Initial Coin Offering and Platform Building

Jiasun Li* William Mann†

August 31, 2018

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 between transaction counterparties induced by a *cross-side* network effect. In addition, we rationalize several empirical features of the ICO structure in the presence of a critical mass requirement imposed by a *same-side* network effect. Our model provides guidance for both regulators and practitioners to discern which ICOs are economically valuable.

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

---

*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]

Such a startling growth can be interpreted in different ways. While an enthusiast would argue that the numbers speak for themselves, establishing ICOs as a valuable innovation in entrepreneurship, a skeptic may instead voice concerns over irrational exuberance. Indeed, as is often the case with a new market, many proposed ICOs are misguided. Furthermore, some may seek only to skirt existing securities laws. These facts have provoked controversy about the integrity of the ICO market.[2]

In response, regulators across the globe have taken vastly different approaches toward this new market, ranging from promotion to case-by-case investigation to outright bans. This diversity of responses reflects different understanding about the essence of a token, partially due to the diversity of the ICO tokens themselves: Instead of the original purpose of serving as an internal medium of exchange, tokens in many recent ICOs have different attributes, such as cashflow rights to future earnings. Many of these would be pure securities under the Howey test and should be regulated as such. However, not all cases are so clear-cut, as many tokens – including the classic medium-of-exchange tokens – are claimed to be "utility tokens" that play a distinct economic role. These "utility tokens" are surrounded by controversy over their true legal status, and by a related confusion over their real economic value, if any.[3]

---

[1] [Link]. Other sources provide estimates that are of a similar order of magnitude. For example, Coinschedule reports $3.7 billion of ICO proceeds in 2017 [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] In a hearing organized by the Senate Committee on Banking, Housing and Urban Affairs on February 6, 2018, the SEC chairman Jay Clayton claimed "Every ICO I've seen is a security" [Link]. While on June 14, 2018, William Hinman, SEC Director of the Division of Corporation Finance, stated that Ether and Bitcoin

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 investors to separate the wheat from the chaff among ICOs. It could also guide 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, the academic literature is still awaiting such a theory.

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 Ethereum, which is building a decentralized virtual machine as an infrastructure for smart contract execution, and Filecoin, which is setting up a network to allow peer-to-peer storage space sharing. As users on such platforms largely benefit from interacting with other users, there exist network effects, in that the value of the platform to each user increases with the activities of others. Such strategic complementarities among users lead to multiple equilibria, including an inefficient one that suffers from coordination failures. We will show that tokens and ICOs can be devices to resolve coordination failures, select the efficient equilibrium, and support platform building.

One important 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 effect with a simple model of trade on a platform: On the 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 date, it is rational for that side not to participate

---

are not securities [Link].

either, so a no-trade equilibrium exists despite the fact that trade is always 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 participate in the platform, which in turn motivates them to participate as well. Our proof applies reasoning based on forward induction: Potential users should reasonably conclude that anyone who purchases a token intends to spend it later. Thus, our analysis explains why users are willing to purchase a token that has 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 tokens and ICOs for platform operation, we further shed light on the ICO process itself. We extend the *cross-side* network effect model to include a *same-side* network effect, in which a user's gain increases when there is a critical mass of other users of the same type. 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. The entrepreneur could still induce full participation by giving the tokens away, but this is not privately optimal, so a socially valuable platform may be forfeited.

One simple way to avoid this new coordination problem is to designate users to move sequentially. Each user then rationally chooses to participate in the ICO, knowing that this 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 join, the mere existence of enough stages coupled with the right price schedule across stages motivates all users to join the platform immediately. Section 3 leverages this insight to explain several empirical observations in ICO structures, including rapid uptakes, escalating price schedules, and private pre-ICOs.

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 reasoning 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.

Overall, we provide a theoretical framework to understand how tokens and ICOs 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 aid in designing effective and transparent ICO regulation, and can inform best practices among both investors and entrepreneurs regarding the use of this novel approach to launching a business.

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.

Finally, we provide support for the SEC's "substance" principle, by showing that some tokens may serve as devices to facilitate successful platform launches without necessarily involving financing purposes.[4] These tokens may not simply be securities that fall under the jurisdiction of existing securities laws; but rather they are part of the operation process to fuel the build-up of a platform-like project featuring network effects and spur the growth of a socially valuable enterprise.[5] 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).

