1	USA	0.2270	MtGox partners with e-payment company Paxum
2011-01-06	1	EMU	0.1858	Bitcoin-Central EUR/BTC exchange opens
2011-04-01	1	POL	0.0072	Bitomat PLN/BTC exchange opens
2011-06-08	1	CAN	0.0244	CaVirTex CAD/BTC exchange opens
2011-06-13	1	CHN	0.1029	BTCC China CNY/BTC exchange opens
2011-07-28	1	BRA	0.0357	Mercado Bitcoin BRL/BTC exchange opens
2011-08-27	1	JPN	0.0839	MtGox opens JPY/BTC
2011-09-02	1	AUS	0.0190	MtGox opens AUD/BTC
2011-09-06	1	GBR	0.0359	MtGox opens GBP/BTC
2012-02-10	-1	USA	0.2158	Paxum exits bitcoin business
2012-08-17	1	RUS	0.0295	BTC-e opens RUB/BTC
2013-03-20	1	IND	0.0241	LocalBitcoins opens INR/BTC
2013-05-14	-1	USA JPN	0.2842	MtGox suspends fund transfers
2013-09-03	1	KOR	0.0169	Korbit KRW/BTC exchange opens
2013-10-29	1	CAN	0.0239	World first Bitcoin ATM opens
2013-12-03	-1	CHN	0.1240	China bans financial institutions from using bitcoin
2013-12-18	-1	CHN	0.1240	BTC China suspends deposits in yuan
2014-01-30	1	CHN	0.1316	BTC China reinstates deposits in yuan
2014-02-09	1	IDN	0.0112	Indodax opens IDR/BTC
2014-02-25	-1	JPN	0.0612	MtGox shuts down
2014-03-08	1	JPN	0.0612	ANX opens JPY/BTC
2014-10-14	1	PAK	0.0031	Urdubit PKR/BTC exchange opens
2015-07-08	1	NGA	0.0066	BitX opens NGN/BTC
2017-08-13	-1	NPL	0.0003	Nepal bans bitcoin and other cryptocurrencies
2017-09-30	-1	CHN	0.1501	China's exchanges shut down
2017-11-20	-1	MAR	0.0014	Morocco Central Bank bans transactions in bitcoin
2017-12-10	1	USA	0.2409	Future trading starts at CBOE

Continued on next page

Table 3: Market access events

Date	Effect	Regions	Weight	Description
2018-01-01	-1	EGY	0.0029	Egypt's grand mufti issues a fatwa declaring bitcoin trading unlawful under Sharia law
2018-01-13	-1	IDN	0.0121	Bitcoin banned in Indonesia
2018-01-16	-1	CHN	0.1586	China bans citizens from trading bitcoin
2018-04-06	-1	PAK	0.0036	Pakistan Central Bank bans Bitcoin trading by financial companies
2018-04-08	-1	PAK	0.0036	Urdubit closes
2018-05-29	1	IDN	0.0121	Bitcoin can be legally traded as a commodity in Indonesia
2018-06-20	-1	KOR	0.0189	Bithumb suspends all deposits and withdrawals
2018-07-06	-1	IND	0.0318	Indian central bank forbids banks from dealing with entities working with digital currencies
2018-08-01	-1	KOR	0.0189	Bithumb suspends new account registration
2018-08-04	1	KOR	0.0189	Bithumb reopens deposits and withdrawals
2018-08-16	1	THA	0.0059	Thailand's SEC authorizes seven cryptocurrency firms, including five crypto exchanges, to operate in the country
2018-08-30	1	KOR	0.0189	Bithumb resumes accepting new user accounts
2018-10-02	1	IDN	0.0121	Indonesia permits futures trading of crypto assets
2018-11-12	1	RUS	0.0193	Singapore's Huobi opens an office in Russia, with Russian language support

Table 4: Transaction benefits events

Date	Effect	Illegal	Description
2011-01-23	1	1	Silk Road opens
2011-02-25	1	0	CoinCard service opens
2011-06-08	1	0	BTC Buy service opens
2011-06-30	1	1	Black Market Reloaded opens
2012-09-04	-1	0	CoinCard trading service permanently closed
2012-11-15	1	0	WordPress accepts bitcoin
2013-02-06	1	0	PizzaForCoins allows users to order pizza delivery with bitcoins
2013-04-03	-1	0	BTC Buy stops selling prepaid cards
2013-05-09	1	0	Gyft accepts bitcoin
2013-08-27	1	0	eGifter accepts bitcoin
2013-10-02	-1	1	Silk Road closes
2013-11-06	1	1	Silk Road 2.0 opens
2013-11-22	1	0	CheapAir accepts bitcoin for flights
2013-11-27	1	0	Shopify adds a bitcoin payment option for its sellers
2013-12-02	-1	1	Black Market Reloaded closes
2014-01-09	1	0	Overstock.com accepts bitcoin
2014-01-24	1	0	TigerDirect accepts bitcoin
2014-02-03	1	0	CheapAir accepts bitcoin for hotel reservations
2014-06-10	1	0	REEDS Jewelers accepts bitcoin
2014-06-11	1	0	Expedia accepts bitcoin for hotel reservation
2014-07-01	1	0	Newegg accepts bitcoin
2014-07-18	1	0	Dell accepts bitcoin
2014-08-14	1	0	DISH Network accepts bitcoin
2014-11-06	-1	1	Silk Road 2.0 closes
2014-12-11	1	0	Microsoft accepts bitcoin from US customers
2014-12-22	1	1	opening of AlphaBay
2015-01-22	1	0	Paypal accepts bitcoin
2015-02-19	1	0	Dell Expands bitcoin payments to UK and Canada
2015-02-19	1	0	Payment processor Stripe offers bitcoin integration
2016-03-03	1	0	Bidorbuy accepts bitcoin
2017-04-27	1	0	Valve accepts bitcoin
2017-07-05	-1	1	AlphaBay closes

