UNIL | Université de Lausanne
Département de finance

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

FINANCE RESEARCH SEMINAR
SUPPORTED BY UNIGESTION

Bitcoin as Decentralized Money: Prices, Mining, and Network Security

Emiliano S. PAGNOTTA,
Imperial College, London

Friday, May 17, 2019, 10:30-12:00
Room 126, Extranef building at the University of Lausanne

UNIGESTION

Bitcoin as Decentralized Money: Prices, Mining, and Network Security

Emiliano S. Pagnotta[*†]

Abstract

We address the determination and evolution of bitcoin prices in a simple monetary economy that captures the salient features of a decentralized network. Network users forecast the transactional and resale value of bitcoin holdings and consider the risk of a network attack. Miners contribute resources that enhance network security and compete for mining rewards received in units of the same unbacked token. In equilibrium, the overall production of network security and the bitcoin price are jointly determined. We characterize how the network technologies and participants, users and miners, affect the number and dynamic stability properties of equilibria. We find that the relation between bitcoin prices and the supply growth rate is not monotonic: the same price is consistent with different rates. The model's outcomes demonstrate how intrinsic price–security feedback effects can amplify or moderate the price volatility effect of demand shocks. We find rational patterns of price momentum, and that small and large stochastic bubbles can exist in general equilibrium and show how the probability of bursting decreases with the bitcoin price. JEL Codes: E40; E42; G12; G15; G18

First draft: July 12, 2018. *Current draft*: December 12, 2018

[*]Imperial College London. Email: epagnott@ic.ac.uk.

[†]This paper builds on previous work in "Pricing Satoshis" presented at the 2018 Finance Theory Group London meeting, the 2018 NBER Asset Pricing Summer Institute, the Einaudi Institute for Economics and Finance and Imperial College London. For helpful conversations and comments I thank Franklin Allen, Fernando Alvarez, Andrea Buraschi, Jonathan Chiu, Will Cong, Jason Donaldson, Maryam Farboodi, Harrison Hong, Marcin Kacperczyk, Andrei Kirilenko, Francesco Lippi, Hanno Lustig, Alex Michaelides, David Miles, Monika Piazzesi, Jose Scheinkman, Michael Sockin, Savi Sundaresan, Nick Szabo, and Stijn Van Nieurburgh and participants at the 2019 American Economic Association meetings, the 2019 American Financial Association Meetings, and the Bloomberg Crypto Summit. The usual disclaimers apply.

The rapid growth of Bitcoin has sparked heated debates. The issue of bitcoin[1] price determination and price volatility is particularly elusive. On the one hand, in investment and entrepreneurial circles, it is often argued that the price reflects fundamental factors such as the growth in the number of network participants and the quality of the underpinning technology. A prominent view in the academic and policy communities, on the other hand, is that bitcoins are just a bubble that will eventually burst and, therefore, bitcoin prices are meaningless. Reaching a consensus on these issues is challenged by the fact that traditional monetary and asset pricing models were not designed around a decentralized network (DN), such as Bitcoin, but a centralized network (CN) run by an institution such as a central bank, government, or a corporation.[2]

What is different about Bitcoin? Any financial network needs to be secured. Digital transfers of ownership, in particular, require some form of verification and it should be difficult for a malicious attacker to manipulate the recorded history. In a CN, a specific trusted node assumes such operational responsibility and, in exchange, charges users with fees. In the Bitcoin DN, verification and updates to the system ledger (blockchain) are not delegated to a single node but, rather, to a set of *miners*. Miners validate new blocks of bitcoin transfers every 10 minutes, on average, and add them to the system ledger. Which miner adds the new block is the result of a non-cooperative competitive process where each miner uses computer power, measured as the *hash rate*, to solve a mathematical problem based on a cryptographic algorithm. The reward to the winning miner consists of newly minted bitcoins and is awarded provided the winning miner respected a set of consensus rules that prevents frauds; otherwise, the investment in computer power is entirely lost.[3]

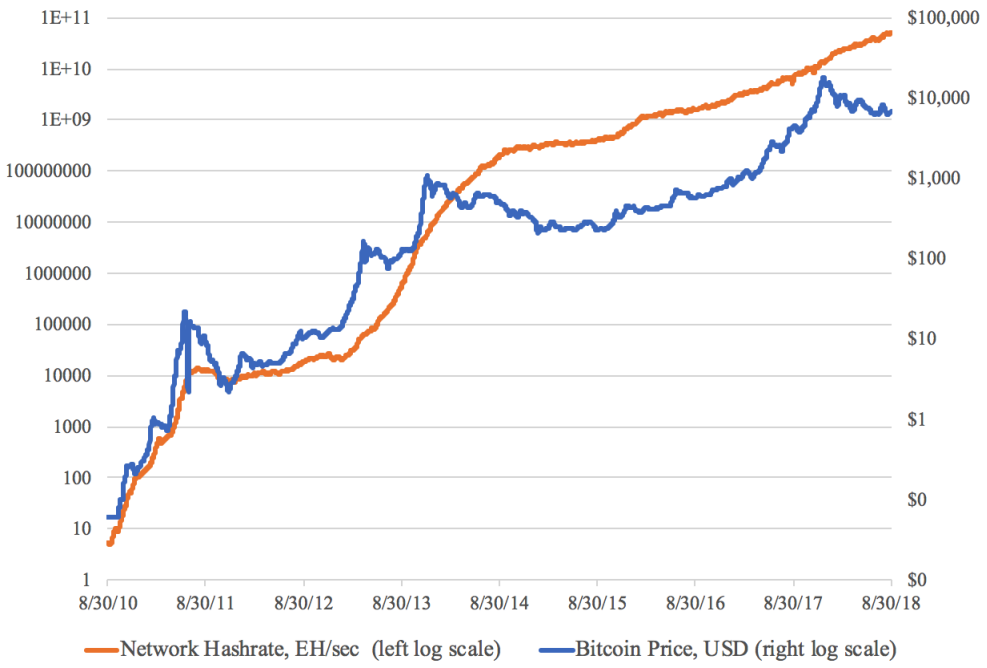
This system of incentives is a breakthrough innovation by Nakamoto (2008) and has the property that, for a given level of miner decentralization, network security is increasing in the amount of total computer power in the network, the system hash rate. Figure 1 shows that, since its inception,

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

[2] Excellent up-to-date surveys of traditional monetary models are provided by Rocheteau and Nosal (2017) and Walsh (2017).

[3] 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* (PoW). See Antonopoulos (2017) for an excellent summary of the consensus rules. The reward to the winning miner is the first transfer in each block (the Coinbase transaction) and consists, as of 2018, of 12.5 bitcoins and fees that users making transfers in that block pay to the winning miner.

Figure 1. Bitcoin Price and Network Hash Rate: August 2010 to August 2018 (source: smartbit.com.au)



Bitcoin has experienced a remarkable increase in *both* the price of the token and the network hash rate. Intuitively, higher prices should provide stronger incentives for miners and increase the provision of computing resources. In turn, a more secure network should reduce users' uncertainty about attacks and fraud, increasing the demand for the DN token and its price. How are prices and network security related in general? What does such intrinsic economic link imply for bitcoin prices and volatility?

In this paper, we develop a framework where the supply and demand for the services of a DN can be jointly analyzed. On the demand side, overlapping generations of consumers hold bitcoins for their transactional services and speculative value. As in the case of communication networks, the value of the services can increase with the network size. Because the network is decentralized, consumers perceive transfers in the network to be resistant to censorship risk (see Section 1.1). However, they internalize the possibility of large-scale attacks, to which they are risk averse, that could compromise *both* the usefulness of transactional network services and the market value of the token. The network is secured against attacks by an oligopoly of noncooperating miners who

contribute computational resources that enhance network security and compete for mining rewards that are received in units of the same token used by consumers. The token then simultaneously serves an *exchange* function for consumers and an *incentive* function for miners, a property that we label as *unity* (Definition 1).

To develop intuition about consumers' demand, and to provide a natural benchmark to bitcoins, we begin analyzing a partial equilibrium setting. In particular, we consider a token that violates unity because the security of its network is insensitive to the token price.[4] We find that consumers' demand increases with the exogenous level of network security, the expected holding period return, and the strength of network effects, and decreases with censorship risk aversion. Under fairly general conditions, a single stationary equilibrium with a positive and constant network market capitalization exists and is dynamically unstable, implying that only one price path is consistent with that equilibrium (Proposition 1). The properties of this economy are intuitive and, abstracting from network aspects, similar to those of other monetary environments (see Section 2.4).

For Bitcoin, however, network security is endogenous and depends on miners investment. We follow Pagnotta and Buraschi (2018) and model the strategic game among miners as an oligopolistic game in computing capacity so that, in each period, the probability of earning the mining reward is proportional to that investment. The resulting system hash rate is a function that increases with the number of miners and with the value of the mining reward and decreases with mining costs (Proposition 2). The equilibrium price and hash rate are the simultaneous solution to three conditions: (i) agents optimally choose their holdings to maximize the intertemporal utility, (ii) miners optimally supply resources in exchange for network assets, and (iii) the asset market clears. The decentralized character of the network manifests in the economics of (ii). The unity property of bitcoin prices creates a structural link between (i) and (ii).

In the absence of mining subsidies, a price equal to zero is always an equilibrium. If the price of bitcoin were zero, miners would not provide any resources to the network, its security would be zero, and consumers would not pay a positive price for bitcoins. However, we identify conditions

[4] In Section 1.2, we argue that such a token better resembles Ripple's XRP and Ethereum's ERC-20 tokens. For example, in contrast to Bitcoin, the price of XRP does not determine the level of security in the Ripple network.

for preferences and technologies under which a stationary equilibrium with a positive valuation for bitcoins exists. When this stationary equilibrium is unique, so is the leading price path. Multiple equilibria are common, though, especially when the cost elasticity of network supply is relatively high. For example, with linear mining costs and general network technologies, two positive stationary equilibria emerge. The low-valuation one is dynamically stable and the high-valuation one is dynamically unstable. Therefore, in a general equilibrium economy, the specifics of supply-side technology help to rationalize a broader range of equilibria and price dynamics (Propositions 3 and 4). Multiple equilibria also occur in traditional models of network products (e.g., Easley and Kleimberg (2010)) due to participation externalities, and in monetary overlapping generations models, especially when income effects are strong (e.g., Blanchard and Fisher, 1989). In this paper, however, multiplicity is due to a new channel: price–security feedback effects.[5]

The unity property has important positive implications. We analyze first the effects of changes in the strength of mining competition. Even when all miners are honest, network decentralization impacts the bitcoin price. When the number of miners increases, competition to win the PoW race increases the total amount of hash rate and, thus, the network security level, benefitting users. In equilibrium, the bitcoin price increases (Proposition 5). Perhaps surprisingly, although miners compete in capacity, as in Cournot (1897), the bitcoin price is increasing in total capacity, a "reversed Cournot" outcome. However, the oligopolistic miner competition designed by Nakamoto (2008) is structurally different from Cournot's: miners do not compete in bitcoin units but, rather, in hash rate units, that is, units of network security. We characterize competitive limits representing near-perfect security that provide upper bounds on the market capitalization of the network.

The second implication of unity regards the relation between the creation of new bitcoins and the market price. Arguably, one of the breakthrough features in the system described by Nakamoto (2008) is preventing any network participant, a user or a miner, from directly or indirectly controlling the nominal supply. Such a design is obviously in sharp contrast with any traditional fiat money system, where supply can be politically controlled. It is also in contrast to a metallic monetary

[5] Additionally, unlike the literature on networks, service or product quality in Bitcoin is not determined by a firm but, rather, by an oligopoly of price-taking miners.

system, where, for instance, gold miners can influence the supply by investing more resources into mining. Therefore, monetary policy analysis in the traditional sense of regulating money supply is not possible. However, we investigate the effects of changes in the nominal growth rate of bitcoins, ρ, as a feature of the network protocol. Intuitively, we can distinguish three effects of increases in ρ. First, a contemporaneous supply channel that negatively affects the within-period market clearing price. Second, in a stationary equilibrium with constant real balances, increasing ρ leads to lower expectations on resale prices, lowering the equilibrium price today. Third, a security channel. Miners' compensation is driven by the inflationary reward and, ceteris paribus, a higher mining reward incentivizes miners to invest more resources that secure the network, increasing the network valuation.

The security channel is new to the Bitcoin economy and acts in opposition to the supply and expectation channels. Thus, in contrast to a traditional monetary system, where increasing the nominal growth of money leads to a lower price of money as measured in goods, the relation between ρ and prices is not monotonic for Bitcoin. Under fairly general conditions, we show that an optimal level of ρ exists in the sense of maximizing the network's market capitalization (Proposition 6). Except when the system operates at this optimum, the same equilibrium price is consistent with low– and high–nominal growth regimes. Therefore, contrary to conventional wisdom, one could reduce nominal inflation in a non-negligible manner, as it happens for Bitcoin every four years when the nominal mining reward halves, without a substantial price change.[6]

Third, we show that the price impact of fundamental demand shocks on stationary equilibrium prices is amplified by network security feedback effects (Proposition 7). Everything else being constant, an increase in the network size raises the bitcoin valuation for any given security level. As valuation increases, miners react to better incentives by increasing investment, thus rendering the network more secure and further increasing the upward price movement. This process continues until a new fixed point relating the price and the system hash rate is reached. The analysis of the system steady state also allows us to characterize the network size elasticity of the price in

[6]The mining reward in Bitcoin is programmed to decline by 50% every 210,000 blocks. The first reward halving occurred on November 11, 2012. The second halving occurred on July 9, 2016. The next halving is estimated to take place in May of 2020. See, for example, https://en.bitcoin.it/wiki/Controlled_supply.

closed form. We show that such elasticity decreases with consumers risk aversion and show how it is affected by the mining process. In general, Bitcoin prices do not follow well-known network laws such as Metcalfe's law (Proposition 8).[7]

Fourth, we explore the dynamic process of price adjustment and volatility *outside* of stationary equilibria. For that, we consider in Section 8 an extension with stochastic network growth, and we contrast price dynamics in economies with agents displaying rational and myopic expectations. Myopic agents do not incorporate innovations in network size to beliefs on future prices as they expect constant holding returns. In this case, the sign of price changes in each period is the same as the sign of the contemporaneous change to network size. Thus, observable price movements are a sufficient statistic for the evolution of user adoption. Moreover, relative to a counterfactual token with exogenously given network security, the unity property also exacerbate the out-of-steady-state price volatility of bitcoins. The impact of price–security feedback effects on volatility is, therefore, similar in and out of the steady state.

The behavior of an economy with rational expectation, however, is remarkably different. First, we find that the same network processes induce in this case endogenous price patterns displaying price *momentum*[8] and reversals, such as rational boom-crash cycles that resemble those in Figure 1. For example, starting from a stationary equilibrium, a positive user adoption shock increases the same-period utility of the network services. Rational agents then require lower holding returns for the same tokens and expected prices decline. In equilibrium, those expectations are fulfilled, initiating a process of falling prices. Once this process is in motion, it can continue even when subsequent adoption shocks are negative, depending on the size of the realized shocks. Therefore, the empirical relation between network size and same-period price changes breaks.

Interestingly, with rational expectations, the network security feedback effect embedded in the unity property have the opposite impact on volatility, that is, it *moderates* bitcoin price fluctuations relative to the counterfactual token with exogenous security. Intuitively, following the considered positive shock to adoption with a negative effect on expected prices, miners decrease investment

[7]For a formal application of Metcalfe-like network laws to Bitcoin, see Wheatley, Sornette, Huber, Reppen, and Gantner, 2018

[8]See, for example, Asness, Moskowitz, and Pedersen (2013).

and hash rate declines. Consequently, consumers anticipate a more modest increase in transactional services value on a risk-adjusted basis. The model, therefore, suggests that the relative volatility responses of tokens satisfying and violating unity (e.g., bitcoin and XRP) can be informative about agent's expectation formation. In the interest of space, we delay further discussion of the empirical implications on price dynamics until Section 10.

Fifth, in Section 9, we study a version of the model where stationary equilibria are found even when the network provides *no useful service*. This particular case resembles the stochastic bubble economy studied by Weil (1987). However, a key difference is that, in our framework, *the probability of bubble bursting depends on the price*, a consequence of unity. This fact leads to new equilibria with distinct dynamic properties. In particular, we find that two equilibria with low– and large–value bubbles can emerge. Therefore, one can rationalize paths with prolonged bubble deflation which do not require the bubble to burst.

Related Literature. The paper closest to ours is that of Pagnotta and Buraschi (2018), who, to the best of our knowledge, provide the first equilibrium analysis where bitcoin prices affect miners and consumers simultaneously. We follow that paper's characterization of the unity property and miner competition there and extend the demand and equilibrium analyses to a *dynamic* monetary setting, allowing us to explore intertemporal allocations, the evolution of prices with speculation, the stability of stationary equilibria, and implications for price volatility. To develop a general equilibrium analysis, we seek not to provide a new microfoundation for the use of money but to capture two critical dimensions of the demand for a bitcoin-like token: the ability to conduct exchanges that are resistant to censorship and speculation, that is, purchase and resale. Our demand specification then combines features found in well-known monetary settings with a simple but, to the best of our knowledge, novel characterization of censorship risk using a stochastic number of network connections. Importantly, because of the unity property, the probability distribution of the number of connections explicitly depends on the bitcoin price.

To allow agents to hold bitcoins for speculative reasons, our approach considers intergenerational agent heterogeneity, as is common in overlapping generation monetary models à la Samuelson.[9]

[9]The approach that treats money as an asset that transfer resources intertemporally originates in the seminal

Additionally, this approach facilitates the analysis of price dynamics with changing network size, as in Section 8. Agents can also benefit from network transactional services, which are proportional to the real value of bitcoins and can display network effects (e.g., Katz and Shapiro (1985)). The connection between real monetary balances and the value of transaction services are common to a broad family of monetary models (e.g., Friedman (1969); Walsh (2017, Ch. 2) and the references cited therein). Despite well-known limitations in the welfare evaluation of policy interventions, which is not focus of this paper, we see it as a convenient starting point to address the interaction between consumers and miners in a dynamic setting and it allows us to derive closed-form expressions for equilibrium prices.[10] The analysis in Section 9 highlights that the existence of equilibria in which bitcoins are valued does not rely on the specifics of transactional services.

The proliferation of cryptocurrencies has fostered renewed interest in the economics of privately issued monies. Fernández-Villaverde and Sanches (2016) model competition among private currencies issues by extending the canonical environment in Lagos and Wright (2005) to include profit-maximizing entrepreneurs that can issue monies. Schilling and Uhlig (2018) study a bimonetary economy in the spirit of Bewley's model with a publicly and a privately issued currency. These papers provide valuable insights to understand consumers' choice between monies, exchange rates, and the policy responses of central banks. We do not model this type of competition but focus instead on the interactions between the demand side and the process of creation of new bitcoins. Unlike other private currencies, bitcoins are not issued by entrepreneurs: they are generated through the mining process. We therefore model supply-side profit maximization as a strategic PoW game in units of computer power instead of units of currency. Cong, Li, and Wang (2018) offer a token valuation model that endogenizes adoption and generates feedback effects between adoption and valuation. Sockin and Xiong (2018) study an economy in which tokens serve as a membership certificate that enables households to match and facilitates transactions. Their focus is understanding the role of token prices as an aggregator of users' dispersed information on platform fundamen-

work of Samuelson (1958) and have been extended my many others (e.g., Tirole (1985); Sims (2013); Ljungqvist and Sargent (2018, Ch. 9) and the references cited therein).

[10]The search-based microfoundation of these transaction services were first given by Kiyotaki and Wright (1989) and extended by many others (e.g., Lagos, Rocheteau, and Wright (2017)). An alternative approach to exchange frictions is given by Alvarez and Lippi (2009) who study technical innovation in a stochastic cash inventory model.

tals. Our work complements these papers, since we focus on a different but not mutually exclusive economic mechanism that generates feedback effects between prices and the resistance to attacks.

There is a growing empirical literature on bitcoin and other public blockchains. Athey, Parashkevov, Sarukkai, and Xia (2016) exploit a frictional exchange rate model to obtain some of the earliest evidence of bitcoin adoption and usage. More recently, empirical evidence on bitcoin price formation, risk-return relations, and arbitrage is obtained, among others, by Choi, Lehar, and Stauffer (2018), Ghysels and Nguyen (2018), Liu and Tsyvinski (2018), and Makarov and Schoar (2018); Foley, Karlsen, and Putnins (2018) study consumption of illegal goods. The results in this paper can inform future empirical studies that seek to connect demand and mining fundamentals to price formation.

A related stream of the literature studies the economics of protocols that allow participants to agree on a common output that aggregates private inputs when some "dishonest" participants might "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. Biais, Bisière, Bouvard, and Casamatta (2018) formalize the coordination game among miners within the PoW and discuss the conditions under which public blockchains can be expected to generate a stable consensus. Abadi and Brunnermeier (2018) provide the first formal model of the trade-offs involved between private and public blockchains and analyze competition among them. Saleh (2018) studies proof-of-stake protocols. Studies of the supply side of mining include those of Easley, O'Hara, and Basu (2018) and Huberman, Leshno, and Moallemi (2017), who analyze additional aspects such as Bitcoin mining fees; Cong, He, and Li (2018), who analyze mining pools; and Budish (2018b), who analyzes miners and attack incentives. We contribute to this nascent literature by developing a framework where mining can be analyzed with equilibrium prices.[11]

[11] Another related stream of the literature studies the economics of security tokens and initial coin offerings (e.g., Catalini and Gans (2018)) and the implications of private blockchains and decentralized ledger technologies for central banking, corporate governance, transaction efficiency, and capital markets (e.g., Fung and Halaburda, 2016; Harvey (2016); Malinova and Park (2017); Raskin and Yermack (2016); Yermack (2017)). Cong and He (2018) study the valuation of digital tokens facilitating transactions and business operations on a blockchain. They show that tokens can capitalize the impact of agents' expectations of future technological progress and adoption. While related, security tokens and private blockchains respond to economic incentives that are different from Bitcoin's.

1 Background on the Economics of Bitcoin

This section provides a brief background on the sources of bitcoin demand and the economics of the supply of verification and ledger-updating services in a DN.

1.1 Sources of Fundamental Demand for Bitcoins

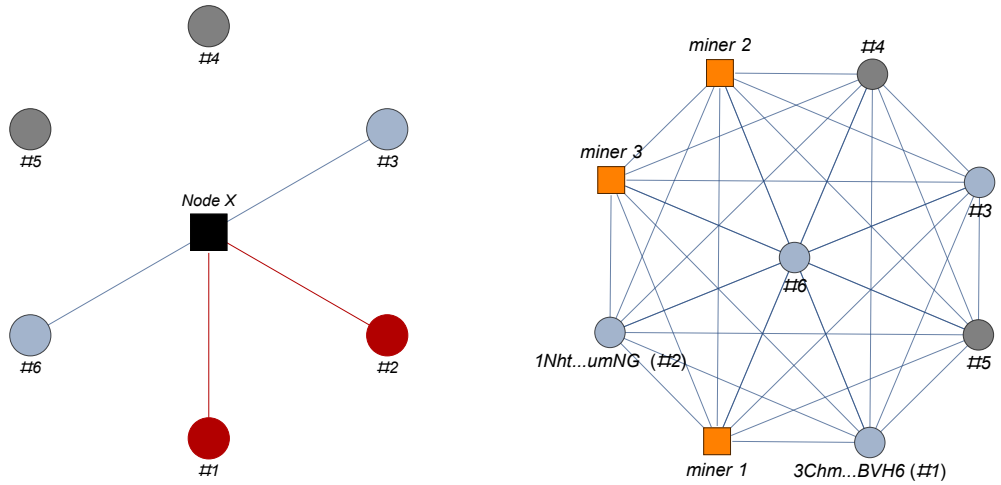
Besides the speculation motive, a frequent argument is that bitcoins are demanded because of low–transaction cost transfers, such as for international remittances among family members, and because the network is difficult to hack. Although these arguments may be correct, we argue that the differences between Bitcoin and traditional financial systems are more profound and relate to its resistance to censorship risk and trustlessness.

