Working Paper presented at the

Peer-to-Peer Financial Systems
2018 Workshop

May, 2018

Initial Coin Offering and Platform Building

Jiasun Li
George Mason University

P2P Financial Systems

Powered by
Exponential Science

Initial Coin Offering and Platform Building

May 31, 2018

Abstract

In an initial coin offering (ICO), a company (or an open-source project) pre-sells tokens which will serve as an internal medium of exchange within a peer-to-peer platform yet to be built. We present a model that rationalizes the use of ICOs for launching such platforms: by adding dynamics to a platform launch, ICOs can 1) solve a coordination failure inherent in many platforms with network effects; and 2) harness the "wisdom of the crowd" by aggregating dispersed information about platform quality. Through either mechanism, an ICO increases platform value, makes the launch of a valuable platform more likely, and thus increases social welfare. We use our model to provide guidance to regulators: We analyze under what circumstances ICOs should be banned or allowed, and discuss governance mechanisms that they should include.

Keywords: coordination game, ICO, FinTech, network effect, wisdom of the crowd

Initial coin offerings, or ICOs, have recently emerged as a popular alternative venture financing method. In a typical ICO, an entrepreneur raises capital by pre-selling a "token" which gives its owner the right to use the company's product or service once it is developed. Many token owners also expect to resell their holdings for financial gain. These features blur the boundary of product pre-sale and security issuance.

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 could be interpreted as evidence of either a valuable innovation, or a dangerous bubble. Since ICOs do not fit neatly into existing securities or consumer-protection laws, regulators are concerned that ICOs may present new opportunities for exploitation or fraud.[2] Indeed, many ICOs are difficult to justify either as products or investments.[3]

One potential regulatory response is to ban ICOs completely. Indeed, some jurisdictions are cracking down: Chinese authorities banned all ICOs in early September 2017, followed by South Korea later that month. While this reaction is understandable given regulators' concerns over market integrity and financial stability, a one-size-fits-all approach also comes at a cost. Stifling a financial innovation, if it ultimately turns out to be valuable, may put one jurisdiction at a competitive disadvantage against those that permit or even promote it.

Other regulators have followed 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".[4]

[1] See here.

[2] For example, the SEC has prosecuted Maksim Zaslavskiy for alleged fraud in REcoin and DRC ICOs.

[3] A widely-cited example is Synthorn (http://synthorn.com/), which proposes to sell a synthetic rhinocerous horn aphrodisiac using the Ethereum blockchain. The Synthorn white paper is only three pages long, with only twelve words on market risk.

[4] See here.

In Canada, the Ontario Securities Commission (OSC) approved the ICO of TokenFunder, even after issuing warnings against ICOs earlier in the year.[5] But a case-by-case approach has its own problems: A lack of clear rules *ex ante* adds another source of risk for startups, investors, and other stakeholders in the the already risky early stage financing world. Table 1 provides a summary of global regulatory responses to ICOs.

In sum, regulators and practitioners are in need of an effective rule-based framework for regulating ICOs, which would preempt fraudulent activity while permitting if not promoting issuances that create economic value, if any. The first step towards such a framework is to have a clear understanding of the fundamental economic value an ICO creates. Yet despite the widespread media attention paid to ICOs, there has been little analysis on just what that value might be.

This paper attempts to fill this gap. We address the fundamental question of when, and by what economic mechanism, the ICO structure may create value for entrepreneurs and users – and, just as importantly, when it does not. Our model builds on the observation that many well-received ICOs have helped to build a platform. Examples include Ethereum, which is building a decentralized virtual machine as infrastructure for smart contract execution; Filecoin, which is setting up a network to allow peer-to-peer storage space sharing; and Unikrn, which is creating a platform for e-sports betting. We focus our analysis on the value of ICOs for launching such platforms.

A salient feature of a platform is that its value is largely driven by the interactions among its users who benefit from each others' participation. We highlight two related channels based on this insight that both lend value to an ICO. First, platform users' directly benefiting from each others' participation generates a strategic complementarity, known as a "network effect" (or a "network externality"): a user's gain from joining a platform increases with the number of other users. Second, information about the platform quality dispersed within

[5] See here and here.

the user base incentivizes each user to learn the "wisdom of the crowd" so as to make more informed participation decisions.

The presence of a network effect creates a strategic complementarity among users of a platform: if the platform does not attract a sufficient number of users, the surplus it can bring to new users will be too low to justify their participation. This creates a chicken-and-egg problem: how can the platform attract users in the first place, if they do not believe that others will join? We argue that an ICO helps to overcome this strategic complementarity.

The intuition behind how the ICO helps the platform overcome a strategic complementarity can be illustrated by a simple two-player game. Suppose there are two prospective users of a platform. Each user can spend C to get access to the platform, and enjoy a surplus of $S > C$ if and only if the other user also joins. Hence the payoff matrix is:

	join	quit
join	$(S-C, S-C)$	$(-C,0)$
quit	$(0,-C)$	$(0, 0)$

Clearly there are two Nash equilibria in this coordination game: either both users join the platform, or neither joins. An entrepreneur launching the platform would like to avoid the second inefficient equilibrium in which she gets zero payoff.

One simple way to avoid the self-fulfilling bad equilibrium is to simply designate one user to be a first-mover and make the first move perfectly observable to the follower. By breaking a simultaneous game into two stages, the entrepreneur effectively converts multiple Nash equilibria into a unique perfect equilibrium, in which the efficient outcome will be selected. Furthermore, we prove that even if there is no designation, i.e. both users can self-select to move first or second, the mere existence of two stages motivates both users to join the platform immediately. Section 2 leverages this insight to explain several empirical observations about the ICO structure, including the relationship between private pre-ICO rounds, public rounds of ICOs, and formal platform launches. Our analysis also explains the

escalating price schedules often observed in public token sales.

The "wisdom of the crowd" aspect of a platform kicks in when prospective users are heterogeneously informed. In a static game without ICOs, only users with relatively high signals will join, even if full participation in the platform is efficient. In such cases, the entrepreneur may be able to induce more participation by setting a low price, but full participation is never obtainable. Furthermore, the loss of profits due to price cutting may prevent some positive NPV platforms with large fixed costs from being launched at all, creating a social welfare loss. An ICO addresses this problem by creating an earlier stage for users to join the platform. Those with high signals join at the earlier stage; then their decisions, in conjunction with the token price, will be informative about the value of the platform. For a valuable platform, participation increases at the second stage, creating a social surplus, some or all of which can be appropriated by the entrepreneur.

Our results provide several implications for policymakers and practitioners. First, we provide a rationale to argue against universal bans adopted by China and Korea. A universal ban of ICO for fear of its (real) problems may risk throwing the baby out with the bathwater. Second, a proposed ICO should explain why a platform-like feature is an essential feature of the project's business model. 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 in this paper. Third, we endorse the SEC's warnings against potential abuse by celebrity-endorsed ICO deals, by rigorously modeling its possibility and the underlying incentives. We emphasize the regulatory role of disclosure requirement of off-chain activities related to ICO issuances. Finally, we provide support for the SEC's "substance" principle, by showing that in contrast to how they are often described, many tokens serve as devices to facilitate a successful platform launch without necessarily serving as a *financing* method. These tokens should not be simply viewed as securities for financing purposes that naturally fall under the jurisdiction of existing securities laws; but rather as

part of the operation process of a platform-like project, which fuel the build-up of network effects and spur the growth of socially valuable enterprises.[6]

Related literature To our best knowledge, we are the first to theoretically model ICO and analyze related topics. Our analysis touches upon multiple fronts of the literature.

Our analysis first contributes to 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.

Our results also relate to the two-sided markets literature, 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 are closely related to the crowdfunding literature. Strausz (forthcoming) and Ellman and Hurkens (2015) study the optimal reward-

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

based 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. Alternative theoretical mechanisms are studied by 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 do respectively learn from the crowd wisdom. We also compare some aspects of our model with all-or-nothing or keep-it-all clauses that have been studied in the context of reward-based crowdfunding, where there is some debate as to their merits in both a relative and an absolute sense (e.g. Cimon, 2017; Brown and Davies (2017); Li (2017); Kumar, Langberg and Zvilichovsky, 2015; Cumming, Leboeuf and Schwienbacher, 2015; and Chang, 2015.) The wisdom of the crowd discussion relates to a growing literature, see e.g. Surowiecki (2005), Da and Huang (2015), Dindo and Massari (2017), Kremer, Mansour and Perry (2014), Kovbasyuk (2011).

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) or new advances of voluntary disclosure (Shen and Zou, 2017). The technical tools used in the second half of our paper are also inspired by the global-games literature (e.g. Carlsson and Van Damme, 1993; Morris and Shin, 1998; and Goldstein and Pauzner, 2005). Finally, the ICO demonstrates the value created by dynamic interactions in the presence of static frictions, as explored generally in papers such as Daley and Green (2012), although our mechanism is different from theirs.

1 Network effects throughout the ICO universe

Network effects describe a situation in which a user's surplus from a transaction increases with the total number of transactions ("the more the merrier"). While established firms often benefit from network effects, start-ups in industries featuring network effects often need to spend significant resources to build up a critical mass before ever taking off. Network effects exist in many business models, and are especially prevalent among those for which ICOs are common. In this section, we describe several categories of network effects and present notable ICO cases within each category. We also highlight several stylized facts about ICOs that will be captured by our model in Section 2.

Social networks Social networks are a quintessential example in which platform success largely hinges on network externalities. If none of your friends are following MySpace anymore, there is little value for you to be active on MySpace either. On the other hand, if many of your friends are sharing interesting things on Facebook, you will enjoy high utility from engaging in the Facebook community. Under our reasoning, social media companies characterized by strong network externalities are likely to use ICOs to achieve the efficient equilibrium outcome with large scale participation.

Consistent with this logic, social media platform Kik launched a crowdsale which 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.[7] 10,026 individuals from 117 countries contributed 168,732 ETH (about $48 million dollars) to the public ICO, which adds to the $50 million raised in an earlier round of private pre-ICO.[8] According the firm's press release, a $98 million ICO proceeds makes Kin "one of the most widely held cryptocurrencies in the world".

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

[8] 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/.

