A Model of Cryptocurrencies*

Michael Sockin† Wei Xiong‡

September 2018

Abstract

This paper develops a model to analyze cryptocurrencies and initial coin offerings (ICOs) as a funding vehicle of new decentralized digital platforms. In our model, a cryptocurrency constitutes membership in a platform developed to facilitate transactions of certain goods or services. The complementarity in the households' participation in the platform acts as an endogenous, yet fragile, fundamental of the cryptocurrency. There exist either two or no equilibria, and the two equilibria, when they exist, have disparate properties. The possibility of no equilibria (platform failure) with the ICO discourages the platform developer from voluntarily committing ex ante to communicate any relevant information about the platform to prospective participants. This is in contrast to a platform launched by a traditional IPO, in which there exists a unique equilibrium and the developer is always willing ex ante to disclose all relevant information.

*PRELIMINARY DRAFT. We thank An Yan for a comment that led to this paper, and Haoxiang Zhu and seminar participants at ITAM, NBER Summer Institute, and Tsinghua University for helpful comments.

†University of Texas, Austin. Email: Michael.Sockin@mccombs.utexas.edu.

‡Princeton University and NBER. Email: wxiong@princeton.edu.

Between 2015 to 2017, over 2000 initial coin offerings (ICOs) emerged to raise more than $4 billion from the public, and to exceed venture capital investments in funding innovative projects related to blockchain technology, according to a report issued by EY Research. Among these ICOs, 1,031 were in the U.S., followed by 310 in Russia, 260 in Singapore, 256 in mainland China, and 196 in Hong Kong. In 2017, the top three ICOs by Tezos, EOS.IO, and BANCOR raised $208 million, 200 million, and 153 million, respectively. These initial successes led to tremendous excitement about cryptocurrencies as a new funding model for innovation in the upcoming digital age. Rampant speculation and volatility in the trading of many cryptocurrencies, however, have also raised concern that they, both coins and tokens, represent potential bubbles. The failure of the DAO only a few months after its ICO raised $150 million in 2016, together with a number of other similar episodes, highlights the risks and potential abuses involved in investing in cryptocurrencies. In response to these concerns, China banned cryptocurrencies at the end of 2017 and South Korea has pursued stern regulatory policies, even though other countries, such as Switzerland and Singapore, remain amenable to them.

Cryptocurrency platforms launched by ICOs represent a unique business model in which initial investors are both future shareholders are potential customers. Often these platforms provide intrinsic benefit to their participants. These benefits can range from the provision of secure and verifiable peer-to-peer transaction services to protection against censorship, taxation, and expropriation by a sovereign, to the maintenance of smart contracts whose execution is governed by blockchain technology, to the support of crowdfunding activities and media content whose sales are brokered in the currency. In addition, a key innovation of these platforms, along with the adoption of blockchain technology for record-keeping, is that they are "trustless" decentralized networks that lack a sovereign or central intermediaries to steward the platform and the currency. Instead of intermediaries, a population of miners are compensated for processing activity on the blockchain with currency according to a Proof of Work (PoW) protocol. In order to properly assess the potential benefits and risks brought about by cryptocurrencies, and to establish a suitable regulatory framework for ICOs, it is important to understand how cryptocurrency trading and the "trustless" nature of cryptocurrency platforms impact participation in the platform, its performance, the price of the currency, and ultimately the success of the ICO.[1] In particular, the ample uncertainty

[1]In addition to ICOs, cryptocurrency coins can be created from forks from existing currencies through airdrops by developers, while ICOs can create tokens that fund projects unrelated to the token platform.

and opacity associated with many of the ICOs, together with the typically observed frenzied trading of cryptocurrencies after their ICOs, raise questions regarding whether such trading serves any socially meaningful role, and whether the trading price and volume may affect the underlying behavior of cryptocurrencies.

To investigate these issues, we develop a model in which a cryptocurrency serves as membership to a platform, created by its developer to facilitate decentralized bilateral transactions of certain goods or services among a pool of households by using a blockchain technology. Households face difficulty in making such transactions outside the platform as a result of severe search frictions. The value of the platform, consequently, lies within its design in filling the households' transaction needs, and in its capability in pooling together a large number of households with the need to trade with each other. We model a household's transaction need by its endowment in a consumption good, and its preference of consuming its own good together with the goods of other households. As a result of this preference, households need to trade goods with each other, and the platform serves to facilitate such trading. Specifically, we assume that, when two housholds are randomly matched, they can trade their goods with each other only if they both belong to the platform. Consequently, there is a key network effect—each household's desire to join the platform grows with the number of other households on the platform and the size of their endowments.

The cryptocurrency in our framework serves dual roles, one as the membership to transact goods with other members, and the other as the initial financing for the platform, covering both compensation to the developer for creating the platform and the fee to coin miners for providing clearing services for the decentralized goods transactions on the platform. To highlight these dual roles, our model features two periods. In the first period, a pool of households with random endowments decide whether to join the platform by purchasing one unit of the cryptocurrency from a centralized market with coin miners supplying the cryptocurrency at a cost. During the second period, households on the platform are randomly matched to transact their goods for consumption. Each household's decision to join the platform trades off the cost of paying for the cryptocurrency with the benefit from transacting goods on the platform. This benefit increases with both the household's good own endowment, which determines its own transaction need, and the average endowments of other households, which determine their transaction needs. We show that each household optimally adopts a cutoff

Our focus is on ICOs applies more generally to any ICO in which usage of the created currency is part of the project's platform. In what follows, we do not make the distinction between coins and tokens.

strategy to purchase the cryptocurrency only if its endowment is higher than a threshold. The threshold and the currency price are jointly determined by the demand-side fundamental, the common endowment of all households, and the supply-side fundamental, the average computing cost for miners in providing clearing services to complete the households' goods transactions on the platform in the second period.

We analyze the equilibrium in two settings, differing in whether the platform's demand and supply fundamentals are publicly observable. In the first setting, where the fundamentals are publicly observable, there exist either two or no rational expectations equilibria. When there are two equilibria, they exhibit opposing behavior. One has a higher cryptocurrency price and a lower equilibrium cutoff for each household's cryptocurrency purchase decision, and the other has a lower price and a higher equilibrium cutoff. These two equilibria are self-enforcing as a result of the network effect—if more (less) households join the platform by choosing a lower (higher) cutoff strategy, each household benefits more (less) from trading goods with others on the platform, and is thus willing to pay a high (low) cryptocurrency price. When the platform's demand and supply fundamentals are sufficiently low, there would be no equilibria, due to the failure of the platform to attract any participant. The presence of no equilibria and two opposing equilibria suggests that one may observe entirely different dynamics of cryptocurrencies in practice, simply as a result of the endogenous and fragile nature of their business model, without necessarily involving any reckless speculation, abuse, or manipulation.

In the second setting, we introduce realistic informational frictions by assuming that the platform fundamentals are not publicly observable.[2] In this setting, each household uses its own endowment and the publicly observed cryptocurrency trading price and volume, which we interpret as activity on the blockchain ledger, as noisy signals to infer the value of the aggregate household demand for the platform. Despite the inherent non-linearity of the equilibrium cryptocurrency price and each household's demand for the currency, we construct a tractable log-linear noisy rational expectations equilibrium for the cryptocurrency market. In the equilibrium, each household again follows a cutoff strategy, as in the perfect-information setting, except that its equilibrium cutoff is determined by linear summary statistics of the publicly observed cryptocurrency price and volume, rather than the households' aggregate endowment and the miners' common mining cost, which are not observable. Interestingly,

[2]Lee, Li, and Shin (2018) provide extensive empirical evidence of asymmetric information among ICO investors, and of the role of ICOs as aggregators of dispersed information.

there again exist two or no cutoff equilibria. The trading price and volume of the cryptocurrency both serve as important channels for not only aggregating private information about its fundamental value, but also facilitating coordination on the high or low price equilibrium. The equilibria disappear when the price and volume signals are sufficiently poor, capturing the ultimate instability of the platform. This possibility of platform failure in turn discourages the platform developer from ex ante full information disclosure of the platform fundamentals, as such disclosure may directly lead to the platform failure in states when the platform's fundamentals are weak, dominating the high profit to the developer in states when the platform fundamentals are strong.

We also examine two alternative arrangements to setting up the platform. In the first, the platform developer sets a membership fee for households to participate in the platform and a separate fee for miners to provide transaction services on the platform, and funds the development of the platform through a traditional IPO by issuing shares based on the profit from the spread between the households' membership fee and the miners' service fee. As the developer acts as a monopolist in determining prices on the two sides of the platform, this ability stabilizes the platform by restoring a unique rational expectations equilibrium. Despite the seemingly different setting, the IPO market exhibits a cutoff equilibrium, with each household using a cutoff strategy to join the platform, each miner using a cutoff strategy to serve the platform, each stock investor using a cutoff strategy to buy or shortsell one share of the platform, and the share price aggregating investors' private information. As a result of this stable equilibrium, the developer is committed ex ante to disclosing any information about the platfom fundamentals, in sharp contrast to the ICO arrangement.

Our analysis demonstrates that cryptocurrencies are vulnerable to large price swings and significant feedback from prices to the real decisions of platform participants. In our second alternative arrangement, households' transactions are instead cleared following a Proof of Stake (PoS) protocol where, instead of a population of miners, there is a population of forgers who compete for fees from completing household transactions by purchasing stakes in the currency alongside households. In contrast to the PoW setting, there is a unique cutoff equilibrium in which the developer chooses the level of household participation through the transaction fee schedule it sets for the currency. While the PoS protocol resolves the issues of instability arising from coordination and scalability of computing resources, the token price is now subject to fluctuations in forgers' cost of capital, as with fiat currencies and traditional

intermediaries, and there is a wedge between maximizing revenue for the developer and maximizing household participation in the platform.

Our work contributes to the emerging literature on cryptocurrencies. Easley, O'Hara, and Basu (2017) analyze the rise of transactions fees in Bitcoin through the strategic interaction of users and miners. Chiu and Koeppl (2017) consider the optimal design of a cryptocurrency, and emphasize the importance of scale in deterring double-spending by buyers. Athey et al (2016) models Bitcoin as a medium of exchange of unknown (binary) quality that allows users to avoid bank fees when sending remittances, and uses the model to guide empirical analysis of Bitcoin users. Cong and He (2017) investigate the tradeoff of smart contracts in overcoming adverse selection while also facilitating oligopolistic collusion, while Biais et al (2017) considers the strategic interaction among miners and Abadi and Brunnermeier (2018) of disciplining writers to a blockchain technology with static incentives. Schilling and Uhlig (2018) study the role of monetary policy in the presence of a cryptocurrency that acts as a private fiat currency. Cong, Li, and Wang (2018) construct a dynamic model of crypto tokens to study the dynamic feedback between user adoption and the responsiveness of the token price to expectations about the future growth in the platform. Pagnotta and Buraschi (2018) also model the cryptocurrency market in an equilibrium framework that admits multiple equilibria, yet their focus is on a quantitative analysis of Bitcoin. Our analysis microfounds the intrinsic value of cryptocurrencies as facilitating household transactions in a general equilibrium framework, and explores the role of the cryptocurrency price as an aggregator of users' dispersed information about the platform's fundamentals.

Our paper also contributes to the growing literature on ICOs. Catalini and Gans (2018) investigate how ICOs differ from traditional equity financing, emphasizing how ICOs can aid entrepreneurs in discovering consumers' valuation of the platform but are subject to issues of commitment when entrepreneurs control token inflation. Li and Mann (2018) also explore network effects in ICOs, yet their focus is on how dynamic dissemination can help overcome coordination failure when the platform requires a critical mass, and how ICOs aggregate useful information for the developer about its product. Chod and Lyandres (2018) study the extent to which ICOs can facilitate risk-sharing between entrepreneurs and investors, without transferring control rights, in the presence of agency issues. In contrast, our analysis attempts to understand what fundamentals determine the price and success of a crypto token and its ICO based on the platform's subsequent performance, and emphasizes the role of

participation as an endogenous, yet fragile fundamental. In addition, we characterize the disparate properties of the two equilibria that naturally arise in our setting, and embed informational frictions to study the informational role of prices and volumes.

Our work is also related to the literature on the role of currency. Samuelson (1958), in his pioneering work, studied the role of money as a bubble asset that acts as a store of value in dynamically inefficient economies. Search models, such as Kiyotaki and Wright (1993) and Lagos and Wright (2005), frame money as a medium of exchange that facilitates bilateral trade when search frictions hinder the double coincidence of wants among trading parties. Cochrane (2005) frames money as a stock claim to the future surpluses of the issuing sovereign, while Kocherlakota (1998) views the history dependence of monetary balances as a primitive form of memory. In our framework, a cryptocurrency represents membership to a decentralized trading platform, and the price of this membership is pinned down by the endogenous expected benefit from participation of the marginal household. While search models such as Kiyotaki and Wright (1993) and Lagos and Wright (2005) can have multiple equilibria because of self-fulfilling expectations that the currency will be accepted in the future, multiple equilibria arise in our setting because the market-clearing price of the cryptocurrency reflects the marginal household's expected surplus from future trade, and there can be either two or zero marginal households that clear the market given the fundamentals. That cryptocurrencies also represents a security in our setting, in which the shareholders are also the customers, is conducive to the study of infantile currencies and ICOs.

Our work also adds to the literature on cutoff equilibrium with dispersed information. With risk-neutral investors and normally distributed payoffs, Morris and Shin (1998) and Dasgupta (2007) analyze coordination and delay in global games, Goldstein, Ozdenoren, and Yuan (2013) investigate the feedback effects of learning by a manager to firm investment decisions, while Albagli, Hellwig, and Tsyvinski (2014, 2015) focus on the role of asymmetry in security payoffs in distorting asset prices and firm investment incentives. Similar to our framework, Gao, Sockin, and Xiong (2018) employ a Cobb-Douglas utility with lognormal payoffs to deliver tractable equilibria, yet their focus is on the dynamic distortion of informational frictions to housing and production decisions. In contrast, our setting features an interaction of search with centralized trading to explain ICOs.

1 The Model

Consider a cryptocurrency, which serves as the membership to a decentralized digital platform with a pool of households who share a certain need to transact goods with each other. The developer of the cryptocurrency designs the platform to reduce the otherwise severe search frictions among the households, and develops the infrastructure that supports the platform. The success of the cryptocurrency is ultimately determined by whether the platform can gather these households together. Households purchase the cryptocurrency as the membership to transact in the platform, with the payment for the currency purchase shared by the developer and platform miners, who provide settlement and accounting services for transactions in the platform.

We analyze a model with two periods $t \in \{1, 2\}$ and three types of agents: households, miners, and the developer. At $t = 1$, households purchase the currency through a centralized exchange to join the platform. In practice, the coin prices during the Initial Coin Offers (ICOs) are often pre-fixed at given levels in order to secure some initial interests in the offerings, while more sales continue after the ICOs at market prices. For simplicity, we include only one trading round in the model, which serves to capture not only the ICO but also trading that follows the ICO. By pooling these extended trading rounds into one trading period in the model,[3] we focus on analyzing how the currency price serves to aggregate the trading needs of the households and affects their participation in the platform.

At $t = 2$, the households in the platform are randomly matched to trade their good endowments. This trade is supported by miners who act as servicers of the decentralized platform, and whose servers compete to clear the transaction on a blockchain for the buyer and seller. We assume that there need to be as many miners as households to support the platform, and that their computing power is perfectly divisible to compete to clear transactions. Households then consume both their own good and their trading partner's good.

