Initial Coin Offerings and Platform Building*

Jiasun Li† William Mann‡

First draft: August 31, 2017
This draft: January 24, 2019

Abstract

In a typical initial coin offering (ICO), an entrepreneur pre-sells digital tokens which will later serve as the medium of exchange on a peer-to-peer platform. We present a model rationalizing ICOs for launching such platforms: By transparently distributing tokens before the platform operation begins, an ICO overcomes later coordination failures during platform operation, induced by a *cross-side* network effect between transaction counterparties. Furthermore, a critical-mass requirement that arises from an endogenous *same-side* network effect during the ICO rationalizes several empirical patterns observed in ICO structures. Our model provides guidance for both regulators and practitioners to discern economically valuable ICOs.

Keywords: coordination, entrepreneurial finance, fintech, ICO, network effect, platform

*For helpful comments we thank audiences at U.S. Securities and Exchange Commission, Bank of Canada, Crypto Valley, George Mason, George Washington, Fudan, Tsinghua, AFA, WFA, EFA, Jackson Hole Finance Conference, ASU Sonoran Winter Conference, FSU SunTrust Conference, Cambridge Alternative Finance Conference, Southern California PE Conference, Tel Aviv University Conference, CICF, Chicago Financial Institution Conference, Emerging Trends in Entrepreneurial Finance Conference, Xi'an Blockchain Workshop, SUNY (Albany) symposium on FinTech & Blockchain, and Shanghai FinTech Forum; conference discussions by Gilles Chemla, Jonathan Daigle, Mohammad Davoodalhosseini, Ioannis Floros, Joshua Gans, Tao Li, Ye Li, Richard Lowery, Evgeny Lyandres, Ser-Huang Poon, Katrin Tinn, Ying Wang, and Ting Xu.

†George Mason University, 4400 University Drive, MSN 5F5, Fairfax, VA 22030. jli29@gmu.edu.

‡UCLA Anderson School of Management, Entrepreneurs Hall C.406, 110 Westwood Plaza, Los Angeles, CA 90095. william.mann@anderson.ucla.edu.

Initial coin offerings, or ICOs, have recently exploded in popularity in the startup world. In a typical ICO, an entrepreneur pre-sells digital tokens which will later serve as the medium of exchange on a peer-to-peer platform. According to CB Insights, "2017 was a record year for equity deals and dollars to blockchain startups, but it was nothing compared to ICO market activity. ICOs raised over $5B across nearly 800 deals in 2017, while equity investors deployed $1B in 215 deals to the sector."[1] This startling growth has been interpreted in conflicting ways. While enthusiasts argue that the numbers speak for themselves, skeptics raise concerns about irrational exuberance. Indeed, as is often the case with a new market, many proposed ICOs are misguided, or even fraudulent.[2] These examples provoke concerns that ICO tokens are simply disguised securities, with no value beyond regulatory arbitrage.

In some recent ICOs, these concerns seem justified, as their tokens carry cash flow or voting rights and may even be explicitly labeled as "security tokens".[3] However, many others, including the classic medium-of-exchange tokens, are claimed to be "utility tokens" that primarily play an operational role. Here things are not so clear-cut. These "utility tokens" are surrounded by controversy over both their legal status and their true economic value, if any. Accordingly, responses from regulators across the globe have been vastly different, ranging from promotions to case-by-case investigations to outright bans.

In sum, regulators and practitioners are in urgent need of an objective, rules-based framework to evaluate ICOs. Since ICOs do not fit neatly into classic models of security issuance or product sale, a necessary first step is to lay out a theory to explain whether, when, and how an ICO can create economic value, other than simply being a disguised security issuance. Such a theory could guide regulators and help investors separate the wheat from the chaff

[1] See `http://www.cbinsights.com/research/blockchain-vc-ico-funding`. Other sources provide estimates of similar orders of magnitudes. For example, Coinschedule reports $3.7 billion of ICO proceeds in 2017 [Link]. Most recently, Coindesk reports a $7.3B ICO proceeds from 192 ICO deals in 2018 Q2 [Link].

[2] For example, the SEC has prosecuted Maksim Zaslavskiy for alleged fraud in REcoin and DRC ICOs. See also cases involving PlexCoin, AriseBank, and Centra Tech.

[3] These tokens would likely meet the Howey test, a legal precedent for determining security status, and should be regulated as securities.

among ICOs. It could also advise entrepreneurs to determine whether an ICO is needed, and if so how best to structure that ICO. Nevertheless, perhaps owing to the nascent nature of the ICO market, as yet there are few such theoretical analyses in the academic literature.

Our paper fills this gap by presenting an economic mechanism through which tokens and ICO structures create value for both entrepreneurs and platform users. We focus on the classic medium-of-exchange tokens commonly observed in many well-received ICOs. Examples include Filecoin, which is setting up a network to allow peer-to-peer storage space sharing;[4] and Ethereum, which is building a decentralized virtual machine as an infrastructure for smart contract execution. As users on such platforms largely benefit from interacting with others, there exist network effects, in that the value of the platform to each user depends on the activities of others. Such strategic complementarities typically lead to multiple equilibria, including an inefficient one suffering from a self-fulling coordination failure. We show that tokens and ICOs could help select the efficient equilibrium and support platform building.

One fundamental coordination failure arising on such platforms involves a *cross-side* network effect, in which each user of the platform cares about the activities of his transaction counterparty on the other side. We study this network effect with a simple model of trade on a platform: Users can provide a service to each other, but must incur a fixed utility cost every time they do so. A coordination problem ensues: If either side believes that the other will not participate at any time, it is rational for this side to not participate either, so a no-trade equilibrium exists despite the fact that trading is socially valuable.

We show that a token specific to the platform can overcome this problem by serving as a coordination device among the users. When a user purchases a token, his decision is publicly observable thanks to the transparency of the smart contract implementing the ICO. The user thus communicates to others his intent to use the platform, which in turn motivates them to participate as well. Our proof applies reasoning based on forward induction: Potential

[4] Filecoin is presented as a central case study in Howell, Niessner and Yermack (2018).

users should reasonably conclude that anyone who has purchased a token intends to spend it later, as otherwise she would have been better off to not have purchased the token in the first place. Thus, our analysis explains why users are willing to purchase tokens that have no use outside of a specific platform, a pattern often puzzling to outside observers. Paradoxically, the token is valuable to the platform precisely *because* it is worthless elsewhere, as this makes a purchase decision a credible commitment to use the platform.

After explaining the role of ICOs for platform operation, we further shed light on the ICO process itself. We extend the *cross-side* network effect model of platform operation to a case with multiple same-side users, and endogenously derive a *same-side* network effect during the ICO that happens before the platform launch: A user's gain from participating in an ICO increases when a critical mass of same-type users participate too. The same-side network effect introduces yet another coordination problem during the ICO: In a simple one-shot token sale, the mere belief among prospective ICO participants of not reaching the critical mass could be self-fulfilling. While the entrepreneur could induce full participation by setting the token price adequate low, it may not be privately optimal, and a socially valuable platform may be forfeited.

Alternative ways to resolve this new coordination failure during the ICO process explains several commonly observed ICO structures. For example, one of them is to designate users to move sequentially. Each user then rationally chooses to participate in the ICO, knowing that her observable behavior encourages later users to do so as well. We extend this intuition by proving that, even if there is no designated order in which users act, the mere existence of enough stages coupled with a right price schedule motivates all users to participate in the ICO immediately. Other ways include rationed discounts to a selected group or returning funding upon failing to reach a critical mass. Section 3 connects these insights to the often-observed empirical patterns of ICO structures: prolonged campaign windows, rapid uptakes, escalating price schedules, pre-ICO discounts, and soft-cap inclusions.

Finally, we analyze how the presence of ICO speculators with private information would affect the role of tokens in resolving the cross-side network effect, in an extended model with fundamental uncertainty about the value of the platform. We confirm that regardless of whether speculation happens or not, in any equilibrium the token's coordinating effect is robust. The reason is that speculators will not buy the token unless it is common knowledge that, when the platform is valuable, the tokens will eventually end up in the hands of the users, as the token price cannot go up indefinitely. Hence there is no tension between the token's ability to coordinate actions among users, and its ability to aggregate the "wisdom of the crowd" through trade by informed token purchasers.

Our results provide several implications for policymakers and practitioners. First, we caution that universal bans of ICOs such as those adopted by China and Korea may risk throwing the baby out with the bathwater: our analysis is thus one step toward distinguishing the baby and the bathwater for more effective regulation. Second, a proposed ICO would benefit from explaining how a platform-like feature characterizes the project's business model. While we do not rule out other channels by which ICOs could create value, we do note that any other proposed channels should be subject to a similar rigorous analysis as pursued in this paper. Third, we endorse the SEC's warnings against potential abuse by celebrity-endorsed ICO deals, by emphasizing the importance of transparent off-chain activities and the regulatory role of disclosure requirement.

Most importantly, we provide support for a "substance" principle that the SEC is currently following, by showing that some tokens may serve as devices to facilitate successful platform launches without necessarily involving financing purposes.[5] These tokens may not simply be securities that fall under the jurisdiction of existing securities laws, but rather can be part of the operational process to fuel the build-up of a socially valuable enterprise featur-

[5] Indeed, Mastercoin's token sale, often referred to as the first ICO in history, "burned" all its proceeds so that the entrepreneur would get zero funding from the sale. (The ICO raised its proceeds in the form of Bitcoin, which can be "burned" by sending them to a verifiably unspendable address.)

ing platform-like network effects.[6] In other words, "utility tokens" can be a valid concept, and should be further studied and clearly distinguished from "security tokens" based on the characteristics of the projects they support (though not necessarily based on the labels attached by the entrepreneurs themselves).

In sum, we provide a theoretical framework to understand how tokens and ICOs could create economic value, emphasizing their role in the building of platforms that rely on user interactions. To be clear, we do not claim that all ICOs fit this description. Rather, the purpose of our framework is to help regulators and practitioners understand when they do or do not create value. Our theory can thus help design effective and transparent ICO regulation, and inform best practices among both investors and entrepreneurs regarding the use of this novel approach to launching a business.

Related literature Several contemporaneous papers analyze the ICO structure theoretically. The most related are Cong, Li and Wang (2018), Sockin and Xiong (2018), and Bakos and Halaburda (2018). Acknowledging the presence of multiple equilibria under network effects, the first two explore the interaction between user adoptions and token prices within the efficient equilibrium, and the latter discusses how token trading could relax capital constraints faced by entrepreneurs developing token based platforms. Our contribution is to show that the ICO structure itself can select the efficient equilibrium out of this multiplicity. Other papers focus on different features of ICOs: Catalini and Gans (2018) show that dynamic pricing can elicit consumers' willingness to pay; Chod and Lyandres (2018) show that an ICO can facilitate risk-sharing without dilution of control; and Canidio (2018) studies the tension between ex-ante financing and ex-post incentives.

Empirically, Howell, Niessner and Yermack (2018) document many important features of the ICO structure in practice. Kostovetsky and Benedetti (2018) document high ICO

[6] A recent statement by Singapore's *de facto* central bank echoes our stance. See here.

returns. Momtaz (2018) analyzes first day returns of ICOs. Lee, Li and Shin (2018) confirm wisdom of the crowd in the ICO setting. Li and Yi (2018) evaluate smart beta strategies in token investment. Adhami, Giudici and Martinazzi (2017) and Amsden and Schweizer (2018) look for ICO success determinants. Hu, Parlour and Rajan (2018) provide investment characteristics of 64 ICOs.

