A Model of Cryptocurrencies*

Michael Sockin†    Wei Xiong‡

February 2022

Abstract

We model a cryptocurrency as membership in a digital platform developed to facilitate transactions between users of certain goods or services. Because membership demand exhibits network effects, the rigidity induced by the cryptocurrency price having to clear membership demand with speculator token supply can lead to market breakdown. We show that token retradability mitigates this risk of breakdown on younger platforms by harnessing user optimism. It worsens this fragility, however, when sentiment trading by speculators crowds out users. Strategic attacks by miners also exacerbate this fragility because users’ anticipation of future losses depresses the token’s resale value.

*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.

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

‡Princeton University and NBER. Email: 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.

Our model analyzes the properties of cryptocurrencies on platforms that rely on network effects. Cryptocurrencies cover a wide range of tokens and coins facilitated by crypto technologies. For simplicity, we anchor our analysis on utility tokens, but our model can also be applied to coins and altcoins. Utility tokens are native currencies accepted on decentralized digital platforms that often provide intrinsic benefit to participants. 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.

We follow Sockin and Xiong (2021) to model a cryptocurrency as membership in 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.  

---

1In 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.
The platform fills the users’ transaction needs by pooling together a large number of users with the need to transact with each other. A user’s transaction need is determined 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, 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. If more users join the platform, each benefits more from joining the platform and is willing to pay a higher token price. Sockin and Xiong (2021) highlight that tokenization helps to decentralize the control of the platform and thus makes it possible for the platform to commit to not abusing its users, even though the commitment comes at the expense of not having an owner with an equity stake to subsidize user participation and maximize the platform’s network effect.

We depart from the emphasis of Sockin and Xiong (2021) on platform governance by focusing on token price dynamics and stability. We assume that, in addition to acting as a membership to fulfill transaction needs, the token is also an investable asset—for both users and speculators with no transaction needs—to capitalize on the future growth of the platform. To analyze these dual roles, our model features infinitely many periods, with users and speculators holding different beliefs about the capital gain from investing in the token. In each period, a new generation of users chooses whether to join the platform by purchasing tokens from both existing token holders and from new token issuance by the platform. The token issuance follows a deterministic schedule and allows us to study the life-cycle dynamics of the platform. In deciding whether to join the platform, a user trades off the cost of buying a token with the benefits from both transacting goods on the platform and expected token price appreciation. 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. This threshold and the token price are jointly determined by users’ token demand, which is based on their common goods endowment and optimism about token price appreciation, and the net supply of tokens by speculators, which is also determined by their sentiment about token price appreciation. Despite the inherent nonlinearity induced by each user’s cutoff strategy, we derive the equilibrium in an analytical form and systematically characterize the
platform’s performance.

Our analysis highlights the ability of token retradability to harness user optimism to mitigate the fragility that network effects introduce onto cryptocurrency platforms. Because of network effects, users’ demand curve for tokens is backward-bending, and the token price may fail to simultaneously clear the supply and demand for tokens. In this case, the token market breaks down, which occurs when the platform’s demand fundamental is sufficiently weak. Users’ optimism about token price appreciation can alleviate this instability by inducing users to join the platform even when their transaction needs are low. In contrast, speculators’ sentiment exacerbates this fragility by raising the cost for users to participate and crowding them out. Consequently, token retradability is a powerful tool for improving platform performance when it capitalizes user optimism. In contrast, it harms performance when it incentivizes outsiders like speculators to hold tokens as well, as their enthusiasm acts as a tax on user participation and exacerbates the platform’s instability. This echos the key insight of Sockin and Xiong (2021) who argue, in the context of platform governance, that cryptocurrency platforms operate best when only users participate.

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. As a result, 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. We illustrate that more mature platforms not only have lower expected log token prices, but also higher log token price volatility, and that these life-cycle effects are more pronounced for platforms whose fundamentals have weaker growth rates. Consequently, the ability of retradability to harness the optimism of users to mitigate platform stability declines as the platform matures.

To further illustrate how outsiders hamper platform performance, we extend the model to incorporate miners who provide accounting and custodial services to record transactions on the platform’s blockchain according to the Proof of Work protocol. 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 trade-off 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 benefit from creating fraudulent seignorage and stealing other miners’ transaction fees. Although such attacks do not directly lead the platform to fail, our analysis shows that users’ anticipation of future losses from miner attacks may exacerbate the fragility of the token market, especially when the mining cost is high. Consequently, having outsiders with whom there is a conflict of interest with users exacerbates the instability of cryptocurrency platforms.

Our framework provides a rich set of empirical predictions for token price appreciation, which is directly measurable by the econometrician and has thus been 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—it equals to the total cost of capital and participation minus the convenience yield from transaction surplus. Consistent with Liu and Tsyvinski (2021), 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 the persistence of user participation costs and convenience yields, as well as the size effect that Liu, Tsyvinski, and Wu (2021) show in the cross-section of cryptocurrency price appreciation.

Our paper contributes to the emerging literature on cryptocurrencies. Biais, Bisiere, Bouvard, Casamatta and Menkveld (2021) 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 the cryptocurrency, as well as subtle interactions between the strategic attacks by miners and the cryptocurrency’s fragility. Cong, Li, and Wang (2021) also emphasize the strong network effect among 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 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 emphasizing the interaction between token retradability, user optimism, and speculator sentiment. In addition, we show that miner attacks may exacerbate
the platform fragility through the users’ anticipation of losses from future attacks. 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. Schilling and Uhlig (2019) study the role of monetary policy in the presence of a cryptocurrency that acts as a private fiat currency.

