A Model of Cryptocurrencies*

Michael Sockin† Wei Xiong‡

October 2018

Abstract

We model a cryptocurrency as both a membership in a decentralized digital platform developed to facilitate transactions of certain goods or services, and as a fee to compensate miners on the platform for their costly custodial services. The rigidity induced by the cryptocurrency price having to clear these two sides, especially with strong complementarity in membership demand, leads to either no or two equilibria. The possibility of no equilibria (platform failure) discourages the platform developer from committing ex ante to disclosing all relevant information about the platform to the public. In contrast, in a conventional two-fee platform, where the developer can set separate membership and service fees, the flexibility in pricing ensures a unique equilibrium. As a result, the developer would prefer full information disclosure if it funds the platform through a traditional IPO.

*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, Tsinghua, UBC, UNC, and Yale for helpful comments.

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

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

Between 2015 and 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. 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.

In this paper, we develop a model to analyze the properties of utility tokens, a subset of cryptocurrencies along with coins and security tokens, and the ICOs that launch them. Utility tokens are native currencies accepted on decentralized digitial platforms that often provide intrinsic benefit to participants. In contrast, coins (and altcoins), such as Bitcoin and Litecoin, are fiat currencies that are maintained on a public blockchain ledger by a decentralized population of record keepers, while security tokens are financial assets that trade in secondary markets on exchanges, and whose initial sale is recorded on the blockchain of the currency that the issuer accepts as payment.[1] The benefits of utility tokens can range from provision of secure and verifiable peer-to-peer transaction services to maintenance of smart contracts, to gaming, sports and prediction betting, and to support of crowdfunding activities and media content whose sales are brokered in the currency. Examples of such utility tokens include Ether, which enables participants to write smart contracts with each other, Filecoin, which matches the demand and supply for decentralized computational storage, and GameCredits, which finances the purchase, development, and consumption of online games and gaming content. A key innovation of these platforms, along with the ability to build global communities and the adoption of blockchain technology for record-keeping, is that they are "trustless" decentralized networks that lack a sovereign or central firm or inter-

[1] Coins are typically created through "forks" from existing currencies, such as Bitcoin Gold from Bitcoin, and by airdrops, in which the developer sends coins to wallets in an existing currency to profit from the price appreciation of its retained stake if the new currency becomes widely adopted. Security tokens are typically sold through ICOs structured as "smart contracts" on existing blockchains such as that of Ethereum.

mediary to steward the platform and the currency. Instead of intermediaries, a population of record keepers are compensated for processing activities on the blockchain with utility tokens according to a consensus protocol, such as with miners and the Proof of Work (PoW) protocol. Development of these platforms is financed by the sale of tokens to investors and potential customers through ICOs, which often represent the exit strategy for the developer after the platform launches.

Decentralized digital platforms have the capacity to build global online ecosystems in which potential customers can self-select into communities in which their interactions are fostered by disruptive and disintermediated technologies targeted to their interests. Since users and record keepers on a platform are both potential customers in its services and investors in its token's price appreciation, utility tokens represent a novel financial instrument that is highly susceptible to real feedback effects from platform performance.[2] In order to properly assess the potential benefits and risks brought about by cryptocurrencies, however, and to establish a suitable regulatory framework for ICOs, it is important to understand how utility token trading and the "trustless" nature of decentralized digital platforms impact participation in the platform, its performance, the price of the currency, and ultimately the success of the ICO. The ample uncertainty and opacity associated with many ICOs, along with the typically observed frenzied trading of cryptocurrencies after their launch, further 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. In addition, since decentralized digital platforms are often predicated upon untested technologies, it is important to undestand how asymmetric information impacts the answers to these questions.

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

[2] In the new monetary literature, fiat money serves as a medium of exchange to overcome a lack of double coincidence of wants. Here, the value of the utility token is precisely in its ability to coordinate agents with gains from trade to join the platform.

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, 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 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 buying the cryptocurrency with the benefit from transacting goods on the platform. This benefit increases with both the household's own goods 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 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.

We analyze the equilibrium in two settings, differing in whether the platform's demand and supply fundamentals are publicly observable. In the first setting, the fundamentals are publicly observable. There exist either two or no rational expectations equilibria as a result of the network effect—if more households join the platform by choosing a lower cutoff strategy, each household benefits more from trading goods with others on the platform, and is thus willing to pay a high cryptocurrency price. As the cryptocurrency price also has to induce an equal number of miners to serve the households, the rigidity leads to no equilibria when either the demand-side or supply-side fundamental is sufficiently weak.

This ultimate platform failure through the ICO arrangement is in sharp contrast to a more

conventional arrangement where the platform developer sets two separate fees, a membership fee for households to join the platform and a separatae service fee for miners. The pricing flexibility given by these two fees ensures a unique equilibrium, even when the supply and demand fundamentals are both weak. When there exist two equilibria, they exhibit opposing behavior. One has a higher cryptocurrency price and a lower equilibrium cutoff, while the other has a lower price and a higher equilibrium cutoff for the same fundamentals. 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. 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 the households' common beliefs, based on the public signals, of the households' aggregate endowment and the miners' common mining cost. Interestingly, there again exist either no or two cutoff equilibria. This possibility of platform failure discourages the platform developer from committing ex ante to fully disclose information about the platform fundamentals, as such disclosure could lead to platform failure in states where its fundamentals are weak.

We also examine two alternative arrangements in setting up the platform. In the first, the developer sets up the aforementioned two-fee 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. There is always a unique 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 information to potential subscribers, in contrast to the ICO arrangement.

In our second alternative arrangement, households' transactions are cleared by a population of forgers following a Proof of Stake (PoS) protocol, instead of a population of miners under the PoW protocol. The forgers 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. While the PoS protocol resolves the issues of instability arising from coordination and scalability of computing resources, the cryptocurrency 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 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) investigates the tradeoff of smart contracts in overcoming adverse selection while also facilitating oligopolistic collusion, while Biais et al (2017) consider the strategic interaction among miners. Abadi and Brunnermeier (2018) examine disciplining writers to a blockchain technology with static incentives, and Saleh (2018) explores how decentralized consensus can be achieved with the Proof of Stake (PoS) protocol. 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 future growth in the platform. Pagnotta and Buraschi (2018) have an equilibrium framework for Bitcoin that also admits multiple equilibria, yet their focus is on a quantitative analysis. Our analysis microfounds the intrinsic value of cryptocurrencies as facilitating household transactions in a general equilibrium framework, and highlights the rigidity of the cryptocurrency price in clearing the supply and demand sides of the cryptocurrency market.

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 highlight inherent fragility of the ICO model and the resulting disincentive for the developer to disclose information.

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. Different from the existence of multiple equilibria in the search models of Kiyotaki and Wright (1993) and Lagos and Wright (2005), our model has either zero or two equilibria, with the no-equilibrium outcome capturing a severe form of fragility for cryptocurrencies.

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 distortion of informational frictions to housing and production decisions. In contrast, our setting features an interaction of search with centralized trading to explain the fragility of ICOs.

1 Examples

To motivate key ingredients of our model and facilitate our discussion, this section breifly describes three ICO examples: Ether, Filecoin and Civil. Ether and Filecoin are two utility tokens, successfully financed by ICOs. In particular, Filecoin had raised a record $257 million. Both Ether and Filecoin feature a population of customers and record keepers. We also describe the failure of Civil's ICO to highlight that ICO funding can be a fragile financing medium.

Ether Ether is a utility token that facilitates peer-to-peer transactions recorded on a public ledger, but also allows for the writing and implementation of smart contracts. These smart contracts are executable code written as an entry on the blockchain ledger that introduces contingency into transactions. For instance, the sale of a house or of equity in an entrepreneurial endeavor can be written as a smart contract, with the transfer of money from the buyer to the seller's wallet releasing the deed to the house, in the case of the former, or the security token that cedes control and dividend rights, in the case of the latter. As many smart contracts and security ICOs are written on the Ethereum blockchain, and are consequently transacted in Ether, this provides an additional benefit to owners of the utility token.[3] An important aspect of Ethereum is that, since it is a relatively small community, the size of the user base is an important determinant of any gains from trade among participants, and consequently the platform is subject to strong network effects.

