Working Paper: November 2020

Decentralizing Money: Bitcoin Prices and Blockchain Security

Emiliano S. Pagnotta
Singapore Management University

SMU
SINGAPORE MANAGEMENT UNIVERSITY

SIM KEE BOON INSTITUTE FOR FINANCIAL ECONOMICS

LEE KONG CHIAN SCHOOL OF BUSINESS

Decentralizing Money: Bitcoin Prices and Blockchain Security

Emiliano S. Pagnotta[‡]

Abstract

We address the determination of bitcoin prices and decentralized security. Users forecast the transactional and resale value of holdings, pricing the risk of malicious systemic attacks. Miners contribute resources to protect against attackers, competing for block rewards. Bitcoin's design leads to multiple equilibria: the same technology and fundamentals are consistent with sharply different price and security levels. Bitcoin's monetary policy can lead to welfare losses and deviations from quantity theory. Price–security feedback amplifies fundamental shocks' volatility impact and leads to boom–busts not driven by fundamentals. We show how Bitcoin's viability versus fiat currency depends on relative acceptability and inflation protection.

JEL Codes: E40; E42; G12; G15; G18

The Review of Financial Studies, *forthcoming*

[*]Imperial College London. Email: esp.research@pm.me.

[†]*First version*: First version: July 12, 2018. *Accepted version*: September 20, 2020. For helpful comments as conference discussants, I thank Matthew Bouvard, Jonathan Chiu, Maryam Farboodi, Nicola Pavanini, Jiasun Li, Michael Sockin, Konstantin Sokolov, and Peter Zimmerman. I also benefitted from conversations with Franklin Allen, Andreas Antonopolous, Andrea Buraschi, Ivan Canay, Will Cong, Marcin Kacperczyk, Andrei Kirilenko, Hanno Lustig, Alex Michaelides, David Miles, Andreas Park, Guillaume Rocheteau, Jose Scheinkman, Nick Szabo, Harald Uhlig, Stijn Van Nieurburgh, Randall Wright, and conference participants at the 2018 Finance Theory Group London, the 2018 Bloomberg Crypto Summit, the 2019 American Economic Association Meetings, the 2019 American Financial Association Meetings, the 2019 European Financial Association, the 2019 Central Bank Research Association Conference, the Second Toronto Fintech Conference, the 2019 Financial Intermediation Research Society Conference, the 2019 Cambridge Centre for Alternative Investment Conference, the 2019 Bank of Canada Money and Banking Workshop, the 2020 American Economic Association Meetings, the 2020 Western Finance Association Meetings, the Crypto and Blockchain Economics Research Forum, the 2020 Nova SBE Fintech Conference, and seminar participants at the Einaudi Institute for Economics and Finance, Imperial College London, Central European University, Durham Business School, and the Swiss Finance Institute @ EPFL. A previous version circulated under the title "Bitcoin as Decentralized Money: Prices, Mining, and Network Security."

The rapid growth of Bitcoin has sparked heated debates. The issue of bitcoin[1] price determination and volatility is particularly elusive. On the one hand, those in investment and entrepreneurial circles often argue that the price reflects fundamental factors such as the security of the underpinning blockchain technology. A prominent view in the academic and policy communities, on the other hand, is that bitcoins are just a bubble that will eventually burst, and therefore, prices are meaningless. Bitcoin's persistently high price volatility is frequently offered as evidence of disconnection from fundamentals.[2] While there could be elements of truth from both perspectives, reaching a consensus is challenged by the fact that traditional monetary and asset pricing models were not designed around a decentralized system, such as Bitcoin.

Two crucial differences are immediately recognizable in the system designed by Nakamoto (2008): the security model and its monetary policy. Security is paramount to any financial network, since transfers of ownership require verification, and it should be difficult for an *attacker* to manipulate historical records. In a centralized system, a specific trusted agent—such as a central bank, government, or a corporation—assumes such responsibility. In Bitcoin, however, verification and updates to the system ledger (blockchain) rely on self-selected noncooperating agents, the miners. The reward to successful miners includes a predetermined number of newly minted bitcoins, which is the sole source of supply increase. Monetary policy is, therefore, not only driven by a software protocol, but intrinsically connected to security. Understanding equilibrium price determination thus requires disentangling how these breakthrough features interplay with bitcoins' monetary function.

In this paper, we analyze an economy where consumers hold intrinsically useless bitcoins for their transactional and/or speculative value. They internalize and price the risk of a system attack that could compromise the ability to transfer bitcoins. The system security reflects the probability of such an attack, driven by the balance of computing power—or *hashrate*—between an attacker and honest miners (just miners hereafter) within the proof-of-work (PoW) contest. The attacker has a given finite budget and a private interest in sabotaging Bitcoin. Miners are profit driven and invest

[1] We follow the standard practice in the developer community of using a lowercase b for the token (bitcoin) and a capital B for the protocol or network (Bitcoin).

[2] For example, an early and influential paper by Yermack (2015) argues that Bitcoin fails to display the main characteristics of money and can be best seen as a speculation device. Consistent with this view, most governments around the world do not recognize Bitcoin as currency.

according to the anticipated real value of block rewards. The critical structural mechanism at work is that bitcoins simultaneously serve an *exchange* role for users and an *incentive* role for miners. We refer to the general equilibrium of this economy as a decentralized monetary equilibrium (DME), with the defining property that the bitcoin price and its system security are *jointly* determined.

Our first main result is that the interaction between users and miners gives rise to multiple self-fulfilling equilibria, which can be ranked according to price–security levels. The reason is that, if agents anticipate the value of bitcoins will be low, miners have little incentive to invest in computational resources, and the security of the network is low. In that case, buyers do not wish to accumulate large real balances, and the resulting valuation for bitcoins is low. The opposite is true when agents anticipate the value of bitcoins will be high. A nonmonetary equilibrium, on the other hand, is always reached if the attacker's pockets are too deep, that is, if miners fail to acquire 50% of the system's computational power.

The important message here is that the security of PoW systems should be seen as an *economic outcome* and not as an embedded property of its blockchain technology, as often presented to businesspeople and regulators. Indeed, the same fundamentals and technology are consistent with equilibria displaying sharply different security levels.[3]

We present this result in Section 2 within a stylized three-period setting that purposely abstracts from a granular description of bitcoin exchanges. This allows us to distill the pivotal role of user–miner complementarities and highlights that the conclusions therein are robust to alternative representations of the demand for a means of exchange.[4] Next, to establish welfare and monetary policy analyses, Section 3 informs agents with more structure to make bitcoin-holding decisions, in the spirit of the Lagos–Rocheteau–Wright (2005, 2005) environment. Our focus is on the properties

[3]While we focus on PoW—spanning Bitcoin and several cryptocurrencies—we expect this implication to extend to blockchains using different consensus algorithms, as long as agents who invest in securing the system are compensated with nominal tokens. For example, the proposed implementations of proof-of-stake in Ethereum contemplate nominal block rewards for validators. Such proposed implementations include Casper the Friendly Finality Gadget, a hybrid of PoW and proof-of stake (PoS), and CBC (correct-by-construction) Casper, entirely based on PoS (e.g., see https://vitalik.ca/general/2018/12/05/cbc_casper.html). In contrast, it does not automatically extend to digital currencies such as Ripple's XRP and Facebook's Libra, whose security relies on trusted verifiers or external elements that are price insensitive (see Section 1).

[4]For example, the function V according to which agents value bitcoins therein can be regarded as a money-in-the-utility-function model, as representing a cash-in-advance constraint, or the reduced form of a search-based model.

of stationary DMEs; under certain conditions, we find an even number of them, which can be ranked not only according to price and security, but also welfare.

Our second contribution is to assess the optimality of monetary policy in a PoW-based system. We do so in regard to three plausible design goals: maximizing the token price, the system's security, and social welfare. A series of related results demonstrate the *impossibility* of simultaneously achieving these goals. To understand the trade-offs, take the valuation goal. A surprising finding is that Bitcoin's monetary policy can lead to violations of the quantity theory. Unlike with central banking, changes in supply growth, ρ, activate two opposing channels. A scarcity channel operates as usual, with less debasing leading to higher token prices. However, there is a new *security channel*: a higher mining reward incentivizes miners to invest, making the attacker's efforts less dangerous. For some equilibria, a value-optimal level for ρ exists; thus, a reduction in miners' nominal reward—such as quadrennial halvings—could leave the price unchanged or even decrease it.

The price-maximizing value is not necessarily optimal for aggregate welfare.[5] This is because bitcoin buyers, unlike a benevolent planner, do not internalize mining costs. Instead, the marginal buyer weighs the expected trade benefit of holdings against the inflation tax embedded in mining rewards—a transfer from users to miners here, with null aggregate effect. Therefore, price and welfare are generally not jointly maximized. We establish conditions that rank these policies according to fundamentals. We show that the ρ value that maximizes security is the highest and leads to both socially excessive mining and a relatively low token price.

Our third contribution is to show how Bitcoin's security model embeds price volatility amplification. We identify two separate mechanisms that are responsible for this conclusion, neither of which being the direct observation that supplies rigidity makes it impossible to accommodate demand fluctuations. The first mechanism concerns the amplification of fundamental shocks due to price–security feedback, which we illustrate considering the repercussions of a decrease in the number of bitcoin buyers. We show that this structural mechanism implies that a demand shock

[5] This is also in contrast with centralized money systems, where both the price of money and welfare are typically highest under the Friedman rule. Replacing a central bank with miners can, therefore, introduce a structural gap between the policies that are optimal for price and welfare.

induces a more pronounced price movement for bitcoin than for other currencies.[6]

The second mechanism concerns the emergence of stochastic equilibria in which expectations about future prices depend on sentiment, driven by the realization of a sunspot process. Any such equilibrium is defined by a set of optimistic and pessimistic states and a transition probability distribution. When optimistic states are observed, users and miners rationally expect high prices in the future, leading to high bitcoin prices in the present moment, and vice versa. We show that the multiplicity of stationary DMEs—stemming from Bitcoin's security model—is a *necessary* condition for the emergence of one such class of equilibria. Therefore, we argue that bitcoins are also more prone to exhibit seemingly irrational price jumps than other currencies.[7]

Finally, we develop an extension in which consumers opt between bitcoins and a fiat currency. While both are intrinsically worthless, we do not follow Kareken and Wallace (1981) in assuming perfect substitutability.[8] Indeed, consumers anticipate retailers might not accept all forms of payment, and they do not regard bitcoins and fiat currency as equally risky. We highlight three emerging insights. First, a sufficient condition for bitcoins to command a positive price is for bitcoins to be essential in some transactions.[9] Second, when bitcoins are valued, one also finds multiple equilibria with distinct price–security levels. This clarifies that multiplicity is inherent to Bitcoin's design, and not a consequence of a lack of payment alternatives. Third, the degree of bitcoin acceptability imposes further restrictions on their value. For example, take the case in which all retailers accept fiat currency, but some also accept bitcoins. We characterize a lower bound for the fiat currency inflation—strictly higher than Bitcoin's—that must be met for bitcoins to command a positive price.

This paper contributes to the small but growing literature on the economics of Bitcoin, blockchains,

[6]Moreover, we argue that the quantitative importance of the amplification mechanism depends on the sign of the shock and the strength of the potential attacker. We provide a related quantitative analysis in Section C of the Internet Appendix.

[7]Here, the impact of non-fundamental sources of uncertainty goes beyond price jumps. Due to miners' rational responses, the realization of a pessimistic state also implies that Bitcoin security can severely worsen, lowering the network life expectancy as measured by the average time until a successful attack. In Section C of the Internet Appendix, we simulate the distribution of attack times when agents ignore sunspots versus when they do not, and find that the expected time can drop significantly when sunspots play a role.

[8]Therefore, the exchange rate indeterminacy result in Kareken and Wallace's paper does not hold here.

[9]The sufficient condition that we establish could easily correspond to the use of bitcoins in the trade of criminalized goods, as documented by Foley et al. (2018). Take the case of the sale of illegal drugs over the dark web. It seems reasonable to regard sellers in that market as unable to accept other electronic forms of electronic payments, such as debit and credit cards. We highlight several more such uses in the discussion section.

and decentralized currencies.[10] In these environments, the multiplicity of equilibria manifests in various forms. Among them, Biais et al. (2019) formalize the coordination among miners regarding which blocks to append to the blockchain and establish conditions for stable consensus. Cong, He, and Wang (2018; 2019) have developed a token valuation framework that generates feedback between adoption and price. Li and Mann (2020) show the role that initial coin offerings can play in facilitating coordination in peer-to-peers platforms. Sockin and Xiong (2018) study decentralized platforms where tokens serve as membership certificates that facilitate transactions, featuring complementarity in membership demand. Our work complements these papers because we focus on a different but not mutually exclusive mechanism that embeds equilibria with price–security feedback. To distill our contribution, however, we intentionally abstract from additional multiplicity sources; absent security concerns, our model always features a unique equilibrium.

Multiplicity can also arise in traditional monetary models due to well-known channels such as entry externalities or storage costs (e.g., see Lagos et al., 2017, and the references therein), which are not featured here.[11] Also related are models of currency attacks against a central bank, where multiplicity is often a consequence of strategic complementarities among speculators.[12] Here, there is no monetary authority, but we do feature strategic complementarities: users' valuations positively incentivize miners' investment, which, in turn, reduces users' risk exposure to a malicious attack, raising valuations. Such a distinct complementarity manifests here to increase the payment system's defenses against sabotage, rather than induce an exchange-rate regime change. It also brings attention to the interaction between agents' beliefs and new economic fundamentals: the primitives of mining and the security function (covered in Sections 2.2 and 2.3).

[10] A related stream of research studies the economics of protocols that allow participants to agree on a common output that aggregates private inputs when some dishonest participants could attack the process. This question, known as the Byzantine agreement, was originally studied by Pease, Shostak, and Lamport (1980) and Lamport, Shostak, and Pease (1982). Nakamoto (2008) proposes a solution based on the PoW protocol.

[11] Equilibria multiplicity leads to price fluctuations driven by nonfundamental factors in Lagos and Wright (2003) and Gu et al. (2019), who feature economies where agents exchange Lucas trees with negative real yields; and in Asriyan et al. (2019), who focus on assets with heterogeneous payoffs under adverse selection. The environment here is fundamentally different: bitcoins do not pay dividends, and we do not incorporate private information.

[12] For example, in Obstfeld (1996), a trader realizes a greater payoff attacking a fixed–exchange rate regime if other traders also attack it. Strategic complementarities can also manifest through information feedback, as shown by Goldstein et al. (2011), where coordination by speculators can persuade the monetary authority to abandon the monetary regime due to weak fundamentals.

Several contemporaneous papers emphasize one or more aspects of the intricate Bitcoin mining ecosystem. While we focus on seigniorage-financed rewards, Easley et al. (2019) and Huberman et al. (2019) analyze the determination of fees with heterogeneous transaction urgency. Cong, He, and Li (2018) analyze risk sharing in mining pools, while Alsabah and Capponi (2019) analyze miners' R&D decisions. Budish (2018) analyzes the extent to which miners can defend Bitcoin against for-profit and sabotage attacks. Lehar and Parlour (2019) analyze the possibility of miner collusion. While their focuses differ, these papers take the value of bitcoin as a given. We contribute by developing a framework where mining outcomes, bitcoin demand, and prices are jointly determined.[13]

Chiu and Koeppl (2019) and Kang (2020) analyze related monetary economies but focus on the conditions under which double-spend attacks can be prevented as a function of the block confirmations required by retailers. Instead, we focus on the risk of sabotage attacks, which yield new equilibria with different positive implications. From a protocol design perspective, Chiu and Koeppl argue that it is optimal to finance the entire security budget with seigniorage, as in our setting, rather than with fees. Therefore, our characterization of the socially optimal inflationary reward complements their findings. A different and interesting angle on welfare is provided by Choi and Rocheteau (2019), whose model treats mining as an occupational choice against other productive uses, providing insights on output and social costs.

Also related is the literature on private monies pioneered by Hayek (1976) and recently fostered by Bitcoin. Among others, Fernández-Villaverde and Sanches (2016) use a search-based model to study competition among private currency issuers; Schilling and Uhlig (2019) study a Bewley-like model with a publicly and a privately issued currency. Although these papers introduce valuable features, they consider alternative payment systems to be perfect substitutes. We contribute in this regard by introducing heterogeneity in acceptance and explicitly incorporating Bitcoin's security shortcomings. This allows us to refine the conditions under which bitcoins can be positively priced.

[13]There is also a recent related literature on "permissioned" blockchains, similar in spirit to the privately secured token we use as a benchmark for Bitcoin. Besides monetary aspects, this literature focuses on implications for smart contracts, central banking, corporate governance, transaction efficiency, and capital markets (e.g., Harvey (2016); Malinova and Park (2017); Raskin and Yermack (2016); Yermack (2017)). Abadi and Brunnermeier (2018) provide a formal analysis of the trade-offs involving public and permissioned blockchains. Hinzen et al. (2019) and Zimmerman (2019) highlight limits to bitcoins' usability due to design aspects of its public blockchain.

1 Background

This section provides a description of how the Bitcoin security model, monetary policy, and attack risk interrelate and clarifies some of our modeling choices. For brevity, we relegate supplemental figures and technical details to Section A of the Internet Appendix (IA hereafter).

1.1 Security Model

Bitcoin's history of transfers is periodically updated in a sequence of blocks. Which particular miner adds a block is the result of a competitive process to solve a mathematical problem based on a cryptographic algorithm.[14] The winning miner is only compensated provided that the miner respected a set of consensus rules that prevents fraud; otherwise, the investment in computer power is entirely lost.[15] The winning miner's compensation, which we shall call the system's security budget, consists of the block reward plus any fees paid by users. Thus far, the block reward is the dominant component of the security budget. For the period from July 2010 to January 2020, on a daily basis, the block reward accounts for a median (mean) proportion of 99.21% (97.57%).[16]

Because the block reward is paid in bitcoins, which have no intrinsic value, miners must input the token price into their decisions. Such a connection finds strong empirical support in the price–hashrate time series displayed in Figure 1. Intuitively, the higher the price, the greater the incentive to respect the consensus rules, and the greater the cost to manipulate the ledger's history. Thus, the token price, p, and the security of the system, indexed by S, are linked. We note that this link is not exclusive to Bitcoin; it is present in blockchain-based networks such as Ethereum, Monero, and Litecoin. To distinguish it from alternatives, we refer to this security model as intrinsic.

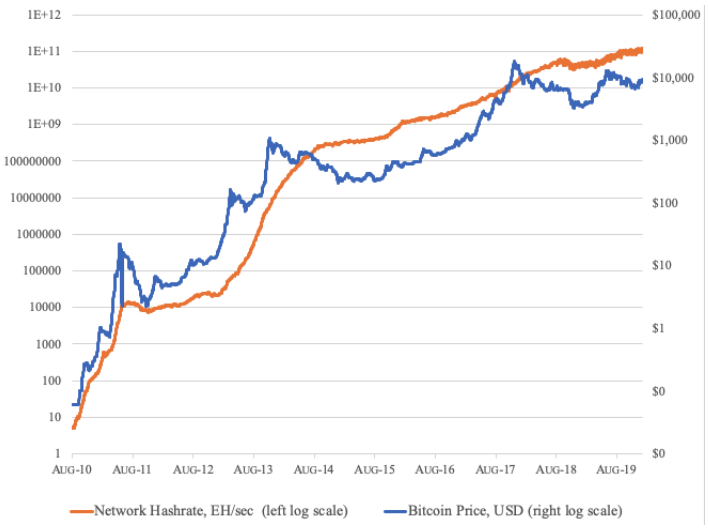
Definition 1. *We say that a token's security is* ***intrinsic*** *when* $p \neq p'$ *implies* $S(p) \neq S(p')$. *Otherwise, we refer to the token's security as* ***extrinsic****.*

[14] The solution to the problem is included in each new block and proves that the miner solved the problem—thus the term *proof-of-work*.

[15] For a textbook introduction to Bitcoin's protocol rules, see Antonopoulos (2017).

[16] See Section A.1 of the IA. An exception is the late part of 2017, when block congestion raised the proportion coming from fees quite substantially. We note that, while the block reward is part of the Bitcoin protocol, the amount collected in fees is not: fees depend on users' decisions. Nakamoto (2008) predicts that fees will slowly replace inflation over time as the total supply slowly approaches its asymptotic limit. There is no built-in protocol feature, however, that increases fees and smooths miners' nominal income.

Figure 1. Bitcoin price and network hashrate: August 2010 to January 2020



In contrast, Ripple is a digital currency system in which approved network members verify transactions. Although transfers of the network token, XRP, are subject to fees to avoid spamming, verifiers (e.g., a trusted bank) are not compensated for their services with XRP. Thus, we label Ripple's security model as extrinsic. The same can be said of similar permissioned blockchains such as Libra, Facebook's proposed digital currency.[17]

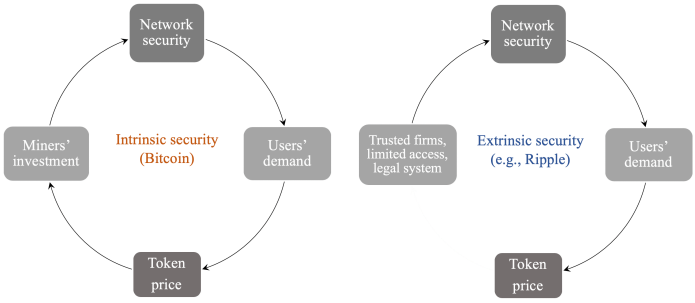
Extrinsic security could stem from the ability to exclude certain participants, reverse transactions, access regulators or the legal system, and so on. Identifying case-by-case sources is not our present focus. What is essential for our purposes is that pricing tokens with intrinsic security requires one to *simultaneously* account for their monetary and security functions, as in Figure 2.

1.2 Monetary Policy

Bitcoin's protocol-driven monetary policy is rigid: no authority can regulate the nominal supply. The only source of bitcoin creation is the block reward that miners receive. Because of its preprogrammed issuance scheme, future bitcoin supply can be approximated quite precisely, as illustrated in Section A.3 in the IA. The initial inflationary reward was set to 50 bitcoins by Nakamoto and is

[17] See https://libra.org/en-US/white-paper and see Section A.2 in the IA for additional examples.

Figure 2. Intrinsic and extrinsic security models



programmed to decline by 50% every 210,000 blocks, or approximately four years.[18] We can view each period between halving as an inflation *era* for Bitcoin. Within an era, nominal supply growth decreases slightly, since total supply increases but the reward stays constant.

1.3 Risk of Network Attacks

If there were no concerns about malicious players, the security task that miners perform would be trivial. Numerous types of mining-based attacks have been described in the computer science literature (see Conti et al., 2018; Kaiser et al., 2018l Liu et al., 2019, and the references therein). From an economic perspective, Budish (2018) considers two broad groups: double-spend and sabotage attacks. Put succinctly, in a double-spending attack, the attacker seeks to purchase a good through a bitcoin transfer and, upon delivery, to broadcast an alternative chain history that includes a transfer of the same coins the attacker's own wallet, rendering the original payment invalid.

The goal of a sabotage attack, on the other hand, is not to transfer the same bitcoins multiple times, but to hurt the network. Rosenfeld (2014) argues that such an effort can be motivated by external profit sources, such as protecting the profits of an incumbent—for example, the banking system or payment processing corporations—or profiting from a short position.[19] The motivation

[18]The first reward halving from 50 to 25 bitcoins occurred on November 11, 2012. The second halving occurred on July 9, 2016. The third halving took place on May 11, 2020. The last reward halving is estimated for 2140; further reductions would require a transfer to miners of less than 10^{-8} bitcoins, or one satoshi, the protocol's unit of account. See, for example, https://en.bitcoin.it/wiki/Controlled_supply.