A notable feature of Kik's ICO is that it imposes a cap on how many Kin a buyer can purchase. This does not seem to be a reasonable move if the company's goal is solely to maximize revenue, but it may help address a network effect, as we show below. Furthermore, Kik explicitly chose an ICO instead of traditional VC financing to foster a community.[9] We will return at the end of our paper to a comparison of these strategic and financing motives behind an ICO.

Sharing economy Network effects also 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 network externality would work toward the efficient equilibrium.

As an example of this intuition, decentralized data storage network Filecoin launched an ICO via CoinList, a joint project between Filecoin developer Protocol Labs and startup investment platform AngelList, and raised approximately $205.8 million over the next month. This added to the $52 million collected in a private presale catered to notable VC firms including Sequoia Capital, Andreessen Horowitz and Union Square Ventures, etc.[10] Filecoin operates like an "Uber for file storage," which aims 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, like many other ICO deals, adopted a sales model in which the mini-

[9] See explanation here.

[10] That launch day "was notable both for the large influx of purchases of Simple Agreements for Future Tokens, or SAFTs (effectively claims on tokens once the Filecoin network goes live), as well as the technology issues that quickly sprouted as accredited investors swamped the CoinList website." See https://www.coindesk.com/257-million-filecoin-breaks-time-record-ico-funding/.

mum price buyers must pay rises as more investors join in. This pattern will emerge endogenously in our model as a way to subsidize first movers and overcome network effects.

Blockchain infrastructure As a decentralized database, a blockchain itself is an example of network effect. When more users are maintaining a blockchain (or mining, in the specific case of the Bitcoin blockchain), its security will be enhanced, and each user will enjoy a higher utility from using the blockchain, thanks to decreased concerns of single-point-of-failure or censorship. It is hence not surprising to see token sales to be widely adopted by entrepreneurs who are developing new blockchains.

The most salient example is the large-scale crowdsale of Ethereum. As a decentralized computing platform featuring smart contract functionality, Ethereum extends the Turing-incomplete language Script embedded in Bitcoin and develops a new blockchain to support the Ethereum Virtual Machine (EVM), a Turing-complete virtual machine, which execute scripts using an international network of public nodes. The project was funded during July-August 2014 by the crowdsale of "ether," a cryptocurrency token used for transfers between accounts as well as compensation to participant nodes for computations performed. The system went live on 30 July 2015, with 11.9 million coins "pre-mined" for the crowdsale. Today, Ethereum has been used as the platform for most other coin offerings.

A separate example comes from the recent open-cap ICO conducted by Tezos. In order to create "a new decentralized blockchain that governs itself by establishing a true digital commonwealth," Tezos raised 65,703 bitcoins and 361,122 ethers (around $232 million) during its crowdsale window of July 1 - 14, 2017. Partially due to the strong network effect embedded in the nature of the project, the campaign end up being the largest crowdsale ever by the time of its completion.

Marketplaces Fostering a well-functioning market has long been recognized in both the finance literature and practice as an example of a coordination game. Barclay and Hen-

dershott (2004) test the theory of "liquidity externality" by studying the after-hours stock market. Most stock exchanges hold policies to subsidize a subset of "market makers" to obtain the critical mass for network effects to work (e.g. historically offering privileges to designated market makers, or recently offering rebates to liquidity providers). Hence we expect startups lauching exchanges or marketplace-like platforms would necessarily find ICOs to be an effective tool.

Indeed, t∅, a subsidiary of online e-commerce marketplace Overstock.com, formally announced on Oct 24, 2017 a campaign to sell Simple Agreements for Future Tokens (SAFTs), a model also used by the Filecoin ICO.[11] According to the company, the t∅ ICO will first run as a private pre-sale from Nov. 15 to Dec. 31 to accredited investors. "The proceeds from the ICO will help the company scale its technology development and regulatory teams, as well as either build or take over a custody and clearing firm".

Prediction and online gambling market are another example of marketplace featuring network externality, as placing bets requires a counterparty. A larger market also improves risk management for the market maker. It is thus not surprising that prediction and online gambling markets have been frequent adopters of ICOs. A prominent example is Unikrn, whose underlying token UnikoinGold – developed to serve as decentralized token for e-sports and gaming – fetched $15 million in pre-sale from private backers including Mark Cuban, and 110,000 ethers in public token sale. Another example is Augur, which attempts to build a decentralized network for accurate forecasting, and which was funded via an online crowdsale during August and October of 2015. In addition to featuring network effects, as a decentralized platform Augur also builds on the notion of the wisdom of the crowd.

Related to the development of prediction markets is the crowdsourcing of computation resources in machine learning/artificial intelligence. Ensemble machine learning algorithms such as AdaBoost or Random Forest require a large volume of parallel training to produce an

[11] https://www.coindesk.com/overstocks-launching-initial-coin-offering-next-month/

accurate outcome. A coordination problem arises here again: Only if a critical mass of data scientists have commited to contribute will the learning outcome be attract enough to new participants; but how can one attract such a critical mass in the first place? An example of an ICO addressing this problem is the crypto-token known as Numeraire. On February 21, 2017, 12,000 data scientists were issued 1 million Numeraires to incentivize the construction of the artificial intelligence hedge fund Numerai. Founder Richard Craib states, "the most valuable hedge fund in the 21st century will be the first hedge fund to bring network effects to capital allocation."[12]

Exchanges

The ICO process An ICO typically works in the following procedure:

1. issuance of ERC-20 tokens
2. mainnet development
3. convert ERC-20 tokens to mainnet cryptocurrencies

2 Model: ICO coordinates the efficient equilibrium

In this section, we build a model to illustrate how an ICO can be used to overcome coordination failures when the underlying project is characterized by network effects. In our model, time is discrete and runs forever. An entrepreneur can incur a fixed cost K to launch a platform, which will then facilitate trade in some service among $2N$ potential users for a potentially-infinite number of periods thereafter. We first describe the operation of this platform once it has launched, then explain how the ICO can aid the launch.

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

2.1 Operation of the platform after launch

Once the platform is launched, each period is divided into two sub-periods, which we label morning and night. Users on the platform are also divided into two types, which we label A and B, with N users within each type. Type A users derive utility from the service provided on the platform in the morning, and can supply that service at a utility cost of c in the night. Type B users have the opposite timing: They can supply the service at cost c in the morning, and derive utility from the service in the night. This setup naturally creates gains from trade between the two 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 moment in time, but rather must interact dynamically to realize the gains from trade.

Within each sub-period (morning or night), trade occurs sequentially: Buyers of the service place their orders one at a time, with each seller receiving only one order.[13] Each seller must decide whether to accept the buyer's proposed payment. The platform specifies the form of payment for transactions, either an external currency (such as dollars or Bitcoin), or internal tokens created specifically for use on the platform.

The utility that each buyer receives from the service sold on the platform depends on the success of other transactions, which generates the network effect that is the focus of our analysis. We assume that buyers only obtain a utility $s > c$ if there are at least M total transactions (a critical mass) within the same sub-period.[14]

Everyone applies a common discount rate r between periods. For simplicity, we assume no discounting within periods. All players are adequately patient such that $\frac{s-c}{r} > s$, meaning that if all prospective users transacted over an infinite horizon, then the lifetime payoff from

[13] The specific ordering by which orders go to sellers is unimportant. It need not be fixed over time, nor common knowledge.

[14] For example, with a distributed file storage platform like Storjcoin, privacy can only be achieved when there are an adequate number of transactions.

the platform for each user is greater than the flow utility s from the service. We also assume that in this full-participation case the platform is positive NPV, i.e. $2NS > K$.

The first issue we address is the choice of payment method on the platform:

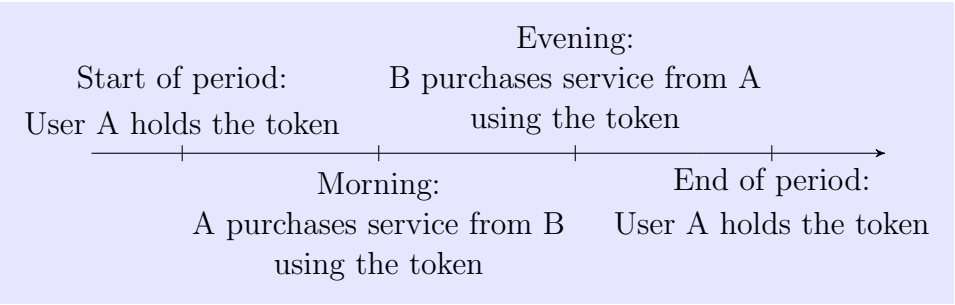
A platform without internal tokens Suppose that all transactions are conducted using dollars as the medium of exchange. At each stage within any period, a buyer purchases the service if she believes that at least M total buyers will do the same. The decentralized nature of the platform prevents effective coordination, and buyers cannot observe the total number of transactions that have occured or will occur in this period. Thus, there exist at least two Nash equilibria: One in which buyers expect adequate participation, and all buy; and another in which buyers do not expect adequate participation, and none buy.

Introducing internal tokens to a platform Suppose instead that the platform specifies some tokens as the only acceptable medium of exchange, as is the usual practice. We assume two defining features of the token that differentiate it from dollars: First, it has no value outside the platform. It cannot be used to purchase other goods or services, nor to pay taxes. Second, users can observe the aggregate ownership and transaction history of tokens on the blockchain, whereas these are not possible when payment occurs through dollars.

Without loss of generality, we assume the platform specifies a price of one token per unit of the service. We will study the initial token purchase decisions by type A users when we analyze ICO in the next section. For the moment we assume that all type A users strictly prefer to each purchase one token prior to the first period, and have done so. Figure 1 illustrates the sequence of moves within each period when the platform operates, assuming all potential trades happen.

We first analyze the buyers' decisions in each sub-period. Here, the network effect comes into play: As in the analysis with dollars, buyers only value the service if at least M total buyers choose to purchase it. However, any buyer who has already acquired a token from

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



the previous stage will purchase the service, because by construction the token has no use outside the platform: if she had not planned to use the token in the current stage, she'd have been better off not accepting the token in the previous stage. Thus, it is precisely the fact that tokens are worthless *outside* the platform that gives them value *within* the platform, by eliminating the coordination problem among the buyers as described above.

