Equilibrium Bitcoin Pricing

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

July 10, 2020

Abstract

We offer an equilibrium model of cryptocurrency pricing and confront it to new data on bitcoin transactional benefits and costs. The model emphasises that the fundamental value of the cryptocurrency is the stream of net transactional benefits it will provide, which depend on its future prices. The link between future and present prices implies that returns can exhibit large volatility, unrelated to fundamentals. We construct an index measuring the ease with which bitcoins can be used to purchase goods and services, and we also measure costs incurred by bitcoin owners. Consistent with the model, estimated transactional net benefits explain a statistically significant fraction of bitcoin returns.

*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 Will Cong, Co-Pier Georg, Patrick Fève, René Garcia, Zhiguo He, Michael Kumhof, Nour Meddahi, Eric Mengus, Julien Prat, George Tauchen, Harald Uhlig, Stefan Voigt and conference and seminar participants in the 2018 Eighth BIS Research Network meeting, the 2018 Becker Friedman Institute Conference on Blockchains and Cryptocurrencies, the 2018 Ridge Forum at the Central Bank of Uruguay, the 2018 EuroFIT Conference at University College London, the 2019 World Economic Forum Davos, the 2019 2nd Toronto FinTech Conference, the 2019 1st Tokenomics Conference in Paris, the 2019 Sustainable Finance Center Conference and Financial Econometrics Conference at Toulouse School of Economics, the 2019 European Summer Symposium in Financial Markets in Gerzensee, the 2019 CEBRA Annual Meeting at Columbia University, the 2019 EFA Meeting in Lisbon, the 2020 AFA meeting in San Diego, 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 Faculty of Economics and Business, University of New South Wales, University Paris Dauphine, University of Technology Sydney and University of Vienna. Financial support from the Jean-Jacques Laffont Digital Chair, the Norwegian Finance Initiative (NFI), the Netherlands Organization for Scientific Research (NWO Vici grant), the ANR under grant ANR-17-EURE-0010 (Investissements d'Avenir program) and EconPol Europe is gratefully acknowledged.

1 Introduction

What is the fundamental value of cryptocurrencies, such as bitcoin? Does the price of bitcoin reflect fundamental values or speculation unrelated to fundamentals? And does the large volatility of cryptocurrencies imply investors are irrational? Several recent empirical papers have offered econometric tests of bubbles in the cryptocurrency market (see for instance Corbet et al., 2018, or Fantazzini et al., 2016, for a review). While these analyses use methods developed for stock markets, cryptocurrencies differ from stocks. This raises the need for a new theoretical and econometric framework, to analyse the dynamics of cryptocurrencies. The goal of the present paper is to offer such a framework and confront it to the data.

We consider overlapping generations of agents, with stochastic endowments, who can trade traditional fiat money (such as dollar) and a cryptocurrency (such as bitcoin). While both can be used to purchase consumption goods in the future, the cryptocurrency can provide transactional benefits that traditional money cannot. For example, citizens of Venezuela or Zimbabwe can use bitcoins to conduct transactions although their national currencies and banking systems are in disarray, while Chinese investors can use bitcoins to transfer funds outside China, in spite of government imposed restrictions on international transfers.[1] Along with these transactional benefits, cryptocurrencies also come with transactions costs: limited convertibility into traditional currencies, transactions costs on exchanges, lower rate of acceptance by merchants, or fees agents must pay to have their transactions mined.[2] In our analysis, investors rationally choose their demand for cryptocurrency based on their expectation of future prices and net transactional benefits.

Transactional benefits are to cryptocurrencies what dividends are to stocks. Other things equal, the larger the transactional benefits, the larger is the price investors are willing to pay for the asset. But there is a major difference. While (in perfect markets) dividends don't depend on stock prices, the transactional benefits provided by cryptocurrencies depend on their price: the transactional advantages of holding one bitcoin are much larger if a bitcoin is worth \$15,000 than if it is worth \$100. This point, which applies to all currencies, not only cryptocurrencies, was already noted in Tirole (1985, p. 1515-1516):

> "... the monetary market fundamental is not defined solely by the sequence of real interest rates. Its dividend depends on its price. [...] the market fundamental of money in general depends on the whole path of prices (to this extent money is a very special asset)."

Thus, the notion of "market fundamental" means something very different for stocks (backed by dividends) and money (backed by transactional services). In particular, the feedback loop from prices to transactional benefits naturally

[1] Although China banned bitcoin exchanges in October 2017, it is still possible for Chinese investors to trade bitcoins via bilateral, peer-to-peer interactions.

[2] Transactions fees for Bitcoin were particularly large during the last quarter of 2017. See `https://en.bitcoin.it/wiki/Transaction_fees`.

leads to equilibrium multiplicity: agents who expect future prices to be high (resp. low) anticipate high (resp. low) future transactional benefits justifying a high (resp. low) price today.

We depart from Tirole (1985) in ways we deem important for the dynamics of cryptocurrencies. First, our model features two currencies, traditional money and cryptocurrency. We thus derive a pricing equation expressing the expected return on the cryptocurrency (say bitcoin) in traditional money (say dollars), which we can confront to observed dollar returns of bitcoin. Second, in addition to transactional benefits we also consider transaction costs, reflecting frauds and hacks and the difficulty to conduct transactions in cryptocurrencies. Allowing for a rich structure of transactional benefits and costs is key to our empirical approach in which we construct measures of these fundamentals. Finally, while Tirole (1985) considers a deterministic environment, we allow endowments, net transactional benefits, and returns to be stochastic. Our econometric analysis sheds light on the relationship between these random variables.

The model delivers the following insights:

- The price of one unit of cryptocurrency at time t is equal to the expectation of its future price at time $t+1$, discounted using a standard asset pricing kernel modified to take into account transactional benefits and costs. These benefits and costs reflect the evolution of variables from the real economy affecting the usefulness of cryptocurrencies, e.g., development of e-commerce or illegal transactions.

- The dynamic structure of equilibrium gives rise to a large multiplicity of equilibria: we show in particular that when agents are risk neutral, if a price sequence forms an equilibrium, then that sequence multiplied by an extrinsic noise term, with expectation equal to one, is also an equilibrium. Such extrinsic noise on the equilibrium path implies, in line with stylised facts, large volatility for cryptocurrency prices, even at times at which the fundamentals are not very volatile.[3] This underscores that the Shiller (1981) critique does not apply to cryptocurrencies.

- When transaction costs are large, investors require large expected returns to hold the cryptocurrency. In contrast, large transactional benefits reduce equilibrium required expected returns. Thus, large observed returns on bitcoin are consistent with the prediction of our model when transactions costs are large and transaction benefits are low.

Next, we confront these predictions of the model to the data. Using the Generalised Method of Moments (GMM), we estimate the parameters of the model and test the restrictions imposed by theory on the relation between cryptocurrency returns and transaction costs and benefits. To do so, we construct a time series of bitcoin prices from July 2010 to December 2018 by compiling data from 20 major exchanges. We also construct three time series that proxy for

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

the transactional costs and benefits of using bitcoin. The first one captures the evolution of the transaction fees that bitcoin users attach to their transaction to induce miners to process them faster. For the other two, we collect information on events likely to affect the costs and benefits of transacting in bitcoin, and categorise these events into two subsamples. The first subsample captures transaction costs: 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 subsample captures 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 a means of payment. From these subsamples we construct two indexes that proxy for the transactional benefits and transaction costs associated with bitcoin at every point in time. Finally, we collect data about thefts and hacks on bitcoin to obtain a measure of the corresponding losses.

Consistent with the model, GMM estimates show a negative and significant relation between expected returns and transactional benefits and a positive and significant relation between expected returns and transactional costs. We also quantify the contribution of the different components of transactional costs and benefits to required expected returns over time. During our entire sample period, the average weekly return is 3.9% with a standard deviation of 17.3%. We estimate that the costs induced by the difficulty to trade bitcoins were large in 2010 and contributed at that time to approximately fifteen percentage points of weekly required return. This later decreased to ten percentage points as investors could more easily trade bitcoins. On the other hand, transaction fees have a negligible impact on required returns. Furthermore, transactional benefits were initially low, reducing the weekly required return by less than one percentage point. As more firms started accepting bitcoins to buy goods and services, transactional benefits became larger, inducing a reduction in the weekly required return of eight to ten percentage points since 2015. The estimation also shows that while fundamentals are significant factors, they only explain a relatively small share of return variations on bitcoin (less than 4%). Viewed through the lenses of our theoretical model, this empirical result suggests that observed bitcoin volatility in large part reflects extrinsic noise.

