DISCUSSION PAPER SERIES

DP20141

MINING SHOCKS, BLOCKCHAIN SECURITY, AND THE VALUE OF BITCOIN

Sören Karau and Emanuel Moench

ASSET PRICING

ISSN 0265-8003

MINING SHOCKS, BLOCKCHAIN SECURITY, AND THE VALUE OF BITCOIN

Sören Karau and Emanuel Moench

Discussion Paper DP20141
Published 17 April 2025
Submitted 16 April 2025

Centre for Economic Policy Research
187 boulevard Saint-Germain, 75007 Paris, France
2 Coldbath Square, London EC1R 5HL
Tel: +44 (0)20 7183 8801
www.cepr.org

MINING SHOCKS, BLOCKCHAIN SECURITY, AND THE VALUE OF BITCOIN

Abstract

We study the implications of Bitcoin's security model for its market valuation. We identify mining shocks by exploiting exogenous variation in mining intensity using a narrative approach in a structural Vector Autoregression. While their impact on transaction speed is short-lived, mining shocks persistently affect trading volumes and market valuations, explaining up to 15 percent of Bitcoin's substantial price variation. Our findings can be rationalized in a theoretical framework where mining shocks affect the likelihood to withstand potential attacks and as such impact investor beliefs about the future state of the network and thus Bitcoin’s usefulness as a means of payment.

JEL Classification: E42, G32, L14, O16

Keywords: Bitcoin, Blockchain, Mining, Proxy var

Sören Karau - soeren.karau@bundesbank.de
Deutsche Bundesbank

Emanuel Moench - e.moench@fs.de
Frankfurt School of Finance & Management and CEPR

Acknowledgements
The views expressed in this paper are those of the authors and do not necessarily coincide with the views of the Deutsche Bundesbank or the Eurosystem. This paper supersedes a previously circulated paper entitled ``Is it Really Mine? Mining Shocks and their Effects on Bitcoin Valuations'' which can be found under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4362032. We thank seminar participants at the Cryptocurrency Research Conference, Frankfurt School of Finance & Management, the Federal Reserve Board, Deutsche Bundesbank and the International Association of Applied Econometrics.

Mining Shocks, Blockchain Security, and the Value of Bitcoin*

Sören Karau[1] **Emanuel Moench**[2]

April 16, 2025

Abstract

We study the implications of Bitcoin's security model for its market valuation. We identify mining shocks by exploiting exogenous variation in mining intensity using a narrative approach in a structural Vector Autoregression. While their impact on transaction speed is short-lived, mining shocks persistently affect trading volumes and market valuations, explaining up to 15 percent of Bitcoin's substantial price variation. Our findings can be rationalized in a theoretical framework where mining shocks affect the likelihood to withstand potential attacks and as such impact investor beliefs about the future state of the network and thus Bitcoin's usefulness as a means of payment.

Keywords: Bitcoin, Blockchain, Mining, Proof of Work, Blockchain Security, Proxy VAR

JEL Codes: E42, G32, L14, O16

---

*The views expressed in this paper are those of the authors and do not necessarily coincide with the views of the Deutsche Bundesbank or the Eurosystem. This paper supersedes a previously circulated paper entitled "Is it Really Mine? Mining Shocks and their Effects on Bitcoin Valuations" which can be found under https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4362032. We thank seminar participants at the Cryptocurrency Research Conference, Frankfurt School of Finance & Management, the Federal Reserve Board, Deutsche Bundesbank and the International Association of Applied Econometrics.

[1]Deutsche Bundesbank, Wilhelm-Epstein-Straße 14, 60431 Frankfurt am Main. Contact e-mail: soeren.karau@bundesbank.de.

[2]Corresponding author. Frankfurt School of Finance & Management and CEPR, Adickesallee 32–34, 60322 Frankfurt am Main, Germany. Contact e-mail: e.moench@fs.de.

1 Introduction

The price of Bitcoin varies considerably. As Bitcoin's supply scheme is mechanical, it is often argued that the drivers of price swings are to be found on the demand side and that they mostly reflect speculative behavior unrelated to fundamentals. Yet, proponents stress that Bitcoin's value derives from its approach to achieve decentralized value transfers by providing miners with incentives to spend resources to validate transactions and secure the transaction record. In this paper, we study the effects of exogenous variations in mining intensity to study the implications of Bitcoin's unique security model for its market value.

The key idea behind Nakamoto's (2008) invention of Proof-of-Work (PoW) is that updating the blockchain by a new block of transactions needs to be costly such that any attempt to attack the network – tempering with the transaction record – is prohibitively expensive. This is achieved by cryptographically chaining any new block to the previous block. As the network accepts the longest chain of blocks as valid, retrospectively changing transactions would therefore require a large amount of computational resources to outcompete the other miners. In other words, to guarantee security, "the size of the mining network needs to be so large that attacks are inconceivable."[1] And it needs to be large always: as pointed out by Budish (2022, p.3), in principle the Bitcoin network "is only as secure at any moment in time as the amount of computing power devoted to maintaining it at any moment in time."[2]

What does such a security model imply for Bitcoin's market valuation? Answering this question empirically is challenging since a close correlation between the system's hashrate – measuring the total computational power employed by all miners – and the market price of Bitcoin is to be expected: as adding a block of transactions entails a reward of newly minted bitcoins (plus transaction fees), a rise in their market value sparks additional mining investment and hence a larger hashrate (Prat and Walter, 2021). As indicated by the blue arrow in Figure 1, causality thus runs from prices to mining (*hashrate follows price*). In this paper, we provide empirical evidence that causality also runs in the opposite direction: *price follows hashrate*.[3] As indicated by the red arrows in Figure 1, a more secure network sparks additional user demand, therefore raising market valuations.

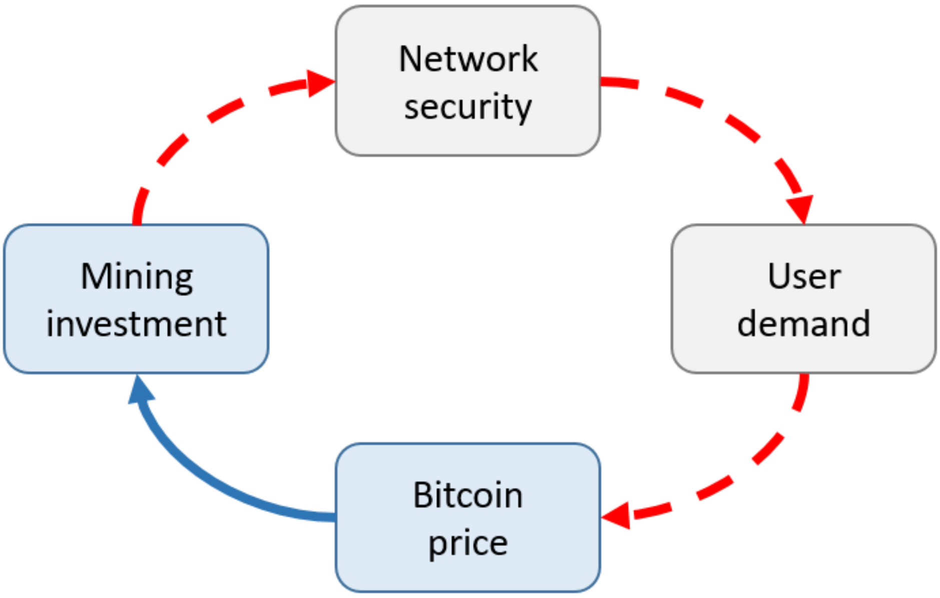
We demonstrate this causality by empirically identifying *mining shocks* – exogenous variations in the hashrate that are not an endogenous response of miners to changing Bitcoin prices – using a Structural Vector Autoregression model of the Bitcoin market.

[1] This statement is part of a `2016 blog post` by Ethereum founder Vitalik Buterin.

[2] This does not imply that the amount of computing power is the only metric determining network security, as incentives or abilities to attack may vary over time.

[3] The idiom *price follows hashrate* is a reference to a `view held` by some members within the Bitcoin community.

Figure 1: FEEDBACK EFFECTS BETWEEN MINING AND BITCOIN PRICE



Note. Figure adapted from Chiu and Koeppl (2022) and Pagnotta (2022).

We adopt two alternative identification schemes to isolate exogenous changes in mining. Our main results are based on a narrative approach in the spirit of Romer and Romer (1989). Specifically, we identify plausibly exogenous events beyond the influence of miners which have affected aggregate mining intensity. We then use these events, which include natural disasters such as floods and fires that destroyed large mining farms, as external instruments in a proxy VAR (Stock and Watson, 2018). In a second approach, we identify mining shocks recursively via timing constraints in the adjustment of mining equipment.

Both identification approaches yield very similar results, showing that shocks to mining activity have statistically significant effects on the U.S. dollar price of Bitcoin up to one year out. They account for ten to 15 percent of the variation in Bitcoin's market value and are thus an economically relevant driver of Bitcoin's substantial price fluctuations. We find evidence of two channels. First, mining shocks impact transaction speed and blockchain congestion by affecting the time it takes for transactions to be added to the blockchain. This *transaction speed channel*, however, is short-lived and vanishes after at most two weeks due to Bitcoin's built-in difficulty adjustment that re-aligns block confirmation times to the 10-minute goal.[4] More importantly, we find long-lasting effects that point to a *security channel*: a drop in mining activity persistently lowers demand for block space, the number of transactions as well as their size and, as a result, the price of Bitcoin.

We corroborate the importance of security considerations in the propagation of mining

[4]The difficulty is automatically adjusted every 2,016 blocks (roughly 2 weeks) based on the average block confirmation time over that period. When blocks are added more slowly than 10 minutes on average, the difficulty is adjusted downwards, and vice versa.

shocks with two exercises which document a state-dependence in the response of Bitcoin valuations to mining shocks. First, we show that mining activity is often elevated after a persistent fall in mining revenues, for example after halving events.We find that mining shocks have significantly larger effects on prices in low- compared to high-revenue regimes. This is consistent with the notion that a fall in mining revenue may give rise to concerns that a high degree of mining intensity could become unsustainable in the future.

Second, we show that mining shocks have larger effects on Bitcoin valuations after the release of new mining hardware. As newly released circuits are often capable of performing many more hashes per second than previous ones, the phasing in of new hardware implies that already-installed mining rigs become less competitive. If some miners cannot pay the fixed costs for upgrading their hardware, this increases the risk of malicious miners entering the network and making it less reliable. Consequently, negative shocks to mining intensity have a stronger effect on Bitcoin valuations in such episodes.

One might be worried that the negative response of Bitcoin prices to exogenous declines in mining activity is partially explained by liquidity-constrained miners cashing out some of their Bitcoin holdings in response to mining disruptions. However, while we provide some evidence for such cashing-out behavior, we show that this does not account for the strong price effects of mining shocks.

We interpret our findings of sizable and persistent price effects of mining shocks through the lens of a model which we detail in the appendix. Specifically, we introduce mining shocks into the framework of Pagnotta (2022), which formalizes the positive feedback effects between mining and security depicted in Figure 1. In the model, the possibility of attacks on the network poses a threat to network security. A high price of Bitcoin thus induces large mining effort by honest miners that the attacker has to compete against. This makes an attack unlikely to succeed, which in itself sustains large user demand and high prices. Conversely, a low price of Bitcoin means low levels of mining investment, security and user demand, making the low price equally self-fulfilling.

Consistent with our empirical results, in this framework mining shocks can impact Bitcoin prices in two ways. First, they can affect the likelihood of successful attacks by altering the relative amount of computing power devoted to attack and defend the network, respectively. Second, mining shocks shift beliefs about the future security of the network and associated Bitcoin prices. Importantly, mining shocks can have price effects without making a successful attack likely. Even moderate shifts in investor beliefs about the future security of the network can induce sizable shifts in current valuations. This helps rationalize our finding of mining shocks having sizable price effects despite the fact that Bitcoin has never been successfully attacked.

In sum, our findings highlight that a meaningful share of Bitcoin price fluctuations is due to variations in the system's hashrate which in turn reflect investors' assessment of the network's security. This is consistent with the security model of Bitcoin which relies on the premise that honest miners are willing and able to spend more resources than potential attackers at any time.

Related Literature. The paper contributes to various strands of the literature. First and foremost, it is related to recent work on mining and security in PoW-based cryptocurrencies. A number of papers provide micro-foundations of miner incentives to attack a blockchain. Budish (2024) studies majority attacks in Bitcoin to either double spend coins or willfully sabotage the network, and emphasizes the large economic costs to achieve decentralized trust. Similarly, Auer (2019) studies payment finality in PoW-based cryptocurrencies. He conducts an analysis of majority attacks and concludes that absent changes, Bitcoin will be subject to large trading frictions or low levels of security when mining income will mostly consist of transaction fees. Our results confirm that already in the past, security concerns have substantially affected Bitcoin's decentralized payment system and its price. Garratt and van Oordt (2023) show that fixed costs to mining equipment and the reliance on mining-specific hardware generally discourage double-spending attacks and hence increase security. We rely on some of the implications of their modeling framework to refine our empirical strategy and sharpen structural identification.

Some recent work embeds security considerations into cryptocurrency valuation frameworks. Most directly we build on the model in Pagnotta (2022) in which Bitcoin's price and the network's security are jointly determined due to the possibility that outside attackers sabotage the system, giving rise to multiple equilibria. One implication is that security levels can amplify how demand and sentiment shocks affect Bitcoin prices.[5] We extend his model and shift the focus to mining not as a propagator but as a source of shocks. Relatedly, Chiu and Koeppl (2022) model the race between honest miners and an attacker attempting to double-spend bitcoins. They show that there is trade-off in PoW cryptocurrencies between security and transaction throughput. Sockin and Xiong (2023) present a model of utility tokens. The possibility of strategic attacks by miners exacerbates fragility because users anticipate future transaction hurdles that depress the token's resale value. As a result, prices vary with marginal costs of mining. Consistent with this prediction, we present evidence that mining affects security and thus the transactional benefits that accrue from PoW-based cryptocurrencies.

Our econometric analysis is related to the growing empirical literature on cryptocurrencies. We focus on one particular driver of Bitcoin price dynamics – mining – and contribute methodologically by applying macro-econometric techniques for identification. Liu and Tsyvinski (2020) conduct a comprehensive analysis of cryptocurrency returns, which they also relate to mining fundamentals. They do not, however, identify structural shocks which we argue is essential to disentangle endogenous from exogenous variations in mining effort. Other non-structural analyses of Bitcoin price dynamics and mining are

[5]Similarly, price-hashrate spirals amplify demand shocks in Pagnotta and Buraschi (2018).

in Bhambhwani et al. (2023), Garratt and van Oordt (2023) and Ciaian et al. (2021).[6] Scharnowski and Shi (2021) study a specific incident that affected mining outcomes in China in 2021, which is also analyzed in Stinner and Tyrell (2022). We also study exogenous variation to mining efforts, but identify many more such events. Using these events as external instruments in a proxy VAR model, we can identify structural mining shocks and study their dynamic propagation in the Bitcoin network, including their impact on valuations. Other empirical analyses of Bitcoin prices unrelated to mining can be found in Makarov and Schoar (2020), Liu et al. (2022), Griffin and Shams (2020) and Karau (2023). Foley et al. (2019) and Makarov and Schoar (2021) feature detailed analyses of blockchain data to study questions related to user behavior, including miners. Halaburda and Yermack (2022) analyze market valuations of listed mining companies. Benetton et al. (2022) look at disruptions in local economies from the electricity usage of close-by mining firms.

Our analysis is also related to the theoretical literature studying the economics of mining in cryptocurrencies without a focus on attack or security considerations. Biais et al. (2019) analyze strategic behavior among miners and incentives to maintain consensus. Easley et al. (2019) study the determination of fees in Bitcoin and show that they are independent of the size of block rewards. Similarly, Huberman et al. (2021) explore the role of fees when market participants are heterogeneous in their urgency to transact. They show that Bitcoin's design protects users from monopoly power in the sense that no miner can affect fees in equilibrium. Our model and empirical analysis show that mining is important for Bitcoin's ability to function as a payment system, and by implication affects its price. Prat and Walter (2021) study the dynamics of entry to mining and show how aggregate mining effort is influenced by technological developments in mining hardware and changes in Bitcoin's market price. A related analysis is in Ma et al. (2018) who stress the potential welfare costs arising from mining competition. In contrast, we focus on the link between mining and Bitcoin prices with the causality going from exogenous changes in mining to Bitcoin valuations. Further, Choi and Rocheteau (2021) develop a model in which private moneys are produced through costly mining but without the need to provide incentives to not manipulate the transaction record. Arnosti and Weinberg (2018) and Capponi et al. (2023) present a model in which miners have heterogeneous costs, leading to the concentration of mining power. While we focus on aggregate mining efforts in our empirical analysis, variations in the concentration of mining power could equally cause price movements through the channels we uncover.