Our analysis of the impact of miner attacks on platform stability overlaps with that of Pagnotta (2020), 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. Easley, O’Hara, and Basu (2019) analyze the rise of transactions fees in Bitcoin through the strategic interaction of users and miners. Chiu and Koepppl (2017) consider the optimal design of a cryptocurrency, and emphasize the importance of scale in deterring double-spending by buyers. Cong and He (2019) investigate the tradeoff of smart contracts in overcoming adverse selection while also facilitating oligopolistic collusion, while Biais, Bisiere, Bouvard and Casamatta (2019) consider the strategic interaction among miners. Capponi, Olafsson, and Alsabah (2021) illustrate how the nature of mining may lead to a concentration of mining power, while Abadi and Brunnermeier (2018) examine disciplining writers to a blockchain technology with static incentives. Saleh (2021) explores how decentralized consensus can be achieved with the Proof of Stake (PoS) protocol. Even without strategic attacks, Capponi, Jia and Wang (2021) demonstrate how miners can impose more subtle costs on users by leaking information about their transactions for front-running.

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 3 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 \( \{N_t, O_t\} \) in each period, with \( N_t \cap O_t = \emptyset \) and \( N_t \cup O_t = [0, 1] \). Let \( X_{i,t} = 1 \) if user $i$ purchases the token, i.e., $i \in N_t$, 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.

We follow Sockin and Xiong (2021) to model the users’ transactions on the platform. 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

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

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

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

where $\varepsilon^A_{t+1} \sim iid N(0, 1)$. 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 $\tau_\varepsilon$ as a measure of dispersion among users in the platform.\footnote{In an earlier version of the paper, we considered an extended setting in which the platform fundamental is unobservable. In this setting, users use their endowments as a private signal about this fundamental, and not only the token price but also the transaction history on the blockchain act as public signals that aggregate their dispersed information. This second public signal reflects that the blockchain technology supporting cryptocurrencies acts as an indelible and verifiable ledger that records the decentralized transactions that take place on the platform. In this extended setting, we show that informational frictions attenuate the risk of breakdown by dampening price volatility and platform performance.}

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 $\eta_i e^{A_{i,t}}$ units of good $i$ to exchange for $\eta_j e^{A_{j,t}}$ units of good $j$. Consequently, both users are able to consume both goods, with user $i$ consuming
\[
C_{i,t}(i) = (1 - \eta_i) e^{A_{i,t}}, \quad C_{j,t}(i) = \eta_i e^{A_{j,t}},
\]
and user $j$ consuming
\[
C_{i,t}(j) = \eta_j e^{A_{i,t}}, \quad C_{j,t}(j) = (1 - \eta_j) e^{A_{j,t}}.
\]
As formally shown by Sockin and Xiong (2021), these consumption allocations between these two paired users can be microfounded through a 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, $P_{t+1} - R P_t$, 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 $\beta$ 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
\[
\max_{X_{i,t}} \left( E \left[ (1 - \beta) U_{i,t} + P_{t+1} \mid I_{i,t} \right] - R P_t - \kappa \right) X_{i,t},
\]
where $I_{i,t}$ 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.\(^3\)

\(^3\)As Liu and Tsyvinski (2021) 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.
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 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. As we will analyze later, this transition underlies several interesting life-cycle 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, \( I_{i,t} \), of each user. In addition to observing the platform fundamental, \( A_t \), each user knows the value of his own goods endowment, \( A_{i,t} \). To facilitate our analysis of how users’ speculation of the token price may affect their participation in the platform, we also endow all users with a public signal about next period’s innovation to aggregate endowment, \( Q_{t+1} \), which by construction is orthogonal to \( A_t \):

\[
Q_t = \varepsilon_{t+1}^A + \tau^{-1/2} \varepsilon_t^Q,
\]

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, \( E[P_{t+1} | I_{i,t}] \), 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. Consequently, \( I_{i,t} = \sigma \left( \{ A_{i,t}, \{ P_s, Q_s \}_{s \leq t} \} \right) \) is user \( i \)'s full information set.

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

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

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 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 \( E[P_{t+1} \mid I_{i,t}] \), the common optimism among users induced
by $Q_t$ helps to overcome their participation cost $\kappa$. Given the cutoff strategy for each user, who participates if $A_{i,t} \geq A^*_i$, the total token demand of users is given by

$$\int_{-\infty}^{\infty} X_{i,t} (I_{i,t}) d\Phi (\varepsilon_{i,t}) = \Phi (\sqrt{\tau} (A_t - A^*_i)).$$  

(3)

### 1.2 Token Supply and Speculators

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

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

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

$$\Phi (y_t) = \Phi (y_0 + tt),$$

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. With our specification, at most a unit measure of tokens exists. All of our key qualitative results are unchanged, however, if instead we capped token supply at some maximum $\bar{y} < \infty$.