However, we must now explain why the sellers would be willing to accept these worthless tokens as payment in exchange for the real utility cost c of providing the service. For this to be rational, today's sellers must believe two things: First, that tomorrow's sellers (today's buyers) will accept the token tomorrow, when today's sellers demand the service. Second, that the critical mass of transactions will happen tomorrow. We address both points below:

Critical mass with tokens Assume for the moment that the first condition in the previous paragraph holds – that is, assume that tomorrow's sellers will accept the tokens in exchange for providing the service – and consider the second question: will the critical mass be achieved tomorrow? Here, the network effect that we specified between *buyers* becomes a coordination problem between today's *sellers*, since they will be the buyers tomorrow: If M sellers accept the coin today, then there will be M buyers tomorrow.

Consider the decision of the M^{th} seller, assuming all previous sellers have accepted the token. If the M^{th} seller accepts as well, there will be aggregate demand of M in the next

period, achieving the critical mass. For this seller, it is clearly rational to accept the token. Knowing this, the prior seller will also rationally accept the token in order to force the M^{th} seller into this situation. Working backwards, each prior seller will also accept the token, forcing the next seller into a situation in which it is rational to accept. Thus, assuming future sellers accept the tokens, there is no doubt that the critical mass will be achieved.

Future sellers will accept the tokens Now return to the condition that was assumed in the previous paragraph: Why should today's sellers believe that tomorrow's sellers will accept the token as payment? It might seem that an equilibrium exists in which future sellers never accept the tokens, causing today's sellers rationally to refuse the tokens as well. However, we are able to rule out such an equilibrium, at least up to a certain horizon of the platform's operation, by applying the *forward induction* equilibrium refinement of Govindan and Wilson (2009) and others.

Roughly speaking, this refinement says that, when an agent is observed to take any action, all other agents should put zero weight on future strategy profiles for the same agent under which the observed action could not possibly have increased the agent's lifetime utility. In our setting, the fact that type A agents paid a positive price for tokens during the ICO puts a lower bound on the length of time that they can be expected to accept the tokens when they are sellers on the platform.

Precisely, denote P as the price at which type A users paid for the tokens during the ICO. Forward induction requires that type B users calculate the number of dates it takes for type A users to attain positive net lifetime utility (evaluated at time zero assuming maximum payoff each date),[15] and then infer that type A users will keep accepting the tokens as sellers for at least that number of dates – as any such strategy profiles would certainly mean that it was suboptimal for the type A user to have purchased the token in the first place.

[15] Hence $(s-c)\left(\frac{1}{1+r}+\cdots+\frac{1}{(1+r)^V}\right) \geq P$.

We denote this number of dates as V, and we can calculate $V = \left\lfloor \ln\left(\frac{s-c}{s-c-rP}\right) \Big/ \ln(1+r) \right\rfloor$. Thus, type B users (the initial sellers) can be confident that the type A users intend to accept the tokens on the platform for at least V periods. This leads to the virtuous outcome in which both sides of the market rationally accept the token, expecting trade to be sustained, at least for periods $1, \ldots, V$. This horizon can be quite long: As an illustration, suppose that $s = 2$, $c = 1$, each period corresponds to one day, $r = 0.1\%$ per day, and $P = \frac{1}{2} \times \frac{s-c}{r} = 500$. Then $V = 693$ days, so that nearly two years can pass before the initial users recover their utility and their intention to continue accepting the token becomes doubtful.

Redemption commitment Beyond the horizon V, in the setup described above, behavior on the platform exhibits multiple equilibria, including the possibility that trade ceases completely after time V. In such an equilibrium, backward induction may render it suboptimal for Type A users to have purchased tokens prior to date 1. To prevent the outcome in which buying tokens is ex-post suboptimal for the Type A users, the entrepreneur includes a redemption option beyond date V, by committing to repurchase tokens on demand for a price of at least c, the flow utility cost of providing the service on the platform. This effectively creates an all-or-nothing mechanism for the service providers at any stage that guarantees their participation: At worst (if the sellers in the next stage choose not to accept the token), the current sellers still break even in utility terms if they accept the token today. Note that the entrepreneur need only guarantee a redemption value of c (or slightly greater), rather than the full token price, which we will show is much higher than c. Thus, when at least M buyers enter a given stage endowed with the token, trade on the platform will be sustained to the next stage with only the repurchase commitment described above.

Theorem 2.1 formalizes all the arguments presented above:

Theorem 2.1. *If $N \geq M$ type A users purchase tokens prior to first day morning for a price of $P \in (s, \frac{s-c}{r})$, and the entrepreneur commits to repurchase the token on demand for*

a price $\tilde{p} \in (c, s)$ after period V, then the unique equilibrium is for trade to happen in every period during an infinite horizon after the initial platform launch. To cover the potential repurchase of tokens, which happens off the equilibrium path, the entrepreneur initially must set aside $\frac{\tilde{p}}{(1+r)^V}$ for each token sold, where $V = \left\lfloor \ln\left(\frac{s-c}{s-c-rC}\right) / \ln(1+r) \right\rfloor$. The entrepreneur's surplus is $NP - K - N\frac{\tilde{p}}{(1+r)^V} > 0$, plus the membership fee (if any) charged to user B.

Proof. We first consider periods 1 to V, during which time the proof relies only on forward induction and the price that was initially paid during the ICO.

Suppose that user A has purchased the token in the ICO for a price of $P \in (s, \frac{s-c}{r})$. At the first date, consider the problem of user B, who initially is the seller of the service. He is willing to accept the token in exchange for providing the service only if he expects that user A will do the same in the next sub-period. Forward induction requires that user B reason as follows: If user A had planned to stop participating in the platform after the first sub-period, he would not have expected sufficient lifetime utility to justify paying $P > s$ for the token in the first place. The decision to have purchased the token is thus taken to be a reliable indicator that user A will accept the token tomorrow if user B accepts it today. This reasoning extends through date V, after which it no longer applies. During this time, the best response for user B is also to accept the token as a seller.

Starting on date V, any seller is willing to supply service in exchange for a token, as the payoff in the next sub-period will be no worse than to sell the token for $\tilde{p}$, which is better than the outside option of zero if the seller rejects the token. The same reasoning carries forward over the infinite horizon of the platform. On the equilibrium path, therefore, the entrepreneur never actually needs to repurchase any tokens. Furthermore, no external financing is required, because the price paid for the tokens is more than sufficient to cover the repurchase requirement, which simply leads to idle funds sitting on the firm's balance sheet. Furthermore, the entrepreneur need only set aside initially the amount $\frac{\tilde{p}}{(1+r)^V} < \tilde{p}$ to cover the potential future repurchase requirement. □

Token redemptions are indeed frequently observed after ICOs, but their role is not always clearly understood. Some view them as a way to decrease the supply of tokens and thereby increase their price; others view them as a means of payout, similar to equity repurchases. But neither argument accurately describes the role of the token redemption in our platform model. Instead, redemption provides a backstop to induce participation by users beyond the horizon that can be inferred based on the ICO sale price. We suggest that regulators and investors should view repurchase commitments as a useful governance requirement in light of the analysis presented here. However, as explained in the Theorem, the commitment need not exist immediately but only after time V. Furthermore, we note that these commitments can be made credible using the "lock time" feature afforded by smart contract technologies.[16]

The key conclusion of this section is that a fundamentally-worthless token can nevertheless sustain trade on a platform, and furthermore can overcome a coordination problem that would exist if trade were specified to happen in external currencies such as dollars. Intuitively, because tokens are worthless outside the platform, the decision to purchase a token credibly communicates an intent to use the platform for at least some duration. Finally, trade can be extended to an infinite horizon by augmenting the token sale with a repurchase commitment at a relatively low price compared to the original sale price of the token. Interestingly, when the entrepreneur extracts *more* of the surplus through a higher ICO price, this has the side effect of *increasing* the amount of time that the platform can operate before the repurchase commitment is necessary to select the good equilibrium.

With these insights in hand, we next turn to an analysis of the initial token sale process.

2.2 Launching the platform: overcoming the critical mass hurdle

Having explained the role of a token in a platform, we can now precisely clarify the role of the ICO. There are *two* coordination problems in the building of platform: First, once the

[16] See Chapter 3.3 of Narayanan et al. (2016).

platform is launched, the coincidence-of-wants problem in motivating users to trade when they produce and consume in different periods. The token discussed in the previous section addresses this problem. Second, there is another coordination problem prior to the platform launch: the platform need to attract enough initial buyers of the token. An initial coin offering (ICO) addresses the second coordination problem.

The entrepreneur has at least two options to launch a platform with tokens.

First, she can sell all the tokens at once immediately before platform launch, and charge a per-capita cost P to all prospective users for one token. As explained in the previous section, the platform launch is only successful if at least M type A users participate. Therefore a type A user's payoff, as a function of his and others' actions, is:

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

where $S = \frac{s-c}{r} > P > 0$ denotes a user's expected equilibrium surplus generated by the platform assuming that the platform operates forever, as defined in the previous section.

Alternatively, the entrepreneur can conduct an ICO prior to platform launch, during which she sells newly-created tokens to prospective users at some unit price schedule P_t.[17] Unlike the immediate platform launch, the ICO can last multiple periods $T \geq 1$. 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.

Definition 2.1.1 (ICO)**.** *An ICO consists of a window period of length T prior to the platform launch, during which tokens that can be used in the future once the platform is up and running are sold at a price schedule P_t, $t = 1, \ldots, T$.*

[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.

Tokens issued during the ICO will be used exclusively as internal currencies once the platform is launched. Furthermore, they can also be redeemed back to the entrepreneur for $\tilde{p}$ beyond some periods V.

Our first key result states that the entrepreneur's choice of T, or how many periods to run the ICO, affects whether a platform launch is viable or not. When $T = 1$, or when the entrepreneur chooses to launch the platform immediately without an ICO at all, then prospective users make simultaneous decisions on whether to subscribe to the platform. In this case, the critical mass requirement generates multiple equilibria: either all prospective users join the platform, or none does. In the latter case, a potentially positive NPV project ends up with a negative value of K purely due to coordination failure. 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 failures.