Related literature Several contemporaneous papers analyze various aspects of ICOs. Sockin and Xiong (2018) and Cong, Li and Wang (2018) embed strategic complementarity of the user base into asset-pricing frameworks. While they both acknowledge potential multiple equilibria in launching a token-based platform with network effects, neither digs into how the ICO process can select the efficient equilibrium, which is a major focus of our discussion. Catalini and Gans (2018) focus on the ability of dynamic ICO pricing to elicit consumers' willingness to pay; Chod and Lyandres (2018) on how the ICO process can facilitate risk-sharing without dilution of control rights; and Canidio (2018) on the tension between ex-ante financing and ex-post incentives, in that entrepreneurs may not actually develop services after selling tokens to fund them.

Empirically, Kostovetsky and Benedetti (2018) document high ICO returns. Amsden and Schweizer (2018) analyze 1,009 ICOs and look for success determinants of ICOS. Lee, Li and Shin (2018) confirm wisdom of the crowd in the ICO setting. Howell, Niessner and Yermack (2018) examine the relationship between issuer characteristics and measures of success. With

---

[4] 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.)

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

a restricted sample, Hu, Parlour and Rajan (2018) provide some investment characteristics of 64 ICOs. Adhami, Giudici and Martinazzi (2017) analyzes 253 ICO campaigns and find that "the probability of an ICOs success is higher if the code source is available when a token presale is organized, and when tokens allow contributors to access a specific service (or to share profits)." Momtaz (2018) analyzes first day returns of ICOs.

Our analysis also touches upon multiple other fronts of the literature:

The first related area is the vast literature on network effects. Evans and Schmalensee (2010) analyze how the initial critical mass hurdle faced by a news business depends on the nature of network effects, the dynamics of customer behavior, and the distribution of customer tastes. Katz and Shapiro (1985) consider Cournot competition among firms with network effects, and show that various expectations of other consumers' choices can lead to multiple rational-expectations equilibria. A related literature studies the coordination problems in adopting new technologies: Farrell and Saloner (1985) show that all firms adopt a new technology when the adoption decisions are made publicly and sequentially, and Dybvig and Spatt (1983) argue that the government can shift the equilibrium to universal adoption by insuring adopters against the risk of inadequate aggregate adoption.

Also related is the literature on the two-sided markets, as reviewed for example in Spulber (2010), Rochet and Tirole (2006), Armstrong (2006), and recently Weyl (2010). Papers in this literature generally focus on static models, and separate user participation decisions from the strategic complementarities in user values. By doing so, they avoid the multiple equilibria/coordination failures in the building of a platform, and focus instead on the platform's optimal tariff. In contrast, we study a dynamic setting that illustrates the role of tokens, and we focus on the stragic participation/usage decisions of platform users, instead of on the platform's tariff.

Because the ICO is a pre-sale of tokens, our results relate to the crowdfunding literature. Strausz (forthcoming) and Ellman and Hurkens (2015) study the optimal rewardbased crowdfunding design with a focus on a trade-off between improved screening/adaption and worsening entrepreneur moral hazard/rent extraction, respectively. Chemla and Tinn (2016) theoretically demonstrates how crowdfunding could help entrepreneurs take informed investment choices through learning from users' crowd wisdom. Different theoretical aspects are studied by 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), and Hakenes and Schlegel (2014). Xu (2016) and Li (2015) provide empirical evidence that in crowdfunding entrepreneurs and follow-up investors respectively learn from the crowd wisdom.

The role of a token within a platform is also reminiscent of the role of money in a general economy, as studied for example in Kocherlakota (1998), where money serves as "memory" (also see Kiyotaki and Wright, 1989). Our results are also of technical interest along several other dimensions. We describe ICOs as a new mechanism to overcome coordination problems, in addition to classic approaches of introducing deposit insurance against inefficient bank-runs (Diamond and Dybvig, 1983), new advances of voluntary disclosure (Shen and Zou, 2017), and global-games (e.g. Carlsson and Van Damme, 1993; Morris and Shin, 1998; and Goldstein and Pauzner, 2005).

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 show up in various different business models, in either indirect (cross-side) or direct (same-side) forms, and illustrate these situations with notable ICO deals. In the process, we also highlight several stylized facts about ICOs to be captured by our model in Section 2. Readers only 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.[6]

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 ICO raised approximately $205.8 million over the next month. This added to the $52 million collected in a *private pre-ICO* catered to notable VC firms including Sequoia Capital, Andreessen Horowitz, and Union Square Ventures, etc.[7] 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 as a way to overcome network effects.