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 holds noisy expectations of the next-period token price:

$$E^S [P_{t+1} \mid I_t] = (1 + e^{\zeta_t}) RP_t,$$

where $I_t$ is the public information set, $RP_t$ is the required risk-neutral return for holding the token to the next period, and $\zeta_t \sim iid \mathcal{N} (0, \sigma^2)$ is the speculators’ aggregate sentiment. We consider speculators to be outsiders to the platform. They are distinct from the users who actually participate on the platform. They do not have private information about the platform’s fundamental or fully understand how to interpret the implications of the same public information as the users. Instead, similar to Black (1986), we argue that 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 currencies, such speculators are likely ubiquitous on cryptocurrency exchanges. We separate the speculators’ sentiment from the users’ optimism so that we can analyze their distinct effects on the token market equilibrium.

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

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

where $\lambda_S > 0$ represents the elasticity of speculators’ token demand with respect to their speculative motive, and $\lambda_P > 0$ represents the elasticity of the speculators’ token demand with respect to the price. When speculators are more optimistic about the next-period token price, their 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 lower demand from the speculators and thus more token supply to the 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 (3), we obtain that

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

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 speculator sentiment $\zeta_t$.\(^4\)

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.\(^5\) In a later section (Section 3), we expand the model to

\(^4\)We implicitly assume a frictionless secondary market for tokens. See, for instance, Capponi and Jia (2021) for liquidity issues associated with cryptocurrency exchanges.

\(^5\)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.
include a group of validators who record the transactions for a fee according to the Proof of Work protocol, 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 Sockin and Xiong (2021), over $A_{i,t}$ for $A_{i,t} \geq A^*_t$ to arrive at the realized surplus from user transactions:

$$
U_t = e^{A_t + \frac{1}{2}((1-\eta_s)^2 + \eta_e^2)\tau^{-1}} \Phi \left( (1 - \eta_s) \tau^{-1/2} + \frac{A_t - A^*_t}{\tau^{-1/2}} \right) \Phi \left( \eta_s \tau^{-1/2} + \frac{A_t - A^*_t}{\tau^{-1/2}} \right).
$$

In contrast to Sockin and Xiong (2021), we assume that the owner can commit to these policies. As the platform’s token base matures from inflation, the compensation to the owner shifts from seignorage to transaction fees.

### 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:

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

where each user’s demand $X_{i,t}$ depends on its information set $I_{i,t}$. 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.

---

6 We assume the owner completes all transactions without censorship or charging monopoly markups. See Huberman, Leshno and Moallemi (2021) for how Proof of Work decentralized consensus can overcome these issues at the cost of transaction delays. We also assume that the owner can commit to a token inflation schedule. See Cong, Li, and Wang (2022) for a setting in which the owner cannot commit.
2 Equilibrium

We characterize the equilibrium in each period \( t \) when \( A_t \) and \( \zeta_t \) 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 \( \zeta_t \). We use the notation \( \mathcal{I}_t = \{ A_t, y_t, Q_t, \zeta_t \} \) to represent the state variables at \( t \), which also represent the set of public information to all users. The public signal, \( Q_t \), contains information about \( A_{t+1} \), and thus is useful to users for forming their expectations about the token price in period \( t+1 \), \( P_{t+1} \). Given that all users 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:

\[
\hat{A}_{t+1} = A_t + \mu + \frac{\tau Q}{\tau + \tau Q} Q_t.
\]

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:

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

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

\[
(1 - \beta) e \left( (1-\delta)(A^*_t - A_t) + A_t + \frac{1}{2} \eta \tau \sigma^{-1} \right) \phi \left( \eta \tau^{-1/2} - \frac{A^*_t - A_t}{\tau^{-1/2}} \right) 1_{\{\tau > t\}} + E \left[ P_{t+1} | \mathcal{I}_t \right] - \kappa
\]

\[
= e^{-\frac{\sqrt{\tau}}{\sqrt{\lambda_S}} (A^*_t - A_t) - \frac{1}{4} \frac{1}{\sqrt{\lambda_S}} y_t + \frac{\lambda_S}{2} \zeta_t},
\]
where $\tau$ is the stopping time for the breakdown of the platform due to the failure of the token market clearing:

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

with $A^c(y_t, Q_t, \zeta_t)$ as a critical level for $A_t$, below which equation (6) has no root.

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

- If $E[P_{t+1} \mid I_t] - \kappa \leq 0$, equation (6) has zero or two roots.
- If $E[P_{t+1} \mid I_t] - \kappa > 0$, equation (6) has one or three roots.

4. In the dynamic equilibrium, the token price $P(A_t, y_t, Q_t, \zeta_t)$ is determined by equation (4) 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 $(A_t, y_t, Q_t, \zeta_t)$, according to equation (4) with $A^*_t$ as an implicit function of these state variables.

