The Review of Financial Studies

Decentralizing Money: Bitcoin Prices and Blockchain Security

Emiliano S. Pagnotta
Imperial College London and Singapore Management University

We address the determination of bitcoin prices and decentralized security. Users forecast the transactional and resale values of holdings, pricing the risk of systemic attacks. Miners contribute resources to protect against attackers and compete for block rewards. Bitcoin's design leads to multiple equilibria: the same blockchain technology is 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 and busts unconnected to fundamentals. We characterize how viability versus fiat currency depends on bitcoin's relative acceptability and inflation protection. (*JEL* E41,E42, E52, G12, G15, G18)

Received February 19, 2020; editorial decision November 7, 2020 by Editor Itay Goldstein. Authors have furnished an Internet Appendix, which is available on the Oxford University Press Web site next to the link to the final published paper online.

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 price reflects

For helpful, detailed, and insightful comments, I am grateful to Itay Goldstein (the editor) and two anonymous referees. 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, and Randall Wright; 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, the Swiss Finance Institute at EPFL, Central European University, Durham Business School, Cass Business School, NUS Business School, CUHK Business School, HKU Business School, University of Luxembourg, and Singapore Management University. Supplementary data can be found on *The Review of Financial Studies* web site. Send correspondence to Emiliano Pagnotta, esp.research@pm.me.

[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).

The Review of Financial Studies 34 (2021) 1–42

doi:10.1093/rfs/hhaa149 Advance access publication 20 January 2021

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 part of a cryptocurrency 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 both perspectives could yield elements of truth, 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 also intrinsically connected to security. To understand equilibrium price determination, we must disentangle the interplay between these breakthrough features and bitcoins' monetary function.

In this paper, we analyze an economy in which 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 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 resultant valuation for bitcoins is low. The opposite

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

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 is that the security of PoW systems should be seen as an *economic outcome* and not as an embedded property of its blockchain technology. Put simply, since the same fundamentals are consistent with outcomes displaying sharply different security levels, one should not regard the blockchain technology as a production function for secure databases; as often presented to businesspeople and regulators.[3]

In Section 2, we present this result 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 Lagos and Wright (2005) and Rocheteau and Wright (2005). Our focus is on the properties 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 by 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.

[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 (see, e.g., Zamfir (2015)). In contrast, they do 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.

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 responsible for this conclusion, neither of which is 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 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 choose 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

[5] This is also in contrast to 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 optimal for price and welfare.

[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 nonfundamental sources of uncertainty goes beyond price jumps. Because of 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.

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, 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 because of well-known channels, such as entry externalities or storage costs (see, e.g., Lagos, Rocheteau, and Wright, 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

[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, Karlsen, and Putnins (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.

[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, Fuchs, and Green (2019), who focus on assets with heterogeneous payoffs under adverse selection. Here, the environment 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

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).

Several contemporaneous papers emphasize one or more aspects of the intricate Bitcoin mining ecosystem. While we focus on seigniorage-financed rewards, Easley, O'Hara, and Basu (2019) and Huberman, Leshno, and Moallemi (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, Fernandez-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

Goldstein, Ozdenoren, and Yuan (2011), where coordination by speculators can persuade the monetary authority to abandon the monetary regime due to weak fundamentals.

[13] A recent related literature tackles "permissioned" blockchains and is 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). Adadi and Brunnermeier (2018) formally analyze trade-offs involving public and permissioned blockchains. Hinzen, John, and Saleh (2019) and Zimmerman (2019) highlight limits to bitcoins' usability due to design aspects of its public blockchain.

explicitly incorporating Bitcoin's security shortcomings. This allows us to refine the conditions under which bitcoins can be positively priced.

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.

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 will 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 refer to such a link as an intrinsic security model.

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**.

We note that the intrinsic link between the token price and security is no longer exclusive to Bitcoin; rather, it is present in blockchain-based networks, such as Ethereum, Monero, and Litecoin. In contrast, Ripple is a digital currency system in which approved network members verify transactions. Although

[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* applies.

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

[16] See Section A.1 of the Internet Appendix. 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.

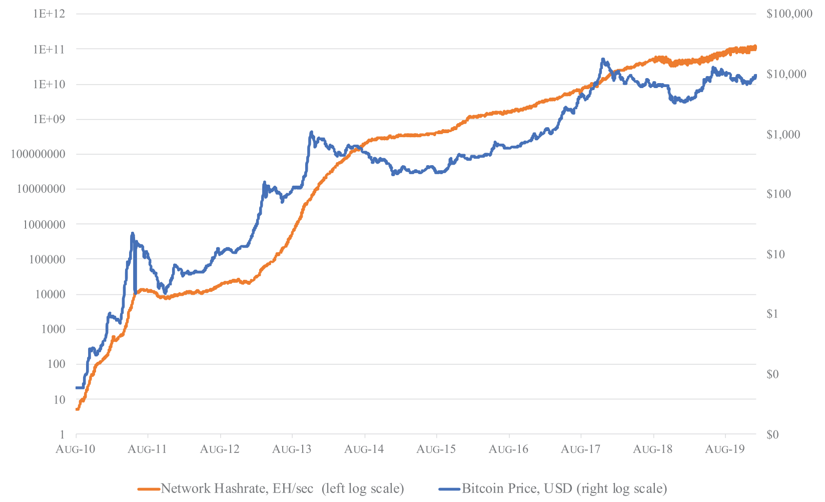


Figure 1
Bitcoin price and network hashrate, August 2010 to January 2020

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 Internet Appendix. The initial inflationary reward was set to 50 bitcoins by Nakamoto and is programmed to decline by 50% every 210,000 blocks, or approximately 4 years.[18] We can view each period between halving

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

[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.