Bitcoin can be seen as a DN with high resistance to censorship risk, implying that its token has spanning properties that are potentially different from traditional Arrow–Debreu securities. In the original Arrow–Debreu approach, it is common to value contingent claims in a state space representation with two dimensions: calendar time and the state of nature, (t, ω). In the case of networks, one should also consider the specific identities i and i' of the agents willing to engage in a transfer, (i, i'), under state (t, ω). Consider the left panel of Figure 2, illustrating the simplest CN controlled by node X. We highlight two potential issues with this traditional design. First, not all agents are linked to the CN. Agents 4 and 5 are unconnected, possibly for reasons related to poor credit history or low income. Besides individual-level reasons, in traditional CNs, large numbers of agents could lose links due to international sanctions that disconnect an entire country from global financial markets. If the lack of participation is involuntary, one can see unconnectedness as a strong form of censorship. Second, even if two agents are part of the CN, they face the risk of censorship in the form of service denial at the time of the transfer. For example, agents 1 and 2 are linked, but a (t, ω)-contingent transfer between them could fail to materialize if X does not authorize it. In the context of state-contingent pricing, therefore, censorship becomes a source of *fundamental* market incompleteness for traditional assets.

In contrast, Bitcoin, illustrated in the right panel of Figure 2, has two distinctive advantages.

Figure 2. Centralized and Decentralized Networks: Censorship Risk Resistance and Connectedness

The left panel shows a CN where a single verifier, node X, has censorship authority over all transfers. The right panel shows a decentralized and complete peer-to-peer network, such as Bitcoin, with $m = 3$ miners.



First, the network design is peer to peer and all users have free entry. Therefore, the network topology is near complete and agents 4 and 5 can make transfers to all other agents. Second, the decentralized economic design offers much higher resistance to censorship in the form of service denial. Relatively to a traditional CN, the mapping of anonymous wallet addresses to individual identities is significantly more challenging.[12] However, even if this were partially possible, no single node updates the transactions in the blockchain but, instead, multiple miners that are located in different geographies and who do not obey a central authority. Therefore, even if one miner tries to stop a transfer from agent 1 to 2, other miners are unlikely to do the same.

Demand for Censorship Resistance. The demand for censorship resistance within networks has multiple sources,[13] including financial repression through governmental capital controls; option-like hedging against government abuses such as arbitrary wealth confiscation or the targeting of political dissidents and/or religious groups; hedging against changes in inheritance laws; the risk of disruptions of the traditional banking system due to bank runs, fiat hyperinflation, or the forced

[12]Bitcoin does not currently offer the best anonymity protection. So-called privacy coins such as Monero, also based on PoW, offer better protection against identity tracking.

[13]For a more comprehensive discussion, see Antonopoulos (2016).

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). Even when the consumption of a particular good or service is not restricted, consumers may demand the services of a DN to protect their privacy, especially in economies where the use of cash is restricted.

Demand for Trustlessness. The demand for the services of DNs can go beyond permitting censorship resistant financial transfers. A second fundamental source is related to the ability to perform trustless exchanges. Trustless networks allow for the coordination of resources towards the production of a specific service in a manner that does not require that the parties either know or trust each other, as in the case of smart contracts (e.g., Szabo, 1994) and decentralized applications (e.g., Wood (2018)). Potential advantages of this form of organization over the traditional firm include minimizing the impact of frictions such as counterparty risk, transaction times and costs, legal and verification costs, as well as information asymmetries through increased transparency. The demand for censorship resistance and the need for trustlessness are not mutually exclusive and, in most cases, they are not independent of each other. For example, DNs can power the contribution of resources to the development of censorship-resistant social media platforms (e.g., Steemit). In this context, the value of censorship resistance naturally resembles that of free speech.

Nondigital Alternatives. We argue that Bitcoin alternatives do not perfectly replicate the features discussed above and, thus, these features help to rationalize positive bitcoin prices. Consider the case of gold. In our view, bitcoin and gold are not perfect substitutes. Through a digital peer-to-peer network, bitcoins can be seamlessly transferred globally at a modest cost. Bitcoin and similar tokens can be used as the base infrastructure for layers of increasingly sophisticated contracts, acting as programmable money. Unlike gold and gold coins, for which purity and very small denominations are a concern, bitcoin benefits from homogeneity and divisibility. Transporting physical gold in the event of armed conflict, say, is more difficult and embeds more considerable

personal safety risks. Multiple types of national border controls undermine the usefulness of gold and other physical objects in the case of crises. A clear advantage of gold, on the other hand, is that it has direct consumption and industrial uses.[14]

In the past, many of the demand sources outlined above have motivated the use of paper cash and the development of significant off-shore markets and shadow banking systems. Unlike bitcoin, paper cash cannot be transferred digitally across the globe or be used for Internet commerce. Physical cash can be seized just as gold can. Besides, governments can outlaw or severely limit the use of cash, for example, by removing large denomination bills. Unlike a network such as Bitcoin, off-shore accounts are expensive and difficult to open and maintain, usually requiring complex legal structures, and are subject to risks themselves, such as confiscation and ownership leaks risks.

To conclude, given the multiple demand sources for censorship risk resistance and trustlessness, networks like Bitcoin offer advantages over preexisting alternatives. We refrain from modeling each of the different possible uses that we have discussed in this section. Instead, as a starting point, we assume that consumers can benefit from Bitcoin services and we develop a framework to value the network token in Sections 2 to 4. The framework nests the case where bitcoins are intrinsically useless and hold for pure speculative reasons (see Section 2.4) and can rationalize purely speculative bubbles, as in Section 9. The quantitative assessment of the usefulness of the Bitcoin network services against available alternatives and the overall welfare consequences of its emergence are empirical questions that are beyond the scope of this study.

1.2 DN Security and the Unity Property

In a DN, operational tasks are not delegated to a single node as in a CN but, instead, distributed across the network. Network security and overall performance, thus, rely on the public network protocols and the behavior of those nodes that can affect the evolution of the transaction history, that is, the miners in Bitcoin.[15] Of course, decentralization is not a binary condition: everything

[14] Sargent and Wallace (1983) are among the first to develop models with commodity money. See Velde and Weber (2000) for a model where gold and silver have monetary and jewelry uses.

[15] In the economic framework we analyze, we emphasize the security of the digital platform as opposed to performance speed (e.g., Pagnotta and Philippon (2018)). The latter is typically higher in CNs, since verification consensus with a single verifier can be achieved automatically. If both a CN and DN competed in the same economy, one would

else being equal, the degree of decentralization increases with the number of miners.

Verifiers in any DN need well-defined economic incentives to contribute resources that deliver high degrees of network security. Consider a generic DN where asset k is transferred. Verifier j contributes h_{jk} resources to the verification task at a cost $C(p, h_{jk})$, where $p = (p_k, p_{-k})$ is the price vector, and receives in exchange revenues $R(p, h_{jk})$. Network trust depends on the total contribution of resources, $H_k = \sum_{j=1:m} h_{jk}$. When the supply of resources is the result of verifiers' profit-optimizing behavior, optimal supply is a mapping $h^* : p \mapsto \mathbb{R}$. In Bitcoin, verifiers are incentivized by the same asset that consumers use for transfers, a property that we label as *unity*. Formally, we present the following definition.

Definition 1. *Consider an asset k transferred in a DN. We say that asset k satisfies **unity** when the endogenous amount of verification resources is given by $h_k^*(p) \neq h_k^*(p_{-k})$ and it does not if $h_k^*(p) = h_k^*(p_{-k})$.*

Table I provides a perspective on the unity property by considering several examples. Blockchain-based payment networks such as Monero, Dash, and Litecoin, share the unity property, since successful miners receive unit of the network's native token. The same is true in the case of Ethereum: miners verifying transfers receive as compensation units of ether, the native token. Additional tokens on the Ethereum network, ERC-20 tokens,[16] however, do not satisfy unity, since compensations for their transfers are paid in ether.

We consider a few additional examples that violate unity. First, in contrast to Bitcoin, the Depository Trust & Clearing Corporation (DTCC) is a centralized depository providing central custody of securities (i.e., a node running a CN). Through its subsidiaries, DTCC provides clearance, settlement, and information services for a range of securities on behalf of buyers and sellers. For its services, DTCC charges a fee. In this network, there is evident lack of unity between the value of the verifier's revenue (DTCC's equity) and the value of the transferred asset, for example, a stock such as Amazon.

expect consumer preferences to involve a trade-off between speed on the one hand and censorship resistance and trustlessness on the other.

[16] According to Etherscan.io, as of October 2018, the ERC-20 tokens with the greatest market capitalization were Binance coin (BNB), Vechain (VEN), and OmiseGo (OMG).

Table I
Digital Assets in Centralized and DNs: Examples

Network	Peer-to-peer	Multiple Verifiers	Free Entry Verifiers	Asset	Unity
Stock Exchanges, DTCC	n	n	n	Public equity	n
Bitcoin	y	y	y	bitcoin	y
Cryptocurrencies	y	y	y	Litecoin, Monero, Dash	y
Ethereum	y	y	y	ether	y
Ethereum	y	y	y	ERC-20 tokens	n
Ripple	n	y	n	XRP	n

Second, there is an emerging class of DNs with no free entry for verifiers, usually referred to as permissioned blockchains. One famous example is Ripple, a digital currency system in which transactions among counterparties are verified by consensus among approved network members on a shared ledger. Independent validating servers constantly compare their transaction records. Transfers of the network token, XRP, are subject to fees to avoid spamming. Verifiers (e.g., commercial banks), however, are not compensated for their services with the network token. Thus, XRP does not satisfy unity.

Definition 2. *We refer to DN tokens that violate unity, such as ERC-20 tokens or Ripple's XRP, as duality tokens.*

2 Network Users and Bitcoin Demand

This section first outlines the economic environment for network participants. Second, based on a given level of network security, it analyzes the bitcoin demand side and derives partial equilibrium prices.

2.1 Environment

Time is discrete and goes on forever. All random variables are defined over a probability space $(\Omega, \mathcal{F}, P)$. There is a single perishable consumption good that acts as the unit of account and can

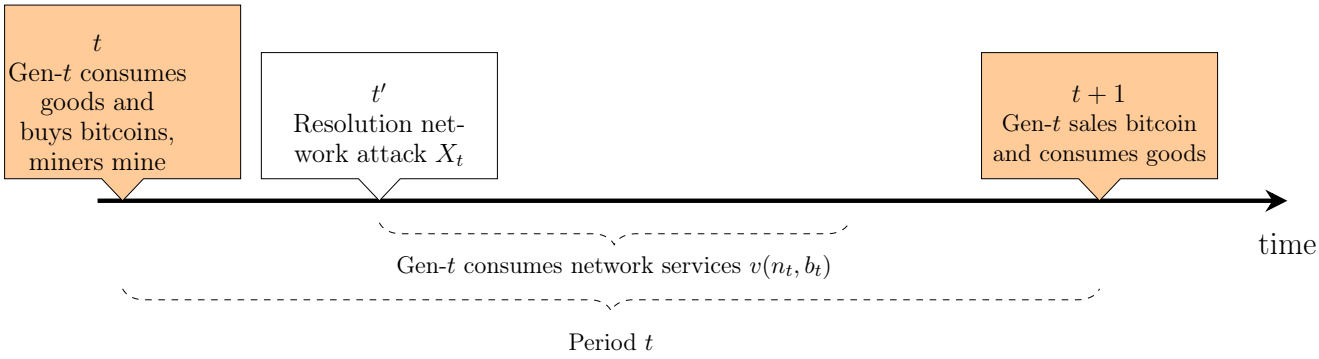
be produced by all agents at unitary marginal cost. There is a single financial network with two types of participants: first, n consumers that demand bitcoins and can benefit from network services and, second, m miners who act as verifiers and compete to confirm new blocks. Consumers and miners are different groups and both groups act as price takers. Consumers live for two periods and consume network services within the first period of life. If born at time t, consumer i's utility in period t is $c_{it} + u(v_{it})$ where $v_{it} \in \mathbb{R}_+$ represents the consumption of network services, $c_i \in \mathbb{R}$ is the net consumption of the good ($c_i < 0$ if production is greater than consumption), and u is a twice continuously differentiable, strictly increasing, and strictly concave function that satisfies $\lim_{v \to 0} u'(v) = \infty$.

Timing and Network Attacks. Network participants are exposed to the risk of a large-scale network attack, as follows. At the beginning of each period t, connections are described by a $(0,1)_{n \times n}-$matrix representing a *feasible* link between agents i and i' if the $(i,i')-$th element is one, that is, the ability of agent i to transfer a given amount of the asset to agent i' and vice versa. If the network survived all past attacks up to time t, given its peer-to-peer design, the set of links is given by a $(1)_{n \times n}-$matrix. Between times t and $t+1$, however, the set of connections could change due to a network attack outcome. In particular, within any period t, the outcome of an attack is captured by a random variable $\tilde{x}_t : \mathcal{F} \to \{0,1\}$ such that

- A realization $x_t = 1$ indicates that the network survives the attack, an event with probability τ_t, and all consumers remain connected within period t.
- A realization $x_t = 0$ indicates a successful attack, an event with probability $1-\tau_t$. If the attack succeeds, all transfers become unfeasible, and the set of connections is thus a $(0)_{n \times n}-$matrix. Moreover, if the attack is successful at time t, the network remains unusable thereafter.

The sequence of decisions and events in each period is illustrated in Figure 3. At the beginning of period t, given the bitcoin price, p_t^B, miner j selects an optimal amount of hash rate, h_{jt}. A consumer born at time t chooses consumption levels and bitcoin holdings to maximize the intertemporal expected utility. Consumers believe that the price of bitcoins, p^B, follows a Markov process, as

Figure 3. Period t Timeline



follows. If bitcoins are not valued at the beginning of time t, $p_t^B = 0$, bitcoins will not be valued at any time $s > t$. If $p_t^B > 0$, on the other hand, there is a probability $1 - \tau_t$ that the network will be successfully attacked within period t and bitcoins will lose their value thereafter. The consumer enjoys network services v_{it} within period t, an amount that depends on the outcome of $\tilde{x}_t$ and purchases at the beginning of period t, B_{it}. If a network attack is successful, then $v_{it} = 0$. In period $t + 1$, users born at time t sell their bitcoins to a new generation of users and consume the total sales revenue.

2.2 Value of Network Services and Bitcoin Demand

The value that consumers derive from the network services depends on two components. First, the value increases with the number of network users, n. As in other information networks, as the number of participants increases, so does the number of possible interactions and exchanges. Due to the peer-to-peer Bitcoin design, we consider n to be the single index of connectedness. Second, the value of services is proportional to the amount of goods that a given amount of bitcoins command. As rationality requires, the service flows that consumer i enjoys depend not on nominal but on real bitcoin balances, $b_{it} = B_{it}p_t^B$. We write $v_i(b_i, n)$ to represent how i values network services, a quantity expressed in units of the consumption good. At time t, agent i could hold the token due to its intrinsic utility, v_{it}, or to transfer resources to period $t + 1$.

If a network attack is successful at time t, we have $v_i(b_{it}, 0) = 0$ for all i. Agents' preferences

satisfy the axioms of expected utility and thus expected network services' utility at time t is given by $\tau_t \times u\left(v_i(b_{it}, n_t)\right) + (1-\tau_t) \times u\left(0\right)$. For any network size and holdings, the expected value of network services increases with the degree of network security, τ_t.

To derive bitcoins' demand, we make the following assumptions.

Assumption A1*a*. $u\left(c, v\right) = c + \frac{v^{1-\sigma}}{1-\sigma}$, $0 < \sigma < 1$.

Assumption A1*b*. $v(b, n) = f\left(n\right) b$, *where* f *is a differentiable function satisfying* $f(0) = f(1) = 0$, $f'(n) \geq 0$ *for* $N > n > 1$, *and* $\lim_{n \to N} f\left(n\right) < \infty$.

A1*b* makes agents in the network *seemingly identical* because, although their specific locations are different, their preferences can be represented by the same expected utility function. The function f summarizes the effect of *network externalities*. Note that a situation in which network services are worthless can be seen as the particular case in which $f(n) = 0$ for all n. If participation in the network were at all times full, $n = N$, on the other hand, we could view $f(n)$ simply as a positive constant.

Under A1*a* and A1*b*, consumers born in period t choose optimal holdings to solve

$$\max_{B_{it}} \mathbb{E}_t \left[x_t \underbrace{\frac{\left(f\left(n_t\right) p_t^B B_{it}\right)^{1-\sigma}}{1-\sigma}}_{\text{transactional service value}} + \delta x_t \underbrace{\left(B_{it} p_{t+1}^B\right)}_{\text{resale value}} \right] - B_{it} p_t^B, \tag{1}$$

where $\delta \in [0, 1]$ is the time discount factor. The consumers' first-order conditions and asset market clearing imply the following equilibrium condition:

$$\underbrace{\left(\frac{\tau_t}{1 - \delta \tau_t \mathbb{E}_t r_{t+1}^B}\right)^{\frac{1}{\sigma}} f\left(n_t\right)^{\frac{(1-\sigma)}{\sigma}}}_{\text{per capita real demand}} = \underbrace{\frac{B_t p_t^B}{n_t}}_{\text{per capita real supply}}, \tag{2}$$

where $r_{t+1}^B := p_{t+1}^B / p_t^B$. Condition (2) simply expresses that the marginal benefit of adding tokens, from either service flows or resale value, must equal the marginal cost. It is evident from equation

(2) that demand increases with the level of network security, the expected holding period return, and the size of the network and decreases with the curvature of the utility function σ.

2.3 Steady-State Equilibrium: Duality Tokens

We first study a partial equilibrium economy where, unlike Bitcoin and any other asset that satisfies unity, the level of network security is exogenous and equal in each period, with a known value $\tau_d \in (0,1)$. To stress the fact that we are interested in the partial equilibrium value, for a given τ_d, here we refer to the asset as a *duality token* and use p to denotes its price. We focus on a steady-state equilibrium in which real token balances are constant, there is no growth in network users, $n_t = n > 0$, and the nominal supply grows at a rate $\rho > 0$, therefore, $B_t = B_{t-1}(1+\rho)$. Given $b_t = B_t p_t$, for real balances to be constant, token prices must be expected to decline at a rate equal to ρ. We focus our attention on expectational equilibria, that is, equilibria where prices follow the outlined Markov process, and the consumers' model of price determination is self-fulfilling.

Assume that, in the first period, the price is positive, therefore, $b_0 > 0$.[17] Then, the optimality condition (2) can be expressed as a nonlinear difference equation in b_t, as follows:

$$\left[b_t - \tau_d f(n)^{1-\sigma} n^{\sigma} b_t^{1-\sigma}\right] = \frac{\delta}{1+\rho}\left[\ \tau_d\ \ b_{t+1} + (1-\tau_d)\times 0\right], \tag{3}$$

where $b_t \geq 0$ for all t. Equation (3) describes the dynamics that are consistent with a rational intertemporal equilibrium until a random time T when a network attack is successful ($b_s = 0$ at any time $s > T$).

Consider the case in which $f(n) > 0$ and let $A_d(b) := b - \tau_d f(n)^{1-\sigma} n^{\sigma} b^{1-\sigma}$ and $D_d(b) := \frac{\delta\tau_d}{1+\rho} b$ represent the left- and right-hand sides of equation (3). Figure 4 represents the diagrams of $A_d(b_t)$ and $D_d(b_{t+1})$. A positive stationary equilibrium $A_d(b_d) = D_d(b_d)$ is given by

$$b_d = \left(\frac{f(n)^{1-\sigma} n^{\sigma} (1+\rho)\tau_d}{1+\rho-\delta\tau_d}\right)^{\frac{1}{\sigma}}. \tag{4}$$

[17] For Bitcoin, the initial supply, B_0, was 50 units. The first issuance took place in January 2009, as part of the first block, also known as the genesis block.

Under A1a, $f(n) > 0$, and $\tau_d \in (0,1)$, one can always find a stationary equilibrium value $b_d > 0$ and such a value is unique.

Consider now a path originating at $b_0 < b_d$. Given b_0, agents expect, with probability $1-\tau_d$, a price of zero next period, so that $b_1 = 0$, and they expect, with probability τ_d, a price equal to $p_1 = b_1/B_1$, where b_1 satisfies equation (3). Given A1a, low values of b yield high marginal utility, making token purchases relatively attractive regarding network services. For agents not to change their holdings, prices must be expected to fall. Therefore, paths originating to the left of b_d involve decreasing real balances over time. Real balances cannot be negative, of course. Some paths, however, like those that reach b'', may not involve negative balances if b jumps to zero when b'' is reached. We reason, analogously, that paths originating to the right of b_d, like that originating at b''', involve increasing real balances over time.

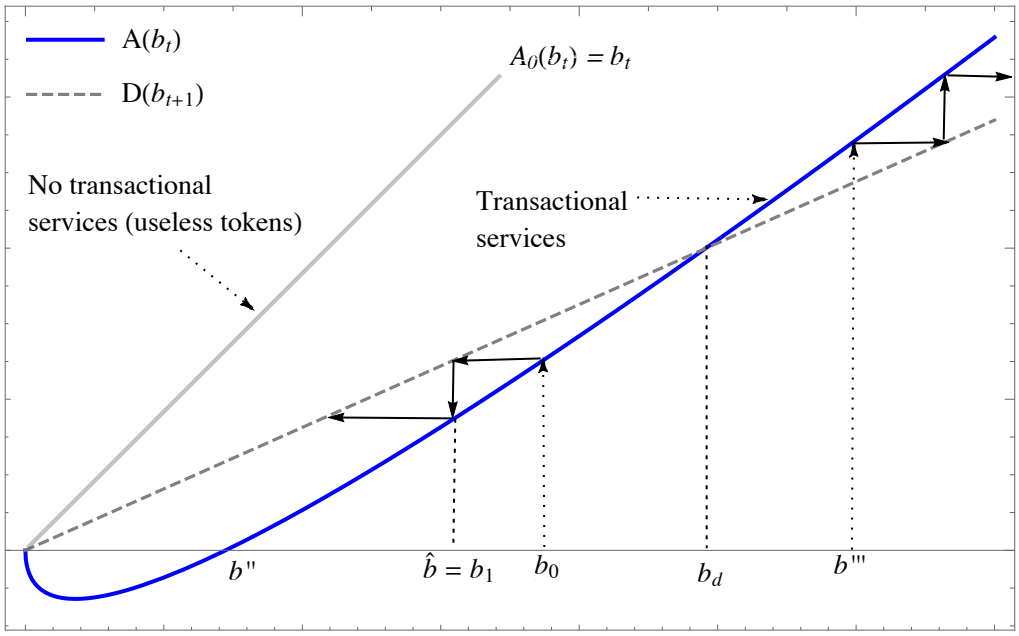
The function $A_0(b) = b$ in Figure 4 represents the case $f(n) = 0$, that is, the zero fundamental value case, where the token can be seen as a pure stochastic bubble (e.g., Blanchard (1979); Weil (1987)). In this case, a positive stationary equilibrium does not exist, since the expected return on such a bubble, a constant equal to $\frac{\tau_d}{1+\rho}$, is lower than the no-trade interest rate, δ^{-1}. The only stationary equilibrium when $f(n) = 0$ is $b = 0$.

The following result summarizes the existence and dynamic stability of stationary equilibria for the duality token.

Proposition 1. *[Stationary Equilibria: Duality token] Assume A1a and A1b. Then, (i) if network services are worthless, $f(n) = 0$, then a positive steady-state value does not exist. (ii) If $f(n) > 0$, there exists a unique steady-state equilibrium value $b_d > 0$. If $b_0 < b_d$, $b_t \to 0$ as $t \to +\infty$. If $b_0 > b_d$, b_t increases unboundedly as $t \to +\infty$.*

The analysis in Proposition 1 is a partial equilibrium one, since it considers an exogenous level of network security. However, it serves as a building block for the general equilibrium analysis in Section 4 and as a useful benchmark against Bitcoin in the remainder of the paper.

Figure 4. Duality Token: Stationary Balances



2.4 Demand-Side Discussion

To capture the critical dimensions of the demand for a bitcoin-like token, our demand specification explicitly addresses the risk of network attacks leading to service denial. For that, we consider a simple but novel characterization of this type of censorship risk in the form of a stochastic network size, with a probability distribution that is derived in the general equilibrium. We discuss examples and extensions in Section 10.2. The characterization of attacks as a binary random variable with permanent effects is for parsimony but not fundamental to the analysis. One could consider instead a range of possible attacks that do not have the same adverse consequences for the network and index network security using a cumulative distribution functions over attack outcomes. Similarly, the assumption $b_s = 0$ for all $s > T$ is not fundamental. At the cost of additional complication, one could also consider price jumps to a low price $\underline{p}$ in case an attack succeeds and then study a version of the model with periodic price crashes. Such extensions would embed the central equilibrium pricing mechanism that we model here.

