On the transmission of news and mining shocks in Ƀitcoin[*]

Ester Faia
Goethe University Frankfurt and CEPR

Sören Karau
Goethe University Frankfurt and Deutsche Bundesbank

Nora Lamersdorf
Goethe University Frankfurt

Emanuel Moench
Deutsche Bundesbank, Goethe University, and CEPR

This draft: September 2019.

Preliminary. Do not circulate without authors' permission

Abstract

Cryptocurrency prices fluctuate strongly despite the fact that their supply typically follows mechanical rules. In this paper we focus on two determinants of Bitcoin valuations. Using an agnostic narrative approach to identify exogenous events related to Bitcoin mining (*mining shocks*) and news affecting investor perception (*news shocks*), we first show that both types of events have sizable and persistent effects on Bitcoin valuation and aggregate mining activity. We then rationalize our findings in a model with search frictions in which heterogeneous investors can trade Bitcoin but have their transactions validated by competitive miners. The model endogenously generates waiting times and an equilibrium distribution of asset positions, which is driven by competition among miners on validation speed. Finally, we use our model to inform sign restrictions in a structural VAR analysis. We confirm the model narrative and our initial findings that both news and mining shocks significantly and persistently affect Bitcoin valuations.

Keywords: Bitcoin, Narrative approach, Electricity costs, Mining competition, Search frictions

*We thank Cyril Monnet and participants at the 2019 Annual Meeting of the Central Bank Research Association (CEBRA) for helpful comments. The views expressed in this paper are those of the authors and do not necessarily represent those of the Deutsche Bundesbank or the Eurosystem.

1 Introduction

Cryptocurrencies such as Bitcoin are a relatively recent phenomenon that is receiving significant attention. They hold features akin to traditional currencies, but are also traded as assets. Most cryptocurrencies have seen wild fluctuations in prices since their inception. This sets them apart from most traditional currencies, but also from many assets traded for speculative motives. The goal of our paper is to investigate some of the main determinants of digital currency price fluctuations. We run our investigation through an empirical analysis based on Bitcoin data and rationalize our findings through the lens of a theoretical model.

As cryptocurrencies are not issued by central banks and their supply is not managed through operational rules that respond endogenously to economic conditions, short-term price fluctuations cannot be driven by the equivalent of monetary policy. Moreover, as they are rarely used as a medium of exchange, the link between cryptocurrency valuation and macroeconomic fundamentals is also presumably tenuous. It thus seems natural to look for price determinants mainly among demand and market-based factors. News regarding the long-run viability and investor perception seems one plausible driver of demand fluctuations. As cryptocurrencies have no intrinsic value, investors' perceptions of their usefulness as a medium of exchange, store of value or profitable investment likely play a key role in determining their demand. Structural features that distinguish crypto from other currency or asset markets represent another potential source of variation. Cryptocurrencies such as Bitcoin are traded either in a primary market, in which the coins are directly transferred on a blockchain, or in exchange markets. A particular feature of direct blockchain trading is that trading completion and settlement in the blockchain depend upon miners who compete to solve cryptograms. Fiercer competition reduces waiting times and lubricates trading through the blockchain. This in turn affects the ease of trade in Bitcoin and hence trading volumes and prices. Against this background, our analysis is centered around two determinants of Bitcoin prices: news that plausibly affects investors' perception of Bitcoin, and innovations to mining competition affecting congestion externalities.

We develop our arguments in three steps. First, we employ a narrative approach to construct shock series which single out exogenous events affecting mining activity and news related to investor perception of Bitcoin. We then compute impulse responses of both Bitcoin prices and mining activity using the method of local projections and establish that both respond significantly and persistently to both types of shocks.

Second, we rationalize these findings in a structural model of Bitcoin trading. To capture the two elements discussed above we develop a dynamic search model in which investors hold heterogeneous preferences and frequently change their perception of the traded asset. As in other heterogeneous agents models, changes in the distribution of preferences or in the model's equilibrium conditions endogenously lead to changes in the distribution of asset positions.[1] In

[1] The closest antecedent to our model is Lagos and Rocheteau (23). Their work follows the tradition of modeling equilibria in over-the-counter markets through search frictions (see also Duffie, Garleanu and Pedersen (11) and Duffie, Garleanu and Pedersen (12)). A detailed account of the related literature follows in Section 2.

equilibrium, agents with high valuations of the asset endogenously become buyers and traders with low valuations become sellers. As the long run supply of the currency is fixed, short-run fluctuations in prices are largely driven by investors' net demand as determined by their valuations. To model the market structure as realistically as possible, we allow investors to trade on two markets, a primary market where transactions are recorded on a blockchain, and a secondary market, managed by exchanges on which bitcoins can be traded against other currencies upon a fee. In both markets search frictions imply that investors' contact rate of counterparties is lower than one. In particular, trades over the blockchain are completed only after they have been validated by miners, contributing to the congestion externalities characterizing blockchain trading. Most importantly, we model the validation waiting time as an endogenous variable dependent upon competition among miners. These are rewarded for their services only in the event that they solve the cryptogram first. This triggers competition for investing in technology that increases validation speed, which we model through an arms' race game among miners. For instance, as mining costs rise, miners' incentives to validate transactions fall.[2] This leads to a rise in validation waiting times, thus endogenously increasing frictions in blockchain trading. Net demand for the asset then reflects the extent of trading frictions, determining how quickly each investor can buy or sell should her perception of the asset change. These congestion externalities feed through to prices, which in the model are determined by a market clearing mechanism akin to a double auction. We visualize these channels by simulating the model and computing impulse response functions to unexpected, albeit persistent, shocks to preferences and to the cost of mining. The resulting impulse responses are qualitatively in line with the responses obtained via our narrative approach.

Finally, in a third step we estimate a structural vector autoregression (VAR) in order to verify our initial empirical findings in light of the theoretical model's transmission mechanisms. To that end, we employ time series data on Bitcoin prices, aggregate mining activity, transaction confirmation times, trading volumes and investor interest, measured as Google searches of Bitcoin related search terms. We then identify structural shocks to news and mining through a set of sign restrictions implied by the structural model. We find significant and persistent responses of Bitcoin valuations and mining activity to both shocks which are quantitatively and qualitatively similar to the ones resulting from the narrative approach and those from the theoretical model.

The paper is structured as follows. The next section reviews the expanding empirical and theoretical literature on Bitcoin and other crypto assets, highlighting the novelty of our paper. Section 3 shows the results from the narrative approach. Section 4 presents the equilibrium model and its solution. Section 5 follows with the results from the structural VAR identified via sign restrictions. Section 6 concludes.

[2]In practice, mining costs are mainly driven by computing hardware and electricity prices. We capture both in our narrative approach.

2 Literature Review and Institutional Background

As digital currencies are a relatively recent phenomenon, there is only a small but fast growing literature. In the following review we summarize the existing literature, including papers that are not directly related to our work. We further provide a brief description of the institutional and technological background. The core idea of our work, explored empirically and rationalized through a model, is to assess to what extent Bitcoin prices are driven by market-related characteristics, such as search frictions or mining, and how much is instead driven by news-driven investor demand. A few recent papers also examine the role of news. In the last part of this section we highlight the complementary and novel nature of our work relative to those.

Since the inception of Bitcoin, the first cryptocurrency, a number of papers have carefully described its institutional and technological aspects and commented on the underlying economic incentives. In this vein are the works of Yermack (47) and Velde (45), an early policy report by the ECB (13), and the technical reports by e.g. Badev and Chen (3) or Lo and Wang (25).

Early models of digital currencies were built by computer scientists or physicists,[3] who focused on cyber-security, but did not study the incentives or behaviour of participants and the role of the market characteristics in affecting prices in a general equilibrium framework.

A key aspect of the technological innovation of Bitcoin is represented by a new transaction validation method, which is based on finding solutions to cryptograms, and the recording of the completed transaction on a digital ledger. Validation is carried out through the activity of miners, who can freely enter the network and compete for solving the cryptograms first. Blocks of transactions are validated and stored only upon solving a cryptogram. Miners are rewarded only when they solve it first.[4] Competition among miners can be modelled through strategic games and there are a number of papers along this dimension. Ma, Gans and Tourky (28) propose an R&D arms' race game. In their work, which we build upon, miners compete on speed, and more investment in R&D makes it more likely for them to be the first to solve the cryptogram. The model features oligopolistic competition and miners extract rents due to the presence of entry barriers, represented by the cost of computing. Another aspect of the validation technology concerns the majority voting system, which allows other miners to check the proposed solution and to confirm or reject it. To tackle this aspect the work by Biais, Bisière, Bouvard and Casamatta (5) examines the conditions under which a coordination game among miners leads to consensus about the cryptogram solution. Both papers cited above focus on the validation methodology and examine miners' strategic interaction.

Another strand of the literature focuses on the monetary aspects of digital currencies. Chiu and Koeppl (8) extend the work of Lagos and Wright (24) for traditional currencies to the digital world. The theoretical work by Fernandez-Villaverde and Sanches (14) models privately issued digital currencies, while the empirical analysis by Agarwal and Kimball (1) argues that the adoption of digital currencies can facilitate the implementation of a negative interest rate

[3] For a review see Narayanan et al. (32). See also the work of Rosenfeld (38) or Ron and Shamir (37) on other aspects of the algorithm and the network.

[4] The solution proposed by the first miner is checked by the others and the validation of the block is completed once the majority of miners confirm the solution's validity.

policy. Bolt and Van Oordt (7) study the determinants of the exchange value of virtual currencies relative to central-bank issued fiat money based on quantity-theoretic considerations, incorporating the role of speculators as regulating the effective supply of bitcoins in circulation. Keister and Sanches (27) analyze the role of Bitcoin as publicly issued digital currency. Monetary aspects are examined also in the work of Weber (44), which compares the fixed money supply of digital currencies to the Gold Standard, and Schilling and Uhlig (40), who build a simple and elegant model on Bitcoin value vis-a-vis other currencies. Auer and Claessens (2) study the impact of regulation of cryptocurrencies on their valuations and trading volumes.

A number of works view Bitcoin as a new asset class and examine the role of information for their pricing within the group of distributed ledgers. In this vein are the theoretical works of Cong and He (9) or Malinova and Park (29). Empirical facts on the role of cryptocurrencies as financial instruments are presented in Hu, Parlour and Rajan (20) and Makarov and Schoar (30). Finally, the work by Sockin and Xiong (41) identifies cryptocurrencies as new financial products by highlighting their role as a platform, of which one has to be a member to participate. In this respect households' characteristics and their participation in the platform also matter for the determination of the cryptocurrency's value.

Digital currencies have benefits, but also several risks including that of manipulation. This is examined in Gandal, Hamrick, Moore, and Oberman (15). Griffin and Shams (16) focus on the role of Tether, a stable coin pegged to the US dollar, in driving cryptocurrency valuations and find evidence that overissuance of Tether was used to manipulate Bitcoin prices. Speculative attacks are studied by Routledge and Zetlin-Jones (39).

Bitcoins are traded both directly, in a market akin to a payment system, and through exchanges. In both markets investors experience search costs, which affect transaction waiting times. The role of waiting times is examined in the theoretical work by Huberman, Leshno, and Moallemi (19), who build a static queuing game. In contrast, in our model waiting time emerges from the frictions in a random search model with heterogeneous agents. Higher congestion externalities via longer waiting times reduce trading volumes and thus market liquidity.

In our empirical analysis, we measure news to investors' perception of Bitcoin through a narrative approach as well as using Google searches and find a significant role for news shocks related to investor attitude on prices and volumes. Other authors have examined and found evidence for the role of investor interest, see for instance the empirical studies by Urquhart (43), Kristoufek (22) or Liu and Tsyvinski (26). The latter paper shows empirically that momentum and investor attention are more important factors than fundamentals in driving Bitcoin prices.[5]

Our analysis is complementary to Liu and Tsyvinski (26) as we compare the role of market structure and mining and distinguish it from that of investor attention and perception. We further rationalize the role of market structure through a search model with heterogeneous investors and search frictions related to mining.[6] Moreover, we test the transmission mechanism in a structural VAR analysis with identifying assumptions implied by from the transmission

[5]Momentum is examined also in Stoffels (42).

[6]Empirically the role of network externalities and market structure is assessed also in the work of Kondor, Csabai, Szüle, Pósfai and Vattay, (2014), who apply graph analysis on the network of transactions.

mechanism in the model.

3 Two Stylized Facts

We start our analysis with an agnostic empirical analysis of potential drivers of Bitcoin prices. We adopt a narrative approach, following the work by Romer and Romer (35), Romer and Romer (36), Ramey (34) and many others who have used a similar approach to identify exogenous changes to monetary or fiscal policy. Specifically, we construct two different shock series related to two types of events, *i.e.* events that could influence investors' perception of Bitcoin and events that affect Bitcoin mining. Using the method of local projections, introduced by Jordá (21), we then assess the dynamic responses of Bitcoin prices and mining activity, measured by the network's hashrate, to these two shock series.

3.1 Constructing News and Mining Shocks

News shocks. To collect a series of exogenous news shocks related to investor perception of Bitcoin, we use a variety of sources. First, we parse all articles regarding Bitcoin in *Bloomberg* (Terminal, 'News' function) that were published between January 2012 and September 2018. We double-check our results by additionally browsing through all Bitcoin related articles in *The Financial Times* (online version) for the same period.[7] Furthermore, we compare our event list with lists on various web pages.[8] We focus on news that could be considered as a shock to investor attitudes, *i.e.* which arguably should have a strong impact on investors' perception of Bitcoin as a profitable investment, useful medium of exchange or store of value.[9] In the literature, news shocks affect investors' beliefs but should not have any effect on aggregate fundamentals. While in the context of Bitcoin it is not unambiguous what the fundamentals are, one should expect regulatory changes to affect aggregate fundamentals. Therefore, we decided to exclude all the events from our list that are somehow related to regulatory changes.[10] Furthermore, there are many news about Bitcoin price developments in the media, especially at the end of 2017. However, since the news events need to be exogenous with regard to the response variable in order to be a suitable shock series, we exclude this type of news from our list.

To give the reader a better impression of the type of events we have in mind, consider an incident at the end of 2012. On the 15th of November that year, WordPress, a large online publishing medium and content management system, announced that it would begin accepting

[7]There are a few cases in which the news appeared in *Bloomberg* first. For those, we assign to this event the date of when it was published first.

