NBER WORKING PAPER SERIES

A MODEL OF CRYPTOCURRENCIES

Michael Sockin
Wei Xiong

Working Paper 26816
http://www.nber.org/papers/w26816

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
March 2020

We thank An Yan for a comment that led to this paper, and Will Cong, Haoxiang Zhu, Aleh Tsyvinski, and seminar participants at ITAM, NBER Asset Pricing Meeting, NBER Summer Institute, Tsinghua, UBC, UNC, and Yale for helpful comments. The views expressed herein are those of the authors and do not necessarily reflect the views of the National Bureau of Economic Research.

A Model of Cryptocurrencies
Michael Sockin and Wei Xiong
NBER Working Paper No. 26816
March 2020
JEL No. G19

ABSTRACT

We model a cryptocurrency as membership in a decentralized digital platform developed to facilitate transactions between users of certain goods or services. The rigidity induced by the cryptocurrency price having to clear membership demand with supply of token by speculators, especially with strong complementarity in membership demand, can lead to market breakdown. While user optimism mitigates the market fragility by increasing user participation, speculator sentiment exacerbates it by crowding users out. Informational frictions attenuate the risk of breakdown by dampening price volatility and platform performance. Furthermore, the users' anticipation of losses from strategic attacks by miners exacerbates the market fragility.

Michael Sockin
Department of Finance
UT Austin McCombs School of Business
Austin, TX 78712
michael.sockin@mccombs.utexas.edu

Wei Xiong
Princeton University
Department of Economics
Bendheim Center for Finance
Princeton, NJ 08450
and NBER
wxiong@princeton.edu

The rapid growth of the cryptocurrency market in the last few years promises a new funding model for innovative digital platforms. Rampant speculation and volatility in the trading of many cryptocurrencies, however, have also raised substantial concerns that associate cryptocurrencies with 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, particularly highlights the risks and fragility of cryptocurrencies. Understanding the risks and potential benefits of cryptocurrencies requires a systematic framework that incorporates several integral characteristics of cryptocurrencies—their roles in funding digital platforms and in serving as investment assets of speculators, and their integration of blockchain technology with decentralized consensus protocols to record transactions on the platforms. We develop such a model in this paper.

Specifically, our model analyzes the properties of utility tokens, a subset of cryptocurrencies along with coins and security tokens. Utility tokens are native currencies accepted on decentralized digital platforms that often provide intrinsic benefit to participants.[1] The benefits of utility tokens can range from provision of secure and verifiable peer-to-peer transaction services to the maintenance of smart contracts. 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 contents. The development of these platforms is financed by the sale of tokens to investors and potential users through the issuance of utility tokens.

In our model, 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 users by using a blockchain technology. Users face difficulty in making such transactions outside the platform as a result of severe search frictions. The value of the platform, consequently, lies with its design in filling the users' transaction needs, and in its capability in pooling together a large number of users with the need to transact with each other. We

[1] 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. 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.

model a user's transaction need by its endowment in a consumption good, and its preference of consuming its own good together with the goods of other users. As a result of this preference, users need to trade goods with each other, and the platform serves to facilitate such trading. Specifically, we assume that, when two users 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 user's desire to join the platform grows with the number of other users on the platform and the size of their goods endowments.

In addition to serving as the membership to transact goods with other users, the cryptocurrency in our model is also an investable asset—for both users and speculators with no transaction needs—to capitalize on the future growth of the platform. To systematically analyze these dual roles, our model features an infinitely many periods, with users and speculators holding different beliefs about the capital gain from investing in the token issued by the platform. In each period, a new generation of users choose whether to join the platform by purchasing the tokens, partly from users of the previous period and partly from new token issuance, which follows a deterministic schedule. In making its decision, each user trades off the cost of buying a token with the benefits from transacting goods on the platform and from the expected token price appreciation. We show that each user optimally adopts a cutoff strategy to join the platform by purchasing the token only if its goods endowment is higher than a threshold. The threshold and the token price are jointly determined by the users' common goods endowment and optimism about the token price appreciation, which determine the users' token demand, and the speculators' sentiment about the token price appreciation, which determines the supply of tokens to users.

We analyze the equilibrium in two settings, one with perfect information and the other with realistic informational frictions. In the latter setting, the platform's demand fundamental (i.e., the users' common goods endowment) is unobservable and each user uses its own goods endowment as private information and other public signals, including the token price, to infer the demand fundamental. In both of these settings, despite the inherent nonlinearity induced by each user's cutoff strategy for joining the platform, we are able to derive a tractable token price function and an analytical equilibrium condition for each user's participation threshold in each period, which allow us to systematically characterize the token market equilibrium.

As a result of the network effect—if more users join the platform, each user benefits

more from joining the platform and is thus willing to adopt a lower participation threshold and pay a higher token price—the token market may break down under certain conditions. That is, there may not exist any equilibrium price to clear the users' token demand with the token supply. In particular, the token market breaks down if the platform's demand fundamental is sufficiently low or if the speculators' sentiment is sufficiently high. Interestingly, users' optimism about the token price appreciation mitigates the fragility of the token market by inducing them to join the platform even when the benefits of trading their endowments are low, while the speculators' sentiment exacerbates the fragility by raising the users' participation cost and crowding them out.

Since the supply of tokens increases deterministically over time, the platform exhibits life-cycle effects that are governed by the substitution of the token's current convenience yield and expected capital gains, which jointly determine the total token return to each user. The inflation of the token base over time lowers expected capital gains by shifting out the token supply curve. Consequently, the region of market breakdown and the relative weight of the convenience yield in the total token return increase over time. Both of these effects in turn raise the sensitivity of the user base to the current demand fundamental and log token price volatility over time.

Our analysis also shows that informational frictions attenuate the token market fragility by dampening the responses of the users' beliefs to fundamental shocks. This dampening effect is particularly strong in our dynamic setting as each user needs to forecast the expectations of future users, leading to a bias reminiscent of Allen, Morris and Shin (2006), even though our setting is highly nonlinear. Furthermore, informational frictions dampen platform performance because the equilibrium token price is a convex function of the users' common belief of the platform's demand fundamental, following the Bayesian persuasion arguments of Aumann and Maschler (1995) and Kamenica and Gentzkow (2011).

We also extend the model to incorporate miners who follow the Proof of Work protocol to provide accounting and custodial services to record transactions on the platform's blockchain. Each miner incurs a computational cost in providing the service, and is compensated by the seignorage from token inflation, which diminishes deterministically over time, and a transaction fee, which is a fraction of the transaction surplus of the users on the platform. This tradeoff determines the number of miners on the platform. When the number of miners falls sufficiently low, some corrupt miners may choose to attack the cryptocurrency so that

they can gain from creating fraudulent seignorage and stealing other miners' transaction fees. While such attacks do not directly lead the platform to fail, our analysis shows that the users' anticipation of future losses from miner attacks may exacerbate the fragility of the token market, especially when the mining cost is high.

Our framework provides a rich set of empirical predictions for token price appreciation, which is directly measurable by the econometrician and thus the focus of most empirical studies. As only part of users' token return, the expected token price appreciation is determined by the marginal user's equilibrium condition—as the total cost of capital and participation minus the convenience yield from transaction surplus. Consistent with Liu and Tsyvinski (2019), our model predicts a role for both news and investor sentiment in explaining the time series of cryptocurrency price appreciation, not through risk premia but rather by predicting the marginal user's convenience yield. In addition, our model can rationalize the momentum patterns that they observe in token price appreciation, through persistence of user participation costs and convenience yields, as well as the size effect that Liu, Tsyvinski, and Wu (2019) show in the cross-section of cryptocurrency price appreciation.

Our paper contributes to the emerging literature on cryptocurrencies. Easley, O'Hara, and Basu (2019) 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) model 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) investigate the tradeoff of smart contracts in overcoming adverse selection while also facilitating oligopolistic collusion, while Biais et al (2019) 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 (2019) study the role of monetary policy in the presence of a cryptocurrency that acts as a private fiat currency.

Biais et al (2018) develop a structural model of cryptocurrency pricing with transactional benefits and costs from hacking and estimate the model with data on Bitcoin. Our model shares a similar pricing model, but differs by deriving a strong network effect in the transactional benefits of cryptocurrency, as well as subtle interactions between the strategic

attacks by miners and the fragility of the cryptocurrency. Cong, Li, and Wang (2018) also emphasize the strong network effect in platform users by constructing 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. Our model differs from theirs in microfounding the network effect, in highlighting the fragility of the platform induced by the rigidity of the token price in clearing the users' token demand under the network effect with the token supply, and in showing that miner attacks may exacerbate the platform fragility through the users' anticipation of losses from future attacks. This effect of miner attacks on platform stability overlaps with the analysis of Pagnotta and Buraschi (2018) and Pagnotta (2018), who develop an equilibrium framework for Bitcoin with a focus on the interaction between the network of users and the investment of miners into network security. While their analysis shows that this interaction can amplify the volatility of Bitcoin price, they do not address the platform fragility induced by the users' network effect.

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. Furthermore, Goldstein, Ozdenoren, and Yuan (2013) investigate feedback effects of learning on firm investment decisions, Albagli, Hellwig, and Tsyvinski (2014a, 2015) focus on the role of asymmetry in security payoffs in distorting asset prices and firm investment incentives, and Gao, Sockin, and Xiong (2018) analyze the distortion of informational frictions in housing markets. Like our model, Albagli, Hellwig, and Tsyvinski (2014b) also investigate how dispersed information in a dynamic setting impacts asset prices with non-linear payoffs, yet their emphasis is on explaining the overpricing of downside risk in bond markets. In contrast, our model examines how informational frictions, operating through a Keynesian Beauty Contest, dampen cryptocurrency platform performance when the convenience yield of the platform is endogenously formed by its users.

1 The Model

Consider a cryptocurrency, which serves as the membership to a digital platform with a pool of users who share a certain need to transact goods with each other. The platform serves to reduce search frictions among these users. The benefits to participating on a utility token platform, such as Ether or FileCoin, include securing transactions and writing smart

contracts to sharing in gaming content and providing secure file storage. As the value of the token may appreciate with the development of the platform over time, it also serves as an investable asset for users and speculators to speculate about the growth of the platform.

The model is discrete time with infinitely many periods: $t = 1, 2, ...$ There are three types of agents on the platform: users, speculators, and an owner. The success of the cryptocurrency is ultimately determined by whether the platform can gather a large number of users together. In each period, a new generation of users purchase the cryptocurrency as the membership to join the platform, and then are randomly matched with each other to transact their goods endowments. We choose this specific form of gains from trade to facilitate analysis within a standard trade framework. The goods transactions are supported by the owner of the decentralized platform who acts as a service provider and completes all user transactions. It records these transactions in an indelible ledger called the blockchain. Since the owner can add and modify records, or blocks, on the blockchain, the blockchain is called a permissioned blockchain. We will extend the model in Section 4 to incorporate decentralized miners, who follow the Proof of Work protocol to record transactions on a public blockchain. Although the model features overlapping generations of users and speculators, the setting is nonstationary because the demand fundamental follows a random walk and the supply of available tokens is deterministically increasing over time.

1.1 Users

There are overlapping generations of users that join the platform. In each period t, there is a pool of potential users, indexed by $i \in [0, 1]$. These potential users have needs to transact goods with each other. Each of them may choose to purchase a unit of the cryptocurrency, which we call a token of the platform, in order to participate on the platform. We can divide the unit interval into the partition $\{\mathcal{N}_t, \mathcal{O}_t\}$ in each period, with $\mathcal{N}_t \cap \mathcal{O}_t = \varnothing$ and $\mathcal{N}_t \cup \mathcal{O}_t = [0, 1]$. Let $X_{i,t} = 1$ if user i purchases the token, i.e., $i \in \mathcal{N}_t$, and $X_{i,t} = 0$ if he chooses not to purchase. An indivisible unit of currency is commonly employed in search models of money, such as Kiyotaki and Wright (1993). If user i at $t = 1$ chooses to purchase the token, it purchases one unit at the equilibrium price P_t, denominated in the consumption numeraire. In the next period $t + 1$, each user from period t resells his token to future users and to speculators.

In each period, user i is endowed with a certain good and is randomly paired with a

potential trading partner, user j, who is endowed with another good. Users i and j can transact with each other only if both have the token. After their transaction, user i has a Cobb-Douglas utility function over consumption of his own good and the good of user j according to

$$U_{i,t}\left(C_{i,t}, C_{j,t}; \mathcal{N}_t\right) = \left(\frac{C_{i,t}}{1-\eta_c}\right)^{1-\eta_c} \left(\frac{C_{j,t}}{\eta_c}\right)^{\eta_c}, \tag{1}$$

where $\eta_c \in (0,1)$ represents the weight in the Cobb-Douglas utility function on his consumption of his trading partner's good $C_{j,t}$, and $1-\eta_c$ is the weight on consumption of his own good $C_{i,t}$. A higher η_c means a stronger complementarity between the consumption of the two goods. Both goods are needed for the user to derive utility from consumption. If one of them is not a member of the platform, there is no transaction. As a result, each of them gets zero utility in the absence of a transaction. This setting implies that each user cares about the pool of users on the platform, which determines the probability of completing a transaction.

The goods endowment of user i is $e^{A_{i,t}}$, where $A_{i,t}$ is comprised of a component A_t common to all users and an idiosyncratic component $\varepsilon_{i,t}$:

$$A_{i,t} = A_t + \tau_{\varepsilon}^{-1/2}\varepsilon_{i,t},$$

with $\varepsilon_{i,t} \sim \mathcal{N}(0,1)$ being normally distributed and independent with each other, across time, and from A_t. We assume that $\int \varepsilon_{i,t} d\Phi\left(\varepsilon_{i,t}\right) = 0$ at each date by the Strong Law of Large Numbers. The aggregate endowment A_t follows a random walk with a constant drift $\mu \in \mathbb{R}$:

$$A_t = A_{t-1} + \mu + \tau_A^{-1/2}\varepsilon_{t+1}^A,$$

where $\varepsilon_{t+1}^A \sim iid\ \mathcal{N}(0,1)$. The aggregate endowment A_t is a key characteristic of the platform. A cleverly designed platform serves to attract users with strong needs to transact with each other. As we will show, a higher A_t leads to more users on the platform, which, in turn, implies a higher probability of each user to complete a transaction with another user, and furthermore each transaction gives greater surpluses to both parties. One can therefore view A_t as the demand fundamental for the cryptocurrency, and τ_ε as a measure of dispersion among users in the platform.

We start with describing each user's problem in period t, conditional on joining the platform and meeting a transaction partner, and then go backward to describe his earlier decision on whether to join the platform. At t, when user i is paired with another user j on

the platform, we assume that they simply swap their goods, with user i using $\eta_c e^{A_{i,t}}$ units of good i to exchange for $\eta_c e^{A_{j,t}}$ units of good j. Consequently, both users are able to consume both goods, with user i consuming

$$C_{i,t}(i) = (1-\eta_c)\, e^{A_{i,t}},\ C_{j,t}(i) = \eta_c e^{A_{j,t}}$$

and user j consuming

$$C_{i,t}(j) = \eta_c e^{A_{i,t}},\ C_{j,t}(j) = (1-\eta_c)\, e^{A_{j,t}}.$$

We formally derive these consumption allocations between these two paired users in Appendix A through a microfounded trading mechanism between them. Furthermore, we can use equation (1) to compute the utility surplus $U_{i,t}$ of each user from this transaction.

Before finding a transaction partner on the platform, each user needs to decide whether to join the platform by buying the token. In addition to the utility surplus, $U_{i,t}$, from the transaction, there is also a capital gain from retrading the token, $P_{t+1} - RP_t$, with $R \geq 1$ being the interest rate for the holding period. We assume that users have quasi-linear expected utility, and incur a linear utility gain equal to this capital gain net of a fixed participation cost $\kappa > 0$ if they choose to join the platform. The participation cost may be either pecuniary or mental, and could represent, for instance, the cost of setting up a wallet and installing the software necessary for participating on the platform. Furthermore, we assume that each user needs to give a fraction β of his utility surplus $U_{i,t}$ from the transaction as service fee to the platform.

In summary, user i makes his purchase decision at t according to

$$\max_{X_{i,t}} \ \left(E\left[(1-\beta)\, U_{i,t} + P_{t+1} \mid \mathcal{I}_{i,t}\right] - RP_t - \kappa\right) X_{i,t}, \tag{2}$$

where $\mathcal{I}_{i,t}$ is the information set of user i at date t. Note that the expectation of the user's utility flow is regarding the uncertainty associated with matching a transaction partner, while the expectation of the capital gain from holding the token is regarding the uncertainty in the growth of the platform. By adopting a Cobb-Douglas utility function with quasi-linearity in wealth, users are risk-neutral with respect to the token's capital gain.[2]

An important aspect of our analysis is how the weights of the token's convenience yield and capital gain transition over the life of the platform. When the platform is young, there

[2] As Liu and Tsyvinski (2018) find little evidence that cryptocurrencies load on conventional sources of systematic risk, such as market or style factors, such an assumption for the token market is realistic.

are few tokens in circulation and users benefit more from the token price appreciation. When the platform matures, there are many tokens in circulation and users benefit mostly from the convenience yield from transactions on the platform. This transition underlies several interesting implications that more mature platforms might be more vulnerable to market breakdown, that younger platforms might have higher market capitalizations, and that token price volatility is increasing over time.

We now describe the information set, $\mathcal{I}_{i,t}$, of each user. We assume that while each user knows the value of his own goods endowment, $A_{i,t}$, when joining the platform, the users do not directly observe the aggregate endowment, A_t, As such, they will have to form expectations about the aggregate endowment when deciding whether to join the platform and, consequently, the token price serves to aggregate their dispersed information.

To facilitate our analysis of how users' speculation of the token price may affect their participation in the platform, we endow all users with a public signal about next period's innovation to aggregate endowment, ε_{t+1}^{A}, which by construction is orthogonal to A_t:

$$Q_t = \varepsilon_{t+1}^{A} + \tau_Q^{-1/2}\varepsilon_t^{Q},$$

where $\varepsilon_t^{Q} \sim iid\ \mathcal{N}(0,1)$. This public signal is similar to a "news" shock in the language of Beaudry and Portier (2006). Since the public signal only reveals information about next period's A_{t+1}, it only impacts users' decisions through their beliefs about the next period's token price, $E[P_{t+1} \mid \mathcal{I}_{i,t}]$, and therefore represents a speculative shock to all of the users. Even though we use the term "user optimism" to denote the speculative shock induced by the public signal Q_t, the users are fully rational in information processing in our model.

In addition to their private endowment, the market-clearing price of the token, and the public signal Q_t, users also observe a noisy public signal V_t about the volume of transactions that take place on the platform in period t. 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 token. Assuming an equilibrium in which users follow a cutoff strategy, such that they participate if $A_{i,t} \geq A_t^*$, we follow Sockin (2019) and assume that the volume signal takes the following form

$$V_t = \Phi\left(\sqrt{\tau_\varepsilon}\left(A_t - A_t^*\right) + \varepsilon_t^{V}\right)^2,$$

where $\Phi(\cdot)$ is the CDF of normal distribution and $\varepsilon_t^{V} \sim \mathcal{N}(0, \tau_v^{-1})$ is independent of all other

shocks in the economy. This specification has the appeal that the volume signal is always between 0 and 1, and is highly correlated with the volume of traded tokens.[3] Since the CDF of normal distribution is a monotonically increasing function, we can invert V_t to construct an additive summary statistic:

$$v_t = \tau_\varepsilon^{-1/2} \Phi^{-1} \left(V_t^{1/2} \right) + A_t^* = A_t + \tau_\varepsilon^{-1/2} \varepsilon_t^V, \tag{3}$$

which serves as the volume statistic.[4] The precision of the volume statistic is $\tau_\varepsilon \tau_v$, so that the less dispersed the endowments of users, the more informative is the volume signal.