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

---

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

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

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.[8]

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.[9] 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 *private pre-ICO*.[10] 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. Further in that respect, Kik explicitly chose an ICO instead of traditional VC financing in order to foster a community.[11]

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) and gives each user a higher utility from using the blockchain. At the same time, a greater number of users should increase mining payoffs through 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-

---

[8] As with Uber, Facebook could not have used an ICO when it was launched in 2004.

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

[10] 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/.

[11] See explanation here.

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."[12]

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 once launched enables $2N$ potential users to provide services to each other. Our goal is to illustrate the role of internal tokens and the corresponding ICO process in preventing coordination failures in both the operation and launching of this platform. For ease of exposition, we first describe a sub-game: the platform's operation once it has already been launched, illustrating how specialized tokens sustain trades. We then move backward and analyze a larger game that includes a prior stage during which tokens are distributed, known as an ICO, and explain several commonly observed empirical patterns in ICO processes.

2.1 Operation of the platform after launch

There are an infinite number of periods, each divided into two sub-periods, denoted as morning and night. The $2N$ potential users of the platform are also divided into two types, denoted as A and B, with each type having N users. In the morning, each type A user derives utility from a service that can be purchased on the platform from type B users, and in the night, each type A user can provide the same service but no longer derives utility from it. Type B users have the opposite timing: They each can provide the service in the morning, and derive utility from it at night. This setup naturally creates gains from trade between

---

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

the two user types without any fundamental asymmetry between them. It also creates a coincidence-of-wants problem, in that the two types of agent 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. Since all users within the same type are identical, we focus on symmetric strategies within the same type: all users of a given type always take the same action at any point in time. We hence only need to consider a representative user for either side. With slight abuse of notion, we denote the two representative users for each side as A and B. At any sub-period, transactions happen only when both type A and B users participate, upon which each 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, and a transaction is socially valuable, i.e. $s - c - 2u > 0$. 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. Everyone applies a common discount rate r between sub-periods (for conciseness we also define $\rho \equiv \frac{1}{1+r}$).

Due to the utility cost u to each side, there exists a *cross-side* network effect by which buyers care about the participation decisions of the sellers, and vice versa. In sections 2.1.1, 2.1.2, and 2.2, we illustrate the role of tokens and ICOs in resolving coordination failures in platform operation induced by this network effect, taking the surplus s as a constant. In section 3, we additionally consider a *same-side* network effect where s depends on the number of transactions taking place on the platform. This additional consideration helps explain many commonly-observed empirical patterns in ICO structuring.

The first issue we address is the choice of payment method on the platform. We compare platform launches and operation with or 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,[13] 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 have already been distributed through an ICO.

---

[13] 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.

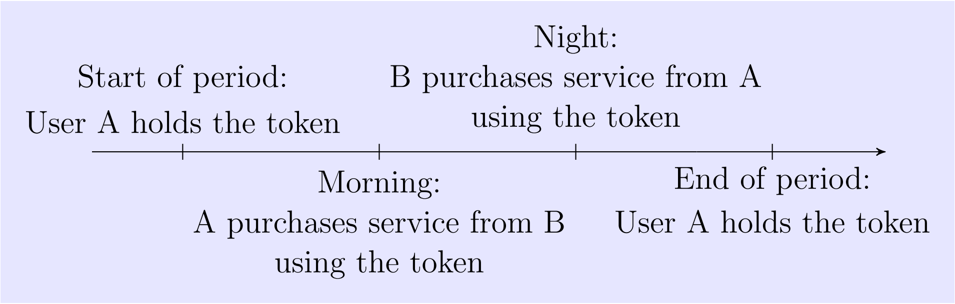
Definition 2.1 (Token)**.** *A (utility) token for a platform is an internal digital currency within the platform that has the following properties:*

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.*[14]

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 all type A users have 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.

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



---

[14] 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.

We are interested in all 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 representative users, with one for each type (A and B).*
2. *4 states: (B, A), (A, A), (B, B), and (A, B), where the first argument represents which side demands the service, and the second represents which side holds the tokens.*[15]
3. *64 strategy profile pairs, which are products of each side's 8 strategies: type A has*

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

   and type B has

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

   The strategies are interpreted as follows: for example, $(yyyn)$ for type 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 type. In other words, V^s_{ijk} captures the present value of future life-time payoffs for the type k user at state ij when both users play the strategy pair s. These value functions are uniquely determined by a set*

---

[15] For example, (B, A) represents a night (meaning that type B users demand the service) in which all tokens are held in the hands of type A users.

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

Assuming all type A users have already made sunk decisions to acquire tokens prior to platform launch, then 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 no representative user of either side could attain a higher value function through a unilateral deviation at state (A, A).