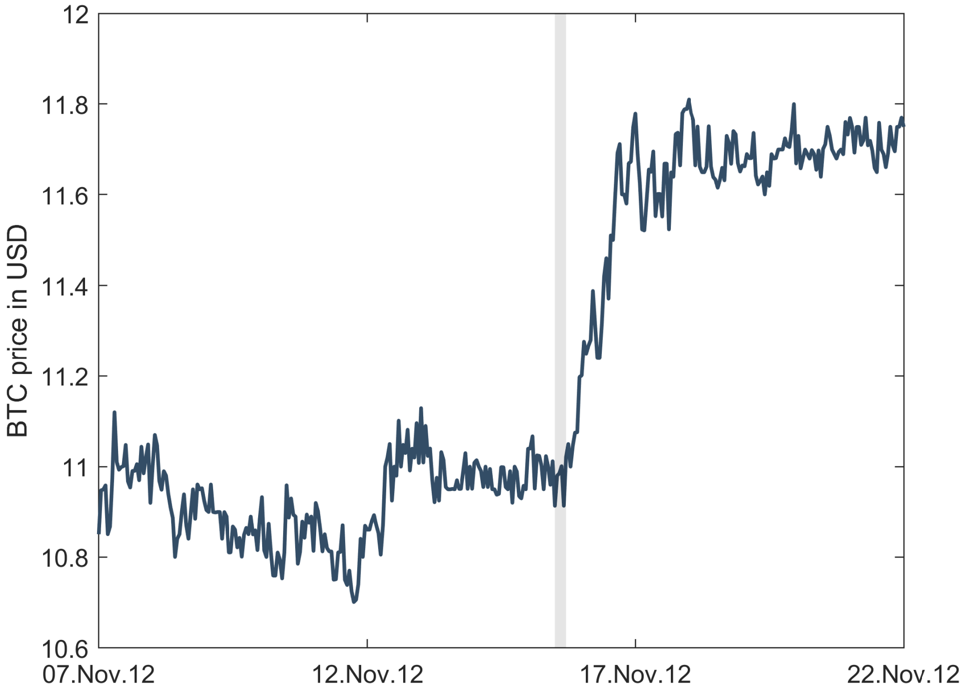
[8]For example on https://99bitcoins.com/bitcoin/historical-price/. As a final check that we have not missed any important events, we use daily data from Google Trends on the search term "bitcoin" and compared the days with extraordinary high search volume (the top 2.5%) with our event list. In case one of these days were not included in our list yet, we browsed for a possible reason for an increase in the search volume, and added this event to our list. However, these additionally added events are very few.

[9]Since the decision whether some news should be regarded as a shock to investor perceptions is sometimes not unambiguous, we ran several robustness checks with different shock selections.

[10]As mentioned in section 2, Auer and Claessens (2) study responses of Bitcoin prices to regulatory events.

Bitcoin as payment for its services, making it the biggest company at the time to do so. These news were reported by Forbes,[11] and received widespread attention in the technical community surrounding cryptocurrencies. Technology website ArsTechnica,[12] quoted Jerry Brito, a then researcher at George Mason University, as suggesting that "[t]his is a huge boost for Bitcoin (...) It's going to introduce a lot of people to Bitcoin and it's a vote of confidence." Figure 1 shows that the announcement had a clear impact on the Bitcoin price in US dollars, which jumped by around seven% after the event.[13]

Figure 1: Example of a news shock event



Note. Figure shows Bitcoin price in USD at Mt.Gox around 15th November 2012, when WordPress announced that the company would begin accepting Bitcoin as payment. Hourly data, source: bitcoincharts.com/charts/.

While the visual inspection of Figure 1 points to a fairly immediate market response to the news, we are also interested in tracing out the medium-run dynamic responses of prices as well as those of aggregate mining activity. As described, we do so below in a local projection analysis. To that end, we first assign to each positive shock a value of +1, and to each negative shock a value of –1. Importantly however, in order to weight each event by its significance as well as to ensure its exogeneity, we construct an attention index along the lines of Baker and Bloom (4). First, we download daily data from Google Trends on the respective Google search volume seven days before and seven days after the event (the event day itself is included in these second seven days). We then compare the average search volume before and after the

[11]See https://www.forbes.com/sites/jonmatonis/2012/11/16/whats-your-bitcoin-strategy-wordpress-now-accepts-bitcoin-across-the-planet/#433566375f62.

[12]See https://arstechnica.com/information-technology/2012/11/wordpress-now-accepting-payment-in-bitcoin/.

[13]In Appedix A we describe another exemplary event that led to a decline in Bitcoin prices.

incident. We consider an event as anticipated and discard if it had a larger Google search volume before the day of the shock than after. For the remaining events we then calculate the attention indices as follows:

$$\text{Att. Index} = log(1 + \text{Google searches after event}) - log(1 + \text{Google searches before event})$$

Using these attention indices, we then impose a weight on each event that is proportional to its importance.[14] Using the methodology, we arrive at a list of roughly 80 news shocks, which can be seen in Table 4 in Appendix A. While many events have relatively small weights of below 0.5, there are some with weights of up to 1.7. Events are distributed relatively equally across time with each year in the time sample featuring six to 15 events.

Mining shocks. Our second shock series refers to events affecting the mining of Bitcoin. Miners, the providers of validation services in the blockchain, solve complex mathematical problems to perform their services. The miner (or mining pool) who solves the problem first is rewarded a certain amount of bitcoins, which are newly created, in addition to the fees for all transactions in the block. In order to keep the time it takes for blocks to get confirmed to around ten minutes, the Bitcoin protocol stipulates a difficulty adjustment roughly every two weeks. More specifically, based on the time it took to mine the past 2016 blocks, the difficulty is changed up- or downward in such a way as to eliminate – in expectation – any deviations from the ten minute target. In order to construct a mining shock series, we use exogenous events that can be considered as having a large impact on mining behavior. We consider three types of events: changes in the costs of mining, significant innovations in mining hardware, and external circumstances that temporarily reduce mining power substantially.[15]

According to Vries (46), electricity costs spent for mining have a share of total mining costs of at least 60%. Hence, changes in energy prices should affect mining activities significantly. Hileman and Rauchs (18) estimate that around 60% of the major mining pools are based in China (followed by the US with only 16%).[16] Therefore, changes in Chinese energy prices should clearly influence a large share of mining activities globally. Most of these Chinese mining companies are located in the provinces Sichuan and Qinghai.[17] There are four such events in our sample when energy prices in these regions were changed. We define an increase in electricity prices as a negative shock, a decrease as a positive one.

Bitcoin mining also depends crucially on the hardware used. For instance, the introduction

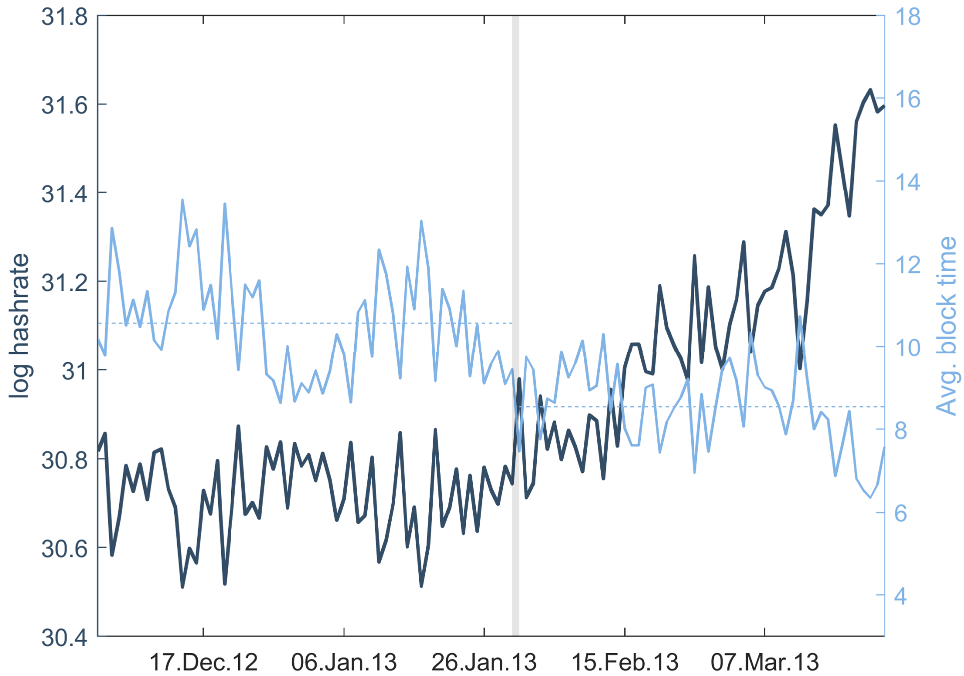
[14]Note that, with this method, events that do not have any change in their Google searches after the event compared to the days before the event, obtain a weight of zero. Hence, events that do not seem to impact investors, are also excluded from our news shock series.

[15]The two halving events of the mining reward from 50 to 25 in November 2012 and from 25 to 12.5 in July 2016 could also be considered as having an impact on mining behavior. However, since the mining reward halves every 210,000 blocks and the dates are therefore to fairly predictable, we exclude these events from our mining shock series.

[16]Of course, some members of a mining pool could still be based in another country, but the fact that around 75% of all mining pools' websites have a Chinese version is another indicator for China being the country with the most mining activities.

[17]See https://www.ccn.com/bitcoin-miners-in-chinas-remote-regions-are-undeterred-by-restrictions/.

Figure 2: Example of a mining shock event



Note. Figure shows the log aggregate hashrate (dark blue, left scale) and block confirmation times (light blue, right scale) around January 30th 2013, when the ASIC mining technology was first introduced. Dashed horizontal lines indicate average block confirmation times in minutes in the periods before and after the event. Data source: https://www.blockchain.com/charts/.

of application-specific integrated circuit (ASIC) chips for Bitcoin miners represented a big step forward in terms of mining efficiency and speed. This event is depicted in Figure 2. According to bitcointalk.com, the first ASIC miner arriced on January 30th 2013. As can be seen from the figure, the likely rollout of ASIC hardware in the following weeks led to a clear break in the trend of aggregate mining activity as measured by the network's hashrate. As each increase in the hashrate should, for a given difficulty level, lead to a probabilistic decline in block confirmation times, the figure also shows the average time in minutes for a block to be mined. There is indeed a drop of block confirmation times following the event. However, strikingly, this decline persists for almost three months, in which the average time is reduced from roughly ten to around 8.3 minutes. This is despite the fact that, as described, there is a difficulty adjustment roughly every two weeks in order to bring the time it takes for blocks to be confirmed back to ten minutes. We conclude from this data that the introduction of new powerful mining hardware must have pushed against the current difficulty limits multiple times, with each difficulty adjustment – based on the past two weeks' block times – being insufficient to eliminate a persistent drop in block confirmation times in the face of renewed increases in the hashrate due to the hardware rollout. In other words, the mining shock must have been hump-shaped, resulting in long-lived declines in block times.

While the introduction of ASIC mining was perhaps the most important milestone in Bitcoin mining hardware development, there are a few more similar events in our sample. A thorough account of Bitcoin discussion platforms and websites reveals that three new mining machines received particular attention and could be considered as major improvements in terms of electrical efficiency and price per hash.[18] Since it usually takes a few weeks until the first users adopt a new machine, we define as the event date the one when a new mining machine is discussed on one of the most popular Bitcoin discussion platforms for the first time. As the arrival of more efficient Bitcoin hardware has a clear positive influence on mining activity, we assign to the four technological events a +1 in our mining shock series.

Finally, we add to the list of mining shocks a number of events that led to temporary declines in mining activity. We include two incidents in which a substantial amount of a mining pool's hardware was destroyed by either a fire (October 2014 in Thailand) or a flood (July 2018 in Sichuan, China). In addition, the second half of 2017 saw some competition for mining power play out between Bitcoin and Bitcoin Cash. The latter was born from a hard fork in August 2017. Initially it started out with only a tiny amount of mining power devoted to it relative to the difficulty level. However, the fact that implemented in Bitcoin Cash's protocol is a rule for extraordinary difficulty adjustments made it attract substantial shares of Bitcoin's aggregate hashrate.[19] Coupled with regular difficulty adjustments, this led at least twice to a substantial share of mining power moving away from Bitcoin towards Bitcoin Cash as the latter temporarily became much more profitable to mine. As can be seen from Figure 9 in Appendix A, this resulted in large spikes in block confirmation times in Bitcoin lasting for several days. Accordingly, to these events, as to the accidents mentioned above, we assign values of -1. All mining events are summarized in Table 5 in Appendix A.

3.2 Impulse Response Analysis using Local Projections

With the two shock series at hand, we explore the dynamic effects of exogenous changes to investor perception and mining on two response variables of interest, namely the log prices of Bitcoin, measured in US dollars, and the log of the hashrate, *i.e.* the aggregate mining activity in the network.[20] We run the analysis in weekly frequency. To that end we aggregate both shock series by simply taking the sum of all shocks taking place in a given week, while we take weekly averages for all other variables. Our main results are based on the time sample from August 2012 to September 2017.[21]

Let y_{t+h} be the response variable of interest in week $t+h$, ϵ_t the shock observed in week t, α_h some horizon-specific constant, and x_t a set of control variables. Following Jordá (21), we then estimate the following regressions:

[18] See https://www.bitcoinmining.com/bitcoin-mining-hardware/.

[19] More precisely, Bitcoin Cash's protocol stipulates that if only six or fewer blocks are found in twelve hours, the difficulty is adjusted downward by 20%.

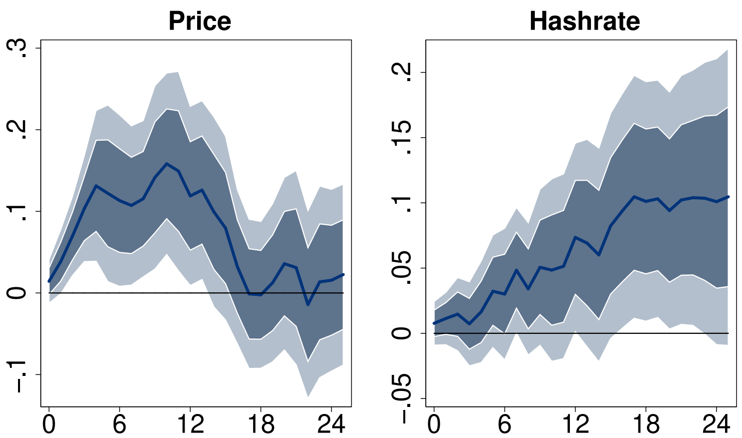
[20] We collect the data, as well as that for the control variables, from blockchain.com/charts/.