As with many cryptocurrency platforms, Ethereum facilitates secure transactions by writing details of each transaction and smart contract contingency to an indelible public ledger legitimized through a decentralized consensus protocol.[4] Since Ether follows the Proof of Work (PoW) consensus protocol, each transaction is submitted to a queue of miners who compete to decrypt the details of the transaction, and reencrypt it to have a required number of leading zeros. The first miner to complete this task, is given the right to add the block to an existing blockchain. If others add to this miner's block, then the miner's block is legitimized,

[3] The DAO, for instance, was a private equity venture that issued DAO tokens in exchange for Ether. Its ICO raised over $150M in Ether from over 11,000 investors.

[4] A common misconception is that cryptocurrencies are prone to hacks. Most hacks, such as those on Mt. Gox and Coinrail, are on private exchanges that are unrelated to the blockchain technology supporting the hacked currencies. Attacks on the blockchain are through distortions to the ledger, such as "double-spending" that creates fradulent blocks by sending conflicting transactions and undoing others. This, however, requires having sufficient control of the maintenance of ledger. Krypton, Shift, and Bitcoin Gold suffered such "51% attacks", in which hackers temporarily gained control of 51% of their record-keeping services.

the transaction is completed, and the miner shares the block reward, which is payment in Ether through inflation of the token base. By paying miners in Ether, it incentivizes them to preserve "trust" in the platform to maintain Ether's monetary value, and this inflation rate is hard-wired into Ethereum's code. Since mining is computationally costly and entails risk, most miners participate in mining pools to provide mutual insurance by sharing their fees. In addition, having a diffuse mining base guards Ethereum against attacks by making it difficult for hackers to hijack maintenance of the ledger, a venture that becomes more profitable the more activity there is on the blockchain.[5]

Filecoin Filecoin is a utility token on a planned decentralized file-sharing platform. The platform's concept is that buyers who have a demand for storing their data securely can pay in Filecoin to those with a supply of excess storage space on their hard drives to store their files. Suppliers bid for the right to store a file, which is then copied, encrypted, broken into pieces, and scattered across the winning suppliers. In addition to buyers and sellers, there are locators who are compensated by the buyer for disassembling, and later reassembling, the scattered files. The addresses of the scattered pieces will be recorded on a blockchain ledger by a population of miners according to, as of now, a Proof of Replication protocol. As with Ether, these miners are compensated with Filecoin through inflation of the token base according to a predetermined schedule.

Civil To illustrate that ICOs are susceptible to failure, Civil was a planned online journalism platform that partnered with Forbes and The Associated Press to publish news on its blockchain. It sought to raise between $8M and $24M through its ICO by selling CVL tokens to investors. In October 2018, however, it canceled its ICO after raising less than $1.5M, and refunded its 1,012 investors their token purchases.

Key features These examples help to illustrate several important features of utility tokens and ICOs. The first is that Ether and FileCoin rely on having a large membership on their platforms for participants to realize potential gains from trade. In our model, we adopt a specific form of gain through the exchange of endowments between platform participants,

[5]Budish (2018) argues that the benefits of attacking the blockchain increase as cryptocurrencies such as Bitcoin become more widely adopted, and the currency experiences price appreciation. This places an economic upper bound on the price of the currency that ties it to the computational cost of a 51% attack. In 2015, the Bitcoin mining pool ghash.io voluntarily committed to reducing its share of mining power from over 50% to less than 40% to assuage fears of a potential attack on the currency.

similar to the international trade literature, although, in practice, the specific nature of these gains from trade can be different and more general than the form we adopt. To capture the network effects arising from endogenous participation, we assume severe search frictions in that potential participants randomly meet but can only transact with each other if they are both members of the platform. This reflects that a utility token platform is useful for realizing potential gains from trade only if there is a sizable population on the platform. The second key feature is that miners compete to complete customer transactions, and are compensated in the platform's utility tokens with a fixed inflation rate. These miners face heterogeneous costs, as evidenced by the geographic concentration of Bitcoin and Ether miners in areas with low electricity costs, such as the rural U.S., China, and Russia. Third, a diffuse mining pool is needed as the platform grows to ensure its reliability, and we capture this feature by assuming that trade on the aggregate platform is a Leontief function in the number of participants and in the number of miners. Fourth, in these ICOs, the developer sells tokens to investors and potential customers in advance of the platform's launch. The ICO represents both a key source of financing and revenue for the developer and an exit strategy, since the platform will be decentralized and maintained by its users. Finally, ICOs are fragile and can fail to raise sufficient funding, as illustrated by Civil.

2 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 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 on the platform, with the payment for the currency purchase shared by the developer and platform miners, who provide clearing 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,[6] we focus on analyzing how the token 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. As shown by the examples of Ether and FileCoin, the benefits to participating on a utility token platform can range from secure transactions to writing smart contracts, sharing in gaming content, and providing secure file storage. We choose this specific form of gains from trade to facilitate analysis within a standard trade framework. The goods transactions are supported by miners who act as service providers of the decentralized platform, and who compete to clear each 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. Households then consume both their own good and their trading partner's good.

2.1 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 on the platform. 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 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.[7]

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

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

where $\eta_c \in (0, 1)$ represents the weight in the Cobb-Douglas 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

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

[7] In practice, many ICOs are launched through smart contracts written on existing blockchains, such as ERC20 token platforms like Ethereum, and tokens are consequently purchased in these currencies. We abstract from identifying the numeraire in our analysis for simplicity.

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 on the platform, which ultimately defines the cryptocurrency's demand 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 $\int \varepsilon_i d\Phi\left(\varepsilon_i\right) = 0$ by the Strong Law of Large Numbers. The aggregate endowment A is a key characteristic of the platform. A cleverly designed 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, 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 analyzing a benchmark case in which 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 search costs that make direct trade prohibitively costly. 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.

At $t = 2$, when household i is paired with another household j on the platform, we

assume that they would simply swap their goods, with household i using $\eta_c e^{A_i}$ units of good i to exchange for $\eta_c e^{A_j}$ units of good j. Consequently, both households are able to consume both goods, with household i consuming

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

and household j consuming

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

We formally derive these consumption allocations between these two paired households in Appendix A through a microfounded trading mechanism between them.

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 the reservation utility of 0 from not trading with any partner. We quote the price of the cryptocurrency at $t = 1$ in terms of the numeraire good. As we only allow one round of trading at $t = 1$, this avoids the complication of re-trading the cryptocurrency.

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

$$\max_{X_i} \{E[U_i|\mathcal{I}_i] - P, 0\}. \tag{2}$$

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.

It then follows that household i's purchase decision is given by

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

As the household's expected utility is monotonically increasing with its own endowment, regardless of other households' strategies, it is optimal for each household to use a cutoff

strategy. This in turn leads to a cutoff equilibrium, 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 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 utility token by providing accounting and custodial services using its underlying blockchain technology, and facilitating the decentralized trades among households on the platform at $t = 2$. 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.[8] 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 $t = 2$.[9]

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: $e^{-\omega_i} S_i$, 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,

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

[9] 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.

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 $t=2$.[10] Miners in the currency at $t=1$ maximize their revenue:

$$\Pi_s\left(S_i\right) = \max_{S_i} \ \left(\left(1-\rho\right)P - e^{-\omega_i}\right) S_i. \tag{3}$$

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

$$S_i = \begin{cases} 1 & \text{if} \quad \left(1-\rho\right)P \geq e^{-\xi+e_i} \\ 0 & \text{if} \quad \left(1-\rho\right)P < e^{-\xi+e_i} \end{cases}. \tag{4}$$

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.[11]

2.3 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

[10] 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.

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

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

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

2.4 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:

- Household optimization: each household chooses X_i at $t = 1$ to solve its maximization problem in (2) for whether to purchase the cryptocurrency.
- Miner optimization: each miner chooses S_i at $t = 1$ to solve his maximization problem in (3).
- 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.