Related literature. Our analysis is related to the classic literature in monetary economics in which money enables agents to carry mutually beneficial trades they could not realise without money (Samuelson, 1958, Tirole, 1985 and Wallace, 1980). In a similar OLG setting, Saleh (2020) compares equilibrium prices and welfare in two protocols: proof-of-burn and proof-of-work, while Garratt and Wallace (2018) revisit the indeterminacy of exchange rates between two currencies shown in Kareken and Wallace (1981) by introducing storage costs for the traditional currency and a risk of currency crash for the cryptocurrency. In Pagnotta (2020), this crash risk is interpreted as a security breach and is endogenously decreasing in the computing power deployed by miners. This creates a feedback loop where a higher bitcoin price stimulates miners' investments, which improves security and in turn raises the bitcoin price.[4]

In a model where agents have an infinite horizon, Schilling and Uhlig (2019a) derive a version of the exchange rate indeterminacy result but also the existence of a speculative equilibrium where agents hold the cryptocurrency in anticipation of its appreciation. Schilling and Uhlig (2019b) extend this framework to asymmetric transaction costs. Benigno, Schilling and Uhlig (2019) analyse monetary policy and equilibrium relations between interest rates and exchange rates. In a search setting inspired by Lagos and Wright (2005), Fernández-Villaverde and Sanches (2019) and Hendry and Zhu (2019) study the stability and welfare implications of the private supply of money (cryptocurrency) alongside a government-backed currency. Chiu and Koeppl (2017) use a similar search model to study the optimal design of a cryptocurrency protocol. Vis-à-vis this literature, our contribution is to propose a simple model capturing the transactional costs and benefits of cryptocurrencies to generate a pricing equation and confront it to the data.

A second stream of literature proposes pricing models in which the distinctive feature of cryptocurrencies is to give access to a trading network (see Pagnotta, 2020 and Cong, Li and Wang, 2020). Sockin and Xiong (2020) highlight that the complementarity in users' decisions to adopt a cryptocurrency generates multiple equilibria. Athey et al. (2016) analyse the dynamics of cryptocurrency adoption when it serves both as means of payment and speculative instrument. Our model differs from that literature in that we don't cast exchanges of goods for cryptocurrencies in terms of networks.

On the empirical side, Makarov and Schoar (2020), Borri and Shakhnov (2019) and Hautsch, Scheuch, and Voigt (2020) document cryptocurrency mispricing and arbitrage opportunities across exchanges. Abstracting from these admittedly important short-term frictions, our work focuses on the longer term dynamics of the fundamental value of bitcoin. This relates our paper to Liu and Tsyvinski (2018), Bianchi (2018) and Bhambhwani, Delikouras and Korniotis (2019). Liu and Tsyvinski (2018) and Bianchi (2018) document that bitcoin or other cryptocurrencies do not show any exposure to common aggregate risk factors (market portfolio, macro factors). Bhambhwani, Delikouras and Korniotis (2019) perform a multi factor analysis of 38 cryptocurrencies and highlight that computing power and network size are cryptocurrency pricing factors. The main difference between that literature and our paper is that we take a structural econometric approach to confront the theory to the data. Our indexes 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 indexes 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.

[4]Relatedly, Prat and Walter (2018) analyse miners' incentives to enter and build capacity.

In the next section we present our theoretical analysis. Section 3 presents the econometric method we develop to confront the theory to the data. Section 4 describes our sample and data collection procedure. The empirical analysis is presented in Section 5. Section 6 concludes. Some proofs and discussions are relegated to the appendix.

2 Theoretical model

2.1 Assumptions

There is one consumption good and three assets: a cryptocurrency, in supply X_t at time t, a standard currency in fixed supply m, and a risk-free asset in zero net supply: what is lent by one agent is borrowed by another one.

There are investors, miners and hackers. All are competitive and take prices as given. We consider miners and hackers to introduce two important features of the cryptocurrency, the creation of new coins and the risk of hacks, but, in our model, their actions are very simple. They perform their activity and then sell their cryptocurrency holdings and consume. In contrast, we analyse the consumption and savings decisions of investors, which, combined with market clearing, pin down equilibrium pricing.

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

Similarly, at each time t, a new generation of hackers is born. Hackers born at time t try to steal some cryptocurrency. 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 time $t+1$, hackers sell their stolen coins against consumption goods, which they consume before exiting the market.

Finally, a mass one continuum of investors are born at each date. They can invest and consume at two dates, have separable utility $u(.)$ over each consumption, with $u^{'} > 0$ and $u^{''} \leq 0$, and discount factor β. At each date, their utility is defined over consumption, which reflects transactional costs and benefits of using cryptocurrencies. 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 time t, each young investor is endowed with e_t^y units of consumption good, can buy q_t units of cryptocurrency, or coins, at unit price p_t, $\hat{q}_t$ units of traditional fiat currency at unit price $\hat{p}_t$, and can save s_t. For notational simplicity, the consumption good is the numeraire (as in Garratt and Wallace, 2018). That is, p_t (resp. $\hat{p}_t$) is the number of units of consumption good that can be purchased with one unit of cryptocurrency (resp. standard currency) at date t.

When buying cryptocurrency, each investor incurs a cost $\varphi_t(q_t)p_t$ that reduces his consumption, with $\varphi' \geq 0$. The investor's budget constraint is:

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

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 time t.[5]

When old at time $t+1$, each investor gets endowment e_{t+1}^o and consumes endowment plus savings, plus proceeds from sale of currencies. For the traditional fiat 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

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

where q_t is the amount of cryptocurrency sold at $t+1$ and $\theta_{t+1} q_t p_{t+1}$ reflects transactional services/benefits generated by cryptocurrencies. Those benefits can stem from the ability to send money to another country, without using the banking system, and without being controlled by the government. Also, cryptocurrencies can enable agents to purchase enhanced goods. Since the agent uses that cryptocurrency to buy consumption at time $t+1$ the transactional benefits reflect the time $t+1$ price.

Equation (2) covers two cases: If $\theta_{t+1} \geq -1$, then old agents sell all their holdings of cryptocurrency q_t. If $\theta_{t+1} < -1$, then old agents would be better off not selling their holdings if p_{t+1} was strictly positive. In that case, equilibrium will imply $p_{t+1} = 0$ as discussed below.

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.

2.2 Equilibrium and optimality conditions

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) at each time t, $\{q_t, \hat{q}_t, s_t\}$ maximises young consumers' expected utility over periods t and $t+1$ given prices and subject to the budget constraints (1) and (2) and to consumptions c_t^y and c_{t+1}^o being positive,

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

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

From (i), a young investor at date t solves

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

where μ is the multiplier of the constraint that consumption must be positive and E_t is the expectation conditional on time t information. Assume first that this constraint does not bind. The first order optimality condition with respect to q_t, together with market clearing, yields

$$p_t = \beta E_t \left[\frac{u'(c_{t+1}^o)}{u'(c_t^y)} (1 - h_{t+1}) \frac{(1 + \theta_{t+1})}{(1 + \varphi_t'(X_t))} p_{t+1} \right]. \tag{3}$$

The first order condition with respect to s_t is

$$\beta = \frac{1}{1 + r_t} \frac{u'(c_t^y)}{E_t \left[u'(c_{t+1}^o) \right]}. \tag{4}$$

On the equilibrium path, at time t old investors cannot borrow or lend, since they won't be present in the market at time $t+1$. Hence, in equilibrium $s_t = 0$. So the interest rate must adjust so that (4) holds when evaluated at $s_t = 0$.

Denote

$$1 + \mathcal{T}_{t+1} = \frac{1 + \theta_{t+1}}{1 + \varphi_t'(X_t)}. \tag{5}$$

$\mathcal{T}_{t+1}$ 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 (4) to replace β into (3), we obtain our first proposition.

Proposition 1 *The equilibrium price of the cryptocurrency at time t is*

$$p_t = \frac{1}{1 + r_t} E_t \left(\frac{u'(c_{t+1}^o)}{E_t \left[u'(c_{t+1}^o) \right]} (1 - h_{t+1}) \left(p_{t+1} + \mathcal{T}_{t+1} p_{t+1} \right) \right). \tag{6}$$

In the appendix, we complete the proof of Proposition 1 by showing that (6) also holds when the constraint that consumption is positive binds. When consumption is zero, if p_t was strictly lower than the RHS of (6), the agent would like to borrow in order to buy more cryptocurrencies. That would contradict equilibrium in the zero-supply risk-free asset market. In other words, r_t adjusts so that (6) holds.