1.1 Households

We consider a pool of households, indexed by $i \in [0, 1]$. These households are potential users of the cryptocurrency as a result of their trading needs. Each of them may choose to purchase a unit of the cryptocurrency in order to participate in the platform. We can

[3] See Li and Mann (2018) for a model of the trading rounds during ICOs.

divide the unit interval into the partition $\{\mathcal{N}, \mathcal{O}\}$, with $\mathcal{N} \cap \mathcal{O} = \varnothing$ and $\mathcal{N} \cup \mathcal{O} = [0,1]$. Let $X_i = 1$ if household i purchases the cryptocurrency, i.e., $i \in \mathcal{N}$, and $X_i = 0$ if it does not. An indivisible unit of currency is commonly employed in search models of currency, such as Kiyotaki and Wright (1993). If household i at $t = 1$ chooses to purchase the cryptocurrency, it purchases one unit at the equilibrium price P.

Household i is endowed with a certain good and randomly meets a trading partner, household j on the platform at $t = 2$. Household i has a Cobb-Douglas utility function over consumption of its own good and the good of household j according to:

$$U(C_i, C_j; \mathcal{N}) = \left(\frac{C_i}{1-\eta_c}\right)^{1-\eta_c} \left(\frac{C_j}{\eta_c}\right)^{\eta_c}, \tag{1}$$

where $\eta_c \in (0,1)$ represents the weight in the Cobb-Douglas utility function on its consumption of its trading partner's good C_j, and $1-\eta_c$ is the weight on consumption of its own good C_i. A higher η_c means a stronger complementarity between the consumption of the two households' goods. We assume that both goods are needed for the household to derive utility from consumption, and the utility is zero in the absence of trading. This utility specification implies that each household cares about the aggregate endowment of all other households in the platform, which ultimately defines the cryptocurrency's fundamental.

The good endowment of household i is e^{A_i}, where A_i is comprised of a component A common to all households and an idiosyncratic component ε_i:

$$A_i = A + \varepsilon_i,$$

where $A \sim \mathcal{N}\left(\bar{A}, \tau_A^{-1}\right)$ and $\varepsilon_i \sim \mathcal{N}\left(0, \tau_\varepsilon^{-1}\right)$ are both normally distributed and independent of each other. Furthermore, we assume that $\int \varepsilon_i d\Phi(\varepsilon_i) = 0$ by the Strong Law of Large Numbers. The aggregate endowment A is a key characteristic of the platform. A cleverly designed platform serves to attract households with strong needs to trade with each other. One can thus view A as the demand fundamental for the cryptocurrency or the strength of the platform, and τ_ε as a measure of dispersion among households in the platform.

In practice, A is usually not directly observed by the potential users as a result of realistic informational frictions. The ICO and the trading of the cryptocurrency serves to not only provide funding to support the platform but also to aggregate information directly from the households about the potential demands for transaction services provided by the cryptocurrency and the platform. To highlight this role, we will proceed with first ana-

lyzing a benchmark case when A is publicly observable, and then an extended case when informational frictions prevent A from being directly observed by all agents.

We start with describing each household's problem at $t = 2$ and then go backward to describe its problem at $t = 1$. A realistic feature of decentralized digital platforms is that many transactions clear on decentralized servers that record the transactions on blockchains. At $t = 2$, household i is randomly matched with another household j and, if both households own the cryptocurrency, then they can trade their goods with each other. Mutual ownership of the cryptocurrency (i.e., membership to the platform) is necessary to transact because of realistic issues of fraud, asymmetric information, or transaction costs that make direct trade prohibitively costly. For instance, while goods inventories are harder to observe, payment through the cryptocurrency is difficult to falsify and can be verified on the blockchain. As only owners of the cryptocurrency can trade with each other, the probability of a currency owner to trade with another household increases with the ownership of the cryptocurrency.

We quote both the price of the cryptocurrency at $t = 1$ and the price of the goods at $t = 2$ in terms of the numeraire good. As we only allow one round of trading of the cryptocurrency at $t = 1$, this avoids the complication of re-trading the cryptocurrency at $t = 2$ together with the goods trading.

A household who owns the currency $\mathcal{N}$ maximizes its utility at $t = 2$ by choosing its consumption demand $\{C_i, C_j\}$ conditional on a successful match:

$$\begin{aligned} U_i &= \max_{\{C_i, C_j\}} U(C_i, C_j; \mathcal{N}) \\ &\quad \text{such that } \; p_i C_i + p_j C_j = p_i e^{A_i}, \end{aligned} \tag{2}$$

where p_i is the price of its good. We assume that at $t = 2$, the platform strength A is publicly observed by all agents even in the case where A is not initially observable at $t = 1$. Households behave competitively and take the prices of their goods as given. We assume that households do not discount their final consumption at $t = 1$.

At $t = 1$, each household needs to decide whether to join the platform by buying the currency. In addition to the utility flow U_i at $t = 2$ from final consumption, we assume that households have quasi-linear expected utility at $t = 1$, and incur a linear utility penalty equal to the price of the cryptocurrency P if they choose to join the platform. Given that households have Cobb-Douglas preferences over their consumption, they are effectively risk-neutral at $t = 1$, and their utility flow is then the expected value of their final consumption bundle less the cost of the currency. Households choose whether to buy the currency subject

to a participation constraint that their expected utility from the purchase $E[U_i|\mathcal{I}_i] - P$ must (weakly) exceed a reservation utility, which we normalize to 0. One can interpret the reservation utility as from the alternative choice of not trading with any partner.

In summary, household i makes its purchase decision at $t = 1$:

$$\max_{X_i} \{E[U_i|\mathcal{I}_i] - P, 0\}. \tag{3}$$

subject to its information set $\mathcal{I}_i$. In the perfect-information benchmark, each household observes not only its own A_i but also the platform fundamental A. In the case with informational frictions, each household observes only its own A_i but not A.

1.2 Miners

The cryptocurrency is supported by a Proof of Work (PoW) protocol for clearing transactions on blockchains. There is a population of potential miners, indexed on a continuous interval $[0, 1]$, who maintain the platform at $t = 2$. These miners mine the cryptocurrency by providing accounting and custodial services using its underlying blockchain technology, and facilitating the decentralized trades among households on the platform at $t = 2$.[4] In practice, several miners are randomly drawn from a queue to compete to complete each transaction, and miners often pool their revenue to insure each other against the risk of not being selected.[5] For simplicity, we assume that each miner is assigned to clear the transaction of one household on the platform. That is, if a miner accepts payment at $t = 1$, he agrees to clear a transaction at $t = 2$ if needed.[6]

Miner i provides the computing power to facilitate a trade between households, subject to a cost of setting up the required hardware and software to mine the cryptocurrency: $e^{-\omega_i} S_i$,

[4] In practice, many ICOs are executed through smart contracts written on existing blockchain architecture, such as Ethereum. We consider payment to miners in a native currency to study a closed digital ecosystem.

[5] See Cong, He and Li (2018) for an extensive analysis of this issue.

[6] While our matching protocol helps with tractability of the model, our qualitative insights only require that more miners are needed when more households subscribe to the platform. In practice, many PoW protocols, such as those of Bitcoin and Ethereum, set the difficulty of mining (the hashrate) to maintain a fixed average time for new blocks to be added to the blockchain. Without additional miners, this hashrate would fall as more subscribers join these platforms so that existing miners could accommodate the larger volume of transactions. As mining becomes easier, however, the platform would become more vulnerable to strategic attacks, such as fifty-one percent attacks, "double spending" fraud, and transaction failures, since the computational cost for such attacks would decline while the benefit from manipulating the currency and collecting tokens from mining would increase. Chiu and Koeppl (2017) shows that having a more diverse mining population mitigates the inefficiencies arising from strategic incentives to "double spend". Pagnotta and Buraschi (2018) finds that having a larger mining population reduces the vulnerability to attacks of currencies with PoW protocols.

where $S_i \in \{0,1\}$ is the miner's decision to mine and

$$\omega_i = \xi + e_i,$$

is the miner's productivity, which is correlated across miners in the currency through the common component ξ. It is realistic to assume heterogeneity among miners, with less efficient miners employing more costly technologies. We assume that ξ represents an unobservable, common supply shock to the mining costs of the cryptocurrency and, from the perspective of households and miners, $\xi \sim \mathcal{N}\left(\bar{\xi}, \tau_{\xi}^{-1}\right)$. Furthermore, $e_i \sim \mathcal{N}\left(0, \tau_e^{-1}\right)$ such that $\int e_i d\Phi\left(e_i\right) = 0$ by the Strong Law of Large Numbers.

Miners receive a fraction $1-\rho \in (0,1)$ of the proceeds from selling the cryptocurrency at $t=1$ to households at price P, which serves as the fee for clearing transactions at $t=2$.[7] Miners in the currency at $t=1$ maximize their revenue:

$$\Pi_s\left(S_i\right) = \max_{S_i} \ \left(\left(1-\rho\right)P - e^{-\omega_i}\right) S_i. \tag{4}$$

Since miners are risk-neutral, it is easy to determine each miner's optimal supply curve:

$$S_i = \begin{cases} 1 & \text{if} \quad \left(1-\rho\right)P \geq e^{-\xi+e_i} \\ 0 & \text{if} \quad \left(1-\rho\right)P < e^{-\xi+e_i} \end{cases}. \tag{5}$$

In the cryptocurrency market equilibrium, the common mining cost ξ represents the supply shock. Also note that when the platform strength A is unobservable, ξ may also affect the demand side by interfering the households' learning about A.

The Proof of Work protocol intimately links the price of the currency to the marginal cost of mining, since miner optimization imposes that $P = \frac{1}{1-\rho}e^{-\omega^*}$ for the marginal miner ω^*. This feature highlights the issue of limited scalability of PoW cryptocurrencies, as both the price of the cryptocurrency and the computational resources devoted to supporting it must escalate with the size of the household population on the platform. As the platform grows, the price of the currency must rise to entice more miners to support it. This feature also distinguishes cryptocurrencies from fiat currencies, where the marginal cost of printing money is zero. As a result, the conventional Friedman Rule does not apply: the nominal interest rate for PoW cryptocurrencies should not be zero.[8]

[7] To focus on the broader implications of the cryptocurrency for households, we abstract from the strategic considerations that miners face in adding blocks to the blockchain to collect fees, such as consensus protocols and on which chain to add a block. See, for instance, Easley, O'Hara, and Basu (2017) and Biais et al (2017) for game theoretic investigations into these issues.

[8] This observation is also discussed in Schilling and Uhlig (2018), though their focus is on price stability rather than optimal monetary policy.

1.3 Developer

The developer creates the platform at $t = 1$. It establishes the code that specifies the protocol of how transactions in the platform are cleared and recorded on the blockchain, how more currency is created, such as through mining, and how it can be stored in virtual wallets. It receives a fraction ρ of the revenue P from the sales of the currency, with ρ being fixed as part of the technology. The remaining revenue is paid to miners as part of the PoW protocol in exchange for their accounting services at $t = 2$. A lower ρ can be viewed as a higher profitability of mining that entices more miners to support the platform. The revenue for the developer is thus

$$\Pi_D = E\left[\rho P \int_{-\infty}^{\infty} X_i d\Phi\left(\varepsilon_i\right)\right].$$

1.4 Rational Expectations Equilibrium

Our model features a rational expectations cutoff equilibrium, which requires clearing of the cryptocurrency market that is consistent with the optimal behaviors of households and miners, as well as clearing of each traded good between two matched households:

- Household optimization: each household chooses X_i at $t = 1$ to solve its maximization problem in (3) for whether to purchase the cryptocurrency, and then chooses $\{C_i, C_j\}$ at $t = 2$ to solve its maximization problem in (2) for trading and consumption of the two goods with its matched trading partner.

- Miner optimization: each miner chooses S_i at $t = 1$ to solve his maximization problem in (4).

- At $t = 1$, the cryptocurrency market clears:

$$\int_{-\infty}^{\infty} X_i\left(\mathcal{I}_i\right) d\Phi\left(\varepsilon_i\right) = \int_{-\infty}^{\infty} S_i\left(\omega_i, P\right) d\Phi\left(e_i\right),$$

  where each household's demand X_i depends on its information set $\mathcal{I}_i$, and each miner's supply of computing services $S_i\left(\omega_i, P\right)$ depends on its productivity ω_i and the currency price P. The demand from households and supply from miners are integrated over the idiosyncratic components of their endowments $\{\varepsilon_i\}_{i\in[0,1]}$ and costs $\{e_i\}_{i\in[0,1]}$, respectively.

- At $t = 2$, the market for household i's good between two matched trading partners clears:

$$C_i(i) + C_i(j) = e^{A_i}.$$

2 The Perfect-Information Setting

In this section, we focus on the setting with the platform strength A and the miners' mining cost ξ being publicly observable at $t = 1$.

2.1 Choices of Households

At $t = 2$, households that have chosen to purchase the cryptocurrency need to make their consumption decisions. Household i has e^{A_i} units of good i for consumption and for trading with another household. It maximizes its utility function given in (2). The following proposition describes each household's consumption choice. Its marginal utility of good consumption also gives the equilibrium good price.

Proposition 1 *Households i's optimal good consumption at $t = 2$ are:*

$$C_i(i) = (1 - \eta_c) e^{A_i},\ C_j(i) = \eta_c e^{A_j},$$

and the price of its produced good is:

$$p_i = e^{\eta_c (A_j - A_i)}.$$

Furthermore, the expected utility benefit of household i at $t = 1$ is given by:

$$E\left[U\left(C_i, C_j; \mathcal{N}\right) \middle| \mathcal{I}_i\right] = e^{(1-\eta_c)A_i + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} E\left[e^{\eta_c A} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) \middle|\ \mathcal{I}_i\right],$$

and the ex ante utility of all households before observing their endowment is:

$$U_0 = e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\varepsilon^{-1}} \Phi\left(\left(1 - \eta_c\right)\tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) - \Phi\left(\frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) P.$$

Proposition 1 shows that each household spends a fraction $1 - \eta_c$ of its endowment on consuming its own good $C_i(i)$ and a fraction η_c on the good produced by its trading partner $C_j(i)$. When $\eta_c = 1/2$, the household consumes the two types of goods equally. The price of each good is determined by its output relative to that of the other good. One household's good is more valuable when the other household has a greater endowment, and consequently

each household needs to take into account the endowment of its trading partner when making its own decision. The proposition demonstrates that the expected utility of a household in the platform is determined by not only its own endowment e^{A_i} but also the endowments of other households. This latter component arises from the complementarity in the household's utility function.

We now discuss each household's decision on whether to purchase the cryptocurrency at $t = 1$. As a result of its Cobb-Douglas utility, the household is effectively risk-neutral over its aggregate consumption, and its optimal choice reflects the difference between its expected output if it buys the currency and is matched with a trading partner, and the cost of the cryptocurrency, i.e., the price P to buy a unit of the currency. It then follows that household i's purchase decision is given by

$$X_i = \begin{cases} 1 & \text{if } E\left[U\left(C_i, C_j; \mathcal{N}\right) | \mathcal{I}_i\right] \geq P \\ 0 & \text{if } E\left[U\left(C_i, C_j; \mathcal{N}\right) | \mathcal{I}_i\right] < P \end{cases}.$$

This decision rule for its purchase supports our conjecture to search for a cutoff strategy for each household, in which only households with endowments above a critical level A^* buy the currency. This cutoff is eventually solved as a fixed point in the equilibrium, and equates the currency price with the expected utility of the marginal household from joining the platform.

2.2 The Equilibrium

We now proceed to discuss the equilibrium at $t = 1$. We characterize each household's cryptocurrency purchase decision and the currency price at $t = 1$, taking the choice of the developer as given. Households will sort into the cryptocurrency platform according to a cutoff equilibrium determined by the net benefit of joining the platform, which trades off the opportunity of trading with other households on the platform with the cost of acquiring the platform membership (i.e., the cryptocurrency price). Despite the inherent nonlinearity of our framework, we derive a tractable cutoff equilibrium that is characterized by the solution to a fixed-point problem over the endogenous cutoff of the marginal household that purchases the cryptocurrency, A^*, as summarized in the following proposition.