In classical asset market models with dispersed information, e.g., Grossman and Stiglitz (1980) and Hellwig (1980), trading volume plays no role in learning.[5] [6] In our setting, users learn from both the price and volume of the cryptocurrency when deciding whether to purchase it. As such, volume provides a complementary source of information to the token price. Let $\mathcal{I}_t = \sigma\left(\{P_s, Q_s, V_s\}_{s \leq t}\right)$ be the tribe formed by all public information. In addition to the public information, each user also observes his own private endowment, $A_{i,t}$. We denote $\mathcal{I}_{i,t} = \sigma\left(\left\{A_{i,t}, \{P_s, Q_s, V_s\}_{s \leq t}\right\}\right)$ as the user i's full information set.

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

$$X_{i,t} = \begin{cases} 1 & \text{if } E\left[(1-\beta) U_{i,t} + P_{t+1} - RP_t \mid \mathcal{I}_{i,t}\right] \geq \kappa \\ 0 & \text{if } E\left[(1-\beta) U_{i,t} + P_{t+1} - RP_t \mid \mathcal{I}_{i,t}\right] < \kappa \end{cases}.$$

As the user's expected utility is monotonically increasing with his own endowment, regardless of other users' strategies, it is optimal for each user to use a cutoff strategy when next period's price is increasing in the demand fundamental. This, in turn, leads to a cutoff equilibrium, in which only users with endowments above a critical level A_t^* buy the token. This cutoff is eventually solved as a fixed point in the equilibrium to equate the token price, net of

[3] The noise in the volume signal reflects that, in practice, the anonymous nature of cryptocurrency transactions makes it difficult to accurately assess the volume of actual transactions, since transferring cryptocurrencies across wallets, in which no actual tokens are traded between two parties, is a transaction that hits the blockchain, while innovations such as the Lightning Network process small transactions off the blockchain. We parameterize the uncertainty arising from these issues as measurement error.

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

[5] 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.

[6] This is, in part, an artifact of the CARA-Normal framework, 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 model with a cutoff equilibrium is that we can incorporate a noisy volume signal while still maintaining tractability.

the expected resale value and participation cost, with the expected transaction utility of the marginal user from joining the platform. As each user's participation strategy also depends on his expected token resale value $E\left[P_{t+1} \mid \mathcal{I}_{i,t}\right]$, the common optimism among users induced by Q_t and the private optimism induced by $A_{i,t}$ with informational frictions helps to overcome their participation cost κ. Given the cutoff strategy for each user, who participates if $A_{i,t} \geq A_t^*$, the total token demand of users is given by

$$\int_{-\infty}^{\infty} X_{i,t}\left(\mathcal{I}_{i,t}\right) d\Phi\left(\varepsilon_{i,t}\right) = \Phi\left(\sqrt{\tau_\varepsilon}\left(A_t - A_t^*\right)\right). \tag{4}$$

1.2 Token Supply and Speculators

The supply of tokens, $\Phi\left(y_t\right)$, grows over time according to a pre-determined schedule

$$\Phi\left(y_t\right) = \Phi\left(y_{t-1} + \iota\right),$$

where $\Phi\left(\cdot\right)$ is the normal distribution function. This leads to a supply of tokens

$$\Phi\left(y_t\right) = \Phi\left(y_0 + \iota t\right),$$

with y_0 as the supply at the Initial Coin Offering (ICO). This specification captures, as in practice, that the increase in supply from token inflation tapers over time. For PoW platforms, such as Bitcoin and Ethereum, the number of new coins and tokens created by inflation periodically halves over time, according to a predetermined schedule, so that the total supply asymptotes to a fixed limit.[7]

In addition to the token inflation, we assume that there is a continuum of myopic speculators, who trade the token to speculate on its price fluctuation over time. Speculators provide liquidity by buying tokens, including those from the old generation of users, and then selling them to the new generation of users. We assume speculators hold noisy expectations of the next-period token price:

$$E^S\left[P_{t+1} \mid \mathcal{I}_t\right] = \left(1 + e^{\zeta_t}\right) RP_t,$$

where RP_t is the required risk-neutral return for holding the token to the next period, and $\zeta_t \sim iid\ \mathcal{N}\left(0, \sigma_\zeta^2\right)$ is the speculators' aggregate sentiment, which is not observable to the users. We consider speculators to be outsiders to the platform. They are distinct from

[7] With this specification, at most a unit measure of tokens exists. All of our key qualitative results remain unchanged, however, if instead we cap token supply at a maximum smaller than one unit.

users who actually participate on the platform. As such, they do not have private information about the platform's demand fundamental or fully understand how to interpret the implications of the same public information as users. Instead, these speculators may trade overconfidently on noisy information or on spurious correlations that give rise to mispecified technical trading strategies. Given the nascent and highly speculative nature of the cryptocurrency universe, and the limited data availability on the performance of its thousands of constituent cryptocurrencies, such speculators are likely ubiquitous.

Through the speculators' trading, we assume that the net supply of token to users is

$$\Phi\left[y_t - \lambda_S \log\left(E^S\left[P_{t+1} \mid \mathcal{I}_t\right] - RP_t\right) + \lambda_P \log\left(RP_t\right)\right] = \Phi\left(y_t - \lambda_S \zeta_t + \left(\lambda_P - \lambda_S\right) \log\left(RP_t\right)\right),$$

where $\lambda_S \log\left(E^S\left[P_{t+1} \mid \mathcal{I}_t\right] - RP_t\right)$ represents speculators' token demand driven by their speculative motive with $\lambda_S > 0$, and $\lambda_P \log\left(RP_t\right)$ represents the speculators' token supply in response to the price with $\lambda_P > 0$. When the speculators are more optimistic about the next-period token price, their token purchase tightens the token supply to users. On the other hand, if the token price is higher, the usual downward-sloping demand effect leads to stronger selling by the speculators and therefore more token supplied to users. To ensure an upward-sloping net supply curve with respect to the token price, we impose that

$$\lambda_P > \lambda_S.$$

By equating the supply with the users' token demand in (4), we obtain that

$$P_t = \frac{1}{R} \exp\left(\frac{\sqrt{\tau_\varepsilon}}{\lambda_P - \lambda_S}\left(A_t - A_t^*\right) - \frac{1}{\lambda_P - \lambda_S} y_t + \frac{\lambda_S}{\lambda_P - \lambda_S} \zeta_t\right), \tag{5}$$

where the market-clearing token price P_t is a log-linear function of the platform's demand fundamental A_t, the users' participation threshold A_t^*, the token supply y_t, and the speculators' sentiment ζ_t. Note that this log-linear price function holds even though the users' demand fundamental A_t and the speculators' sentiment ζ_t are not publicly observable to the users. Instead, the informational frictions affect each user's participation threshold A_t^*, which is yet to be determined by each user's optimal strategy in equilibrium. Each user's participation threshold also depends on the token market dynamics and the user's expectation of future token price appreciation.

1.3 Owner

The platform requires record keeping of all transactions. For the baseline model, we assume that the owner of the platform completes all user transactions each period and records these

transactions on the blockchain.[8] In a later section (Section 4), we expand the model to include a group of miners, who record the transactions for a fee and who may also attack the cryptocurrency. In the baseline setting, the payment to the owner in period t is both the seignorage from the scheduled inflation of the token base, $\Phi(y_{t-1}+\iota)-\Phi(y_{t-1})$, and the transaction fees from users:

$$\pi_t = (\Phi(y_{t-1}+\iota)-\Phi(y_{t-1}))P_t + \beta U_t,$$

where U_t is the total transaction surplus on the platform. The owner has no use for tokens and, potentially for liquidity reasons, sells them immediately to speculators. Assuming a cutoff strategy for users, we can integrate the expression for the expected utility of a user that joins the platform, as derived in Proposition 7 of Appendix A, over $A_{i,t}$ for $A_{i,t} \geq A_t^*$ to arrive at the realized surplus from user transactions:

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

As the platform's token base matures from inflation, the compensation to the owner shifts from seignorage to transaction fees.[9]

1.4 Rational Expectations Equilibrium

Our model features a rational expectations cutoff equilibrium, which requires the rational behavior of each user and the clearing of the token market:

- User optimization: each user chooses $X_{i,t}$ in each period t to solve his maximization problem in (2) for whether to purchase the token.

- In each period, the token market clears:

$$\int_{-\infty}^{\infty} X_{i,t}(A_{i,t},P_t)\,d\Phi(\varepsilon_{i,t}) = \Phi(y_t-\lambda_S\zeta_t+(\lambda_P-\lambda_S)\log(RP_t)), \tag{6}$$

  where each user's demand $X_{i,t}$ depends on its information set $\mathcal{I}_{i,t}$. The demand from users is integrated over the idiosyncratic component of their endowments $\{\varepsilon_{i,t}\}_{i\in[0,1]}$, which also serves as the noise in their private information.

[8] In contrast to traditional multi-sided platforms, such as in Rochet and Tirole (2003) and Evans (2003), the owner issues a native token to users that has a floating exchange rate with other tokens and currencies instead of collecting discriminating participation fees. This potentially buffers the pricing of the platform's services from external shocks, such as monetary policy shocks to fiat currencies, by denominating them in the native token, and disciplines their valuation through price discovery in financial markets.

[9] We assume the owner completes all transactions without censorship or charging monopoly markups. See Huberman et al (2018) for how Proof of Work decentralized consensus can overcome these issues at the cost of transaction delays.

2 Perfect Information Equilibrium

Before we analyze the equilibrium with informational frictions, we first analyze a benchmark equilibrium with perfect information in this section. The key characteristics of the perfect information equilibrium also hold in the equilibrium with information frictions.

Specifically, we characterize the equilibrium in each period t when A_t and ζ_t are publicly observable. In this case, the token market is characterized by the following state variables: the users' demand fundamental A_t, the token supply y_t, the users' optimism driven by the public signal Q_t, and the speculators' sentiment ζ_t. We use the notation $\mathcal{I}_t = \{A_t, y_t, Q_t, \zeta_t\}$ to represent the state variables at t, which are also equivalent to the set of public information discussed earlier. Note that the volume signal V_t is not a state variable, but the public signal, Q_t, which contains information about A_{t+1}, is still useful to users for forming their expectations about the token price in period $t+1$, P_{t+1}. Given that all users now have a common expectation about P_{t+1}, we drop the i subscript from their information sets. After observing Q_t, users share the same posterior belief about A_{t+1}, which is normal with the following conditional mean:

$$\hat{A}_{t+1} = A_t + \mu + \frac{\tau_Q}{\tau_\varepsilon + \tau_Q} Q_t.$$

As we discussed earlier, the noise in Q_t is a shock to the users' speculative optimism, since it has no impact on their current surplus from transacting with other users on the platform.

In each period, users sort into the platform according to a cutoff equilibrium determined by the net benefit of joining the platform, which trades off the opportunity of transacting with other users on the platform and the expected token price appreciation with the cost of participation. 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 user that purchases the token, A_t^*, as summarized in the following proposition.

Proposition 1 *The rational expectations equilibrium exhibits the following properties:*

1. *Regardless of other users' strategies, it is optimal for each user i to follow a cutoff strategy in purchasing the token:*

$$X_{i,t} = \begin{cases} 1 & \text{if } A_{i,t} \geq A^*\left(A_t, y_t, Q_t, \zeta_t\right) \\ 0 & \text{if } A_{i,t} < A^*\left(A_t, y_t, Q_t, \zeta_t\right) \end{cases}$$

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

$$\begin{aligned}
&(1-\beta)\, e^{(1-\eta_c)(A_t^*-A_t)+A_t+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-\frac{A_t^*-A_t}{\tau_\varepsilon^{-1/2}}\right)\mathbf{1}_{\{\tau>t\}}+E\left[P_{t+1}|\mathcal{I}_t\right]-\kappa \\
= \;& e^{-\frac{\sqrt{\tau_\varepsilon}}{\lambda_P-\lambda_S}(A_t^*-A_t)-\frac{1}{\lambda_P-\lambda_S}y_t+\frac{\lambda_S}{\lambda_P-\lambda_S}\zeta_t}, \qquad (7)
\end{aligned}$$

where τ is the stopping time for the breakdown of the platform due to the failure of the token market clearing:

$$\tau=\left\{\inf\ t:\quad A_t<A^c\left(y_t,Q_t,\zeta_t\right)\right\},$$

with $A^c\left(y_t,Q_t,\zeta_t\right)$ as a critical level for A_t, below which equation (7) has no root.

3. *In each period t, there may be no or multiple equilibria, depending on the users' expected token resale value:*

   - *If $E\left[P_{t+1}\mid\mathcal{I}_t\right]-\kappa\leq 0$, equation (7) has zero or two roots.*
   - *If $E\left[P_{t+1}\mid\mathcal{I}_t\right]-\kappa>0$, equation (7) has one or three roots.*

4. *In the dynamic equilibrium, the token price $P\left(A_t,y_t,Q_t,\zeta_t\right)$ is determined by equation (5) according to the users' equilibrium cutoff A_t^* and how users coordinate on their expectations of future equilibria.*

Proposition 1 characterizes the cutoff equilibrium in the platform, and confirms the optimality of a cutoff strategy for users in their choice to purchase the token. Users in each period sort into the platform based on their endowments, with those with higher endowments, and thus more gains from trade, entering the platform. In this cutoff equilibrium, the token price is a correspondence of the token market state variables $\left(A_t,y_t,Q_t,\zeta_t\right)$, according to equation (5) with A_t^* as an implicit function of these state variables.

Equation (7) provides a fixed-point condition to determine the optimal cutoff in each period. The left-hand side of equation (7) reflects the expected benefit to a marginal user with $A_{i,t}=A_t^*$ from acquiring a token to join the platform: the first term is the expected utility flow from transacting with another user on the platform, while the other terms $E\left[P_{t+1}\mid\mathcal{I}_t\right]-\kappa$ represent other benefits, given by the user's expected next-period token price (i.e., the expected token price under rational expectation $E\left[P_{t+1}\mid\mathcal{I}_t\right]$ with the public signal Q_t) net of the user's participation cost κ. The right-hand side of equation (7) reflects the cost of purchasing a token.

Figure 1 illustrates how the intersection of the two sides, each of which is plotted against $A_t^* - A_t$ determines the equilibrium cutoff. The dashed bell-shaped line depicts the left-hand side of equation (7) in a benchmark case when $E\left[P_{t+1} \mid \mathcal{I}_t\right] - \kappa = 0$. That is, it captures a marginal user's expected utility flow from transacting with another user. Note that this curve goes to zero when $A_t^* - A_t$ goes to either $-\infty$ or ∞. If $A_t^* \searrow -\infty$, the marginal user's own endowment is so low that there cannot be any gain from transacting with the other user. On the other hand, if $A_t^* \nearrow \infty$, the equilibrium cutoff is so high that there are so few other users on the platform to transact with the marginal user. This network effect makes her expected utility from transaction zero, despite her high endowment. Once the two end points are determined, it is intuitive that the marginal user's expected utility flow from transacting with another user on the platform has a bell shape.

The right-hand side of equation (7) is a negative exponential function of $A_t^* - A_t$, because the number of users on the platform is decreasing with the equilibrium cutoff A_t^* and because the token price is an increasing function of the number of users as in equation (5). Figure 1 shows that either the dashed bell-shaped curve intersects with the solid negative exponential curve twice if they intersect, or not at all if the solid curve lies above the bell-shaped curve. The latter case is particularly important as it represents the breakdown of the token market and, consequently, the failure of the platform. This happens when the expected utility from transacting is strictly lower than the cost of acquiring the token, either as a result of the small token supply y_t or strong speculator sentiment ζ_t. Proposition 1 shows that these two curves do not intersect when A_t falls below a critical level $A_t^c\left(y_t, Q_t, \zeta_t\right)$, which is determined by the other three state variables.

The terms $E\left[P_{t+1} \mid \mathcal{I}_t\right] - \kappa$ may move the bell curve of the marginal user's expected benefit from participating in the platform up or down relative to the benchmark case. If $E\left[P_{t+1} \mid \mathcal{I}_t\right] - \kappa > 0$, possibly as a result of the users' optimism about the future token price appreciation (i.e., positive shock to Q_t), the bell curve moves up relative the benchmark dashed curve in Figure 1. In this case, the bell curve may intersect with the negative exponential curve either once (as illustrated by the dotted curve) or three times.

If $E\left[P_{t+1} \mid \mathcal{I}_t\right] - \kappa < 0$, either as a result of users' pessimism or a high participation cost κ, the bell curve moves down relative to the benchmark dashed line in Figure 1, creating the possibility for the token market to break down. That is, an increase in κ may lead to the failure of the platform. As each user does not account for his participation decision

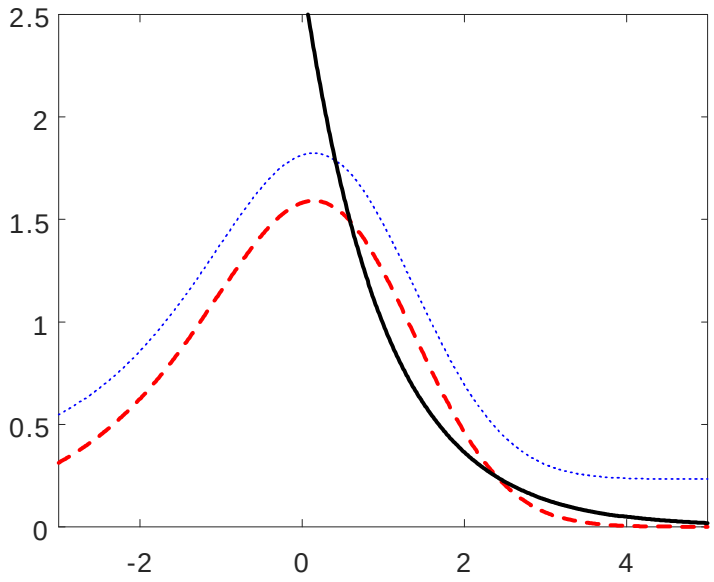

Figure 1: An illustration of the left-hand and right-hand sides of equation (7).

on other users through the network effect, this externality exacerbates the effect of κ on the equilibrium user participation. Interestingly, users' optimism offsets the effect of their participation cost, thus helping to overcome the network externality.

Market breakdown The market breakdown is caused by the network effect in the user demand for tokens and the rigid supply by the speculators. The following proposition characterizes the conditions for market breakdown to occur.

Proposition 2 *As a result of the network effect, no equilibria exist, i.e., the token market breaks down, under the following conditions:*

1. *The net speculative motive of users,* $E\left[P_{t+1} \mid \mathcal{I}_t^*\right] - \kappa$, *is nonpositive.*

2. *The users' demand fundamental is sufficiently low, i.e.,* $A_t < A^c\left(y_t, Q_t, \zeta_t\right)$, *or equivalently speculator sentiment is sufficiently high, i.e.* $\zeta_t > \zeta^c\left(A_t, y_t, Q_t\right)$.