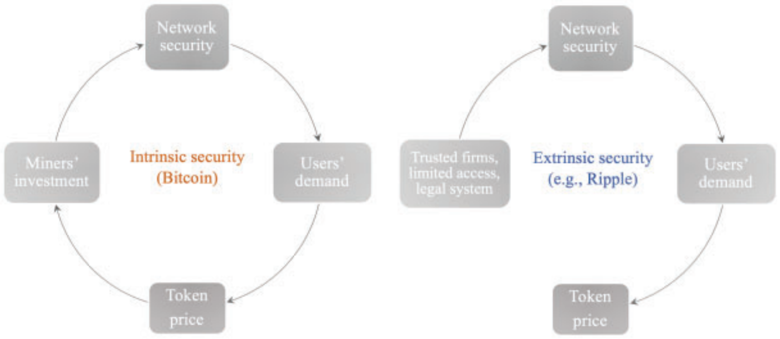

Network security
Miners' investment
Intrinsic security (Bitcoin)
Users' demand
Token price
Network security
Trusted firms, limited access, legal system
Extrinsic security (e.g., Ripple)
Users' demand
Token price

Figure 2
Intrinsic and extrinsic security models

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, Jurado, and Ledger, 2018; 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 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]

[19] The scope for sabotage attacks has arguably recently increased, 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.

[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

Like Budish, we argue for the importance of considering explicit sabotage attacks. 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.

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 is unitary. There is also an intrinsically useless and transferrable token, bitcoin, in supply B. Agent i can purchase any nonnegative amount B_{it} at a price p_t that is taken as given, thereby becoming a Bitcoin user. Agents acquire bitcoins because,

cryptocurrencies pose a national security risk (see Brambrough 2019). Policy makers 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., Aure 2020). The G-20 group has repeatedly warned against the money laundering and terrorist financing risks that cryptoassets 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., Goh 2019) are consistent with increasing the chances of a successful sabotage attack. Kaiser, Jurado, and Ledger (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 US$860,000/hr. While that rate is prohibitively high for most individuals interested in a double-spend attack, it is not without reach for economic superpowers, or even global financial corporations.

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, $c_{it} - l_{it} + \mathbb{E}_t(V(B_{it} p_t) + \delta c_{it+1})$, 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: $\max_{b_{it} \geq 0} S_t(f V(b_{it}) + (1-f)\delta b_{it} R) - b_{it}$.

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

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

excluding transactions based on user fees. Hence, we concentrate on equilibria in which fees are negligibly small.[23]

Because 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 $\max_{h_j \geq 0} \mathbb{P}(h_j, h_{-j}) \times \delta \psi \mathbb{E}_t^1 p_{t+1} - C(h_j)$, 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.

[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). 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 2 weeks (2,016 10-min 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 s. (see, e.g., https://etherchain.org/charts).

[25] Miners form rational expectations about price but act on the subjective probability of receiving the reward equal to one; in doing so, they display bounded rationality. Throughout the paper, we focus on how bitcoin users, not miners, price security risks. Relaxing this rationality constraint imposes no additional complexity here, since doing so 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.

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 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.

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 $A > 0$.[28] 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]

[26] To help with the interpretation, we can further disaggregate the mining cost equation as cost=electricity price (US$/kWh) * efficiency hardware (kWh/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, the 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 Internet Appendix.

[28] Alternatively, one could consider a connection between A and p. The resultant equilibrium connections would be similar provided miners are more sensitive to variations in the bitcoin price; that is, if $\frac{A}{H}$ decreases with p. 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, still would be present.

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

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

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

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: $\lim_{H\to+\infty}S=\lim_{A\downarrow 0}S=1$, $\lim_{H\downarrow A}S=0$, 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

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

We will 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 resultant valuation for bitcoins is low. The opposite is true when the value of

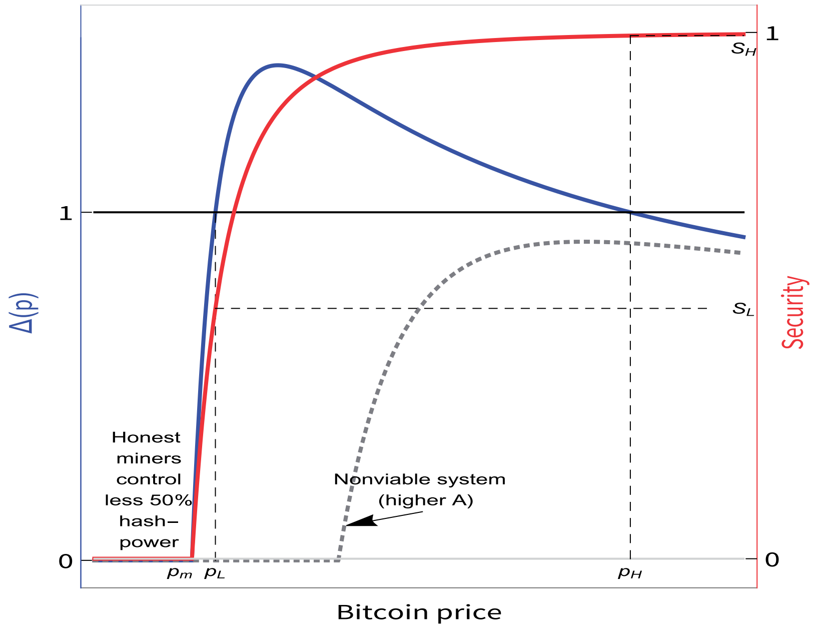


Figure 3
Equilibrium determination of bitcoin price and security

bitcoins is perceived to be high, making a high-value, high-security equilibrium self-fulfilling.

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 $A \rightarrow 0$, the bitcoin economy converges to that with $\overline{S} \rightarrow 1$, 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 represents 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 $c_t - l_t + u(q_t) + \delta c_{t+1}$, 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

[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 Internet Appendix. 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.