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

Theorem 2.2. *Suppose the entrepreneur, instead of launching the platform immediately, announces an ICO during which tokens will be sold that grant future access to the service provided by the platform. The ICO 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 all users who purchased tokens will participate. 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. Then in any subgame perfect equilibrium in pure strategies, all users purchase tokens and join the platform by time $t = T - M + 1$.*

Proof. 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 C. 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. □

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 2.2 explains many ICO stylized facts introduced in Section 1, 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 T periods, and must also discount the price of the coins by $(1 + r)^T$. 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. This assumption is realistic because it is costly to maintain the ICO indefinitely. Aside from the direct costs of maintaining the website, there are the larger opportunity costs of keeping the entrepreneur and any other necessary employees committed to the potential platform launch. T will therefore be constrained by the capital available to the entrepreneur or team launching the platform.

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 give away some coins up front, 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 that are sold. If the entrepreneur gives away m tokens up front, then conducts an ICO lasting $M - m$ periods, her total revenues will be given by $(N - m) \times \frac{P}{(1+r)^{M-m}}$. This expression is concave in m under certain conditions,[18] yielding the revenue-maximizing decision (by first order condition with respect to m) $N - m = \frac{1}{\ln(1+r)}$. As the discount rate increases, the entrepreneur optimally gives away more tokens up front and sells fewer tokens during the ICO. Such practices empirically resemble 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 given out for free (or sold at a steep discount) during the pre-ICO, the pre-ICO must be rationed or otherwise everyone would participate and the entrepreneur would end up with nothing. Furthermore, the tokens should only be given to those whom the entrepreneur knows can commmit to using the platform once launched, as otherwise such tokens may not add to the critical mass requirement.

ICO mega-deals From the proof of Theorem 2.2 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 (as the user's payoff does not differ from when he participates in the ICO or the actual platform launch conditional on a successful platform launch that attracts full participation), but to avoid a coordination failure. This explains why an ICO can often attract large amounts of capital very rapidly even when a company

[18] More precisely, a sufficient condition for the problem to be concave is $N < \frac{2}{ln(1+r)}$. Thus, if the user base is very large or the discount rate is very small, there may not be an interior optimal number of tokens to give away. The entrepreneur would optimally either sell them all, or give them all away. (In the latter case the entrepreneur would choose not to pursue the platform in the first place, due to the fixed cost K.)

has not yet launched a product. Empirically, the ICO universe often features "mega-deals", which are often described in media 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 2.2 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.

ICO bootstrapping platform launch The result on ICO mega-deals that all users immediately jump on the ICO bandwagon depends on the assumption that all users share the same M. In ongoing work, we will allow M to be heterogeneous across users. When each user i has possibly heterogeneous critical mass requirements M_i, the entrepreneur often will only need to accommodate a subset of users' M_i. This is because low M_i users can often "bootstrap" the process and motivate users with higher M_i to join as well.

Escalating price schedules Theorem 2.2 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 from a formal platform launch (conditional on the platform being successfully launched). Hence, while an ICO does superficially resemble financing methods like equity, it is not fundamentally a *financing* method, and it is only a convenient coincidence that the ICO raises large sum of funds at an early stage when they are likely valuable. The value of an ICO our framework is really about resolving a coordination failure, and it may be regarded as an organic element of a platform operation.

In Theorem 2.2, 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 M, and the

rate r should adjust accordingly. We analyze fundamental uncertainty in Section 3.

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 (and the price of the tokens will remain stable at S). In ongoing work, with the introduction of private information, we could model speculation.

Soft cap In summary, we demonstrate that for projects that need to quickly build up network effect, an ICO or pre-ICO helps overcome the critical-mass constraint. While ICOs do raise funds, they are more appropriately viewed as part of the operational process of project launches. In Section 3, we introduce uncertainty and provide an alternative channel for ICOs to create value, which will be compared with the network effect channel.

3 ICO harnesses the wisdom of the crowd

The multi-stage nature of ICOs offers an alternative channel other than breaking the network effect to create value: When the user community is adequately dispersed, and they possess useful information about the platform prospect in a decentralized way, introducing an ICO also helps harness their wisdom of the crowd. This channel works without necessarily assuming the presence of a network effect, so we shut it down in the analysis to follow. In the absence of a network effect, we assume the actual platform launch takes place within one stage, and the ICO can occur in a single prior stage.

We assume a continuum of users in this section for both expositional ease and to highlight the decentralized assumption about the user community. To be realistic as well as consistent with the analysis in the previous section, we also conduct all analysis with a discrete number of players in Appendix B, where we also illustrate the importance of a disclosure requirement

of celebrity/high-influence endorsement to prevent manipulation.

Again the risk-neutral entrepreneur can incur a fixed cost K to launch a platform, after which the entrepreneur can charge a per-capita cost C to a unit continuum of users for access to the platform. If the entrepreneur chooses to issue tokens as internal currencies to use the platform, C could be interpreted as the price for the tokens.[19] An individual user's payoff as a function of his action is then:

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

In the case where $T = 1$, S represents each user's surplus from using the platform in one period.[20] We assume a fundamental uncertainty about the surplus S: possible values of S are normalized to $S \in \{0, 1\}$, and the realization of S depends on the state of nature. All users share the common prior $\mathbb{P}(S = 1) = p$, and each user gets a noisy private signal X about the value of S, which is the only difference among them. We assume that the signals X are distributed according to the conditional distribution functions $(X|S = 1) \sim F_H$ and $(X|S = 0) \sim F_L$. Conditional on the realization of S, the signals X are independent of each other. Denote $F(x) \equiv pF_H(x) + (1 - p)F_L(x)$.

We assume that $f(x) \equiv F'_H(x)/F'_L(x)$ satisfies the monotone likelihood ratio property (MLRP), $f'(X) > 0$, which implies that $F_H(x) < F_L(x)$ for all x. In other words, for any given x, knowing $F_S(x), S \in \{H, L\}$ is perfectly revealing of the underlying state S. This property will be useful in the derivation of the ICO case later.

[19] In the prior section, the token price was labeled P. In this section, the model must deal with probabilities, which we denote with the usual symbol $\mathbb{P}(\cdot)$. To avoid any potential confusion, in this section we change the notation for the token price to C .

[20] When $T > 1$, S not only includes each user's surplus from using the platform in one period, but also the present value of all future resale prices of the token

3.1 The entrepreneur's problem without an ICO

Given a price C to join the platform, user i joins if and only if $\mathbb{P}(S = 1|X_i) \geq C$. Thus, a cutoff x^* is defined by setting this expression to equality,

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

The entrepreneur's problem is $\max_C C \times (1 - F(x^*))$, which yields the first-order condition

$$m_F(x^*) = C \times \frac{dx^*}{dC} \tag{2}$$

where m_F is the Mills ratio corresponding to the distribution F, defined as $m_F(x) \equiv \frac{1-F(x)}{F'(x)}$. The derivative $\frac{dx^*}{dC}$ comes from implicitly differentiating (1), which defines x^*.

This is a standard monopolist's problem: Condition (1) characterizes the user's demand, and condition (2) characterizes the entrepreneur's optimal price policy subject to that demand. Define C^* and x^* as the solutions to the pair of equations (1) and (2).

From these conditions we can see that there will be less than full participation, regardless of the state of nature, because no signal is high enough to guarantee that the state is good. Moreover, even when the state is good so that the potential surplus from launching the platform is 1, the entrepreneur captures less than this since both the price of the coin and the mass of participants will be less than one.

In general, the problem is that the static nature of the game prevents any state-contingent payoffs. The ICO will introduce dynamics that loosen this restriction and thereby increase efficiency.

3.2 The entrepreneur's problem with an ICO

We model the ICO as a pre-sale of tokens, each of which provides the right for one user to access the platform once it is launched later. Users can choose to join at time 0 or 1, and the entrepreneur sets prices C_0 and C_1 that are specific to these dates. We shut down any discounting between the two dates. The mass who join at time 0 is labeled μ and is public knowledge as of time 1. This mass constitutes the information that is released via the ICO, which is the role of the ICO in this model.

We will show that, by combining μ and C_0 with the common-knowledge distribution of signals and states, all agents perfectly observe the state at $t = 1$. If it is revealed that $S = 1$, all users join the platform at $t = 1$; otherwise none do. Thus if $S = 1$, the entrepreneur sets $C_1 = 1$ and captures all remaining surplus from the users who have not yet joined.

To show this, we characterize the time-zero participation decision by the users. At time zero, user i will make his decision by forming expectations about prices and information at time 1. He will join if and only if $Pr(S = 1|X_i) - C_0 \geq 0$ and $Pr(S = 1|X_i) - C_0 \geq \mathbb{E}[Pr(S = 1|X_i, \mu) - C_1^*|X_i]$. Applying iterated expectations to simplify the second of these, user i participates at time zero if and only if

$$C_0 \leq \min(Pr(S = 1|X_i), \mathbb{E}[C_1^*|X_i]) \tag{3}$$

This implies that the ICO participants are those who expect that both the surplus *and* the later price will be higher than C_0. In fact, these two conditions are redundant to each other: Because $C_1^* = 1$, we have $\mathbb{E}[C_1^*|X_i] = \mathbb{E}[\mathbb{1}\{S = 1\}|X_i] = Pr(S = 1|X_i)$. So we ultimately have a simple cutoff x_0^* defined by

$$C_0 = Pr(S = 1|x_0^*) \tag{4}$$

Notice that this mapping from price to cutoff signal is identical to (1). The price C_0 in this section may be different from the optimal C^* derived in that section (and we will show that it is), but given any value of C_0, we have the same logic as before, that the cutoff value of x^* will be the one at which the conditional probability of the good state equals that price.

Given a value of C_0, all agents with $X_i \geq x_0^*$ join the ICO at time 0, so all agents then observe $F_s\left(f^{-1}\left(\frac{C_0}{1-C_0} \times \frac{1-p}{p}\right)\right)$. This expression can only take on one of two potential values based on the potential values of s, and both of these potential values are common knowledge. Therefore, immediately after the ICO, everyone perfectly knows the state, verifying the conjecture made above. If it was revealed that $S = 1$, then all agents join the platform at time 1, and otherwise none do.