Finally, there is a growing literature on price formation in cryptocurrencies and the economics of blockchains. In the model of Biais et al. (2023), cryptocurrency prices

[6] Of these, only Bhambhwani et al. (2023) is interested in the question we study, namely how changes to mining affect prices. Unlike us, however, they do not identify exogenous variation in mining but instead conduct a cointegration analysis. Garratt and van Oordt (2023) study the opposite relation from prices to mining, whereas Ciaian et al. (2021) do not relate mining outcomes to prices.

fluctuate with sunspot-driven extrinsic volatility. Cong et al. (2022) develop a token valuation framework in which there are feedback effects from adoption to token price. Chiu and Koeppl (2019) model settlement properties of securities trading in PoW blockchains. While the precise mechanism is different from the one we study, in their framework a similar trade-off is present: mining is costly and incentives have to be provided to avoid manipulation.

Outline. Section 2 features the empirical analysis. We first describe our data, model and identification approach in Section 2.1, and then present the main results in Section 2.2. In Section 2.3, we study state-dependence and time variation in the effects of mining shocks on Bitcoin valuations and provide several robustness results in Section 2.4 and in Appendix A. In Section 3, we interpret our results through the lens of a model which formalizes how variations in mining effort can affect Bitcoin valuations through the system's security. We present the model in Appendix B. Section 4 concludes.

2 Empirical Analysis

This section presents our main empirical analysis. We first describe our data as well as estimation and identification approach. We then present impulse response functions (IRFs) to structurally-identified mining shocks and assess their quantitative importance for explaining variation in Bitcoin prices by means of forecast error variance decompositions (FEVDs). After an analysis of state-dependent responses, we close by conducting a comprehensive set of robustness checks to validate our findings.

2.1 Data and Empirical Approach

Our main empirical model is a structural VAR that allows us to identify exogenous changes in mining intensity and trace their dynamic impact on several measures of Bitcoin trading and valuation.

Data. The baseline model consists of eight variables, as summarized in Table 1. The first four capture mining input, mining outcomes and mining rewards. The estimated total *hashrate* measures how many guesses miners perform in a certain amount of time to solve cryptograms, and is therefore a metric of the system's total mining intensity. The mining *difficulty* level represents how hard it is to find a hash that meets the protocol-designated requirement. Bitcoin's protocol stipulates that the difficulty is adjusted every 2,016 blocks (roughly two weeks) as a function of the average block confirmation time over that period. If cryptograms are solved more slowly than ten minutes on average, the difficulty is adjusted downwards, and vice versa. The median *confirmation time*, measured in minutes it takes to validate a transaction and add it to the blockchain, can be thought of as a metric of both mining effort relative to the system's difficulty level and of transaction demand. Transaction confirmation times can increase when either the hashrate falls relative to the difficulty level (such that block confirmation times increase) or when high demand for block space causes congestion.[7] The total U.S. dollar value of *mining fees* represents a source of mining income, to which miners might endogenously respond to. In addition, fees also respond to transaction demand as users tend to bid up fees in order to have miners preferentially include their transactions when there is congestion.

In addition to these mining-related variables we employ variables that capture trading outcomes and speculative interest in Bitcoin. The median *transaction size* in U.S. dollars and the total *number of transactions* in the blockchain measure transaction volume in the decentralized payment network.[8] Additionally, we use the number of Google search queries for the term "Bitcoin" as a proxy for outside investors becoming interested in Bitcoin as an investment. Finally, we add the price of Bitcoin in U.S. dollars as the primary variable of interest.

The data are taken from cryptocurrency data providers often used in applied work. As our primary source we rely on data from `coinmetrics.io` but make sure that our results are robust to using data from other providers. Following Sims et al. (1990), we estimate the model in levels to preserve possible cointegrating relationships in the data.[9] All variables enter in logs with the exception of transaction confirmation times, which are measured in minutes. All model specifications are estimated on weekly data from the beginning of July 2013 (shortly before the introduction of application-specific integrated circuits, ASICs) to the end of July 2022 and feature 12 lags, corresponding to one quarter. We choose the weekly data frequency for several reasons. First, this choice minimizes noise in the data which arises to the the randomness involved in solving cryptographic puzzles.[10] Second, weekly data do not suffer from potential day-of-the-week effects, see also Biais et al. (2023). Finally, we rely on weekly data as we cannot in all cases establish the precise day of the event we use in the construction of our instrument. We discuss robustness to the choice of sampling frequency in Appendix A.3.

[7]Pending Bitcoin transactions are collected in memory pools before miners add them to their blocks. If the number of pending transactions is larger than the available block space, the average time it takes for transactions to be added to the blockchain rises, even if block confirmation times do not change.

[8]These variables are based on blockchain data and apply heuristics that attempt to filter out within-entity transactions.

[9]For instance, Bhambhwani et al. (2023) find evidence of a cointegrating relationship between the price of PoW cryptocurrencies and their hashrates. We make sure that our main results also hold when specifying the model in first differences, see Section 2.4.

[10]Common cryptocurrency websites therefore `often suggest to use smoothed or weekly data`.

Table 1: Main variables used in the empirical analysis

Variable	Unit/transformation	Source
Hashrate	log TH/s	coinmetrics.io
Difficulty	log	coinmetrics.io
Transaction confirmation time (median)	minutes	blockchain.com
Transaction fees (total)	log USD	coinmetrics.io
Transaction size (median)	log USD	coinmetrics.io
Number of transactions	log	coinmetrics.io
Google web searches of "Bitcoin"	log index	Google trends
Bitcoin price	log USD	coinmetrics.io

Note. The table lists the variables included in the baseline VAR model, alongside their sources.

Estimation. We characterize the joint dynamics of the eight Bitcoin-related variables using a Vector Autoregressive (VAR) model which we estimate using standard Bayesian methods. Details are provided in Appendix A.4.

Identification. We seek to separate exogenous variations in mining intensity, which we label *mining shocks*, from the endogenous responses of miners to other shocks. Given free-entry in the mining market and in the absence of other frictions, the system's hashrate is expected to endogenously respond to changes in mining revenue which, in turn, is driven by the price of Bitcoin – the blue arrow in Figure 1.[11] To overcome this challenge, we make use of two distinct identification schemes. Our baseline approach is to construct an external instrument based on a narrative approach (Romer and Romer, 1989), and feed it into a proxy VAR model in the spirit of Mertens and Ravn (2013) and Stock and Watson (2018). We briefly outline this approach below and provide more details in Appendix A.4. As an alternative approach, we exploit timing constraints in the adjustment of mining equipment to identify shocks recursively, as detailed in an extensive robustness exercise in Section 2.4. Despite being econometrically very different, both approaches yield essentially the same results, highlighting the robustness of our analysis.

Following Mertens and Ravn (2013) and Stock and Watson (2018), one can use external instruments – sometimes called proxies – in a VAR to use information from outside the model to determine the extent to which unexpected variations in endogenous variables are due to a shock of interest, denoted as ϵ_t^m. We apply this approach to isolate variations in the hashrate's VAR residuals that are due to exogenous changes in mining. For an instrument series Z_t to be valid, it needs to be *relevant* and *exogenous*:

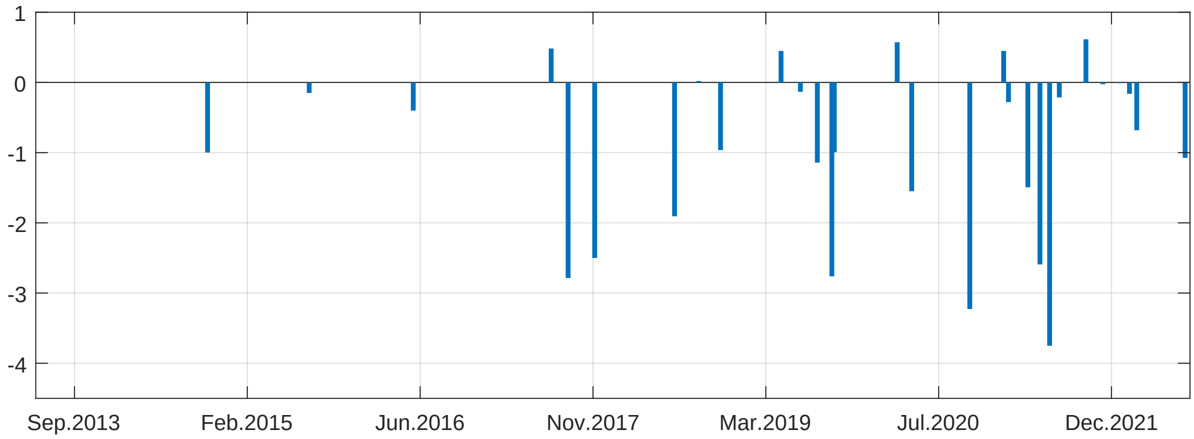
$$\mathbb{E}[Z_t \epsilon_t^{m\prime}] \neq 0, \tag{1}$$

$$\mathbb{E}[Z_t \epsilon_t^{q\prime}] = \mathbf{0}. \tag{2}$$

The condition in Equation (1) states that for an instrument Z to be relevant, it

[11] We provide evidence of causality running in this direction in Section 2.4.

Figure 2: Instrument used in the proxy VAR to identify mining shocks



Note. Instrument values result from the weighting scheme in Equation (3), such that the dimension of the instrument corresponds to (negative) deviations in minute from the 10-minute goal stipulated in the Bitcoin protocol.

needs to be (strongly) correlated with the structural shock ϵ_t^m. The second condition in Equation (2) requires that the instrument be exogenous and thus uncorrelated with shocks ϵ_t^q that are not related to mining.

We operationalize this idea by collecting a list of events that are likely to have had a sizable impact on mining intensity but were plausibly due to exogenous events rather than a response by miners to price changes. These events include natural disasters such as floods and fires that destroyed large mining farms, heat waves and storms that caused mining farms to go offline due to power outages, other changes in weather conditions that affected mining in Chinese provinces (that for a long time were home to the majority of mining activity), as well as large-scale seizures of mining hardware or the closing of entire mining farms by authorities. In total the list comprises 31 events, as described in Table A.1, along with their assigned instrument values.

In our baseline analysis, we construct shock values based on a weighting scheme in the spirit of Baker and Bloom (2013). This has the advantage that we can include information on how impactful each event has been. Precisely, we specify:

$$Z_t = (\Delta\text{block confirmation time}_t) \times \mathbb{I}, \tag{3}$$

in which $\Delta\text{blocktime}_t$ is the time in minutes it took for the average block to be added to the chain, expressed in deviations from the ten-minute target.[12] The idea is that large shocks to mining should have a large impact on the time it takes for cryptograms to be solved, given a certain difficulty level. The quantitative change in block confirmation

[12] We use daily data on block confirmation times (obtained from `www.coinmetrics.io`) in those cases for which we can time the event precisely, and use weekly averages otherwise.

times will therefore provide a measure of how substantial a mining event was.[13] Moreover, if the change in block confirmation times goes in the wrong direction – for instance an increase after an event that should have a positive impact on mining intensity – we discard the event altogether. We therefore only keep events in which the block confirmation time response aligns with our assessment of the sign of the shock, captured by the indicator variable $\mathbb{I}$ in Equation (3). This results in the removal of two events in the baseline specification.

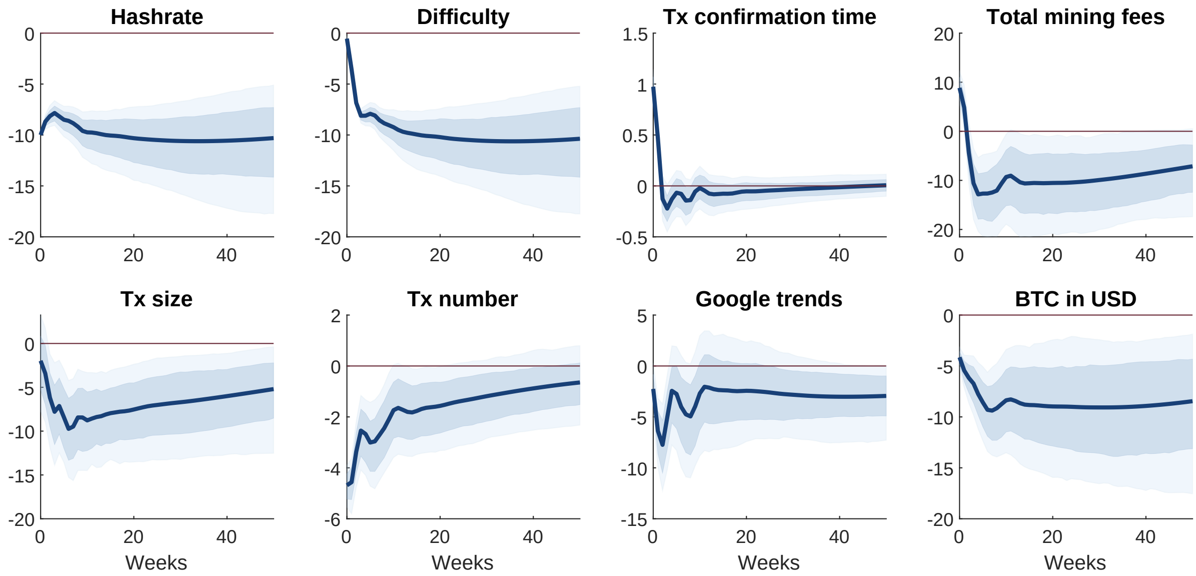
Figure 2 shows the resulting instrument series that we use in our baseline specification. Mining-related incidents occur throughout the sample, although we observe more events in recent years. Due to the weighting scheme, we can interpret the size of the values as deviations in minutes from the ten-minute goal. Two important incidents occurred in August and November 2017. These were related to the hard fork of Bitcoin Cash (BCH), which resulted in competition for mining effort between the two cryptocurrencies. Other particularly important events are specific to China as the long-term dominant mining domicile (see e.g. Cambridge Centre for Alternative Finance, 2021). They include the flooding of mining farms in the summer of 2018, COVID-19-related restrictions in the migration of Chinese miners in December 2020, the flooding of a coal mine in April 2021, as well as shutdowns of entire mining farms in the context of the Chinese mining ban in mid-2021. We discuss the choice of events in more detail in Section 2.4 and show that our results are robust to excluding various sets of events, either with respect to their category or period of time. In addition, we consider alternative weighting schemes (e.g. simply classifying the incidents to be either positive or negative and form an indicator variable). No matter the precise specification, our instruments are strong, as indicated by first-stage F-statistics greater than 30 when regressing the instrument on the hashrate residuals.

2.2 Main Results

The impact of mining shocks. Figure 3 shows impulse response functions (IRFs) to a contractionary mining shock in our proxy VAR model. The exogenous decrease in mining intensity leads to a highly persistent fall in the network's hashrate. This persistence is likely due to the path-dependence in mining effort that arises due to the endogenous difficulty adjustment. Initially, the exogenous decrease in mining intensity is associated with a rise in the time it takes to solve the cryptograms. This leads to a drop in the difficulty level, as shown in the second panel. Absent any further shocks, this decline is very long-lived and the hashrate persistently remains below its initial level.

[13] We also experiment with other weighting schemes that take into account differences of block confirmation times over longer horizons or make use of changes in difficulty adjustments. These approaches yield similar results.

Figure 3: Impulse response functions (IRFs) to a negative mining shock



Note. Impulse responses to a mining shock identified in the proxy VAR, normalized to decrease the hashrate by 10 percent. Shaded areas denote 68% and 90% confidence bands. All values in percent(age points), except for transaction confirmation time, which is measured in minutes. Time sample: July 2013 to July 2022.

The endogenous difficulty adjustment also explains the impulse responses of transaction confirmation times in the third panel. They rise on impact, but the effect vanishes as the system's difficulty adjusts. After this adjustment, confirmation times even drop slightly below their initial level, likely reflecting a fall in the demand for block space. This is consistent with the response of transaction fees in the fourth panel. Fee income from mining rises significantly on impact but decreases strongly and persistently thereafter. While the short-lived increase is again caused by slower processing of transactions until the difficulty adjustment is completed (Huberman et al., 2021; Easley et al., 2019), the protracted subsequent fall likely signals reduced transaction demand.