We combine network attack risks with elements found in well-known settings. We briefly com-

ment on these, as follows. As in traditional communications networks (e.g., Economides (1996); Metcalfe (2013)), when $f'(n) > 0$, it is implicit in A1*b* that consumers value connections with others uniformly over the network and, therefore, network effects do not depend on identities. The fact that real balances drive the value of transaction services is a simplification found in a broad family of monetary models à la Sidrauski (e.g., Friedman (1969); Benhabib, Schmitt-Grohe, and Uribe (2001)). Brock (1974) and Feenstra (1986), among others, show how this approach finds equivalences in the cash-in-advance constraint approach. Although the key equilibrium implications for prices and network security in this economy do not depend on the specific formulation of v, the reduced-form approach embedded in A1*b* limits one's ability to study the welfare effects of changes in transactional or search frictions, an important research topic but not the focus of this paper. We see the the approach in A1*b* as a convenient first step to study price dynamics in a DN system and leave the desirable integration of more explicit frictional frameworks for future work.

The lack of a pure bubble stationary equilibrium when $f(n) = 0$ is not general but stems from the fact that, when utility is quasi-linear in the consumption good, the inflation-adjusted expected return on the bubble, $\frac{\tau_d}{1+\rho}$, is *always* less than the no-trade interest rate, δ^{-1}. We relax this assumption in Section 9 and characterize economies for which such stationary equilibria exist. In the remainder of the paper, we maintain the quasi-linear utility specification to isolate the general equilibrium pricing channels that are specific to the bitcoin economy from additional well-known restrictions on the existence and multiplicity of equilibria in more general utility settings. The latter include the possibility or cycles and chaos, for example, when income effects are strong.[18]

3 Technology and Network Hash Rate Supply

This section formalizes the concept of network security and characterizes miners' supply of verification resources, system hash rate.

[18] Manuelli (1990) and Blanchard and Fisher (1989), respectively, offer excellent discussions of the existence and stability of equilibria in monetary overlapping generations economies.

3.1 Network Security

We consider network security a technological primitive that is driven by the amount of computational resources invested in by miners, H.[19] Because network security represents the probability of attack survival, we assume the following.

Assumption A2*a*. $\tau : \mathbb{R}_+ \to [0,1]$ *is a non-decreasing, continuous mapping satisfying* $\tau(0) = 0$, $\tau(\infty) = 1$, *with a continuous first derivative* τ' *that satisfies* $0 < \tau'(0) < \infty$.

The increasing character of τ is intuitive: the more computing power miners supply, the more difficult it is for an attacker to either commit fraud or censor others' transactions. An implicit assumption is that miners do not act maliciously to undermine trust in the network. Moreover, any potential attacker has a finite attack budget that does not depend on the model's endogenous quantities. The assumption $\tau(0) = 0$ is also intuitive: if there were no resources to secure the network, any attacker with a positive budget would be successful.

3.2 Nakamoto Competition

The strategic game among miners follows that of Pagnotta and Buraschi (2018). There are m identical risk-neutral miners who contribute hash rate h in a competition to verify blocks of transactions in period t. We assume that the PoW difficulty level adjusts to ensure that the corresponding block is verified within period t. Miner j provides h_j and, conditional on some miner winning (i.e., conditional on a block verification), j wins the PoW race with a probability $\pi(h_j, h_{-j})$, $h_{-j} = \sum_{k \neq j} h_k$. Due to the random brute force nature of the PoW hashing race, the proportion of blocks verified by j is proportional to h_j; therefore, $\pi(h_j, h_{-j}) = \frac{h_j}{H}$, $H = h_j + h_{-j}$. Miners do not consume network

[19] This is, of course, a simplification. Additional important factors include the skills and work commitment of the developer community supporting the open-source code. The implicit assumption here is that developers' efforts have been exerted before the network operates and verifiers commit resources. A fuller description of the consensus protocol in Bitcoin would also assign a role to nonmining full nodes, that is, nodes that do not mine but keep a copy of the entire blockchain of transactions and therefore help to keep miners honest. See the documentation at the Bitcoin website (https://bitcoin.org/en/developer-documentation) for more details on the specifics. A critical economic difference between miners, on the one hand, and developers and nonmining full nodes, on the other, is that only miners are incentivized through network tokens. Developers and full nodes in Bitcoin do not receive token rewards. Therefore, we model hash rate supply as a price-sensitive quantity and reflect other aspects, such as the quality of the code, as price-inelastic parameters.

services. Therefore, within period t, if a miner receives a reward in bitcoins, the miner instantly sells that amount at the bitcoin market price p_t^B.[20]

The PoW reward for the sole winner is $B_{t-1}\rho$ bitcoins (12.5 bitcoins per block as of 2018), where B_{t-1} represents the outstanding stock of bitcoins at the beginning of period t before the mining reward is earned and ρ is the inflationary reward parameter. Because the reward increases the bitcoin supply, the postmining supply is $B_t = B_{t-1}(1+\rho)$. For a given price p^B and premining supply $B_{t-1} = B$, the expected revenue of miner j is $R(h_j; p^B) = B\rho p^B \times \pi(h_j, h_{-j})$.

Providing hash rate is costly. We consider a cost-of-mining function, $C : h_j \to \mathbb{R}_+$, which is an increasing, twice-differentiable function that satisfies $C(0) = 0$ and captures all associated costs such as hardware and power consumption.[21] Optimization of the miner's profits, $\max_{h_j} R(h_j; H, p^B) - C(h_j)$, yields the following result.

Proposition 2. *In a symmetric Nakamoto equilibrium, (i) the competitive provision of hash rate H^* is given by mh^*, where*

$$h_t^* C'(h_t^*) = B_{t-1}\rho p_t^B \left(\frac{m-1}{m^2}\right). \tag{5}$$

Moreover, aggregate hash rate supply, $H^* = mh^*$, satisfies: (ii) $\frac{dH^*}{dp^B} > 0$, (iii) $\frac{dH^*}{dm} > 0$, (iv) $\frac{dH^*}{d\rho} > 0$, and (v) if C' increases point-wise for every h^*; H^* then decreases.

The behavior of miners' hash rate supply, as characterized in Proposition 2, is key to analyze the response of the equilibrium bitcoin price to changes in the environment. Part (ii) reflects the intuition that, ceteris paribus, a higher bitcoin price induces miners to supply more computing resources. Network security, $\tau(H^*)$, therefore, is a function of p^B, consistent with the characterization of unity in Definition 1. With homogeneous miners, we have $\frac{dH^*}{dm} > 0$, which yields a monotonically positive relation between the number of miners and the system hash rate. Thus, in this environment, but

[20] The assumption that miners sell their rewards within the same period instead of accumulating rewards is consistent with a situation in which miners do not regard themselves as having a speculative advantage over users and where electric power, their main input, is not paid in bitcoins.

[21] For simplicity, we do not distinguish how resources are split between hardware and power consumption. Bitcoin uses the Secure Hash Algorithm SHA-256 algorithm for block verification, which is processor-intensive and thus incentivizes miners to acquire application-specific integrated circuit (ASIC) equipment. The latter is more efficient than regular CPUs or GPU cards. Instead, other DNs use memory-intensive algorithms (e.g., Litecoin's Scrypt and Vertcoin's Lyra2REv2), with which ASIC miners are less effective, in an attempt to preserve high levels of mining decentralization.

not without loss of generality, system hash rate is a sufficient statistic for the level of network decentralization. Parts (iv) and (v) are immediate implications of the optimality condition.

The derivation of Proposition 2 focuses on the noncooperative competitive process among honest miners that provides the minimum structure that is required for the general equilibrium price analysis of Section 4. Of course, the setting does not capture every aspect of the mining process. For example, we abstract from many intricacies of Bitcoin consensus rules. Moreover, for analytical tractability, we have simplified the analysis by considering miners small enough so as to not internalize their price impact. Therefore, Proposition 2 could underestimate the equilibrium hash rate supply relative to a situation in which miner j anticipates selling any mining reward at a price equal to $p^B + \frac{\partial p^B}{\partial h_j}$. A dozen large mining pools dominate the mining process.[22] However, the typical pool has a large number of small investors pooling resources to minimize uncertainty over the value of rewards. Participants can increase their share in the pool to increase the expected reward as the aggregate probability of winning increases in the pool's total computing power. Therefore, the approximation here could be reasonable if mining pool participants internalize the positive relation between hash power and rewards but regard themselves unable to affect the global bitcoin price. We discuss additional related aspects in Section 10.1.

3.3 Examples

To develop results, we consider specific technology functions (τ, C). We first consider network security functions that satisfy A2a, as follows.

Assumption A2b. *The rational security function is given by* $\tau_r(H) = \frac{H}{\phi^{-1}+H}$, $\phi > 0$.

Assumption A2c. *The exponential security function is given by* $\tau_e(H) = 1 - e^{-\phi H}$, $\phi > 0$.

Assumption A2d. *The logistic security function is given by* $\tau_l(H) = \frac{1}{1+e^{-\phi(H-\underline{H})}}$, $\phi, \underline{H} \geq 0$.

The network security parameter, ϕ, captures the incidence of all the price-insensitive factors that affect the likelihood of a successful attack. These include factors such as the specifics of the

[22] See, for example, https://www.blockchain.com/en/pools.

consensus protocol, the quality of the network open-source code, the number of non-mining full nodes, and any given budget constraint that network attackers face.

We now consider specific cost functions.

Assumption A3*a*. *The power cost function is given by* $C_\gamma(h) = ch^\gamma$, *where* γ *is a positive integer and* $c > 0$.

For concreteness, consider the following two examples of price-sensitive network security.

Example 1. Under A3*a*, by Proposition 2, $H_t^* = \left(B_{t-1}\rho p_t^B \left(\frac{m-1}{\gamma c_\gamma}\right) m^{\gamma-2}\right)^{\frac{1}{\gamma}}$. If $\gamma = 1$ and τ is rational (A2*b*), $\tau_r(H) = \frac{B_{t-1}\rho p_t^B \frac{m-1}{mc}}{\phi^{-1}+B_{t-1}\rho p_t^B \frac{m-1}{mc}}$.

Example 2. Under A3*a*, if costs are quadratic ($\gamma = 2$) and τ is exponential (A2*c*), $\tau_e(H) = 1 - e^{-\phi\sqrt{B_{t-1}\rho p_t^B\left(\frac{m-1}{2c}\right)}}$.

Consistent with Proposition 2(v), an increase in c reduces miners' profitability, hash rate supply, and network security in both examples. Under A2*b* or A2*c* or under A2*d* provided $H > \underline{H}$, a decrease in the price-insensitive parameter ϕ has the same qualitatively effect of reducing the probability of a successful attack.

4 General Equilibrium

Based on the demand and supply analyses in previous sections, we study an equilibrium in which the price of the token and network security are jointly determined. The program for consumers is now

$$\max_{B_{it}} \left(\underbrace{\frac{\left(f\left(n_t\right) p_t^B B_{it}\right)^{1-\sigma}}{1-\sigma}}_{\text{transactional service value}} + \delta \mathbb{E}_t \underbrace{\left(B_{it} p_{t+1}^B\right)}_{\text{resale value}} \right) \underbrace{\tau\left(H\left(p_t^B\right)\right)}_{\text{network security}} - \underbrace{B_{it} p_t^B}_{\text{cost}}. \tag{6}$$

We define the equilibrium concept, as follows.

Definition 3. *A general equilibrium is a sequence* $\left\{b_t, h_t, p_t^B\right\}_{t=0}^{+\infty}$ *of holdings decisions by consumers,* b*; network hash rate provision decisions by miners,* h*; and prices,* p^B, *such that: (i) con-*

sumers maximize expected utility, (ii) miners maximize profits, and (iii) the asset market clears.

We are interested in sequences that start with a positive value for bitcoins and characterize the equilibrium dynamics until a random time T when an attack drives the price to zero thereafter. Based on previous results, the characterization of equilibrium restrictions on the endogenous variables for a set of beliefs and technologies is straightforward.

Proposition 3. *[General Equilibrium Price] Consider the network economy described in Sections 2 and 3 with a single asset, bitcoin, miners providing hash rate and competing within Nakamoto competition, and consumers maximizing intertemporal expected utility under A1a and A1b. In the general equilibrium, the network hash rate is given by mh^*, where h^* satisfies $h^*C'(h^*) = B_{t-1}\rho p_t^B\left(\frac{m-1}{m^2}\right)$, and the bitcoin price satisfies*

$$p_t^B = \left(\frac{\tau(mh^*(p_t^B))}{1-\tau(mh^*(p_t^B))\delta\mathbb{E}_t r_{t+1}^B}\right)^{\frac{1}{\sigma}} \frac{f\left(n_t\right)^{\frac{1-\sigma}{\sigma}} n_t}{B_{t-1}\left(1+\rho\right)}, \quad \textit{if} \quad f(n) > 0, \tag{7}$$

$$p_t^B = \tau\left(mh^*\left(p_t^B\right)\right)\delta\mathbb{E}_t p_{t+1}^B, \quad \textit{if} \quad f(n) = 0. \tag{8}$$

Note that, regardless of whether Bitcoin offers valuable network services—that is, regardless of the value of $f(n)$—Proposition 3 highlights the equilibrium connection between the prices and network security, a consequence of *unity*: if network security is null, bitcoins are always worthless. The case $f(n) = 0$ resembles the case of stochastic bubbles with fiat money (e.g., Blanchard (1979); Weil (1987)). However, we highlight a crucial difference: the Markov transition matrix here is driven by endogenous network security, which, in any equilibrium, depends on the bitcoin price. Therefore, even when $f(n) = 0$, we cannot solely rely on traditional monetary equilibria characterizations.

4.1 Stationary Equilibria

We now study the existence and properties of a stationary equilibrium with constant real bitcoin balances and a given network size. It is again convenient to consider the nonlinear difference equation

in b_t associated with the equilibrium price equation (7):

$$\left[b_t - \tau\left(H(b_t)\right)\left(f\left(n\right)\right)^{1-\sigma} n^{\sigma} b_t^{1-\sigma}\right] = \frac{\delta}{1+\rho}\tau\left(H(b_t)\right) b_{t+1}, \tag{9}$$

where $b_t \geq 0$. Equation (9) describes the system dynamics until a random time T when a network attack is successful and where the distribution of T is consistent with the optimal hash rate production of miners. Under what conditions does a stationary solution to equation (9) exist? Can this economy lead to multiple equilibria? The following proposition summarizes our analysis of these issues.

Proposition 4. *[Existence and Stability of Stationary Equilibrium] Assume A1a and A1b and A2a. Then,*

(i) $b = 0$ is always a stationary equilibrium. If $f(n) = 0$, $b = 0$ is unique.

(ii) Assume $f(n) > 0$ and that miners' cost function is as in A3a and convex ($\gamma > 1$). If $\sigma > \frac{1}{\gamma}$, there exists at least one positive steady-state equilibrium. If τ is globally concave, such a positive stationary equilibrium is unique.

(iii) Assume $f'(n) > 0$ and that miners' cost function is as in A3a and linear, with $\gamma = 1$. Then, there exists a network size $\underline{n}$ such that, if $n \geq \underline{n} > 0$, a positive stationary equilibrium exists. There is a threshold value $\overline{n} > \underline{n}$ such that the lowest-price positive stationary equilibrium is dynamically stable if $n \in [\underline{n}, \overline{n}]$ and dynamically unstable otherwise.

(iv) If one or more positive stationary equilibria exist and τ belongs to any of the set of functions in A2b–A2d, the highest-price stationary equilibrium is dynamically unstable.

We elaborate on the economic intuitions. In the absence of mining subsidies, Proposition 3 implies that an equilibrium with $p_t^B = 0$ always exists. As in Proposition 1, a consequence of A1*a* is that no positive stationary equilibrium exists when $f(n) = 0$ (see Section 2.4). Unlike the zero-price stationary equilibrium for a duality token in Proposition 1, however, for bitcoin, $p_t^B = 0$ might not be necessarily an absorbing state. Although one would not expect mining subsidies, the presence of a few "convinced miners," such as those mining bitcoin in 2009–2010 when no apparent market for

bitcoin existed yet, could drive the system from a zero price to a positive price. This is because, in that case, the system would have $H(p^B = 0) > 0$ and, at least theoretically, a positive stationary equilibrium could be reached.s

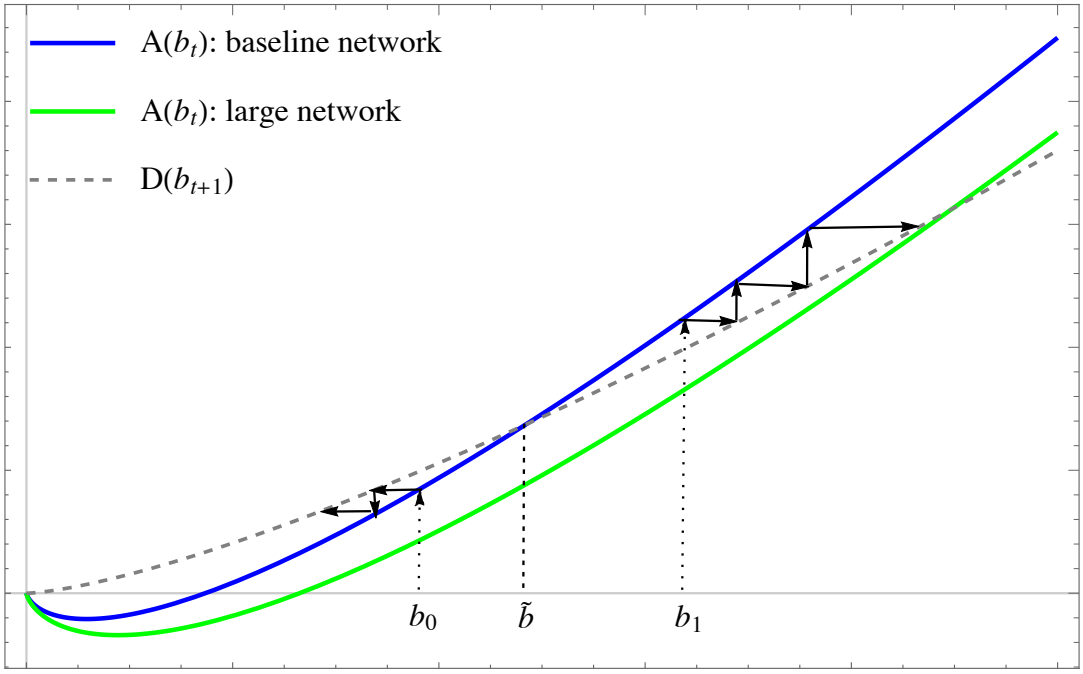
Many monetary models where money increases utility share the property that zero real balances are a stationary equilibrium. However, this non-monetary equilibria might not be robust to preferences that display the property $\lim_{\mu \to 0} \mu u'(\mu) > 0$, where μ denotes real money balances. The same holds for the duality token case in Section 2. For example, if $u(v(n, b)) = \ln(f(n)b)$, then $\lim_{b \to 0} bu'(b) > 0$ and $b = 0$ is not an equilibrium. In contrast, $b = 0$ is still a stationary equilibrium for a token that satisfies unity due to the endogenous reaction of network security. If, indeed, $\lim_{b \to 0} bu'(b) > 0$, $b = 0$ is still a stationary solution to equation (9) given $\tau(H(0)) = 0$: consumers never value the services of an insecure network.

Proposition 4 also shows that one or more positive steady-state equilibria can be found, depending on the specifics of the technology and preferences. Panel (a) of Figure 5 displays an economy such as that in part (ii) with quadratic mining costs, $\gamma = 2$, and $\sigma > \frac{1}{\gamma}$. The behavior of this economy resembles that in Figure 4: we have $\lim_{b \to 0} A(b) < 0$ and the function A crosses D from below at a positive stationary value $\tilde{b}$. Moreover, with a globally concave security function, such as τ_r, such an equilibrium is unique. The dynamic behavior is similar as well. However, we must now take into account the fact any price change dp_t^B affects miners' incentives and, therefore, affects network security by an amount $\tau'\left(H\left(p_t^B\right)\right) H'\left(p_t^B\right) dp_t^B$. Intuitively, when p_t^B grows large, $\tau \to 1$ and $\tau' \to 0$, implying that $\lim_{b \to +\infty} A'(b) = 1$ and $\lim_{b \to +\infty} D'(b) = \frac{\delta}{1+\rho}$. When $b_t \to 0$, $D'(b) \to 0$ and the slope of $A'(b)$ depends on the interaction between marginal changes in security, $\tau' H_b$, and utility, $bu'(b) \propto b^{1-\sigma}$. When miners face convex costs, Proposition 2 implies that $H_b \propto b^{\frac{1}{\gamma}-1}$ (there is a one-to-one mapping between p^B and b). Therefore, when the curvature parameter σ is sufficiently large, $A'(b) \to -\infty$ as $b \to 0$. By continuity of A and D, a value $\tilde{b}$ satisfying $A(\tilde{b}) = D(\tilde{b})$ exists.

The contrast with a duality token becomes more apparent in the linear cost economy of Panel (b) of Figure 5. Under the assumptions considered, the security response term $\tau' H_b \propto \tau'$, since H_b

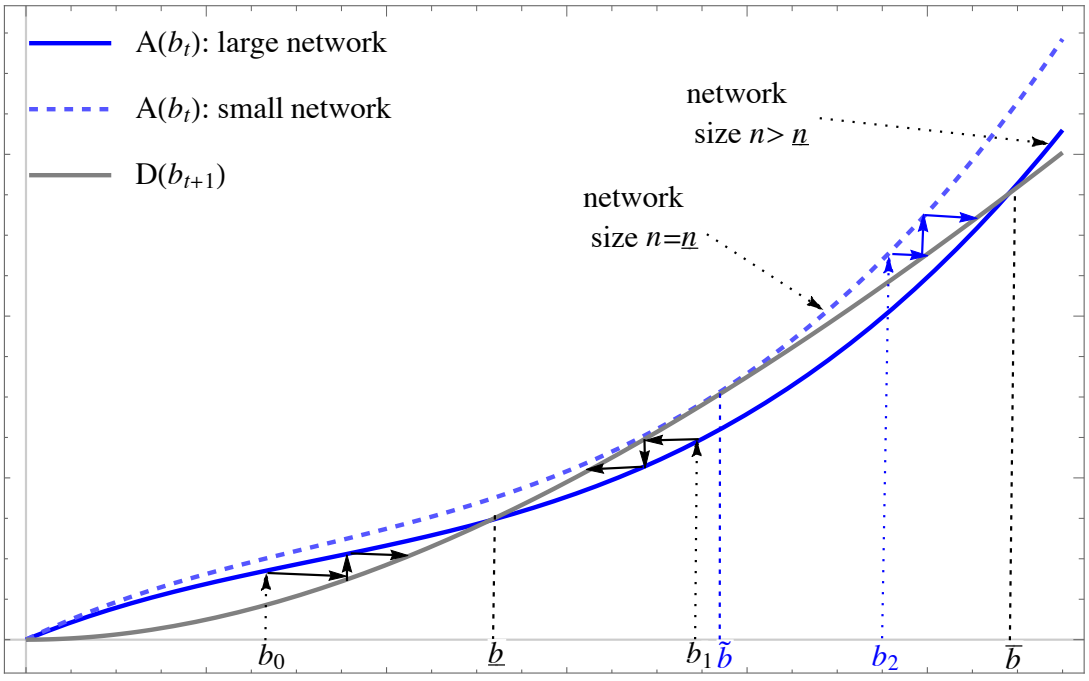
Figure 5. Stationary Equilibria

(a) Unique Positive Stationary Equilibrium



Bitcoin real balances (b)

(b) Multiple Positive Stationary Equilibria



Bitcoin real balances (b)

is constant. Therefore, $\lim_{b\to 0^+} A'(b) > 0$. Whether an equilibrium with positive balances exists depends on the value of $f(n)$. Panel (b) displays two possible cases. The solid blue line corresponds to a case with two positive stationary equilibria. The one with the lowest value, $\underline{b}$, has A crossing D from above. Using equation (9), one can see that expectations that are consistent with intertemporal optimization imply that $\underline{b}$ is dynamically stable. For example, a path that starts at b_0 converges over time to $\underline{b}$ from the left; and a path that starts at b_1 converges over time to the same point from the right. Indeed, an infinite number of bitcoin price paths that converge to the same stationary point.

