A Model of Cryptocurrencies*

Michael Sockin† Wei Xiong‡

March 2018

Abstract

The surge in the number of initial coin offerings (ICOs) in recent years has led to both excitement about cryptocurrencies as a new funding model for innovations in the digital age, and to anxiety about a potential bubble. This paper develops a model to address several basic questions: What determines the fundamental value of a cryptocurrency? How would market trading interact with its fundamentals in an uncertain and opaque environment? 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. When the transaction demand for the platform is unobservable, the trading price and volume of the cryptocurrency serve as important channels for not only aggregating private information about its fundamental, but also facilitating coordination on a certain equilibrium.

*PRELIMINARY DRAFT. We thank An Yan for a comment that led to this paper.
†University of Texas, Austin. Email: Michael.Sockin@mccombs.utexas.edu.
‡Princeton University and NBER. Email: wxiong@princeton.edu.

In 2015-2017, over 2000 initial coin offerings (ICOs) emerged to raise over \$4 billion from the public, exceeding 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 successes led to great excitements about cryptocurrencies as a new funding model for innovations in the upcoming digital age. Rampant speculation and volatility in the trading of many cryptocurrencies, however, have also created enormous anxiety about cryptocurrencies as a potential bubble. The failure of the DAO only a few months after its ICO raising \$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 and South Korea banned cryptocurrencies at the end of 2017, even though other countries such as Switzerland and Singapore remain amenable to them.

In order to properly assess the potential benefits and risks brought by cryptocurrencies and establish a suitable regulatory framework for ICOs, it is important to understand several basic questions about the technology: What is a cryptocurrency? Is it a medium for transaction, a commodity, or a security? Depending on how we classify this key characteristic, we may adopt different valuation models and assign entirely different valuations and risk attributes to a cryptocurrency. The ample uncertainty and opacity associated with many of the ICOs, together with the typically observed frenzied trading of cryptocurrencies after their ICOs, raise further questions regarding whether such trading serves any socially meaningful role, and whether the trading price and volume may affect the underlying behavior of the cryptocurrencies.

In this paper, we develop a model to address some of these questions. In our model, a cryptocurrency serves as the 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. The households face difficulty in making such transactions outside the platform as a result of severe search frictions. The value of the platform, consequently, lies with 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 households are randomly matched, they can trade their goods with each other only if they both belong to the platform. Consequently, each household's desire to join the platform grows with the chance of meeting other households in the platform, and in the size of their endowments.

The cryptocurrency serves dual roles in the platform, 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. These dual roles make ICOs in sharp contrast to the traditional project financing mechanisms, such as IPOs and VC financing, which usually separate investors from business customers. As a result of these dual roles, the trading price and volume of the cryptocurrency not only provide financing of the cryptocurrency, but also directly impact the business operations of the platform.

To highlight these dual roles, we construct a model with two periods. In the first period, a pool of households with random endowment shocks 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, the households in 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 own endowment, which determines its own need to transact goods on the platform, and the average endowments of other households, which determine their transaction needs. We show that each household optimally adopts a cutoff strategy to purchase the cryptocurrency only if its endowment is higher than an equilibrium threshold, while the equilibrium cryptocurrency price is jointly determined by the common endowment of all households, and a supply shock reflecting the average computing cost for miners in providing accounting services to complete the transactions of households at the second date.

We analyze two settings, differing in whether the households' aggregate goods endowment is observable, which captures the demand fundamental for the platform. In the first setting, where the platform fundamental is publicly observable, there exist either two or no cutoff equilibria. When there are two equilibria, they exhibit opposing behavior. One of the equilibria 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 complementarity among the households' trading needs—if more households join the platform by choosing a lower cutoff strategy, they all benefit more from trading goods in the platform, and are therefore willing to pay a high cryptocurrency price. On the other hand, if each household chooses a higher cutoff strategy, there will be less households in the platform, making the platform less desirable, and lowering the price of the cryptocurrency. The presence of these 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 absence of a sovereign to provide guidance and support the platform, cryptocurrencies are vulnerable to these large price swings, and large investors may act as cryptocurrency whales to help coordinate participant expectations.

This problem worsens in our second setting, in which the platform fundamentals are not publicly observable based on realistic considerations. In this setting, each household needs to use its own endowment and the publicly observed trading price and volume of the cryptocurrency as noisy signals to infer the value of the aggregate household demand for the platform. Despite the highly non-linear equilibrium cryptocurrency price and the complexity involved in constructing each household's learning and in aggregating their cryptocurrency demands, we manage to construct a tractable log-linear noisy rational expectations equilibrium for the cryptocurrency market. In the equilibrium, each household again uses 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, 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 coordination on the high or low price equilibrium. As the high and low price equilibria have very disparate behavior, the currency price and equilibrium cutoff also have opposing reactions to news in these two sources of public information, which makes it difficult for outsiders to diagnose the health of the currency based on the price alone.

Our work contributes to the emerging literature on cryptocurrencies and ICOs. 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 it aggregates useful information for the developer about its product. 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, highlight the importance of scale in deterring double-spending by buyers and of alternative mining methods, such as Proof of Stake (PoS) to Proof of Work (PoW) in reducing inefficienct settlement delay and transaction fees. Cong and He (2017) investigate the tradeoff of smart contracts in overcoming adverse selection while also facilitating oligopolic 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. In contrast, our analysis attempts to understand what fundamentals determine the price and success of an ICO, 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 (1985), 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. 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 money represents a security in our setting, in which the shareholders are also the customers, is conducive to the study of infantile currencies and, consequently, ICOs.