This interpretation is corroborated by a decline in the variables directly measuring transfer activity within the blockchain. Both the size as well as the number of transactions decrease persistently. Finally, and most importantly, the price of Bitcoin declines persistently and remains lower for many months after the initial shock. Hence, exogenous variations in mining activity exert a long-term impact on the price of Bitcoin.

We interpret these impulse response functions as evidence of two channels through which mining shocks impact the system. First, there is a *transaction speed channel* by which mining affects settlement speed. Higher blockchain congestion leads to higher fees, which makes it more costly to use Bitcoin to transfer value. This channel is short-lived, however, as it is shut off by the endogenous difficulty adjustment after at most two weeks. The fact that fees, blockchain activity and prices all continue to be affected long after this adjustment points instead to a second mechanism: mining fundamentals impact Bitcoin market valuations via a *security channel*. Before providing more evidence in favor of this channel in Section 2.3, we now quantify the extent to which variation in prices is explained by mining shocks.

Share of variation explained by mining shocks. A useful feature of our empirical framework is that it allows us to compute forecast error variance decompositions (FEVDs) to assess the quantitative importance of mining shocks for explaining variation of Bitcoin prices and the other endogenous variables in the VAR. Figure 4 shows the results. Most variation in the hashrate is explained by the mining shock in the week in which the shock occurs, with the share gradually falling to 50 percent over longer horizons. This shows that our identification approach captures the main drivers of mining effort. The same is true with respect to difficulty adjustments: as expected, the explained variation on impact is zero, but rises sharply with the two-week adjustment, and then stays persistently high.

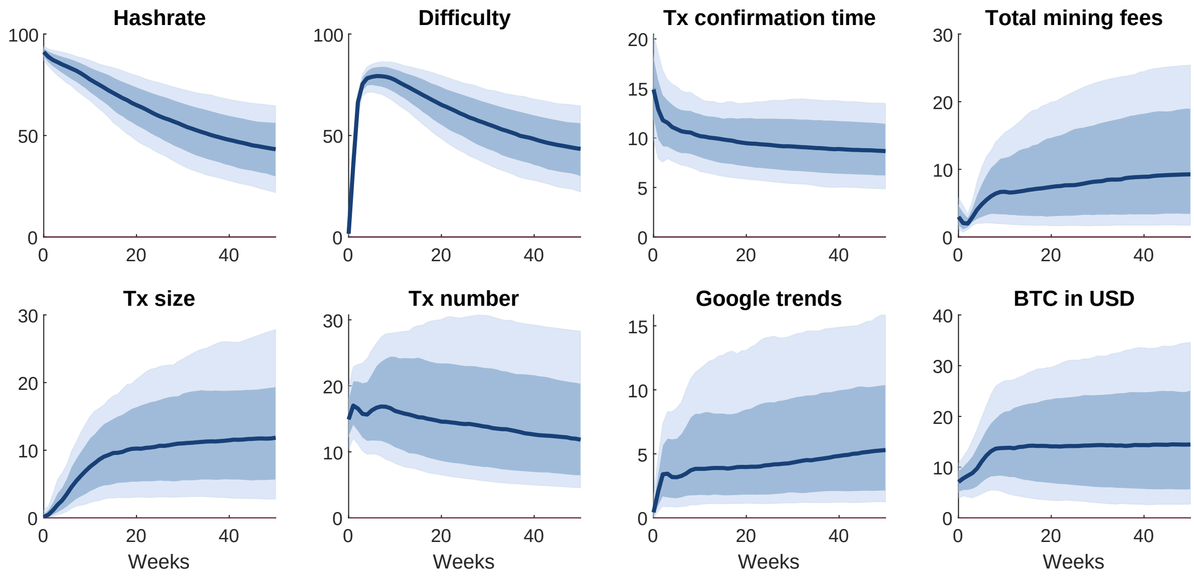
Initially, around a quarter of transaction confirmation times are captured by the mining shock, a share that drops quickly after the endogenous difficulty adjustment. The explained shares of mining income from fees is about ten percent in the medium run. Similarly, more than ten percent of the variation of the size and number of blockchain transactions is explained by the mining shock even a year later, confirming that exogenous changes to mining effort have quantitatively meaningful long-lived effects on the use of Bitcoin. Finally, and most importantly, mining shocks account for about 15 percent of the variation in Bitcoin prices at horizons up to one year. These shocks thus represent an economically significant source of Bitcoin's substantial price volatility.

2.3 Additional Evidence for a Security Channel

In this section we refine our empirical strategy to study state-dependence in the response of Bitcoin prices to mining shocks. We have already established that the short-lived transaction channel – through which mining shocks affect transaction validation speed for at most two weeks – cannot explain sustained price effects of hashrate variations. The following results corroborate our interpretation of a second and quantitatively important security channel through which mining shocks exert a long-lived impact on the Bitcoin market.

The role of mining profitability. As argued in Garratt and van Oordt (2023), the presence of fixed costs has important implications for mining. Absent short-run adjustments in mining efficiency or costs, mining revenues and mining profitability are tightly interconnected. As the market price of Bitcoin determines the USD value of the newly minted coins (the coinbase rewards), a fall in the price lowers the present value

Figure 4: Share of forecast error variance explained by mining shocks (FEVD) in proxy VAR



Note. FEVD to mining shock identified in the proxy VAR. Shaded areas denote 68% and 90% confidence bands. Values in percent. Time sample: July 2013 to July 2022.

of installed mining hardware. The same is true for quadrennial halving events, after which coinbase rewards are cut in half. In these periods, the Bitcoin community pays particular attention to the hashrate, as investors try to assess the durability and resilience of miners.[14] A sustained high or even rising hashrate is then often seen as evidence that the mining industry is healthy and hence that the system will continue to provide enough incentives for high levels of security going forward.[15]

This provides us with a testable implication. As we will discuss in more detail in Section 3, mining shocks might not only affect the perceived risk of an attack today but can also inform investor beliefs about the future security of the network and hence the future value of Bitcoin. If this is correct, a given mining shock should lead to larger shifts in investor beliefs in periods of income stress – and therefore should be associated with larger price effects.

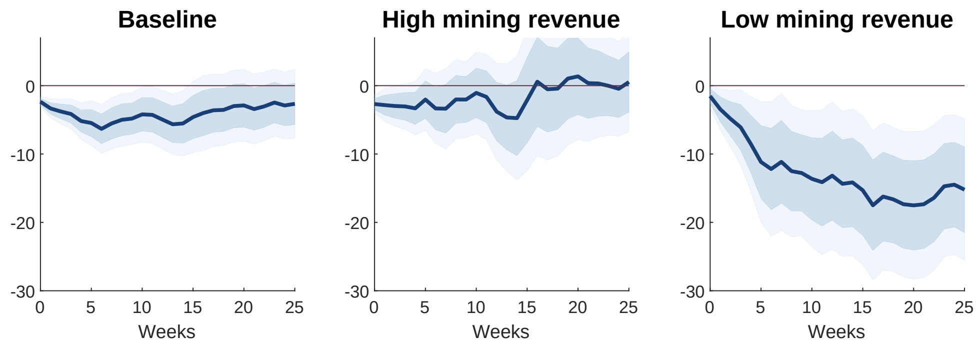
We test this prediction by running the following set of local projections that allow us to estimate regime-dependent impulse responses (Auerbach and Gorodnichenko, 2013; Falck et al., 2021):

$$y_{t+i} = \alpha_i + F(z_{t-1})(\beta_{i,L}\epsilon_t + \gamma_{i,L}y_{t-1}) + [1 - F(z_{t-1})](\beta_{i,H}\epsilon_t + \gamma_{i,H}y_{t-1}) + e_t, \qquad i = 0, 1, ..., I \tag{4}$$

[14]See for instance articles on cointelegraph.com before the halving in 2020, after which an article on decrypt.co noticed an initial "worrying post-halving dip".

[15]For instance, following the hashrate's recovery some time after China banned Bitcoin mining in 2021, a CNBC article quotes industry participants: "The bitcoin network withstood an attack by a major superpower and emerged stronger than ever six short months later."

Figure 5: Local projection IRFs of BTC price to a mining shock: mining revenue regimes



Note. Local projection IRFs to mining shock extracted from proxy VAR, as in Equation (4). Baseline response (left), response in high- (middle) and low- revenue regime (right panel). Values in percent. Shaded areas denote 68% and 90% confidence bands.

in which i denotes the forecast horizon, y_t is the log price of Bitcoin and ϵ_t is the mining shock identified in the proxy VAR.[16] The regime-dependent parameters $\beta_{i,L}$ and $\beta_{i,H}$ estimate the response of Bitcoin's price to a mining shock when mining income is low and high, respectively. The function $F(z_{t-1}) \in [0, 1]$ indicates the probability of being in the low-income regime with z_{t-1} measuring a drop in mining revenues. Following the literature, we specify $F(z_{t-1})$ as a logistic function that allows for a smooth transition between states (Granger and Teraesvirta, 1993):

$$F(z_{t-1}) = \frac{exp(\theta \frac{z_{t-1}-c}{\sigma_z})}{1 + exp(\theta \frac{z_{t-1}-c}{\sigma_z})}, \tag{5}$$

where c and σ_z are the median and standard deviation of z_{t-1}. The parameter θ determines the shape and steepness of $F(z_{t-1})$. We set $\theta = 1.5$ as in Auerbach and Gorodnichenko (2013) but our results are robust to a wide range of parameters.[17] As regime-indicating variable z_{t-1} we use short-run changes in the *hashprice* (mining revenues per hash per second) in USD terms that we obtain from `coinmetrics.io`.[18] While this series features a downward trend due to improvements in mining hardware – which we address below –, short-term changes in the series mostly reflect shifts in mining profitability arising from variations in the market price of Bitcoin and transaction fees, difficulty adjustments as well as halving events.

Figure 5 shows the results. The left panel depicts impulse responses of the market

[16] As suggested by Montiel Olea and Plagborg-Møller (2021), we include lagged values of the dependent variable on the right-hand side of the regression to ensure robust inference. Adding other variables as controls is not necessary (these are already accounted for as the structural shocks are derived from the residuals of the VAR that includes all covariates); doing so hardly affects results.

[17] We experiment with values ranging from as low as 0.5 to 5 and confirm our results throughout.

[18] We use percentage changes over the previous four weeks but our results are robust to varying the time frame, for instance from one-week to six-week changes.

price of Bitcoin to mining shocks without differentiating between regimes. The finding of a negative and significant response serves as a further robustness check to our main results and as a benchmark for the regime-specific responses in the other two panels.[19] The middle panel shows that the effect in a high-revenue regime is considerably smaller and short-lived than in the baseline case, in line with the prediction that investors do not perceive variations in the hashrate as indicative of a shift towards a lower-security equilibrium. Conversely, the effect of a mining shock in a low-revenue state (right panel) is substantially larger and more persistent. A decline in the price of Bitcoin, say, or a halving event makes mining less profitable and reinforces investor concerns about the future state of the network. As we outline below in SECTION 3, a given exogenous change in the system's hashrate can then reinforce the downward spiral towards a possible lower-security equilibrium and hence has a more pronounced effect on Bitcoin valuations.[20]

THE ROLE OF MINING HARDWARE UPGRADES. The previous exercise relied on the idea that the effects of mining shocks should vary with mining income as low-profitability periods are those that investors are concerned about when assessing the likely future state of the system. We exploit the fact that the same is true with respect to periodic advances in mining hardware technology. For instance, following the initial employment of application-specific integrated circuit chips (ASICs) in 2013, the development of different variants of the widely-used Antminer rigs represented major improvements in mining hardware. As these newly released circuits are often capable of performing many more hashes per second than previous generations, the phasing in of new hardware means that already-installed mining rigs become less competitive. If not all honest miners can pay the fixed costs for upgrading their hardware, these periods then represent an opportunity for a malicious actor to buy into the market and compete. To the extent that this raises security concerns, mining shocks should have larger valuation effects also in these periods.

We test this prediction by running local projections as follows:

$$y_{t+i} = \alpha_h + \beta_{i,1}\epsilon_t + \beta_{i,2}(\epsilon_t \times M_t) + \gamma_{i,M}M_t + \gamma_{h,y}y_{t-1} + e_t, \quad i = 0, 1, ...I, \tag{6}$$

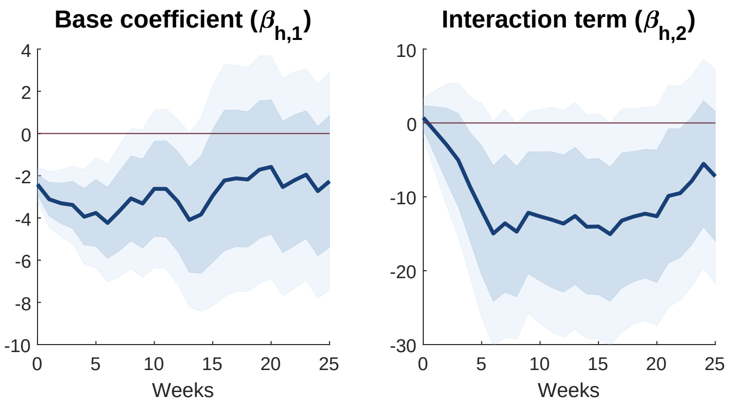
in which y_t and ϵ_t are again the log price of Bitcoin and structural mining shocks extracted from the VAR, respectively. M_t is an indicator variable equal to one if there there was a major release of new mining hardware in the current or previous six weeks, and zero otherwise.[21] To construct M_t, we use the list of 13 hardware releases in Ciaian et al. (2021) that fall in our time sample and which we reproduce in TABLE A.2. Hence, in contrast

[19] As we normalize the structural shocks, the size of the effect is not comparable to that in the VAR.

[20] These results are also consistent with the view that incentives for honest behavior among miners fall following a decline in mining revenues, and hence that double-spending attacks become more likely.

[21] We obtain similar results when varying the number of weeks. While the effect gets weaker for longer time frames, we obtain a statistically significant interaction term for up to ten weeks time spells.

Figure 6: Local projection IRFs of BTC price to a mining shock: interaction with mining hardware upgrades



Note. Local projection IRFs to mining shock extracted from proxy VAR, as in Equation (6). Baseline response (left) and response of interaction coefficient (right panel) with major hardware release as described in main text. Values in percent. Shaded areas denote 68% and 90% confidence bands.

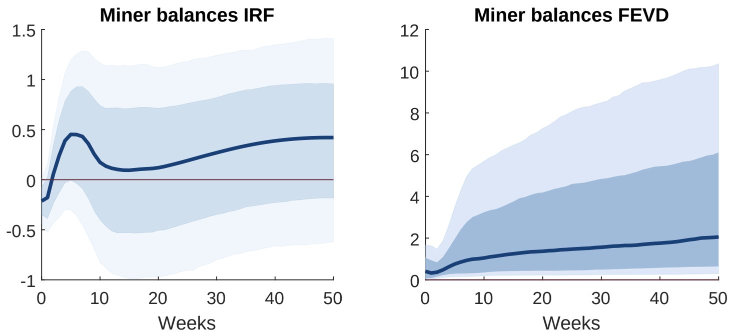
to specification (4) we do not identify different regimes as we lack a regime-indicating variable that varies continuously. Instead, we construct two sets of impulse responses: the $\beta_{i,1}$ coefficients measure the baseline responses to mining shocks. The $\beta_{i,2}$ coefficients on the interaction term, in turn, measure to what extent the price responsiveness to mining shocks differs in periods when new mining hardware was just released.

Figure 6 provides the results. As a confirmation of the main findings, the left-hand panel shows a statistically significantly negative price impact of an exogenous fall in mining effort. More importantly, the right-hand panel reveals that prices are indeed roughly three times as sensitive when new mining hardware has just become available, in line with the notion that the system is more vulnerable to attack.

Cashing out of miners. As a final exercise we study an alternative, and possibly complementary, explanation for the price effects of mining shocks: the cashing out behavior of miners. In their detailed study of the Bitcoin blockchain, Makarov and Schoar (2021) observe that miners sometimes accumulate substantial sums of coins. When miners come under income stress they might sell accumulated coin holdings, thus contributing to downward pressure on the price of Bitcoin. As they disturb or prohibit mining operations, income stress might also be caused by negative mining shocks. It is therefore important to assess to what extent our results could be driven by the cashing out behavior of miners.