Equilibrium multiplicity. The multiplicative structure of the pricing equation (6), in which p_{t+1} multiplies all the other terms on the right-hand-side, implies there are multiple equilibria. For instance, as is standard in OLG models of money, there exists an equilibrium in which the cryptocurrency price is equal to zero at all dates (see for instance Kareken and Wallace, 1981 or Garratt and Wallace, 2018). The intuition is the following: if a young investor at date t anticipates that $p_{t+1} = 0$, then for any strictly positive price $p_t > 0$, he does not want to buy any strictly positive quantity q_t. Indeed, choosing $q_t > 0$ does not increase his consumption at $t+1$, and strictly reduces his consumption at t. In that case market clearing can only occur if $p_t = 0$.

Note that p_t can be strictly positive in equilibrium even if the cryptocurrency price may fall to zero in future periods, as long as the probability of this happening is strictly lower than one in any given period. Furthermore, if the price reaches 0 at some date T then (6) implies $p_{T+1} = 0$ with probability one, and by induction, the cryptocurrency price remains equal to 0 after T.

Bounded prices. There is a natural bound on equilibrium prices in our model. In equilibrium at each date t the entire supply of bitcoin is purchased by the young generation. Budget constraint and market clearing therefore imply that

$$e_t^y \geq (X_t + \varphi_t(X_t))p_t. \tag{7}$$

If p_t was higher than $\frac{e_t^y}{X_t+\varphi_t(X_t)}$, young investors could not buy the bitcoin holdings of old investors, miners and hackers, which would contradict market clearing.

Fundamental value, price and transactional benefit. Equation (6) states that the price of the cryptocurrency at time 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 time $t+1$ and its net transactional benefit. This pricing equation is similar to that which would obtain for other assets, e.g., stocks, except that, for stocks, the second term would not be there, and the third term would be different.

In (6) the net transactional benefit (in the third term) is equal to a scalar multiplied by the price of the cryptocurrency. Other things equal, the larger the cryptocurrency price, the larger its net transactional benefit. This differs from stocks traded in a perfect market in which the stock price at t reflects the expectation of the price at $t+1$ plus profits or dividends at $t+1$, which do not depend on the $t+1$ stock price. Thus, while, for stocks, dividends cause fundamental value and therefore prices, in contrast, for currencies, prices cause transactional benefits and therefore fundamental value.

Note that (6) implies that the price at time $t+1$ verifies

$$p_{t+1} = E_{t+1}\left[\frac{1-h_{t+2}}{1+r_{t+1}}\frac{u'(c^o_{t+2})}{E_{t+1}\left[u'(c^o_{t+2})\right]}(p_{t+2} + \mathcal{T}_{t+2}p_{t+2})\right]. \tag{8}$$

Substituting (8) into (6) yields

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

Iterating we obtain our next proposition.

Proposition 2 *The equilibrium price of the cryptocurrency at time t is equal to the present value of the risk-adjusted expectation of the stream of net transactional benefits until $t+K$ plus the price at time $t+K$, net of losses due to hacking*

$$p_t = E_t\left(\sum_{k=1}^{K}\left(\prod_{j=1}^{k}\frac{1-h_{t+j}}{1+r_{t+j-1}}\frac{u'(c^o_{t+j})}{E_t\left[u'(c^o_{t+j})\right]}\mathcal{T}_{t+k}p_{t+k}\right)+\left(\prod_{j=1}^{K}\frac{1-h_{t+j}}{1+r_{t+j-1}}\frac{u'(c^o_{t+j})}{E_t\left[u'(c^o_{t+j})\right]}\right)p_{t+K}\right), \tag{9}$$

or equivalently

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

The first term on the right-hand-side of (9) is the stream of net transactional benefits, corresponding to the fundamental value of the currency. When the price of the currency remains bounded, the second term on the right-hand-side of (9) goes to 0 as K goes to infinity. In that case, the current price is just the expectation of the infinite stream of net transactional benefits.

Equation (9) illustrates how the cryptocurrency price today, p_t, depends on the expectation of net transactional benefits that can be arbitrarily far in the future. For instance, a high price today is not inconsistent with a low expected net transactional benefit next period, if one expects the transactional benefit or the price to be high in the future.

Equation (10) provides a lower bound for net transactional benefits compatible with strictly positive prices. To see this, suppose that the net transactional benefit $\mathcal{T}_{t+k}$ falls below -1 with probability 1 in some period $t+k$ arbitrarily far in the future. From the definition of $\mathcal{T}$ in (5), this is equivalent to the transactional benefit θ_{t+k} being also strictly lower than -1. Then p_{t+k} must be 0 since there is no supply of cryptocurrency from old agents at any strictly positive price, and the only price p_t that can satisfy (10) is 0. Alternatively, suppose that the probability the transactional benefit falls below -1 is strictly lower than 1 in every period. In that case, p_t may still be positive, but if $\mathcal{T}_{t+k} < -1$ realises at some period $t+k$, we must have $p_{t+k} = 0$ for markets to clear. It follows that the cryptocurrency price remains at 0 in every period after $t+k$.

3 Econometric model and implications

The equilibrium price formulae presented above involve pricing kernels, which are difficult to estimate. To abstract from this difficulty, in our econometric framework we make the following assumption:

Assumption A1 *Investors are risk neutral.*

In practice, A1 should be innocuous because, during our sample period, the capitalisation of bitcoin has only been a small fraction of aggregate wealth, so the risk of changes in marginal consumption induced by bitcoin returns cannot have been very large in the aggregate. Indeed, Liu and Tsyvinski (2018) 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.

3.1 Exogenous volatility

Under A1, the equilibrium pricing relation (6) simplifies to

$$p_t = \frac{1}{1+r_t} E_t \left(\left(1 - h_{t+1}\right) \left(1 + \mathcal{T}_{t+1}\right) p_{t+1} \right). \tag{11}$$

That is

$$p_t = E_t \left[\left(\prod_{k=1}^{K} (1 - h_{t+k}) \frac{(1 + \mathcal{T}_{t+k})}{1 + r_{t+k-1}} \right) p_{t+K} \right]. \tag{12}$$

Relying on (12), we obtain the next proposition.

Proposition 3 *Consider a sequence of prices $\{p_t\}_{t=1,..,\infty}$ satisfying (12). If agents' consumption is strictly positive on the equilibrium path, there exists a constant $\lambda > 0$ and a sequence of random variables $\tilde{u}_\tau$, $E_t(\tilde{u}_\tau) = 1$, such that the new price sequence*

$$\{\bar{p}_t\}_{t=1,..,\infty} = \left\{ \lambda \left(\prod_{\tau=1}^{t} u_\tau \right) p_t \right\}_{t=1,..,\infty}, \tag{13}$$

also satisfies (12), and therefore is also an equilibrium.

The proposition states that the equilibrium pricing equation (12) is consistent with arbitrary randomness in prices unrelated to the fundamental variables $(\theta_t, h_t, \varphi_t)$. This reflects the multiplicative structure of the equilibrium pricing of the currency. This implies that, in contrast with the argument invoked by Shiller (1981) for stocks (whose prices are more volatile than would be warranted by the volatility of the dividends which underly their fundamental value), larger volatility of bitcoin prices than of variables affecting bitcoin's fundamental value (i.e., net transactional benefits) is not sufficient to reject rational expectations equilibrium.[6] The variance of $\tilde{u}_\tau$ cannot be infinite, however, because prices must remain within bounds, as noted in the previous section (see Equation 7).

[6] Campbell and Shiller (1988) emphasise that stock price changes can also stem from changes in discount rates, reflecting changes in risk premia. This differs from the economic mechanism at play in Proposition 3, in which agents are risk neutral.

3.2 Moment conditions

Proceeding as for (11), one obtains the price of fiat currency,[7]

$$\hat{p}_t = \frac{1}{1+r_t} E_t \left(\hat{p}_{t+1} \right). \tag{14}$$

In practice, since the first public quotation of bitcoin prices, in 2010, inflation in the US has been low and not very volatile. In line with this observation, and in order to simplify the econometric analysis, we hereafter maintain the following assumption:

Assumption A2 *Inflation in the standard currency between time t and time $t+1$ is known at time t.*

Under A2, in (14) $\hat{p}_{t+1}$ is in the information set used to take the expectation. Hence (14) simplifies to

$$\hat{p}_t = \frac{\hat{p}_{t+1}}{1+r_t}, \tag{15}$$

which reflects that, in our simple model, the short-term inflation rate is one to one with the short-term interest rate.[8]

Dividing (11) by (15), the price of the cryptocurrency relative to the traditional fiat currency, $\frac{p_t}{\hat{p}_t}$, (e.g., the price of bitcoin in dollars) writes as:

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

which simplifies to

$$\frac{p_t}{\hat{p}_t} = E_t \left[\left(1 - h_{t+1}\right) \left(1 + \mathcal{T}_{t+1}\right) \frac{p_{t+1}}{\hat{p}_{t+1}} \right]. \tag{16}$$

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

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

Substituting in (16) we obtain our next proposition.