[21] In line with the structural VAR analysis in section 5 below, we choose not to include the period around Winter 2017/18 in the sample for two reasons. First, as discussed in Hale et al. (17), the peak of the meteoric rise in Bitcoin's price during that time coincided with the introduction of futures on Bitcoin, which for the first time enabled pessimistic investors to actively short Bitcoin and bet on its decline. The authors argue that this fundamentally changed the way Bitcoin prices were determined and led to the observed collapse in the price around the change of the year. Second, Griffin and Shams (16) convincingly argue that over-issuance of Tether, a stable coin tied to the US dollar, was increasingly used to manipulate Bitcoin prices after the Summer of 2017. That being said, our results in the local projection analysis are robust to the inclusion of the period in question, and indeed remain robust when we extend the sample to May 2019.

$$y_{t+h} = \alpha_h + \phi t + \gamma_h \epsilon_t + \sum_{p=1}^{P} \delta_{p,h} \epsilon_{t-p} + \sum_{q=1}^{Q} \beta_{q,h} x_{t-q} + u_{t+h}, \;\; h = 0, 1, ..., 24 \tag{1}$$

The coefficients of interest in these regressions are γ_h. They measure the response of the dependent variable y to an impulse of ϵ_t in period $t+h$, controlling for past shocks and the influence of other explanatory variables.[22] The set of control variables includes lagged values of the response variable, log prices and of the total transaction volume, *i.e.* both in the blockchain and on major cryptocurrency exchanges. Since both the the log price and the log of the hashrate exhibit a strong trend, we additionally include a linear time trend into the regressions. Standard errors are computed using the Newey and West (33) covariance estimator where we allow the maximum lag order of autocorrelation to increase with the horizon.

Figure 3: Impulse responses to news shocks in the local projection analysis



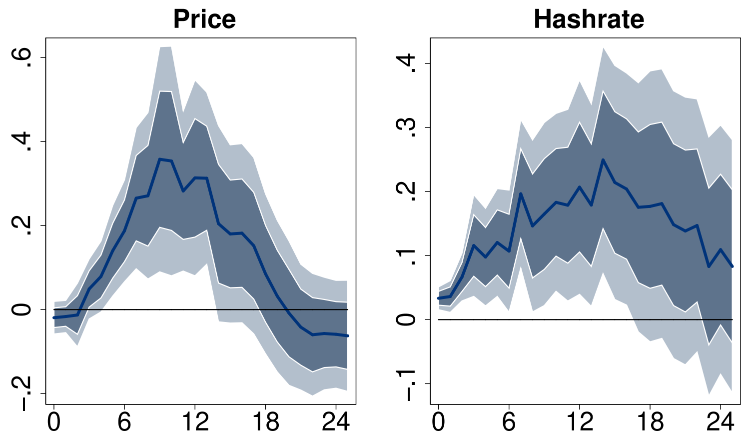
Note. Impulse responses to a news shock in the local projection analysis. Events and their respective weights are listed in Table 4 in Appendix A. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.

Figure 3 shows point estimates of the impulse responses, γ_h, along with their 90% and 68% confidence intervals, to a news shock. Prices respond fairly quickly, as could perhaps be expected from the exemplary news events discussed above. However, tracing out the response in the local projections reveals that it is hump-shaped and persists for many weeks before gradually declining. What is more, also the hashrate increases although significantly so only with a delay of several weeks.

Figure 4 shows the equivalent responses to mining shocks. We observe a significant immediate increase in the hashrate following the shock, reassuring us that the events we have collected indeed capture relevant shocks to mining activity. However, perhaps more surprisingly, as in the case of news shocks we find that prices increase significantly for several weeks after the mining shock. Although there is no significant reaction on impact, the response is again hump-shaped and peaks only after roughly two months.

[22]We set $P = Q = 8$, but the results are robust to other choices of P and Q.

Figure 4: Impulse responses to mining shocks in the local projection analysis



Note. Impulse responses to a mining shock in the local projection analysis. Events are listed in Table 5 in Appendix A. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.

4 A Dynamic Search Model of Bitcoin Trading and Prices

In the preceding section we have established two stylized facts employing agnostic empirical methods. We have found evidence of a positive and significant response of Bitcoin prices and aggregate mining activity to both news shocks as well as to shocks conducive to Bitcoin mining. In the following, we develop a model of Bitcoin trading in order to rationalize these results. Subsequently, we will employ the model to inform a more structural empirical analysis based on the model's transmission mechanisms.

4.1 Model Overview

The model captures the main structure of Bitcoin trading following the institutional background described in Section 2. Investors who intend to trade Bitcoins can do so either by trading directly with a counterparty or through an exchange. There are two important building blocks. First, investors are heterogeneous in their preferences and frequently change their preference type, which creates the scope for trading. Second, in both markets investors face search frictions.

The first type of market, in which investors search and trade directly with a counterparty, is meant to capture the trading which takes place over the blockchain. Search frictions within this market are captured by a lower than one probability of meeting a counterparty. Further, the probability of completing a transaction in the same market depends not only upon the probability of meeting a counterparty, but also upon the probability that miners validate the transaction by adding it to the blockchain. This also implies that overall transaction waiting times in this market depend on how fast validation services are performed, which in turn depends on the total hashrate or the technological investment employed by miners. In the model, miners compete on speed through an oligopolistic game. Specifically, they choose how much to invest in the crytpogram-solving technology by maximizing per-period profits under a classical downward sloping demand for their validation services. Note that miners receive the fee only in the event in which they solve the cryptogram first, hence strategic interactions take place on the technological investment needed to beat competitors on speed. The equilibrium technological investment that results from this game of interaction ultimately depends, for given number of competitors, upon primitives related to the cost of mining. For instance, and to fix ideas, an increase in electricity costs reduces miners' incentives to invest in computing technology, leading to a reduction of validation speed and an increase in transaction waiting time. In the model, this leads to a decline in trading volumes and prices.

Investors can also trade in secondary markets, in which prices are formed by exchanging Bitcoins with traditional currencies. This is done by contacting exchanges, which act as dealers. In this market, search frictions are captured by a probability lower than one of meeting an exchange. The latter retains some bargaining power through which she can set fees.

Prices in the model result from a market clearing condition, whose structure is akin to a double-auction that captures the actual clearing system employed by exchanges. This implies that prices depend upon a number of forces channeled through both markets. Specifically, motivated by the results of the narrative analysis, we consider two main channels. First, investors' perception affects net demand for Bitcoin and therefore its exchange rate directly. Second, any exogenous changes in search frictions stemming from shocks to mining, by impacting waiting times, also affect trading volumes and prices.

4.2 Formal Model Description

In what follows we describe the model formally and subsequently provide a quantitative assessment through simulations. The latter are presented in the form of impulse response functions to shocks.

4.2.1 Assumptions: agents, assets and markets

The benchmark structure featuring search frictions and investors' heterogeneity is akin to the one in the model by Lagos and Rocheteau (23). Search frictions are captured by a probability of meeting counterparty lower than one. Differently from their analysis, trading of Bitcoins in our model takes place in two markets, the blockchain whereby investors can trade directly, and through exchanges in a secondary market, whereby the digital currency s exchanged against other currencies. Moreover, trading completion in the blockchain depends not only on investors' meeting probabilities, but also on miners' validations of the corresponding transactions. We endogenize the latter via a miners' competition game on speed. This implies that in both markets the trading delays, or the probability of meeting a counterparty depends upon the activity of miners over the blockchain and upon dealers in the secondary market. In turn miners' competition affects search frictions over the blockchain and dealers' bargaining power affects the trading delays in the secondary market.

Time is continuous, starts at $t = 0$ and goes on forever. There is a unit measure of infinitely-lived risk-averse investors who invest in a numéraire and in the digital currency. There is also a unit measure of infinitely-lived risk-neutral exchanges. Meeting between exchanges and investors allows the latter to complete trading in the secondary market. Exchanges hold a bargaining power upon which they extract a fee which is bargained with the investors. Finally, there is a unit measure of risk-neutral miners whose role is that of validating transactions. They receive fees from traders, too, but also, and for our purposes more importantly, they are compensated by a mining reward in the form of newly minted coins. Each miner receives the reward only in the event that she solves the cryptogram first. This results in a competition on speed, which is achieved through investment in R&D. We will return to this aspect below.

There is one asset, Bitcoin, which produces one perishable consumption good called fruit, and a numéraire, which can be interpreted here as another currency, say US dollars. Bitcoins are durable, perfectly divisible and in fixed supply in equilibrium, $B \in R+$. Each unit of the digital currency produces a return in terms of a unit flow of fruit. The numéraire good is produced and enters the utility of all agents.

4.2.2 Preferences

Investors are heterogeneous in their asset valuations. The instantaneous utility function of an investor is $u_i(b) + \bar{c}$, where $b \in \mathbb{R}_+$ represents the holdings of Bitcoins, $\bar{c} \in \mathbb{R}$ is the numéraire good ($\bar{c} < 0$ if the investor holds more dollars than he consumes), and $i \in \mathbb{X} = \{1, ..., I\}$ indexes a preference type. The utility function $u_i(b)$ is continuously differentiable, strictly increasing and strictly concave. Note that we follow the convention in Lagos and Rocheteau (23) and Duffie, Garleanu and Pedersen (11) of assuming that the instantaneous utility directly depends upon Bitcoin holdings[23].

Each investor receives a preference shock which determines her Bitcoin net demand and follows a Poisson distribution with arrival rate δ, which is independently distributed across investors. Investors draw the preference state i with probability π_i, where $\sum_{i=1}^{I} \pi_i = 1$, independent of the investors' current preference state. Any change in investors' valuations of the digital currency implies the need to change asset positions endogenously, hence to trade. Intuitively investors with high asset valuation endogenously and as result of their optimization become buyers. The opposite is true for investors holding low valuations. The preference shocks capture investor perception about the digital currency valuation. Note, that consistently with our previous discussion, the preference distribution is ex ante exogenous, albeit it can affect the distribution of buyers and sellers. Hence in equilibrium it can affect prices through its impact on the market clearing condition.

Following Lagos and Rocheteau (23) we simplify the traders' population by assuming that exchanges and miners do not hold Bitcoins, but only consume the numéraire. All agents discount at the rate $r > 0$. Asset holdings and preference types lie in the sets $\mathbb{R}_+$ and $\mathbb{X}$, respectively, and vary across investors and over time. The distribution of heterogeneity is described with a probability space (S, Σ, H_t), where $S = \mathbb{R}_+ \times \mathbb{X}$, Σ is a σ algebra on the state space S and H_t is a probability measure on $\hat{I}\pounds$ which represents the distribution of investors

[23]The alternative assumption that investors' instantaneous utility depends on consumption and savings thus also affecting the equilibrium asset allocation would not materially change the main transmission channels occurring in our markets, but would make the model significantly more complex.

across asset holdings and preference types at time t.

4.2.3 Value Functions

We denote the Poisson rate of trading completion within the blockchain by β. As we clarify below, this can further be broken up into two components, namely the contact rate with a counterparty (denoted by λ) and the validation rate determined by the miners' competition (denoted by $1/\mu$). For the secondary market we define the Poisson contact rate with the exchanges as α. The timing T_α and T_β denote the next time the investor happens to trade on the blockchain (through a miner) and through an exchange, respectively. Finally we denote by $T_{\alpha+\beta}$ the first time that the investor will trade either directly or through an exchange.

Following the stopping-time methodology we can write the value function of investor i at time t, $V_{i,t}(b)$, as follows:

$$V_{i,t}(b) = \mathbb{E}_i \left[\begin{array}{c} \int_t^{T_{\alpha+\beta}} e^{-r(s-t)} u_{k(s)}(b) ds \\ +e^{-r(T_\alpha - t)}[V_{k(T_\alpha),T_\alpha}(b_{k(T_\alpha)}(T_\alpha)) - p(T_\alpha)(b_{k(T_\alpha)}(T_\alpha) - b) - \phi^e_{k(T_\alpha),T_\alpha}(b)]\mathbb{I}_{t=T_\alpha} \\ +e^{-r(T_\beta - t)}[V_{k(T_\beta),T_\beta}(b_{k(T_\beta)}(T_\beta)) - p(T_\beta)(b_{k(T_\beta)}(T_\beta) - b) - \phi^b_{k(T_\beta),T_\beta}(b)]\mathbb{I}_{t=T_\beta} \end{array} \right] \tag{2}$$

where $k(s) \in \mathbb{X}$ denotes the investor's preference type at time s. The expectations operator, $\mathbb{E}_i$, is taken with respect to the random variables T_α, T_β and $T_{\alpha+\beta}$ and $k(s)$. The intervals $T_\alpha - t, T_\beta - t$ and $T_{\alpha+\beta} - t$ are all distributed exponentially with the expected value $\frac{1}{\alpha}$, $\frac{1}{\beta}$ and $\frac{1}{\alpha+\beta}$, respectively. Furthermore, $\mathbb{I}_{t=T_\alpha}$ and $\mathbb{I}_{t=T_\beta}$ are indicator functions for the first occurring event.

The first term on the right side of (2) contains the expected discounted utility flows enjoyed by the investor over the interval of time $[t, T_{\alpha+\beta}]$. The flow utility is indexed by the preference type of the investor, $k(s)$, which follows a compound Poisson process. The second term on the right side of (2) is the expected discounted utility of the investor from the time when she next trades with an exchange onwards. At time T_α, the investor meets the exchange and can readjust her currency holdings from b to $b_{k(T_\alpha)}(T_\alpha)$. In this event, the investor purchases the quantity $b_{k(T_\alpha)}(T_\alpha) - b$ (or sells if this quantity is negative) at a price $p(T_\alpha)$. The third term contains the continuation value when the investor trades with other investors directly. When trading with an exchange, the investor has to pay a fee $\phi^e_{k(T_\alpha),T_\alpha}(b)$ that is set according to Nash bargaining. While the fee to exchanges is endogenous and depends upon asset positions, we treat the mining fee $\phi^b_{k(T_\beta),T_\beta}$ as fixed. In addition to the fee, miners receive the right to mine a fixed amount of bitcoins in the event that they solve the cryptogram first.[24]

Note that investors' value function depends upon the fee bargained with the exchanges. To latter is determined through the solution Nash bargaining, for which we need to define also the Exchanges' value function, something which we do in the next sub-section.

[24]At the moment the reward is 12.5 Bitcoin. As mentioned earlier, this reward is halved every 210,000 blocks. Hence, more precisely, the reward is fixed for a specific period of time, which are roughly four years.