More broadly, our paper relates to a vast literature on firms facing network effects, e.g. Katz and Shapiro (1985) and Evans and Schmalensee (2010). Our theory also touches upon the two-sided markets literature, e.g. Spulber (2010), Rochet and Tirole (2006), Armstrong (2006), and Weyl (2010). These papers generally focus on calculating the platform's optimal tariff, and avoid multiple equilibria by separating user participation decisions from the strategic complementarities in user values, which is in contrast to our analysis on the role of ICO/tokens in equilibrium selection. Finally, network effects are also emphasized in the standards adoption literature: e.g. Farrell and Saloner (1985) and Dybvig and Spatt (1983).

Since ICOs involve pre-sales of tokens, our results relate to the crowdfunding literature: Strausz (forthcoming), Ellman and Hurkens (2015), Chemla and Tinn (2016), Cimon (2017), Brown and Davies (2017), Li (2017), Liu (2018), Cumming, Leboeuf and Schwienbacher (2015), Chang (2015), Belleflamme, Lambert and Schwienbacher (2014), Grüner and Siemroth (2015), Kumar, Langberg and Zvilichovsky (2015), Hakenes and Schlegel (2014), Xu (2016), and Li (2015), among others.

The role of a token within a platform is also reminiscent of the role of money in a general economy. Our model of bilateral trade without coincidence of wants bears a particular resemblance to Townsend (1980), and to a lesser extent Kocherlakota (1998) and Kiyotaki and Wright (1989). However, to our knowledge the argument that forward induction helps select the efficient equilibrium in such a setting is novel. The role of ICOs as a mechanism to overcome coordination problems also adds to existing approaches, such as the classic introduction of deposit insurance against inefficient bank-runs (Diamond and Dybvig, 1983), global-games (e.g. Carlsson and Van Damme, 1993; Morris and Shin, 1998; and Goldstein and Pauzner, 2005), and new advances on voluntary disclosures (Shen and Zou, 2017).

1 Network effects on platforms conducting ICOs

A network effect (or network externality) describes a phenomenon in which a user's surplus from transacting within a platform increases with the total number of transactions on the platform. Network effects are prevalent across many industries and business models, and especially in those where ICOs are common. In this section, we demonstrate how network effects appear in various business models, and illustrate these situations with notable ICO deals. In the process, we also highlight several stylized facts about ICOs later to be captured by our model in Section 2 and 3. Readers more interested in the model can skip this section entirely and move on to Section 2 directly.

Sharing economy Network effects play a crucial role in developing a sharing economy, as often discussed in the literature on two-sided markets. As an illustration, note that the presence of more riders on Uber incentivizes more drivers to participate, as they would expect higher and more steady traffic; similarly, more drivers providing ride-sharing incentivizes more riders to use Uber, due to its increased convenience and reliability. Hence we expect sharing-economy platforms to take advantage of ICOs in order to attract the necessary critical mass so that cross-side network effect would work toward the efficient equilibrium.[7]

Indeed, on August 10, 2017 decentralized data storage network Filecoin launched an ICO via CoinList, a joint project between Filecoin developer Protocol Labs and startup investment platform AngelList. Filecoin operates like an "Uber for file storage," aiming to provide a decentralized network for digital storage through which users can effectively rent out their spare capacity. In return, those users receive Filecoins as payment. The Filecoin

[7] Uber itself could not have used ICOs when it was founded in 2009, as ICOs did not exist yet.

ICO raised approximately $205.8 million over the next month. This added to the $52 million collected in a **pre-ICO** catered to notable VC firms including Sequoia Capital, Andreessen Horowitz, and Union Square Ventures.[8] The Filecoin ICO, like many others, adopted an **escalating price schedule** in which the minimum price buyers must pay rises as more investors join in. Both features will emerge endogenously in our model.

Social networks Social networks are also quintessential examples of platforms for which success largely hinges on network effects. As fewer friends are active on MySpace, the value of being active on MySpace also decreases. On the other hand, as more friends begin to share content on Facebook, the value of being engaged with the Facebook community increases. Due to this same-side network effect, social media startups are likely to utilize ICOs.[9]

Consistent with this view, on September 12, 2017, social media platform Kik launched a crowdsale that offered buyers the chance to purchase Ethereum-based tokens known as Kin that will serve as a tradable internal currency within Kik's social media universe and power future apps on its platform.[10] 10,026 individuals from 117 countries contributed 168,732 ETH (about $48 million dollars) to the *public ICO*, which added to the $50 million raised in an earlier round of *pre-ICO*.[11] According the firm's press release, its $98 million in ICO proceeds makes Kin "one of the most widely held cryptocurrencies in the world".

A notable feature of Kik's ICO is a cap imposed on how many Kin a buyer can purchase. This does not seem reasonable if the company's goal is solely to maximize revenue, but it does help address network effects, as will become more clear later. Further in this respect, Kik explicitly chose an ICO instead of traditional VC financing in order to foster a community.[12]

[8] See https://www.coindesk.com/257-million-filecoin-breaks-time-record-ico-funding/.

[9] As with Uber, Facebook could not have used an ICO when it was launched in 2004. Although rumors go that Facebook is mulling an ICO [Link].

[10] Kik currently has up to 15 million monthly active users.

[11] See Kik's dedicated ICO website: https://kin.kik.com/ as well as https://www.coindesk.com/kik-ico-raises-98-million-but-falls-short-of-target/ and https://techcrunch.com/2017/09/26/kik-ico-100-million/.

[12] See explanation here.

Blockchain infrastructure A blockchain, as a decentralized database, is itself an example of a cross-side network effect. A greater number of miners enhances a blockchain's security (e.g. by alleviating concerns over single-point-of-failures or censorship as well as by increasing the cost to launch a 51% attack) and gives each user a higher utility from using the blockchain. At the same time, for a given level of blockchain throughput a greater number of user activities tend to increase mining payoffs via higher transaction fees. Hence, not surprisingly, token sales are widely adopted by entrepreneurs to jump-start new blockchains.

A salient example comes from Ethereum's large-scale crowdsale. As a decentralized computing platform featuring smart contract functionality, Ethereum extends Bitcoin's Turing-incomplete Script language and develops a new blockchain to support the Turing-complete Ethereum Virtual Machine (EVM), executing smart contracts with an international network of public nodes. The project was funded during July-August 2014 by a crowdsale of "ether," an internal cryptocurrency within Ethereum, with an *escalating price schedule*. The system went live on 30 July 2015, with 11.9 million coins "pre-mined" for the crowdsale. Today, Ethereum has also been used as platform for most other coin offerings.

Marketplaces The finance literature has long recognized the development of a well-functioning market as a coordination game. For example, Barclay and Hendershott (2004) test the theory of "liquidity externality" by studying the after-hours stock market. New markets often strive for a critical mass of active participants to build up network effects, while even mature markets, including many stock exchanges, hold policies to subsidize a subset of "liquidity makers" to balance with "liquidity takers" (historically offering privileges to designated market makers, and recently offering rebates to liquidity providers). We hence expect ICOs to be effective tools for startups lauching exchanges or other marketplace-like platforms.

Prediction markets offer an example of a marketplace featuring this network effect, as placing bets requires a counterparty, and a larger market improves risk management for market makers. Not surprisingly, prediction markets have been quick adopters of ICOs. A prominent example is Augur, which attempts to build a decentralized network for accurate forecasting, and was funded via an online crowdsale during August and October of 2015.

Another example of such a marketplace comes from crowdsourcing computation resources for machine learning/artificial intelligence. Ensemble machine learning algorithms such as AdaBoost or Random Forest require a large volume of parallel training to produce an accurate outcome. A coordination problem arises again: Only if a critical mass of data scientists have committed to contribute will the learning outcome be attractive enough to new participants; but how can one attract such a critical mass in the first place? An ICO solution is seen from a crypto-token known as Numeraire. On February 21, 2017, 12,000 data scientists were issued 1 million Numeraires as incentives for constructing the artificial intelligence hedge fund Numerai. Founder Richard Craib stated that "the most valuable hedge fund in the 21st century will be the first hedge fund to bring network effects to capital allocation."[13]

2 Model: ICO coordinates the efficient equilibrium

In this section, we build a discrete-time, infinite-horizon model to describe the operation of a platform. An entrepreneur can pay a fixed cost K to develop a platform, which enables potential users to provide services to each other once launched. Our goal is to illustrate the role of internal tokens and the corresponding ICO process in preventing coordination failures in both the operation and launch of this platform. For ease of exposition, we first describe a sub-game: the platform's operation once it has already been launched. We then move backward and analyze a larger game that includes a prior stage during which tokens are distributed, known as an ICO, illustrating how specialized tokens sustain trades.

[13] https://medium.com/numerai/a-new-cryptocurrency-for-coordinating-artificial-intelligence-on-numerai-9251a131419a.

2.1 Operation of the platform after launch

Time is discrete with an infinite number of periods each divided into two sub-periods, denoted as morning and night. There are two potential users of the platform denoted as A and B.[14] In the morning, user A derives utility from a service that can be purchased on the platform from user B, and in the night, user A can provide the same service but no longer derives utility from it. User B has the opposite timing: he can provide the service in the morning, and derive utility from it at night. This setup naturally creates gains from trade between the two users without any fundamental asymmetry between them. It also creates a coincidence-of-wants problem, in that the two users never have a mutually-beneficial transaction at any single point in time, but rather must interact dynamically to realize the gains from trade.

Within each sub-period (morning or night), to either purchase or provide a service on the platform incurs a utility cost of u. A user can also choose to not participate at all, in which case she receives zero payoff. At any sub-period, transactions happen only when both A and B participate, upon which the service buyer gets a surplus of s, and the service provider incurs an additional cost of c. All these quantities are measured in utility terms. Everyone applies a common discount rate $\rho < 1$ between sub-periods (when convenient we also use r defined from $\rho \equiv \frac{1}{1+r}$). We assume that full trade during each period is ex ante optimal for B despite having to wait for the service, $\rho s - c - (1+\rho)u > 0$. This in turn implies that full trade is also optimal for A during each period ($s - \rho c - (1+\rho)u > 0$), and that trade is socially optimal in every period ($s - c - 2u > 0$).

The platform specifies the form of payment for transactions: either an external currency (fiat money such as dollars or major cryptocurrencies such as Bitcoin or Ether), or internal tokens specifically minted for exclusive use on the platform. To consider which of these is preferable, in the next section we compare the equilibria of the platform's operation with

[14] Each user could be interpreted as a representative player for one side of the market. We will further study the case of multiple users on each side in Section 3.

and without platform-specific tokens.

2.1.1 A platform without internal tokens

When the platform uses a generic currency as its medium of exchange, coordination failures may arise in every sub-period, leading to an inefficient equilibrium. Intuitively, a user who believes that the other side will not participate will rationally choose not to participate either, leading to a self-fulfilling equilibrium in which valuable gains of trade are forfeited. The source of this coordination problem is a cross-side network effect in which each side of the market cares about the actions of the other side. We formalize this intuition below.

Lemma 2.1 (Coordination problems on a generic currency platform)**.** *When a generic currency is accepted as the medium of exchange on a platform, there exists an inefficient equilibrium in which no trade ever takes place.*

Proof. Since the game satisfies continuity at infinity,[15] we only need to show that there is no profitable one-shot unilateral deviation by either the buyer or the seller from an equilibrium in which no users participate in the platform. To see this, observe that the payoff to any deviator changes from 0 to $-u$ at the point of time when she deviates. □

The possibility of a coordination failure renders generic currencies undesirable for platform operation. In the next two sections we will show that this coordination failure can be eliminated if platform-specific tokens are used as the medium of exchange, given that those tokens were distributed in sale through an ICO.

