An Equilibrium Valuation of Bitcoin and Decentralized Network Assets

Emiliano S. Pagnotta*and Andrea Buraschi†

March 21, 2018

Abstract

We address the valuation of bitcoins and other blockchain tokens in a new type of production economy: a decentralized financial network (DN). An identifying property of these assets is that contributors to the DN trust (miners) receive units of the same asset used by consumers of DN services. Therefore, the overall production (hashrate) and the bitcoin price are jointly determined. We characterize the demand for bitcoins and the supply of hashrate and show that the equilibrium price is obtained by solving a fixed-point problem and study its determinants. Price-hashrate "spirals" amplify demand and supply shocks.

JEL Codes: G12, G15, G18

*Imperial College London. Email: epagnott@ic.ac.uk
†Imperial College London. Email: a.buraschi@imperial.ac.uk

"I think the internet is going to be one of the major forces for reducing the role of government. The one thing that's missing but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A." Milton Friedman, 1999[1].

The rapid growth of Bitcoin over the last decade has sparked an intense debate in the investment community and policy circles. Two questions are at the center of this debate. What type of asset is bitcoin?[2] What is its fundamental value? Opinions diverge greatly on whether bitcoins are a currency, a commodity, a security, for example; but a prominent view is that bitcoin and similar "blockchain tokens" are not a new asset class and that they either have zero fundamental value or that their fundamental value cannot be determined.[3] Reaching a consensus on these issues is challenged by the lack of a formal model where the interaction between demand and supply for bitcoins can be analyzed.

We develop an equilibrium framework where these questions can be addressed. On the demand side, consistent with Friedman's conjecture, consumers value (i) the censorship resistance (CR) of transactions and (ii) the ability to engage in trustless exchanges. Thus, they value the consumption of services in a decentralized peer-to-peer (P2P) network providing these features where a token, such as bitcoin, is stored and transferred. As we discuss in Section 1, transfers of this token may represent a payment or other type of information exchange (e.g., as in decentralized applications) and the number of these uses is rapidly expanding due to constant innovation.[4] We abstract from modeling all of the potential specific uses, which are mostly unobservable. Instead, we take a different route and model the properties and value of the network where the token trades. For parsimony, we focus on a small set of observables that drive network value. First, the number of users, reflecting the strength of network externalities. Second, on the supply side, the miners, who provide computing resources that affect the network's trustworthiness ("trust" hereafter) by which we mean value-enhancing properties related to the absence of frauds and resistance to censorship and attacks. Because the network is decentralized, those who provide resources need to be incentivized to do so. They are incentivized by the same token through a non-cooperative game that resembles proof-of-work (PoW, Nakamoto (2008)). The token thus simultaneously serve two functions, a property that we label as *unity* (Definition 1). To find the value of the token, one then needs to solve a fixed-point problem that characterizes the interaction between consumers and miners.

[1] Interview conducted by NTUF (1999), https://www.youtube.com/watch?v=6MnQJFEVY7s

[2] We follow the common practice in the developer community of using lower case b for the token (bitcoin) and capital B for the protocol or network (Bitcoin).

[3] We are unaware of a formal analysis showing that the bitcoin price is merely a bubble with no fundamental value. Opinion pieces making claims that Bitcoin is value-less, on the other hand, are plentiful. See, for example, https://krugman.blogs.nytimes.com/2013/12/28/bitcoin-is-evil/. More recently, Agustín Carstens Carstens, head of the Bank for International Settlements, described bitcoin as "a combination of a bubble, a Ponzi scheme and an environmental disaster" in a speech given on February 6, 2018, at the University of Goethe.

[4] DN assets can be used in the context of smart contracts (Wood (2018)), and holdings in DN assets can often play different economic roles (e.g., in connection with a property title, copyrights, collectibles; as an option to hedge against various risks).

Bitcoin is the first member of a class of assets, decentralized network assets (DNAs), that share the unity property in decentralized networks; which gives rise to specific asset pricing implications that distinguish it from other asset classes.[5] The fundamental value of bitcoin is determined in equilibrium (Theorem 1) and depends on consumer preferences, i.e., risk aversion and censorship aversion, the usefulness of the network, driven by its size and its trust, and the industrial organization of the mining market. We describe the characteristics of the equilibrium price as they relate to these fundamentals (Propositions 3 and 4). Moreover, we study a quantitative version of the model and calibrate it using Bitcoin network data to discuss its economic implications (Sections 5-7).

To formalize the unique properties of bitcoin as an asset, we begin by characterizing its role as an incentive device that enables the allocation of resources within a new form of institutional environment, i.e., a DN. The supply of financial and economic services is not run by a trusted central unit or network node. Instead, services are provided and managed in a P2P network that does not require trust in any node and thus reduces the role of institutions and governments. Independently of our views about its potential welfare implications (which we do not address in this paper), this is arguably one of the most significant business innovations since the internet. Indeed, since its early days, digital financial networks have relied exclusively on financial institutions serving as trusted third parties under the traditional profit-maximizing firm model. In contrast to Bitcoin, for instance, Visa runs its payment-processing network by verifying IOUs transfers denominated in a central bank currency, such as USD, and charges fees for this service. One can think of the IOUs on the USD as "dollar tokens." Plausibly, the equilibrium value of the USD is exogenous to Visa's network value. The latter is driven by this firm's ability to collect fees in the market for payment networks. Therefore, although the value of Visa shares depends on the size and trustworthiness of Visa, Visa shares do not satisfy unity.

Section 3 provides a framework that captures salient features of Bitcoin. We assume that agents' utility from accessing the network depends on its participants and its trust. Given the near-complete topology of the P2P Bitcoin network, we capture network externalities in a stylized fashion, as a function of the total number of participants. All consumers are risk-averse to changes in future network size, but they differ in their valuation of the network services, i.e., their fundamental demand for CR is heterogeneous. Network trust is a single-dimensional function of the total amount of computing resources, i.e., system hashrate, that a finite number of homogeneous risk-neutral miners contribute. The equilibrium price and hashrate is the simultaneous solution to three conditions: (a) agents optimally choose their assets inter-temporally to maximize the services received from traditional goods and those obtained in the DN; (b) miners optimally supply resources in exchange for network assets; and (c) the asset market clears. The decentralized character of the network manifests in the economics of (b). The Unity property of bitcoin prices creates a structural link

[5] Additional examples with relatively large market capitalization include Ethereum, Litecoin, Dash, and Monero.

between (a) and (b).

We show that, under fairly general conditions, two equilibria in this economy exist. In the absence of mining subsidies, a price equal to zero is always an equilibrium. Indeed, if the price of bitcoin were zero, miners would not provide any resource to the network, and its trust would be zero. Consumers would derive no utility from the system and would not pay a positive price for bitcoins. If network trust increases "fast enough" near a price of zero, however, an equilibrium with a strictly positive price can also be shown to exist (Proposition 2) if a positive mass of agents values CR or trustlessness. On the demand side, the price increases with the number of network participants and the average censorship aversion value. Furthermore, if consumers expect a higher (lower) network size in the future, the market clearing price increases (decreases) today. Thus, high volatility in expectations on network size will translate into high price volatility. This intuitive property finds a formal representation in the closed-form expressions in Theorem 1.

Under general conditions on the effect of the supply side parameters on network trust, we derive a series of testable predictions. Proposition 3 shows that, perhaps counterintuitively, the price decreases with the marginal cost of mining, which is driven by factors such as electricity costs,[6] due to the reduction in the equilibrium network trust (measured in hashrate), thus reducing the bitcoin valuation. We also show that the price increases in the number of miners. In the limit, when mining is perfectly competitive, we show that the cost of mining a bitcoin is a constant proportion of the price and that proportion only depends on the curvature of the cost function and not on other supply-side parameters (Proposition 5). To illustrate, if the cost function were given by a β-power of the hashrate, that limit mining cost equals $1/\beta \times$ price. Finally, the price is not monotonic in the inflationary reward offered to miners. For small values of the reward, bitcoin injections increase the incentive for miners to provide trust; however, above a given threshold, the effect becomes negative due to the debasing influence of bitcoin inflation. The model thus implies an "optimal monetary policy" regarding an inflation rate that maximizes the market capitalization of Bitcoin.

To address a series of questions related to the behavior of bitcoin prices, we calibrate the economy to properties of the Bitcoin network at the end of 2017 when the price was USD 14,200. We find that the price of bitcoins is very susceptible to the fundamental properties of demand and supply. As an illustration, tripling the current network size raises the equilibrium price from USD 14,200 to 77,627. A 100% increase in mining costs, on the other hand, lowers the price to USD 13,330; while in the competitive limit, with an infinite number of miners, the price increases but moderately to USD 14,974. We further discuss the price effect of miner's reward halving, which predictably occurs every four years, and numerically illustrate how one would misprice bitcoin by following a partial equilibrium valuation approach.

This paper is related to two streams of the financial economics literature. Our first contribution

[6] See also Section 6.2 for an extension that models mining difficulty level adjustments.

relates to the asset pricing literature. A stream of this literature investigates production-based asset pricing models and link asset prices to fundamentals such as investment and productivity. Cochrane (1988, 1991) was among the first to study the link between a firm's return to investment and its market return, both theoretically and empirically. An incomplete list of additional studies includes Jermann (1998), Berk, Green, and Naik (1999), Kogan (2004), Cooper (2006), Li, Livdan, and Zhang (2009), Belo (2010), and Eisfeldt and Papanikolaou (2013). Our paper is, to the best of our knowledge, the first to study the general equilibrium of a DN economy and to derive closed-form solutions linking the bitcoin price to market fundamentals.[7]

On the asset demand side, we model the value of services with network effects (e.g., Katz and Shapiro (1985); Economides (1996)) but with vertically-differentiated preferences reflecting different degrees of censorship aversion. Unlike traditional models with vertically-differentiated preferences (e.g., Shaked and Sutton (1982)), the quality of the product (trust in the DN services) is (i) stochastic, as it depends on future network participation, to which consumers are risk-averse, and (ii) is not determined by a firm; rather, by an oligopoly of price-taking miners.[8] On the supply side, we highlight the importance played by the production of network trust. Although miners compete in capacity (hashrate), competition among them is unlike that in Cournot (1897) as the relation between total capacity (total hashrate) and the price (the bitcoin price) is *reversed*: they are positively related. This is because of a structural difference between *Nakamoto's competition* for verifications (Section 3.2) and Cournot's: miners do not compete in bitcoin units but hashrate, i.e., units of Bitcoin network trust.

Moreover, the non-linearity of the resulting equilibrium price has important consequences. First, it violates the conditions of the Riesz representation theorem for Hilbert spaces (as discussed in Hansen and Richard (1987)); which implies that empirical tests on the efficiency of bitcoin prices cannot rely on martingale representations. Second, it can give rise to price spirals that may help to explain the large observed bitcoin price volatility. This effect is because network trust depends on the hashrate supply which, in turn, depends on miners' sensitivity to the price of the verification rewards. Thus, exogenous shocks to fundamentals can initiate price-hashrate spirals (see a quantitative analysis in Section 6.1 and a discussion in Section 6).

A second 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 may "attack" the process. This question, known as the "Byzantine agreement," was originally studied by Pease et al. (1980) and Lamport et al. (1982). Nakamoto (2008) proposes a solution based on the

[7]Decentralized financial networks are specific examples of financial networks (e.g., Allen and Gale (2000). For a recent survey of contributions in the field of network economics, see Bramoulle et al. (2016)). We differ from this literature as we characterize a new class of financial networks with decentralized verification of transfers and study the pricing equilibrium for the assets that trade in them in a setting where the trust of verification is endogenous.

[8]Moreover, to allow for richer links with observed quantities, and in contrast to much of this literature, we do not restrict consumers' demand to be binary.

PoW protocol. Analyses of the implications of blockchains and decentralized ledger technologies for central banking, corporate governance, transaction efficiency and capital markets include Raskin and Yermack (2016), Yermack (2017), Harvey (2016), and Malinova and Park (2017). Biais, Bisière, Bouvard, and Casamatta (2018), Cong and He (2018) and Saleh (2017) model the PoW and the proof-of-stake consensus protocols and show the conditions required for the existence of equilibria in each. Easley, O'Hara, and Basu (2017) and Huberman, Leshno, and Moallemi (2017) analyze bitcoin mining fees. We contribute to this nascent literature by developing a framework where equilibrium asset prices and mining investment for bitcoins and other DNAs can be characterized.

1 The Economics of DNAs

This section provides background on the economics of decentralized financial networks, the main properties that characterize the demand for their assets, and the unity property.

1.1 Demand Side

Two fundamental motives driving the demand for DN are related to their censorship resistance properties and their trustlessness, especially in connection with decentralized applications and smart contracts. These motives are not mutually exclusive and, in most cases, they are not independent from each other. We provide a brief discussion of each.[9]

Demand for Censorship Resistance. The demand for CR within networks has multiple sources, including financial repression through governmental capital controls; option-like hedging against government abuses such as arbitrary wealth confiscations 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 forced maturity conversion of bank deposits; the ability to secure wealth transfers in the event of armed conflicts, territorial invasions, civil wars, refugee crises, etc. In the past, these factors have motivated the development of significant off-shore markets and shadow banking systems. Moreover, CR demand can originate from the criminalization of certain consumer goods which previously increased the need for cash (such as alcohol, cannabis, or a not-yet-approved medicine) and services (such as gaming/gambling/prediction markets). Consumers may demand the services of a DN to protect privacy, especially in economies where the use of cash is restricted.

DNAs can also power the contribution of resources to the development of censorship-resistant social media platforms (e.g., Steem for Steemit). They can also contribute to mitigating internet

[9] For a more comprehensive review, see Antonopoulos (2016)

censorship more broadly (e.g., Substratum for web hosting). In this context, the value of CR naturally resembles that of free speech.

Spanning. The CR of DNAs implies that their spanning properties are potentially different than traditional Arrow-Debreu claims. In the original Arrow-Debreu approach, it is common to value contingent claims in a state space representation that include two dimensions: calendar time and the state of nature, (t, ω). In the case of DNAs, one should also consider the specific identities i and i' of the agents willing to engage in a transfer, (t, ω, ii'). In the presence of censorship, traditional assets may not be able to span all states. Consider, for instance, the left panel of Figure 1. Agent 1 and 2 are linked only indirectly to other agents in the network through node X. A (t, ω)-contingent transfer of an asset from 1 to 2 may fail to materialize if X does not authorize it. Besides the provided individual-level examples above, additional cases are offered by international sanctions that disconnect an entire country from global financial markets. In the context of state-contingent pricing, censorship becomes a source of *fundamental* market incompleteness for traditional assets that can help to rationalize positive DNAs prices.