To do so we rely on estimates by `glassnode studio`. Specifically, we add to our baseline VAR model their (logged) series on the number of coins that are held by entities that are identified and labeled as miners. While it is generally difficult to measure the activity of specific on-chain entities with precision, identifying miners is facilitated by the

Figure 7: IRFs and FEVD of miner balances



Note. Impulses responses to a mining shock normalized to decrease the hash rate by 10 percent (left) and forecast error variance decomposition (right) of miner balances added to the baseline model (Figures 3 and 4). Values in percent. Shaded areas denote 68% and 90% confidence bands.

fact that coinbase rewards, the newly minted coins that accrue to miners, are easily visible in the blockchain. We nonetheless note that the employed data series likely tracks only a part of all miner holdings. The results should, however, provide a solid indication of whether coin holdings are systematically liquidated when miners are hit by the identified shocks.

Figure 7 shows the impulse response and forecast error variance decomposition of miner balances to a negative mining shock.[22] In line with the notion that miners cash out some of their coin holdings following such a negative shock, miner balances fall on impact (left panel). However, the response is very short-lived, hardly significantly different from zero and quantitatively small, with miner balances falling only by less than half a percent – not even one tenth of the impact response of the price of Bitcoin to the shock. The variance decomposition in the right panel paints a similar picture: mining shocks account for only a very small fraction of variation in miner balances throughout. We conclude that cashing out behavior by miners following mining shocks is unlikely to account for the substantial price effects of mining shocks we document.

2.4 Robustness and Additional Findings

In this section we provide robustness checks along several dimensions, including variations of the VAR model, instrument choice, estimation methods and identification schemes.

Model specifications and impulse response estimation. We verify that our main results are robust to varying the number of lags in the baseline VAR and using flat instead of standard Minnesota-type priors. We also confirm that our main results hold

[22]Results for the other eight variables in the model look essentially identical to the main results in Figures 3 and 4.

when specifying the hashrate and the price of Bitcoin in log differences rather than log levels. Even specifying all potentially non-stationary series in first differences leaves our main result unaffected – mining shocks have significant price effects.[23]

External instrument: choice and weighting of events. The process of constructing the instrument naturally involves some discretion on the part of the researcher in choosing relevant events. We took care to only include events that were not clearly too small to have had any plausible effect on aggregate mining or that stretch over an extended period and are hence difficult to time. However, given the importance for identification in the proxy VAR, we here discuss additional potential concerns regarding the set of events.

Importantly, our identification does not rely on the assumption that the events capture only mining-related external factors that impact the Bitcoin market. Instead, it only requires that the instrument series does not *systematically* take up such variation. For instance, on 9 June 2021 the Chinese Qinghai province ordered local mining operations to halt – a negative mining shock –, while on the same day El Salvador's Congress voted to adopt Bitcoin as legal tender – arguably a positive sentiment/demand shock, which sent Bitcoin prices sharply higher. Including this event will not undermine identification as long as the other events do not systematically correlate with similar confounding factors.

Another potential concern relates to the potential endogeneity of some of the events. For instance, a crackdown on mining by Iranian authorities related to excessive energy consumption could to some extent be an indirect response due to a rise in Bitcoin prices in so far as this had sparked higher mining activity in the region in the first place. We note that such endogeneity would only unduly inflate our estimated price response to the extent that it was *systematic* and introduced *positive* correlation between prices and hashrate. As crackdown events are expected to reduce, not further increase, aggregate mining activity, falsely including such events in the absence of any effects on prices would only attenuate, and not amplify, our results.

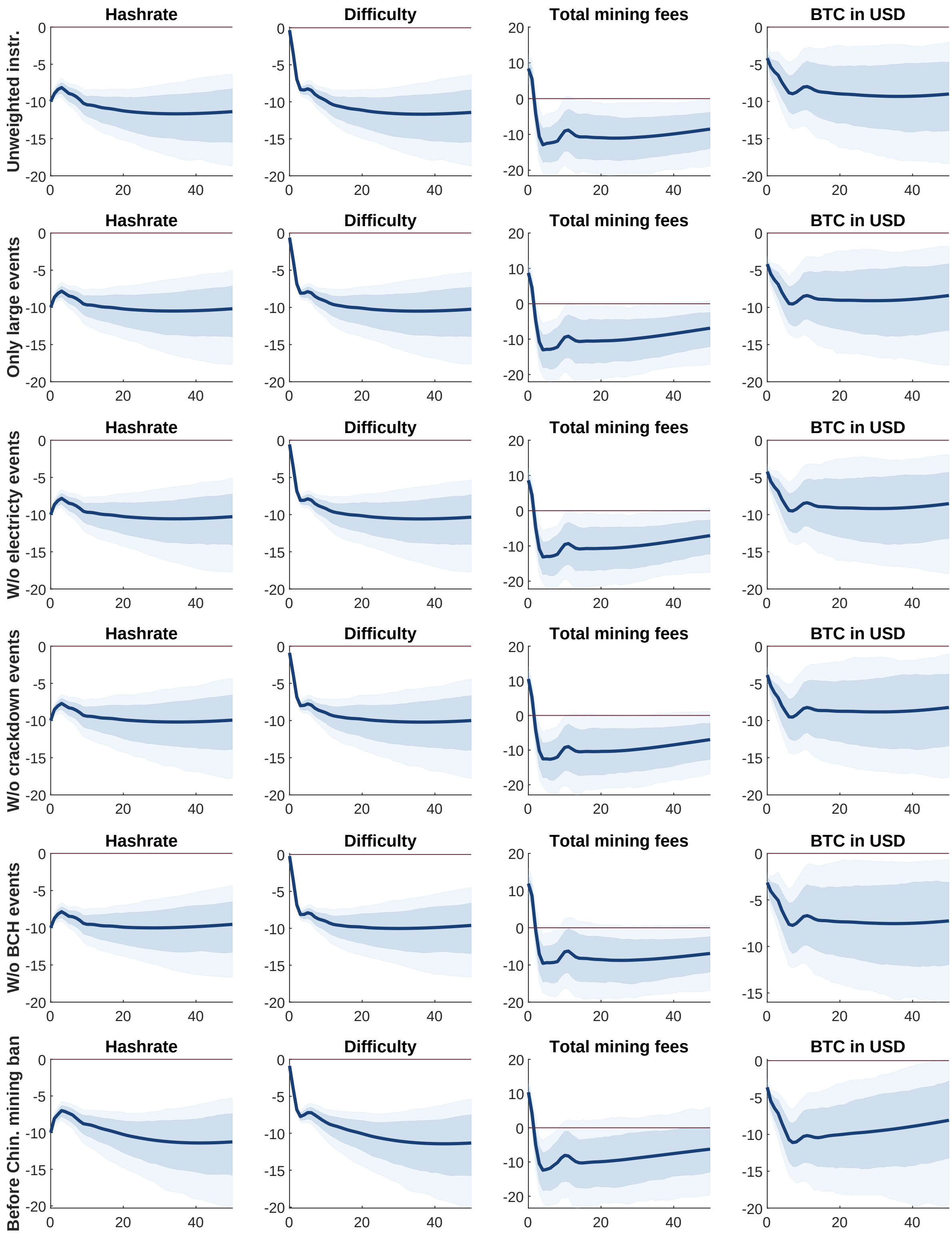
In addition to these general considerations, we run several robustness checks to make sure that our results are not driven by a certain type of events or particular episodes, as summarized in Figure 8. In order to preserve space, we only report responses of the mining-related variables and the price of Bitcoin.[24]

The first row shows results when using an unweighted instrument, where positive (negative) events get assigned a 1 (-1) and all other weeks a 0. One potential advantage of using this simple indicator instrument lies in the fact that the baseline weighting scheme might fail to capture exogenous mining variation if in a certain week other shocks

[23]The uncertainty bands for most of the other variables become much wider, ruling out any analysis of the propagation channels.

[24]The other impulse responses also do not change much compared to the baseline results.

Figure 8: Robustness: IRFs with varying instruments



Note. Impulse responses to a mining shock identified in the proxy VAR, normalized to decrease the hash rate by 10 percent, with varying instruments. All values in percent(age points). Shaded areas denote 68% and 90% confidence bands.

that drive block confirmation times in a direction inconsistent with the assigned sign of the mining shock. The figure shows that results are hardly changed when using the unweighted instrument.[25]

The second row shows results when using an instrument that only includes large, impactful events. As described in Detail in Appendix A.3, solving cryptograms involves randomness such that some variations in the measured hashrate are to expected even in the absence of any actual changes in mining effort. To ensure that the instrument does not merely pick up such noise, we exclude those events for which block confirmation times fail to show statistically significant deviations from the ten-minute average. We determine the corresponding threshold values by simulating the solving of 50,000 cryptograms and end up including only 15 events for which block confirmation times lie two standard deviations above or below ten minutes. As shown in the second row, results hardly change.

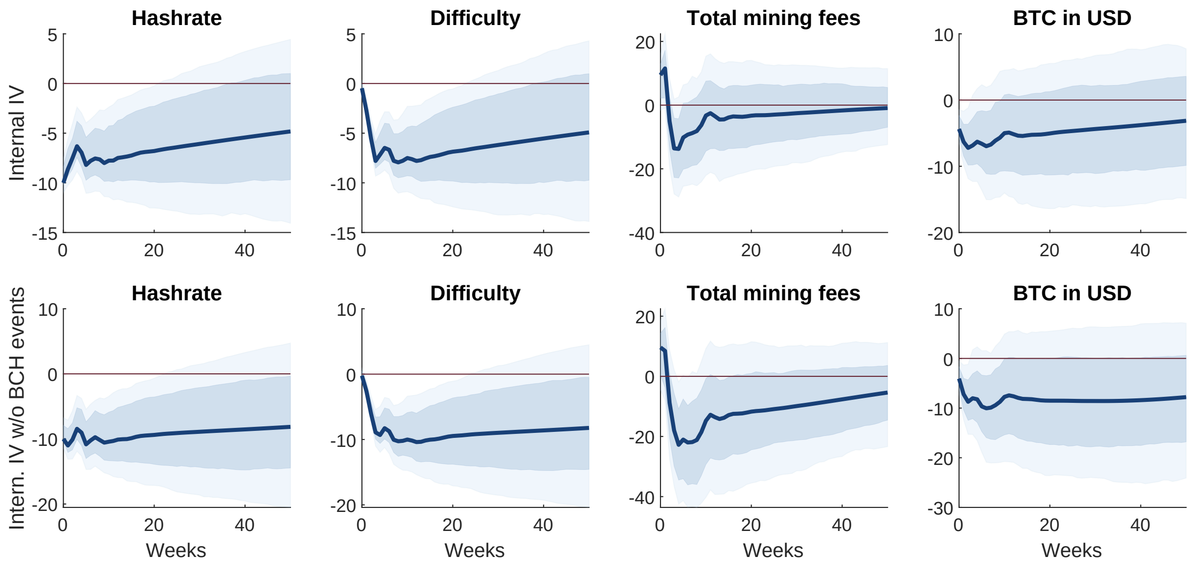
Moreover, impulse responses look very similar when excluding all events related to the change of electricity prices in important Chinese provinces (third row) or crackdown events where mining was banned and/or hardware was confiscated by local authorities (fourth row). The same is true when removing two events that are related to the creation of Bitcoin Cash (BCH) in mid- to late-2017. As a result of the *blocksize wars*, Bitcoin Cash was created as a hard fork of Bitcoin. As both protocols are based on the SHA-256 hashing algorithm, miners could solve cryptograms for both cryptocurrencies using the same hardware. Following the lowering of the BCH-difficulty, in August and November 2017 Bitcoin miners for some time switched to mining Bitcoin Cash, resulting in massive spikes in block confirmation times in Bitcoin. These events could potentially not only capture concerns about mining but broader changes in sentiment towards Bitcoin versus its newly created offshoot. Reassuringly, impulse responses are very similar to the baseline results when excluding these two events (fifth row). The last row in Figure 8 confirms our results when estimating the model only until April 2021, i.e. when entirely excluding the Chinese mining ban in mid-2021. Our findings are therefore not driven by this single episode – arguably the most impactful disruption to Bitcoin mining to date.[26]

Finally, we note that our main results also hold using an internal instrument VAR instead of an external instrument (proxy) VAR following the approach in Plagborg-Møller and Wolf (2021a) and Miranda-Agrippino and Ricco (2023). As these authors show, directly including the instrument in the VAR and ordering it first in a recursive identification scheme does not require an invertibility assumption, which sometimes may not hold in practice. On the other hand, this approach is less flexible since it treats the instrument as the underlying structural shock of interest, assuming that the shock is measured

[25] We also verify our results when we compute the instrument weights from changes in the hashrate itself, i.e. when we replace $\Delta \text{blocktime}_t$ with $-\Delta \text{hashrate}_t$ in Equation (3).

[26] With this robustness check we also address a related concern around an event in mid-May 2021, when a partial Chinese mining ban was first announced. Although there were several other mining-related instances in China and other countries in the same week, Bitcoin trading was further restricted in China – which might have had an independent impact on Bitcoin prices.

Figure 9: Robustness: IRFs with internal IV



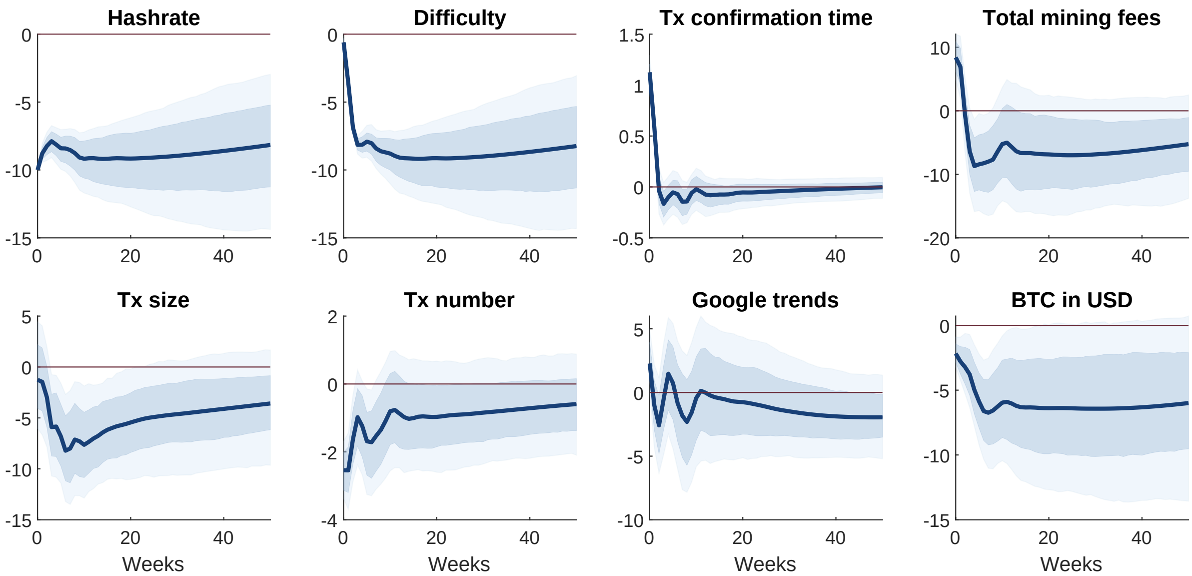
Note. Impulse responses to a mining shock identified in an internal IV model, normalized to decrease the hash rate by 10 percent. Lower panel leaves out two events around the Bitcoin cash (BCH) hard fork in mid- and end-2017. All values in percent(age points). Shaded areas denote 68% and 90% confidence bands.

exhaustively and without measurement error. As shown in Figure 9, the IRFs based on the internal IV approach are very similar to the baseline results (first row), and even more so when we exclude the two short-lived events related to the hardfork of Bitcoin Cash (second row).

Recursive identification of mining shocks. In principle, miners should continuously adjust their activity in response to changes in mining revenue. In reality, however, various frictions likely lead to delays in this adjustment. A case in point is the period from late 2017 until mid-2018. While the price of Bitcoin was on a downward trend since its late-2017 peak, mining intensity and the system's difficulty kept increasing until late August 2018 (Auer, 2019). Such a delayed response is likely the result of two particularities of Bitcoin mining. First, ordering and installing new mining equipment takes time, sometimes weeks or months. An immediate adjustment to changes in revenue is therefore only possible if previously installed hardware is switched off (or later on again). Second, mining equipment has a substantial fixed cost component and is highly specialized such that it cannot simply be repurposed. Here, we exploit this fact to motivate an alternative identification scheme.