The second and highest-value stationary equilibrium, $\overline{b}$, has A crossing D from below, implying that $\overline{b}$ is dynamically unstable. Figure 5(b) illustrates Proposition 4(iv): paths starting at a value greater than $\overline{b}$ in Panel (b) (or $\tilde{b}$ in Panel (a)) are divergent, with p_t^B increasing unboundedly. The fact that these paths do not violate consumers' budget constraints is simply a consequence of unitary marginal utility and marginal production cost of the consumption good.[23]

Figure 5(b) also displays a tangency equilibrium point, $\tilde{b}$, for a network size $\underline{n}$, the lowest value that yields a positive stationary equilibrium. For any lower network size, the diagram of A does not meet that of D and $b = 0$ is the only stationary solution. Equilibrium $\tilde{b}$ is a knife-edge case but with interesting dynamic properties. Paths that start at values lower than $\tilde{b}$ converge to this value. Instead, paths that start at a value greater that $\tilde{b}$ diverge away from $\tilde{b}$.

There is an additional distinction between economies such as those in (ii) and (iii) of Proposition 4 regarding the network size. Figure B1 in Appendix B shows economies for which $\lim_{b\to o^+} A'(0) > 0$ for various network sizes. With the possible exception of the tangency equilibrium, if a positive stationary equilibrium exists for these, that with the lowest value has A crossing D from above, such as the baseline network with a solid line. That with the highest value displays the opposite pattern. Therefore, an increase in the network size can have opposite effects on the value of the new stationary equilibria. The figure shows that a network size increase lowers the value of $\underline{b}$. Such

[23] If one considers a traditional finite endowment environment, as in Section 9, such paths become immediately unfeasible. Alternatively, such explosive paths could be ruled out by adding a constraint bounding the value of bitcoin transactional services from above (Obstfeld and Rogoff (1986)). Furthermore, one could consider sunspot equilibria, where consumers and miners expect paths starting at $b_t > \overline{b}$ display $b_{t+1} = \overline{b}$ with some exogenous but positive probability.

a negative change occurs for low values of network security, for which relatively small changes in n can produce significant changes in the expected utility of network services. Intuitively, this type of behavior resembles that of economies with strong income effects.[24] A secure network such as Bitcoin is arguably more likely to behave like $\overline{b}$, for which $A'\left(\overline{b}\right) > D'(\overline{b})$. We refer to stationary equilibria such as the latter as regular.

Definition 4. Consider a positive stationary solution to equation (9), $\tilde{b}$, and $\epsilon > 0$. We say that solution $\tilde{b}$ is regular if $\lim_{\epsilon \to 0} A'(\tilde{b} - \epsilon) - D'\left(\tilde{b} - \epsilon\right) > 0$ and $\lim_{\epsilon \to 0} A'(\tilde{b} + \epsilon) - D'\left(\tilde{b} + \epsilon\right) > 0$.

Using this definition, we can state the following lemma.

Lemma 1. *Let ω be the vector of parameters and $y\left(b, \omega\right) := \left(\frac{f(n)^{1-\sigma} n^{\sigma} \tau(H(b))(1+\rho)}{1+\rho-\delta\tau(H(b))}\right)^{\frac{1}{\sigma}}$. If a stationary equilibrium value $\tilde{b}$ is regular, then, in a neighborhood of $\tilde{b}$, $sign\left(\frac{d\tilde{b}}{d\omega}\right) = sign(y_{\omega})$.*

Corollary 1. *Assume A1a, A1b and $f'(n) > 0$. If a stationary solution to equation (9), $\tilde{b}$, is regular, the value $\tilde{b}$ increases with network size.*

Regular stationary equilibria share the intuitive property of increasing in value with n. Moreover, Proposition 4 indicates that, if only one stationary equilibrium exists, it must be regular. To analyze how the a stationary market equilibria is affected by changes in the environment, in Sections 5 to 7 we concentrate on regular stationary equilibria. Such a focus also facilitates connections between bitcoin and the duality token in Section 2. We address dynamics out of steady state in Section 8.

5 Bitcoin Prices and Mining Competition

Unlike institutions in regulated payment systems, miners in Bitcoin have free entry and exit. In this section, we examine how equilibrium prices are affected by changes in the strength of mining competition as given by the total number of miners. To gain a quantitative perspective on the

[24] As is well-known, in an economy with power preferences, the concavity parameter σ controls both the elasticity of intertemporal substitution and the degree of risk aversion. Under A1*a* with $\sigma > 1$, for example, consumers' elasticity of intertemporal substitution is low and their desire to smooth consumption is high. In the presence of higher expected network services, everything else being constant, the associated wealth effect induces consumers to value present consumption more and could decrease the demand for bitcoin, lowering its price at time t.

general equilibrium effects, we also consider a quantitative version of the model. We do not, however, attempt to make precise counterfactual price predictions, since the structural estimation of deep preference and technology parameters is beyond the scope of our study.

5.1 The Number of Miners

Proposition 2 shows that, under Nakamoto competition, when miners take the price as a given, an increase in the number of miners intensifies competition to win the PoW race and increases the total amount of hash rate. The following result shows that, in general equilibrium, the effect on the price is positive as well.

Proposition 5. *The equilibrium price of bitcoin increases with the number of miners, m. In the perfect competitive limit, $m \to \infty$,*

$$\lim_{m\to\infty} p_t^B := p_t^\infty = \left(\frac{1+\rho}{1+\rho-\delta}\right)^{\frac{1}{\sigma}} \frac{n_t}{B_t} \left(f\left(n_t\right)\right)^{\frac{(1-\sigma)}{\sigma}}. \tag{10}$$

The intuition is simple. Everything else being constant, as m increases, so does the system hash rate, increasing the network security value $\tau(H)$. Network users, therefore, experience a reduction in censorship risk, that is, a lower probability of a successful attack, $1-\tau\left(H\right)$. The resulting new equilibrium price is higher. Perhaps surprisingly, although miners compete in capacity, h, as in traditional Cournot competition, *the bitcoin price is increasing in total capacity*, $H = \sum_{j=1:m} h_j$. This connection between capacity and price seems to yield a reverse Cournot outcome. However, oligopolistic Nakamoto competition is unlike Cournot's: miners do not compete in bitcoin units but, rather, in hash rate units, that is, *units of network security*. The issuance of bitcoin units, instead, is beyond any participant's ability.

Note that, when $m \to \infty$, $\tau(H) \to 1$. Therefore, the limit price expression p_t^∞ given in (10) coincides with the perfect security limit equilibrium price of the duality token, $\lim_{\tau^d\to 1} p_t^d$. Moreover, under A2*b* or A2*c*, an increase in the fundamental security parameter ϕ has the same qualitative effect on the price. Moreover, the perfect competition limit price, $m \to \infty$ with $\phi > 0$ and the limit price corresponding to $\phi \to \infty$ with $m > 2$, coincide. The latter could be seen as the counterfactual

limit case in which noncompensated security drivers, such as the quality of the open-source code, perfectly secure the network.

5.2 Implications for Bitcoin Prices: A Quantitative Perspective

We now develop a quantitative version of the model. We interpret the time period as representing a month and consider an economy with a rational network security function, τ_r, as in A2*b*; a quadratic cost function as in A3*a*, with $\gamma = 2$; we set $f(n) = \theta \log(n)$, with $\theta > 0$, in the spirit of Odlyzko's law;[25] and consider a utility curvature parameter $\sigma = 0.6$. It is easy to verify that this economy satisfies the the conditions in Proposition 4 for the existence of a unique positive stationary equilibrium in real bitcoin balances that is given at time time t by

$$p_t^B = \left(\frac{\tau_r\left(p_t^B\right)(1+\rho)}{1+\rho-\delta\tau_r\left(p_t^B\right)} \right)^{\frac{1}{\sigma}} \left(\frac{n_t\left(\theta \log n_t\right)^{\frac{(1-\sigma)}{\sigma}}}{B_{t-1}(1+\rho)} \right), \tag{11}$$

$$\tau_r\left(p_t^B\right) = \frac{\sqrt{B\rho p_t^B\left(\frac{m-1}{c}\right)}}{\phi^{-1}+\sqrt{B\rho p_t^B\left(\frac{m-1}{c}\right)}}.$$

To calibrate the model parameters, we consider a set of observables characteristics for the Bitcoin network as of June 30, 2018. On that date, the bitcoin price was approximately USD 6,381, and the network hash rate was 35.6 exahash per second (see Figure 1). The total supply of bitcoins at that time, 17.124 million, represents the premining supply at time t, B_{t-1}. Given a reward of 12.5 bitcoins per mined block (as of 2018), there are, on average, $6 \times 24 \times 365/12 = 4,380$ blocks per month. Thus, given B_{t-1}, $\rho = \frac{12.5 \times 4,380}{17,124,175} \approx 0.32$ percent or 3.9 percent annually. Blockchain.com reports that the top 10 mining pools (e.g., BTC.com, AntPool, ViaBTC) regularly account for more than 90 percent of the system hash rate. Interpreting a miner in the model as a mining pool, we set $m = 10$. For the network size, we set n equal to 20 million. Such a value is of the same order of magnitude as the total number of Blockchain.com Bitcoin wallets created as of June 2018 (approximately 26 million).[26] Given (p^B, ρ, m), the cost parameter, c, is obtained by inverting

[25] See, for example, http://www.dtc.umn.edu/~odlyzko/doc/metcalfe.pdf.

[26] Although Blockchain.com is one of the most important Bitcoin wallet supplier, it is not, of course, the only one. For example, Coinbase.com, the largest U.S. Bitcoin exchange by the number of users, reported having over 12

TABLE II
Bitcoin Network Calibration: Parameter Values

	Supply and Mining						N. Size	Preferences		
Parameter	ρ (%)	m	B	c	γ	ϕ	n	δ	σ	θ
Value	0.32	10	17.1m	0.18m	2	0.52	20m	0.95	0.6	35.27

equation (5) and matching the observed hash rate. The time discount parameter is $\delta = 0.95$, consistent with values in standard asset pricing. Given the observed hash rate, we set parameter ϕ to yield a "small probability" of network attack over a given year equal to 2 percent. Of course, it is not possible to calibrate this probability directly, since no successful large-scale attack to Bitcoin has been registered. Given the observed strength of the network, we view 2 percent as a rather conservative value. Given the values of all the other parameters, θ is set by inverting equation (11) to match the observed price. The parameters values are summarized in Table II.

We now evaluate numerically the results in Proposition 5. The calibration suggests that when m increases 50 percent to 15, the equilibrium hash rate increases by 33 percent and the bitcoin price increases by 13 percent to USD 7,198. In the limit, with perfect miner competition, p_t^{∞} equals USD 10,979. The calibration thus implies a security-driven price gap of about 72% between the perfectly competitive price and the oligopolistic price with $m = 10$.

6 "Optimal" Bitcoin Supply

A breakthrough feature in the work of Nakamoto (2008) is the prevention of any network participant, a user or miner, from directly or indirectly controlling the supply of bitcoins. This is obviously in sharp contrast with any traditional fiat money system, electronic or otherwise, run by a central bank. Therefore, analyzing monetary policy in the traditional sense of regulating money supply is not possible.

However, it is interesting to study what is the effect of a change in the token supply growth rate

million customers at the end of 2017. At the same time, one user can create more than one wallet, not necessarily with the same wallet provider, making an accurate estimation of the number of users difficult. In the absence of any commonly accepted method to estimate the number of network users, we refrain to claim that 20 million is a realistic figure. Following the calibration approach in this section, a smaller n value would imply a larger value of the preference parameter θ and vice-versa.

on its market value. Consider first the stationary equilibrium price of the duality token in Section 2.3. From equation (4):

$$p_t^d = \underbrace{\frac{nf(n)^{\frac{1-\sigma}{\sigma}}}{(1+\rho)\,B_{t-1}}}_{\text{supply channel}} \underbrace{\left(\frac{\tau_d(1+\rho)}{1+\rho-\delta\tau_d}\right)^{\frac{1}{\sigma}}}_{\text{expectations channel}}. \tag{12}$$

We can distinguish on the right-hand side of equation (12) two distinct effects of changes in ρ. First, a supply channel affects within-period market clearing: Everything else being constant, increasing supply in period t has the effect of reducing the equilibrium price as the token becomes less scarce. Second, an expectations channel: In a stationary equilibrium with constant real balances, increasing ρ leads to lower expectations of resale prices, lowering the equilibrium price today. The combined effect of the supply and expectation channels imply that, for a token with price-insensitive network security, an increase in ρ unambiguously decreases the token price.

Consider now a stationary price equilibrium:

$$p_t^B = \underbrace{\frac{nf(n)^{\frac{1-\sigma}{\sigma}}}{(1+\rho)\,B_{t-1}}}_{\text{supply channel}} \underbrace{\left(\frac{\tau(H_t(\rho))(1+\rho)}{1+\rho-\delta\tau(H_t(\rho))}\right)^{\frac{1}{\sigma}}}_{\text{expectations and security channels}}. \tag{13}$$

We can distinguish in equation (13) *three* distinct channels by which changes in ρ can affect the bitcoin price. The supply and the expectations channel are as above.[27] There is, however, an additional security channel: Absent other forms of compensation to miners, such as fees, their inflationary reward is driven by ρ.[28] Ceteris paribus, a higher mining reward incentivizes miners to secure the network better, increasing the bitcoin price.

The relative strength of each channel depends on the primitives of the economy. Intuitively, when ρ is low, the positive price effects of the network security channel should dominate. When ρ is high, on the other hand, the negative supply and expectation channels should dominate. We are

[27] In the Bitcoin protocol, miners' reward is expressed as the amount of Satoshis in the Coinbase transaction—the first transaction in each block—and not a fraction of the outstanding supply. Of course, given B_{t-1}, there is a one-to-one mapping between the nominal reward, $B_{t-1}\rho$, and the supply growth level, ρ.

[28] Currently, the inflationary reward dominates compensation from fees. Historically, fees represent less than 1 percent of the total reward. The Bitcoin protocol is designed to slowly replace inflation by user fees over time as the total supply slowly approaches the limit of 21 million bitcoins around the year 2140. Note that fees are paid in units of bitcoins. Therefore, the unity property we define here is also intrinsic to Bitcoin in the long run.

interested in determining whether there is a ρ value that finds the optimal balance between these opposite forces in the sense of maximizing the network's market capitalization, $B_t p_t^B$.

Proposition 6. *Assume the conditions for a regular stationary equilibrium. Assume that mining costs are linear and that the network security function τ is strictly concave. Then, there is a value $\overline{\rho}$ given by $V(n,m) = W(\overline{\rho})$, where $V(n,m) := nf(n)^{\frac{1-\sigma}{\sigma}} \frac{m-1}{m}$ and*

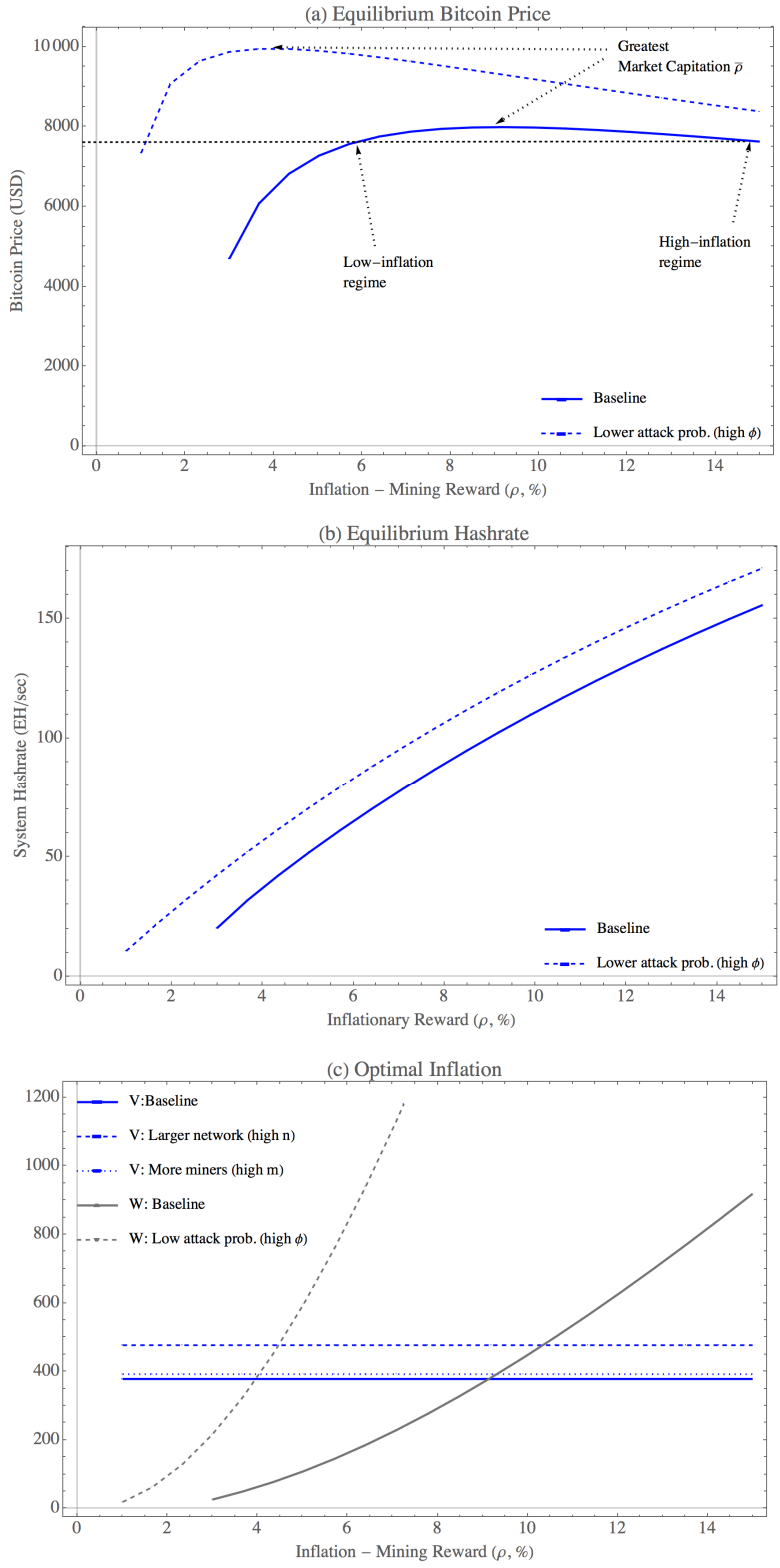
$$W(\rho) := \frac{\tau^2(\rho)}{\tau'(\rho)} \left(\frac{1+\rho-\delta\tau(\rho)}{(1+\rho)^{1+\sigma}} \right)^{\frac{1}{\sigma}} ((1+\rho-\delta\tau(\rho))\sigma+\delta)\, c,$$

where $\tau(\rho)$ represents $\tau(H^*(\rho))$, such that, if $\rho < \overline{\rho}$, the equilibrium bitcoin price increases with ρ. If, on the other hand, $\rho > \overline{\rho}$, the equilibrium bitcoin price decreases with ρ.

The existence of an optimal growth rate level for bitcoin market capitalization does not rely on mining costs being linear, but a linear cost function yields a simpler expression for W. Panels (a) and (b) of Figure 6 show how the regular equilibrium bitcoin price and total hash rate change with different values of ρ. The solid line corresponds to primitives that are identical to the baseline calibration, except for mining costs. We can see that the equilibrium price is indeed concave in ρ. For the baseline calibration, the highest price is achieved with ρ near 9 percent. It is difficult to quantitatively assess such value, since it directly depends on the unobservable probability of an attack conditional on H. For example, given the observed hash rate in June 2108, $H_{6:2018}$, increasing the security parameter ϕ so as to lower the probability of a successful attack from 0.02 to $\tau(H_{6:2018}) = 0.005$ (corresponding to the dashed line), yields an optimal ρ of 3.9 percent, approximately equal to the current observed level. It is also worth noting that, as Panel (b) illustrates, in general equilibrium, better network fundamentals (higher ϕ values) lead not only to a higher valuation, but also to a higher equilibrium hash rate supply, further increasing network security.

Another interesting implication of Proposition 6 is that, for any value $\rho \neq \overline{\rho}$, the same equilibrium bitcoin price is consistent with two different supply growth levels, one low- and one high-growth regime. Although the Bitcoin protocol displays no flexibility around ρ, Bitcoin inflation decreases every four years at a predictable rate (e.g., $\rho_{2020} = 0.5\rho_{2016} = 0.25\rho_{2012}$ and so on). It is often

Figure 6. Bitcoin Price and Hash Rate: Changes in the Nominal Supply Growth



informally argued that "reward halving" increases the bitcoin price. However, Proposition 6 shows that the price effect of a change in ρ is nonmonotonic. At least theoretically, one could reduce supply growth significantly without any substantial price change by transitioning from the high- to the low-growth regime at the time of a reward halving. Generally, whether a predictable reward halving has a positive effect on the price depends on whether the system is to the left or the right of the market capitalization–maximizing value $\overline{\rho}$.

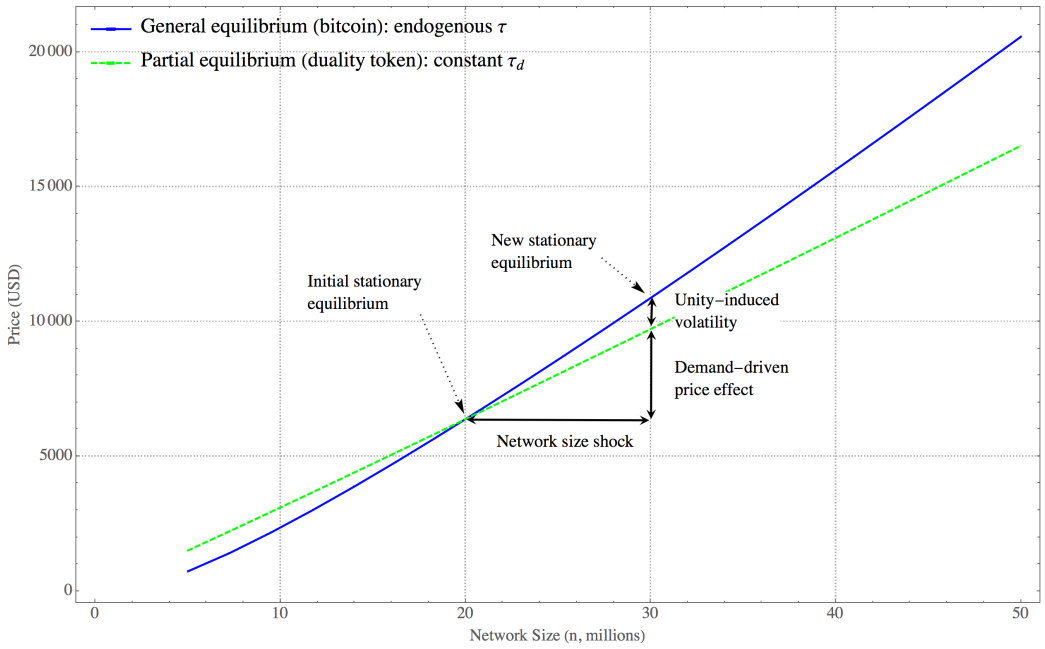
Panel (c) of Figure 6 displays the functions V and W in Proposition 6. The optimal ρ value is found at a point $W(\overline{\rho}) = V(n, m)$. Function W depends on the specifics of technologies τ and C as well as the curvature parameter σ; for concave τ such as that under A2*b*, it is an increasing function of ρ. Function V is flat, since it does not depend on ρ. Moreover, it is increasing in the network size n. The solid line corresponds to the baseline values $(n, m) = (20\text{m}, 10)$. The dashed line for the larger network corresponds to $(25\text{m}, 10)$. Everything else being constant, an increase in the size of the network leads to a greater intersection value $\overline{\rho}$. Intuitively, a greater network size moderates the negative supply effect and increases the demand for network security. Ceteris paribus, an increase in m intensifies miners' competition and raises hash rate output and user valuation, leading to a slight increase in $\overline{\rho}$.