Non-Digital Alternatives. It has been informally argued that bitcoin can be seen as digital gold. In our view, they are not perfect substitutes. Through a digital P2P network, bitcoins can be seamlessly transferred globally at modest cost. Bitcoin and similar DNAs can be used as the base infrastructure for layers of increasingly sophisticated contracts. Unlike gold and gold coins, for which purity and very small denominations are a concern, bitcoin benefits from homogeneity and divisibility. Both gold and bitcoin arguably offer better CR than regulated payment networks. However, 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 CR properties of physical assets.[10] A clear advantage of gold, on the other hand, is that it has commodity uses beyond being a reserve of value.

Demand for Trustlessness. The demand for DNAs can go beyond pure financial transfers. Fundamentally, trustless networks allow for the coordination of resources towards the production of a certain service in a manner that does not require that the parties either know or trust each other. 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,

[10]The limited effectiveness of physical gold to hedge against the possibility of theft finds several historical examples. Nazi Germany is reported to have expropriated about $550m in gold from foreign governments, including $223m from Belgium and $193m from the Netherlands. These figures do not include gold and other instruments stolen from private citizens or companies. China found itself vulnerable to two separate accounts of looting. The first was in 1937 when Japan invaded China. In this occasion, it is reported that approximately 6,600 tonnes of gold were removed from the then capital Nanking. The second occurred in 1948, when Chiang Kai-shek, who was losing the civil war, planned a retreat to Taiwan and is reported to have removed about 100 tons of gold reserves from the former capital.

as well as information asymmetries through increased transparency. Simple types of decentralized applications include smart contracts (Szabo, 1994), i.e., a computerized transaction protocol that executes the terms of a contract,[11] crowd-computing and crowd-file-storage networks, and the creation of game tokens and digital collectives (e.g., a cryptographically-secured digital image or music file with artistic value). Several DNs are being developed to deploy more elaborate trustless decentralized applications, and each DN has a supporting DNA that both developers and users demand (e.g., ETH, ETC, EOS, ADA, NEO). Although one can distinguish original sources of demand for both CR and trustlessness, we note that in many cases they are not unrelated. In particular, the recent exponential growth of initial coin offerings (ICOs) arguably highlights a substantial latent demand for permissionless (CR) innovation.[12]

Implications for Preferences. Based on these observations, we assume that agents value both CR and trustlessness and endow them with heterogeneous preferences, indexed by a parameter $\theta \sim [0, \Theta]$, that reflect the desire for the services of DNs that provide them with these two features. For example, an individual that does not care either about censorship risk or trustlessness has $\theta = 0$. The degree of censorship aversion is reflected in a higher θ value. In the particular case in which no individual cares about censorship risk or trustlessness, one would have $\Theta = 0$, and the fundamental value of a DNA offering such feature would be zero. For conciseness, we label θ as censorship aversion.

1.2 Supply Side and The Unity Property

Transfers of assets through a digital ledger require verification because digital files, unlike physical objects, can be easily duplicated or changed. For this, a digital financial network needs verifiers. In a centralized network (CN), a specific node (a firm or an institution) is entrusted with the responsibility of verification. In exchange, it charges users with fees. In a DN, verification tasks are not delegated to a single node but to different members of the network. Trust does not rely on a node, but on the behavior of the network and its protocols.[13] Verifiers in a DN need well-

[11] Let us list a few specific smart contract examples: (a) property ownership could be transferred automatically upon receipt of DNA funds (e.g., "mulitsig" contracts); (b) credits under service level agreements could be automatically paid at the point of violation; (c) securities could be traded without the need for central securities depositories; (d) complex supply chains: "if entity A receives good B at their warehouse in location C, then the supplier D located several steps above the supply chain will deliver funds to another defined entity."

[12] On the entrepreneur side, CR is vital as otherwise innovation could be outlawed prematurely by legacy regulations. This is especially a concern for projects that are global in reach. On the investor side, DNs offering CR (e.g., Ethereum) allow individuals to participate in seed equity investments even when they do not meet 'qualified investor' status according to governmental regulations.

[13] In the economic framework we analyze, we emphasize trust in verifications as opposed to speed performance. The latter is typically higher in CNs as verification consensus with a single verifier can be achieved automatically. Modeling speed performance would require a dynamic framework, but, arguably, the value of pure speed performance provision in dynamic exchanges is better understood (e.g., Pagnotta and Philippon (2017)). If both a CN and DN

defined economic incentives to contribute resources that deliver high degrees of trust, which is a fundamental innovation in Nakamoto (2008). The more computing power miners supply, the more difficult it is for any single node to either commit a fraud (e.g., spending the same token twice) or to censor someone else's transfers, thus increasing trust in the network. Based on this property, we model trust in the network as a function of the total amount of computing resources that verifiers supply.[14]

Let us consider a 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 $R(p, h_{jk})$. The 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,

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 $h^*(p) \neq h^*(p_{-k})$ and it does not if $h^*(p) = h^*(p_{-k})$.*

Other blockchain-based assets like Ethereum also share this property as miners verifying transfers of ether, the native token, receive units of ether as compensation. Let us consider two examples that violate unity.

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, e.g., a stock like Google.

There is an emerging class of DNs with no free entry to 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. The independent validating servers constantly compare their transaction records. Trans-

competed in the same economy, one would expect that consumer preferences trade-off speed on the one hand and CR and trustlessness on the other.

[14] This is a simplification. Additional important factors include the skills and work commitments 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 non-mining full nodes, i.e., 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 on the Bitcoin website for more details on the specifics. A critical economic difference between miners, on the one hand, and developers and non-mining 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 hashrate supply as a price-sensitive quantity and reflect other aspects like the quality of the code as price-inelastic parameters (e.g., parameter ϕ in Section 5).

fers 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, and thus XRP does not satisfy unity.

2 Modeling Decentralized Networks

This section formalizes the DN economy and proposes a stylized model for its valuation.

2.1 Network Types

A financial network is a collection of business entities (nodes) connected by relationships (described by a topology) over an asset or a set of assets $\mathcal{A} = \{a_1, ..., a_K\}$, each in non-negative supply a_k, with $\#\mathcal{A} = K$. A digital financial network uses a digital ledger to record transactions and ownership of these assets.

Definition 2. Digital Financial Network: A 4-tuple $\mathscr{F} = (\{\mathcal{N}, G\}, \{\mathcal{M}, L\})$ where:

- $\mathcal{N} = \{1, ..., n\}$ is a set of nodes, with $\#\mathcal{N} = n$. G is a topology or graph that fully characterizes the links among the nodes.
- $\mathcal{M} = \{1, ..., m\}$ is the set of verifiers, with $\mathcal{M} \subseteq \mathcal{N}$ and $\#\mathcal{M} = m$. $L \in \mathbb{R}^{n \times k}$ is the digital ledger matrix.

The ledger satisfies market clearing conditions for the asset: $\sum_{i=1:N} L_{ik} = a_k$. For networks that transfer a single asset, like Bitcoin, one can write $L \subseteq [0, a]^n$. We take G to be an $n \times n$ matrix where $G_{ii'}$ represents a link between agents i and i'. A connection represents the ability of agent i to transfer a given amount of an asset to agent i'. We focus on undirected, unweighted graphs where $G_{ii'} = 1$ denotes a connection and $G_{ii'} = 1$ implies $G_{i'i} = 1$.

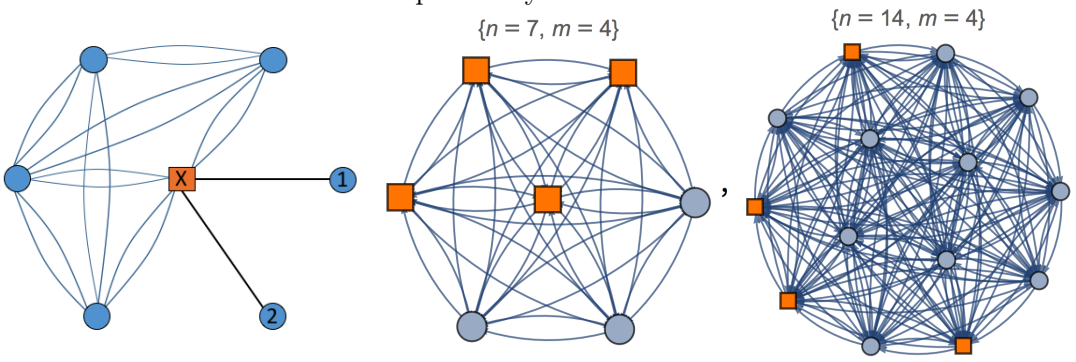
Verification and consensus can be achieved either centrally or in a decentralized fashion. In traditional financial networks, network consensus is given to a designated trusted node ("institution") and thus $\#\mathcal{M} = 1$. We label such networks as *centralized* (CN). When, on the other hand, $\#\mathcal{M} > 1$, we label the network as *decentralized* (DN). The degree of decentralization, for a given $\#\mathcal{N}$, increases in $\#\mathcal{M}$. We illustrate the process of verification and CR further in Appendix A.

2.2 Modeling the Value of DNs

Agents value the ability to trade assets in DNs. Presumably, however, not all networks are equally valuable. What then is the overall value of a given digital financial network $\mathscr{F}$? To answer this question, we need to specify a mapping $(\{\mathcal{N}, G\}, \{\mathcal{M}, L\}) \mapsto \mathbb{R}$ that quantifies the network value as a function of its characteristics. This is not an easy task. In a general financial network, both

Figure 1. Censorship, Spanning, and Decentralized Financial Networks

The left panel shows a centralized network where a verifier (square node) has censorship authority on agents 1 and 2, who cannot transfer wealth directly without the explicit authorization of institution "X". The middle and right panels show decentralized and complete P2P networks with the number of connections equal to $n(n-1)$ and $n = 7$ and 14, respectively. The number of verifiers (square nodes) is $m = 4$ and transfers occur independently of the identities of sender and receiver.



the topologies describing users' connections, connections between users and verifiers, as well as the properties of the verification process, can all be complex and difficult to define. We consider some simplifications to keep the analysis tractable.

Network Effects In the case of DNs, such as Bitcoin, a helpful feature is its digital P2P character: all users and verifiers are connected to each other and thus the topology is near-complete. Unlike regulated and centralized financial networks, all it is required to transfer bitcoins from one Bitcoin wallet to another is to specify the receiver wallet's address. Figure 1 illustrates this fact for small networks. In the context of undirected, unweighted graphs, G can, therefore, be represented as a matrix 1_{nn}. Making each user equally important, we then characterize $\{\mathcal{N}, G\}$ by $\#\mathcal{N} = n$ and the network effects by a network law function $\lambda : n \to \mathbb{R}$. Let us consider an example.

Example 1. Consider a DN $\{n, 1_{nn}, m, [0, a]^n\}$ where a DNA in supply a is transferred. Each participant values a link to another participant by an amount that is equivalent to l units of a consumption good. Then, $\lambda(n) = l(n-1)n$.

As the number of participants increases so does the number of possible exchanges among the participants and the value of the network services. To develop the analysis and derive asset pricing results, we only rely on λ being an increasing function.

Because the number of possible connections in digital networks typically increase more than linearly with the number of participants, it is reasonable to assume that the value of the network is convex in n. A conventional approach to estimate the value of near-complete networks, like the internet, is to take the value to be proportional to $n(n-1)$, which is widely referred to as Metcalfe's

law.[15] While we use a similar network law for the purposes of calibration in Section 5, we do not claim that Metcalfe's law or any other alternative network law is the correct model to explain the dynamics of bitcoin prices.[16] Instead, we provide in Section 3 an equilibrium framework that makes the implications of such assumptions empirically testable.

Network Trust and the Value of the Network Network trust is solely a function of the resources invested by verifiers, H. With homogeneous verifiers in $\mathcal{M}$, the total amount of resources is then a multiple m of the resources h invested by each verifier, i.e., $H = h \times m$. We then consider a trust mapping $\tau : H \to \mathbb{R}$ that depends on the specifics of the network consensus protocol. For the case of Bitcoin, we derive mappings explicitly in Sections 3 and 6.2.

Based on the above simplifications, we then write the value of network $\mathscr{F} = \{\{n, 1_{nn}\}, \{m, L\}\}$ as $v\left(\lambda(n), \tau(H)\right)$: the network value, in units of a consumption good that serves as a numeraire, depends on the number of users and the strength of the network effects, captured by the network law $\lambda\left(n\right)$, and its trust which is driven by the total amount of resources H supplied by the m verifiers, $\tau(H(m))$. We consider the following restrictions on v.

Assumption 1. *[A1] The value of the network is given by* $v\left(\lambda(n), \tau(H)\right) = \lambda(n) \times \tau\left(H\right)$*, with* $\tau' \geq 0$*,* $\lambda' \geq 0$*,* $\tau(0) = 0$*, and* $\lambda(1) = 0$*.*

A1 precludes the case where network size and trust are perfect substitutes, i.e., $v = \lambda(n) + \tau(H)$. This implies that, independently of its size, the value of the network is zero if its trust is zero, i.e., $v(n, 0) = 0$ for $\forall n$. Moreover, if a person were the only participant, the network's value would be zero to that person, i.e., $v(\lambda(1), \tau) = 0$ for $\forall \tau$.

If the mapping τ expresses the survival probability to network attacks, by which we mean events that may compromise the immutability of L or the CR character of the network, then the image of τ finds natural bounds and we can write $\tau : H \to [0, 1]$ and $v\left(\lambda(n), 1\right) = \lambda(n)$. The following example illustrates a network value v based on this intuition.

Example 1 (continued)**.** Given the system hashrate, H, trust is given by $\tau(H) = 1 - e^{-\phi H}$ where $\phi > 0$ is a technological parameter related to the quality of the DN open-source code. Each verifier produces a fixed amount of hashrate h, so $H(m) = mh$ and $\tau(H) = 1 - e^{-\phi hm}$. Thus, the per unit value of the DN is $\frac{1}{a}\left[\lambda(n-1)n \times (1 - e^{-\phi hm})\right]$.

It is easy to verify that this example satisfies A1.

[15] The argument that the value of a network is proportional to the square of the number of participants has been used in other contexts, e.g., to explain the impact that increased adoption has on the economic value of social networks such as Facebook or Tencent (e.g., Metcalfe (2013)).

[16] Alternatives include Sarnoff's function, $v \propto n$, Odlyzko's function, $v \propto n \log(n)$, and Reed's function, $v \propto 2^n$.