3 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 $t = 1$. 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 1 *In the perfect-information setting, the equilibrium exhibits the following properties:*

1. *Regardless of others' strategies, it is optimal for each household i to follow a cutoff strategy in its cryptocurrency purchase decision:*

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

2. *In the equilibrium, the cutoff A^* solves the following fixed-point condition:*

$$e^{(1-\eta_c)(A^*-A)+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\frac{\eta_c}{\sqrt{\tau_\varepsilon}}-\sqrt{\tau_\varepsilon}\left(A^*-A\right)\right)=e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}(A^*-A)-\xi-\log(1-\rho)} \quad (5)$$

   where $\Phi(\cdot)$ is the CDF function of normal distribution. There are either no equilibria when A or ξ is sufficiently small, or two equilibria with cutoffs $\underline{A}^*(A,\xi) < \bar{A}^*(A,\xi)$, respectively.

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

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

4. *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.*

Proposition 1 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 to enter the platform at $t = 1$. In this cutoff equilibrium, the cryptocurrency price is a correspondence

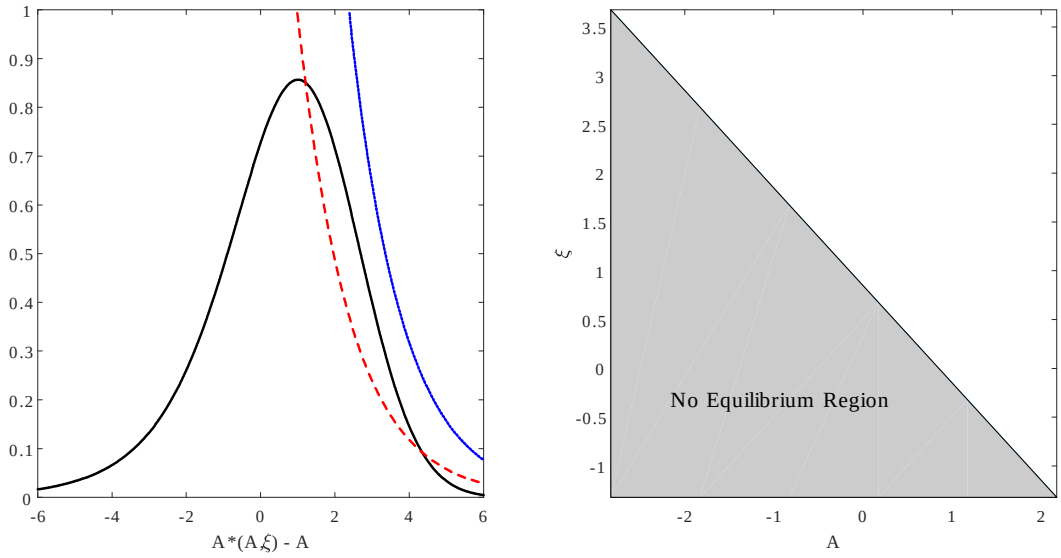

Figure 1: An illustration of equilibrium outcomes when platform fundamentals are observable. The left panel depicts the left-hand and right-hand sides of Equation (5), while the right panel depicts the region of no equilibria with respect to A and ξ.

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. We illustrate these possible outcomes by using a numerical example in Figure 1. Specifically, the left panel depicts the left-hand and right-hand sides of equation (5) against $A^* - A$, which determines the household population on the platform, by taking the values of A and ξ as given. The left-hand side (LHS) is the expected utility of a marginal household with endowment A^* from joining the platform. Note that the LHS has a bell-shaped curve with respect to $A^* - A$. For a given level of A, as A^* rises, the marginal household has a stronger transaction need, which in turn makes its expected utility from joining the platform higher. There is, however, a counter force from the network effect—the rising cutoff A^* reduces the household population on the platform, which makes it more difficult for the marginal household to find a trading partner and thus reduces its expected utility. The result of these offsetting effects is the bell-shaped curve with respect to $A^* - A$. Also note that taken $A^* - A$ as given (i.e., fixing the household population in the platform), the LHS is increasing with A, i.e., the marginal household's expected utility is increasing with the households' aggregate transaction need.

The right-hand side (RHS) is the price of buying the cryptocurrency and thus the cost of joining the platform. The price of the currency is decreasing with both $A^* - A$ and ξ, because the household population on the platform is decreasing with $A^* - A$ and because the miners' mining cost is decreasing with ξ. In this plot, the dotted line correspondes to the RHS with a lower value of ξ, while the lower, dashed line to a higher value of ξ.

Given the layout of these two curves, there may be no equilibria if the downward slopping line lies above the bell-shaped curve. This happens either when ξ is sufficiently small, which makes the RHS too high, or when A is sufficiently small, which makes the LHS too low. In other words, when either A or ξ is sufficiently small, no one enters the platform, making it undesirable even for households with the highest demand to enter. This ultimate failure of the platform emerges from the strong network effect in an environment where a single price is unable to clear simultaneously the demand and supply sides of the cryptocurrency.

The network effect plays a key role, as in the absence of the network effect the marginal household's expected utility would be an increasing curve with its transaction demand A^*, thus always intersecting with the RHS at a unique point. One may wonder in this situation with low aggregate demand from the households, why there cannot be an equilibrium with a high cutoff that leads to at least some households with strong demands on the platform. Such an equilibrium is not feasible because the low household participation on the platform implies a low currency price (determined by the small need for miners' transaction service on the supply side). The low price further implies a low cost to join the platform, which in turn leads to a large pool of households joining the platform, and which eventually invalidates the market clearing of the currency. The inability of the single currency price to accommodate the two sides, in particular with the strong network effect driving the demand side, is the key force driving the ultimate failure of the platform.

When the equilibria exist, there are two, as shown by Figure 1: one with a lower cutoff $\underline{A}^*$, in which a larger population enter the platform and thus a higher price, and one with a higher cutoff $\bar{A}^*$, in which few households enter the platform and thus a lower price.[12] This again occurs because of the strong network effect in the households' transactions on the platform. Households with the highest endowments always want to enter the platform but, if too few others enter, then the marginal benefit of trading on the platform is low, since the probability

[12] 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.

of meeting another household on the platform is low. This leads to a low price for the cryptocurrency. If instead many households enter, then the marginal benefit of entering the platform is high, sustaining a high price.[13] Proposition 1 also provides several comparative statics of the two equilibria. As a result of the nature of the two equilibria, they behave exactly the opposite along many dimensions. 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 occurs in the low price equilibrium in which the cryptocurrency price falls and less household join the platform.

The existence of multiple equilibria can help rationalize a wide spectrum of observed dynamics of different cryptocurrencies—large price swings, confusion and self-fulfilling traps that lead to their failure, while the potential for market failure can explain why most cryptocurrencies have little adoption and trade at low valuations, despite having similar features to more successful currencies. Furthermore, the absence of a stabilizing hand in cryptocurrencies also explains why large investors have an incentive to act like the so-called "coin whales", because our model implies that 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.[14]

To conclude this section, we compare the performance of the platform to a two-fee benchmark setting to demonstrate that it is the rigidity of the dual role of the ctyptocurrency price that is the source of the platform's fragility.

Two-Fee Platform Consider a conventional two-fee platform setting, in which the developer sets a membership fee Q for households to enter the platform. and a separate service fee F to compensate miners. With these two fees, the market clearing among households and miners imposes that the fee to miners needs to satisfy

$$F = e^{-\omega^*} = e^{-\xi - \sqrt{\frac{\tau_\varepsilon}{\tau_e}}(A^* - A)}, \tag{6}$$

where A^* again indexes the endowment of the marginal household that joins the platform. This equation determines the fee F from the household cutoff A^* based on the required

[13] 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).

[14] 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.

compensation for miners in order to service the population of households on the platform. The membership fee, Q, meanwhile, is again equal to the expected utility of the marginal household with endowment A^* :

$$Q = e^{(1-\eta_c)A^* + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - A^*}{\tau_\varepsilon^{-1/2}}\right). \tag{7}$$

Offering this price of membership ensures that households with endowments above A^* will join the platform, while those below will not. Consequently, the developer's choice of the two fees is equivalent to choosing A^*, with an objective of maximizing the profit from launching the platform:

$$\begin{aligned} \Pi_D &= \sup_{A^*} E\left[(Q - F)\, 1_{\{A \geq A^*\}}\right] \\ &= \sup_{\vartheta} \left(e^{(1-\eta_c)\tau_\varepsilon^{-1/2}\vartheta + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - \vartheta\right) - e^{-\xi - \tau_e^{-1/2}\vartheta}\right) \Phi\left(-\vartheta\right), \end{aligned} \tag{8}$$

where $\vartheta = \sqrt{\tau_\varepsilon}\,(A^* - A)$. Notice that, at $\vartheta = \infty$, $\Pi_D = 0$ since no households join the platform, while as $\vartheta \to -\infty$, $\Pi_D \to -\infty$ as the cost of supporting the platform explodes. Furthermore, since the profit from selling household membership is bounded from above, there exists a unique optimum and thus a unique equilibrium on this two-fee platform even when A and ξ are both small. This alternative setting thus demonstrates that the failure and multiplicity of equilibria of the original platform arise because the cryptocurrency price on the original platform cannot adjust to simultaneously satisfy the demand from households and the supply from miners.[15]

4 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

[15] 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.