Proposition 2 *In the perfect-information setting, there are two rational expectations equilibria when A or ξ is sufficiently large, with cutoffs $\underline{A}^*(A, \xi) < \bar{A}^*(A, \xi)$, respectively, in which the following hold:*

1. *Household i follows a cutoff strategy in its cryptocurrency purchase decision:*

$$X_i = \begin{cases} 1 & \text{if } A_i \geq A^* \\ 0 & \text{if } A_i < A^* \end{cases},$$

where $A^* \in \left\{\underline{A}^*, \bar{A}^*\right\}$ *solves*

$$e^{\left(1-\eta_c+\sqrt{\tau_\varepsilon/\tau_e}\right)(A^*-A)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - \frac{A^*-A}{\tau_\varepsilon^{-1/2}}\right) = e^{-A-\xi-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho)} \quad (6)$$

where $\Phi(\cdot)$ *is the CDF function of normal distribution.*

2. *The cryptocurrency price takes a log-linear form:*

$$\log P = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}(A - A^*) - \xi - \log(1-\rho).$$

3. *In the high (low) price equilibrium with the equilibrium cutoff* $\underline{A}^*$ *(*$\bar{A}^*$*), the cryptocurrency price* P*, the developer's revenue* $\Pi_D = \rho\Phi\left(\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)P$*, and the ex ante utility of households* U_0 *are increasing (decreasing) in* A*, and the number of households that purchase the currency is increasing (decreasing) in* A *and* ξ*.*

4. *No household buys the cryptocurrency if* A *or* ξ *is sufficiently small.*

Proposition 2 characterizes the cutoff equilibrium in the platform when A and ξ are publicly observed at $t = 1$, and confirms the optimality of a cutoff strategy for households in their choice to purchase the cryptocurrency. Households sort into the platform based on their endowments, with those with higher endowments and thus more gains from trade with other households to enter the platform at $t = 1$. In this cutoff equilibrium, the cryptocurrency price is a correspondence of both the demand and supply fundamentals. Despite its log-linear representation, the price P is actually a generalized linear correspondence of $\sqrt{\frac{\tau_\varepsilon}{\tau_e}}A - \xi - \log(1-\rho)$, since A^* is an implicit function of A and ξ.

As a result of the complementarity in the households' decision to buy the cryptocurrency, there are either no or two equilibria in the cryptocurrency market. There are no equilibria when the platform fundamentals are sufficiently weak, i.e., when either A or ξ is sufficiently small. When this occurs, no one enters the platform, making it undesirable even for households with highest demands to enter. This ultimate failure of the platform emerges from the strong network effect in an environment without a central player to coordinate the demand

and supply sides of the cryptocurrency.[9] As we shall show in a later section, a unique equilibrium emerges in a traditional IPO setting with the developer sets a membership fee for the households to enter the platform and a separate fee for miners to provide transaction services on the platform.

When the equilibria exist, there are two: one with a high price and a lower cutoff $\underline{A}^*$, in which a larger population enter the platform, and one with a low price and a higher cutoff $\bar{A}^*$, in which few households enter the platform. This occurs again because of the strong network effect in the households' trading on the platform. The household with the highest endowments would always enter the platform but, if too few others enter, then the marginal benefit of trading on the platform is low, since the probability of meeting another household on the platform is low. This leads to a low price for the cryptocurrency. That the low price is not zero distinguishes it from a fiat currency, and reflects our stance that the currency has intrinsic value to households. If instead many households enter, then the marginal benefit of entering the platform is high, sustaining a high price.[10]

We illustrate the intuition for these possible outcomes by using a numerical example with the following parameters:

$$\tau_A = \tau_\xi = 1, \tau_\varepsilon = \tau_e = .5, \bar{A} = \bar{\xi} = 0, \ \eta_c = .3, \text{ and } \rho = .5.$$

Figure 1 depicts the left-hand and right-hand sides of equation (6) against $A^*(A,\xi) - A$. The left-hand side (LHS) is the bell-shaped line, while the right-hand side (RHS) is the flat line $\exp(-A - \xi - \log(1-\rho))$. The dotted line is the RHS when $A = \xi = 0$, while the lower, dashed line sets $A = \tau_\varepsilon^{-1/2}$ at one standard deviation away from 0. The y-intercept of the flat line is decreasing in both A and ξ. As one can see, the flat lines intersect the bell-shaped curve generically at two points, with the intersection on the left side of the bell corresponding to the high price equilibrium with the lower cutoff, while the intersection on the right side is the low price equilibrium with the higher cutoff. As A increases, then intersections shift down the y-axis, and correspond to a lower cutoff $\underline{A}^*(A,\xi) - A$ in the high price equilibrium, and a higher cutoff $\bar{A}^*(A,\xi) - A$ in the low price equilibrium. Whenever the flat line is

[9] Note that the discreteness of the household entry decision is not sufficient for the multiplicity of equilibria. The models of Albagli, Hellwig, and Tsyvinski (2014, 2015) and Gao, Sockin, and Xiong (2018) also have economic agents facing a discrete choice problem, yet in their settings the cutoff equilibrium is unique.

[10] This network effect leads to a backward-bending demand curve for the currency. Backward-bending demand curves can also arise from unobserved portfolio insurance motives, as in Gennotte and Leland (1990), learning by less informed investors, as in Barlevy and Veronesi (2000,2003) and Yuan (2005), and from endogenous collateral margins for arbitrageurs, as in Brunnermeier and Pedersen (2009).

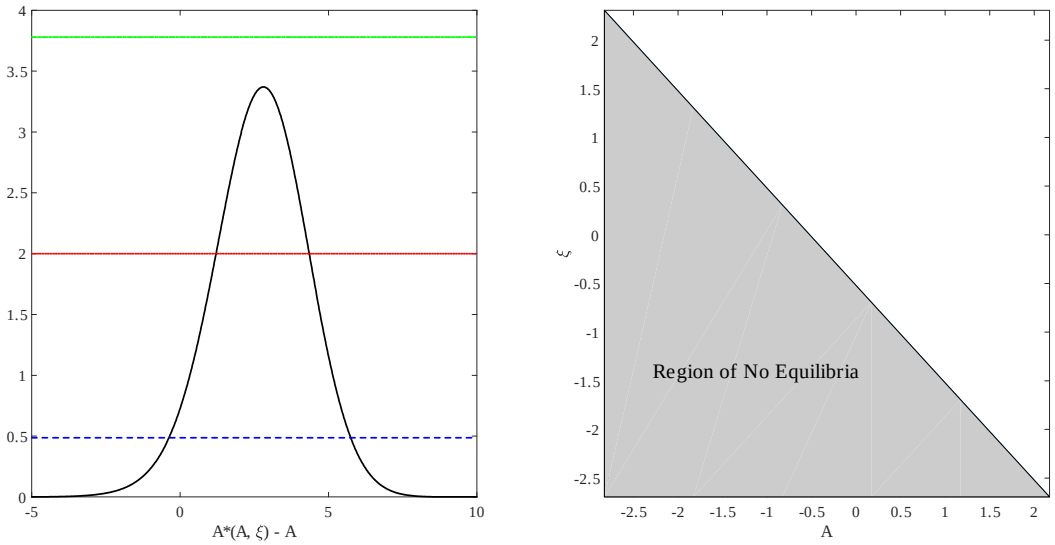


Figure 1: An illustration of equilibrium outcomes when platform fundamentals are observable. The left panel plots the left-hand and right-hand sides of Equation (6), while the right panel plots the region of no equilibria with respect to A and ξ.

above the bell-shaped curve, corresponding to very low values of the demand and supply fundamentals, no cutoff equilibrium exists, and no households purchase the cryptocurrency.

Proposition 2 also provides several comparative statics of the two equilibria. As a result of the nature of the two equilibria, they behave exactly opposite in many ways. As the demand and supply fundamentals increase, the cryptocurrency price increases and more households join the platform in the high price equilibrium, while the opposite happen in the low price equilibrium with the cryptocurrency price dropping and less household joining the platform.

The possibility of market failure and the multiplicity of equilibria are intimately related. The bell-shaped curve characterizing the rational expectations equilibria in Figure 1 arises because participation is an endogenous fundamental for the platform, as a high marginal household expects few trading partners while a low marginal household expects little gains from trade, and the rigidity of the Proof of Work protocol introduces the horizontal line. As a result, the potential for multiplicity when the line and the curve intersect is also responsible for the nonexistence of equilibria, since it is then possible for the line to lie above the curve. Intuitively, the line is above the curve when the token price cannot rise enough to induce a sufficient enough miners to match household participation when the platform fundamentals are sufficiently weak. In the section on alternative platform arrangements, we highlight that this instability vanishes if instead the platform were launched with an IPO or transactions

were cleared with the alternative Proof of Stake (PoS) protocol.

The potential for market failure and equilibria multiplicity when there is household participation has important implications for the stability of new decentralized digital platforms. Even a platform with a strong demand fundamental A may attract little interest from potential users, and this is self-sustaining, even though it could support a much larger subscriber base. On the other hand, another platform with a weaker fundamental may attract more interest from households through a high-price equilibrium. The existence of multiple equilibria and the potential swing between the multiple equilibria help to rationalize a wide spectrum of observed dynamics of different cryptocurrencies—large price swings, confusion and self-fulfilling traps that lead to their failure. This can potentially rationalize why most cryptocurrencies have very little adoption and trade at low valuations, despite having similar features to more successful currencies.

While much of the current policy debate about cryptocurrencies emphasizes that they do not fall within the purview of any government regulatory agency, such as the SEC, that could protect consumers, our analysis suggests that less attention is given to another important feature that distinguishes cryptocurrencies from national currencies: the lack of a central authority, which can provide necessary policy interventions to stabilize markets. The government, as a large player that internalizes how economic actors make decisions and how prices are determined, for instance, plays a pivotal role in setting agent expectations on the future path of the markets, and helps to stabilize prices by committing to act to ensure this path. The absence of a stabilizing hand in cryptocurrencies also explains why large investors have an incentive to act like the so-called coin whales. According to our model, it can be socially beneficial for large investors to take on strategic positions to push the price of a cryptocurrency to its high price equilibrium.[11]

While market failure contributes to the severe instability associated with cryptocurrencies, the multiplicity of equilibria (when they exist) also underscores and exacerbates the challenges in evaluating the fundamental value of a cryptocurrency in practice. When the price of a cryptocurrency rises, it may have opposite implications about the underlying platform depending on whether the market is in the high price or low price equilibrium. These problems become particularly relevant when realistic informational frictions about the platform makes its fundamentals not directly observable to the public, which we analyze in the

[11] Consistent with this, Lee, Li, and Shin (2018) show that large investors purchase a sizable percentage of tokens during the initial days of successful ICOs.

next section.

3 The Setting with Unobservable Fundamentals

Motivated by realistic informational frictions, we now assume that both the households' common endowment A and the miners' common mining cost ξ are not observable to households at $t = 1$ when they need to make the decision of whether to purchase the cryptocurrency and join the platform. Instead, each household observes its own endowment A_i, which combines the aggregate endowment of the relevant households A and the household's own attribute ε_i. Thus, A_i also serves as a noisy private signal about A at $t = 1$. The parameter τ_ε governs both the dispersion in endowments and the precision of this private signal. As $\tau_\varepsilon \to \infty$, the households' signals become infinitely precise and the informational frictions about A vanish. Households care about the aggregate endowment because of complementarity in their demand for consumption. Consequently, while a household may know its own endowment, complementarity in consumption demand motivates it to pay attention to the price of the cryptocurrency to learn about the level of aggregate endowment A, which eventually determines the chance of trading with another household on the platform.

In addition to their private endowment and the market-clearing price of the cryptocurrency, households also observe a noisy signal V about the number of other households that have joined the platform at $t = 1$. An advantage of the blockchain technology that cryptocurrencies employ is that it acts as an indelible and verifiable ledger that records decentralized transactions that take place in the cryptocurrency. As such, it provides a history of public information about the volume of trade in the cryptocurrency. Given a cutoff equilibrium in which households with endowment signals above A^* buy the cryptocurrency, we assume that the volume signal takes the following form:

$$V = \Phi\left(\sqrt{\tau_\varepsilon}\left(A - A^*\right) + \varepsilon_V\right),$$

where $\Phi(\cdot)$ is the CDF of normal distribution and $\varepsilon_V \sim \mathcal{N}\left(0, \tau_v^{-1}\right)$ is independent of all other shocks in the economy. This specification has the appeal that the volume signal is always between 0 and 1 for plausibility, and is highly correlated with the number of coins in active circulation.[12]

[12]The noise in the signal reflects that, in practice, the anonymous nature of the transactions makes it difficult to assess the effective supply of cryptocurrencies in circulation, since transferring cryptocurrencies

To forecast the platform fundamental A, each household's information set $\mathcal{I}_i$ now includes its own endowment A_i, the volume signal V, and the equilibrium cryptocurrency price P. As in the perfect-information setting, we can verify that each household would still use a cutoff strategy, and the equilibrium cryptocurrency price would still be a nonlinear correspondence of A, which poses a challenge to our derivation of households' learning about A. It turns out that after a nonlinear transformation the information content of P can be summarized by a summary statistic z that is linear in A and the supply shock ξ:

$$z = A - \sqrt{\frac{\tau_e}{\tau_\varepsilon}} \left(\xi - \bar{\xi}\right). \tag{7}$$

In our analysis, we shall first conjecture this linear summary statistic for the equilibrium price and then verify that it indeed holds in the equilibrium. This conjectured linear statistic helps to ensure tractability of the equilibrium despite that the equilibrium cryptocurrency price is highly nonlinear. Since the CDF of the normal distribution is a monotonically increasing function, we can invert V to construct an additive summary statistic v:

$$v = \tau_\varepsilon^{-1/2} \Phi^{-1}(V) + A^* = A + \tau_\varepsilon^{-1/2} \varepsilon_V, \tag{8}$$

which serves as the volume statistic. Interestingly, the precision of the volume statistic is $\tau_\varepsilon \tau_v$, so that the less dispersed the endowments of households, the more informative is the volume signal.[13]

By solving for the learning of households based on the conjectured summary statistic from the housing price and the volume statistic, and clearing the aggregate cryptocurrency demand of the households with the supply from miners, we derive the cryptocurrency market equilibrium. The following proposition summarizes the equilibrium price and each household's cryptocurrency demand in this equilibrium.

Proposition 3 *When the platform fundamentals A and ξ are not publicly observable at $t = 1$, there are generically two rational expectations equilibria, in which the following hold:*

across wallets, in which no actual currency is traded between two parties, is a transaction that hits the blockchain. Furthermore, while the underlying code of cryptocurrencies records the total supply of coins, even as new coins are mined, the effective supply of coins in circulation is estimated in a manner similar to asset float for stocks. Some developers, for instance, retain ownership of a fraction of the total supply of coins in escrow accounts, and some coins sit in accounts that are no longer active. We parameterize the residual uncertainty arising from these issues as measurement error.

[13] In contrast to Kocherlakota (1998), in which memory implicitly encoded in monetary balances is used for individual monitoring, memory encoded in the ledger is explicit and serves as an aggregate signal about the currency's fundamental.

1. *The cryptocurrency price takes the same log-linear form as in the perfect-information setting:*

$$\log P = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A - A^*\right) - \xi - \log\left(1-\rho\right), \tag{9}$$

where the cutoff A^* is a correspondence of price statistic z and volume statistic v, rather than A and ξ.