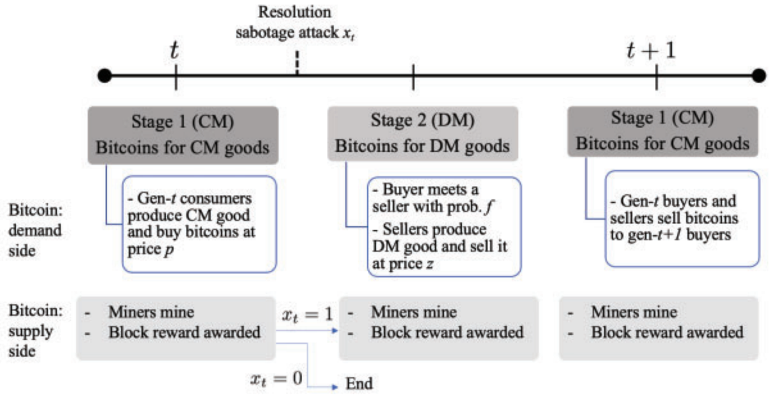


Figure 4
Timeline

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 $s > t$. 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

[31] Zhu (2008) extensively discusses how the choice of linear utility for the CM good consumption makes this combination of overlapping generation and search elements observationally equivalent to that of Lagos and Wright (2005), who present infinitely lived agents. Consistent 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.

born at time t maximizes intertemporal expected utility,

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

subject to the budget constraint $B_{it}p_t+c_{it}\le l_{it}$. Given that credit is not available, buyers in the DM are constrained by $z_tq_{it}^d\le B_{it}p_t$, 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

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

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 null or unbounded production.

Next, we characterize the demand for bitcoin holdings in a partial equilibrium, that is, taking $\{S_t\}_{t\ge0}$ as a given sequence.

Lemma 2. In any equilibrium, for all t, $\delta S_t\mathbb{E}_t^1\frac{p_{t+1}}{p_t}\le1$ and $p_t=\delta S_t\mathbb{E}_t^1p_{t+1}(1+f(u'(q(B_t^d)-1)^+)$. 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 $p_t=\delta S_t\mathbb{E}_t^1p_{t+1}(1+f(u'(\delta\frac{B_t}{n}\mathbb{E}_t^1p_{t+1})-1))$.

This lemma bounds the risk-adjusted expected holding returns that are compatible with a monetary equilibrium. When $\frac{\delta S_t\mathbb{E}_t^1p_{t+1}-p_t}{p_t}<0$, 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 $zq\le b$ 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 $\left\{B_{it},q_t^d,q_t^s,h_t,z_t,p_t\right\}_{t=0}^{\tau}$ 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 4-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

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

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

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

where $q(b_{t+1}) = \frac{\delta}{\rho}\frac{b_{t+1}}{n}$. The right-hand side of Equation (7) can be written as D, for which a stationary solution is a value b_{ss} such that $b_{ss} = D(b_{ss})$. Equivalently, b_{ss} must satisfy

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

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

[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 stabilizes.

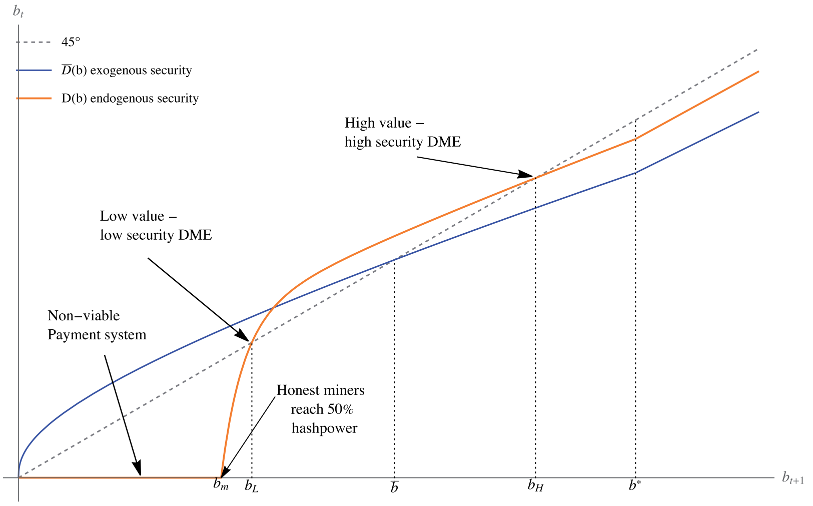


Figure 5
Decentralized monetary equilibria: Existence and multiplicity

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, $i_B(b) := \frac{\rho}{S(b,A)\delta} - 1$.[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 $u'(0) > \frac{1}{f}(\frac{\rho}{\delta \overline{S}} + f - 1)$.

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

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

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 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 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.

[37] Equivalently, one can consider the attackers' mining investment to offset any potential social benefits from a successful attack, such as regulation enforcement. The case with large positive attack externalities is less interesting, since the planner can always set ρ at a level 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.

[38] To see this, use $b_i = \frac{b}{n}$ to express (4) as a choice over q: $\max_{q\geq 0} Sf(u(q)-q) - q\left(\frac{\rho}{\delta} - S\right)$. Similarly, combine (6) and (9) to express the constrained planner's objective as $fS(u(q)-q) - \frac{m-1}{m}(\rho-1)q$. 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, $u'(q_{\text{cp}}) = 1 + \frac{1}{fS}\frac{m-1}{m}(\rho-1)$. Since $\frac{\rho}{\delta} - S > \frac{m-1}{m}(\rho-1) > 0$, 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 in which 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.

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 between all three.

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.

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

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

where b_H is the highest solution to (8), $S=S(b_H,A)$, and $\sigma(b_H)$ 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. As an

[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.

illustration, 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 $S\rightarrow 1$ leads to $\rho_V\rightarrow 1$: 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 $(\rho, p_H(\rho))$ is concave. The top panel 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.