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.

While the equilibrium cryptocurrency price is nonlinear, 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:

$$z = A - \sqrt{\frac{\tau_e}{\tau_\varepsilon}} \left(\xi - \bar{\xi}\right). \tag{9}$$

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.

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.[16]

[16] 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 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.

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

$$v = \tau_{\varepsilon}^{-1/2}\Phi^{-1}(V) + A^* = A + \tau_{\varepsilon}^{-1/2}\varepsilon_V, \tag{10}$$

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.[17]

To forecast the platform's demand fundamental A, each household's information set $\mathcal{I}_i$ now includes its own endowment A_i, the equilibrium cryptocurrency price P, and the volume signal V. Conditional on the public signals P and V, which are equivalent to their summary statistics z and v, the households hold the following common belief about the platform fundamental $A|z, v \sim \mathcal{N}(\hat{A}, \hat{\tau}_{A,c})$ with

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

Then, the households' common belief about the supply fundamental is

$$\hat{\xi} = E(\xi|z,v) = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}E(A - z|z,v) + \bar{\xi} = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(\hat{A} - z\right) + \bar{\xi}$$

Further conditional on its own endowment A_i, household i's private belief is given by

$$\begin{aligned} \hat{A}_i &= \hat{\tau}_A^{-1}\left(\hat{\tau}_{A,c}\hat{A} + \tau_\varepsilon A_i\right), \\ \hat{\tau}_A &= \tau_A + \tau_v + \frac{\tau_\varepsilon}{\tau_e}\tau_\xi + \tau_\varepsilon. \end{aligned} \tag{11}$$

By solving each household's cryptocurrency demand and clearing the aggregate demand 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 2 *When the platform fundamentals A and ξ are not publicly observable at $t = 1$, we have the following properties about the equilibrium: there are either no or two rational expectations equilibria, in which the following hold:*

[17] 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:*

$$\log P = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A - A^*\right) - \xi - \log\left(1-\rho\right), \tag{12}$$

where the cutoff A^* is a correspondence of the households' common belief $\hat{A}$ and $\hat{\xi}$, rather than A and ξ.

2. *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 $A^*\left(\hat{A}, \hat{\xi}\right)$ solves

$$\begin{aligned} & e^{\left(1-\eta_c\hat{\tau}_{A,c}\hat{\tau}_A^{-1}\right)\left(A^*-\hat{A}\right)+\hat{A}+\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}\left(A^*-\hat{A}\right)}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right) \\ = \; & e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A^*-\hat{A}\right)-\hat{\xi}-\log(1-\rho)} \end{aligned} \tag{13}$$

which has either no solutions or two solutions.

3. *There are no equilibria if $\hat{A}+\hat{\xi}$ is sufficiently low. It is sufficient, albeit unnecessary, that*

$$1 - \frac{1}{2}\eta_c + \frac{\tau_\varepsilon}{\hat{\tau}_{A,c}} - \sqrt{\frac{1}{4}\eta_c^2 + \frac{\hat{\tau}_{A,c}+\tau_\varepsilon}{\hat{\tau}_{A,c}+2\tau_\varepsilon}\tau_\varepsilon} > 0$$

for the linear boundary of the no-equilibrium region to expand as τ_v increases.

4. *When $\hat{A}+\hat{\xi}$ is sufficiently large, there are two 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 population 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 2 confirms even when the platform fundamentals A and ξ are not publicly observable, the equilibrium cryptocurrency price in (12) takes exactly the same log-linear form as in the perfect-information setting (Proposition 1). The only difference is the equilibrium cutoff A^* used by the households. With the fundamental variables A and ξ being unobservable, the households use the publicly observed price and volume signals z and v to

form common beliefs $\hat{A}$ and $\hat{\xi}$, which are the commonly perceived demand and supply fundamentals, respectively. Each household's private information about their own endowment allows it to further sharpen its private belief $\hat{A}_i$. The fixed-point condition in (13) is similar to (5) for the perfect-information setting, with a few key differences: $\hat{A}$ replaces A, $\hat{\xi}$ replaces ξ, and learning modifies various coefficients in the marginal household's expected utility on the left-hand side. Being the only difference in the equilibrium price correspondence from the perfect-information setting, the equilibrium cutoff $A^*\left(\hat{A}, \hat{\xi}\right)$ is the only channel through which informational frictions affect the market equilibrium.

As in the perfect-information setting, there are again either no or two equilibria. This situation arises from solving A^* from its fixed-point condition given in (13), which, like (5), may have either zero or two real solutions. There are no equilibria when the publicly perceived platform fundamentals $\hat{A}$ and $\hat{\xi}$ are sufficiently weak so that the marginal household's expected utility from joining the platform on the LHS, regardless the choice of the cutoff A^*, is strictly dominated by the cost of acquiring the cryptocurrency on the RHS.

When two equilibria exist, one has a lower equilibrium cutoff and a higher cryptocurrency price, while the other has a higher equilibrium cutoff and a lower price. Like in the perfect-information setting, these two equilibria again behave in opposite ways. Proposition 2 formally shows that in response to a shock to the volume signal, the equilibrium cutoff A^* and the cryptocurrency price P have opposite reactions across the two equilibria.

4.1 Impact of Information Frictions

We first examine how information frictions affect the boundary of the no-equilibrium region. Figure 2 depicts this boundary on a domain of $\hat{A}$ and $\hat{\xi}$ for three different values of τ_v, the precision of the volume signal. As τ_v increases from a finite value to ∞, the information frictions disappear as the volume signal fully reveals the demand fundamental. This plot shows several interesting features. First, the boundary for the platform failure has a slope of -1, which suggests that the platform fails when $\hat{A}+\hat{\xi}$ drops below a threshold, as formally shown by Proposition 2. Second, the platform failure boundary moves parallelly upward as τ_v increases, which shows that platform failure becomes more likely as information frictions dissipate. Information frictions, consequently, make platform failure less likely, and Proposition 2 provides a sufficient condition as to when this holds true more generally.

While this pattern may seem initially surprising, one can interpret it from the fixed-

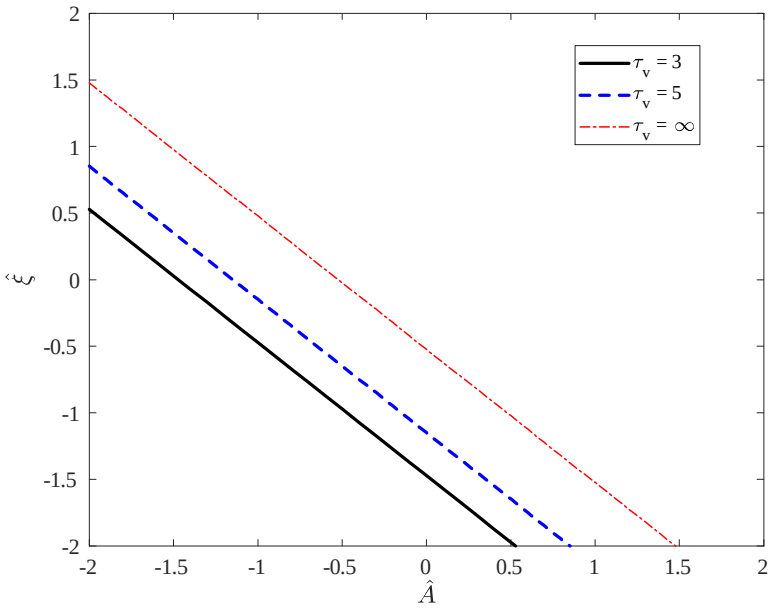

Figure 2: The boundary of the no-equilibrium region for different values of the volume signal τ_v