2. *The posterior of household i conditional on z, v, and its own endowment A_i is Gaussian with the conditional mean $\hat{A}_i$ and variance $\hat{\tau}_A$ given by*

$$\begin{aligned}\hat{A}_i &= \hat{\tau}_A^{-1}\left(\tau_A\bar{A} + \tau_v v + \frac{\tau_\varepsilon}{\tau_e}\tau_\xi z + \tau_\varepsilon A_i\right),\\ \hat{\tau}_A &= \tau_A + \tau_v + \frac{\tau_\varepsilon}{\tau_e}\tau_\xi + \tau_\varepsilon.\end{aligned}$$

3. *Household i follows a cutoff strategy in its cryptocurrency choice:*

$$X_i = \begin{cases} 1 & \text{if } A_i \geq A^* \\ 0 & \text{if } A_i < A^* \end{cases},$$

where $A^*\left(z,v\right)$ solves equation (19) in the Appendix.

4. *There are either two or no equilibria, and equilibria fail to exist if z is sufficiently low (high) when $\tau_A + \tau_v \geq (<)\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\tau_\xi$ or v is sufficiently low. When the two equilibria exist, in response to a positive shock ε_V to the volume signal, the equilibrium cutoff A^* decreases, and both the cryptocurrency price and the number of households that purchase the cryptocurrency increase in the high price equilibrium, while the shock has the opposite effects in the low price equilibrium.*

Proposition 3 confirms even when the platform fundamentals A and ξ are not publicly observable, the equilibrium cryptocurrency price in (9) takes exactly the same log-linear form as in the perfect-information setting (Proposition 2). The only difference is the equilibrium cutoff A^* used by the households. With the fundamental variables A and ξ being unobservable, each household has to make its decision based on its own endowment A_i, together with the publicly observed price and volume signals, which are equivalent to the two summary statistics z and v. The equilibrium cutoff A^* now becomes a correspondence of z and v. Being the only difference in the equilibrium price correspondence from the perfect-information setting, $A^*\left(z,v\right)$ is also the only channel through which the households' learning of A through the price and volume signals affects the market equilibrium.

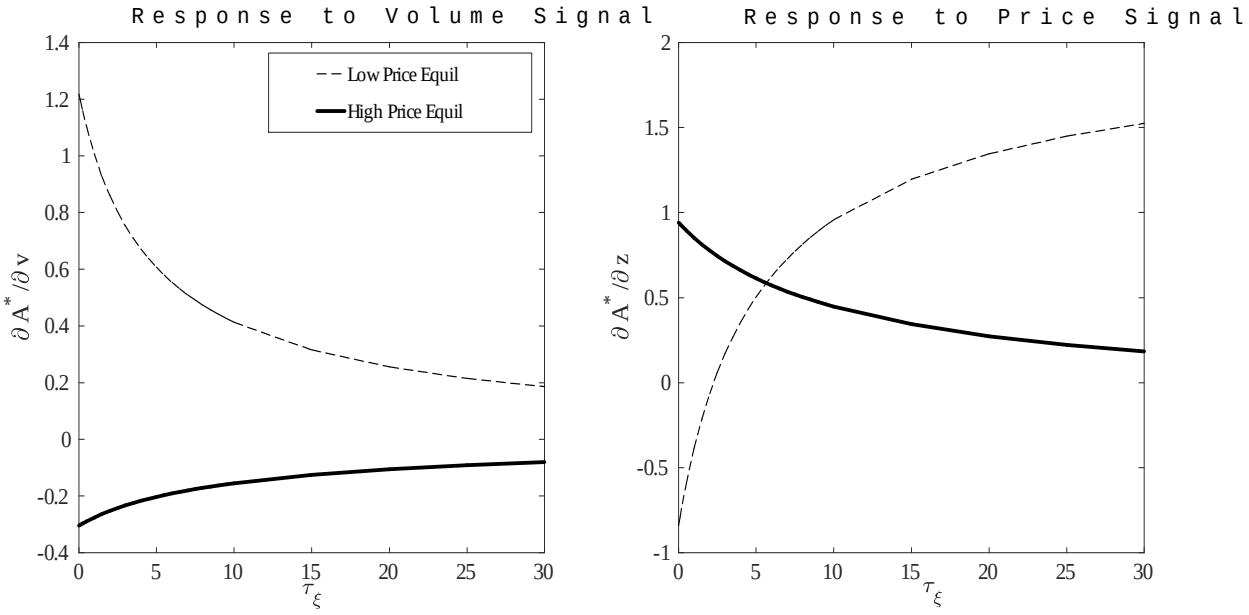


Figure 2: The equilibrium cutoff $A^*(z, v)$ with respect to z and v in the high-price and low-price equilibria across different values of τ_ξ.

As in the perfect-information setting, there are again either none or two equilibria. This situation arises from solving $A^*(z, v)$ from its fixed-point condition given in equation (19), which is similar to equation (6) and may have either zero or two real solutions. There are no equilibria when the publicly observed platform fundamentals are sufficiently weak, i.e., when z is sufficiently large (small) when the cost (information) effect dominates, or v is sufficiently small since it is a signal of a weak demand fundamental.

When two equilibria exist, one has a lower equilibrium cutoff for households' cryptocurrency purchase decision and a higher cryptocurrency price, while the other has a higher equilibrium cutoff and a lower price. These two equilibria again behave in opposite ways. Proposition 3 formally shows that in response to a shock to the volume signal, the equilibrium cutoff A^* and cryptocurrency price P have opposite reactions across the two equilibria.

3.1 Learning from Price and Volume

We now discuss how learning induced by informational frictions regarding the platform fundamentals A and ξ affects responses of the equilibrium to various shocks, by taking a given equilibrium. Following our earlier discussion, learning operates through the network effect, as each household needs to form an expectation of the number of household population

joining the platform and its probability of matching with a trade counterpart on the platform.

Figure 2 depicts the responses of the equilibrium cutoff $A^*(z, v)$ to shocks to both v and z, as measured by $\frac{\partial A^*}{\partial v}$ and $\frac{\partial A^*}{\partial z}$, across the high-price and low-price equilibria. The left panel shows how a random shock to the volume statistic affects A^*. Note that such a shock has no effect on the equilibrium in the perfect-information setting. The left panel shows that in the high-price equilibrium, the equilibrium cutoff A^* moves down in response to an increase in v, a positive signal about the platform fundamental A, indicating that more households join the platform. In contrast, A^* reacts positively to v in the low-price equilibrium, causing a smaller population to enter the platform. Interestingly, the reactions in both equilibria diminish as τ_ξ increases. This is because the reactions in A^* are driven by the households' learning about A from the volume signal v. As τ_ξ rises, the price of the cryptocurrency becomes more informative about A and, as a result, crowds out the learning effect of v. Overall, this panel shows that household learning exacerbates the effect of the volume noise on the equilibrium cutoff A^* and thus the equilibrium price.

In classical asset market models with dispersed information, e.g., Grossman and Stiglitz (1980) and Hellwig (1980), trading volume plays no role in learning,[14] and is often studied only for its empirical predictions, as in, for instance, Wang (1994) and He and Wang (1995).[15] In our setting, households learn from both the price and volume of the cryptocurrency when deciding whether to purchase it. As such, volume provides a complementary source of information to the cryptocurrency price and, as can be seen in the left panel of Figure 2, any noise in the volume signal distorts households' participation decisions.

The right panel illustrates how the cutoff A^* responds to a shock to the price statistic z, which, as given in (7), represents a linear combination of the demand-side fundamental A and the supply-side fundamental ξ. For τ_ξ close to 0, z contains little information about A. Consequently, an increase in z does not generate any learning effect, but only the cost effect. As a result, less households enter the platform in the high price equilibrium, in response to the higher price of entry, while more households enter in the low price equilibrium, as the

[14] This is, in part, an artifact of the CARA-Normal paradigm, in which trading volume is the expectation of a folded normal random variable. This makes learning intractable if a noisy version of trading volume were observed. An advantage of our focus on a cutoff equilibrium is that we are able to incorporate a noisy measure of volume while still maintaining tractability.

[15] Notable exceptions are Blume, Easley, and O'Hara (1994) and Schneider (2009). In the former, past prices and volumes trivially reveal the sufficient statistics of all past trader private information (which still contain residual uncertainty because of correlated signal error). In the latter, trading volume provides a signal about how informative prices are about an asset's fundamentals.

low price equilibrium features an opposite reaction to prices. As τ_ξ increases, however, the role of a higher z in reflecting a higher A becomes more pronounced, and the learning effect begins to offset the cost effect of a higher price. As a result, less households are crowded out by a higher price in the high price equilibrium, as they believe the higher price also reflects a higher benefit from joining the platform.

Learning in Dynamic Setting Learning within equilibria can be even more destabilizing in a dynamic setting, as uncertainty about the future degree of coordination on the platform impacts the decision of households to join today. While with perfect information, the ability to resell the currency at a later date always entices more households to join the platform initially,[16] retrading in the presence of informational frictions can unravel the rational expectations equilibrium. Since the currency price and the platform fundamentals have the opposite relation across the high and low price equilibria, and a household's type cannot be separated from its private signal about the demand fundamental, households most optimistic about trading with each other are not those most optimistic about the profit from reselling the currency if they expect a low price equilibrium in the future. As a result, a rational expectations equilibrium can cease to exist today. This highlights the inherent intertemporal fragility of coordination that arises with informational frictions, as a small shift in perceptions of a low price equilibrium tomorrow can cause massive fluctuations in market outcomes day as rational expectations equilibria in the cryptocurrency may break down.

Learning across Equilibria An implicit assumption underlying our analysis is that market participants can coordinate on a high or low price equilibrium. This separates the inference and coordination problems, enabling market participants to glean successfully the sufficient statistics from the price and volume signals. Once they correctly recover the linear summary statistics z and v, they can reconstruct the trading price P and volume V, for a given equilibrium cutoff $A^*(z,v) \in \left\{\underline{A}^*(z,v), \bar{A}^*(z,v)\right\}$, according to:

$$\begin{aligned} P &= \frac{1}{1-\rho}\exp\left(z - \sqrt{\frac{\tau_\varepsilon}{\tau_e}}A^*\right), \\ V &= \Phi\left(v - \sqrt{\tau_\varepsilon}A^*\right), \end{aligned}$$

which are the outcomes actually observed by market participants.[17]

[16] This dynamic adoption channel is featured in Cong, Li, and Wang (2018).

[17] In technical terms, we implicitly assumed the equivalence of $\sigma(\{v,z\})$ and $\sigma(\{P,V\})$ without modeling the coordination device, i.e. sunspot. We did this for parsimony of exposition.

It is less clear, however, how such coordination arises in practice, or to predict which equilibrium will manifest at any given moment in the cryptocurrency market.[18] For every price-volume pair, an observer can rationalize two different sets of sufficient statistics, one corresponding to a conjecture of a high-price equilibrium and the other to that of a low-price equilibrium, with only one being the correct inference. This dual inference problem makes it particularly difficult for outsiders to interpret market conditions from prices, potentially leading to erratic trading behavior by speculators based on technical analysis. Depending on an outside investor's assessment of which equilibrium the market is currently in, for instance, it may adopt either a trend-chasing or contrarian strategy, and can dramatically reverse its strategy if it speculates that the market might switch equilibria. Such volatile behavior can act as an additional source of nonfundamental instability in cryptocurrency markets.

This potential confusion arising from the instability of the platform also introduces a secondary role for volume as a signal about coordination in conjunction with prices. Observing a history of past prices and volumes can help resolve confusion about coordination as an econometrician can test whether the observed correlations between fundamentals and past market outcomes coincide with their predicted counterparts. In the short-run, however, such analysis is limited, and having volume as a second source of information is even more important. In practice, we view this volume signal as being analogous to the volume of transactions recorded on the ledgers of the cryptocurrency, and our analysis emphasizes the importance of examining both prices and quantities in cryptocurrency markets. Consequently, any fundamental analysis of the cryptocurrency should look beyond prices and to volumes as an anchor.

3.2 Incentive to Information Disclosure

The instability endemic to decentralized digital platforms also shapes the incentives for the developer to disclose public information about the platform fundamentals. Since the launch of the ICO can result in one of two equilibria with disparate behaviors, or platform failure if no rational expectations equilibria exist, the developer's payoff profile is nonconvex in the posterior belief of households. This nonconvexity reduces the value of voluntary disclosure, as the developer would prefer some degree of opacity in information it conveys to households.

[18] One proposed selection argument is stability of the equilibria, as discussed in Manzano and Vives (2010). This refinement, however, is a criterion based on how agents' optimal policies react to an out-of-equilibrium perturbation to the price schedule. Along the equilibrium path, it is less clear such equilibria could be ruled out.

To illustrate this point, we proceed in the spirit of the Bayesian Persuasion literature, e.g., Aumann and Maschler (1995) and Kamenica and Gentzklow (2015), in which we consider the hypothetical situation in which the developer could commit to communicate a (potentially garbled) public signal to households about the demand fundamental once the platform is launched. Such a public signal can, for instance, be in the form of a whitepaper, other financial disclosures about the platform, an experiment such as beta testing by potential customers, or publication of consumer reviews.

As the space of potential messages by the developer (sender) is unbounded, and there is a continuum of heterogeneously and privately informed receivers (households), our ability to characterize the optimal information structure is limited, and we restrict our attention to when all agents hold homogeneous normal priors. The following proposition establishes the key result.

Proposition 4 *When the platform is funded by an ICO, the developer prefers some opacity over full disclosure of platform fundamentals.*

The competitive and decentralized nature of the ICO token price materially impacts the value of public information for the developer. While the developer's profit can be strictly convex in the low price equilibrium for certain parameters, it must be strictly concave for low realizations of the posterior in the high price equilibrium. Futher, since nonexistence of an equilibrium garners zero profit for the developer, there is a step function in profit when the posterior mean in sufficiently small. As such, the value of public information depends on the prior, and will likely include a mixture of pooling signals for low realizations and being fully transparent for high realizations of the demand fundamental.

Although the developer benefits from some persuasion, our analysis suggests it has incentive to withold information if disclosure is voluntary. Such an observation can rationalize the opacity of current ICOs, in which fraud has been sufficiently rampant to garner the attention of the SEC, and suggests a stronger need for regulation than in the IPO market.

4 Alternative Platform Arrangements

In this section, we consider two alternative arrangements for the decentralized digital platform to highlight how its intrinsic fragility shapes the value of voluntary disclosure for the developer, and how it stems from the competitive nature of how tokens are distributed to

households and miners. In the first, we examine the developer's profit and performance of the platform from funding the platform through a traditional Initial Public Offering (IPO) arrangement, rather than an ICO. We compare the market outcomes across the IPO and ICO settings and, in particular, show that the developer is more willing to disclose information when the platform is funded by an IPO, and that the instability of rational expectations equilibria endemic to market-clearing vanishes. In the second, we investigate an ICO on a blockchain supported instead by a Proof of Stake (PoS) protocol to explore how an alternative protocol for clearing transactions impacts the performance of the ICO and the platform.

4.1 Initial Public Offering

In this subsection, we examine an alternative funding arrangement for the developer to launch the platform through a more traditional IPO to illustrate that the difference in funding medium drastically changes the value of public information for the developer. Since the developer can act as a monopolist in selling platform memberships and compensating miners, it can avoid the market failure of the ICO by willingly absorbing a loss to clear both sides of the market. This ability restores uniqueness of the rational expectations equilibrium and convexity to the developer's profit from the ICO in the households' common belief about the demand fundamental.[19] As a result, the developer has incentive to provide full transparency when disclosing relevant information about the platform to households.

To illustrate this point, suppose that, instead of issuing cryptocurrency to households with a floating price determined by market-clearing, at $t = 1$ the developer sets a compensation fee for miners $e^{-\omega^*}$, which is equal to the cost of the marginal miner, based on his belief about the demand fundamental, A. At $t = 2$, the developer sets the membership price P in a silent-bid competitive auction, in which households submit their bid schedules for platform participation based on their knowledge of their type, A_j, and all available public information. The stop-out rate from this auction is then the cost of membership for all participating households. For simplicity, we assume that the average log cost of mining, ξ, is common knowledge, since it will not impact our results.