Our work also adds to the literature related to 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 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. While Goldstein, Ozdenoren, and Yuan (2013) also features multiple equilibria, multiplicity in their setting arises from the self-fulfilling nature of trading on investment decisions, while in our setting it occurs because the benefits of participating in the cryptocurrency are endogenous to the size of its membership.

Our paper also contributes to the literature that explores the asset pricing implications of strategic complementarity. Plantin (2009) demonstrates that holders of privately placed securities must offer a "coordination premium" when the future liquidity of the market relies on the participation of future less-informed investors, while Malherbe (2014) illustrates that equilibria multiplicity can arise because firm cash hoarding endogenously determines the severity of adverse selection in the future spot market for credit. Asriyan, Fuchs, and Green (2017) show how endogenous liquidity stemming from issues of adverse selection can give rise to multiple equilibria in a dynamic setting, and this can generate nonfundamental price volatility from sentiment shocks. In our setting, multiplicity arises because the decision to purchase the cryptocurrency, which can be viewed as a security, is intimately tied to the benefits from trading opportunities with the currency in the future. Since the shareholders are the customers in the ICO, the dividend of this security is endogenous, and this distinguishes our setting from models of IPOs, venture capital, and the secondary market trading analyzed in these other papers.

1 The Model

Consider a cryptocurrency, which serves the membership to a 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 coin miners, who provide settlement and accounting services for transactions in the platform.

We analyze this cryptocurrency with the model of two periods $t \in \{1, 2\}$ and three types of agents: households, coin 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,[1] we focus on analyzing how the currency price serves to aggregate the trading needs of the households and affect their participation in the platform. Nevertheless, we call the trading round in the model the ICO.

At $t = 2$, the households in the platform are randomly matched to trade endowments. This trade is supported by two miners whose servers clear the transaction on a blockchain for the buyer and seller. Households then consume both their own good and their trading partner's consumption 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. We can 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

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

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 during the ICO.

Household i has a Cobb-Douglas utility function over consumption of its own good and that of a trading partner, household j, that it randomly meets at $t = 2$ in the platform, according to:

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

where $\eta_c \in (0,1)$ represents the weight in the Cobb-Douglas production function on its consumption of its trading partner's good C_j , and $1 - \eta_c$ is the weight on its own consumption good C_i. A higher η_c means a stronger complementarity between the consumption of household i and its consumption of the good endowed to the other household with which it trades at $t = 2$. We assume that both goods are needed for the household to derive utility from consumption, and if it receives its endowment without trading then it receives zero utility from it. This utility specification implies that each household cares about the aggregate endowment of all other households in the platform, and this will ultimately define the currency's fundamental.

The 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 $\int \varepsilon_i d\Phi\left(\varepsilon_i\right) = 0$ by the Strong Law of Large Numbers. The aggregate endowment A is a key characteristic of the platform. A cleverly designed cryptocurrency serves to attract a platform of households with a high value of A so that the households in the platform have 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 between 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 analyzing 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 cryptocurrencies is that many transactions are decentralized and clear on decentralized servers that record the transaction 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:

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

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 buy it and 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 the expected value of finding another currency in which to exchange less the cost of search for that currency.

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

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

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

There is a population of coin 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 between households in the platform at $t = 2$. Miners also face uncertainty about the aggregate strength of the cryptocurrency platform, and the ability of the supply side to respond to the demand for the transaction services. Specifically, miner i provides the computing power to facilitate a trade between households subject to a cost to setting up the required hardware and software to mine the cryptocurrency: $e^{-\omega_i} S_i$, 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 builders in the currency through the common component ξ. It is realistic to assume heterogeneity in the technologies to which miners have access for mining the cryptocurrency, with less efficient miners employing more costly technologies. We assume that ξ represents an unobserved, 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 $1 - \rho_s \in (0, 1)$ of the proceeds from selling the cryptocurrency at $t = 1$ to households at price P, which serves as the fee for clearing transactions at $t = 2$.[2] Miners in the currency at $t = 1$ maximize their revenue:

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

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

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

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 cryptocurrency technology is supported by a Proof of Work (PoW) protocol for recording transactions on blockchains. Each miner, in return for receiving payment for

[2] 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.

the cryptocurrency that it sells to households, provides computing power to facilitate one potential transaction between households in the platform that is added to the chain at $t = 2$. To ensure there are enough servers to clear all household transactions, the platform requires at least as many miners as households to prevent a failed transaction, since each transaction requires two miners. We assume miners have commitment so that if they accept payment at $t = 1$, they agree to clear a transaction at $t = 2$ if needed.

1.3 Developer

The developer of the cryptocurrency creates the platform at $t = 1$. It establishes the code that specifies the protocol of how transactions in the platform of owners of the cryptocurrency 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_s of the revenue P from the Initial Coin Offering (ICO), with ρ_s fixed as part of the technology.[3] The remaining revenue is paid to miners as part of the Proof of Work (PoW) protocol in exchange for their accounting services at $t = 2$. A lower ρ_s can be viewed as a higher profitability of mining that entices more miners to support the platform.

The developer receives the revenue from the ICO:

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

1.4 Rational Expectations Cutoff 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

[3] As in practice, the developer no longer controls the cryptocurrency or maintains its operation after the ICO, and consequently has no role at $t = 2$. By designing the ledger at $t = 1$, and abandoning it at $t = 2$, however, the developer indirectly commits to a quality of transparency in the subsequent transactions that occur in the currency.