3 The Satoshi Asset Pricing Model

To further characterize equilibrium prices, we need to provide more structure to consumer preferences and verifiers' profit maximization problem. The demand side follows the guidelines of Sections 1 and 2.2, but we introduce network size risk, to which consumers are risk-averse. On the supply side, we model competition among verifiers in the spirit of Bitcoin's PoW (thus the choice of Nakamoto competition for the game among miners and Satoshi to denote the model) and refer to the DNA as bitcoin. We note, however, that other DNs, such as Litecoin, follow the Bitcoin model and reach verification consensus through PoW implementations (sometimes with different mining algorithms).

3.1 Environment

There are two periods, t and $t+1$, and a DN $\mathscr{F}_B = \{n, 1_{nn}, m, L\}$ with a single asset, bitcoin, whose price p_B we seek to determine. Verifiers are homogeneous miners providing hashrate to the network and competing within PoW consensus. Network trust depends on the total hashrate provided by the miners, H. The total asset supply is $B_t > 0$, thus $L \subset [0, B]^n$. Agents have heterogeneous preferences that can be represented by an additively separable utility function $U : \mathbb{R}^2_+ \to \mathbb{R}$. At time t agents can either consume or purchase a number of bitcoins b which, at time $t+1$, entitles them to DN services. Utility is equal to $e + \theta u\left(bv\right)$, where e represents an endowment and, as in Section 2.2, $v\left(\lambda(n_{t+1}), \tau(H)\right)$ is a function of the future network size n_{t+1} and trust τ that represents the value of the network per bitcoin in units of the consumption good. The parameter $\theta \in [0, \Theta)$ captures agents' desires for DN services, and we thus refer to it as censorship aversion. Consumer types θ are distributed according to a cumulative distribution F_θ. At time t, there are n_t users who form expectations over future network size $n_{t+1} \in [0, N)$ according to a cumulative distribution F_n. Both F_θ and F_n are twice-differentiable with log-concave density functions that are positive everywhere. For simplicity, we take future endowments as deterministic. An agent with type θ then solves

$$\max_b \left(e_t - p_B b\right) + \delta \mathbb{E}_n \left[e_{t+1} + \theta u\left(bv\left(\lambda(n_{t+1}), \tau(H)\right)\right) | \mathcal{F}_t\right], \tag{1}$$

where δ is the time discount factor. We can now formally define an equilibrium in this environment.

Definition 3. *A Satoshi equilibrium in $\mathscr{F}_B$ is a set of holdings decisions by consumers, $\{b(\theta) : \theta \in [0, \Theta)\}$, network hashrate provision decisions by miners, h, and a price, p_B, such that: (i) consumers maximize expected utility, (ii) miners maximize profits, and (iii) the asset market clears: $n_t \left(\int b\left(\theta, p_B\right) dF_\theta\right) = B_t$.*

The following example illustrates a partial equilibrium price (i.e., exogenous τ) in a setting with risk-neutral consumers.

Example 2. Let $u(c) = c$. The solution to program 1 requires $p_B = \theta\delta\mathbb{E}_n\left[v\left(\lambda(n_{t+1}), \tau\right)\right]$. Due to the linearity of the utility function, all consumers with types θ_h satisfying $p_B < \theta_h\delta\mathbb{E}_n\left[v\left(\lambda(n_{t+1}), \tau\right)\right]$ spend their endowment in the asset, i.e., $b(\theta_h, p_B) = \frac{e_t}{p_B}$. Let $\hat{\theta}$ be the marginal investor demanding a positive amount of bitcoin. Market clearing then requires $n_t \int_{\hat{\theta}}^{\Theta} b(\theta, p_B) dF_\theta = B_t$. The equilibrium price and marginal type satisfy the following system: $p_B = \hat{\theta}\delta\mathbb{E}_n\left[v\left(\lambda(n_{t+1}), \tau\right)\right]$ and $p_B = \frac{e_t n_t}{B_t}\left[1 - F_\theta\left(\hat{\theta}\right)\right]$. With a uniform distribution of types, the price is given by

$$p_B = \frac{\frac{e_t n_t}{B_t}\delta\mathbb{E}_n\left[v\left(\lambda(n_{t+1}), \tau\right)\right]\Theta}{\frac{e_t n_t}{B_t} + \delta\mathbb{E}_n\left[v\left(\lambda(n_{t+1}), \tau\right)\right]\Theta}. \tag{2}$$

Equation (2) in this simple example illustrates a general feature: if consumers don't value the services of the DN, i.e., $\Theta = 0$, regardless of the network characteristics, the only equilibrium bitcoin price is $p_B = 0$.

3.2 Nakamoto Competition

Consider m identical risk-neutral miners who act as price takers and contribute hashrate h in a competition to verify blocks of transactions. The network PoW reward is $B_t\rho$ coins with a value equal to $B_t\rho p_B$. Here, ρ represents an inflation rate and, thus, total supply in period $t+1$ is $B_{t+1} = B_t(1+\rho)$. Let $C : h \to \mathbb{R}$ be an increasing, convex, twice-differentiable function that represents the cost of mining. The cost-of-mining function captures all associated costs for a given and known PoW difficulty level.[17] The expected revenue of a miner j providing h_j is $R(p_B, h_j) = B_t\rho p_B \times \pi_{\text{win}}(h_j, h_{-j})$ where π_{win} is the probability of winning the PoW race and h_{-j} represents the hashrate provision of the other $m-1$ miners. We take π_{win} to be proportional to each miner j's hashrate: $\pi_{\text{win}}(h_j, h_{-j}) = \frac{h_j}{\sum_{\kappa=1:m} h_\kappa}$. Optimization of the miner's profits, $\max_{h_j} R(p_B, h_j, h_{-j}) - C(h_j)$, yields the following.

Proposition 1. *(i) The competitive provision of hashrate H^* is given by mh^*, where*

$$h^* C'(h^*) = B_t\rho p_B\left(\frac{m-1}{m^2}\right). \tag{3}$$

Moreover, aggregate hashrate supply satisfies: (ii) $\frac{dH^*}{dp_B} > 0$; (iii) $\frac{dH^*}{dm} > 0$; (iv) $\frac{dH^*}{d\rho} > 0$; and (v) $\frac{dH^*}{d\chi} < 0$ where $\chi := C'(h^*)$.

[17] For simplicity, we do not distinguish here how resources are split among 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 are more efficient than regular CPUs or GPU cards. Instead, other DNAs use memory intensive algorithms (e.g., Litecoin's Scrypt and Vertcoin's Lyra2REv2) for which ASIC miners are less effective in an attempt to preserve high levels of mining decentralization. See Section 6.2 for an extension with endogenous difficulty level.

The resulting network trust $\tau(H)$ is a function of p_B, which is consistent with the characterization of unity in Definition 1. Naturally, ceteris paribus, a higher bitcoin price induces miners to supply more computing resources. The behavior of miners' hashrate supply as a function of the supply-side parameters, as characterized in Proposition 1 (iii)-(v), is key to analyze the response of the equilibrium bitcoin price to changes in the environment. In particular, with homogenous miners, we have $\frac{dH^*}{dm} > 0$, which yields a monotonically positive relation between the number of miners and the system hashrate. Thus, in this environment, system hashrate is a sufficient statistic for the level of network decentralization as defined in Section 2.

3.3 Equilibrium

To summarize the equilibrium implications, in the remainder of the paper we focus on CRRA utility functions $u = \frac{(bv)^{1-\sigma}}{1-\sigma}$, $\sigma > 0$.

Theorem 1. *[Equilibrium Bitcoin Price] Consider the two-period network economy $\mathscr{F}_B = \{n, 1_{nn}, m, [0, B]^n\}$ described above with a single asset, bitcoin, miners competing within a PoW consensus algorithm by providing hashrate h, and consumers maximize intertemporal expected utility by selecting at time t optimal bitcoin holdings b. In a Satoshi equilibrium, type's θ bitcoin demand is $b(\theta, p_B) = \left(\frac{\delta\theta}{p_B}\int v(\lambda(n_{t+1}), \tau(H(p_B))^{1-\sigma} dF_n\right)^{\frac{1}{\sigma}}$; the network hashrate is given by mh^*, where h^* is defined in equation (3), and the bitcoin price satisfies:*

$$p_B = \delta\left(\frac{n_t}{B_t}\right)^{\sigma}\left(\mathbb{E}_\theta\left(\theta^{\frac{1}{\sigma}}\right)\right)^{\sigma}\mathbb{E}_n\left(v\left(\lambda(n_{t+1}), \tau(mh^*(p_B))\right)^{1-\sigma}\right). \tag{4}$$

Theorem 1 characterizes the equilibrium bitcoin price for a given set of primitive functions describing preferences, beliefs, and technology. It also highlights the connection between the equilibrium values of the price and network trust, as driven from equilibrium hashrate, a consequence of *unity*. Interestingly, the reader may interpret Nakamoto's competition as a form of "reversed Cournot's": although miners compete in capacity (h), ceteris paribus, the price is *increasing* in total capacity (H). This is because in Nakamoto's, unlike in Cournot's, miners do not compete in bitcoin units but hashrate units, i.e., units of Bitcoin network trust.

To analyze the properties of the equilibrium, we consider a restriction on the function v.

Corollary 1. *Let A1 hold so that the per-unit network value at time $t+1$ is $\frac{1}{B_{t+1}}\tau(H)\lambda(n_{t+1})$. Then, the equilibrium price satisfies*

$$p_B = \delta\frac{n_t^\sigma}{B_t}\left(\frac{\tau(mh^*(p_B))}{1+\rho}\right)^{1-\sigma}\left(\int\theta^{\frac{1}{\sigma}}dF_\theta\right)^{\sigma}\int\lambda(n_{t+1})^{1-\sigma}dF_n. \tag{5}$$

From Corollary 1 we know that, if $p_B = 0$, $h^* = 0$ and thus H^*. Under A1, $\tau(0) = 0$ and,

therefore, in the absence of mining subsidies, Theorem 1 implies that an equilibrium with $p_B = 0$ always exists. One can show that, under certain conditions, a second equilibrium with a strictly positive price must also exist.

Proposition 2. *[Existence] Assume A1, then an equilibrium with $p_B = 0$ always exists. Moreover, assume $\sigma < 1$, $\mathbb{E}_\theta \theta^{\frac{1}{\sigma}} < \infty$, and let $\tau : \mathbb{R}_+ \to [0, \overline{\tau}]$, $\overline{\tau} < \infty$, be a continuous differentiable function. Let $N \geq n > 1$, with $N \in \mathbb{R}_+$ representing the entire population, with $\lambda(N) < \infty$. Let $C'(0)$ and $C''(0)$ be finite. Then, a Satoshi equilibrium with a strictly positive price exists.*

Intuitively, proposition 2 shows that for a positive price equilibrium to exist, besides a positive mass of agents with $\theta > 0$, it is sufficient for network trust to grow sufficiently fast near a price of zero and that the size of the network effects are bounded. The proposition highlights the fact that, regardless the state of the bitcoin network, both zero and positive bitcoin prices can be rationalized as equilibrium outcomes.[18]

3.4 Explicit Solutions

In this section, we develop an explicit solution by selecting specific primitives $(C, F_\theta, F_n, \lambda, \tau)$. Let us first consider the cost of mining function C.

Assumption 2. *[A2] $C(h) = \frac{c}{2}h^2$ with $c > 0$.*

Corollary 2. *Assume A2. Then, by Proposition 1, $H = \sqrt{B\rho p_B \left(\frac{m-1}{c}\right)}$.*

We next consider the distribution functions for investor types and future network size.

Assumption 3. *[A3] (i) $\theta \sim$ Uniform[0,Θ]; (ii) $n_{t+1} = n_t \nu$, $\nu \sim$ Gamma with shape parameter $\kappa \geq 0$ and scale parameter $\alpha \geq 0$.*

Assumption 3 (ii) reflects the intuition that expectations on future network size are influenced by the current size. The Gamma distribution is analytically convenient as it allows for tractable computation of prices under several network laws λ.[19] None of A3(i)–(ii) are essential to the analysis. By selecting appropriate λ and τ functions that satisfy A1, we can then express the price of bitcoin as a function of parameters only.

[18] However, these two equilibria may not be equally stable in a dynamic economy. For example, the presence of a few "convinced miners," such as those mining bitcoin in 2009-2010 where no apparent market for bitcoin yet existed, could drive the system from a zero price to a positive price.

[19] The same can be said for several of the Gamma distribution particular cases such as the exponential, Erlang, and Chi-squared distributions.

Corollary 3. *Assume A1–A3 and* $\lambda(n_{t+1}) = n_{t+1}^2$. *Moreover, let* $\tau(H) = \frac{H}{\overline{H}}$, $\overline{H} > 0$, *for* $H \leq \overline{H}$ *and* $\tau(H) = 1$ *otherwise. For sufficiently large* $\overline{H}$ *(i.e.,* $\overline{H} > H^*$*), the equilibrium price of Bitcoin is*

$$p_B = \frac{1}{B_t}\left[\delta n_t^{2-\sigma}\Theta\left(1+\sigma\right)^{-\sigma}\left(\frac{\sqrt{\rho}}{1+\rho}\frac{1}{\overline{H}}\right)^{1-\sigma}\left(\frac{m-1}{c}\right)^{\frac{1-\sigma}{2}}\alpha^{2(1-\sigma)}\frac{\Gamma\left(\kappa+2(1-\sigma)\right)}{\Gamma\left(\kappa\right)}\right]^{\frac{2}{1+\sigma}}. \tag{6}$$

The pricing equation (6) is in closed-form and provides a convenient tool to address several quantitative questions related to what drives the value of a bitcoin, which is the topic of Section 5.

4 Implications for the Bitcoin Price

In this section, we perform several comparative statics to investigate the link between the equilibrium bitcoin price and the demand- and supply-side parameters. We consider the conditions in Proposition 1 to hold so that the positive equilibrium price that we study here exists. We also study asymptotic relations between the price and the cost of mining when verification in the network approaches perfect competition.

4.1 Prices and Demand-Side Parameters

Using equation (5), we can study the effect of changes in demand-side parameters. The equilibrium bitcoin price is influenced by the current size of the network, n_t, and consumers' beliefs about future size $\mathbb{E}_n(n_{t+1})$. It is also influenced by preference parameters, namely, censorship aversion $\theta \in [0, \Theta)$ and the curvature of u, σ. As it 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. In the range $0 < \sigma < 1$, the higher the value of $\mathbb{E}_n(n_{t+1})$, the higher the equilibrium price, consistent with economic intuition.[20] We thus discuss comparative statics under such parameter restriction.