Proposition 4 *Under A1 and A2, the rate of return on the cryptocurrency price expressed in traditional fiat currency (ρ_{t+1}) is such that*

$$E_t \left[\left(1 - h_{t+1}\right) \frac{1+\theta_{t+1}}{1+\varphi_t'(X_t)} \left(1 + \rho_{t+1}\right) \right] - 1 = 0. \tag{17}$$

[7] As for bitcoin, there exists an equilibrium such that the price of the fiat currency is zero at all dates. Obstfeld and Rogoff (1983) show that such equilibria can be ruled out if the central bank commits to an arbitrarily small redemption value for money (for an alternative reason based on government's fiscal power, see Gaballo and Mengus, 2018). In line with this idea, we focus on equilibria in which the equilibrium price of central bank currency is strictly positive.

[8] The inflation rate is i_{t+1} such that: $\hat{p}_t/\hat{p}_{t+1} = 1 + i_{t+1}$ which is equal to $1/(1 + r_t.)$

Equation (17) 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), or using it to invest in dollars. Equation (17) yields the moment conditions we use in our econometric analysis.

To see the intuition more clearly, note that a first-order Taylor expansion of (17), for ρ_{t+1}, h_{t+1}, $\varphi_t^{'}$ and θ_{t+1} close to 0, yields

$$E_t\left[\rho_{t+1}\right] \approx \varphi_t'(X_t) + E_t(h_{t+1}) - E_t(\theta_{t+1}). \tag{18}$$

That is, the expected return on the cryptocurrency must be (approximately) equal to the marginal transaction cost ($\varphi_t'(X_t)$), plus the expected cost of hacks ($E_t(h_{t+1})$), minus the expected transactional benefits ($E_t(\theta_{t+1})$).

4 Data

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.[9] Pooling all transaction prices in each currency, we split each UTC day in 5-minute intervals. 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) and compute an unweighted average daily price. This time series is illustrated in Figure 1.

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

[9]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.

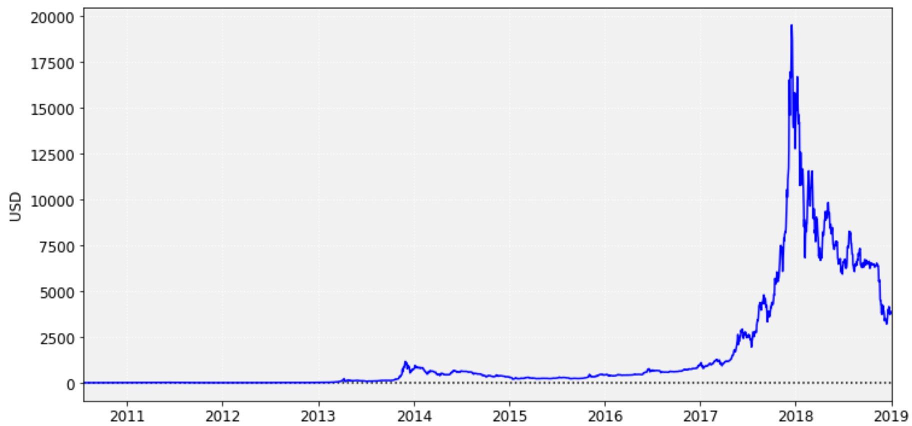

Figure 1: Bitcoin price, in USD

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.[10] From that value, we further exclude amounts that are likely to result from "self churn" behaviour, that is, transfers among adresses belonging to the same participant.[11] The time series of transaction volume is illustrated in Figure 2.[12]

The time series of miners' fees (in percent of transaction volume) is depicted in Figure 3. 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,

[10]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.

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

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

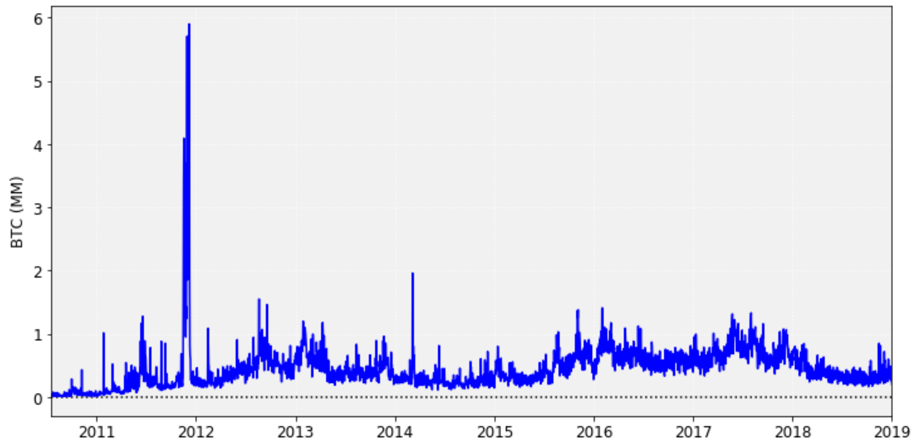

Figure 2: Estimated transaction volume, in millions of BTC

Leshno and Moalleni, 2019, 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.[13] We collected the amounts of the losses and the times at which they were 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 4. The corresponding events are listed in Table 3 in Appendix 3. 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.

As explained below, we constructed two indexes 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 4 in

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

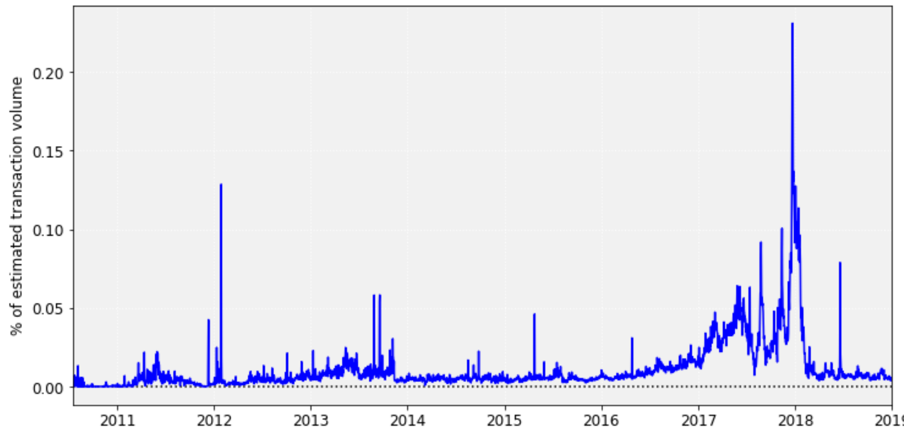

Figure 3: Miners' fees, in percent of estimated transaction volume

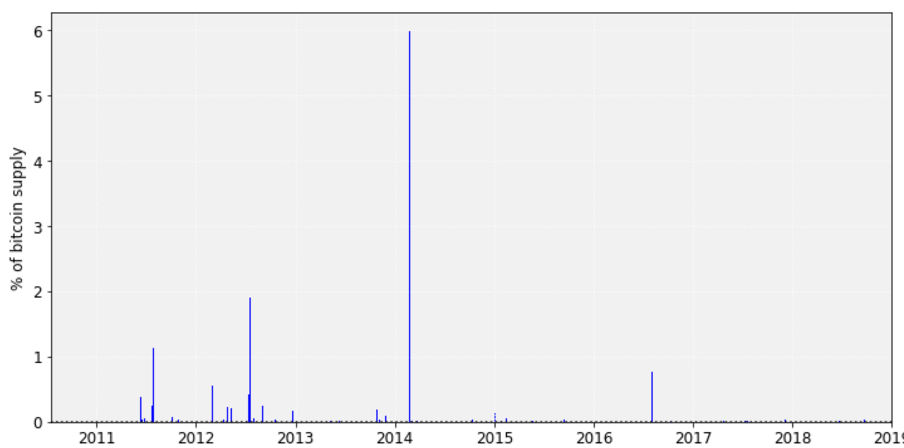

Figure 4: Hacks, thefts and other losses of bitcoins, in percent of bitcoin supply

Appendix 3). We considered three categories of events. The first category relates to exchange platforms.[14] 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.[15] 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 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.[16] 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 5 in Appendix 3. 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 indexes is illustrated in Figure 5. 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

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

[15] 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/`).