Equation (6) provides a fixed-point condition to determine the optimal cutoff in each period. The left-hand side of equation (6) 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 $E[P_{t+1} \mid I_t] - \kappa$ represent the user’s expected next-period token price net of the user’s participation cost $\kappa$. The right-hand side of equation (6) 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 (6) in a benchmark case when $E[P_{t+1} \mid I_t] - \kappa = 0$. 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 $\infty$. 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 $A^*_t \not\to \infty$, 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 (6) 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 (4). 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 $\zeta_t$. Proposition 1 shows that these two curves do not intersect when $A_t$ falls below a critical level $A^*_t \left(y_t, Q_t, \zeta_t\right)$, 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
$E [P_{t+1} \mid I_t] - \kappa > 0$, 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 to 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 $E [P_{t+1} \mid I_t] - \kappa < 0$, either as a result of users’ pessimism or a high participation cost $\kappa$, 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 $\kappa$ may lead to the failure of the platform. As each user does not account for his participation decision on other users through the network effect, this externality exacerbates the effect of $\kappa$ 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, $E [P_{t+1} \mid I_t] - \kappa$, is nonpositive.
2. The users’ demand fundamental is sufficiently low, i.e., $A_t < A^c (y_t, Q_t, \zeta_t)$, or equivalently speculator sentiment is sufficiently high, i.e. $\zeta_t > \zeta^c (A_t, y_t, Q_t)$.

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

Proposition 2 characterizes the determinants of the fundamental critical level $A^c (y_t, Q_t, \zeta_t)$ for the token market breakdown to occur. On the demand side, the users’ speculative motive, 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
Table I: Baseline Model Parameters

<table>
<thead>
<tr>
<th>Demand Fundamental:</th>
<th>$\mu = 0.01$, $\tau_A = 10$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Platform:</td>
<td>$y_0 = -0.84$</td>
</tr>
<tr>
<td>Sentiment:</td>
<td>$\tau_Q = 100$, $\tau_\xi = 2$, $\lambda_S = 1$, $\lambda_P = 2$</td>
</tr>
<tr>
<td>Users:</td>
<td>$\tau_\theta = 1$, $\eta_c = 0.3$, $\kappa = 0.03$, $R = 1.02$</td>
</tr>
</tbody>
</table>

$A$ 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 (2021) emphasize the role of token resale in 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
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 panel), and token supply (right panel) in the perfect information equilibrium. Baseline values are \( \zeta = 0 \), \( Q = 0 \), and \( y = 0.9 \).

(dynamic) stability of the potential equilibria.\(^7\) 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, \( Q_t \).

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

\(^7\)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 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
Figure 4: An illustration of the unconditional expected log token price (left panel) and log price volatility (right panel) over time. The solid line is the case when the growth rate of the fundamental is $\mu = 0.01$ and the dashed is the case in which $\mu = 0.10$.

holding the token. Since users are risk-neutral, the sum of the two pieces always equal the cost of carry plus the participation cost, $R + \frac{\kappa}{P_t}$ 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 $\mu$ and the token supply $y_t$ are the two key model parameters that determine the expected token price. We illustrate these effects in Figure 4 for two values of $\mu$. A platform with a higher $\mu$ 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 $\mu$ is high, the expected token price remains higher over time. Since more of the token return for high $\mu$ 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 $\mu$ 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.
3 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.\(^8\)

To illustrate how consensus protocols can impact platform performance and stability, we consider a simple extension of our setting in this section that incorporates Proof of Work mining. Our general insight will, however, also be valid for other consensus protocols, such as Proof of Stake, as long as the interests of validators may conflict with those of users. 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.\(^9\) 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 \(\xi_t\) measures the miner’s mining efficiency by inversely parameterizing the miner’s cost of mining. This mining efficiency \(\xi_t\) 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 \(\beta U_t\), which is a fraction of the transaction surplus, and the seignorage from token inflation, \((\Phi(y_t + \tau) - \Phi(y_{t-1})) P_t\). Consistent with many token platforms with PoW

---

\(^8\)This issue has also received significant attention in the literature. See, for instance, Chiu and Koeppl (2017), Pagnotta (2020), and Budish (2018).

\(^9\)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 (2021) 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).
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 \( \frac{\beta(y_{t-1} + t) - \Phi(y_{t-1})}{N_{M,t}} - e^{-\xi_t} \) in expected net gain.\(^{10}\)

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

\[
(\Phi(y_t + \psi_t) - \Phi(y_t)) P_t + \frac{(\Phi(y_{t-1} + t) - \Phi(y_{t-1})) P_t + \frac{\beta}{2} U_t}{2} \geq \alpha N_{M,t}^2, \tag{7}
\]

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 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 the Internet Appendix, 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 \( \xi_t \) thus maximizes his expected gain:

\[
\Pi_j = \max_{M_{j,t}} \left( \frac{(\Phi(y_{t-1} + t) - \Phi(y_{t-1})) P_t + \frac{\beta}{1+\chi_t} U_t}{1+\chi_t} - e^{-\xi_t} \right) M_{j,t}, \tag{8}
\]

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.

Note that relative to the equilibrium characterized in Section 2, the miners’ common mining efficiency \( \xi_t \) becomes an additional state variable. The following proposition shows that strategic attacks occur when either \( A_t \) or \( \xi_t \) falls below a certain level.

\(^{10}\)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 (2019) and Biais et al. (2019) for game theoretic investigations into these issues.
Proposition 4  The equilibrium has the following properties:

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

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

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 4, a strategic attack occurs when the mining fundamental and/or the user demand fundamental are sufficiently weak, since in these situations the number of 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 5 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 $\xi_t$, as formally derived in Proposition 4. 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.\textsuperscript{11} 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 5 (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

\textsuperscript{11}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.
on the platform’s stability.