Proposition 3. *The bitcoin price (i) increases with the average value of censorship aversion* θ*, (ii) with the average expected size of the future network, and (iii) with the current size of the network,* n_t*. (iv) The price is, in general, non-monotone in the utility curvature parameter* σ*.*

An increase in the current network size n_t increases asset demand raising the equilibrium price. Censorship aversion affects p_B via the scale factor $\left(\int \theta^{\frac{1}{\sigma}} dF_\theta\right)^\sigma$, a quantity that increases with the

[20] On the other hand, when $\sigma > 1$, consumers elasticity of intertemporal substitution (EIS) is low and consumers desire to smooth consumption is high. In the presence of higher expected future network, the expected value of $v(n_{t+1}, \tau)$ is also high. Everything else being constant, the associated wealth effect at $t+1$ induces consumers to value present consumption more and may decrease the demand for bitcoin, lowering its price at time t. This rather counterintuitive relation may not arise in economies with an additional non-DNA investment opportunity that allows agents to consume more in the present while enjoying higher network services in the future. To distinguish risk aversion from EIS, it is possible to consider more flexible preferences such as Epstein-Zin's, but at the cost of additional complexity and without adding significant new insights. We leave such extensions for future work.

average value of θ for a general distribution function F_θ. For a general distribution F_n, $\lambda' > 0$ implies that the equilibrium price at time t is increasing in the expected network size $\mathbb{E}_n(n_{t+1})$. In general, the sensitivity of the price to parameter σ depends on the specific functional form of the primitives. Under the conditions of Corollary 3, for example, the price decreasing with σ.

4.2 Prices and Supply-Side Parameters

The mining market structure, i.e., miner competition, mining rewards, and mining costs, affects the supply of hashrate and thus the trust of the network, τ. The equilibrium price effect of these parameters is as follows.

Proposition 4. *The price of bitcoin (i) increases with the number of miners m and (ii) decreases with the marginal cost of mining. Keeping the miners' reward constant, the price decreases with supply, B_t. Moreover, if τ' is decreasing at the equilibrium hashrate level, then (iii) there is a finite value $\overline{\rho}$ such that, if $\rho < \overline{\rho}$ the price increases with ρ. If, on the other hand, $\rho > \overline{\rho}$, the price decreases with ρ.*

It is immediately clear from Proposition 1 that an increase in the marginal cost of mining induces miners to provide less hashrate, which reduces network trust and ultimately the equilibrium price. An increase in the number of miners intensifies competition and causes a higher equilibrium hashrate and therefore a higher price. The total supply of bitcoins, for a given mining reward at time $t+1$, has the unambiguous effect of reducing the equilibrium price as the asset becomes less scarce. In the Bitcoin protocol, the reward is set as a single parameter as part of the coinbase transaction, not an explicit function of current supply (i.e., $B_t \rho p_B$). This is because the coinbase reward is the unique source of new bitcoins. We, therefore, investigate the effect of changes in the mining reward through changes in ρ.

The price effect of a change in the inflationary reward parameter, ρ, is non-monotonic. The reason is that ρ affects the equilibrium bitcoin price through two channels. The first relates to the monetary incentive for miners to contribute hashrate. ceteris paribus, a larger value of ρ increases H, as equation (3) indicates, and thus increases p_B. The second channel relates to the debasing effect of new bitcoin injections, which, by reducing scarcity, reduces the equilibrium price. The analysis thus suggests that, for a DNA like bitcoin, if the marginal value of trust is decreasing, there exists an optimal monetary policy in the sense of maximizing the market capitalization of the network Bp_B. Although the Bitcoin protocol displays no flexibility regarding the value of ρ, this fact would be of relevance to developers who have the objective to maximize the value of a new network. In a particular parameter environment, the sign of $\frac{\partial p_B}{\partial \rho}$ depends on the incentive-inflation trade-off. We explore this relation quantitatively in Section 5.

4.3 The Cost of Mining Bitcoin with Perfect Competition

Naturally, the intensity of competition among miners also impacts the "minting" cost of a new bitcoin, μ_B, as given by the ratio between the total cost of mining $mC\left(h^*(m)\right)$ and the increase in supply $B_t\rho$. One would expect that, as competition intensifies, profit margins compress, the total hashrate in the system increases and, ceteris paribus, the unitary minting cost increases as well. But what is the minting cost under perfect competition? (i.e., when the number of miners grows unboundedly). The following proposition establishes the limiting behavior under general conditions.

Proposition 5. *Let μ_B be the cost of mining one bitcoin, i.e., $\mu_B = \frac{mC(h^*(m))}{B\rho}$, for a twice differentiable function C. Assume that $\lim_{m\to\infty} p = \bar{p}$ and $\lim_{m\to\infty} \mu_B = \bar{\mu}$. Then, as $m \to \infty$ the price converges to a known proportion of the average cost:*

$$\bar{\mu} = \zeta \bar{p}. \tag{7}$$

$$\zeta = \lim_{m\to\infty} \frac{C'\left(h^*\right)}{\left(C' + h^* C''(h^*)\right)} \tag{8}$$

Proposition 5 yields an interesting insight: as competition intensifies, the minting cost becomes a constant proportion of the bitcoin price and that proportion only depends on the properties of C and not on other parameters of the hashrate supply environment. This provides us with a sharp prediction on the long-term relationship between the price and mining costs in the absence of barriers to entry.

Example 3. (i) if $C(h) = ch^\beta$, $\beta \geq 1$, $\lim_{m\to\infty} \mu_B = \frac{\bar{p}}{\beta}$. (ii) If $C(h) = ae^{\beta h}$, $\lim_{m\to\infty} \mu_B = \bar{p}$.

Under A1, the number of miners impact the equilibrium price through the trust function τ and, therefore, under the conditions of Proposition 2, a finite equilibrium limit price $\bar{p}$ and limit minting cost $\bar{\mu}$ exist.

5 A Quantitative Analysis of the Bitcoin Network and Equilibrium Prices

We consider an explicit equilibrium price like that in Section 3.4 except for the network trust function τ. We parametrize the latter using an exponential model $\tau(H) = 1 - e^{-\phi H}$ which allows for smooth price responses to changes in hashrate provision over $H \in [0, \infty)$. Intuitively, as in Example 1, the probability that the network resists an attack positively depends on system hashrate and price-insensitive factors such as the quality of the code captured by ϕ. More specifically,

$$p_B = \frac{\delta n_t^{2-\sigma}}{B_t} \left(\frac{1 - e^{-\phi\sqrt{B\rho p_B\left(\frac{m-1}{c}\right)}}}{1+\rho} \right)^{1-\sigma} \Theta\left(1+\sigma\right)^{-\sigma} \alpha^{2(1-\sigma)} \frac{\Gamma\left(\kappa + 2(1-\sigma)\right)}{\Gamma\left(\kappa\right)}. \tag{9}$$

We calibrate this economy using a set of observable characteristics at the end of 2017 as shown in Figure 9. At that time, the bitcoin price, p_B, was approximately USD 14,200 (Figure 9a in Appendix B). We interpret time $t+1$ as representing one year after. The value of the calibrated parameters is summarized in Table I.

Supply and Mining. The total supply of Bitcoins, B, is 16.8 million (Figure 9d). The PoW reward parameter ρ is computed on an annual basis using the current supply and a reward of 12.5 bitcoins per mined block (the coinbase transaction as of 2016), with an average of $6 \times 24 \times 365 = 52,560$ per year. Thus, $\rho = \frac{12.5 \times 52,560}{B} \approx 3.9\%$. Blockchain.info provides hashrate distribution statistics showing that the top-10 mining pools (e.g., BTC.com, AntPool, ViaBTC) account, on average, for more than 90% of the system hashrate. We then set $m = 10$. Given (p_B, ρ, m), the cost parameter, c, is obtained by matching the observed hashrate, $H = 15$ exa hashes/second (Figure 9f), and inverting equation 3. We calibrate ϕ next, which we interpret as a network technology parameter that reflects the ability of the network to resist an attack that compromises its security. Intuitively, this parameter reflects the trust of the open-source code and therefore the skills of the (uncompensated) developers that contribute to it. Given the observed hashrate H, we calibrate parameter ϕ to yield a "small" probability of network failure over a given year equal to 0.1.[21]

Network Size and Preferences. We assume that the initial size of the network is the number of unique addresses in transactions at the end of 2017 (Figure 9c), so $n_{2017} = 850,800$. Of course, the number of addresses in a single day of transactions does not equal the total number of users in the network; the latter is surely larger. However, the approximation can be helpful provided there is a stable relationship between these two quantities. We normalize the shape distribution parameter $\kappa = 1$ and set the value of α by, first, fitting an exponential function to the observed number of unique addresses in the network from 2011 to 2017 and, second, extrapolating the value to the end of 2018. This procedure yields $\mathbb{E}(n_{2018}) = n_{2017} \times 1.78$, so the expected size of the network at the end of 2018 is $1,517,984$. The time discount parameter, δ, is consistent with values in standard asset pricing. $\sigma = 0.5$ captures the notion that the representative bitcoin investor is not highly risk-averse. Given the value of all other parameters, the censorship aversion coefficient Θ is set to match the observed price of USD 14,200 by inverting equation 6.

5.1 How do Demand Shocks Affect the Price?

Figure 2 shows the effect of two demand-side parameters: n_t and σ. The value of bitcoin is increasing with the current and expected sizes of the network, which relate through A3(ii). A threefold increase

[21] Of course, it is not possible to calibrate this probability directly as there are no registered successful attacks to Bitcoin in its history. Given the observed resilient of the Bitcoin network, we view 0.1 as a rather conservative value.

TABLE I
Bitcoin Price Calibration: Parameter Values

	Supply and Mining					Network Size			Preferences		
Parameter	ρ	m	B	c	ϕ	n	α	κ	δ	σ	Θ
Value	0.039	10	16.8E+6	3.73E+8	0.153	850,800	1.78	1	0.98	0.5	229

in the current network size corresponds to an increase in the bitcoin price from USD 14,200 to 77,627.[22] A higher expected network size increases expected marginal utility of bitcoin holdings, thus increasing current demand and increases the price. In turn, since miners' incentives are proportional to p_B, the competitive provision of hashrate increases, thus increasing the equilibrium H and further increasing p_B due to unity. Indeed, tripling n_t increases H from 15 to 35 EX/sec.[23]

An increase in the curvature of the CRRA function, proxied by the parameter σ, has the effect of reducing p_B as bitcoin holdings are risky due to the uncertainty about the future network size. In particular, the calibration shows that a 20% increase in σ significantly reduces p_B to USD 2,418.[24] The roles played by the expected network size and risk attitude (σ) are interesting since it helps to explain the significant observed volatility of bitcoin prices. Changes in expectations about regulatory policies affecting future network size, for example, have large direct implications on the equilibrium valuation. Moreover, the price changes can be dramatic if, in turn, policy shocks induce a regulation-fear increase in risk aversion. We discuss implications for price volatility further in Section 6.

The supply side of verifications in $\mathscr{F}_B$ is equally important, but changes in mining parameters lead to more moderate price responses relative to changes in preferences and network size. We investigate some quantitative effects of the former next.

5.2 Do Increases in Mining Costs Raise the Price?

It is sometimes informally argued that the cost of mining bitcoins serves as a "price floor" for the asset. The Satoshi equilibrium does not display such property (Proposition 4). Figure 3 illustrates this fact by displaying the effects of changes in the cost parameter c on equilibrium prices (left panel) and hashrate (right panel). A 90% decrease in c leads to a price increase to USD 14,970 while a 100% increase in the same parameter leads to a drop in bitcoin prices to USD 13,330. Shocks that affect the cost of mining, e.g., electricity costs or mining taxes, thus have traceable implications on the

[22] The calibration also shows that, naturally, the bitcoin price is also sensitive to changes in the expected network size keeping n_t stays constant. An increase in the distribution scale parameter α from 1.78 to 4, keeping n_t constant, shows a more than twofold increase in the equilibrium price to USD 33,142.

[23] With $m = 20$, the same change in n_t increases H to 51 Ex/sec.

[24] The equilibrium p_B is, naturally, also sensitive to the censorship aversion distribution in the network. In this parametrization, as we increase Θ by 50%, keeping everything else constant, p_B increases by a similar factor to USD 21,798.

Figure 2. USD Bitcoin Price: Demand-Side Comparative Statics.

The panel on the left shows the effect of changes in the network size (n_t) on the equilibrium price. The panel on right shows the effect of changes in relative risk aversion (σ). Parameter values are described in Table I.

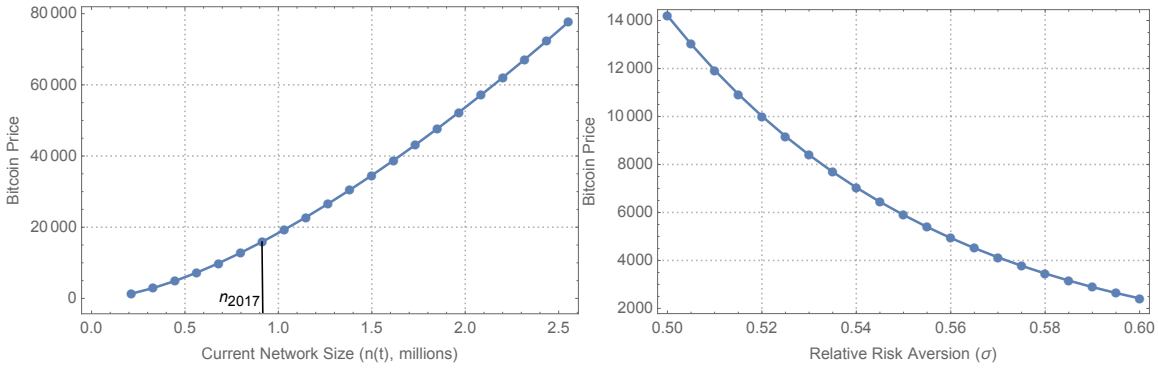
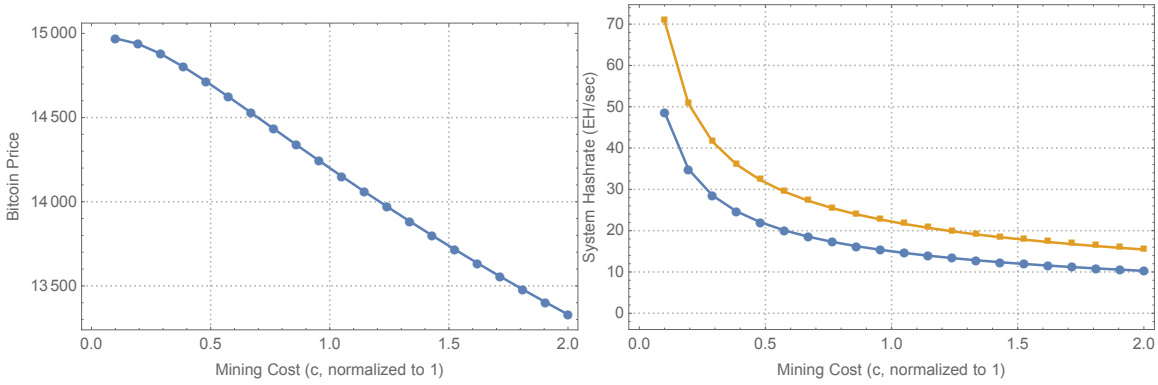


Figure 3. USD Bitcoin Price and Hashrate: Changes in Mining Costs.