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:

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

  where each household's demand $X_i\left(A_i, P\right)$ depends on its productivity A_i and the currency price P,[4] and each builder's housing supply $S_i\left(\omega_i, P\right)$ 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:

$$C_i\left(i\right) + C_j\left(i\right) = e^{A_i}.$$

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

[4]Note that each household's demand for the cryptocurrency may also directly depend on the network strength A if it is publicly observed, as in the perfect-information benchmark.

proposition describes each household's consumption choice. Its marginal utility of goods consumption also gives the equilibrium goods price.

Proposition 1 *Households i's optimal goods 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 of household i at $t = 1$ is given by

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

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

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

Proposition 1 shows that each household spends a fraction $1 - \eta_c$ of its endowment (excluding housing wealth) on consuming its own good $C_i(i)$ and a fraction η_c on goods produced by its trading partner $C_j(i)$ if they match. When $\eta_c = 1/2$, the household consumes its own good and the goods of its neighbors equally. The price of each good is determined by its output relative to that of its partner to the extent that there is complementarity in their consumption. 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, which is the price P to buy a unit of the currency. It then follows that household i's purchase decision is given by

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

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.

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 owning the currency, which trades off the opportunity of trading with other households in the trading platform with the price of 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 generically two cutoff equilibria, 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:*

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

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

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

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

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

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

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

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

Proposition 2 characterizes the cutoff equilibrium in the platform when A is publicly observed at $t = 1$, and confirms the optimality of a cutoff strategy for households in their choice to purchase the cryptocurrency. Households sort based on their endowments into the platform, with those with higher endowments, who expect more gains from trade with other households in the platform, entering and participating in decentralized trading at $t = 2$. In this cutoff equilibrium, the cryptocurrency price is a function of both the demand and supply fundamentals but, despite its log-linear representation, it is actually a generalized linear function of $\sqrt{\frac{\tau_\varepsilon}{\tau_e}} A - \xi - \log(1 - \rho_s)$, 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 generically two equilibria in the cryptocurrency market: 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 because households have backward-bending demand curves and, consequently, a high or a low price equilibrium can be self-confirming.[5] The household with the highest endowments enter first but, if too few others enter, then the marginal benefit of trading in the platform is low, since

[5] Backward-bending demand curves can also arise from 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).

the probability of meeting another household in the platform is low. This leads to a low price. If instead many households enter, then the marginal benefit of entering the platform is high, sustaining a high price. It is also possible that no household buys the cryptocurrency if A or ξ are sufficiently small.[6]

We illustrate the intuition for this multiplicity with a numerical example, in which we choose the following parameters:

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

The left-hand side (LHS) of equation (6), which determines the cutoff, is bell-shaped in $A^*(A,\xi) - A$, and corresponds to the backward-bending demand curve of households, while the right-hand side (RHS) is the straight line $\exp(-A - \xi - \log(1-\rho_s))$. 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 above the bell-shaped curve, corresponding to very low realizations of the demand and supply fundamentals, no cutoff equilibrium exists, and no households purchase the cryptocurrency.

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

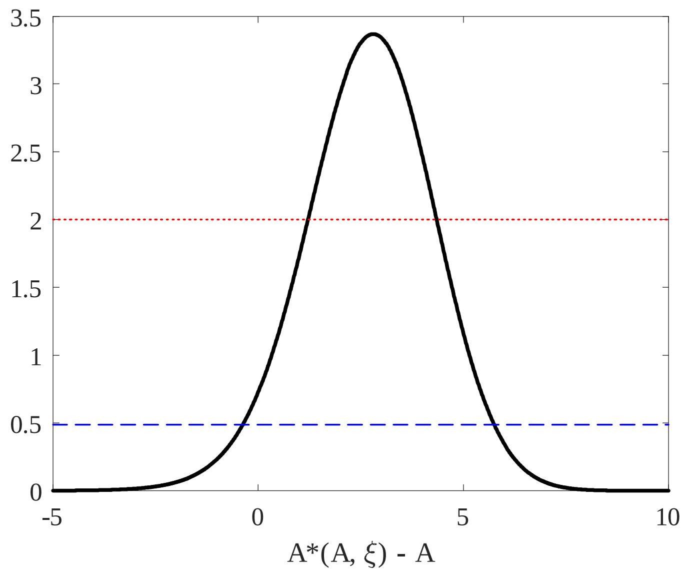

Figure 1: Plot of Left-hand Side and Right-Hand Side of Equation (6)

The existence of the two equilibria is directly related to the ICO funding model. In this model, buyers of the cryptocurrency are also the customers that the funded business (i.e., the platform) aims to serve, in sharp contrast to the typical models of funding new business projects by venture capitalists or by IPOs, in which investors and customers are usually different. As a result of this direct overlap between investors and customers of cryptocurrencies, there is a strong interaction between the funding cost and the business operation, which ultimately underlies the multiple equilibria.[7]

Proposition 2 also provides several comparative statics of the two equilibria. Due to 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 by buying the cryptocurrency 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.

[7] Treating equation (6) as a functional fixed-point equation that iterates over the cutoff A^*, one can show that the high price equilibrium is stable while the low price is unstable, in the sense that the market returns to the equilibrium following small perturbations to the cutoff.