Definition 2.3 (Equilibrium)**.** *A symmetric, Markovian, pure strategy equilibrium of the platform's operation is a pair of type A's and B's strategy profiles so that at state* (A, A)*, neither user has a profitable 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. *If* $\rho \geq \frac{u+c}{s-u}$*, there exist only two possible equilibrium outcomes: An efficient outcome in which type A and B users 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.*[16] *If* $\rho < \frac{u+c}{s-u}$*, then only the inefficient equilibrium outcome exists.*

Proof. By iterated elimination of strictly dominated strategies. □

The condition on ρ shows that users must be sufficiently patient for the efficient equilibirum outcome to obtain. More importantly for our purposes, even when users are sufficiently patient, the inefficient equilibirum always exists due to the possibility of coordination failure.

---

[16] 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).

Based solely on the above two lemmas, one may conclude that outcomes are the same regardless of whether trade is specified to happen in external currencies or 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 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 may 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 (all tokens are spent) in every sub-period; and an inefficient equilibrium in which no transactions ever occur. We now consider the decision of a representative type A user whether or not to purchase the token at an initial date before the first date of platform operation.

Before the platform begins operating, the representative type A user can choose whether to purchase a token for a price $P > 0$ offered by the entrepreneur. If he chooses not to purchase the token, the game ends and all users receive payoffs of zero. If instead the type A user chooses to purchase the token, then the game proceeds to the subgame analyzed in the previous section, beginning at state (A, A) in which type 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 date of the platform's 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, the type A users have the power to select the efficient equilibrium outcome and prevent the inefficient one. To obtain this result, we apply the *forward induction* equilibrium refinement (Govindan and Wilson, 2009). Intuitively, forward induction 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. In our specific game, when one platform user owns the token, other users infer that she obtained it in the past at a cost (either by purchasing the token during the ICO for a positive price, or later by providing the service at a utility cost), and therefore can confidently conclude that she intends to spend it. This information is a powerful mechanism to select the efficient equilibrium. This result is presented in Theorem 2.3:

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

Proof. Consider the decision of a representative type B user in the first morning of platform operation. His decision depends on beliefs about the strategy profile of the representative user of type A, who just bought the token. Forward induction requires type B's belief to put zero probability on any strategy profiles in which type A does not attempt to spend the token at (A, A). The reason is that at state (A, A) type 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.

Type 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:

Type B, like type A, prefers the equilibrium in which the two users trade the token forever. At this point, he knows that type A will play y at state (A, A), but what will type

A do in state (B, B)? If type A is confident that type B will play y at state (B, B), it will be rational for type A to do the same, in order to return the game to the state in which type A receives the surplus from the service. And type A is indeed confident about this outcome, thanks again to forward induction: Otherwise, type 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), type B is confident that type A will play y, making it rational for type 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). □

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

Multiple key 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 also helps in this regard.

Several other features of the setup in this section 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 their token to a replacement user.

3 Structuring an ICO

The previous section explained that an initial coin offering (ICO) creates value in the presence of a cross-side network effect, by effectively collapsing all intertemporal coordination problems into the ICO preceding the platform launch. In this section, we put a richer structure on the ICO process, first with a *same*-side network effect, and then with fundamential uncertainty and private information. We use these features to explain many empirically relevant stylized facts about ICOs, and to demonstrate robustness of our core results to adding speculators into the model.

3.1 Same-side network effect

Separately from cross-side network effects, many platforms also feature a *same*-side network effect, by which users care directly about the actions of other same-type users. In this section, we show how ICOs can be structured to address a second coordination problem induced by this second type of network effect: the need to attract enough initial users during the ICO. The features we derive are indeed consistent with those commonly observed in ICOs.

To see how the second coordination problem arises, consider the same platform operation process as described in the previous section, except that the flow utility s to the buyer from a successful transaction is no longer a constant but is an increasing function $s(n)$, where n is the number of transactions on the platform each period, or equivalently the number of tokens sold during the ICO when there is full participation each period. This specification for $s(n)$ captures the same-side network effect in reduced form. For simplicity, we specify that $s(n)$ is equal to zero unless $n \geq M$, where M is an exogenous critical mass requirement. If this critical mass is achieved, then $s(n)$ is equal to s from the previous section.

We continue to focus on equilibria featuring symmetric strategies by players during the ICO stage. As in the prior section, any user who purchases a token initially will trade on the platform every period once it launches. Then, assuming that the critical mass M was achieved during the ICO, each user's willingness to pay is equal to

$$V(n) \equiv \frac{1}{\rho(\rho+2)} \left(s(n) - \frac{c}{1+\rho} \right),$$

which is simply the capitalized value of future utility flows. If the critical mass is not achieved, $V = 0$.