The critical level $A^c\left(y_t, Q_t, \zeta_t\right)$ *is decreasing in the user optimism* Q_t *and increasing in speculator sentiment* ζ_t *and the user participation cost* κ.

Proposition 2 characterizes the determinants of the fundamental critical level $A^c\left(y_t, Q_t, \zeta_t\right)$ for the token market breakdown to occur. On the demand side, the users' speculative motive,

Table I: Baseline Model Parameters

Demand Fundamental:	$\mu = 0.01,\ \tau_A = 10$
Platform:	$y_0 = -.84$
Sentiment:	$\tau_Q = 100,\ \tau_\zeta = 2,\ \lambda_S = 1,\ \lambda_P = 2$
Users:	$\tau_\theta = 1,\ \eta_c = 0.3,\ \kappa = 0.03,\ R = 1.02$

driven by their optimism, helps to overcome the participation externality. On the supply side, speculators' sentiment has the opposite effect.

To further illustrate the properties of the token market equilibrium, we provide a series of numerical examples based on the parameter values given in Table I. Figure 2 depicts the fundamental critical level A^c across speculator sentiment (the left panel), user optimism (the middle panel), and token supply (the right panel). When the platform fundamental A is below A^c, the token market breaks down. The left panel shows that as speculator sentiment increases, the crowding out effect of speculators holding more tokens lowers user participation, shifting up the region of breakdown. In contrast, the middle panel shows that an increase in user optimism, which incentivizes more users to participate, has the opposite effect and shifts down the region of breakdown. Taken together, these two panels illustrate the opposite effects generated by users' optimism and speculators' sentiment on the fragility of the platform, as formally established by Proposition 2.

The right panel of Figure 2 shows that an increase in token supply, by lowering the expected retrade value of the token, increases the breakdown boundary. When the token base is small, there are at least two advantages: First, it is easier to clear markets with a small pool of users. Second, the expected growth of the token value is also higher. As the token supply inflates over time, the effects of token supply imply that the platform becomes more fragile over time, as the token's expected retrade value falls and user participation is driven more by the flow of convenience yields from transactions on the platform. This pattern thus suggests that large market capitalization tokens, such as Ethereum, might be more fragile and thus have more pronounced price volatility than small capitalization tokens. Interestingly, while Cong, Li and Wang (2018) emphasize the role of token resale in

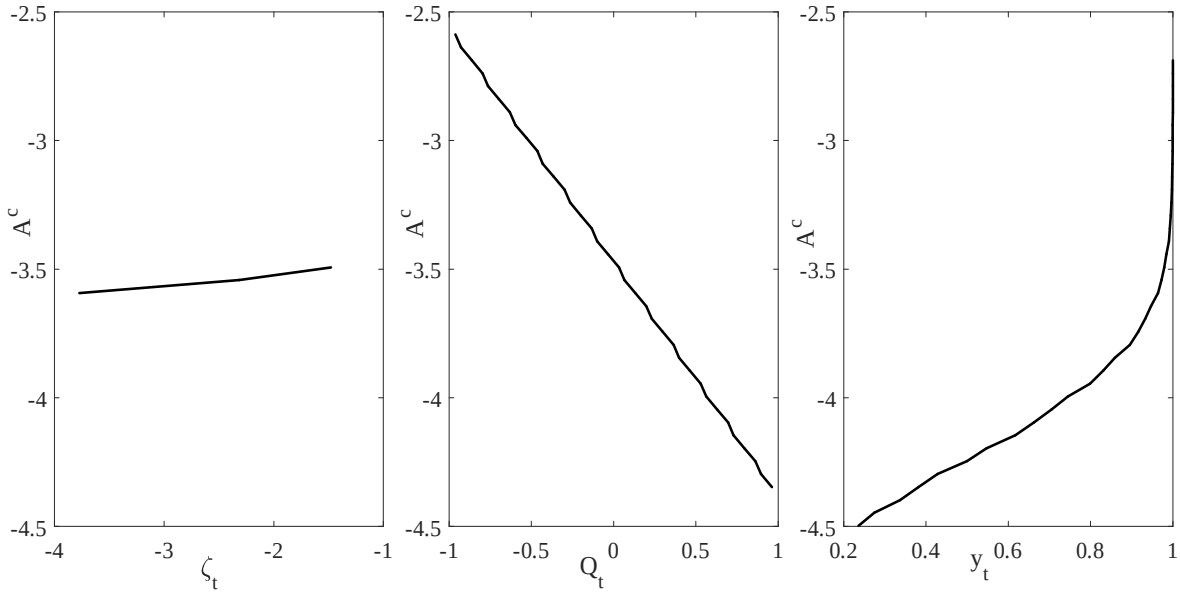

Figure 2: An illustration of the market breakdown boundary for the demand fundamental A^c with respect to speculator sentiment (left panel), user optimism (middle pannel), and token supply (right panel) in the perfect information equilibrium. Baseline values are $\zeta = 0$, $Q = 0$, and $y = 0.9$.

facilitating adoption, our model shows that it also helps to stave off failure of the platform.

User participation and token price For the simplicity of our analysis, we assume that all users coordinate on the highest price (i.e., the lowest cutoff) equilibrium in each period, regardless of how many equilibria exist. One can motivate this refinement based on the (dynamic) stability of the potential equilibria.[10] Then, the following proposition derives several comparative statistics of the equilibrium user participation and token price.

Proposition 3 *The equilibrium has the following properties:*

1. *Demand fundamental: the token price and the fraction of users that participate in the platform are increasing in the demand fundamental, A_t.*

2. *User Optimism: the token price and the fraction of users that participate in the platform are increasing in user optimism, Q_t.*

[10]The second (high cutoff) and third (highest cutoff) equilibria may or may not exist at any given date, depending on the expected retrade value of the token. As such, they are dynamically unstable, and we can eliminate them as predictions for the equilibrium outcome. In addition, the second (high cutoff) equilibria is unstable even fixing the token's expected retrade value. Introducing a small amount of noise into users' participation decisions, for instance, and letting this noise become arbitrarily small would ensure convergence away from this second equilibrium to the highest price equilibrium.

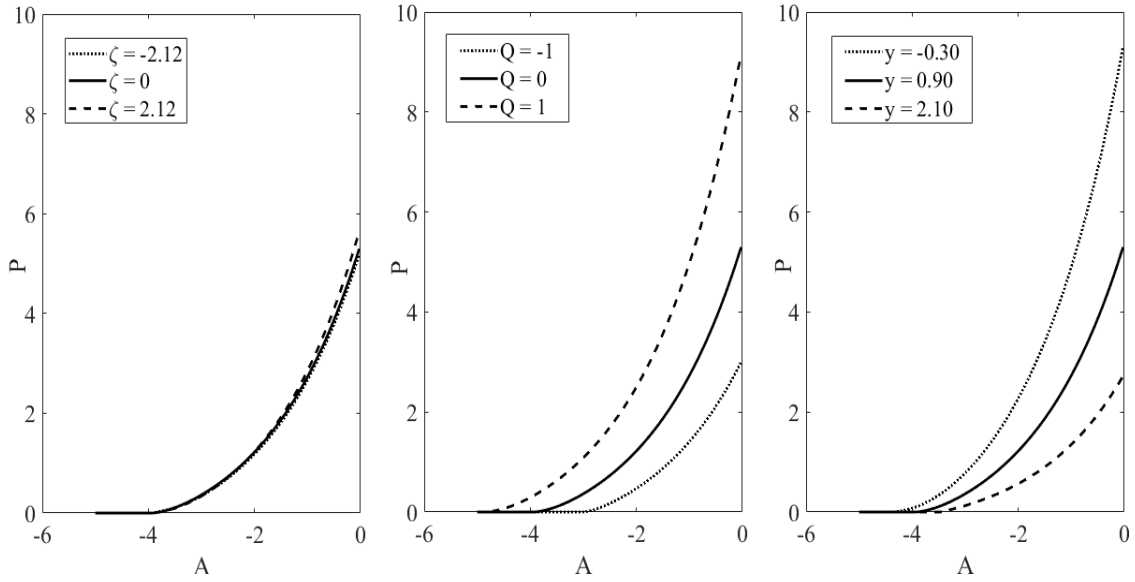

Figure 3: An illustration of the token price across the demand fundamental for different values of speculator sentiment (left panel), user optimism (middle panel), and the token supply (right panel). Baseline values are $\zeta_t = 0$, $Q_t = 0$, and $y = 0.9$.

3. *Speculator Sentiment: the fraction of users that participate in the platform is decreasing in speculator sentiment, ζ_t, while the token price is increasing (decreasing) in ζ_t when $A_t^* - A_t$ is sufficiently negative (positive).*

Figure 3 illustrates the equilibrium token price across the demand fundamental A for different values of speculator sentiment (the left panel), user optimism (the middle panel), and token supply (the right panel). The middle panel shows that the token price is increasing with user optimism, as formally established by Proposition 3. The left panel shows that the token price is also increasing with speculator sentiment, which holds, as established by Proposition 3, only when the demand fundamental is high. The difference across user optimism is more pronounced because user optimism increases user participation by raising their expectations of the token's resale value, which in turn raises the price today; speculator sentiment, in contrast, raises the token price, but also crowds out user participation, which, in turn, lowers the price, leading to a more muted overall effect on the token price. Finally, the right panel shows that the token price is decreasing in token supply because it lowers the expected retrade value of the token.

Life-cycle Effects Since our model is nonstationary with the token supply increasing deterministically over time, it has nuanced implications for how platform performance varies over the platform's life cycle. Central to understanding this pattern is the tension between the contemporaneous convenience yield and the capital gains in each user's total return from holding the token. Since users are risk-neutral, the sum of the two pieces always equal the cost of carry plus the participation cost, $R + \kappa/P_t$ in equilibrium. Thus, when expected future token price appreciation is high, the current demand fundamental and convenience yield must be low.

The demand fundamental's expected growth rate μ and the token supply y_t are the two key model parameters that determine the expected token price. A platform with a higher μ will, on average, see A_t trend upward over time, sustaining a high expected token price, while a high y_t depresses token prices across all values of A_t from supply saturation. The tension between the convenience yield and the expected future token price also impacts the log token price volatility over time. When the demand fundamental growth rate μ is high, the expected token price remains higher over time. Since more of the token return for high μ platforms is from the capital gains part of the token return, the user base is less sensitive to instantaneous fluctuations in the demand fundamental, which drive the convenience yield. As such, we expect higher μ platforms to have lower token price volatility. In contrast, as the token supply increases, both the region of market breakdown and the importance of the convenience yield in token returns increase, leading to a more volatile token price.

To see this graphically, we consider two platforms that differ only in the expected fundamental growth rate, one with $\mu = 0.01$ and the other with $\mu = 0.10$. To avoid concerns that the patterns are driven by the token supply asymptoting to 1, which covers the full population of users, we instead assume a maximum token supply of 0.90.[11] Figure 4 illustrates our intuition. When the expected growth rate of the demand fundamental is small ($\mu = 0.01$), the token supply effect dominates and the expected log token price is falling over time, while the log token price volatility is rising over time. In contrast, when the expected growth rate is high ($\mu = 0.10$), the expected token price declines more slowly over time and log price volatility is more attenuated. Taken together, our analysis suggests that stronger platforms (with a higher μ) see both higher expected token prices and lower log token price volatility, while weaker platforms (with a lower μ) experience a quicker decline in their expected token

[11] With a fixed token supply less than 1, we must now iterate over a fixed point equation to find the terminal value of the token price and then backwardly solve the model when the supply is less than 0.90.

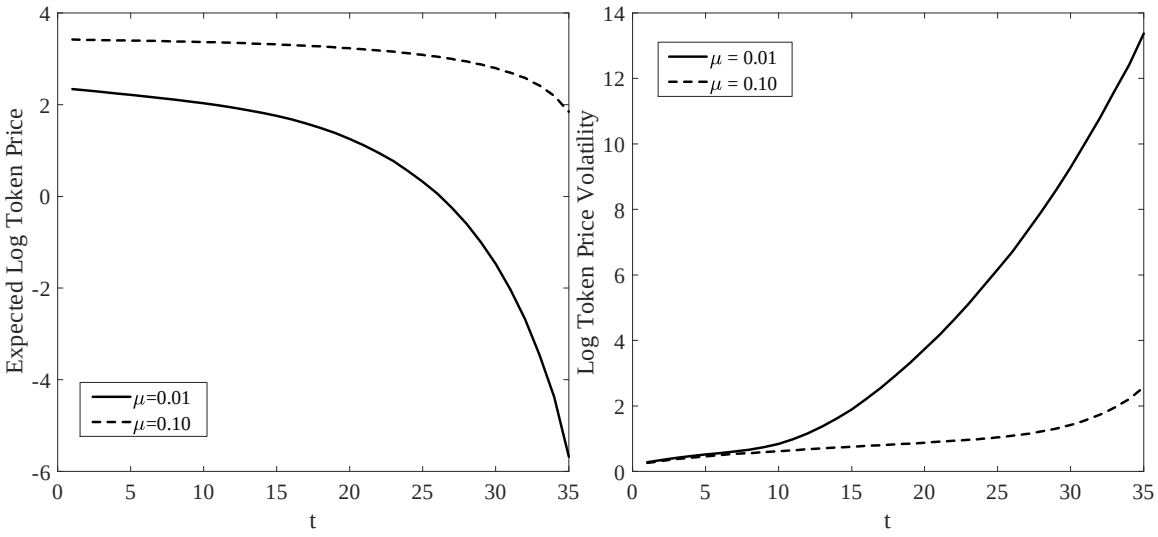

Figure 4: An illustration of unconditional expected log token price (left panel) and unconditional log price volatility (right panel) over time. The solid line is for a demand fundamental growth rate $\mu = 0.01$,and the dashed is for $\mu = 0.10$. The maximum token supply is 0.90.

price and a more pronounced increase in token price volatility over time.

3 Informational Frictions Equilibrium

In this section, we analyze the more realistic setting with informational frictions, in which both the users' demand fundamental A_t and the speculators' sentiment ζ_t are not publicly observable. As such, each user needs to form an expectation about A_t before making his token purchase decision. A key insight from this section is that informational frictions will act akin to insurance on the platform against failure from market breakdown, mitigating breakdown when the demand fundamental is weak at the cost of more tepid performance when the fundamental is strong. They dampen platform performance because users, facing the non-trivial inference problem, under-react to the fundamental.

As we discussed earlier, even though both A_t and ζ_t are not publicly observable, the token price nevertheless takes the same log-linear form given in (5), as in the perfect-information case. It is convenient to denote p_t as the sufficient statistic for the information contained by the token price P_t:

$$p_t = \frac{(\lambda_P - \lambda_S)\log(RP_t) + y_t}{\sqrt{\tau_\varepsilon}} + A_t^* = A_t + \frac{\lambda_S}{\sqrt{\tau_\varepsilon}}\zeta_t, \tag{8}$$

which is a linear combination of the two unobservables A_t and ζ_t. Equivalently, the token

price is given by

$$P_t = \frac{1}{R}\exp\left(\frac{\sqrt{\tau_\varepsilon}}{\lambda_P - \lambda_S}\left(p_t - A_t^*\right) - \frac{1}{\lambda_P - \lambda_S}y_t\right).$$

Despite the seemingly tractable price function, the token-market equilibrium is highly nonlinear as a result of the cutoff strategy used by each user, which is captured by the equilibrium threshold A_t^*, which is a nonlinear function of the state variables at t, and which serves as the channel for informational frictions to affect the equilibrium.

To forecast the platform's demand fundamental A_t in each period, each user's information set $\mathcal{I}_{i,t}$ now includes its own endowment $A_{i,t}$ and the public information set $\mathcal{I}_t = \sigma\left(\left\{\{p_s, v_s, Q_s\}_{s\leq t}\right\}\right)$, which include the history of equilibrium token price, volume, and the public signal. In what follows, we focus on the deterministic steady-state of the Kalman Filter recursion for users' belief formation, the proof of its characterization is given in the proof of Proposition 4. Conditional on the public information set $\mathcal{I}_t$, users hold the following common posterior belief about the platform fundamental $A_t \mid \mathcal{I}_t \sim \mathcal{N}(\hat{A}_t, \Sigma_A)$ with the conditional mean $\hat{A}_t$ determined by the following iterative dynamics:

$$\hat{A}_t = \hat{A}_{t-1} + \mu + \Sigma_A^{-1}\begin{bmatrix} \frac{\tau_Q}{\frac{1}{2}+\sqrt{\frac{1}{4}+\frac{\tau_A+\tau_Q}{\tau_\varepsilon\tau_v+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}}}} \\ \frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2} \\ \tau_\varepsilon\tau_v \end{bmatrix}' \begin{bmatrix} Q_{t-1} \\ p_t - \hat{A}_{i,t-1} - \mu \\ v_t - \hat{A}_{i,t-1} - \mu \end{bmatrix},$$

and the conditional variance at a steady-state level:

$$\Sigma_A = \sqrt{\left(\frac{1}{2\left(\tau_A+\tau_Q\right)}\right)^2 + \frac{1}{\tau_A+\tau_Q}\frac{1}{\tau_\varepsilon\tau_v+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}}} - \frac{1}{2\left(\tau_A+\tau_Q\right)}.$$

The users' common belief $\hat{A}_t$ summarizes the relevant information in $\{p_s, v_s, Q_{s-1}\}_{s\leq t}$ regarding the current-period demand fundamental A_t. The current period signal Q_t contains information about the future innovation to A_{t+1}, but not about the current period A_t. As a result, $\hat{A}_t$ does not subsume the information in Q_t, which serves as a shock to the users' speculative demand for the token, just as in the perfect information equilibrium. Furthermore, the token market's common belief about speculator sentiment is

$$\hat{\zeta}_t = E\left(\zeta_t \mid \mathcal{I}_t\right) = \frac{\sqrt{\tau_\varepsilon}}{\lambda_S}\left(\hat{A}_t - p_t\right),$$

which is derived from the definition of p_t. Taken together, we can represent the state of the token market by the following state variables: $\mathcal{I}_t = \left\{\hat{A}_t, Q_t, \hat{\zeta}_t, y_t\right\}$, which summarize

all relevant information in the public information set and which are almost the same as the state variables in the perfect-information equilibrium, except with the actual values of A_t and ζ_t replaced by the users' common filtered beliefs, $\hat{A}_t$ and $\hat{\zeta}_t$.

Further conditional on its own endowment $A_{i,t}$, user i's private belief is also Gaussian $A_t \mid \mathcal{I}_{i,t} \sim \mathcal{N}(\hat{A}_{i,t}, \Sigma_i)$, with its conditional mean and variance given by

$$\begin{aligned} \hat{A}_{i,t} &= \Sigma_i \Sigma_A^{-1} \hat{A}_t + \Sigma_i \tau_\varepsilon A_{i,t}, \\ \Sigma_i^{-1} &= \Sigma_A^{-1} + \tau_\varepsilon. \end{aligned} \tag{9}$$

In addition to the common optimism introduced by the public signal, Q_t, about next period's innovation to A_{t+1}, users now have heterogeneous beliefs about the current value of A_t because each user's private endowment, $A_{i,t}$, acts as a private signal about A_t. Since the demand fundamental is persistent, this also translates to heterogeneous beliefs about next period's demand fundamental A_{t+1}, and consequently about the token's expected retrade value.