Finally, we analyze the entrepreneur's problem at time zero: The entrepreneur chooses C_0 to maximize expected profit,

$$\max_{C_0} \quad C_0 \times (1 - F(x_0^*)) + p \times F(x_0^*) \tag{5}$$

Compared to the no-ICO problem, this adds in a probability p that the state is revealed to be positive and all remaining customers buy in at price 1. This leads to the first-order condition

$$m_F(x_0^*) = (C_0 - p) \times \frac{dx_0^*}{dC_0} \tag{6}$$

Comparing with (2), we see that the potential for second-stage profits increases C_0 above the no-ICO price, via p. Intuitively, the entrepreneur is willing to accept a greater risk of losing customers by pricing too high at time zero, anticipating that if $S = 1$ he will be able to extract greater rents from these users later on.

Our main result in this section is the following

Theorem 3.1. *The entrepreneur achieves greater expected profit with than without the ICO.*

Proof. The entrepreneur would already be strictly better off with the ICO than without simply by setting C_0 equal to C^* from the non-ICO case, because with probability p he can now extract full surplus from everyone who did not buy in at time zero. In fact, in equilibrium he sets $C_0 > C^*$, but this is only done if it weakly increases his profits relative to setting $C_0 = C^*$. □

Discussion. The core intuition behind this results is that the entrepreneur is much better off when he has two stages over which to sell his product. However, this effect should not be interpreted as price discrimination: Conditional on a good state, the price actually increases over time, and the agents with the highest willingness to pay (the highest signals) actually pay the lowest price. Instead, the key mechanism here is the wisdom-of-the-crowd assumption. The ICO reveals the highest signals to all users, allowing all to judge the quality of the platform. Unlike the static game, there is then an additional time period at which the entrepreneur can sell access to the platform and realize the surplus from doing so.

3.3 Allowing for speculation in the ICO

ICOs are often described as an investment opportunity for those who buy in, and as an alternative financing source to debt or equity for the companies who undertake them. In this section, we analyze the gains to speculating in an ICO.

We introduce a unit mass of "speculators" who derive no utility from joining the platform, but can buy access to the platform at time zero and re-sell it later. They get their own signals about the platform quality separately from the users. The entrepreneur has no way to distinguish them from the other users, so they pay the same price as everyone else. We analyze the incentives of these speculators to buy and sell tokens at time zero and 1.

The main result of this analysis is that, while there may be a positive volume of speculative trade, this has no impact on the prices or allocations of the model and there are no

economic profits to speculation. To be clear, speculators may expect a positive return to their investment, even unconditionally, but this is a fair return for the risk of platform failure and does not distort prices away from what was derived above.

We assume the entrepreneur commits not to change the supply of coins ex post. This is a credible assumption because, if the entrepreneur finds it beneficial to make this commitment, blockchain technology provides a mechanism for him to do so. This assumption was not relevant before, as the entrepreneur was the only seller, but with opportunistic speculators also selling at time 1 there may be an incentive to create additional coins without this assumption.

First, we show that the prices derived in the previous section are still an equilibrium, although the volume of trade may change. At those prices, speculators with signals above x_0^* buy, anticipating that if $S = 1$ they can resell at time one for a price of 1. This means there is twice as much volume as without resale. However, at time one, the total supply of coins on the market is the same; the only difference is that relatively less of that supply comes from the entrepreneur. At a price of 1, none of the sellers want to keep their coins, and all of the buyers are willing to buy, so this price is still an equilibrium.

A separate question is whether any other prices might constitute an equilibrium as well. More precisely, it might seem natural that a price war could break out among sellers at $t = 1$, driving the price of tokens below 1. The equilibrium described in the previous paragraph implicitly has sellers at time 1 colluding not to do this, but it might seem that any one of them has an incentive to do so if they could.

However, note that the aggregate supply of coins sold at time 1 does not change. Each seller gets a mass of demand equal to the mass of coins that he sells; even if a different seller tried to undercut the entrepreneur with a lower price, this would not decrease the residual demand facing the entrepreneur after that seller exhausted his supply. Thus, regardless of what other agents do, the entrepreneur (and every seller in the model) can still charge a

price of 1 to his buyers at the second date. That price therefore becomes the unique optimal price for every agent in the optimal.

Nevertheless, the presence of the speculators does force the entrepreneur to sell more coins at the first stage. Does this ultimately decrease his expected profit? Can he increase the price at time zero? Let F^s be the CDF of signals to the speculators. We simply change the entrepreneur's problem to

$$\max_{C_0} \quad C_0 \times \min\left(1, 1 - F\left(x_0^*\right) + 1 - F^s\left(x_0^*\right)\right) + p \times \max\left(0, F\left(x_0^*\right) - \left(1 - F^s(x_0^*)\right)\right) \tag{7}$$

First, consider the possibility that the speculators demand more the entire supply at time zero. This is inconsistent with equilibrium: In this case, the only market-clearing price at time 1 will be less than one, and all speculators know this and will not demand to buy any coins. Therefore, we can restrict attnetion to cases where the speculators' demand is small enough to not exceed one at time zero.

With that observation, we can focus on the first-order condition as characterizing the solution to the problem. This condition is

$$\frac{1 - F(x_0^*) + 1 - F^s(x_0^*)}{F'(x_0^*) + F^{s'}(x_0^*)} = (C_0 - p) \times \frac{dx_0^*}{dC_0} \tag{8}$$

which is a straightforward generalization of (6).

We can rewrite the LHS of (8) as a weighted average:

$$\frac{1 - F(x_0^*) + 1 - F^s(x_0^*)}{F'(x_0^*) + F^{s'}(x_0^*)} = \frac{F'(x_0^*)}{F'(x_0^*) + F^{s'}(x_0^*)} \times m(x_0^*) + \frac{F^{s'}(x_0^*)}{F'(x_0^*) + F^{s'}(x_0^*)} \times m^s(x_0^*)$$

If the speculators and investors draw signals from the same distribution, then this analysis shows that there is ultimately no effect on the entrepreneur's revenue compared to the no-resale case. The mass of speculators selling at time 1 is completely offset by their buying at

time zero, since the coins are fairly priced at both dates.

3.4 Adding a critical-mass constraint

In this section we combine the network effect and wisdom of the crowd and show how the ICO can address both at once. We again model the critical mass requirement in a simple way, by assuming that the per-capita surplus S is realized if and only if at least a measure α of users join the platform. Therefore an individual user's payoff as a function of his action is:

$$\begin{cases} 0, \text{ if he does not participate} \\ -C, \text{ if he participates but there are less than } \alpha \text{ total participants} \\ S - C, \text{ if he participates and there are more than } \alpha \text{ total participants} \end{cases}$$

The rest is as in the core model: We normalize $S \in \{0, 1\}$, depending on the state of nature. All agents share the common prior $\mathbb{P}(S = 1) = p$. Each user gets a noisy private signal X about the value of S, and this is the only difference among them. We assume that the signals X are distributed according to the conditional distribution functions $(X|S = 1) \sim F_H$ and $(X|S = 0) \sim F_L$. Conditional on the realization of S, the signals X are independent of each other. We continue to assume that $f'(X) > 0$ where $f(x) \equiv F'_H(x)/F'_L(x)$.

3.4.1 Entrepreneur's problem in a one-stage game

We first analyze the case in which there is no ICO. The entrepreneur makes the entry decision, and conditional on entering the market, sets the cost C to maximize profit. While a high value of C clearly increases that profit, two forces discourage the entrepreneur from setting the value of C too high. First, as before, a high value of C increases the minimum private signal X that a user must have to find it profitable to join the platform. Second, conditional on an individual users's private signal, the network effect further deters the user

from joining, as she anticipates a smaller set of other users joining. The entrepreneur thus needs to to choose C to extract as much surplus from the users, while internalizing the effect of C on the critical mass α requirement.

Formally, user i joins the platform if and only if

$$\mathbb{P}(\text{at least } \alpha \text{ users join and } S = 1 \,|\, X_i) \geq C. \tag{9}$$

By Bayes' rule, the probability in (9) is equal to

$$\mathbb{P}(\text{at least } \alpha \text{ users join } |\, S = 1,\, X_i) \times \mathbb{P}(S = 1 | X_i).$$

Due to no correlation in the signals conditional on the fundamental, the first term

$$\mathbb{P}(\text{at least } \alpha \text{ investors join } |\, S = 1,\, X_i) = \mathbb{P}(\text{at least } \alpha \text{ investors join } |\, S = 1). \tag{10}$$

The second term $\mathbb{P}(S = 1|X)$ can be expanded as

$$\frac{p \times f_H(X)}{p \times f_H(X) + (1-p) \times f_L(X)} = \frac{p \times f(X)}{p \times f(X) + (1-p)}.$$

Hence, (9) is equivalent to

$$\mathbb{P}(\text{at least } \alpha \text{ investors join } | S = 1) \times \frac{p \times f(X)}{p \times f(X) + (1-p)} \geq C \tag{11}$$

In equilibrium each investor follows a cutoff strategy of participating in the platform if and only if his signal is higher than some x^*, which is the same for all investors due to the symmetry of the setup. Depending on the realization of the underlying state $S \in \{H, L\}$, a measure of $1 - F_S(x^*)$ users (those with high enough signals) will participate. Given the structure of the economy and the entrepreneur's choice of C, users know with certainty

whether this mass is greater than α.