The panel on the left shows the effect of changes in mining costs (c) on the equilibrium price (left panel) and system hashrate (right panel). Parameter values are described in Table I.



bitcoin price. The negative effect on mining costs on the price relate to hashrate supply. To study the quantitative effects on hashrate, we consider two different competitive environments with 10 and 20 miners. We can see that when the number of miners doubles, the system hashrate increases from the baseline 15 to 22.18 EX/sec. The system hashrate is convex in the cost parameter. A 90% reduction of c increases H significantly to about 50 EX/sec with 10 miners and over 70 EX/sec with 20 miners. An increase of 100%, on the other hand, induces a decrease to 10.3 and 15.43 EX/sec, respectively.

5.3 How do Miners and Developers affect the Price?

Bitcoin network security can be achieved by either increasing the number of miners, thus increasing system hashrate (Proposition 1) or by "writing a better code," a channel that is captured here in a stylized fashion by the effect of the resistance to attacks parameter ϕ on network trust, τ. Indeed, if a major glitch in the code were to drive ϕ to zero (e.g., if minting of new bitcoins were possible without PoW, allowing for double-spending), the only equilibrium price would be $p_B = 0$. As the number of miners triples to 30, the equilibrium bitcoin price increases from USD 14,200 to 14,863 (see left panel of Figure 4). Similarly, increases in ϕ lead to less than proportional increases in p_B. Doubling ϕ, for example, increases the price to USD 14,900. Since both the price impact of miners and developers occur through the network trust function τ, the perfect competition limit price ($m \to \infty$, $\phi > 0$) and "perfect code" limit price ($\phi \to \infty$, $m \geq 2$) coincide at USD 14,974.

5.4 Do Reward Halving Increase the Price?

Bitcoin inflation decreases every four years at a predictable rate ($\rho_{2020} = 0.5\rho_{2016} = 0.25\rho_{2012}$).[25] But do "reward halving," as it is often informally argued, increase the bitcoin price? As discussed in Proposition 4, if the marginal value of trust is decreasing, an increase in the inflation reward ρ has a non-monotonic effect on p_B. That is, for small values of ρ, injections of bitcoins increases their equilibrium price and the sign is the opposite for large values of ρ. The right panel of Figure 4 shows that the equilibrium price is indeed concave in ρ. Thus, whether a predictable reward halving has a positive effect on the price, depends on which side of the network market capitalization maximizing value, $\overline{\rho}$, the system is currently at.[26]

5.5 How do Costs and Demand Affect Miners' Profits?

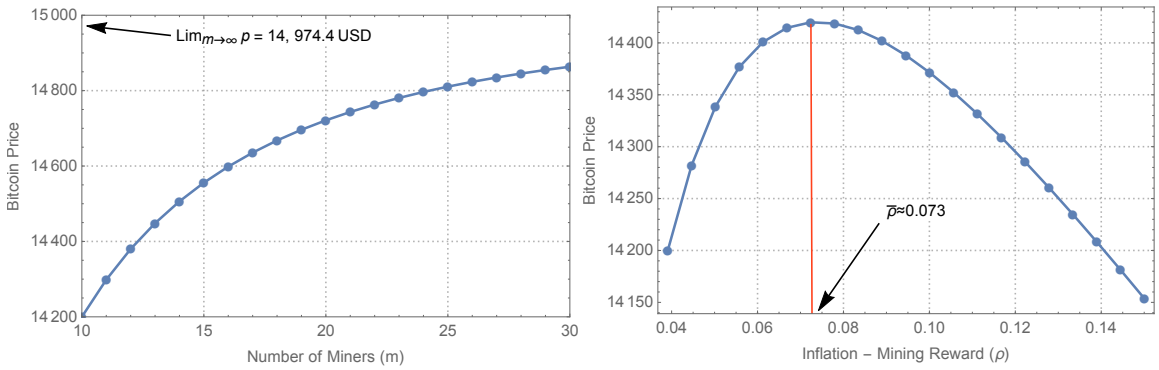
Figure 5 displays the effects of changes in network size (left panel) and mining costs (right panel) on miners' profits. We consider two different competitive environments with 10 and 20 miners. We can see that when the number of miners doubles, profits decrease from USD 512m to only USD 254m per mining pool. An increase in the current size of the network has a significant effect on profits due to higher demand for bitcoins at time t and a change in the expected size of the network at time $t+1$. With 10 miners, tripling n_t increases profits to more than USD 2.8b per mining pool. With 20 miners, the same change in n_t increases profits per mining pool to USD 1.34b. Miners

[25] One simplification in this environment is that miners do not collect fees. 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.

[26] In the calibration, the network market capitalization maximizing inflation value, $\overline{\rho}$, is approximately 7.3%, a value that is greater than $\rho_{2017} \approx 3.9\%$. We note that this calibration exercise is limited in reach and intended as an academic quantitative exploration the bitcoin price and not as investment advice. In particular, $\overline{\rho}$ depends on difficult to calibrate parameters like ϕ. A more secure network would likely display a lower value of $\overline{\rho}$, implying that the upcoming 2020 reward halving could also increase be price.

Figure 4. USD Bitcoin Price: Changes in the Number of Miners and the Inflation-Reward Parameter.

The panel on the left shows the effect of changes in the number of miners (m) on the equilibrium price. The panel on right shows the effect of changes in inflation-reward parameter (ρ). Parameter values are described in Table I.



profits are much less sensitive to changes in c as changes in this parameter cause more moderate price reactions. For example, an increase of 100% in c reduces profits by 6.28% and 3.22% with 10 and 20 miners.[27] As discussed in Section 4.3, an increase in the number of miners impacts the minting cost of a bitcoin, μ_B. In particular, doubling the number of miners increases the minting cost from USD 6,388 to 6,992. The calibration analysis uses A2 and, therefore, by Proposition 5, $\lim_{m\to\infty} \mu_B = \frac{\bar{p}}{2} =$ USD7,487.

5.6 The General Equilibrium Pricing Implications of Unity

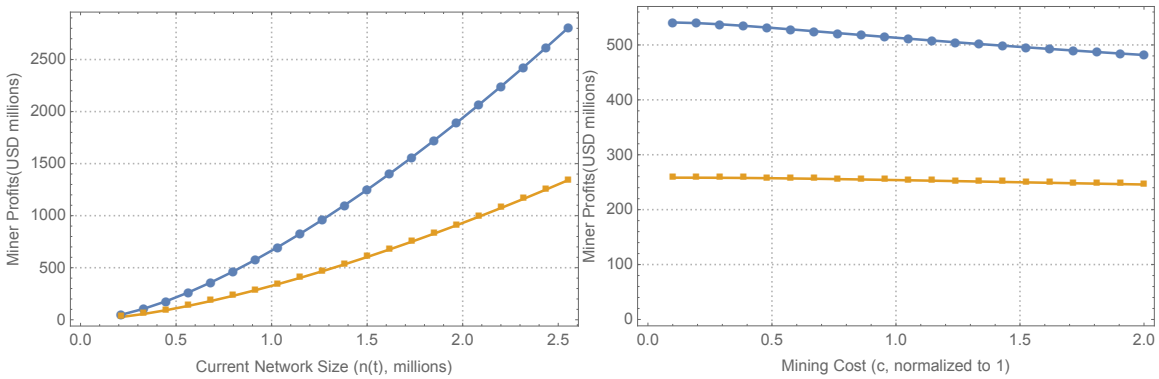
To illustrate the price-hashrate feedback effect embedded in the unity property of bitcoin and DNAs, Figure 6 displays both a general and a (fictitious) partial equilibrium price schedule for different network sizes. The left panel shows price schedules for the baseline calibration. The partial equilibrium price is computed using a formula analogous to that in equation (9), but with a price-insensitive hashrate of 15 EX/sec (i.e., a fixed value regardless of network size). We can observe that the general equilibrium price schedule is steeper than its partial equilibrium counterpart and, thus, its price is lower (higher) for network sizes that are lower (higher) than the baseline value of $850,800$ (for which the endogenous hashrate is exactly equal to 15 EX/sec).

The price gap between the general and the partial equilibrium prices depends on the trust of the open-source code, captured by ϕ, that, for a given H, determines the network resistance to attacks. Intuitively, a network that is more prone to attacks, displays a higher sensitivity to changes in network size because an increase (decrease) in price leads to more significant changes in network trust. The right panel of Figure 6 displays a case where $\phi = 0.015$, a value that is ten times

[27] We study in Section 6.2 an extension where the cost function parameter depends on hashrate choices.

Figure 5. Equilibrium Miners' Profits

The left panel shows the effect of the network size (n_t) on miner profits. The right panel shows the effect of the cost parameter c on miner profits. The circle- and square-dotted lines correspond to networks with 10 and 20 miners, respectively.



lower than in the baseline calibration and, thus, leads to a probability of a successful attack that is eight times larger. Under such conditions, the price gap is large, e.g., for a network size equal to $2.5n_{2017}$, the difference between the general and the partial equilibrium prices exceeds USD 20,000 per bitcoin. Failing to consider the fixed-point character of DNA valuation, therefore, could lead to severe mispricing.

6 A Discussion of Implications for Bitcoin Price Volatility

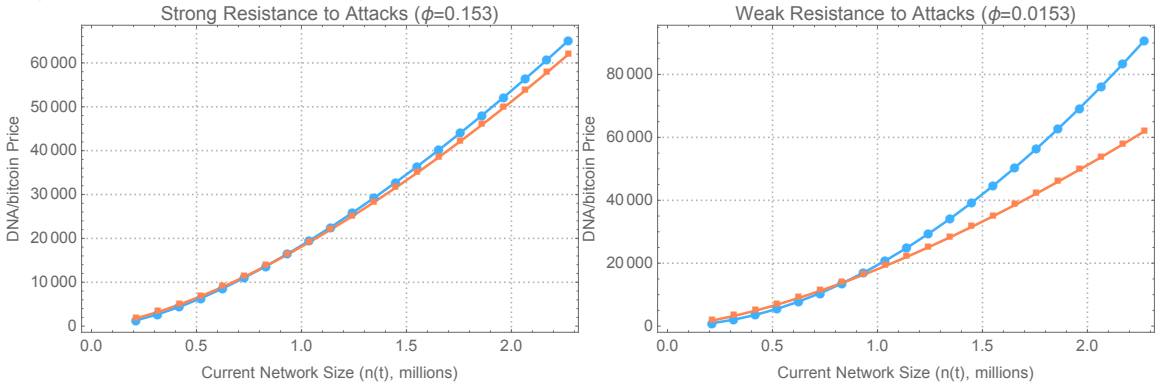
This section discusses the implications of the model for bitcoin price volatility, mining activity, and regulatory actions.

6.1 Price-Hashrate Spirals

As discussed in Sections 3-5, the unity property has implications for the behavior of bitcoin prices and those of related DNAs. We describe here the intuitive effects of a sudden demand shock that, over time, could lead to a price-hashrate spiral. Consider, for instance, a sudden drop in the expected number of future network users, $\mathbb{E}_n(n_{t+1})$. The immediate effect is to reduce the expected value of $v(\lambda(n_{t+1}), \tau(H))$. As a consequence, the price drops. The non-linearity of the price functional (4), however, can give rise to a price spiral because the initial price drop reduces the economic incentive for miners to provide hashrate thus reducing network trust τ. As a consequence, the expected value of $v(\lambda(n_{t+1}), \tau(H))$ drops even further and, therefore, it induces additional negative pressure to the bitcoin price. The feedback loop continues until the new equilibrium price and hashrate are achieved. The additional volatility induced by the initial shocks is, as described in Theorem 1, not evidence of "irrational exuberance" and depends on the sensitivity of network trust to hashrate,

Figure 6. The General Equilibrium Pricing Implications of Unity

This figure shows the behavior of the equilibrium bitcoin price (blue circle-dotted line) and that resulting from a partial equilibrium where network trust is kept constant (orange square-dotted line). The left (right) panel shows prices as a function of current network size for the baseline ϕ value (lower than baseline value). Parameter values are described in Table I.



$\tau'(H)$, and miners' sensitivity to the value of the verification rewards, $H'(p)$. The price-hashrate spiral is illustrated by the solid-line connections in Figure 7.

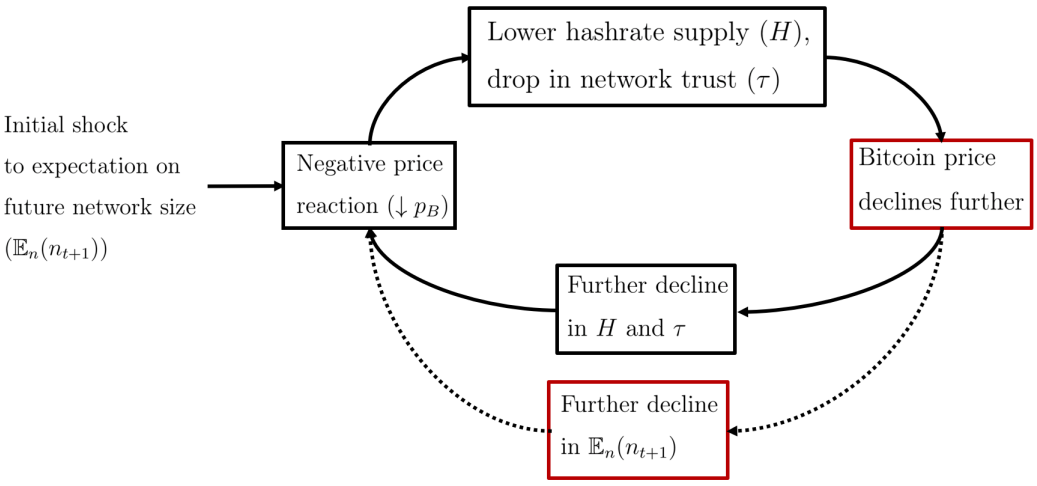
Price swings could be even stronger if the initial price decline lowered expectations on n_{t+1} even further. Consider, for example, a setting where bitcoins trade globally around the clock, but with informational frictions due to rational inattention. Bitcoin holders in country A may learn about a negative shock to $\mathbb{E}_n(n_{t+1})$ (e.g., a national ban) before consumers in country B. The latter only update their information sets on the ban after observing a significant price decline (a "bitcoin crash" reported in the news). The additional negative pressure on the price induces consumers in country C to update their expectations on n_{t+1} and so on. Such a, arguably realistic, price-hashrate-expectations spiral is illustrated by the solid and dotted-line connection in Figure 7.