The multiplicity of equilibria can cause a viable currency to fail. Even a platform with a strong demand fundamental A may attract little interest from investors, and this is self-sustaining, even though it could support a much larger subscriber base. Since the revenue from developing the platform in the high price equilibrium, $\frac{\rho_s}{1-\rho_s}\Phi\left(\frac{A-\underline{A}^*}{\tau_\varepsilon^{-1/2}}\right)e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}(A-\underline{A}^*)-\xi}$, is strictly higher than in the low price equilibrium, $\frac{\rho_s}{1-\rho_s}\Phi\left(\frac{A-\bar{A}^*}{\tau_\varepsilon^{-1/2}}\right)e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A-\bar{A}^*\right)-\xi}$, the developer also prefers the high price equilibrium, since the currency would then be both viable and more profitable. The existence of multiple equilibria also motivates large traders, such as the so-called coin whales in practice, to take on strategic positions to push the price of a cryptocurrency to its high price equilibrium. To the extent that all agents involved in the platform, including the developer, the households, and the miners, benefit from the high price equilibrium, such strategic trading may be socially beneficial.

While much of the current media and policy debate about cryptocurrencies emphasizes that they do not fall within the purview of any goverment 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 and other financial instruments: the lack of a sovereign that provides policy interventions to control inflation, set exchange rates, and promote economic activity. The government, as a large player that internalizes how economic actors make decisions and how prices are determined, plays a pivotal role in setting agent expectations on the future path of the economy, and helps stabilize prices and exchange rates by committing to act to ensure this path. In the absence of such guidance and policy interventions, however, it is not so surprising that cryptocurrencies are often associated with large price swings, confusion, and potentially self-fulfilling traps that lead to their failure. The absence of a stabilizing hand also explains why large investors have an incentive to act like cryptocurrency whales.

The multiplicity of equilibria also underscores and exacerbates the challenges in evaluating the fundamental value of a cryptocurrency in practice, and helps to rationalize a wide spectrum of observed dynamics of different cryptocurrencies. 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. This problem becomes particularly relevant when realistic informational frictions about the platform makes its fundamental not directly observable to the public. We analyze this issue in the 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' ming 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. Intuitively, A_i 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 in the platform.

In addition to their private signals 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 the 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. Since households buy the currency for decentralized trading with each other at $t = 2$, this volume is akin to the demand fundamental in our setting. Anticipating a cutoff equilibrium in which households with endowment signals above A^* buy the cryptocurrency, we construct a volume signal:

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

where $\Phi(\cdot)$ is the CDF of normal distribution and $\varepsilon_V \sim \mathcal{N}(0, \tau_v^{-1})$ independent of all other shocks in the economy. This specification has the appeal that the volume signal is always between 0 and 1, and is highly correlated with the number of decentralized transactions that are added to the ledger at $t = 2$, which, by the weak LLN, is $\Phi\left(\sqrt{\tau_\varepsilon}\,(A - A^*)\right)^2$. This volume signal can also be viewed as the number of coins in active circulation.

The noise in the signal reflects that, in practice, blockchains from the ledger are an imperfect signal about the demand for trade in the cryptocurrency. Only a fraction of transactions, for instance, hit the blockchain, where they are recorded, because of how costly it is to pay transaction fees to miners in Proof of Work (PoW) coins. As such, many transactions, such as the purchase and sale of coins with another currency, take place on exchanges and never hit the blockchain. In addition, the anonymous nature of the transactions makes it difficult to assess the effective supply of cryptocurrencies in circulation, since transferring cryptocurrencies across wallets, in which no actual currency is traded between two parties, is a transaction that hits the blockchain.[8] 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 currency 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.

Since the CDF of the normal distribution is a monotonically increasing function, we can invert V to construct an additive summary statistic v:

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

[8] Even now, some cryptocurrencies are adopting "no knowledge proof" encryption to be able to verify transactions without having to disclose any of the underlying details of the transaction recorded on the chain.

which, in the sequel, serve as the volume signal about the cryptocurrency. Interestingly, the precision of the volume signal is $\tau_\varepsilon \tau_v$, which reveals that the less dispersed the endowments of households, the more informative is the history of transactions recorded in the currency's ledger.

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. Like in the perfect-information setting, each household would still use a cutoff strategy, and the equilibrium cryptocurrency price is a nonlinear function of A, which posts a challenge to our derivation of households' learning of A. It turns out that the information content of P can be summarized by a summary statistic z that is linear in A and the supply shock ξ:

$$z = A - \sqrt{\frac{\tau_e}{\tau_\varepsilon}}\xi.$$

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.

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 price and each household's cryptocurrency demand in this equilibrium.

Proposition 3 *If the platform fundamental A is not publicly observable at $t = 1$, there are generically two cutoff equilibria, in which the following hold:*

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

$$\log P = \sqrt{\frac{\tau_\varepsilon}{\tau_e}} (A - A^*) - \xi - \log(1 - \rho_s). \tag{7}$$

2. *The posterior of household i conditional on the summary statistic of the cryptocurrency price z, the volume signal summary statistic 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 $A^*(z, v)$ solves equation (17) in the Appendix.

4. *There are either two or no equilibria. 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 shock has the opposite impact in the low price equilibrium.*

Proposition 3 confirms even when the platform fundamental A is not publicly observable, the equilibrium cryptocurrency price in (7) takes exactly the same log-linear form as in the perfect-information setting, as shown by 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, as captured by the two summary statistics z and v. While each household continues to use the cutoff strategy, the equilibrium cutoff A^* now becomes a function of z and v. Being the only difference in the equilibrium price function from the perfect-information setting, $A^*(z, v)$ is also the only channel, through which the households' learning of A through the price and volume signals affects the market.