[15] An extensive form game satisfies continuity at infinity if $\forall \epsilon > 0$ there exists T such that for any player i and any game path z, z' with the same initial T-length histories, the payoffs satisfy $|V_i(z) - V_i(z')| < \epsilon$. Any game with discount rate $\rho < 1$ and bounded payoffs at any point of time satisfies continuity at infinity.

2.1.2 Introducing internal tokens to a platform

In this section we consider the operation of a platform using an internal token as the medium of exchange. Without loss of generality, we assume that the platform's protocol specifies that each unit of the service costs one token.

We first formally lay out the key characteristics of a platform-specific token.

Definition 2.1 (Token)**.** *A (utility) token for a platform is an internal digital currency within the platform that has the following properties:*

1. *No intrinsic value: while tokens are designated as the medium of exchange on the platform, they are of no use outside the platform: they cannot be used to purchase other goods or services.*[16]

2. *Transparency: Users can perfectly observe the aggregate amount of tokens sold by checking the ICO smart contract.*

We proceed by describing the platform operation assuming user A has already purchased one token prior to the first period. (In Section 2.2 we will prove that this is indeed the unique equilibrium outcome.) Figure 1 then illustrates the sequence of moves within each period when the platform operates, assuming all potential trades happen.

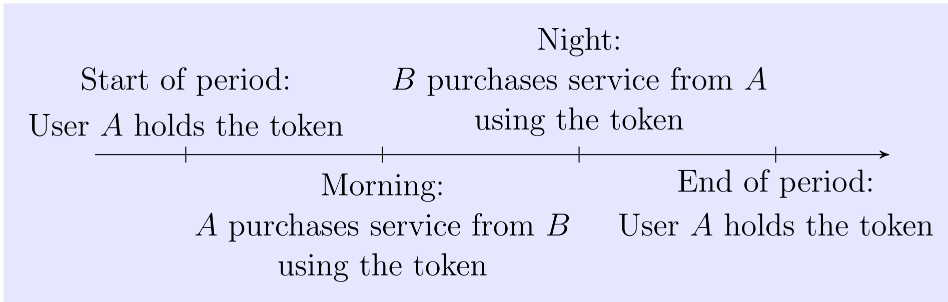
We are interested in Markovian pure strategies of both users, for which the platform's operation can be summarized recursively in the following game:

Definition 2.2 (Platform operation with tokens)**.** *The operation of a platform with internal tokens can be summarized by a game characterized by*

1. *2 users, A and B.*

[16]Tokens may, over time, endogenously obtain value outside of the platform such as in secondary market exchanges. Our analysis only requires them to have no such use when first introduced, or more precisely that any such value is less than the initial price of acquiring the tokens.

Figure 1: **Sequence of moves within each period**



2. *4 states:* (B, A), (A, A), (B, B), *and* (A, B), *where the first argument represents which user demands the service, and the second represents which user holds the token.*[17]

3. *64 strategy profile pairs, which are products of each user's 8 strategies: user A has*

$$\{(yyyn), (yynn), (ynyn), (ynnn), (nyyn), (nynn), (nnyn), (nnnn)\},$$

and user B has

$$\{(nyyy), (nyyn), (nyny), (nynn), (nnyy), (nnyn), (nnny), (nnnn)\}.$$

The strategies are interpreted as follows: for example, $(yyyn)$ *for user A means that A chooses a strategy profile to sell service in state (B, A), buy service in state (A, A), sell service in state (B, B), and not buy service in state (A, B).*

4. *512 value functions* V^s_{ijk} *(one for each of the 64 strategy pairs, 2 types, and 4 states). For a specific strategy profile pair s,* $(i, j) \in \{(B, A), (A, A), (B, B), (A, B)\}$ *stands for the states, and* $k \in \{A, B\}$ *stands for the user. In other words,* V^s_{ijk} *captures the present value of future lifetime payoffs for the user k at state ij when both users play the strategy pair s. These value functions are uniquely determined by a set of linear*

[17] For example, (B, A) represents an evening (meaning that user B demands the service) in which the token is held in the hands of user A.

equations (8 for each strategy pair) that are consistent with Markovian state transitions. Appendix B illustrates a subsample of all the 8×64 equations.

When user A has already made the sunk decision to acquire the token prior to platform launch, the subgame of platform operation starts from state (A, A). Hence, a strategy profile pair constitutes an equilibrium of the platform's operation if and only if neither user could attain a higher value function through a unilateral deviation at state (A, A).

Definition 2.3 (Equilibrium)**.** *A Markovian pure strategy equilibrium in platform operation is a pair of user A's and B's strategies so that at state* (A, A)*, neither user has a profitable unilateral deviation.*

Effectively, an equilibrium is an element in the set of the 64 strategy profile pairs that survives iterated elimination of strictly dominated strategies by comparing V_{AAA} and V_{AAB} across unilateral deviations by A and B, respectively.

Lemma 2.2 characterizes all equilibrium outcomes for a platform operating with tokens.

Lemma 2.2. *There exist only two possible equilibrium outcomes: An efficient outcome in which users A and B trade and realize the gains from trade at each point in time, and an inefficient outcome in which trade never happens at any point in time.*[18]

Proof. By iterated elimination of strictly dominated strategies. □

Based solely on the above two lemmas, one may conclude that outcomes are the same regardless of whether trade is specified to happen in generic currencies or platform-specific tokens. However, we have not yet discussed the mechanism by which the tokens were distributed to users in the first place. In the next section, we add this mechanism, consider the

[18] There are in total 12 equilibria with these properties: (y, y, y, n) and (n, y, y, y); (y, y, y, n) and (n, y, y, n); (n, y, y, n) and (n, y, y, y); (n, y, y, n) and (n, y, y, n); (n, n, y, n) and (n, n, y, y); (n, n, y, n) and (n, n, y, n); (n, n, y, n) and (n, n, n, y); (n, n, y, n) and (n, n, n, n); (n, n, n, n) and (n, n, y, y); (n, n, n, n) and (n, n, y, n); (n, n, n, n) and (n, n, n, y); (n, n, n, n) and (n, n, n, n).

full game, and demonstrate our first key result: the inefficient equilibrium is ruled out when tokens are initially distributed via an ICO.

2.2 ICO selects the efficient equilibrium

Having explained how tokens can sustain trade in the operation of the platform, we can now precisely clarify the role of an initial coin offering (ICO).

As described in the previous section, there are only two possible equilibrium outcomes once the platform begins operation: An efficient equilibrium in which all possible transactions occur (and the token is spent) in every sub-period; and an inefficient equilibrium in which no transactions ever occur. We now consider user A's decision whether to purchase the token or not, at a time before the first period of platform operation.

Before the platform begins operating, user A can choose whether to purchase a token for a price $P > 0$ offered by the entrepreneur. If A chooses not to purchase the token, the game ends and both users receive payoffs of zero. If instead user A chooses to purchase the token, then the game proceeds to the subgame analyzed in the previous section, beginning at state (A, A) in which user A both demands the service and possesses the token. We define this additional period prior to platform launch, during which the tokens are sold, as an ICO:

Definition 2.4 (ICO)**.** *An ICO is the sale of tokens prior to the first period of platform operation. After a successful ICO, the model in Section 2.1.2 becomes a subgame of this extended game, starting at state (A,A).*

Our main result is that, thanks to the existence of the token, user A has the power to select the efficient equilibrium outcome and prevent the inefficient one. Intuitively, when one platform user owns the token, other users infer that she has obtained it at a cost (either by purchasing it during the ICO for a positive price, or later by providing the service at a cost), and therefore can confidently conclude that she intends to spend it (as otherwise she should not have paid the cost to acquire the token in the first place). This information is a powerful mechanism to select the efficient equilibrium. Theorem 2.3 presents this result:

Theorem 2.3 (ICO selects the efficient equilibrium)**.** *When the entrepreneur conducts an ICO prior to platform launch, the efficient equilibrium outcome is the only one that survives rational reasoning.*

Proof. Consider the decision of user B in the first morning of platform operation. His decision depends on beliefs about the strategy profile of user A, who just bought the token. User B's belief puts zero probability on any strategy profiles in which user A does not attempt to spend the token at (A, A). The reason is that at state (A, A) user A has just taken a costly action – paying a positive price for the tokens – which would lead to a negative lifetime utility unless she spends the token in this state.

User B therefore can be confident that, if he also plays y, he will receive the token. This will incur a utility cost to type B of $u + c$, for participating in the platform and providing the service, and will also transition the game to state (B, B). To determine whether this decision by type B is rational, we next reason one step ahead:

User B, like user A, prefers the equilibrium in which the two users trade the token forever. At this point, he knows that A will play y at state (A, A), but what will A do in state (B, B)? If A is confident that B will play y at state (B, B), it will be rational for A to do the same, in order to return the game to the state in which A receives the surplus from the service. Indeed A should be confident about this outcome: Otherwise, B would not have accepted the token (and incurred the utility cost) at state (A, A).

Thus, once the game has transitioned to state (B, B), user B is confident that user A will play y, making it rational for B to also play y at that state. This knowledge of how the game is expected to evolve makes it rational for type B to play y at state (A, A). □

Remark: The logic in the proof applies the *forward induction* equilibrium refinement formalized in Govindan and Wilson (2009), which requires all players in a game to believe that the observed past actions chosen by other players were rational given their knowledge of their future actions. Behaviors consistent with forward induction refinement have been demonstrated in laboratory settings. Most notably for our purposes, van Huyck, Battalio and Beil (1993) conduct an experiment bearing a close similarity to an ICO, and find that reasonings in line with forward induction have strong power to achieve efficient coordination.[19]

Altogether, thanks to the observable and costly token purchase by user A before the platform launch, the unique equilibrium outcome of the game converges to the efficient one. Observing token purchases, user B infers an efficient equilibrium outcome and plays accordingly, and the efficient outcome is self-fulfilling. Our theory thus rationalizes the use of platform-specific tokens in peer-to-peer transactions.

Multiple insights can be drawn from this analysis. The most important is that tokens are useful to the platform precisely *because* they are useless outside of it. This fact makes the token purchase a credible way to communicate future play and rule out the inefficient equilibrium outcome. The transparency of the ICO smart contract and its underlying blockchain plays an important role in this regard.

Several features of this setup would also be straightforward to generalize. For example, it is not necessary to assume that the users live forever; in any sub-period in which they own the token, they could sell it to a replacement user. The replacement user's purchase of the token communicates intent to use the platform, and efficient trade can proceed.

While a prepaid platform membership charge may appear to achieve the same costly commitment signal function as a token, we note that a tokens that keep changing hands between users are generally superior to memberships. This is because for a membership to be sold once to achieve commitment value, it has to be priced so high that it extracts all consumer surplus and leaving users indifferent to purchase or not. A token, on the other

[19] Another recent experimental evidence is provided by Avoyan and Ramos (2017).

hand, leverages the forward induction insight every time it changes hands, so that it helps achieve coordination while still leaving positive surpluses to users.

3 Structuring an ICO

The previous section explains how an initial coin offering (ICO) creates value in the presence of a cross-side network effect, by eliminating coordination failures in the platform operation. In this section, we focus more on the ICO process itself and explore the richness of ICO structures: First, we show that another *same-side* network effect arises endogenously when there are multiple users within each side of the platform. We use this insight to explain many stylized facts about ICO structures in practice. Second, we consider an extended model with fundamental uncertainty and private signals about platform quality, in order to demonstrate robustness of our core results to the presence of speculators.

3.1 Two players within each type

We first extend the previous section to accommodate multiple players within each side. For ease of exposition we study the simplest case with four users: two of type A (denoted as player 1 and 2) for one side, and two of type B (denoted as player 3 and 4) for another.