As detailed in Garratt and van Oordt (2023), taking into account the non-reusable nature of mining rigs has important implications for the response of miners to fluctuations in prices as it introduces downward rigidity. Since miners seek to recover the fixed costs incurred from installing new mining hardware, small to moderate drops in revenue will

Figure 10: Robustness: IRFs to a negative mining shock identified recursively



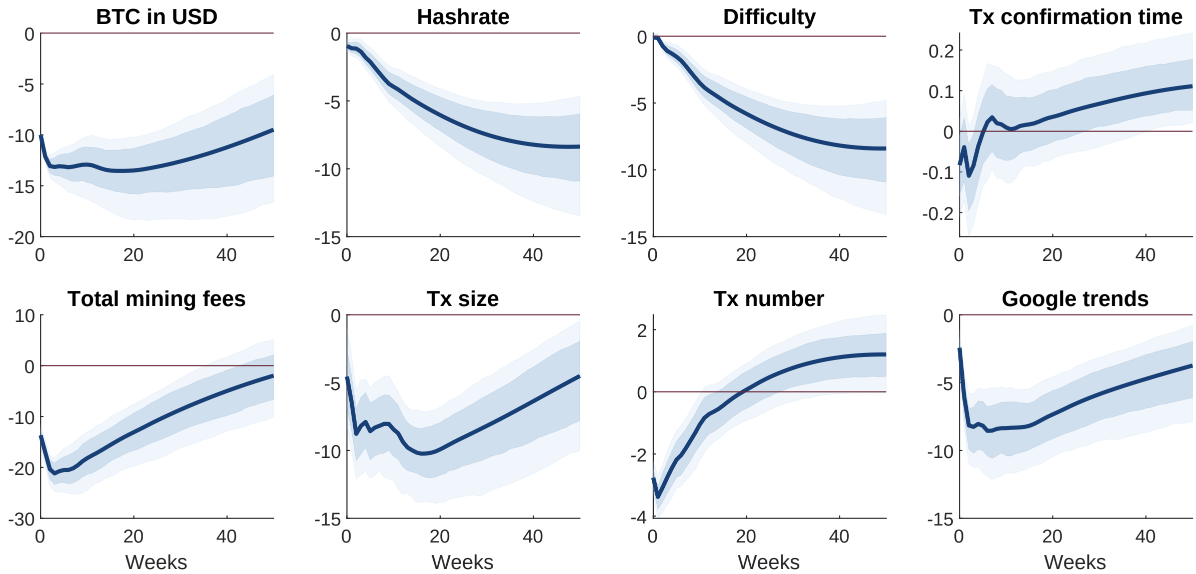
Note. Impulse responses to a mining shock identified in recursive VAR with logged hashrate ordered first, normalized to decrease the hash rate by 10 percent. All values in percent(age points), except for transaction confirmation time, which is measured in minutes. Shaded areas denote 68% and 90% confidence bands.

typically not lead them to switch off their equipment. Indeed, Makarov and Schoar (2022, p.7) note that Bitcoin miners "usually operate close to full capacity", and media coverage of mining farms attest the validity of this notion.[27]

Taking these considerations into account, our alternative identification scheme orders the hashrate first in a recursive VAR. This approach is identical to the well-known “Choleski approach” popularized in monetary economics by Sims (1980). Here, it relies on the assumption that unexpected variations in total mining intensity from one week to the next are not due to a contemporaneous response by miners to changes in the other variables in the system. Instead, all variation in mining that is not accounted for by the autoregressive structure of the endogenous model variables is either random or due to exogenous adjustments by miners which we seek to identify. In addition to its simplicity, an important advantage of this identification scheme is that all time series variation informs the shock identification, not just particular events at certain points in time as in our baseline approach. A second advantage is that this approach is not susceptible to concerns that the mining events used in the narrative approach may pick up variations in mining intensity that are due to other, non-mining-related drivers. Although we addressed these concerns above, the recursive identification therefore serves as an additional

[27]For instance, according to reports by CNBC and advancedmining.io, operators’ main concern is to make sure that all mining rigs run 24 hours a day, seven days a week, all year-round. A Bitcoin news report mentions that constant monitoring and the securing of a reliable source of energy are essential to avoid having any machines idle. A sustained drop in mining revenues, however, can cause miners to at least temporarily shut down operations.

Figure 11: IRFs to a negative "price shock" identified recursively



Note. Impulse responses to a "price shock" identified in recursive VAR with logged BTC price ordered first, normalized to decrease the price by 10 percent. All values in percent(age points), except for transaction confirmation time, which is measured in minutes. Shaded areas denote 68% and 90% confidence bands.

useful robustness exercise.

Figure 10 shows impulse responses to a recursively identified mining shock. Strikingly, despite the different identification assumptions, the responses are very similar to those obtained in our baseline approach in Figure 3. In particular, mining shocks are associated with a persistent decline of the hashrate and only a short-lived increase in confirmation times. Mining fee income falls on impact but then slowly recovers. We see similar dynamics for the size and number of transactions. Most importantly, mining shocks have a significant and persistent impact on Bitcoin prices. In Appendix A.2, we address potential endogeneity concerns and show that this result is not invalidated by failing to capture that miners may be switching on or off their equipment in response to large changes in Bitcoin's market price.

Recursive identification: feedback from prices to mining. As a final exercise we modify the recursive identification scheme and order Bitcoin prices first in the system of variables, i.e. we identify "price shocks". The idea here is not to identify and differentiate all the actual structural drivers that impact Bitcoin valuations. Instead, we think of these shocks as a shorthand of all factors that affect prices over and above what can be explained by the autoregressive model structure. This is useful for two reasons. First, it can be used to study feedback effects from prices to mining effort. Second, this serves as an additional plausibility check of our main results.

Figure 11 shows impulse responses to the price shock, normalized to lower Bitcoin valuations by 10 percent on impact. The shock is persistent and leads to decreased blockchain activity as measured by the number of transactions and their size, as well as how often Google users search for Bitcoin. Notably, the aggregate hashrate also declines after some delay, confirming our expectation that there is causality from prices to mining effort – the blue arrow in FIGURE 1 in the introduction ("*hashrate follows price*").

Importantly, the responses in FIGURE 11 further corroborate our identification of mining shocks. First, we see that the hashrate responds only little and sluggishly on impact. This validates our recursive identification scheme for mining shocks: in the short term, miners hardly respond to a shock that captures all the unexplained variation in Bitcoin prices. Second, the dynamics of the endogenous variables following a price shock are very different relative to the mining shock. In particular, fees and confirmation time responses do not switch signs after the two-week difficulty adjustment. Both of these observations make it seem unlikely that our baseline identification unduly assigns variation in the data to a mining shock which actually results from an endogenous hashrate adjustment via prices.

3 Discussion

In this section, we discuss our empirical results through the lens of a theoretical model in which shocks to mining activity have implications for the perceived security of the Bitcoin network and as such affect the price of Bitcoin. The model is a simple extension of the theoretical framework offered in Pagnotta (2022), which shows that potential sabotage attacks can give rise to multiple equilibria. We delegate all model equations to Appendix B, and instead focus on delivering the model's intuition here.

In the model, Bitcoin users are motivated to hold coins because they anticipate unique beneficial trading opportunities, contingent on the blockchain network remaining operational. Miners, incentivized by block rewards that depend on expected future Bitcoin prices, invest in computational power to secure the blockchain. The security of the system is determined by the relative computational power between honest miners and an attacker (saboteur) who aims to undermine the network by creating disruptive forks, thus destroying confidence and the value of bitcoins.

The existence of multiple equilibria emerges because users' valuation of Bitcoin and miners' investments in security reinforce each other. When users believe Bitcoins have high value, they hold larger balances, increasing their market price. As a result, they incentivize miners to commit more resources, thus increasing blockchain security and confirming users' positive beliefs. Conversely, low expectations lead to lower holdings, reduced mining efforts, lower security, and validation of pessimistic expectations. Consequently, the same economic fundamentals can support equilibria at both low-security, low-price and high-security, high-price levels.

The simplest way to extend the model is by introducing exogenous variation in the resources that honest miners employ. Starting from the high-value, high-security equilibrium, a negative mining shock lowers the hashrate employed to protect the system from the saboteur. Successful sabotage becomes more likely for any given price of Bitcoin. But as investors anticipate the lower levels of blockchain security, demand falls, which further lowers miners' incentives to invest. As a result, the equilibrium shifts downward, featuring lower levels of security and prices. This model extension therefore offers a simple way to rationalize the valuation effects of mining shocks that we have documented.

One avenue to also quantitatively account for the sizable effects would be to have mining shocks also impact equilibrium selection in a dynamic version of the model. Since future equilibria are outcomes of the strategic interactions between hashrate and price, any factor that influences one of these variables would alter the perceived probabilities of different equilibria occurring. This also fits the widespread discussions around the hashrate within the Bitcoin community. These discussions often do not so much focus on current attack risks but instead draw implications for the long-run viability of Bitcoin. A high mining intensity as measured by the hashrate is seen as a sign of a healthy state of the network, especially if the price of Bitcoin is significantly below a previous peak, or after exogenous disruptions.

A striking example is the Chinese mining ban in mid-2021. With the majority of hash power at the time being deployed in China,[28] the ban raised concerns whether it would be possible to relocate activities and operate under similarly favorable conditions elsewhere. If frictions in the migration process and higher electricity prices in other jurisdictions lowered miners' profitability, the result would be lower aggregate mining intensity. In the model context, a future high-security, high-value equilibrium would be less likely to come about or more difficult to sustain.

Yet, after an initial fall in mid-2021, the hashrate recovered. In all likelihood this process was aided by a boom in the price of Bitcoin in late 2021 coupled with an inflow of new investors in the context of the COVID-19 pandemic.[29] This made mining profitable even under otherwise less favorable conditions, and mining activity shifted to countries such as Kazakhstan, Russia, Iran and the United States. Through the lens of the model, a low-security, low-value equilibrium was avoided due to other exogenous factors.

[28] Widely-cited estimates suggest that on average almost 70% of Bitcoin mining was located in China between late 2019 and late 2020 and still above 50% in early 2021 (Cambridge Centre for Alternative Finance, 2021).

[29] See for instance Auer et al. (2023). There are even reports of pandemic stimulus funds being used to set up new mining operations in the US.

4 Conclusion

Do fundamentals impact Bitcoin market valuations? In this paper we attempt to answer this question by studying mining shocks – exogenous changes to the system's computational power devoted to validate new and secure existing transactions.

In the first part of the paper, we employ a structural vector autoregression to isolate exogenous variations in mining intensity. In addition to a short-lived transaction speed channel, we find evidence of a longer-lasting security channel, through which mining shocks have a significant and persistent impact on Bitcoin prices. Indeed, they account for up to 15 percent of Bitcoin's substantial price volatility. Additional analyses show that the effects of mining shocks on Bitcoin prices differ substantially across periods of high and low mining revenue and after the introduction of new mining technology.

In the second part of the paper, we rationalize our empirical findings in a theoretical framework building on Pagnotta (2022). The model features multiple equilibria that come about due to feedback effects between prices and blockchain security. Mining shocks can affect current attack risk but also shift investor expectations about whether the network will stay in a high-security, high-price equilibrium.

One way to read our results is that Bitcoin does, as argued by its proponents, derive some part of its market value from its unique approach to secure its transaction record in a decentralized manner. At the same time, our findings imply that this approach comes with vulnerabilities. Instead of being subject to a single point of failure as in centralized payment systems, users are subject to exogenous variations in mining intensity around the globe that introduce fluctuations in trading outcomes at the margin. Rather than smoothly running in the background, mining is not innocuous for Bitcoin's ability to function as a payment system, and by implications to its market price. Indeed, it is one additional source of Bitcoin's large price volatility.

Our findings have implications for the future of Bitcoin and other PoW-based cryptocurrencies. Some of the events exploited in our narrative identification approach involve incidents where mining hardware was confiscated by authorities due to concerns about its impact on local electricity provision. To the extent that concerns about high energy usage were to grow in the future, this might result in additional regulatory interventions. Similarly, the declining role of block rewards (Auer, 2019) or changes in the specificities of mining hardware (Budish, 2024) could undermine the incentives to provide mining effort for transaction validation. Our results suggest that this would not be without consequences for Bitcoin trading activity and its market valuation.

References

Arnosti, N. and Weinberg, M. (2018). Bitcoin: A Natural Oligopoly. *Conference Paper, 10th Innovations in Theoretical Computer Science Conference.*

Auer, R. (2019). Beyond the doomsday economics of 'proof-of-work' in cryptocurrencies. *BIS Working Papers*, 765.

Auer, R., Cornelli, G., Doerr, S., Frost, J., and Gambacorta, L. (2023). Crypto trading and Bitcoin prices: evidence from a new database of retail adoption. *BIS Working Papers*, 1049.

Auerbach, A. J. and Gorodnichenko, Y. (2013). Fiscal Multipliers in Recession and Expansion. In *Fiscal Policy after the Financial Crisis*, NBER Chapters, pages 63–98. University of Chicago Press.

Baker, S. R. and Bloom, N. (2013). Does Uncertainty Reduce Growth? Using Disasters as Natural Experiments. *NBER Working Papers*, 19475.

Benetton, M., Compiani, G., and Morse, A. (2022). When Cryptomining Comes to Town: High Electricity-Use Spillovers to the Local Economy. *Mimeo.*

Bhambhwani, S. M., Delikouras, S., and Korniotis, G. M. (2023). Blockchain characteristics and cryptocurrency returns. *Journal of International Financial Markets, Institutions and Money*, 86:101788.

Biais, B., Bisiere, C., Bouvard, M., , and Casamatta, C. (2019). The Blockchain Folk Theorem. *The Review of Financial Studies*, 32(5):1662–1715.

Biais, B., Bisière, C., Bouvard, M., Casamatta, C., and Menkveld, A. J. (2023). Equilibrium Bitcoin Pricing. *Journal of Finance*, 78(2):967–1014.

Bonneau, J. (2018). Hostile blockchain takeovers (short paper). *mimeo, New York University.*

Budish, E. (2022). The Economic Limits of Bitcoin and Anonymous, Decentralized Trust on the Blockchain. *Becker Friedman Institute Working Papers*, 2022-83.

Budish, E. (2024). Trust at scale: The economic limits of cryptocurrencies and blockchains. *The Quarterly Journal of Economics*, 140(1):1–62.

Cambridge Centre for Alternative Finance (2021). New data reveals timeline of china's bitcoin mining exodus. https://www.jbs.cam.ac.uk/2021/new-data-reveals-timeline-of-chinas-bitcoin-mining-exodus, accessed: 2025-03-20.

Capponi, A., Olafsson, S., and Alsabah, H. (2023). Proof-of-Work Cryptocurrencies: Does Mining Technology Undermine Decentralization? *Management Science*, 69(11):6455–6481.

Chiu, J. and Koeppl, T. (2022). The Economics of Cryptocurrencies: Bitcoin and Beyond. *Canadian Journal of Economics*, 55:1–37.

Chiu, J. and Koeppl, T. V. (2019). Blockchain-Based Settlement for Asset Trading. *Review of Financial Studies*, 32(5):1716–1753.

Choi, M. and Rocheteau, G. (2021). Money Mining and Price Dynamics. *American Economic Journal: Macroeconomics*, 13(4):246–294.

Ciaian, P., d'Artis Kancs, and Rajcaniova, M. (2021). Interdependencies between Mining Costs, Mining Rewards and Blockchain Security. *mimeo*.

Cong, L. W., Li, Y., and Wang, N. (2022). Token-based platform finance. *Journal of Financial Economics*, 144(3):972–991.

Easley, D., O'Hara, M., and Basu, S. (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics*, 134(1):91–109.

Eyal, I. and Sirer, E. G. (2013). Majority is not enough: Bitcoin mining is vulnerable. *CoRR*, abs/1311.0243.

Falck, E., Hoffmann, M., and Hürtgen, P. (2021). Disagreement about inflation expectations and monetary policy transmission. *Journal of Monetary Economics*, 118:15–31.

Foley, S., Karlsen, J. R., and Putniņš, T. J. (2019). Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies? *Review of Financial Studies*, 32(5):1798–1853.

Garratt, R. J. and van Oordt, M. R. C. (2023). Why fixed costs matter for proof-of-work–based cryptocurrencies. *Management Science*, 69(11):5284–5307.

Giannone, D., Lenza, M., and Primiceri, G. E. (2015). Prior Selection for Vector Autoregressions. *The Review of Economics and Statistics*, 97(2):436–451.

Granger, C. and Teraesvirta, T. (1993). *Modelling Non-Linear Economic Relationships*. Oxford University Press.

Griffin, J. M. and Shams, A. (2020). Is Bitcoin Really Untethered? *Journal of Finance*, 75(4):1913–1964.

Halaburda, H., Haeringer, G., Gans, J., and Gandal, N. (2022). The microeconomics of cryptocurrencies. *Journal of Economic Literature*, 60(3):971–1013.