4 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 (6), these three components satisfy the following relationship:

$$R = \frac{(1 - \beta) U^*_t}{P_t} + \frac{E[P_{t+1} | \mathcal{I}_t]}{P_t} - \frac{\kappa}{P_t}.$$ 

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 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.\(^{12}\) 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.\(^{13}\)

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

$$\frac{E[P_{t+1} | \mathcal{I}_t]}{P_t} - R = \frac{\kappa}{P_t} - \frac{(1 - \beta) U^*_t}{P_t}.$$ 

Consistent with the empirical findings of Hu, Parlour, and Rajan (2018) and Liu and Tsyvinski (2021), the expected excess capital gain in our setting does not exhibit conventional risk premia. The capital gain may still exhibit predictability through the underlying state variables that explain the convenience yield. These state variables are the demand fundamental,\(^{12}\)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.\(^{13}\)A subtle issue is how to measure the marginal user’s convenience yield in practice. If users were all identical, then 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.
user optimism, speculator sentiment, and token supply. Liu and Tsyvinski (2021), for in-
stance, show that investor attention, measured either with Google searches or Twitter post
counts for "Bitcoin", predicts future cryptocurrency returns, with positive (negative) atten-
tion, as measured by keywords, positively (negatively) predicting future weekly returns.14
Liu and Tsyvinski (2021) 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,
our model predicts a size effect in the capital gain of cryptocurrencies. This prediction
is consistent with Liu, Tsyvinski, and Wu (2021), who find a size factor in the cross sec-
tion of cryptocurrency returns, with size measured as either market capitalization, price, or
maximum price.

In addition, the persistence of the two return components $\frac{P_t}{I_t}$ and $\frac{(1-\beta)U_t^*}{P_t}$ in (9) can lead
to a positive autocorrelation in the capital gain:
\[
\text{Cov}
\left(
\begin{array}{c}
P_{t+2} \\
P_{t+1} \\
P_t \\
\end{array}
\right| I_{t-1}
\right)

= \text{Cov}
\left(
\begin{array}{c}
\frac{\kappa}{P_{t+1}} \\
\frac{(1-\beta)U_{t+1}^*}{P_{t+1}} \\
\frac{\kappa}{P_t} \\
\end{array}
\right| I_{t-1}
\right) > 0,
\]

because the innovations $\frac{P_{t+1} - E[P_{t+1} | I_t]}{P_t}$ and $\frac{P_{t+2} - E[P_{t+2} | I_{t+1}]}{P_{t+1}}$ are uncorrelated with rational
expectations. This positive autocorrelation implies momentum, as empirically documented
by Liu and Tsyvinski (2021) 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 (2021), 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 (9), 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

---

14Although the measure is constructed with searches for "Bitcoin" specifically, we view this measure as a
noisy proxy for interest in cryptocurrencies more generally.
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.

5 Conclusion

This paper develops a model to analyze price dynamics and stability of cryptocurrencies.
In our model, a cryptocurrency constitutes both an asset and a 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. In such a
setting, token retradability plays an important role in harnessing the optimism of users to
mitigate this instability. In contrast, it can exacerbate such fragility if it attracts speculators
whose enthusiasm crowds out users. These observations echo the key insight of Sockin and
Xiong (2021) that cryptocurrency platforms operate best in the absence of non-user partici-
pants, who could introduce conflicts of interest with users. As a result of token inflation, this
novel benefit of token retradability fades as the platform matures and the token price be-
comes driven more by the current platform fundamental. We further illustrate how outsiders
can exacerbate the platform’s instability by introducing miners to validate transactions on
the blockchain. The potential for strategic attacks feeds 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 implications 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.

Beaudry, Paul, and Franck Portier (2006), Stock Prices, News, and Economic Fluctuations,

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


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

Capponi, Agostino and Ruizhe Jia (2021), The Adoption of Blockchain-based Decentralized Exchanges, mimeo Columbia University.

Capponi, Agostino, Ruizhe Jia and Ye Wang (2021), The Evolution of Blockchain: From Lit to Dark, mimeo Columbia and ETH Zürich.


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


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


---

**Proofs of Propositions**

**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 $P_{t+1}$, $E[P_{t+1} \mid \mathcal{I}_t]$, 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 $A_{t+1} \mid \mathcal{I}_t \sim \mathcal{N}(\hat{A}_{t+1}, \hat{\tau}_A^{-1})$, where the conditional estimate and precision satisfy

\[
\hat{A}_{t+1} = A_t + \mu + \frac{\tau Q}{\tau \varepsilon + \tau Q} Q_t, \\
\hat{\tau}_A = \tau \varepsilon + \tau Q.
\]

We define $\tau$ 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 $\tau$ 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

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

which is monotonically increasing with the user’s own endowment $A_{i,t}$. Note that $E\left[e^{\eta_c A_{jt}} \mid \mathcal{I}_t\right]$ 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

\[
E[U_{i,t} \mid \mathcal{I}_t, \tau > t] = e^{(1-\eta_c)A_{i,t} + \eta_c A^*_t + \frac{1}{2}\eta_c^2 \tau \varepsilon^{-1} \Phi \left(\eta_c \tau \varepsilon^{-1/2} + \frac{A_t - A^*_t}{\tau \varepsilon^{-1/2}}\right)} 1_{\{\tau > t\}},
\]
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 $A_{it} = A^*_i$. As this marginal user must be indifferent to his purchase choice, it follows that