The operation of the platform in each period is similar as before: Every morning, players 1 and 2 derive utility from the service, which could be provided by users 3 and 4. Player 1 or 2 can each attempt to purchase the service, provided she has a token at hand. At the same time, players 3 and 4 each decides whether to offer the service. During the night, the timing is reversed: Players 1 and 2 decide whether to provide services, and player 3 and 4 can each attempt to purchase the service provided she holds a token.

At any point in time, if the number of orders to buy equals to the number of orders to sell, all these orders clear. In this case, as in the previous section, all buyers receive a flow utility of $s - u$, and all sellers incur a flow cost of $c + u$. However, with four players, we must also consider the case in which the buy and sell orders do not balance. In this case, all parties that attempt to buy or sell always incur the participation cost u, yet the actual transaction (including the utility flows s and c, as well as the transfer of the token) is routed with equal probability to either players on the side with excess participation. For example, if there are two attempted buyers but only one seller, each buyer incurs the participation cost u for sure, but has only a 50% chance of realizing the transaction, spending her token, and receiving the surplus s. Otherwise (with 50% chance) she simply retains her token and realizes no utility flows beyond the cost u. The seller, meanwhile, incurs the cost $u + c$ and receives a token for sure. A player who attempts to purchase the service without owning a token simply incurs the cost u, and should trivially never do so.

As in the previous section, we first consider the platform operation, taking as given the distribution of tokens prior to the first date; then later we will endogenize the distribution by consider player 1 and 2's optimal decisions during an ICO before platform launch. Since we now have two players of type A, we must consider two separate cases: In the first case, only one of the two A players acquires a token prior to platform launch, so there is only one token in circulation on the platform. In the second case, both type A players acquire tokens prior to the launch and there are two tokens in circulation.

Only one token in circulation At any point in time there are 8 states ij, where $i \in \{1, 2\}$ indicates whether it is morning or night (i.e. whether type A or B users demand the service, where 1 stands for type A and 2 for type B), and $j \in \{1, 2, 3, 4\}$ indicates which player currently holds the token. For example, state 24 indicates a night (type B users demand the service) in which player 4 holds the token.

Each player's strategy defines a set of contingent action for all 8 states, and each player has 8 possible pure strategies, described in Table 1. Here, y means to purchase service when on the demand side, or to provide service when on the the supply side; n means to not purchase service on the demand side, or to not provide service on the the supply side.

Table 1: **All possible strategy profiles with one token in circulation**

corresponding state	11	12	13	14	21	22	23	24
player 1's strategy (to buy/sell?)	y or n	n	n	n	n	n	y or n	y or n
player 2's strategy (to buy/sell?)	n	y or n	n	n	n	n	y or n	y or n
player 3's strategy (to buy/sell?)	y or n	y or n	n	n	n	n	y or n	n
player 4's strategy (to buy/sell?)	y or n	y or n	n	n	n	n	n	y or n

Note that in Table 1, we significantly reduce the dimensionality of each player's strategy by taking advantage of the fact that no player without a token will attempt to purchase the service. For example, in the middle four columns, the token is held by a player who happens to be not deriving utilities from services, and thus no players will attempt to buy or sell.

From Table 1 we can see that there are $8^4 = 4096$ possible strategy profiles in this game. For each strategy profile, there are 32 value functions, measuring the continuation value for each of the four players in each of the eight states. We can solve for these value functions from the Markov transition equations that relate them to each other via the transition probabilities between states.

Lemma 3.1. *The strategy profile described in Table 2, where all players choose y whenever possible, constitutes a Nash equilibrium.*

Table 2: **One particular strategy profile**

corresponding state	11	12	13	14	21	22	23	24
player 1's strategy (to buy/sell?)	y	n	n	n	n	n	y	y
player 2's strategy (to buy/sell?)	n	y	n	n	n	n	y	y
player 3's strategy (to buy/sell?)	y	y	n	n	n	n	y	n
player 4's strategy (to buy/sell?)	y	y	n	n	n	n	n	y

The initial state of the platform operation is a morning, with the token in the hands of a type A player who has acquired it prior to the platform launch. Due to symmetry between user 1 and 2, without loss of generality we assume that it is user 1 who has purchased a token. Hence the initial state is 11. We are interested in player 1's and 2's initial value, or V_{111} and V_{112} (we denote player k's continuation value in state ij as value function V_{ijk}).

Solving for the value functions using the Markov transition matrices determined by the strategy profile in Table 2 (also illustrated in the proof of Lemma 3.1 in the appendix) gives

Lemma 3.2. *Under the equilibrium strategy profile in Table 2, where all players choose y whenever possible, in the first morning of platform operation the continuation values to the type A players who did and did not purchase the token are given, respectively, by* $V_{111} = \frac{(2-\rho^2)s-(2+2\rho-\rho^2)u-\rho c}{2(1-\rho^2)}$ *and* $V_{112} = \frac{\rho^2 s-\rho(2+\rho)u-\rho c}{2(1-\rho^2)}$.

Later, when we analyze the decision to purchase tokens prior to the platform launch, we will revisit the values V_{111} and V_{112}. To that end, we denote $V_L = V_{111}$ and $V_l = V_{112}$. It is easy to verify that $V_L > V_l$. This is not surprising: the type A user who starts with a token should enjoy a higher initial value than the player who does not (of course, we have not yet accounted for the cost to purchase the token in the first place). We will compare these values with the case characterized in the next section, in which both type A users have participated in the ICO and there are thus two tokens in circulation.

Two tokens in circulation When both player 1 and player 2 purchase tokens before the platform starts operation, at any point in time there will always be two tokens in circulation. The state space is larger in the two-token case as we need to take into account the token distribution. Specifically, there are 20 states ijk, where $i \in \{1, 2\}$ indicates whether type A or B users demand the service, and $jk \in \{11, 12, 13, 14, 22, 23, 24, 33, 34, 44\}$ indicates which player(s) currently has(have) tokens at hand. For example, state 224 indicates a night, meaning that type B users demand the service, in which player 2 and 4 each have one token. State 144 indicates a morning, meaning that type A users demand the service, in which both tokens are in the hands of player 4. Each player's strategy defines a set of contingent action for all 20 states. Indeed each player has $2^{14} = 16384$ possible pure strategies:

Table 3: **All strategy profiles**

state	111	112	113	114	122	123	124	133	134	144	211	212	213	214	222	223	224	233	234	244
1's strategy	y/n	y/n	y/n	y/n	n	n	n	n	n	n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n
2's strategy	n	y/n	n	n	y/n	y/n	y/n	n	n	n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n
3's strategy	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	n	n	y/n	n	n	y/n	n	y/n	y/n	n
4's strategy	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	y/n	n	n	n	y/n	n	n	y/n	n	y/n	y/n

For each of the 16384^4 strategy profiles described in Table 3 we can derive a set of Markov transition matrices determining each player's value functions at each state ($4 \times 20 = 80$ value functions for each strategy profile). Using the same logic as for the one-token case, we have

Lemma 3.3. *The strategy profile given in Table 4 in which all players choose y whenever possible constitutes a Nash equilibrium, in which $V_{1121} = V_{1122} = \frac{s-u-\rho(c+u)}{1-\rho^2}$, where V_{ijkl} captures player l's continuation value in state ijk.*

Table 4: **One particular strategy profile**

state	111	112	113	114	122	123	124	133	134	144	211	212	213	214	222	223	224	233	234	244
1's strategy	y	y	y	y	n	n	n	n	n	n	y	y	y	y	y	y	y	y	y	y
2's strategy	n	y	n	n	y	y	y	n	n	n	y	y	y	y	y	y	y	y	y	y
3's strategy	y	y	y	y	y	y	y	y	y	y	n	n	y	n	n	y	n	y	y	n
4's strategy	y	y	y	y	y	y	y	y	y	y	n	n	n	y	n	n	y	n	y	y

We denote $V_H = V_{1121} = V_{1122} = \frac{s-u-\rho(c+u)}{1-\rho^2}$, and it is easily verified that

$$V_H - V_l > V_L \tag{1}$$

where V_l and V_L were derived in the previous subsection when only player 1 participates in the ICO before platform launch.

3.2 A new coordination problem during ICO

Based on the analysis in the previous section, with two players on each side, the decisions of player 1 and 2 during the ICO stage can be summarized by yet another coordination game presented in Table 5 (where we denote the token price as P):[20]

Table 5: **Payoff matrix for ICO participation decision**

	y	n
y	$(V_H - P, V_H - P)$	$(V_L - P, V_l)$
n	$(V_l, V_L - P)$	$(0, 0)$

Based on this payoff matrix, several equilibrium outcomes are possible, depending on the value of the token price P:

1. if $P < V_L$, a unique equilibrium where both type A users choose y;
2. if $V_L \leq P \leq V_H - V_l$, multiple equilibria (both users choose y or both users choose n);
3. if $V_H - V_l < P$, a unique (uninteresting) equilibrium where both users choose n.

Thus, when the token price is sufficiently high, a new coordination problem endogenously arises during the ICO, before the beginning of platform operation. In the remaining analysis, unless otherwise specified, we will restrict attention to this case of multiple equilibria by assuming $V_H - V_l > P > V_L$.

Same-side network effect The new coordination problem derived above can be interpreted as a *same-side* network effect, as each type A user during the ICO (not platform operation at more) directly cares about the actions of the other same-side user. The intuition comes from the fact that the more type A users participating in the ICO, the more

[20]For ease of exposition, we assume no discounting between the ICO and the first morning of platform operation. Otherwise we only need to discount V_H, V_L, and V_l by the appropriate discount rate; the implications of the analysis remain unchanged.

tokens in circulation, and the higher chance for any type A user to be able to successfully transact after the first morning. This same-side network effect generates a critical mass requirement: a type A user will only find it optimal to participate in the ICO if she believes both users from type A will participate (i.e. at least a critical mass of $M = 2$ users will participate).[21] In this section, we present several structures an entrepreneur could use in an ICO to ensure participation from a critical mass. We theoretically demonstrate the effectiveness of these methods, and empirically connect to their wide use in actual ICO structures.

The simplest way to conduct an ICO is to distribute all the tokens in one shot, i.e. to charge each buyer a cost $P > 0$ per token during a window that only lasts for one period. Under this approach, the total surplus of the platform with full participation is $2 \times V_H - K$. However, as seen from Table 5 the entrepreneur can only guarantee full participation by charging a price of V_L or less. If the fixed cost K of platform development satisfies $K > 2V_L$, launching the platform will not be privately optimal from the entrepreneur's perspective. This is particularly problematic when $2V_H > K$, as an otherwise socially optimal project may be forfeited.

An alternative method available to the entrepreneur is to sell the tokens in an ICO that lasts multiple periods $T > 1$, during which the token price follows a schedule P_t, where t indexes the time points during the ICO. Since the number of tokens that have been sold is public knowledge at all times, thanks to the transparency afforded by the blockchain, a multi-period ICO effectively converts an otherwise simultaneous-move game (of ICO participation) into a sequential-move one.

Theorem 3.4. *Suppose the entrepreneur announces an ICO that consists of 2 periods during which tokens will be sold, and a price schedule P_t (the price at which the tokens will be sold at time $t \in \{1, 2\}$) of $P_1 = \rho P_2$ and $V_L < P_2 < V_H$. Then both type A users will purchase tokens*

[21] To stay consistent with the prior section, we explicitly analyze the case where $M = 2$. However, the results of this section naturally extend to the case where $M > 2$ as well. See Theorem C.1 in the Appendix.

during the first period of the ICO and all possible trading will happen once the platform begins operation.

