Initial Coin Offerings, Speculation and Asset Tokenization

Article *in* Management Science · June 2020

Gerry Tsoukalas
University of Pennsylvania

Serguei Netessine
University of Pennsylvania

Initial Coin Offerings, Speculation and Asset Tokenization*

Jingxing (Rowena) Gan, Gerry Tsoukalas, Serguei Netessine†

June 29, 2020

Abstract

Initial Coin Offerings (ICOs) are an emerging form of fundraising for Blockchain-based startups. We examine how ICOs can be leveraged in the context of asset tokenization, whereby firms issue tokens backed by future assets (i.e., inventory) to finance growth. We (i) make suggestions on how to design such "asset-backed" ICOs—including optimal token floating and pricing for both utility and equity tokens (aka, Security Token Offerings, STOs)—taking into account moral hazard (cash diversion), product characteristics and customer demand uncertainty, (ii) make predictions on ICO success/failure, and (iii) discuss implications on firm operating strategy. We show that in unregulated environments, ICOs can lead to significant agency costs, underproduction, and loss of firm value. These inefficiencies, however, fade as product margins and demand characteristics (mean/variance) improve, and are less severe under equity (rather than utility) token issuance. Importantly, the advantage of equity tokens stems from their inherent ability to better align incentives, and thus continues to hold even absent regulation.

Keywords: Asset Tokenization, Blockchain, Crowdfunding, Cryptocurrency, Initial Coin Offerings, ICOs, Moral Hazard, Security Token Offerings, STOs, Speculators, Tokenized Inventory.

1 Introduction

Initial Coin Offerings (ICOs) are an emerging form of fundraising for blockchain-based startups in which digital coins, also known as "tokens", are issued to investors in exchange for funds to help finance business. The tokens can have a variety of uses, but most commonly, they are either used for consumption of the company's goods and services once they become available (utility tokens), or offered as shares of the company's future profit (equity tokens). The latter type of issuance is more often referred to as a Security Token Offering (STO) in practice, though to ease exposition, we will maintain the single "ICO" acronym for the rest of the paper (and clarify when needed). This new way of crowdfunding[1] startup projects has gained momentum since 2017 with the total amount raised skyrocketing to thirty billion dollars by the end of 2019 (source: icobench.com). The growth of token offerings is also challenging the dominance of traditional means of raising

*This project is funded by the Ripple Research Fund at the Wharton School and the Mack Institute Research Fellowship.

†OID Department, The Wharton School, University of Pennsylvania, Philadelphia, PA 19104. Gan: ganj@wharton.upenn.edu, Tsoukalas: gtsouk@wharton.upenn.edu, Netessine: netessin@wharton.upenn.edu.

[1]We discuss differences between token offerings and other early-stage financing methods in §5.

capital. During Q2 2018, ICO projects raised a total volume of $7.5 billion (Forbes 2018), which is 45% of the amount raised by the US IPO market ($16.0 billion) or 31% of the amount raised by the US venture capital markets ($23 billion) during the same period, as reported by CB Insights (CB Insights 2018) and PwC (Thomson 2018).

Research Questions Following this trend, the academic literature on token offerings is also rapidly growing, particularly in finance and economics, where the focus has been on topics such as empirically characterizing the drivers of ICO success or on comparing this new form of financing to more traditional financing methods. There is also a growing literature in operations management studying the interplay between firm operations and financing decisions (see literature review for details). This paper focuses on a question that is potentially relevant to both of these literatures: Is asset tokenization a viable means to finance startups? More specifically, we focus on token offerings for product market firms facing customer demand uncertainty, in unregulated environments, and ask: How should future working assets (such as inventory) be tokenized as a function of product, firm and customer demand characteristics? That is, what type of tokens—utility vs. equity—and how many should be issued? How should they be priced? Further, how do these choices affect firm operating strategy, and the odds of ICO failure or success? Finally, what are some of the salient features distinguishing ICOs from other forms of financing?

Properties of Token Offerings A typical token offering proceeds as follows. A startup first publishes a white paper with or without a minimum viable product for demonstration and then issues its platform-specific tokens. The typical white paper usually delivers the key information of the project, including the token sale model that specifies the token price, the sale period, the sales cap (if any), etc.[2] During the crowdsale, investors purchase tokens using either fiat currencies, or, more commonly, digital currencies such as Bitcoin and Ether.