By solving each user's token demand and clearing the users' aggregate demand with the supply from the speculators, we derive the token market equilibrium. The following proposition summarizes the equilibrium price and each user's optimal token demand in this equilibrium.

Proposition 4 *In the presence of informational frictions, the token market equilibrium exhibits the following properties:*

1. *If other users follow a cutoff strategy, it is optimal for each user i to follow a cutoff strategy in purchasing the token:*

$$X_{i,t} = \begin{cases} 1 & \text{if } A_{i,t} \geq A^* \left(\hat{A}_t, y_t, Q_t, \hat{\zeta}_t \right) \\ 0 & \text{if } A_{i,t} < A^* \left(\hat{A}_t, y_t, Q_t, \hat{\zeta}_t \right) \end{cases},$$

   where the cutoff A_t^* is measurable with respect to the public information set.

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

$$\begin{aligned} &(1-\beta)\, e^{\hat{A}_t + \left(1 - \frac{\eta_c}{1+\tau_\varepsilon \Sigma_A}\right)\left(A_t^* - \hat{A}_t\right) + \frac{1}{2}\eta_c^2\left(\Sigma_i + \tau_\varepsilon^{-1}\right)} \\ &\qquad \cdot \Phi\left(\eta_c \sqrt{\tau_\varepsilon^{-1} + \frac{\Sigma_A}{1+\tau_\varepsilon \Sigma_A}} + \frac{\sqrt{\tau_\varepsilon}\left(\hat{A}_t - A_t^*\right)}{\sqrt{\left(1+\tau_\varepsilon\Sigma_A\right)\left(1+2\tau_\varepsilon\Sigma_A\right)}} \right) \mathbf{1}_{\{\tau > t\}} \\ &+ E\left[P_{t+1} | \mathcal{I}_t^*\right] - \kappa = e^{-\frac{\sqrt{\tau_\varepsilon}}{\lambda_P - \lambda_S}\left(A_t^* - \hat{A}_t\right) + \frac{\lambda_S}{\lambda_P - \lambda_S}\hat{\zeta}_t - \frac{1}{\lambda_P - \lambda_S} y_t}, \end{aligned} \tag{10}$$

where $\mathcal{I}_t^*$ is the information set of the marginal user whose endowment is $A_{i,t} = A_t^*$, and τ is the stopping time for the breakdown of the platform:

$$\tau = \left\{\inf\ t: \quad \hat{A}_t < A^c\left(y_t, Q_t, \hat{\zeta}_t\right)\right\},$$

with $A^c\left(y_t, Q_t, \hat{\zeta}_t\right)$ as a critical level for $\hat{A}_t$, below which equation (10) has no root.

Proposition 4 confirms that even when A_t and ζ_t are not publicly observable, each user continues to follow a cutoff strategy for his token purchase decision, except that the equilibrium threshold A_t^* is determined by the users' common beliefs $\hat{A}_t$ and $\hat{\zeta}_t$. The fixed-point condition for A_t^* in (10) is similar to (7) for the perfect-information setting, with a few key differences: $\hat{A}_t$ replaces A_t, $\hat{\zeta}_t$ replaces ζ_t, and learning modifies various coefficients in the marginal user's expected utility on the left-hand side to reflect the additional uncertainty that the demand fundamental is unobserved.

The equilibrium cutoff $A^*\left(\hat{A}_t, y_t, Q_t, \hat{\zeta}_t\right)$ is the only channel for informational frictions to directly affect the market equilibrium. By distorting users' expectations of the retrade value of the token, informational frictions have both a static and a dynamic effect on the platform, specifically by making the equilibrium token price over-weight public information and, consequently, be less responsive to fundamental shocks. To see this, note that the equilibrium token price is crucially determined by the expected convenience yield $(1-\beta)\, E\left[U_{i,t} \mid \mathcal{I}_{i,t}^*\right]$ from the perspective of the marginal user i at date t. Similar to Albagli, Hellwig, and Tsyvinski (2017), the marginal user has a signal realization equal to the participation cutoff, $A_{i,t} = A_t^*$, which is an equilibrium function of all public information, as summarized by $\left\{\hat{A}_t, y_t, Q_t, \hat{\zeta}_t\right\}$. For this particular user, his private signal is not conditionally uncorrelated with this public information, but is instead a function of it. The marginal user therefore overweights the public information when forming his conditional expectation $\hat{A}_{i,t}$.

The dynamic effect further exacerbates this distortion. Specifically, iterating forward on the equilibrium cutoff condition (10) gives

$$P_t = \sum_{t'=t}^{\tau} E\left[\frac{1}{R^{t'+1-t}} E\left[E\left[(1-\beta)\, U_{i,t'} - \kappa \mid \mathcal{I}_{t'}^*\right] \mid \mathcal{I}_{t'-1}^* ...\right] \mid \mathcal{I}_t^*\right],$$

where we have switched the order of summation and expectation because $U_{i,t}$ is nonnegative. In addition, the $E\left[E\left[U_{i,t'} \mid \mathcal{I}_{t'}^*\right] \mid \mathcal{I}_{t'-1}^* ...\right]$ is shorthand for the iterated expectations arising from the Keynesian Beauty Contest that today's marginal user must forecast the expectations of future marginal users, who must themselves forecast the expectations of marginal

users that temporally follow them. Since the information sets across the marginal users are temporally non-nested, these iterated expectations do not collapse to first-order expectations, leading to a bias toward public information, which is reminiscent of Allen, Morris, and Shin (2006) and discussed in the context of downside risk in Albagli, Hellwig, and Tsyvinski (2014b). Given that the marginal user at each date, in equilibrium, overweights the price in inferring the demand fundamental, the price's bias toward the public versus private information through the "forecasting the forecasts" of others is even more acute. Taken together, informational frictions dampen the platform performance by making the equilibrium token price systematically underreact to the users' private information and, consequently, to the fundamental shocks as well.

The following proposition summarizes several properties of the informational frictions equilibrium.

Proposition 5 *The informational frictions equilibrium has the following properties:*

1. *All of the comparative statics for the token price and user participation from Proposition 3 are preserved, except that the users' demand fundamental and speculator sentiment, A_t and ζ_t, are replaced by their filtered counterparts,, $\hat{A}_t$ and $\hat{\zeta}_t$, respectively.*

2. *Consider a temporary increase in uncertainty about the demand fundamental, Σ_A, at date t, leaving the uncertainty Σ_A in all future periods unchanged. This temporary increase in uncertainty lowers (increases) the token price and user participation at date t when the filtered demand fundamental $\hat{A}_t$ and user optimism Q_t are sufficiently high (low) or when filtered speculator sentiment $\hat{\zeta}_t$ is sufficiently low (high).*

Proposition 5 reveals that the comparative statics from the perfect information equilibrium are preserved under informational frictions. This is natural since users form posterior beliefs about the latent states, A_t and ζ_t, by observing the public signals (P_t, V_t, Q_t) and their private information $A_{i,t}$, and then choose their optimal entry decisions as they would under perfect information. The difference is that users now need to account for the additional uncertainty of their inference problem.

The second part of Proposition 5 provides an insight into how informational frictions impact the current-period platform performance. A one-time increase in uncertainty from learning, Σ_A, lowers user participation when the platform fundamentals are strong (high $\hat{A}_t$,

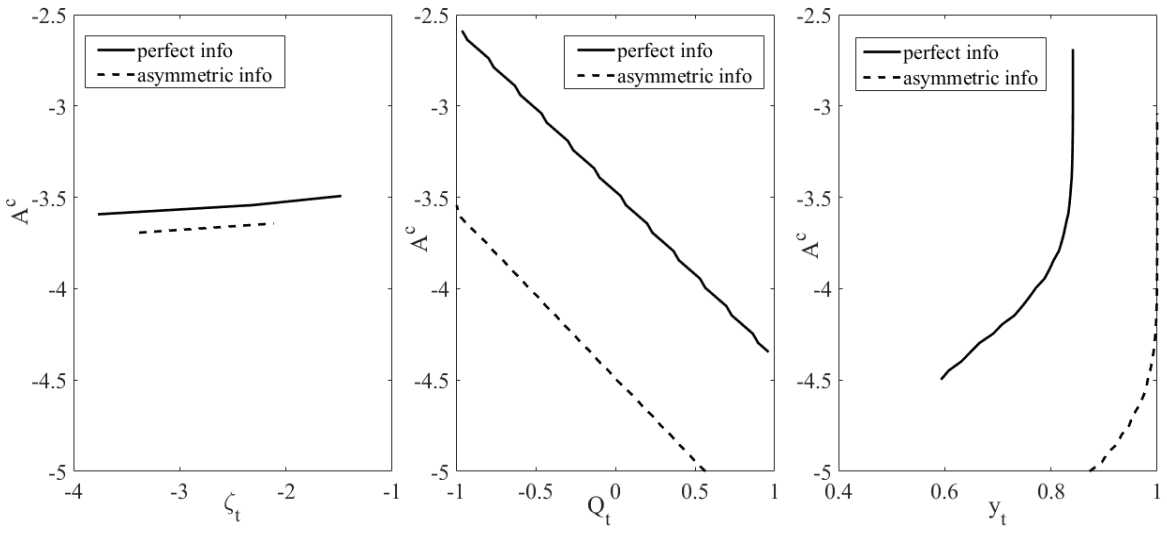

Figure 5: An illustration of the market breakdown boundary across the demand fundamental for different values of speculator sentiment (left panel), user optimism (middle panel), and token supply (right panel) for the cases with perfect information (solid line) and asymmetric information (dashed line). Values are the filtered demand fundamental and speculator sentiment for the asymmetric information case. Baseline values are $\zeta_t = \hat{\zeta}_t = 0,\ Q_t = 0$, and $y = 0.9$.

high Q_t, or low $\hat{\zeta}_t$), and raises participation when the fundamentals are weak. As such, informational frictions are dampening, in that the platform performs less well when the fundamentals are strong, and less poor when the fundamentals are weak. A limitation of this analysis, however, is that it abstracts from the effect of a persistent increase in Σ_A at all future dates, which further feeds back into the expected retrade value of the token by changing the cutoff function at all future dates. As informational frictions systematically dampen the poor performance of the platform, this dynamic feedback effect can further shrink the region of market breakdown.

As part of the analysis, we establish that the token price is convex in the filtered demand fundamental whenever an equilibrium exists, which is important for conveying the intuition of the role of informational frictions.

To fully understand how informational frictions dampen platform performance, we appeal to the logic of the Bayesian Persuasion literature, e.g., Aumann and Maschler (1995) and Kamenica and Gentzkow (2015). A key idea of the Bayesian Persuasion analysis is that since the token price is convex with respect to the filtered demand fundamental $\hat{A}_t$ whenever an equilibrium exists, informational frictions lower the token price. This is because more information makes the users' common belief $\hat{A}_t$ more responsive to the actual value of A_t,

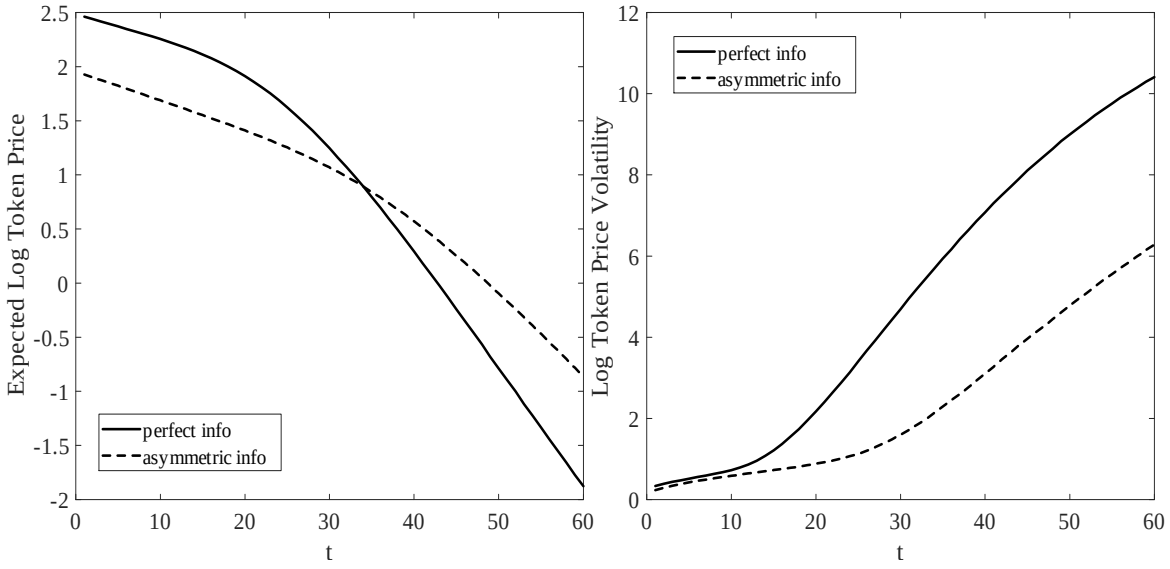

Figure 6: An illustration of the unconditional expected log token price (left panel) and log price volatility (right panel) over time. The solid line is the perfect information case and the dashed is the asymmetric information case under the assumption $A_0 = \hat{A}_0 = 0$.

so that users benefit more from the possible high values of A_t although do not lose as much from the possible low values. By Jensen's Inequality, the higher variance of user beliefs $\hat{A}_t$ raises the unconditional average of token price. On the other hand, informational frictions make $\hat{A}_t$ underreact to both high values and low values of the demand fundamental, thus also reducing the region of market breakdown. In this sense, informational frictions introduce a tradeoff between platform fragility (market breakdown) and performance (high participation when the demand fundamental is strong).

Figure 5 is the asymmetric information analogue of Figure 2 with $\tau_v = 1$. Similar to the perfect information equilibrium, the left panel demonstrates that market breakdown occurs when the filtered demand fundamental $\hat{A}_t$ is sufficiently weak, while this boundary shifts down when the filtered speculator sentiment $\hat{\zeta}_t$ is low (left panel), user optimism Q_t is high (middle panel), or when the token supply y_t is small (right panel). Interestingly, market breakdown occurs at lower values of the filtered demand fundamental than with perfect information, with the exception of high values of filtered speculator sentiment since it is negatively correlated with the filtered demand fundamental. This is because users underreact to negative information about the platform and, consequently, are willing to participate over a wider region of the filtered demand fundamental.

Figure 6 shows the unconditional expected log token price and log price volatility as the platform matures, assuming initially that $A_0 = \hat{A}_0 = 0$. While the expected token price is lower with informational frictions, the expected log price (left panel) overtakes its perfect information counterpart as the platform matures. This occurs because of the dampening mechanism discussed earlier. As a result of informational frictions, the region of market breakdown is smaller than with perfect information, and this boosts the expected log price by minimizing downside risk. Consistent with dampening, the log token price volatility is lower with informational frictions, as users underreact to new information that arrives on the platform.

Taken together, informational frictions attenuate platform fragility. Not only is market breakdown less likely with informational frictions, especially when the platform is young, but it also mutes token price volatility. The cost of this dampening, however, is the worsened platform performance when the demand fundamental is strong, because users underreact to A_t and thus under-participate when A_t is actually high. As a result, the expected token price is also lower with informational frictions as a result of the convexity of the price function. This cross-subsidization of informational frictions, consequently, mitigates platform fragility at the expense of a lowered token price by expectation. In this way, informational frictions act as a form of insurance that protects against weak fundamentals at an insurance premium.

4 Mining and Strategic Attacks

Up until now, we have assumed that the cryptocurrency platform has a permissioned blockchain because the owner verifies and completes all transactions. A key feature of the blockchain technology underpinning cryptocurrencies, however, is that they are permissionless and verify transactions through decentralized consensus, amongst an anonymous population of miners, while maintaining trust in the cryptocurrency by deterring strategic attacks. The risk of strategic attacks by miners is a central concern for cryptocurrency platforms. Attacks on Bitcoin Gold, ZenCash, Vertcoin, Monacoin, Ethereum Classic, Verge (twice) have already led to losses of approximately \$18.6M, \$550K, \$50K, \$90K, \$1.1M, and \$2.7M, respectively. Such attacks include, for instance, fifty-one percent attacks that lead to "double spending" fraud and transaction failures through denials of service.[12]

[12] This issue has also received significant attention in the literature. See, for instance, Chiu and Koeppl (2017), Pagnotta (2018), and Budish (2018).

To illustrate how Proof of Work mining can impact platform performance and stability, we consider a simple extension of our perfect information setting in this section. We now assume that in each period, a new population of potential miners mine the token by providing accounting and custodial services using its underlying blockchain technology.[13] As in practice, there is free entry of miners onto the platform.

All miners provide computing power to facilitate transactions among users, subject to a cost of setting up the required hardware and software to mine the token: $e^{-\xi_t} M_{j,t}$, where $M_{j,t} \in \{0,1\}$ is the miner's decision to mine and ξ_t measures the miner's mining efficiency by inversely parameterizing the miner's cost of mining. This mining efficiency ξ_t is common to all miners and follows an AR(1) process:

$$\xi_t = \xi_{t-1} + \tau_\xi^{-1/2} \varepsilon_t^\xi,$$

with $\varepsilon_t^\xi \sim iid\ \mathcal{N}(0,1)$. Instead of the platform owner, miners are compensated with the transaction fee βU_t, which is a fraction of the transaction surplus, and the seignorage from token inflation, $(\Phi(y_{t-1}+\iota) - \Phi(y_{t-1}))\, P_t$. Consistent with many token platforms with PoW mining, miners also earn transaction fees since, over time, the number of tokens created by inflation will diminish. It is thus necessary to shift the compensation toward fees. Miners have no use for tokens and sell them to users and speculators. If $N_{M,t}$ miners join the platform at date t, each miner earns $\frac{\beta U_t + (\Phi(y_{t-1}+\iota) - \Phi(y_{t-1}))P_t}{N_{M,t}} - e^{-\xi_t}$ in expected net gain.[14]

Suppose that when a strategic attack occurs, users lose half of their transaction surplus from failed transactions in the current period as a result of service delays and denials. The interruption of service also reduces transaction fees by half. Furthermore, we assume that a strategic attack occurs whenever

$$(\Phi(y_t + \psi\iota) - \Phi(y_t))\, P_t + \frac{(\Phi(y_{t-1}+\iota) - \Phi(y_{t-1}))\, P_t + \frac{\beta}{2} U_t}{2} \geq \alpha N_{M,t}^2, \tag{11}$$

where $\alpha, \psi > 0$. On the left-hand side of this condition, the first term has the interpretation of fraudulent seignorage created by corrupt miners from double spending, and the second is

[13] 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. See Cong, He and Li (2018) for an extensive analysis of this issue. Our modeling of mining as a static problem when there is free-entry is consistent with that in Abadi and Brunnermeier (2018).

[14] To focus on the broader implications of the cryptocurrency for users, 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.

half the mining fees, in the forms of legitimate seignorage and transaction fees, earned from mining the attack. The right-hand side is the cost of attack, which is a convex function of the number of miners, reflecting that a larger pool of miners makes it increasingly costly for corrupt miners to acquire the necessary computing power for completing a 51% attack. In Appendix B, we provide a microfoundation for this strategic attack condition, although all that we require is that strategic attacks occur whenever the cost of mining is sufficiently high and the number of miners is sufficiently low.