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 nonmonotonic: the price can increase or decrease.[40]

In sum, 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.

[40] To evaluate different scenarios quantitatively, in Section C.3 of the Internet Appendix, we simulate events studies in which 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 at the perfectly competitive limit $m\rightarrow\infty$, while security is highest. To see this, note that, in any stationary DME, $\Pi=\left(\frac{\rho-1}{2}\right)\frac{\delta}{\rho}\frac{b_{ss}}{m}$.

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.

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

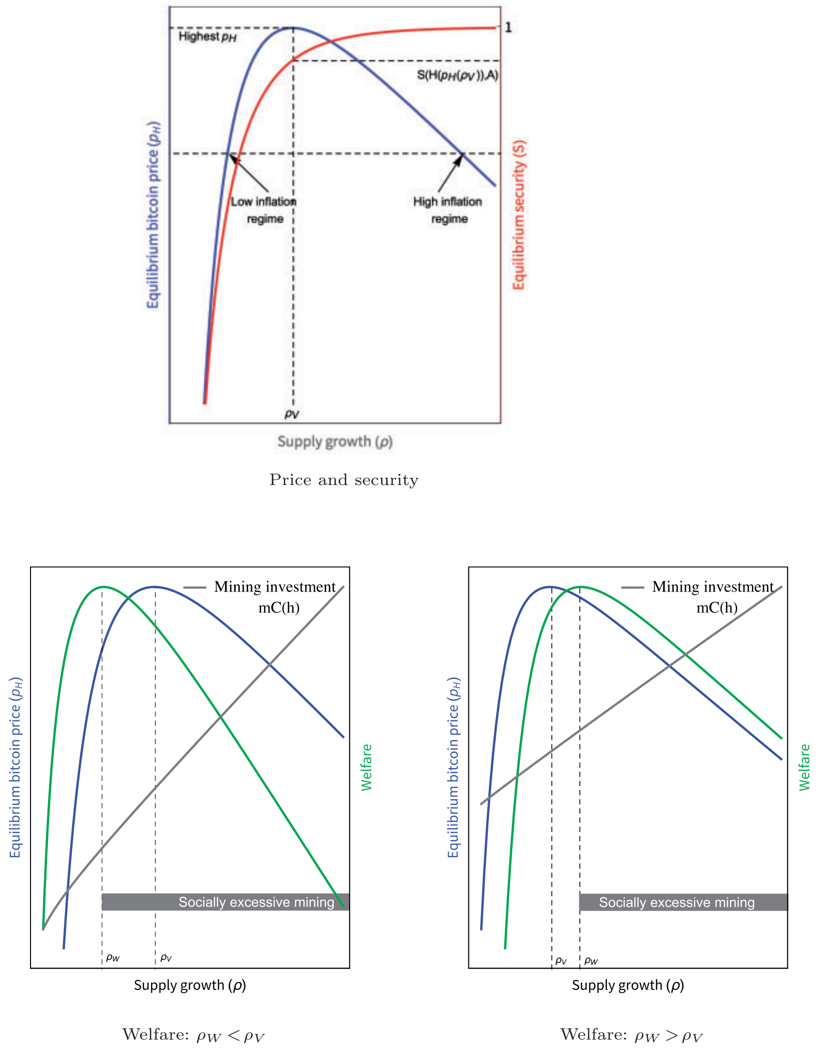
We are interested in this section in the optimal monetary policy from the perspective of a benevolent planner, denoted as ρ_W. We begin by considering the benchmark economy without mining investment and a given security level $\overline{S}$. In that case, the first-best DM surplus can be achieved by $\overline{\rho}_W = \overline{S}\delta < 1$.[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 2017, chap. 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

[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 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.



Price and security

Welfare: $\rho_W < \rho_V$

Welfare: $\rho_W > \rho_V$

Figure 6
Bitcoin supply growth: Relations with price, security, and welfare
The top- and bottom-left panels correspond to the utility function parameter $\sigma = 0.5$. The bottom-right panel corresponds to $\sigma = 1.5$. All other parameters are as in the baseline calibration in Section C of the Internet Appendix.

equal, the planner is involved with the amount invested in mining, not with buyers' inflation tax; a mere transfer from 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 bottom panels are otherwise identical but feature a low and a high σ value.[44] In the bottom-left 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 bottom-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.

[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.

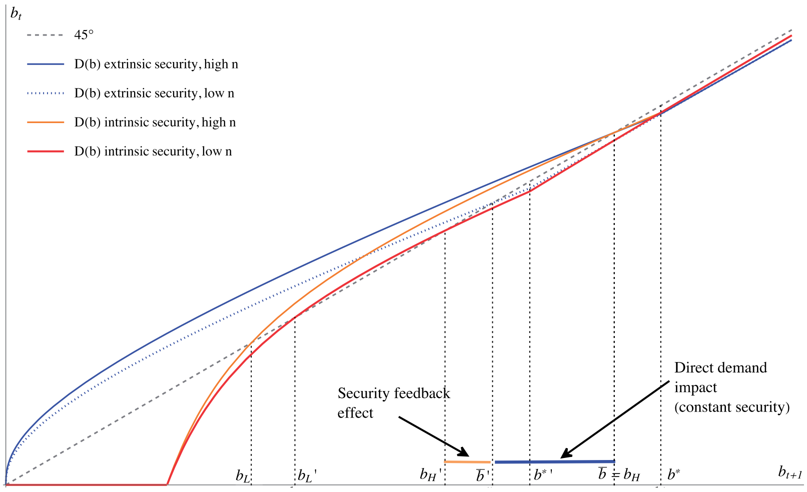


Figure 7
Price change amplification of an adverse change in the number of buyers

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: $b_H = \overline{b}$.

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: $\left|\frac{db_H}{dn}\right| > \left|\frac{d\overline{b}}{dn}\right|$.