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

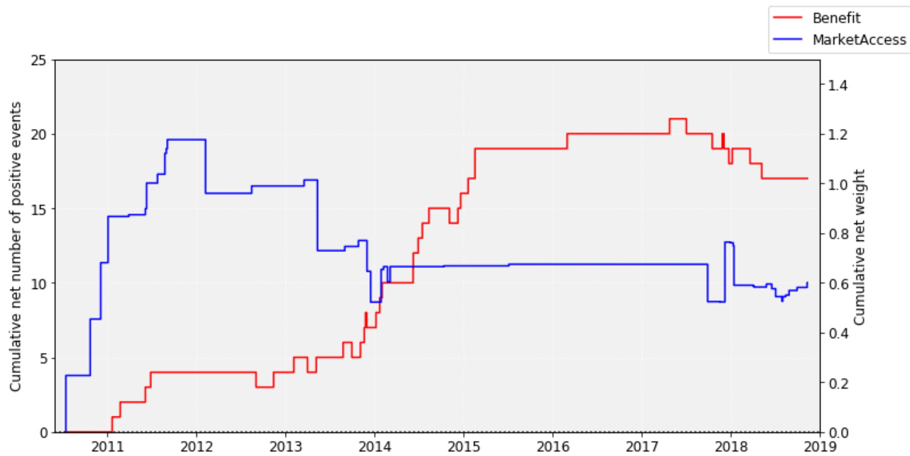

Figure 5: *MarketAccess* and *Benefit* indexes

stopped accepting payments in bitcoins.

5 Estimation and results

This section first describes how the General Method of Moments (GMM) is used to estimate the equilibrium bitcoin pricing equation. It then presents results starting with ordinary least squares (OLS) estimation of a *linearised* version of the pricing equation.[17] The OLS parameter estimates are then converted into starting values for the GMM optimisation. The section closes with presenting the GMM results and discussing a couple of issues that merit attention.

5.1 Estimation methodology

We start by discussing how the various components of the pricing equation (17) are measured. The bitcoin price p_t and the fraction of bitcoins hacked or lost h_t are directly observed as presented in Section 4. The transactional benefit and cost however need proxies. The transactional benefit θ_{t+1} is proxied by

$$\theta_{t+1} = \alpha_0 + \alpha_1 Benefit_{t+1}, \tag{19}$$

where α_0 and α_1 are parameters to be estimated, and $Benefit_{t+1}$ is the index described in the previous section. The transactional cost φ'_t is proxied by

$$\varphi'_t = \beta_0 + \beta_1 CostMiningFee_{\mathrm{t}} + \beta_2 CostMarketAccess_{\mathrm{t}}, \tag{20}$$

[17] Useful references on the use of GMM to estimate pricing equations are Hansen (1982), Hansen and Singleton (1982), and Cochrane (2005).

where β_0, β_1, and β_2 are estimated and $CostMarketAccess_t$ measures the cost of accessing bitcoin markets:

$$CostMarketAccess_{\mathrm{t}} = \frac{1}{1 + MarketAccess_{\mathrm{t}}}. \tag{21}$$

Note that this conversion purposefully lets the cost tend to zero when *MarketAccess* tends to infinity.

The α and β parameters are estimated as follows. Define the residual e_{t+1} as

$$e_{t+1} = D_{t+1}\,(1 - h_{t+1})\,(1 + \rho_{t+1}) - 1, \tag{22}$$

where the deflator D_{t+1} is defined as

$$D_{t+1} = \frac{1 + \alpha_0 + \alpha_1 Benefit_{t+1}}{1 + \beta_0 + \beta_1 CostMiningFee_t + \beta_2 CostMarketAccess_t}. \tag{23}$$

The equilibrium pricing equation (17) implies that $E_t(e_{t+1}) = 0$ where the subscript on E denotes that the expectation is conditional on all information available at t. Invoking the law of iterated expectations this implies that for any random variable v_t with an outcome that is observable at or before time t, the following equation holds:

$$E\,(v_t e_{t+1}) = 0. \tag{24}$$

Such variable v_t is referred to as an instrument. Equation (24) is used to estimate the model parameters: $\{\alpha_0, \alpha_1, \beta_0, \beta_1, \beta_2\}$. A detailed description of the estimation procedure is in Appendix 6 (see page 29).

We picked the following instruments:

- All model variables evaluated at time t.
- The exponentially weighted moving average of bitcoin return with a half-life of one year.
- The exponentially weighted moving average of the number of bitcoins hacked, again with a half-life of one year.

The two variables that were added to the core set of model variables were picked for their relatively high correlation with future bitcoin return (to avoid weak-instrument bias). More specifically, the correlation of their value at time t with bitcoin return at $t + 1$ is 0.09 and -0.14, respectively.

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 estimation contains 432 observations and runs from the week of September 26, 2010, until the week of December 23, 2018.[18] Several forks

[18]Note that this weekly sample starts somewhat later than the daily sample described in Section 4. The reason is that we use lags in the estimation and thus can only retain weeks for which the lagged variables are also observed.

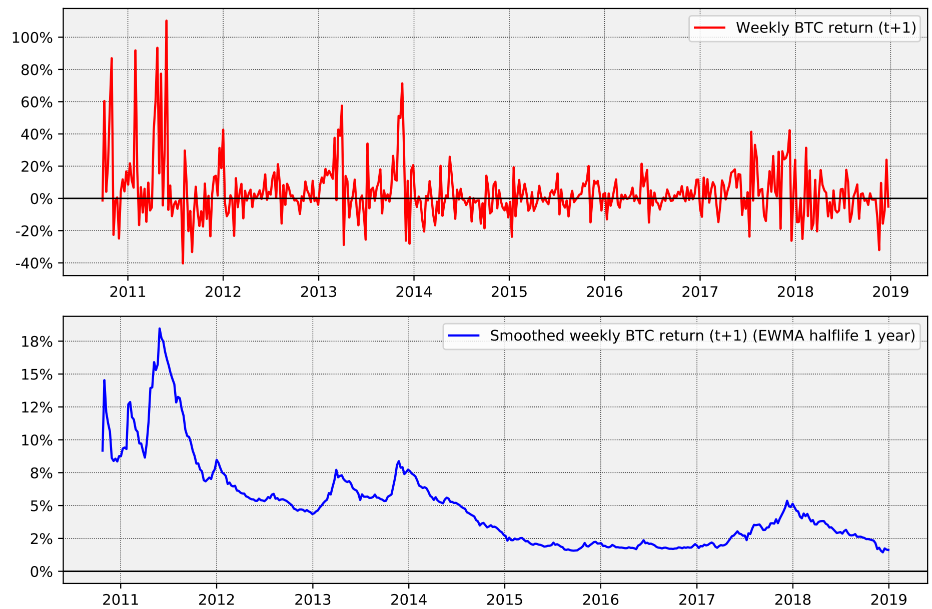

Figure 6: Bitcoin price dataThis figure plots weekly bitcoin returns expressed in USD. The top graph plots raw returns. The bottom graph smooths these returns by plotting an exponentially weighted moving average of these returns with a half-life of one year.

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 6 in Appendix 3 presents the forks considered and the value of the new currencies.

The top panel of Figure 6 plots the raw weekly bitcoin return series in USD, net of hacked coins. This is the series for which the equilibrium pricing equation (17) 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 estimated, overlaying it with the model-implied required return to verify model fit.

5.2 Results

OLS results. Table 1 Panel (a) presents the results of OLS estimation of the linearised model in (18). Model (1) only features an intercept, which picks

Table 1: OLS estimates of the linearised bitcoin pricing model

This table presents OLS estimates of a linearised version of the equilibrium bitcoin pricing equation. The dependent variable is net Bitcoin return (i.e., net of fraction of hacked coins). Panel (a) presents the parameter estimates for the Bitcoin pricing equation and Panel (b) does the same except that *all* regressors are observed at time t. t-values are in parentheses and statistical significance is indicated by one, two, or three stars corresponding to the 10%, 5%, or 1% level, respectively.