Consider the incentives of miners to join the platform at date t. With rational expectations, miners choose whether to join, fully anticipating the possibility of a strategic attack. Miner j with the common mining efficiency ξ_t thus maximizes his expected gain:

$$\Pi_j = \max_{M_{j,t}} \left(\frac{\left(\Phi\left(y_{t-1}+\iota\right) - \Phi\left(y_{t-1}\right)\right) P_t + \frac{\beta}{1+\chi_t} U_t}{\left(1+\chi_t\right) N_{M,t}} - e^{-\xi_t} \right) M_{j,t}, \tag{12}$$

where $\chi_t \in \{0,1\}$ is the indicator for whether there is a strategic attack at date t. The $\frac{1}{1+\chi_t}$ factor reflects that the mining pool receives only $\frac{1}{2}$ of the total mining revenue from completing less than half of the blocks when a strategic attack occurs.

For simplicity, we characterize strategic attacks by miners under the perfect information setting when the platform's demand fundamental A_t is publicly observable. Note that relative to the perfect information equilibrium characterized in Section 2, the miners' common mining efficiency ξ_t becomes an additional state variable. The following proposition shows that strategic attacks occur when either A_t or ξ_t falls below a certain level.

Proposition 6 *The equilibrium has the following properties:*

1. *There exists a critical level $\xi^a\left(A_t, y_t, Q_t, \zeta_t\right)$ such that strategic attacks occur when $\xi_t < \xi^a\left(A_t, y_t, Q_t, \zeta_t\right)$.*

2. *There exists a critical level $A^a\left(y_t, Q_t, \zeta_t, \xi_t\right)$, which is decreasing in ξ_t, such that strategic attacks occur when $A_t < A^a\left(y_t, Q_t, \zeta_t, \xi_t\right)$.*

3. *Both an attack equilibrium and a no-attack equilibrium can exist as a result of the positive relationship between the benefits and costs of attacks.*

From Proposition 6, a strategic attack occurs when the mining fundamental and/or the user demand fundamental are sufficiently weak, since in these situations the number of

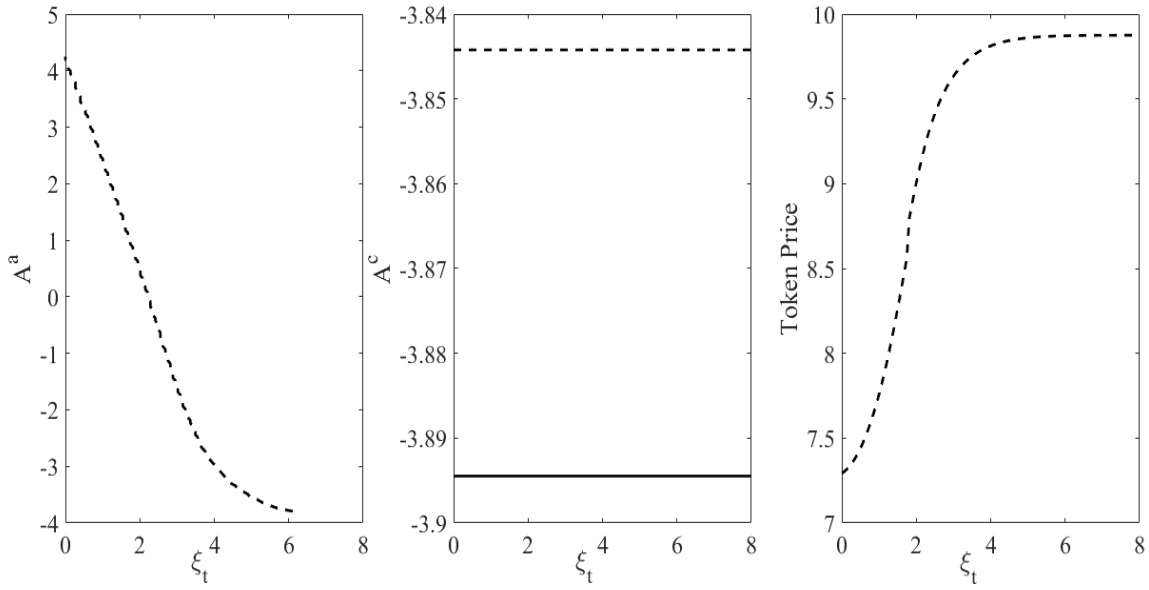

Figure 7: An illustration of the strategic attack boundary (left), the market breakdown boundary (middle), and the token price (right) with respect to mining fundamental ξ_t. Market breakdown boundary without mining (solid line) is for comparison. User optimism is turned off ($\tau_Q = 0$) in this illustration. Baseline values are $\zeta_t = 0$, and $y_t = 0.90$.

miners is too small to deter a strategic attack. Although the impact of each strategic attack is transitory, the occurrence of strategic attacks is persistent, since an attack will occur every period in which the platform is in the attack region. As attacks reduce the token price and thus the incentives of miners to join the platform, it may be possible for both a no-attack equilibrium and an attack equilibrium to be self-fulfilling.

Figure 7 depicts the strategic attack boundary (left panel) and the platform breakdown boundary with and without mining (middle panel) for $\tau_\xi = 10,\ \alpha = 0.8$, and $\psi = 3$. Miners choose to attack the cryptocurrency if the user fundamental A_t falls below the attack boundary A^a. This attack boundary is decreasing with the mining fundamental ξ_t, as formally derived in Proposition 6. While each strategic attack does not lead to the failure of the platform, the expected losses induced by future attacks lead to a higher threshold A^c for market breakdown. As such, the possibility of strategic attacks by miners also exacerbates platform fragility.

As our analysis highlights, the PoW protocol introduces several novel features to cryptocurrency platforms. First, the anticipation of future attacks makes such a strategic attack easier to execute through an adverse feedback loop. An attack lowers the revenue each

honest miner receives, which reduces the number of miners that join the platform and thus lowers the cost of an attack. Interestingly, the decentralized consensus protocol exacerbates the problem, by dispersing the revenue from mining over the whole population of miners. As a result, an honest miner captures only a fraction of the revenue that is recovered by increasing its own mining power to preempt attacks.[15] In this way, decentralized consensus averts internalization of incentives to ensure the platform security.

Second, the feedback effects from mining to the platform token's intrinsic value through service delays and denials are peculiar to the decentralized consensus protocol. Users are also shareholders in the platform through the retradability of the token. As such, delays, and expectations of future delays, have an important impact on the token price because they reduce user participation and, consequently, demand for the token.

Finally, from Figure 7 (right panel), there is a non-linear relation between the mining fundamental and token price. When the mining fundamental is far away from the strategic attack boundary, an incremental change in the efficiency of mining has a limited impact on the token price, since the probability of an attack is small. When the mining fundamental is close to the strategic attack boundary, however, a small change in the efficiency of mining can have a substantial impact on the token price, which in turn leads to a substantial impact on the platform's stability.

The role of rational bubbles The presence of mining on the platform introduces a role for rational bubbles to improve the platform's security and stability by inflating the token price that compensates miners for their services. Since our setting features overlapping generations of agents over an infinite horizon, it is also suitable for investigating the role of rational bubbles, which we briefly discuss here. Suppose that we augment the token price with a rational bubble $b_t \geq 0$ that, following Blanchard and Watson (1982), satisfies the following law of motion:

$$b_{t+1} = \begin{cases} \frac{Rb_t}{(1-\rho)\Pr(\tau > t+1 \mid \mathcal{I}_t)} & \text{if } \tau > t+1 \\ 0 & \text{otherwise} \end{cases},$$

[15] While, in principle, mining pools could coordinate to preempt a strategic attack, their primary function is risk-sharing. Further, such coordination would undermine the spirit of the decentralized consensus protocol. In May 2019, the BTC.top and BTC.com mining pools, with combined 44% mining power, were criticized for coordinating an "attack" on the BTC Cash blockchain to reverse a hacker's transactions.

where ρ is an exogenous probability of the bubble bursting in the next period and R is the gross interest rate in the economy.[16] Since the bubble also bursts if the token market breaks down, the endogenous possibility of market breakdown from the users' coordination failure raises the return on the bubble, conditional on the platform's survival. Interestingly, when the platform is most vulnerable is also when the bubble sees its largest ex post price appreciation conditional on survival.

To save space, we briefly discuss several possible effects of this rational bubble, without formally characterizing them. First, it has no direct effects on users since they always pay the fair value to purchase the token. Second, the rational bubble reduces the likelihood of strategic attacks by miners, because it raises the token price and miners are partially compensated by seignorage from token inflation. Third, the lower likelihood of strategic attacks today and in the future raises the token's expected retrade value, increases user participation, and consequently the token price and transaction surplus today. Fourth, when the platform matures, however, all miner revenue is derived from transaction fees, and the rational bubble ceases to have real effects. Finally, the bubble bursting for exogenous reasons is also a source of instability on the platform, as it generates a sudden drop in the token price and consequently a fall in user participation.

5 Empirical Implications

In this section, we discuss several empirical implications of our conceptual framework for cryptocurrency returns. Cryptocurrency returns in our framework have three components: a convenience yield of the marginal user, which acts like a dividend, a capital gain from the token price appreciation, and an embedded discount in the token price to compensate users for their participation cost. By the marginal user's equilibrium condition in (7), these three components satisfy the following relationship:

$$R = \frac{(1-\beta)\, U_t^*}{P_t} + \frac{E\left[P_{t+1} \mid \mathcal{I}_t\right]}{P_t} - \frac{\kappa}{P_t}.$$

In contrast to fiat currencies, the expected capital gain can be quite positive, despite token inflation, and substantial, which has attracted many speculators to the nascent asset

[16] To avoid the restrictive conditions in Santos and Woodford (1998), since tokens are in positive supply, we implicitly assume users are unconstrained in their resources in the numeraire to purchase tokens. This assumption reflects that cryptocurrencies, in practice, are a small part of the overall asset universe and, if the rest of the economy grows sufficiently fast, then users could, in principle, finance the bubble.

class. In addition, and novel to cryptocurrencies, the convenience yield is created by shareholders acting in their dual capacity as users of the platform, which gives rise to a feedback mechanism from the cryptocurrency return to user participation.[17] As the platform matures and participation increases, the cryptocurrency return transitions from being driven more by the capital gain component to more by the convenience yield.[18]

The empirical literature is mostly focused on the capital gain component of the cryptocurrency return, as it is directly measurable by the econometrician. In equilibrium, the expected excess capital gain can be expressed as

$$\frac{E\left[P_{t+1} \mid \mathcal{I}_t\right]}{P_t} - R = \frac{\kappa}{P_t} - \frac{(1-\beta)\, U_t^*}{P_t}. \tag{13}$$

Consistent with the empirical findings of Hu, Parlour, and Rajan (2018) and Liu and Tsyvinski (2019), the expected excess capital gain in our setting does not exhibit conventional risk premia. The capital gain may still exhibit predictibility through the underlying state variables that explain the convenience yield. These state variables are the demand fundamental, user optimism, speculator sentiment, and token supply. In the presence of informational frictions, the demand fundamental and speculator sentiment are replaced by their filtered counterparts, which are linear functions of the full history of token prices, trading volumes, and public news signals. Liu and Tysvinski (2019), for instance, show that investor attention, measured either with Google searches or Twitter post counts for "Bitcoin", predicts future cryptocurrency returns, with positive (negative) attention, as measured by keywords, positively (negatively) predicting future weekly returns.[19] Liu and Tsyvinski (2019) also find that investor sentiment, measured as either the log ratio between the number of positive and negative phrases of cryptocurrencies in Google searches or the ratio of trading volume to return volatility, predicts future cryptocurrency returns.

Our model also suggests the participation cost borne by users, which is not directly observed by the econometrician, as an additional channel of return predictability. As this cost effect is inversely related to the token price and, consequently, market capitalization,

[17] Shams (2019) provides evidence of the importance of network effects for cryptocurrency returns by showing that return comovement arising from overlapping exposures to demand shocks is significantly stronger among "high community-based" cryptocurrencies.

[18] A subtle issue is how to measure the marginal user's convenience yield in practice. If users were all identical, then $\frac{U_t}{\sqrt{V_t}}$, which is similar to the average transaction fee, would be this yield. With selection onto the platform, however, a reasonable, noisy proxy is the minimum transaction size on the blockchain.

[19] Although the measure is constructed with searches for "Bitcoin" specifically, we view this measure as a noisy proxy for interest in cryptocurrencies more geneally.

our model predicts a size effect in the capital gain of cryptocurrencies. This prediction is consistent with Liu, Tsyvinski, and Wu (2019), who find a size factor in the cross section of cryptocurrency returns, with size measured as either market capitalization, price, or maximum price.

In addition, the persistence of the two return components $\frac{\kappa}{P_t}$ and $\frac{(1-\beta)U_t^*}{P_t}$ in (13) can lead to a positive autocorrelation in the capital gain:

$$Cov\left(\left.\frac{P_{t+2}}{P_{t+1}}, \frac{P_{t+1}}{P_t}\right| \mathcal{I}_{t-1}\right) = Cov\left(\left.\frac{\kappa}{P_{t+1}} - \frac{(1-\beta)\,U_{t+1}^*}{P_{t+1}}, \frac{\kappa}{P_t} - \frac{(1-\beta)\,U_t^*}{P_t}\right| \mathcal{I}_{t-1}\right) > 0,$$

because the innovations $\frac{P_{t+1}-E[P_{t+1} \mid \mathcal{I}_t]}{P_t}$ and $\frac{P_{t+2}-E[P_{t+2} \mid \mathcal{I}_{t+1}]}{P_{t+1}}$ are uncorrelated with rational expectations. This positive autocorrelation implies momentum, as empirically documented by Liu and Tsyvinski (2019) in the prices of cryptocurrencies. Furthermore, the momentum effect in our model is independent of investor attention and sentiment, which is also consistent with Liu and Tsyvinski (2019), who find time-series momentum over 1-to-8 week horizons that is not subsumed by their measures of attention or sentiment.

Finally, our extension with mining suggests that the capital gain from a cryptocurrency has a non-linear relation with the marginal cost of mining. When the cost of mining is low relative to the strategic attack threshold, small changes in it have a muted impact on the capital gain, as the potential loss from strategic attacks, which can be viewed as an extended form of the participation cost in (13), is small. As the mining cost increases toward the strategic attack boundary, however, incremental changes become more relevant. Our model therefore predicts that measures of mining costs should have more predictive power for the capital gain when there is a nontrivial chance of strategic attacks, such as when the hash rate or the number of miners is low.

6 Conclusion

This paper develops a model to analyze cryptocurrencies. In our model, a cryptocurrency constitutes membership in a platform developed to facilitate transactions of certain goods or services. As a result of the strong network effect among users to participate on the platform and the rigidity induced by market-clearing with token speculators, the market can break down with no equilibrium. While user optimism of future price appreciation raises user participation, and consequently reduces the risk of breakdown, speculator sentiment instead exacerbates it by crowding out users. The presence of realistic informational frictions

also mitigates this risk of market breakdown because users systematically underreact to information about platform fundamentals, both favorable and unfavorable, at the cost of worse average platform performance. In addition, the potential for strategic attacks when transactions are recorded on a blockchain by miners acts as a drag on the platform by feeding back into both the incentives of miners to mine and of users to join the platform, which makes such attacks more likely. Our model also provides several predictions for cryptocurrency price changes that are broadly consistent with recent empirical evidence.

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 (2014a), Risk-Taking, Rent-Seeking, and Investment when Financial Markets are Noisy, mimeo Bank of Chile, Toulouse School of Economics, and Yale University.

Albagli, Elias, Christian Hellwig, and Aleh Tsyvinski (2014b), Dynamic Dispersed Information and the Credit Spread Puzzle, mimeo Bank of Chile, 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.

Allen, Franklin, Stephen Morris, and Hyun Song Shin (2096), Beauty Contests and Iterated Expectations in Asset Markets, *Review of Financial Studies* 19.3, 719-752.

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

Beaudry, Paul, and Franck Portier (2006), Stock Prices, News, and Economic Fluctuations, *American Economic Review* 96, 1293-1307.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta (2019), The Blockchain Folk Theorem, *Review of Financial Studies* 32.5, 1662-1715.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, Catherine Casamatta, and Albert Menkveld (2018), Equilibrium Bitcoin Pricing, Working paper.

Blanchard, Olivier J. and Mark W. Watson (1982), Bubbles, Rational Expectations,and Financial Markets,î inCrisis in the Economic and Financial Structure, ed. by P. Wachtel, pp. 295ñ315. Lexington, Lexington, MA.

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

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

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

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.

Diba, B. T., and H. I. Grossman (1988), The Theory of Rational Bubbles in Stock Prices, Economic Journal 98, 746-754.

Easley, David, Maurenn O'Hara, and Soumya Basu (2019), From Mining to Markets: The Evolution of Bitcoin Transaction Fees, *Journal of Financial Economics*, forthcoming.

Evans, David (2003), The Antitrust of Multi-sided Platform Markets, *Yale Journal on Regulation* 20, 325-381.

Gao, Zhenyu, Michael Sockin, and Wei Xiong (2019), Learning about the Neighborhood, mimeo CUHK, UT Austin, and Princeton University.

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.

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

Hu, Albert, Christine Parlour, and Uday Rajan (2018), Cryptocurrencies: Stylized Facts on a New Investible Instrument, mimeo Changsha Intelligent Driving Institute, UC Berkeley, and University of Michigan Ross School of Business.

Huberman, Gur, Jacob Leshno, and Ciamac C. Moallemi (2019), An Economic Analysis of the Bitcoin Payment System, mimeo Columbia Business School.

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

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

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

Liu, Yukun and Aleh Tsyvinski (2019), Risks and Returns of Cryptocurrency, mimeo Rochester Simon Business School and Yale University.

Liu, Yukun, Aleh Tsyvinski, and Xi Wu (2019), Common Risk Factors in Cryptocurrency, mimeo Rochester Simon Business School, Yale University, and NYU.

Pagnotta, Emiliano (2018), Bitcoin as Decentralized Money: Prices, Mining, and Network Security, mimeo Imperial College.

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

Rochet, Jean-Charles and Jean Tirole (2003), Platform Competition in Two-sided Markets, *Journal of the European Economics Association* 1, 990-1029.

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

Schilling, Linda and Harald Uhlig (2019), Some Simple Bitcoin Economics, *Journal of Monetary Economics* 106, 16-26.

Shams, Amin (2019), What Drives the Covariation of Cryptocurrency Returns?, mimeo Ohio State University.

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

Sockin, Michael (2019), Informational Frictions in Intermediated Credit Markets, mimeo UT Austin.

Appendix A Microfoundation of Goods Trading

In this Appendix, we microfound the goods trading between two users when they are matched on the platform at date t. For clarity, we ignore the impact of strategic attacks on the likelihood of transactions being completed. As all objects are at date t, we omit time subscripts to economize on notation. We assume that user i maximizes its utility by choosing its consumption demand $\{C_i, C_j\}$ through trading with its trading partner user j subject to its budget constraint:

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

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

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

Furthermore, we assume that the goods endowments of the two users, A_i and A_j, are observable to them at the time of their trading, regardless of whether the platform strength A is publicly observed. Users behave competitively and take the prices of their goods as given.