Halaburda, H. and Yermack, D. (2022). Bitcoin mining meets Wall Street: A study of publicly traded crypto mining companies. *Mimeo.*

Huberman, G., Leshno, J. D., and Moallemi, C. (2021). Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *Review of Economic Studies*, 88, 3011–3040.

Kaiser, B., Jurado, M., and Ledger, A. (2018). The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin. *CoRR*, abs/1810.02466.

Karau, S. (2023). Monetary policy and bitcoin. *Journal of International Money and Finance*, 137:102880.

Kroll, J. A., Davey, I. C., and Felten, E. W. (2013). The economics of bitcoin mining, or bitcoin in the presence of adversaries.

Litterman, R. B. (1986). Forecasting with Bayesian Vector Autoregressions – Five Years of Experience. *Journal of Business & Economic Statistics*, 4(1):25–38.

Liu, Y. and Tsyvinski, A. (2020). Risks and Returns of Cryptocurrency. *The Review of Financial Studies*, 34(6):2689–2727.

Liu, Y., Tsyvinski, A., and Wu, X. (2022). Common Risk Factors in Cryptocurrency. *The Journal of Finance*, LXXVII(2).

Ma, J., Gans, J. S., and Tourky, R. (2018). Market Structure in Bitcoin Mining. *NBER Working Papers*, 24242.

Makarov, I. and Schoar, A. (2020). Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics*, 135(2):293–319.

Makarov, I. and Schoar, A. (2021). Blockchain Analysis of the Bitcoin Market. *NBER Working Paper*, 29396.

Makarov, I. and Schoar, A. (2022). Cryptocurrencies and Decentralized Finance. *NBER Working Paper*, 30006.

Mertens, K. and Ravn, M. O. (2013). The Dynamic Effects of Personal and Corporate Income Tax Changes in the United States. *American Economic Review*, 103(4):1212–1247.

Miranda-Agrippino, S. and Ricco, G. (2018). Bayesian Vector Autoregressions. *Bank of England Working Papers*, 756.

Miranda-Agrippino, S. and Ricco, G. (2023). Identification with external instruments in structural vars. *Journal of Monetary Economics*, 135:1–19.

Montiel Olea, J. L. and Plagborg-Møller, M. (2021). Local projection inference is simpler and more robust than you think. *Econometrica*, 89(4):1789–1823.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Technical report.

Pagnotta, E. S. (2022). Decentralizing Money: Bitcoin Prices and Blockchain Security. *The Review of Financial Studies*, 35(2):866–907.

Pagnotta, E. S. and Buraschi, A. (2018). An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. *mimeo, https://ssrn.com/abstract=3142022*.

Plagborg-Møller, M. and Wolf, C. K. (2021a). Local Projections and VARs Estimate the Same Impulse Responses. *Econometrica*, 89(2).

Plagborg-Møller, M. and Wolf, C. K. (2021b). Supplement to "Local Projections and VARs Estimate the Same Impulse Responses". *Econometrica*, 89(2).

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

Romer, C. D. and Romer, D. H. (1989). Does Monetary Policy Matter? A New Test in the Spirit of Friedman and Schwartz. In *NBER Macroeconomics Annual 1989, Volume 4*, NBER Chapters, pages 121–184. National Bureau of Economic Research, Inc.

Scharnowski, S. and Shi, Y. (2021). Bitcoin Blackout: Proof-of-Work and the Centralization of Mining. *mimeo, https://ssrn.com/abstract=3936787*.

Sims, C. A. (1980). Macroeconomics and reality. *Econometrica*, 48(1):1–48.

Sims, C. A., Stock, J. H., and Watson, M. W. (1990). Inference in Linear Time Series Models with Some Unit Roots. *Econometrica*, 58(1):113–144.

Sockin, M. and Xiong, W. (2023). A model of cryptocurrencies. *Management Science*, 69(11):6684–6707.

Song, Y. and Aste, T. (2020). The Cost of Bitcoin Mining Has Never Really Increased. *Frontiers in Blockchain*, 3(565497).

Stinner, J. and Tyrell, M. (2022). Proof-Of-Work Consensus Under Exogenous Distress: Evidence from Mining Shocks in the Bitcoin Ecosystem. *Mimeo*.

Stock, J. H. and Watson, M. W. (2018). Identification and Estimation of Dynamic Causal Effects in Macroeconomics Using External Instruments. *Economic Journal*, 128(610):917–948.

A Additional Results and Supporting Materials

A.1 Mining Shock Events

Table A.1: Mining shock events used to construct instrument

Date	Event	Sign	Weight
14.10.2014	Bitcoin mining facility in Thailand destroyed in major fire.	-1	-0.99
01.08.2015	Increase in electricity price in Qinghai Province, China.	-1	-0.15
01.06.2016	Increase in electricity price in Sichuan Province, China.	-1	-0.40
01.07.2017	Decrease in electricity price in Sichuan Province, China.	1	0.48
22.08.2017	Hard fork leads to competition over mining power between Bitcoin and Bitcoin Cash.	-1	-2.80
11.11.2017	Renewed competition over mining power between Bitcoin and Bitcoin Cash.	-1	-2.50
27.06.2018	Floods in Sichuan, China, destroy major mining centers.	-1	-1.91
01.09.2018	Decrease in electricity price in China's Sichuan Province.	1	0.02
05.11.2018	Cryptocurrency mining farms in Chinese provinces Xinjiang and Guizhou shut down for "tax inspections".	-1	-0.96
30.04.2019	Decrease in electricity price in Chinese Sichuan province.	1	0.44
27.06.2019	Iranian authorities seize mining machines amid spike in electricity consumption.	-1	-0.13
17.08.2019	Floods in Sichuan, China, cause damage to Bitcoin mining operations.	-1	-1.14
23.09.2019	Chinese authorities conduct inspections in Inner Mongolia to close 'illegal' mining operations; national Government of Kyrgyzstan orders the cutting off of power of at least 45 large mining farms.	-1	-2.76
30.09.2019	Major fire at a Bitcoin mining farm in China; roughly $10M worth of mining equipment is lost. Afterwards no block found for roughly 2 hours.	-1	-0.99
01.04.2020	Decrease in electricity price in Xinjiang Province, China.	1	0.57
13.05.2020	Mining farms in Chinese province of Sichuan turn off their mining machines due to electricity shortages.	-1	-1.55
26.10.2020	Wet season in Sichuan ends and with it cheap electricity for mining farms. Migration to Xinjiang and Inner Mongolia is hampered by COVID-19-related restrictions.	-1	-3.23
11.12.2021	Iranian police confiscate some 45,000 bitcoin mining machines that were illegally using subsidized electricity.	-1	0
01.02.2021	Decrease in electricity price in Sichuan Province, China.	1	0.45
15.02.2021	Most Bitcoin mining farms in Texas go offline amid largest forced power outage in U.S. history from winter storm.	-1	-0.28
16.04.2021	Flood in Chinese coal mine that miners rely on for energy causes subsequent safety inspections by Chinese authorities leading to enforced electricity blackout.	-1	-1.49
17.05.2021	Power outages in in Sichuan, China, where all large consumers of the region's hydro-power are subject to all-day power restrictions; Chinese government officials call for a crackdown on mining in a statement; Iran bans Bitcoin mining effective immediately until September amid power outages, while official mining farms voluntarily shut down power; Kyrgyzstan seizes 2,000 cryptocurrency mining devices.	-1	-2.59
21.06.2021	Sichuan authorities order shutdown of 26 mining farms and order energy companies to stop supplying power to miners. Previously, hopes that Chinese mining ban announced in May would only apply to dirty mining (coal-powered farms in Inner Mongolia and Xinjiang) but not the hydro-powered Sichuan farms.	-1	-3.75
12.07.2021	Ukraine authorities shut down largest illegal crypto mining farm in the country; Malaysian police seize more than 1000 mining rigs and destroy them with steamroller after alleged electricity theft by miners.	-1	-0.21
01.10.2021	Iranian government lifts ban on mining for cryptocurrency for licensed operators.	1	0.61
17.11.2021	Kirghiz authorities shut down Bitcoin mining farm operating 2,500 mining rigs.	-1	-0.02
28.12.2021	Iranian government renews ban on cryptocurrency mining over blackouts concerns.	-1	0
05.01.2022	Kazakhstan's government temporarily shuts down internet connection amid escalating protests, cutting off Bitcoin miners; around the same time Kosovo bans Bitcoin mining amid energy crisis.	-1	-0.01
01.02.2022	Bitcoin miners power down operations in Texas amid winter storm.	-1	-0.16
22.02.2022	Kazakh authorities terminate 13 cryptocurrency mining operations, announces crackdown in days to come, in which over 100 crypto mining farms are shut down.	-1	-0.68
11.07.2022	Texas heatwave and energy crunch curtails Bitcoin mining as miners voluntarily power down operations.	-1	-1.07

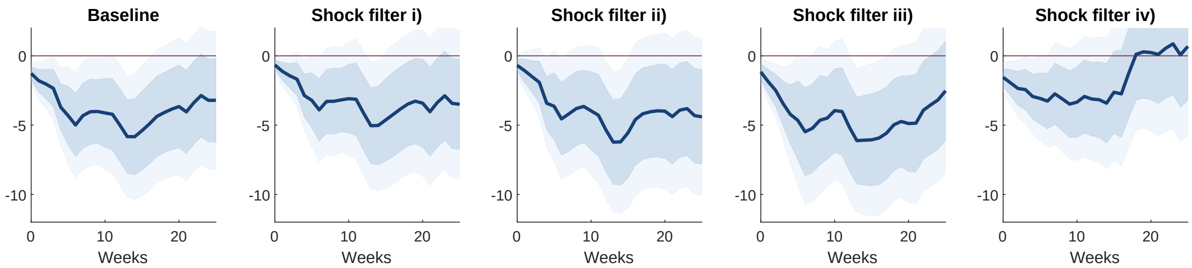
Note. Events used to construct the mining shock instrument in the VAR analysis. *Sign* denotes the value in the binary setup (Plagborg-Møller and Wolf, 2021b), *Weight* denotes the (negative) difference in average block confirmation times (in minutes) relative to the 10-minute goal around the respective event.

Table A.2: Major releases of new mining hardware within our time sample

Date	Name of mining hardware	J/Th
05.10.2013	KnCMiner Jupiter	1,484
01.12.2013	Antminer U1	1,250
03.03.2014	Bitfury BF864C55	500
22.07.2014	RockerBox	316
16.09.2014	ASICMiner BE300	187
19.08.2015	BM1385	181
23.09.2015	PickAxe	140
01.06.2016	Antminer S9-11.5	98
01.02.2017	Antminer R4	97
15.02.2018	Ebang Ebit 10	92
01.05.2018	8 Nano Compact	51
09.04.2019	Antminer S17	36
23.03.2020	Antminer S19 Pro	30

Note. Major releases of new mining hardware used to construct M_t in equation (6). Source: Ciaian et al. (2021) based on Song and Aste (2020).

Figure A.1: Robustness: local projection IRFs to (filtered) mining shocks identified recursively



Note. Local projection impulse responses to a mining shock identified recursively. Baseline version uses all shocks, the remaining specifications filter shocks according to the criteria described in the main text. Values in percent. Shaded areas denote 68% and 90% confidence bands. Time sample: July 2013 to June 2022.

A.2 Additional Empirical Results

Recursive identification: addressing endogeneity concerns. As outlined in Section 2.4, the existence of fixed costs should generally alleviate endogeneity concerns as small declines in the price of Bitcoin will not cause miners to adjust their mining effort. Larger price declines on the other hand may do so, provided that revenues drop below marginal costs, which are due mostly to maintainence and electricity expenses. Large, one-time price drops or continued declines in the price of Bitcoin that accumulate over time might then cause some miners to incur losses from continued operation, in which case they will respond by temporarily shutting off and perhaps even selling part of their hardware. Conversely, after such a decline has occurred, a rise in Bitcoin prices might induce them to activate hardware that was previously switched off. These considerations may to some extent call into question the recursive identification scheme that relies on miners not contemporaneously reacting to variations in revenues, such as changes in fees or the price of Bitcoin. Here we address these concerns as follows.

In a first step we recreate the mining shock series implied by the recursive identification – we do so by the means of time series regressions but could equally extract the shock series directly from the VAR model; the latter approach yields essentially identical results – and use them in a local projection analysis in which we regress the logged price of Bitcoin onto the shocks. As before under the external instrument approach, this first serves as a robustness check to the impulse responses derived from the VAR. More importantly however it constitutes a benchmark for a subsequent filtering exercise. Namely, in a second step, we keep identified shocks only when certain conditions are satisfied, and set them to zero otherwise:

1. The absolute change in Bitcoin prices is less than 20 percent in the current week. The idea is that concurrent drops or jumps in the exchange rate might induce miners

to immediately switch off (or on again) previously installed mining gear even in the presence of fixed costs if price changes are large enough.

2. The cumulative Bitcoin price decline in the last three weeks (i.e. the current and previous two weeks) is less than 20 percent. The idea here is similar to the previous point, yet we allow for continued price declines that might make miners incur losses even in the absence of large price drops in any one week.

3. The sign of the change in Bitcoin prices in the last three weeks is not the same. The idea is to be agnostic on size of price changes but filter out periods of sustained changes in one direction.

4. The current Bitcoin price is not below a previous historical peak that was reached less than two years ago.[30] The idea here is that miners might have invested in mining hardware in the past, have switched off operations after a sustained price decline and could potentially endogenously switch back on their hardware after some price threshold is reached when prices recover.

FIGURE A.1 shows results to the baseline specification and the four filtering exercises. Reassuringly, results look very similar, implying that our findings in the baseline case are not driven by periods that would invalidate the timing restrictions in adjustment that our alternative identification relies on.

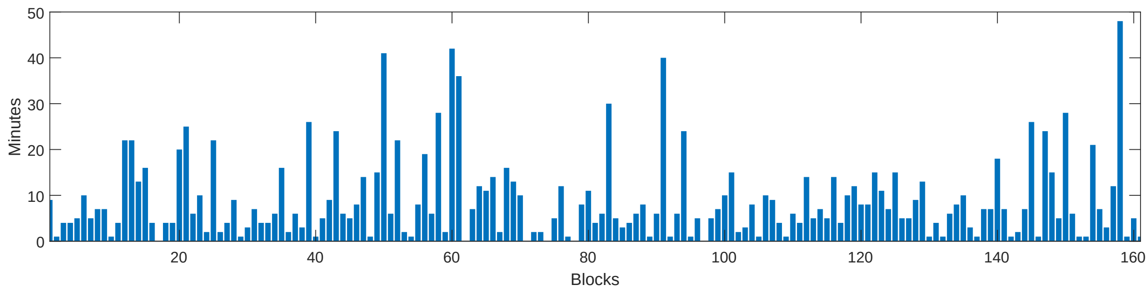
[30]We choose a two-year cut-off period as the average life span of mining hardware is sometimes `reported to be around two years`. Given that additionally there regularly are milestones in the development of mining hardware that make old rigs uncompetitive in comparison (a fact that we exploited earlier), we would not expect more than two-year old mining hardware to be switched on again after some increases in Bitcoin prices. Having said that, we obtain statistically significant impulse responses to mining shocks even when filtering out past-peak episodes without any cut-off.

A.3 On the Choice of Weekly Data

The hashrate as a measure of total mining effort cannot be observed directly. Instead, estimates are based on block confirmation times, i.e. the time intervals that it took to add blocks to chain, relative to the 10-minute goal when taking into account the current difficulty level.[31] The process of finding solutions to cryptograms involves randomness. Hashrate estimates will therefore vary over time even when the actual total mining effort is constant. The choice of the most appropriate data frequency is therefore directly tied to how large the random fluctuations in block confirmation times are. In the following we look at empirical examples and then simulate block confirmation times and from that conclude that weekly time spells are most appropriate for our empirical analysis.

Figure A.2 shows block confirmation times on 14 January 2022, a randomly chosen day without any known mining disruptions and without a difficulty adjustment. Roughly 160 blocks were added to the blockchain on that day, slightly more than the 144 that would be expected based on the 10-minute goal per block. One striking feature is the large standard deviation, with some cryptograms being solved after one minute, while others took almost 50.