Variable	Model		
	(1)	(2)	(3)
Panel (a): OLS estimates linearised model			
Intercept	0.039^{***} (4.68)	-0.16 (-1.57)	-0.15 (-1.46)
$Benefit_{t+1}$		-0.0061^{***} (-4.35)	-0.0054^{***} (-4.13)
$CostMiningFee_t$		0.78 (1.37)	
$CostMarketAccess_t$		0.52^{**} (2.44)	0.50^{**} (2.33)
R^2	0.00	0.04	0.04
#Observations	432	432	432
Panel (b): OLS estimates linearised model, all regressors observed at time t			
Intercept	0.039^{***} (4.68)	-0.16 (-1.57)	-0.15 (-1.45)
$Benefit_t$		-0.0061^{***} (-4.35)	-0.0054^{***} (-4.13)
$CostMiningFee_t$		0.79 (1.38)	
$CostMarketAccess_t$		0.52^{**} (2.43)	0.49^{**} (2.32)
R^2	0.00	0.04	0.04
#Observations	432	432	432

up the average weekly bitcoin return of 3.9%. Model (2) is the full-fledged model and its estimation shows that only $\mathit{Benefit}_{t+1}$ and $\mathit{CostMarketAccess}_t$ are statistically significant. Importantly, the coefficients carry the right sign: a negative one for the benefit variable and a positive one for the cost variable. $\mathit{CostMiningFee}_t$ is insignificant and is therefore removed in Model (3) where the other two explanatory variables remain significant with the same sign. To check robustness, Panel (b) presents the estimation results when all regressors are observed at time t. The results are very similar to those presented in Panel (a). With intent, we keep the discussion of the OLS results brief, as this specification only serves to show that GMM results are robust and to set reasonable starting values for the GMM numerical optimisation.

GMM results. Before implementing GMM, one identification issue needs to be resolved. Equations (22) and (23) suggest that it will be hard to separately identify the two coefficients associated with the two intercepts terms: α_0 and β_0. To grasp the intuition consider the simple case in which the benefits and costs of holding bitcoins are constant through time: $\alpha_1 = \beta_1 = \beta_2 = 0$. In this case, (22) simplifies to (using (23)):

$$e_{t+1} = (1 - h_{t+1}) \frac{1 + \alpha_0}{1 + \beta_0} (1 + \rho_{t+1}) - 1. \tag{25}$$

Clearly, only the ratio $(1+\alpha_0)/(1+\beta_0)$ is identified, not the coefficients α_0 and β_0 separately. In other words, any value of this ratio can be generated by an infinite number of (α_0, β_0) pairs. If however α_1, β_1, and β_2 are not zero, it is not strictly the case that α_0 and β_0 are unidentified.[19] But, trying to estimate both of them generates numerical instability and large standard errors. To avoid these problems we set α_0 to zero and, when interpreting the estimate for β_0, we will bear in mind that it reflects the intercepts of both the costs and the benefits of holding bitcoins. It turns out that the issue becomes moot in our application as the estimate of β_0 is not statistically different from zero.

Table 2 presents the GMM estimation results. Model (1) is the full-fledged model without any parameter constraint (other than $\alpha_0 = 0$). The intercept is insignificant. The other parameters carry the predicted sign and all are significant except for $\mathit{CostMiningFee}_t$. In line with our model, the bitcoin required return significantly decreases in the proxy for transactional benefits ($\hat{\alpha}_1 > 0$ where hats denote parameter estimates). The required return significantly increases in the cost of market access ($\hat{\beta}_2 > 0$).

Model (2) and (3) drop the insignificant variables in Model (1) starting with the intercept as it is the least significant one. As $\mathit{CostMiningFee}_t$ remains insignificant in Model (2) it is also dropped from the model. Model (3) features only $\mathit{Benefit}_{t+1}$ and $\mathit{CostMarketAccess}_t$ which are both highly significant. Note that significance is higher than what it was for OLS which suggests that honoring the model-implied non-linearity is important.

[19]Strictly speaking, the intercepts become mathematically identified but only through second-order terms. The first-order approximation of the model as derived in (18) shows that they are not identified in a first-order approximation.

Table 2: GMM estimates of model parameters
This table presents GMM estimates of the model parameters. t-values are in parentheses and statistical significance is indicated by one, two, or three stars corresponding to the 10%, 5%, or 1% level, respectively.

Variable	Parameter	Model (1)	Model (2)	Model (3)
$Benefit_{t+1}$	α_1	0.0064^{***} (3.57)	0.0055^{***} (4.15)	0.0051^{***} (3.94)
$Intercept$	β_0	-0.17 (-1.27)		
$CostMiningFee_t$	β_1	0.84 (1.36)	0.75 (1.24)	
$CostMarketAccess_t$	β_2	0.56^{*} (1.85)	0.20^{***} (4.97)	0.20^{***} (4.96)
#Observations		432	432	432

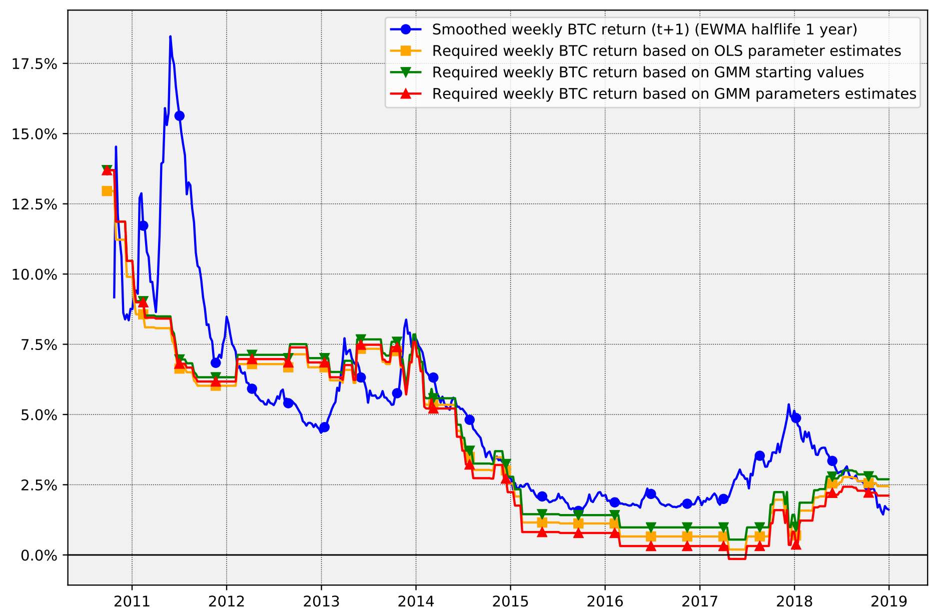

Figure 7: Illustration of model fit. This graph plots the smoothed realised net return on bitcoin overlaid with model-implied required returns. The models include: the linearised model estimated with OLS, the baseline model evaluated at GMM starting values and the model evaluated at GMM estimates.

A natural way to judge model fit is to plot the smoothed realised bitcoin return of Figure 6 and overlay it with the model-predicted required return implied by (17). We assume that $Benefit_{t+1}$ is known at time t (similar to what we did for inflation in A2). This is a rather innocuous assumption given that $Benefit_t$ is a rather persistent series (see Figure 5). Assuming further that h_{t+1} is independent of ρ_{t+1} with constant mean $\bar{h}$, straightforward manipulation of (17) yields the required bitcoin expected return:

$$E_t\left(\rho_{t+1}\right) = \frac{1 + \hat{\beta}_0 + \hat{\beta}_2 \, CostMarketAccess_{\mathrm{t}}}{\left(1 - \bar{h}\right)\left(1 + \hat{\alpha}_1 Benefit_{\mathrm{t+1}}\right)} - 1. \tag{26}$$

Figure 7 plots smoothed realised returns overlaid with required returns based on GMM estimates. For completeness it also features required returns based on the linearised model that was estimated with OLS as well as required returns based on GMM starting values (calibrated from these OLS estimates). All required-return series seem to track the time-varying mean of the realised return series rather well, which suggests that the model fits the data reasonably well.

Economic significance. 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 (18) allows us to do so.

Figure 8 illustrates the decomposition of the model-implied required return. The top graph depicts the total required return which is the sum of the three components that follow in the three graphs below it. The figure leads to the following observations. First, the model-implied (weekly) required return on bitcoin hovers between 0% and 15%. Second, the contribution of hack risk is relatively small, as it amounts to 0.04%. Third, the benefit component starts around 0% and steadily grows in size to -10% and levels off somewhat in magnitude to end around -8%. This demonstrates that, with transactional opportunities growing through time, the required return on bitcoin becomes substantially lower (i.e., up to 10 percentage points per week lower). Finally, the difficulty to access the bitcoin market adds almost 15% to the required return initially, but within a year it drops to slightly less than 10% weekly and stays at this level throughout. Overall, the decomposition illustrates that time variation in the required return on bitcoin is economically significant, it is high initially due to the high cost of market access but decreases through time primarily due to a gradual increase in transactional benefit.

Finally, how much of the time variation in bitcoin return can be attributed to a changing model-implied required return? Let us compute an R^2. The standard deviation of the model-implied required return is 3.3%. For *realised* returns it is 17.3%. The R^2 therefore is $0.033^2/0.173^2 = 3.6\%$. Thus, changes in fundamental variables explain only a small fraction of the variation in bitcoin returns.