Upon obtaining the bargained fee we can solve for the investors' optimization problem, which determines the asset positions. Given the latter we can solve for the clearing price, which emerges in the secondary market through a mechanism akin to a double-auction. Up to this stage all values are conditional on the contact rates in the secondary and the primary markets, namely α and β. In the last step the latter will be broken into two parts, the exogenous congestion rate in the blockchain and the validation rate, which depends on the competition among miners.

4.2.4 Exchange and miner value functions and the distribution of investors between the two markets

We assume that exchanges do not accumulate and trade Bitcoins themselves. As noted in Lagos and Rocheteau (23),this assumption does not alter the main dynamics of the model, but allows us to simplify the evolution of the investors' positions.

Exchanges only receive fees from all investors who trade via them at the first time T_α, which they then consume:

$$V_t^e = \mathbb{E}\left\{e^{-r(T_\alpha - t)}\left[\int_S \phi^e_{i,T_\alpha}(b)dH_{T_\alpha} + V^e(T_\alpha)\right]\right\} \tag{3}$$

where the integral is taken over the measure of investors' types S. Similar assumptions apply to miners, whose per-period net gains are modelled at a later stage.

Likewise miners do not accumulate and trade the Bitcoin that they receive from the validation services. They only receive fees, R, from all investors who trade via them at the first time T_β, which they then consume:

$$V_t^m = \mathbb{E}\left\{e^{-r(T_\beta - t)}\left[\int_S R^m_{i,T_\beta}(b)dH_{T_\beta} + V^m(T_\beta)\right]\right\} \tag{4}$$

where the integral is taken over the measure of investors' types S. Similar assumptions apply to miners, whose per-period net gains are modelled at a later stage.

The distribution of investors between the two markets is exogenous. The value of the digital currency is indeed determined as if investors can freely move between the two markets. Hence the effects of competition between the two markets manifest in prices. If the trading delay β increases this subjects exchanges to higher competition, inducing them to change prices. In this context the actual partition of investors between them is indeterminate and we assign it exogenously.[25]

[25] Miao (31) studies a search model where investors endogenously choose between trading through market-makers or in a decentralzied market. Also we consider an extension of the model along similar lines. We do so by identifying a marginal investor who is, based on her current preference state, indifferent between trading in either of the two markets. Investors with a higher preference weight then endogenously choose to trade in one of the two markets, and *vice versa*. The current version of the paper does not yet feature this endogenous allocation of investors.

4.2.5 Nash bargaining and gains from trade

When the investor meets an exchange both parties negotiate a new asset position, b', and a fee, ϕ^e. They do so according to Nash bargaining, where exchanges' bargaining power is η. If an agreement is reached and the investor i trades with the exchange at time t, her utility from that point onwards is:

$$[V_{i,t}(b_i^{'}) - p(t)(b_i^{'} - b) - \phi_{i,t}^e]\mathbb{I}_{t=T_\alpha} \tag{5}$$

If no agreement is reached, the investor loses the possibility of trading in that period and gets the fall back value function, $V_{i,t}(b_i)$, with the old asset position. In this case the investor shall resort upon trading solely over the blockchain. The net gain from trade through an exchange hence is:

$$S = [V_{i,t}(b_i^{'}) - p(t)(b_i^{'} - b) - \phi_{i,t}^e]\mathbb{I}_{t=T_\alpha} - V_{i,t}(b_i), \tag{6}$$

whereas the exchange gets $V_t^e + \phi^e$ if an agreement is reached and V_t^e if no agreement is reached. Hence its net surplus from agreement is ϕ^e. The Nash bargaining optimization for each investor i reads as follows:

$$\left[b_{i,t}, \phi_{i,t}^e\right] = \arg \max_{(b',\phi^e)} \left[[V_{i,t}(b_i^{'}) - V_{i,t}(b_i) - p(t)(b_i^{'} - b) - \phi_{i,t}^e]\mathbb{I}_{t=T_\alpha}\right]^{1-\eta} [\phi^e]^\eta \tag{7}$$

The asset position in the secondary market results from maximizing total surplus:

$$b_{i,t} = \arg \max_{b' \geq 0} \left[V_{i,t}(b_i^{'}) - p(t) b_i^{'}\right] \tag{8}$$

While the exchange fee is given by its bargaining share times the gains from trade:

$$\phi_{i,t}^e(b) = \eta \left[[V_{i,t}(b_i^{'}) - V_{i,t}(b_i) - p(t)(b_i^{'} - b)]\mathbb{I}_{t=T_\alpha}\right] \tag{9}$$

4.2.6 Investors' optimization

Given the bargaining agreement with the exchange and given the contact rate for trading over the blockchain, we now solve for the desired investment in Bitcoins by maximizing the value functions. First, we can substitute the exchange fee into the investors' value function. This results in the following:

$$V_{i,t}(b) = \mathbb{E}_i \left[\begin{array}{c} \int_t^{T_{\alpha+\beta}} e^{-r(s-t)} u_{k(s)}(b) ds \\ +e^{-r(T_\alpha - t)} \left\{ \begin{array}{c} (1-\eta) \left[\max_{b' \geq 0} (V_{k(T_\alpha),T_\alpha}(b') - p(T_\alpha)(b' - b))\right] \\ +\eta V_{k(T_\alpha),T_\alpha}(b) \end{array} \right\} \mathbb{I}_{t=T_\alpha} \\ +e^{-r(T_\beta - t)} [V_{k(T_\beta),T_\beta}(b') - p(T_\beta)(b' - b) - \phi^b] \mathbb{I}_{t=T_\beta} \end{array} \right] \tag{10}$$

where the asset optimization problem when trading with the exchange is subject to a short sale constraint, $b' \geq 0$. Note that the bargaining weight affects the meeting probability. Specifically, following Lagos and Rocheteau(23), we note that the investor's payoff is the same he would get in an alternative environment where he meets dealers according to a Poisson process with arrival rate $\alpha(1-\eta)$, but instead of bargaining, he readjusts his asset position and extracts the whole surplus with probability $1-\eta$. With probability η he cannot readjust his asset position and has no gain from trade. This implies that from the standpoint of the investor, the value function in (10) is payoff-equivalent to an alternative one in which he meets dealers according to a Poisson process with arrival rate $\kappa = \alpha(1-\eta)+\beta$. The rationale underlying this formulation is akin to one in which the investor extracts the whole surplus:

$$V_{i,t}(b) = \mathbb{E}_i \left[\begin{array}{c} \int_t^{T_{\alpha(1-\eta)+\beta}} e^{-r(s-t)} u_{k(s)}(b) ds \\ +e^{-r(T_{\alpha(1-\eta)}-t)} \left\{ \begin{array}{c} \left[\max_{b'\geq 0}(V_{k(T_{\alpha(1-\eta)}),T_{\alpha(1-\eta)}}(b') - p(T_{\alpha(1-\eta)})b')\right] \\ +p(T_{\alpha(1-\eta)})b \end{array} \right\} \mathbb{I}_{t=T_{\alpha(1-\eta)}} + \\ +e^{-r(T_\beta - t)}[V_{k(T_\beta),T_\beta}(b') - p(T_\beta)(b'-b)]\mathbb{I}_{t=T_\beta} \end{array} \right] \tag{11}$$

Next, we can combine the continuation values from both trading via the exchange and trading over the blockchain to obtain:

$$V_{i,t}(b) = \bar{U}_i(b) + \mathbb{E}_i \left[e^{-r(T_\kappa - t)} \left\{ p(T_\kappa)b + \left[\max_{b'\geq 0}(V_{k(T_\kappa),T_\kappa}(b') - p(T_\kappa)b') \right] \right\} \right] \tag{12}$$

where $\kappa \equiv \alpha(1-\eta)+\beta$ indicates the effective arrival rate of a trading opportunity, either directly (and through the miners' validation) or through the exchange, and where

$$\bar{U}_i(b) \equiv \mathbb{E}_i \left[\int_t^{T_\kappa} e^{-r(s-t)} u_{k(s)}(b) ds \right] \tag{13}$$

is the average utility over the various possible preference states.

From (12) the optimization problem of an investor can be written as follows:

$$\max_{b'\geq 0} \left[\bar{U}_i(b') - \left\{ p(t) - \mathbb{E}\left[e^{-r(T_\kappa - t)} p(T_\kappa) \right] \right\} b' \right] \tag{14}$$

Resorting on Lemma 2 of Lagos and Rocheteau (23), we can further simplify the investor's optimization problem as follows. An investor with preference type i and asset holdings b who readjusts her asset position at time t solves the following optimization problem:

$$\max_{b'\geq 0} \left[\bar{u}_i(b') - q(t)b' \right] \tag{15}$$

where:

$$\bar{u}_i(b') = (r+\kappa)\bar{U}_i(b') = \frac{(r+\kappa)u_i(b) + \delta\sum_j^I \pi_j u_j(b)}{r+\kappa+\delta} \tag{16}$$

and:

$$\begin{aligned} q(t) &= (r+\kappa)\left\{p(t) - \mathbb{E}\left[e^{-r(T_\kappa - t)}p(T_\kappa)\right]\right\} \\ &= (r+\kappa)\left\{p(t) - \kappa\int_0^\infty e^{-(r+\kappa)s}p(t+s)ds\right\} \end{aligned} \tag{17}$$

where $q(t)$ is the opportunity cost plus the expected discounted capital loss, while $\bar{u}_i(b')$ is the expected discounted utility (both expressed in flow terms) that the investor experiences by holding b from time t until her next opportunity to trade.

From the above the investor's optimizing condition that determines the asset holding distribution reads as follows:

$$\bar{u}_i'(b') = q(t) \tag{18}$$

Intuitively, at the optimum the desired asset holding is such that the marginal utility equates the opportunity cost or the unitary return on the currency.

4.2.7 Bitcoin price and double auction

For the determination of the optimal asset holding we do not need to know the asset price $p(t)$; the opportunity cost $q(t)$ is sufficient. The latter is determined in equilibrium by a market clearing condition. Once determined it will in turn affect the asset price according to (17). Differentiating the latter with respect to time implies:

$$rp(t) - \dot{p}(t) = q(t) - \frac{\dot{q}(t)}{(r+\kappa)}, \tag{19}$$

which in turn leads to a relation between the level of the opportunity cost, $q(t)$, and the currency value, $p(t)$, as follows:

$$p(t) = \int_0^\infty e^{-(r+\kappa)s}\left[q(t) - \frac{\dot{q}(s)}{(r+\kappa)}\right]ds. \tag{20}$$

Finally, the opportunity cost is determined by the market clearing condition that equates desired aggregate demand of Bitcoins with aggregate fixed supply:

$$\sum_{i=1}^I n_i(t)b_i(t) = B \tag{21}$$

where $n_i(t)$ denotes the measure of investors with the preference type i at time t and is given by

$$n_i(t) = e^{-\delta t}n_i(0) + (1 - e^{-\delta t})\pi_i. \tag{22}$$

The market clearing condition (21) is akin to a double-auction used by exchanges in the Bitcoin market. Exchanges act like Walrasian auctioneers and determine the equilibrium return of the currency, $q(t)$, by equating the aggregate net demand that they receive from the investors with aggregate supply.

4.2.8 Endogenizing waiting times in the blockchain

A distinct feature of Bitcoin is that all transactions taking place over the blockchain have to be validated by miners by solving cryptograms. Hence the overall waiting time over the blockchain can be broken into two parts: a contact rate with counterparties, λ, and a validation rate, μ. The latter, however, depends upon miners' incentives to provide the validation service, which in turn depends upon the degree of market competition among them. We therefore endogenize μ by linking it to an arms' race game among the miners. Prior to detailing the game, we set the stage and describe how mining revenues depend on market equilibrium conditions through the Bitcoin exchange rate.

The miners are rewarded for their services with newly minted coins and transaction fees paid by the sending entity. We do not model the mining fees specifically but focus on the reward of newly minted coins. These are important because changes in the Bitcoin exchange rate affect miners' incentives to invest in mining technology.[26] Given that each mining pool is rewarded only in the event that it solves the cryptogram first, miners compete for speed by investing in mining technology. Employing mining technology entails a per period cost which we assume to be quadratic in the level of the employed technology.

Next, we describe the miner's game of strategic interaction. As mentioned earlier, miners compete on speed, which ultimately depends upon the investment in R&D, which is captured by the system's hashrate (see Ma et al. (28)). Miners are denoted by $m = \{1, ..., M\}$. Their equilibrium strategy profile $x^* = \{x_1^*, ..., x_M^*\}$ delivers their investment in R&D, and finally the hashrate they employ. In order to control the supply of Bitcoins, based on the past two weeks' block times, the Bitcoin protocol specifies an adjustment of the difficulty level K approximately every two weeks. All miners face the same cost function $c : \mathbb{R}_+ \to \mathbb{R}_+$, where $c(x_m)$ is an analytic strictly increasing convex function, parameterized as follows: $c(x_m) = \nu_1 + \nu_2/2(x_m)^2$. Investing in R&D gives miners the potential opportunity to solve a cryptogram first, hence adding their block to the blockchain and collecting the mining fees for all transactions in it in addition to the coin reward. As R&D investment is costly, each miner solves a rent-cost trade-off by choosing an optimal technology level, taking the strategies of all other miners as given. The solution to the joint miners' maximization problem represents a Nash equilibrium. Similar to our assumption for exchanges which follows Lagos and Rocheteau (23), we assume that the successful miners immediately consume their mining reward. Hence, in our model newly minted Bitcoin do not affect the equilibrium allocation.

The mining pool which solves the cryptographic puzzle first is awarded newly minted coins and the sum of the mining fees contained in its block, while all other miners receive a payoff of $-c(x_m)$. The probability that a miner solves the puzzle first depends upon its investment

[26] Although the newly mined coins represent short-run changes in the money supply, these are fairly predictable and we therefore treat Bitcoin supply as fixed, as it will be in the long run.

x_m. Specifically, we assume that the technology for solving computational puzzles is a random time t_m at which K computations are completed by miner m and that it follows a Poisson process, $X(t_m) = Poisson(x_m)$. The latter is independent among miners. We denote by x_m the expected number of computations that a miner m will complete in a time interval t given their choice of technology. In turn, the random variable t_m follows a Gamma distribution, whose density is $\gamma_{K,x_m}(t_m) = \frac{(t_m)^{K-1}}{\Gamma(K)} x_m^K \exp(-x_m t_m)$.