6.2 Adjustments in Mining Difficulty

In the static model of Section 3, the cost of mining, like all other functions, is characterized by time-invariant parameters. In the Bitcoin network, on the other hand, adjustments to the difficulty level of the PoW algorithm may occur approximately every two weeks (2016 blocks) as a function of the average block confirmation time over that two-week period. Motivated by this fact, we consider in this section an extension where the difficulty level is, similarly, endogenously determined. The intuition that the extension conveys is that the addition of endogenous difficulty level creates a cushioning effect on the system hashrate and thus may tamper bitcoin price volatility.

Let the cost of mining for miner j be $\tilde{C}(h_j, h_{-j}) = d(H)C(h_j)$ where h_{-j} represents the hashrate provision of the other $m-1$ miners, d represents the difficulty level and, as in Section 3.2, $C(h_j)$ is an increasing function of h_j only. Following the logic of the Bitcoin network, we set $d(H) = \eta H$, where

Figure 7. A Price-Hashrate Spiral



η represents a target block confirmation time (currently 600 seconds) and H is the hashrate. Thus, the expected revenue of a miner j providing h_j is $\Pi(p_B, h_j, h_{-j}) = B_t \rho p_B \times \pi_{\text{win}}(h_j, h_{-j}) - \eta H C(h_j)$. Optimization of the miner's profits yields the following.

Proposition 6. *With an endogenous difficulty level, the competitive provision of hashrate is given by $m\hat{h}$, where*

$$\hat{h}\left[C(\hat{h})\eta + \eta m\hat{h}C'(\hat{h})\right] = B_t \rho p_B \left(\frac{m-1}{m^2}\right). \tag{10}$$

Moreover, under A2, the optimal hashrate supply satisfies $h^* > \hat{h}$ when the mining reward is sufficiently high and $h^* < \hat{h}$ when the mining reward is sufficiently low.

By replacing C' for $\tilde{C}'$ in the proof of Proposition 4, one can also see that the first order condition (10) still implies that a higher marginal cost of mining lowers the equilibrium price.

6.3 Local Regulatory Actions

Several countries have either introduced or considered introducing regulatory measures to limit the use of DNAs, for example by limiting the transfers from bank deposits to bitcoin exchanges. Our framework helps explaining how limiting the size of a DN, for example, can have multiple-fold implications on equilibrium prices through changes in current demand or expectations of future network size. A further implication is that the impact of regulatory restrictions in countries with a large number of miners, such as the People's Republic of China, is possibly of greater significance than that in countries with a similar number of users but a smaller number of miners, such as the United Kingdom. Indeed, until 2017, China had become home to one of the largest bitcoin mining

industries due to its inexpensive power and local chipmaking factories. In early 2018, however, the People's Bank of China has proposed measures to forbid mining activities in the country. Thus, in addition to reducing the expected number of bitcoin nodes in China, such regulations could have the effect of reducing global network trust. As a consequence, everything else being constant, a bitcoin ban in China has a greater price impact potential than an equivalent regulation in the United Kingdom.

As discussed in Section 2, however, one of the key properties of DNs is offering CR in transactions. Therefore, an unintended consequence of participation restrictions could be an increase in the fundamental demand for CR, i.e., an increase in the mean value of θ. If such feedback effect on preferences were significant, the long-term price impact of restricting participation could, in principle, be positive.[28]

7 Concluding Remarks and Extensions

To focus on the critical valuation mechanism in a DNA and keep the analysis tractable, we have made several simplifying assumptions. This section briefly discusses some limitations and suggest several exciting extensions to this base model, which we leave to future research.

1. *Speculative Demand for Bitcoins.* We have modeled an equilibrium model of the bitcoin market where demand stems from the value of DN services. Arguably, a portion of the observed bitcoin demand also stems from pure speculative motives. It would be interesting to add a population of speculators, possibly with $\theta = 0$, to that of consumers with a fundamental demand for bitcoins and analyze the resulting equilibria with and without short-selling constraints. Such extension would allow one to study the relative importance of speculation as a source of volatility vis-a-vis the fundamentals of the bitcoin market.

2. *Competition and the Threat of Entry.* Regulation is not the only factor that can influence $\mathbb{E}_n(n_{t+1})$. Indeed, the proliferation in recent years of alternatives to Bitcoin introduces a different source of risk for any similar asset, namely, consumers may derive higher utility from emergent competing network, thus undermining the value of network externalities to the incumbent ones. The game-theoretic specifics of these threats are complex to model as decision making and governance in DNs are strikingly different from those in traditional firms.

3. *Multiple periods and continuous time.* Suppose there is an exogenous process of network adoption, $\{n_t\}$, which follows an Ito process dn_t, and an endogenous process of network trust $\{\tau_t\}$ which characterize the state of the network. Let $\mathcal{A}V$ be the infinitesimal generator applied to the value function $V(t, n_t, \tau_t)$. Then the optimal holdings of bitcoins need to satisfy the following

[28] Such feedback effect on preferences finds non-financial counterparts. For example, the disclosure of secret government surveillance programs (e.g., the Edward Snowden disclosure) has, arguably, increased the underlying demand for the ability of text messaging apps to provide strong encryption.

Bellman-Jacobi equation: $\delta V(t, n_t, \tau_t) = \max_b \{u(t, n_t, \tau_t) + V_t(t, n_t, \tau_t) + \mathcal{A}V(t, n_t, \tau_t)\}$, for some process $dn_t = \mu_i(t)dt + dW_t$. One can conjecture that the final solution is a stochastic process for b_t with $db_t = \mu_b(n_t, \tau_t)dt + \sigma_b(n_t, \tau_t)dW_t$. Since p_B is a non-linear function of the Brownian process b_t, the volatility of the price process depends on the uncertainty about the adoption rate and σ_b.

4. *Alternative consensus algorithms.* We have modeled the supply of hashrate in a fashion that resembles PoW, where miners add external resources to the system to increase the probability of verifying a block of transfers. Not every DN uses PoW though. Exceptions with considerable market capitalization include NEO, Ripple, and Cardano. It would be interesting to analyze the equilibrium pricing implications of a different consensus mechanism. In proof-of-stake, for example, the probability of verifying can be tied to DNA holdings directly and thus all nodes could, in principle, earn verification rewards. Much of the analysis in this paper could be of use for these alternative assets, but the economics of Section 3.2 would change.

5. *Heterogeneous miners.* We have modeled competition among identical miners. As a consequence, the system hashrate is a sufficient statistic for network decentralization. If, on the other hand, the system had large and small miners, modeling trust may be more complex. In particular, one may consider $\tau : H \times F_H \to \mathbb{R}$ where F_H represents the distribution of total hashrate among miners.

6. *Structural Estimation of Network Utility.* The literature in economics and finance has long debated the specific form of a network utility in the context of the internet or personal ties. Unlike other protocols with network effects, Bitcoin and similar DNAs are *traded*. A researcher may exploit this fact and use an empirical version of our model to estimate deep parameters. For example, the equations in Section 3 offer moment restrictions such as

$$p_B - \text{parameters} \times \left(\mathbb{E}_\theta\left(\theta^{\frac{1}{\sigma}}\right)\right)^\sigma \mathbb{E}_\text{n}\left(v\left(\lambda(n_{t+1}), \tau(H)\right)^{1-\sigma}\right) = 0,$$

that a researcher may exploit to learn about deep parameters of λ or τ based on DNAs prices and using GMM-like methods. Alternatively, a researcher may be interested in deep preference parameters such as those reflecting censorship aversion.

7. *Portfolios of DNA*s. Another interesting extension is to allow for competing DNAs and the formation of "crypto portfolios." In the context of our framework, DNAs 1 and 2 can be differentiated due to their relative investor base, $n_{1,t}/n_{2,t}$, the consensus algorithm (e.g., proof of work vs. proof of stake), their specific network effects λ_i, their supply B_i or inflation rate ρ_i, transaction speed, fees, governance, and anonymity, etc. What would be the resulting equilibrium prices in the presence of heterogeneous preferences over such features?

8. Forks. The economics in this model could serve as the starting point of a model with forks. Forks can occur because, for instance, developers create an update of the protocol without full community consensus. Examples include the hard fork of Ethereum Classic from Ethereum in 2016

and Bitcoin Cash from Bitcoin in 2017. The fork creates two networks, "legacy" and "new," with two different ledgers, L_{leg} and L_{new}. If the fork occurs between times t and $t+1$, consumers who hold b units of the DNA at time t will then hold b units of *both* networks at time $t+1$. Before any portfolio rebalancing, i.e., with constant n, the consumer then enjoys a new utility level that can be written as $u\left[b\left(v_{\text{leg}}\left(\lambda(n),\tau(H_{\text{leg}})\right)+v_{\text{new}}\left(\lambda(n),\tau(H_{\text{new}})\right)\right)\right]$. If the PoW mining algorithm remains the same, miners will allocate hashrate across chains and we would expect, during equilibrium, that they remain indifferent to which is mined as they stay equally profitable. For example, both Bitcoin and Bitcoin Cash use SHA-256. If the algorithm changes, however, miners of the legacy chain may be unable to use their ASIC hardware to mine the new chain (e.g., the Bitcoin Gold fork in November 2017). Each case has different implications for the resulting network qualities H_{leg} and H_{new} and, therefore, for the long-term price relation between the forked tokens.

References

Allen, F. and D. M. Gale (2000, feb). Financial Contagion. *Journal of Political Economy 108*(1), 1.

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

Belo, F. (2010). Production based measures of risk for asset pricing. *Journal of Monetary Economics 57*(2), 146–163.

Berk, J. B., R. C. Green, and V. Naik (1999). Optimal investment, growth options, and security returns. *Journal of Finance 54*(5), 1553–1607.

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

Bramoulle, Y., A. Galeotti, and B. Rogers (2016). *The Oxford Handbook of the Economics of Networks*. Oxford University Press.

Cochrane, J. (1988). Production-based asset pricing. *Unpublished working paper 2776. National Bureau of Economic Research, Cambridge, MA.*.

Cochrane, J. (1991). Production-based asset pricing and the link between stock returns and economic fluctuations. *Journal of Finance 46*, 207–234.

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

Cooper, I. (2006). Asset pricing implications of non-convex adjustment costs and irreversibility of investment. *Journal of Finance 61*(1), 139–170.

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

Easley, D., M. O'Hara, and S. Basu (2017). From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Working Paper*.

Economides, N. (1996, oct). The Economics of Networks. *International Journal of Industrial Organization 14*(6), 673–699.

Eisfeldt, A. and D. Papanikolaou (2013). Organization capital and the cross-section of expected returns. *Journal of Finance 68*(4), 1365–1406.

Hansen, L. P. and S. F. Richard (1987). The Role of Conditioning Information in Deducing Testable Restrictions Implied by Dynamic Asset Pricing Models. *Econometrica 55*(3), 587.

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. *Working Paper*.

Jermann, U. (1998). Asset Pricing in Production Economies. *Journal of Monetary Economics*, 257–275.

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

Kogan, L. (2004). Asset prices and real investment. *Journal of Financial Economics 73*, 411–431.

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

Li, E., D. Livdan, and L. Zhang (2009). Anomalies. *Review of Financial Studies 22*, 4301–4334.

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

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*.

Pagnotta, E. S. and T. Philippon (2017). Competing on Speed. *Econometrica forthcomin*.

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*.

Saleh, F. (2017). Blockchain Without Waste: Proof-of-Stake. *Working Paper*.

Shaked, A. and J. Sutton (1982). Relaxing Price Competition Through Product Differentiation. *Review of Economic Studies 44*, 3–13.

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

Wood, G. (2018). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, 1–32.

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

Proofs

Proof of Proposition 1

Part (i). Miner j takes the price as given and solves $\max_{h_j} B\rho p p_B \times \pi_{\text{win}}(h_j) - C(h_j)$, with first order condition $B\rho p p_B \frac{\partial \pi_{\text{win}}(h_j^*)}{\partial h_j} = C'(h_j^*)$. Using $\frac{\partial \pi_{\text{win}}}{\partial h_j} = \frac{H-h_j}{H^2}$ we get $B\rho p p_B = \frac{C'(h_j^*)H^2}{H-h_j^*}$. With symmetric identical miners, $H = hm$. So the equilibrium symmetric hashrate satisfies $C'(h^*)h^* = B\rho p p_B \frac{m-1}{m^2}$.

Parts (ii)-(v) can be proved by applying the implicit function theorem to express the near-equilibrium response in h^* for each corresponding 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 totally differentiating the first-order condition, $\frac{dh^*}{dm}[C'(h^*)+h^*C''(h^*)] - B\rho p p_B \frac{m^2-2m(m-1)}{m^4} = 0$. From $H^* = mh^*$, it follows that $\frac{dH^*}{dm} = h^* + m\frac{dh^*(m)}{dm}$. Thus, $\frac{dH^*}{dm} = h^* - \frac{(m-2)}{m^2}\frac{B\rho p}{(C'+h^*C'')}$. Multiplying both sides of the latter inequality by $C'(h^*) > 0$, we have

$$h^*C'(h^*) - \left(\frac{m-2}{m-1}\right)\left(\frac{m-1}{m^2}B\rho p p_B\right)\frac{C'(h^*)}{(C'+h^*C'')} > 0$$

Since, in equilibrium, $h^*C'(h^*) = B\rho p\frac{m-1}{m^2}$, the previous condition is equivalent to $\frac{(m-1)}{(m-2)} > \frac{C'}{(C'+h^*C'')}$. The term $\frac{(m-1)}{(m-2)}$ is greater than 1 for any $m \geq 2$. By $C'' > 0$, the right-hand side is lower than one. We conclude that $\frac{dH^*}{dm} > 0$. For (iv), $\frac{dh^*}{d\rho} = Bp_B\frac{m-1}{m^2}[C'(h^*) + h^*C''(h^*)]^{-1} > 0$. The result follows. For (v), $\chi\frac{dh^*}{d\chi} = -h^*$. Since $\chi > 0$, then $\frac{dh^*}{d\chi} < 0$ and $\frac{dH^*}{d\chi} < 0$. □

Proof of Theorem 1

From the first order condition of the consumer program (1), optimal holdings b_θ for an individual with type θ satisfy:

$$b\left(\theta, p_B\right) = \left(\frac{\delta}{p_B}\right)^{1/\sigma} \theta^{1/\sigma} \left[\int v\left(\lambda\left(n_{t+1}\right), \tau\right)^{1-\sigma} dF_n\right]^{1/\sigma}.$$

The market clearing conditions require that the total demand of bitcoins $n_t \int b_\theta dF_\theta$ is equal to the supply B_t. Thus, $n_t \left(\frac{\delta}{p_B}\right)^{1/\sigma} \left[\int \theta^{1/\sigma} dF_\theta\right] \left[\int v\left(\lambda\left(n_{t+1}\right), \tau\right)^{1-\sigma} dF_n\right]^{1/\sigma} = B_t$. Consumers' optimizations and market clearing thus imply the following partial equilibrium price:

$$p_B(H) = \delta \left(\frac{n_t}{B_t}\right)^{\sigma} \left[\int \theta^{1/\sigma} dF_\theta\right] \left[\int v\left(\lambda\left(n_{t+1}\right), \tau(H)\right)^{1-\sigma} dF_n\right]. \tag{11}$$

Miners' optimal supply is, for a given p_B, $h^*(p_B)$, where h^* is characterized by equation (3) in Proposition 1. With homogeneous miners, hashrate in the system is given by $H^* = mh^*$. Thus, if one finds a value $p_B \geq 0$ that satisfies

$$p_B = \delta \left(\frac{n_t}{B_t}\right)^{\sigma} \left[\int \theta^{1/\sigma} dF_\theta\right] \left[\int v\left(\lambda\left(n_{t+1}\right), \tau(mh^*(p_B))\right)^{1-\sigma} dF_n\right],$$

then p_B is a Satoshi equilibrium price. □

Proof of Proposition 2

By Proposition 1, with $p = 0$ miners always provide zero hashrate and $H = m \times 0 = 0$. Under A1, $\tau(H(0)) = 0$. Thus an equilibrium with $p = 0$ always exists.