Several important stylized features of ICOs can be understood in the context of overcoming the critical mass hurdle induced by a same-side network effect, as we explain next. We do not attempt to characterize the optimal combination of any of the following features that should appear in any given ICO, or rank their effectiveness, as this is not our primary goal and would require a much more complex model. Our point is rather that the connection between the model and the features of this market lend support to our view that many ICOs are fundamentally about addressing network effects.

Theorem 3.4 explains why ICOs often have **escalating price schedules over time** within **prolonged campaign windows**. For example, Ethereum's crowdsale lasted from July to August 2014, and the price of each ether increased roughly every two weeks. This result is important because the price escalation is common knowledge, even though the ICO in our model does not serve a financial purpose: The value of an ICO in our framework is really about resolving a coordination failure, and it may be regarded as an organic element of a platform operation. Nevertheless, token purchasers in our model would rationally expect price appreciation, which is currently an important component of the Howey test for security status. We expand on this implication in Section 4.[22]

Theorem 3.4 also shows that even though the campaign could last a prolong period, given an escalating price schedule users participate immediately, not to increase payoff but to avoid a coordination failure. This explains why purchase activities during an ICO are often concentrated in the beginning of the campaign (**rapid uptake**). Empirically, the ICO universe often features "mega-deals" described as "fetching millions in minutes". Such a

[22]In Theorem 3.4, the token price grows at the discount rate $r = \frac{1}{\rho} - 1$. Without any fundamental uncertainty, as we assume here, r should be equal to the risk-free rate. In practice, there is likely uncertainty about either the surplus s or cost c, and the rate r should adjust accordingly. We analyze fundamental uncertainty in Section 3.3.

pattern may appear at first glance like irrational exuberance. While we do not rule out this possibility, Theorem 3.4 indicates that a rapid uptake could have rational foundations.

An alternative approach to the one described in Theorem 3.4 is for the entrepreneur to conduct a **discounted pre-ICO**, in which a selected group is invited by the entrepreneur to purchase a limited number of tokens at a discount before the ICO opens to the general public. Specific to our model, if the entrepreneur selects a particular type A user and offers her a token with a price no more than V_L, the selected user will rationally purchase the token, as she will enjoy a positive utility from using the platform at this low price regardless of whether the other type A user eventually buys the token or not. After the selected user's purchase, the other type A user will be willing to pay up to V_H for the token, as the critical mass will be met upon her purchase. This observation could also explain **escalating price schedules over sales progress**, in which the price of tokens will increase once a certain number of tokens are sold.

Finally, a probably most powerful alternative approach toward the same-side network effect is to include a **soft cap** in the ICO smart contract, which automatically reimburses ICO participants if a pre-set funding target is not met by the end of the campaign. A soft cap effectively provides an insurance to ICO participants against missing the critical mass hurdle, and selects the efficient equilibrium in a similar spirit to deposit insurance in Diamond and Dybvig (1983). The strong and autonomous enforcement power of smart contracts are particularly useful for implementing a trustless soft cap (Cong and He (2018)).

3.3 Robustness to private information and speculation

Another frequently-mentioned benefit of an ICO, as a specific form of crowdfunding using blockchain-based smart contract, is its ability to aggregate information dispersed among market participants, often known as harnessing the "wisdom of the crowd". In our analysis so far, the "wisdom of the crowd" effect has been absent, as there has been no uncertainty in the model yet. In practice, however, many ICO token purchasers seem to be speculators whose actions are only based on expectations of future price increases rather than true intent to use the platform. In this section, we consider how such a pattern affects our main results.

Our goal in this extension is not to comprehensively analyze a model with information aggregation, as this would distract from the main focus of our paper, which is the coordinating effect of token sales. Rather, we seek to address one specific robustness concern with our main results: One might worry that, when many token purchasers are pure speculators who do not plan to use the token, this weakens the power of the token to select the efficient equilibrium, since the purchase decision by a speculator does not signal her future intent to use the platform. The main result of this section is to rule out this concern. Even when some or all of the initial purchasers are pure speculators, the token sale selects the efficient equilibrium as before.

First we describe the additional structure we must put on the model in order to analyze this issue. Suppose that nature draws a state $\sigma \in \{H, L\}$, with $Pr(\sigma = H) = p$. The state σ is not revealed to any player until after the ICO, when the platform launches. There exist some potential purchasers of the token, labeled "speculators," who derive no utility from the platform but are endowed with a signal $x_i \in \{H, L\}$, with $Pr(x_i = H|\sigma = H) = Pr(x_i = L|\sigma = L) = \pi > 1/2$. Conditional on the state, signals are independent across speculators. Finally, the flow utility s to users of the platform is realized only if $\sigma = H$. Otherwise, they get no utility from the platform, which is then socially worthless. Because σ is revealed before trade begins on the platform, if $\sigma = L$ then there is never any trade, and the payoff to a purchaser of the token is simply the price of the token, $-P$.

There are gains to speculation in this extended model for speculators with positive signals: Conditional on $\sigma = H$, the price of the token will converge to V by the time trade begins on the platform, but will start out at a lower value initially, being marked down due to the possibility that the platform is not actually valuable. Speculators with positive signals have incentives to buy tokens and sell later on once the price has appreciated to V.

Now we can state the main result of this section. The logic behind this result is simple, and can be seen without solving the model completely. It relies only on the fact that actions are common knowledge in any equilibrium, as well as a standard transversality assumption that a bubble in the price of the token cannot be permanently sustained.

Lemma 3.5 (Speculation does not cause a coordination problem)**.** *Assume that the price of the token does not grow faster than the discount rate on average. Any equilibrium of the extended model with speculation features full participation by platform users when* $\sigma = H$*.*

Proof. After trade begins on the platform, the social value of the platform is common knowledge, and so speculators no longer have any superior information. Given this, and the assumption that the nominal return on the token price does not exceed the discount rate, speculators no longer have any reason to hold the token. Thus, in any equilibrium in which speculators purchase tokens during the ICO, they must know that they can sell the tokens to users before the platform launches. Since actions are common knowledge in equilibrium, any potential users also know this fact, and so any time a token is purchased by a speculator during the ICO, this communicates that a user intends to participate in the platform later on, which is the only requirement for the ICO to select the efficient equilibrium.

To restate this argument in the opposite direction, suppose a speculator is unable to find a buyer for the token, meaning that a potential user refuses to purchase it. In any equilibrium featuring this outcome, it would not have been rational for the speculator to purchase the token in the first place. □

To be clear, this result does not state whether speculation will or will not happen. There are multiple equilibria in this regard, and we do not suggest any mechanism to select one from the other. Instead, the point of our analysis is that the ability of the ICO to coordinate actions among platform *users* is robust, regardless of whether speculation occurs.

4 Implications for regulators and practitioners

Based on our analysis of how ICOs can generate economic value for certain early stage projects, we discuss implications for the recent debates over the growth and regulation of the ICO market.

First, much of the recent debate over ICOs has focused on fitting them into existing securities laws, with particular attention to classifying tokens as "security" or "utility" tokens and applying existing standards like the Howey test.[23] We set aside this purely legal debate, and offer a fresh perspective based on the economic principle of efficiency. Through a rigorous analysis of the value of so-called "utility tokens," we shed light on when these should be restricted, allowed, or even promoted.

We show that, even without serving primarily as a *financing* tool, ICOs can create economic value. In our model, the ICO does result in cash inflows to the startup, and these likely occur at a time when it needs funds, yet financing is not the primary function accomplished by the ICO. Rather, an ICO can be an integrated part of the platform's operational process of building up user interactions.[24] This result shows that a universal ban on ICOs – as implemented by China and South Korea – may be misguided.

Furthermore, in our model, an ICO can still feature patterns like price appreciation that are a standard marker of security status under the "Howey Test," and our results suggest that such markers may be too rigid. If ICOs were broadly classified as securities, and token purchases were then restricted to those who are considered "qualified investors" under current securities law, many valuable ICOs would be rendered infeasible, as these rules would exclude many of the very users that the ICO is intended to coordinate.

[23] In a Senate hearing on February 6, 2018, the SEC chairman Jay Clayton famously claimed "Every ICO I've seen is a security" [Link]. On June 14, 2018, William Hinman, SEC Director of the Division of Corporation Finance, stated that Ether and Bitcoin are not securities. https://www.sec.gov/news/speech/speech-hinman-061418.

[24] This view is echoed by Ryan Zurrer, Principal and Venture Partner of Polychain Capital, who has stated that ICOs are about fostering a community, and that "tokens act like rocket fuel for network effects."

Instead, our theory suggests looking to the underlying business model of the project launching the ICO – that is, to the function of the ICO, not its form. If credible network effects exist, then an ICO is potentially a reasonable undertaking, and restricting access to only qualified investors could do more harm than good by destroying the power of the ICO to select an efficient equilibrium. If not, and no alternative justification could be given, then it is less likely that the ICO structure is critical to the success of the project, and one should then be concerned about the ICO being misguided or misleading.

For entrepreneurs, we therefore suggest that a project issuing "utility tokens" be always very clear on how the issued tokens serve as a critical element in the project. While speculators may naturally be attracted, the fundamental purpose of issuing utility tokens should be to facilitate platform building, rather than to raise investment capital. Projects that ignore or muddy this distinction should be closely examined by both investors and regulators.

For regulators, we suggest giving leeway to proposed ICOs that justify themselves in terms of the benefits described in the paper. This may require carving out a special regulatory category for tokens that otherwise might fall under current legal definitions of securities. On the other hand, ICOs that do not explicitly justify their structuring should be viewed skeptically. In our model, the specific challenge addressed by the ICO is a coordination failure arising from the network effect. While we do not necessarily rule out other channels by which ICOs could create value, we do note that any such benefit should be subject to a similarly rigorous analysis as pursued here.

Second, the value of a token in our framework – its ability to credibly signal future use – relies on the transparency of token-related activities, which is partially guaranteed by the (almost) real-time records with the ICO smart contract on the blockchain. Therefore, caution is warranted about potential abuses or manipulations off the blockchain. For example, one manipulation a dishonest entrepreneur can commit is to offer private off-chain side payments to bribe for fake participation in the ICO. This can take the form of an undisclosed, compensated celebrity endorsement.[25] In response, we suggest regulators to impose disclosure requirement of off-chain activities. The SEC's approach toward celebrity endorsement of ICOs is, according to our theory, stepping toward the right direction in this respect.

Most importantly, we hope that our analysis provides a preliminary framework towards a rule-based ICO regulation. Most major economies today have been following a case-by-case approach.[26] While flexibility is appealing in dealing with a new market, a case-by-case approach ultimately creates its own problems: A lack of clear rules ex ante adds another source of risk to startups, ICO participants, and other stakeholders in the the already risky early stage financing space. It is timely to have a rule-based regulatory framework based on a clear theoretical understanding of when ICOs do and do not create value.

5 Conclusion

In this paper, we develop a framework to understand the role of tokens and ICOs in the development of platforms. Setting aside the current legal debate over whether or not tokens are securities, we take an economic perspective, asking if and when token sales create value, and using economic efficiency as the criterion. We highlight that tokens can serve as a device to prevent inefficient coordination failure for projects that feature network effects.

Our findings have implications for regulators as well as practitioners in the growing ICO market. History has taught us that financial innovations are often accompanied by overenthusiasm and the exploitation of holes in existing legal frameworks, and indeed many proposed ICOs at the moment are likely to be low-quality or even fraudulent. Nevertheless, this market has the potential to create value in the world of entrepreneurship, in ways not

[25] The SEC has specifically warned that celebrity ICO endorsements could be illegal, see https://www.coindesk.com/sec-celebrity-ico-endorsements-illegal/.