[19] Although the developer, in principle, could vary the fraction of the membership price paid to miners, ρ, in the ICO, it cannot prevent market failure and equilibria multiplicity since it is set ex ante.

Then, the developer's profit from the IPO is:

$$\Pi_D^{IPO} = P\Phi\left(\frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) - e^{-\omega^*}\Phi\left(\frac{\omega^* - \xi}{\sqrt{\tau_e}}\right),$$

where, to ensure equal numbers of households and miners on the platform, ω^* needs to satisfy:

$$\frac{A - A^*}{\tau_\varepsilon^{-1/2}} = \frac{\xi - \omega^*}{\tau_e^{-1/2}}.$$

In the IPO, the developer securitizes this expected profit from the platform as stock to a unit continuum of outside investors at a market value of S. Similar to households, we assume that investors have dispersed information about the platform demand fundamental, A, such that investor j is endowed with a private signal:

$$s_j = A + \tau_s^{-1/2}\varepsilon_j,$$

where $\varepsilon_j \sim \mathcal{N}(0,1)$ such that the Strong LLN holds in the continuum. Investors are risk-neutral and investor i takes a position x_i in the stock to maximize its expected profits. As is standard in the literature, we assume investors face bounded position limits, and can either buy or sell one unit of stock ($x_i \in [-1,1]$). In addition, there are noise traders in the stock that take an aggregate position $2\Phi\left(\tau_\varphi^{1/2}\varphi\right)$, where $\varphi \sim \mathcal{N}(0,1)$.

Standard results in the literature suggest that investors optimally follow a cutoff strategy, buying the stock if $s_j \geq s^*$, and short-selling if $s_j \leq s^*$. We then conjecture that the stock price S takes the following form:

$$S = E\left[\Pi_D \mid s^*, s_j = s^*\right],$$

where:

$$s^* = A + \sqrt{\frac{\tau_\varphi}{\tau_s}}\varphi,$$

is the signal of the marginal investor. We assume that the developer has no private information, and chooses the membership fee to maximize the expected profit of the platform, so that there is no conflict of interest with new shareholders.

We then have the following proposition characterizing the noisy rational expectations cutoff equilibrium with the IPO.

Proposition 5 *When the platform is funded by an IPO, 1) the developer chooses the fee to miners* $e^{-\omega^*} = e^{\tau_e^{-1/2}w - \xi}$, *where* w *solves the program (21); 2) the stock price* S *takes the*

following form:

$$S = \left(\frac{e^{\hat{A}+\left(\left(1-\frac{\eta_c \hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\frac{\tau_s}{\hat{\tau}_{A,D}}\frac{\tau_A}{\hat{\tau}_{A,D}}+\frac{\tau_s \tau_\varphi^{-1}}{\hat{\tau}_{A,D}}\right)\left(A-\hat{A}+\sqrt{\frac{\tau_\varphi}{\tau_s}}\varphi\right)-\left(1-\frac{\eta_c \hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\tau_\varepsilon^{-1/2} w}}{\Phi\left(\eta_c \tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1} e^{-\frac{1}{2}\left(1-\frac{\eta_c \hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}-\frac{1}{2}\eta_c^2\left(\left(\tau_A+\tau_s\tau_\varphi^{-1}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}} - e^{\tau_e^{-1/2} w-\xi} \right) \Phi(w),$$

where $\hat{\tau}_{A,D} = \tau_A + \tau_s \tau_\varphi^{-1}$*, and* S *is an increasing function of* s^**; and 3) investors and households both follow their conjectured cutoff strategies.*

Proposition 5 confirms the conjectured cutoff equilibrium for the IPO. The stock price is equal to the valuation of the platform's expected profit from the perspective of the marginal investor. Instead of the token's price, the stock price aggregates valuable information about the platform's potential, as well as about the noise trading in the stock market. As investors are a different source of information than platform participants, and are likely further removed in assessing the benefits of the platform's operations, this difference in the financing medium represents an important distinction between IPOs and ICOs in the presence of informational frictions.

In the absence of informational frictions, it is not surprising that the developer would always prefer to raise funds through the IPO, since it acts as a monopolist in setting the mining fee, whereas it and the memership price are determined by market-clearing in the ICO. Our interest is in understanding how differences in the architectures of the two financing mediums shape the role and value of information in launching the platform. While a comprehensive comparison is beyond the scope of this paper, we can provide some insight into the value of public information to the developer.

To make our analysis comparable across the two funding mediums, we again restrict attention to the value of the public information received by the households about the demand fundamental for the developer's profit. The following proposition establishes the key distinction we wish to highlight between IPOs and ICOs with respect to information disclosure.

Proposition 6 *When the platform is funded by an IPO, the developer prefers full disclosure of public information relevant to the platform.*

Proposition 6 establishes that, if able to communicate information about their common demand to households, a developer would prefer to make any disclosure as informative as possible in an IPO. The intuition is that the developer's profit is now strictly convex in the

posterior belief of households about the demand fundamental, and therefore the developer would want their common beliefs to be as volatile as possible, and more disclosure increases the variance of the conditional mean. Consquently, the developer has incentive to disclose voluntarily as much information as possible to potential customers about the platform, in contrast to the ICO.

4.2 Proof of Stake Protocol

In this subsection, we illustrate that the fragility of the digital platform, with equilibria multiplicity and nonexistence, stems from its decentralized nature when supported by the Proof of Work protocol. Much of the recent debate about cryptocurrencies is about the potential transition from the Proof of Work (PoW) protocol, which underlies most cryptocurrency coins and tokens that exist, to a Proof of Stake (PoS) consensus protocol.[20] In a PoS protocol, owners of the currency called "forgers" act as intermediaries, and clear transactions for fees with a likelihood proportional to their latent stake in the currency. This stake is often measured as coins or tokens in a wallet that have been inactive for a certain period of time. An important feature of PoS is that it does not suffer from the scalability issue of PoW, in that more intensive computing power of miners is required as the network grows. Although PoS restores existence and uniqueness of an equilibrium in the ICO, the sale of tokens to forgers crowds out household participation on the platform, and distorts the developer's incentives to maximize participation when launching it.

We now consider a slightly modified setting to explore the tradeoffs of PoS. Instead of having miners supply accounting services in exchange for currency, or payment by inflation, we have a unit continuum of forgers that purchase a fraction of the currency, which we normalize to be in unit supply, as their stakes. A stake of size p_i in the currency will entitle an intermediary to a fraction $\left(\int_0^1 p_j dj\right)^{-1} p_i$ of the total fees from providing accounting services to clear household transactions at $t = 2$. The fee, set by the developer, is a fraction θ of the endowment of each household that trades at $t = 2$, while completing each transaction costs a forger a fraction $\lambda \in (0, 1)$ of this value. Since households intend to trade on the platform, their currency account is considered active and, as such, they are not entitled to participate in clearing transactions.

We assume intermediaries of each type are atomistic and identical. Each buys a fraction

[20] Many platforms with ICOs, for instance, are designed as smart contracts written onto existing blockchain architecture, such as Ethereum, which employ a PoW protocol.

p_i of the currency subject to a common noisy cost of capital ψ where $\psi \sim \mathcal{N}\left(\bar{\psi}, \tau_{\psi}^{-1}\right)$. is normally distributed. Forger i solves the optimization program:

$$\Pi_0^i = \sup_{p_i} \left[\frac{\theta - \lambda}{\int_0^1 p_j dj} e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\varepsilon^{-1}} \Phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}} \right) \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}} \right) - e^{\psi} P \right] p_i,$$

subject to the market-clearing condition for the currency:

$$\int_{-\infty}^{\infty} X_i\left(A_i, P\right) d\Phi\left(\varepsilon_i\right) + \int_0^1 p_i di = 1.$$

Assuming a cutoff strategy for households, we can solve the market-clearing condition to relate the total stake of forgers to the marginal household with type A^* :

$$\int_0^1 p_i di = \Phi\left(\frac{A - A^*}{\sqrt{\tau_\varepsilon}} \right).$$

Define $A^* = A + \tau_\varepsilon^{-1/2} s$. Furthermore, since the program for forgers is linear in p_i, it follows that the expression in parentheses must be zero, and therefore that s solves:

$$e^{-(1-\eta_c)\tau_\varepsilon^{-1/2} s + \frac{1}{2}(1-\eta_c)^2 \tau_\varepsilon^{-1}} \frac{\Phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2} - s \right)}{\Phi\left(-s\right)} = \frac{1-\theta}{\theta - \lambda} e^{\psi}.$$

for them to be indifferent to the size of their stake.[21] Consequently, $s = h\left(\frac{1-\theta}{\theta-\lambda} e^{\psi}\right)$. Since the LHS satisfies:

$$\frac{d \log LHS}{ds} = -\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} + \frac{\phi\left(-s\right)}{\Phi\left(-s\right)} - \frac{\phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2} - s \right)}{\Phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2} - s \right)},$$

which attains its maximum as $s \to \infty$, $\frac{d \log LHS}{ds} \to 0$, and therefore the LHS is (weakly) monotonically decreasing in s from ∞ to 1. It then follows that s exists and is unique, provided that $\frac{1-\theta}{\theta-\lambda} e^{\psi} \geq 1$, and that $h'\left(\frac{1-\theta}{\theta-\lambda} e^{\psi}\right)$, $h''\left(\frac{1-\theta}{\theta-\lambda} e^{\psi}\right) \geq 0$.

Substituting the marginal household cutoff A^* into the price of the currency, given by the utility of the marginal household, we arrive at:

[21] A corner solution in which all households buy the curreny ($p_i = 0 \ \forall \ i$) can be ruled out *a.s.* since the currency price would have to collapse to zero to ensure all households, even those with extremely low endowments, participate. Then, however, the cost of acquiring a stake is zero, while transaction fees are positive, violating the choice of forgers not to buy a stake.

If forgers bought all the currency ($\int_0^1 p_j dj = 1$), then the currency price would also collapse to zero. We can rule out this outcome by considering a sequence of platforms that provide an $\varepsilon_n > 0$ (arbitrarily small) benefit to each household for participating, and taking the limit as this small benefit approaches zero. Such a refinement would not, in contrast, resolve the multiplicity in the PoW setting.

$$P = (1-\theta)\, e^{(1-\eta_c)\tau_\varepsilon^{-1/2} h\left(\frac{1-\theta}{\theta-\lambda}e^{\psi}\right)+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} \Phi\left(\eta_c\tau_\varepsilon^{-1/2} - h\left(\frac{1-\theta}{\theta-\lambda}e^{\psi}\right)\right),$$

which is unique given a choice of fees θ. As A^* is increasing in ψ, it follows that the currency price is decreasing in ψ for a fixed choice of fees θ.

Suppose that the developer chooses θ to maximize its expected revenue, internalizing its impact on household and forger participation:

$$\Pi_0^D = \sup_{\theta} (1-\theta)\, e^{(1-\eta_c)\tau_\varepsilon^{-1/2} h\left(\frac{1-\theta}{\theta-\lambda}e^{\psi}\right)+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} \Phi\left(\eta_c\tau_\varepsilon^{-1/2} - h\left(\frac{1-\theta}{\theta-\lambda}e^{\psi}\right)\right).$$

It then follows from the FONC that at an interior solution that the optimal $\theta = \frac{1+\lambda x}{1+x}$ satisfies:[22]

$$\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - h\left(xe^{\psi}\right)\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - h\left(xe^{\psi}\right)\right)} - (1-\eta_c)\,\tau_\varepsilon^{-1/2} = \frac{1}{h'\left(xe^{\psi}\right)e^{\psi}x\,(1+x)}.$$

Since the LHS is monotonically increasing from $-(1-\eta_c)\,\tau_\varepsilon^{-1/2}$ to ∞, while the RHS is monotonically decreasing from ∞ to 0, it follows an interior optimal choice of x, and consequently θ, exists and is unique. Consequently, their is an optimal fee that the developer can set to maximize its revenue from the ICO. Interestingly, the optimal choice of θ is independent of the platform's demand fundamental A, and only a function of the cost of capital of forgers ψ. As A^* tends to ∞ when $\frac{1-\theta}{\theta-\lambda}e^{\psi} \to 1$, earning zero revenue for the developer, it follows that at the optimum θ will be such that $\frac{1-\theta}{\theta-\lambda}e^{\psi} > 1$.

In the PoS network, there is no issue of fragility in the cryptocurrency, despite the dual nature of ICO investors. Since the price of the cryptocurrency scales with the expected transaction fees paid to forgers, it is the inverse relationship between the aggregate stake of forgers, p, and the population of households that participates in the platform that leads to a unique cutoff for households A^*. Since forgers are paid in transaction fees rather than tokens, which are a cost to them with pPoS, this additional flexibility in the token price allows it to adjust to be able to clear the market for both households and forgers for any realization of the fundamentals. As a result, the currency price is also no longer linked to the marginal cost of mining, as in the PoW protocol; instead, it depends on the forger's cost of capital ψ, similar to the role of financial frictions in fiat currencies intermediated by traditional intermediaries, as in Gabaix and Maggiori (2015). When the opportunity cost to providing

[22] Notice that $\theta - \lambda = \frac{1-\lambda}{1+x} > 0$, and therefore forgers will always earn a positive revenue from transaction fees at an interior optimal choice of x.

accounting services increases, a higher ψ, forgers requires a higher return to participate, and this reduces the entry of households to lower the currency price and, consequently, the cost of acquiring their stake.

In addition, the currency developer can maximize its profits from the ICO through the appropriate choice of fees θ, which trades off participation by households in the platform with participation by forgers. With the PoS protocol, the developer also does not have to be concerned about the potential for coordination failure by households, as it did with PoW. While the platform no longer suffers from fragility, however, PoS does introduce a different distortion: maximizing developer revenue is not necessarily equivalent to maximizing household participation in the platform, as the currency is sold to both households and forgers, while it is with PoW because price and quantity are both increasing in the number of participating households. Such a wedge may not be desirable from a social perspective because the expected social surplus from the platform is equal to the total endowment of participating households less the fraction λ burned to complete the transactions. As such, the fees given to forgers represent zero-sum transfers for which forgers compete by acquiring stakes in the currency that can potentially crowd out households.

5 Conclusion

Since the shareholders who participate in ICOs are also the customers that use the currency to trade goods and services, cryptocurrencies and their underlying platforms are subject to more pronounced feedback from financial market outcomes to real decisions than traditional financial assets. As a result, there is an intimate link between the success of the ICO and the viability of the currency as membership to a network. This link gives rise to the possibility of coordination failure, whereby the currency price and the volume of coins in active circulation reflect whether the market is in an equilibrium in which the currency price is high (low) and many (few) households participate, and there is the possibility for market failure. As the two equilibria, when they exist, have very disparate properties, observing the same price and volume fluctuations have very different implications for diagnosing the health of the currency depending on the equilibrium.

Since cryptocurrencies are not supported by a sovereign or central intermediaries that can help coordinate participants along an equilibrium path, multiplicity and nonexistence of equilibria has a destabilizing impact on the currency. Furthermore, it can invite manipula-

tion from large investors. While having stake holders in the currency act as intermediaries with the Proof of Stake protocol helps resolve the issues of multiplicity and scalability of the platform, it makes the currency susceptible to fluctuations in their cost of capital, and introduces a wedge for the developer between maximizing revenue from the ICO and maximizing household participation.

In the presence of realistic informational frictions, the currency price and volume take on an additional dimension as useful signals about the demand fundamental underlying the cryptocurrency. Coordination issues also extend to this incomplete information setting, and the market reacts very differently to news stemming from these signals depending on whether the market is in the high or low price equilibrium. One cannot, therefore, easily disentangle inference about the fundamental from that about coordination, and there are many ways to rationalize any price fluctuations from the perspective of an outsider. Analyzing measures of quantities, such as the volume of transactions recorded on its ledgers, can provide helpful insight when trying to tether valuations of these cryptocurrencies, while technical analysis can worsen price fluctuations. In addition, the fragile nature of the ICO reduces the incentives for the developer to voluntarily disclose information relevant about the platform to households, whereas it would prefer to fully disclose any information if the platform were funded by an IPO.