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

which is equivalent to

$$(1 - \beta) e^{(1 - \eta_c) A_{i,t} + \eta_c A_t + \frac{1}{2} \eta_c^2 \tau \varepsilon^{-1}} \Phi \left( \eta_c \tau \varepsilon^{-1/2} + \frac{A_t - A^*_i}{\tau \varepsilon^{-1/2}} \right) 1_{\{\tau > t\}} + E [P_{t+1} | \mathcal{I}_t] = RP_t + \kappa, \quad (A1)$$

with $A_{i,t} = A^*_i$. Fixing the critical value $A^*_i$, the expected token price $E [P_{t+1} | \mathcal{I}_t]$, and the price $P_t$, we see that the LHS of equation (A1) is monotonically increasing in $A_{i,t}$, since $1 - \eta_c > 0$. This confirms the optimality of the cutoff strategy that users with $A_{i,t} > A^*_i$ acquire the token to join the platform, and users with $A_{i,t} < A^*_i$ do not. Since $A_{i,t} = A_t + \varepsilon_{i,t}$, it then follows that a fraction $\Phi \left( -\sqrt{\tau \varepsilon} (A^*_i - A_i) \right)$ of the users enter the platform, and a fraction $\Phi \left( \sqrt{\tau \varepsilon} (A^*_i - A_i) \right)$ choose not to. As one can see, it is the integral over the idiosyncratic endowment of users $\varepsilon_i$ that determines the fraction of potential users on the platform.

By substituting $P_t$ from equation (4) into equation (A1), we obtain an equation to determine the equilibrium cutoff $A^*_i = A^*_i (\mathcal{I}_t)$:

$$(1 - \beta) e^{A_t + (1 - \eta_c) (A^*_i - A_t) + \frac{1}{2} \eta_c^2 \tau \varepsilon^{-1}} \Phi \left( \eta_c \tau \varepsilon^{-1/2} + \frac{A_t - A^*_i}{\tau \varepsilon^{-1/2}} \right) 1_{\{\tau > t\}} + E [P_{t+1} | \mathcal{I}_t]$$

$$= e^{\sqrt{\tau \varepsilon} (A^*_i - A_i)} - \frac{1}{\eta \kappa} y + \frac{\lambda_S}{\eta \kappa} \zeta_i + \kappa. \quad (A2)$$

Define $z_i = \sqrt{\tau \varepsilon} (A^*_i - A_i)$, which determines the population that buys the token. We can rewrite equation (A2) as

$$(1 - \beta) e^{[\frac{(1 - \eta_c) \tau \varepsilon^{-1/2}}{\eta \kappa} + \frac{1}{\eta \kappa} y] z_i + A_t + \frac{1}{2} \eta_c^2 \tau \varepsilon^{-1} \Phi \left( \eta_c \tau \varepsilon^{-1/2} - z_i \right) 1_{\{\tau > t\}}$$

$$+ e^{\frac{1}{\eta \kappa} y} \left( E [P_{t+1} | \mathcal{I}_t] - \kappa \right) = e^{- \frac{1}{\eta \kappa} y} + \frac{\lambda_S}{\eta \kappa} \zeta_i. \quad (A3)$$

Note that the first term in the LHS of equation (A3) has a humped shape with respect to $z_i$, and the second term is an exponential function of $z_i$ with a coefficient that may be either positive or negative. As the RHS of equation (A3) is constant with respect to $z_i$, this equation may have zero, one, two, or three roots:

- If $E [P_{t+1} | \mathcal{I}_t] - \kappa \leq 0$, 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 (A3) has no root.
2. If $LHS(\tilde{z}) > RHS$, then equation (A3) has two roots.

- If $E[P_{t+1} | \mathcal{I}_t] - \kappa > 0$, the LHS is non-monotonic with $LHS(-\infty) = 0$, $LHS(\infty) = \infty$, and one local maximum $\tilde{z}$ and one local minimum $\hat{z}$ in $(-\infty, \infty)$, and it may intersect the RHS at one or three points:

3. If $RHS < LHS(\tilde{z})$ or if $RHS > LHS(\hat{z})$, then equation (A3) has one root.

4. If $LHS(\tilde{z}) < RHS < LHS(\hat{z})$, then equation (A3) 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 (A3). Thus, equation (A3) has no root when $A_t$ is sufficiently small. For this situation to occur, the speculative motive, $E[P_{t+1} j I_t]$, must be nonpositive, otherwise equation (A3) has one or three roots. This condition is also satisfied when $A_t$ is sufficiently small because $E[P_{t+1} | \mathcal{I}_t]$ 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 $\tau$ 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, $E[U_{i,t} | \mathcal{I}_t, \tau > t]$, 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.

**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 speculative sentiment, notice from equation (A3) that, when $E[P_{t+1} | \mathcal{I}_t] - \kappa$ is nonpositive, there is a critical value of speculative sentiment $\zeta_t^c(A_t, y_t, Q_t)$:

$$\zeta_t^c = \frac{\lambda_P - \lambda_S}{\lambda_S} \log \left\{ \sup_{z_t} \left\{ (1 - \beta) e^{[1-\eta_\varepsilon]r_{\varepsilon}^{-1/2} + \frac{1}{2} \lambda_P \lambda_S z_t + A_t + \frac{1}{2} \eta_\varepsilon \tau_{\varepsilon}^{-1/2} - z_t} + e^{\frac{1}{2} \lambda_P \lambda_S z_t - E[P_{t+1} | \mathcal{I}_t]} \right\} \right\} + \frac{y_t}{\lambda_S},$$

such that no equilibrium exists if $\zeta_t \geq \zeta_t^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 $\zeta_t$ exacerbates the market breakdown region by lowering user participation. Since $\zeta_t$ 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, $\kappa$, 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 $A^c(y_t, Q_t, \zeta_t)$.