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 $\overline{b}$, with security held constant, is given by $\left|\overline{b}' - \overline{b}\right|$. 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 traced graphically as $\left|b'_H - \overline{b}'\right|$. 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 equilibrium 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 Nonfundamental uncertainty, price booms, and crashes

We observe more frequent booms and busts in the bitcoin's price than that for most currencies. What makes them particularly puzzling is that they often occur without any apparent link to fundamentals (e.g., Bhambhwani, Delikouras, and Korniotis 2019). In this section, we analyze the potential role of nonfundamental 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

[45] We provide a quantitative perspective of this point in Section C.4 of the Internet Appendix. 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/US$ 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 US$951 to US$14,388), then decreased by 74% in 2018 (to US$3,743), and rose again by nearly 100% in 2019 (to US$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 Internet Appendix).

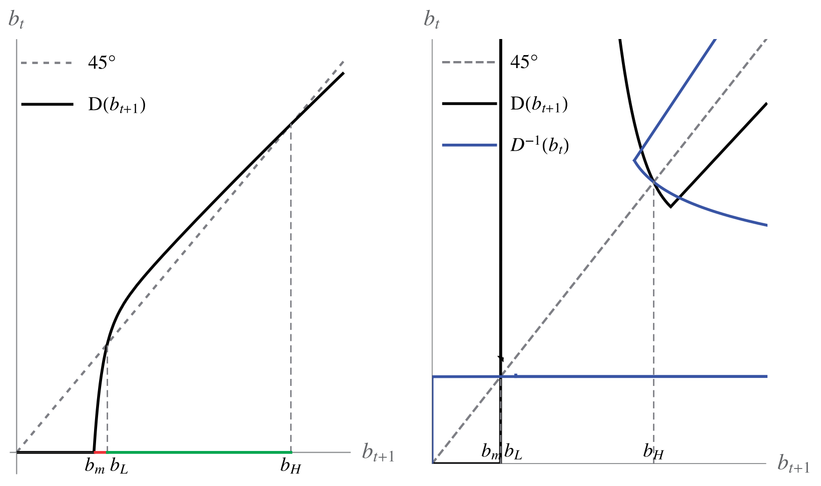


Figure 8
Sunspot equilibria
The left (right) panel corresponds to the utility parameter $\sigma=0.5$ ($\sigma=7$). All other parameters are as in the baseline calibration in Section C of the Internet Appendix.

in (1), but based on a valuation for balances given by $\mathbb{E}_\omega b = \phi_\omega b_\omega + (1-\phi_\omega) b_{\omega'}$, $\omega \neq \omega'$. 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:

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

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 that

Type I equilibria can exist *only* 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 Types I and II equilibria.

Since both types are viable for Bitcoin, we can say that, relative to other currencies, bitcoins are more prone to exhibiting 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 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 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

[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.

[48] Lester, Postlewaite, and Wright (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. Because of the transparency of the public Bitcoin ledger, one can argue that counterfeiting is not a primary concern for bitcoins.

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,

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

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

where $i_M := \frac{\gamma}{\delta} - 1$, $i_B(b) := \frac{\rho}{S(H(b),A)\delta} - 1$, $\lambda_\tau(\mu, b) := \left(u'(q_\tau(\mu, b)) - 1\right)^+$, 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]

In the remainder of this section, we focus on particular cases. First, we consider the case in which no seller accepts both fiat currency and bitcoins, $f_{MB} = 0$. For example, regular internet sellers like Amazon, who accept only fiat card payments, and dark web sellers like Silk Road, who 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 then is 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 $i_M - S i_B(b) = (f_M + (1 - S) f_{MB}) \lambda_M(\mu)$; for this equation to hold, we need $i_M > S i_B(b)$. 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

[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 $\lambda_M(\mu) = \lambda_{MB}(\mu, 0)$.

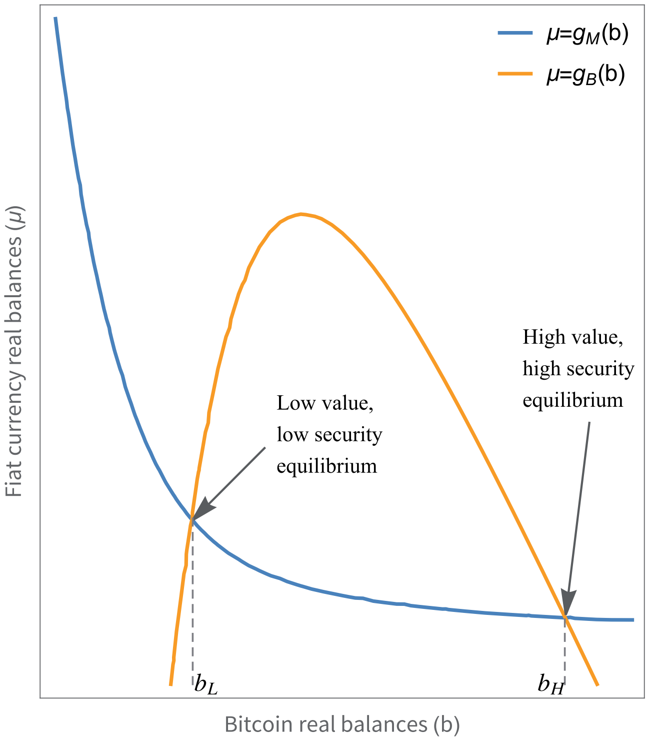


Figure 9
Stationary DMEs in a bimonetary economy
This figure graphs the set of equilibria in an economy in which bitcoins are inessential for commerce ($f_B = 0$) and the bitcoin supply growth is relatively low ($\rho < \gamma$).

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. If the central bank followed a deflationary or constant-supply policy, bitcoin demand would be naught.