point condition in (13). Notice that the cost of joining the platform is independent of τ_v, while the marginal household's expected utility from joining the platform depends on it. Suppose now that τ_v falls, so that information frictions on the platform become more severe, and, for intuition, consider the value of the LHS when $A^* = \hat{A}$. As a result of increased information frictions, the marginal household faces greater uncertainty about A, which increases the marginal household's expected utility through two channels. First, the Cobb-Douglas utility implies that the household has a convex gain from transacting with other households on the platform, which rises with higher uncertainty, as reflected by the term $\frac{1}{2}\eta_c^2\hat{\tau}_A^{-1}$ in the exponential function. Second, the selection of households with transaction needs highly than the cutoff on the platform further convexifies the marginal household's gain from transaction on the platform, as reflected by the term $\eta_c\sqrt{\frac{1}{\tau_\varepsilon}+\frac{1}{\hat{\tau}_A}}$ in the Φ function. Since informational frictions raise the utility of the marginal household, this induces the entrance of more households for the same cryptocurrency price.

We now discuss how informational frictions affect the equilibrium cutoff A^* in a high-price or low-price equilibrium. Figure 3 depicts the response of the equilibrium cutoff $A^*\left(\hat{A},\hat{\xi}\right)$ to a shock to v, as measured by $\frac{\partial A^*}{\partial v}$, across the high-price and low-price equilibria. Note that such a shock has no effect on the equilibrium in the perfect-information setting. The figure shows that in the high-price equilibrium, the equilibrium cutoff A^* moves down in response

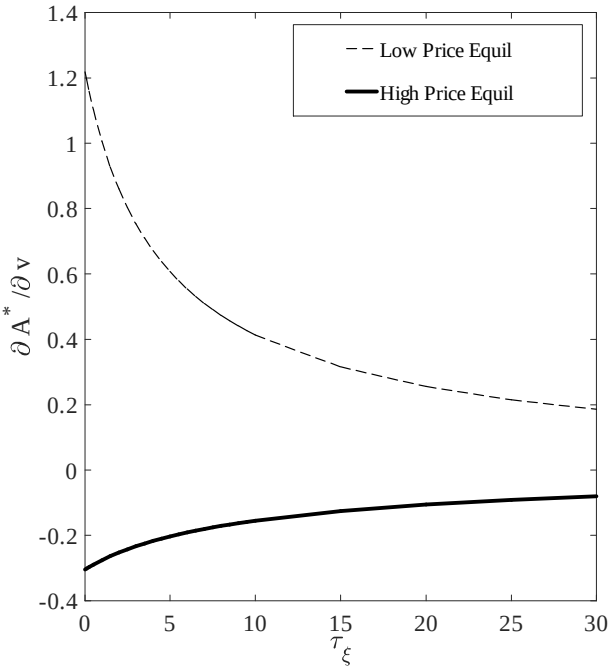

Figure 3: The equilibrium cutoff A^* with respect to the volume signal v in the high-price and low-price equilibria across different values of τ_ξ.

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 figure 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,[18] and is often studied only for its empirical predictions, as in, for instance, Wang (1994) and He and Wang (1995).[19] In our setting, households learn from both the price and volume of the cryptocurrency when

[18] 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.

[19] 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.

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.

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.[20] 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.

Our analysis of volume as a signal that drives household cryptocurrency demand also gives rise to several empirical predictions. First, since households learn from volume when choosing their demand, our model predicts that volume is a factor that helps explain the cross-section of cryptocurency prices, and consequently returns if investors are under-diversified. Second, large, non-fundamental swings in cryptocurrency prices would be accompanied by comparable swings in measures of platform activity, such as the number of active tokens in circulation or the volume of transactions on the blockchain ledger. Third, our model can rationalize the large cross-section of coins and tokens, in which the vast majority have trivial value, and furthermore, among similar platforms, those with stronger measures of volume command higher prices (conditional on the high-price equilibrium).

[20] 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. 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.

4.2 Incentives to Disclose Information

The instability endemic to decentralized digital platforms also shapes the incentives of the developer to disclose public information about the platform fundamentals. To illustrate this point, we proceed in the spirit of the Bayesian Persuasion literature, as in Aumann and Maschler (1995) and Kamenica and Gentzklow (2015). Specifically, we consider whether the developer would ex ante commit to disclosing a (potentially garbled) public signal about the demand fundamental once the platform is launched. Such a public signal can, for instance, be in the form of a beta testing by potential customers, publication of user reviews, or other financial disclosures about the platform. The premise of this analysis is that the developer can choose the precision of the signal, but cannot bias it.

As the space of potential messages by the sender (the developer) is unbounded, and there is a continuum of heterogeneously and privately informed receivers (households), our ability to characterize the optimal information structure is limited. To convey a basic insight about the developer's preference for disclosure, we examine how the developer's expected profit varies with the households' common belief $\hat{A}$, which is conditional on the public signals z and v. Note that households' private information would lead to dispersion in their private beliefs. Nevertheless, the Law of Large Number implies that the developer's expected profit is determined by the households' common belief $\hat{A}$. A key idea of the Bayesian Persuasion analysis is that if the developer's expected profit is convex with respect to $\hat{A}$, it would prefer to full information disclosure, as any disclosure makes the households' common belief $\hat{A}$ closer to the actual value of A, thus allowing the developer to profit more from the possible high values of A although not so much less from the possible low values. On the other hand, if the developer's expected profit is concave with respect to $\hat{A}$, it would prefer no disclosure.

Since the launch of the ICO can result in platform failure if the households' common posterior belief $\hat{A}$ is sufficiently low, the developer's expected payoff is nonconvex with respect to the households' common belief. This nonconvexity reduces the value of full disclosure, and may make the developer prefer no disclosure, especially when the households' common belief is close to the no-equilibrium region. We summarize this result in the following proposition.

Proposition 3 *When the platform is funded by an ICO, the developer prefers some opacity over full disclosure of platform fundamentals. If the probability of a low price equilibrium is sufficiently small, then the developer would prefer to pool low realizations of the demand fundamental near the boundary of the non-equilibrium region, and to be fully transparent for*

sufficiently high realizations.

While the developer benefits from some disclosure, our analysis suggests that it has incentive to withhold information, especially when the perceived fundamentals by the public are low. This result can rationalize the opacity widely observed in many ICOs.

5 Alternative Platform Arrangements

In this section, we consider two alternative arrangements for the decentralized digital platform. 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 show that the developer is always willing to disclose information when the platform is funded by an IPO. 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.

5.1 Initial Public Offering

In this subsection, we examine an alternative funding arrangement for the developer to launch the platform through a more traditional IPO based on the two-fee platform arrangement discussed in Section 3. Recall that as the developer sets two separate fees, one membership fee for households to join the platform and the other to compensate the miners, the increased flexibility from these two fees avoids the market failure of the ICO. In particular, this ability restores uniqueness of the rational expectations equilibrium and convexity to the developer's profit from the platform in the households' common belief about the demand fundamental. As a result, the developer has incentive to provide full transparency when disclosing relevant information about the platform to the public.

To illustrate this point, we further expand the two-fee platform arrangement in Section 3 by allowing the developer to securitize the platform's profit given in (8) as stock to a unit continuum of outside investors at a market value of S. In this IPO, the share issuance provides funding to the developer and the share price aggregates information among stock investors about the platform fundamentals. 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:

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

where $\epsilon_j \sim \mathcal{N}(0,1)$ 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, e.g., Goldstein, Ozdenoren, and Yuan (2013) and Albagli, Hellwig, and Tsyvinski (2014, 2015), 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 who take an aggregate stock position $2\Phi\left(\tau_\varphi^{1/2}\varphi\right)$, where $\varphi \sim \mathcal{N}(0,1)$ is a random variable.