Figure A.2: Observed block confirmation times on 14 January 2022

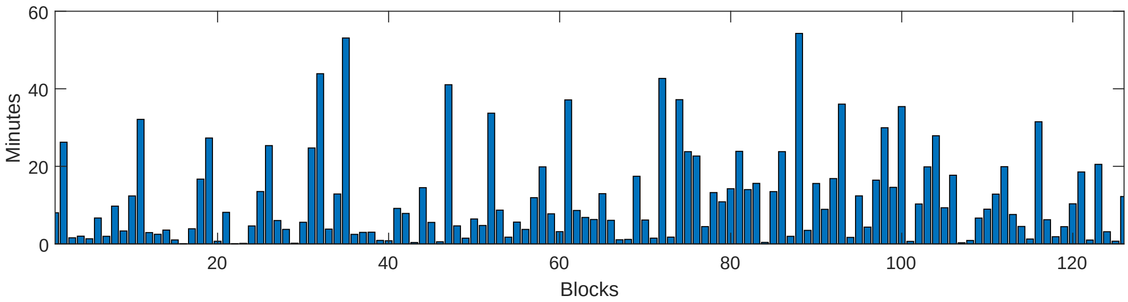


In order to assess to which degree this randomness translates into data of lower frequency, we rely on simulations. The success of solving cryptograms can be modeled by a Poisson distribution, such that the interval between blocks is Gamma-distributed (see for instance Ma et al., 2018). Specifying the parameters such that the average block confirmation time is ten minutes, we create artificial data for one hypothetical day in Figure A.3. The picture looks very similar to the empirically observed one, indicating a good model fit.

We then compute daily averages over 100 days and contrast this with weekly averages in the first panel of Figure A.4. Although, by construction, mining fundamentals are constant in these simulations, there is still a large fluctuations in average daily block confirmation times, which vary between eight and twelve minutes. In other words, even fairly large empirically observed variation in daily hashrate data will often simply reflect

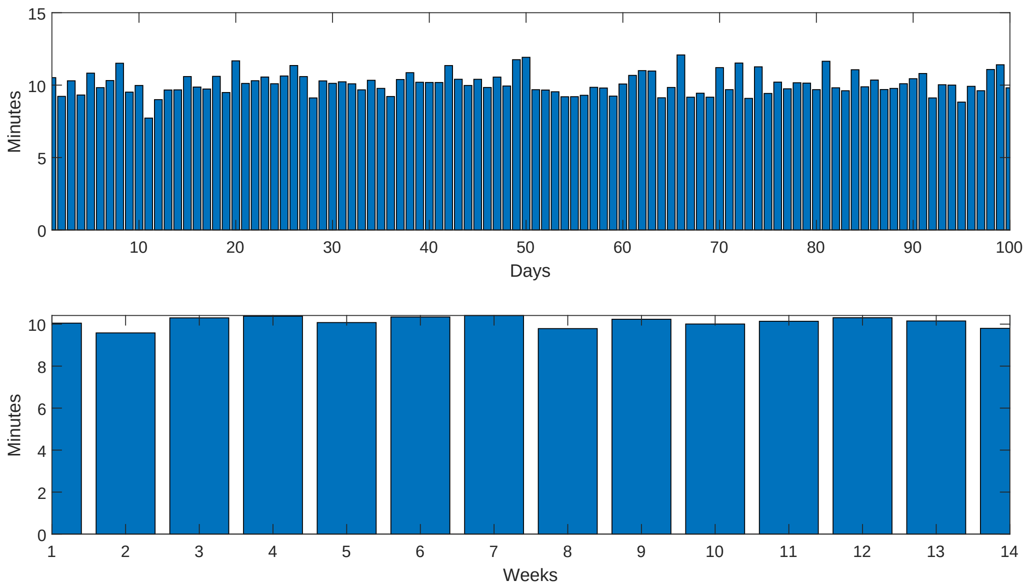
[31] For instance, coinmetrics.io calculates its hashrate estimate (in terra hashes per second) as $(bc/144) \times K \times (2^32/10^{12})/600)$, in which bc is the daily number of added blocks and K is the difficulty.

Figure A.3: Simulated block confirmation times for one day



noise. In contrast, weekly averages are more stable (second panel), such that a given observed deviation from the 10-minute goal is much more likely to reflect actual changes in aggregate mining effort. Taken together with the fact that for many of our events we cannot precisely establish a single day when the respective incident happened, we therefore specify our model in weekly frequency. This reflects common practice both on analytical cryptocurrency websites as well as academic analyses.[32]

Figure A.4: Simulated block confirmation times: daily and weekly



Finally, we use our simulation exercise in order to refine our instrument in a robustness check in Section 2.4. Specifically, we exclude all events in which the observed weekly variation in the hashrate did not deviate statistically significantly from ten minutes. In order to derive a confidence band, we simulate 50,000 blocks and find that weeks with deviations of more than 0.63 minutes lie outside the 90% band.

[32]Common cryptocurrency websites `often suggest to use smoothed or weekly data`. Biais et al. (2023) use weekly data in their empirical analysis as well, also in order to avoid day-of-the-week effects.

A.4 VAR Estimation

Proxy VAR Model Description. The main analysis is based on a structural VAR model represented by

$$\mathbf{A}_0\mathbf{y}_t = \mathbf{k} + \mathbf{A}_1\mathbf{y}_{t-1} + ... + \mathbf{A}_p\mathbf{y}_{t-p} + \epsilon_t, \quad \epsilon_t \sim \mathcal{N}(\mathbf{0}, \mathbf{I}),$$

where $\mathbf{y}_t$ is an $(n \times 1)$ vector of endogenous variables, and $\mathbf{k}$ is a vector of constants. The corresponding reduced-form VAR is:

$$\mathbf{y}_t = \mathbf{c} + \mathbf{B}_1\mathbf{y}_{t-1} + ... + \mathbf{B}_p\mathbf{y}_{t-p} + \mathbf{u}_t, \quad \mathbf{u}_t \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}),$$

with $\mathbf{c} = \mathbf{A}_0^{-1}\mathbf{k}$ and $\mathbf{B}_i = \mathbf{A}_0^{-1}\mathbf{A}_i$ and $\mathbf{u}_t = \mathbf{A}_0^{-1}\epsilon_t$.

Building on Stock and Watson (2018) and Mertens and Ravn (2013), we partition the shock vectors into those mining shocks, ϵ_t^m, and any other structural innovations, $\epsilon_t^{q\prime}$, with corresponding residual vectors $\mathbf{u}_t = [u_t^m, \mathbf{u}_t^{q\prime}]'$. Denoting the impact matrix $\mathbf{A}_0^{-1}$ as $\mathbf{S}$, the interest lies in that set of coefficients, column $\mathbf{s}$, that measures the initial impact to a structural mining shock. In what follows, we denote as $\mathbf{s}^q$ the initial impact of ϵ_t^p on $\mathbf{u}_t^q$, while s^m is the corresponding impact on the reduced-form mining residual u_t^m.

As outlined in the main text, to construct the instrument series we collect a list of incidents that were plausibly exogenous but are likely to have had a sizable impact on aggregate mining effort. For these instruments to be valid, the instrument series $\mathbf{Z}_t$ needs to be *relevant* and *exogenous* as follows:

$$\mathbb{E}[Z_t \epsilon_t^{m\prime}] \neq 0, \tag{A.1}$$

$$\mathbb{E}[Z_t \epsilon_t^{q\prime}] = \mathbf{0}. \tag{A.2}$$

To estimate impulse responses to a structural mining policy shock, we obtain estimates of $\mathbf{s}$ as follows. We extract the residuals $\mathbf{u}_t$ from the reduced-form VAR and use them in a two-stage least squares regression which include $\mathbf{Z}_t$ as instruments. In the first stage, u_t^m is linearly projected on $\mathbf{Z}_t$, delivering the fitted values $\hat{u}_t^m$. The latter, which are by assumption orthogonal to the remaining shocks ϵ_t^q, can be used in the second-stage regression:

$$\mathbf{u}_t^q = \frac{\mathbf{s}^q}{s^m}\hat{u}_t^m + \xi_t. \tag{A.3}$$

This procedure ensures that $\frac{\mathbf{s}^q}{s^m}$ is consistently estimated and can be used to obtain $\mathbf{s}$. We then normalize s^m so that the initial increase in the hashrate is equal to 10 percent. Given the high number of parameters to be estimated and in order to avoid overfitting, we estimate the proxy VAR via Bayesian methods using standard macro-econometric priors as described next.

Bayesian Estimation. As is common in the structural VAR literature, we employ Bayesian techniques in order to impose more structure on the estimation and avoid overfitting given the relatively modest size of observations. We use standard Minnesota priors (as in Litterman, 1986) that are cast in the form of a Normal-Inverse-Wishart prior, which conveniently is the conjugate prior for the likelihood of a VAR with Gaussian innovations (see Miranda-Agrippino and Ricco, 2018).

Consider the setup for the proxy VAR:

$$\mathbf{A}_0\mathbf{y}_t = \mathbf{k} + \mathbf{A}_1\mathbf{y}_{t-1} + ... + \mathbf{A}_p\mathbf{y}_{t-p} + \epsilon_t, \quad \epsilon_t \sim \mathcal{N}(\mathbf{0}, \mathbf{I}), \tag{A.4}$$

where $\mathbf{y}_t$ is an $(n \times 1)$ vector of endogenous variables, and $\mathbf{k}$ is a vector of constants. The corresponding reduced-form VAR is:

$$\mathbf{y}_t = \mathbf{c} + \mathbf{B}_1\mathbf{y}_{t-1} + ... + \mathbf{B}_p\mathbf{y}_{t-p} + \mathbf{u}_t, \quad \mathbf{u}_t \sim \mathcal{N}(\mathbf{0}, \mathbf{\Sigma}), \tag{A.5}$$

with $\mathbf{c} = \mathbf{A}_0^{-1}\mathbf{k}$, $\mathbf{B}_i = \mathbf{A}_0^{-1}\mathbf{A}_i$ and $\mathbf{u}_t = \mathbf{A}_0^{-1}\epsilon_t$.

For Bayesian estimation, we specify a multivariate normal distribution for the regression coefficients, and an inverse Wishart distribution for the covariance matrix of the error term:

$$\mathbf{\Sigma} \sim \mathcal{IW}(\underline{\mathbf{S}}, \underline{\nu}), \tag{A.6}$$

$$\beta|\Sigma \sim \mathcal{N}(\underline{\beta}, \Sigma \otimes \underline{\mathbf{\Omega}}). \tag{A.7}$$

$\beta = vec([\mathbf{c}, \mathbf{B}_1, ..., \mathbf{B}_p]')$ are the stacked coefficient matrices and $\underline{\mathbf{S}}$, $\underline{\nu}$, $\underline{\beta}$ and $\underline{\mathbf{\Omega}}$ are hyper-parameters. Specifically, $\underline{\mathbf{S}}$ and $\underline{\nu}$ are, respectively, the scale matrix and the degrees of freedom of the prior inverse Wishart distribution. As is standard, we specify $\underline{\mathbf{S}}$ as a diagonal matrix with entries σ_i^2 equal to the residual variance of the regression of each variable onto its own first lag. The degrees of freedom are set to $\underline{\nu} = n + 2$ so as to ensure that the prior variances of the coefficient matrices exist and $\mathbb{E}(\beta) = \underline{\beta}$ and $\mathbb{V}ar(\beta) = \underline{\mathbf{S}} \otimes \underline{\mathbf{\Omega}}$.

We use a standard "Minnesota"-type prior in the spirit of Litterman (1986), which assumes the coefficient matrices to be independently normally distributed. Specifically, their first two moments are:

$$\mathbb{E}[(\mathbf{B_l})_{\mathbf{i,j}}|\mathbf{\Sigma}] = \begin{cases} \delta_i & i = j, l = 1 \\ 0 & \text{otherwise} \end{cases} \tag{A.8}$$

$$\mathbb{V}ar[(\mathbf{B_l})_{\mathbf{i,j}}|\mathbf{\Sigma}] = \begin{cases} \frac{\lambda^2}{l^2} & i = j, \forall l \\ \frac{\lambda^2}{l^2}\frac{\Sigma_{i,i}}{\sigma_j^2} & i \neq j, \forall l \end{cases} \tag{A.9}$$

where $(B_l)_{i,j}$ is the response of variable i to variable j at lag l. As the VAR is estimated in levels, we set $\delta_i = 1$, implying random-walk behavior of the underlying time series.As is common, we formalize the idea that more recent lags of a variable tend to be more informative by specifying l^2 in the variance entries. Hence, equation (A.9) ensures a decaying variance of parameters for more distant lags and is, together with the assumptions above, achieved by specifying

$$\underline{\mathbf{\Omega}} = \begin{bmatrix} \phi & \mathbf{0} \\ \mathbf{0} & diag([1^2, 2^2, ..., p^2])^{-1} \otimes diag([\sigma_1^2, \sigma_2^2, ..., \sigma_p^2])^{-1} \end{bmatrix}, \tag{A.10}$$

where ϕ is a large number, implying a flat prior on the constant terms.

The hyperparameter λ controls the overall tightness of the Minnesota prior, which is determined optimally in the spirit of hierarchical modeling as in Giannone et al. (2015).

Combining the prior specification with the likelihood function, the posteriors can be shown to correspond to (see Miranda-Agrippino and Ricco, 2018):

$$\mathbf{\Sigma}|\mathbf{y} \sim \mathcal{IW}(\bar{\mathbf{S}}, \bar{\nu}) \tag{A.11}$$

$$\beta|\Sigma, \mathbf{y} \sim \mathcal{N}(\bar{\beta}, \mathbf{\Sigma} \otimes \bar{\mathbf{\Omega}}), \tag{A.12}$$

with

$$\bar{\mathbf{\Omega}} = (\underline{\mathbf{\Omega}} + \mathbf{x}'\mathbf{x})^{-\mathbf{1}}, \tag{A.13}$$

$$\bar{\beta} = vec(\bar{\mathbf{B}}) = vec\Big(\bar{\mathbf{\Omega}}\Big(\underline{\mathbf{\Omega}}^{-1}\underline{\mathbf{B}} + \mathbf{x}'\mathbf{x}\hat{\mathbf{B}}\Big)\Big), \tag{A.14}$$

$$\bar{\mathbf{S}} = \hat{\mathbf{B}}'\mathbf{x}'\mathbf{x}\hat{\mathbf{B}} + \underline{\mathbf{B}}'\underline{\mathbf{\Omega}}^{-\mathbf{1}}\underline{\mathbf{B}} + \underline{\mathbf{S}} + \Big(\mathbf{y} - \mathbf{x}\hat{\mathbf{B}}\Big)'\Big(\mathbf{y} - \mathbf{x}\hat{\mathbf{B}}\Big) - \bar{\mathbf{B}}'\Big(\underline{\mathbf{\Omega}}^{-\mathbf{1}} + \mathbf{x}'\mathbf{x}\Big)\bar{\mathbf{B}}, \tag{A.15}$$

where $\mathbf{x}_t = [\mathbf{1}, \mathbf{y}_{t-1}, ..., \mathbf{y}_{t-p}]$ is the projection set of lagged endogenous variables. The credible sets are then constructed by drawing from the posteriors and for each draw making use of the external instruments approach outlined in the main text.

B A Model of Mining Shocks and Blockchain Security

We have documented sizable and persistent effects of mining shocks on Bitcoin prices. This section describes a deliberately stylized model that will prove useful to rationalize our empirical findings. Following some conceptual considerations in Section B.1, we describe the baseline version of the model in Section B.2, building directly on Pagnotta (2022). We then extend the model to study the effects of mining shocks in Section B.3.

B.1 Conceptualizing Network Attacks

Several recent papers feature formal economic analyses of attacks on PoW blockchains (for instance Budish, 2024; Auer, 2019; Garratt and van Oordt, 2023; see also Section 3 in Halaburda et al., 2022 for an overview). A common element in these models is that the system has to provide incentives for owners of mining hardware to "mine honestly", i.e. validate transactions without manipulating the transaction record. Most broadly, one can differentiate between double-spending and sabotage attacks (Budish, 2024).[33] The main focus and innovation in Nakamoto's, 2008 PoW was to achieve a distributed, yet synchronized ledger that avoids double spending. In a double-spending attack, a network node would send bitcoins, receive some good or asset in return and try to revoke the payment by mining an alternate chain that does not include the relevant transaction. If successful in outcompeting the other "honest" miners, the attacker's chain will be longer and, by the "longest-chain rule", will be adopted by the network. In such a case, the attacker could spend the coins again.