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

[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 $i_M - S i_B(b) = (1-S) f \lambda_M(\mu)$, which yields a similar lower bound for γ and the possibility of multiple equilibria.

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 $\gamma>\rho+\delta(1-S(b_{ss},A))$.

7. Discussion

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

7.1 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 Internet Appendix 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. Bhambhwani, Delikouras, and Korniotis (2019) provide further empirical support. The authors 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]

7.2 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 Internet Appendix.

[51] While less tightly connected, a growing body of related evidence is being documented on risk-return relations for bitcoin and other cryptocurrencies (e.g., Bianchi and Dickerson 2018; Borri and Shakhnov 2018; Ghysels and Nguyen 2018).

[52] Bitcoin's perceived network security was compromised in a few well-known episodes, with immediate adverse valuation effects. These include the March 11, 2013, 6-hr fork that created a lack of consensus in the network and an instant 24% drop in price, though without malicious intent (for a discussion, see Buterin 2013).

7.3 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 no mechanism 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.

7.4 Nonfundamental volatility

We find that bitcoins' prices can fluctuate stochastically as nonfundamental 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, Delikouras, and Korniotis (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 do not feature irrational agents or upper bounds for the acceptability of bitcoins.

7.5 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. (2020) 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

[53] Nakamoto (2008) does not outline a precise monetary policy, but its software implementation outlines the design (see Section A.4 of the Internet Appendix). Other blockchains follow more flexible models. For example, Ethereum's monetary policy is subject to revisions that are discussed within that community of developers.

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

[55] In addition, Liu and Tsyvinski (2020) find that both momentum and public attention, proxied for 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.

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, the expectation of a relatively high f_B and bitcoin price values with repressive authorities seems reasonable.[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).

8. Concluding Remarks

We have presented a tractable decentralized monetary economy in which users' and miners' decisions affect each other, and the evolutions of bitcoin prices and security are jointly determined. The model outcomes demonstrate how ignorance of 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

[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 12 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). (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 as the second most-active country, scaled by the number of internet users and purchasing power (see Chainalysis Team 2020).

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 we observed heterogeneity in the level of impatience across agents, user-initiated fees could play an allocative role, as demonstrated by Easley, O'Hara, and Basu (2019) and Huberman, Leshno, and Moallemi (2019). The integration of a rich fee bidding game into a general equilibrium monetary framework is an exciting avenue of work.

Our focus on seigniorage-financed security also highlights challenges inherent in 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 ensures such a shift in revenue source. Second-layer networks, such as Lightning, can help mitigate scaling limitations, but their net impact of on-chain fees is still uncertain. Whether security can remain at high levels beyond 2140 is, therefore, an important open question.

A. 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 Internet Appendix. 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.

A.1 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 $\Delta'(p)\rightarrow\frac{\overline{B}}{n}fV''\left(\frac{\overline{B}}{n}p\right)<0$. 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 $\Delta'(\hat{p})=0$. □

A.2 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

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

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,

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

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 (A.1) 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

$$\mathcal{W}_{ss}/n = f S(H(q_{ss}), A)(u(q_{ss}) - q_{ss}) - \frac{m-1}{m}(\rho - 1) q_{ss}, \tag{A.2}$$

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 $\mathcal{W}_L$:

$$\underbrace{f S_H H_q(q_L)(u(q_L) - q_L)}_{\text{I}>0} + \underbrace{f S\big(u'(q_L) - 1\big)}_{\text{II}>0} - \underbrace{\frac{m-1}{m}(\rho - 1)}_{\text{III}>0}. \tag{A.3}$$

Expression I in (A.3) 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 $f\big(u'(q_L) - 1\big) = \frac{\rho}{\delta S(q_L, A)} - 1$. 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 $\mathcal{W}_H > \mathcal{W}_L$. □

A.3 Proof of Proposition 3

Let $y(b; \rho) := \frac{\delta S}{\rho}\left(f\big(u'(q(b, \rho)) - 1\big) + 1\right)$; 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 Internet Appendix 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,

$$y_\rho = \frac{\delta}{\rho^2}\{(\rho S_H H_\rho - S)(f\big(u'(q(b)) - 1\big) + 1) - S f q(b) u''(q(b))\}. \tag{A.4}$$

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 (A.4), we obtain

$$y_\rho = \frac{\delta}{\rho^2} S \left(\underbrace{\left(\frac{k(1-S)}{S(\rho-1)} - 1 \right)}_{\text{I}} \underbrace{\left(f\left(u'(q(b)) - 1\right) + 1\right)}_{\text{II}>0} + \underbrace{\left(-fq(b)u''(q(b))\right)}_{\text{III}>0} \right). \tag{A.5}$$

Expression II on the right-hand side of (A.5) 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 (A.5) being equal to zero, which requires that:

$$\left(1 - \frac{k(1-S)}{S(\rho-1)}\right)\left(f\left(u'(q(b)) - 1\right) + 1\right) = fu'(q(b))\sigma(b), \tag{A.6}$$

where $\sigma(b) := -q(b)\frac{u''(q(b))}{u'(q(b))}$. Combining expressions (A.6), $\text{II} = \frac{\rho}{\delta S} = i_B + 1$ 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 (A.6), 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 $b_H = p_H B$. □

A.4 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 (A.2) subject to buyers' optimality restriction from (8). Note that the planner's ρ choice affects $b(\rho)$ and $q(b,\rho)$. We obtain the marginal social benefit (MSB) of a change in ρ by total differentiation of the expected DM trade surplus:

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

$$S\frac{q}{\rho}\left(\epsilon_{S,\rho} f \left(\frac{u(q)}{q} - 1 \right) + f\left(u'(q) - 1\right)\left(\epsilon_{b,\rho} - 1\right) \right), \tag{A.7}$$

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:

$$MSC = \frac{q}{\rho}\frac{m-1}{m}\left((\rho - 1)\epsilon_{b,\rho} + 1\right). \tag{A.8}$$