[19]The scope for sabotage attacks has arguably increased recently, since many fiat-settled derivative products exist (e.g., from the CME Group), allowing for convenient short exposures to the bitcoin price. Although we do not model a separate bitcoin derivative or lending market that facilitates shorting, our framework embeds a negative relation between the efforts of the attacker and the underlying price.

could also originate in the success of a competing cryptocurrency, especially when the same mining equipment is used. Arguably stronger in scale is the possibility of not-for-profit actions by a governmental agency. Economic superpowers such as the United States and China and multilateral agencies such as the G20, have repeatedly expressed concerns about the national security, environmental, and financial stability hazards of cryptocurrencies.[20]

Like Budish, we argue that it is important to consider sabotage attacks explicitly. A double-spend attacker is interested in preserving the value of the recovered bitcoins and that of any specialized mining equipment. This fact creates a natural limit to the attack scale, to avoid a sharp price drop once the attack is identified. Moreover, being a for-profit effort, double-spend attacks might not be as much of a concern for Bitcoin relative to small blockchains, given its immense mining investment: they embed huge risky bets. Also critical is the fact that retailers can protect their wealth by requiring multiple-block payment confirmations before transferring goods. A saboteur is not dissuaded by the lack of within-network profits.[21]

Equally important, from the perspective of equilibrium pricing, is the fact that a sabotage attack is more akin to an *aggregate* source of risk, since it affects *all* participants, not just one or a few retailers. Therefore, we embed within a general equilibrium economy a stylized *saboteur* who could create disruptive blockchain histories (forks) designed to undermine confidence and destroy Bitcoin.

[20] As cryptocurrencies gain economic importance, one finds an increasing number of signals of such future actions. To cite a few examples, U.S. Treasury Secretary Steven Mnuchin has warned that cryptocurrencies pose a national security risk (see https://www.forbes.com/sites/billybambrough/2019/07/16/bitcoin-and-crypto-suddenly-branded-a-national-security-issue/#327b254f1a59). Policymakers expressed concerns during the Libra Congress hearing. Before the U.S. Congress Committee of Financial Services, the Federal Reserve Chairman Jerome Powell has warned that private digital currencies could come "fairly quickly" in a way that is "systemically important" (see, e.g., https://www.ccn.com/bitcoin-price-soars-jerome-powell-confirms-cryptos-threat-to-dollar). The G-20 group has repeatedly warned against the money laundering and terrorist financing risks that crypto-assets create. For instance, on June 9, 2019, a G20 Finance Ministers and Central Bank Governors Meeting communiqué asked the Financial Stability Board to "monitor risks and consider work on additional multilateral responses as needed" (https://www.mof.go.jp/english/international_policy/convention/g20/communique.htm). Agustín Carstens Carstens, head of the Bank for International Settlements, described bitcoin as "a combination of a bubble, a Ponzi scheme and an environmental disaster" in a speech given on February 6, 2018, at the University of Goethe. Chinese officials' efforts to ban bitcoin mining (see, e.g., https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4) are consistent with increasing the chances of a successful sabotage attack. Kaiser et al. (2018) provide an extensive discussion of potential hashrate-based attacks from China.

[21] According to the website Crypto51 (crypto51.app), as of February 2020, the market cost of matching Bitcoin's hashrate was approximately USD 860,000/hour. While that rate is prohibitively high for most individuals interested in a double-spend attack, it is not so for economic superpowers, or even global financial corporations.

2 Prices, Mining, and Security in a Three-Period Economy

In this section we show how user–miner complementarities in Bitcoin lead to equilibrium multiplicity, using a simple finite horizon setting. The characterizations of the mining game and attack risks serve as building blocks in the remainder of the paper.

2.1 Environment and Bitcoin Users

Consider two dates, t and $t+1$. At t, a continuum of n homogeneous agents can produce and consume a perishable good whose price acts as the numeraire. The marginal utility of consumption and disutility of production are unitary. There is also an intrinsically useless and transferrable token, bitcoin, in supply B. Agent i can purchase any non-negative amount B_{it} at a price p_t that is taken as given, thereby becoming a Bitcoin user. Agents acquire bitcoins because, if its transfer system is operational at an interim subperiod t', they expect to find uniquely beneficial exchange opportunities with probability f. We assume here that any holder i of a real balance $b_{it} = p_t B_{it}$ values those opportunities according to $V(\cdot)$, a continuous, strictly increasing and concave function that is twice differentiable and satisfies $V(0) = 0$, $V'(0) = +\infty$, and $V(\tilde{b}) = \tilde{b}$ for some $\tilde{b} > 0$.

The presence of a malicious agent, a saboteur, exposes all Bitcoin users to the risk of a systemwide attack between t and t'. The attack outcome is captured by the realization of a binary random variable $\tilde{x_t}$: $x_t = 1$ indicates that the network survives the attack and a new block of transactions will be added to the predetermined ledger, an event with probability S; $x_t = 0$ indicates a successful attack, an event with probability $1 - S_t$. Following an attack, the network is unusable and bitcoins become worthless. We refer to S, a key endogenous object, as the *security function*.

At $t+1$, if the attack failed, users sell any remaining bitcoin holdings in a liquidation market displaying perfectly elastic demand at an uncertain price p_{t+1}. Users' expectation of future prices is given by $\mathbb{E}_t p_{t+1} = S_t \mathbb{E}_t^1 p_{t+1} + (1 - S_t) \times 0$, where $\mathbb{E}_t^1$ denotes the expectation operator conditional on $x_t = 1$ and any available information at t. We require beliefs to satisfy $R := \mathbb{E}_t^1 \frac{p_{t+1}}{p_t} < \frac{1}{\delta S}$; otherwise, agents' expected utility would be increasing in bitcoins and demand would be unbounded.

Given beliefs and time preference $\delta \in (0, 1)$, agents maximize expected utility at t, $c_{it} - l_{it} +$

$\mathbb{E}_t\left(V\left(B_{it}p_t\right)+\delta c_{it+1}\right)$, over goods consumption c, disutility of production l, and bitcoin holdings, subject to the budget constraints $B_{it}p_t+c_t\leq l_t$ and $c_{t+1}\leq B_{it}p_{t+1}$. Expanding the expectation and incorporating the constraints, agent i's program becomes: $\max_{b_{it}\geq 0} S_t\left(fV\left(b_{it}\right)+\left(1-f\right)\delta b_{it}R\right)-b_{it}$.

It is helpful to consider a benchmark where security $\overline{S}\in(0,1]$ stems from a trusted institution rather than miners' actions. There can be at most one equilibrium price in that case. Provided $V'(0)$ is sufficiently large, a solution must exist, and we can associate any such security level $\overline{S}$ with a corresponding equilibrium price $\overline{p}_t>0$. To understand how the interrelation between users and miners can affect this conclusion, we turn to mining activities.

2.2 Miner Competition

At the beginning of t, $m\geq 2$ identical risk-neutral miners invest in computing power to win a block verification reward within a noncooperative PoW game. Miners are subject to a one-period reward lock. If a miner wins a block reward within t, the miner receives the reward at $t+1$, sells it at the prevailing price and consumes the proceeds.[22] We assume that the block size is large enough to include all contemporaneous transactions and that miners cannot commit to excluding transactions based on user fees. Hence, we concentrate on equilibria in which fees are negligibly small.[23]

Due to the random nature of the PoW race, the proportion of blocks verified by miner j is proportional to its computer power contribution. If a block confirmation occurs, j wins with probability $\mathbb{P}(h_j,h_{-j})=\frac{h_j}{H}$, $H=h_j+h_{-j}$. We assume that the PoW difficulty level adjusts to ensure that each block is verified within the corresponding period.[24]

Miners act as price takers and form expectations about next period's bitcoin prices. Conditional on winning, a miner expects revenues equal to $\psi\mathbb{E}_t^1 p_{t+1}$, where ψ represents the block reward in units of bitcoins. We simplify things by considering a single program for all miners given by

[22] As part of the decentralized verification process, each reward is locked for 100 blocks, or approximately $16\frac{2}{3}$ hours. After that period, miners can freely spend the proceeds.

[23] The Bitcoin Core wallet sets a minimum default fee of 10 nanobitcoins per vbyte (which represents 1/4,000,000th of the maximum size of a block). Such a tiny fee ensures that miners do not regard the transfer as spam. Fees are not mandatory, though.

[24] Mining difficulty in the Bitcoin network is determined approximately every two weeks (2,016 10-minute blocks) as a function of the average block confirmation time over that period. Therefore, the difficulty level is constant in the short run, but not over an extended period. In the Ethereum network (Metropolis release), difficulty levels are recomputed with every new block. As of August 2020, the average block confirmation time was within 14–15 seconds.

$\max_{h_j \geq 0} \mathbb{P}(h_j, h_{-j}) \times \delta\psi\mathbb{E}_t^1 p_{t+1} - C(h_j)$, where $C : h_j \to \mathbb{R}_+$ is the cost of mining function, an increasing, twice-differentiable function that satisfies $C''(h) \geq 0$ and $C(0) = 0$.[25] We search for a symmetric Nash equilibrium, which yields the following characterization of miners' investment.

Lemma 1. *In a symmetric mining equilibrium, (i) the system's hashrate, H_t^*, is given by mh_t^*, where*

$$h^* C'(h^*) = \left(\frac{m-1}{m^2}\right) \underbrace{\delta\psi\mathbb{E}_t^1 p_{t+1}}_{\text{Exp. real block reward}} . \tag{1}$$

Moreover, (ii) H^* increases with the nominal block reward and the expected bitcoin price, (iii) $\frac{dH^*}{dm} > 0$, and (iv) if C' increases point-wise for every h, H^* then decreases.

Part (ii) of Lemma 1 reflects the intuition that, ceteris paribus, a higher nominal reward or a higher expected bitcoin price induces miners to invest in more computing resources. The fact that miners are homogeneous yields a monotonically positive relation between the number of miners and the system hashrate. Point (iv) highlights that the cost of mining does not affect the allocation of the reward across miners, but is directly related to the total computing power in the system.

Hereafter, we focus on the case of linear mining costs $\kappa \times h$, where $\kappa > 0$ captures the costs of inputs, electricity, and any leasing hardware per unit of computational power.[26] Such a case best represents mining firms that are small enough to act as price takers in input markets.[27]

2.3 Security Function

We consider a source of aggregate risk in the form of a sabotage attack. Because such an attack on Bitcoin has not yet been observed, the specifics are not readily available. For concreteness, we

[25] Miners form rational expectations about the price but act on a subjective probability of receiving the reward equal to one, thus displaying bounded rationality. Rather than on miners, throughout the paper we focus on how bitcoin users price security risks. Relaxing this rationality constraint imposes no additional complexity here, since it solely requires multiplying miners' revenue by S. However, doing so could increase the number of general equilibrium allocations by making $S(H(p))$ a correspondence, without adding significant insights.

[26] To help with the interpretation, we can further disaggregate the mining cost equation as cost=electricity price (USD/kW h) * efficiency hardware (kW h/GH/s) * hashrate (GH/s). In this specification, electricity power is measured in dollars per kilowatt–hour and efficiency is measured in the number of kilowatt–hours to maintain a hashrate of a gigahash per second. For a given hardware efficiency, parameter κ can be interpreted as the product of the first two terms on the right-hand side of the equation.

[27] We consider an extension with a convex cost function in Section D of the IA.

consider the realization of a disruptive fork with $k > 1$ blocks, by which we mean the emergence of one (or multiple) alternative block history that creates a confidence crisis among users. As an example, the saboteur could mine numerous empty blocks, denying service to other users and/or inducing merchants to stop accepting bitcoins. The attacker could also employ hash power to generate multiple persistent forks in the blockchain, thereby undermining consensus and persuading honest miners to leave. We interpret parameter k as the minimum block length for such a disruptive fork to lead to a collapse in bitcoin demand.[28]

What is the likelihood of such an event? The answer must depend on the balance of computing resources between honest and malicious agents. To avoid excessive complexity, we regard the saboteur as a single agency endowed with a constant use-it-or-lose-it budget across periods that affords a hashrate $A > 0$. To assign probabilities to outcomes, imagine that once H has been determined on date t, a subgame arises in which the saboteur and miners play a race that ends when the former generates a k-block fork. At each step of the subgame, a PoW-like gamble takes place where miners and the saboteur have computing power given by H_t and A. The deficit of k blocks decreases by one with probability $\alpha := \frac{A}{A+H_t}$, and increases by one with probability $1-\alpha = \frac{H_t}{A+H_t}$, as in a binomial random walk. If this race continued forever within the subgame, the probability of eliminating the deficit of k blocks would be $\left(\frac{\alpha}{1-\alpha}\right)^k = \left(\frac{A}{H_t}\right)^k$, provided $\alpha < \frac{1}{2}$, and one otherwise.[29]

Next, we specify a security function that is consistent with the subgame above:

$$S\left(H_t, A\right) = \begin{cases} 1 - \left(\frac{A}{H_t}\right)^k & H_t > A, \\ 0 & \text{else.} \end{cases} \tag{2}$$

Function (2) allows for a tractable pricing analysis and, as Nakamoto first highlighted, it captures the notion that Bitcoin is not viable when honest miners control less than 50% of the hash power. Moreover, (2) satisfies the following intuitive properties: $\lim_{H\to+\infty} S = \lim_{A\downarrow 0} S = 1$, $\lim_{H\downarrow A} S = 0$,

[28] Alternatively, one could also consider sabotage attacks of heterogeneous strength. For example, the saboteur could periodically broadcast disruptive chains of length shorter than k, followed by negative valuation changes, not necessarily taking the price to zero. However, the key mechanism we model, connecting valuations to security, would still be present.

[29] This probability is a known result in gambler's ruin problems (e.g., Feller, 1968, Ch. XIV); we therefore omit the proof.

and, if $H_t > A$, $S_A < 0$ and $S_H > 0$. We informally refer to increases in A as increases in the saboteurs' budget. In what follows, we take k and A as a given and use (2) to endogenize the security level in the general equilibrium.

2.4 Indeterminacy of Price and Security in PoW Blockchains

Unlike for the extrinsic security benchmark, it is only by studying the relations between demand fundamentals, mining incentives, and the depth of the saboteur's pockets that we can assess whether a general equilibrium allocation exists, one in which the bitcoin price and security are jointly determined. To begin, we note that a situation in which the value of bitcoins stays at zero always represents an equilibrium. Absent external subsidies, if the price is zero, miners do not contribute security resources; in turn, users do not exchange any amount of goods for unsecured tokens.

Given token-holding decisions and market clearing, $nB_{it} = B$, miners' optimal investment in (1), and the security function in (2), we can reduce the system of optimality conditions to:

$$S\left(H\left(p_t\right), A\right)\left(fV'\left(\frac{B}{n}p_t\right) + \left(1-f\right)\delta R\right) = 1. \tag{3}$$

We shall show that, if it does exist, an equilibrium with a positive bitcoin price is no longer unique.

Proposition 1. *Assume extrinsic security $\overline{S}$. A single equilibrium exists if and only if $V'(0) > \frac{1}{f}(\frac{1}{\overline{S}} - (1-f)\delta R)$. Assume intrinsic security and a saboteur's hashrate $A > 0$. There is a population size $\hat{n}(A)$ such that if $n > \hat{n}(A)$, a general equilibrium must exist. Generally, if a general equilibrium exists, there is an even number of them, which can be ranked by price–security levels.*

Proposition 1 highlights that the multiplicity of equilibria originates in the strategic complementarities between users and miners. The intuition is that, if the value of bitcoins is perceived to be low, honest miners have little incentive to invest in computational resources, and the security of the network is low. In that case, agents do not wish to accumulate large real balances, and the resulting valuation for bitcoins is low. The opposite is true when the value of bitcoins is perceived to be high, making a high-value, high-security equilibrium self-fulfilling.

Figure 3. Equilibrium determination of bitcoin price and security

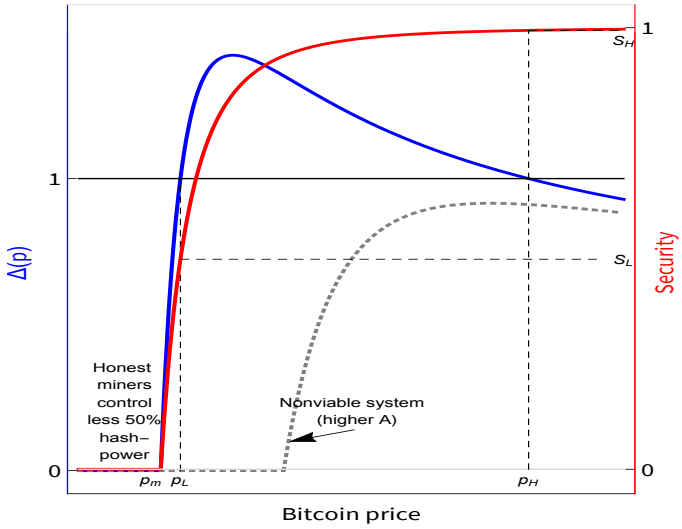


Figure 3 illustrates the equilibrium determination. Note that, for any given A, first, if the bitcoin price is sufficiently low, that is, $p \leq p_m := H^{-1}(A)$, the miners' economic incentive is not strong enough to amass 50% of the hashrate. In that case, the saboteur always succeeds, and the viability of bitcoins as a means of exchange vanishes. A general equilibrium is found when $\Delta(p_t) = 1$, where Δ represents the left-hand side of (3). Two such equilibria exist in the displayed economy, which can be ranked according to price and security levels: $p_H > p_L$ and $S_H > S_L$.

Second, a general equilibrium can be found, provided the number of interested buyers is high enough. Intuitively, if competition for bitcoins is strong enough, the anticipated value of the nominal block reward is sufficient to induce an investment $H > A$. Conversely, one can establish that, for a fixed n, the existence and properties of an equilibrium depend on how resourceful the attacker is. At one extreme, when $A \to 0$, the bitcoin economy converges to that with $\overline{S} \to 1$, a full-security economy with a unique equilibrium. At the other extreme, one can identify the maximum value that A can take to be compatible with an equilibrium. The dashed curve in Figure 3 illustrates an economy in which A is too high for an equilibrium with a positive price and security to exist.

To sum up, the noncooperative interaction between users and miners can bootstrap an equilibrium with a positive bitcoin price and some protection against malicious attackers. However, there is no one-to-one mapping between technological primitives and the security level: the same

fundamentals are compatible with a strongly or a weakly secured payment system. Put simply, one can only assess the security properties of a particular *equilibrium allocation* in a system such as Bitcoin, but not that of its blockchain technology.

3 Decentralized Monetary Framework and Welfare

The previous section elicited a fundamental mechanism in the Bitcoin system that generates a multiplicity of price–security ranked equilibria. In the remainder of the paper, we seek to understand its implications for welfare, the design of monetary policy, and price fluctuations. In this section, we therefore consider a more granular microfoundation for the use of bitcoins as a means of exchange, with an endless horizon, since we rule out token holdings providing enjoyment or dividend flows.[30]

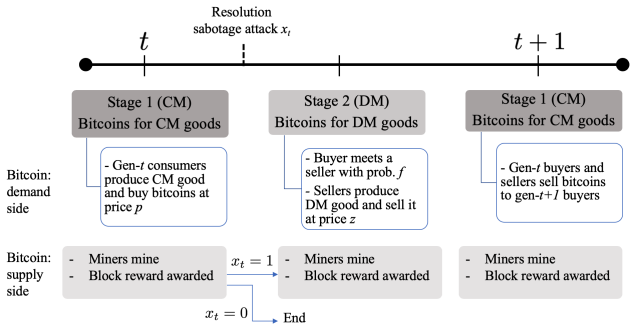
3.1 Bitcoin Demand

An endless sequence of dates is divided into two stages where different markets for perishable goods operate, both with Walrasian pricing. The first-stage market is frictionless, while the second-stage market is subject to meeting frictions, similar to the competitive equilibrium of Rocheteau and Wright (2005). Following convention, we refer to the first and second stages as the centralized market (CM) and the decentralized market (DM). All agents can produce and consume the CM good, which acts as the numeraire. Agents are divided into two types according to their roles in the DM: *sellers* can produce, but do not wish to consume; *buyers* wish to consume, but cannot produce. Such heterogeneity generates demand for bitcoins as a means of exchange; for buyers to consume the good in the DM—the *bitcoin good*. A buyer meets a seller with probability f and trades at a price z. All agents are anonymous, so credit arrangements are not possible.

Instead of assuming a liquidation market, the intertemporal consistency of users' holding decisions depends on an explicit demographic process. Each period t, a continuum of n buyers who live for three subperiods is born. Buyers born at time t have a lifetime utility given by

[30] Besides these essential motivations, the analysis in this section allows us to characterize dynamic stability properties of equilibria. For brevity, we defer such an analysis to Section B of the IA. Furthermore, in Section C therein, we develop a quantitative version of the model that illustrates how positive and welfare outcomes can sharply differ across equilibria.

Figure 4. Timeline



$c_t - l_t + u(q_t) + \delta c_{t+1}$, where c and q represent the consumption of the numeraire and bitcoin goods. Old buyers sell their bitcoin holdings, enjoy consuming the CM good with the proceeds, and then die.[31] Unless otherwise stated, u is assumed to be have the same properties as V in Section 2.1. A fundamental difference is that u is now defined over the consumption of goods. Sellers born at t do not need to accumulate bitcoins in that period's CM. Those who meet a buyer in the period's DM can produce any amount at a unitary marginal disutility of production. At the first stage of period $t+1$, sellers can exchange any bitcoin holdings for the CM good, from which they derive linear utility. Therefore, their lifetime utility is $-q_t + \delta c_{t+1}$.

Figure 4 summarizes the sequence of events in each period of this dynamic setting. On the supply side, miners compete for block verifications in each stage, as in Section 2.2, and receive rewards at the beginning of the subsequent CM. They do not consume the bitcoin good nor store bitcoins; the winning miner sells the reward immediately after receiving it to consume.[32] The resolution of the sabotage attack happens between the CM and the DM, before buyers and sellers meet. The fundamentals of security are as described by (2).

Buyers and sellers believe that the bitcoin price follows a Markov process, as follows. If bitcoins are not valued at the beginning of time t, $p_t = 0$, bitcoins will not be valued at any time $s > t$.

[31] As extensively discussed by Zhu (2008), the choice of linear utility for the CM good consumption makes this combination of overlapping-generation and search elements to be observationally equivalent to that of Lagos and Wright (2005), who present infinitely lived agents. Consistently with Zhu's arguments, our results can be derived by adopting either specification.

[32] The fact that miners sell their rewards once available best represents a situation in which miners do not regard themselves as having a speculative advantage over others and/or in which their main inputs (i.e., electricity) are not paid in bitcoins. In a general equilibrium, though, holding bitcoins across periods is costly, implying that miners would not hold them if given a choice.

Instead, if $p_t > 0$, the expected price next period is given by $S_t \mathbb{E}_t^1 p_{t+1}$: the price is zero following an attack. A buyer i born at time t maximizes intertemporal expected utility,

$$\max_{B_{it}, c_{it}, l_{it}} c_{it} - l_{it} + S_t \left(f \max_{q_{it}^d \leq \frac{B_{it} p_t}{z_t}} \left\{ u\left(q_{it}^d\right) + \delta \mathbb{E}_t^1 ((B_{it} - \frac{z_t q_{it}^d}{p_t}) p_{t+1}) \right\} + (1-f)\, \delta \mathbb{E}_t^1 \left(B_{it} p_{t+1}\right) \right) \quad (4)$$

subject to the budget constraint $B_{it} p_t + c_{it} \leq l_{it}$. Given that credit is not available, buyers in the DM are constrained by $z_t q_{it}^d \leq B_{it} p_t$, where q_i^d is the quantity agent i demands. The efficient exchange quantity, q^*, is given by $u'(q^*) = 1$, so that the buyer's marginal utility equals the seller's marginal cost of production. Let b^* denote the real bitcoin transfer required to get q^*.