Overall, the analysis in this section shows that the behavior of the supply side of the Bitcoin monetary system is fundamentally different from traditional monetary economies (e.g., Rocheteau and Nosal (2017); Walsh (2017)). First, by design, no economic agent can influence money supply in Bitcoin. Second, changes to the nominal growth rate of money, such as those embedded in reward halving, have consequences on contemporaneous prices that are potentially different, as explained by three distinct channels. Arguably, the impact of the supply and expectations channels are qualitatively similar in traditional economies and in Bitcoin.[29] The network security channel, however, is new to the Bitcoin economy. Moreover, the unity property generates a structural link between the supply and the security channels, since the Coinbase reward to miners is the unique

[29]The mechanics of each channel are, of course, not identical. In fiat systems, for example, there are multiple sources of changes to money supply such as regulatory actions and banks credit expansion. Moreover, relative to centrally controlled monetary systems, there is significantly less uncertainty about future Bitcoin nominal inflation. Therefore, in traditional systems, agents could regard inflation uncertainty as an additional risk factor.

Figure 7. The General Equilibrium Pricing Implications of Unity

This figure shows the bitcoin price (solid line) and a duality token price (dashed line), that is, that resulting from a partial equilibrium where network security is kept constant. Parameter values are given in Table II.



source of new bitcoins.

7 Network Size and Unity-Induced Volatility

A central implication of Section 4 is that bitcoin prices and network security are always jointly determined in equilibrium, a consequence of unity. This section shows that such an equilibrium link embeds implications for price volatility. As a benchmark, we consider a duality token with an identical level of network security in the stationary steady state. We illustrate this connection using shocks to network size, to which all DN assets are intrinsically exposed.

Proposition 7. *[Unity Induced Volatility] Consider a duality token and a unity token that are otherwise identical. Suppose that the conditions for a unique positive stationary equilibrium stated in Proposition 4 are met for the unity token. Given the regular stationary equilibrium value, b_u, set τ_d, the network security of the duality token, to equal $\tau\left(H\left(b_u\right)\right)$. Then, a shock to the network size*

induces a greater price change for the unity token: $\left|\frac{db_u}{dn}\right| > \left|\frac{db_d}{dn}\right|$. *The unity-induced price volatility increases with the values of* $H_b(b_u)$ *and* $\tau'(b_u)$.

The economic intuition of Proposition 7 is simple. An increase in network size, for example, increases the strength of network effects $f(n)$ and it increases the investor competition for the tokens. These factors apply upward pressure on the price for both types of token. For bitcoin, however, miners' incentives are directly proportional to the price. Therefore, an increase in the price generates a positive hash rate supply reaction and, thus, an increase in network security that *feeds back the upward pressure on the price*. This feedback effect is absent for the duality token.

Figure 7 displays the equilibrium price reactions of a unity and a duality token to different network sizes using the quantitative version in Section 5.2. The solid line represents the unity token price given by equation (11). The dashed line represents the counterfactual partial equilibrium schedule that is computed using equation (11), but with a price-insensitive hash rate of 35.6 exahash per second, so that $1-\tau_d = 0.02$. These curves illustrate the price–security feedback effect embedded in the unity property. The general equilibrium diagram is steeper. Thus, the price is lower (higher) for network sizes that are lower (higher) than the baseline value of 20 million. The parameter configuration suggests that the price reaction gap can be substantial. For example, an increase in network size of 50 percent leads to a price increase of 71.8 percent for the unity token price and an increase of only 53 percent for the duality token price. The price reaction gap, *unity-induced volatility*, is explained by the price–security feedback effect driven by the term $\tau' H_b$. Failing to consider this aspect of bitcoin-like tokens in valuation could, therefore, lead to severe mispricing.

7.1 Do Bitcoin Prices Follow Metcalfe's Law?

A long-standing argument, generally referred to as Metcalfe's law, is that the value of a near-complete communication network such as the Internet grows as the square of the number of its users (e.g., Metcalfe (2013)). Because Bitcoin is a peer-to-peer network, is it often informally claimed that the bitcoin price should also follow Metcalfe's law.[30] Such conjecture seems prima

[30] See, for example, the discussion in Wheatley, Sornette, Huber, Reppen, and Gantner (2018).

facie consistent with the nonlinear growth in bitcoin prices relative to its users in recent years. Understanding the specific connection between bitcoin prices and network size, however, requires the explicit modeling of an equilibrium economy.

Let $\eta := \frac{dp}{dn}\frac{n}{p}$ denote the network size price elasticity of a particular token, with $\eta^{\text{Metcalfe}} = 2$. For the economies analyzed in the previous section, we can state the following.

Proposition 8. *[Equilibrium Network's Laws] Consider a duality and a unity token that are otherwise identical. Suppose that the conditions for a unique positive stationary equilibrium of Proposition 4(ii) are met for the unity token. Then,*

$$\eta^d = \frac{(1-\sigma)}{\sigma}\frac{nf'(n)}{f(n)} + 1,$$
$$\eta^B = \eta^d \frac{\sigma}{\sigma - \chi(b)},$$

where $\chi(b) := \frac{\tau'(b)H'(b)b}{\tau(b)}\left(\frac{1+\rho}{1+\rho-\delta\tau(b)}\right)$.

For a duality token, η^d only depends on preference parameters. We consider some examples.

Example 3. Let $f(n) \propto n^\alpha$. Then, $\eta^d = \frac{(1-\sigma)\alpha}{\sigma} + 1$. Note that, in the particular case in which $\alpha = \frac{\sigma}{1-\sigma}$, then $\eta^d = \eta^{\text{Metcalfe}}$. If $\alpha > \frac{\sigma}{1-\sigma}$, then the network size elasticity is greater than Metcalfe's and vice versa.

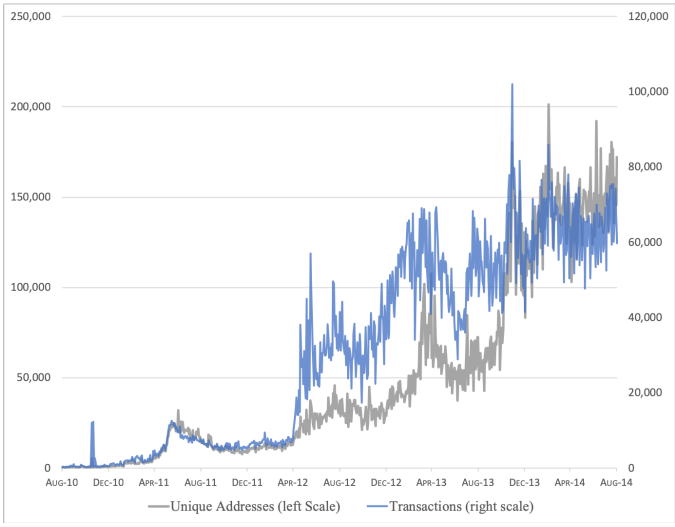
Example 4. Let $f(n) \propto \log(n)$, as in the baseline calibration. Then, $\eta^d = \frac{(1-\sigma)}{\sigma}\frac{1}{\log(n)} + 1$. For large value of the network size and intermediate values of σ, $\eta^d \approx 1$, as Figure 7 illustrates.

In the case of unity tokens such as bitcoin, the network elasticity coefficient η^B also depends on supply-side parameters and technologies and the equilibrium value of real balances. Therefore, it is difficult to assess ex ante how η^B globally relates to η^{Metcalfe} or to any alternative network law.[31] However, the equilibrium restrictions on prices and network security in Propositions 3 and 4 provide moment conditions that an empirical researcher can exploit to learn about unobservable deep parameters such as the shape of f.

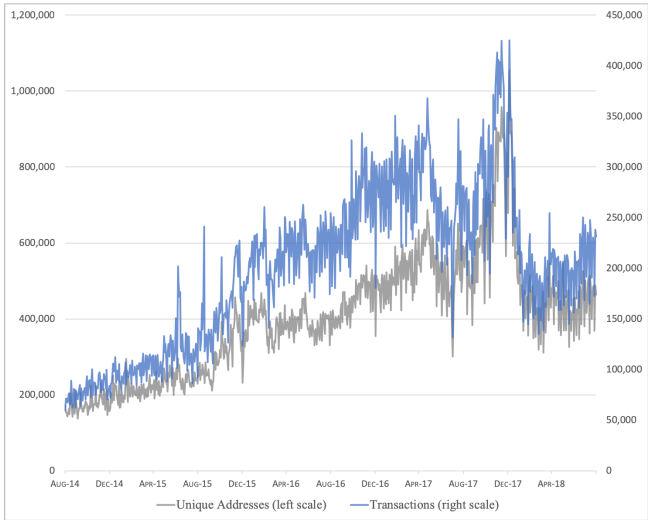
[31] Well-known laws in the modeling of networks include Sarnoff's function, $v \propto n$; Odlyzko's function, $v \propto n\log(n)$; and Reed's function, $v \propto 2^n$.

Figure 8. Bitcoin Network: Daily Unique Addresses and Number of Transactions (source: blockchain.com)

(a) Quadrennial Aug-2010 to Aug-2014



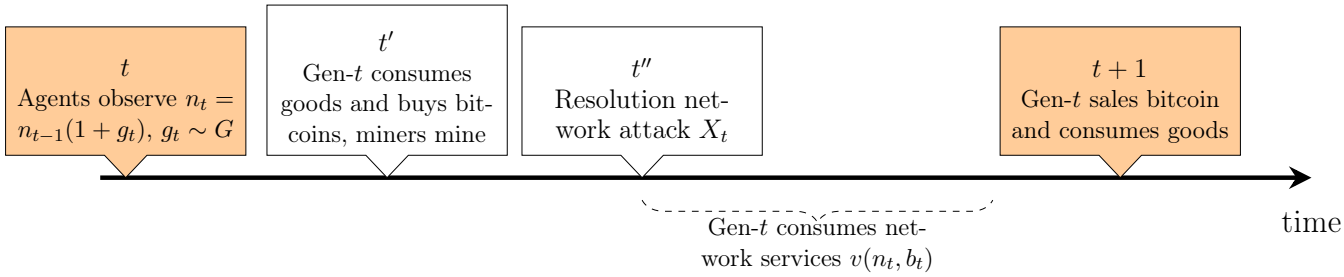
(b) Quadrennial Aug-2014 to Aug-2018



8 Network Size Shocks, Expectations, and Price Volatility

Section 7 shows how unity exacerbates bitcoin price volatility relative to an otherwise identical duality token, but focuses entirely on changes to stationary equilibria. To illustrate the consequences of unity on bitcoin price volatility more broadly, we consider an extension that adds a source of high-frequency stochasticity to the economy in the form of shocks to the network size. Intuitively, over a given period, the number of active participants in the network can fluctuate depending on factors such as time-varying intrinsic needs, as described in Section 1, news coverage, or the emergence of promising alternatives. One could use the total number of wallets as an imperfect measure of total participation at a point in time, as in Section 4, but such measure is less useful to capture active participation as it is nondecreasing and many addresses are used only once. Although it is challenging to fully characterize the fluctuations in Bitcoin participation, other proxies can be helpful. Figure 8 shows the evolution of two such proxies measured at the daily level: the number of unique addresses and the number of transactions in newly confirmed blocks. We can see that over a period such as quadrennial, these variables display significant fluctuations, suggesting that the size of the network might also subject to sizable positive and negative shocks.

Figure 9. Timeline with Stochastic Network Growth



We model network size shocks as follows. At the beginning of each period t, before decisions are made, the size of the newly born generation is drawn from the process $n_t = n_{t-1}(1+g_t)$, where $g_t \sim G$ and $\mathbb{E}_{t-s} g_t = 0$ for all $s > 0$. Users and miners learn about the realization of n_t and then make decisions as in Section 2. The timeline of the extension is illustrated in Figure 9. We simulate price paths that start from a given value $p_0 > 0$. In subsequent periods, based on information about n, the equilibrium in Definition 3 requires miners to set h optimally and network users to respect intertemporal rationality, as given by equation (9).

We develop the intuition for price formation in this setting. Starting from $b_0 = B_0 p_0$, agents expect b_1 next period to be equal to zero with probability $1 - \tau(H(b_0))$ or to be equal to b_1 with probability $\tau(H(b_0))$, where b_1 satisfies (9). Therefore, the self-fulfilling equilibrium price in period 1 is given by

$$p_1 = \frac{(1+\rho)\left[b_0 - \tau(H(b_0))\left(f(n_0)\right)^{1-\sigma} n_0^{\sigma} b_0^{1-\sigma}\right]}{\delta \tau(H(b_0)) B_1}.$$

If the network survives, there is a new young generation of size $n_1 = n_0(1+g_1)$ is observed at the beginning of period 1. The determination of p_2 therefore depends on the random shock g_1. Analogously, p_{t+1} must satisfy $p_{t+1} = \frac{1+\rho}{\delta \tau(b_t) B_{t+1}}\left[b_t - \tau(b_t)(f(n_t))^{1-\sigma} n_t^{\sigma} b_t^{1-\sigma}\right]$, where for $t > 0$, n_t depends on the realization of g_t. Because the network size varies with time, so does the diagram of the left-hand side of equation (9). Define $A(b, n_t) := b - \tau(b)\left(f(n_t)\right)^{1-\sigma} n_t^{\sigma} b^{1-\sigma}$. A positive realization of g_t shifts the graph of $A(\cdot, n_t)$ downward as it increases the value of network services and, everything else being constant, it lowers the expectation of b for next period. Intuitively, a higher network service value requires lower expected holding period returns in equilibrium. Conversely, a

negative realization of g_t shifts the graph of $A(\cdot, n_t)$ upward.

8.1 Simulating Price Paths

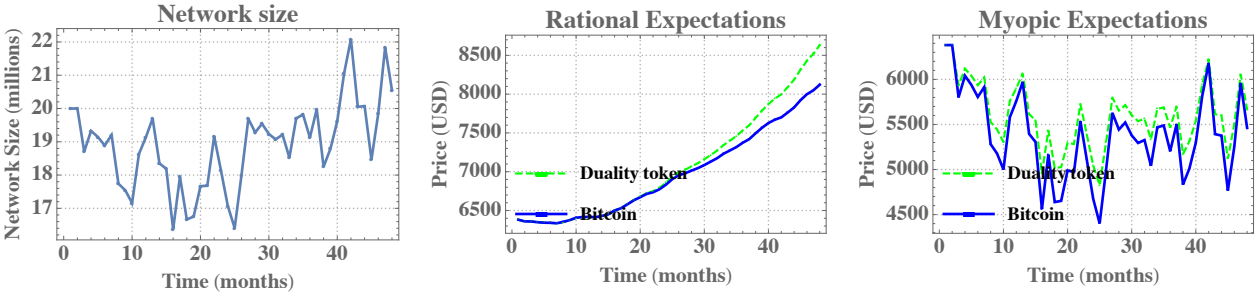
To initialize the algorithm, we use the baseline calibration values in Table II. Therefore, the value p_0 represents a unique regular stationary equilibrium and, in the absence of shocks, the value b_0, conditional on network survival, is constant (see the top panel of Figure 5). We set G to be uniform with support $[-0.1, 0.1]$. Based on these values, we simulate 48-month paths for network size and prices that are conditional on network survival. For Bitcoin, that period corresponds to that between supply growth adjustments. We simulate a partial and a general equilibrium price path $\left\{p_t^d, p_t^B\right\}_{t=0}^{48}$, labeled duality token and bitcoin, respectively. For the former, we use equation (3) and set a constant probability of attack success $1 - \tau_d = 1 - \tau\left(H(b_0)\right) = 0.02$. Each simulation path starts at $t = 0$ with identical prices and identical network security levels.

Figure 10 displays simulated time series. The left column corresponds to network size. The center column shows price paths that are consistent with rational expectations, as described above. To highlight the key role of belief formation, we also simulate paths considering agents with myopic expectations. These agents, shown in the right column, do not update beliefs taking innovations to network size into consideration. Instead, they expect prices to decline at a rate ρ over time, as in the initial stationary equilibrium.

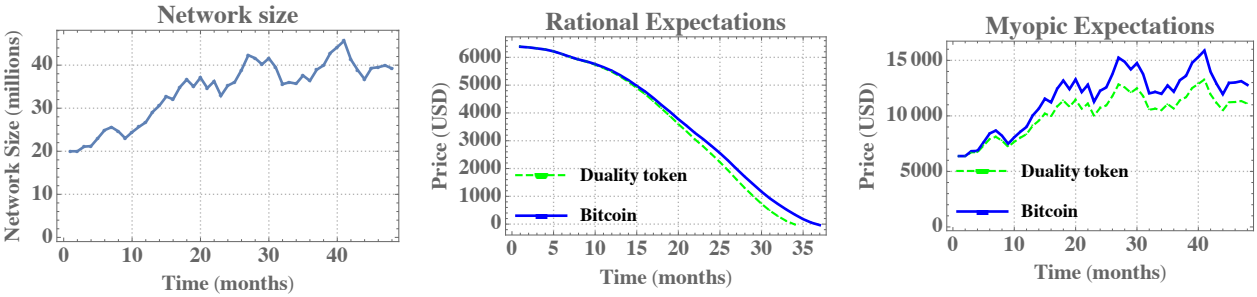
In Panel (a) of Figure 10, the initial fall in network size decreases the expected value of network services and shifts the graph of the function $A\left(\cdot, n_t\right)$ upward. Token prices must increase in order for holdings to be optimal. Note that the price increase is more pronounced for the duality token. Indeed, even though the network has fewer participants, rising bitcoin prices positively feeds back network security levels over time. Therefore, the *risk-adjusted* decline in service utility is less pronounced in general equilibrium. Panel (b) shows the opposite dynamics. The value of network services increases with network size and expected equilibrium prices decline. The price decline is more pronounced in the case of the duality token, since network security general equilibrium effects work in the opposite direction here, reducing bitcoin security over time. This fact requires higher

Figure 10. Stochastic Network Size and Dynamic Price Adjustments: Simulated Paths

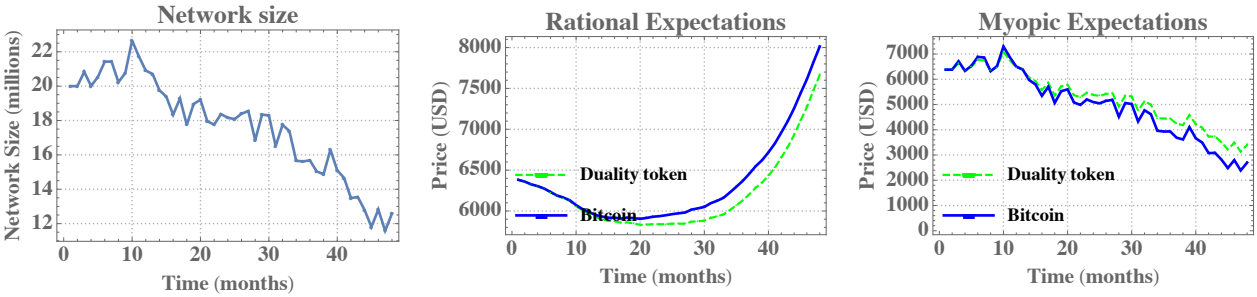
(a) A Divergent Rational Price Path



(b) A Convergent Rational Price Path



(c) A Rational Crash-boom Price Cycle



(d) A Rational Boom-crash Price Cycle

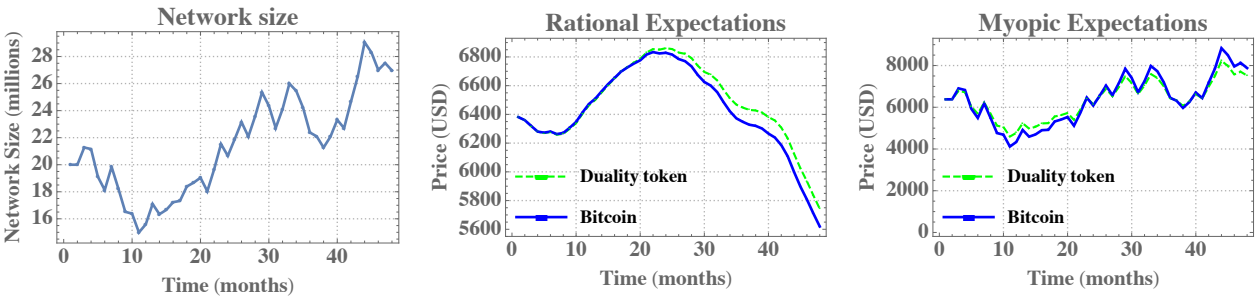
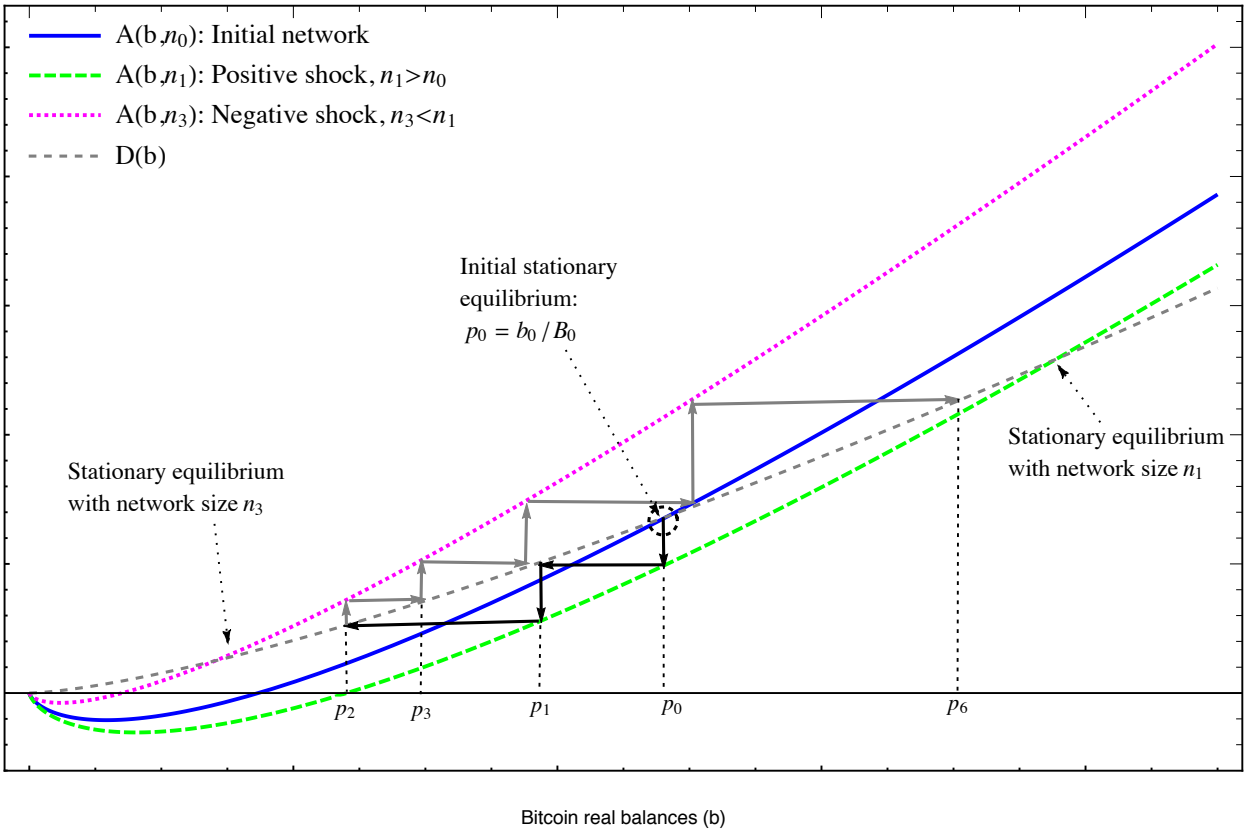


Figure 11. Bitcoin Price Adjustment to Network Size Shocks



bitcoin prices in equilibrium relative to the duality token's, which delays the converge of the bitcoin price to zero by 5 months.