Next, we evaluate whether $MSB \gtreqless MSC$ at $\rho = \rho_V$. Using $\epsilon_{b,\rho}(\rho_V) = 0$ in (A.7) and (A.8), it follows that $MSB < MSC$ if:

$$S\left(\epsilon_{S,\rho} f \left(\frac{u(q)}{q} - 1 \right) - f\left(u'(q) - 1\right) \right) < \frac{m-1}{m}. \tag{A.9}$$

Substituting $i_B = f\left(u'(q) - 1\right)$ from (8) in (A.9), we obtain the inequality in (iii). If (A.9) holds, social welfare is enhanced by setting ρ_W below ρ_V. If the inequality in (A.9) is reversed, $MSB > MSC$; thus, it is socially optimal to set $\rho_W > \rho_V$. □

A.5 Proof of Proposition 6

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

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

Multiply both sides by b_H and rearrange to get

$$\left\{\frac{\delta}{\rho}S_H H\big(f\big(u'(q(b_H))-1\big)+1\big)+\frac{\delta}{\rho}Sfu''(q(b_H))q(b_H)\right\}db_H=\left\{Sfu''(q(b_H))q(b_H)^2\right\}dn. \tag{A.10}$$

Analogously, for the token with extrinsic security, we get

$$\left\{\frac{\delta}{\rho}\overline{S}fu''\big(q\big(\overline{b}\big)\big)q\big(\overline{b}\big)\right\}d\overline{b}=\left\{\overline{S}fu''\big(q\big(\overline{b}\big)\big)q\big(\overline{b}\big)^2\right\}dn. \tag{A.11}$$

Given $b_H=\overline{b}$, the right-hand sides of Equations (A.10) and (A.11) coincide. Therefore, we must have

$$\underbrace{\left\{\frac{\delta}{\rho}S_H H\big(f\big(u'(q(b_H))-1\big)+1\big)+\frac{\delta}{\rho}Sfu''(q(b_H))q(b_H)\right\}}_{y_b(b_H)}db_H=\underbrace{\left\{\frac{\delta}{\rho}\overline{S}fu''\big(q\big(\overline{b}\big)\big)q\big(\overline{b}\big)\right\}}_{\overline{y}_b(\overline{b})}d\overline{b}. \tag{A.12}$$

The first bracketed term on the left-hand size of (A.12) is positive at a DME, while the second is negative. From Lemma E1 in the Internet Appendix, we know that the sum must be negative: $y_b(b_H)=\left(\frac{D'(b_H)-1}{b_H}\right)<0$. Therefore, $|y_b(b_H)|<\left|\overline{y}_b(\overline{b})\right|$, implying that $|db_H|>\left|d\overline{b}\right|$. □

A.6 Proof of Proposition 7

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

$$\phi_1=\frac{\frac{D(b_2)}{S(b_2)}-\frac{b_1}{S_1}}{\frac{D(b_2)}{S(b_2)}-\frac{D(b_1)}{S(b_1)}},\ \phi_2=\frac{\frac{b_2}{S_2}-\frac{D(b_1)}{S(b_1)}}{\frac{D(b_2)}{S(b_2,A)}-\frac{D(b_1)}{S(b_1)}}. \tag{A.13}$$

Sunspot equilibria can exist under two types of conditions. For Type I, the denominator in (A.13) 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 $S_1>S(b_1)$, 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 $S_2<S(b_2)$, 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 (A.13) 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. □

A.7 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). □

References

Abadi, J., and M. Brunnermeier. 2018. Blockchain economics. Working Paper, Princeton University.

Alsabah, H., and A. Capponi. 2019. Pitfalls of bitcoin's proof-of-work: R&D arms race and mining centralization. Working Paper, Columbia University.

Antonopoulos, A. M. 2017. *Mastering Bitcoin: Programming the open blockchain*. Sebastopol, CA: O'Reilly.

Asriyan, V., W. Fuchs, and B. Green. 2019. Liquidity sentiments. *American Economic Review* 109:3813–48.

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia. 2016. Bitcoin pricing, adoption, and usage: Theory and evidence. Working Paper, Stanford Graduate School of Business.

Aure, F. 2020. Bitcoin price soars as Jerome Powell confirms crypto's threat to U.S. dollar. CCN.com, October 4. https://www.ccn.com/bitcoin-price-soars-jerome-powell-confirms-cryptos-threat-to-dollar

Azariadis, C. 1981. Self-fulfilling prophecies. *Journal of Economic Theory* 25:380–96.

Benetton, M., G. Compiani, and A. Morse. 2019. CryptoMining: Local evidence from China and the US. Working Paper, University of California, Berkeley.

Bhambhwani, S., S. Delikouras, and G. M. Korniotis. 2019. Do fundamentals drive cryptocurrency prices? Working Paper, HKUST.

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The blockchain folk theorem. *Review of Financial Studies* 32:1662–715.

Biais, B., C. Bisière, M. Bouvard, C. Casamatta, and A. Menkveld. 2020. Equilibrium bitcoin pricing. Working Paper, HEC Paris.

Bianchi, D., and A. Dickerson. 2018. Trading volume in cryptocurrency markets. Working Paper, Queen Mary University of London.

Borri, N. and K. Shakhnov. 2018. The cross-section of cryptocurrency returns. Working Paper, LUISS University.

Brambrough, B. 2019. Bitcoin and crypto suddenly branded a 'national security issue.' *Forbes*, July 16. https://www.forbes.com/sites/billybambrough/2019/07/16/bitcoin-and-crypto-suddenly-branded-a-national-security-issue/?sh=627b95651a59

Budish, E. B. 2018. The economic limits of bitcoin and the blockchain. Working Paper, University of Chicago.