To prove the existence of an equilibrium with strictly positive price, let

$$f(p, \omega) := \left(\tau\left(H(p)\right)\right)^{1-\sigma} \delta \frac{n_t^\sigma}{B_t} (1+\rho)^{\sigma-1} \left(\int \theta^{\frac{1}{\sigma}} dF_\theta\right)^{\sigma} \int \lambda\left(n_{t+1}\right)^{1-\sigma} dF_n, \tag{12}$$

which can be written as $f(p) = \left(\tau\left(H(p)\right)\right)^{1-\sigma} \mathrm{f}$ where f is independent of p. Since $\lambda(N) < \infty$ and $\mathbb{E}_\theta \theta^{\frac{1}{\sigma}} < \infty$, f is bounded above. Thus, by A1, (a) $f(0) = 0$. As $p \to +\infty$, $\lim f(p) \leq (\overline{\tau})^{1-\sigma} \mathrm{f} = \overline{p}$. Thus, for p sufficiently large, (b) $f(p) < p$. Consider now the following limit:

$$\begin{aligned}\lim_{p \to 0^+} f'(p) &= \lim_{p \to 0^+} \mathrm{f}\,(1-\sigma)\, \frac{\tau'(mh^*(p))}{\tau^\sigma(mh^*(p))} \frac{dH^*(p)}{dp}. \\ &= \mathrm{f}\,(1-\sigma)\, B\rho \frac{m-1}{m} \lim_{\mathbf{p} \to \mathbf{0}^+} \frac{\tau'(mh^*(p))}{\tau^\sigma(mh^*(p))} \left[C'(h^*) + h^* C''(h^*)\right]^{-1}.\end{aligned}$$

where the second equality stems from the proof of Proposition 1(ii). Using $\lim_{p \to 0^+} h^*(p) = 0$ from

Proposition 1, $C'(0)$,$C''(0) < \infty$, and $\tau(0) = 0$ from A1, we conclude that $\lim_{p\to 0^+} f'(p) = \frac{+}{0} = +\infty$. Therefore, (c) $f(p) > p$ in a neighborhood of zero. Results (a)-(c) imply that, if τ is continuous, the assumptions of the proposition are sufficient for $f(p)$ to equal p for a strictly positive value of p.

Example: Panel (a) of Figure 8 illustrates the intuition of the proof by showing the point of intersection between $f(p)$ and p using $\tau(H) = 1 - e^{-\phi H}$ as in Section 5. In this economy, there is a unique strictly positive equilibrium price. In general, the total number of equilibria depends on the specific functional forms of $\tau(H)$ and $H(p)$.

We note that sufficient conditions for the existence of a positive equilibrium price could be derived in the absence of A1, i.e., by establishing a more general relation between functions v and τ. □

To prove the following proposition, we first state and prove a lemma.

Lemma 1. *Assume the conditions in Proposition 2 so a positive equilibrium price p exists. Let $F(p,\omega) := p - f(p,\omega)$ where ω is a parameter of the model and $f(p) = (\tau(H(p)))^{1-\sigma}\,\mathrm{f}$ is given by equation (12). Then, around the equilibrium positive price (i) $\frac{dp_B}{d\omega} = \frac{f_\omega}{1-f_p}$ and (ii) $f_p < 1$. Thus, the sign of $\frac{dp_B}{d\omega}$ is the same as f_ω.*

Proof. Part (i) is simply an implication of the Implicit Function Theorem. Part (ii). From the assumptions in Proposition 2, we know that for $\lim_{p\to 0^+} f_p > 1$. Moreover, we know that $f(p)$ is bounded above so that $\lim_{p\to\infty} f_p < 1$. Therefore, if $f(p)$ is continuous, at $f(p) = p$ we must have that $f_p < 1$. Thus, $\frac{dp_B}{d\omega} \geq 0$ if and only if $f_\omega \geq 0$.

Panel (b) of Figure 8 illustrates this fact for the baseline calibration. The value of f_p near the equilibrium price of USD 14,200 is indeed lower than 0.1. □

Proof of Proposition 3.

Parts (i)-(ii) Consider the equilibrium price in equation (5):

$$p = \delta \frac{n_t^\sigma}{B_t} \left(\frac{\tau(H(p))}{(1+\rho)} \right)^{1-\sigma} \left(\int \theta^{\frac{1}{\sigma}} dF_\theta \right)^\sigma \int \lambda \left(n_{t+1}\right)^{1-\sigma} dF_n.$$

We can write the price as $p = X(\mu_\theta)Y(p)$, where $X(\mu_\theta) := \left(\mathbb{E}_\theta \left(\theta^{\frac{1}{\sigma}} \right) \right)^\sigma$, $\mu_\theta := \int \theta dF_\theta$, and $Y(p) > 0$. By Lemma 1, $\frac{dp}{d\mu_\theta} > 0$ if and only if $X' > 0$. To show that X is increasing, it is sufficient that $\int \theta^{\frac{1}{\sigma}} dF_\theta$ is increasing in μ_θ, which is implied by the fact that $\theta^{\frac{1}{\sigma}}$ is a monotonically increasing function of θ. Thus, if $\mu_{\theta,h} = \int \theta F_{\theta,h} > \mu_{\theta,l} = \int \theta F_{\theta,l}$ then $X(\mu_{\theta,h}) > X(\mu_{\theta,l})$. Note that, under the assumptions of Proposition 2, $\left(\int \theta^{\frac{1}{\sigma}} dF_\theta \right) < \infty$. The proof of part (ii) is similar and thus omitted.

Part (iii). Note that $f_n = \sigma\delta \frac{n_t^{\sigma-1}}{B_t} \left(\frac{\tau(H(p))}{(1+\rho)} \right)^{1-\sigma} \left(\int \theta^{\frac{1}{\sigma}} dF_\theta \right)^\sigma \int \lambda \left(n_{t+1}\right)^{1-\sigma} dF_n > 0$. By Lemma 1, $\frac{dp}{dn_t} > 0$.

Part (iv). Assume that all consumers have the same type $\theta > 0$, i.e., F_θ is degenerate. To compute f_σ, let us write f in equation (12) as $f = \frac{\delta\theta}{B} f_1 f_2 f_3$, where: $f_1(\sigma) = n_t^\sigma$, $f_2(\sigma) = \left(\frac{\tau(H)}{1+\rho}\right)^{1-\sigma}$, $f_3(\sigma) = \int \lambda \left(n_{t+1}\right)^{1-\sigma} dF_n$. Note the $f_i > 0$ for all $i \in \{1,2,3\}$. By the chain rule: $f_\sigma = \frac{\delta\theta}{B}\left[f_1' f_2 f_3 + f_1 f_2' f_3 + f_1 f_2 f_3'\right]$. First, $f_1' = \ln(n_t) n_t^\sigma > 0$. $f_2' = -\ln\left(\frac{\tau(H)}{1+\rho}\right)\left(\frac{\tau(H)}{1+\rho}\right)^{1-\sigma}$. Thus, the sign of f_2 depends on that of $\ln(\tau(H))$ and is, in principle, undetermined. If, for example, τ has an image given by $[0,1]$, and in Section 5, then $f_2' > 0$. Third, to compute f_3', note that the assumptions in Proposition 2 are satisfy those of the Dominated Convergence Theorem. Therefore, $f_3' = -\int \lambda \left(n_{t+1}\right)^{1-\sigma} \log(\lambda(n_{t+1})) dF_n$. Let $\underline{n} > 1$ be the lower bound of the support of F_n. If $\lambda(\underline{n}) > 1$, then $f_3' < 0$. Thus, the sign of f_σ is ambiguous even when all investors have the same type. Moreover, if F_θ is non-degenerate, then one needs to consider an additional term $f_4(\sigma) = \left(\int \theta^{\frac{1}{\sigma}} dF_\theta\right)^\sigma$. The sign of f_4' is ambiguous as well and, thus, in principle, the effect of σ on p_B may be non-monotonic. □

Proof of Proposition 4.

Part (i). To simplify the exposition and without much loss of generality, we assume $m \geq 2$ to be a continuous variable. We can write $f(p,m) = \hat{\mathrm{f}}\tau(H(m))^{1-\sigma}$, $\hat{\mathrm{f}} > 0$. It follows that $\frac{df}{dm} = \hat{\mathrm{f}}\left(1-\sigma\right)\tau^{-\sigma}\tau'\left[\frac{dH^*}{dm}\right]$. Since each of the terms in $\hat{\mathrm{f}}\left(1-\sigma\right)\tau^{-\sigma}\tau'$ is positive, $\frac{df}{dm} > 0$ if and only if $\frac{dH^*}{dm} > 0$, which has been proven in Proposition 1. Thus, $\frac{df}{dm} > 0$ and, by Lemma 1, we also have $\frac{dp_B}{dm} > 0$.

Part (ii). Let $\chi := C'(h)$ and write $f(p,\chi) = \tau\left(H(\chi)\right)^{1-\sigma}\hat{\mathrm{f}}$, $\hat{\mathrm{f}} > 0$. Then, $f_\chi = (1-\sigma)\hat{\mathrm{f}}\tau^\sigma\tau'\frac{dH}{d\chi}$. By Proposition 1, $\frac{dH^*}{d\chi} < 0$, which implies that $f_\chi < 0$ and $\frac{dp_B}{d\chi} < 0$.

Part (iii). For convenience, rewrite $f(p,\rho)$ as $\left(\frac{\tau(H(p))}{(1+\rho)}\right)^{1-\sigma}\mathrm{f}$, with $\mathrm{f} > 0$ independent of p and ρ. Thus,

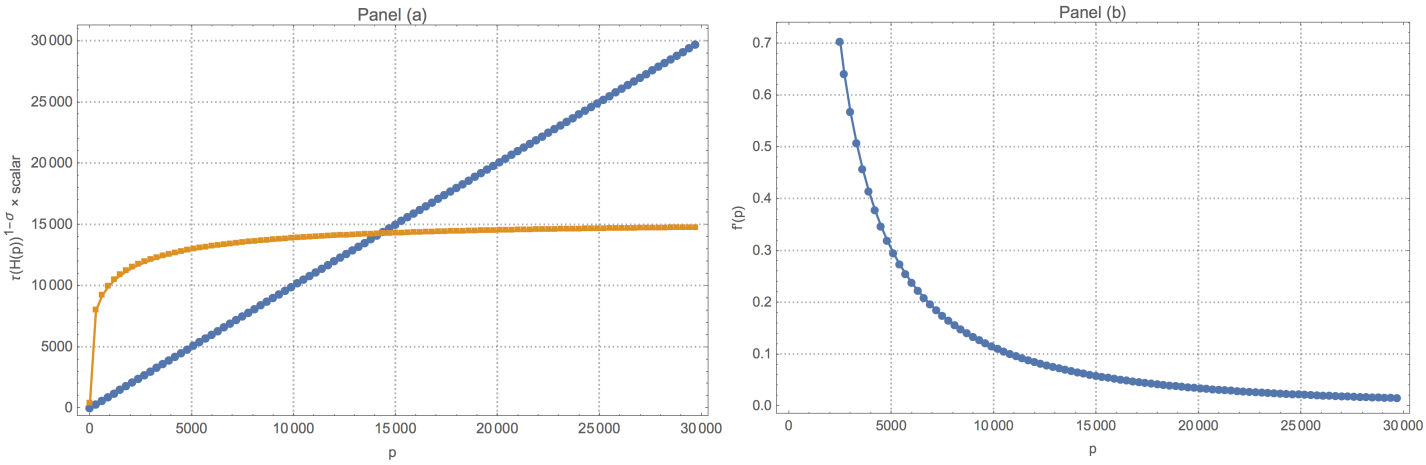
$$\frac{df}{d\rho} = \frac{(1-\sigma)}{(1+\rho)}\frac{f(p,\rho)}{\tau\left(H\right)}\Bigg[\underbrace{\tau'(H)\frac{dH}{d\rho}(1+\rho) - q(H)}_{\xi(\rho)}\Bigg]$$

Since $\frac{(1-\sigma)}{(1+\rho)}\frac{f(p,\rho)}{\tau(H)} > 0$, then $\frac{df}{d\rho} > 0$ if and only if $\xi(\rho) = \left[\tau'(H)\frac{dH}{d\rho}(1+\rho) - \tau(H)\right] > 0$. Notice that from Proposition 1 we have $\frac{dH^*}{d\rho} > 0$. As $\rho \to 0$, $H^* \to 0$ and $\tau \to 0$. Thus, $\lim_{\rho\to 0}\frac{dH^*}{d\rho} = \frac{m-1}{m}\frac{Bp}{[C'(0)]} > 0$. Moreover, from Assumption 1, $\tau'(0) > 0$, from which it follows that $\xi(0) > 0$ and $\frac{df}{d\rho} > 0$ at $\rho = 0$.