The probability that a miner m wins by realizing a time $t_m < t_n$ for all $n \neq m$, given her investment, x_m, and that of all others, x_{-m}, is given by the cumulative density function of the minimum order statistic of the gamma random variable t_m across all miners:

$$P(t \in \{t_m < t_n \text{ for all } n \neq m\}) = \prod_{-m} \left[1 - \int_0^{t_m} \gamma_{K,x_m}(t_m) dt_m\right] \tag{23}$$

This implies that the expected payoff from the investment of miner m is:

$$\pi(x_m) = \phi^b_{k(T_\beta),T_\beta} \prod_{-m} \left[1 - \int_0^{t_m} \gamma_{K,x_m}(t_m) dt_m\right] - c(x_m), \tag{24}$$

where $\phi^b_{k(T_\beta),T_\beta} = \iota p + f$ is the mining reward consisting of the (fixed) fee f and the coinbase ιp, with ι equal to 12.5 at the time of writing and p being the market clearing price in the current period. Each miner will choose x_m by maximizing the above profit function, taking as given the investment of all other miners.

Definition 1. *A Nash equilibrium is a strategy profile $x^* = \{x_1^*, ..., x_M^*\}$ that solves the maximization problem of all miners and the expected time required to solve the proof-of-work, given (K, x^*), is $\mu_K = \min\{t_1, ..., t_M\}$.* The solution that satisfies the Nash equilibrium defined above is the vector $x^* = \{x_1^*, ..., x_M^*\}$ that solves the set of M first order conditions:

$$\frac{\partial \pi(x_m)}{\partial x_m} = \phi^b_{k(T_\beta),T_\beta} \frac{\partial P(t \in \{t_m < t_j \text{ for all } n \neq m\})}{\partial x_m} - \frac{\partial c(x_m)}{\partial x_m} = 0 \tag{25}$$

and the following set of second order conditions:

$$\frac{\partial^2 \pi(x_m)}{\partial x_m^2} = \phi^b_{k(T_\beta),T_\beta} \frac{\partial^2 P(t \in \{t_m < t_n \text{ for all } n \neq m\})}{\partial x_m^2} - \frac{\partial^2 c(x_m)}{\partial x_m^2} = 0 \tag{26}$$

It can be shown (see Ma et al. (28)) that a unique solution to the Nash equilibrium exists and that all miners adopt the same symmetric strategy. Once the optimal solution for x^* is obtained, we can compute the validation rate $\mu(K, \nu)$. As μ is determined by the difficulty level, K, and the cost of investment, c which itself depends on ν_1 and ν_2, the block arrival rate will depend upon these parameters as well. As stated earlier, we then link the block arrival times to trading frictions in that they affect the delays investors face in primary market trades. Specifically, we set $\beta = \lambda/\mu(K, \nu)$.

4.3 Model calibration

As stated earlier, our goal is to examine the impact of shocks to two distinct primitives of the model on the Bitcoin price. Specifically, we solve our model numerically and compute impulse responses to the following two unexpected, albeit persistent, ("MIT") shocks, capturing innovations of news and mining as in section 3. The model is solved globally and the resulting model-based impulse response functions will subsequently be used to impose identifying assumptions in the structural VAR. They are hence intended to provide a set of identifying assumptions, although the model is calibrated so as to produce sizeable impulse responses as well, similar to those in the structural VAR below.

Table 1: Model calibration

Parameter	Value	Description
B	1	Asset supply (normalization)
I	10	Number of preference states
r	0.05^{52560}	Discount rate
ξ	I/8	Spread parameter in preference distr.
θ	7	Spread parameter in preference weight distr.
σ	0.8	Risk aversion parameter in CRRA utility
δ	3	Arrival rate of preference shock
λ	20	Arrival rate of primary market trading meeting in minutes
β	2	Effective arrival rate of primary market trading opportunity
ρ	0.75	Shock persistence parameter
μ	10	Block arrival time in minutes
α	0.4	Arrival rate of exchange trading meeting
η	0.5	Bargaining power of exchange
κ	2.2	Effective arrival rate of trading opportunity
M	10	Number of mining pools
ν_1	3.68	Mining fixed costs
ν_2	0.4	Mining marginal (electricity) costs
K	258.8	Mining difficulty

Table 1 shows the chosen parameter values. We divide a day in 144 10-minute windows, which we take as the model's unit of time based on the average length it takes for new blocks to arrive. The asset supply is normalized to unity and we consider a generic number of $I = 10$ preference states which can be thought of as deciles of the distribution of Bitcoin investors. The parameters ξ and θ are chosen so as to produce a fairly unequal distribution of asset holdings in equilibrium.[27] The risk aversion parameter σ is set to a value somewhat below unity in order to produce positive price responses to an easing of search frictions, in line with our observations

[27] On November 12, 2017 *Bloomberg* reported that about 40% of Bitcoin are held by only about 1000 users, see https://www.bloomberg.com/news/articles/2017-12-08/the-bitcoin-whales-1-000-people-who-own-40-percent-of-the-market.

in Section 3 above.[28]

The value of $\delta = 4$ for the arrival rate of preference shocks is meant to induce a high frequency of trading needs. The block arrival rate μ is normalized to ten minutes, which is transformed to an effective arrival rate per 10-minute window of primary market trading opportunities of $\beta = 2$ by multiplying with the arrival rate of meetings, λ. The arrival rate of exchange meetings is set to $\alpha = 0.4$ in order to induce a ratio of blockchain to exchange market trading of 5, roughly in line with the median ratio over the period under investigation. These choices result in an effective arrival rate of trading opportunities $\kappa \equiv \alpha(1-\eta)+\beta$ of slightly above two. Regarding the primitives of the mining part of the model, we set the number of mining pools to ten. Although, for instance www.blockchain.info, currently tracks the hashrate distribution of no less than 17 pools, many of them are significantly smaller than the largest seven or eight. As in the model all mining pools are identical in size, we choose a number of ten pools as a compromise. Finally, we normalize the electricity costs parameter ν_2 to 0.4 and from the equilibrium conditions in the mining sector we get a value for the fixed costs ν_1 of 3.68 and for the difficulty K of 258.8.

Table 2: Functional forms

	Functional form	Description
u_i	$\epsilon_i \frac{a^{1-\sigma}}{(1-\sigma)}$	Utility function
ϵ_i	i^{θ}/I^{θ}	Preference weight
π_i	$\frac{\xi^{i-1}/(i-1)!}{\sum_{j=1}^{I}\xi^{j-1}/(j-1)!}$	Preference probability

Table 2 presents the chosen functional forms that complement the parameter calibration. The preference probability distribution for ϵ_i approximates a somewhat skewed normal density. Under such a calibration, investors are most likely to get a preference index of around two, which implies a fairly low evaluation weight. This then translates into heterogeneous desired asset holdings, which in turn means that most investors hold below one Bitcoin but a few hold large amounts of more than 1000.

We now turn to the dynamic analysis of the model, while a detailed explanation of the model's equations and numerical solution is relegated to Appendix B.

4.4 Quantitative Model Analysis

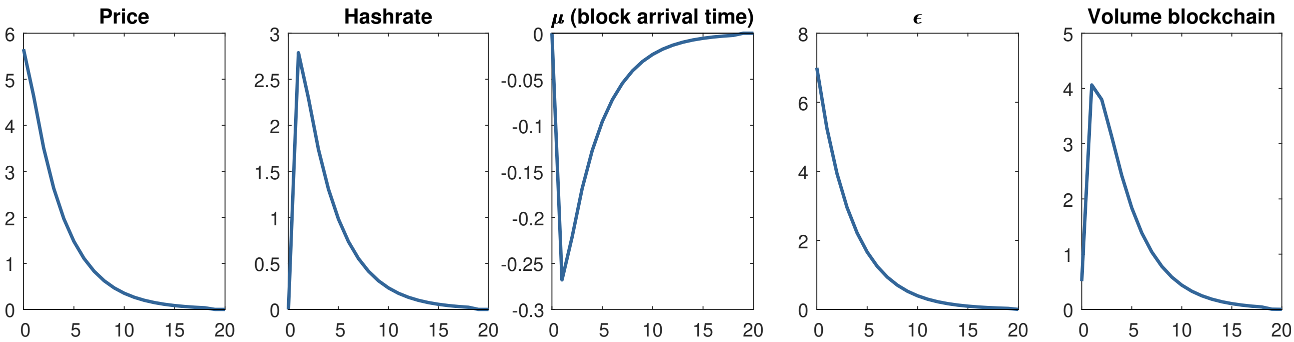
In what follows we present impulse response functions of selected variables to our two shocks of interest. Shocks are unexpected but have a mild persistence captured by an autoregressive parameter of $\rho = 0.75$.[29] The first is a shock to the distribution of the preference parameter

[28]As shown in Lagos and Rocheteau (23), there is no price response to changes in the trading frictions under $\sigma = 1$, whereas $\sigma > 1$ implies a price decline. As we have found significant positive price responses to what can be considered as exogenous shocks to mining frictions, we set σ to a value below 1.

[29]This mild persistence on a 10-minute basis is chosen for illustrative purposes. Indeed, in the VAR analysis below, based on weekly data, we assume that shocks affect volumes and mining variables for more than one week and find that prices respond for multiple weeks, in accordance with our results earlier from the local projections analysis.

characterizing the instantaneous utility (labeled ϵ).[30] This in the spirit of Blanchard et al.(6) where agent's utility contemporaneously responds to news about future productivity. The second shock again mirrors our analysis in section 3 and is meant to capture the three broad categories of mining-related shocks we identified. For simplicity, we implement it here as a shock to marginal (electricity) costs, ν_2. The shock sizes are chosen so as to produce considerable responses in trading volumes and prices, roughly in line with the ones we observe in the structural VAR analysis further below. In particular, we choose the mining shock to as to produce a fall in block confirmation times of around one minute.

Figure 5: Impulse responses to a news (ϵ) shock in the model



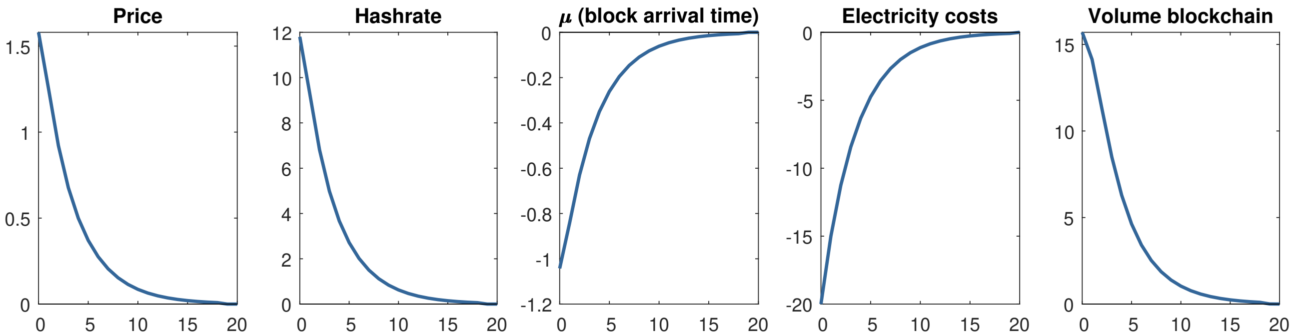
Note. Impulse responses to a news (ϵ) shock in the Bitcoin trading model. The shock parameter is ϵ_i for the upper half of all investors in the model.

Figure 5 shows impulse responses of five key variables to the news shock, mirroring those employed in the subsequent VAR analysis below. A positive shock to investor perception increases prices. This is fairly mechanical in the model as higher preference weights imply higher asset valuations in equilibrium. However, it also triggers portfolio adjustments and increases trading volumes. With increased prices, investing in mining technology becomes more profitable. Accordingly, miners increase their equilibrium technology, which results in a decline of block arrival times. This represents an easing of trading frictions and hence amplifies the response of trading volumes and the price. Note that, in line with our finding in section 3, here we assume that miners respond only with a delay to the increased price, reflecting adjustment costs and time lags that are likely to be present. This assumption is also incorporated in the VAR analysis below and is incorporated here for consistency.

Figure 6 shows impulse responses to an exogenous decline to the cost of mining as captured by the electricity cost parameter ν_2. A fall in the marginal cost of mining increases, for a given level of the difficulty, the equilibrium hashrate miners employ. This results in reduced transaction validation times by around one minute. Holders of Bitcoin, aware that they will be able to sell (or buy) more quickly in the future should the need arise, adjust their positions. Accordingly, trading volumes increase. However, as investors will be willing to hold greater quantities of Bitcoin with the fall in confirmation times, the equilibrium price increases to clear the market given the fixed supply of coins. Again miners endogenously respond by increasing

[30] More precisely, we increase of utility weights in investors' CRRA utility functions for the upper half of the investor population.

Figure 6: Impulse responses to a mining (ν_2) shock in the model



Note. Impulse responses to a mining shock in the Bitcoin trading model in the form of a fall in electricity costs (ν_2).

mining power as the now higher price raises mining profitability even more. This feedback effect leads to lower trading frictions and higher Bitcoin valuations than would arise from the initial mining impact alone.

5 Structural VAR analysis

In the preceding section, we set out to rationalize the two stylized facts established in the first part of the paper, namely that both mining activity and Bitcoin prices respond to news related to investor perceptions as well as to incidents related to mining. In this section, we run an additional empirical analysis and estimate a structural VAR model that complements the local projection analysis in section 3 in a number of important ways. First, using sign and zero restrictions based on the model developed in section 4, we are able to test the model's transmission mechanism empirically. In particular, finding significant price responses to both shocks from a model-implied identification scheme would serve as implicit verification of the model's narrative. Second, as shock identification comes from within the model, we are able to use all observations instead of relying on a somewhat limited number of events. Third, we are able to explicitly disentangle the two shocks of interest econometrically. Finally, the VAR estimation allows us to quantify the shocks and the effects they have on prices.

5.1 Data and Shock Identification via Sign Restrictions.

In order to keep the empirical analysis concise but still be able to do justice to the model's narrative, we consider a VAR model with five key variables as our baseline specification.[31] More precisely, we seek to empirically mirror as closely as possible the discussion of the theoretical model above and include in the VAR time series of Bitcoin prices, the aggregate hashrate, a measure of transaction waiting times, a measure of investor interest, and aggregate blockchain transaction volumes in BTC.

In order to construct a metric of investor interest, we follow the literature on sentiment

[31] In Appendix E we show that even a smaller model with only four variables we are able to verify our findings.

in financial markets, and construct a time series measure of Bitcoin investor perception from Google Trends data (Da et al. (10)). Specifically, for each week we look up the number of Google searches of the word "Bitcoin" with positively associated words like "rich", "buy" and "invest" and take positive news to investor attitures to correspond to the log of the averages of nine such search terms. What is more, in the VAR model, instead of using block arrival times as a measure of mining output, we use median transaction confirmation times. This metric is highly correlated with block validation times, but has the advantage that it captures congestion effects from an overcrowded network.[32] Empirically, the model equivalent of what investors ultimately care about is not the time the next block arrives but the time it takes for their own transactions to be included in a block. Hence, transaction confirmation times are our preferred measure.