Our work, consequently, cautions any attempt at valuation or regulation of cryptocurrencies that fails to account for their dual role as securities and mediums of exchange.

References

Abadi, Joseph and Markus Brunnermeier (2018), Blockchain Economics, mimeo Princeton University.

Albagli, Elias, Christian Hellwig, and Aleh Tsyvinski (2014), Risk-Taking, Rent-Seeking, and Investment when Financial Markets are Noisy, mimeo USC Marshall, Toulouse School of Economics, and Yale University.

Albagli, Elias, Christian Hellwig, and Aleh Tsyvinski (2015), A Theory of Asset Prices based on Heterogeneous Information, mimeo Bank of Chile, Toulouse School of Economics, and Yale University.

Aumann, Robert J. and Michael B. Maschler (1995), Repeated Games with Incomplete Information, MIT press, Cambridge University Press, 1995.

Barlevy, Gadi and Pietro Veronesi (2000), Information Acquisition in Financial Markets, *Review of Economic Studies* 67, 79-90.

Barlevy, Gadi and Pietro Veronesi (2003), Rational Panics and Stock Market Crashes, *Journal of Economic Theory* 110, 234-263.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta (2017), The Blockchain Folk Theorem, mimeo Toulouse School of Economics and McGill School of Management.

Blume, Lawrence, David Easley, and Maureen O'Hara (1994), Market Statistics and Technical Analysis: The Role of Volume, Journal of Finance 49, 153-181.

Brunnermeier, Markus K. and Lasse Pedersen, Market Liquidity and Funding Liquidity (2009), *Review of Financial Studies* 22, 2201-2238.

Catalini, Christian and Joshua S Gans (2018), Initial Coin Offerings and the Value of Crypto Tokens, NBER.

Chiu, Jonathan and Thorsten V. Koeppl (2017), The Economics of Cryptocurrencies - Bitcoin and Beyond, mimeo Victoria and Queen's University.

Chod, Jiri and Evgeny Lyandres (2018), A Theory of ICOs: Diversification, Agency, and Information Assymetry, mimeo Boston College and Boston University.

Cochrane, John (2005), Money as Stock, *Journal of Monetary Economics* 52, 501-528.

Cong, Lin William and Zhiguo He (2017), Blockchain Disruption and Smart Contracts, mimeo University of Chicago Booth School of Business.

Cong, Lin William, Zhiguo He and Jiasun Li (2018), Decentralized Mining in Centralized Pools, mimeo University of Chicago Booth School of Business.

Cong, Lin William, Ye Li, and Neng Wang (2018), Tokenomics: Dynamic Adoption and Valuation, mimeo University of Chicago Booth School of Business, Ohio State University, and Columbia Business School.

Dasgupta, Amil (2007), Coordination and Delay in Global Games, *Journal of Economic Theory* 134, 195-225.

Easley, David, Maurenn O'Hara, and Soumya Basu (2017), From Mining to Markets: The Evolution of Bitcoin Transaction Fees, mimeo Cornell University.

Gao, Zhenyu, Michael Sockin, and Wei Xiong (2018), Learning about the Neighborhood, mimeo CUHK, UT Austin, and Princeton University.

Gennotte, Gerard, and Hayne Leland (1990), Market Liquidity, Hedging, and Crashes, *American Economic Review* 80, 999-1021.

Goldstein, Itay, Emre Ozdenoren and Kathy Yuan (2013), Trading frenzies and their impact on real investment, *Journal of Financial Economics*, 109(2), 566-582.

Grossman, Sanford and Joseph Stiglitz (1980), On the impossibility of informationally efficient markets, *American Economic Review* 70, 393-408.

He, Hua and Jiang Wang (1995), Differential Information and Dynamic Behavior of Stock Trading Volume, *The Review of Financial Studies* 8, 919-972.

Hellwig, Martin (1980), On the aggregation of information in competitive markets, *Journal of Economic Theory* 22, 477-498.

Lee, Jongsub, Tao Li, and Donghwa Shin (2018), The Wisdom of Crowds and Information Cascades in FinTech: Evidence from Initial Coin Offerings, mimeo Warrington College of Business and Prineton University.

Kamenica, Emir and Matthew Gentzkow (2011), Bayesian Persuasion, *American Economic Review* 101, 2590–2615.

Kiyotaki, Nobuhiro and Randall Wright (1993), A Search-Theoretic Approach to Monetary Economics, *American Economic Review* 83, 63-77.

Kocherlakota, Narayana (1998), Money is Memory, *Journal of Economic Theory* 81, 232-251.

Lagos, Richard and Randall Wright (2005), A Unified Theory for Monetary Theory and Policy Analysis, *Journal of Political Economy* 113, 463-484.

Li, Jiasun and William Mann (2018), Initial Coin Offering and Platform Building, mimeo George Mason University and UCLA Anderson School of Management.

Gabaix, Xavier and Matteo Maggiori (2015), International Liquidity and Exchange Rate Dynamics, *Quarterly Journal of Economics* 130, 1369-1420.

Morris, Stephen and Hyun Song Shin (1998), Unique equilibrium in a model of self-fulfilling currency attacks, *American Economic Review*, 587-597.

Pagnotta, Emiliano S. and Andrea Buraschi (2018), An Equilibrium Valuation of Bitcoin and Decentralized Network Assets, mimeo Imperial College London.

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

Schilling, Linda and Harald Uhlig (2018), Some Simple Bitcoin Economics, mimeo University of Utrecht and University of Chicago.

Schneider, Jan (2009), A Rational Expectations Equilibrium with Informative Trading Volume, *Journal of Finance* 64, 2783-2805.

Wang, Jiang (1994), A Model of Competitive Stock Trading Volume, *Journal of Political Economy* 102, 127-168.

Yuan, Kathy (2005), Asymmetric Price Movements and Borrowing Constraints: A Rational Expectations Equilibrium Model of Crises, Contagion, and Confusion, *Journal of Finance* 60, 379-411.

Appendix Proofs of Propositions

A.1 Proof of Proposition 1

The first order conditions of household i's optimization problem in (2) respect to $C_i(i)$ and $C_j(i)$ at an interior point are:

$$C_i(i) \quad : \quad \frac{1-\eta_c}{C_i(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_i, \tag{10}$$

$$C_j(i) \quad : \quad \frac{\eta_c}{C_j(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_j, \tag{11}$$

where θ_i is the Lagrange multiplier for the budget constraint. Rewriting (11) as

$$\eta_c U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_j C_j(i).$$

Dividing equations (10) by this expression leads to $\frac{\eta_c}{1-\eta_c} = \frac{p_j C_j(i)}{p_i C_i(i)}$, which in a symmetric equilibrium implies $p_j C_j(i) = \frac{\eta_c}{1-\eta_c} p_i C_i(i)$. By substituting this equation back to the household's budget constraint in (2), we obtain:

$$C_i(i) = (1-\eta_c) e^{A_i}.$$

The market-clearing for the household's good requires that $C_i(i) + C_i(j) = e^{A_i}$, which implies that $C_i(j) = \eta_c e^{A_i}$.

The first order condition in equation (10) also gives the price of the good produced by household i. Since the household's budget constraint in (2) is entirely in nominal terms, the price system is only identified up to θ_i, the Lagrange multiplier. We therefore normalize θ_i to 1. It follows that:

$$p_i = \frac{1-\eta_c}{C_i(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = e^{\eta_c (A_j - A_i)}. \tag{12}$$

Furthermore, given equation (1), it follows since $C_i(i) = (1-\eta_c) e^{A_i}$ and $C_j(i) = \eta_c e^{A_j}$ that:

$$U\left(C_i(i), C_j(i); \mathcal{N}\right) = e^{(1-\eta_c)A_i} e^{\eta_c A_j} = p_i e^{A_i},$$

from substituting with the household's budget constraint at $t = 2$.

It then follows that, conditional on meeting another holder of the crypto currency, then the expected utility of investor i conditional on $\mathcal{I}_i$ and a successful match (given by the dummy M) is:

$$E\left[U\left(C_i\left(i\right), C_j\left(i\right); \mathcal{N}\right) \middle| \ \mathcal{I}_i, M\right] = e^{(1-\eta_c)A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \frac{\Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right)},$$

and, since the probability of meeting another holder of the crypto currency is $\Phi\left(\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)$, the expected utility of investor i is:

$$E\left[U\left(C_i\left(i\right), C_j\left(i\right); \mathcal{N}\right) \middle| \ \mathcal{I}_i\right] = e^{(1-\eta_c)A_i + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} E\left[e^{\eta_c A} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) \middle| \ \mathcal{I}_i\right].$$

Finally, the ex ante expected utility of a household before it learns its endowment A_i :

$$\begin{aligned}
U_0 &= E\left[\max_{X_i}\left\{E\left[U_i|\mathcal{I}_i\right] - P, 0\right\}\right] \\
&= E\left[e^{(1-\eta_c)A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) - P \mid A, \xi\right] \\
&= e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\varepsilon^{-1}} \Phi\left(\left(1 - \eta_c\right)\tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) - P\Phi\left(\frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) \\
&= u_0 - P\Phi\left(\frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right),
\end{aligned}$$

where u_0 is the utility benefit of entering the currency platform.

A.2 Proof of Proposition 2

When all households and miners observe A directly, there are no longer information frictions in the economy. From Proposition 1, the expected utility of household i at $t = 1$ who chooses to buy the currency is:

$$E\left[U_i|\mathcal{I}_i\right] = e^{(1-\eta_c)A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right),$$

Since the household with the critical productivity A^* must be indifferent to its purchase choice at the cutoff, it follows that $E\left[U_i|\mathcal{I}_i^*\right] - P = 0$, which implies:

$$e^{(1-\eta_c)A_i} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) = e^{-\frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1} - \eta_c A} P, \text{ with } A_i = A^* \tag{13}$$

which implies the benefit of joining the platform is offset by the cost of acquiring the currency.

Fixing the critical value A^* and price P, we see that the LHS of equation (13) is increasing in monotonically in A_i, since $1-\eta_c > 0$. This confirms the optimality of the cutoff strategy that households with $A_i \geq A^*$ acquire the currency, and households with $A_i < A^*$ not to join the platform. Since $A_i = A + \varepsilon_i$, it then follows that a fraction $\Phi\left(-\sqrt{\tau_\varepsilon}\,(A^* - A)\right)$ enter the platform, and a fraction $\Phi\left(\sqrt{\tau_\varepsilon}\,(A^* - A)\right)$ choose not to. As one can see, it is the integral over the idiosyncratic endowment of households ε_i that determines the fraction of households on the platform.

From the optimal supply of computing services by miner i on the platform (5), there exists a critical value ω^* :

$$\omega^* = -\log P - \log(1-\rho), \tag{14}$$

such that miners with productivity $\omega_i \geq \omega^*$ mine the currency. Thus, a fraction $\Phi\left(-\sqrt{\tau_e}\,(\omega^* - \xi)\right)$ mine the currency on the platform. Imposing market-clearing, it must be the case that

$$\Phi\left(-\sqrt{\tau_\varepsilon}\,(A^* - A)\right) = \Phi\left(-\sqrt{\tau_e}\,(\omega^* - \xi)\right).$$

Since the CDF of the normal distribution is montonically increasing, we can invert the above market-clearing conditions, and impose equation (14) to arrive at

$$\log P = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}\,(A - A^*) - \xi - \log(1-\rho). \tag{15}$$

By substituting for P in equation (13), we obtain an equation to determine the equilibrium cutoff $A^* = A^*(A, \xi)$:

$$e^{\left(1-\eta_c+\sqrt{\tau_\varepsilon/\tau_e}\right)A^*}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right) = e^{\left(\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\right)A - \xi - \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1} - \log(1-\rho)}. \tag{16}$$

We can rewrite equation (16) as:

$$e^{\left(1-\eta_c+\sqrt{\tau_\varepsilon/\tau_e}\right)s}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - \frac{s}{\tau_\varepsilon^{-1/2}}\right) = e^{-A-\xi-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho)}, \tag{17}$$

where $s = A^* - A$ determines the population that buys the currency. Notice that the LHS of equation (17) is log concave, since the CDF of the normal distribution is log concave and the exponential function is log-linear. Consequently, $\frac{d^2 \log LHS}{ds^2} < 0$.

Note that the LHS of equation (17) is independent of A. Direct algebra can also verify that the LHS is a quasiconcave bell curve of s, while the RHS is a horizontal line. Given that the LHS is quasiconcave in s, it achieves a maximum at $\hat{s}$ such that $\frac{d \log LHS}{ds}\big|_{s=\hat{s}} = 0$. Since the RHS of (17) is fixed, it follows that the LHS and RHS of equation (17) intersect generically twice, with once being a knife-edge case when the equilibrium s is $\hat{s}$. Therefore, there are generically two cutoff equilibria. It can occur, however, that the RHS of equation (17) is

above the LHS evaluated at $\hat{s}$, and then the cost of buying the currency always exceeds its value for the marginal household. From the RHS, this can occur if A or ξ is sufficiently small, and then no household buys the currency.

In what follows, let the high price equilibrium, corresponding to a lower cutoff threshold, for s be $\underline{s}$ and the low price equilibrium for s be $\bar{s}$, which correspond to cutoffs $\underline{A}^*$ and $\bar{A}^*$. If we increase A or ξ, then the RHS of equation (17) decreases, and this implies for the high price equilibrium that $\underline{s}$ decreases, while for the low price equilibrium $\bar{s}$ increases. Since the population that purchases currency, $\Phi\left(-\sqrt{\tau_\varepsilon}s\right)$, is strictly increasing in s, our comparative statistics for $-s$ consequently also apply to the population.

In addition, since $P = \exp\left(-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}s - \xi - \log\left(1-\rho\right)\right)$, it further follows that the currency price is increasing in A for the high price equilibrium $\underline{s}$, and is decreasing in A and ξ for the low price equilibrium $\bar{s}$. Since the developer's revenue from the ICO Π_D is $\rho\Phi\left(-\sqrt{\tau_\varepsilon}s\right)P$, it follows that:

$$\frac{d}{dA}\Pi_D = -\rho\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\frac{ds}{dA}\Phi\left(-\sqrt{\tau_\varepsilon}s\right)P\left(1+\sqrt{\tau_e}\frac{\phi\left(-\sqrt{\tau_\varepsilon}s\right)}{\Phi\left(-\sqrt{\tau_\varepsilon}s\right)}\right) > 0,$$

In the high price equilibrium, $\frac{ds}{dA} < 0$, and therefore the developer's revenue is increasing in A, while in the low price equilibrium, $\frac{ds}{dA} > 0$, and the developer's revenue is instead decreasing in A.