To launch a platform that uses tokens, the entrepreneur must first distribute them to users via an ICO.[17] She has at least two options to do so. First, she can sell all the tokens at once immediately before platform launch, in an ICO that lasts for only one period, and charge each user a cost $P > 0$ per token. Under this option, the multiple possible values of V create the second coordination problem mentioned above: The platform is socially valuable, with a total surplus of $N \times V$, but the entrepreneur can only guarantee participation by giving the tokens away for free, in which case she recoups no rents from the platform and any fixed cost $K > 0$ is enough to prevent the platform from being launched in the first place.

To see this formally, suppose the entrepreneur sets a price $P > K/N > 0$ in the hopes of achieving a positive ex-post payoff from having launched the platform. The lifetime payoff to a user of type A, as a function of both his own and others' actions during the ICO, is

$$\begin{cases} 0, \text{ if he does not buy the token} \\ -P < 0, \text{ if he buys the token but fewer than } M \text{ users do} \\ V - P > 0, \text{ if he buys the token and at least } M \text{ users do} \end{cases}$$

Clearly, there are multiple symmetric, self-fulfilling equilibria given this payoff function: One in which all users join and the entrepreneur recovers an ex-post surplus of $P \times N - K > 0$; and another in which no users join and the entrepreneur bears a utility loss of K. The possibility of this negative outcome due to coordination failure may cause a valuable platform not to be launched in the first place.

The entrepreneur's second option to distribute the tokens is to sell the tokens during an

---

[17] In practice, speculators may purchase tokens without intending to use them, but there is no role for speculation in the model without introducing uncertainty and private signals. We analyze speculation when we introduce these features into the model later in the paper.

ICO that lasts multiple periods $T > 1$ with the token price following a schedule P_t, where t indexes the time periods during the ICO. The number of tokens that have been sold is public knowledge at all times, thanks to the transparency afforded by the blockchain.

The key result in this section is that the entrepreneur's choice of T, or how many periods to run the ICO, affects whether or not the platform launch is privately optimal. When $T = 1$, then prospective users make simultaneous decisions on whether to subscribe to the platform, as in the simultaneous-move payoff function described above. The critical mass requirement generates multiple equilibria, including one in which no users join. Anticipating this inefficient outcome, the entrepreneur may choose not to launch a potentially valuable platform. The same logic holds whenever $1 \leq T < M$: There exist multiple equilibria, in some of which the platform is unsuccessful due to coordination failure.

However, when $T \geq M$, coordination failures are eliminated in any sub-game perfect equilibrium in pure strategies. This is summarized in the following theorem.

Theorem 3.1. *Suppose the entrepreneur announces an ICO that consists of a number of periods* $T \geq M$ *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* $P < V$*. Then in any subgame perfect equilibrium in pure strategies, all users purchase tokens and join the platform by time* $t = T - M + 1$*.*

Proof. See Appendix C. □

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.

Theorem 3.1 explains many stylized facts about ICOs, as discussed below.

Importance of the potential ICO duration Even though an ICO with $T = M$ will only last one period in equilibrium, and the platform will launch immediately afterward, the entrepreneur must still announce a *possible* (and credible) horizon for the ICO of M periods, and must also discount the initial price of the coins by $(1 + r)^M$. Both of these features are due to the off-equilibrium-path reasoning of the potential users: To guarantee their immediate participation, they must be assured that all other users will eventually join, and that there can be no strategic benefit to waiting to join, even if (off the equilibrium path) no other users join at $t = 1$. On the other hand, the logic in the proof also assumes a definite *end* date to the ICO, so that it cannot last forever. Note that the credibility of all these requirements are guaranteed thanks to the self-enforcing smart contracts used.

Escalating price schedules Theorem 3.1 also explains the often observed escalating price schedules in ICO deals. Note that under the price schedule, the present value of the entrepreneur's proceeds in an ICO does not really differ from that in a formal platform launch (conditional on the platform being successfully launched). 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.

In Theorem 3.1, the token price grows at the discount rate r. 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 the critical mass requirement N, and the rate r should adjust accordingly. We analyze fundamental uncertainty in Section 3.2.

Pre-ICO token discounts The requirement to discount the price of the tokens by T periods leads to an interesting tradeoff: It may be optimal to underprice or even give away some coins up front to committed users, simply to move closer to the critical threshold, shortening the necessary length of the ICO, and thereby attaining a greater price for the remaining tokens.