To interpret that result it is useful to bear in mind that, in our theoretical model, return volatility can include extrinsic noise in addition to changes in fundamental variables, as stated in Proposition 3. Thus, in the framework of

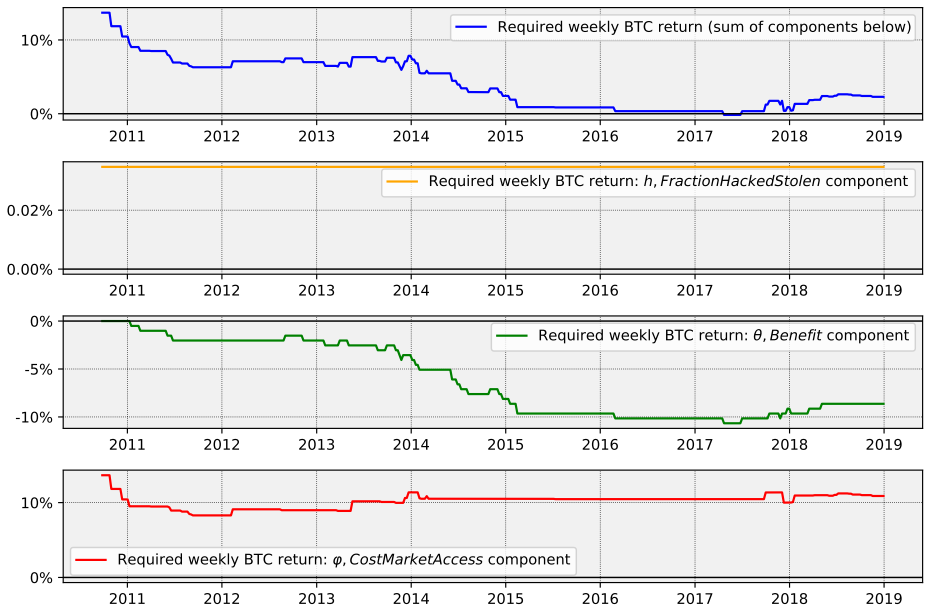

Figure 8: Bitcoin required return. This figure plots the required bitcoin return and a decomposition of this return across all model variables that contribute to it. The decomposition is based on a first-order approximation of the equilibrium pricing model. The top graph plots the total required return and the three graphs below it decompose it into three components. The decomposition is based on Model (3) in Table 2.

our model, our empirical results suggest a decomposition of the total variance of bitcoin returns: 3.6% stem from changes in fundamentals, while the remaining 96.4% reflect extrinsic noise.

Discussion. Extrinsic noise as in Proposition 3, however, cannot entirely rationalise high-frequency bitcoin dynamics. In the model, innovations in the extrinsic noise at time $t+1$ cannot be predicted based on what is known at time t. Correspondingly, the residuals (22) cannot be predicted using time t information. This does not hold out in the data as residuals from our estimation are positively autocorrelated. This suggests the presence of high-frequency frictions that our simple perfect-markets model does not account for. One candidate friction is slow price discovery due to imperfect arbitrage. Makarov and Schoar (2020) show that restrictions to capital flows across countries can delay price adjustments. Hautsch, Scheuch, and Voigt (2020) show that slow and uncertain settlement also impedes arbitrage.

Finally, one might be concerned about stationarity, given that the bitcoin price seems to behave like a random walk. However, the moment condition (17) used in the GMM estimation is expressed in terms of bitcoin returns, not prices. A Dickey-Fuller test based on raw bitcoin returns rejects the null hypothesis of non-stationarity at a significance level of 1%.

6 Conclusion

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

We then confront the equilibrium pricing equation to 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, i.e. its transaction costs and benefits. We show that these fundamentals are significant determinants of bitcoin returns, and we provide quantitative measures of their relative importance over time. We also find that a large part of the variation in prices is not explained by our proxies, which can reflect extrinsic noise or other frictions.

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 (6) 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

$$-u'(c_t^y) p_t + \beta \mathbb{E}_t \left[u'(c_{t+1}^o)(1 - h_{t+1}) \frac{(1 + \theta_{t+1})}{1 + \varphi'(q_t)} p_{t+1} \right] = \mu p_t \tag{27}$$

$$-u'(c_t^y) + \beta(1 + r_t) \mathbb{E}_t \left[u'(c_{t+1}^o) \right] = \mu \tag{28}$$

$$-u'(c_t^y) \hat{p}_t + \beta \mathbb{E}_t \left[u'(c_{t+1}^o) \hat{p}_{t+1} \right] = \mu \hat{p}_t \tag{29}$$

Suppose $\mu > 0$, i.e., the consumption non-negativity constraint binds. Then combining (27) and (28) yields the cryptocurrency pricing equation (6) in Proposition 1, which simplifies to (11) when investors are risk-neutral.

Similarly, combining (28) and (29) yields the fiat currency pricing equation:

$$\hat{p}_t = \frac{1}{1 + r_t} \mathbb{E}_t \left[\frac{u'(c_{t+1}^o)}{\mathbb{E}_t [u'(c_{t+1}^o)]} \hat{p}_{t+1} \right]$$

which simplifies to (14) when agents are risk-neutral. All the other derivations in the main text follow from these results. QED

Proof of Proposition 3:

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

by (12). Thus, because $E_t(u_\tau) = 1$, $\forall \tau > t$,

$$\begin{aligned}
\bar{p}_t &= \lambda \left(\prod_{\tau=1}^{t} u_\tau \right) E_t \left[\left(\prod_{k=1}^{K} (1 - h_{t+k}) \frac{(1 + \mathcal{T}_{t+k})}{1 + r_{t+k-1}} \right) \left(\prod_{\tau=t+1}^{t+K} \tilde{u}_\tau \right) p_{t+K} \right] \\
&= E_t \left[\left(\prod_{k=1}^{K} (1 - h_{t+k}) \frac{(1 + \mathcal{T}_{t+k})}{1 + r_{t+k-1}} \right) \lambda \left(\prod_{\tau=1}^{t} u_\tau \right) \left(\prod_{\tau=t+1}^{t+K} \tilde{u}_\tau \right) p_{t+K} \right] \\
&= E_t \left[\left(\prod_{k=1}^{K} (1 - h_{t+k}) \frac{(1 + \mathcal{T}_{t+k})}{1 + r_{t+k-1}} \right) \bar{p}_{t+K} \right],
\end{aligned}$$

where the last equality stems from the definition of $\bar{p}_{t+K}$. This shows that each price $\bar{p}_t$ verifies (12). $\{\bar{p}_t\}$ is therefore an equilibrium price sequence as long as $\bar{p}_t \leq \frac{e_t^y}{X_t + \varphi_t(X_t)}$. QED

Appendix 2: Details of the GMM estimation

We use standard two-step GMM to estimate the model. The GMM penalty function that was minimised with respect to the model parameters is:

$$P = m'Wm \in \mathbb{R}, \tag{30}$$

where m is a vector that collects the inner products of the model's residuals ($e \in \mathbb{R}^{T-1}$) and the n instrumental variables that appear as columns in $V \in \mathbb{R}^{(T-1)\times n}$, and $W \in \mathbb{R}^{n\times n}$ is the standard weighting matrix. Formally, m can be written as:[20]

$$m = V'e \in \mathbb{R}^{n\times 1} \tag{31}$$

$$\text{where} \begin{cases} e = \begin{pmatrix} e_2 & \cdots & e_{t+1} & \cdots & e_T \end{pmatrix}', \\ v = \begin{pmatrix} v_1 & \cdots & v_t & \cdots & v_{T-1} \end{pmatrix}' \in \mathbb{R}^{(T-1)\times 1}. \end{cases} \tag{32}$$

In the first step of the estimation the weighting matrix W is taken to be the identity matrix.[21] The parameters estimated by minimising P in this first step are then used to compute the moment covariance matrix which serves as W in the second step. The parameter estimates resulting from this second step are the final estimates.

Statistical inference follows standard procedure. Let $G \in \mathbb{R}^{n\times n}$ be the gradient of the n moments (i.e., the n elements of m) used in the GMM penalty function in (30), with respect to the deep parameters. The covariance matrix of the estimators is:

$$\left(G' \left(\frac{1}{T} M'M \right)^{-1} G \right)^{-1}, \tag{33}$$

where $M \in \mathbb{R}^{(T-1)\times n}$ stacks the columns associated with the empirical moments. The first column, for example, is:

$$e \circ v_1 \in \mathbb{R}^{(T-1)\times 1}, \tag{34}$$

where $\circ$ is the Hadamard product (i.e., element-wise multiplication) and v_1 is the first column of V.