[26] For example, in its July 25, 2017 Investor Bulletin, the SEC states that "depending on the facts and circumstances of each individual ICO, the virtual coins or tokens that are offered or sold may be securities". See here. In Canada, on Oct 25, 2017 the Ontario Securities Commission (OSC) approved the ICO of TokenFunder, even after issuing warnings against ICOs earlier in the year. See here and here.

currently accomplished by classic security issuance. By offering a theoretical analysis of this potential, we help regulators and practitioners separate the wheat from the chaff in this emerging market to promote its more healthy growth.

References

Adhami, Saman, Giancarlo Giudici, and Stefano Martinazzi. 2017. "Why do businesses go crypto? An empirical analysis of Initial Coin Offerings." 7

Amsden, Ryan, and Denis Schweizer. 2018. "Are Blockchain Crowdsales the New 'Gold Rush'? Success Determinants of Initial Coin Offerings." 7

Armstrong, Mark. 2006. "Competition in Two-Sided Markets." *The RAND Journal of Economics*, 37: 668–691. 7

Avoyan, Ala, and Joao Ramos. 2017. "A Road to Efficiency Through Communication and Commitment." 19

Bakos, Yannis, and Hanna Halaburda. 2018. "The role of cryptographic tokens and icos in fostering platform adoption." 6

Barclay, Michael J, and Terrence Hendershott. 2004. "Liquidity externalities and adverse selection: Evidence from trading after hours." *The Journal of Finance*, 59(2): 681–710. 10

Belleflamme, Paul, Thomas Lambert, and Armin Schwienbacher. 2014. "Crowdfunding: Tapping the right crowd." *Journal of Business Venturing*, 29(5): 585–609. 7

Brown, David C, and Shaun William Davies. 2017. "Financing Efficiency of Securities-Based Crowdfunding." *Available at SSRN.* 7

Canidio, Andrea. 2018. "Financial incentives for open source development: the case of Blockchain." *Working Paper.* 6

Carlsson, Hans, and Eric Van Damme. 1993. "Global games and equilibrium selection." *Econometrica: Journal of the Econometric Society*, 989–1018. 8

Catalini, Christian, and Joshua Gans. 2018. "Initial Coin Offerings and the Value of Crypto Tokens." *Working Paper.* 6

Chang, Jen-Wen. 2015. "The Economics of Crowdfunding." 7

Chemla, Gilles, and Katrin Tinn. 2016. "Learning through Crowdfunding." *CEPR Discussion Paper No. DP11363.* 7

Chod, Jiri, and Evgeny Lyandres. 2018. "A Theory of ICOs: Diversification, Agency, and Asymmetric Information." *Working Paper.* 6

Cimon, David. 2017. "Crowdfunding and Risk." *Working Paper.* 7

Cong, Lin William, and Zhiguo He. 2018. "Blockchain disruption and smart contracts." National Bureau of Economic Research. 28

Cong, Lin, Ye Li, and Neng Wang. 2018. "Tokenomics: Dynamic Adoption and Valuation." *Working Paper.* 6

Cumming, Douglas J., Gaël Leboeuf, and Armin Schwienbacher. 2015. "Crowdfunding models: Keep-it-all vs. all-or-nothing." *Discussion Paper.* 7

Diamond, Douglas W., and Philip H. Dybvig. 1983. "Bank runs, deposit insurance, and liquidity." *The journal of political economy*, 401–419. 7, 28

Dybvig, Philip, and Chester Spatt. 1983. "Adoption Externalities as Public Goods." *Journal of Public Economics*, 20: 231–247. 7

Ellman, Matthew, and Sjaak Hurkens. 2015. "Optimal crowdfunding design." *Available at SSRN 2709617.* 7

Evans, David S, and Richard Schmalensee. 2010. "Failure to launch: Critical mass in platform businesses." *Review of Network Economics*, 9(4). 7

Farrell, Joseph, and Garth Saloner. 1985. "Standardization, Compatibility, and Innovation." *RAND Journal of Economics*, 16: 70–83. 7

Goldstein, Itay, and Ady Pauzner. 2005. "Demand–deposit contracts and the probability of bank runs." *the Journal of Finance*, 60(3): 1293–1327. 8

Govindan, Srihari, and Robert Wilson. 2009. "On forward induction." *Econometrica*, 77(1): 1–28. 19

Grüner, Hans Peter, and Christoph Siemroth. 2015. "Cutting out the Middleman: Crowdinvesting, Efficiency, and Inequality." 7

Hakenes, Hendrik, and Friederike Schlegel. 2014. "Exploiting the Financial Wisdom of the Crowd–Crowdfunding as a Tool to Aggregate Vague Information." *Available at SSRN 2475025.* 7

Howell, Sabrina T., Marina Niessner, and David Yermack. 2018. "Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales." 3, 6

Hu, Albert, Christine A Parlour, and Uday Rajan. 2018. "Cryptocurrencies: Stylized Facts on a New Investible Instrument." 7

Katz, Michael, and Carl Shapiro. 1985. "Adoption Externalities as Public Goods." *The American Economic Review*, 75: 424–440. 7

Kiyotaki, Nobuhiro, and Randall Wright. 1989. "On money as a medium of exchange." *Journal of political Economy*, 97(4): 927–954. 7

Kocherlakota, Narayana R. 1998. "Money is memory." *Journal of Economic Theory*, 81(2): 232–251. 7

Kostovetsky, Leonard, and Hugo Benedetti. 2018. "Digital Tulips? Returns to Investors in Initial Coin Offerings." 6

Kumar, Praveen, Nisan Langberg, and David Zvilichovsky. 2015. "(Crowd) Funding Innovation." *Available at SSRN 2600923*. 7

Lee, Jongsub, Tao Li, and Donghwa Shin. 2018. "The Wisdom of Crowds and Information Cascades in FinTech: Evidence from Initial Coin Offerings." 7

Li, Emma. 2015. "The Usual Suspects: Experienced Backers and Early Stage Venture Success." *Working Papar*. 7

Li, Jiasun. 2017. "Profit Sharing: A Contracting Solution to Harness the Wisdom of the Crowd." 7

Li, Jiasun, and Guanxi Yi. 2018. "Smart Beta Strategies in Cryptoasset Investment." 7

Liu, Shannon. 2018. "A Theory of Collective Investment with Application to Venture Funding." 7

Momtaz, Paul P. 2018. "Initial coin offerings." 7

Morris, Stephen, and Hyun Song Shin. 1998. "Unique equilibrium in a model of self-fulfilling currency attacks." *American Economic Review*, 587–597. 8

Rochet, Jean-Charles, and Jean Tirole. 2006. "Two-sided markets: a progress report." *The RAND journal of economics*, 37(3): 645–667. 7

Shen, Lin, and Juanyuan Zou. 2017. "Intervention with Voluntary Participation in Global Games." *Working Paper*. 8

Sockin, Michael, and Wei Xiong. 2018. "A Model of Cryptocurrencies." *Working Paper*. 6

Spulber, Daniel F. 2010. "Solving the circular conundrum: communication and coordination in internet markets." *Nw. UL Rev.*, 104: 537. 7

Strausz, Roland. forthcoming. "A Theory of Crowdfunding-a mechanism design approach with demand uncertainty and moral hazard." *American Economic Review.* 7

Townsend, Robert. 1980. "Models of Money with Spatially Separated Agents." In *Models of Monetary Economies.* , ed. J. H. Kareken and Neil Wallace, 265–304. Minneapolis:Federal Reserve Bank of Minneapolis. 7

van Huyck, John B, Raymond C Battalio, and Richard O Beil. 1993. "Asset Markets as an Equilibrium Selection Mechanism: Coordination Failure, Game Form Auctions, and Tacit Communication." *Games and Economic Behavior*, 5: 485–504. 19

Weyl, E Glen. 2010. "A price theory of multi-sided platforms." *The American Economic Review*, 100(4): 1642–1672. 7

Xu, Ting. 2016. "The Informational Role of Crowdfunding." *Available at SSRN 2637699.* 7

Appendix

A Summary of International Regulatory Responses

Table 6: International regulatory responses to ICOs

Jurisdiction & Regulator	**Date**	**Regulatory Responses**
Australian Securities & Investments Commission (ASIC)	09/2017	state that the legality of an ICO depends upon its detailed circumstances, and "in some cases, the ICO will only be subject to the general law and the Australian user laws". [Link]
(**Canada**) Quebec Autorite des marches financiers	09/06/2017	Exploring and sandbox certain deals. [Link]
(**Canada**) Ontario Securities Commission	10/25/2017	approve the ICO of TokenFunder, even after issuing warnings against ICOs earlier in the year. [Link] and [Link]
(**China**) PBOC & other six regulators	09/04/2017	ban all ICOs within the People's Republic of China. [Link]
(**China**) National Internet Finance Association (NIFA)	01/26/2017	warn citizens against participating in overseas initial coin offerings (ICOs) and cryptocurrency trading. [Link] and [Link]
(**France**) Autorité des marchés financiers	by 10/2017	working on regulations. [Link]
German Financial Supervisory Authority (BaFin)	11/15/2017	discuss ICO risks to consumers. [Link]
HM Government of **Gibraltar**	10/12/2017	publish the Financial Services (Distributed Ledger Technology Providers) Regulations 2017 together with a Bill for an Act to amend the Financial Services (Investment and Fiduciary Services) Act. [Link]
Gibraltar government and Gibraltar Financial Services Commission (GFSC)	02/09/2018	anounce plan to present the first ICO regulations in the world, which will introduce the concept of regulating authorized sponsors responsible for assuring compliance with disclosure and financial crime rules. [Link]
(**Hong Kong**) Securities and Futures Commission	09/05/2017	state that depending on the facts and circumstances, digital tokens may be subject to securities laws. [Link]
	01/29/2018	launch a campaign to educate the public on the risks associated with ICO and cryptocurrency investment. [Link]
(**Japan**) Financial Services Agency	10/30/2017	clarify that Payment Services Act or Financial Instruments & Exchange Act may apply based on ICO structure. [Link]
(**Isle of Man**) Deptment of Economic Development	by 09/06/2017	has created a friendly regulatory framework [Link]
Israel Securities Authority	09/01/2017	announce plans to form a panel to regulate ICOs. [Link]
(**Malaysia**) Securities Commission (SC)	01/09/2018	issue a cease-and-desist to the CopyCash Foundation ahead of its planned ICO. [Link]
Malta's Financial Services Authority (MFSA)	10/23/2018	propose rule for investment funds that focus on cryptocurrencies [Link]; publish feedback on 01/22/2018 [Link]