Finally, expressing the ex ante expected utility of a household before it learns its endowment A_i, U_0, as:

$$U_0 = u_0 - P\Phi\left(-\frac{s}{\tau_\varepsilon^{-1/2}}\right).$$

Then, given that:

$$\frac{ds}{dA} = -\frac{1}{\frac{d\log LHS}{ds}},$$

where:

$$\frac{d\log LHS}{ds} = 1-\eta_c+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\frac{1}{\tau_\varepsilon^{-1/2}}\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-\frac{s}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-\frac{s}{\tau_\varepsilon^{-1/2}}\right)},$$

it follows, with some manipulation, that:

$$\begin{aligned}\frac{dU_0}{dA} &= -\frac{ds}{dA}\left(\left(1-\eta_c+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)u_0 - \sqrt{\frac{\tau_\varepsilon}{\tau_e}}P\Phi\left(-\frac{s}{\tau_\varepsilon^{-1/2}}\right)\right)\\ &= -\frac{ds}{dA}\left(\left(1-\eta_c\right)u_0+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}U_0\right).\end{aligned}$$

Since $U_0 = E\left[\max_{X_i}\left\{E\left[U_i|\mathcal{I}_i\right]-P,0\right\}\right]$, it follows that $E\left[U_i|\mathcal{I}_i\right]-P \geq 0$, and therefore $u_0 \geq P\Phi\left(-\frac{s}{\tau_\varepsilon^{-1/2}}\right)$. Consequently, since $\frac{ds}{dA} < 0$ in the high price equilibrium:

$$\frac{dU_0}{dA} > 0,$$

while, since $\frac{ds}{dA} > 0$ in the low price equilibrium:

$$\frac{dU_0}{dA} > 0.$$

Uniqueness of the rational expectations equilibrium we have characterized follows from the cutoff strategies being the unique solution to the respective optimization problems of households and miners.

A.3 Proof of Proposition 3

Given our assumption about the sufficient statistic in cryptocurrency price, each household's posterior about A is Gaussian $A\,|\mathcal{I}_i \sim \mathcal{N}\left(\hat{A}_i, \hat{\tau}_A^{-1}\right)$ with conditional mean and variance:

$$\begin{aligned}
\hat{A}_i &= \bar{A} + \tau_A^{-1}\left[\begin{array}{ccc} 1 & 1 & 1 \end{array}\right]\left[\begin{array}{ccc} \tau_A^{-1}+\tau_v^{-1} & \tau_A^{-1} & \tau_A^{-1} \\ \tau_A^{-1} & \tau_A^{-1}+z_\xi^{-2}\tau_\xi^{-1} & \tau_A^{-1} \\ \tau_A^{-1} & \tau_A^{-1} & \tau_A^{-1}+\tau_\varepsilon^{-1} \end{array}\right]^{-1}\left[\begin{array}{c} v-\bar{A} \\ z-\bar{A} \\ A_i-\bar{A} \end{array}\right] \\
&= \hat{\tau}_A^{-1}\left(\tau_A\bar{A} + \tau_v v + z_\xi^2\tau_\xi z + \tau_\varepsilon A_i\right), \\
\hat{\tau}_A &= \tau_A + \tau_v + z_\xi^2\tau_\xi + \tau_\varepsilon.
\end{aligned}$$

Note that the conditional estimate of $\hat{A}_i$ of household i is increasing in its own productivity A_i. This completes our characterization of learning by households and the developer.

By substituting the expressions for K_i and l_i into the utility of household i given in Proposition 1, we obtain:

$$\begin{aligned}
E\left[U_i|\mathcal{I}_i\right] &= e^{(1-\eta_c)A_i+\eta_c A^*+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} E\left[e^{\eta_c(A-A^*)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)\middle|\ \mathcal{I}_i\right] \\
&= e^{(1-\eta_c)A_i+\eta_c\hat{A}_i+\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2} + \frac{\hat{A}_i+\eta_c\hat{\tau}_A^{-1}-A^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right).
\end{aligned}$$

Since the posterior for $A - A^*$ of household i is conditionally Gaussian, it follows that the expectations in the expressions above are functions of the first two conditional moments $\hat{A}_i - A^*$ and $\hat{\tau}_A$. Notice that:

$$\frac{d\log E\left[U_i|\mathcal{I}_i\right]}{dA_i} = 1 - \frac{\tau_A+\tau_v+z_\xi^2\tau_\xi}{\tau_A+\tau_v+z_\xi^2\tau_\xi+\tau_\varepsilon}\eta_c + \frac{\frac{1}{\tau_\varepsilon^{-1/2}}\frac{\tau_\varepsilon}{\hat{\tau}_A}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\frac{\phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\hat{A}_i+\eta_c\hat{\tau}_A^{-1}-A^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)}{\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\hat{A}_i+\eta_c\hat{\tau}_A^{-1}-A^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)} \geq 0,$$

confirming the optimality of the cutoff strategy for household i.

Since the household with the critical productivity A^* must be indifferent to its currency choice at the cutoff, it follows that $U_i - P = 0$, which implies:

$$e^{(1-\eta_c)A_i+\eta_c\hat{A}_i+\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\hat{A}_i+\eta_c\hat{\tau}_A^{-1}-A^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)=P \quad \text{with} \quad A_i=A^*. \tag{18}$$

Those with the LHS above P purchase the currency, and those below choose to refrain. This equation does not depend on the unobserved A or the supply shock ξ. As a result, $A^* = A^*(\log P, v)$.

It then follows from market-clearing that:

$$\Phi\left(-\sqrt{\tau_\varepsilon}\left(A^*-A\right)\right)=\Phi\left(-\sqrt{\tau_e}\left(\omega^*-\xi\right)\right).$$

Since the CDF of the normal distribution is montonically increasing, we can invert this market-clearing condition, and impose equation (14) for the minor's critical level ω^* to arrive at:

$$\log P=\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A-A^*\right)-\xi-\log\left(1-\rho\right),$$

from which follows that:

$$z=\sqrt{\frac{\tau_e}{\tau_\varepsilon}}\left(\log P+\log\left(1-\rho\right)+\sqrt{\frac{\tau_e}{\tau_\varepsilon}}\bar{\xi}\right)+A^*=A-\sqrt{\frac{\tau_e}{\tau_\varepsilon}}\left(\xi-\bar{\xi}\right),$$

and therefore $z_\xi = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}$. This confirms our conjecture for the sufficient statistic of the currency price and that learning by households is indeed a linear updating rule.

As a consequence, the conditional estimate of household i is:

$$\begin{aligned}\hat{A}_i &= \hat{\tau}_A^{-1}\left(\tau_A\bar{A}+\tau_v v+\frac{\tau_\varepsilon}{\tau_e}\tau_\xi z+\tau_\varepsilon A_i\right),\\ \hat{\tau}_A &= \tau_A+\tau_v+\frac{\tau_\varepsilon}{\tau_e}\tau_\xi+\tau_\varepsilon.\end{aligned}$$

Substituting for prices, and simplifying A^* terms, we can express equation (18) as:

$$e^{\left(1-\eta_c\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)A^*+\eta_c\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}\hat{A}}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}\left(\hat{A}-A^*\right)+\eta_c\hat{\tau}_A^{-1}}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)=e^{\sqrt{\frac{\tau_\varepsilon}{\tau_e}}z-\bar{\xi}-\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)-\log(1-\rho)}, \tag{19}$$

substituting for $\hat{A}_i^*$, the posterior belief when $A_i = A^*$:

$$\hat{A}_i^*=\hat{\tau}_A^{-1}\left(\tilde{\tau}_{A,c}\hat{A}+\frac{\tau_\varepsilon\tau_\xi}{\tau_e}z+\tau_\varepsilon A^*\right),$$

and $A \mid (z,v) \sim \mathcal{N}\left(\hat{A}, \tilde{\tau}_{A,c}^{-1}\right)$ is the posterior belief about A given only public information:

$$\begin{aligned}\hat{A} &= \hat{\tau}_{A,c}^{-1}\left(\tau_A \bar{A} + \tau_v v + \frac{\tau_\varepsilon}{\tau_e}\tau_\xi z\right), \\ \hat{\tau}_{A,c} &= \tau_A + \tau_v + \frac{\tau_\varepsilon}{\tau_e}\tau_\xi.\end{aligned}$$

Letting $s = A^* - \hat{A}$, we can consequently rewrite the above as:

$$e^{\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}\right)s}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\eta_c\hat{\tau}_A^{-1}-\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}s}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right) = e^{\left(\frac{\tau_A+\tau_v}{\hat{\tau}_{A,c}}\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\frac{\frac{\tau_\varepsilon}{\tau_e}\tau_\xi}{\hat{\tau}_{A,c}}\right)z-\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)\frac{\tau_v}{\hat{\tau}_{A,c}}v-\bar{\xi}-\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)\frac{\tau_A}{\hat{\tau}_{A,c}}\bar{A}-\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau\right.} \tag{20}$$

Similar arguments to those in the proof of Proposition 2 then establish that the LHS is bell-shaped in s, and independent of z and v, while the RHS is log-linear in z and v. Since the RHS of equation (20) is fixed as a horizontal line, while the LHS is bell-shaped, it follows that generically there are either two or no cutoff equilibria in the economy. Furthermore, since the RHS is linear in z and v, it follows an equilibrium fails to exist when z is sufficiently low (high) when $\tau_A + \tau_v \geq (<) \sqrt{\frac{\tau_\varepsilon}{\tau_e}}\tau_\xi$ or v is sufficiently low, and the horizontal line is above the maximum value of the bell-shaped curve of the LHS.

Note now that, since the RHS of equation (19) is fixed with respect to v, while the RHS is increasing in v through $\hat{A}$. It follows from the Implicit Function Theorem that:

$$\frac{dA^*}{d\varepsilon_V} = -\frac{\tau_v^{1/2}}{\hat{\tau}_A}\frac{\eta_c + \frac{\frac{1}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}(\hat{A}-A^*)+\eta_c\hat{\tau}_A^{-1}}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)/\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}(\hat{A}-A^*)+\eta_c\hat{\tau}_A^{-1}}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)}{1-\eta_c\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\frac{\frac{1}{\tau_\varepsilon^{-1/2}}\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}(\hat{A}-A^*)+\eta_c\hat{\tau}_A^{-1}}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)/\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}(\hat{A}-A^*)+\eta_c\hat{\tau}_A^{-1}}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right)}.$$

Since the RHS is hump-shaped in A^*, it follows that the denominator is positive in the high price equilibrium, and negative in the low price equilibrium. It then follows that A^* shifts down in the high price equilibrium after a positive shock to ε_V, and shifts up in the low price equilibrium. Since this noise impacts A^* and not A or ξ, it follows that the currency price and population that buy the currency increases in the high price equilibrium, and decreases in the low price equilibrium.

Uniqueness of the rational expectations equilibrium we have characterized then follows from the cutoff strategies being the unique solutions to the respective optimization problems of households and miners. As all households share a common posterior about A after observing the token price, their private beliefs about A and their private type A_j are perfectly

positively correlated, confirming the optimality of their cutoff strategy in their private type. Miners, regardless of their beliefs about A, will follow a cutoff strategy in deciding whether to mine. Given that households and miners follow cutoff strategies, the functional form for the token price follows from market-clearing, and the posterior beliefs of households are then given as conjectured.

A.4 Proof of Proposition 4

To understand the value of providing public information to the developer, we first characterize the shape of its payoff profile in each of the three possible equilibrium regions, high price, low price, and nonexistant, realization-by-realization for (z, v). As we will characterize this realization-by-realization, we do not, for the moment, need to take a stand on the distribution of this common prior belief of households $A \mid z, v$, other than it is normal $\mathcal{N}\left(\hat{A}, \hat{\tau}_{A,c}\right)$, where $\hat{\tau}_{A,c} = \tau_A + \tau_v + \frac{\tau_\varepsilon}{\tau_e}\tau_\xi$, or on the prior belief of the developer and households about which equilibrium will realize (high or low) when both exist.

First, we consider the case when there is an equilibrium, high or low price. The expected profit of the developer, conditional on the realization of the public signals z and v, is then:

$$E\left[\Pi_D \mid z, v\right] = \frac{\rho}{1-\rho} e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}b - \hat{\xi}} \Phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right),$$

where we conveniently define $b = A^* - \hat{A}$, and we recognize that $z = A - \sqrt{\frac{\tau_e}{\tau_\varepsilon}}\left(\xi - \bar{\xi}\right) = \hat{A} - \sqrt{\frac{\tau_e}{\tau_\varepsilon}}\left(\hat{\xi} - \bar{\xi}\right)$. By differentiating this expression twice with respect to $\hat{A}$ as it acts through A^*, we find that:

$$\begin{aligned}
\frac{\frac{d^2 E[\Pi_D \mid z,v]}{d\hat{A}^2}}{\frac{\rho}{1-\rho}e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}b-\hat{\xi}}} &= \left[\frac{\tau_\varepsilon}{\tau_e}\Phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right) + \sqrt{\tau_\varepsilon}\frac{2\sqrt{\frac{\tau_\varepsilon}{\tau_e}} + \frac{\tau_\varepsilon b}{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)\right]\left(\frac{db}{d\hat{A}}\right)^2 \\
&\quad - \left[\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\Phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right) + \frac{\sqrt{\tau_\varepsilon}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)\right]\frac{d^2 b}{d\hat{A}^2},
\end{aligned}$$

where, by applying the Implicit Function Theorem, we have:

$$e^{\hat{A}+\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)b-\eta_c\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}b+\frac{1}{2}\eta_c^2\hat{\tau}_A^{-1}} - e^{-\hat{\xi}-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho)} = 0,$$

from Proposition 3:

$$\begin{aligned}\frac{db}{d\hat{A}} &= -\frac{1}{1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}-\frac{\sqrt{\tau_\varepsilon}\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}\frac{\phi(x)}{\Phi(x)}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}},\\ \frac{d^2b}{d\hat{A}^2} &= -\frac{\tau_\varepsilon\left(\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}\right)^2}{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}\left(\frac{db}{d\hat{A}}\right)^3\frac{\phi(x)}{\Phi(x)}\left(x+\frac{\phi(x)}{\Phi(x)}\right),\end{aligned}$$

where $x=\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{-\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}b+\eta_c\hat{\tau}_A^{-1}}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}$, $\hat{\tau}_A=\hat{\tau}_{A,c}+\tau_\varepsilon$, and $x+\frac{\phi(x)}{\Phi(x)}\geq 0$.

Let us first assess the curvature of the profit function in the low price equilibrium. Since $\frac{db}{d\hat{A}}>0$ in the low price equilibrium, by similar arguments for $\frac{ds}{dA}$ in Proposition 2, $\frac{d^2b}{d\hat{A}^2}\leq 0$, and we focus on the coefficient of the $\left(\frac{db}{d\hat{A}}\right)^2$ terms. Notice the coefficient on the $\left(\frac{db}{d\hat{A}}\right)^2$ term tends to $\frac{\tau_\varepsilon}{\tau_e}$ as b becomes arbitrarily negative, and 0 as b becomes arbitrarily positive. It remains then to check its critical values, $b^*=-\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}\right)\sqrt{\frac{1}{\tau_\varepsilon\tau_e}}\pm\sqrt{\frac{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}{\tau_\varepsilon}}$. At the larger root, the coefficient is unambiguously positive, while at the negative root, we require that:

$$\tau_e^{-1/2}\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}+\left(1-\sqrt{\frac{\tau_e}{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)\frac{\phi\left(1+\sqrt{\frac{1}{\tau_e}\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}\right)}\right)}{\Phi\left(1+\sqrt{\frac{1}{\tau_e}\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}\right)}\right)}\geq 0$$

for the first term to be positive. It is sufficient that $\sqrt{\frac{\tau_e}{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}<1$ for $E\left[\Pi_D\mid z,v\right]$ to be convex if $\hat{A}$, which is satisfied for $\tau_e<1$.[23] Consequently, it is possible for the developer's profit to be strictly convex in the low price equilibrium for τ_e sufficiently small.