The value that a seller j born at time t can obtain is given by:

$$\max_{q_{jt}^s} \left\{ -q_{jt}^s + \delta \mathbb{E}_t^1 \left(\left(\frac{z_t q_{jt}^s}{p_t} \right) p_{t+1} \right), 0 \right\}. \quad (5)$$

It is apparent from (5) that, provided sellers break even, which requires $\delta \mathbb{E}_t^1 \frac{p_{t+1}}{p_t} = \frac{1}{z_t}$, they are indifferent between any two positive production levels. We construct equilibria with this property; otherwise, the solution to the sellers' problem would require either a null or unbounded production.

Next, we characterize the demand for bitcoin holdings in a partial equilibrium, that is, taking $\{S_t\}_{t \geq 0}$ as a given sequence.

Lemma 2. *In any equilibrium, for all t, $\delta S_t \mathbb{E}_t^1 \frac{p_{t+1}}{p_t} \leq 1$ and $p_t = \delta S_t \mathbb{E}_t^1 p_{t+1} (1 + f(u'(q(B_t^d) - 1)^+)$. If the inequality is strict, all buyers demand the same bitcoin holdings $\frac{B_t}{n}$, the bitcoin good market clears at $q_t < q^*$, and there is a unique market clearing price $p_t = \delta S_t \mathbb{E}_t^1 p_{t+1} (1 + f(u'(\delta \frac{B_t}{n} \mathbb{E}_t^1 p_{t+1}) - 1))$.*

This lemma bounds the risk-adjusted expected holding returns that are compatible with a monetary equilibrium. When $\frac{\delta S_t \mathbb{E}_t^1 p_{t+1} - p_t}{p_t} < 0$, carrying a balance is costly; buyers will try to avoid doing so and will demand quantities of the bitcoin good below the efficient level q^*. The optimality condition in the lemma implies a positive relation between the security of the system and the demand for bitcoins. It also expresses that p_t equals the present value of the risk-adjusted expected price, plus a term reflecting bitcoins' usefulness as a liquidity instrument. Such a term is driven by the probability of finding trading opportunities, f, and by the Lagrangian multiplier associated

with relaxing the constraint $zq \leq b$ on the trade surplus, $(u'(q) - 1)^+$. We follow convention in referring to the latter as the *liquidity premium*, which is positive if $q < q^*$ and equals zero otherwise.

3.2 DME: Multiplicity and Welfare

We define a DME as a sequence $\{B_{it}, q_t^d, q_t^s, h_t, z_t, p_t\}_{t=0}^{\tau}$ of consumption, production, and saving decisions by buyers and sellers, hashrate decisions by miners, and positive prices, such that, for all t, buyers' and sellers' decisions satisfy (4) and (5); miners maximizes expected profits; security is given by (2); and all markets clear. Because equilibria depend on beliefs about the future value of bitcoins, the conceivable set is large. Instead of characterizing every possible equilibrium, we focus on whether there is a stationary DME with constant real quantities, and, if so, whether it is unique.

Bitcoins' supply growth is roughly constant within a four-year inflation era,[33] and is expected to halve at a quadrennial frequency until 2140. Unless one introduces a form of block congestion, there is no stationary DME with a vanishing nominal growth $\rho_t \to 1$; a perennially shrinking block reward leads to a security level that is inconsistent with a positive bitcoin price. Characterizing a functioning system that approaches the last halving event requires fees that somehow offset the loss of seigniorage, as argued by Nakamoto (2008). Accordingly, we pursue a two-part strategy. In the remainder of this section, we search for stationary DMEs with a positive and constant $\rho > 1$, constant real balances, and bitcoin prices that users and miners (conditionally) expect to decrease at the same rate, $\mathbb{E}_t^1 \frac{p_{t+1}}{p_t} = \rho^{-1}$ for all t. We consider that to be a helpful approximation *within* an inflation era.[34] Subsequently, we study the effect of supply growth changes in Section 4.

Accordingly, we reduce the model as follows. Given $B_{t+1} = B_t + 2\psi_t$, a constant ρ implies $\frac{\psi_t}{B_t} = \frac{\rho-1}{2}$. From (1), we can then write

$$H(b) = \left(\frac{m-1}{m}\right)\frac{\delta}{\rho}\left(\frac{\rho-1}{2\kappa}\right)b, \tag{6}$$

[33] This is especially the case since the reward halving in 2016, when the third inflation era began. For example, the nominal growth rates at the beginning and the end of the third inflation era are 4.17% and 3.58%; those for the fourth era, which started in May 2020, are 1.79% and 1.67%; and those for the fifth era, which starts in 2024, are 0.83% and 0.81%. As the outstanding supply increases, the ratio between these rates mechanically approaches one.

[34] Given constant real quantities, falling bitcoins prices are merely a consequence of growing supply with a constant number of bitcoin buyers. Accordingly, we can regard the steady-state characterization here as the one expected once the user base becomes stable.

and thereby express security as a function of b and A. Rearranging buyers' optimal demand condition in Lemma 2, for real balances below b^*, we must have

$$b_t = \frac{\delta}{\rho} S\left(b_{t+1}, A\right) b_{t+1} \left\{1 + f\left(u'\left(q\left(b_{t+1}\right)\right) - 1\right)\right\}, \tag{7}$$

where $q\left(b_{t+1}\right) = \frac{\delta}{\rho}\frac{b_{t+1}}{n}$. Denoting the right-hand side of equation (7) as D, a stationary solution is a value b_{ss} such that $b_{ss} = D(b_{ss})$. Equivalently, b_{ss} must satisfy:

$$f\left(u'\left(q\left(b_{ss}\right)\right) - 1\right) = \frac{\rho}{S\left(b_{ss}, A\right)\delta} - 1. \tag{8}$$

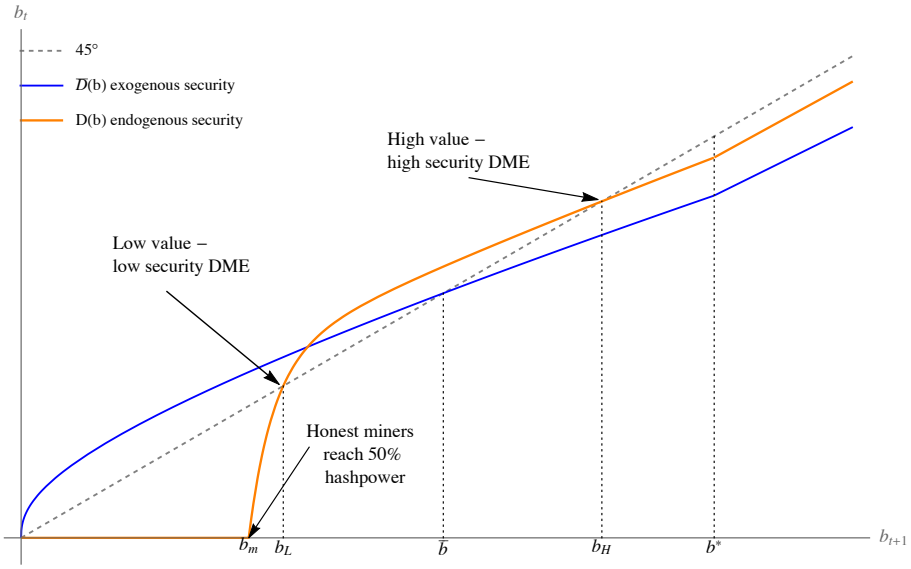
The condition in (8) expresses that b_{ss} makes the marginal usefulness of bitcoins equal to their marginal carrying cost. To see this, note that the left-hand side depends on the probability of finding trading opportunities and on the liquidity premium, expressing the payoff from a marginal unit of wealth that is liquid; that is, it can be used to acquire more of the bitcoin good. The right-hand side measures how costly it is for buyers to carry bitcoins and can be interpreted as a risk-adjusted analogue of the nominal interest rate, $i_B\left(b\right) := \frac{\rho}{S(b,A)\delta} - 1$.[35] Such a cost is positively related to the tax from inflationary rewards, and it is negatively related to the system's security.

An analysis of miners' and users' optimality in (6) and (8) allow us to characterize existence and uniqueness of a DME. Three main features are shared with the finite horizon setting in the previous section: a monetary equilibrium is not viable for $b \leq b_m = p_m B$; if the number of users is sufficiently large, the system can support an equilibrium with a strictly positive bitcoin price and security; such an equilibrium is not unique. Figure 5 illustrates the determination of equilibria in the (b_{t+1}, b_t) space. Two stationary DMEs exist in the displayed economy, b_L and b_H, which we refer to as the low and the high equilibria, respectively. The figure also displays the extrinsic security benchmark, $\overline{D}$. Where its unique equilibrium $\overline{b}$ is relative to b_L and b_H depends on the value of $\overline{S}$.[36]

[35] To facilitate this interpretation, imagine a one-period bond issued in the CM at a nominal price of Q *bitcoins* that cannot be used as a medium of exchange in the DM. This bond is redeemable for one bitcoin in the following CM, but defaults with probability $1 - S$. For agents to be indifferent about holding it, the bitcoin price of the newly issued bond must solve $Q_t p_t = \delta S \mathbb{E}_t^1 p_{t+1}$. Therefore, in a steady state, $Q = \frac{\delta S}{\rho}$, and the implicit nominal interest rate is $i_B = \frac{1}{Q} - 1 = \frac{\rho}{\delta S} - 1$. Since $S \leq 1$, $\rho > 1$ is sufficient for $i_B > 0$.

[36] If security is extrinsic, there is a single stationary monetary equilibrium if and only if $u'(0) > \frac{1}{f}(\frac{\rho}{\delta \overline{S}} + f - 1)$.

Figure 5. Decentralized monetary equilibria: Existence and multiplicity



However, this setting enables an explicit welfare assessment of equilibria. We take social welfare to be the sum of the surplus amounts that buyers, sellers, and miners realize, assigning a zero weight to the attacker,[37] net of mining costs. At the beginning of each period, each miner commits to invest an irrecoverable amount $\kappa h(b_{ss})$ in each stage. Using (6), the period's welfare can be expressed as

$$\mathcal{W}_{ss} = \mathbb{E}\underbrace{\left(u\left(q\left(b_{ss}\right)\right) - q\left(b_{ss}\right)\right)n}_{\text{bitcoin good trade surplus in the DM}} - \underbrace{\left(\frac{m-1}{m}\right)(\rho-1)\frac{\delta}{\rho}b_{ss}}_{\text{aggregate mining investment}}, \tag{9}$$

where the expectation is over security outcomes and trade opportunities in the bitcoin good market. Only the DM surplus appear in (9), since exchanges in the CM represent zero-sum utility transfers.

Using (9), we establish two welfare properties. First, consider the case in which buyers formed bitcoin demand decisions in the same environment, but sought to (altruistically) maximize (9) instead of (4). Such a case resembles the problem of a *constrained* planner who *cannot* affect the system design but internalizes mining costs. Perhaps surprisingly, the demand for bitcoins would

[37] Equivalently, one can consider any potential social benefits from a successful attack, such as regulation enforcement, to be offset by the attackers' mining investment. The case with large positive attack externalities is less interesting, since the planner can always set ρ at a level that is too low for a monetary equilibrium to exist. Alternatively, if the attack generated negative externalities, for example, discouraging investment elsewhere, the planner would seek to increase the security budget further.

then be higher. The reason is that balances' carrying cost associated with (4), which input the inflationary reward, can be shown to be above mining costs.[38]

Second, we can rank welfare outcomes across DMEs: the high equilibrium leads both to a higher trade volume q and also to greater social welfare. Indeed, the equilibrium condition (8) implies that an increase in the exchange quantity from q_L to $\tilde{q}$, provided $\tilde{q} < q^*$, leads to an enhancement in the expected trade surplus that is greater than the corresponding increase in mining costs.

We summarize the main results in this section in the following proposition.

Proposition 2. *A stationary DME must exist, provided n is sufficiently large. Generally, if it does exist, there is an even number of them that can be ranked according to price, security, and welfare.*

4 Implications for the Design of Monetary Policy under PoW

Nakamoto's protocol prevents any agent, user or miner, from influencing bitcoins' supply. Therefore, analyzing monetary policy in the traditional sense of regulating the money supply is not possible. Instead, this section adopts a protocol design perspective. The main results establish the optimal monetary policy associated with three goals, namely, maximizing bitcoin's market value, the system's security, and social welfare, and characterizes the relations among them.

4.1 Value-Optimal Monetary Policy

We begin by considering the optimal policy regarding market value. Recall that a central implication of the quantity theory is that increases in the growth of nominal balances have a negative effect on the price of money. This implication holds in our benchmark with extrinsic security. Increasing supply growth ρ through direct transfers to agents, or a nominal dividend, has the effect of reducing the equilibrium token price as it becomes less scarce.

[38] To see this, use $b_i = \frac{b}{n}$ to express (4) as a choice over q: $\max_{q \geq 0} Sf\left(u\left(q\right) - q\right) - q\left(\frac{\rho}{\delta} - S\right)$. Similarly, combine (6) and (9) to express the constrained planner's objective as $fS\left(u\left(q\right) - q\right) - \frac{m-1}{m}\left(\rho - 1\right)q$. The first-order conditions require, for buyers, $u'\left(q_{\text{buyer}}\right) = 1 + \frac{1}{fS}\left(\frac{\rho}{\delta} - S\right)$; for the constrained planner, $u'\left(q_{\text{cp}}\right) = 1 + \frac{1}{fS}\frac{m-1}{m}\left(\rho - 1\right)$. Since $\frac{\rho}{\delta} - S > \frac{m-1}{m}\left(\rho - 1\right) > 0$, and u' is strictly decreasing, it follows that $q_{\text{buyer}} < q_{\text{cp}} < q^*$; therefore, $b_{\text{buyer}} < b_{\text{cp}}$. One can show that the general equilibrium of the economy where demand is based on (9) also features multiplicity. Bitcoin prices would be higher in such an economy than in a DME if one compares the high equilibria, and lower if one compares the low equilibria. The intuition is similar to a fundamental shift in demand in Section 5.1.

Bitcoin is different, since we can distinguish *two* distinct channels by which changes in ρ affect the bitcoin price. While the scarcity channel operates as above, there is a *security* channel that is new to the Bitcoin economy. Since there are no dividends for bitcoin users, all new issuances are restricted to miner rewards. Increasing the latter incentivizes miners' investment, strengthening resistance against a malicious player, thus generating upward price pressure.

The relative strength of each channel depends on the fundamentals. Intuitively, when ρ is low, the security channel should be relatively stronger, and increases in ρ should have a positive price effect; when ρ is high, the negative scarcity effect should dominate. We are interested in whether there is a ρ value that finds the optimal balance in the sense of maximizing the market value of bitcoins. The following proposition shows that we can characterize such value for a high DME.[39]

Proposition 3. *The value-optimal nominal growth rate, ρ_V, is implicitly given by*

$$\epsilon_{S,\rho}\left(\rho_V\right) = 1 - \frac{i_B(\rho_V) + f}{i_B(\rho_V) + 1}\sigma(b_H), \tag{10}$$

where b_H is the highest solution to (8), $S = S\left(b_H, A\right)$, and $\sigma\left(b_H\right)$ is the coefficient of relative risk aversion at b_H, and $\epsilon_{S,\rho} := \frac{dS}{d\rho}\frac{\rho}{S}$. If $\rho < \rho_V$, p_H increases with ρ; if $\rho > \rho_V$, p_H decreases with ρ.

Equation (10) expresses that ρ_V renders the marginal value of security gains equal to the marginal impact on buyers' and sellers' carrying costs. To illustrate, consider the special case with $f = 1$ and a constant $\sigma \in (0, 1)$. The right-hand side of (10) becomes $1-\sigma$. Since $\epsilon_{S,\rho}(\rho_V) = \frac{k(1-S)}{S(\rho_V - 1)}$, $\rho_V = 1 + \frac{k(1-S)}{(1-\sigma)S}$. From this we infer that an increase in k causing $S \to 1$ leads to $\rho_V \to 1$: as security needs progressively diminish, the value-optimal amount of mintage approaches zero.

Proposition 3 implies that the behavior of the supply side of Bitcoin is fundamentally different from that of traditional monetary economies, since the graph $(\rho, p_H\left(\rho\right))$ is concave. The left of Figure 6 illustrates this property. For values $\rho > \rho_V$, the negative impact of the scarcity channel is stronger than that of the security channel, and the price declines. A direct implication is that, unless $\rho = \rho_V$, the same p_H is consistent with two different regimes, with low or high supply growth.

[39] For the low DME, one can show that, if a solution to equation (10) exists, it does not satisfy the second-order conditions for a maximum.

Besides protocol design concerns, Proposition 3 has practical implications for understanding changes in bitcoin prices over time. Commentators often argue that a block reward halving causes the bitcoin price to increase; in contrast, we find that the price effect of a change in ρ is non-monotonic: the price can increase or decrease.[40]

To sum up, the general equilibrium relation between supply growth and price depends on the environment, as in (10), and should thus be considered with more scrutiny than a simple application of Fisher's equation of exchange would suggest. Such careful consideration is particularly important for Bitcoin, since its design prevents any issuances directed to holders; if one introduced these, a violation of the quantity theory would become less likely.

4.2 Security-Optimal Monetary Policy

We now ask what is the supply growth rate that maximizes the system's security? The answer links to miner incentives. Naturally, miners' investment is not based solely on the bitcoin price, but, rather, the product between that price and the block reward. Provided such product increases, one could observe that prices and miners' hashrate move in *opposite* directions, as graphically illustrated on the left panel of Figure 6 as one move to the right of ρ_V. Accordingly, we seek to determine what is the growth rate that maximizes miners' expected income, which, in a steady state can be expressed as $\frac{\rho-1}{2}\frac{\delta}{\rho}b_{ss}(\rho)$.[41] It is clear that income is highest in the high DME, and its maximizing value ρ_S is as follows.

Proposition 4. *The supply growth rate that maximizes miners' security budget is given by*

$$\underbrace{\frac{b_H}{\rho_S}}_{\text{Qty. effect}} + (\rho_S - 1)\underbrace{\left(\frac{1}{\rho_S}\frac{db_H}{d\rho} - \frac{b_H}{\rho_S^2}\right)}_{\text{value effect}} = 0. \tag{11}$$

The security-optimal rate ρ_S is higher than that maximizing the market value of bitcoin, ρ_V.

[40] To evaluate different scenarios quantitatively, in Section C.3 of the IA, we simulate events studies where ρ halves.

[41] Alternatively, one can seek to maximize miners' seigniorage, Π, defined as the difference between miners' real reward and the cost of mining. However, miners' seigniorage vanishes in the perfectly competitive limit $m \to \infty$, while security is highest. To see this, note that, in any stationary DME, $\Pi = \left(\frac{\rho-1}{2}\right)\frac{\delta}{\rho}\frac{b_{ss}}{m}$.

The proof is immediately evident, as follows. Since $\rho > 1$ in any DME, for (11) to hold, one must have $\frac{db_H(\rho_S)}{d\rho} < 0$. From Proposition 3, real balances in the high DME decrease for values higher than ρ_V, implying $\rho_S > \rho_V$. Intuitively, bitcoin buyers are concerned with both the inflation tax and security risks. Minimizing the latter exclusively leads to a relatively weak user demand and, thus, a lower token valuation.

4.3 Socially Optimal Monetary Policy

We are interested in this section in the optimal monetary policy from the perspective of a benevolent planner, denoted as ρ_W. We begin by considering the benchmark economy without mining investment and a given security level $\overline{S}$. In that case, the first-best DM surplus can be achieved by $\overline{\rho}_W = \overline{S}\delta < 1$.[42] The intuition is that the net nominal growth must be negative so that the token price appreciation is sufficient to compensate for attack risks and impatience, inducing buyers to carry enough balances to achieve an efficient exchange.[43] This is a version of the Friedman rule, which is the optimal monetary policy in many monetary environments (Rocheteau and Nosal, 2017, Ch. 6). The adjustment by $\overline{S}$ simply reflects the lack of a risk-free saving technology.

For Bitcoin, negative nominal growth is arguably unfeasible due to taxation challenges. More importantly, $\rho_W \leq 1$ would be undesirable with seigniorage-financed security, since a null exchange surplus would be achieved with null security. In this regard, a Friedman rule cannot be optimal.

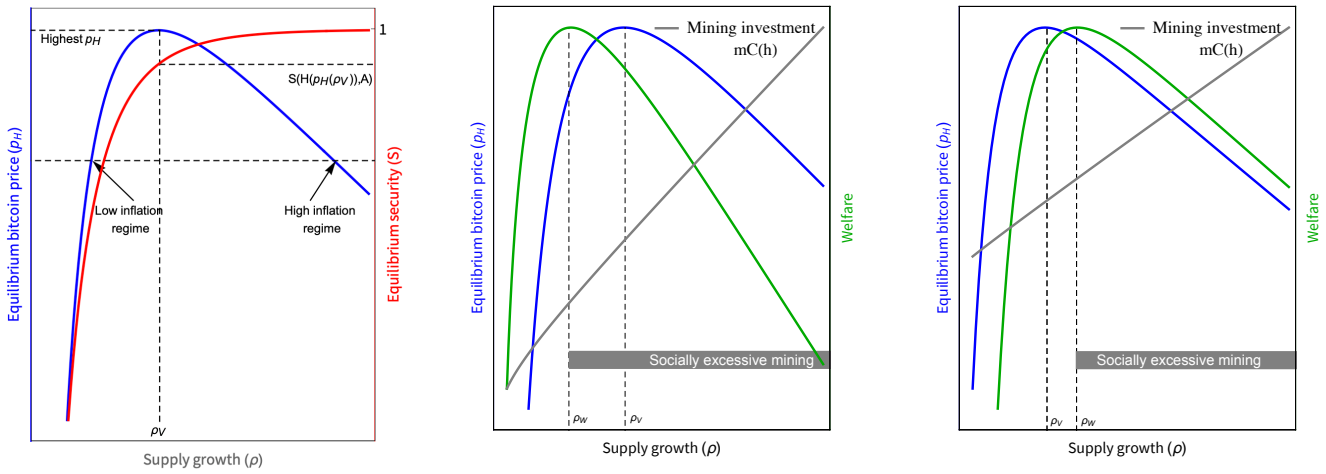
Instead, the socially optimal policy is implicitly given by $\frac{d\mathcal{W}}{d\rho}(\rho_W, b(\rho_W)) = 0$ from (9), subject to the satisfaction of users' and miners' optimality in (6) and (8). We note that the social and private benefits associated a change in ρ on the trade surplus coincide; buyers capture the entire surplus. The social and private costs, however, are different. Buyers are concerned with balances' carrying costs regarding issuances received by the miners and attacks' risk. All else equal, the planner is involved with the amount invested in mining, not with buyers' inflation tax; a mere transfer from

[42] Note that for $S_t = \overline{S} \in (0, 1]$, we can express (8) as $u'(\overline{q}_{ss}) = 1 + \frac{1}{f}\left(\frac{\overline{\rho}_W}{\delta \overline{S}} - 1\right)$. Therefore, $\overline{\rho}_W = \overline{S}\delta$ implements the efficient allocation: $u'(\overline{q}_{ss}; \overline{\rho}_W) = 1$.

[43] A traditional implementation of the Friedman rule in fiat monetary systems involves taxation. Interestingly, Cong et al. (2019) find that negative nominal growth is achievable in permissioned token platforms through owners' buybacks and token burns.

Figure 6. Bitcoin supply growth: Relations with price, security, and welfare

The left and middle (right) panels correspond to the utility function parameter $\sigma = 0.5$ ($\sigma = 1.5$). All other parameters are as in the baseline calibration in Section C of the IA.



(a) Price and security (b) Welfare: $\rho_W < \rho_V$ (c) Welfare: $\rho_W > \rho_V$

users to miners. Hence, the monetary policy that most benefits buyers and that which is socially optimal could differ. The planner finds that mining investment increases with ρ up to ρ_S; the effect on private carrying costs is ambiguous, since an increase in S could decrease the ratio $\frac{\rho}{\delta S}$.