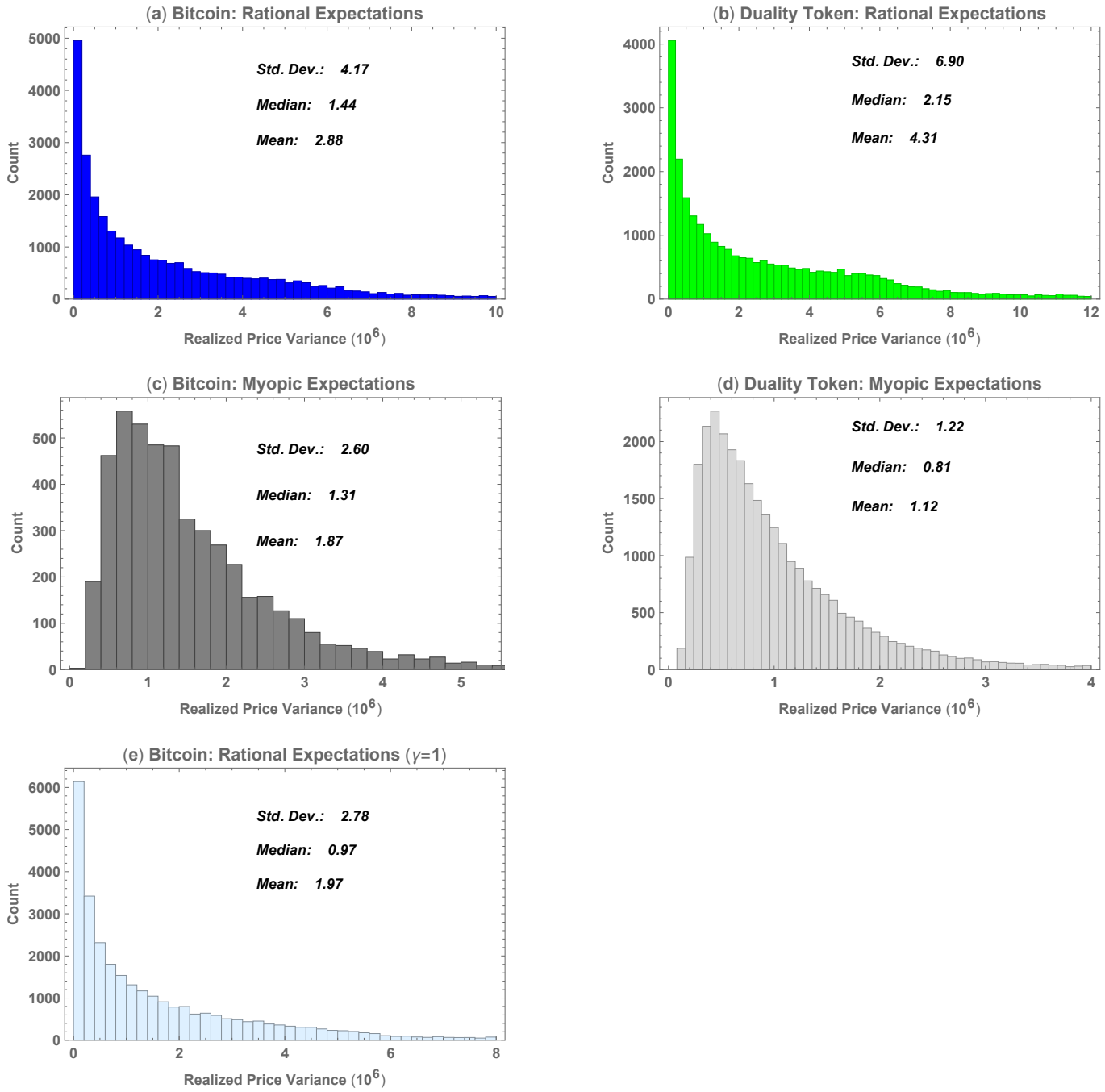
Taken together, note that the dynamic adjustment of prices away from the initial steady state has the duality token experiencing *larger price movements*, in contrast to the comparative static result in Proposition 7. The latter shows that network shocks are amplified by unity if one compares the value of *stationary equilibria balances* before and after the network size change. Outside stationary equilibrium paths, however, the general equilibrium consequences of unity could be the opposite, to moderate price swings.

Note that economies with myopic agents display strikingly different dynamics. The rightmost graph of Panel (a) of Figure 10 shows that the prices of both tokens decrease, reflecting worse demand fundamentals as the network size declines. However, the price decrease for bitcoin is more pronounced, since the negative demand-based shock feeds back lower hash rate supply and weaker

network security. In Panel (b), on the other hand, with an increasing network size the bitcoin price increases at a faster rate. The nonstationary dynamic price paths in this case, therefore, better resemble the steady-state implications of Proposition 7. Said differently, when agents do not revise their expectations relative to the initial stationary equilibrium, unity amplifies price volatility *both* in and out of the steady state.

We now analyze some exciting network size paths that generate momentum and reversals in dynamic price adjustment. Panel (c) of Figure 10, as Panel (a), displays a decreasing network size. However, there is a brief initial increase in n that, in contrast to Panel (a), sets token prices on a declining path for about 20 months. The persistent decline in the number of users eventually shifts price expectations upward, as in Panel (a). The combination of these effects induce a crash-boom cycle. The sequence of shocks is reversed in Panel (d) of Figure 10, and the price path displays a boom-crash cycle. Why do price adjustments with rational expectations display momentum and reversals? It is insightful to analyze the process of expectation adjustment for a network size that first increases and then declines.Figure 11 displays an economy that, at $t = 1$, receives a positive network size shock, $g_1 > 0$, driving the economy outside of the initial stationary equilibrium. Consistent with intertemporal rationality, the price decreases to $p_1 = \frac{b_1}{B_1}$. Given $g_2 = 0$, the price transitions next period to p_2. At time $t = 3$, a shock $g_3 < 0$ reduces the expected utility of network services, driving the function $A(\cdot, n_3)$ upward. At value b_2, $A(b_2, n_3) > D(b_2)$. Therefore, bitcoin holdings become less useful and, to compensate, the price must increase to a new equilibrium in which $p_3 > p_2$. The economy then shifts at time $t = 3$ from a decreasing to an increasing price path. We note that this type of pattern does not occur with a constant network size, as illustrated by Figure 5. Moreover, the intricate adjustments of price expectations displayed in the center column of Panels (c) and (d) of Figure 10 are in contrast with the myopic case of the graphs in the right column. For the latter, once again, prices move in tandem with network size shocks and price swings out of the steady state are amplified by unity.

Figure 12. Bitcoin Price Variance: Baseline Network Size Shocks



This figure shows, on the left column, simulation results for the bitcoin price variance and, on the right column, the price variance for an otherwise identical token with exogenous security level (duality token). Panels (a) and (b) correspond to the baseline model. Panels (c) and (d) correspond to a model with consumers displaying myopic expectations. Panel (e) is identical to (a) except for a linear mining cost function. Parameter values are described in Table II.

8.2 The Distribution of the Bitcoin Price Variance

To generalize this section's implications, we now use simulations characterize the conditional distribution of the bitcoin price variance. Panels (a) and (b) of Figure 12 show that, for the baseline model with rational expectations, the mean price variance value is *lower* for bitcoin than for the duality token that violates unity. Consistent with the intuition developed above, the unity property moderates the impact of network size shocks on expectations in equilibrium. Following a positive participation shock, network services become more valuable and an equilibrium requires a lower future price. In turn, the price decline induces lower network security, moderating the expected increase in network service utility. Analogously, following a negative participation shock, the general equilibrium induces an increase in network security and moderates the positive impact on price expectations.

Panels (c) and (d) of Figure 12 show that, for the version of the model with myopic agents, the mean price variance value is *higher* for bitcoin than for the duality token. Consistent with the intuition above, when agents do not revise their expectations on price changes, positive network participation shocks induce higher network utility and higher prices. Moreover, in the general equilibrium, the resulting increase in network security amplifies the size of the upward bitcoin price movement.

For robustness, Panel (e) of Figure 12 shows the distribution of the bitcoin price variance with an alternative, linear mining cost function (A3a with $\gamma = 1$).[32] We can see that the qualitative relation between bitcoin and the duality token in Panel (b) is the same. The change in network supply elasticity widens the gap between the mean values of price variance. The implications here are also robust to alternative values of network participation shock variance as illustrated in Figures B2 and B3 in Appendix B.

Overall, the model extension analyzed in this section highlights the fact that general equilibrium effects are essential to understanding the evolution of bitcoin prices outside of a steady state and the bitcoin price variance more broadly. Moreover, the dynamic process of price adjustment can be

[32]The cost function parameter is calibrated so that the initial price p_0 is also a regular stationary equilibrium.

remarkably different, depending on the process of belief formation. We have considered the extreme opposites of rational and myopic expectations. It would be interesting for future research to analyze alternative belief processes and the role of learning.

9 Purely Speculative Bitcoin Bubbles

When utility is transferable among agents, that is, under A1a, Sections 2 and 4 show that no stationary equilibrium exists if bitcoins yield no transactional value. This section characterizes the conditions under which such a purely speculative bubble equilibrium exists and shows that multiple bubble-like equilibria can be found.

Consider the environment of Section 2 with the following characteristics. Let $u(c,v) = u(c)$, where u is a strictly concave function and $\lim_{c\to} u'(c) = \infty$. Let e_1 and e_2 represent the nonstochastic endowments that the young and old generations receive, respectively, at the beginning of each period t. The unconstrained optimization problem can be written as

$$\max{}_{B_{it}} \mathbb{E}_t \left[u\left(e_1 - B_{it} p_t^B\right) + \delta x_t u\left(e_2 + B_{it} p_{t+1}^B\right)\right]. \tag{14}$$

In an interior solution, optimal holdings must satisfy

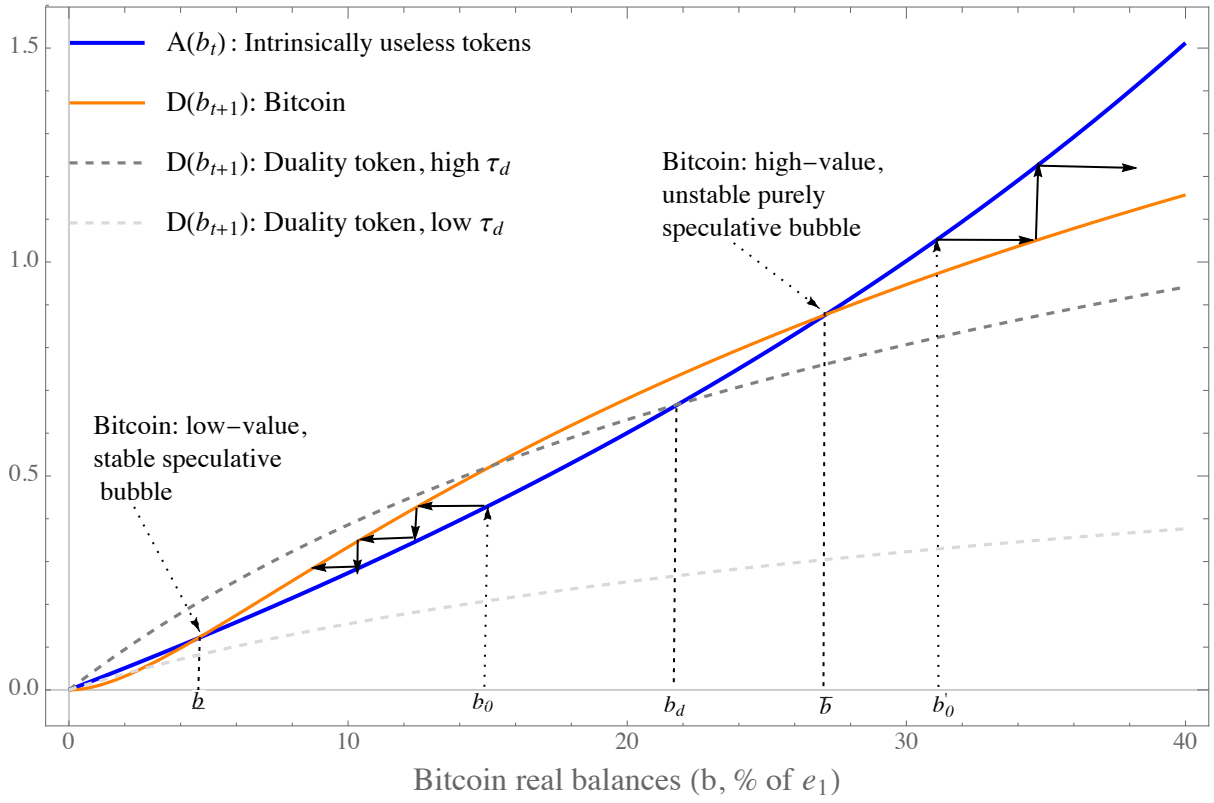
$$u'\left(e_1 - B_{it} p_t^B\right) p_t^B = \delta \tau_t \mathbb{E}_t u'\left(e_2 + B_{it} p_{t+1}^B\right) p_{t+1}^B.$$

Given $b_t = p_t^B B_{it}$, we can summarize the optimality conditions using the following difference equation:

$$u'\left(e_1 - b_t\right) b_t = \frac{\delta \tau_t}{1+\rho} u'\left(e_2 + \frac{b_{t+1}}{1+\rho}\right) b_{t+1}, \tag{15}$$

and $b_t \leq e_1$. We represent the left- and right-hand sides of equation (15) by $A(b_t) := b_t u'(e_1 - b_t)$ and $D(b_{t+1}) := \frac{\delta}{1+\rho}\tau_t u'\left(e_2 + \frac{b_{t+1}}{1+\rho}\right) b_{t+1}$, respectively. In the partial equilibrium case of duality tokens, as in Section 2.3, $\tau_t = \tau_d$. In the general equilibrium case of Bitcoin, as in Section 4.1,

Figure 13. Stationary Equilibria: The Case of Pure Speculation



$\tau_t = \tau\left(H_t\left(p_t^B\right)\right)$.

Consider the case of duality tokens for which the probability of network survival is exogenous. Under the assumption that u is such that the interest rate elasticity of savings is nonnegative when $\tau_d \to 1$, so that D is an increasing function of b in $(0, e_1)$, Weil (1987) shows that a positive stochastic bubble exists and it is unique if and only if the economy is dynamically inefficient and τ is sufficiently high. In this setting, an analogous stationary equilibrium requires that the no-trade interest rate $R := \frac{u'(e_1)}{\delta u'(e_2)}$ be lower than one and that the probability of network survival τ_d satisfy $\frac{\tau_d}{1+\rho} > R$, so that the inflation-adjusted return on the bubble is not lower than the no-trade interest rate.

Figure 13 displays the function $A(b_t)$ and the functions $D(b_{t+1})$ for two duality tokens. In the first case (dark gray line), τ_d is high and a stationary bubble $b_d > 0$ satisfying $A(b_d) = D(b_d)$ exists. Paths originating at b values to the left of b_d, such as b_0, imply that $b_t \to 0^+$ as $t \to \infty$. Paths

originating at b values to the right of b_d, such as b_0', imply that b_t grows unboundedly as $t \to \infty$, which is infeasible, given that the budget constraint of young consumers requires $b_t < e_1$ for all t. In the second case (light gray line), τ_d is too low and there is no long-term equilibrium in which the real value of the token is positive.

The previous cases do not capture the general equilibrium interactions between price and network security that are intrinsic to Bitcoin. Even when network transactional services are not present, the properties of technology primitives (τ, C) can give rise to one or more positive bubble equilibria with different dynamic properties. Figure 13 illustrates this for the case of linear mining costs (A3a, $\gamma = 1$) and rational security function (A2c). For a value $b \approx 0$, network security is approximately zero, implying that $A(b) > D(b) \approx 0$. Network security increases with b, but at a nonconstant rate. If the rate of increase in τ is sufficiently high for low values of b, a stationary equilibrium exists $\underline{b} > 0$ exists and, unless D is tangent to A at $\underline{b}$, it must have D intersecting A from below. As the rate of τ increase is declining, and $u'(e_1 - b)$ is increasing in b, the highest value stationary equilibrium must be found at a point $\overline{b}$ with D intersecting A from above.

As in Section 4, we find that the low-value stationary equilibrium is dynamically unstable. Therefore, even when no transactional services exist, one can find an arbitrarily large number of price paths that converge to $\underline{b}$, such as the path that starts at b_0. On the other hand, the only price path that is consistent with $\overline{b}$ is the one that starts at $\overline{b}$. As in the case of exogenous network security, paths originating at b values to the right of $\overline{b}$, such as b_0', imply that b_t grows unboundedly as $t \to \infty$, which is infeasible, given that the budget constraint of young consumers. In contrast to the previous case, if $\overline{b}$ were the starting point, a negative shock would dynamically drive the economy not to a price of zero but to a low–value bubble. The unity property, therefore, rationalizes a price path were the bubble *deflates* but does not *burst*.

Overall, the analysis of the endowment economy in this section shows that the existence of multiple stationary equilibria in which bitcoins are valued does not rely on the quasi-linear utility specification of Section 2 or A1a or A1b. It also highlights the importance of modeling the interaction between the demand and the supply sides of the Bitcoin system, even in the absence of network

effects.

10 A Discussion of Implications

In this section, we provide further perspective on the model empirical implications and discuss potential limitations and extensions.

10.1 Prices, Mining, and Hash Rate

A direct empirical implication of the analysis in Section 4 is that bitcoin prices and the network hash rate are positively related in the general equilibrium. We have argued that such positive relation stems from the interaction of two factors. First, consumers value network security, which increases in the system hash rate. Second, miners' supply positively respond to the value of the network token. The long-term evolution of these key quantities in the Bitcoin network, as displayed in Figure 1, provide strong support to this prediction. To further assess the implied relation between prices and hash rate, we investigate its behavior in the second most important PoW chain by market capitalization, Ethereum. Figure 14 shows the evolution of the Ethereum hash rate and the price of the native token, ether. Despite the shorter history of the Ethereum network relative to Bitcoin, one also observes a strong positive relation between the market price and the system hash rate.

An additional fact that provides supports to the notion that consumers value network security is that Bitcoin remains the most actively used network despite the availability of many alternative blockchains with essentially the same open source code and design, but with significantly lower transactions fees and hash power. Examples include Bitcoin clones (e.g., Litecoin) and forks of the original Bitcoin chain (e.g., Bitcoin Gold). If consumers did not value network security, it is unclear why they would not coordinate around the use of a cheaper-to-operate network.

We briefly comment on the supply-side assumptions potential limitations, as follows.

Miner Size. Proposition 2 considers competition among identical miners. Consequently, the system hash rate is a sufficient statistic for network decentralization. Of course, this is not without

Figure 14. Ether Price and Ethereum Hash Rate: August 2015 to August 2018 (source: etherscan.io and coinmarketcap.com)

loss of generality. If, on the other hand, the system had large and small miners, modeling network security would be more complex. In particular, one may consider a more sophisticated mapping τ that depends both on the aggregate value and the distribution of hash rate among miners. The considered simplification is reasonable, provided there are sufficient noncolluding mining operations of similar installed capacity. Arguably, collusion in Bitcoin is difficult with strict free entry of competing miners who are not forced to disclose identities. Besides collusion, the analysis of mining pools by Cong, He, and Li (2018) suggest an interesting intrinsic mechanism by which large pools find incentives to adjust their fees to prevent high levels of centralization.

Difficulty Adjustments. Mining difficulty in the Bitcoin network is determined approximately every two weeks (2016 ten-minutes blocks) as a function of the average block confirmation time over that two-week period. Therefore, the difficulty level is constant in the short run (within two weeks) but not over an extended period. In the model's characterization of mining revenue, the PoW race has one winner per period regardless of the total amount of hash rate. Therefore, we implicitly

assume that mining difficulty adjusts to create block confirmations at regular time intervals.[33] One limitation of this assumption is that price–hash rate dynamics within difficulty adjustments might not be well captured in times of high volatility. For example, in August 2017, several Bitcoin miners moved their hash power to mine Bitcoin Cash, a newly created chain. Therefore, the pace of Bitcoin block confirmations slowed momentarily until the difficulty level dropped two weeks later. Modeling high-frequency dynamics thus requires difficulty levels that are fixed in the short run and adjusting the revenue function to account for the time-varying probability of a block confirmation within difficulty adjustments.

Entry. The number of miners is a primitive here. Of course, one can extend the model to incorporate a miner entry stage that precedes the equilibrium price determination. For example, one could consider a given entry cost κ and solve for the equilibrium number of entrants using a zero-profit entry condition. Thereby, instead of studying the general equilibrium implications of exogenous changes in m, such as those driven by unanticipated regulatory shocks, one can study the effects of changes in κ. Because a lower κ intuitively leads to a greater m, the effects of increasing m or lowering κ should be similar. Thus, one does not seem to gain additional insights by endogenizing m. If the cost of entry were time varying, such an extension could enhance the analysis of price volatility.

10.2 Network Attacks

Well-known potential attacks include fraud, for example, double-spending, as described by Nakamoto (2008), and service denial, a form of censorship. Theoretical attacks include "selfish mining" (Eyal and Sirer (2013)) and "sabotage attacks" (for a discussion, see Budish (2018a)). As of yet, no successful large-scale attacks against Bitcoin have been recorded and, therefore, a full empirical description is not available.[34] However, a precedent is given by a sequence of double-spending attacks

[33] In the Ethereum network (Metropolis release), difficulty levels are recomputed with every new block. As of August 2018, the average block confirmation time in the Ethereum network was within 14–15 seconds.

[34] There are a few well-known episodes where the perceived Bitcoin network security was compromised, with immediate adverse valuation effects. These include the March 11, 2013 6-hour fork that created lack of consensus in the network and an instant 24 percent drop in price (for a discussion, see https://bitcoinmagazine.com/articles/bitcoin-

TABLE III
Majority Hash Rate Attacks to PoW Blockchains: Examples

Token Name	Symbol	Month of the attack	Begin-month price (satoshis)	End-month price (satoshis)	Return (BTC)	Begin-month price (USD)	End-month price (USD)	Return (USD)
Bitcoin Gold	BTG	May 2018	787,000	576,600	-26.73%	71.46	42.90	-39.97%
Verge	XVG	May 2018	877	512	-41.62%	0.0794	0.0385	-51.51%
Monacoin	MONA	May 2018	55,540	43,970	-20.83%	5.05	3.30	-34.65%
ZenCash	ZEN	June 2018	407,000	278,000	-31.70%	30.45	17.73	-41.77%

Source: Prices are from Coinmarketcap.com. Attacks periods are from Coindesk.com and several media sources. Begin-month (end-month) prices correspond to the first day of the attack month (following month). Returns correspond to the same calendar month return. One BTC equals 100 million satoshis.

to Bitcoin Gold in May 2018 that allegedly generated up to USD 18 million for the attacker.[35] Measured in bitcoins, Bitcoin Gold displayed on that month a price drop of 27% (40% in measured in USD). Table III shows additional examples of majority hash rate attacks to PoW cryptocurrencies.

If a malicious attacker had access to the majority of the network hash power, one could envision additional events that would be likely to induce a sudden panic and an even stronger price crash. For example, the attacker could mine empty blocks for a long period, effectively denying service to network users. A second example would be if the attacker used her hash power to generate multiple persistent forks to the blockchain, thereby creating confusion and undermining consensus.

Implications for Attack Incentives. The unity property *moderates* the impact of *for-profit hacking*. Consider, for instance, a potential hacker with the ability to compromise the network's security and double-spend a nominal amount of bitcoins, B. Any attempt to double-spend a fraction ξB could be regarded as a network attack by other participants, thereby reducing both the bitcoin price and the value of the residual stock $(1-\xi)B$. Importantly, in the extreme case in which a hacker were able to compromise the cryptographic security of the network and steal other users' bitcoins, the hacker might not find an incentive to do so on a large scale, since, otherwise, the price of the token would immediately go to zero, rendering the hacking effort unprofitable. It is worth

network-shaken-by-blockchain-fork-1363144448).

[35] For a discussion, see http://fortune.com/2018/05/29/bitcoin-gold-hack/. Regarding the Ethereum blockchain, the most important documented event is the DAO hack in June 2016, which produced a day's drop of more than 30% in the price of ether (e.g., see www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html).

noting that no such general equilibrium effects exist for physical alternatives to bitcoin like cash or gold. On the other hand, an attacker could combine some form of system sabotage with a derivative position that increases in value if the bitcoin price decreases, such as a long put option. It is not clear that the unity property would moderate such type of attack.

It seems important to highlight that the implications of Proposition 7 for the security of unity assets should be interpreted with caution, that is, as an everything else being constant result against an idealized counterfactual token. In particular, the results do not imply that duality tokens are unconditionally more stable or secure. First, what determines the actual security level τ_d of a duality token, such as XRP, or even a potential central bank–sponsored token, is outside of the model. The enormous increase in the bitcoin hash rate in recent years shown in Figure 1 suggests that the current security levels achieved by Bitcoin are very costly to replicate for any network. Second, the environment here accounts for aggregate security risks and not for individual-level censorship risk. Arguably, the decentralized consensus model of Bitcoin offers better protection against service denials than the considered alternatives. Third, unlike enterprise or government networks, the market for Bitcoin security embeds the free entry of current and future competitors, ceteris paribus, increasing the total provision of security resources. Finally, it would be inappropriate to apply Proposition 7 to a unity and a duality token that exist in the same DN and are thus intrinsically connected (e.g., ether and ERC-20 tokens). We leave the characterization of the security of multiple-token networks for future research.