We now turn our analysis to the high price equilibrium, in which $\frac{d^2b}{dA^2}\geq 0$. We now express the second derivative of the developer's expected profit with respect to $\hat{A}$ as:

$$\begin{aligned}\frac{\frac{d^2E[\Pi_D\mid z,v]}{d\hat{A}^2}}{\rho P\left(\frac{db}{d\hat{A}}\right)^2} &= \frac{\tau_\varepsilon}{\tau_e}\Phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)+\frac{\sqrt{\tau_\varepsilon}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\left(2\sqrt{\frac{\tau_\varepsilon}{\tau_e}}+\frac{\tau_\varepsilon b}{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}\right)\phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)\\ &\quad -\frac{\tau_\varepsilon\left(\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}\right)^2}{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}\frac{\frac{\phi(x)}{\Phi(x)}\left(x+\frac{\phi(x)}{\Phi(x)}\right)\left(\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\Phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)+\frac{\sqrt{\tau_\varepsilon}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\phi\left(\frac{-\sqrt{\tau_\varepsilon}b}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}}\right)\right)}{1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}-\frac{\sqrt{\tau_\varepsilon}\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}\frac{\phi(x)}{\Phi(x)}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}}.\end{aligned}$$

[23] The condition $\frac{\hat{\tau}_A}{\hat{\tau}_{A,c}}>\tau_e$ actually suggests the condition is satisfied when the informational advantage of households over the common belief is sufficiently high.

As $b \to -\infty$, it is straightforward to verify that $\frac{d^2E[\Pi_D \mid z,v]}{d\hat{A}^2} \to \rho\frac{\tau_\varepsilon}{\tau_e}P = \infty$. In contrast, as b approaches its critical value, b_{crit}, such that $1 + \sqrt{\frac{\tau_\varepsilon}{\tau_e}} - \eta_c\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A} = \frac{\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}}{\frac{\tau_\varepsilon^{-1/2}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\frac{\phi(x)}{\Phi(x)}}$, then $\frac{d^2E[\Pi_D \mid z,v]}{dA^{*2}} \to -\infty$.[24]

We now notice that the sum of the first two terms of $\left[\rho P\left(\frac{db}{d\hat{A}}\right)^2\right]^{-1}\frac{d^2E[\Pi_D \mid z,v]}{dA^{*2}}$ are bounded from above, while the third term is monotonically decreasing in b (as $b = \frac{\hat{\tau}_A}{\hat{\tau}_{A,c}}\eta_c\left(\tau_\varepsilon^{-1} + \hat{\tau}_A^{-1}\right) - x\frac{\hat{\tau}_A}{\hat{\tau}_{A,c}}\sqrt{\tau_\varepsilon^{-1} + \hat{\tau}_A^{-1}}$) until it is arbitrarily negative. Consequently, there exists a value b^{**} such that $\frac{d^2E[\Pi_D \mid z,v]}{d\hat{A}^2} < 0$ for $b \in (b^{**}, b_{crit})$, while, for b sufficiently negative, $\frac{d^2E[\Pi_D \mid z,v]}{d\hat{A}^2} > 0$. Then, $\frac{d^2E[\Pi_D \mid z,v]}{d\hat{A}^2}$ has a region for which it is strictly concave for b sufficiently large, and approaching b_{crit}, and strictly convex for b sufficiently small wherever a cutoff equilibrium exists. While difficult to show, it is actually the case that these regions are connected, and the turning point unique. It is therefore impossible, regardless of the parameters, for the payoff profile of the developer to be strictly convex in the high price equilibrium.

The above computaitons have established, when an equilibrium exists, that while it is possible for the payoff to the developer to be strictly convex in the low price equilibrium, it necessarily has regions of concavity for low realizations of (z, v) and convexity for high realizations of (z, v). regardless of the underlying parameters. This non-convexity in the high price equilibrium occurs because of the jump in the developer's profits from zero with nonexistence to a positive number when a high price equilibrium begins to exist.

Finally, when an equilibrium does not exist, then the developer's profit is flat at zero when (z, v) are sufficiently low.

Tying together the three pieces of possible outcomes, we see that the developer's profit is zero for sufficiently low realizations of (z, v), and then it jumps up as a step function when an equilibrium exists. As (z, v) continues to increase, the payoff profile is necessarily concave and then convex in the high price equilibrium, although it can be strictly convex in the low price equilibrium. This fully characterizes the developer's profit for any (z, v) pair.

As we can see, as a result of the nonexistence of an equilibrium, the developer's profit displays nonconvexities for low realizations of (z, v) at the critical boundary at which equilibria begin to exists. This is reflected in the shape of the payoff profile in the high price equilibrium, which is necessarily has a region of concavity close to this critical boundary.

From the Bayesian Persuasion analysis of Aumann and Maschler (1995) and Kamenica and Gentzklow (2015), we can therefore conclude that, since Π_D is neither strictly concave nor strictly convex across all realizations of (z, v), it follows that full disclosure is generically

[24] The developer's revenue actually collapses to zero at the critical point where $\frac{d^2E[\Pi_D \mid P]}{dA^{*2}} \to -\infty$.

not optimal, and the optimal disclosure policy will depend on households' posterior about A given public information (the prior from the developer's perspective), and the developer's beliefs about the probability of coordination between the high and low price equilibrium when both exist.

A.5 Proof of Proposition 5

We first analyze the decision of the developer to choose the miner fee $e^{-\omega^*}$. By choosing ω^*, the developer determines the marginal miner that provides mining services to the platform. Note that the publicly observed stock price S conveys information about A. Suppose that S is an invertible function of the marginal investor's signal s^*. Then, the posterior of the developer and miners, who observe only the public signal S, is Gaussian $\mathcal{N}\left(\hat{A}, \hat{\tau}_A\right)$, where:

$$\begin{aligned}\hat{A} &= \frac{\tau_A}{\tau_A + \tau_s\tau_\varphi^{-1}}\bar{A} + \frac{\tau_s\tau_\varphi^{-1}}{\tau_A + \tau_s\tau_\varphi^{-1}}s^*, \\ \hat{\tau}_{A,D} &= \tau_A + \tau_s\tau_\varphi^{-1},\end{aligned}$$

which we will confirm in the sequel.

Household i, given its information set $\{A_i, s^*, \omega^*, \xi\}$, form its expectations about the platform demand fundamental, A, when submitting its bid schedule to the developer. From its optimization program, this bid schedule will be a step function in which its demand is 1 if the membership price is equal to or below a reservation price P_i, and 0 otherwise.

$$\begin{aligned}P_i &= e^{(1-\eta_c)A_i + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} E\left[e^{\eta_c A_j}\middle|\ \mathcal{I}_i, A_j \geq A^* = A + \sqrt{\frac{\tau_e}{\tau_\varepsilon}}(\omega^* - \xi)\right] \\ &= e^{(1-\eta_c)A_i + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} E\left[e^{\eta_c A + \eta_c\varepsilon_j}\middle|\ \mathcal{I}_i, \varepsilon_j \geq \sqrt{\tau_e}(\omega^* - \xi)\right] \\ &= e^{(1-\eta_c)A_i + \eta_c\hat{A}_i + \frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1} + \tau_\varepsilon^{-1}\right)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{\sqrt{\tau_e}(\xi - \omega^*)}{\tau_\varepsilon^{-1/2}}\right).\end{aligned}$$

Since household i observes ω^*, and knows ξ, it knows exactly the fraction of the population that will enter the platform, the second term in the final expression, but still must form expectations about the average productivity of this population, reflected in the $\hat{A}_i$ term. Consequently, the demand schedule of household i is $X_i = \mathbf{1}\{P \leq P_i\}$.

As the developer observes the demand schedules, it will choose the membership price P to equal the reservation price of the marginal household in the platform, A^*. It then follows that we can express the membership price as:

$$P = e^{(1-\eta_c)A^* + \eta_c\hat{A}_i^* + \frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1} + \tau_\varepsilon^{-1}\right)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right),$$

Since ω^*, which is set by the developer, and ξ are known to households, they do not need to form expectations about the size of the membership platform. Given that:

$$\hat{A}_i^* = \frac{\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\hat{A} + \frac{\tau_\varepsilon}{\hat{\tau}_{A,D}+\tau_\varepsilon}A^*,$$

it follows, since, by market-clearing, $A^* = A + \sqrt{\frac{\tau_e}{\tau_\varepsilon}}(\omega^* - \xi)$, that:

$$P = e^{A^* + \frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\left(\hat{A}-A^*\right) + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{\sqrt{\tau_e}(\xi-\omega^*)}{\tau_\varepsilon^{-1/2}}\right).$$

Since ξ is known, let $w = \sqrt{\tau_e}(\xi - \omega^*)$, and recognizing that:

$$\begin{aligned} & E\left[e^{A^* + \frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\left(\hat{A}-A^*\right) + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{w}{\tau_\varepsilon^{-1/2}}\right) \mid s^*\right] \\ = \; & e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w + \frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1} + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{w}{\tau_\varepsilon^{-1/2}}\right), \end{aligned}$$

we can then express the developer's program as:

$$\Pi_D^{IPO} = \sup_w \left(\frac{e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w + \frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1} + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}} - e^{\tau_e^{-1/2}w-\xi} \right)\Phi(w). \tag{21}$$

It follows from the developer's program, the FONC can be expressed as:

$$\begin{aligned} 0 \; = \; & \frac{1}{\tau_\varepsilon^{-1/2}}e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w + \frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1} + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}\phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{w}{\tau_\varepsilon^{-1/2}}\right)\Phi(w) \\ & - \left(1 - \frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}\frac{e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w + \frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1} + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}}\Phi(w) \\ & -\tau_e^{-1/2}e^{\tau_e^{-1/2}w-\xi}\Phi(w) + \left(\frac{e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w + \frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1} + \frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} + \frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}} - e^{\tau_e^{-1/2}w-\xi} \right. \end{aligned}$$

From the FONC, it follows that the condition is not sufficient since $w = -\infty$ (no households enter) is a critical point. As $w \to -\infty$, the expected profit is 0, while as $w \to \infty$, it becomes arbitrarily negative as the cost of maintaining the platform rises exponentially while the revenue falls. While difficult to show formally, the developer's program has an interior maximum. This suggests, by applying the Implicit Function Theorem to the FONC at this interior optimum, that $\frac{dw}{d\hat{A}} \geq 0$, since, with some manipulation:

$$\frac{dFONC}{d\hat{A}} = \tau_e^{-1/2}e^{\tau_e^{-1/2}w-\xi}\Phi(w) + e^{\tau_e^{-1/2}w-\xi}\phi(w) > 0,$$

and $\frac{dFONC}{dw} < 0$ by the concavity of the developer's program at the interior optimum.

From the perspective of investor j, their posterior belief about the demand fundamental is Gaussian $\mathcal{N}\left(\hat{A}_j, \hat{\tau}_{A,I}\right)$, where:

$$\begin{aligned} \hat{A}_j &= \frac{\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_s}\hat{A} + \frac{\tau_s}{\hat{\tau}_{A,D}+\tau_s}s_j, \\ \hat{\tau}_{A,I} &= \hat{\tau}_{A,D}+\tau_s. \end{aligned}$$

Their expected profit from the stock is:

$$E\left[\Pi_D^{IPO} \mid s^*, s_j\right] = \left(\frac{e^{\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\left(\hat{A}_j-\hat{A}-\tau_\varepsilon^{-1/2}w\right)+\hat{A}+\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}+\frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}} - e^{\tau_e^{-1/2}w}$$

which we can express as:

$$E\left[\Pi_D^{IPO} \mid s^*, s_j\right] = \left(\frac{e^{\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\left(\frac{\tau_s}{\hat{\tau}_{A,D}+\tau_s}\left(s_j-\hat{A}\right)-\tau_\varepsilon^{-1/2}w\right)+\hat{A}+\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}+\frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}}$$

Differentiating this expected dividend from the stock with respect to the private signal s_j, we find that:

$$\begin{aligned} \frac{dE\left[\Pi_D^{IPO} \mid s^*, s_j\right]}{ds_j} &= \frac{\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\frac{\tau_s}{\hat{\tau}_{A,D}+\tau_s}e^{\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\left(\frac{\tau_s}{\hat{\tau}_{A,D}+\tau_s}\left(s_j-\hat{A}\right)-\tau_\varepsilon^{-1/2}w\right)+\hat{A}+\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}} \\ &\geq 0, \end{aligned}$$

The expected dividend is, consequently, monotonic in investor $j's$ signal, since $\frac{dE\left[\Pi_D^{IPO} \mid s^*, s_j\right]}{ds_j} \geq 0$. This verifies the optimality of the conjectured cutoff strategy for investors. Consequently, it is optimal for investors to follow a cutoff strategy, and buy if $s_j \geq s^*$, and short-sell if $s_j < s^*$. Market-clearing then implies that:

$$s^* = A + \sqrt{\frac{\tau_\varphi}{\tau_s}}\varphi,$$

as conjectured. The stock price is then given by $S = \left[\Pi_D^{IPO} \mid s^*, s_j = s^*\right]$, so that:

$$S = \left(\frac{e^{\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\left(\frac{\tau_s}{\hat{\tau}_{A,D}+\tau_s}\left(s^*-\hat{A}\right)-\tau_\varepsilon^{-1/2}w\right)+\hat{A}+\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}+\frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}} - e^{\tau_e^{-1/2}w-\xi}\right)\Phi$$

which, substituting for s^* and $\hat{A} = \frac{\tau_A}{\hat{\tau}_{A,D}}\bar{A} + \frac{\tau_s\tau_\varphi^{-1}}{\hat{\tau}_{A,D}}s^*$, can be expressed as:

$$S = \left(\frac{e^{\bar{A}+\left(\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\frac{\tau_s}{\hat{\tau}_{A,D}}\frac{\tau_A}{\hat{\tau}_{A,D}}+\frac{\tau_s\tau_\varphi^{-1}}{\hat{\tau}_{A,D}}\right)\left(A-\bar{A}+\sqrt{\frac{\tau_\varphi}{\tau_s}}\varphi\right)-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\tau_\varepsilon^{-1/2}w}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1} e^{-\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}-\frac{1}{2}\eta_c^2\left(\left(\tau_A+\tau_s\tau_\varphi^{-1}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}} - e^{\tau_e^{-1/2}w-\xi} \right) \Phi(w),$$

Finally, to establish that S is monotonically increasing in s^*, we see that:

$$\frac{dS}{ds^*} = \frac{\left(\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\frac{\tau_s}{\hat{\tau}_{A,D}}\frac{\tau_A}{\hat{\tau}_{A,D}}+\frac{\tau_s\tau_\varphi^{-1}}{\hat{\tau}_{A,D}}\right) e^{\bar{A}+\left(\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\frac{\tau_s}{\hat{\tau}_{A,D}}\frac{\tau_A}{\hat{\tau}_{A,D}}+\frac{\tau_s\tau_\varphi^{-1}}{\hat{\tau}_{A,D}}\right)\left(s^*-\bar{A}\right)-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\tau_\varepsilon^{-1/2}w}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1} e^{-\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}-\frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}} \Phi(w) \geq 0,$$

and consequently the sufficient statistic s^* is invertible from observing the stock price, as conjectured.

A.6 Proof of Proposition 6

We consider the developer's expected profit from the IPO based on the common beliefs of households. Differentiating equation (21) with respect to the conditional estimate $\hat{A}$ at its optimum twice, and invoking the envelope condition, we find that:

$$\begin{aligned}
\frac{d^2\Pi_D^{IPO}}{d\bar{A}^2} &= \frac{e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w+\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1}+\frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}}\Phi(w) \\
&\quad + \left(\tau_e^{-1/2}+\frac{\phi(w)}{\Phi(w)}\right)e^{\tau_e^{-1/2}w-\xi}\Phi(w)\frac{dw}{d\hat{A}} \\
&> 0,
\end{aligned}$$

since $\frac{dw}{d\hat{A}} \geq 0$ from the proof of Proposition 5.

Consequently, the developer's expected profit is strictly convex in the conditional estimate $\hat{A}$ state-by-state for any posterior precision $\hat{\tau}_{A,D}$, and therefore under any normal prior.

From the Bayesian Persuasion analysis of Aumann and Maschler (1995) and Kamenica and Gentzklow (2015), we can therefore conclude that, since Π_D^{IPO} is strictly convex in the message received by households under any normal prior, full disclosure is optimal for the developer.