Buterin, V. 2013. Bitcoin network shaken by blockchain fork. *Bitcoin Magazine*, March 13. https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448

Cass, D., and K. Shell. 1983. Do sunspots matter? *Journal of Political Economy* 91:193–227.

Chainalysis Team. 2020. Hyperinflation and sanctions evasion: What on-chain data tells us about Venezuelans' trust in cryptocurrency. *Chainalysis Blog*, August 27. https://blog.chainalysis.com/reports/venezuela-cryptocurrency-market-2020

Chiu, J., and T. V. Koeppl. 2019. The economics of cryptocurrencies bitcoin and beyond. Working Paper.

Choi, M., and G. Rocheteau. 2019. Money mining and price dynamics. Working Paper, Bank of Canada.

Cong, L. W., Z. He, and J. Li. 2018. Decentralized mining in centralized pools. Working Paper, University of Chicago.

Cong, L. W., Y. Li, and N. Wang. 2018. Tokenomics: Dynamic adoption and valuation. Working Paper, University of Chicago.

———. 2019. Token-based platform finance. Working Paper, University of Chicago.

Conti, M., K. E. Sandeep, C. Lal, and S. Ruj. 2018. A survey on security and privacy issues of bitcoin. *IEEE Communications Surveys and Tutorials* 20:3416–52.

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

Feller, W. 1968. *An Introduction to probability theory and its applications*, third ed. Hoboken, NJ: Wiley.

Fernandez-Villaverde, J., and D. R. Sanches. 2019. Can currency competition work? *Journal of Monetary Economics* 106:1–15.

Foley, S., J. R. Karlsen, and T. J. Putnins. 2019. Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? *Review of Financial Studies* 32:1798–853.

Ghysels, E., and G. Nguyen. 2018. Price discovery of a speculative asset: Evidence from a bitcoin exchange. Working Paper, UNC.

Goh, B., and A. John. 2019. China wants to ban bitcoin mining. Reuters, April 9. https://www.reuters.com/article/us-china-cryptocurrency/china-wants-to-ban-bitcoin-mining-idUSKCN1RL0C4

Goldstein, I., E. Ozdenoren, and K. Yuan. 2011. Learning and complementarities in speculative attacks. *Review of Economic Studies* 78:263–92.

Gu, C., G. Menzio, R. Wright, and Y. Zhu. 2019. Toxic assets and market freezes. Working Paper, University of Missouri.

Harvey, C. R. 2016. Cryptofinance. Working Paper, Duke University.

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, New York University.

Huberman, G., J. D. Leshno, and C. Moallemi. 2019. An economic analysis of the bitcoin payment system. Working Paper, Columbia Business School.

Kaiser, B., M. Jurado, and A. Ledger. 2018. The looming threat of China: An analysis of Chinese influence on bitcoin. Working Paper, Princeton University.

Kang, K.-Y. 2020. Cryptocurrency and double spending history: Transactions with zero confirmation. Working Paper, Yonsei University.

Kareken, J., and N. Wallace. 1981. On the indeterminancy of equilibrium exchange rates. *Quarterly Journal of Economics* 96:207–22.

Lagos, R., G. Rocheteau, and R. Wright. 2017. Liquidity: A new monetarist perspective. *Journal of Economic Literature* 55:371–440.

Lagos, R., and R. Wright. 2003. Dynamics, cycles, and sunspot equilibria in genuinely dynamic, fundamentally disaggregative models of money. *Journal of Economic Theory* 109:156–71.

———. 2005. A unified framework for monetary theory and policy analysis. *Journal of Political Economy* 113:463–84.

Lamport, L., R. Shostak, and M. Pease. 1982. The byzantine generals problem. ACM Transactions on Programming Languages and Systems 4:382–401.

Lehar, A., and C. A. Parlour. 2019. Miner collusion and the bitcoin protocol. Working Paper, University of Calgary.

Lester, B., A. Postlewaite, and R. Wright. 2012. Information, liquidity, asset prices, and monetary policy. *Review of Economic Studies* 79:1209–38.

Li, J., and W. Mann. 2020. Digital tokens and platform building. Working Paper, George Mason University.

Liu, Y., and A. Tsyvinski. 2020. Risks and returns of cryptocurrency. *Review of Financial Studies*. Advance Access published September 26, 2020, 10.1093/rfs/hhaa113.

Liu, Z., N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-c. Liang, and D. I. Kim. 2019. A survey on blockchain: A game theoretical perspective. *IEEE Access* 7:47615–43.

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. Working Paper, University of Toronto.

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* 40:1037–1047.

Pease, M., R. Shostak, and L. Lamport. 1980. Reaching agreement in the presence of faults. *Journal of the ACM* 27:228–34.

Raskin, M., and D. Yermack. 2016. Digital currencies, decentralized ledgers, and the future of central banking. Working Paper, New York University.

Rocheteau, G., and E. Nosal. 2017. *Money, payments, and liquidity*. Cambridge: MIT Press.

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

Rosenfeld, M. 2014. Analysis of hashrate-based double spending. arXiv, preprint, https://arxiv.org/abs/1402.2009.

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. Working Paper, UT Austin.

Yermack, D. 2015. Is bitcoin a real currency? An economic appraisal. In *Handbook of digital currency: Bitcoin, innovation, financial instruments, and big data*, 31–43. Amsterdam, the Netherlands: Elsevier.

Yermack, D. 2017. Corporate governance and blockchains. *Review of Finance* 21:7–31.

Yu, Y., and J. Zhang. 2020. Flight to bitcoin. Working Paper, Singapore Management University.

Zamfir, V. 2015. Introducing Casper “the Friendly Ghost." *Ethereum Blog*, August 1. https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/.

Zhu, T. 2008. An overlapping-generations model with search. *Journal of Economic Theory* 142:318–31.

Zimmerman, P. 2019. Blockchain structure and cryptocurrency prices. Working Paper, Bank of England.