Like the perfect-information setting, there are again either two equilibria or no equilibria at all. This situation arises from solving $A^*(z,v)$ from its fixed-point condition given in equation (17), which is similar to equation (6), albeit more complex. Equation (17) may have either two solutions or no real solution, which leads to the existence of two or no equilibria. When two equilibria exist, one of them has lower equilibrium cutoff for households' cryptocurrency purchase decision and higher cryptocurrency price, while the other has higher equilibrium cutoff and 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.

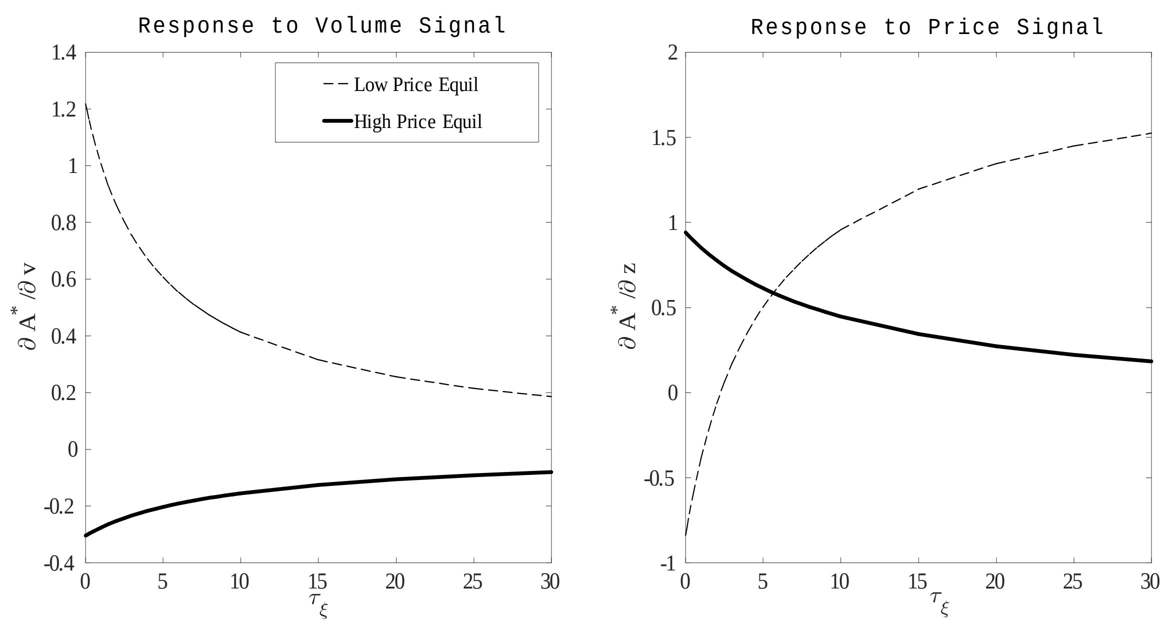

Figure 2: Responses of $A^*(z,v)$ to v and z in the high-price and low-price equilibria across different values of τ_ξ.

To further illustrate the key properties of these two equilibria, Figure 3 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 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, indicating that more households join the platform. In contrast, A^* reacts positively to v, 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 the platform fundamental 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.

The right panel illustrates how the cutoff A^* responds to a unit impulse to the sufficient statistic in the price z. For τ_ξ close to 0, the currency price contains little information about the demand fundamental, and consequently the cost effect dominates the impact of an increase in z. 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 low price equilibrium features an opposite reaction to prices. As τ_ξ increases, however, the role of a higher z in reflecting a higher demand fundamental 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. Interestingly, the learning effect dominates in the low price equilibrium for sufficiently high τ_ξ: less households enter the platform because of the increased optimism about the demand fundamental, as a higher A raises the cutoff in the low price equilibrium.

In traditional asset market models with dispersed information, in the Grossman and Stiglitz (1980) and Hellwig (1980) paradigms, trading volume plays no role in learning,[9] and is often studied only for its empirical predictions, as in, for instance, Wang (1994) and He and Wang (1995).[10] In our setting, households learn from both the cryptocurrency price and volume when deciding whether to purchase the cryptocurrency. As such, volume provides

[9]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.

[10]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.

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. Since the precision of the volume signal is increasing in the precision of each household's private information τ_ε, it mitigates the information asymmetry more than an exogenous public signal: when households know more (high τ_ε), the volume signal is more informative, and similarly when households know less (low τ_ε). In addition, households substitute toward (away) from this source of information the less (more) informative is the price. Consequently, our model suggests that market participants should pay more attention to the records of the decentralized ledgers the more homogeneous are the users of the currency.