10.3 Further Implications for Price Dynamics and Volatility

Price Momentum, Booms, and Crashes. The empirical evidence by Liu and Tsyvinski (2018) suggests that price momentum is one of the most important factors that explain risk-return behavior for bitcoin. Our model rationalizes momentum in bitcoin prices as the outcome of distinct forces. The simplest source of such dynamic pattern is the perturbation of regular stationary equilibria (Definition 4) which are dynamically unstable, as illustrated in the top panel of Figure 5. This source is common to tokens that do not satisfy unity (e.g., Ripple's XRP) as illustrated in Figure

4. The extension in Section 8 shows that both types of tokens can display periods of mania and crashes as a function of shocks to network participation, a fact that is also consistent with the importance of the empirical proxies for investor attention that Liu and Tsyvinski consider. Perhaps surprisingly, these patterns in the model arise even when participation shocks are i.i.d. and are the result of rational equilibrium outcomes.

The unity property can rationalize other type of momentum patterns that are not observed for tokens such as XRP. Even when the network size is constant, for example, bitcoin prices can endogenously recover after sudden crashes. On example of such dynamic pattern is illustrated by the bottom panel Figure 5: If the economy starts at the low stationary equilibrium value $\underline{b}$, a sudden crash to b_0 is followed by progressive price recovery due to the endogenous response of miners analyzed in Sections 3 and 4. A second example is found for economies where all tokens are purely speculative and serve no transactional purpose. Indeed, the unity property can rationalize a deflating bitcoin bubble illustrated by the transition from a high- to a low-value bubble in Figure 13 that follows a negative shock.

Policy Bans and Volatility. The role played by network size shocks in the presence of price–security feedback effects seem important to explain the significant volatility of bitcoin prices. Changes in expectations about regulatory policies affecting future network size, for example, could have direct implications on the current equilibrium valuation. Moreover, the price changes could be dramatic if, in turn, policy shocks induce a spike in risk aversion driven by the fear of regulation. A further implication of the unity property is that the impact of regulatory restrictions in countries with large numbers of miners, such as those undertaken by the People's Republic of China in 2017–2018, is likely of greater significance than that in countries with a similar numbers of users but a smaller number of miners, such as the United Kingdom.

11 Concluding Remarks

We have modeled a tractable DN economy where the evolution of prices and the security of the network can be jointly analyzed. Despite its simplicity, the setting yields insightful implications for the equilibrium relation between the demand and the supply sides of the bitcoin market. Because the most critical general equilibrium predictions are a consequence of unity, we believe that our results can be helpful in understanding the market for other network assets that satisfy this property, and those for which network's consensus relies on PoW more specifically.

To focus on the critical valuation mechanism and keep the analysis tractable, we have made several simplifying assumptions such as restricting the space of available networks to a singleton. More generally, consumers face choices between various centralized and decentralized financial networks, including those operated by central banks and many digital alternatives to bitcoin, with distinct security models and subject to different types of regulations. We certainly do not claim that the trade-offs associated to these consumer choices are irrelevant for valuation and welfare assessments. To the contrary, such an analysis seems indeed necessary to better understand the future of monetary policy. We do argue, however, that the building blocks of our model can be helpful in analyzing the equilibrium interaction of prices, the provision of security resources, and censorship risks in more complex environments.

References

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

Alvarez, F. and F. Lippi (2009). Financial Innovation and the Transactions Demand for Cash. *Econometrica 77*(2), 363–402.

Antonopoulos, A. M. (2016). *The Internet of Money* (Volume 1 ed.). Merkle Bloom LLC.

Antonopoulos, A. M. (2017). *Mastering Bitcoin: Programming the Open Blockchain* (2nd ed.). Sebastopol: O'Reilly.

Asness, C. S., T. J. Moskowitz, and L. H. Pedersen (2013). Value and Momentum Everywhere. *Journal of Finance 68*(3), 929–985.

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

Benhabib, J., T. Schmitt-Grohe, and M. Uribe (2001). Monetary policy and multiple equilibria. *American Economic Review 74*(2).

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta (2018). The Blockchain Folk Theorem. *TSE Working Paper*.

Blanchard, O. J. (1979). Speculative Bubbles, Crashes and Rational Expectations. *Economics Letters 3*, 387–389.

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

Brock, W. A. (1974). Money and Growth: The Case of Long Run Perfect Foresight. *Journal of Economic Dynamics and Control 15*(3), 750–777.

Budish, E. (2018a). The Economic Limits of the Blockchain (in 3 Equations). pp. 1–16.

Budish, E. B. (2018b). The Economic Limits of Bitcoin and the Blockchain. *U. of Chicago Working Paper*.

Catalini, C. and J. S. Gans (2018). Initial Coin Offerings and the Value of Crypto Tokens. *MIT Working Paper*.

Choi, K. J., A. Lehar, and R. Stauffer (2018). Bitcoin Microstructure and the Kimchi Premium. *U. of Calgary Working Paper*.

Cong, L. W. and Z. He (2018). Blockchain Disruption and Smart Contracts. *U of Chicago Working Paper*.

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

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

Cournot, A. A. (1897). *Researches into the Mathematical Principles of the Theory of Wealth*. London: Macmillan.

Easley, D. and J. Kleimberg (2010). *Networks, Crowds, and Markets*. New York: Cambridge University Press.

Easley, D., M. O'Hara, and S. Basu (2018). From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Cornell U. Working Paper*.

Economides, N. (1996). The Economics of Networks. *International Journal of Industrial Organization 14*(6).

Eyal, I. and E. G. Sirer (2013). Majority is not Enough: Bitcoin Mining is Vulnerable. *Cornell U. Working Paper*.

Feenstra, R. C. (1986). Functional Equivalence Between Liquidity Costs and the Utility of Money. *Journal of Monetary Economics 17*(2), 271–291.

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

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

Friedman, M. (1969). The Optimum Quantity of Money. In *The Optimum Quantity of Money and Other Essays*. Aldine Publishing Company.

Fung, B. S. C. and H. Halaburda (2016). Central Bank Digital Currencies: A Framework for Assessing Why and How. *Bank of Canada Staff Discussion Paper*.

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

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

Huberman, G., J. D. Leshno, and C. Moallemi (2017). Monopoly Without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *Columbia U. Working Paper*.

Katz, M. L. and C. Shapiro (1985). Network Externalities, Competition and Compatibility. *American Economic Review 75*, 424–440.

Kiyotaki, N. and R. Wright (1989). On Money as a Medium of Exchange. *Journal of Political Economy 97*, 927–54.

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

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

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

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

Ljungqvist, L. and T. J. Sargent (2018). *Recursive Macroeconomic Theory* (4th ed.). Cambridge, MA: The MIT Press.

Makarov, I. and A. Schoar (2018). Trading and Arbitrage in Cryptocurrency Markets. *Working Paper*.

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

Manuelli, R. (1990). Existence and Optimality of Currency Equilibrium in Stochastic Overlapping Generations Models: The Pure Endowment Case. *Journal of Economic Theory 51*(2), 268–294.

Metcalfe, B. (2013). Metcalfe's Law after 40 Years of Ethernet. *IEEE Computer Society 46*(12), 26–31.

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

Obstfeld, M. and K. Rogoff (1986). Ruling Out Divergent Speculative Bubbles. *Journal of Monetary Economics 17*, 349–362.

Pagnotta, E. S. and A. Buraschi (2018). An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. *Imperial College London Working Paper*.

Pagnotta, E. S. and T. Philippon (2018). Competing on Speed. *Econometrica 86*(3), 1067–1115.

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

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

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

Saleh, F. (2018). Blockchain Without Waste: Proof-of-Stake. *McGill U. Working Paper*.

Samuelson, P. A. (1958). An Exact Consumption-Loan Model of Interest with and without the Social Contrivance of Money. *Journal of Political Economy 66*(6), 467–482.

Sargent, T. J. and N. Wallace (1983). A Model of Commodity Money. *Journal of Monetary Economics 12*(1), 163–187.

Schilling, L. and H. Uhlig (2018). Some Simple Bitcoin Economics. *Becker Friedman Institute Working Paper No 2018-21*.

Sims, C. A. (2013). Paper Money. *American Economic Review 103*(2), 563–584.

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

Szabo, N. (1994). Smart Contracts: Building Blocks for Digital Markets. *Extropy 16*.

Tirole, J. (1985). Asset Bubbles and Overlapping Generations. *Econometrica 53*(6), 1499–1528.

Velde, F. R. and W. E. Weber (2000). A Model of Bimetallism. *Journal of Political Economy 108*(6), 1210–1234.

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

Weil, P. (1987). Confidence and the Real Value of Money in an Overlapping Generations Economy. *The Quarterly Journal of Economics 102*(1), 1–22.

Wheatley, S., D. Sornette, T. Huber, M. Reppen, and R. N. Gantner (2018). Are Bitcoin Bubbles Predictable? Combining a Generalized Metcalfe's Law and the LPPLS Model. *ETH Zurich Working Paper*.

Wood, G. (2018). Ethereum: a Secure Cecentralised Generalised Transaction Ledger. *Ethereum Project Yellow Paper*.

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

Online Appendix to "Bitcoin as Decentralized Money: Prices, Mining, and Network Security"

Emiliano Pagnotta

Imperial College London

Appendix A Notation

- n_t: number of network participants at time t
- m: number of miners
- v: network service flow (in units of the consumption good)
- p^B: bitcoin price
- B: supply of bitcoins, where B_{t-1} is the supply at the beginning of period t (before mining) and B_t is that in period t (after mining)
- B_i: consumer's i's bitcoin holdings (nominal balances)
- b_i: consumer's i's bitcoin holdings (real balances)
- ρ: inflationary reward parameter (ρB is the Coinbase reward)
- τ: network security
- h_j: hash rate provided by miner j. $H = \sum_j h_j$ is the system hash rate
- ϕ: resistance to attack parameter
- u: Bernoulli utility
- σ: curvature parameter of u
- f: network effects' function
- δ: time discount parameter
- C: mining cost function

Appendix B Supplemental Figures

Figure B1. Stationary Bitcoin Balances and Network Size: General Equilibrium

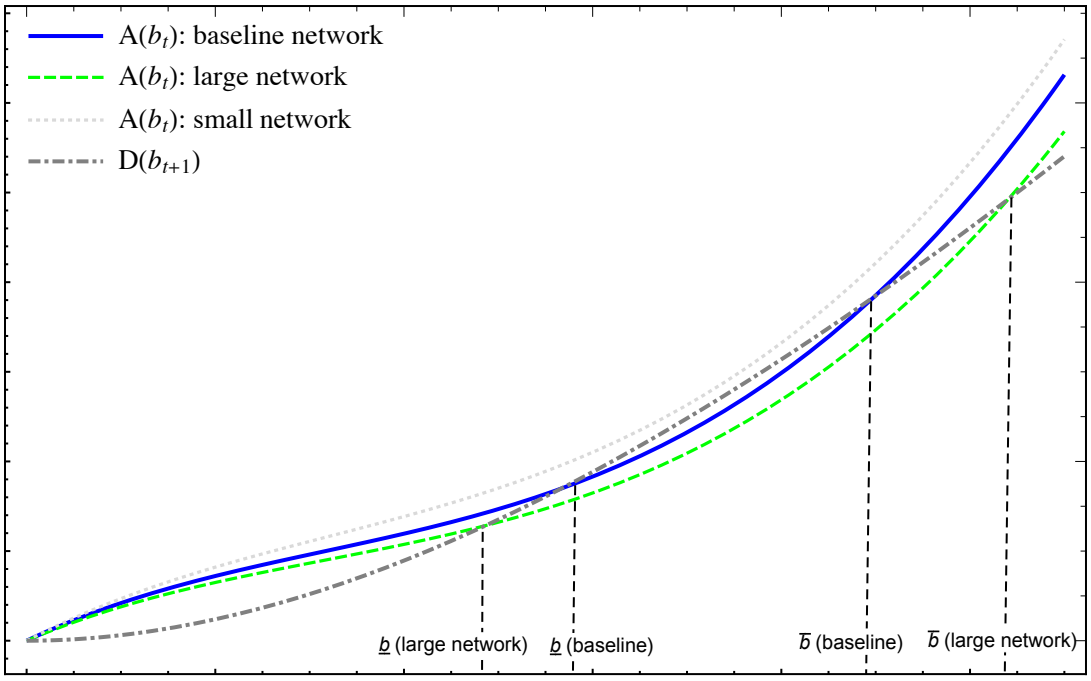
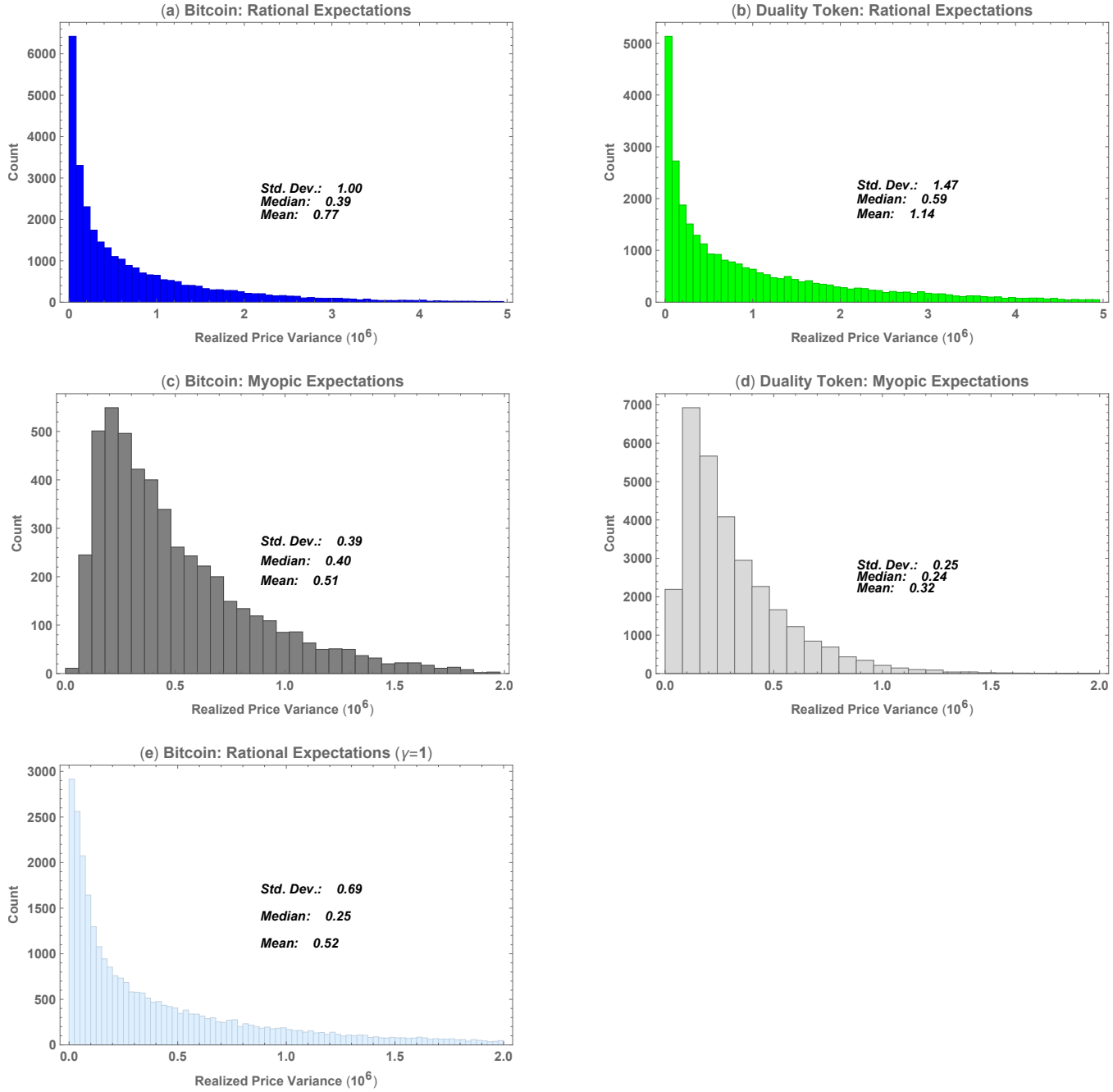
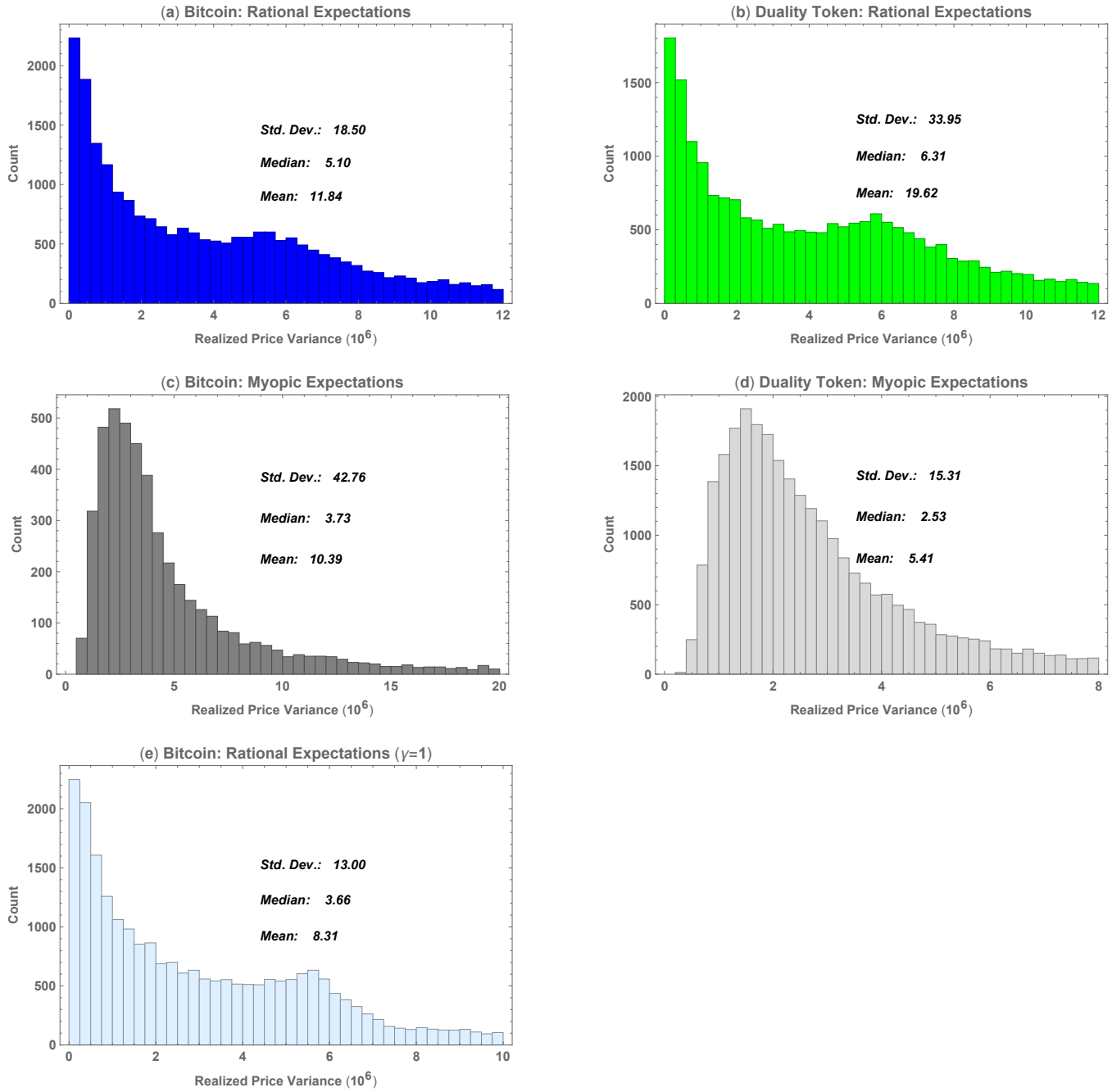


Figure B2. Realized Bitcoin Price Variance: Small Network Size Shocks ($g = 0.05$)



This figure shows, on the left column, simulation results for the bitcoin price variance and, on the right column, the price variance for an otherwise identical token with exogenous security level (duality token). Panels (a) and (b) correspond to the baseline model. Panels (c) and (d) correspond to a model with consumers displaying myopic expectations. Panel (e) is identical to (a) except for a linear mining cost function. Parameter values are described in Table II.

Figure B3. Realized Bitcoin Price Variance: Large Network Size Shocks ($g = 0.2$)



This figure shows, on the left column, simulation results for the bitcoin price variance and, on the right column, the price variance for an otherwise identical token with exogenous security level (duality token). Panels (a) and (b) correspond to the baseline model. Panels (c) and (d) correspond to a model with consumers displaying myopic expectations. Panel (e) is identical to (a) except for a linear mining cost function. Parameter values are described in Table II.

Appendix C Proofs

Proof of Proposition 2

Part (i). We simplify the notation using $B_{t-1} = B$ and $p_t^B = p^B$. Miner j takes the price as given and solves $\max_{h_j} B\rho p^B \times \pi(h_j, h_{-j}) - C(h_j)$, with first-order condition $B\rho p^B \frac{\partial \pi(h_j,h_{-j})}{\partial h_j} = C'(h_j)$. Using $\frac{\partial \pi(h_j,h_{-j})}{\partial h_j} = \frac{H-h_j}{H^2}$, we obtain $B\rho p^B = \frac{C'(h_j^*)H^2}{H-h_j^*}$. With symmetric identical miners, $h_j = h_k$, for any j and k, so the equilibrium symmetric hash rate satisfies $C'(h^*)h^* = B\rho p^B \frac{m-1}{m^2}$.

Parts (ii) to (v) can be proven by applying the implicit function theorem to express the near-equilibrium response in h^* for each parameter change. For (ii), we have $\frac{dh^*}{dp^B}[C'(h^*) + h^*C''(h^*)] - B\rho\frac{m-1}{m^2} = 0$. Since $H^* = mh^*$, then $\frac{dH^*}{dp^B} = \frac{B\rho\frac{m-1}{m}}{C'(h^*)+h^*C''(h^*)} > 0$. For (iii), to simplify the exposition and without much loss of generality, we assume $m \geq 2$ to be a continuous variable. From $H^* = mh^*$, it follows that $\frac{dH^*}{dm} = h^* + m\frac{dh^*(m)}{dm}$. From totally differentiating the first-order condition, we have $\frac{dH^*}{dm} = h^* - \frac{(m-2)}{m^2}\frac{B\rho p^B}{(C'+h^*C'')}$, which implies that

$$\begin{aligned}\frac{dH^*}{dm}C'(h^*) &= h^*C'(h^*) - \left(\frac{m-2}{m-1}\right)\left(\frac{m-1}{m^2}\right)B\rho p^B\frac{C'(h^*)}{(C'(h^*)+h^*C''(h^*))},\\ &= h^*C'(h^*)\left(1 - \left(\frac{m-2}{m-1}\right)\left(\frac{C'(h^*)}{(C'(h^*)+h^*C''(h^*))}\right)\right),\end{aligned} \tag{16}$$

where the second equality relies on the equilibrium relation 5. Note that $C'(h^*) > 0$, $\frac{m-2}{m-1} < 1$ and, by $C'' \geq 0$ and $h^* \geq 0$, $\frac{C'}{C'+h^*C''} \leq 1$. Therefore, the right-hand side of equation (16) is positive and we conclude that $\frac{dH^*}{dm} > 0$. For (iv), differentiation of the first-order condition yields $\frac{dh^*}{d\rho} = Bp^B\frac{m-1}{m^2}[C'(h^*) + h^*C''(h^*)]^{-1} > 0$. For (v), note that, if C' marginally increases pointwise for every h, then $dh^* < 0$ to satisfy equation (5) and $dH^* < 0$. □

Proof of Proposition 3

Under A1*a* and A1*b*, the unconstrained optimization problem can be written as

$$\max_{B_{it}} \mathbb{E}_t\left[-B_{it}p_t^B + x_t\frac{\left(f(n_t)p_t^B B_{it}\right)^{1-\sigma}}{1-\sigma} + x_t\delta B_{it}p_{t+1}^B)\right]. \tag{17}$$

Given the distribution of x_t, the solution to (17) is the same as the solution to

$$\max_{B_{it}}\left[-B_{it}p_t^B + \tau(H_t)\left(\frac{\left(f\left(n_t\right)p_t^B\right)^{1-\sigma}B_{it}^{1-\sigma}}{1-\sigma} + \delta\mathbb{E}_t B_{it}p_{t+1}^B\right)\right].$$

In an interior solution, the first-order condition implies that

$$\tau(H_t)\left(f\left(n_t\right)^{1-\sigma}\left(p_t^B\right)^{1-\sigma}B_{it}^{-\sigma}+\delta\mathbb{E}_t p_{t+1}^B\right)=p_t^B.$$

If $f(n)=0$, then the equilibrium price is $p_t^B=\tau\left(H\left(p_t^B\right)\right)\delta\mathbb{E}_t p_{t+1}^B$, as in equation (8). If $f(n)>0$, using the symmetric asset market clearing condition, $B_{it}n_t=B_t$, the supply law of motion, $B_t=B_{t-1}\left(1+\rho\right)$, and, rearranging, one obtains expression (7). □

Proof of Proposition 4

For (i), note that, from Proposition 2, if $p_t^B=0$, $h_t^*=0$. By A2*a*, we have $\tau(0)=0$ and, therefore, $p_t^B=0$ implies $\tau\left(mh_t^*\right)=0$.