Table 3: Sign and zero restrictions used in the VAR analysis

	Mining	News
Price		
Hashrate	+	0,+
Transaction conf. time	−	0
News	0	+
Trading volume blockchain	+	+

Note. Zero restrictions are imposed on impact, sign restrictions for an additional three periods. The hashrate is restricted not to respond on impact but with a delay of one period.

Table 3 summarizes the model-implied sign and zero restrictions we impose. A positive mining shock (for instance from a decline in electricity costs, as in Figure 6) induces an increase of the total hashrate employed by the system. Miners therefore employ relatively many resources relative to the system's current difficulty level, and transaction confirmation times fall. In the model, this raises blockchain trading volumes and Bitcoin prices. As the latter is the main variable of interest, we leave it unrestricted. As our goal is to differentiate the shocks as clearly as possible, we impose a zero restriction on the news measure on impact.

In contrast, for the identification of the news shock we impose an increase in the measure of investor interest. In line with the model, trading volumes are assumed to increase as well. Again for the purpose of shock differentiation, as well as because we deem it realistic, we further assume that it takes time for miners to adjust to innovations in investor interest that potentially affect Bitcoin prices and therefore mining incentives.[33] We therefore impose zero restrictions on both the hashrate and transaction confirmation times to a news shock. Finally, we identify

[32] In particular, at the end of 2016, the network for the first time hit the block size limit of 1 mega byte. This resulted in additional waiting times for traders to get their transactions confirmed even though block validation times did not materially increase.

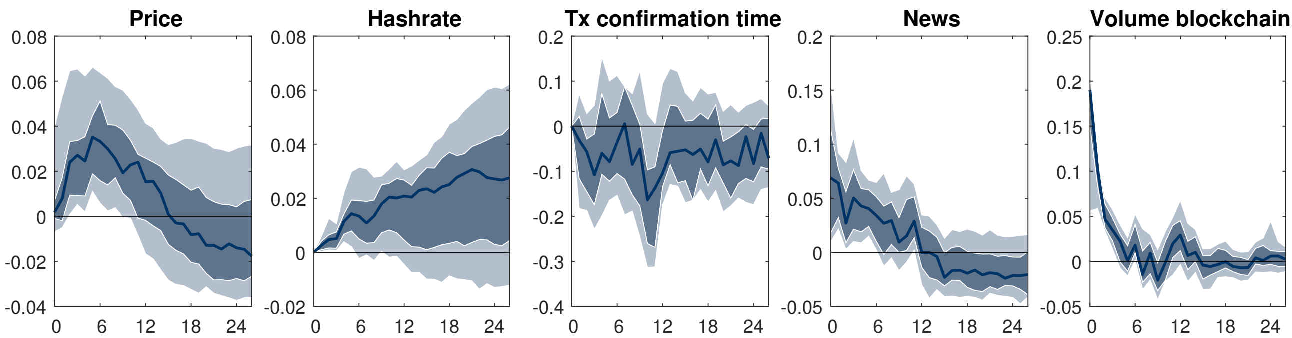
[33] It seems reasonable to assume that adjustments in mining hardware do not happen instantaneously, see e.g. Ma et al. (28). Additionally, this is confirmed by our local projection analysis in section 3, where we find a significant response only with some delay.

the news shock as increasing mining power in line with our findings in section 3.[34] Again, we do not restrict prices as their response is the main object of interest.

5.2 VAR Results

The model includes a time trend and is estimated on weekly data over the period of August 2012 to September 2017, in order to mirror as closely as possible the local projection analysis in section 3. We estimate the model with twelve lags. Shocks are identified based on the restrictions in Table 3, where all zero restrictions are imposed on impact, and the sign restrictions for an additional three periods.

Figure 7: Impulse responses to a news shock in the VAR



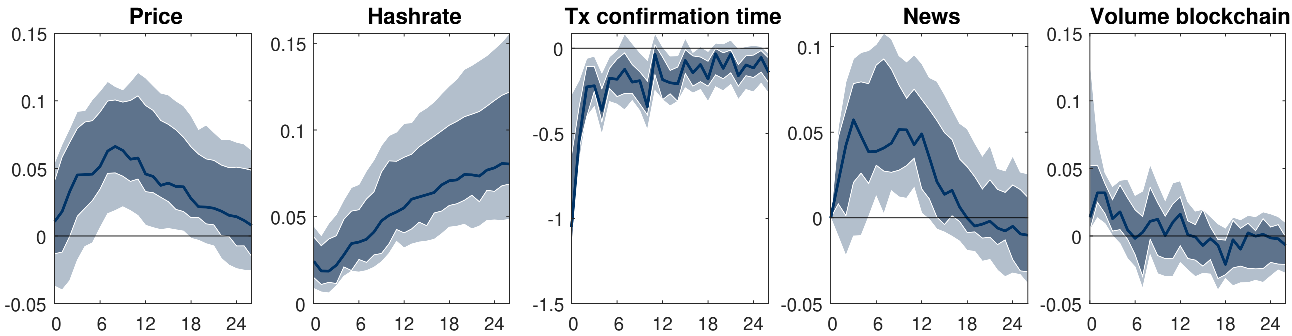
Note. Impulse responses to a news shock with identifying restrictions imposed as in Table 3. Time sample: 2012:08-2017:09. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.

Figure 7 shows impulse responses to a positive news shock. A one standard deviation increase in our news measure by assumption increases trading volumes, while hash power only increases with a delay, similar to our earlier finding. Transaction confirmation times fall with a delay as the increased mining efforts push against given difficulty levels, although the decline is only borderline significant on the 90% level. Most importantly for our purposes, however, Bitcoin prices increase significantly and persistently, with a peak response of almost 4% after six weeks, before gradually falling again.

Figure 8 shows impulse responses to a mining shock. Here, the hashrate increases on impact. This is associated with a fall in confirmation times of around one minute, before gradually fading away. Our news measure is assumed not to respond initially but there is evidence of an endogenous increase in investor interest to mining shocks with some delay. Again, most strikingly, Bitcoin prices increase persistently with some delay. Their median response peaks after several weeks at around 6% before again gradually fading away. Like in the case of the news shock, this response is remarkably similar to our initial findings using the exogenous shock events in the local projection analysis. In sum, the results of the structural VAR analysis

[34]Imposing only a zero restriction leaves price responses hardly changed but results in persistent declines of the hashrate to news shocks when no additional restriction is imposed. As this stands in contrast to our findings in section 3 and as we want to make sure that we identify a comparable shock as well as possible, we impose the delayed sign restriction.

Figure 8: Impulse responses to a mining shock in the VAR



Note. Impulse responses to a mining shock with identifying restrictions imposed as in Table 3. Time sample: 2012:08-2017:09. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.

corroborate those from the agnostic narrative approach as well as the transmission mechanism implied by the model. Both news and mining shocks have sizable and long-lasting effects on Bitcoin valuations and trading volumes.

6 Conclusion

Prices of cryptocurrencies vary substantially even though their supply follows fixed rules. In this paper, we show that demand motives and frictions in trading are key determinants of Bitcoin valuations. We construct two narrative shock series that capture exogenous events related to news regarding investor perception as well as to Bitcoin mining. The former captures changes in the acceptance of Bitcoin as a payment medium, major investment announcements and hacks or attacks of exchanges. The latter covers events related to changes in mining costs or innovations in technological mining equipment. We employ these shocks in an agnostic local projection analysis and find that both types of shocks significantly and persistently affect prices and aggregate mining activity.

We then develop a narrative to the above evidence by building a model in which investors, holding heterogeneous asset valuations, trade in markets with search frictions. The presence of heterogeneous agents allows us to determine equilibrium asset positions endogenously, which in turn affects prices through a classical market clearing condition. We model one particularity of Bitcoin, namely that miners need to validate transactions, as affecting trading frictions. As miners compete on speed by solving computationally intensive cryptograms, shocks to mining, for instance from changes in electricity costs, affect competition and hence the timing of transaction validation. This then feeds back into queuing times in blockchain trading and affects trading volumes and asset valuations.

Having rationalized our initial findings from the local projections analysis, we use the model to inform structural identification via sign restrictions in a VAR analysis. The results from the structural VAR confirm that both news and mining shocks have a substantial and persistent impact on Bitcoin prices.

References

[1] Agarwal, R. and M. Kimball, (2015). “Breaking through the Zero Lower Bound.” IMF Working Paper WP/15/224.

[2] Auer, R. and Claessens, S. (2018). “Regulating cryptocurrencies: assessing market reactions. ” BIS Quarterly Review September 2018.

[3] Badev, A. and M. Chen, (2014). “Bitcoin: Technical Background and Data Analysis.” Finance and Economics Discussion Series, Federal Reserve Board.

[4] Baker, S. R. and N. Bloom (2013). “Does Uncertainty Reduce Growth? Using Disasters as Natural Experiments.” NBER Working Paper No. 19475.

[5] Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2018). “The blockchain folk theorem.” Swiss Finance Institute Research Paper No. 17-75.

[6] Blanchard, O. J., J.-P. L’Huillier and G. Lorenzoni (2013). “News, Noise, and Fluctuations: An Empirical Exploration.” *American Economic Review*, 103(7): 3045–3070.

[7] Bolt, W. and M. van Oordt. (2018). “On the Value of Virtual Currencies.” *Journal of Money, Credit and Banking.*

[8] Chiu, J. and T. Koeppl (2017). “The Economics of Cryptocurrencies – Bitcoin and Beyond.” Working Paper.

[9] Cong, L. W. and Z. He (2018). “Blockchain Disruption and Smart Contracts.” *Review of Financial Studies*, forthcoming.

[10] Da, Z., J. Engelberg, and P. Gao (2011). “In Search of Attention.” *The Journal of Finance,* 66 (5):1461–1499.

[11] Duffie, D., N. Garleanu, and L.H. Pedersen (2005). “Over-The-Counter Markets.” *Econometrica* 73(6), 1815-1847.

[12] Duffie, D., N. Garleanu, and L.H. Pedersen (2007). “Valuation in Over-the-Counter Markets.” *Review of Financial Studies,* 20(6),1865-1900.

[13] ECB (2012). “Virtual Currency Schemes.”

[14] Fernandez-Villaverde, J. and D. Sanches (2016). “Can Currency Competition Work?” National Bureau of Economic Research Working Paper No. 22157.

[15] Gandal, N., J.T. Hamrick, T. Moore, and T. Oberman (2018). “Price manipulation in the Bitcoin ecosystem.” *Journal of Monetary Economics,* Volume 95, pp. 86-96.

[16] Griffin, J. M. and A. Shams (2018). “Is Bitcoin Really Un-Tethered?”

[17] Hale, G., A. Krishnamurthy, M. Kudlyak, and P. Shultz (2018). "How Futures Trading Changed Bitcoin Prices." *FRBSF Economic Letter,* 2018-12, Federal Reserve Bank of San Francisco.

[18] Hileman, G. and M. Rauchs (2017). "Global Cryptocurrency Benchmarking Study." *University of Cambridge*

[19] Huberman, G., J.D. Leshno, and C. Moallemi (2017). "Monopoly without a monopolist : An economic analysis of the bitcoin payment system." Research Discussion Papers 27/2017, Bank of Finland.

[20] Hu, A., C. A. Parlour, and U. Rajan (2018). "Cryptocurrencies: Stylized Facts on a New Investible Instrument." Working Paper.

[21] Jordá, O. (2005). "Estimation and Inference of Impulse Responses by Local Projections." *American Economic Review*, 95(1), pp. 161-182.

[22] Kristoufek, L. (2015). "What are the main drivers of the Bitcoin price? Evidence from wavelet coherence analysis". PlOS one: 1-15.

[23] Lagos, R. and G. Rocheteau (2009). "Liquidity in Asset Markets With Search Frictions." *Econometrica*, 77(2):403–426.

[24] Lagos, L. and R. Wright (2005). "A unified framework for monetary theory and policy analysis." *Journal of Political Economy*, 113.3 (2005): 463-484.

[25] Lo, S. and J.C. Wang (2014). "Bitcoin as Money?" Current Policy Perspectives, Federal Reserve Bank of Boston, 14-4.

[26] Liu, Y. and A. Tsyvinski (2018). "Risks and Returns of Cryptocurrency." NBER Working Paper No. 24877.

[27] Keister, T. and D. Sanches, (2018). "Managing Aggregate Liquidity: The Role of a Central Bank Digital Currency." Mimeo.

[28] Ma, J., J. Gans, and R. Tourky (2018). "Market Structure in Bitcoin Mining." NBER Working Paper, No. 24242.

[29] Malinova, K, and A. Park (2017), "Market Design for Trading with Blockchain Technology." Working Paper.

[30] Makarov, I. and A. Schoar (2018). "Trading and arbitrage in cryptocurrency markets." Working Paper.

[31] Miao, J. (2006): "A Search Model of Centralized and Decentralized Trade." *Review of Economic Dynamics*, 9, 68—92.

[32] Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder (2016). "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction." Princeton University Press.

[33] Newey, W.K. and K.D. West (1987). "A Simple, Positive Semi-definite, Heteroskedasticity and Autocorrelation Consistent Covariance Matrix." *Econometrica*, 55(3), pp. 703-708.

[34] Ramey, V.A. (2011). "Identifying Government Spending Shocks: It's all in the Timing." *The Quarterly Journal of Economics*, 126(1), pp. 1-50

[35] Romer, C. and D. Romer. (2004). "A New Measure of Monetary Shocks: Derivation and Implications." *American Economic Review*, Vol. 94, No. 4., pp. 1055-1084.

[36] Romer, C. and D. Romer. (2010). "The Macroeconomic Effects of Tax Changes: Estimates Based on a New Measure of Fiscal Shocks." *American Economic Review*, 100(3), pp. 763-801.

[37] Ron, D. and A. Shamir (2013)."Quantitative Analysis of the Full Bitcoin Transaction Graph." In: Sadeghi AR. (eds) Financial Cryptography and Data Security. FC 2013. Lecture Notes in Computer Science, vol 7859. Springer, Berlin, Heidelberg.

[38] Rosenfeld, M. (2011). "Analysis of Bitcoin Pooled Mining Reward Systems." http://arxiv.org/pdf/1112.4980v1.pdf.

[39] Routledge, B. and A. Zetlin-Jones (2018). "Currency stability using blockchain technology." Working Paper.

[40] Schilling, L. and H. Uhlig (2018). "Some Simple Bitcoin Economics." NBER Working Paper No. 24483.