If the entrepreneur gives away m tokens up front, then conducts an ICO lasting $N-m$ periods, her total revenues will be given by $(N-m) \times \frac{P}{(1+r)^{N-m}}$. This expression is concave in m under certain conditions,[18] yielding the revenue-maximizing decision (by first order condition with respect to m) $N-m = \frac{1}{\ln(1+r)}$. This practice resembles the frequently-observed private-round "pre-ICOs," in which an exclusive group is invited by the entrepreneur to purchase tokens at a discount even before an ICO opens to the general public.

We note that, since the tokens are underpriced during the pre-ICO, the pre-ICO must be rationed or otherwise everyone would participate and the entrepreneur would end up with nothing. Furthermore, if the tokens are given away completely for free, they should only be given to users for whom it is common knowledge that they will use the platform once launched (for example, enthusiasts who have credibly communicated that intent through other means), as the fact that these tokens are given away for free means that other players will not apply forward induction when reasoning about the actions of the recipients.

ICO mega-deals From the proof of Theorem 3.1 we see that given the token pricing schedule, it is indeed a dominant strategy for any user to participate in the ICO immediately, not necessarily to increase payoff, but to avoid a coordination failure. This explains why an ICO can often attract large amounts of capital very rapidly even when a company has not yet launched a product. Empirically, the ICO universe often features "mega-deals," sometimes described as "fetching millions in minutes". Such a pattern may appear at first glance like irrational exuberance. While we do not rule out the possibility of bubbles in the current ICO market, Theorem 3.1 indicates that the large scale of some ICO deals may also have rational foundations: while accelerating the build-up of network effects and resolving a coordination problem that is endemic to platform-based startups, ICOs effectively front-load future users.

---

[18] More precisely, a sufficient condition for the problem to be concave is $N < \frac{2}{\ln(1+r)}$. Thus, for a large user base or a low discount rate, there may not be an interior optimal number of tokens to give away.

3.2 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 3.2 (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. $\square$

To be clear, this result does not state whether speculation will or will not happen. There are multiple equilibria, and we do not suggest any mechanism to select one from the other. In this sense, the wisdom of the crowd may be a fragile effect in our setting. 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 may generate economic values for certain early stage projects, we discuss implications for the recent debate over ICO regulations.

First, contemporary dialogue over ICOs has mainly been legal in nature, focusing on how to apply existing security laws and practices such as the Howey test. We set aside this legal approach and instead pursue an economic analysis, using efficiency as the criterion for assessing when ICOs, especially ICOs of many self-claimed "utility" tokens, should be restricted, allowed, or even promoted. As few rigorous economic analyses of ICOs currently exist, our study offers a fresh perspective.

In a strictly legal sense, the specific question of whether a token sold in a particular ICO is a security is outside the scope of this paper, but in economic terms, our model suggests that for many platform-based ventures the answer may be no. An ICO does lead to cash inflows to the startup, likely at a time when it needs funds, yet financing may not necessarily be the main purpose of an ICO. Rather, an ICO may be an integrated part of a platform's operational process to build up user interactions.[19] Since in reality many tokens may blend both security and utility features, we suggest regulators, entrepreneurs, and ICO participants to clearly distinguish the security and utility aspects of any tokens to be issued.

Second, since the effectiveness of tokens as credible signals of future use (in the case

---

[19] To borrow words from Ryan Zurrer, Principal & Venture Partner of Polychain Capital, ICO is about fostering a community and "tokens act like rocket fuel for network effects."

of network effect) or platform quality (in the case of fundamental uncertainty and private information) relies on the transparency of token activities, which is partially guaranteed by (almost) real-time recording within the ICO smart contract, cautions should be given to potential off-chain abuses or manipulations. For example, one manipulation a dishonest entrepreneur can exploit is to offer private off-chain side payments to bribe for fake ICO activities. In response, we suggest regulators to impose necessary 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.

Third, by identifying an important channel through which ICOs could create economic values, we caution against universal ICO bans currently adopted by Chinese and South Korean authorities since September 2017. While these regulators' concerns over market integrity and financial stability are understandable, such extreme regulatory reactions do come at costs: The indiscriminate stifling of a financial innovation that is valuable under certain conditions may put one jurisdiction at a competitive disadvantage against those that permit or even promote it.

For entrepreneurs, we suggest a project issuing "utility tokens" to be always very clear on how the issued tokens serve as an integrated element in the project. While qualified investors may be free to speculate, the fundamental purpose of such ICOs should be to facilitate platform building, rather than returns on capital. Companies that ignore or muddy this distinction should be viewed skeptically by both investors and regulators.