The following proposition establishes the relation between the socially optimal monetary policy and the considered alternatives.

Proposition 5. *The socially optimal monetary policy ρ_W satisfies the following properties: (i) $\rho_W > 1 > \overline{\rho}_W$; (ii) $\rho_W < \rho_S$; and (iii) $\rho_W < \rho_V$ provided $S\left(\epsilon_{S,\rho} f\left(\frac{u(q)}{q} - 1\right) - i_B\right) < \frac{m-1}{m}$ at $\rho = \rho_V$, and $\rho_W > \rho_V$ if the inequality is reversed.*

The intuition for (ii) is that a planner would not select $\rho_W > \rho_S$ because such a policy would result in greater distortions on q and, by the definition of ρ_S, in lower security as well. The case $\rho_W = \rho_S$ could only hold in the counterfactual scenario in which q were unaffected by ρ.

We note that the inequality in (iii) expresses the relation between the marginal impacts of a change in ρ near ρ_V on the trade surplus (left-hand side) and mining costs (right-hand side). The net effect on the trade surplus depends on the positive effects on security, measured by the elasticity

term $\epsilon_{S,\rho}$, and the negative effect on q due to inflation; captured by i_B in an equilibrium. Regarding costs, a marginal increase in ρ has only a quantity effect on miners' reward, since $\frac{db(\rho_V)}{d\rho} = 0$. The planner is concerned with the fraction $\frac{m-1}{m}$ of that reward spent in mining, not with miners' profits.

Depending on the primitives, there could be socially excessive mining at ρ_V. We illustrate this point with an example in Figure 6, using a generalized CRRA function $u(q) = \frac{1}{1-\sigma}((q+\xi)^{1-\sigma} - \xi^{1-\sigma}),\xi \approx 0, \sigma > 0$. The middle and right panels are otherwise identical but feature a low and a high σ value.[44] In the middle panel, at $\rho = \rho_V$, the marginal impact of a change in ρ on carrying costs is lower than that on mining costs; again, due to the beneficial increase in S in regards to i_B. Accordingly, the planner would find it optimal to reduce the bitcoin issuance rate to economize on mining costs. The opposite holds in the economy displayed on the right panel: the marginal impact of a change in ρ at ρ_V is lower on mining costs. Relative to ρ_V, the planner seeks to marginally increase ρ to provide miners with better incentives and increase the trade surplus' expected value.

5 Implications for Bitcoin Price Volatility

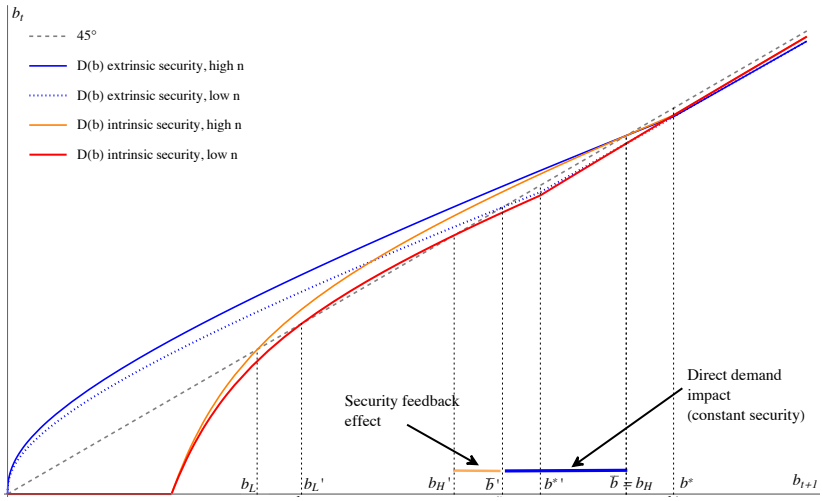
What does Bitcoin's security model imply for price volatility? We identify two mechanisms with the potential to amplify price fluctuations, each associated with a distinct source of uncertainty. The first mechanism is the amplification of a fundamental shock in bitcoins' demand, and the second is volatility induced by sentiment shifts that are unrelated to fundamentals.

5.1 Bitcoin's Security and Price Amplification of Fundamental Shocks

Consider a fundamental change in money demand due to a change in the number of bitcoin buyers. We contrast the steady-state equilibrium response for tokens with intrinsic and extrinsic security. To establish a meaningful contrast, we concentrate on the high DME, since the low DME is unique to bitcoins. Bitcoin security is $S(b_H, A)$ and an otherwise identical token has security $\overline{S}$. From (8), if $\overline{S} = S(b_H, A)$, the stationary value of real balances must coincide: $b_H = \overline{b}$.

[44] We note that one can illustrate the same point using other model parameters. The utility curvature parameter σ intuitively connects to the value of the trade surplus. Equilibria with relatively high σ values display relatively high trade surpluses; also high security levels, since buyers are willing to pay a high price for the token that miners receive as rewards, increasing the system's security budget.

Figure 7. Price change amplification of an adverse change in the number of buyers



How is the value of each token affected by a change in n? In the extrinsic case, we know from Lemma 2 that an increase in n raises the marginal value of liquidity in the DM; thus, the new steady-state price must be higher, and vice versa. The following proposition shows that, for bitcoins, an identical change in n causes *greater* equilibrium price movements.

Proposition 6. *Consider a high DME for Bitcoin with security* $S(b_H, A)$ *and an otherwise identical token with extrinsic security* $\overline{S} = S(b_H, A)$*. A change in the number of buyers induces a more significant equilibrium price change for bitcoins:* $\left|\frac{db_H}{dn}\right| > \left|\frac{d\bar{b}}{dn}\right|$.

Figure 7 illustrates the equilibrium price change. A decrease from a high to a low value of n causes the demand for real balances to weaken. The direct impact of this change in demand on $\bar{b}$, with security held constant, is given by $\left|\bar{b}' - \bar{b}\right|$. For Bitcoin, however, miners' incentives are also affected, generating a negative system hashrate response and, thus, a decrease in security that *feeds back* the downward pressure on the price. The price impact of the endogenous security response can be graphically seen as $\left|b_H' - \bar{b}'\right|$. Conversely, a positive increase in demand would generate a positive mining response, and a greater equilibrium price increase for bitcoins. Therefore, failing to consider the structural connection between price and security could lead to systematic mispricing and underestimating the price volatility for bitcoins and similar PoW blockchains.

We comment further on the interpretation of this result. First, if one naively ignored the equi-

librium price–security connection, one should not expect pricing errors to be symmetric. Provided that mining investment has a decreasing marginal impact on security, mispricing is likely to be more pronounced for *negative* shocks.[45] Second, we should not expect this type of amplification to be a transient effect, but a structural feature. Since the system's security is tied to an internal budget, the probability distribution over security outcomes depends on the bitcoin price. Third, because meaningful price changes are more likely to trigger security reassessments, this mechanism connects more naturally to long-term price movements[46] (quarterly, yearly) rather than high-frequency ones.

5.2 Non-fundamental Uncertainty, Price Booms, and Crashes

We observe more frequent booms and busts in the bitcoin's price than for most currencies. What makes them particularly puzzling is that they often occur without any apparent link to fundamentals (e.g., Bhambhwani et al., 2019). In this section, we analyze the potential role of non-fundamental uncertainty (Azariadis, 1981; Cass and Shell, 1983) by constructing equilibria in which the price of bitcoin can jump based on agents' sentiments, which are driven by sunspots. We show how the scope for such unpredictable jumps is broader for bitcoins than for traditional currency.

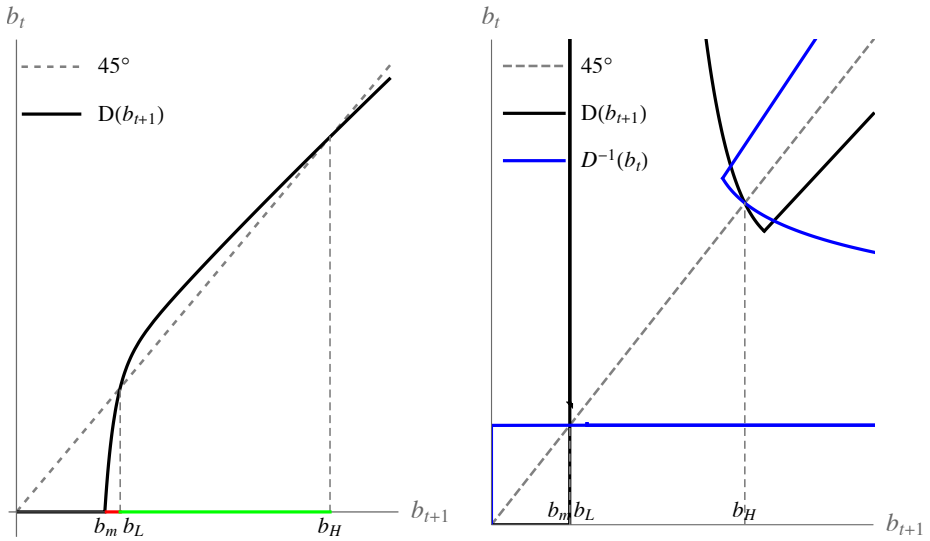
Following Lagos and Wright (2003), we focus on stationary equilibria in which bitcoin balances change stochastically as a function of the realization of a sunspot variable, but not of time. We consider a two-state Markov chain with states $\omega \in \{1, 2\}$ and $\phi_\omega := \mathbb{P}(\omega_{t+1} = \omega | \omega_t = \omega)$. The realization of the sunspot is publicly observed at the beginning of each DM, which affects the terms of trade. When agents observe ω, the value of real balances is b_ω and the quantity exchanged is $q_\omega = \frac{\delta}{\rho}\frac{b_\omega}{n}$. Without loss of generality, let $\omega = 2$ be the optimistic state, $b_2 > b_1$. In the CM, in turn, miners and buyers make decisions anticipating that sentiment could change later in the same period. Miner investment is as in (1), but based on a valuation for balances given by

[45] We provide a quantitative perspective that illustrates this point in Section C.4 of the IA. By decomposing the effect of fundamental shocks, we also show that the relative importance of the security amplification mechanism increases in the strength of the attackers' commitment as measured by A.

[46] The bitcoin/USD exchange rate can experience massive displacements yearly that begets security reassessments. To illustrate, during the recent boom and bust cycle, the bitcoin price increased by 1,413% in 2017 (from USD 951 to USD 14,388), then decreased by 74% in 2018 (to USD 3,743), and rose again by nearly 100% in 2019 (to USD 7,432). Although Bitcoin did not experience successful attacks during the 2018 price downturn, several smaller PoW chains did (see Section A.5 of the IA).

Figure 8. Sunspot equilibria

The left (right) panel corresponds to the utility parameter $\sigma = 0.5$ ($\sigma = 7$). All other parameters are as in the baseline calibration in Section C of the IA.



$\mathbb{E}_\omega b = \phi_\omega b_\omega + (1-\phi_\omega) b_{\omega'}$, $\omega \neq \omega'$. For buyers, given a security assessment $S_\omega := S(\mathbb{E}_\omega b, A)$, the natural extension of the program in (4) results in a two-equation system determining b_1 and b_2:

$$b_\omega = \frac{\delta}{\rho}\left(\phi_\omega S_\omega b_\omega \left(f\left(u'\left(q_\omega\right)-1\right)+1\right) + \left(1-\phi_\omega\right) S_\omega b_{\omega'} \left(f\left(u'\left(q_{\omega'}\right)-1\right)+1\right)\right), \omega \neq \omega'. \tag{12}$$

For a given b_1 and b_2, we are interested in whether probabilities $\phi_\omega \in (0,1)$ that satisfy (12) can be found to support sunspot equilibria. This is possible under two types of conditions:

- Type I: $D(b_2) > b_2 > b_1 > D(b_1)$,
- Type II: $D(b_1) > b_2 > b_1 > D(b_2)$.

Type I requires function D to cross the 45-degree line from below between b_1 and b_2, as in the left panel of Figure 8. One finds therein a continuum of such equilibria for $b_1 \in (b_m, b_L)$ and $b_2 \in (b_L, b_H)$, as shown by the red and green segments. Type II requires D to cross the line from above, as in the right panel. In this case, b_1 and b_2 belong to the area of overlap between $D(b)$ and $D^{-1}(b)$ in the proximity of b_H.

The existence of Type II equilibria relies on the specifics of the preferences and parameters. For example, regarding the figure's parametrization, a large value of the utility parameter σ is needed. Therefore, regardless of the security model, Type II equilibria may or may not exist. It is important to stress is that Type I equilibria can *only* exist when the security function and the token price interrelate—yielding multiple DMEs—as we state in the following proposition.

Proposition 7. *Only Bitcoin can satisfy the existence conditions for Type I and II equilibria.*

Since both types are viable for Bitcoin, we can say that, relative to other currencies, bitcoins are more prone to exhibit seemingly irrational and unpredictable price jumps.[47] Indeed, for some primitives, conventional currencies on a stationary equilibrium path would never feature price booms and crashes, while bitcoins can, as in the left panel of Figure Figure 8.

6 Bitcoin in a Bimonetary Economy

In this section, we consider an extension with two payment systems, Bitcoin and a fiat currency. Although we do not attempt to model every conceivable difference between these systems, we emphasize that they are *not* perfect substitutes. Our differentiating focus is on security risks and their liquidity function regarding one's ability to conduct certain transactions. Allowing for such heterogeneity helps in clarifying the conditions under which bitcoins are valued. It also illustrates the model's application to more complex settings.

The determination of Bitcoin's security is as in Section 3. Fiat currency can be purchased in the CM at a price ϕ and is not subject to sabotage attacks. The growth rate of fiat supply, M, is constant and denoted $\gamma = M_{t+1}/M_t$. We focus on steady-state equilibria in which real quantities, including real monetary balances $b_t = p_t B_t$ and $\mu_t = \phi_t M_t$, are constant over time; accordingly, agents expect $\frac{\phi_{t+1}}{\phi_t} = \gamma^{-1}$ and $\frac{p_{t+1}}{p_t} = \rho^{-1}$.

On the transaction side, we consider the possibility that not all sellers accept each form of

[47] Although we focus on price volatility in this section, the emergence of sunspot equilibria also affects the system's ability to resist attacks. When sunspot equilibria exist, each generates a transition matrix over states $\{0, b_1, b_2\}$. If the quantitative gap between b_1 and b_2 is large, the system's lifetime could be meaningfully affected by nonfundamental sentiment shifts. Section C.5 of the IA provides examples.

money in the DM.[48] More specifically, buyers anticipate three types of meetings $\tau \in \{B, M, MB\}$, reflecting whether sellers accept bitcoins only, fiat currency only, or both. We denote as f_τ the probability that the buyer meets a seller of type τ and $f = \sum_\tau f_\tau$. The competitive prices for the goods traded in the DM are z_B if bitcoins are used and z_M if the fiat currency is used.

The sellers' break-even condition resembles that in previous sections; for sellers to be indifferent between any two production levels, one needs z_B and z_M to compensate for their balances' carrying cost. Thus, $z_B = \frac{\rho}{\delta}$ and $z_M = \frac{\gamma}{\delta}$. An MB-type seller is willing to exchange a given production level q_{MB} with buyer i for any combination of b_i and μ_i as long as $q_{MB} = \left(\frac{b_i}{z_B} + \frac{\mu_i}{z_M}\right)$.

The buyers' program is a generalization of (4) that yields an optimal choice of bitcoin and fiat holdings. Besides the corresponding budget constraints, buyers face a liquid wealth constraint in the DM that now depends on the type of seller in a given meeting. When both monies are valued in a given equilibrium, buyers' choices must satisfy the conditions listed in the following lemma.

Lemma 3. *In any stationary equilibrium in which bitcoins and the fiat currency have positive prices,*

$$i_B(b_{ss}) = f_B \lambda_B (b_{ss}) + f_{MB} \lambda_{MB} (\mu_{ss}, b_{ss}), \tag{13}$$

$$i_M = (f_M + (1 - S(H(b_{ss}), A)) f_{MB}) \lambda_M (\mu_{ss}) + S(H(b_{ss}), A) f_{MB} \lambda_{MB} (\mu_{ss}, b_{ss}), \tag{14}$$

where $i_M := \frac{\gamma}{\delta} - 1$, $i_B(b) := \frac{\rho}{S(H(b),A)\delta} - 1$, $\lambda_\tau(\mu, b) := (u'(q_\tau(\mu, b)) - 1)^+$, *and* $S(H(b), A)$ *and* $H(b)$ *are as in (2) and (8), respectively.*

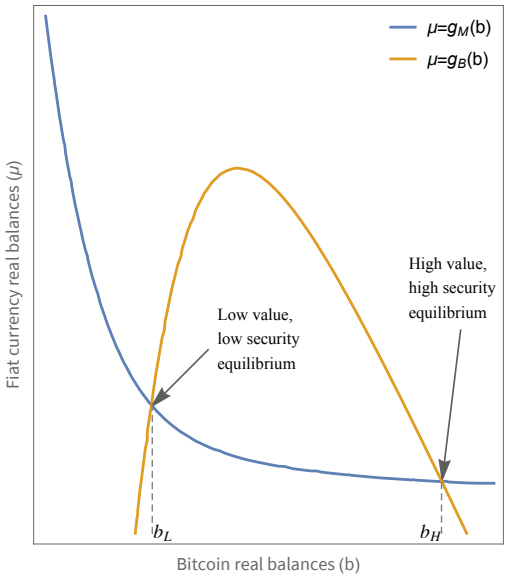
The system (13)–(14) is a generalization of (8); similarly, i_B and i_M express buyers' marginal carrying costs of bitcoin and fiat currency balances. Given that both bitcoins and fiat currency are intrinsically useless, this system indicates that the equilibrium value of real balances in each case must equalize their marginal carrying costs to the marginal value of their liquidity service.[49]

[48] Lester et al. (2012) consider a related environment but with asymmetric information and risk of counterfeiting. Their focus is on sellers' decision to invest in learning about the quality of each money. We abstract from such decisions and focus instead on the connections between acceptability and security. Due to the transparency of the public Bitcoin ledger, one can argue that counterfeiting is not a primary concern for bitcoins.

[49] Similarly to the analysis in Lemma 2, we note that the liquidity premium λ_τ corresponding to a type-τ meeting is positive as long as $q_\tau < q^*$; liquid wealth is valuable at the margin in a such case. If b and μ are positive in equilibrium, we must have $q_B < q_{MB}$ and $q_M < q_{MB}$; otherwise, buyers would want to readjust their holdings. Finally, $\lambda_{MB} > 0$ holds if $q_{MB} < q^*$; otherwise, $\lambda_{MB} = 0$ in (13) and (14). Note also that $\lambda_M(\mu) = \lambda_{MB}(\mu, 0)$.

Figure 9. Stationary DMEs in a bimonetary economy

This figure represents the set of equilibria in an economy where no buyers accept only bitcoins ($f_B = 0$) and the bitcoin supply growth is relatively low ($\rho < \gamma$).



In the remainder of this section, we focus on particular cases of interest. First, we consider the case in which no seller accepts both fiat currency and bitcoins, $f_{MB} = 0$. For example, if regular Internet sellers like Amazon accept only fiat card payments and dark web sellers like Silk Road accept only bitcoins. From Lemma 3, it is immediately clear that we can derive the value of bitcoins using (2), (6), and (13) alone. Therefore, the value of bitcoins is equivalent to that obtained in (8). A first conclusion is then that, from a pricing perspective, Proposition 2 best represents bitcoin's value when either form of money is essential for a given transaction.

Now consider the case in which all sellers accept fiat currency, but some also accept bitcoins ($f_B = 0$). Combining (13) and (14), we obtain $i_M - Si_B(b) = (f_M + (1 - S) f_{MB}) \lambda_M(\mu)$; for this equation to hold, we need $i_M > Si_B(b)$. Therefore, we can establish a lower bound for the fiat currency inflation rate γ, which becomes a necessary condition for bitcoins to be valued. A second conclusion is then that, if bitcoins are inessential for commerce, we only expect consumers to demand bitcoins in economies where the fiat inflation tax is high. There could be no bitcoin demand if the central bank followed a deflationary or constant-supply policy.

Figure 9 illustrates the equilibrium determination of b and μ in an economy with $f_{MB}, f_M > 0$, $f_B = 0$, and $\gamma > \rho$. The functions $\mu = g_B(b)$ and $\mu = g_M(b)$ are implicitly defined by (13) and (14), respectively. Importantly, as in previous sections, the complementarities between bitcoin users and miners yield a multiplicity of price–security ranked equilibria.[50] A third conclusion is then that Bitcoin's security model can generate multiplicity *regardless* of whether bitcoins are essential in transactions. This fact highlights that the main conclusion of Propositions 1 and 2 is not a result of assuming that only bitcoins are available as a means of payment.

We group the conclusions derived above in the following proposition.

Proposition 8. *Consider the set of bimonetary stationary equilibria. (i) If bitcoins are valued, their price and security are not uniquely determined. (ii) If $f_{MB} = 0$ and $f_B > 0$, bitcoin real balances and security are as in Proposition 2. (iii) If bitcoins are inessential for commerce ($f_B = 0$), but $b_{ss} > 0$, then the fiat currency monetary policy must satisfy $\gamma > \rho + \delta\left(1 - S\left(b_{ss}, A\right)\right)$.*

7 Discussion

We present a succinct discussion of our results and establish connections with empirical findings.

Price Formation and Hashrate. An essential empirical implication of our model is that bitcoin prices and the system's hashrate are positively related in the general equilibrium. The long-term evolution of these key quantities, as displayed in Figure 1, provides strong support. To further assess this implication, we document in Section A.4 of the IA the joint evolution of prices and the hashrate for Ethereum, the second largest PoW blockchain by market capitalization, and Litecoin, one of Bitcoin's clones with the longest history. For these, we also find a robust positive relation. Further empirical support is provided by Bhambhwani et al. (2019), who find that the aggregate hashrate has a long-term (cointegration) relation with the bitcoin price, and the same holds for a set of cryptocurrencies that rely on Bitcoin's security model.[51]

[50] A related case—arguably a less empirically realistic one—is that in which all sellers accept both fiat currency and bitcoins; thus, these are perfect substitutes as means of payment. Bitcoins and fiat currency are not, however, perfect substitutes regarding security. In this case, $f = f_{MB}$, and (13) and (14) reduce to $i_M - Si_B(b) = (1 - S) f\lambda_M(\mu)$, which yields a similar lower bound for γ and the possibility of multiple equilibria.

[51] While less tightly connected, there is a growing body of related evidence on risk-return relations for bitcoin and

Security Budget and Network Attacks. As of yet, no successful hashrate attack against Bitcoin have been recorded.[52] Our results highlight that such robustness must be seen as an equilibrium economic outcome—one with a high-security budget—and not as a byproduct of its blockchain technology. This vital distinction is best illustrated by the successful attack history of blockchains that, despite sharing Bitcoin's features and security model, have failed to achieve one such reliable budget. We document several related episodes in Table A2 in the IA.

Monetary Policy in PoW Blockchains. Although maximizing the token's value, the system's security, and social welfare can all be plausible design goals, we have shown that no monetary policy achieves these objectives at once. We note that the once-and-for-all implementation of Bitcoin's monetary policy does not seem the solution to any formal design goal.[53] In particular, given that there is no mechanism that renders ρ close to ρ_W, miner security investment can be expected to be socially inefficient.[54] While a monetary policy reformulation in Bitcoin is unlikely, our results can help to clarify its private and social costs and offer guidance in the design of new systems.

Non-fundamental Volatility. We find that bitcoins' prices can fluctuate stochastically as non-fundamental sentiment changes, and the scope for such unpredictable jumps is greater than for traditional currencies. This result corresponds well to several empirical findings. For example, Bhambhwani et al. (2019) find that bitcoin prices deviate from fundamentals in response to a sentiment factor based on momentum.[55] Our result also suggests that the unprecedented volatility that Bitcoin has exhibited thus far cannot be entirely attributable to behavioral biases and/or limited use in commerce, although these factors can also play a role. Indeed, we feature neither

other cryptocurrencies (e.g., Bianchi and Dickerson, 2018; Borri and Shakhnov, 2018; Ghysels and Nguyen, 2018).