Jurisdiction & Regulator	Date	Regulatory Responses
(**New Zealand**) Financial Markets Authority	10/2017	release guidelines on the current regulatory environment in regards to ICOs.
Philipines Securities and Exchange Commission	01/09/2018	issue cease-and-desist order against KropCoins. [Link]
	01/10/2018	issue warnings to ICOs. [Link]
	01/29/2018	crafting rules: likely no ban but registration required. [Link]
(**Russia**) Vladimir Putin	10/2017	mandate new regulations including the application of securities laws to initial coin offerings (ICOs). [Link]
(**Russia**) Finance Ministry	01/26/2018	introduce a draft federal law on the regulation of digital assets and initial coin offerings. [Link] and [Link]
Monetary Authority of **Singapore**	08/01/2017	suggest potential case-by-case regulation. [Link]
	11/14/2017	outline when ICOs are and aren't securities. [Link]
	01/08/2019	updated ICO guidelines for more consumer protection [Link]
(**South Korea**) Financial Services Commission	09/28/2017	ban all ICOs. [Link]
Swiss Financial Market Supervisory Authority	09/29/2017	clarify ICOs not regulated under Swiss law, but "due to the underlying purpose and specific characteristics of ICOs, various links to current regulatory law may exist". Also announce investigations of an unspecified number of coin offerings. [Link]
(**UAE**) Abu Dhabi Global Market Financial Services Regulatory Authority	10/09/2017	describe ICOs as a "novel and potentially more cost-effective way of raising funds for companies and projects, argue against a "one size fits all" approach, and indicate regulations on a case-by-case basis. [Link]
(**U.K.**) Financial Conduct Authority	09/12/2017	issue user warning. [Link]
	12/15/2017	propose a "deeper examination" to "determine whether or not there is need for further regulatory action". [Link]
U.S. Securities and Exchange Commission (SEC)	07/2017	indicate potential application of federal securities laws, determined on a case-by-case basis. [Link]
	09/2017	charged Maksim Zaslavskiy for fraud in connection with the ICOs for RECoin and DRC World. [Link]
	10/2017	rule that celebrity ICO endorsements must disclose the amount of any compensation. [Link]
	12/11/2017	Chairman Jay Clayton issue "Statement on Cryptocurrencies and Initial Coin Offerings". [Link]
	12/11/2017	institute cease-and-desist against Munchee Inc. [Link]
	01/30/2018	halt the self-claimed $600M coin offering by AriseBank. [Link]
	06/14/2018	William Hinman, the SEC's director of corporate finance, said the agency did not view bitcoin or ether as securities
U.S. Commodity Futures Exchange Commission (CFTC)	01/24/2018	charged Randall Crater, Mark Gillespie, as well as My Big Coin Pay, Inc. in connection with a cryptocurrency scam. [Link]

Jurisdiction & Regulator	Date	Regulatory Responses
(**U.S.**) Office of the Secretary of the Commonwealth of Massachusetts Securities Division	01/19/2018	charge resident Kirill Bensonoff and his company, Caviar with violating securities and business laws through an ICO. [Link]
(**U.S.**) Wyoming lawmakers	01/25/2018	file a bill to grant exemptions to ICO Utility Tokens. [Link]
(**U.S.**) Texas State Securities Board (TSSB)	01/24/2018	put an cease-and-desist order on an overseas ICO of R2B Coin [Link]
International Organization of Securities Commissions (IOSCO)	01/19/2018	issue notice alerting investors to the perceived risks associated with ICOs. [Link]

Also see Links for updates to global regulator statements.

B Markovian transition equation sets

The 64 strategy pairs each has 8 Markovian transition equations defining value functions (all 512 equations available upon request). For brevity we list 8 strategy pairs (8×8 equations).

1.1: A's and B's strategies: (y, y, y, n) and (n, y, y, y)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = s - u + \rho V_{BBA}, V_{AAB} = -c - u + \rho V_{BBB}$

$V_{BBA} = -c - u + \rho V_{AAA}, V_{BBB} = s - u + \rho V_{AAB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = -u + \rho V_{BBB}$

1.2: A's and B's strategies: (y, y, y, n) and (n, y, y, n)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = s - u + \rho V_{BBA}, V_{AAB} = -c - u + \rho V_{BBB}$

$V_{BBA} = -c - u + \rho V_{AAA}, V_{BBB} = s - u + \rho V_{AAB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = 0 + \rho V_{BBB}$

1.3: A's and B's strategies: (y, y, y, n) and (n, y, n, y)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = s - u + \rho V_{BBA}, V_{AAB} = -c - u + \rho V_{BBB}$

$V_{BBA} = -u + \rho V_{ABA}, V_{BBB} = 0 + \rho V_{ABB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = -u + \rho V_{BBB}$

1.4: A's and B's strategies: (y, y, y, n) and (n, y, n, n)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = s - u + \rho V_{BBA}, V_{AAB} = -c - u + \rho V_{BBB}$

$V_{BBA} = -u + \rho V_{ABA}, V_{BBB} = 0 + \rho V_{ABB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = 0 + \rho V_{BBB}$

1.5: A's and B's strategies: (y, y, y, n) and (n, n, y, y)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = -u + \rho V_{BAA}, V_{AAB} = 0 + \rho V_{BAB}$

$V_{BBA} = -c - u + \rho V_{AAA}, V_{BBB} = s - u + \rho V_{AAB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = -u + \rho V_{BBB}$

1.6: A's and B's strategies: (y, y, y, n) and (n, n, y, n)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = -u + \rho V_{BAA}, V_{AAB} = 0 + \rho V_{BAB}$

$V_{BBA} = -c - u + \rho V_{AAA}, V_{BBB} = s - u + \rho V_{AAB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = 0 + \rho V_{BBB}$

1.7: A's and B's strategies: (y, y, y, n) and (n, n, n, y)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = -u + \rho V_{BAA}, V_{AAB} = 0 + \rho V_{BAB}$

$V_{BBA} = -u + \rho V_{ABA}, V_{BBB} = 0 + \rho V_{ABB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = -u + \rho V_{BBB}$

1.8: A's and B's strategies: (y, y, y, n) and (n, n, n, n)

$V_{BAA} = -u + \rho V_{AAA}, V_{BAB} = 0 + \rho V_{AAB}, V_{AAA} = -u + \rho V_{BAA}, V_{AAB} = 0 + \rho V_{BAB}$

$$V_{BBA} = -u + \rho V_{ABA}, V_{BBB} = 0 + \rho V_{ABB}, V_{ABA} = 0 + \rho V_{BBA}, V_{ABB} = 0 + \rho V_{BBB}$$

C Proofs

Proof of Lemma 3.1. The proof is standard and closely follows the definition of Nash equilibrium. We nevertheless sketch an outline here.

To check that a strategy profile is an equilibrium, we only need to show there is no profitable unilateral deviation. Specifically, we compare the value functions for each player at the initial state of the game under the given strategy profile with the value functions at the initial state for the same player under any of that player's 7 unilateral deviations (the different decisions the player could make in each state, holding fixed the strategies of the other players). If none of the four players has a profitable unilateral deviation, the strategy profile is an equilibrium.

The initial state of the game is that the token is in the hands of the type A player who received it prior to the platform launch. Without loss of generality, we assume this to be player 1, so that the initial state is 11. Following the logic above, we then focus on $V_{111}, V_{112}, V_{113}$, and V_{114}, which are each player's value at the beginning of platform operation, conditional on player 1 purchasing a token during the ICO prior to platform operation. To verify an equilibrium, we compare each of these value functions with their respective unilateral deviations.

To illustrate the procedure to solve value functions, we take the given strategy profile in Table 2 as an example. If we express each player k's continuation value in state ij as value function V_{ijk}, then under the given strategy profile the relevant value functions V_{ij1} satisfy the following equations:

$$\begin{aligned}
V_{111} &= -u + s + \frac{1}{2}\rho(V_{231} + V_{241}) \\
V_{121} &= \frac{1}{2}\rho(V_{231} + V_{241}) \\
V_{131} = \rho V_{231}, V_{141} = \rho V_{241}, V_{211} = \rho V_{111}, V_{221} &= \rho V_{121} \\
V_{231} &= -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{111} + V_{121}) \\
V_{241} &= -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{111} + V_{121}) \\
V_{112} &= \frac{1}{2}\rho(V_{232} + V_{242}) \\
V_{122} &= -u + s + \frac{1}{2}\rho(V_{232} + V_{242}) \\
V_{132} = \rho V_{232}, V_{142} = \rho V_{242}, V_{212} = \rho V_{112}, V_{222} &= \rho V_{122}
\end{aligned}$$

$$V_{232} = -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{112} + V_{122})$$
$$V_{242} = -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{112} + V_{122})$$
$$V_{113} = -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{233} + V_{243})$$
$$V_{123} = -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{233} + V_{243})$$
$$V_{133} = \rho V_{233}, V_{143} = \rho V_{243}, V_{213} = \rho V_{113}, V_{223} = \rho V_{123}$$
$$V_{233} = -u + s + \frac{1}{2}\rho(V_{113} + V_{123})$$
$$V_{243} = \frac{1}{2}\rho(V_{113} + V_{123})$$
$$V_{114} = -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{234} + V_{244})$$
$$V_{124} = -u - \frac{1}{2}c + \frac{1}{2}\rho(V_{234} + V_{244})$$
$$V_{134} = \rho V_{234}, V_{144} = \rho V_{244}, V_{214} = \rho V_{114}, V_{224} = \rho V_{124}$$
$$V_{234} = \frac{1}{2}\rho(V_{114} + V_{124})$$
$$V_{244} = -u + s + \frac{1}{2}\rho(V_{114} + V_{124}),$$

which is a simple linear equation set of 32 equations and 32 varibles (V_{ijk}) to solve. □

Proof of Theorem 3.4. We prove a stronger result of Theorem C.1. □

Theorem C.1. *Suppose the entrepreneur announces an ICO that consists of a number of periods $T \geq M = 2$ during which tokens will be sold, and a price schedule P_t that the tokens will follow during $t = 1, \ldots, T$. Whenever M tokens have been sold, the platform will be launched, and users who purchased tokens can trade as described in previous sections. Suppose the price schedule satisfies $P_t = \frac{P}{(1+r)^{T-t}}$, where r is the common discount rate applied to the future service provided by the platform, and $P < V_H$. Then in any subgame perfect equilibrium in pure strategies, all users purchase tokens and join the platform by time $t = T - M + 1$.*

Although the theorem allows for the entrepreneur to set T strictly greater than M, note that the optimal decision is to set $T = M$, as this maximizes the price at which the tokens are sold. Thus, for simplicity, we consider only ICOs with $T = M$ in the following discussion.

Proof of Theorem C.1. By induction: First, suppose $T = M = 1$. Then there is effectively no coordination problem. The entrepreneur offers one period for consumers to join the platform at a price of (close to) V_H. In the unique Nash equilibrium, all users will join immediately.

Next, suppose $T > M = 1$. In the first $T - M$ periods, there can be multiple equilibria and potentially any number of users will join. However, regardless of users' decisions during these first periods, by time T the problem will reduce to the case analyzed in the previous paragraph, and all users will join at that date if they have not already.

Now suppose that $T = M > 1$, and the entrepreneur announces an ICO as described in the statement of the theorem above. Suppose further (the induction hypothesis) that for all $m < M$, the theorem holds: that is, if the critical mass on the platform were m, and the ICO lasted $T \geq m$ periods with the price following $P_t = \frac{P}{(1+r)^{m-t}}$, then all users would join immediately and the platform would launch.

Consider in this case the decision of an individual user at $t = 1$. In making her decision whether to join the platform, she must consider her payoff as a function of other users' decisions. If this user joins the platform today, then regardless of how many other users (if any) join at the same time, the subgame in the next period will be an ICO with $T - 1$ periods and (at most) $M - 1$ users remaining who must join to reach the critical threshold. This subgame will satisfy the induction hypothesis, guaranteeing that all users will join and the critical threshold will be reached.

On the other hand, if the user in question does not join the platform immediately, then it is possible (if no other users join at the same time) that the subgame in the next period will be an ICO in which M additional users are required to reach the critical threshold, but there are only $T - 1$ periods remain in which for them to join. This game would not satisfy the induction hypothesis, and there will be no guarantee of avoiding the coordination failure.