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.\textsuperscript{15}

Suppose that the token price at date $t+1$, $P_{t+1}$, is increasing in $A_t$ for all $(y_t, Q_t, \zeta_t)$ 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

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

where the expectation is take over $\varepsilon_{t+1}$. Consequently, $E[P_{t+1} \mid I_t]$ is increasing in $A_t$. Then, we can rewrite equation (A3) as the function $G_t$

$$
G_t = (1 - \beta) e^{(1 - \eta_0)^{\tau_\varepsilon^{-1/2} + \frac{1}{\lambda_p - \lambda_S}} z_t + A_t + \frac{1}{2} \eta_0^2 \tau_e^{-1}} \Phi \left( \eta_0 \tau_e^{-1/2} - z_t \right) \mathbf{1}_{\{\tau > t\}} + e^{\frac{1}{\lambda_p - \lambda_S} \tau_t} (E[P_{t+1} \mid I_t] - \kappa) - e^{-\frac{1}{\lambda_p - \lambda_S} y_t + \frac{\lambda_S}{\lambda_p - \lambda_S} \zeta_t} \equiv 0. \tag{A4}
$$

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

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

\textsuperscript{15}Our proof is based on a modified argument of Milgrom and Roberts (1994) for comparative statics in the presence of strategic complementarity.
where
\[ \frac{\partial G_t}{\partial A_t} = (1 - \beta) e^{[(1 - \eta_c) \tau_\varepsilon^{-1/2} + \frac{1}{\lambda_\varepsilon} y_t + \frac{1}{\lambda_\xi} \xi_t]} \frac{\partial E[P_{t+1} | I_t]}{\partial A_t} > 0. \]

In the high price equilibrium, the RHS of equation (A3) intersects the hump-shaped curve of the LHS in \( z_t \) on the left-side of the hump, and consequently \( \frac{\partial G_t}{\partial z_t} \geq 0. \) 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 \( P_t = e^{- \frac{1}{\lambda_\varepsilon} \xi_t - \frac{1}{\lambda_\xi} \xi_t y_t} + e^{\frac{1}{\lambda_\varepsilon} \xi_t} \frac{\partial E[P_{t+1} | I_t]}{\partial A_t} > 0. \)

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.

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 \( \zeta_t \) 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 (A4) as
\[ H_t \equiv (1 - \beta) e^{[(1 - \eta_c) \tau_\varepsilon^{-1/2} (z_t + \lambda_\xi \xi_t) + A_t + \frac{1}{\lambda_\varepsilon} \tau_\varepsilon^{-1} \Phi( - z_t + \lambda_\xi \xi_t) 1_{\{\tau > t\}} - e^{- \frac{1}{\lambda_\varepsilon} \xi_t - \frac{1}{\lambda_\xi} \xi_t y_t} + E[P_{t+1} | I_t] - \kappa = 0, \]

where the change of variables \( \tilde{z} \) now absorbs speculator sentiment, so that the price is

\[ P_t = e^{- \frac{1}{\lambda_\varepsilon} \xi_t - \frac{1}{\lambda_\xi} \xi_t y_t}. \]

Since speculator sentiment is i.i.d., and the equilibrium is Markovian in the state space \((A_t, y_t, Q_t, \xi_t)\), 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
\[ \frac{\partial \tilde{z}_t}{\partial \xi_t} = - \frac{dH_t/d\xi_t}{dH_t/d\tilde{z}_t}. \]

Since \( \tilde{z} \) enters \( H_t \) symmetrically as \( z \) does in equation (A3), \( dH_t/d\tilde{z}_t > 0 \) in the high price equilibrium. In contrast, \( dH_t/d\xi_t \) is
\[ dH_t/d\xi_t \propto (1 - \eta_c) \tau_\varepsilon^{-1/2} \frac{\Phi( - z_t - \lambda_\xi \xi_t)}{\Phi( - z_t + \lambda_\xi \xi_t)} = (1 - \eta_c) \tau_\varepsilon^{-1/2} \frac{\Phi( - z_t + \lambda_\xi \xi_t)}{\Phi( - z_t + \lambda_\xi \xi_t)}. \]

Consequently, if \( z_t \) is sufficiently small, then \( dH_t/d\xi_t > 0 \), while if \( z_t \) is sufficiently large, then \( dH_t/d\xi_t < 0 \). Since \( \frac{\partial P_t}{\partial \xi_t} = - \frac{1}{\lambda_\varepsilon - \lambda_\xi} P_t \frac{\partial \tilde{z}_t}{\partial \xi_t} \), it follows that \( \frac{\partial P_t}{\partial \xi_t} > 0 \) for \( z_t \) sufficiently small, and \( \frac{\partial P_t}{\partial \xi_t} < 0 \) for \( z_t \) sufficiently large. Since \( z_t = A_t - A_t \), the result follows.