[41] Sockin, M. and W. Xiong, (2018). "A model of cryptocurrencies." Working paper.

[42] Stoffels, J. (2017). "Asset pricing of cryptocurrencies and momentum based patterns." Working Paper.

[43] Urquhart, A. (2018). "What causes the attention of bitcoin?" Working Paper.

[44] Weber, W. E. (2016). "A Bitcoin standard: Lessons from the Gold Standard." Bank of Canada Staff Working Paper 2016-14.

[45] Velde, F. (2013). "Bitcoin: A Primer." Chicago Fed Letter, 317.

[46] Vries, A. (2018). "Bitcoin's Growing Energy Problem." *Joule*, Commentary, Vol. 2, Issue 5, pp. 801-805

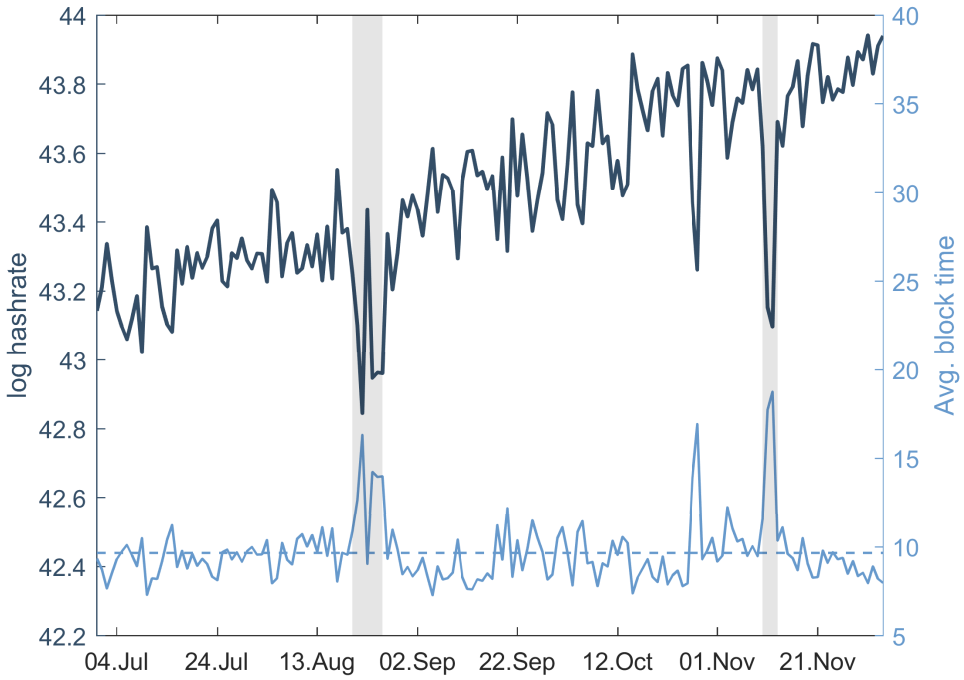
[47] Yermack, D. (2014). "Is Bitcoin a Real Currency? An economic appraisal." NBER Working Paper No. 19747.

Appendix

A Shock Events for Local Projection Analysis

In this section we provide one more example of mining shocks and list all events used for the construction of the two shock series.

Figure 9: Example of a mining shock event



Note. Figure shows the log aggregate hashrate (dark blue, left scale) and block confirmation times (light blue, right scale) around July to November 2017, when the hard fork of Bitcoin Cash and subsequent difficulty adjustments led to declines in the hashrate devoted to mining Bitcoin. Data source: https://www.blockchain.com/charts/.

In Table 4, we provide the list of events selected from news items on *Bloomberg* and *The Financial Times* that are considered as exogenous news shocks affecting investor perception of Bitcoin.

Table 4: Events for news shocks

Date	Event	p/n	weight
13.02.2012	TradeHill (Exchange) shuts down	-1	0.36
01.03.2012	Thousands of Bitcoins stolen in a hack on Linode	-1	1.51
26.04.2012	Be Your Own Bank: Bitcoin Wallet for Apple	+1	0.85
21.08.2012	Bitcoin company says debit cards coming in two months	+1	0.15
05.09.2012	$250,000 worth of Bitcoins stolen in net heist	-1	1.18
15.11.2012	Wordpress Accepts Bitcoin	+1	1.48
20.03.2013	Bitcoin apps soar in Spain after savings levy in Cyprus	+1	0.08
04.04.2013	World's largest Bitcoin exchange: We are suffering attack on our servers	-1	0.13
14.05.2013	US seizes accounts of Bitcoin exchange (Mt Gox)	-1	0.17

01.07.2013	Winklevoss twins create fund to invest in Bitcoin market swings	+1	1.10
30.08.2013	Tradehill Shuts Down (Again)	-1	0.12
25.09.2013	SecondMarket Inc. plans first US fund investing solely in Bitcoin	+1	1.60
01.10.2013	Silk Road site shut down and founder arrested	-1	0.81
24.10.2013	Fortress principal Novogratz says he has put personal money into Bitcoin	+1	1.44
30.10.2013	First Bitcoin ATM Installed in Vancouver Coffee Shop	+1	0.20
27.01.2014	Charlie Shrem (Bitcoin Foundation) charged as Silk Road case expands	-1	1.22
05.02.2014	Apple removes popular Bitcoin program Blockchain from App Store	-1	0.55
07.02.2014	Mt. Gox halts acitivity after technical problems	-1	0.46
11.02.2014	Bitstamp halts withdrawals, citing web attack	-1	0.71
24.02.2014	Mt. Gox closes	-1	0.46
05.03.2014	Flexcoin (Bitcoin bank) shuts after Bitcoins stolen	-1	0.28
08.05.2014	ETF started by Winklevosses will be listed on Nasdaq	+1	1.53
29.05.2014	Dish Network signs up to accepting Bitcoin	+1	1.61
18.07.2014	Dell Accepts Bitcoin	+1	1.09
13.08.2014	CAVIRTEX Brings Bitcoin ATMs to Canada's Malls and Tourist Spots	+1	0.30
08.09.2014	Paypal Subsidiary Braintree to Accept Bitcoin	+1	0.57
23.09.2014	PayPal expands acceptance of Bitcoin drastically	+1	0.23
11.12.2014	Microsoft to accept payments made in bitcoins	+1	0.72
04.01.2015	Bitcoin exchange Bitstamp halted after security breach	-1	0.80
20.01.2015	Coinbase has raised $75 million in financing (largest founding round yet)	+1	0.27
26.01.2015	Bitcoin gets first regulated US exchange	+1	0.17
06.03.2015	uTorrent caught installing a Bitcoin miner	-1	1.50
17.03.2015	World Bitcoin Association files for bankruptcy in NY	-1	1.18
23.03.2015	Nasdaq announces partnership with Bitcoin startup Noble Markets	+1	0.73
29.04.2015	Coinbase opens Bitcoin exchange in UK	+1	0.56
30.04.2015	Goldman Sachs and IDG Capital invest $50 million in bitcoin startup	+1	1.61
01.08.2015	MtGox bitcoin chief Mark Karpeles arrested in Japan	-1	0.76
05.10.2015	Winklevoss twins prepare to launch bitcoin exchange	+1	0.52
03.11.2015	Bitcoin Sign Accepted into Unicode	+1	0.74
03.12.2015	Goldman Sachs files patent for virtual settlement currency	+1	0.77
14.01.2016	Lead developer quits bitcoin saying it 'has failed'	-1	0.66
04.04.2016	OpenBazaar Launched	+1	0.23
06.04.2016	Barclays partners with blockchain-backed payments app Circle (uses Bitcoin)	+1	1.33
27.04.2016	Steam Accepts Bitcoin	+1	0.17
09.05.2016	Swiss city to accept bitcoin as payment for urban services	+1	0.81
17.06.2016	$50 million stolen from Ethereum	-1	0.27
03.08.2016	Bitcoin plunges after hackers breach H.K. Exchange, steal coins	-1	0.51
21.09.2016	Bitcoin to get first-ever daily auctions on Winklevoss's Gemini	+1	0.45
13.02.2017	Winklevoss twins increase bitcoin ETF offering to $100 million	+1	0.07
22.05.2017	Peach becomes Japan's first airline to accept payment in bitcoin	+1	0.48
11.07.2017	Austrian post begins selling bitcoins in 1,800 branches	+1	0.14
20.12.2017	Coinbase halts Bitcoin Cash transactions amidst accusations of insider trading	-1	0.13
28.12.2017	Bitstamp bitcoin withdrawals delayed	-1	0.51
17.01.2018	Investors face barriers trying to turn bitcoin profits into pounds	-1	0.07
26.01.2018	Coincheck says $400 million in currency lost in hack	-1	0.69
30.01.2018	Facebook bans adds tied to bitcoin	-1	0.13
07.03.2018	Crypto exchange Binance faced large scale theft attempt	-1	1.05
14.03.2018	Google bans crypto advertisements	-1	0.30

13.04.2018	Bitcoin heist of $3 million reported by India's coinsecure	-1	0.49
02.05.2018	Goldman Sachs announces to open a Bitcoin trading operation	+1	1.00
10.06.2018	South Korean crypto exchange, CoinRail has been hacked	-1	1.70
20.06.2018	S.Korean crypto exchange Bithumb says 35b Won of coins stolen	-1	0.46
26.06.2018	Facebook is lifting ban on crypto ads	+1	0.19
16.07.2018	BlackRock looks into crypto and blockchain	+1	1.76
03.08.2018	NYSE's owner announced launch of Bakkt, a federal regulated market for Bitcoin	+1	0.44
05.09.2018	Goldman Sachs drops crypto trading plans	-1	0.94
18.09.2018	Japanese Zaif exchange hacked loosing about $60 million in crypto	-1	0.53

In Table 5 we list the events that we classify as shocks affecting mining competition. These events capture changes in the circumstances of mining (such as changes in electricity prices or the big flood destroying mining centers) and significant innovations in mining hardware, such as the introduction of a new mining computer that uses ASIC chips.

Table 5: Events for mining shocks

Date	Event	Shock type
30.01.2013	First ASIC miner arrived at end user (bitcointalk.com)	+1
14.10.2014	Fire destroys mining farm in Thailand	-1
01.08.2015	Increase in electricity price in Qinghai Province	-1
13.09.2015	First review of Antminer S7 (bitcoinist.com)	+1
21.11.2015	First review of Avalon 6 (bitcointalk.org)	+1
01.06.2016	Increase in electricity price in Sichuan Province	-1
16.06.2016	First review of Antminer S9 (bitcoinist.com)	+1
01.07.2017	Reduction in electricity price in Sichuan Province	+1
01.08.2017	Hard fork attracts mining power towards Bitcoin Cash	-1
01.05.2018	Reduction in electricity price in Sichuan Province	+1
01.07.2018	Sichuan floods destroy Bitcoin mining centers	-1

B Equilibrium Model Equations

B.1 Steady State System

As a first step, consider the subsystem containing each investor's FOC and the desired market clearing condition:

$$\bar{u}_i' = q$$

$$B = \sum_{i=1}^{I} \pi_i b_i$$

This $I+1$ system of equations is solved using a Newton solver. Subsequently, we can solve for all trading-related remaining steady-state variables of interest sequentially:

$$p = q/r$$

$$n_{ij} = \frac{\delta \pi_i \pi_j + \mathbb{I}_{i=j}(\alpha+\beta)\pi_i}{\alpha+\beta+\delta}$$

$$V = \frac{\alpha+\beta}{2} \sum_{i=1}^{I} \sum_{j=1}^{I} n_{ij} |b_i - b_j|$$

$$V^e = \frac{\alpha}{2} \sum_{i=1}^{I} \sum_{j=1}^{I} n_{ij} |b_i - b_j|$$

$$V^b = \frac{\beta}{2} \sum_{i=1}^{I} \sum_{j=1}^{I} n_{ij} |b_i - b_j|$$

$$\phi_{ij}^e = \frac{\eta[\bar{u}_i(b_i) - \bar{u}_i(b_j) - q(b_i - b_j)]}{r + \alpha + (1-\eta)}$$

Based on these steady-state values and a fixed number of miners M as well as cost parameter ν_2 we find values for the equilibrium technology level x^*, the difficulty K and fixed mining costs ν_1 that support these values. This is achieved by solving the following system containing the miners' FOC, an entry condition, and the requirement that the minimum amount of time it takes all miners to solve a cryptogram is in expectation equal to the desired target time μ^*:[35]

$$\nu_2 x^* = p - (M-1) f(K, x^*)[1 - F(K, x^*)]^{M-2}(-K/x^{*2})$$

$$p = M(\nu_1 + \nu_2/2x^{*2})$$

$$\mu^* = \int_0^\infty [1 - F(t, K, x^*)]^M dt,$$

where $f()$ is the probability density and $F()$ the cumulative density function of the Gamma distribution.

[35]For more details and a derivation of these equations see Ma et al. (28).

C Solution to the Investors' Maximization Problem

In this section we shall solve the maximizaztion problem of the investor's value function upon substituting the fee that she shall pay to the exchanges. Hence we start by substituting into (2) the bargained exchange fee, (9). This leads to (10). With an effective arrival rate of exchange trades of $\alpha(1-\eta)$ we then arrive at (11), and can further combine the arrival rates into $\kappa = \alpha(1-\eta)+\beta$. The investor's value function then becomes:

$$V_{i,t}(b) = \mathbb{E}_i \left[\begin{array}{c} \int_t^{T_\kappa} e^{-r(s-t)} u_{k(s)}(b) ds \\ +e^{-r(T_\kappa - t)} \left\{ p(T_\kappa)(b) + \left[\max_{b' \geq 0} (V_{k(T_\kappa),T_\kappa}(b') - p(T_\kappa)(b')) \right] \right\} \mathbb{I}_{t=T_\kappa} \end{array} \right] \tag{27}$$

Now define:

$$\bar{U}_i(b) \equiv \mathbb{E}_i \left[\int_t^{T_\kappa} e^{-r(s-t)} u_{k(s)}(b) ds \right] \tag{28}$$

From (27) the problem of an investor with preference shock i who gains access to the market at time t is given by:

$$\max_{b' \geq 0} \left[\bar{U}_i(b') - \left\{ p(t) - \mathbb{E}\left[e^{-r(T_\kappa - t)} p(T_\kappa) \right] \right\} b' \right] \tag{29}$$

Equation (28) can be written recursively as:

$$(r+\kappa)\bar{U}_i(b) = u_i(b) + \delta \sum_{j=1}^{I} \pi_j \left[\bar{U}_j(b) - \bar{U}_i(b) \right] \tag{30}$$

upon multiplying (30) through by π_i, summing over i, solving for $\sum_{j=1}^{I} \pi_j \bar{U}_i(b)$ and substituting back into (30) one obtains $\bar{U}_i(b) = \frac{\bar{u}_i(b)}{r+\kappa}$ where:

$$\bar{u}_i(b) = \frac{(r+\kappa)u_i(b) + \delta \sum_j \pi_j u_j(b)}{r+\kappa+\delta} \tag{31}$$

One should then simplify the term:

$$\mathbb{E}e^{-r(T_\kappa - t)} p(T_\kappa) = \kappa \int_0^\infty e^{-(r+\kappa)s} p(t+s) ds \tag{32}$$

Upon substituting (32) back into (29) and multiplying for $(r+\kappa)$ we obtain the optimization problem in (15). Note also that we can write:

$$\begin{aligned} q(t) &= (r+\kappa) \left\{ p(t) - \mathbb{E}\left[e^{-r(T_\kappa - t)} p(T_\kappa) \right] \right\} \\ &= (r+\kappa) \left\{ p(t) - \kappa \int_0^\infty e^{-(r+\kappa)s} p(t+s) ds \right\} \end{aligned} \tag{33}$$

which is again part of the simplified optimization problem in (15). The investor's optimization problem can then be solved via the problem outlined in (15) rather than in the more complex solution of the Hamiltonian Jacobi Bellman (HJB).