The entrepreneur thus has two possible regions of price setting strategies: First, set C so low that $1-F_H(x^*) \geq \alpha$; second, set C so high that $1-F_H(x^*) < \alpha$. The second case is clearly ruled out in equilibrium, because in this case no user expects the critical mass requirement to be satisfied in any state of nature, so none of them will participate and the entrepreneur's revenue would be zero. In the first case, $\mathbb{P}(\text{at least } \alpha \text{ investors join } | S = 1) = 1$, and so (11) reduces to

$$\frac{p \times f(X)}{p \times f(X) + (1-p)} \geq C \tag{12}$$

and for a given C chosen by the entrepreneur, x^* is defined by setting the above expression to equality:

$$\frac{p \times f(x^*)}{p \times f(x^*) + (1-p)} = C. \tag{13}$$

Hence, we obtain the entrepreneur's problem below:

The entrepreneur's problem The entrepreneur chooses C to maximize her payoff

$$pC \times (1 - F_H(x^*)) + (1-p)C \times (1 - F_L(x^*)), \tag{14}$$

subject to

$$\frac{pf(x^*)}{pf(x^*)+(1-p)} = C \qquad \text{(user IC)} \tag{15}$$

$$1 - F_H(x^*) = \alpha \qquad \text{(critical mass)} \tag{16}$$

Attaching multiplier λ to constraint (16), the first-order condition for this constrained problem is thus

$$m_F(x^*) = \left(C + \lambda \frac{F_L'(x^*)}{F'(x^*)} \right) \times \frac{dx^*}{dC} \tag{17}$$

Comparing condition (17) with condition (2) in Section 3, the difference is the new term inside parentheses. Because this term is always positive, we see that the platform is priced

lower than it was without the critical-mass feature. This is intuitive: The lower price is the mechanism by which the entrepreneur induces participation by the critical mass α.

3.4.2 Introducing ICO

Again ICO is interpreted as a pre-sale of tokens that give access to the platform once it is launched in the second stage. Without re-sale, the entrepreneur enjoys a profit of (before the fixed cost K)

$$pC_0 \times (1 - F_H(x_1^*)) + (1-p)C_0 \times (1 - F_L(x_1^*)) + pS \times [1 - (1 - F_H(x_1^*))], \tag{18}$$

where x_1^* denote the cutoff of signals above which the user will participate in the ICO. The first term represents revenues from the ICO, while the second term denotes revenues from the actual launch of the platform.

A user will participate in the ICO if and only if

$$\mathbb{P}(S = 1|X) \geq C_0,$$

(i.e. participating in ICO is not expected to result in a loss, and (for a continuum of users) is no worse than waiting). For the marginal user at the signal cutoff

$$\frac{p \times f(x_1^*)}{p \times f(x_1^*) + (1-p)} = C_0$$

Hence with the introduction of ICO, the entrepreneur's problem becomes the following

The entrepreneur's problem with ICO The entrepreneur sets C_0 to maximize

$$pC_0 \times (1 - F_H(x_1^*)) + (1-p)C_0 \times (1 - F_L(x_1^*)) + pS \times [1 - (1 - F_H(x_1^*))], \tag{19}$$

subject to

$$\frac{p \times f(x_1^*)}{p \times f(x_1^*) + (1-p)} = C_0 \text{ (user IC)} \tag{20}$$

We note that with ICO the entrepreneur's problems is exactly the same as the one without the critical mass requirement. Without ICO, however, the entrepreneur faces an additional critical mass constraint. Hence, an ICO adds additional value by eliminating this constraint whenever it is binding.

Comparing the entrepreneur's problem with and without the ICO illustrates two important implications of the ICO: First, with the ICO, the entrepreneur only needs to subsidize a smaller set of ICO participants: those with particularly high private signals about the social value of the platform. She can charge the full user surplus created by the platform to the remaining mass of users (the second term in (46)). ICO effectively serves as a screening device in front of investors with different level of asymmetric information, and helps reduce the "lemon" discount. Second, thanks to the coordinating effect of the ICO participants, the entrepreneur no longer needs to take into account the α critical mass, hence relaxing constraint (16) when optimizing.

ICO expands social surplus The discussion on how ICO harnesses the wisdom of the crowd illustrates the social value of an ICO. Simply put, when there is a fixed cost to socially-valuable entrepreneurship and the entrepreneur is allowed to obtain greater rents, then social surplus may be expanded. We make this logic explicit in Appendix C.1.

Manipulation and fraud We caution that unlike the network effect channel, the the wisdom of the crowd channel may be subject to abuse and manipulation. Appendix C.2 will give further discussion.

4 Implications for policymakers as well as practitioners

Our model generates a mechanism by which an initial coin offering can play a valuable economic role for an early stage project. Here, we discuss implications of our findings for the recent debate over optimal regulatory treatment of ICOs.

First, the current debate over ICOs has been focused on how existing securities laws should apply to regulating the new innovation. Our analysis instead inquires after the economic value creation of ICOs. We use social welfare as the criteria for assessing when ICOs should be restricted, and when they should be allowed. By distilling the multistage platform launch feature of many ICOs deals, our baseline model also provides a framework to help analyze other related regulatory issues in further development of the paper.

Second, we discuss the narrow question of whether coins sold in an ICO are securities like traditional debt or equity claims. In a strictly legal sense, this question is outside the scope of this paper, but in economic terms, our model suggests that for platform-based ventures the answer may be no. An ICO leads to cash inflows, likely at a time when the firm needs funds, yet that financing is not necessarily the purpose of the ICO. Rather, the structure can be an integrated part of the operational process of the platform, which leads to an efficient users participation outcome. Although the price of coins may increase endogenously over time, the ICO does not have to overcome any financial constraint that would prevent the issuance of a traditional equity security. 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."

The implications of this observation are twofold:

On the one hand, a token-issuing project should be very clear on how the newly minted tokens serve as an integrated element in the project. While qualified investors are free to speculate on the price path of an ICO, the fundamental purpose of an ICO is to induce

efficient participation, not necessarily to provide a return on capital. Companies that ignore or muddy this distinction should be viewed skeptically by both investors and regulators.

On the other hand, companies that justify a proposed ICO in terms of the benefits described in this paper should be given leeway to execute them. This may require carving out a special regulatory exemption if ICO tokens do indeed fall under the existing legal definition of a security; our model justifies why such an exemption could have economic value, and why the resulting ICOs represent a valuable innovation. Of course, such exemptions should not exempt oversight of other dimensions of project risks. For example, the requirement to disclose compensations for celebrity endorsement should be enforced to prevent manipulation. Governance measures should be erected to enforce any repurchase obligations offered by the entrepreneur.

In contrast, ICO structure that do not explicitly appeal to any challenge should be discouraged or scrutinized: In our model, the specific challenge is a coordination failure arising from the network effect. While there is no way to prove that network effect is the only mechanism justifying an ICO, we view it as likely the primary benefit from analyzing existing deals. 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 a proposed offering. An ICO that fails this test is at higher risk of being the kind of pump-and-dump scheme that damages the integrity of financial markets and motivates securities regulation in the first place.

We can also use our model to consider optimal governance provisions in an ICO. In principle, the contract underlying the purchase of a token should include investor protections analogous to those in other product markets or financial markets. This topic has received relatively little attention in the press, but it is a potentially rich area for legal research, and a few high profile examples illustrate the stakes and the challenges involved:

One important and unique governance challenge in an ICO is the possibility of devalua-

tion: After selling coins to ICO participants, a company has every incentive to expropriate the value of those coins. A prominent and extreme example was Storjcoin, which simply began accepting forms of payment other than tokens for its platform.[21] Our analysis then suggests that token sales should include contractual protection against this possibility. This conclusion is an important caution for potential token purchasers. It also provides another dimension along which regulators can judge proposed offerings, and along which high-quality offerings can separate themselves.

A more subtle way to accomplish this devaluation would be through dilution: If the company creates and sells more coins after the ICO, it effectively realizes seignorage revenue and expropriates some of the value of coins held by the ICO participants. This creates a difficult tradeoff, as new coin issuance may also be necessary to expand the network, which benefits existing participants via the network effect. ICO tokens should then include governance mechanisms controlling the expansion of the coin base via seasoned coin offerings, to allow for valuable network expansion while preventing opportunistic dilution.[22]

Interestingly, blockchain technology provides a mechanism to address this issue via "smart contracts." The technology allows the ICO seller to credibly pre-commit to an algorithm by which future coins will (or will not) be added to the current stock. This is interesting because it provides a clear justification for implementing ICOs as crowdfunding on a blockchain, rather than simply being a form of store credit. Nevertheless, even after making use of this technology, it is likely that the ICO seller cannot fully specify the contract governing optimal coin issuance. Or the issuer may simply deploy a new smart contract as minting different but related tokens. In this case, regulators and investors should be aware of how residual control rights regarding the expansion of the coin base are allocated in the contract underlying the

[21] See https://safenetforum.org/t/storj-screws-their-ico-token-holders-big-time-by-accepting-direct-fiat-payments/12859.

[22] Note that the dilution problem for coins is worse than for equity, where the funds flowing into the firm's balance sheet compensate old investors and offset the dilution effect.

token sale.

A second set of governance problems arise from the moral hazard inherent in providing funds for any purpose to an early-stage company. Since risk is always inherent in pre-purchasing a product that does not yet exist, many commentators have highlighted the importance of "capped" ICOs to provide proper incentives for sellers to develop their products post-sale. An ICO cap is a limit on the volume of tokens that can be sold in the ICO, which is simply a requirement that the seller retain a minimum stake in the company post-ICO. This incentive mechanism works exactly like the retention of an equity stake in a public offering, and the straightforward implication is that sellers in an ICO should retain a stake in the tokens they sell, to align their incentives with coin purchasers in addition to equity owners of the firm. Again, investors regulators both can make use of this implication in their decisions about proposed ICOs.

Finally, our analysis illustrates one fundamental challenge for which there is no easy answer: A growing concern in the ICO community is that the increasing number of pre-sale rounds create opportunities for Ponzi-scheme ICOs, with each round paying off the previous round's investors by pumping up the coin price long enough for the previous investors to exit.[23] While this is a real concern, our analysis highlights that a dynamic sequencing of sale rounds is in fact essential to the mechanism by which the ICO overcomes the coordination problem inherent in a network setting. Thus, dynamic sales should not be prevented out of hand, but rather should be an area of close study for regulators and academics seeking to separate valuable from wasteful ICOs. In ongoing work we develop an analysis of the tradeoff balancing the benefit of network effects and information aggregation, against the costs of potential fraudulent manipulation.