\[ ^{16} \frac{\partial G_t}{\partial z_t} = 0 \text{ at the critical value of } z_t \text{ at which breakdown occurs if the fundamentals deteriorate.} \]
Proof of Proposition 4

From the miner optimization problem (8), 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

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

Substituting the optimal number of miners, $N_{M,t}$ from (8) into the attack condition given in (7) conjecturing an attack, $\chi_t = 1$, we can define

$$f(y_t, P_t, E[U_t | I_t]) = \left(\Phi(y_t + \psi t) - \frac{1}{2} \Phi(y_t) - \frac{1}{2} \Phi(y_t - \iota)\right) P_t$$

$$+ \frac{1}{2} \beta E[U_t | I_t] - \frac{\alpha e^{2\xi_t}}{4} \left(\Phi(y_t) - \Phi(y_t - \iota)\right) P_t + \frac{\beta U_t}{2}.$$  

There is an attack whenever $f(y_t, P_t, U_t) > 0$. It is clear since $\xi$ enters only through the quadratic term that there exists a threshold $\xi^c(A_t, Q_t, \zeta_t)$ such that:

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

where:

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

Assume now that $E[U_t | I_t]$ 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:

$$x_t = \frac{\Phi(y_t) - \Phi(y_t - \iota)}{2},$$

and rewrite $f(y_t, P_t, E[U_t | I_t])$ as:

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

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.

\footnote{Since there is no profit when $f(y_{t-1}, P_t, E[U_t | I_t]) = 0$, and only a loss in revenue from honest mining, it follows that miners would rather not attack at the indifference threshold.}
Consequently, since $P_t$ and $U_t$ are (weakly) increasing in $A_t$, it follows there is a connected set $\mathcal{A}_t = \{A_t : A_t < A^a(y_t, Q_t, \zeta_t; \xi_t)\}$, 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 $A_t < \mathcal{A}_t$.

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 $\mathcal{\bar{A}}_t = \{A_t : A_t > \bar{A}^a(y_t, Q_t, \zeta_t; \xi_t)\}$, where $\bar{A}^a(y_t, Q_t, \zeta_t; \xi_t) = \sup_{A_t} \{f(y_t, P_t, x_t) = 0\}$, such that $\chi_t = 0$ when $A_t > \bar{A}_t$.

Consequently, it follows that there is a strategic attack when $A_t \in \mathcal{A}_t$, and no attack when $A_t \in \mathcal{\bar{A}}_t$. What remains is to determine if $\mathcal{A}_t \cup \mathcal{\bar{A}}_t = \mathbb{R}$ or if there are more strategic attack regions for some $A_t > \mathcal{A}_t$. 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 $x_t$,

$$\frac{\beta}{2} E[U_t \mid \mathcal{I}_t] = \frac{1}{\alpha e^{2\xi_t}} + \sqrt{\left(\frac{1}{\alpha e^{2\xi_t}}\right)^2 + 4 \frac{\Phi(y_{t-1} + \psi_t) - \Phi(y_t)}{\alpha e^{2\xi_t}}} P_t - (\Phi(y_t) - \Phi(y_t - \ell)) P_t. \tag{A5}$$

Therefore, it must be the case that $A^a(y_t, Q_t, \zeta_t; \xi_t) = \bar{A}^a(y_t, Q_t, \zeta_t; \xi_t)$, 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 (A5) that, since a higher $\xi_t$ 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 $\xi_t$.

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 $\bar{A}_t$. 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 $\Phi(y_t + \psi t) - \Phi(y_t) P_t$ 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, $\xi_t$, 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 $\xi_t$. 
In this Online Appendix, we provide a microfoundation for the strategic attack condition in the main paper. 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.\textsuperscript{18}

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 (e.g., 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 $\Phi (y_t + \psi t) - \Phi (y_t)$, for $\psi > 0$, and the miner sells these additional tokens to earn $(\Phi (y_t + \psi t) - \Phi (y_t)) P_t$ in additional revenue. These additional tokens have to be absorbed by users and speculators by increasing the effective token supply to $\Phi (y_t + \psi t)$. In addition, because the corrupt miners add over half the blocks to the blockchain, they earn fifty percent of the transaction fees from users and seignorage.

\textsuperscript{18}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.
As a result of increased waiting times and service denials, users also experience a loss in expectation of half their trade surplus.\textsuperscript{19}

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.\textsuperscript{20} To join the strategic attack, a potential attacker has to pay a participation cost, which can be viewed as the cost or disutility of coordinating with the other attackers. We normalize this cost 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 half of the seignorage and transaction fees, is greater than the cost of doubling the existing computing power of the mining community

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

When this happens, a strategic attack occurs. When this condition is satisfied, however, all miners will want to attack the platform, which will dilute the mining power and undermine a strategic attack. 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 $\Pr (\text{Attack}) = p_t$. 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

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

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

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

otherwise there is no attack. Consequently, we can interpret the strategic attack condition (7) 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.

\textsuperscript{19}Hackers have also engaged in 51\% attacks to disrupt the blockchain to undermine confidence in the cryptocurrency. Although hackers can double spend, they cannot steal tokens from user wallets.

\textsuperscript{20}Implicitly, we assume that, to avoid detection by the mining pool, that these rogue miners must acquire additional computing power to compete with their own honest mining.