C.1 Dynamic System of Equations

We compute dynamic responses of the equilibrium variables following a shock to the parameters ν_2 and some ϵ_i. The shock is modeled as an "MIT" autoregressive shock, *i.e.* agents consider it zero probability events which then decay according to an Ornstein-Uhlenbeck process of the form

$$dX(t) = \nu(X - X(t))dt, \tag{34}$$

with $X = \{\nu_2, \epsilon_i\}$.

Solution is done via a Newton-type solver to solve the system for all periods $t + h$ with $h = 1, 2, ..., H$.

$$\bar{u}_i'(t) = q(t)$$

$$B = \sum_{i=1}^{I} n_i(t) b_i(t)$$

$$p(t) = \int_t^\infty e^{r(s-t)} \left[q(s) - \frac{\dot{q}(s)}{r + \kappa(t)} \right] ds$$

$$\nu_2 x^*(t) = p(t) - (M-1) f(t, K, x^*(t)) [1 - F(K, x^*(t))]^{M-2} (-K/x^*(t)^2)$$

$$\mu(t) = \int_0^\infty [1 - F(s, K, x^*(t))]^M ds,$$

The first two equations stem from the investor's optimization in the search part of the model, in which $n_i(t) = e^{-\delta t} n_i(0) + (1 - e^{-\delta t})\pi_i$, for some starting values $n_i(0)$. In particular, if we start in steady state, then $n_i(t) = \pi_i$ for all t. The third equation computes the asset price, in which $\kappa(t) = \alpha(1 - \eta) + \lambda/\mu(t)$. The remaining equations stem from the mining part, in which miners endogenously respond to the current exchange rate, which feeds into their revenues. Note that the dynamic system above does not feature the entry condition anymore as we abstract, given the relative stability of the number of mining pools over time, from pools entering or exiting the market.

We may also note that the set of optimal asset positions $b_i(t)$ changes once the model is shocked. More specifically, for each value of the exogenous shock process there is a new set of optimal asset positions for all investors. While for the computation of prices and mining variables it is sufficient to track these optimal asset positions each at a time, to calculate dynamic trading volumes we additionally need to track how many investors remain in some previously optimal positions after conditions change.[36] This is done by tracking the object $n_{ij}(t,\tau)$, which can be thought of, together with $n_i(t)$, as the equivalent of the Kolmogorov Forward (Fokker-Planck) equation in other continuous-time heterogeneous agent models, but is again simplified by the fact that it does not depend on endogenous variables:

$$n_{ij}(t,\tau) = (\alpha+\beta(t))e^{-(\alpha+\beta(t))\tau}\Big[(1-e^{\delta\tau})\pi_i + e^{-\delta\tau}\mathbb{I}=j\Big]n_j(t-\tau)$$

$n_{ij}(t,\tau)$ is time-t density of investors of type i who are holding asset position $a_j(t-\tau)$, *i.e.*, investors whose last trade was at time $(t-\tau)$ when their preference type was j, and who have preference type i at time t. Consequently, this density controls the evolution of all remaining variables that depend on the difference between current and desired asset holdings. We then can compute $n_{ij}(t)$, which is the density of investors in state j with desired asset holdings i in time t and is effectively achieved by integrating over all previous τ periods. Based on this, we can compute the dynamic versions of trade volumes, fees and related variables:

$$V(t) = \frac{\alpha+\beta(t)}{2}\sum_{i=1}^{I}\sum_{j=1}^{I} n_{ij}(t)|b_i(t)-b_j(t)|$$

$$V^e(t) = \frac{\alpha}{2}\sum_{i=1}^{I}\sum_{j=1}^{I} n_{ij}(t)|b_i(t)-b_j(t)|$$

$$V^b(t) = \frac{\beta(t)}{2}\sum_{i=1}^{I}\sum_{j=1}^{I} n_{ij}(t)|b_i(t)-b_j(t)|$$

$$\phi^e_{ij}(t) = \frac{\eta[\bar{u}_i(b_i(t)) - \bar{u}_i(b_j(t)) - q(t)(b_i(t)-b_j(t))]}{r+\alpha+(1-\eta)}$$

D Efficiency of Prices

Establishing the determinants of digital currency prices leads to the question of their efficiency properties. We address this issue in this section. To this purpose we lay down the planner solution. The comparison between this and the competitive economy will speak upon the size of the efficiency mismatch.

The planner maximizes the sum of the investors utility under commitment. This means to take the sum over all investors, i and also to compute the value function over the integral up to the infinite horizon (commitment solution). It shall be mentioned that this planner is neglecting the utility of the dealer or at least the rent he extracts is set to zero (no monopoly

[36] While the steady-state system is based on a fixed number of possible desired asset holdings (that stem from the investor's FOC), the implementation of the dynamic model is made more complicated by the existence of shocks. In particular, when calculating $n_{ij}(t)$, we need to take into account that the desired asset holdings change in the following sense. Due to the trading frictions, following a shock, there is a positive mass of investors holding not only the wrong amount of assets relative to their own current type, but an amount of assets that, after the shock, none would like to trade into in the first place. In other words, with I investors, there may be a positive mass of investors in up to $I(1+\hat{T})$ asset grid points, with $\hat{T}$ being the number of periods the system is not in steady state following the shock. While, with a shock with autoregressive decay, in principle the asset grid would hence be infinite, the code keeps track of a finite number of periods, making the asset grid finite as well.

under social planner). Since there is no dealers' rent $\kappa_1 \equiv \alpha + \beta$. the planner takes into account the technological constraints, that are that demand clears with supply and the evolution of investors' types.

Social planner problem (aggregate welfare is not per period value function, but sum over infinite horizon):

$$\max_{b_i(t) \geq 0} \left[\int_0^{\infty} \frac{\kappa_1}{r + \kappa_1} \sum_{i=1}^{I} \hat{u}_i(b_i(t)) n_i(t) e^{-rt} dt \right] \tag{35}$$

where $\hat{u}_i(b_i(t)) = \frac{(r+\kappa_1)u_i(b)+\delta \sum_j^I \pi_j u_j(b)}{r+\kappa_1+\delta}$ but where now s.to:

$$\sum_{i=1}^{I} n_i(t) b_i(t) = B \tag{36}$$

where $n_i(t)$ denotes the measure of investors with the preference type i at time t and is given by

$$n_i(t) = e^{-\delta t} n_i(0) + (1 - e^{-\delta t}) \pi_i. \tag{37}$$

Define $\lambda(t)$ as the shadow price of wealth or the Lagrange multiplier on constraint 21. The first order condition to the above problem reads as follows:

$$\hat{u}_i'(b_i(t)) = \lambda(t) \tag{38}$$

Proposition 1. The solution to the planner optimization problem is equivalent to the solution of the competitive economy to the extent that $\eta = 0$.

Proof: Note that $\hat{u}_i'(b_i(t)) = \bar{u}_i'(b_i(t))$ *to the extent that* $\kappa_1 = \kappa$ *that is when* $\eta = 0$. *This also implies that the right hand side shall be the same, hence* $\lambda(t) = q(t)$.

E Robustness Checks for the Empirical Analyses

In this section we conduct robustness checks of our empirical analyses. First, Figures 10 and 11 show that our results of an increase of both prices and mining activity following both news and mining shocks in the local projection analysis still hold when we extend the time sample to May 2019, *i.e.* when we include the strong increase and then collapse in Bitcoin prices in Winter 2017/18. Figures 12 and 13 show the equivalent results for the VAR.

Figure 10: Impulse responses to news shocks in the local projection analysis (until May 2019)

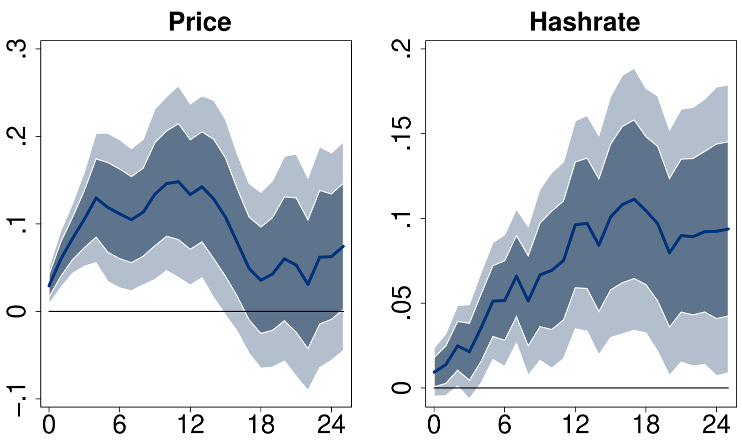
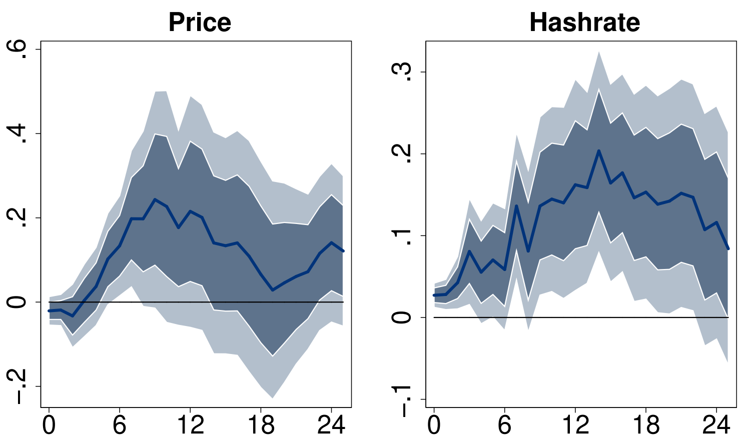
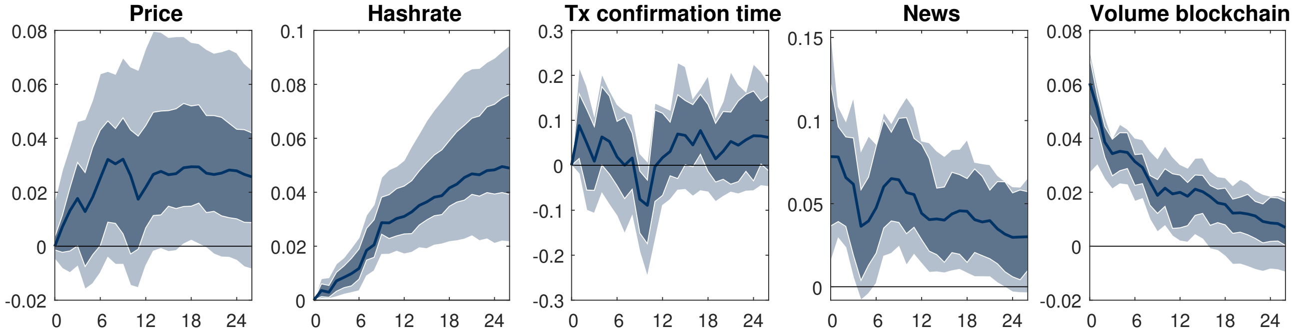


Figure 11: Impulse responses to mining shocks in the local projection analysis (until May 2019)



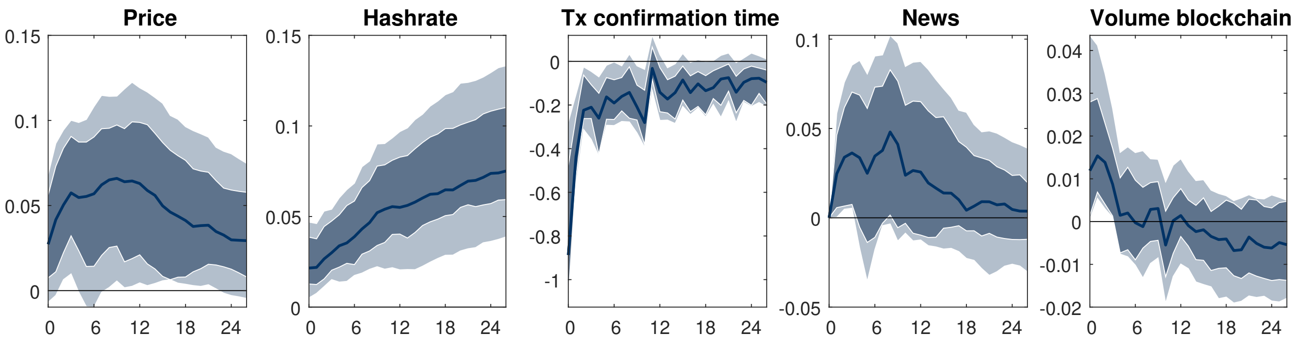
Note. Impulse responses to a news shock in the local projection analysis. Events their respective weights are listed in Table 4 in Appendix A. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.

Figure 12: Impulse responses to a news shock in the VAR (until May 2019)



Note. Impulse responses to a news shock with identifying restrictions imposed as in Table 3. Time sample: 2012:08-2019:05. Time sample: 2012:08-2019:05. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.

Figure 13: Impulse responses to a mining shock in the VAR (until May 2019)



Note. Impulse responses to a mining shock with identifying restrictions imposed as in Table 3. Time sample: 2012:08-2019:05. Dark shaded areas denote 68% confidence bands, light shaded areas 90%.