Continued on next page

Table 4: Transaction benefits events

Date	Effect	Illegal	Description
2017-10-19	-1	0	Dell no longer accepts bitcoin
2017-11-29	1	0	Roadway Moving Company accepts bitcoin
2017-12-06	-1	0	Steam no longer accepts bitcoin
2017-12-26	-1	0	Microsoft no longer accepts bitcoin
2018-01-09	1	0	Microsoft resumes bitcoin payments
2018-03-23	-1	0	Payment processor Stripe ends support for bitcoin
2018-05-10	-1	0	Expedia no longer accepts bitcoin

Table 5: Bitcoin forks and cash-in opportunities for bitcoin owners

Cryptocurrency	Ticker	Fork type	Created from	Snapshot date	Ratio	Price date	Market price in USD
Clams	CLAM	Airdrop	BTC, LTC, DOGE	2014-05-12	4.60545574	2014-08-26	0.532033
Bitcore	BTX	Airdrop	BTC	2017-04-26	0.5	2017-04-27	23.72
Bitcoin Cash	BCC, BCH	Hard fork	BTC	2017-08-01	1	2017-08-01	380.1
Bitcoin Gold	BTG	Hard fork	BTC	2017-10-24	1	2017-10-24	142.92
Bitcoin Diamond	BCD	Hard fork	BTC	2017-11-24	10	2017-11-24	69.30
United Bitcoin	UBTC	Hard fork	BTC	2017-12-11	1	2017-12-18	432.92
Super Bitcoin	SBTC	Hard fork	BTC	2017-12-12	1	2017-12-15	343.19
BitcoinX	BCX, BTCX	Hard fork	BTC	2017-12-12	10000	2017-12-15	0.089588
Lightning Bitcoin	LBTC	Airdrop	BTC	2017-12-18	1	2018-01-03	222.65
Bitcoin God	GOD	Hard fork	BTC	2017-12-27	1	2018-01-12	109.39
Bitcoin File	BIFI	Hard fork	BTC	2017-12-27	1000	2018-06-28	0.00447597
Bitcoin SegWit2X	B2X	Hard fork	BTC	2017-12-28	1	2017-12-28	392.65
Bitvote	BTV	Hard fork	BTC	2018-01-19	1	2018-03-29	0.287713
Bitcoin Interest	BCI	Hard fork	BTC	2018-01-20	1	2018-05-03	22.35
Bitcoin Atom	BCA	Hard fork	BTC	2018-01-24	1	2018-01-24	413.21
Bitcoin Cash Plus	BCP	Hard fork	BTC	2018-02-18	1	2018-02-18	6.4577
Bitcoin Private	BTCP	Airdrop	BTC, ZCL	2018-02-28	1	2018-02-28	62.81
MicroBitcoin	MCB	Hard fork	BTC	2018-05-29	10000	2018-10-03	0.00097624
Bitcoin Zero	BZX	Airdrop	BTC, LTC, HXX	2018-08-31	1	2018-10-03	0.051983
ANON	ANON	Airdrop	BTC, ZCL	2018-09-10	1	2018-09-14	1.75

Table 5 lists the Bitcoin forks (up to 2018) that granted "free coins" to bitcoin owners. The table reports the name of the cryptocurrency forked from Bitcoin, the tickers under which it is or has been quoted on exchange platforms, the type of fork (a hard fork materialises as a new branch hooked on the main blockchain; an airdrop is a separate blockchain for a cryptocurrency whose initial ownership is based on the main chain), the cryptocurrencies that have been forked or used for airdrops (in the latter case, ownership of new units of cryptocurrency could be granted to owners of more than one cryptocurrency, creating a so-called "fork-merge"), the day of the snapshot of the main chain that determines to which addresses new units of cryptocurrency have been granted (for a hard fork, this is the day of the last common parent block; for airdrop, this is the day of a snapshot block, that is, the block used as a reference to grant new units of cryptocurrency), the number of new units of cryptocurrency each bitcoin held at the time of the snapshot granted, the earliest day (at or after the snapshot date) at which a market price was available (as reported by CoinMarketCap, CoinGecko, or BitInfocharts), and the closing price in USD of the cryptocurrency for that day. Thus, the value in USD a bitcoin owner could cash in from each bitcoin held at the time of the snapshot is the ratio times this market price. Note: two cryptocurrencies granted new units of cryptocurrency per Bitcoin address (and not in proportion of the amount held): Clams has been granted to Bitcoin addresses with a balance of more than 0.001 bitcoins; Bitcore has been granted to Bitcoin addresses with a balance of 0.01 bitcoins or more. We neglect these exceptions, applying these two ratios per-bitcoin instead.