The aim of sabotage instead is not to re-spend coins as a participant but to actively harm the network. For instance, were attackers able to acquire or confiscate large enough amounts of mining hardware, they could arbitrarily exclude transactions or continuously mine empty blocks, such that Bitcoin would seize to be usable to transfer value. This could be motivated by financial gain – protecting an existing competing business model or profiting from a large short position on Bitcoin – or for political or ideological reasons. Indeed, China, as home to the majority of mining operations for a long time, repeatedly

[33] Bonneau (2018) gives a more nuanced informal overview of different attack types. Eyal and Sirer (2013) analyze a minority attack in which large miners try to obtain a disproportionate share of mining rewards.

expressed strong opposition to the use of cryptocurrencies,[34] as have multiple other state actors, citing inter alia environmental concerns and risk to financial stability or monetary sovereignty.

Notably, as discussed in Budish (2024) and Garratt and van Oordt (2023), the presence of non-repurposable mining hardware together with the fact that a successful attack will likely cause a fall in the value of Bitcoin, provides incentives for miners not to manipulate: doing so would reduce the present value of their mining equipment, raising the cost of the attack. Hence, whereas a subsequent fall in the price of Bitcoin may act as a natural bound on double-spending attempts, it is the very point of a sabotage attack. Further, unlike double-spending attacks, sabotage attacks represent a risk to all network participants at the same time, not just a small subset of those who accept Bitcoin as a form of payment for goods or assets, such as online retailers or exchange trading platforms.

For these reasons, we adopt, and extend, the framework developed in Pagnotta (2022) that focuses attention on potential sabotage attacks. We note, however, that the threat of other types of attacks could in principle similarly make mining shocks affect Bitcoin valuations via their effects on network security. After describing how this framework gives rise to equilibrium multiplicity in Section B.2, we extend it in Section B.3 by introducing mining shocks, and formulate two security channels by which these can affect prices.

B.2 A Bitcoin asset pricing model with mining

Here we describe the baseline model that features interactions among Bitcoin users, miners, and a potential saboteur who may attempt to compromise the blockchain. For additional details the reader is referred to Pagnotta (2022).

The model includes a continuum of n homogeneous investors who can produce and consume a perishable good, with the price of this good serving as the numeraire. These agents have the option to purchase Bitcoins at a price p_t, which they value due to the potential for uniquely beneficial exchange opportunities in a subsequent interim subperiod t'. The utility derived from holding Bitcoins is represented by a continuous, strictly increasing, and concave function $V(\cdot)$, which captures the value agents place on the opportunities provided by Bitcoin transactions.

There is a malicious agent, termed a saboteur, who poses a risk of a systemwide attack between periods t and t'. The outcome of such an attack is binary: either the network

[34] Kaiser et al. (2018) discusses China's concern about, but strong influence over, Bitcoin in detail. As a case in point, some time before the exodus out of China, an article at `digiconomist.net` warned against what Kroll et al. (2013) call a *Goldfinger attack*, through which the large concentration of mining power could become a significant security risk: "If China were to confiscate all of the available Bitcoin mining equipment within its borders, it could theoretically completely paralyze the Bitcoin network. Earlier this year the Iranian government seized thousands of Bitcoin miners, and there's no guarantee China won't ever do the same."

survives and a new block is added to the ledger, or the attack is successful, rendering Bitcoins entirely worthless. The probability of the network surviving an attack is denoted by $S \in (0,1)$, which is referred to as the security function, specified below.

In case the attack fails, in period $t+1$ investors can sell their Bitcoin holdings in a liquidation market at the uncertain price p_{t+1}. Following the notation in Pagnotta (2022) and defining E_t^1 as the expectations operator conditional on an unsuccessful attack, investors' expectation of future prices is $E_t p_{t+1} = S_t E_t^1 p_{t+1} + (1-S_t) \times 0$. Denoting returns $R_{t+1} = E_t^1 \frac{p_{t+1}}{p_t}$ (with $R_{t+1} < \frac{1}{\delta S_t}$),[35] and time preference rate $\delta \in (0,1)$, investors maximize $c_{it} - l_{it} + E_t(V(B_{it}p_t) + \delta c_{i,t+1})$ subject to the budget constraints $B_{it}p_t + c_{it} \leq l_{it}$ and $c_{t+1} \leq B_{it}p_{t+1}$, where B_{it} is the non-negative amount of Bitcoins held and l_{it} are labor hours. Denoting $b_{it} = p_t B_{it}$ as real Bitcoin holdings, we can simplify the problem to:

$$\max_{b_{it} \geq 0} S_t(fV(b_{it}) + (1-f)\delta b_{it} R_{t+1}) - b_{it}, \tag{A.16}$$

where f is the probability with which holders find an exchange opportunity.

At the start of period t, miners invest in computational power to verify blocks and earn rewards. The share of blocks verified by a miner is proportional to their computational power contribution. The cost function for mining, $C(h)$, is assumed to be increasing and convex. Miners are risk-neutral, act as price takers, and form expectations about future Bitcoin prices. Hence, each miner j maximizes $P(h_j, h_{-j}) \cdot \delta\psi E_t^1[p_{t+1}] - C(h_j)$, where $-j$ denotes the other miners, δ is the time preference and ψ represents the block reward in bitcoins. Miners' optimal investment is then characterized by a symmetric Nash equilibrium, where the system's hashrate $H = hm$ is determined by individual investments in hashing h times the number of miners m:

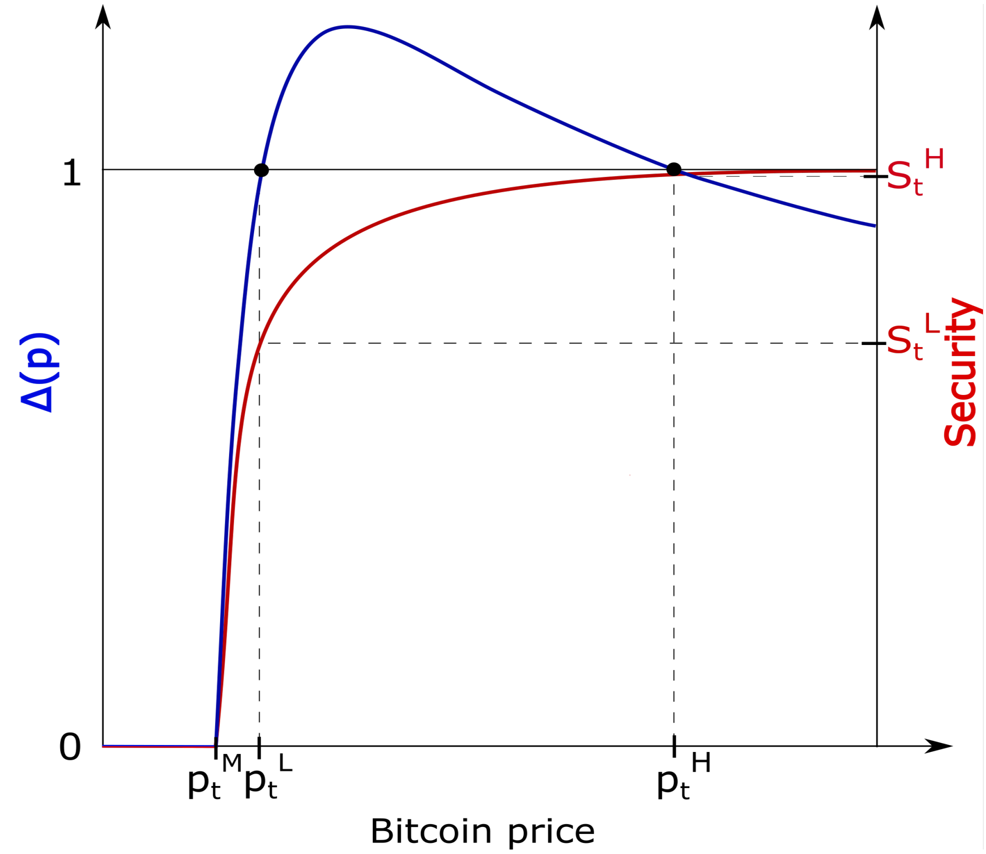
$$H_t = \left(\frac{m(m-1)}{m^2}\right) \frac{\delta\psi}{\kappa} E_t^1[p_{t+1}] \tag{A.17}$$

in which for simplicity we have specified a linear cost function, i.e. $C'(h) = \kappa$. Equation (A.17) can be interpreted as a free-entry condition: miners enter the market until rewards from mining break even with mining costs. Equation (A.17) therefore formalizes the blue arrow in the introduction of the main text in FIGURE 1: an increase in mining revenues from a higher Bitcoin price leads to a rise in mining investment in equilibrium.

The presence of a saboteur introduces an aggregate source of risk, as a successful attack would affect all participants in the Bitcoin network. In the model, the saboteur is a single entity with a fixed budget that allows for a constant hashrate A. The likelihood of a successful attack by the saboteur in the interim period t' is modeled as a binomial random walk, with the probability of ultimately eliminating a deficit of k blocks given by $\left(\frac{A}{H_t}\right)^k$, provided the saboteur's hashrate is less than half of the total hashrate, and one

[35] If R_{t+1} were larger than $\frac{1}{\delta S_t}$, demand for Bitcoin would not be bounded.

Figure A.5: Equilibrium multiplicity of Bitcoin price and security



Note. Figure adapted from Pagnotta (2022). The blue line depicts the left-hand side of equation (A.19), the red curve depicts security levels according to (A.18). An equilibrium is found where the blue line equals unity.

otherwise.

The security function consistent with such a game between honest miners and the saboteur is then given by:

$$S(H_t, A) = \begin{cases} 1 - \left(\frac{A}{H_t}\right)^k & \text{if } H_t > A, \\ 0 & \text{else.} \end{cases} \tag{A.18}$$

This function captures the notion that the security of Bitcoin decreases as the hashrate controlled by the saboteur, A, approaches the total hashrate, H_t. The parameter k represents the minimum block length for a disruptive fork to lead to a collapse in Bitcoin demand.

The equilibrium price and security of Bitcoin are then jointly determined by the interaction of user demand, miner investment, and the saboteur's actions. Given market clearing, $nB_{it} = B$, optimal investor demand (A.16), the free-entry condition (A.17), and the security function (A.18), we can summarize the equilibrium conditions as:

$$S(H(p_t), A)\left(fV'\left(\frac{B}{n}p_t\right) + (1-f)\delta R_{t+1}\right) = 1 \tag{A.19}$$

An equilibrium requires that investors' marginal utility of Bitcoin trading opportunities and the discounted expected return R, adjusted for the level of network security, equals one. As the security level itself depends on the Bitcoin price, there is no unique equilibrium: a high perceived value of Bitcoin incentivizes miners to invest in computational resources, thereby increasing network security and supporting a high equilibrium price to begin with. Conversely, a low-security, low-price equilibrium is equally self-fulfilling.

We visualize equilibrium multiplicity in Figure A.5. The red line depicts the security level S_t, governed by equation (A.18). Provided $H_t > A$, S_t increases in p_t since a higher Bitcoin price incentivizes miners to invest more resources into hashing. The blue line depicts the left-hand side of equation (A.19), labeled as $\Delta(p)$. If there were no security risks ($S_t = 1$), $\Delta(p)$ would fall monotonically in the current price of Bitcoin as capital returns decline. Yet, with sufficiently low levels of security for low Bitcoin prices, $\Delta(p)$ initially increases with Bitcoin valuations, and, as a result, security increases as well. Two equilibria can be found where the blue line equals unity: in one, both security and the current price are low (p_t^L, S_t^L), in the other both are high (p_t^H, S_t^H). Importantly, below a threshold price p_t^M, miners abstain from investing in mining such that $S_t = 0$ regardless of the current price. Also, if $A > H_t$, no positive-price equilibrium can exist: as sabotage would always be successful, there is no demand for Bitcoin and prices are zero. We will return to this point below.

B.3 The effects of mining shocks

We extend the model and introduce mining shocks as an exogenous wedge in the free-entry condition (A.17) in the baseline model:

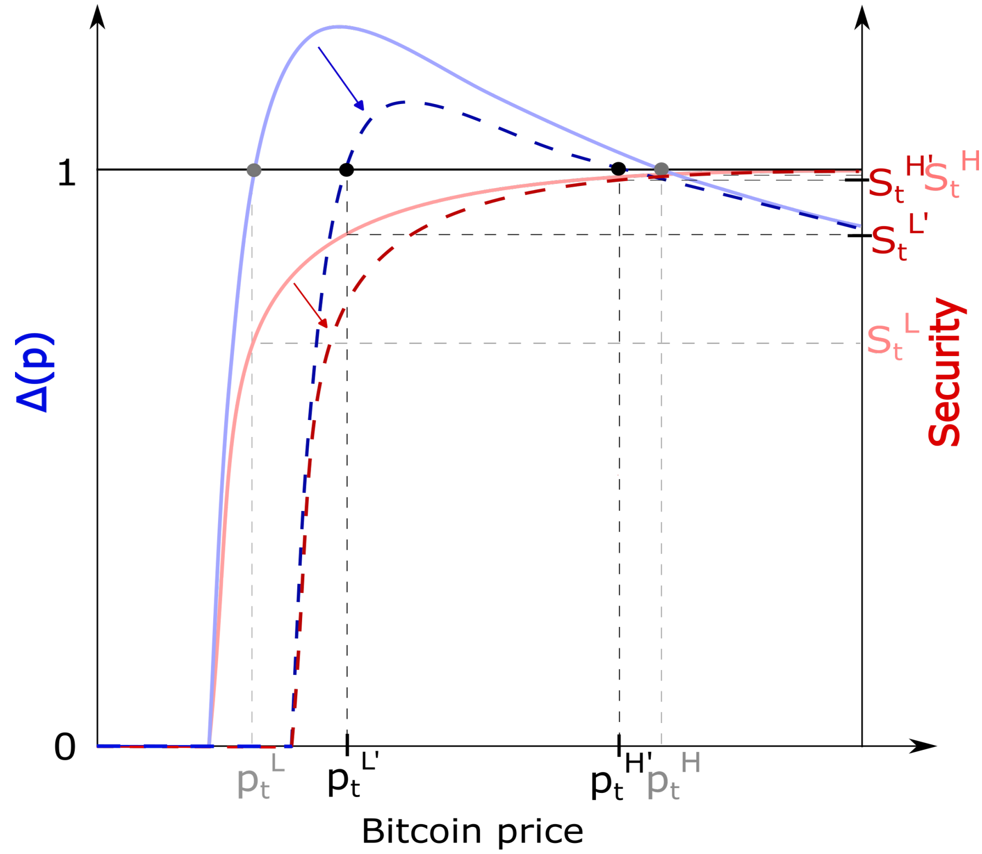
$$H_t = \left(\frac{m(m-1)}{m^2}\right)\frac{\delta\psi}{\kappa}E_t^1[p_{t+1}] + \epsilon$$

One can think of ϵ as an exogenous increase in the price of electricity or the destruction or confiscation of mining hardware. The presence of the mining shock implies that miners can only hash at the rate $H_t - \epsilon$ as opposed to H_t in the baseline model.[36] Identifying the effects of this type of shock on the Bitcoin ecosystem and its price was the main goal of our empirical analysis in Section 2.

The effect of the shock is represented by the dashed lines in Figure A.6. Compared to the baseline case, both curves shift downwards. As miners now secure the network

[36] As miners are symmetric in the baseline model, we can think of ϵ simply as the aggregate of individual mining shocks that hit all miners, i.e. $\epsilon = m\epsilon(j)$.

Figure A.6: Mining shock affecting current security levels



Note. A mining shock in period t shifts both the blue (left-hand side of equation (A.19)) and the red curve (equation A.18) downwards, changing the multiple price-security equilibria.

with fewer resources, successful sabotage becomes more probable for each given price of Bitcoin. As investors anticipate the lower levels of security, demand for Bitcoin falls, which again feeds back into lower security levels. As a result, the high-value equilibrium shifts to the left, featuring lower levels of security ($S_t^{H\prime} < S_t^H$) and prices ($p_t^{H\prime} < p_t^H$).

Importantly, the opposite happens with the low-value equilibrium, which shifts to the right. This may be surprising at first. The result arises because, in order to achieve any positive p_t^L, it is necessary that $H_t(p_t^L) > A$. Accordingly, lower levels of mining effort imply that p^L has to be higher to attain any positive price equilibrium ($p_t^{L\prime} < p_t^L$). Equivalently, there is now a larger flat section of the curve, i.e. higher levels of prices than before are characterized by $S_t = 0$ and hence do not permit a functioning network ($p_t^{M\prime} > p_t^M$).

In sum, the model implies that in the high-value equilibrium mining shocks can lead to a fall in prices, although the system continues to display fairly high levels of security (with $S_t^{H\prime}$ almost has high as S_t^H). In other words, mining shocks need not make an imminent successful attack much more likely to have price effects.