Consider $\rho > 0$. To study the behavior of the function $\xi(\rho)$ is useful to compute $\frac{d\xi}{d\rho}$.

$$\frac{d\xi}{d\rho} = (1+\rho)\left[\tau''(H)\left(\frac{dH}{d\rho}\right)^2 + \tau'(H)\frac{d^2H}{d\rho^2}\right].$$

Figure 8. Determination of Equilibrium Prices



From Proposition 1, $\frac{d^2H^*}{d\rho^2} = 0$. Thus, $\frac{d\xi}{d\rho}$ can be further simplified to $\frac{d\xi}{d\rho} = (1+\rho)\tau''(H)\left(\frac{dH}{d\rho}\right)^2$. When $\tau'' < 0$, then $\frac{d\xi}{d\rho} < 0$ for any $\rho > 0$, which implies that there must exist a positive value $\overline{\rho}$ such that for $\rho < \overline{\rho}$ the function $\xi(\rho) > 0$, so that also $\frac{df}{d\rho} > 0$, and for $\rho > \overline{\rho}$ the function $\xi(\rho) < 0$, which also implies that $\frac{df}{d\rho} < 0$. The bitcoin price is maximized at the value $\overline{\rho}$

For $\rho \to \infty$, notice that $\frac{dH^*}{d\rho} = \frac{m-1}{m}\frac{Bp_B}{[C'(h^*)+h^*C''(h^*)]} > 0$. Thus $\frac{dH^*}{d\rho} \to 0^+$. It follows that $\left(\tau'(H)\frac{dH}{d\rho}(1+\rho) - \tau(H)\right) \to -\overline{\tau} < 0$, so that $\frac{df}{d\rho} \to 0^-$.□

Proof of Proposition *5*.

From Proposition 1, $h^*C'(h^*) = B\rho p\frac{m-1}{m^2}$. Unless $\lim_{m\to\infty} p = \infty$, we have $\lim_{m\to\infty} h^*C'(h^*) = 0$, therefore $\lim_{m\to\infty} h^* = 0$. This implies that when we consider $\lim_{m\to\infty}\mu_B = \lim_{m\to\infty}\frac{mC(h^*(m))}{B\rho}$, the numerator leads to an indeterminacy of the type $\infty \times 0$. However, one can rearrange the expression as $\left(\frac{C(h^*(m))}{B\rho}\right)\left(\frac{1}{m^{-1}}\right)$ and compute the limit using L'Hospital rule. So we have

$$\lim_{m\to\infty}\mu_B = \lim_{m\to\infty}\left(\frac{\frac{1}{B\rho}C\left(h^*(m)\right)}{m^{-1}}\right) = \lim_{m\to\infty}\frac{\left(\frac{1}{B\rho}C\left(h^*(m)\right)\right)'}{(m^{-1})'}$$
$$= \lim_{m\to\infty}\frac{\left(\frac{1}{B\rho}C'\left(h^*(m)\right)\frac{dh^*}{dm}\right)}{(-m^{-2})}. \tag{13}$$

From Proposition 1, we know that $\frac{dh^*}{dm} = -\frac{B\rho p(m-2)}{m^3(C'+h^*C'')}$. Replacing in (13), we obtain

$$\lim_{m\to\infty}\mu_B = \lim_{m\to\infty}\frac{\frac{1}{B\rho}C'(h^*)}{-m^{-2}}\frac{-B\rho p(m-2)}{m^3(C'+h^*C'')}$$
$$\lim_{m\to\infty}\mu_B = \lim_{m\to\infty}\frac{C'(h^*)}{(C'+h^*C''(h^*))}\lim_{m\to\infty}p.$$

If the price limit exists, $\lim_{m\to\infty}p=\overline{p}$, we conclude that $\bar{\mu}=\overline{p}\,\zeta$, $\zeta=\lim_{m\to\infty}\frac{C'(h^*)}{(C'+h^*C''(h^*))}$.□

Proof of Proposition 6.

Miner j takes the price as given and solves $\max_{h_j} B\rho p_B\times\pi_{\text{win}}(h_j,h_{-j})-\eta HC(h_j)$, with first order condition

$$B\rho p_B\frac{H-\hat{h}_j}{H^2}=C(\hat{h}_j)\eta+\tau HC'(\hat{h}_j).$$

where $\hat{h}_j$ represents the optimal hashrate for miner j, with $\frac{\partial\pi_{\text{win}}}{\partial h_j}=\frac{H-h_j}{H^2}$. With symmetric identical miners, $\hat{H}=\hat{h}m$, therefore

$$\hat{h}\left[C(\hat{h})\eta+\eta m\hat{h}C'(\hat{h})\right]=B\rho p_B\frac{m-1}{m^2}. \tag{14}$$

Note that the right-hand side of equation (14) is the same as that of equation (3). Therefore, for the same price p_B, $\hat{h}\eta\left[C(\hat{h})+m\hat{h}C'(\hat{h})\right]=h^*C'(h^*)$. From A2, $C(h)=h^2$ (up to a positive constant), thus

$$\hat{h}^2\hat{h}^2\left[\eta\left(\frac{1}{2}+m\right)\right]=h^{*2}.$$

We conclude that $\hat{h}>h^*$ if and only if $\hat{h}^2\left[\eta\left(\frac{1}{2}+m\right)\right]<1$. For this inequality to hold one requires low value of $\hat{h}$. Because $\hat{h}$ is increasing in the reward, we conclude that $\hat{h}>h^*$ for a sufficiently low reward and vice-versa. □

Details on Example 3.

(i) Let us consider a cost function $C(h)=ch^\beta$. Under A2, optimality requires $C'(h^*)h^*=B\rho p_B\frac{m-1}{cm^2}$,so that $(h^*)^\beta=\frac{B\rho}{c\beta}\frac{m-1}{cm^2}p_B$ and $H^*=mh^*$. Let the average cost of mining one bitcoin $\mu_B=\frac{mC(h^*)}{B\rho}=\frac{mc}{B\rho}(h^*)^\beta$. Substituting for the optimal hashrate, $\mu_B=\frac{1}{\beta}\frac{m-1}{m}p_B$. Thus, for $m\to\infty$, $\lim_{m\to\infty}\mu_B=\frac{1}{\beta}\overline{p}$.

(ii) Let $C(h)=ae^{\beta h}$. Then, $C'=a\beta e^{\beta h}$, $C''=a\beta^2e^{\beta h}$. Thus,

$$\bar{\mu}=\overline{p}\lim_{m\to\infty}\frac{a\beta e^{\beta h^*}}{(a\beta e^{h^*}+ah^*\beta^2e^{\beta h^*})}=\overline{p}\lim_{m\to\infty}\frac{a\beta}{a\beta(1+h^*\beta)}=\overline{p}$$

where the last result follows from 1. □

Appendix A. Verification, CR, and Ledger Dynamics: An Illustration.

Section 1 discusses the economics of the verification process in DNs. To clarify the relation between verification and censorship resistance, this appendix provides a simple illustration.

Consider a financial network $\mathscr{F} = (\{\mathcal{N}, G\}, \{\mathcal{M}, L\})$ that allows for transfers on an asset in positive net supply a_k and let $L \in \mathbb{R}^{n\times k}$ be a digital ledger, i.e. a matrix that specifies how much agent i owns of asset k, which satisfies market clearing conditions for the asset $\sum_{i=1:N} L_{ik} = a_k$. Let $x_{ii'k}(t) \in \mathbb{R}_+$ denote a transfer by which agent i sends to i' an amount of x units of asset k at time t. Although $x_{ii'k}$ is accounting-wise equivalent to $-x_{i'ik}$, negative transfers may not be allowed. For a transfer $x_{ii'k}(t) \geq 0$ initiated by i to be *feasible* it has to satisfy the following two properties: [F1] $G_{ii'} = 1$ and [F2] $L_{ik}(t) \geq x_{ii'k}(t)$ ("i owns enough of k"). Feasibility then amounts to connectivity and no external subsidies.

The verification process, i.e., a set of verifiers and a network consensus rule, establishes whether the transfer is authorized. A verifier j observes an announced transfer $x_{ii'k}$ and assigns it a positive verification status. Whether the transfer effectively affects the state of L depends on whether verifier j has network consensus. In open environments, network consensus is difficult to achieve due to the well-known Byzantine Generals Problem (Lamport et al. (1982)). Here, it amounts to avoiding "double spending" (i.e., $L_{ik}(t+1) > L_{ik}(t) - x$) and/or reverting transfers (i.e., $L_{i'k}(t+1) < L_{i'k}(t) - x$). In the case of Bitcoin, the first financial network to satisfactorily solve this problem, network consensus is achieved by providing economic incentives to those verifiers who modified the ledger (miners). When a transfer achieves verification consensus, the ledger balance of the sender (receiver) is reduced (increased) by x, so that $L_{ik}(t+1) = L_{ik}(t) - x$ and $L_{i'k}(t+1) = L_{i'k}(t) + x$.

Censorship resistance means that if F1 and F2 are satisfied for $x_{ii'k}(t) > 0$, then *for any* $(i, i') \in \mathcal{N}$, $L_{i'k}(t+1) = L_{i'k}(t) + x$. That is, regardless of user identities, i' receives the transfer from i provided the transfer is feasible. The degree of censorship resistance can be characterized as the probability that no censorship based on identities occur for such transfer. A DN such as Bitcoin that allows free entry to users, free entry to verifiers, and CR can be characterized as *permissionless.*

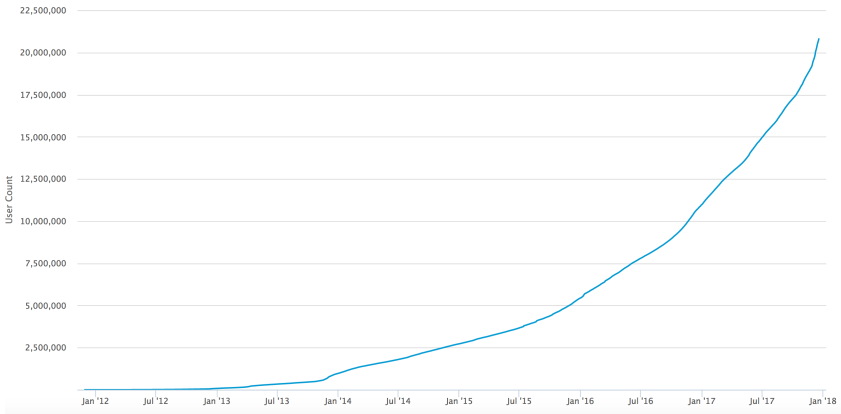
Appendix B: The State of the Bitcoin Network (12/31/2017)

Figure 9. Bitcoin Network: Price and Users

Panel (a) shows the price of Bitcoin in USD (logarithmic scale). Panel (b) shows the number of Blockchain wallet users. Panel (c) shows the number of unique addresses used on the Bitcoin blockchain. Source: Blockchain.info.

(a) USD Price

(b) Number of Wallets



(c) Number of Unique Addresses

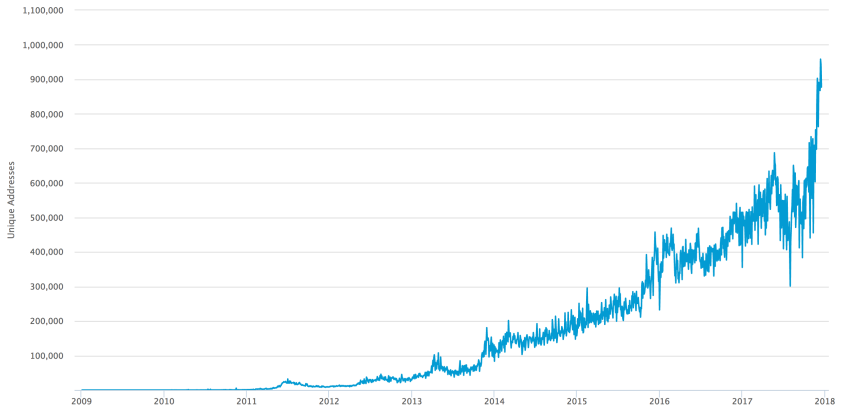
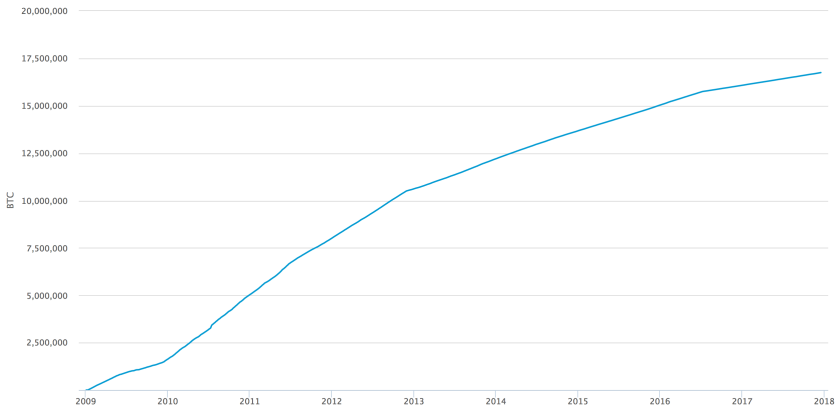


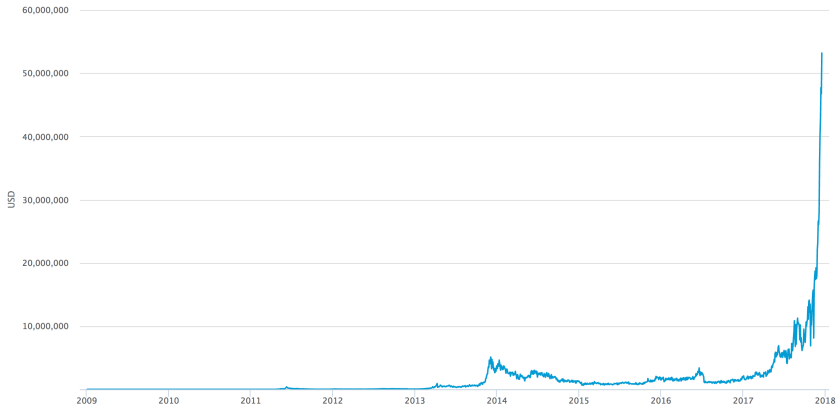
Figure 9 (Continued). Bitcoin Network: Mining Activity

Panel (a) shows the total supply of Bitcoin (number of coins mined). Panel (b) shows the mining revenue as given by the value of the coinbase rewards and transaction fees paid to miners. Panel (c) shows the estimated number of tera hashes per second (trillions of hashes per second). Source: Blockchain.info.

(d) Bitcoins in Circulation



(e) Mining Revenue



(f) Total Hash Rate