An important implicit assumption underlying our analysis with informational frictions 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 according to:

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

since $A^*(z,v) \in \left\{\underline{A}^*(z,v), \bar{A}^*(z,v)\right\}$, which are what is actually observed by market participants.[11] From the proof of Proposition 3, each (z,v) pair maps to two (P,V) pairs, one corresponding to a high price equilibrium, $\underline{A}^*(z,v)$, and the other to a low price equilibrium, $\bar{A}^*(z,v)$. By similar logic, each (P,V) pair maps to two (z',v') pairs, one rationalizing (P,V) as a high price equilibrium $\underline{a}^*(P,V)$, and the other as a low price equilibrium $\bar{a}^*(P,V)$, with the lower case a^* denoting a different cutoff mapping than A^*. While there is only one fixed point, i.e. either $\underline{A}^*(z,v) = \underline{a}^*(P,V)$ or $\bar{A}^*(z,v) = \bar{a}^*(P,V)$, it is not clear to an outsider

[11] 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.

from just observing the price on which equilibrium market participants are coordinating. Consequently, the nature of the market makes it is difficult for outsiders and regulators to interpret market conditions, which is particularly problematic since the response of the market to changes in fundamentals is very different across the high and low price equilibria.

This potential confusion introduces a secondary role for volume as a signal about coordination in conjunction with prices. While any given cryptocurrency price could be rationalized as corresponding to a high or low price equilibrium, the volume signal provides a second piece of information. A high price with a high volume signal is indicative of a high price equilibrium, while a low price with low volume suggests the market has coordinated on a low price equilibrium. 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.

Our analysis also suggests that, in the presence of informational frictions, the dual inference problem makes it particularly difficult for outsiders to infer both the fundamental and the nature of the equilibrium from prices. This may lead to erratic trading behavior by outside investors based on technical analysis. In particular, a rising price is positively correlated with higher fundamental in the high price equilibrium, while indicative of lower fundamental in the low price equilibrium. Thus, depending on an investor's assessment of which equilibrium the market is currently in, he may adopt either trend-chasing or the opposite contrarian strategy. Furthermore, the investor may choose to dramatically reverse the strategy if he speculates that the market is switching from one equilibrium to the other.

4 Conclusion

We develop a model of the initial coin offering (ICO) of a cryptocurrency to understand what fundamentals govern its success and the price at which the currency trades. Our analysis reveals that, since the shareholders who participate in the ICO are also the customers that use the currency to trade goods and services, there is an intimate link between the success of the ICO and the viability of the currency as a medium of exchange. This link gives rise to the possibility of coordination failure, in which the currency price and the volume of coins in active circulation reflect whether the market is in a high price equilibrium, in which the currency price is high and many households participate, or a low price equilibrium, in which the currency price is low and few coins are in active circulation. Importantly, these two equilibria have very disparate properties and, as a result, observing the same price and volume fluctuations have very different implications for diagnosing the health of the currency depending on the equilibrium. As cryptocurrencies are not backed by a sovereign that can help coordinate platform participants along an equilibrium path, this multiplicity has a pronounced and destabilizing impact on the currency, and invites manipulation from large investors.

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. Since coordination issues also extend to this incomplete information setting, the market reacts very differently to news stemming from these price and volume signals depending on whether the market is in the high or low price equilibrium. Furthermore, inference about the fundamental and coordination cannot easily be disentangled, which suggests that there are many ways to rationalize any price fluctuations from the perspective of an outsider. Our analysis suggests that analyzing measures of quantities for cryptocurrencies, such as the volume of transactions recorded on its ledgers, can provide helpful insight when trying to tether valuations of these cryptocurrencies, and that technical analysis can potentially worsen price fluctuations. To assess whether there is a bubble, one must first take a stance on an asset's fundamentals, and our work cautions an approach that does not take into account the dual roles of the currency as a security and a medium 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.

Asriyan, Vladimir, William Fuchs, and Brent Green (2017), Sentiment, Liquidity, and Asset Prices, mimeo CREI, UT Austin, UC Berkeley.

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 Fold 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.

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

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.

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.

Kurlat, Pablo and Laura Veldkamp (2015), Should We Regulate Financial Information, *Journal of Economic Theory* 158, 697-720.

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

Malherbe, Frederic (2014), Self-fulfilling Liquidity Dry-ups, *Journal of Finance* 69, 947–970.

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

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

Plantin, Guillaume (2009), Learning by Holding and Liquidity, *Review of Economic Studies* 76, 395–412.

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.

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:

$$C_i(i) \quad : \quad \frac{1-\eta_c}{C_i(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_i, \tag{8}$$

$$C_j(i) \quad : \quad \frac{\eta_c}{C_j(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_j, \tag{9}$$

where θ_i is the Lagrange multiplier for the budget constraint. Rewriting (9) as

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

Dividing equations (8) 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 $p_j C_j\left(i\right) = \frac{\eta_c}{1-\eta_c} p_i C_i\left(i\right)$. By substituting this equation back to the household's budget constraint in (2), we obtain:

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

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

The first order condition in equation (8) 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:

$$p_i = \frac{1-\eta_c}{C_i\left(i\right)} U\left(C_i\left(i\right), C_j\left(i\right); \mathcal{N}\right) = e^{\eta_c\left(A_j - A_i\right)}. \tag{10}$$

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

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

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:

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

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:

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

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 builders 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 neighborhood choice at the cutoff, it follows that $E\left[U_i|\mathcal{I}_i^*\right]-P=0$, which implies:

$$e^{(1-\eta_c)A_i}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)=e^{-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\eta_c A}P, \text{ with } A_i=A^* \tag{11}$$

which implies the benefit of living with more productive households is offset by the higher cost of living in the neighborhood.