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

5 Conclusion

In this paper, we develop a framework to discuss optimal regulation toward initial coin offerings. Instead of following the conventional wisdom by focusing on whether tokens should be regarded as utility, security, or other legal categorizations, we take a economic perspective, and ask if and when token sales are value-creating or value-destroying from a social welfare perspective. We highlight two specific settings in which an ICO can create value: First, when projects feature network effects – that is, the surplus realized by any user increases in the size of the total user base. Second, when projects feature the "wisdom of the crowd" – that is, private signals about project value that are dispersed among its potential users.

Both of these settings characterize recent tech startups, especially those that use ICOs. In either scenario, the ICO creates value by increasing the expected profit for the entrepreneur launching the project. Since these profits are necessary to overcome fixed costs, the ICO allows a greater range of socially-valuable projects to proceed.

Our findings have implications for securities regulators concerned with the growing popularity of initial coin offerings. Because financial innovations are often accompanied by fraud that exploits holes in existing legal frameworks, a natural reaction is to ban the innovation completely. Indeed, many proposed ICOs likely do not serve important economic functions. But some do, and an ideal regulatory response would be to separate the wheat from the chaff by allowing them to proceed. Our model provides guidance in allowing that to happen. In ongoing work, we explicitly analyze traditional governance mechanisms in the setting of our model to provide further insights in these directions.

References

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

Carlsson, Hans, and Eric Van Damme. 1993. "Global games and equilibrium selection." *Econometrica: Journal of the Econometric Society*, 989–1018. 7

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

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

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

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

Daley, Brendan, and Brett Green. 2012. "Waiting for News in the Market for Lemons." *Econometrica*, 80(4): 1433–1504. 7

Da, Zhi, and Xing Huang. 2015. "Harnessing the Wisdom of Crowds." *Available at SSRN 2731884*. 7

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

Dindo, Pietro, and Filippo Massari. 2017. "The Wisdom of the Crowd Revisited." *Cowles Foundation GE conference paper*. 7

Dybvig, Philip, and Chester Spatt. 1983. "Adoption Externalities as Public Goods." *Journal of Public Economics*, 20: 231–247. 6

Ellman, Matthew, and Sjaak Hurkens. 2015. "Optimal crowdfunding design." *Available at SSRN 2709617*. 6

Evans, David S, and Richard Schmalensee. 2010. "Failure to launch: Critical mass in platform businesses." *Review of Network Economics*, 9(4). 6

Farrell, Joseph, and Garth Saloner. 1985. "Standardization, Compatibility, and Innovation." *RAND Journal of Economics*, 16: 70–83. 6

Goldstein, Itay, and Ady Pauzner. 2005. "Demand–deposit contracts and the probability of bank runs." *the Journal of Finance*, 60(3): 1293–1327. 7

Govindan, Srihari, and Robert Wilson. 2009. "On forward induction." *Econometrica*, 77(1): 1–28. 16

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

Katz, Michael, and Carl Shapiro. 1985. "Adoption Externalities as Public Goods." *The American Economic Review*, 75: 424–440. 6

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

Kovbasyuk, Sergei. 2011. "Wisdom of the Crowd." *American Economic Association Annual Meeting*. 7

Kremer, Ilan, Yishay Mansour, and Motty Perry. 2014. "Implementing the Wisdom of the Crowd." *Journal of Political Economy*, 122(5): 988–1012. 7

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

Morris, Stephen, and Hyun Song Shin. 1998. "Unique equilibrium in a model of self-fulfilling currency attacks." *American Economic Review*, 587–597. 7

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton University Press. 19

Rochet, Jean-Charles, and Jean Tirole. 2006. "Two-sided markets: a progress report." *The RAND journal of economics*, 37(3): 645–667. 6

Shen, Lin, and Juanyuan Zou. 2017. "Intervention with Voluntary Participation in Global Games." *Working Paper*. 7

Spulber, Daniel F. 2010. "Solving the circular conundrum: communication and coordination in internet markets." *Nw. UL Rev.*, 104: 537. 6

Strausz, Roland. forthcoming. "A Theory of Crowdfunding-a mechanism design approach with demand uncertainty and moral hazard." *American Economic Review*. 6

Surowiecki, James. 2005. *The wisdom of crowds.* Anchor. 7

Weyl, E Glen. 2010. "A price theory of multi-sided platforms." *The American Economic Review*, 100(4): 1642–1672. 6

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

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]
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]
(**U.S.**) Wyoming lawmakers	01/25/2018	file a bill to grant exemptions to ICO Utility Tokens. [Link]

Jurisdiction & Regulator	Date	Regulatory Responses
(**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]

Links to global regulator statements.

B Discrete number of users with wisdom of the crowd

The assumption of a continuum of users in our main analysis illustrates our main ideas in an elegant and concise manner. It does, however, generate one unrealistic feature: the entrepreneur in our model extracts all the social surplus created by the platform, leaving zero to the users. In this section, we show that when we adopt the more realistic assumption of a discrete number of users, this problem no longer exists, while our main conclusions remain intact. All assumptions are exactly the same as in Section 3, except that instead of a unit continuum of users, there is a discrete number N of them.

B.1 The entrepreneur's problem without an ICO

Given a price C, each user i follows the same cutoff strategy as in Section 3. The entrepreneur's expected profit is different from that section, because we now integrate over a discrete instead of a continuous distribution: Let M represent the number of users who join the platform (i.e. those with signals higher than x^*). Then for $m \in \{0, 1, 2, ..., N\}$,

$$\mathbb{P}(M = m) = \binom{N}{m}(1 - F_S(x^*))^m F_S^{N-m}(x^*) \tag{21}$$

Hence, we obtain the entrepreneur's problem below:

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

$$p\sum_{m=0}^{N} Cm\binom{N}{m}(1-F_H(x^*))^m F_H^{N-m}(x^*)+(1-p)\sum_{m=0}^{N} Cm\binom{N}{m}(1-F_L(x^*))^m F_L^{N-m}(x^*), \tag{22}$$

subject to

$$\frac{pf(x^*)}{pf(x^*)+(1-p)} = C \text{ (user IC)} \tag{23}$$

B.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 $S \in \{H, L\}$, 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

$$\mathbb{P}(S = 1|X, m) \geq C_1, \tag{24}$$

where

$$\begin{aligned}
\mathbb{P}(S = 1|X, m) &= \frac{p\mathbb{P}(X, m|S = 1)}{p\mathbb{P}(X, m|S = 1) + (1 - p)\mathbb{P}(X, m|S = 0)} \\
&= \frac{p\mathbb{P}(X|S = 1)\mathbb{P}(m|X, S = 1)}{p\mathbb{P}(X|S = 1)\mathbb{P}(m|X, S = 1) + (1 - p)\mathbb{P}(X|S = 0)\mathbb{P}(m|X, S = 0)} \\
&= \frac{pf(X)\mathbb{P}(m|X, S = 1)}{pf(X)\mathbb{P}(m|X, S = 1) + (1 - p)\mathbb{P}(m|X, S = 0)}
\end{aligned} \tag{25}$$

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 (25)=

$$\begin{aligned}
&\frac{pf(X)\binom{N-1}{m}(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1}}{pf(X)\binom{N-1}{m}(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1} + (1 - p)\binom{N-1}{m}(1 - F_L(x_0^*))^m(1 - F_L(x_0^*))^{N-m-1}} \\
= &\frac{pf(X)(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1}}{pf(X)(1 - F_H(x_0^*))^m(1 - F_H(x_0^*))^{N-m-1} + (1 - p)(1 - F_L(x_0^*))^m(1 - F_L(x_0^*))^{N-m-1}}
\end{aligned} \tag{26}$$

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

$$\frac{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1 - F_H(x_0^*))^m F_H^{N-m-1}(x_0^*) + (1 - p)(1 - F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)} = C_1(m) \tag{27}$$

Notice that for any given x_0^* and m the entrepreneur always set $C_1(m)$ 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 $C_1(m)$ is not credible.

A user participates in the ICO if and only if

$$\mathbb{P}(S = 1|X) \geq C_0 \tag{28}$$

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

$$\mathbb{P}(S = 1|X) - C_0 \geq \mathbb{E}_m \left[\mathbb{P}(S = 1|X, m) - C_1(m)|X\right], \tag{29}$$

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

Since $\mathbb{E}_m\left[\mathbb{P}(S=1|X,m)-C_1(m)|X\right]=$

$$\mathbb{P}(S=1|X)-\sum_{m=0}^{N-1}\left[C_1(m)\binom{N-1}{m}\frac{pf(X)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^mF_L^{N-m-1}(x_0^*)}{pf(X)+(1-p)}\right]$$

the two conditions (28) and (29) are expanded to

$$\frac{pf(x_0^*)}{pf(x_0^*)+(1-p)}\geq C_0 \tag{30}$$

$$\sum_{m=0}^{N-1}\left[C_1(m)\cdot\binom{N-1}{m}\cdot\frac{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^mF_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right]\geq C_0 \tag{31}$$

Since $\forall m, x_1^*(m)\leq x_0^*$, by (27)

$$C_1(m)\leq\frac{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)}{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^mF_L^{N-m-1}(x_0^*)}, \tag{32}$$

hence the left hand side of (31)$\leq$

$$\begin{aligned}&\sum_{m=0}^{N-1}\left[\frac{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)}{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^mF_L^{N-m-1}(x_0^*)}\right.\\&\left.\cdot\binom{N-1}{m}\cdot\frac{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^mF_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right]\\=&\sum_{m=0}^{N-1}\left[\frac{pf(x_0^*)(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\cdot\binom{N-1}{m}\right]=\frac{pf(x_0^*)}{pf(x_0^*)+(1-p)}.\end{aligned} \tag{33}$$

Hence we do not need to consider (30) as it is absorbed by (31). In sum, with the introduction of ICO, the entrepreneur's problem becomes the following:

The entrepreneur's problem with ICO The entrepreneur sets C_0 and $C_1(m), m\in\{0,1,2,...,N-1\}$ to maximize his profit (before the fixed cost K)

$$\begin{aligned}&Np\sum_{m=0}^{N-1}C_1(m)\left(F_H(x_0^*)-F_H(x_1^*(m))\right)\binom{N-1}{m}(1-F_H(x_0^*))^mF_H^{N-m-1}(x_0^*)\\+\;&N(1-p)\sum_{m=0}^{N-1}C_1(m)\left(F_L(x_0^*)-F_L(x_1^*(m))\right)\binom{N-1}{m}(1-F_L(x_0^*))^mF_L^{N-m-1}(x_0^*),\\+\;&NC_0\times[p(1-F_H(x_0^*))+(1-p)(1-F_L(x_0^*))]\end{aligned} \tag{34}$$

subject to

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

$$\frac{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)} = C_1(m) \tag{35}$$