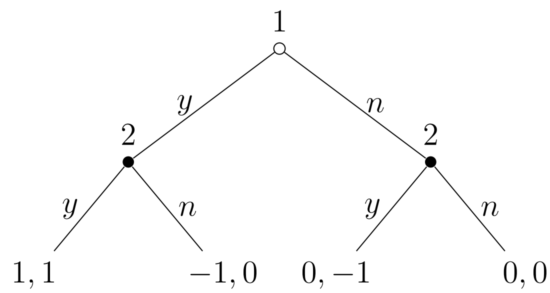
If the price of tokens is expected to decline in real terms during the ICO, then it may still be rational for the user to delay joining the platform, balancing the probability of platform failure against the time value lost by buying in early. However, if $P_2 \geq P_1 \times (1 + r)$, then there is no reason to wait. Regardless of the perceived probabilities of other users' actions, the individual user will rationally join immediately to force the subgame with a positive outcome, and thereby guarantee that the critical threshold is reached and the platform is launched. Following the same logic, all users will join at $t = 1$.

Finally, consider $T > M > 1$. As in the case $M = 1$, there are multiple equilibria for the first $T - M$ periods, after which the unique outcome is for all users to join. □

Remark The proof is a generalization of the following simple intuition. In a 2-by-2 game with the following payoff matrix:

	y	n
y	(1,1)	(−1,0)
n	(0,−1)	(0, 0)

Clearly there are two Nash equilibria in this coordination game: (y, y) and (n, n). Without changing the payoffs, if the entrepreneur simply change the simultaneous move game into a sequential move game by *designating* a first mover, clearly the only subgame perfect equilibrium will be (y, y).



Theorem C.1 extends the above intuition to the case with an arbitrary number of players, as well as allowing players to freely choose when to move without a designated sequence.

D ICO and wisdom of the crowd

While the main focus of paper is to analyze the role of ICOs and tokens in resolving coordination failures during platform building, we note that an ICO structure could in addition aggregate dispersed private information among potential users. This wisdom-of-the-crowd channel could work independently and create additional values. In the following analysis, we assume away network effect to illustrate this "wisdom of the crowd' channel.

Again the risk-neutral entrepreneur can incur a fixed cost K to launch a platform whose operation is identical to what is described in Section 2.1, and the entrepreneur can charge a per-capita price P to each users for access to the platform. If we assume away any same-side network effect, an individual user's payoff as a function of his action is then given by:

$$\begin{cases} 0, \text{ if he does not participate} \\ V - P, \text{ if he participates} \end{cases}$$

where V represents the present value of each user's surplus from using the platform.

A major deviation here from the analysis in Section 2 is the assumption of a fundamental uncertainty about the surplus V: for simplicity possible values of V are normalized to $V \in \{0, 1\}$, and the realization of V depends on the state of nature. All users share the common prior $\mathbb{P}(V = 1) = p$, and each user gets a noisy private signal X about the value of V, which is the only difference among them. We assume that the signals X are distributed according to the conditional distribution functions $(X|V = 1) \sim F_H$ and $(X|V = 0) \sim F_L$. Conditional on the realization of V, the signals X are independent of each other.

As shorthand notations, we denote $F(x) \equiv pF_H(x)+(1-p)F_L(x)$ and $f(x) \equiv F'_H(x)/F'_L(x)$. We assume that $f(\cdot)$ satisfies the monotone likelihood ratio property (MLRP), i.e. $f'(X) > 0$, which implies that $F_H(x) < F_L(x)$ for all x. In other words, for any given x, knowing $F_V(x), V \in \{H, L\}$ is perfectly revealing of the underlying state V.

D.1 The entrepreneur's problem with a single-stage ICO

Given a token price P, each user i participates in an ICO if and only if $\mathbb{P}(V = 1|X_i) \geq P$. Thus, a cutoff x^* is defined by setting this expression to equality,

$$\mathbb{P}(V = 1|x^*) \equiv P \tag{2}$$

Let M represent the number of users who participates in the ICO (i.e. those with signals higher than x^*). Then for $m \in \{0, 1, 2, ..., N\}$,

$$\mathbb{P}(M = m) = \binom{N}{m}(1 - F_V(x^*))^m F_V^{N-m}(x^*) \tag{3}$$

Hence, we obtain the entrepreneur's problem below:

The entrepreneur's problem The entrepreneur chooses P to maximize expected payoff

$$p \sum_{m=0}^{N} Pm \binom{N}{m}(1 - F_H(x^*))^m F_H^{N-m}(x^*) + (1-p) \sum_{m=0}^{N} Pm \binom{N}{m}(1 - F_L(x^*))^m F_L^{N-m}(x^*), \tag{4}$$

subject to

$$\frac{pf(x^*)}{pf(x^*) + (1-p)} = P \text{ (user IC)} \tag{5}$$

D.2 The entrepreneur's problem with an ICO

Denote m as the number of users who participate in ICO (that is, join at time zero) and n as the number who participate in the actual platform launch (that is, join at time one). Because m is indicative of the underlying state $V \in \{H, L\}$, at the second stage when the platform is actually launched, all players will make decisions with the additional signal m. A user will participate if and only if

$$\mathbb{P}(V = 1|X, m) \geq P_1, \tag{6}$$

where

$$\begin{aligned}
\mathbb{P}(V = 1|X, m) &= \frac{p\mathbb{P}(X, m|V = 1)}{p\mathbb{P}(X, m|V = 1) + (1-p)\mathbb{P}(X, m|V = 0)} \\
&= \frac{p\mathbb{P}(X|V = 1)\mathbb{P}(m|X, V = 1)}{p\mathbb{P}(X|V = 1)\mathbb{P}(m|X, V = 1) + (1-p)\mathbb{P}(X|V = 0)\mathbb{P}(m|X, V = 0)} \\
&= \frac{pf(X)\mathbb{P}(m|X, V = 1)}{pf(X)\mathbb{P}(m|X, V = 1) + (1-p)\mathbb{P}(m|X, V = 0)}
\end{aligned} \tag{7}$$

Denote x_0^* as the signal cutoff above which the user will participate in the ICO, then when $X < x_0^*$ (i.e. if he has not participated in the ICO), we have (7)=

$$\begin{aligned} & \frac{pf(X)\binom{N-1}{m}(1-F_H(x_0^*))^m(1-F_H(x_0^*))^{N-m-1}}{pf(X)\binom{N-1}{m}(1-F_H(x_0^*))^m(1-F_H(x_0^*))^{N-m-1}+(1-p)\binom{N-1}{m}(1-F_L(x_0^*))^m(1-F_L(x_0^*))^{N-m-1}} \\ = & \frac{pf(X)(1-F_H(x_0^*))^m(1-F_H(x_0^*))^{N-m-1}}{pf(X)(1-F_H(x_0^*))^m(1-F_H(x_0^*))^{N-m-1}+(1-p)(1-F_L(x_0^*))^m(1-F_L(x_0^*))^{N-m-1}} \end{aligned} \tag{8}$$

Hence a user who has not participated in the ICO (i.e. $X < x_0^*$) will participate in the second stage if and only if his signal is higher than the cutoff x_1^* given by

$$\frac{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)} = P_1(m) \tag{9}$$

Notice that for any given x_0^* and m the entrepreneur always set $P_1(m)$ low enough to ensure $x_1^*(m) < x_0^*$, because otherwise she earns zero in the second stage. In another word, the entrepreneur faces a Coase conjecture and any promises to keep a high $P_1(m)$ is not credible.

A user participates in the ICO if and only if

$$\mathbb{P}(V=1|X) \geq P_0 \tag{10}$$

i.e. she expects no loss from participating in the ICO, and

$$\mathbb{P}(V=1|X) - P_0 \geq \mathbb{E}_m\left[\mathbb{P}(V=1|X,m) - P_1(m)|X\right], \tag{11}$$

i.e. she is better off participating in the ICO than waiting.

Since $\mathbb{E}_m\left[\mathbb{P}(V=1|X,m) - P_1(m)|X\right] =$

$$\mathbb{P}(V=1|X) - \sum_{m=0}^{N-1}\left[P_1(m)\binom{N-1}{m}\frac{pf(X)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(X)+(1-p)}\right]$$

the two conditions (10) and (11) are expanded to

$$\frac{pf(x_0^*)}{pf(x_0^*)+(1-p)} \geq P_0 \tag{12}$$

$$\sum_{m=0}^{N-1}\left[P_1(m)\cdot\binom{N-1}{m}\cdot\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right] \geq P_0 \tag{13}$$

Since $\forall m, x_1^*(m) \leq x_0^*$, by (9)

$$P_1(m) \leq \frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}, \tag{14}$$

hence the left hand side of (13)$\leq$

$$\sum_{m=0}^{N-1}\left[\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}\right.$$
$$\left.\cdot\binom{N-1}{m}\cdot\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right]$$
$$= \sum_{m=0}^{N-1}\left[\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\cdot\binom{N-1}{m}\right]=\frac{pf(x_0^*)}{pf(x_0^*)+(1-p)}. \tag{15}$$

Hence we do not need to consider (12) as it is absorbed by (13). In sum, with the introduction of ICO, the entrepreneur's problem becomes the following:

The entrepreneur's problem with ICO The entrepreneur sets P_0 and $P_1(m), m \in \{0,1,2,...,N-1\}$ to maximize his profit (before the fixed cost K)

$$Np\sum_{m=0}^{N-1}P_1(m)\left(F_H(x_0^*)-F_H(x_1^*(m))\right)\binom{N-1}{m}(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)$$
$$+\quad N(1-p)\sum_{m=0}^{N-1}P_1(m)\left(F_L(x_0^*)-F_L(x_1^*(m))\right)\binom{N-1}{m}(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*),$$
$$+\quad NP_0\times\left[p(1-F_H(x_0^*))+(1-p)(1-F_L(x_0^*))\right] \tag{16}$$

subject to

1. conditional on x_0^*, $\forall m \in \{0,1,2,...,N-1\}$ $x_1^*(m)$ is given by

$$\frac{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}=P_1(m) \tag{17}$$

2. x_0^* is given by

$$\sum_{m=0}^{N-1}\left[P_1(m)\binom{N-1}{m}\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right]=P_0 \tag{18}$$

Analysis of the entrepreneur's problem The entrepreneur's payoff with ICO is alternatively given by

$$\text{argmax}_{\{x_0^*,x_1^*(m)\}}N\sum_{m=0}^{N-1}\binom{N-1}{m}\frac{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}\cdot$$

$$\Big\{p\left(F_H(x_0^*)-F_H(x_1^*(m))\right)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)\left(F_L(x_0^*)-F_L(x_1^*(m))\right)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)$$
$$+ \frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}[p(1-F_H(x_0^*)) + (1-p)(1-F_L(x_0^*))]\Big\} \tag{19}$$

In comparison, the entrepreneur's payoff without ICO is

$$\begin{aligned}
&\sum_{m=0}^{N} \frac{pf(x^*)}{pf(x^*)+(1-p)} m \binom{N}{m} \left[p(1-F_H(x^*))^m F_H^{N-m}(x^*) + (1-p)(1-F_L(x^*))^m F_L^{N-m}(x^*)\right] \\
= \; & N \frac{pf(x^*)}{pf(x^*)+(1-p)} \left[p(1-F_H(x^*)) + (1-p)(1-F_L(x^*))\right], \qquad (20)
\end{aligned}$$

Comparing the entrepreneur's payoff with or without ICO, we get Theorem D.1.

Theorem D.1. *The entrepreneur achieves greater expected profit with than without the ICO.*

Proof. (19) is no smaller than when x_0^* is forcibly set to 1, which is equal to

$$\text{argmax}_{\{x_1^*(0)\}} N \frac{pf(x_1^*(0))}{pf(x_1^*(0))+(1-p)} \cdot \left[p\left(1-F_H(x_1^*(0))\right) + (1-p)\left(1-F_L(x_1^*(0))\right)\right] = (20)$$

Hence introducing ICO always improves the entrepreneur's payoff. □