It is intuitive that each investor optimally follows a cutoff strategy with a cutoff s^* of buying the stock if $s_j \geq s^*$, and short-selling if $s_j \leq s^*$. We then conjecture that the stock price S is determined by the expected platform profit by the marginal investors with a private signal equal to the cutoff s^*:

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

where s^* has to clear the market with the noise traders:

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

We assume that the developer has no private information, and chooses the service fee F in (6) and the membership fee Q in (7) based on the public information set, which includes the share price S, to maximize the platform's expected profit, so that there is no conflict of interest with shareholders.

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

Proposition 4 *When the two-fee platform is funded by an IPO, 1) the platform's equilibrium profit is given by (23) in the Appendix; 2) the stock price S takes the form given in (24), and is an increasing function of s^*; and 3) investors and households both follow their conjectured cutoff strategies.*

Proposition 4 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 cryptocurrency price, the stock price aggregates valuable information about the platform's fundamentals among stock investors, who are a different source of

information than platform participants. This is another important distinction between IPOs and ICOs in the presence of informational frictions.

The pricing flexibility of the two-fee platform ensures the stability of the platform and leads to a different incentive for the platform developer to disclose information to the public. We examine this incentive by following the Bayesian Persuasion analysis outlined in Section 4.2 and state the result in the following proposition.

Proposition 5 *When the two-fee platform is funded by an IPO, the developer prefers full disclosure of information relevant to the platform.*

Different from the ICO setting, Proposition 5 establishes that when funded by an IPO, the developer of a two-fee platform prefers full information disclosure. As the platform no longer faces the failure induced by the no-equilibrium outcome, the developer's profit is now strictly convex with respect to the households' common belief about the platform's demand fundamental. Consequently, it is to the developer's benefit to bring the households' common belief as close to the true value as possible, in contrast to the ICO setting.

5.2 Proof of Stake Protocol

In this subsection, we discuss an alternative Proof of Stake (PoS) consensus protocol for cryptocurrencies. 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 PoS protocol.[21] 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 (i.e., more intensive computing power of miners is required as the network grows). Our analysis shows that 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,

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

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 fee 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 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 in the forger's profit must be zero, and thus 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.[22] Consequently, $s = h\left(\frac{1-\theta}{\theta-\lambda} e^{\psi}\right)$. Since

[22] A corner solution in which all households buy the currency ($p_i = 0 \ \forall \ i$) 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.

the LHS satisfies

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

which attains its maximum as $s \to \infty$, $\frac{d\log LHS}{ds} \to 0$, 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

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

which is unique, given a choice of fee 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:

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

It then follows from the FONC that at an interior solution that the optimal $\theta = \frac{1+\lambda x}{1+x}$ satisfies:[23]

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

Since the LHS is monotonically increasing from $-\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}$ 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, there 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 market failure in the cryptocurrency. Since the price of the cryptocurrency scales with the expected transaction fees paid to forgers, it is

[23] 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.

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 PoS, 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 accounting services increases, i.e., 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 fee θ, which trades off participation by households on the platform with participation by forgers. With the PoS protocol, the developer no longer have to be concerned about the potential coordination failure among households, as it does with PoW. 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.

6 Conclusion

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. As a result of the rigidity induced by the dual roles of the cryptocurrency price in serving as a membership fee for households to join the platform and as a service fee for miners to provide transaction services on the platform, there exist either no equilibria or the two equilibria, which, if they exist, have disparate properties. This is in contrast to

alternative platform arrangements in which the developer sets separate fees for household membership and for compensating miners, such as with an IPO or with a Proof of Stake protocol, which ensures a unique equilibrium because of the flexibililty in pricing. The possibility of no equilibria (platform failure) with the ICO discourages the platform developer from voluntarily committing ex ante to disclose all relevant information about the platform to prospective participants. If instead the developer financed the platform with a traditional IPO, it would have incentive ex ante to disclose all relevant information about the platform.

References

Athey, Susan, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia (2016), Bitcoin Pricing, Adoption, and Usage: Theory and Evidence, mimeo Stanford University Graduate School of Business.

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.

Budish, Eric (2018), The Economic Limits of Bitcoin and the Blockchain, mimeo University of Chicago.

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.

Saleh, Fahad, (2018), Blockchain Without Waste: Proof-of-Stake, mimeo McGill University.

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 A Microfoundation of Goods Trading

In this appendix, we microfound the goods trading between two households when they are matched on the platform at $t = 2$. We assume that household i maximizes its utility by choosing its consumption demand $\{C_i, C_j\}$ through trading with its trading partner household j subject to its budget constraint:

$$\begin{aligned} U_i &= \max_{\{C_i, C_j\}} U(C_i, C_j; \mathcal{N}) \\ &\quad \text{such that } \; p_i C_i + p_j C_j = p_i e^{A_i}, \end{aligned} \tag{14}$$

where p_i is the price of its good. Similarly, household j solves a symmetric optimization problem for its trading strategy. We also impose market clearing for each household's good between the two trading partners:

$$C_i(i) + C_i(j) = e^{A_i} \quad \text{and} \quad C_j(i) + C_j(j) = e^{A_j}.$$

Furthermore, we assume that the endowments of both households A_i and A_j are publicly observable, regardless of whether the platform strength A is publicly observed at $t = 1$. Households behave competitively and take the prices of their goods as given.

Proposition 6 *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

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

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

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

Proposition 6 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 $C_j(i)$. 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.

Appendix B Proofs of Propositions

B.1 Proof of Proposition 1

When all households and miners observe A directly, there are no longer information frictions in the economy. From Proposition 6, 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:

$$e^{(1-\eta_c)A_i+\eta_c A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)=P,\ \text{with}\ \ A_i=A^* \tag{15}$$

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 (15) 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 $\Phi\left(-\sqrt{\tau_\varepsilon}\left(A^*-A\right)\right)$ enter the platform, and a fraction $\Phi\left(\sqrt{\tau_\varepsilon}\left(A^*-A\right)\right)$ 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 (4), there exists a critical value ω^* :

$$\omega^* = -\log P - \log\left(1-\rho\right), \tag{16}$$

such that miners with productivity $\omega_i \geq \omega^*$ mine the currency. Thus, a fraction $\Phi\left(-\sqrt{\tau_e}\left(\omega^*-\xi\right)\right)$ mine the currency on the platform. 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 monotonically increasing, we can invert the above market-clearing conditions, and impose equation (16) to arrive at

$$\log P = \sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A-A^*\right)-\xi-\log\left(1-\rho\right). \tag{17}$$

By substituting for P in equation (15), we obtain an equation to determine the equilibrium cutoff $A^* = A^*\left(A,\xi\right)$:

$$e^{(1-\eta_c)(A^*-A)+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)=e^{\sqrt{\frac{\tau_\varepsilon}{\tau_e}}(A-A^*)-\xi-\log(1-\rho)}. \tag{18}$$

We can rewrite equation (18) as

$$e^{\left(1-\eta_c+\sqrt{\tau_\varepsilon/\tau_e}\right)s}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-\frac{s}{\tau_\varepsilon^{-1/2}}\right)=e^{-A-\xi-\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}-\log(1-\rho)}, \tag{19}$$

where $s = A^* - A$ determines the population that buys the currency. Notice that the LHS of equation (19) 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 (19) 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 (19) is fixed, it follows that the LHS and RHS of equation (19) 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 (19) 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 (19) 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:

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

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:

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

Uniqueness of the rational expectations equilibrium that we have characterized follows from the cutoff strategies being the unique solution to the respective optimization problems of households and miners. To see this, consider the problem of household i when all other households follow arbitrary strategy profiles. As the allocation at $t=2$ is unique, it follows that household i joins the platform if $E\left[U_i\,|\mathcal{I}_i\right] = E\left[e^{(1-\eta_c)A_i+\eta_c A_j}\,|\mathcal{I}_i, i\in\mathcal{N}\right]$ exceeds the membership price P.