For regulators, we suggest giving leeway to proposed ICOs that justify themselves in terms of the benefits described in this paper. This may require carving out a special regulatory exemption for tokens that do fall under the legal definitions of securities. Of course, such exemptions should not prevent oversight of other dimensions of project risks: For example, the requirement to disclose compensations for celebrity endorsement as discussed above to prevent manipulation, or other governance measures to prevent entrepreneur absconding with raised funds, from which we abstract away in the current paper.[20]

In contrast, 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 other justifications for an ICO may exist, we view coordination as likely the primary benefit of "utility" tokens. We also note that any other proposed benefit of ICOs should be subject to a similar scrutiny as conducted in this paper before being accepted as a justification for offering. A claimed utility token that fails this test may simply be a classic security issuance in disguise.

Finally, our analysis provides regulators a preliminary framework toward a rule-based ICO regulation. Most major economies today have been following a case-by-case approach. 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".[21] In Canada, the Ontario Securities Commission (OSC) approved the ICO of TokenFunder, even after issuing warnings against ICOs earlier in the year.[22] But a case-by-case approach has 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.

5 Conclusion

In this paper, we develop a framework to understand the role of tokens and ICOs in the development of platforms. Instead of following the conventional legal perspective of focusing on whether tokens should be regarded as utilities, securities, or other categorizations, we

---

[20] An ICO with a "hard cap" may provide proper incentives against this moral hazard problem. A hard cap is a limit on the number of tokens to be sold in an ICO, which essentially requires the issuer to retain a minimum number of tokens post-ICO, similar to the retention of an equity stake in a public offering.

[21] See here.

[22] See here and here.

take an economic perspective, and ask if and when token sales are value-creating or value-destroying, using social welfare as the main criterion. We highlight that tokens can serve as a device to prevent inefficient coordination failures for projects that feature network effects.

Our findings have implications for regulators as well as practitioners in the growing ICO market. Just as history has taught us that financial innovations are often accompanied by exploitations of enthusiasm as well as holes in existing legal frameworks, at the moment many proposed ICOs are indeed hypes or even scams. By offering an explanation of how tokens create value, we help regulators and practitioners separate the wheat from the chaff in this emerging market for 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."

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

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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.*

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

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

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

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

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

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

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

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

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

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

Liu, Shannon. 2018. “A Theory of Collective Investment with Application to Venture Funding.”

Momtaz, Paul P. 2018. “Initial coin offerings.”

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

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

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

Sockin, Michael, and Wei Xiong. 2018. “A Model of Cryptocurrencies.” *Working Paper.*

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

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

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

Xu, Ting. 2016. “The Informational Role of Crowdfunding.” *Available at SSRN 2637699.*

Appendix

A Summary of International Regulatory Responses

Table 1: 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]
(**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]
(**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]

Jurisdiction & Regulator	**Date**	**Regulatory Responses**
(**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 Theorem 3.1. 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. □

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,

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

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

$$\mathbb{P}(M = m) = \binom{N}{m}(1 - F_V(x^*))^m F_V^{N-m}(x^*) \tag{2}$$

Hence, we obtain the entrepreneur's problem below:

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

$$p\sum_{m=0}^{N} Pm\binom{N}{m}(1-F_H(x^*))^m F_H^{N-m}(x^*)+(1-p)\sum_{m=0}^{N} Pm\binom{N}{m}(1-F_L(x^*))^m F_L^{N-m}(x^*), \tag{3}$$

subject to

$$\frac{pf(x^*)}{pf(x^*) + (1-p)} = P \text{ (user IC)} \tag{4}$$

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

$$\mathbb{P}(V = 1|X, m) \geq P_1, \tag{5}$$

where

$$\begin{aligned} \mathbb{P}(V = 1|X, m) &= \frac{p\mathbb{P}(X, m|V = 1)}{p\mathbb{P}(X, m|V = 1) + (1-p)\mathbb{P}(X, m|V = 0)} \\ &= \frac{p\mathbb{P}(X|V = 1)\mathbb{P}(m|X, V = 1)}{p\mathbb{P}(X|V = 1)\mathbb{P}(m|X, V = 1) + (1-p)\mathbb{P}(X|V = 0)\mathbb{P}(m|X, V = 0)} \\ &= \frac{pf(X)\mathbb{P}(m|X, V = 1)}{pf(X)\mathbb{P}(m|X, V = 1) + (1-p)\mathbb{P}(m|X, V = 0)} \end{aligned} \tag{6}$$