Numerical issues. To come up with sensible starting values in the numerical optimization for the GMM estimation, we take the following approach:

First, we Taylor expand (22) around the mean explanatory variables to convert the OLS estimates of Table 1 to reasonable starting values for $\{\alpha_i, \beta_j\}$ of (23). Define the net bitcoin return as:

$$r_t = (1 - h_t)(1 + \rho_t) - 1. \tag{35}$$

[20]Note that the length of the time series is $T - 1$ as opposed to T as next week's residual e_{t+1} is multiplied by the instrumental variables realised/known at time t (v_t).

[21]All instrumental variables are standardised to ensure equal weighting in the first stage of GMM. The only exception is the intercept variable as standardisation is not meaningful for a variable that is constant.

Then, assuming x_{t+1} is known at time t and, for simplification, assume x_{t+1} and y_t are univariate,

$$\mathrm{E}\left(\left(1+r_{t+1}\right)D_{t+1}\right)=1 \Leftrightarrow \mathrm{E}\left(r_{t+1}\right)=\frac{1}{D_{t+1}}-1=\frac{1+\beta_0+\beta_1 y_t}{1+\alpha_1 x_{t+1}}-1. \tag{36}$$

Then Taylor expanding (36) around the mean of x_{t+1} and y_t denoted $\bar{x}$ and $\bar{y}$ respectively, one gets:

$$\begin{aligned}\mathrm{E}\left(r_t\right) \approx & \underbrace{\frac{1+\beta_0+\beta_1\bar{y}}{1+\alpha_1\bar{x}}+\alpha_1\frac{1+\beta_0+\beta_1\bar{y}}{\left(1+\alpha_1\bar{x}\right)^2}\bar{x}-\beta_1\frac{1}{1+\alpha_1\bar{x}}\bar{y}-1}_{b_0}+ \\ & \underbrace{-\alpha_1\frac{1+\beta_0+\beta_1\bar{y}}{\left(1+\alpha_1\bar{x}\right)^2}}_{b_1}x_{t+1}+\underbrace{\beta_1\frac{1}{1+\alpha_1\bar{x}}}_{b_2}y_t,\end{aligned} \tag{37}$$

where $\{b_0, b_1, b_2\}$ are the regression coefficients of the OLS regression

$$r_{t+1}=b_0+b_1 x_{t+1}+b_2 y_t. \tag{38}$$

Then taking the simple average on both sides of (38) yields:

$$\frac{1+\beta_0+\beta_1\bar{y}}{1+\alpha_1\bar{x}}=b_0+b_1\bar{x}+b_2\bar{y}+1. \tag{39}$$

Therefore using the definition of b_1 in (37) into (39) yields:

$$b_1=\left(b_0+b_1\bar{x}+b_2\bar{y}+1\right)\frac{-\alpha_1}{1+\alpha_1\bar{x}}. \tag{40}$$

The estimate of α_1, denoted by adding a hat, becomes

$$\hat{\alpha}_1=\frac{-b_1}{1+b_0+2b_1\bar{x}+b_2\bar{y}}. \tag{41}$$

What remains is to solve for both betas. Let us first consider the definition of b_1 from (37) with α_1 replaced by its estimate $\hat{\alpha}_1$ from (41):

$$b_2=\beta_1\frac{1}{1+\hat{\alpha}_1\bar{x}} \tag{42}$$

which yields

$$\hat{\beta}_1=b_2\left(1+\hat{\alpha}_1\bar{x}\right). \tag{43}$$

Finally plug the estimates $\hat{\alpha}_1$ from (41) and $\hat{\beta}_1$ from (43) into b_0 as defined in (37) to get:

$$b_0=\frac{1+\beta_0+\hat{\beta}_1\bar{y}}{1+\hat{\alpha}_1\bar{x}}+\hat{\alpha}_1\frac{1+\beta_0+\hat{\beta}_1\bar{y}}{\left(1+\hat{\alpha}_1\bar{x}\right)^2}\bar{x}-\hat{\beta}_1\frac{1}{1+\hat{\alpha}_1\bar{x}}\bar{y}-1 \tag{44}$$

which yields

$$b_0 - \frac{1}{1+\hat{\alpha}_1\bar{x}} - \frac{\hat{\alpha}_1\bar{x}(1+\hat{\beta}_1\bar{y})}{(1+\hat{\alpha}_1\bar{x})^2} + 1 = \frac{1}{1+\hat{\alpha}_1\bar{x}}\left(1 + \frac{\hat{\alpha}_1\bar{x}}{1+\hat{\alpha}_1\bar{x}}\right)\beta_0 \tag{45}$$

and therefore

$$\hat{\beta}_0 = \frac{\hat{\alpha}_1\bar{x}\left(\hat{\alpha}_1\bar{x} - \hat{\beta}_1\bar{y}\right)}{1+2\hat{\alpha}_1\bar{x}} + \frac{(1+\hat{\alpha}_1\bar{x})^2}{1+2\hat{\alpha}_1\bar{x}}b_0. \tag{46}$$

Second, the parameter values computed in the previous step are used as starting values in a standard steepest-descent algorithm (Broyden-Fletcher-Goldfarb-Shanno algorithm) that minimises the GMM penalty function of (30). The parameters that minimise this function become the GMM estimates.

Appendix 3: Additional tables

Table 3: 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
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

Continued on next page

Table 3: Hacks, thefts and losses events

Date	Amount (BTC)	Description
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 admins assets sized by FBI
2017-07-20	1200	Hansas 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 4: 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
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

Continued on next page

Table 4: Market access events

Date	Effect	Regions	Weight	Description
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	Thailands 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	Singapores Huobi opens an office in Russia, with Russian language support

Table 5: 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
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 6: 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 6 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.

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.

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.

Bianchi, D., 2018, "Cryptocurrencies as an Asset Class: an Empirical Assessment", Working paper, Queen Mary University of London.

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.

Chiu, J. and T. Koeppl, 2017, "The economics of cryptocurrencies - Bitcoin and beyond.", Working paper, Queen's University.

Cochrane, J. H., 2005, "Asset Pricing ", Revised Edition, Princeton University Press.

Cong, L. W., Y. Li, and N. Wang., 2020, "Tokenomics: Dynamic Adoption and Valuation ", forthcoming *Review of Financial Studies*.

Corbet, S., B. Lucey and L. Yarovaya, 2018, "Datestamping the Bitcoin and Ethereum bubbles", *Finance Research Letters* 26, pp. 81-88.

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.

Fantazzini, D., E. Nigmatullin, V. Sukhanovskaya, and S. Ivliev, 2016, "Everything you always wanted to know about bitcoin modelling but were afraid to ask: Part 1", *Applied Econometrics* 44, pp. 5-24.

Fernández-Villaverde, J., and D. Sanchez, 2019, "Can currency competition work?", *Journal of Monetary Economics* 106, pp. 1-15.

Gaballo, G. and E. Mengus, 2018, "Time-Consistent Fiscal Guarantee for Monetary Stability", 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.

Hansen, L., 1982, "Large Sample Properties of Generalized Method of Moments Estimators", *Econometrica* 50, pp. 1029-1054.

Hansen, L., and K. Singleton, 1982, "Generalized Instrumental Variables Estimation of Nonlinear Rational Expectations Models", *Econometrica* 50, pp. 1269-1286.

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, 2019, "An Economic Analysis of the Bitcoin Payment System", Columbia Business School Research Paper No. 17-92.

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

Kalodner, H., S. Goldfeder, A. Chator, M. Möser, and A. Narayanan, "BlockSci: Design and applications of a blockchain analysis platform", Working paper, 2017. 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*, pp. 463-484.

Liu, Y. and A. Tsyvinski, 2018, "Risks and returns of cryptocurrency." Working paper, Yale University.

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

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`

Obstfeld, M. and K. Rogoff, 1983, "Speculative Hyperinflations in Maximizing Models: Can We Rule Them Out", *Journal of Political Economy* 91, pp. 675–687.

Pagnotta, E., 2020, "Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security," Working Paper.

Prat, J., and B. Walter, 2018, "An Equilibrium Model of the Market for Bitcoin Mining," Working Paper.

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.

Schilling, L. and H. Uhlig, 2019b, "Currency Substitution under Transaction Costs," *AEA Papers and Proceedings* 109, pp. 83-87.

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," Working Paper.

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.

Zimmerman, P, 2020, "Blockchain and price volatility", mimeo Said Business School.