Since household i is atomistic, it follows that $E\left[U_i\,|\mathcal{I}_i\right] = e^{(1-\eta_c)A_i}E\left[e^{\eta_c A_j}\mid A, i\in\mathcal{N}\right]$, where $E\left[e^{\eta_c A_j}\mid A, i\in\mathcal{N}\right]$ is independent of A_i. It then follows that household i will follow a cutoff strategy that is mononotonic in its own type A_i. As such, all households for which $A_i \geq \log P - \log E\left[e^{\eta_c A_j}\mid A, i\in\mathcal{N}\right]-(1-\eta_c)$ will join the platform. Similarly, those households for which A_i is below the threshold will exit or refrain from joining the platform. Iterating on this algorithm, when households reoptimize from the conjectured equilibrium, the resulting equilibrium that survives the iterated elimination of dominated strategies is the cutoff equilibrium. In addition, miners, regardless of their beliefs about A, will follow a cutoff strategy in deciding whether to mine. Consequently, it is the unique rational expectations equilibrium.

B.2 Proof of Proposition 2

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 6, 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

$$e^{(1-\eta_c)A_i+\eta_c\hat{A}_i+\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\hat{A}_i+\eta_c\hat{\tau}_A^{-1}-A^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right) = P \quad \text{with} \quad A_i = A^*. \tag{20}$$

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, $A^* = A^*\left(\log P, v\right)$.

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 (16) for the minor's critical level ω^* to arrive at

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

Given the definition of z in (9), we have

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

In this form, z is indeed a summary statistic of $\log P$.

By substituting in P and $\hat{A}_i$ from (11), we can express equation (20) as

$$\begin{aligned}
& e^{\left(1-\eta_c\hat{\tau}_{A,c}\hat{\tau}_A^{-1}\right)\left(A^*-\hat{A}\right)+\hat{A}+\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}\left(A^*-\hat{A}\right)}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right) \\
= \quad & e^{-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(A^*-\hat{A}\right)-\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\left(\hat{A}-z\right)-\bar{\xi}-\log(1-\rho)}
\end{aligned} \tag{21}$$

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

$$\begin{aligned}
& e^{\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}\right)s}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\eta_c\hat{\tau}_A^{-1}-\frac{\tilde{\tau}_{A,c}}{\hat{\tau}_A}s}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\right) \\
= \quad & e^{\left(\frac{\tau_A+\tau_v}{\hat{\tau}_{A,c}}\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\frac{\frac{\tau_\varepsilon}{\tau_e}\tau_\xi}{\hat{\tau}_{A,c}}\right)z-\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)\frac{\tau_v}{\hat{\tau}_{A,c}}v-\bar{\xi}-\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}\right)\frac{\tau_A}{\hat{\tau}_{A,c}}\bar{A}-\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)-\log(1-\rho)}.
\end{aligned} \tag{22}$$

Similar arguments to those in the proof of Proposition 1 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 (22) 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.

Rewriting equation (22) as equation (13) given in the statement of the proposition, the condition for non-existence can be expressed as:

$$\hat{A}+\hat{\xi}\leq-\log\max_s\left\{e^{\left(1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}}-\eta_c\hat{\tau}_{A,c}\hat{\tau}_A^{-1}\right)s+\frac{1}{2}\eta_c^2\left(\hat{\tau}_A^{-1}+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}s}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)\right\}-\log\left(1-\rho\right),$$

since this is when the RHS of equation (13) is above the hump-shaped curve of the LHS, preventing markets from equilibrating. It follows that the non-existence region is separated by the line $\hat{A} = h(\tau_v) - \hat{\xi}$, where we have parameterized the intercept by τ_v as our measure of the degree of informational frictions on the platform. As $\tau_v \nearrow \infty$, the platform converges to its perfect-information benchmark.

Let $\bar{s}(\tau_v)$ be the argument that maximizes the above objective. Invoking the Envelope Theorem on the intercept, $h(\tau_v)$:

$$\begin{aligned}\frac{d\log h(\tau_v)}{d\tau_v} &= -\left(\eta_c\tau_\varepsilon\hat{\tau}_A^{-2} + \frac{\left(\frac{3}{2}+\frac{1}{2}\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)\hat{\tau}_A^{-2}}{\left(\frac{1}{\tau_\varepsilon}+\frac{1}{\hat{\tau}_A}\right)^{3/2}}\frac{\phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}\bar{s}}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)}{\Phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}\bar{s}}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)}\right)\bar{s} \\ &\quad -\frac{1}{2}\eta_c^2\hat{\tau}_A^{-2} - \frac{1}{2}\frac{\eta_c\hat{\tau}_A^{-2}}{\sqrt{\frac{1}{\tau_\varepsilon}+\frac{1}{\hat{\tau}_A}}}\frac{\phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}\bar{s}}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)}{\Phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}\bar{s}}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)}.\end{aligned}$$

The second two terms are negative, while it is sufficient for $\bar{s} \geq 0$, for the $\frac{d\log h(\tau_v)}{d\tau_v} < 0$. The FONC from the above program, assuming an interior $s > -\infty$, is:

$$1 - \eta_c\hat{\tau}_{A,c}\hat{\tau}_A^{-1} - \frac{\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\frac{\phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}s}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)}{\Phi\left(\frac{\eta_c\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)-\frac{\tau_\varepsilon\tilde{\tau}_{A,c}}{\hat{\tau}_A}s}{\sqrt{\tau_\varepsilon\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_A}\right)}}\right)} = 0.$$

Since the objective is hump-shaped in s, we require that the LHS of FOC, evaluated at $s = 0$, is positive. Invoking that $\frac{\phi(-x)}{\Phi(x)} < \frac{-x}{2} + \frac{\sqrt{x^2+4}}{2}$ for the hazard rate of the normal distribution, it follows that it is sufficient that:

$$1 - \frac{1}{2}\eta_c\hat{\tau}_{A,c}\hat{\tau}_A^{-1} - \hat{\tau}_{A,c}\hat{\tau}_A^{-1}\sqrt{\frac{1}{4}\eta_c^2 + \frac{\tau_\varepsilon\hat{\tau}_A}{\tau_\varepsilon+\hat{\tau}_A}} > 0,$$

which we can rewrite as:

$$1 - \frac{1}{2}\eta_c + \frac{\tau_\varepsilon}{\hat{\tau}_{A,c}} - \sqrt{\frac{1}{4}\eta_c^2 + \frac{\hat{\tau}_{A,c}+\tau_\varepsilon}{\hat{\tau}_{A,c}+2\tau_\varepsilon}\tau_\varepsilon} > 0.$$

If this condition is satisfied, then $\frac{d\log h(\tau_v)}{d\tau_v} < 0$, and the intercept shrinks as τ_v increases. Consequently, the non-existence region shrinks as informational frictions dissipate on the platform.

Note now that, since the RHS of equation (21) 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 similar arguments to the proof in the perfect-information settings. 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.

B.3 Proof of Proposition 3

To understand the value of information disclosure to the developer, we first characterize the shape of its payoff profile in each of the three possible equilibrium outcomes, high price, low price, and nonexistant, realization-by-realization for (z, v). Before each household uses its private signal, the households' common belief conditional on the public signals is $A|z, v \sim \mathcal{N}\left(\hat{A}, \hat{\tau}_{A,c}\right)$. While private signals lead to dispersed beliefs among the households around the common belief $\hat{A}$, the Law of Large Numbers implies that the developer's profit is determined by the households' common belief. Thus, we examine how the developer's expected profit varies with $\hat{A}$.

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

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

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

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

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 2:

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

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 1, $\frac{d^2b}{d\hat{A}^2} \leq 0$, and we focus on the coefficient of the $\left(\frac{db}{d\hat{A}}\right)^2$ term. Notice the coefficient of the $\left(\frac{db}{d\hat{A}}\right)^2$ term goes 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 value, $b^* = -\left(1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}\right)\sqrt{\frac{1}{\tau_\varepsilon\tau_e}} \pm \sqrt{\frac{1+\frac{\tau_\varepsilon}{\hat{\tau}_{A,c}}}{\tau_\varepsilon}}$. 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 with respect to $\hat{A}$, which is satisfied for $\tau_e < 1$.[24] Consequently, it is possible for the developer's profit to be strictly convex in the low price equilibrium for τ_e being 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

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

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 $1+\sqrt{\frac{\tau_\varepsilon}{\tau_e}} - \eta_c\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A} = \frac{\frac{\hat{\tau}_{A,c}}{\hat{\tau}_A}\tau_\varepsilon^{-1/2}}{\sqrt{1+\frac{\tau_\varepsilon}{\hat{\tau}_A}}}\frac{\phi(x)}{\Phi(x)}$, then $\frac{d^2E[\Pi_D \mid z,v]}{dA^{*2}} \to -\infty$.[25]

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.