Fixing the critical value A^* and price P, we see that the LHS of equation (11) is increasing in monotonically in A_i, since $1-\eta_c>0$. This confirms the optimality of the cutoff strategy that households with $A_i\geq A^*$ enter the neighborhood, and households with $A_i<A^*$ choose to live somewhere else. Since $A_i=A+\varepsilon_i$, it then follows that a fraction $\Phi\left(-\sqrt{\tau_\varepsilon}\left(A^*-A\right)\right)$ enter the neighborhood, and a fraction $\Phi\left(\sqrt{\tau_\varepsilon}\left(A^*-A\right)\right)$ choose to live somewhere else. As one can see, it is the integral over the idiosyncratic productivity shocks of households ε_i that determines the fraction of households in the neighborhood.

From the optimal supply of housing by builder i in the neighborhood (5), there exists a critical value ω^* :

$$\omega^*=-\log P-\log\left(1-\rho_s\right), \tag{12}$$

such that builders with productivity $\omega_i \geq \omega^*$ build houses. Thus, a fraction $\Phi\left(-\sqrt{\tau_e}\left(\omega^*-\xi\right)\right)$ build houses in the neighborhood. Imposing market-clearing, it must be the case 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 the above market-clearing conditions, and impose equation (12) to arrive at

$$\log P=\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A-A^*\right)-\xi-\log\left(1-\rho_s\right). \tag{13}$$

By substituting for P in equation (11), we obtain an equation to determine the equilibrium cutoff $A^*=A^*\left(A,\xi\right)$:

$$e^{\left(1-\eta_c+\sqrt{\tau_\varepsilon/\tau_e}\right)A^*}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)=e^{\left(\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\right)A-\xi-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho_s)}. \tag{14}$$

Let the log of the LHS of equation (14) be $f\left(A^*\right)$ as a function of A^*. Taking the derivative of $f\left(A^*\right)$ with respect to A^* gives

$$\frac{df}{dA^*}=1-\eta_c+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\frac{1}{\tau_\varepsilon^{-1/2}}\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)}.$$

Notice as $A^*\to-\infty$, $\frac{df(A^*)}{dA^*}\to 1-\eta_c+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}>0$, while as $A^*\to\infty$, then:

$$\left.\frac{df}{dA^*}\right|_{A^*\to\infty}\to 1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}+\lim_{A^*\to\infty}\frac{A-A^*}{\tau_\varepsilon^{-1}}\to-\infty.$$

Furthermore, we recognize that:

$$\frac{d^2f}{dA^{*2}}=-\frac{1}{\tau_\varepsilon^{-1/2}}\left(\eta_c+\frac{A-A^*}{\tau_\varepsilon^{-1}}+\frac{1}{\tau_\varepsilon^{-1/2}}\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)}\right)\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)},$$

which achieves its maximum at $A\to\infty$, where $\frac{d^2f}{dA^{*2}}=0$. Consequently, $\frac{d^2f}{dA^{*2}}\leq 0$, and therefore $f\left(A^*\right)$ is concave and therefore hump-shaped in A^*. Furthermore, the LHS of (14) tends to 0 as $A^*\to-\infty$ and $A^*\to\infty$. Therefore, the LHS of (14) is quasiconcave in A^*.

Notice that we can rewrite equation (14) as:

$$e^{\left(1-\eta_c+\sqrt{\tau_\varepsilon/\tau_e}\right)s}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-\frac{s}{\tau_\varepsilon^{-1/2}}\right)=e^{-A-\xi-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho_s)}, \tag{15}$$

where $s = A^* - A$ determines the population that buys the currency. Notice that the LHS of equation (15) is log concave, since the pdf and CDF of the normal distribution is log concave and the exponential function is log-linear. Consequently, $\frac{d^2 \log LHS}{ds^2} < 0$.

Notice that the properties of the LHS of equation (15) are the same as for A^* in equation (14), and, importantly, the LHS is now independent of A. The LHS is then a quasiconcave bell curve as a function 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 (15) is fixed, it follows that the LHS and RHS of equation (15) intersect generically twice, with once being a knife-edge case when the equilibrium s is $\hat{s}$. Therefore, there are generically two cutoff equilibrium. It can occur, however, that the RHS of equation (15) 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 are 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 (15) 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 $P = \exp\left(-\sqrt{\frac{\tau_\varepsilon}{\tau_e}} s - \xi - \log\left(1-\rho_s\right)\right)$, 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 $\rho_s \Phi\left(-\sqrt{\tau_\varepsilon} s\right) P$, it follows that:

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

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:

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

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:

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

A.3 Proof of Proposition 3

Given our assumption about the sufficient statistic in housing 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:

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

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 currency developer.

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

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

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 $\hat{\tau}_A$. Let

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

Define $x = \frac{A-A^*}{\tau_\varepsilon^{-1/2}}$, and the function $g(x)$:

$$g(x) = e^{\eta_c \tau_\varepsilon^{-1/2} x}\Phi\left(\eta_c \tau_\varepsilon^{-1/2} + x\right),$$

as the term inside the bracket. Then, it follows that:

$$\frac{d \log g(x)}{dx} = \eta \tau_\varepsilon^{-1/2} + \frac{\phi\left(\eta_c \tau_\varepsilon^{-1/2} + x\right)}{\Phi\left(\eta_c \tau_\varepsilon^{-1/2} + x\right)} > 0,$$

and therefore $\frac{dg(x)}{dx} > 0$, since $g(x) \geq 0$. Consequently, it follows that $\frac{dG}{dx}(x, \hat{\tau}_A) > 0$, since this holds for all realizations of $A - A^*$. That the inequality is strict comes from recognizing, as $x \to -\infty$, by L'Hospital's Rule:

$$\lim_{x \to -\infty} \frac{d \log g(x)}{dx} = -\lim_{z \to -\infty} x = \infty.$$