[52] There are a few well-known episodes where Bitcoin's perceived network security was compromised, with immediate adverse valuation effects. These include the March 11, 2013, six-hour fork that created lack of consensus in the network and an instant 24% drop in price, though without malicious intent (for a discussion, see https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448).

[53] A precise monetary policy is not outlined by Nakamoto (2008), but its design was outlined in the software implementation (see Section A.4 of the IA). Other blockchains follow more flexible models. For example, monetary policy in Ethereum is subject to revisions that are discussed within that community of developers.

[54] Benetton et al. (2019) empirically estimate mining social costs using a sample of Chinese and U.S. mining firms.

[55] In addition, Liu and Tsyvinski (2018) find that both momentum and public attention, proxied by Internet search trends and Twitter activity, help to explain the time series of bitcoin returns. Makarov and Schoar (2020) show that capital controls and other limits to arbitrage contribute to the deviation of bitcoin prices from fundamentals. The sentiment equilibria that we characterize also embeds a time-series correlation between bitcoin holding returns and trade volume. This property seems consistent with the study by Borri and Shakhnov (2018), who attribute the volume–return pattern of bitcoin–dollar trades attributable to speculation rather than to fundamentals.

irrational agents nor upper bounds for the acceptability of bitcoins.

Bitcoin Usage. Our model features the use of bitcoin as a means of exchange for some transactions. Some of the earliest related evidence is provided by Athey et al. (2016). Biais et al. (2019) develop an empirical test relating the market value of bitcoins with transactional benefits, which are proxied by retailer acceptance. Besides legal status uncertainty and taxation, a frequent argument is that large price volatility prevents more widespread use (Yermack (2015)). Our results on the structural amplification of volatility suggest that such a challenge is likely to be enduring.

The bimonetary analysis highlights Bitcoin's potential in two specific circumstances. The first one is when private agents suffer from incomplete connectivity due to governmental restrictions on using currency or the banking system. In that regard, Bitcoin can function as a stateless system offering a high degree of censorship resistance. Formally, we can associate the latter with $f_B > 0$; if B-type sellers are the government's economic or political targets of a service-denial attack. The greater the number of restrictions, the greater the scope for Bitcoin to complete the network of economic relations domestically, or abroad, under international sanctions. Therefore, it seems reasonable to expect a relatively high f_B and bitcoin price values with repressive authorities.[56]

The second circumstance is when bitcoins can offer protection against fiat currency inflation, regardless of whether bitcoins are essential for specific trades.[57] This model implication corresponds well to industry reports that rank unstable high-inflation countries, such as Venezuela, among those with the highest Bitcoin usage per capita,[58] and to the evidence by Yu and Zhang (2020).

[56]The demand for censorship resistance has multiple sources associated with governments' actions, including financial repression through capital controls; international sanctions; option-like hedging against abuses such as wealth confiscation or the targeting of political dissidents and/or religious groups; hedging against changes in inheritance laws; forced maturity conversion of bank deposits; the ability to secure wealth transfers in the event of armed conflicts, territorial invasions, civil wars, and refugee crises; and the criminalization of certain consumer goods (e.g., alcohol, cannabis, or yet unapproved medicines) and/or services (e.g., gaming, gambling, prediction markets). There is increasing evidence on how bitcoins and similar tokens are used in these regards. For example, reflecting the demand to circumvent capital controls, the firm Chainalysis reported that more than $50 billions worth of cryptocurrency moved from China-based to overseas addresses in the twelve months before August 2020 (https://www.bloomberg.com/news/articles/2020-08-20/crypto-assets-of-50-billion-moved-from-china-in-the-past-year). Foley, Karlsen, and Putnins (2018) provide evidence on the use of bitcoins in criminalized trades.

[57]We note that these two circumstances are not mutually exclusive. Indeed, high-inflation countries usually enforce tight capital controls, such as disallowing people's access to foreign currencies for international remittances, making bitcoins more appealing.

[58]For example, Venezuela is ranked third on the Chainalysis 2020 Geographic Crypto Usage Index. LocalBitcoins, a peer-to-peer exchange, ranks Venezuela the second most active country, scaled by the number of Internet users and purchasing power (see https://blog.chainalysis.com/reports/venezuela-cryptocurrency-market-2020).

8 Concluding Remarks

We presented a tractable decentralized monetary economy where users' and miners' decisions impact each other and the evolutions of bitcoin prices and security are jointly determined. The model outcomes demonstrate how ignoring these general equilibrium connections—as in the benchmark considered—can lead one to mischaracterize the equilibrium set, underprice/overprice the token depending on assumptions about security, underestimate price volatility, and wrongly conclude that Bitcoin's declining supply growth mechanically increases its value. We believe that our results can help understand other markets for network assets that rely on PoW consensus.

We conclude by discussing limitations and opportunities for future work. We focused on equilibria that do not display congestion. Intuitively, in our setting, it is sufficient for the block size to exceed the data storage needs with n transfers. If the block size were smaller, not all buyers would be able to acquire bitcoins. An equilibrium would then require buyers to be indifferent about buying bitcoins. This could be achieved with mixed strategies if those who buy bitcoins pay transaction fees of a value matching their trade surplus, thus redistributing resources from users to miners. This observation is decisively not to suggest that abstraction from fees is without loss of generality. If agents' impatience were heterogeneous, for example, user-initiated fees could play an allocative role, as demonstrated by Easley et al. (2019) and Huberman et al. (2019). The integrating a rich fee bidding game within a general equilibrium monetary framework is an exciting avenue of work.

Because our analysis focuses on seigniorage-financed security, it also highlights challenges regarding Bitcoin's monetary policy, which eliminates issuances in the long term. If bitcoin usage continues to grow over the coming decades, one can, like Nakamoto, hope that user fees compensate for some or all of the loss of miner revenue. However, there is no built-in mechanism that makes such a shift in revenue source to be granted. Second layer networks such as Lightning can help with the scaling limitations but its net impact of on-chain fees is still uncertain. Whether security can remain at high levels beyond 2140 is, therefore, an important open question.

References

Abadi, J. and M. Brunnermeier (2018). Blockchain Economics. *Princeton U. Working Paper*.

Alsabah, H. and A. Capponi (2019). Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. *Working Paper*.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain*. O'Reilly.

Asriyan, V., W. Fuchs, and B. Green (2019). Liquidity Sentiments. *American Economic Review 109*(11), 3813–3848.

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia (2016). Bitcoin Pricing, Adoption, and Usage: Theory and Evidence. *Working Paper*.

Azariadis, C. (1981). Self-Fulfilling Prophecies. *Journal of Economic Theory 25*, 380–396.

Benetton, M., G. Compiani, and A. Morse (2019). CryptoMining : Local Evidence from China and the US. *Working Paper*.

Bhambhwani, S., S. Delikouras, and G. M. Korniotis (2019). Do Fundamentals Drive Cryptocurrency Prices? *Working Paper*.

Biais, B., C. Bisi, M. Bouvard, C. Casamatta, and A. Menkveld (2019). Equilibrium Bitcoin Pricing. *Working Paper*.

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta (2019). The blockchain folk theorem. *Review of Financial Studies 32*(5), 1662–1715.

Bianchi, D. and A. Dickerson (2018). Trading Volume in Cryptocurrency Markets. *Working Paper*.

Borri, N. and K. Shakhnov (2018). The Cross-Section of Cryptocurrency Returns. *SSRN Electronic Journal*.

Budish, E. B. (2018). The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper No 24717*.

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

Chiu, J. and T. V. Koeppl (2019). The Economics of Cryptocurrencies Bitcoin and Beyond. *SSRN Electronic Journal*.

Choi, M. and G. Rocheteau (2019). Money Mining and Price Dynamics. *Working Paper*.

Cong, L. W., Z. He, and J. Li (2018). Decentralized Mining in Centralized Pools. *Working Paper*.

Cong, L. W., Y. Li, and N. Wang (2018). Tokenomics: Dynamic Adoption and Valuation. *W. Paper*.

Cong, L. W., Y. Li, and N. Wang (2019). Token-Based Platform Finance. *Working Paper*.

Conti, M., K. E. Sandeep, C. Lal, and S. Ruj (2018, oct). A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys and Tutorials 20*(4), 3416–3452.

Easley, D., M. O'Hara, and S. Basu (2019). From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics 134*(1), 91–109.

Feller, W. (1968). *An Introduction to Probability Theory and its Applications* (Third ed.). Wiley.

Fernández-Villaverde, J. and D. R. Sanches (2016). Can Currency Competition Work? *PIER Working Paper No. 16-008*.

Foley, S., J. R. Karlsen, and T. J. Putnins (2018). Sex , Drugs , and Bitcoin : How Much Illegal Activity is Financed Through Cryptocurrencies? *Review of Financial Studies (forthcoming)*.

Ghysels, E. and G. Nguyen (2018). Price Discovery of a Speculative Asset: Evidence from a Bitcoin Exchange. *UNC Working Paper*.

Goldstein, I., E. Ozdenoren, and K. Yuan (2011). Learning and complementarities in speculative attacks. *Review of Economic Studies 78*(1), 263–292.

Gu, C., G. Menzio, R. Wright, and Y. Zhu (2019). Toxic Assets and Market Freezes. *Working Paper*.

Harvey, C. R. (2016). Cryptofinance. *Working Paper*.

Hayek, F. A. (1976). *The Denationalization of Money*. London: The Institute of Economic Affairs.

Hinzen, F. J., K. John, and F. Saleh (2019). Bitcoin's Fatal Flaw : The Limited Adoption Problem. *Working Paper*.

Huberman, G., J. D. Leshno, and C. Moallemi (2019). An Economic Analysis of the Bitcoin Payment System. *Working Paper*.

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

Kang, K.-Y. (2020). Cryptocurrency and Double Spending History: Transactions with Zero Confirmation. *Working Paper*.

Kareken, J. and N. Wallace (1981). On the Indeterminancy of Equilibrium Exchange Rates. *The Quarterly Journal of Economics 96*(2), 207–222.

Lagos, R., G. Rocheteau, and R. Wright (2017). Liquidity: A New Monetarist Perspective. *Journal of Economic Literature 55*(2), 371–440.

Lagos, R. and R. Wright (2003). Dynamics, cycles, and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money. *Journal of Economic Theory 109*(2), 156–171.

Lagos, R. and R. Wright (2005). A Unified Framework for Monetary Theory and Policy Analysis. *Journal of Political Economy 113*(3), 463–484.

Lamport, L., R. Shostak, and M. Pease (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems 4*(3), 382–401.

Lehar, A. and C. A. Parlour (2019). Miner Collusion and the BitCoin Protocol. *Working Paper*.

Lester, B., A. Postlewaite, and R. Wright (2012). Information, liquidity, asset prices, and monetary policy. *Review of Economic Studies 79*(3), 1209–1238.

Li, J. and W. Mann (2020). Digital Tokens and Platform Building. *Working Paper*.

Liu, Y. and A. Tsyvinski (2018). Risks and Returns of Cryptocurrency. *NBER W.P. 24877*.

Liu, Z., N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-c. Liang, and D. I. Kim (2019). A Survey on Applications of Game Theory in Blockchain. *IEEE Access*, 1–26.

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

Malinova, K. and A. Park (2017). Market Design with Blockchain Technology. *U. of Toronto Working Paper*.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *White Paper*.

Obstfeld, M. (1996). Models of currency crises with self-fulfilling features. *European Economic Review 40*(95), 1037–1047.

Pease, M., R. Shostak, and L. Lamport (1980). Reaching Agreement in the Presence of Faults. *Journal of the ACM 27*(2), 228–234.

Raskin, M. and D. Yermack (2016). Digital Currencies, Decentralized Ledgers, and the Future of Central Banking. *NBER Working Paper 22238*.

Rocheteau, G. and E. Nosal (2017). *Money, Payments, and Liquidity*. Cambridge: The MIT Press.

Rocheteau, G. and R. Wright (2005). Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium. *Econometrica 73*(1), 175–202.

Rosenfeld, M. (2014). Analysis of Hashrate-Based Double Spending. *Working Paper*.

Schilling, L. and H. Uhlig (2019). Some Simple Bitcoin Economics. *Journal of Monetary Economics 106*, 16–26.

Sockin, M. and W. Xiong (2018). A Model of Cryptocurrencies. *UT Austin Working Paper*.

Yermack, D. (2015). Is Bitcoin a Real Currency? An Economic Appraisal. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*, 31–43.

Yermack, D. (2017). Corporate Governance and Blockchains. *Review of Finance 21*(1), 7–31.

Yu, Y. and J. Zhang (2020). Flight to Bitcoin. *Working Paper*.

Zhu, T. (2008). An overlapping-generations model with search. *Journal of Economic Theory 142*(1), 318–331.

Zimmerman, P. (2019). Blockchain Structure and Cryptocurrency Prices. *Working Paper*.

Appendix: Proofs of Propositions

This Appendix contains the proofs of proposition in the main body of the paper. Proofs of lemmas are found in Section E of the IA. Subsequently, we sometimes avoid displaying the dependency of S and its derivatives on $(H(b), A)$ and $H(b)$ on b for compactness of notation.

Proof of Proposition 1

The necessary and sufficient condition for the existence of equilibrium under extrinsic security follows immediately from (3). Since V' is strictly decreasing, there can be at most one equilibrium.

Consider the case of intrinsic security and let $\pi = \{p > 0 : \Delta(p) = 1\}$ be the set of positive values satisfying (3), where $\Delta(p)$ represents the left-hand side of (3). Let p_m be defined by $p_m = H^{-1}(A)$ according to (1). Clearly, $\tilde{p} \in [0, p_m]$ cannot be in π since $H(\tilde{p}) \in [0, A]$; given (2), $S(H(\tilde{p}), A) = 0$. For $p > p_m(A)$, instead, we must have $S(H(p), A) > 0$. Since V' is decreasing and $V'(0) = +\infty$, by continuity, there must be a sufficiently large $\hat{n}(A)$ such that $\Delta(p; \hat{n}(A)) \geq 1$. Therefore, when the population of buyers is large enough, π must contain at least one element.

Next, we argue that if the set π is not empty, the number of equilibria is even. Computing $\Delta'(p)$ and using market clearing, we obtain

$$\Delta'(p) = S_H H_p \left(fV'\left(\frac{\overline{B}}{n}p\right) + (1-f)\delta R \right) + S(H(p), A)\frac{\overline{B}}{n} fV''\left(\frac{\overline{B}}{n}p\right).$$

For the smallest element in π, p_L, $\Delta(p)$ must cross 1 from below, so $\Delta'(p_L) > 1$. Next, note that from (2), $S_H = \left(\frac{A}{H}\right)^k \frac{k}{H}$; from (1), $H_p = \frac{m-1}{m}\left(\frac{\delta\psi R}{\kappa}\right)$. Combining these expressions, $S_H H_p = \left(\frac{A}{H}\right)^k \frac{k}{p}$. Thus, for sufficiently large p values, $S(H(p), A) \approx 1$, $S_H H_p \approx 0$, and $\Delta'(p) \to \frac{\overline{B}}{n} fV''\left(\frac{\overline{B}}{n}p\right) < 0$. We conclude that, if there exists a stationary value $p_L > 0$ with $\Delta'(p_L) > 1$, there must be another solution $p_H > p_L$ with $\Delta'(p_H) < 0$ so that Δ crosses 1 from above. Since this conclusion holds regardless of V's specific functional form, the number of elements in π must be even. An exception is the special case of a tangency value $\hat{p}$ such that $\Delta(\hat{p}) = 1$ and $\Delta'(\hat{p}) = 0$. □

Proof of Proposition 2

The existence and multiplicity part of the proof follows similar steps to those in Proposition 1. Still, we must account for the optimality conditions in the DM exchange and supply growth. Let $\beta = \{b_{ss} : b_{ss} = D(b_{ss}), b_{ss} > 0\}$ be the set of positive values satisfying (8). Let b_m be defined by $b_m = H^{-1}(A)$ according to (6). For $b \leq b_m(A)$, we must have $S(H(b), A) = 0$; for $b > b_m(A)$, $S(H(b), A) > 0$. Since u' is a decreasing function, and $u'(0) = +\infty$, by continuity, for values $b > b_m(A)$ there must be a sufficiently large $\hat{n}(A)$ such that $D(b; \hat{n}(A)) \geq b$. Therefore, when the population of buyers is large enough, β must contain at least one element.

If the set β is not empty, the number of DMEs is even. To see this, from the right-hand side of (7) we obtain

$$D'(b) = \frac{\delta}{\rho}\{S_H H_b b + S(b,A)\}\left\{fu'\left(\frac{\delta}{\rho}\frac{b}{n}\right) + (1-f)\right\} + \left(\frac{\delta}{\rho}\right)^2 \frac{f}{n} S(b,A)\, bu''\left(\frac{\delta}{\rho}\frac{b}{n}\right).$$

For the smallest element in β, b_L, $D(b)$ must cross b from below on the (b_{t+1}, b_t) plane, so $D'(b_L) > 1$. Next, consider $b > b^*$. From Lemma 2, $D(b) = \frac{\delta}{\rho} S(b,A)\, b$; combining with (6), $D'(b) = \frac{\delta}{\rho}\{S_H H + S(b,A)\}$. From (2), $S_H H = k\left(\frac{A}{H}\right)^k$. Therefore,

$$\lim_{b\to+\infty} D'(b) = \lim_{b\to+\infty} \frac{\delta}{\rho}\left\{k\left(\frac{A}{H(b)}\right)^k + S(b,A)\right\} = \frac{\delta}{\rho} < 1. \tag{15}$$

We conclude that if there exists a stationary solution $b_L > 0$ with $D'(b_L) > 1$, there must another solution $b_H > b_L$ with $D'(b_H) < 1$ so that D crosses the 45-degree line from above. Because (15) holds regardless of the functional form of u, the number of elements in β must be even. An exception with no crossings is the particular case where D is tangent to the 45-degree line at a point b_{ss} such that $D'(b_{ss}) = 1$.

We now compare welfare outcomes across stationary DMEs. Expand the expectation in (9) and combine with (6) to obtain

$$\mathcal{W}_{ss}/n = fS(H(q_{ss}), A)(u(q_{ss}) - q_{ss}) - \frac{m-1}{m}(\rho - 1) q_{ss}, \tag{16}$$

where we used $q_{ss} = \frac{\delta b_{ss}}{\rho n}$ to conveniently express welfare as a function of q. Now, consider the effect of a marginal increase in q on $\mathcal{W}_L$:

$$\underbrace{fS_H H_q(q_L)(u(q_L) - q_L)}_{\text{I}>0} + \underbrace{fS\left(u'(q_L) - 1\right)}_{\text{II}>0} - \underbrace{\frac{m-1}{m}(\rho - 1)}_{\text{III}>0}. \tag{17}$$

Expression I in (17) reflects a security enhancement; it must be positive given (2) and Lemma 1. Expression II reflects the marginal change in the value of the trade surplus; it must be positive since $q_L < q^*$ by Lemma 2. Expression III reflects the positive marginal increase in mining costs. Social welfare increases with q only if the constant term III is small relative to I and II between q_L and q_H. To assess the latter, note that, from (8), it must hold that $f(u'(q_L) - 1) = \frac{\rho}{\delta S(q_L, A)} - 1$. Therefore, II equals $\frac{\rho}{\delta} - S(q_L, A)$. Since $S < 1$ for $q > 0$, $\frac{\rho}{\delta} > 1$, and $\frac{m-1}{m} < 1$, we must have II>III. Thus, an increase in q over q_L raises social welfare. Since $q_H > q_L$, we conclude that $\mathcal{W}_H > \mathcal{W}_L$. □

Proof of Proposition 3

Let $y(b;\rho) := \frac{\delta S}{\rho}\left(f\left(u'\left(q\left(b,\rho\right)\right)-1\right)+1\right)$; b satisfying $y(b;\rho)-1=0$ is equivalent to (8). By the implicit function theorem, in the vicinity of b, $\frac{db}{d\rho} = -\frac{y_\rho}{y_b}$; Lemma E1 in the IA shows that $y_b < 0$ for the high DME. We have $\frac{db}{d\rho}=0$ if and only if $y_\rho = 0$. Computing y_ρ,

$$y_\rho = \frac{\delta}{\rho^2}\{(\rho S_H H_\rho - S)(f\left(u'\left(q\left(b\right)\right)-1\right)+1) - Sfq\left(b\right)u''\left(q\left(b\right)\right)\}. \tag{18}$$

Using equation (6), $H_\rho = \frac{H}{\rho(\rho-1)}$, and, from (2), $S_H = k\left(\frac{A}{H}\right)^k \frac{1}{H}$. Therefore, $\rho S_H H_\rho = \left(\frac{A}{H}\right)^k \frac{k}{\rho-1} = (1-S)\frac{k}{\rho-1}$. Combining the latter expression with (18), we obtain

$$y_\rho = \frac{\delta}{\rho^2} S \left(\underbrace{\left(\frac{k\left(1-S\right)}{S\left(\rho-1\right)}-1\right)}_{\text{I}} \underbrace{\left(f\left(u'\left(q\left(b\right)\right)-1\right)+1\right)}_{\text{II}>0} + \underbrace{\left(-fq\left(b\right)u''\left(q\left(b\right)\right)\right)}_{\text{III}>0} \right). \tag{19}$$

Expression II on the right-hand side of (19) is positive by Lemma 2. Expression III captures the change in the terms of trade in the DM and is positive because $u''<0$. Expression I can be positive or negative. For low ρ values, $\rho \approx 1$, I is positive, implying that $y_\rho > 0$—marginal security gains are large. When ρ is large enough, I becomes negative, implying that we can have $y_\rho < 0$. If $y_\rho > 0$ for low ρ values and $y_b < 0$ for high ρ values, by continuity, there must be a value ρ_V satisfying $y_b(\rho_V) = 0$. Such a value is implicitly defined by the right-hand side of (19) being equal to zero, which requires that:

$$\left(1-\frac{k\left(1-S\right)}{S\left(\rho-1\right)}\right)\left(f\left(u'\left(q\left(b\right)\right)-1\right)+1\right) = fu'\left(q\left(b\right)\right)\sigma\left(b\right), \tag{20}$$

where $\sigma\left(b\right) := -q(b)\frac{u''(q(b))}{u'(q(b))}$. Combining expressions (20), $\text{II} = \frac{\rho}{\delta S} = i_B + 1$ and $fu'(q) = i_B + f$ from (8), and $\epsilon_{S,\rho}(\rho_V) = \frac{k(1-S)}{S(\rho_V-1)}$ we obtain (10). Note that if a value ρ_V solves (20), from Lemma E1, the second-order conditions for such solution to maximize real balances are only met by the high equilibrium. The fact that $\frac{dp_H}{d\rho} > 0$ for $\rho < \rho_V$ and $\frac{dp_H}{d\rho} < 0$ for $\rho > \rho_V$ follows from $b_H = p_H B$. □

Proof of Proposition 5

Parts (i) and (ii) follow from the arguments in Section 4.3. For (iii), consider the planner's objective function in (16) subject to buyers' optimality restriction from (8). Note that the planner's ρ choice affects $b(\rho)$ and $q\left(b,\rho\right)$. We obtain the marginal social benefit (MSB) of a change in ρ by total

differentiation of the expected DM trade surplus:

$$MSB = \underbrace{S_H\left(H_\rho + H_b\frac{db}{d\rho}\right)}_{\text{security enhacement}} f\left(u\left(q\right)-q\right) + \underbrace{Sf\left(u'(q)-1\right)\left(q_\rho + q_b\frac{db}{d\rho}\right)}_{\text{effect on DM exchange } q} = S\frac{q}{\rho}\left(\epsilon_{S,\rho} f\left(\frac{u(q)}{q}-1\right) + f\left(u'(q)-1\right)\left(\epsilon_{b,\rho}-1\right)\right), \tag{21}$$

where the second line uses $q_b = \frac{q}{b}$, $q_\rho = -\frac{q}{\rho}$, and $\epsilon_{z,\rho} := \frac{dz}{d\rho}\frac{\rho}{z}$. Analogously, we obtain the marginal social cost (MSC) of a change in ρ by total differentiation of the mining investment:

$$MSC = \frac{q}{\rho}\frac{m-1}{m}\left(\left(\rho-1\right)\epsilon_{b,\rho}+1\right). \tag{22}$$