To characterize existence and uniqueness, consider a stationary solution to equation (9):

$$\left[b-\tau\left(H(b)\right)\lambda\left(n\right)b^{1-\sigma}\right]=\frac{\delta}{1+\rho}\tau\left(H(b)\right)b,$$

where $\lambda\left(n\right):=f\left(n\right)^{1-\sigma}n^{\sigma}$. A solution $b^*>0$ satisfies $b^*=\left(\frac{\lambda(n)(1+\rho)\tau(H(b^*))}{1+\rho-\delta\tau(H(b^*))}\right)^{\frac{1}{\sigma}}$.

We define

$$\begin{aligned}A(b)&:=\left[b-\tau\left(H\left(b\right)\right)\lambda\left(n\right)b^{1-\sigma}\right],\\ D(b)&:=\frac{\delta}{1+\rho}\tau\left(H\left(b\right)\right)b.\end{aligned}$$

To determine whether a solution $A\left(b^*\right)=D(b^*)$ exists, with $b^*>0$, we study the limits of

$$A'(b)=1-\lambda(n)\left[\tau'(H\left(b\right))H'(b)b^{1-\sigma}-\left(1-\sigma\right)\frac{\tau(H\left(b\right))}{b^{\sigma}}\right], \tag{18}$$

$$D'(b)=\frac{\delta}{1+\rho}\left(\tau'(H\left(b\right))H'(b)b+\tau(H\left(b\right))\right). \tag{19}$$

Step 1: $b\to+\infty$**.** Consider the behavior of $A'(b)$ as $b\to+\infty$:

$$\lim_{b\to+\infty}A'(b)=\lim_{b\to+\infty}\left(1-\lambda(n)\left(\tau'(H(b))H'(b)b^{1-\sigma}-\left(1-\sigma\right)\frac{\tau(H\left(b\right))}{b^{\sigma}}\right)\right).$$

Note that $\frac{\tau(H(b))}{b^{\sigma}}\to 0$ as $b\to+\infty$. The term $\tau'(H(b))H'(b)b^{1-\sigma}$ has an undetermined limit of the form $0\times\infty$. We consider specific technologies.

If $H'(b)=c>0$ and $\tau=\tau_r$, as in A2*b*, then

$$\lim_{b\to+\infty}\tau_r'(H(b))b^{1-\sigma}c=\lim_{b\to+\infty}\frac{\phi b^{1-\sigma}c}{\left(1+cb\phi\right)^2}=$$

If $\tau = \tau_e$, as in A2*c*, then

$$\lim_{b\to+\infty} \tau_e'(H(b))b^{1-\sigma}c = \lim_{b\to+\infty} \phi\frac{b^{1-\sigma}c}{e^{\phi cb}} = 0.$$

If $\tau = \tau_l$, as in as in A2*d*, then

$$\lim_{b\to+\infty} \tau_l'(H(b))b^{1-\sigma}c = \lim_{b\to+\infty} \frac{c\phi e^{\phi(cb+\underline{H})}b^{1-\sigma}}{\left(e^{\phi cb}+e^{\phi\underline{H}}\right)^2} = 0.$$

Therefore, if the cost function is linear, $\lim_{b\to+\infty} A'(b) = 1$. If the cost function is convex, $H'(b)$ is a decreasing function and the same conclusion holds. Using similar arguments, we have that $\lim_{b\to+\infty} D'(b) = \frac{\delta}{1+\rho}$. Therefore, for any of the considered network security technologies,

$$\lim_{b\to+\infty} A'(b) = 1 > \lim_{b\to+\infty} D'(b) = \frac{\delta}{1+\rho} > 0,$$

implying that, if more than one positive stationary equilibrium value b^* exists, the largest value, $\bar{b}$, displays $A'(\bar{b}) > D'(\bar{b})$ and thus must be dynamically unstable, proving (iv).

Step 2: $b \to 0+$ with a convex cost function. To prove (ii), consider now the case of a convex cost function such as that in A3*a* with $\gamma > 1$. From Example 1, we know that $H'(b) = kb^{\frac{1}{\gamma}-1}$, $k > 0$. Therefore,

$$\begin{aligned} A'(b) &= 1 - \lambda(n)\tau'(H(b))kb^{\frac{1}{\gamma}-\sigma} + \lambda(n)\left(1-\sigma\right)\tau(H(b))b^{-\sigma}, \\ D'(b) &= \frac{\delta}{1+\rho}\left(\tau'(H(b))kb^{\frac{1}{\gamma}} + \tau(H(b)\right), \end{aligned} \tag{20}$$

where we can see that whether $\lim_{b\to0^+} A'(b) < 0$ depends on $\lim_{b\to0^+} \tau'(H(b))$ and the sign of the term $\frac{1}{\gamma} - \sigma$. If $\lim_{b\to0^+} \tau'(H(b))$ is positive and finite, a condition that is satisfied by A2*b* to A2*d* (e.g., if $\tau = \tau_e$, $\lim_{b\to0^+} \tau'(H(b)) = \phi > 0$), then the number of stationary equilibria solely depends on $\frac{1}{\gamma} - \sigma$. If $\frac{1}{\gamma} < \sigma$, then $\lim_{b\to0^+} \tau'(H(b))kb^{\frac{1}{\gamma}-\sigma} = \infty$. Thus, $\lim_{b\to0^+} A'(b) < 0$ and, if an equilibrium exists, $A(b)$ must intersect $D(b)$ from below, since $\lim_{b\to0^+} D'(b) = 0$. Considering that $\lim_{b\to+\infty} A'(b) > \lim_{b\to+\infty} D'(b) > 0$, we conclude that, if $\frac{1}{\gamma} < \sigma$, by continuity of A and D, a positive stationary equilibrium must exist. If τ is globally concave, τ' is monotonically decreasing and such an equilibrium is unique. If $\frac{1}{\gamma} \geq \sigma$, then $\lim_{b\to0^+} \tau'(H(b))kb^{\frac{1}{\gamma}-\sigma} = 0$, $\lim_{b\to0^+} A'(b) = 1$, and there can be multiple stationary equilibria. If more than one stationary equilibria exists, the first crossing of A must be from above, implying that the smallest positive stationary equilibrium, $\underline{b}$, is dynamically stable.

Step 3: $b \to 0+$ with a linear cost function. To prove (iii), we analyze the behavior of A' as $b \to 0+$ with a linear cost function, so that, by Proposition 2, $H'(b) = c > 0$. The term $\lim_{b\to 0+} (1-\sigma)\frac{\tau(H(b))}{b^\sigma}$ leads to a $\frac{0}{0}$ limit indeterminacy. We apply L'Hospital's rule,

$$\lim_{b\to 0+} \frac{(1-\sigma)\,\tau(H(b))}{b^\sigma} = \lim_{b\to 0+} \frac{(1-\sigma)\,\tau'(H(b))cb^{1-\sigma}}{\sigma} = 0$$

where the last equality uses the fact that $\tau'(0) < \infty$. Similarly, the terms $\tau'(H(b))cb^{1-\sigma}$ in (18) and $\tau'(H(b))cb$ in (19) converge to 0 as $b \to 0+$. So, with linear costs, we have $\lim_{b\to 0+} A'(b) = 1$ and $\lim_{b\to 0+} D'(b) = 0$.

Therefore, the slope of D increases from zero to $\frac{\delta}{1+\rho}$ as b grows large. Given $\lambda(n) > 0$, the slope of A first decreases from one and then increases again so that $\lim_{b\to+\infty} A'(b) = 1$. If more than one stationary equilibrium value $b^* > 0$ exists, for the smallest one, $\underline{b}$, the intersection between A and D must have A crossing from above. For the largest equilibrium value, $\overline{b}$, we must have A crossing D from below. Therefore, we conclude that $\underline{b}$ is dynamically stable and $\overline{b}$ is not. exists, there are at least. Everything else being constant, whether a positive stationary equilibrium exists in the first place depends on the value of $f(n)$. If $f(n) \approx 0$, $A(b) > D(b)$ for all $b > 0$ and no positive stationary equilibrium exists. If $f'(n) > 0$, by continuity of A and D, there must be a value $\underline{n}$ such that A is tangent to D at a value $b^* > 0$. If $n > \underline{n}$, A must then cross D at least once. □

Proof of Lemma 1.

Let $Y(b,\omega) = b - y(b,\omega)$ and let $\tilde{b}$ be a positive stationary equilibrium, $Y(\tilde{b},\omega) = 0$. By the implicit function theorem, around $\tilde{b}$, $\frac{d\tilde{b}}{d\omega} = \frac{y_\omega(\tilde{b})}{1-y_b(\tilde{b})}$. If $y_b\left(\tilde{b}\right) < 1$, then the sign of $\frac{d\tilde{b}}{d\omega}$ is the same as $y_\omega\left(\tilde{b}\right)$. It therefore suffices to show that the condition for equilibrium regularity implies that $y_b(\tilde{b}) < 1$. Note that $y_b\left(\tilde{b}\right) < 1$ can be expressed as follows:

$$\begin{aligned}
\left(\frac{\lambda(n)\tau(H(b))(1+\rho)}{1+\rho-\delta\tau(H(b))}\right)^{\frac{1-\sigma}{\sigma}} \lambda(n)(1+\rho)\frac{\tau'H'(1+\rho-\delta\tau)+\tau\delta\tau'H'}{(1+\rho-\delta\tau(H(b)))^2} &< \sigma \\
\left(\frac{\lambda(n)\tau(H(b))(1+\rho)}{1+\rho-\delta\tau(H(b))}\right)^{\frac{1-\sigma}{\sigma}} (1+\rho)\frac{\tau'}{\tau}H'\frac{\tau\lambda(n)(1+\rho)}{1+\rho-\delta\tau(H(b))^2} &< \sigma \\
\tau'H'\tilde{b}\frac{(1+\rho)\tau(H(b))}{1+\rho-\delta\tau(H(b))} &< \sigma\tau^2.
\end{aligned}$$

Equivalently, $\tau'H'\tilde{b}s(\tilde{b}) < \sigma\tau^2$, where $s(\tilde{b}) := \frac{\tau(H(\tilde{b}))(1+\rho)}{1+\rho-\delta\tau(H(\tilde{b}))}$.

Now, using the definitions of A and D, we find the condition $A'\left(\tilde{b}\right) > D'\left(\tilde{b}\right)$ implies that

$$\left[1-\lambda(n)\tilde{b}^{-\sigma}\left(\tilde{b}\tau'H'+(1-\sigma)\,\tau\right)\right] > \frac{\delta}{1+\rho}\left[\tilde{b}\tau'H'+\tau\right]. \tag{21}$$

The equilibrium condition $Y(b,\omega)=0$ can be written as $\tilde{b}^{-\sigma}=\frac{1}{\lambda(n)s\left(\tilde{b}\right)}$. Using this expression and rearranging, we can write the inequality (21) as

$$\begin{aligned}
1-\frac{1}{s}\left(\tau' H'\tilde{b}+(1-\sigma)\,\tau\right) &> \frac{\delta}{1+\rho}\left[\tau' H'\tilde{b}+\tau\right] \\
1-\frac{\left(\tau' H'\tilde{b}+\tau\right)}{s}+\frac{\sigma\tau}{s} &> \frac{\delta}{1+\rho}\left[\tau' H'\tilde{b}+\tau\right] \\
\frac{\sigma\tau}{s} &> \left(\frac{\delta}{1+\rho}+\frac{1}{s}\right)\left[\tau' H'\tilde{b}+\tau\right]-1 \\
\frac{\sigma\tau^2}{s} &> \left(\frac{\delta\tau}{1+\rho}+\frac{\tau}{s}\right)\left[\tau' H'\tilde{b}+\tau\right]-\tau \\
\Rightarrow \sigma\tau^2 &> s\tau' H'\tilde{b}.
\end{aligned}$$

Therefore, $A'\left(\tilde{b}\right)>D'\left(\tilde{b}\right)$ implies $y_b\left(\tilde{b}\right)<1$. Moreover, under the regularity condition, if $f'(n)>0$, then $\lambda'(n)>0$, $y_n>0$, and $\frac{d\tilde{b}}{dn}>0$, proving Corollary 1. □

Proof of Proposition 5

By Lemma 1, it is sufficient to show that an increase in m or ϕ increases $s:=\frac{\tau(H(b))}{1+\rho-\delta\tau(H(b))}$, since $y=(\lambda(n)(1+\rho))^{\frac{1}{\sigma}}\left(\frac{\tau}{1+\rho-\delta\tau}\right)^{\frac{1}{\sigma}}$. By the chain rule,

$$\frac{ds}{dm}=\frac{\frac{\partial\tau}{\partial H}(1+\rho)}{[1+\rho-\delta\tau(H)]^2}\frac{dH}{dm}.$$

From Proposition 2, we know that $\frac{dH}{dm}>0$. Thus $\frac{ds}{dm}>0$ and, by Lemma 1, $\frac{db}{dm}>0$, implying $\frac{dp^B}{dm}>0$.

Let us now consider the effect of changes in ϕ. We have that $\frac{ds}{d\phi}=\frac{\frac{\partial\tau}{\partial\phi}(1+\rho)}{[1+\rho-\delta\tau]^2}$. Therefore, it is enough to show that the sign of $\frac{\partial\tau}{\partial\phi}$ is positive. Under A2*b*, $\frac{\partial\tau}{\partial\phi}=\frac{H}{\phi^2\left(H+\frac{1}{\phi}\right)^2}>0$. Under A2*c*, $\frac{\partial\tau}{\partial\phi}=He^{-\phi H}>0$. Thus $\frac{ds}{d\phi}>0$ and by Lemma 1 $\frac{db}{d\phi}>0$, implying $\frac{dp^B}{d\phi}>0$. □

Proof of Proposition 6

We express the regular equilibrium price as $p_t^B-y(p_t^B,\rho)=0$, where

$$y(p_t^B,\rho):=\underbrace{\left(\frac{\tau(H(\rho))(1+\rho)}{1+\rho-\delta\tau(H(\rho))}\right)^{\frac{1}{\sigma}}}_{F(\tau(H(\rho)),\rho)}\underbrace{\frac{nf(n)^{\frac{1-\sigma}{\sigma}}}{(1+\rho)\,B_{t-1}}}_{G(\rho)}.$$

By the implicit function theorem, $\frac{dp_t^B}{d\rho} = \frac{y_\rho}{[1-y_p]}$. By Lemma 1, regularity of the equilibrium implies that $y_p < 1$. Therefore, the sign of $\frac{dp_t^B}{d\rho}$ is given by the sign of y_ρ, given by

$$y_\rho = (\underbrace{F_1 \tau' H_\rho}_{\text{security}} + \underbrace{F_2}_{\text{expectations}})G + \underbrace{FG'}_{\text{supply}}. \tag{22}$$

Let $\xi := \frac{\tau(H(\rho)(1+\rho)}{1+\rho-\delta\tau(H(\rho))}$. The optimal inflation $\overline{\rho}$ is a solution to $y_\rho(\overline{\rho}) = 0$. Computing the terms in (22), we obtain

$$\frac{1}{\sigma}\xi(\overline{\rho})^{\frac{1}{\sigma}}\left(\xi(\overline{\rho})\left(\frac{\tau'\left(H(\overline{\rho})\right)H_\rho\left(\overline{\rho}\right)}{\tau^2\left(H(\overline{\rho})\right)} - \frac{\delta}{(1+\overline{\rho})^2}\right)\right)\frac{1}{1+\overline{\rho}} - \frac{1}{(1+\overline{\rho})^2} = 0. \tag{23}$$

Assume a solution exists for a general cost function and consider a concave function τ so that τ' is decreasing. If $\rho > \overline{\rho}$, the negative supply and expectation effects become stronger for ρ. Given a decreasing τ', the marginal network security effect weakens. Therefore, we must have $y_\rho < 0$ for $\rho > \overline{\rho}$. Using an analogous argument, we have $y_\rho > 0$ for $\rho < \overline{\rho}$. Thus, the price is maximized at $\overline{\rho}$.

We now compute the value of $\overline{\rho}$ under A3*a* with $\gamma = 1$. Re-arranging equation (23), we obtain

$$H_\rho = \frac{\tau^2}{\tau'\left(1+\rho\right)^2}\left(\left(1+\rho-\delta\tau\right)\sigma+\delta\right). \tag{24}$$

By A3*a*, $\gamma = 1$, and Proposition 2, $H_\rho = p_t^B\left(\frac{B_{t-1}(m-1)}{cm}\right)$. Combining H_ρ and the equilibrium price condition $p_t^B - y(p_t^B, \rho) = 0$ and substituting back in (24) yields

$$nf(n)^{\frac{1-\sigma}{\sigma}}\left(\frac{m-1}{cm}\right) = \frac{\tau^2}{\tau'\left(1+\rho\right)}\left(\frac{\tau(1+\rho)}{1+\rho-\delta\tau}\right)^{-\frac{1}{\sigma}}\left(\left(1+\rho-\delta\tau\right)\sigma+\delta\right). \tag{25}$$

Note that the left- and right-hand sides of equation (25) correspond to the definitions of V and W, respectively. □

Proof of Proposition 7

We show that $db_u > db_d$ when $dn > 0$ and $db_u < db_d$ when $dn < 0$. To simplify notation, let $\lambda\left(n\right) := f\left(n\right)^{1-\sigma} n^\sigma$. From equation (3),

$$db_d\left[1 - \frac{\delta\tau_d}{1+\rho} - \tau_d\lambda\left(n\right)\left(1-\sigma\right)b_d^{-\sigma}\right] = \left[\lambda'(n)\tau_d b_d^{1-\sigma}\right]dn. \tag{26}$$

From equation (9),

$$db_u\left[A'(b_u) - D'(b_u)\right] = \left[\lambda'(n)\tau\left(b_u\right)b_u^{1-\sigma}\right]dn, \tag{27}$$

where

$$A'(b_u) = 1 - \lambda(n)\left[\tau'(H(b_u))H'(b_u)b_u^{1-\sigma} - (1-\sigma)\frac{\tau(H(b_u))}{b_u^{\sigma}}\right],$$
$$D'(b_u) = \frac{\delta}{1+\rho}\left(\tau'(H(b_u))H'(b_u)b_u + \tau(b_u)\right).$$

Let $dn > 0$. Given $b_u = b_d$, the right-hand sides of equations (26) and (27) coincide. Therefore,

$$db_u\left[A'(b_u) - D'(b_u)\right] = db_d\left[1 - \frac{\delta\tau_d}{1+\rho} - \tau_d\lambda(n)(1-\sigma)b_d^{-\sigma}\right].$$

We have $db_u > db_d$ if and only if

$$\left[A'(b_u) - D'(b_u)\right] < 1 - \frac{\delta\tau_d}{1+\rho} - \tau_d\lambda(n)(1-\sigma)b_d^{-\sigma}. \tag{28}$$

Using $\tau(H(b_u)) = \tau_d$, and rearranging terms, one can show that the inequality holds if and only if

$$\tau'(H(b_u))H'(b_u)b_u\left(\lambda(n)b_u^{-\sigma} + \frac{\delta}{1+\rho}\right) > 0. \tag{29}$$

The above inequality is satisfied given that $b_u > 0$, $\tau' > 0$ by A2*a*, and $H' > 0$ by Proposition 2. An analogous argument implies that $db_u < db_d$ for a negative network size shock. Expression (29) shows that the price reaction gap increases in τ' and H'. □

Proof of Proposition 8.

To simplify notation, let $\lambda(n) := f(n)^{1-\sigma}n^{\sigma}$. Note that, given that $b_t = p_tB_t$ and that supply is not affected by n, $\eta := \frac{dp}{dn}\frac{n}{p} = \frac{db}{dn}\frac{n}{b}$. From equation (4), a positive stationary equilibrium b_d satisfies

$$\frac{db_d}{dn} = \frac{\lambda'(n)}{\sigma\lambda(n)}\left(\frac{\lambda(n)(1+\rho)\tau_d}{1+\rho-\delta\tau_d}\right)^{\frac{1}{\sigma}} = \frac{\lambda'(n)}{\sigma\lambda(n)}b_d.$$

Therefore, $\eta^d = \frac{1}{\sigma}\frac{n\lambda'(n)}{\lambda(n)}$, and using the definition of λ

$$\eta^d = \frac{(1-\sigma)f(n)^{-\sigma}f'(n)n^{\sigma+1} + \sigma n^{\sigma}f(n)^{1-\sigma}}{\sigma f(n)^{1-\sigma}n^{\sigma}}$$
$$= \frac{(1-\sigma)}{\sigma}\frac{nf'(n)}{f(n)} + 1.$$

Consider now a token satisfying unity. From equation (9), a positive stationary equilibrium b is

given by

$$b = \left(\frac{\lambda(n)\,\tau(H(b))(1+\rho)}{1+\rho-\delta\tau(H(b))} \right)^{\frac{1}{\sigma}}, \tag{30}$$

and satisfies $\frac{db}{dn} = \frac{\lambda'(n)\tau(b)b^{1-\sigma}}{A'(b)-D'(b)}$. Therefore,

$$\eta^B = \frac{n\lambda'(n)\tau\left(H(b)\right)b^{-\sigma}}{1-\lambda(n)\left(\tau'\left(H(b)\right)H'\left(b\right)b^{1-\sigma}+(1-\sigma)\frac{\tau(H(b))}{b^{\sigma}}\right)-\frac{\delta}{1+\rho}\left(\tau'\left(H(b)\right)H'\left(b\right)b+\tau\left(H(b)\right)\right)}. \tag{31}$$

Combining expressions (30) and (31) and using $x := 1+\rho-\delta\tau\left(H(b)\right)$, we find

$$\begin{aligned}
\eta^B &= \frac{n\lambda'(n)}{\lambda\left(n\right)}\frac{x}{x-\left(\left(1+\rho\right)\lambda\tau'H'b^{1-\sigma}+\left(1-\sigma\right)x\right)-\delta\tau'H'b} \\
&= \frac{n\lambda'(n)}{\lambda\left(n\right)}\frac{x}{x-\left(1-\sigma\right)x-\tau'H'b\left(\delta+\left(1+\rho\right)\lambda b^{-\sigma}\right)} \\
&= \frac{n\lambda'(n)}{\lambda\left(n\right)}\frac{1}{\sigma-\tau'H'b\left(\frac{\delta}{x}+\frac{1}{\tau}\right)} \\
&= \frac{n\lambda'(n)}{\lambda\left(n\right)}\frac{1}{\sigma-\frac{\tau'H'}{\tau}b\frac{1+\rho}{(1+\rho-\delta\tau)}} \\
&= \eta^d\frac{\sigma}{\sigma-\chi(b)},
\end{aligned}$$

where $\chi(b) := \frac{\tau'H'b}{\tau}\left(\frac{1+\rho}{1+\rho-\delta\tau}\right) > 0$. □