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:

$$e^{\frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1} + (1-\eta_c)A_i + \eta_c A^*} G\left(\hat{A}_i - A^*, \hat{\tau}_A\right) = P, \; A_i = A^* \tag{16}$$

which does not depend on the unobserved A or the supply shock ξ, and we have substituted for u_0. As such, $A^* = A^*(\log P, v)$. Furthermore, since $\hat{A}_i^*$ is increasing in A_i and $G\left(\hat{A}_i^* - A^*, \tau_A\right)$ is (weakly) increasing in $\hat{A}_i$, it follows that the LHS of equation (16) is (weakly) monotonically increasing in A_i, confirming the cutoff strategy assumed for households is optimal. Those with the RHS being nonnegative purchase the currency, and those with it being negative choose to refrain.

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 the above market-clearing condition, and impose equation (12) to arrive at:

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

from which follows that:

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

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:

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

Substituting for prices, and simplifying A^* terms, we can express equation (16) as:

$$e^{\left(1+\sqrt{\tau_\varepsilon/\tau_e}\right)A^*}G\left(\hat{A}_i^*-A^*,\hat{\tau}_A\right)=e^{z-\sqrt{\frac{\tau_e}{\tau_\varepsilon}}\bar{\xi}-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho_s)},\tag{17}$$

where

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

is the posterior belief when $A_i=A^*$. Notice that the LHS of equation (17) is continuous in A^*.

Now let us rewrite equation (16) as:

$$\exp\left(h\left(A^*\right)\right)=e^{z-\sqrt{\frac{\tau_e}{\tau_\varepsilon}}\bar{\xi}-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho_s)},$$

where:

$$h\left(A^*\right)=\left(1+\sqrt{\tau_\varepsilon/\tau_e}\right)A^*+\log G\left(\hat{A}_i^*-A^*,\hat{\tau}_A\right),$$

and it follows that:

$$\frac{dh}{dA^*}=1+\sqrt{\tau_\varepsilon/\tau_e}+\frac{1}{G\left(\hat{A}_i^*-A^*,\hat{\tau}_A\right)}\left.\frac{dG\left(x,\hat{\tau}_A\right)}{dz}\right|_{x=\hat{A}_i^*-A^*}\frac{d\left(\hat{A}_i^*-A^*\right)}{dA^*}.$$

Since $\frac{dG(x,\hat{\tau}_A)}{dx}\geq 0$, by the above arguments, and:

$$\begin{aligned}\frac{d\left(\hat{A}_i^*-A^*\right)}{dA^*} &= \hat{\tau}_A^{-1}\frac{d}{dA^*}\left(\tau_A\left(\bar{A}-A^*\right)+\tau_v\left(v-A^*\right)+\frac{\tau_\varepsilon}{\tau_e}\tau_\xi\left(z-A^*\right)\right)\\ &= -\hat{\tau}_A^{-1}\left(\tau_A+\frac{\tau_\varepsilon}{\tau_e}\tau_\xi\right)<0,\end{aligned}$$

since z is independent of A^*, it follows that the second term in $\frac{dh}{dA^*}$ is negative.

As $A^* \to -\infty$, since $\Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right) \to 1$, we see, by rewriting $h(A^*)$ as:

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

that:

$$\lim_{A^* \to -\infty} \frac{dh}{dA^*} = 1 - \eta_c + \sqrt{\tau_\varepsilon/\tau_e} + \hat{\tau}_A^{-1} \tau_\varepsilon > 0,$$

while as $A^* \to \infty$, one has that:

$$\lim_{A^* \to \infty} \frac{dh}{dA^*} = 1 + \sqrt{\tau_\varepsilon/\tau_e} - \hat{\tau}_A^{-1} \left(\tau_A + \frac{\tau_\varepsilon}{\tau_e} \tau_\xi\right) \lim_{A^* \to \infty} \frac{d}{dx} \log G(x, \hat{\tau}_A) \bigg|_{x = A - A^*} = -\infty,$$

since $\lim_{x \to -\infty} \frac{d \log g(x)}{dx} = \infty$, and $G(E[x], \hat{\tau}_A)$ is an expectation over $g(x)$.

As $A^* \to -\infty$, we also notice that:

$$\lim_{A^* \to -\infty} \exp(h(A^*)) = 0.$$

and, by the Sandwich Theorem, one also has that:

$$\lim_{A^* \to \infty} \exp(h(A^*)) = 0.$$

In addition, similar arguments to those in Proposition 2, suitably modified, reveal that $\frac{d^2 h}{dA^{*2}} \leq 0$. As such, $\exp(h(A^*))$ is quasiconcave in A^*. Since the RHS of equation (16) is fixed as a horizontal line, while the LHS is bell-shaped, it follows that generically there are two cutoff equilibria in the economy, when a cutoff equilibrium in the economy with informational frictions exists.

Notice now that, since $G\left(\hat{A}_i^* - A^*, \hat{\tau}_A\right)$ is monotonically increasing in its first argument, and $\hat{A}_i^*$ is increasing in v, it follows that the bell-shaped curve of the LHS of equation (16) shifts up for each value of A^* from an increase in the noise shock ε_v to v. Given that the RHS of equation (16)is fixed with respect to the noise in the volume signal ε_v, it 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.