Proposition 7 *User i's optimal good consumptions are*

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

and the price of his good is

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

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

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

and the ex ante utility benefit of all users before observing their goods endowments is

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

Proposition 7 shows that each user spends a fraction $1-\eta_c$ of his endowment on consuming his own good $C_i(i)$ and a fraction η_c on the good of his trading partner $C_j(i)$. The price of each good is determined by its endowment relative to that of the other good. One user's good is more valuable when the other user has a greater endowment, and consequently each user needs to take into account the endowment of his trading partner when making his own decision. The proposition demonstrates that the expected utility of a user in the platform is determined by not only his own endowment e^{A_i} but also the endowments of other users. This latter component arises from the complementarity in the user's utility function.

Appendix B Microfoundation for Strategic Attacks

In this Appendix, we provide a microfoundation for the strategic attack condition in the main text. Specifically, we examine whether rogue miners wish to collude to engage in a 51% "double spending" attack. This requires that a group of miners amasses enough computational power, compared to the rest of the mining community, to be able to verify, on average, the majority of transactions on the blockchain. Conceptually, by winning enough blocks to add to the blockchain, these corrupt miners will be able to eventually validate their own blocks on the longest chain, or to mine secretly a second chain longer than the current blockchain and broadcast it to the mining community as the legitimate chain. When this

occurs, these miners can reverse their own transactions to undo their expenditures, returning their spent tokens to their wallet to be spent again. This is the so-called "double spending" problem. By creating duplicate tokens, the strategic attack temporarily increases the token supply through fraudulent inflation.[20]

The benefits and costs of of a 51% attack are linked to participation by both users and miners. As more miners join the mining pool, the probability of completing any transaction and adding it to the blockchain falls, increasing the effective computational cost of attacking the currency. In addition, user and miner participation also increase the computational cost of an attack through the difficulty of mining each transaction, or the hashrate. Many PoW protocols, such as those of Bitcoin and Ethereum, set the hashrate to maintain a fixed average time for new blocks to be added to the blockchain, and the hashrate increases in the number of users and miners to prevent blocks from being added too quickly. As a consequence, having more subscribers and a more diverse mining pool can make the platform more secure.

We assume that miners lack commitment, which is consistent with the static incentives miners face because of free entry (Abadi and Brunnermeier (2018)). Any miner can attack the blockchain by engaging in a fifty-one percent attack to "double spend" the coins they receive from seignorage. If corrupt miners attack the blockchain, the strategic attack artificially inflates the token base by $\Phi\left(y_t+\psi\iota\right)-\Phi\left(y_t\right)$, for $\psi>0$, and the miner sells these additional tokens to earn $\left(\Phi\left(y_t+\psi\iota\right)-\Phi\left(y_t\right)\right)P_t$ in additional revenue. These additional tokens have to be absorbed by users and speculators by increasing the effective token supply to $\Phi\left(y_t+\psi\iota\right)$. In addition, since the corrupt miners add over half the blocks to the blockchain, they earn fifty percent of the transaction fees from users and seignorage. As a result of increased waiting times and service denials, users also experience a loss in expectation of half their trade surplus.[21]

To acquire fifty-one percent of the computing power, corrupt miners must replicate the mining power of the existing $N_{M,t}$ miners by expending a convex technological cost $\alpha N_{M,t}^2$, where $\alpha>0$. That the cost is convexly increasing in the number of miners $N_{M,t}$ reflects that it is increasingly difficult to acquire more mining power because of additional hardware and electricity costs.[22] To join the strategic attack, a potential attacker has to pay a participation

[20]To date, the major attacks on blockchains have been 51%. In 2015, the Bitcoin mining pool ghash.io voluntarily committed to reducing its share of mining power from over fifty percent to less than forty percent to assuage fears of it coordinating a potential 51% attack amongst its miners on the currency. There is even a website, Crypto51, that tracks the computational cost of a 51% attack in real-time.

[21]In addition to fraud and theft, hackers have engaged in 51% attacks to disrupt the blockchain and deny service to undermine confidence in the cryptocurrency. It should be stressed that, while hackers can disrupt the blockchain and double spend, they cannot steal tokens from user wallets.

[22]Implicitly, we assume that, to avoid detection by the mining pool, which could result in punishment and unraveling the attack, that these rogue miners must acquire additional computing power to compete with their own honest mining.

cost, which can be viewed as the cost or disutility of coordinating with the other attackers, that we normalize to 1 in the numeraire good.

Suppose that $N_{M,t}$ miners providing mining services at date t and that a fraction p_t of miners attack and split the proceeds from the attack equally. They then need to acquire half of total mining power and, consequently, they must acquire $N_{M,t}$ in additional mining power. An attack will occur when the benefit, the fraudulent seignorage and additional $\frac{1}{2}$ fraction of the seignorage and transaction fees, is greater than the cost of doubling the existing computing power of the mining community

$$\left(\Phi\left(y_t+\psi\iota\right)-\Phi\left(y_t\right)+\frac{1}{2}\left(\Phi\left(y_t\right)-\Phi\left(y_t-\iota\right)\right)\right)P_t+\frac{1}{2}\frac{\beta}{2}U_t-\alpha N_{M,t}^2\geq 0,$$

When this situation happens, a strategic attack occurs. Notice, however, that when this condition is satisfied that all miners will want to attack the platform, which will dilute the mining power and undermine a strategic attack. If all miners increase their mining by $N_{M,t}$ units, then the no miner achieves fifty-one percent of the mining power on the platform. As this cannot be an equilibrium, the miners must play a mixed strategy when a strategic attack is possible. The probability of a miner attacking, p_t, is the date t probability then ensures that every miner is indifferent to attacking based on the outcome of an i.i.d. draw of a Bernoulli random variable with $\Pr\left(Attack\right)=p_t$. By the weak LLN, exactly a fraction p_t of the existing mining pool will attack. This probability satisfies that the fraction $\frac{1}{p_t}$ of the revenue from attacking is offset by the disutility of participation

$$\frac{\left(\Phi\left(y_t+\psi\iota\right)-\frac{1}{2}\Phi\left(y_t\right)-\frac{1}{2}\Phi\left(y_t-\iota\right)\right)P_t+\frac{1}{2}\frac{\beta}{2}U_t-\alpha N_{M,t}^2}{p_t N_{M,t}}-1=0,$$

from which follows, when $p_t>0$, that

$$p_t=\frac{\left(\Phi\left(y_t+\psi\iota\right)-\frac{1}{2}\Phi\left(y_t\right)-\frac{1}{2}\Phi\left(y_t-\iota\right)\right)P_t+\frac{1}{2}\frac{\beta}{2}U_t-\alpha N_{M,t}^2}{N_{M,t}}.$$

otherwise there is no attack. Consequently, we can interpret the strategic attack condition (11) as arising from a 51% attack on the currency, and the possibility of attack leads to a stability boundary in the state space of the platform.

Appendix C Proofs of Propositions

C.1 Proof of Proposition 1

We first examine the decision of a user to purchase the token. We first recognize that each user's expectation about P_{t+1}, $E\left[P_{t+1}\middle|\,\mathcal{I}_t\right]$, depends on each user's expectation of A_{t+1}. By

the Bayes Rule, it is straightforward to conclude that the conditional posterior of users about A_{t+1} after observing A_t and Q_t is Gaussian $A_{t+1}|\mathcal{I}_t \sim \mathcal{N}\left(\hat{A}_{t+1}, \hat{\tau}_A^{-1}\right)$, where the conditional estimate and precision satisfy

$$\begin{aligned} \hat{A}_{t+1} &= A_t + \mu + \frac{\tau_Q}{\tau_\varepsilon + \tau_Q} Q_t, \\ \hat{\tau}_A &= \tau_\varepsilon + \tau_Q. \end{aligned}$$

We define τ as the stopping time, at which the platform fails as a result of the breakdown of the token market. We shall derive the conditions that determine τ later. Conditional on $t < \tau$, the expected utility of user i, who chooses to purchase the token at t, from transacting with another user is

$$E\left[U_{i,t} \,|\mathcal{I}_t,\ \tau > t,\ A_{it},\ \text{matching with user } j\right] = e^{(1-\eta_c)A_{i,t}} E\left[e^{\eta_c A_{j,t}} \,|\mathcal{I}_t\right],$$

which is monotonically increasing with the user's own endowment $A_{i,t}$. Note that $E\left[e^{\eta_c A_{j,t}} \mid \mathcal{I}_t\right]$ is independent of $A_{i,t}$, but dependent on the strategies used by other users. It then follows that user i will follow a cutoff strategy that is monotonic in its own type $A_{i,t}$.

Suppose that every user uses a cutoff strategy with a threshold of A_t^*. Then, the expected utility of user i is

$$E\left[U_{i,t}|\mathcal{I}_t, \tau > t\right] = e^{(1-\eta_c)A_{i,t} + \eta_c A_t + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A_t - A_t^*}{\tau_\varepsilon^{-1/2}}\right) \mathbf{1}_{\{\tau > t\}},$$

since losing a transaction is independent of the identities of the two transacting parties.

To determine the equilibrium threshold, consider a user with the critical endowment $A_{it} = A_t^*$. As this marginal user must be indifferent to his purchase choice, it follows that

$$E\left[(1-\beta)\, U_{i,t} + P_{t+1} |\, \mathcal{I}_t, A_{it} = A_t^*\right] = RP_t + \kappa,$$

which is equivalent to

$$(1-\beta)\, e^{(1-\eta_c)A_{i,t} + \eta_c A_t + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A_t - A_t^*}{\tau_\varepsilon^{-1/2}}\right) \mathbf{1}_{\{\tau > t\}} + E\left[P_{t+1} |\, \mathcal{I}_t\right] = RP_t + \kappa, \quad (15)$$

with $A_{i,t} = A_t^*$. Fixing the critical value A_t^*, the expected token price $E\left[P_{t+1} |\, \mathcal{I}_t\right]$, and the price P_t, we see that the LHS of equation (15) is monotonically increasing in $A_{i,t}$, since $1 - \eta_c > 0$. This confirms the optimality of the cutoff strategy that users with $A_{i,t} \geq A_t^*$ acquire the token to join the platform, and users with $A_{i,t} < A_t^*$ do not. Since $A_{i,t} = A_t + \varepsilon_{i,t}$, it then follows that a fraction $\Phi\left(-\sqrt{\tau_\varepsilon}\,(A_t^* - A_t)\right)$ of the users enter the platform, and a fraction $\Phi\left(\sqrt{\tau_\varepsilon}\,(A_t^* - A_t)\right)$ choose not to. As one can see, it is the integral over the idiosyncratic endowment of users ε_i that determines the fraction of potential users on the platform.

By substituting P_t from equation (5) into equation (15), we obtain an equation to determine the equilibrium cutoff $A_t^* = A_t^*(\mathcal{I}_t)$:

$$\begin{aligned}
&(1-\beta)\, e^{A_t+(1-\eta_c)(A_t^*-A_t)+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A_t-A_t^*}{\tau_\varepsilon^{-1/2}}\right)\mathbf{1}_{\{\tau>t\}}+E\left[P_{t+1}\middle|\,\mathcal{I}_t\right] \\
= \;& e^{\frac{\sqrt{\tau_\varepsilon}}{\lambda_P-\lambda_S}(A_t-A_t^*)-\frac{1}{\lambda_P-\lambda_S}y_t+\frac{\lambda_S}{\lambda_P-\lambda_S}\zeta_t}+\kappa. \qquad (16)
\end{aligned}$$

Define $z_t = \sqrt{\tau_\varepsilon}\,(A_t^* - A_t)$, which determines the population that buys the token. We can rewrite equation (16) as

$$\begin{aligned}
&(1-\beta)\, e^{\left[(1-\eta_c)\tau_\varepsilon^{-1/2}+\frac{1}{\lambda_P-\lambda_S}\right]z_t+A_t+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_t\right)\mathbf{1}_{\{\tau>t\}} \qquad (17) \\
&\qquad +e^{\frac{1}{\lambda_P-\lambda_S}z_t}\left(E\left[P_{t+1}\middle|\,\mathcal{I}_t\right]-\kappa\right) \;=\; e^{-\frac{1}{\lambda_P-\lambda_S}y_t+\frac{\lambda_S}{\lambda_P-\lambda_S}\zeta_t}
\end{aligned}$$

Note that the first term in the LHS of equation (17) has a humped shape with respect to z_t, and the second term is an exponential function of z_t with a coefficient that may be either positive or negative. As the RHS of equation (17) is constant with respect to z_t, this equation may have zero, one, two, or three roots:

- If $E\left[P_{t+1}\middle|\,\mathcal{I}_t\right]-\kappa \leq 0$, the LHS has a humped shape with a maximum at $\bar{z}$, and it may intersect with the RHS at zero or two points:
  1. If $LHS(\bar{z}) < RHS$, then equation (17) has no root.
  2. If $LHS(\bar{z}) > RHS$, then equation (17) has two roots.
- If $E\left[P_{t+1}\middle|\,\mathcal{I}_t\right]-\kappa > 0$, the LHS is non-monotonic with $LHS(-\infty)=0$, $LHS(\infty)=\infty$, and one local maxium $\ddot{z}$ and one local minimum $\dot{z}$ in $(-\infty,\infty)$, and it may intersect the RHS at one or three points:
  3. If $RHS < LHS(\dot{z})$ or if $RHS > LHS(\ddot{z})$, then equation (17) has one root.
  4. If $LHS(\dot{z}) < RHS < LHS(\ddot{z})$, then equation (17) has three roots.

In the first scenario outlined above, there is no equilibrium, and the token market breaks down. Note that A_t shifts up and down the left-hand side of equation (17). Thus, equation (17) has no root when A_t is sufficiently small. For this situation to occur, the speculative motive, $E\left[P_{t+1}\mid\mathcal{I}_t\right]-\kappa$, must be nonpositive, otherwise equation (17) has one or three roots. This condition is also satisfied when A_t is sufficiently small because $E\left[P_{t+1}\mid\mathcal{I}_t\right]$ is increasing with A_t. Thus, the token market breaks down when A_t falls below a certain critical level,

which we denote as $A^c(y_t, Q_t, \zeta_t)$. Thus, the stopping time τ of the platform's disbandment is

$$\tau = \{\inf\ t:\ A_t < A^c(y_t, Q_t, \zeta_t)\}.$$

Finally, note that, since the only difference among users is the value of their transaction benefit, $E[U_{i,t} \mid \mathcal{I}_t, \tau > t]$, which is monotonically increasing in $A_{i,t}$ regardless of the mass of users that join the platform, it follows that, regardless of the strategies of other users, it is always optimal for each user i to follow a cutoff strategy.

C.2 Proof of Proposition 2

The first part of the proposition follows from the derivation of Proposition 1 and the definition of A^c. This proof characterizes the determinants of the fundamental critical level A^c.

With regard to speculator sentiment, notice from equation (17) that, when $E[P_{t+1} \mid \mathcal{I}_t] - \kappa$ is nonpositive, there is a critical value of speculator sentiment $\zeta^c(A_t, y_t, Q_t)$:

$$\begin{aligned}\zeta_t^c \;=\; \frac{\lambda_P - \lambda_S}{\lambda_S} \log\Bigg\{\sup_{z_t}\Bigg\{(1-\beta)\, e^{\left[(1-\eta_c)\tau_\varepsilon^{-1/2} + \frac{1}{\lambda_P - \lambda_S}\right] z_t + A_t + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_t\right) \\ + e^{\frac{1}{\lambda_P - \lambda_S} z_t}\left(E[P_{t+1} \mid \mathcal{I}_t] - \kappa\right)\Bigg\}\Bigg\} + \frac{y_t}{\lambda_S},\end{aligned}$$

such that no equilibrium exists if $\zeta_t \geq \zeta^c(A_t, y_t, Q_t)$, with the convention that $\zeta_t^c = -\infty$ if the argument in the log is negative.

It is straightforward to see that, in the high price (low cutoff) equilibrium, the Implicit Function Theorem implies that $\frac{dz_t}{d\zeta_t} > 0$. Since the user participation is $\Phi(-z_t)$, it follows that an increase in ζ_t exacerbates the market breakdown region by lowering user participation. Since ζ_t is i.i.d., there is only this static impact of an increase in speculator sentiment on the equilibrium cutoff. As such, by lowering user participation, it shifts up $A^c(y_t, Q_t, \zeta_t)$ for any given pair of $\{y_t, Q_t\}$.

We next consider how user optimism Q_t impacts the market breakdown region. Since user optimism Q_t raises each user's estimate of the resale value of the token at date $t+1$, it raises user participation and the token price at date t. Since Q_t is i.i.d., this is the only impact of an increase in user optimism. As such, it shifts down the market breakdown threshold, $A^c(y_t, Q_t, \zeta_t)$, for any given pair of $\{y_t, \zeta_t\}$.

Similarly, an increase in the user participation cost, κ, deters user participation at all dates and therefore exacerbates the market breakdown by both increasing the cost today and lower the expected retrade value of the token tomorrow through the reduced participation in the future. As such, it also shifts up $A^c(y_t, Q_t, \zeta_t)$.

C.3 Proof of Proposition 3

We first establish that the map from the demand fundamental A_t to the equilibrium user cutoff for joining the platform is monotone when the highest price equilibrium is always played.[23]

Suppose that the token price at date $t+1$, P_{t+1}, is increasing in A_t for all (y_t, Q_t, ζ_t) triples in the high price equilibrium. Then, since A_t follows a random walk, its cumulative distribution function satisfies the Feller Property, and the conditional expectation operator preserves this relation

$$\frac{\partial E\left[P_{t+1} \mid \mathcal{I}_t\right]}{\partial A_t} = E\left[\frac{\partial P\left(A_t + \mu + \varepsilon_{t+1}, y_{t+1}, Q_{t+1}, \zeta_{t+1}\right)}{\partial A_t} \mid \mathcal{I}_t\right] > 0,$$

where the expectation is take over ε_{t+1}. Consequently, $E\left[P_{t+1} \mid \mathcal{I}_t\right]$ is increasing in A_t.Then, we can rewrite equation (17) as the function G_t

$$\begin{aligned} G_t &= (1-\beta)\, e^{\left[(1-\eta_c)\tau_\varepsilon^{-1/2} + \frac{1}{\lambda_P - \lambda_S}\right] z_t + A_t + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_t\right) \mathbf{1}_{\{\tau > t\}} \\ &\quad + e^{\frac{1}{\lambda_P - \lambda_S} z_t} \left(E\left[P_{t+1} \middle| \mathcal{I}_t\right] - \kappa\right) - e^{-\frac{1}{\lambda_P - \lambda_S} y_t + \frac{\lambda_S}{\lambda_P - \lambda_S} \zeta_t} \\ &\equiv 0. \end{aligned} \tag{18}$$

Assuming existence of an equilibrium, applying the Implicit Function Theorem to G_t, one has that

$$\frac{\partial z_t}{\partial A_t} = -\frac{\partial G_t / \partial A_t}{\partial G_t / \partial z_t},$$

where

$$\frac{\partial G_t}{\partial A_t} = (1-\beta)\, e^{\left[(1-\eta_c)\tau_\varepsilon^{-1/2} + \frac{1}{\lambda_P - \lambda_S}\right] z_t + A_t + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_t\right) + e^{\frac{1}{\lambda_P - \lambda_S} z_t} \frac{\partial E\left[P_{t+1} \mid \mathcal{I}_t\right]}{\partial A_t} > 0.$$

In the high price equilibrium, the RHS of equation (17) intersects the hump-shaped curve of the LHS in z_t on the left-side of the hump, and consequently $\frac{\partial G_t}{\partial z_t} \geq 0$.[24] It then follows that, in the high price equilibrium, $\frac{\partial z_t}{\partial A_t} < 0$. Therefore, user participation $\Phi(-z_t)$ is increasing in A_t.