Next, we evaluate whether $MSB \gtreqless MSC$ at $\rho = \rho_V$. Using $\epsilon_{b,\rho}\left(\rho_V\right) = 0$ in (21) and (22), it follows that $MSB < MSC$ if:

$$S\left(\epsilon_{S,\rho} f\left(\frac{u\left(q\right)}{q}-1\right) - f\left(u'(q)-1\right)\right) < \frac{m-1}{m}. \tag{23}$$

Substituting $i_B = f\left(u'(q)-1\right)$ from (8) in (23), we obtain the inequality in (iii). If (23) holds, social welfare is enhanced by setting ρ_W below ρ_V. If the inequality in (23) is reversed, $MSB > MSC$; thus, it is socially optimal to set $\rho_W > \rho_V$. □

Proof of Proposition 6

We assume that $S(b_H, A) = \overline{S}$, implying $b_H = \bar{b}$. Differentiating equation (8) at $b_{ss} = b_H$:

$$\left\{-\frac{\delta}{\rho}\frac{1}{n}Sfu''\left(q\left(b_H\right)\right)q\left(b_H\right)\right\}dn + \left\{\frac{\delta}{\rho}S_H H_b\left(f\left(u'\left(q\left(b_H\right)\right)-1\right)+1\right) + \frac{\delta}{\rho}Sfu''\left(q\left(b_H\right)\right)\frac{\delta}{\rho}\frac{1}{n}\right\}db_H = 0.$$

Multiplying both sides by b_H, and rearranging

$$\left\{\frac{\delta}{\rho}S_H H\left(f\left(u'\left(q\left(b_H\right)\right)-1\right)+1\right) + \frac{\delta}{\rho}Sfu''\left(q\left(b_H\right)\right)q\left(b_H\right)\right\}db_H = \left\{Sfu''\left(q\left(b_H\right)\right)q\left(b_H\right)^2\right\}dn. \tag{24}$$

Analogously, for the token with extrinsic security:

$$\left\{\frac{\delta}{\rho}\overline{S}fu''\left(q\left(\bar{b}\right)\right)q\left(\bar{b}\right)\right\}d\bar{b} = \left\{\overline{S}fu''\left(q\left(\bar{b}\right)\right)q\left(\bar{b}\right)^2\right\}dn. \tag{25}$$

Given $b_H = \overline{b}$, the right-hand sides of equations (24) and (25) coincide. Therefore, we must have

$$\underbrace{\left\{\frac{\delta}{\rho}S_H H\left(f\left(u'\left(q\left(b_H\right)\right)-1\right)+1\right)+\frac{\delta}{\rho}Sfu''\left(q\left(b_H\right)\right)q\left(b_H\right)\right\}}_{y_b(b_H)}db_H = \underbrace{\left\{\frac{\delta}{\rho}\overline{S}fu''\left(q\left(\overline{b}\right)\right)q\left(\overline{b}\right)\right\}}_{\overline{y}_b(\overline{b})}d\overline{b}. \quad (26)$$

The first bracketed term of the left-hand size of (26) is positive at a DME, while the second is negative. From Lemma E1 in the IA, we know that the sum must be negative: $y_b(b_H) = \left(\frac{D'(b_H)-1}{b_H}\right) < 0$. Therefore, $|y_b\left(b_H\right)| < \left|\overline{y}_b(\overline{b})\right|$, implying that $|db_H| > \left|d\overline{b}\right|$. □

Proof of Proposition 7

From the conditions in (12), we solve for (ϕ_1, ϕ_2):

$$\phi_1 = \frac{\frac{D(b_2)}{S(b_2)} - \frac{b_1}{S_1}}{\frac{D(b_2)}{S(b_2)} - \frac{D(b_1)}{S(b_1)}}, \quad \phi_2 = \frac{\frac{b_2}{S_2} - \frac{D(b_1)}{S(b_1)}}{\frac{D(b_2)}{S(b_2,A)} - \frac{D(b_1)}{S(b_1)}}. \quad (27)$$

Sunspot equilibria can exist under two types of conditions. For Type I, the denominator in (27) is positive. The full set of conditions for Type I is as follows: $\phi_1 > 0$ requires $\frac{D(b_2)}{S(b_2)} > \frac{b_1}{S_1}$; $\phi_1 < 1$ requires $\frac{b_1}{S_1} > \frac{D(b_1)}{S(b_1)}$; $\phi_2 > 0$ requires $\frac{b_2}{S_2} > \frac{D(b_1)}{S(b_1)}$, and $\phi_2 < 1$ requires $\frac{D(b_2)}{S(b_2)} > \frac{b_2}{S_2}$. Therefore, the joint satisfaction of these conditions requires b_1 and b_2 to satisfy $\frac{D(b_1)}{S(b_1)} < \frac{b_1}{S_1} < \frac{D(b_2)}{S(b_2)}$ and $\frac{D(b_1)}{S(b_1)} < \frac{b_2}{S_2} < \frac{D(b_2)}{S(b_2)}$. Since $S_1 > S\left(b_1\right)$, for $\frac{D(b_1)}{S(b_1)} < \frac{b_1}{S_1}$ to hold, it is necessary that $D(b_1) < b_1$. Similarly, since $S_2 < S\left(b_2\right)$, for $\frac{b_2}{S_2} < \frac{D(b_2)}{S(b_2)}$ to hold, it is necessary that $D(b_2) > b_2$. Therefore, D must cross the 45-degree line from below between b_1 and b_2, $D(b_1) < b_1 < b_2 < D(b_2)$, which only holds in the intrinsic security case.

For Type II, the denominator in (27) is negative. Existence require that b_1 and b_2 satisfy $\frac{D(b_1)}{S(b_1)} > \frac{b_1}{S_1} > \frac{D(b_2)}{S(b_2)}$ and $\frac{D(b_1)}{S(b_1)} > \frac{b_2}{S_2} > \frac{D(b_2)}{S(b_2)}$. In this case, D crosses the 45-degree line from above between b_1 and b_2, and these values are in the area of overlap between $D(b)$ and $D^{-1}(b)$ around b_H. If $S(b_1) \approx S(b_2)$ for this range of values, a sufficient condition is that $D'(b) < -1$ around b_H. □

Proof of Proposition 8

The proof of the existence of multiple equilibria is similar to that for Propositions 1 and 2 and is therefore omitted. Part (ii) follows directly from Lemma 3. Finally, note that, if $f_B = 0$, a necessary condition for the system (13) and (14) to hold is that $i_M > S(b_{ss}, A) i_B$. Using the definitions of i_M and i_B one obtains the lower bound for γ in (iii). □

Internet appendix to:

"Decentralizing Money: Bitcoin Prices and Blockchain Security"

Emiliano S. Pagnotta*

Contents

A Empirical Supplement **1**

A.1 Security Budget: Block Reward and Fees 1

A.2 Security Models and a Token Taxonomy 1

A.3 Bitcoin's Monetary Policy 3

A.4 Price and Hashrate Time Series for other PoW Blockchains 4

A.5 Examples of Hashrate-Based Attacks 5

B Supplement to Section 3: The Dynamic Stability of DMEs **6**

C Quantitative Supplement **8**

C.1 Parameter Values 8

C.2 Equilibrium Outcomes 9

C.3 Block Reward Halving and Price Changes 9

C.4 Volatility Amplification of Fundamental Shocks 10

C.5 Non-fundamental Uncertainty, Expected Time to Attack, and the Saboteur's Resources 10

D Implications for the Mining Industry and Minting Costs **13**

D.1 Miner Entry and Profits 13

D.2 Perfect Mining Competition and Minting Costs 14

*Imperial College London. Email:esp.research@pm.me

E Proof of Lemmas 15

F Proofs of Internet Appendix Propositions 18

A Empirical Supplement

This section supplements the discussion in Section 1 and documents related empirical facts.

A.1 Security Budget: Block Reward and Fees

The compensation to a miner winning the PoW contest consists of an inflationary block reward and fees. Panel A of Figure A1 shows the percentage of miners' daily revenues from fees. With some exceptions, most notably the late part of 2017, the dominant component of the security budget has been the block reward. On a daily basis, the median and mean values of the proportion from fees are 0.79% and 2.43%, respectively.

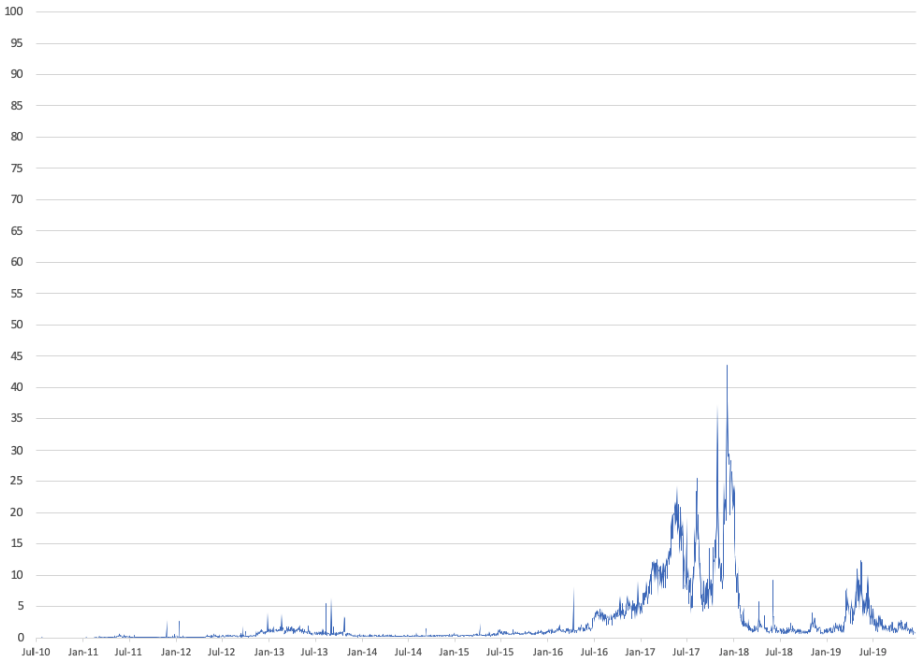
Fees are determined in a user auction for block space (Easley et al., 2019; Huberman et al., 2019). The fact that fees thus far represent a small fraction of miners revenue is consistent with low block congestion. Panel B of Figure A1 displays the time series of the mined block sizes relative to the block capacity limit. The latter is determined as follows. In May 2013, a Bitcoin protocol update set an explicit block size limit of 1 MB. Before that, the block capacity was within the range 500–750 kb (see, e.g., https://en.bitcoin.it/wiki/Block_size_limit_controversy). The figure shows that the block size is below the block capacity for virtually Bitcoin's entire history up to August 2017: the proportion of days with average block sizes exceeding 999 kb is 0.5%. In August 2017, activations of the SegWit protocol update (see https://en.bitcoin.it/wiki/Segregated_Witness) increased the block capacity up to 4 MB. The effective block capacity positively depends on the voluntary adoption of SegWit wallets, which has gradually increased over time. Lehar and Parlour (2019) document that block congestion has remained low after the implementation of SegWit.

A.2 Security Models and a Token Taxonomy

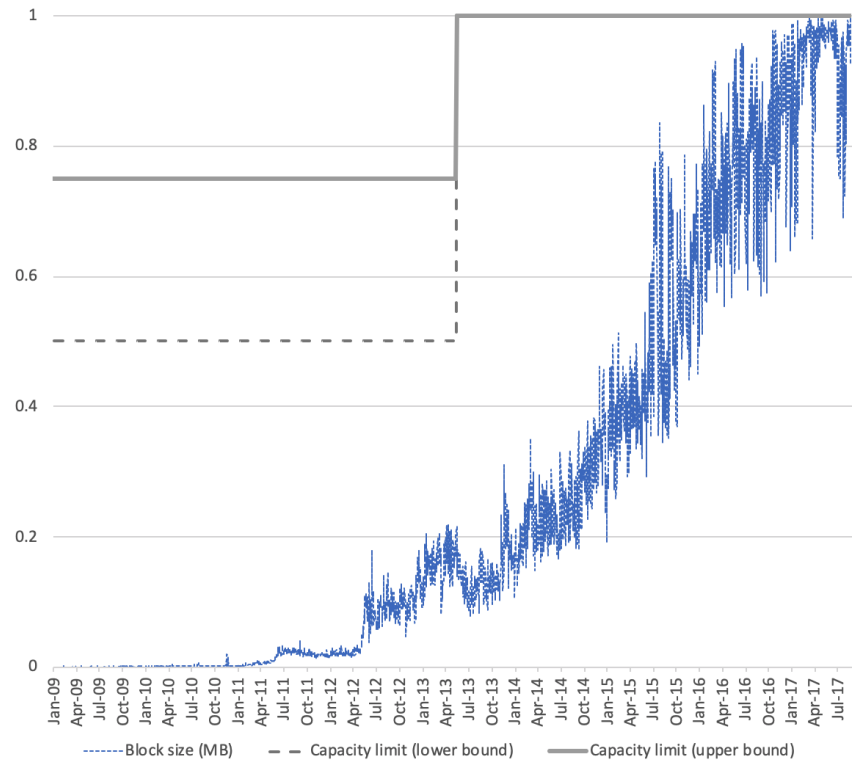
Definition 1 provides a classification for tokens and digital assets based on their security model. Blockchains that follow Bitcoin's PoW have an intrinsic model, since the internal security budget depends on the token's price. Table A1 provides some examples, including Ether, Litecoin, and Monero.

Regarding the extrinsic security model, besides the examples of Ripple's XRP and Libra discussed in Section 1, consider the Depository Trust & Clearing Corporation (DTCC), a centralized depository providing for the custody of securities. Through its subsidiaries, DTCC provides clearance, settlement, and information services for a range of securities on behalf of buyers and sellers. DTCC charges a dollar fee for its services; therefore, there is a clear separation between the value of the verifier's revenue and the value of the transferred asset, for example, a stock such as Amazon. Put differently, the security of the DTCC network is not affected by Amazon's price. Similarly, the security of ERC-20 tokens within

Figure A1
Bitcoin fees and block congestion



(a) Percentage of miners' daily revenue from fees: July 2010–January 2020



(b) Bitcoin block congestion: January 2009–August 2017
Sources: Coinmetrics.io and Blockchain.com.

the Ethereum network (e.g., Binance, VeChain, OmiseGo) does not depend on their token price, since compensations for their transfers is paid using Ether.

Table A1
Digital tokens in centralized and decentralized networks: Examples

Network	Peer-to-peer	Multiple verifiers	Free entry of verifiers	Token/asset	Intrinsic security
Stock exchanges, DTCC	n	n	n	Public equity	n
Bitcoin	y	y	y	Bitcoin	y
Cryptocurrencies	y	y	y	Litecoin, Monero, etc.	y
Ethereum	y	y	y	Ether	y
Ethereum	y	y	y	ERC-20 tokens	n
Ripple	n	y	n	XRP	n
Libra	n	y	n	Libra	n

A.3 Bitcoin's Monetary Policy

Bitcoin's monetary policy is not fully described in Nakamoto (2008), but its details are outlined in the Bitcoin protocol.[1] The initial reward was set to 50 by Nakamoto, and it halves every 210,000 blocks, for as long as it is greater than 10^{-8} (one satoshi). One can then write the evolution of the bitcoin supply in block time, as follows:

$$B_J = \sum_{j=1}^{\min\{J,\mathcal{J}\}} \frac{50}{2^{K(j)}}, K(j) = \left\lfloor \frac{j}{210,000} \right\rfloor, \tag{A.1}$$

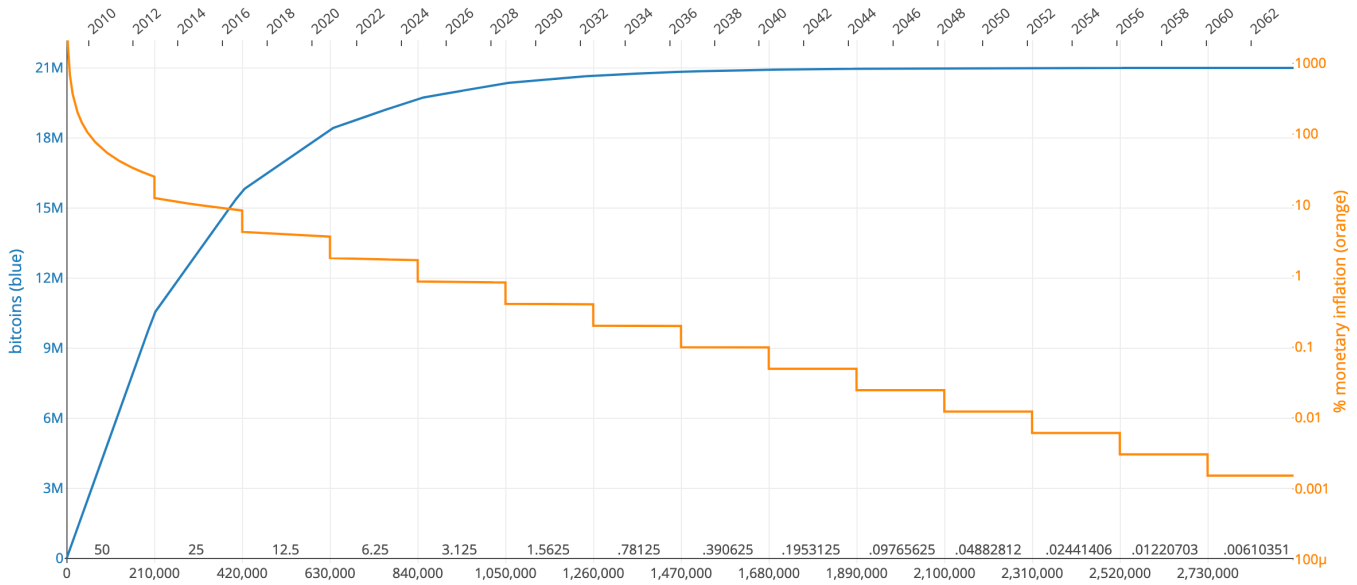
where 50 represents the initial number of bitcoins per block, J represents the block height, $K(j)$ represents the number of reward halving events up to block j, and $\mathcal{J} = 33 \times 210,000$. Beyond block $\mathcal{J}$ (estimated to be mined around 2140), bitcoin issuance stops; the supply limit can therefore be expressed as

$$B_{\text{limit}} = \sum_{i=0}^{32} \frac{50}{2^i} \times 210,000 \approx 2.1 \times 10^7.$$

Equation (A.1) provides a good yet imperfect approximation of the evolution of supply in *calendar* time, for the following reasons. First, each calendar block confirmation time is random. Periodic mining difficulty adjustments moderate the dispersion of confirmation times around the 10-minute target. However, these adjustments occur approximately every two weeks (2,016 blocks), implying that deviations from the target can happen within that period, especially at times of large bitcoin price movements. Figure A2 displays the evolution of supply in blocks and calendar time, assuming 10-minute confirmation times. Second, custodial risk—losing one's private key—implies that the stock bitcoins stored in irretrievable wallets is weakly increasing over time. Such an unobservable stock reduces the effective supply from the amount shown in (A1).

[1] For details and projections, see, for example, https://bitcoin.org/en/developer-guide, https://en.bitcoin.it/wiki/Controlled_supply

Figure A2
Bitcoin inflation eras and total supply



Source: bashco.github.io.

A.4 Price and Hashrate Time Series for other PoW Blockchains

Figure A3
Ether: USD price and hashrate: August 2015–January 2020

Sources: Coinmetrics.io.

Figure A4
Litecoin: USD price and hashrate: August 2015–January 2020

Sources: Coinmetrics.io.

A.5 Examples of Hashrate-Based Attacks

Table A2 provides examples of recent hashrate-based attacks to PoW cryptocurrencies. For each episode, the table shows the monthly returns measured in USD and BTC. For example, Bitcoin Gold, a fork of Bitcoin, experienced a sequence of double-spend attacks in May 2018. Its price measured in bitcoins at the end of that month was 27% lower (40% if measured in USD). In January 2019, following a 50% decline in its price and hashrate relative to four months prior, Ethereum Classic also experienced a double-spend attack and several deep block reorganizations.[2] This attack was significant, given the relatively high market capitalization ranking of this token at the time.

[2] A timeline is provided by the exchange Coinbase (https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de).

Table A2
Examples of majority hashrate attacks to PoW blockchains

Token Name	Symbol	Month of the attack	Beginning-of-month price price (satoshis)	End-of-month price (satoshis)	Return (BTC)	Beginning-of month price (USD)	End-of-month price price (USD)	Return (USD)
Bitcoin Gold	BTG	May 2018	787,000	576,600	-26.73%	71.46	42.90	-39.97%
Verge	XVG	May 2018	877	512	-41.62%	0.0794	0.0385	-51.51%
MonaCoin	MONA	May 2018	55,540	43,970	-20.83%	5.05	3.30	-34.65%
ZenCash	ZEN	June 2018	407,000	278,000	-31.70%	30.45	17.73	-41.77%
Ether. Classic	ETC	Jan 2019	136,884	113,699	-16.94%	5.23	4.02	-23.14%

Source: Prices are from CoinMarketCap. Attacks periods are from CoinDesk and several media sources. Beginning-of-month (end-of-month) prices correspond to the first day of the attack (following) month. One BTC equals 100 million satoshis.

B Supplement to Section 3: The Dynamic Stability of DMEs

We have shown conditions for the existence of stationary DMEs. There can be other equilibria for which b changes over time. Generally, to say more about the dynamic characteristics of a given equilibrium, one must be specific about the utility function and parameter values. Consider the following representation of preferences:

$$u(q) = \frac{1}{1-\sigma}\left((q+\xi)^{1-\sigma} - \xi^{1-\sigma}\right), \xi \in [0,1), \sigma > 0, \tag{B.1}$$

which generally yields two DMEs.[3] Intuition from standard dynamic analyses (Blanchard and Fisher (1989); Walsh (2017)) suggests that the dynamic behavior of a given DME depends on the utility curvature parameter σ. This intuition is correct for the high DME. In contrast, given Bitcoin's security model, we can establish stability properties for the low DME that hold for *any* continuous utility function.