2. x_0^* is given by

$$\sum_{m=0}^{N-1}\left[C_1(m)\binom{N-1}{m}\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}\right] = C_0 \tag{36}$$

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

$$\begin{aligned}&\text{argmax}_{\{x_0^*,x_1^*(m)\}} N\sum_{m=0}^{N-1}\binom{N-1}{m}\frac{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)}{pf(x_1^*(m))(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}\cdot\\ &\Big\{p\left(F_H(x_0^*)-F_H(x_1^*(m))\right)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)\left(F_L(x_0^*)-F_L(x_1^*(m))\right)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)\\ &+\frac{pf(x_0^*)(1-F_H(x_0^*))^m F_H^{N-m-1}(x_0^*)+(1-p)(1-F_L(x_0^*))^m F_L^{N-m-1}(x_0^*)}{pf(x_0^*)+(1-p)}[p(1-F_H(x_0^*))+(1-p)(1-F_L(x_0^*))]\Big\}\end{aligned} \tag{37}$$

In comparison, the entrepreneur's payoff without ICO is

$$\begin{aligned}&\sum_{m=0}^{N}\frac{pf(x^*)}{pf(x^*)+(1-p)}m\binom{N}{m}\left[p(1-F_H(x^*))^m F_H^{N-m}(x^*)+(1-p)(1-F_L(x^*))^m F_L^{N-m}(x^*)\right]\\ =\;& N\frac{pf(x^*)}{pf(x^*)+(1-p)}\left[p(1-F_H(x^*))+(1-p)(1-F_L(x^*))\right],\end{aligned} \tag{38}$$

Comparing the entrepreneur's payoff with or without ICO, we get the following main result:

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

Proof. (37) is no smaller than when x_0^* is forcibly set to 1, which is equal to

$$\text{argmax}_{\{x_1^*(0)\}} N\frac{pf(x_1^*(0))}{pf(x_1^*(0))+(1-p)}\cdot\left[p\left(1-F_H(x_1^*(0))\right)+(1-p)\left(1-F_L(x_1^*(0))\right)\right] = (38)$$

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

C Additional discussions on wisdom of the crowd

C.1 ICO expands social surplus

The role of the ICO in our framework is to incentive participation in cases where this would create social surplus. In this section, we show formally that the ICO therefore expands social surplus. To our knowledge, this is the first formal demonstration of a valuable economic role for ICOs, in contrast to most commentary which has focused on their facilitation of fraud and skirting of securities regulations.

Note that, in all cases, expected social surplus is equal to the mass of users who join the platform in the good state, times the probability p of that state occurring. Consider first the model without the critical-mass constraint. Without an ICO, the mass of users who participate in the positive state is $1 - F_H(x^*)$. With the ICO, that mass is 1, as all users end up joining sooner or later. The same intuition holds with the critical-mass constraint: Without the ICO, some agents will fail to participate in the positive state, whereas with the ICO they all will at one of the two dates.

In any of these cases of our model, users receive none of the surplus created by the platform. This is because we assume that the platform provider can act as a monopolist and appropriate all surplus. However, this assumption could be relaxed. The important observation is that the increased profit to the monopolist arises due to the creation of surplus. In this sense, ICOs in our model serve a socially-valuable purpose.

We could also formalize the intuitions with several theorems. First, without ICO certain positive NPV projects may be forgone.

Theorem C.1. *There exist values of p, α, and K for which projects are positive NPV yet not funded in equilibrium.*

Proof. First define $\overline{K} \equiv pS$. Clearly a project has positive NPV if and only if $K < \overline{K}$.

Next define $\underline{K}$ as the entrepreneur's revenue from optimally pricing the platform. Hence

$$\underline{K} \equiv \max_X \frac{pf(X)}{pf(X) + (1-p)}[1 - F_H(X)]$$

if $1 - F_H(X) \geq \alpha$ at the optimal X, or otherwise $\underline{K} \equiv \alpha\tilde{C}$, where $\tilde{C}$ satisfies

$$\tilde{C} = \frac{pf(\tilde{X})}{pf(\tilde{X}) + (1-p)}, \tag{39}$$

in which

$$1 - F_H(\tilde{X}) = \alpha. \tag{40}$$

It is easy to see that if and only if $K > \underline{K}$, the entrepreneur would suffer an expected loss if she incurred K to launch the platform. In equilibrium such projects will be unfunded.

Hence inefficient coordination could happen for p and α if as defined $\underline{K} < \overline{K}$, which is (after some simplifying algebra) if

$$(\alpha - p)f(\tilde{X}) < 1 - p, \tag{41}$$

where $\tilde{X}$ is defined as $1 - F_H(\tilde{X}) = \alpha$. □

Theorem C.2 redoes the analysis for the ICO case.

Theorem C.2. *For some p and α there exists $\underline{\underline{K}}$ and $\overline{K}$ such that projects with $\underline{\underline{K}} < K \leq \overline{K}$ are positive NPV yet unfunded in equilibrium.*

Proof. Similar to the case without ICO, define $\overline{K} \equiv pS$. Clearly a project has positive NPV if and only if $K < \overline{K}$. Define $\underline{\underline{K}}$ as

$$\max_x \frac{p \times f(x)}{p \times f(x) + (1-p)} \times (1 - F_H(x)) + \times[1 - \times(1 - F_H(x))]. \tag{42}$$

If and only if $K > \underline{\underline{K}}$, the entrepreneur would suffer an expected loss if she incurred K to launch the platform. In equilibrium such projects will be unfunded. □

Theorem C.3. *For all α, p, f_H, and f, we have $\underline{\underline{K}} \geq \underline{K}$. Hence the parameter regions in which coordination failure happens is smaller when we introduce ICO.*

Proof.

$$\begin{aligned}
\underline{\underline{K}} &= \max_x \frac{p \times f(x)}{p \times f(x) + (1-p)} \times (1 - F_H(x)) + \times[1 - \times(1 - F_H(x))] \\
&\geq \frac{p \times f(\tilde{X})}{p \times f(\tilde{X}) + (1-p)} \times (1 - F_H(\tilde{X})) + [1 - \beta \times (1 - F_H(\tilde{X}))] \\
&\geq \frac{p \times f(\tilde{X})}{p \times f(\tilde{X}) + (1-p)} \times (1 - F_H(\tilde{X})) \\
&= \tilde{C} \times \alpha \\
&= \underline{K}
\end{aligned}$$

□

C.2 Manipulation and fraud

We caution that unlike the network effect channel, the the wisdom of the crowd channel may be subject to abuse and manipulation. Because follow-up users learn about the project type (H or L) from both the price charged and the number of participants in ICO, one fraud the entrepreneur can commit is to offer private off-chain side payments to some individuals to induce higher ICO participation. The combination of higher ICO participation and the

public on-chain price may create a false impression upon follow-up users that the project is high quality. As long as the increase in proceeds the entrepreneur collects is higher than the side payment required, there is room for manipulation. We derive the parameter ranges in which such fraud can happen below.

The model framework is similar as before. A risk-neutral fraudulent entrepreneur incurs a fixed cost K to launch a platform, after which the entrepreneur charges a monopolistic per-capita cost C to a unit continuum of users for access to the platform. An individual user's payoff is:

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

where $S \in \{0, 1\}$ with common prior $\mathbb{P}(S = 1) = p$. users are identical except for their private signals X, where $X|S = 1 \sim F_H$ and $X|S = 0 \sim F_L$, and conditionally independent across individuals. The signals satisfy MLRP: $f(x) \equiv F'_H(x)/F'_L(x) \Rightarrow f'(x) > 0$. The additional assumption we make in the fraud case is that the entrepreneur has perfect private knowledge that the underlying state is low (i.e. $S = 0$), but this ugly truth is not known to the users.

No ICO When the platform launches in one period without ICO, the entrepreneur's problem is mimic the innocent users and choose C to maximize her payoff

$$C \times [p(1 - F_H(x^*)) + (1 - p)(1 - F_L(x^*))], \tag{43}$$

subject to

$$\mathbb{P}(S = 1|x^*) = \frac{pf(x^*)}{pf(x^*) + (1 - p)} = C \text{ (user IC)} \tag{44}$$

Denote C^* as the solution to the maximization problem, then the entrepreneur's payoff is

$$C^* \times (1 - F_L(x^*)), \tag{45}$$

Introducing ICO With ICO, the fraudulent entrepreneur could mislead the public by mimicking the innocent ones who sets C_0 and C_1 to maximize

$$C_0 \times [p(1 - F_H(x_0^*)) + (1 - p)(1 - F_L(x_0^*))] + pC_1 \times [1 - (1 - F_H(x_0^*))], \tag{46}$$

subject to

$$\frac{p \times f(x_0^*)}{p \times f(x_0^*) + (1 - p)} = C_0 \text{ (user IC)} \tag{47}$$

$$C_1 = 1 \tag{48}$$

To create the illusion that the project is of high type, the entrepreneur could offer side payments of at least C_0 to $F_L(x_0^*) - F_H(x_0^*)$ users (e.g. high influence early movers or

celebrities) and lure them to join in the first stage. In this case, the entrepreneur's payoff would be

$$C_0 \times (1 - F_L(x_0^*)) + C_1 \times [1 - (1 - F_H(x_0^*))], \tag{49}$$

Note that if the entrepreneur does not bribe early movers his payoff would be

$$C_0 \times (1 - F_L(x_0^*)), \tag{50}$$

which is strictly lower. Hence the fraudulent entrepreneur always has strict incentives to conduct compensated endorsement. If such compensation is not observed by follow-up users, these followers will be misled into a scam. This observation highlights the importance of disclosure requirement for ICO.

Note that the fraud problem is most severe when the user demography is not decentralized, because the manipulation can target only a small set of individual and prevents leakage (for example, celebrity endorsement).