Furthermore, since $P_t = e^{-\frac{1}{\lambda_P - \lambda_S} z_t - \frac{1}{\lambda_P - \lambda_S} y_t + \frac{\lambda_S}{\lambda_P - \lambda_S} \zeta_t}$, it follows that

$$\frac{\partial P_t}{\partial A_t} = -\frac{P_t}{\lambda_P - \lambda_S} \frac{\partial z_t}{\partial A_t} > 0.$$

Consequently, P_t is increasing in A_t in the high price equilibrium. Since the choice of t and $t+1$ are arbitrarily, P_t is increasing in A_t generically if the high price equilibrium is played at each date.

[23] Our proof is based on a modified argument of Milgrom and Roberts (1994) for comparative statics in the presence of strategic complementarity.

[24] $\frac{\partial G_t}{\partial z_t} = 0$ at the critical value of z_t at which breakdown occurs if the fundamentals deteriorate.

Finally, since user optimism Q_t enters into the user's problem by raising the expected resale token price, it raises user participation and the token price. In contrast, speculator sentiment ζ_t lowers user participation by leading to nonfundamental upward pressure on the token price. Since it also lowers user participation, the overall impact on the token price is ambiguous. To see this, we rewrite equation (18) as

$$\begin{aligned} H_t \equiv\ & (1-\beta)\, e^{(1-\eta_c)\tau_\varepsilon^{-1/2}(\tilde{z}_t+\lambda_S\zeta_t)+A_t+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-\tilde{z}_t-\lambda_S\zeta_t\right)\mathbf{1}_{\{\tau>t\}} \\ & -e^{-\frac{1}{\lambda_P-\lambda_S}\tilde{z}_t-\frac{1}{\lambda_P-\lambda_S}y_t}+E\left[P_{t+1}\mid\mathcal{I}_t\right]-\kappa=0, \end{aligned}$$

where the change of variables $\tilde{z}$ now absorbs speculator sentiment, so that the price is $P_t = e^{-\frac{1}{\lambda_P-\lambda_S}\tilde{z}_t-\frac{1}{\lambda_P-\lambda_S}y_t}$. Since speculator sentiment is i.i.d., and the equilibrium is Markovian in the state space (A_t, y_t, Q_t, ζ_t), the retrade value of the token is unaffected by changes in sentiment today. It is straightforward by the Implicit Function Theorem to the above equation that

$$\frac{\partial\tilde{z}_t}{\partial\zeta_t}=-\frac{dH_t/d\zeta_t}{dH_t/d\tilde{z}_t}.$$

Since $\tilde{z}$ enters H_t symmetrically as z does in equation (17), $dH_t/d\tilde{z}_t > 0$ in the high price equilibrium. In contrast, $dH_t/d\zeta_t$ is

$$dH_t/d\zeta_t \propto (1-\eta_c)\,\tau_\varepsilon^{-1/2}-\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-\tilde{z}_t-\lambda_S\zeta_t\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-\tilde{z}_t-\lambda_S\zeta_t\right)}=(1-\eta_c)\,\tau_\varepsilon^{-1/2}-\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_t\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_t\right)}.$$

Consequently, if z_t is sufficiently small, then $dH_t/d\zeta_t > 0$, while if z_t is sufficiently large, then $dH_t/d\zeta_t < 0$. Since $\frac{\partial P_t}{\partial\zeta_t}=-\frac{1}{\lambda_P-\lambda_S}P_t\frac{\partial\tilde{z}_t}{\partial\zeta_t}$, it follows that $\frac{\partial P_t}{\partial\zeta_t} > 0$ for z_t sufficiently small, and $\frac{\partial P_t}{\partial\zeta_t} < 0$ for z_t sufficiently large. Since $z_t = A_t^* - A_t$, the result follows.

C.4 Proof of Proposition 4

In this proof, we construct an equilibrium by conjecturing and verifying that every user follows a cutoff strategy with a threshold of A_t^*. Since there can be multiple equilibria, as in the perfect information model, we assume that users will always coordinate on the lowest threshold (or highest token price) equilibrium. This helps ensure a positive relation between the price and the demand fundamental, A_t, which is needed for a cutoff equilibrium to exist.

Given our assumption about the sufficient statistic in token price in equation (8), the posterior about A_t given all public information is Gaussian $A_t|\mathcal{I}_t \sim \mathcal{N}\left(\hat{A}_t, \Sigma_{A,t}\right)$ with the

conditional mean and variance satisfying the Kalman Filter recursion:

$$\begin{aligned}
\hat{A}_t &= \begin{bmatrix} \tau_A^{-1} \\ \Sigma_{A,t-1}+\tau_A^{-1} \\ \Sigma_{A,t-1}+\tau_A^{-1} \end{bmatrix}' \left(\begin{bmatrix} \tau_Q^{-1} & 0 & 0 \\ 0 & \Sigma_{A,t-1}+\frac{\lambda_S^2}{\tau_\varepsilon\tau_\zeta} & \Sigma_{A,t-1} \\ 0 & \Sigma_{A,t-1} & \Sigma_{A,t-1}+\tau_\varepsilon^{-1}\tau_v^{-1} \end{bmatrix} + \tau_A^{-1}\iota\iota' \right)^{-1} \\
&\quad \cdot \begin{bmatrix} Q_{t-1} \\ p_t - \hat{A}_{i,t-1} - \mu \\ v_t - \hat{A}_{i,t-1} - \mu \end{bmatrix} + \hat{A}_{t-1}, \\
\Sigma_{A,t} &= \Sigma_{A,t-1} + \tau_A^{-1} - \begin{bmatrix} \tau_A^{-1} \\ \Sigma_{A,t-1}+\tau_A^{-1} \\ \Sigma_{A,t-1}+\tau_A^{-1} \end{bmatrix}' \\
&\quad \cdot \left(\begin{bmatrix} \tau_Q^{-1} & 0 & 0 \\ 0 & \Sigma_{A,t-1}+\frac{\lambda_S^2}{\tau_\varepsilon\tau_\zeta} & \Sigma_{A,t-1} \\ 0 & \Sigma_{A,t-1} & \Sigma_{A,t-1}+\tau_\varepsilon^{-1}\tau_v^{-1} \end{bmatrix} + \tau_A^{-1}\iota\iota' \right)^{-1} \begin{bmatrix} \tau_A^{-1} \\ \Sigma_{A,t-1}+\tau_A^{-1} \\ \Sigma_{A,t-1}+\tau_A^{-1} \end{bmatrix}.
\end{aligned}$$

By the Sherman-Morrison formula, since $\iota\iota'$ is an outer product of column matrices, we can express

$$(C+\vec{u}\vec{v}')^{-1} = C^{-1} - \frac{C^{-1}\vec{u}\vec{v}'C^{-1}}{1+\vec{v}'C^{-1}\vec{u}},$$

and therefore

$$\begin{aligned}
&\left(\begin{bmatrix} \tau_Q^{-1} & 0 & 0 \\ 0 & \Sigma_{A,t-1}+\frac{\lambda_S^2}{\tau_\varepsilon\tau_\zeta} & \Sigma_{A,t-1} \\ 0 & \Sigma_{A,t-1} & \Sigma_{A,t-1}+\tau_\varepsilon^{-1}\tau_v^{-1} \end{bmatrix} + \tau_A^{-1}\iota\iota' \right)^{-1} \\
&= \begin{bmatrix} \tau_Q & 0 & 0 \\ 0 & \frac{\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\left(\Sigma_{A,t-1}^{-1}+\tau_\varepsilon\tau_v\right)}{\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v} & -\frac{\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\tau_\varepsilon\tau_v}{\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v} \\ 0 & -\frac{\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\tau_\varepsilon\tau_v}{\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v} & \frac{\tau_\varepsilon\tau_v\left(\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\right)}{\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v} \end{bmatrix} \\
&\quad - \frac{\frac{1}{\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v+\tau_\varepsilon} \begin{bmatrix} \tau_Q\left(\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v\right) \\ \frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\Sigma_{A,t-1}^{-1} \\ \tau_\varepsilon\tau_v\Sigma_{A,t-1}^{-1} \end{bmatrix} \begin{bmatrix} \tau_Q\left(\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v\right) \\ \frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\Sigma_{A,t-1}^{-1} \\ \tau_\varepsilon\tau_v\Sigma_{A,t-1}^{-1} \end{bmatrix}'}{(\tau_A+\tau_Q)\left(\Sigma_{A,t-1}^{-1}+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v\right)+\Sigma_{A,t-1}^{-1}\left(\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}+\tau_\varepsilon\tau_v\right)}.
\end{aligned}$$

It then follows that the above recursion simplifies to

$$\begin{aligned}
\hat{A}_t &= \hat{A}_{t-1} + \mu + \Sigma_{A,t} \begin{bmatrix} \frac{\tau_Q}{1+\left(\tau_A+\tau_Q\right)\Sigma_{A,t-1}} \\ \frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2} \\ \tau_\varepsilon\tau_v \end{bmatrix}' \begin{bmatrix} Q_{t-1} \\ p_t - \hat{A}_{i,t-1} - \mu \\ v_t - \hat{A}_{i,t-1} - \mu \end{bmatrix}, \\
\Sigma_{A,t} &= \frac{1}{\frac{\tau_A+\tau_Q}{1+\left(\tau_A+\tau_Q\right)\Sigma_{A,t-1}} + \frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2} + \tau_\varepsilon\tau_v}.
\end{aligned}$$

Note that the Ricatti Equation for $\Sigma_{A,t}$ has a deterministic steady-state, Σ_A, that satisfies

$$\left(\tau_A+\tau_Q\right)\Sigma_A^2+\Sigma_A-\frac{1}{\tau_\varepsilon\tau_v+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}}=0,$$

which has a unique positive, real root:

$$\Sigma_A=\sqrt{\left(\frac{1}{2\left(\tau_A+\tau_Q\right)}\right)^2+\frac{1}{\tau_A+\tau_Q}\frac{1}{\tau_\varepsilon\tau_v+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}}}-\frac{1}{2\left(\tau_A+\tau_Q\right)}.$$

Consequently, a stationary solution to the Kalman Filter exists and the economy, from any initial conditions, converges to this steady-state solution as $t\to\infty$.

Then, the common conditional belief follows

$$\hat{A}_t=\hat{A}_{t-1}+\mu+\Sigma_A^{-1}\begin{bmatrix}\frac{\tau_Q}{\frac{1}{2}+\sqrt{\frac{1}{4}+\frac{\tau_A+\tau_Q}{\tau_\varepsilon\tau_v+\frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}}}}\\ \frac{\tau_\varepsilon\tau_\zeta}{\lambda_S^2}\\ \tau_\varepsilon\tau_v\end{bmatrix}'\begin{bmatrix}Q_{t-1}\\ p_t-\hat{A}_{i,t-1}-\mu\\ v_t-\hat{A}_{i,t-1}-\mu\end{bmatrix}.$$

Given the steady-state posterior based on common knowledge, it is straightforward by the Bayes Rule to update to the steady-state private posterior of user i, which is Gaussian $A_t|\mathcal{I}_{i,t}\sim\mathcal{N}\left(\hat{A}_{i,t},\Sigma_i\right)$ with the conditional mean and variance given by

$$\begin{aligned}\hat{A}_{i,t}&=\Sigma_i\Sigma_A^{-1}\hat{A}_t+\Sigma_i\tau_\varepsilon A_{i,t},\\ \Sigma_i^{-1}&=\Sigma_A^{-1}+\tau_\varepsilon.\end{aligned}$$

Note that the conditional estimate of $\hat{A}_i$ of user i is increasing in its own endowment A_i.

Given each user's posterior $A_{i,t}$, it is straightforward to construct by the Bayes Rule their posterior for A_{t+1} after observing Q_t, which will also be Gaussian $A_{t+1}|\mathcal{I}_{i,t}\sim\mathcal{N}\left(\hat{A}_{i,t+1},\Sigma_i+\hat{\tau}_A^{-1}\right)$, where the conditional estimate and precision satisfy:

$$\begin{aligned}\hat{A}_{i,t+1}&=\hat{A}_{i,t}+\mu+\frac{\tau_Q}{\tau_A+\tau_Q}Q_t,\\ \hat{\tau}_A&=\tau_A+\tau_Q,\end{aligned}$$

and consequently the conditional forecast of the next period's demand fundamental A_{t+1} by users is also increasing in their endowment. This completes our characterization of learning by users.

We define τ as the stopping time, at which the platform fails as a result of the breakdown of the token market. Then, the expected utility of user i if all other users follow a cutoff

strategy with cutoff A_t^* is

$$\begin{aligned} E\left[U_{i,t}|\mathcal{I}_{i,t},\tau>t\right] &= e^{(1-\eta_c)A_{i,t}+\eta_c A_t^*+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}E\left[e^{\eta_c(A_t-A_t^*)}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A_t-A_t^*}{\tau_\varepsilon^{-1/2}}\right)\middle|\ \mathcal{I}_{i,t}\right] \\ &= e^{(1-\eta_c)A_{i,t}+\eta_c\hat{A}_{i,t}+\frac{1}{2}\eta_c^2\left(\Sigma_i+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\hat{A}_{i,t}+\eta_c\Sigma_i-A_t^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\tau_\varepsilon\Sigma_i}}\right). \end{aligned}$$

It follows that the transaction benefit to user i is monotonically increasing in his private signal, $A_{i,t}$.

Furthermore, let us conjecture that the token price is (weakly) increasing in A_t. Then, it follows that $E\left[P_t\mid\ \mathcal{I}_{i,t}\right]$ is increasing in a user's private signal $A_{i,t}$, since with P_t nonnegative $\frac{\partial}{\partial A_t}E\left[P_t\mid\ \mathcal{I}_{i,t}\right]=E\left[\frac{\partial P_t}{\partial A_t}\mid\ \mathcal{I}_{i,t}\right]$. Consequently, $E\left[(1-\beta)U_{i,t}+P_{t+1}\mid\mathcal{I}_{i,t}\right]$ is also increasing in $A_{i,t}$. As such, the user will follow a cutoff strategy

$$X_{i,t}=\begin{cases}1 & \text{if}\ \ A_{i,t}\geq A^*\left(\hat{A}_t,y_t,Q_t,p_t\right)\\ 0 & \text{if}\ \ A_{i,t}<A^*\left(\hat{A}_t,y_t,Q_t,p_t\right)\end{cases},$$

for a critical productivity $A^*\left(\hat{A}_t,y_t,Q_t,p_t\right)$. Since the household with the critical productivity A_t^* must be indifferent to its token choice at the cutoff, it follows that

$$E\left[(1-\beta)U_{i,t}+P_{t+1}\mid\mathcal{I}_{i,t}\right]+\kappa-RP=0,$$

which implies

$$(1-\beta)\,e^{(1-\eta_c)A_{i,t}+\eta_c\hat{A}_{i,t}+\frac{1}{2}\eta_c^2\left(\Sigma_i+\tau_\varepsilon^{-1}\right)}\Phi\left(\frac{\eta_c\tau_\varepsilon^{-1/2}+\frac{\hat{A}_{i,t}+\eta_c\Sigma_i-A_t^*}{\tau_\varepsilon^{-1/2}}}{\sqrt{1+\tau_\varepsilon\Sigma_i}}\right)+E\left[P_{t+1}\mid\mathcal{I}_{i,t}\right]-\kappa=RP_t$$

with $A_{i,t}=A_t^*$. Those with the LHS above RP_t purchase the currency, and those below choose to refrain. This equation does not depend on the unobserved A_t or speculator optimism, ζ_t. As a result, $A_t^*=A^*\left(\hat{A}_t,y_t,Q_t,p_t\right)$. Substituting for the beliefs of the marginal user, we arrive at the indifference condition

$$\begin{aligned} &(1-\beta)\,e^{A_t^*+\eta_c\Sigma_i\Sigma_A^{-1}\left(\hat{A}_t-A_t^*\right)+\frac{1}{2}\eta_c^2\left(\Sigma_i+\tau_\varepsilon^{-1}\right)}\Phi\left(\eta_c\sqrt{\tau_\varepsilon^{-1}+\Sigma_i}+\frac{\frac{\Sigma_i\Sigma_A^{-1}}{\tau_\varepsilon^{-1/2}}\left(\hat{A}_t-A_t^*\right)}{\sqrt{1+\tau_\varepsilon\Sigma_i}}\right)\mathbf{1}_{\{\tau>t\}} \\ &+E\left[P_{t+1}|\mathcal{I}_t\right]-\kappa=e^{-\frac{\sqrt{\tau_\varepsilon}}{\lambda_P-\lambda_S}(A_t^*-p_t)-\frac{1}{\lambda_P-\lambda_S}y_t}, \end{aligned} \tag{19}$$

which is measurable to the public information. Substituting for Σ_i and

$$\hat{\zeta}_t=\sqrt{\tau_\varepsilon}\left(\hat{A}_t-p_t\right),$$

we recover the cutoff condition stated in the proposition. Since $\left(\hat{A}_t, \hat{\zeta}_t\right)$ is informationally equivalent to $\left(\hat{A}_t, p_t\right)$, we can express the optimal cutoff policy of households as

$$X_{i,t} = \begin{cases} 1 & \text{if } A_{i,t} \geq A^* \left(\hat{A}_t, y_t, Q_t, \hat{\zeta}_t\right) \\ 0 & \text{if } A_{i,t} < A^* \left(\hat{A}_t, y_t, Q_t, \hat{\zeta}_t\right) \end{cases},$$

Given that each user follows a cutoff strategy, it follows that the token price takes the functional form in (5). Thus, we recover the linear statistic p_t from the token price and the linear statistic v_t from the volume signal, both as conjectured.

C.5 Proof of Proposition 5

Rewriting (10) as

$$\begin{aligned} &(1-\beta)\, e^{\left[\left(1-\frac{\eta_c}{1+\tau_\varepsilon \Sigma_A}\right)\tau_\varepsilon^{-1/2} + \frac{1}{\lambda_P - \lambda_S}\right] z_t + \hat{A}_t + \frac{1}{2}\eta_c^2\left(\Sigma_A + \tau_\varepsilon^{-1}\right)} \\ &\cdot \Phi\left(\eta_c \tau_\varepsilon^{-1/2}\sqrt{1 + \frac{\tau_\varepsilon \Sigma_A}{1+\tau_\varepsilon \Sigma_A}} - \frac{z_t}{\sqrt{\left(1+\tau_\varepsilon \Sigma_A\right)\left(1+2\tau_\varepsilon \Sigma_A\right)}}\right) \mathbf{1}_{\{\tau > t\}} \\ &+ e^{\frac{1}{\lambda_P - \lambda_S} z_t} \left(E\left[P_{t+1} | \mathcal{I}_t^*\right] - \kappa\right) = e^{-\frac{1}{\lambda_P - \lambda_S} y_t + \frac{\lambda_S}{\lambda_P - \lambda_S}\hat{\zeta}_t}, \end{aligned} \tag{20}$$

it is immediate that (17) is the informational frictions analogue of (17) with $\hat{A}_t$ replacing A_t, $\hat{\zeta}_t$ replacing ζ_t, and the several terms related to the expected convenience yield for the marginal user now reflecting the uncertainty about A_t through the posterior variance of public beliefs, Σ_A. Notice that the modifications by Σ_A do not alter the sign of any of the modified terms compared to the perfect information case. It then follows that we can repeat the same arguments from Proposition 3 to establish the comparative statics for $\hat{A}_t$, $\hat{\zeta}_t$, and Q_t.