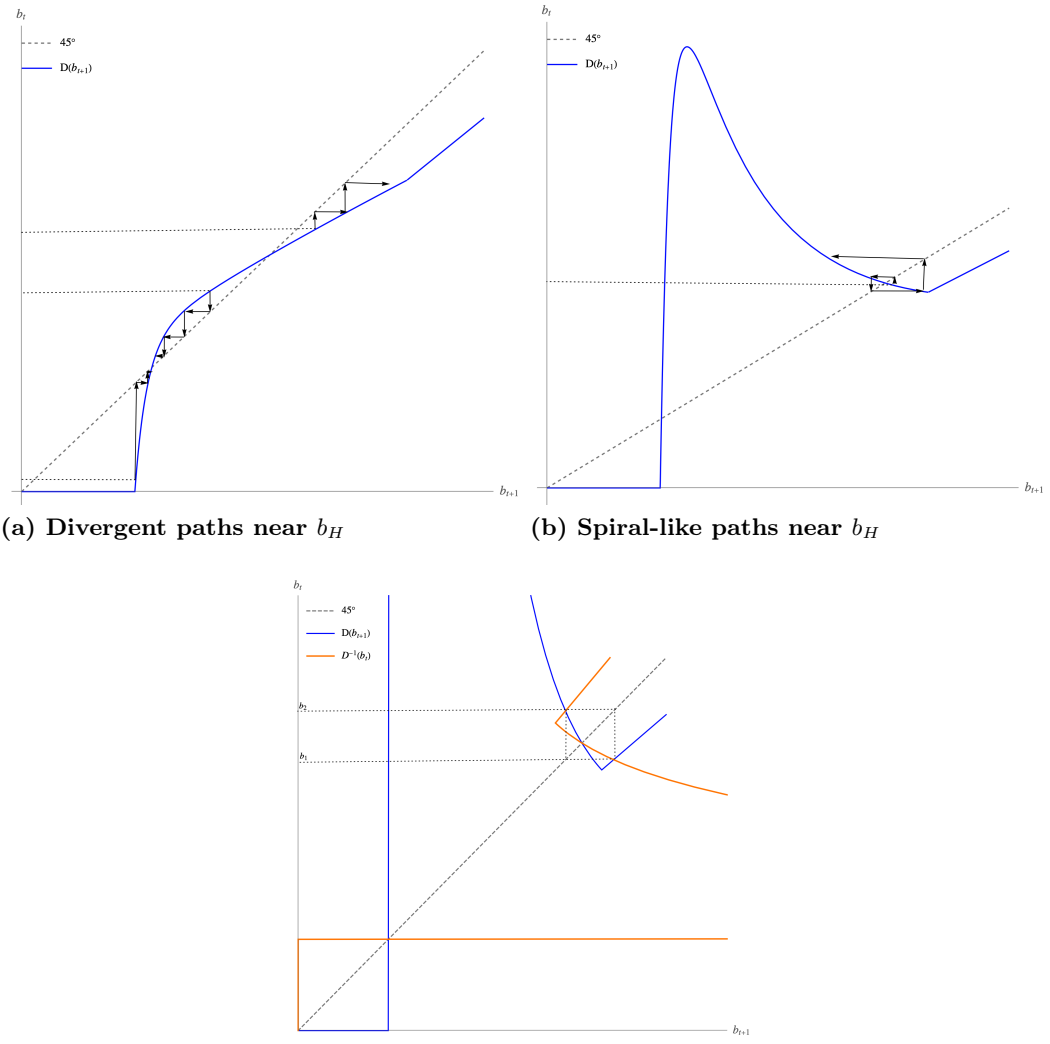
Proposition B1. *Assume that the set of DMEs is non-empty. (i) The lowest DME, b_L, is locally stable: there is a value $\hat{b} > b_L$ such that, for all $b_0 \in \left(0, \hat{b}\right)$, there is an equilibrium starting at b_0 such that $b_t \to b_L$. (ii) Assume that the utility function is as in (B.1) and that b_H satisfies $S\left(H\left(b_H\right), A\right) \approx 1$. Then, there is a threshold value $\hat{\sigma}\left(\delta, \rho, f, \xi\right)$ such that b_H is locally stable if $\sigma > \hat{\sigma}$, and is locally unstable otherwise.*

The driving factor behind the statements in Proposition B1 is the slope of $D(b)$ near a steady-state value b_{ss}. Indeed, the analysis of the dynamic equation $b_t = D\left(b_{t+1}\right)$ suggests that b_{ss} is locally stable when $|D'(b_{ss})| > 1$. For the lowest DME, D must cross the 45-degree line from below in the space (b_{t+1}, b_t) space; therefore, $D'(b_L) > 1$. Again, this property does not depend on the specific utility function: unless it is satisfied, a DME does not exist. Such local stability implies that there is a continuum of equilibria originating near the steady state and converging into it.

[3] An exception is if $D(b)$ is tangent to the 45-degree line at a point $\tilde{b} > 0$, in which case $\tilde{b}$ is unique. If more than two DMEs exist, the results below apply if b_L and b_H are interpreted as the ones with the lowest and the highest values.

In contrast, for the highest DME, we must have $D'(b_H) < 1$, since D must cross the 45-degree line from above. When the curvature parameter is high enough, however, we have $D'(b_H) < 0$. In that case, paths originating near b_H will be spiral-like, where the token's price increases and decreases over time.

Figure B5
Local dynamic stability of DMEs



(a) Divergent paths near b_H

(b) Spiral-like paths near b_H

(c) Two-period cycle near b_H

Figure B5 shows examples using the utility function in (B.1) with $\xi > 0$ and different values of σ. Panel A displays an economy with σ_1 such that $D'(b_H) > 0$, for which the high DME is dynamically unstable; paths that start at $b \approx b_H$ are divergent. Panel B shows an economy with $\sigma_2 > \sigma_1$ such that $D'(b_H) \in (-1, 0)$. Paths starting at $b \approx b_H$ can display divergent spiral trajectories. Panel C displays an economy with $\sigma > \hat{\sigma}$ such that $D'(b_H) < -1$ for $b \approx b_H$, implying that $D(b)$ intersects $D^{-1}(b)$ at two points, b_1 and b_2. Therefore, this economy displays a two-period cycle.

Consistent with Proposition B1, the low DME is dynamically stable, regardless of the value of the utility function parameters.

C Quantitative Supplement

This section develops a quantitative version of the model. Section C.1 explains the calibration of the model parameters. Section C.2 supplements Section 3 by presenting positive and welfare outcomes for each DME. Section C.3 supplements Section 4 by constructing artificial events that resemble the period around the halving of the block reward. Sections C.4 and C.5 supplement the volatility analyses in Section 5.

C.1 Parameter Values

We take the period as representing one month and consider data points from the Bitcoin network as of June 30, 2019, obtained from Blockchain.com and CoinMetrics. At that time, the bitcoin price was USD 10,817, which we interpret as the high equilibrium price, p_H. Other parameter values, summarized in Table C3, are set as follows.

Parameter Calibration. On the supply side, we have $B_0 = 17.79$ million bitcoins, and the system hashrate, H_0, is 58.67 exahashes per second, or approximately 154.15 yottahashes per month. With an average of six blocks mined per hour, there are $4,380$ blocks per month. Given a block reward of 12.5 bitcoins, the monthly supply growth is $\rho_0 = \frac{12.5\times 4,380}{17,790,000} \approx 0.308\%$, or 3.76% annually. Interpreting a miner in the model as a mining pool, we set $m_0 = 10$.[4] Given (p_H, ρ_0, m_0), the cost parameter κ_0 is obtained by inverting equation (6) and matching the observed hashrate.

On the demand side, $\delta_0 = 0.9957$ (0.95 annually), consistent with standard values. We set Bf to match the approximate blockchain volume during June 2019, 5.06 million, obtaining $f_0 = 0.284$.[5] The exact number of bitcoin users is not directly observable, since one user can own multiple anonymous wallets. By assuming that each user has an average of two wallets, we set $n_0 = 20.47$ million, approximately half the number of reported wallets.[6] We represent preferences with (B.1) setting $\xi = 0.01$ and $\sigma = 1/2$, values that are within the range of the money demand estimates of Lagos and Wright (2005).[7]

Security Function. Given the lack of successful attack history, empirically estimating the security function parameters A and k in (2) is not feasible. We therefore consider a range of values that are consistent with the price above being an equilibrium, as follows. For each integer value $k_i \in$

[4] Blockchain.com reports that the top 10 mining pools (e.g., BTC.com, AntPool, ViaBTC) regularly account for more than 90% of the system's hashrate.

[5] Note that the model's expected number of transactions is nf, and the volume per transaction equals buyers' holdings, $\frac{B}{n}$, yielding an average bitcoin volume of Bf per period.

[6] We note that this is a rather conservative number, given the global estimates reported by Rauchs et al. (2018).

[7] Using similar preferences and historical U.S. dollar balances, these authors estimate σ values ranging from 0.16 to 0.48.

Table C3
Parameter values

Supply side				Demand side				
B	ρ (%)	m	κ	δ	σ	ξ	f	n
17.79m	0.308	10	171.58	0.9957	0.5	0.01	0.2844	20.47m

Table C4
Equilibrium outcomes

Security function parameter values					
k	4	6	8	10	12
$A/H_0(\%)$	17.78	31.62	42.67	50.12	56.23
Equilibrium objects					
p_m	1,923.6	3,420.6	4,561.5	5,421.3	6,082.8
p_L	2833.7	4,843.14	6,212.6	7,153.0	7,822.8
S_L	0.788	0.876	0.916	0.937	0.951
q_L	0.244	0.418	0.536	0.617	0.675
$\mathcal{W}_L$	0.126	0.171	0.191	0.202	0.209

$\{4, 6, 8, 10, 12\}$ representing four- to 12-month periods, we invert (8) to compute A_i. Intuitively, if the value of k_i is high, it is more difficult to implement a successful sabotage attack, which demands more computational resources A_i.

C.2 Equilibrium Outcomes

For the considered quantitative model, as in Figure 5, we find two DMEs. For the high DME, the outcomes are as follows. By construction, p_H equals the observed price in all cases, resulting in $S\left(H\left(p_H\right); A_i, k_i\right) = 0.999$ for all i, which yields an annualized probability of a successful attack of 1.19%. The DM trade quantity is $q_H = 0.933$, 94.27% of the efficient trade value $q^* = 1 - \xi = 0.99$. Social welfare in this equilibrium is $\mathcal{W}_H = 0.227$. The bitcoin price associated with the efficient DM good exchange, $p^* = b^*/B$, is USD 11,475.

Table C4 shows the implied p_m values and the resulting outcomes in the low equilibrium for each pair of values $\{k_i, A_i\}$. We note again that reaching any equilibrium displaying $p_L > 0$ requires $H(p_L) > A$. Accordingly, greater A values are associated with greater p_L values.

Unless stated otherwise, in the subsequent quantitative exercises, we adopt the parameter values in Table C3 together with $k = 10$ and $A/H_0 = 50.12\%$ as the baseline calibration.

C.3 Block Reward Halving and Price Changes

To evaluate changes of ρ quantitatively, we exploit the calibrated model to simulate event studies where ρ halves at a normalized time $t = 0$. Such halving events numerically resemble those occurring in 2012, from 25.03% to 12.51%; in 2020, from 3.57% to 1.78%; and that scheduled in 2024, from 1.67% to 0.83%. The parameter values are as in Table C3, but we allow the number of bitcoin buyers to increase

over time, with 20 million in 2012, 40 million in 2020, and 60 million in 2024.[8] All generations of agents behave rationally within an inflation era, except for the generation born at $t-1$, which myopically expects holding returns to stay constant.[9]

Figure C6 shows the resulting price paths. The left (right) columns shows the change in the low (high) DME price. Consistent with the stationarity of real balances, when ρ stays constant, the prices decrease monthly at that rate. We can see that the low-DME price change, $p_{L,0}-p_{L,-1}$, is positive in all cases. However, consistent with Proposition 3, the response of the high equilibrium price is ambiguous. For the highest supply growth era in panel (a), the change in price is positive. Panel (b) shows that the transition to the fourth inflation era displays no significant price change. Panel (c) shows that, for the subsequent halving, the drop in the nominal reward causes an adverse security effect that is not offset by the scarcity channel; therefore, $p_{H,0}-p_{H,-1}<0$.

C.4 Volatility Amplification of Fundamental Shocks

We evaluate the equilibrium price response to a moderate bitcoin adoption shock of 10%. Similar to Figure 7, we decompose the price response into a pure demand effect and a security feedback effect.

Panel (a) of Table C5 shows the results for the baseline calibration. For a positive shock, we can see that the security feedback is responsible for 4.63% of the price displacement; for a negative shock, this proportion is more than twice as large, at 12.92%. Panels (b) and (c) show, respectively, analogous price responses when the initial hashrate of the attacker is 5% higher, as well as when the initial population of buyers is 5% smaller. We can see that, in these cases, the security feedback effect accounts for 25.38% and 28.59%, respectively, of the price changes caused by a negative shock. Generalizing, we can expect more amplification when the attacker is more resourceful and for blockchains with fewer participants.

C.5 Non-fundamental Uncertainty, Expected Time to Attack, and the Saboteur's Resources

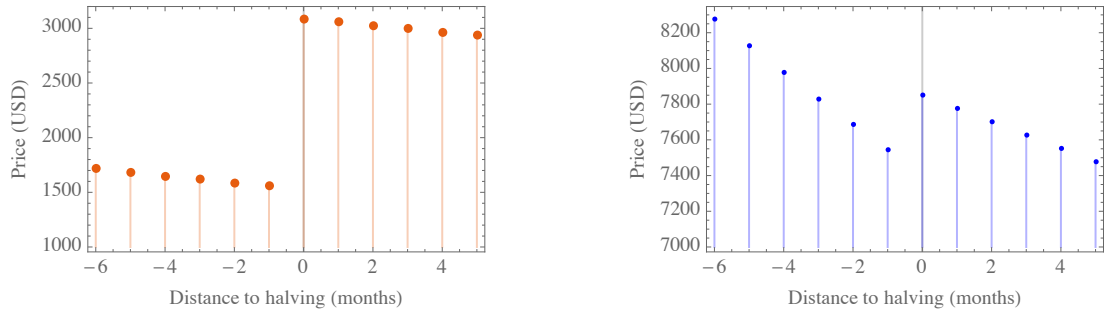
Since the saboteur's resources affect the determination of equilibrium prices and security, they must also affect the price volatility and Bitcoin's life expectancy regarding sunspot equilibria. But how, exactly? An intuitive conjecture is that a more resourceful attacker would make the bitcoin price more unstable and shorten its life expectancy. In this section, we use the quantitative model to construct an example that shows that such intuition is incorrect.

To build a Type I sunspot equilibrium, we solve for b_L, b_H, and the security threshold value b_m, using the baseline calibration. We then set $b_1=\frac{b_m+b_L}{2}$ and $b_2=\frac{b_H+b_L}{2}$ and verify that these values

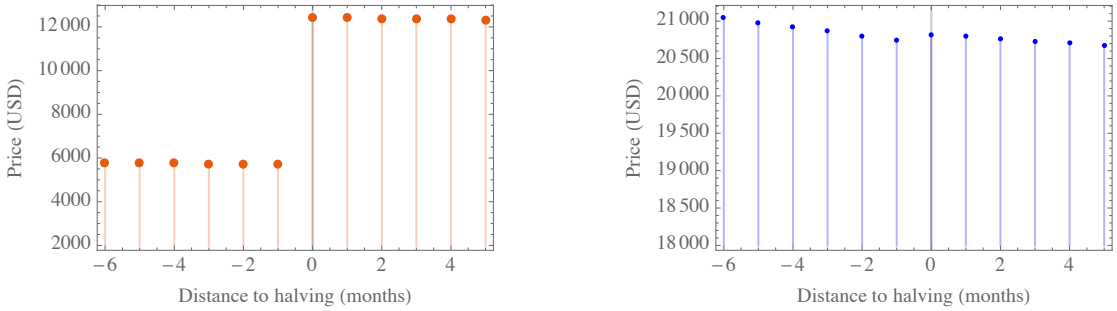
[8] This ensures that a stationary DME always exists. These choices do not affect the conclusions, since the goal is to characterize the direction of price change—for a given n that is *constant* within each event—and not to forecast price levels.

[9] Such myopic agents avoid the necessity of more complicated notation to keep track of time as a state variable, which would not bring additional insights into the systematic connection between monetary policy changes and the security model. Of course, myopic agents would create opportunities for the entry of short-lived arbitrageurs, if that were possible, but that is not our focus. If all agents were rational, the price paths would be smoother, but the conclusions on the direction of price change would remain the same.

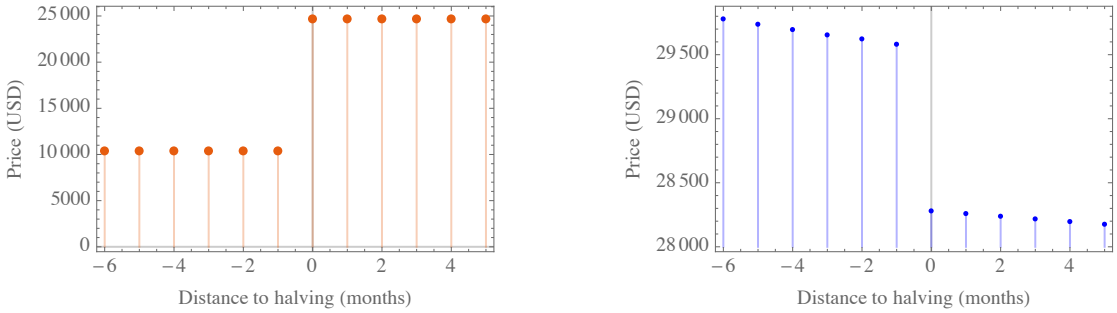
Figure C6
Block reward halving and price changes



(a) Prices around reward halving: Beginning of second inflation era (2012)



(b) Prices around reward halving: Beginning of fourth inflation era (2020)



(c) Prices around reward halving: Beginning of fifth inflation era (2024)

Table C5
Fundamental demand shocks and price–security feedback

	(a) Baseline parameters			(b) Higher attacker hashrate			(c) Smaller blockchain		
	$p_H = 10,817$			$A = 1.05A_0$, $p_H = 10,763.4$			$n = 0.95$, $p_H = 10,221.7$		
Δn	Demand impact	Security feedback	Total impact	Demand impact	Security feedback	Total impact	Demand impact	Security feedback	Total impact
+10%	1,081.7	52.5	1,134.2	1,077.0	84.4	1,161.4	1027.6	29.4	1,057.0
−10%	-1,081.7	-160.5	-1,242.2	-1,077.0	-366.2	-1443.2	-1,027.6	-411.4	-1,439.0
(%)	$\frac{\text{demand}}{\text{total}}$	$\frac{\text{security}}{\text{total}}$	$\frac{\text{total}}{\text{price}}$	$\frac{\text{demand}}{\text{total}}$	$\frac{\text{security}}{\text{total}}$	$\frac{\text{total}}{\text{price}}$	$\frac{\text{demand}}{\text{total}}$	$\frac{\text{security}}{\text{total}}$	$\frac{\text{total}}{\text{price}}$
+10%	95.37	4.63	10.49	92.73	7.27	10.78	97.22	2.78	10.29
−10%	87.08	12.92	-11.48	74.62	25.38	-13.40	71.41	28.59	-14.00

The parameters values are shown in Table C3.

b_t/b_{t+1}	0	b_1	b_2
0	1	0	0
b_1	$1 - S(\mathbb{E}_1 b, A)$	$S(\mathbb{E}_1 b, A)\,\phi_1$	$S(\mathbb{E}_1 b, A)\,(1-\phi_1)$
b_2	$1 - S(\mathbb{E}_2 b, A)$	$S(\mathbb{E}_2 b, A)\,(1-\phi_2)$	$S(\mathbb{E}_2 b, A)\,\phi_2$

Table C6
Transition probability matrix

satisfy the existence conditions in the proof of Proposition 7. Next, by solving the equation system in (12), we obtain the associated probabilities ϕ_1 and ϕ_2. We then repeat this procedure for alternative values of A. For each equilibrium, we simulate dynamic economies according to Table C6 until an attack period τ, setting $\omega_{t=0} = 1$ with probability one-half. We then compute the average attack time (AAT) and the standard deviation of prices until τ. Table C7 shows the outcomes for both the sunspot (left panel) and non-sunspot (right panel) equilibria. For the latter, one AAT estimate is associated with each DME, with no price volatility.

What is the effect of an increase in the saboteur's resources? Contrary to the intuition above, we observe in this example that volatility *decreases* with A. Note that the saboteur's impact on volatility is twofold. There is a value effect, regarding the determination of $p_i = \frac{b_i}{B}$, and a probability effect, regarding the determination of the elements in Table C6. We can see that, as A increases, p_1 and p_2 become closer to each other, reducing volatility regarding jumps $p_1 \to p_2$ and $p_2 \to p_1$. On the probability end, as A increases, state 1 becomes less persistent, while state 2 becomes more persistent. Intuitively, if attack resources increase, agents only coordinate on the sunspot when the persistence of the optimistic state is relatively strong, as in this example, which reduces volatility further in the aggregate.

Turning now to AATs, in the right panel of Table C7, we find striking divergence in security outcomes when agents ignore sunspots. For the baseline parametrization (the row where $A = 1$), the average AATs are 995.65 and 17.29 for the high and low DMEs, respectively. The sunspot AAT value is much closer to the low DME value, at 23.94, which is intuitive, since all paths visit the high–attack risk state b_1 with positive probability.

We can see that, in contrast to the motivating intuition, sunspot AATs do not decrease with A.

A	Sunspot equilibrium (Type I)						Non-sunspot equilibria			
	p_1	p_2	ϕ_1	ϕ_2	Price s.d.	AAT	p_L	AAT low	p_H	AAT high
0.85	5,222	8,357	0.894	0.892	936.95	16.35	5,835	11.62	10,879	5,450
0.9	5,567	8,561	0.883	0.899	906.32	18.51	6,255	12.93	10,867	3,036
1.0	6,287	8,984	0.858	0.922	806.46	23.94	7,153	17.29	10,817	995.65
1.1	7,076	9,429	0.833	0.955	631.13	34.51	8,189	24.59	10.669	335.35
1.15	7,536	9,659	0.822	0.977	457.73	44.97	8,838	34.06	10,480	182.97

Baseline parameter values are described in Table C3. A values are normalized using $A_0 = 1$.

Table C7
Stochastic sunspot equilibria, price volatility, and AATs

Despite its direct negative effect on security ($S_A < 0$), an increase in A has two positive general equilibrium effects on the average lifetime. First, it raises both p_1 and p_2, providing miners with better incentives across states. Second, the increase in A induces less persistence in the riskier state and more persistence in the safer state. The net effect is an increase in the average life. For example, the sunspot equilibrium with $A = 1.15A_0$ displays an expected life of 44.97 (87.8% higher than baseline) and is associated with a reduction from 995.65 to 182.97 for the high-DME lifetime.

Overall, this analysis demonstrates that price stability cannot be used as a reliable proxy for the strength of an attacker's commitment against Bitcoin.

D Implications for the Mining Industry and Minting Costs

Unlike institutions in regulated payment systems, bitcoin miners have free entry and exit. In this section, we investigate the effects of competition intensity on miners' profits, and we analyze the perfectly competitive limits for the bitcoin price and mintage costs. These analyses highlight critical structural differences between mining competition and traditional Cournot competition.

D.1 Miner Entry and Profits

In the system designed by Nakamoto, miners do not compete in prices but, rather, in capacity, similar to Cournot firms. In both cases, an increase in the number of competitors results in an expansion of total capacity (Lemma 1). In sharp contrast, however, we find that the bitcoin price can *increase* in the total number of miners, a reverse Cournot outcome. This is due to a key structural difference. In the Nakamoto system, miners do not compete in bitcoin units—minting is beyond anyone's ability—but, rather, in units of *security inputs*.

For the high DME, a larger number of miners leads to a smaller probability of a successful attack, greater bitcoin demand, and a higher equilibrium valuation. A direct implication of this DME response is that miners' profits are less sensitive to entry relative to an economy where prices and security are not jointly determined.

Proposition D2. *Assume the existence of a high DME with m miners and let $\Pi(b_H, m)$ denote miners' value function. (i) An increase in the number of miners increases b_H. Moreover, (ii) the general equilibrium profit response to entry is smaller than its direct impact: $\left|\frac{d}{dm}\Pi(m, b_H)\right| < \left|\frac{\partial}{\partial m}\Pi(m, b_H)\right|$.*

The intuition for the second part of the proposition is that changes in m have two distinct effects. First, m drives the intensity of the PoW mining contest, which is always negatively related to equilibrium profits. Second, by part (i), the general equilibrium effect on the bitcoin price feeds back on the real value of the mining reward. The second effect is thus *positive*, flattening the miner value function regarding changes in m. For an increase in m,

$$\underbrace{\frac{d}{dm}\Pi(m, b_H)}_{\text{Profit sensitivity to miner entry}} \propto \underbrace{-\frac{b_H}{m}}_{\text{mining contest effect } <0} + \underbrace{\frac{db_H}{dm}}_{\text{mining reward effect } >0}.$$

Remark. Proposition 6 indicates that, from the users' perspective, Bitcoin's security model amplifies the *price volatility* caused by demand-side entry shocks. Proposition D2, on the other hand, indicates that, from the miners' viewpoint, it buffers the *profit volatility* caused by supply-side entry shocks.