[24] 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.

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

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 nonconvexity for low realizations of (z, v) at the critical boundary at which equilibria begin to exist. This is reflected in the shape of the payoff profile in the high price equilibrium, which 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 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.

To provide some characterization of the optimal disclosure policy, we begin by assuming full transparency by the developer and then modifying the disclosure policy. When A is perfectly revealed to households, then there exists a critical A_{crit} below which an equilibrium fails to exist, and the developer's profit is locally a step function. Suppose, for now, that only the high price equilibrium realizes on the platform.

Consider a window $(A_{crit} - \varepsilon, A_{crit} + \varepsilon)$ for $\varepsilon > 0$. Suppose that the developer chooses to bundle all realizations in this window into a coarser disclosure policy, with probability measure d. In doing so, the developer trades off the increased likelihood of a successful launch at a distorted level of revenue, $\int_{A_{crit}-\varepsilon}^{A_{crit}+\varepsilon} P(A, \xi)\, \Phi(A)\, d\Phi^d(A)$ against the lost profit for realizations of A above the A_{crit}, $\int_{A_{crit}}^{A_{crit}+\varepsilon} P(A, \xi)\, \Phi(A)\, d\Phi(A)$:

$$\Delta\Pi_D = \int_{A_{crit}-\varepsilon}^{A_{crit}+\varepsilon} P(A, \xi)\, \Phi(A)\, d\Phi^d(A) - \int_{A_{crit}}^{A_{crit}+\varepsilon} P(A, \xi)\, \Phi(A)\, d\Phi(A).$$

Then, for small enough ε, we can approximate $\Delta\Pi_D$ to first-order terms:

$$\Delta\Pi_D \approx P\left(\tilde{A}, \xi\right) \Phi\left(\tilde{A}\right) \left(\phi(A_{crit} + \varepsilon) + \phi(A_{crit} - \varepsilon)\right) \varepsilon - P(A_{crit} + \varepsilon, \xi)\, \Phi(A_{crit} + \varepsilon)\, \phi(A_{crit} + \varepsilon)\, \varepsilon.$$

Since $P(A, \xi)\, \Phi(A)$ around the critical value is locally strictly concave above the critical point, one has that:

$$P\left(\tilde{A}, \xi\right) \Phi\left(\tilde{A}\right) > \frac{\phi(A_{crit} + \varepsilon)}{\phi(A_{crit} + \varepsilon) + \phi(A_{crit} - \varepsilon)} P(A_{crit} + \varepsilon, \xi)\, \Phi(A_{crit} + \varepsilon),$$

from which follows that:

$$\Delta\Pi_D > 0,$$

and the developer benefits from bundling states near the critical threshold. By continuity, this analysis also applies for low realizations locally away from the critical threshold. Similarly, for a sufficiently far away from the critical value, Π_D is locally convex in the households' posterior mean belief, and therefore

$$\begin{aligned} P\left(\tilde{A},\xi\right)\Phi\left(\tilde{A}\right) \;\leq\; & \frac{\phi\left(a+\varepsilon\right)}{\phi\left(a+\varepsilon\right)+\phi\left(a-\varepsilon\right)}P\left(a+\varepsilon,\xi\right)\Phi\left(a+\varepsilon\right) \\ & +\frac{\phi\left(a-\varepsilon\right)}{\phi\left(a+\varepsilon\right)+\phi\left(a-\varepsilon\right)}P\left(a-\varepsilon,\xi\right)\Phi\left(a-\varepsilon\right), \end{aligned}$$

from which follows that $\Delta\Pi_D \leq 0$. As such, the developer does not benefit from opacity where the profit function is locally convex. For A sufficiently high, the profit function is strictly convex and $\Delta\Pi_D < 0$.

Taken together, the developer has incentive to pool together low states of the demand fundamental near the critical threshold for nonexistence, and to be fully transparent for sufficiently high realizations, where the profit function is locally convex.

In the above, we assumed that only the high price equilibrium realizes on the platform. Our results hold as long as the probability of a low price equilibrium is sufficiently small that the profit function remains strictly concave near the critical threshold, and convex for high realizations of A.

B.4 Proof of Proposition 4

We first analyze the decisions of the developer to choose the miner fee F and the membership fee Q. As we discussed earlier in Section 3, these decisions are equivalent to choosing the marginal investor A^*, as given in (6) and (7), based on the available public information, which includes the publicly observed stock price S. Suppose that S is an invertible function of the marginal investor's signal s^*. Then, the posterior belief conditional on the public signal S is Gaussian $\mathcal{N}\left(\hat{A},\hat{\tau}_{A,D}\right)$, where:

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

Household i, given its information set $\{A_i, s^*, \omega^*, \xi\}$, form its expectations about the platform demand fundamental, A. Since household i observes A^*, it knows ω^*, ξ, and the

fraction of the population that will enter the platform. It will join the platform if the membership fee Q is below its reservation price Q_i:

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

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

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

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

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

we can then express the developer's program as

$$\Pi_D^{IPO} = \sup_w\left(\frac{e^{\hat{A}-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)\tau_\varepsilon^{-1/2}w+\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}+\tau_\varepsilon}\right)^2\hat{\tau}_{A,D}^{-1}+\frac{1}{2}\eta_c^2\left(\left(\hat{\tau}_{A,D}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}}-e^{\tau_e^{-1/2}w-\xi}\right)\Phi(w). \tag{23}$$

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

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

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 when the platform fundamentals are sufficiently strong; otherwise the trivial equilibrium is the only equilibrium.[26] 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

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

[26] In contrast to the ICO, the Envelope Condition reveals that not only is the developer's expected profit continuous in the platform fundmamentals, it is continuously differentiable in them.

which we can express as

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

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

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

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

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

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

$$S = \left(\frac{e^{\bar{A}+\left(\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\frac{\tau_s}{\hat{\tau}_{A,D}}\frac{\tau_A}{\hat{\tau}_{A,D}}+\frac{\tau_s\tau_\varphi^{-1}}{\hat{\tau}_{A,D}}\right)\left(A-\bar{A}+\sqrt{\frac{\tau_\varphi}{\tau_s}}\varphi\right)-\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)\tau_\varepsilon^{-1/2}w}}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{w}{\tau_\varepsilon^{-1/2}}\right)^{-1}e^{-\frac{1}{2}\left(1-\frac{\eta_c\hat{\tau}_{A,D}}{\hat{\tau}_{A,D}}\right)^2\left(\hat{\tau}_{A,D}+\tau_s\right)^{-1}-\frac{1}{2}\eta_c^2\left(\left(\tau_A+\tau_s\tau_\varphi^{-1}+\tau_\varepsilon\right)^{-1}+\tau_\varepsilon^{-1}\right)}}-e^{\tau_e^{-1/2}w-\xi}\right)\Phi\left(w\right). \tag{24}$$

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.

B.5 Proof of Proposition 5

We consider the developer's expected profit from the IPO with respect to the households' common belief $\hat{A}$. Differentiating (23) with respect to $\hat{A}$ at its optimum twice, and invoking the envelope condition, we have

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

since $\frac{dw}{d\hat{A}} \geq 0$ from the proof of Proposition 4. Thus, the developer's expected profit is strictly convex in $\hat{A}$.

B.6 Proof of Proposition 6

The first order conditions of household i's optimization problem in (14) respect to $C_i(i)$ and $C_j(i)$ at an interior point are:

$$C_i(i) \quad : \quad \frac{1-\eta_c}{C_i(i)}U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_i, \tag{25}$$

$$C_j(i) \quad : \quad \frac{\eta_c}{C_j(i)}U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_j, \tag{26}$$

where θ_i is the Lagrange multiplier for the budget constraint. Rewriting (26) as

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

Dividing equations (25) 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 (14), 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 (25) also gives the price of the good produced by household i. Since the household's budget constraint in (14) 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:

$$p_i=\frac{1-\eta_c}{C_i(i)}U\left(C_i(i),C_j(i);\mathcal{N}\right)=e^{\eta_c(A_j-A_i)}. \tag{27}$$

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:

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

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:

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

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

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

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