We now apply the Implicit Function Theorem by rewriting the above expression as

$$\begin{aligned} G \;=\; &(1-\beta)\, e^{\hat{A}_t + \frac{1}{\lambda_P - \lambda_S} z_t + \left(1-\frac{\eta_c}{1+\tau_\varepsilon \Sigma_A}\right)\frac{1}{\sqrt{\tau_\varepsilon}} z_t + \frac{1}{2}\eta_c^2\left(\Sigma_A + \tau_\varepsilon^{-1}\right)} \\ &\cdot \Phi\left(\eta_c \tau_\varepsilon^{-1/2}\sqrt{1 + \frac{\tau_\varepsilon \Sigma_A}{1+\tau_\varepsilon \Sigma_A}} - \frac{z_t}{\sqrt{\left(1+\tau_\varepsilon \Sigma_A\right)\left(1+2\tau_\varepsilon \Sigma_A\right)}}\right) \\ &+ e^{\frac{1}{\lambda_P - \lambda_S} z_t} \left(E\left[P_{t+1} | \mathcal{I}_t^*\right] - \kappa\right) - e^{\frac{\lambda_S}{\lambda_P - \lambda_S}\hat{\zeta}_t - \frac{1}{\lambda_P - \lambda_S} y_t}, \end{aligned}$$

where $G \equiv 0$. Holding fixed the retrade value of the token, $E\left[P_{t+1} | \mathcal{I}_t^*\right]$, it then follows that:

$$\frac{dA_t^*}{d\Sigma_A} = -\frac{dG/d\Sigma_A}{dG/dz_t}.$$

Since (10) is analogous to (7), from the proof of Proposition 1, G is hump-shaped in z_t and, in the high price (low cutoff) equilibrium, $dG/dz_t > 0$.This sign leads to the intuitive

comparative statics, compared to the unstable low price (high cutoff) equilibrium. Consequently, the sign of $dA_t^*/d\Sigma_A$ is negative the sign of $dG/d\Sigma_A$. Notie that Σ_A only enters G through the expected transaction benefit or contemporaneous convenience yield for the marginal household $E\left[U_{i,t} \mid \mathcal{I}_t^*\right]$. It then follows that $dG/d\Sigma_A = dE\left[U_{i,t} \mid \mathcal{I}_t^*\right]/d\Sigma_A$. Since $E\left[U_{i,t} \mid \mathcal{I}_t^*\right]$ is always nonnegative it follows that we can express $dE\left[U_{i,t} \mid \mathcal{I}_t^*\right]/d\Sigma_A$ as

$$\begin{aligned}\frac{dE\left[U_{i,t} \mid \mathcal{I}_t^*\right]}{d\Sigma_A} &= \frac{1}{2}\eta_c^2 + \frac{\eta_c\sqrt{\tau_\varepsilon}}{\left(1+\tau_\varepsilon\Sigma_A\right)^2} z_t \\ &+ \frac{\frac{1}{2}\eta_c\tau_\varepsilon^{-1/2} + \frac{1}{2}\frac{(3+4\Sigma_A)\tau_e}{1+2\tau_\varepsilon\Sigma_A} z_t}{\left(1+\tau_\varepsilon\Sigma_A\right)^{3/2}\sqrt{1+2\tau_\varepsilon\Sigma_A}} \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}\sqrt{1+\frac{\tau_\varepsilon\Sigma_A}{1+\tau_\varepsilon\Sigma_A}} - \frac{z_t}{\sqrt{(1+\tau_\varepsilon\Sigma_A)(1+2\tau_\varepsilon\Sigma_A)}}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}\sqrt{1+\frac{\tau_\varepsilon\Sigma_A}{1+\tau_\varepsilon\Sigma_A}} - \frac{z_t}{\sqrt{(1+\tau_\varepsilon\Sigma_A)(1+2\tau_\varepsilon\Sigma_A)}}\right)}.\end{aligned}$$

Notice that there is a cutoff $z_t^{**} < 0$ such that $\frac{dE[U_{i,t} \mid \mathcal{I}_t^*]}{d\Sigma_A} \geq 0$ if $z_t \geq z_t^{**}$ and $\frac{dE[U_{i,t} \mid \mathcal{I}_t^*]}{d\Sigma_A} < 0$ for $z_t < z_t^{**}$. It then follows that $\frac{dA_t^*}{d\Sigma_A} \leq 0$ for $z_t \geq z_t^{**}$ and $\frac{dA_t^*}{d\Sigma_A} \geq 0$ for $z_t < z_t^{**}$. Consequently, uncertainty Σ_A raises the cutoff when participation is sufficiently high (z_t sufficiently small), while uncertainty lowers the cutoff when participation is sufficiently low (z_t sufficiently large).

We now relax our assumption on the retrade value of the token. Suppose instead of holding fixed the token retrade value, we hold fixed uncertainty Σ_A at date $t+1$. The thought experiment is we are then considering a one time increase in Σ_A at date t. Notice since user and speculator sentiment are i.i.d. that we need only focus on how the token price varies with the demand fundamental, A_t, when forecasting the retrade value of the token tomorrow. Further notice from the law of motion of user beliefs derived in the proof of Proposition 4 that informational frictions have no impact on how the user sentiment signal Q_t is used in forecasting A_{t+1} (same weight in conditional mean $\frac{\tau_Q}{\tau_Q+\tau_A}$).

Notice now that the convexity (or concavity) of the token price in the filtered demand fundamental is given by:

$$\frac{1}{P_t}\frac{\partial^2 P_t}{\partial \hat{A}_t^2} = \left(1 + \left|\frac{\partial A_t^*}{\partial \hat{A}_t}\right|\right)^2 - \frac{\partial^2 A_t^*}{\partial \hat{A}_t^2},$$

since $\frac{dA_t^*}{d\hat{A}_t} \leq 0$ as argued above. Informational frictions preserve the relation found with $\hat{A}_t's$ perfect information counterpart, albeit with underreaction. Notice now, from the equilibrium cutoff condition (17) that, as $\hat{A}_t \to \infty$, $A_t^* \to -\infty$, since the retrade value $E\left[P_{t+1} \mid \mathcal{I}_t^*\right]$ is increasing in A_t and the convenience yield $E\left[U_{i,t} \mid \mathcal{I}_t^*\right]$ becomes unbounded. Consequently, even for the users with the lowest endowments, the benefits of joining become arbitrarily large, which corresponds to an arbitrarily large token price. At the opposite extreme, since the token price is nonnegative, and therefore bounded from below, it either falls to some finite minimum or no long exists if $\hat{A}_t$ falls below its critical threshold $A^c\left(Q_t, y_t, \hat{\zeta}_t\right)$. Since

$\frac{dA_t^*}{d\hat{A}_t} \leq 0$ and $\frac{dA_t^*}{d\hat{A}_t}$ becomes increasingly negative so as to be unbounded for arbitrarily high $\hat{A}_t \leq 0$, it follows that $\frac{d^2A_t^*}{d\hat{A}_t^2} \leq 0$ when an equilibrium exists (and undefined otherwise) and consequently the token price P_t is convex in $\hat{A}_t$ whenever an equilibrium exists. Notice that, if it were not convex, then P_t must then have an even number of inflection points ($\frac{d^2P_t}{d\hat{A}_t^2} = 0$), which can be ruled out intuitively since (by linearity)

$$\frac{\partial E\left[P_t \mid \mathcal{I}_t^*\right]}{\partial \hat{A}_t} = (1-\beta)\sum_{t'=t}^{\tau} E\left[\frac{1}{R^{t'-t}} E\left[E\left[\frac{\partial U_{i,t'}}{\partial \hat{A}_t} \mid \mathcal{I}_{t'}^*\right] \mid \mathcal{I}_{t'-1}^* ...\right] \mid \mathcal{I}_t^*\right],$$

and the only direct impact of $\hat{A}_t$ on $U_{i,t'}$ is to increase the convenience yield by a factor of $e^{\hat{A}_t}$.

Since market breakdown occurs for $p_t \leq A_t^c$, and therefore when A_t is sufficiently small, since the cutoff function at date $t+1$ is unchanged, it then follows that increasing Σ_A at date t lowers 4 for high values of $\hat{A}_t$ where more probability weight is put on the convex part of the price function, and raises it for low $\hat{A}_t$ where more probability weight is put on the concave part of the price function near the step function of the non-existence boundary.

A one time increase in uncertainty therefore subsidizes participation and the token price for low performing platforms (high z_t) at the expense of participation and the token price for high performing platforms (low z_t). From our comparative statics analysis, a high cutoff, z_t, for a fixed y_t corresponds to low $\hat{A}_t$, low Q_t, and high $\hat{\zeta}_t$.

C.6 Proof of Proposition 6

From the miner optimization problem (12), it is straightforward to see that, with free entry, miners must indifferent to participating on the platform. Consequently, the number of potential miners that choose to mine is given by

$$N_{M,t} = \frac{\left(\Phi\left(y_{t-1}+\iota\right) - \Phi\left(y_{t-1}\right)\right) P_t + \frac{\beta}{1+\chi_t} U_t}{1+\chi_t} e^{\xi_t}$$

Substituting the optimal number of miners, $N_{M,t}$ from (12) into the attack condition given in (11) conjecturing an attack, $\chi_t = 1$, we can define

$$\begin{aligned} f\left(y_t, P_t, E\left[U_t \mid \mathcal{I}_t\right]\right) &= \left(\Phi\left(y_t+\psi\iota\right) - \frac{1}{2}\Phi\left(y_t\right) - \frac{1}{2}\Phi\left(y_t-\iota\right)\right) P_t \\ &\quad + \frac{1}{2}\frac{\beta}{2} E\left[U_t \mid \mathcal{I}_t\right] - \frac{\alpha e^{2\xi_t}}{4}\left(\left(\Phi\left(y_t\right) - \Phi\left(y_t-\iota\right)\right) P_t + \frac{\beta}{2} U_t\right)^2. \end{aligned}$$

There is an attack whenever $f\left(y_t, P_t, U_t\right) > 0$.[25] It is clear since ξ enters only through the

[25] Since there is no profit when $f\left(y_{t-1}, P_t, E\left[U_t \mid \mathcal{I}_t\right]\right) = 0$, and only a loss in revenue from honest mining, it follows that miners would rather not attack at the indifference threshold.

quadratic term that there exists a threshold $\xi^c(A_t, Q_t, \zeta_t)$ such that:

$$\{\chi_t = 1 : \xi_t < \xi^a(A_t, Q_t, \zeta_t)\},$$

where:

$$\xi^c(A_t, y_t, Q_t, \zeta_t) = \frac{1}{2}\log\frac{\left(\Phi(y_t+\psi\iota) - \frac{1}{2}\Phi(y_t) - \frac{1}{2}\Phi(y_t-\iota)\right)P_t + \frac{1}{2}\frac{\beta}{2}U_t}{\frac{a}{4}\left(\left(\Phi(y_t) - \Phi(y_t-\iota)\right)P_t + \frac{\beta}{2}E[U_t \mid \mathcal{I}_t]\right)^2}.$$

Assume now that $E[U_t \mid \mathcal{I}_t]$ and P_t are (weakly) increasing in A_t whenever P_t is positive, and we define $P_t = 0$ whenever a market equilibrium does not exist. Define:

$$x_t = \frac{\left(\Phi(y_t) - \Phi(y_t-\iota)\right)P_t + \frac{\beta}{2}U_t}{2},$$

and rewrite $f(y_t, P_t, E[U_t \mid \mathcal{I}_t])$ as:

$$f(y_t, P_t, x_t) = \left(\Phi(y_t+\psi\iota) - \Phi(y_t)\right)P_t + x_t - \alpha e^{2\xi_t}x_t^2.$$

Notice that $f(y_t, P_t, x_t)$ is concave in x_t, increasing for $x_t < \frac{1}{2\alpha e^{2\xi_t}}$ from 0 to $\frac{1}{4\alpha e^{2\xi_t}}$, and then decreasing to $-\infty$ for $x_t > \frac{1}{2\alpha e^{2\xi_t}}$. It has two roots at $x_t \in \left\{0, \frac{1}{\alpha e^{2\xi_t}}\right\}$.

It then follows that a strategic attack occurs whenever $x_t \leq \frac{1}{\alpha e^{2\xi_t}}$, or when A_t is sufficiently small. This occurs because U_t and P_t are (weakly) increasing in A_t and U_t and P_t converge to 0 as $A_t \to -\infty$, as there is no benefit to any (positive measure of) users joining the platform. Consequently, since P_t and U_t are (weakly) increasing in A_t, it follows there is a connected set $\underline{\mathcal{A}}_t = \{A_t : A_t < A^a(y_t, Q_t, \zeta_t; \xi_t)\}$, where $A^a(y_t, Q_t, \zeta_t; \xi_t) = \inf_{A_t}\{f(y_t, P_t, x_t) = 0\}$, such that $\chi_t = 1$ when $A_t < \underline{\mathcal{A}}_t$.

In contrast, when A_t is sufficiently large, it must be the case that $\lim_{A_t\to\infty} f(y_t, P_t, x_t) < 0$ since the highest-order terms in P_t and U_t are quadratic through $-x_t^2$. Consequently, there is a connected set $\bar{\mathcal{A}}_t = \left\{A_t : A_t > \bar{A}^a(y_t, Q_t, \zeta_t; \xi_t)\right\}$, where $\underline{A}^a(y_t, Q_t, \zeta_t; \xi_t) = \sup_{A_t}\{f(y_t, P_t, x_t) = 0\}$, such that $\chi_t = 0$ when $A_t > \bar{\mathcal{A}}_t$.

Consequently, it follows that there is a strategic attack when $A_t \in \underline{\mathcal{A}}_t$ and no attack when $A_t \in \bar{\mathcal{A}}_t$. What remains is to determine if $\underline{\mathcal{A}}_t \cup \bar{\mathcal{A}}_t = \mathbb{R}$ or if there are more strategic attack regions for some $A_t > \underline{\mathcal{A}}_t$. Notice now that $f(y_t, P_t, x_t)$ is a quadratic function of x_t and, by Descartes' Rule of Signs, has at most one positive root, which we know must exist by the above arguments. Consequently, $f(y_t, P_t, x_t)$ has one zero when, substituting for x_t,

$$\frac{\beta}{2}E[U_t \mid \mathcal{I}_t] = \frac{1}{\alpha e^{2\xi_t}} + \sqrt{\left(\frac{1}{\alpha e^{2\xi_t}}\right)^2 + 4\frac{\Phi(y_{t-1}+\psi\iota) - \Phi(y_t)}{\alpha e^{2\xi_t}}P_t} - \left(\Phi(y_t) - \Phi(y_t-\iota)\right)P_t. \tag{21}$$

Therefore, it must be the case that $A^a(y_t, Q_t, \zeta_t; \xi_t) = \underline{A}^a(y_t, Q_t, \zeta_t; \xi_t)$, and therefore the strategic attack region can be characterized as

$$\chi_t = \begin{cases} 1, & \xi_t < \xi^a(A_t, y_t, Q_t, \zeta_t) \\ 0, & \xi_t \geq \xi^a(A_t, y_t, Q_t, \zeta_t) \end{cases},$$

or alternatively

$$\chi_t = \begin{cases} 1, & A_t < A^a(, y_t, Q_t, \zeta_t; \xi_t) \\ 0, & A_t \geq A^a(y_t, Q_t, \zeta_t; \xi_t) \end{cases}.$$

In addition, we recognize from (21) that, since a higher ξ_t lowers the critical $\frac{\beta}{2}U_t$, all else equal, it follows that $A^a(y_t, Q_t, \zeta_t; \xi_t)$ is decreasing in ξ_t.

One may be concerned that no mining equilibrium may exist if, conditional on no attack, miners want to attack the blockchain, while, conditional on an attack, no miner ex post wants to attack the blockchain. This does not occur because the (convex) cost of attacks from less miners falls faster than the benefit from the attack from lower revenue. To see this, notice that the only endogenous object determined by users is A_t^*, and a strategic attack raises A_t^*, lowering prices and transaction fees, by reducing the benefit of joining the platform for all users. This is equivalent to a fall in A_t to some $\tilde{A}_t$. Since if an attack that would occur at A_t would also occur at $A_t' < A_t$, by the above arguments, it follows that if a strategic attack would occur when users and miners do not anticipate an attack, it would also occur if it is anticipated. Consequently, such a strategic attack inconsistency issue does not arise.

Furthermore, although there cannot be an inconsistency in the attack decision on the platform, there can be self-fulfilling prophecies in which both the no attack and the attack equilibria can be sustained. This arises because both the benefit $(\Phi(y_t + \psi\iota) - \Phi(y_t))P_t$ and the cost $x_t - \alpha e^{2\xi_t}x_t^2$ of an attack are positively correlated.

Finally, we verify that the token price and transaction fees are indeed (weakly) increasing in A_t. Let us conjecture that the token price, P_t, and transaction fees are (weakly) increasing in A_t. We further define $P_t = 0$ whenever there is market breakdown. Under this assumption, strategic attacks occur when A_t is sufficiently small by the above arguments. It then follows that strategic attacks preserve the monotonicity of P_t in A_t from Proposition 3, confirming the conjecture. Similarly, since a higher token price is associated with a higher user population, and consequently higher transaction fees, this confirms our second conjecture. Further, since the strategic attacks occur when the mining fundamental, ξ_t, is sufficiently small, and mining has no direct impact on platform performance when there is no strategic attack, it follows that the token price and user participation are (weakly) increasing in ξ_t.

C.7 Proof of Proposition 7

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

$$C_i(i) \quad : \quad \frac{1-\eta_c}{C_i(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_i, \tag{22}$$

$$C_j(i) \quad : \quad \frac{\eta_c}{C_j(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = \theta_i p_j, \tag{23}$$

where θ_i is the Lagrange multiplier for the budget constraint. Rewriting (23) as

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

Dividing equations (22) 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 user's budget constraint in (14), we obtain:

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

The market-clearing for the user'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 (22) also gives the price of the good produced by user i. Since the user'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:

$$p_i = \frac{1-\eta_c}{C_i(i)} U\left(C_i(i), C_j(i); \mathcal{N}\right) = e^{\eta_c(A_j - A_i)}. \tag{24}$$

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 user's budget constraint at $t = 2$.

It then follows that, conditional on matching with another user on the platform, the expected utility of user i conditional on his endowment A_i and a successful match is:

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

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

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

Finally, the ex ante expected utility benefit of a user before it learns its endowment A_i is

$$\begin{aligned} U_0 &= E\left[E\left[U_i|A_i,A\right]|A\right] \\ &= E\left[e^{(1-\eta_c)A_i+\eta_c A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)\mid A\right] \\ &= e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\varepsilon^{-1}}\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right)\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A^*}{\tau_\varepsilon^{-1/2}}\right). \end{aligned}$$