D.2 Perfect Mining Competition and Minting Costs

Next, we analyze the competitive limit $m \to +\infty$ on the bitcoin price and security. We are also interested in characterizing the minting cost of a new bitcoin, given by

$$\mu := \frac{\text{mining costs per block}}{\text{nominal block reward}} = \frac{mC(h)}{\psi}.$$

Because our focus here is on mining costs, we consider a family of cost functions that include linear and convex specifications: $C(h) = \kappa h^\gamma$, $\gamma \in \{1, 2, ...\}$, $\kappa > 0$.

Focusing on stationary allocations, we first ask: what are the hashrate and security limits when $m \to +\infty$? For that, consider a high DME and its corresponding hash investment from Lemma 1: $h = (\frac{m-1}{m^2}(\frac{\rho-1}{2})\frac{\delta}{\rho}\frac{b_H}{\gamma\kappa})^{\frac{1}{\gamma}}$. With linear mining costs, we then obtain

$$\lim_{m\to+\infty} H = \left(\frac{\rho-1}{2}\right)\frac{\delta}{\rho}\frac{b_H^\infty}{\kappa}, \tag{D.1}$$

$$\lim_{m\to+\infty} S(H, A) = 1 - \left(\frac{A}{b_H^\infty}\frac{2\kappa}{(\rho-1)}\frac{\rho}{\delta}\right)^k, \tag{D.2}$$

where $\chi^\infty := \lim_{m\to+\infty}\chi$. Note that, by Lemma 2, we have $b_H^\infty < b^*$, and, thus, $H^\infty < \left(\frac{\rho-1}{2}\right)\frac{\delta}{\rho}\frac{b^*}{\kappa}$ and $S^\infty < 1$. Therefore, equations (D.1) and (D.2) provide a well-defined limit for both the system's hashrate and security.

With quadratic mining costs, we have $H(b_H) = \left(\left(\frac{m-1}{2\kappa}\right)\left(\frac{\rho-1}{2}\right)\frac{\delta}{\rho}b_H\right)^{\frac{1}{2}}$. Unlike the linear case, H scales up proportionally with m, implying that no finite limit exists for H^∞; thus $S^\infty = 1$. One can verify that this implication generalizes to other convex cost functions, as in the following proposition.

Proposition D3. *Consider the limit $m \to +\infty$ of a high DME. (i) With linear mining costs, the security level associated with p_H^∞ is given by (D.2), and $\mu_H^\infty = \frac{\delta}{\rho} p_H^\infty$. (ii) With convex mining costs ($\gamma > 1$), if a DME exists, it is unique, and the equilibrium price p^∞ does not depend on the security function. Moreover, $\mu^\infty = \frac{1}{\gamma}\left(\frac{\delta}{\rho} p^\infty\right)$.*

The fact that H grows unboundedly with $\gamma > 1$ stems from the lack of price decline together with $C'(h) \to 0$, allowing $m \times h$ to grow unboundedly, and resulting in an entirely secure system. Therefore, p^∞ becomes the only equilibrium price and it must coincide with the extrinsic price with $\overline{S} \to 1$. The finding that convex mining costs can generate such a striking security outcome is, of course, not meant to represent a realistic outcome. It is not robust to the presence of positive miner entry costs. It provides, however, a new theory perspective on how miner competition can deliver implications that differ from those in familiar settings like Cournot's.

The competitive limit minting cost in Proposition D3 provides a sharp prediction. The limit cost must be equal to a fraction of the limit price, as given by the inverse of the cost function curvature coefficient. For example, with quadratic costs and $\xi = 0$, the model calibration implies:

$$\mu^\infty = \underbrace{\frac{1}{2}}_{1/\gamma} \times \underbrace{\frac{\delta}{\rho}\left(\frac{f\rho^\sigma}{\rho - \delta(1-f)}\right)^{\frac{1}{\sigma}} \frac{n}{B}\delta^{\frac{(1-\sigma)}{\sigma}}}_{p^\infty = \$11{,}008.7} = \$5,504.35.$$

Therefore, the empirical observation that the mintage cost per bitcoin is below the token price does not constitute direct evidence of market power in the mining sector; neither that miners require a compensation premium for price risk.

E Proof of Lemmas

In this section, we provide the proofs to the lemmas in the main text and we establish an additional lemma. We sometimes avoid displaying the dependency of S and its derivatives on $(H(b), A)$ and $H(b)$ on b for compactness of notation.

Proof of Lemma 1

Part (i). Miner j takes the price as given and solves $\max_{h_{jt}} \delta\psi_t \mathbb{E}_t^1 p_{t+1} \times \mathbb{P}(h_{jt}, h_{-jt}) - C(h_{jt})$, with first-order condition $\delta\psi_t \mathbb{E}_t^1 p_{t+1} \frac{\partial \mathbb{P}(h_{jt}, h_{-jt})}{\partial h_{jt}} = C'(h_{jt})$. Using $\frac{\partial \mathbb{P}(h_{jt}, h_{-jt})}{\partial h_{jt}} = \frac{H_t - h_{jt}}{H_t^2}$, we obtain $\delta\psi_t \mathbb{E}_t^1 p_{t+1} \frac{H_t - h_{jt}^*}{H_t^2} = C'(h_{jt}^*)$. With symmetric identical miners, $h_{jt} = h_t$, for all j, and $H_t = m h_t$, so the equilibrium symmetric hashrate satisfies $C'(h_t^*)h_t^* = \delta\psi_t \mathbb{E}_t^1 p_{t+1}\left(\frac{m-1}{m^2}\right)$.

Parts (ii) to (iv) can be proven by applying the implicit function theorem to express the near-equilibrium response of h^* to each parameter change. For (ii), we have $\frac{dh^*}{d\psi}[C'(h^*) + h^* C''(h^*)] - \delta \mathbb{E}_t^1 p_{t+1} \frac{m-1}{m^2} = 0$. Since $H^* = m h^*$, then $\frac{dH^*}{d\psi} = \frac{\delta \mathbb{E}_t^1 p_{t+1} \frac{m-1}{m}}{C'(h^*) + h^* C''(h^*)} > 0$. The effect of a change in resale price expectations is analogous. For (iii), we simplify the exposition without much loss of generality assuming $m \geq 2$ to be a continuous variable. From $H^* = m h^*$, it follows that $\frac{dH^*}{dm} = h^* + m\frac{dh^*(m)}{dm}$.

From differentiating the first-order condition, $\frac{dH^*}{dm} = h^* - \frac{m-2}{m^2}\frac{\delta\psi_t\mathbb{E}_t^1 p_{t+1}}{(C'+h^*C'')}$, which implies that

$$\begin{aligned}\frac{dH^*}{dm}C'(h^*) &= h^*C'(h^*) - \left(\frac{m-2}{m-1}\right)\left(\frac{m-1}{m^2}\right)\delta\psi_t\mathbb{E}_t^1 p_{t+1}\frac{C'(h^*)}{C'(h^*)+h^*C''(h^*)},\\ &= h^*C'(h^*)\left(1-\left(\frac{m-2}{m-1}\right)\left(\frac{C'(h^*)}{C'(h^*)+h^*C''(h^*)}\right)\right).\end{aligned}$$

Note that $C'(h^*) > 0$, $\frac{m-2}{m-1} < 1$, and, by $C'' \geq 0$ and $h^* \geq 0$, $\frac{C'}{C'+h^*C''} \leq 1$. Therefore, the right-hand side of equation above is positive and we conclude that $\frac{dH^*}{dm} > 0$. For (iv), note that, if C' marginally increases pointwise for every h, then $dh^* < 0$ to satisfy equation (1); thus $dH^* < 0$. □

Proof of Lemma 2

The proof of this lemma extends to this environment the analyses of Lagos and Wright (2003) and Rocheteau and Wright (2005). Here, sellers' problem is relatively simple, since the condition $\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t} = \frac{1}{z_t}$ makes the DM good supply perfectly elastic. Buyers' program can be re-expressed inserting the budget constraint in (4), as follows

$$\max_{b_{it}\geq 0} -b_{it} + S_t\underbrace{\left(f\max_{q_t^d\leq\frac{b_{it}}{z_t}}\left\{u\left(q_{it}^d\right)+\delta\mathbb{E}_t^1\left(\left(b_{it}-z_tq_{it}^d\right)\frac{p_{t+1}}{p_t}\right)\right\}+(1-f)\,\delta\mathbb{E}_t^1\left(b_{it}\frac{p_{t+1}}{p_t}\right)\right)}_{V(b_{it})},$$

or, more compactly, as $\max_{b_{it}\geq 0}\{-b_{it}+S_tV(b_{it})\}$. The first-order condition is $-1+S_tV'(b_{it}) \leq 0$ and $S_tV'(b_{it}) = 1$ if $b_{it} > 0$.

The value q_t^* is the solution to the unconstrained optimization within V, $u'(q_t^*) = z_t\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t} = 1$. Let $b_t^* = q_t^*z_t$. If $b_{it} \geq b_t^*$, a buyer demands q_t^* and we have

$$V(b_{it}) = f\left\{u(q_t^*)+\delta\mathbb{E}_t^1\left((b_{it}-b_t^*)\frac{p_{t+1}}{p_t}\right)\right\}+(1-f)\,\delta\mathbb{E}_t^1\left(b_{it}\frac{p_{t+1}}{p_t}\right),$$

and $V'(b_{it}) = \delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t}$.

If $b_{it} < b_t^*$, the constraint in the DM is binding: $q_t^d = \frac{b_{it}}{z_t}$. In that case, a buyer that meets a seller carries no bitcoins to the next CM and we have

$$V'(b_{it}) = \frac{f}{z_t}u'\left(\frac{b_{it}}{z_t}\right)+(1-f)\,\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t}. \tag{E.1}$$

Given $u'(0) = +\infty$, if $S_t > 0$, $-1+S_tV'(0) = +\infty$. Since $u'' < 0$, $-1+S_tV'(b)$ is a strictly decreasing function of b for all $b \in [0, b^*]$. Moreover, for $b \geq b^*$, the first-order condition is $-1+S_tV'(b) = -1+S_t\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t} \leq 0$. Clearly, if $S_t\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t} > 1$, the buyers' problem has no solution, since buyers would demand an unbounded amount of tokens. If, on the other hand, $S_t\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t} < 1$, there is a unique $\tilde{b} < b^*$ that satisfies $S_tV'\left(\tilde{b}\right) = 1$. Using the market clearing conditions $nB_{it} = B_t$ and $z_t\delta\mathbb{E}_t^1\frac{p_{t+1}}{p_t} = 1$

in $S_t V'\left(\tilde{b}\right)=1$, and rearranging, we obtain the expression in the lemma. □

Proof of Lemma 3

Buyer i's program can be expressed as

$$\max_{\{c_{it},l_{it},b_{it},\mu_{it}\}\geq 0}\left\{c_{it}-l_{it}+\underbrace{f_B\left(S\left(u\left(q_B\left(b_{it}\right)\right)\right)+\frac{\delta}{\gamma}\mu_{it}\right)}_{\text{type-B meeting}}+\underbrace{f_M\left(u\left(q_M\left(\mu_{it}\right)\right)+\frac{\delta S}{\rho}b_{it}\right)}_{\text{type-M meeting}}\right.$$
$$\left.+\underbrace{f_{MB}\left(S\left(u\left(q_{MB}\left(\mu_{it},b_{it}\right)\right)\right)+\left(1-S\right)\left(u\left(q_{MB}\left(\mu_{it},0\right)\right)\right)\right)}_{\text{type-MB meeting}}+\underbrace{\left(1-f\right)\delta\left(\frac{Sb_{it}}{\rho}+\frac{\mu_{it}}{\gamma}\right)}_{\text{no meeting}}\right\}, \tag{E.2}$$

subject to a budget constraint given by $c_{it}+b_{it}+\mu_{it}\leq l_{it}+T_t$, where T is a transfer to accommodate changes in M. Each bracketed term in the above program corresponds to a particular meeting type during the DM; the last term reflects the expected residual value of bitcoin and fiat currency balances if the buyer does not find trade opportunities. Combining (E.2) with the budget constraint, using $q_{MB}\left(\mu,0\right)=q_M\left(\mu\right)$, and re-arranging, we obtain

$$\max_{\{b_{it},\mu_{it}\}\geq 0}-\mu_{it}-b_{it}+T_t+f_BS\left(u\left(q_B\left(b_{it}\right)\right)\right)+\left(f_M+\left(1-S\right)f_{MB}\right)\left(u\left(q_M\left(\mu_{it}\right)\right)\right)$$
$$+Sf_{MB}\left(u\left(q_{MB}\left(\mu_{it},b_{it}\right)\right)\right)+\delta\left(\left(1-f+f_B\right)\frac{\mu_{it}}{\gamma}+\left(1-f+f_M\right)S\frac{b_{it}}{\rho}\right).$$

In an interior solution where $b>0$ and $\mu>0$, the first-order conditions with respect to b and μ yield equations (13) and (14), respectively. □

We present an additional lemma that is used in the proofs of the proposition in the main text.

Lemma E1. *Consider a stationary DME b satisfying $y(b,\theta)-1=0$, $y(b,\theta):=\frac{\delta S}{\rho}\left(f\left(u'\left(q\left(b\right)\right)-1\right)+1\right)$ and θ represents a given parameter—note that b satisfying $y(b,\theta)-1=0$ is equivalent to (8). By the implicit function theorem, in the vicinity of b_{ss}, we have $\frac{db}{d\theta}=-\frac{y_\theta}{y_b}$. At $b=b_H$, we have $y_b<0$; while at $b=b_L$, $y_b>0$. Therefore, at b_H the sign of $\frac{db}{d\theta}$ and that of y_θ coincide; while at b_L they have opposite sign.*

Proof: By definition, $D(b)=y\left(b,\theta\right)b$, therefore, $D'\left(b\right)=y_b\left(b,\theta\right)b+y\left(b,\theta\right)$. As shown in the proof of Proposition 2, $D'\left(b\right)$ is less than one at b_H and greater than one at b_L. For b_H, we must then have $y_b\left(b_H,\theta\right)b+y\left(b_H,\theta\right)<1$, which implies that

$$y_b\left(b_H,\theta\right)<\frac{1-y\left(b_H,\theta\right)}{b_H}=0.$$

Analogously, for b_L, we must have $y_b\left(b_L,\theta\right)b_L+y\left(b_L,\theta\right)>1$, which implies that $y_b\left(b_L,\theta\right)>0$. □

F Proofs of Internet Appendix Propositions

Proof of Proposition B1

In the neighborhood of a stationary DME value b_{ss}, $b_t = D(b_{t+1})$ can be approximated as $b_t \approx D(b_{ss}) + D'(b_{ss})(b_{t+1} - b_{ss})$. Using $b_{ss} = D(b_{ss})$, we can express the approximation as $b_{t+1} - b_{ss} \approx \frac{b_t - b_{ss}}{D'(b_{ss})}$. Therefore, $b_{t+1} \approx b_{ss} + \frac{b_0 - b_{ss}}{(D'(b_{ss}))^t}$. The slope of D at b_{ss} thus determines the local stability properties. When $|D'(b_{ss})| > 1$, b_t approaches b_{ss} for paths that start at b_0 near b_{ss}. When $|D'(b_{ss})| < 1$, b_t diverges from b_{ss}.

Consider now the low DME, b_L. Since $D(b) < b$ for $b < b_L$, we must have $D'(b_L) > 1$. Therefore, paths that start at b_0 near b_L must display $b_t \to b_L$. When $D^{-1}(b_t)$ is single valued, $\hat{b} = b_H$, so for any initial value $b_0 \in (0, b_H)$ there is a equilibrium with the property that $b_t \to b_L$. Otherwise, if $D^{-1}(b_t)$ is a correspondence, we can have $\hat{b} < b_H$.

Consider now the highest DME, b_H. Since D must cross b from above, we must have $D'(b_H) < 1$. The system could only display local stability around b_H if $D'(b_H) < -1$. To characterize such case using (B.1), we must compute $D'(b)$ near b_H. If $S(b_H, A) \approx 1$, $S_H \approx 0$, and for $b < b^*$:

$$D'(b) = \frac{\delta}{\rho}\left(1 - f + f\left(q(b) + \xi\right)^{-\sigma}\left(1 - \sigma\frac{q(b)}{q(b) + \xi}\right)\right). \tag{F.1}$$

From (B.1), it follows that $q_H = \frac{\delta b_H}{\rho n}$ can be expressed as $q_H = \left(\frac{\delta f}{\rho - \delta(1-f)}\right)^{\frac{1}{\sigma}} - \xi$. Combining the latter with (F.1), and rearranging:

$$D'(b_H) = \left(1 - \frac{\delta}{\rho}(1-f)\right)\left(1 - \sigma\frac{(\delta f)^{\frac{1}{\sigma}} - \xi\left(\delta f + \rho - \delta\right)^{\frac{1}{\sigma}}}{(\delta f)^{\frac{1}{\sigma}}}\right) + \frac{\delta}{\rho}(1-f). \tag{F.2}$$

Note that given our parametric restrictions, the right-hand side of the expression above is a continuous and decreasing function of the utility parameter σ. Defining $\hat{\sigma}$ by $D'(b_H, \hat{\sigma}) = -1$ from (F.2), we conclude that b_H is locally stable if $\sigma > \hat{\sigma}$ and locally unstable otherwise.

Proof of Proposition D2

We argue first that $\frac{db_H}{dm} > 0$. From Lemma E1, it suffices that $y_m = S_H H_m \frac{\delta}{\rho}\left\{f\left(u'\left(q(b)\right) - 1\right) + 1\right\} > 0$, which holds since $H_m > 0$ from Lemma 1 and $S_H > 0$ from (2).

To show that $\left|\frac{d}{dm}\Pi(m, b_H)\right| < \left|\frac{\partial}{\partial m}\Pi(m, b_H)\right|$, we note that the maximum attainable value for miners in any given mining stage is $\Pi = \max_{h_j \geq 0} \frac{h_j}{H} \times \delta\psi_t \mathbb{E}_t^1 p_{t+1} - \kappa h_j$. Using (1), $h = \frac{H}{m}$, and (6):

$$\Pi(b_H, m) = \frac{1}{m}\frac{\delta}{\rho}\left(\frac{\rho - 1}{2}\right)b_H - \left(\frac{m-1}{m^2}\right)\frac{\delta}{\rho}\left(\frac{\rho - 1}{2}\right)b_H = \frac{\delta}{\rho}\left(\frac{\rho - 1}{2m^2}\right)b_H.$$

Therefore,

$$\frac{d}{dm}\Pi\left(b_H, m\right) = \{ \underbrace{-\frac{1}{m} b_H}_{\text{competition effect: } \frac{\partial \Pi}{\partial m} < 0} + \underbrace{\frac{db_H}{dm}}_{\text{mining reward effect } > 0} \} \left(\frac{\rho - 1}{2m^2}\right) \frac{\delta}{\rho}, \tag{F.3}$$

which proves the inequality in the proposition. □

Proof of Proposition D3

Consider the average minting cost when $\gamma = 1$, $\mu_t = \frac{m\kappa h_t^*}{\psi_t}$. Substituting for the optimal hashrate and the block reward at b_H

$$\mu_t = \underbrace{\frac{m-1}{m}\frac{\delta}{\rho}\left(\frac{\rho-1}{2}\right) b_H}_{\kappa m h^*} \times \frac{1}{\psi_t} = \frac{m-1}{m}\frac{\delta}{\rho} p_{H,t},$$

where the last equality uses $\frac{\psi_t}{B_t} = \frac{\rho-1}{2}$. Thus, $\lim_{m\to+\infty} \mu_t = \frac{\delta}{\rho} p_{H,t}^{\infty}$, proving part (i).

For part (ii), consider $C(h) = \kappa h^{\gamma}$, $\gamma \in \{2, 3, ...\}$. Since $S^{\infty} = 1$, DME uniqueness follows from Lemma 2.

We now derive the minting cost competitive limit. From Lemma 1, in a stationary allocation, $h^* C'(h^*) = \frac{m-1}{m^2}\frac{\delta}{\rho}\left(\frac{\rho-1}{2}\right) b$. Since $\lim_{m\to+\infty} b$ is finite, we have $\lim_{m\to+\infty} h^* C'(h^*) = 0$, implying that $\lim_{m\to+\infty} h^* = 0$. Thus, $\lim_{m\to+\infty} \mu_t = \lim_{m\to+\infty} \frac{mC(h^*(m))}{\psi}$ leads to an indeterminacy of the type $\infty \times 0$. However, one can rearrange the expression as $\frac{C(h^*(m))}{\psi}\frac{1}{m^{-1}}$ and compute the limit using L'Hospital rule:

$$\lim_{m\to+\infty} \mu_t = \lim_{m\to+\infty} \frac{\left(\frac{1}{\psi_t} C\left(h^*(m)\right)\right)'}{\left(m^{-1}\right)'} = \lim_{m\to+\infty} \frac{\left(\frac{1}{\psi_t} C'\left(h^*(m)\right)\frac{dh^*}{dm}\right)}{\left(-m^{-2}\right)}. \tag{F.4}$$

From Lemma 1, $\frac{dh^*}{dm} = \frac{-\delta\psi_t \mathbb{E}_t^1 p_{t+1}(m-2)}{m^3[C'(h^*)+h^*C''(h^*)]}$. Substituting in (F.4), we obtain

$$\begin{aligned}\lim_{m\to+\infty} \mu_t &= \lim_{m\to+\infty} \frac{\frac{1}{\psi_t} C'\left(h^*\right)}{-m^{-2}} \left(\frac{-\delta\psi_t \mathbb{E}_t^1 p_{t+1}\left(m-2\right)}{m^3[C'(h^*) + h^*C''(h^*)]}\right) \\ &= \lim_{m\to+\infty} \left(\frac{C'\left(h^*\right)}{C'(h^*) + h^*C''(h^*)}\right)\left(\frac{m-2}{m}\right)\frac{\delta}{\rho} p_t = \frac{1}{\gamma}\left(\frac{\delta}{\rho} p_t^{\infty}\right),\end{aligned}$$

which concludes the proof. □

References

Blanchard, O. J. and S. Fisher (1989). *Lectures on Macroeconomics*. Boston: The MIT Press.

Easley, D., M. O'Hara, and S. Basu (2019). From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics 134*(1), 91–109.

Huberman, G., J. D. Leshno, and C. Moallemi (2019). An Economic Analysis of the Bitcoin Payment System. *Working Paper*.

Lagos, R. and R. Wright (2003). Dynamics, cycles, and sunspot equilibria in 'genuinely dynamic, fundamentally disaggregative' models of money. *Journal of Economic Theory 109*(2), 156–171.

Lagos, R. and R. Wright (2005). A Unified Framework for Monetary Theory and Policy Analysis. *Journal of Political Economy 113*(3), 463–484.

Lehar, A. and C. A. Parlour (2019). Miner Collusion and the BitCoin Protocol. *Working Paper*.

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *White Paper*.

Rauchs, M., A. Blandin, K. Klein, G. Pieters, M. Recanatini, and B. Zhang (2018). 2nd Global Cryptoasset Benchmarking Study. Technical report, Cambridge Centre for Alternative Finance, Cambridge.

Rocheteau, G. and R. Wright (2005). Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium. *Econometrica 73*(1), 175–202.

Walsh, C. E. (2017). *Monetary Theory and Policy* (4th ed.). Cambridge, MA: MIT Press.