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 (6)=

$$\begin{aligned} & \frac{pf(X)\binom{N-1}{m}(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1}}{pf(X)\binom{N-1}{m}(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1} + (1-p)\binom{N-1}{m}(1 - F_L(x_0^*))^m(1 - F_L(x_0^*))^{N-m-1}} \\ = & \frac{pf(X)(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1}}{pf(X)(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1} + (1-p)(1 - F_L(x_0^*))^m(1 - F_L(x_0^*))^{N-m-1}} \end{aligned} \tag{7}$$

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

$$\frac{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)} = P_1(m) \tag{8}$$

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

$$\mathbb{P}(V = 1|X) \geq P_0 \tag{9}$$

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

$$\mathbb{P}(V=1|X) - P_0 \geq \mathbb{E}_m\left[\mathbb{P}(V=1|X,m) - P_1(m)|X\right], \tag{10}$$

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 (9) and (10) are expanded to

$$\frac{pf(x_0^*)}{pf(x_0^*)+(1-p)} \geq P_0 \tag{11}$$

$$\sum_{m=0}^{N-1}\left[P_1(m)\cdot\binom{N-1}{m}\cdot\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right] \geq P_0 \tag{12}$$

Since $\forall m, x_1^*(m) \leq x_0^*$, by (8)

$$P_1(m) \leq \frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}, \tag{13}$$

hence the left hand side of (12)$\leq$

$$\begin{aligned} &\sum_{m=0}^{N-1}\left[\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}\right. \\ &\left.\cdot\binom{N-1}{m}\cdot\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right] \\ = &\sum_{m=0}^{N-1}\left[\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\cdot\binom{N-1}{m}\right] = \frac{pf(x_0^*)}{pf(x_0^*)+(1-p)}. \end{aligned} \tag{14}$$

Hence we do not need to consider (11) as it is absorbed by (12). 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)

$$\begin{aligned}
& Np \sum_{m=0}^{N-1} P_1(m) \left(F_H(x_0^*) - F_H(x_1^*(m))\right) \binom{N-1}{m} (1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) \\
+ \quad & N(1-p) \sum_{m=0}^{N-1} P_1(m) \left(F_L(x_0^*) - F_L(x_1^*(m))\right) \binom{N-1}{m} (1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*), \\
+ \quad & NP_0 \times \left[p(1 - F_H(x_0^*)) + (1-p)(1 - F_L(x_0^*))\right]
\end{aligned} \tag{15}$$

subject to

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

$$\frac{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)} = P_1(m) \tag{16}$$

2. x_0^* is given by

$$\sum_{m=0}^{N-1} \left[P_1(m) \binom{N-1}{m} \frac{pf(x_0^*)(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*) + (1-p)} \right] = P_0 \tag{17}$$

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

$$\begin{aligned}
& \text{argmax}_{\{x_0^*, x_1^*(m)\}} N \sum_{m=0}^{N-1} \binom{N-1}{m} \frac{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)} \cdot \\
& \Big\{ p \left(F_H(x_0^*) - F_H(x_1^*(m))\right) (1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p) \left(F_L(x_0^*) - F_L(x_1^*(m))\right) (1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*) \\
& + \frac{pf(x_0^*)(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1-p)(1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*) + (1-p)} \left[p(1 - F_H(x_0^*)) + (1-p)(1 - F_L(x_0^*))\right] \Big\}
\end{aligned} \tag{18}$$

In comparison, the entrepreneur's payoff without ICO is

$$\begin{aligned}
& \sum_{m=0}^{N} \frac{pf(x^*)}{pf(x^*) + (1-p)} m \binom{N}{m} \left[p(1 - F_H(x^*))^m F_H^{N-m}(x^*) + (1-p)(1 - F_L(x^*))^m F_L^{N-m}(x^*)\right] \\
= \quad & N \frac{pf(x^*)}{pf(x^*) + (1-p)} \left[p(1 - F_H(x^*)) + (1-p)(1 - F_L(x^*))\right],
\end{aligned} \tag{19}$$

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

$$\text{argmax}_{\{x_1^*(0)\}} N \frac{pf(x_1^*(0))}{pf(x_1^*(0)) + (1-p)} \cdot \left[p\left(1 - F_H(x_1^*(0))\right) + (1-p)\left(1 - F_L(x_1^*(0))\right)\right] = (19)$$

Hence introducing ICO always improves the entrepreneur's payoff. $\square$