While some successful token offerings were conducted by service platforms such as Ethereum and NEO, in this paper we focus on startups that involve the delivery of physical products instead; these types of token offerings are more recent, and hence, less well-understood. One example is that of Sirin Labs (Sirin Labs 2019): a startup that produces smartphones and other types of hardware and software systems. In 2017, Sirin Labs was able to raise over $150 million from investors through their ICO, by offering them Sirin tokens (SRN). These tokens could subsequently be used to purchase the company's products and participate in its ecosystem, or be sold in the secondary market. Other relevant examples include Honeypod (Honeypod 2018) that develops hardware serving as the main hub interconnecting various devices and providing traffic filtering,

[2]We provide a condensed example of a white paper in Appendix A.2.

and Bananacoin (Bananacoin 2018) which grows bananas in Laos.

Token offerings can have multiple benefits. First, both the startup founders and investors have the opportunity of high financial gains from the potential appreciation of the tokens. Second, ICOs allow for faster and easier execution of business ideas because the ICO tokens generally have secondary-market liquidity, and require less paperwork and bureaucratic processes, than the regulated capital-raising processes do. Third, ICOs provide the project team with access to a larger investor base as the stakeholders typically face less geographical restrictions.

On the other hand, just like the underlying blockchain technology, ICOs are still in their infancy and have some downsides. First, for the project teams, the failure rate of ICOs is high and increasing. Despite a rise in the total investment volume, nearly half of all ICOs in 2017 and 2018 failed to raise any money at all (Seth 2018) and 76% of ICOs ending before September 2018 did not get past their soft cap (Pozzi 2018), i.e., the minimum amount of funds that a project aims to raise. Benedetti and Kostovetsky (2018) claim that only 44.2% of the projects remain active on social media into the fifth month after the ICO. Second, the aspect of quick and easy access to funding with loose regulation attracts unvetted projects and even utter scams, making ICO investments risky. Some entrepreneurs portray deceiving platform prospects in the white papers in an attempt to raise as much money as they can before gradually abandoning their projects. In a review of 1450 ICO cases by the Wall Street Journal, 271 were susceptible to plagiarism or fraud. The profit-seeking yet ill-informed investors can become easy prey and have claimed losses of up to $273 million (Shifflett and Jones 2018). Other disadvantages of ICOs include technical concerns such as the potential theft of tokens through hacks (Memoria 2018).

Model To study some of these issues in the context of asset tokenization, we adopt a game-theoretic approach with three types of players: a firm (token issuer), speculators (token traders) and customers (who buy the product). As in the Sirin Labs example mentioned earlier, the firm seeks to raise funds through an ICO to support the launch of a physical product it wishes to sell in the face of customer demand uncertainty. We first consider a utility-based ICO, whereby the tokens issued by the firm are tied to its (future) inventory. The ICO game develops over three periods. In the first period, the firm announces the total number of tokens available, the sales cap and the ICO token price, and sells tokens (up to the cap) to speculators who make purchase decisions strategically[3]. In the second period, the firm, facing uncertain customer demand, can put the funds raised in the ICO towards production of a single product. Importantly, to reflect the lack

[3] The literature on operational decisions in the presence of strategic agents includes Dana Jr and Petruzzi (2001), Cachon and Swinney (2009), Papanastasiou and Savva (2016), etc. Su (2010) and Milner and Kouvelis (2007) consider similar speculative behavior yet with no financing aspect.

of intermediaries and the lax regulatory environment, we leave the firm with full discretion over what to do with the raised funds, including the option of fully shirking production and diverting raised funds to its pockets (moral hazard). In the final period, demand for the product is realized and customers buy tokens either directly from the firm (if the firm has any tokens remaining) or from speculators in the secondary market, and redeem these tokens for the product, if available, at an endogenously determined equilibrium token price. Finally, we compare this utility-based ICO model to an analogous equity-based ICO model (aka STO), whereby the firm issues tokens that are tied to its future profits (if any), rather than to its future inventory.

Our base model assumes that the main source of risk is future customer demand uncertainty, rather than technological viability. This setting is motivated by several practical examples, including the aforementioned case of Sirin Labs: prior to the ICO, the company had secured Foxconn, a major smartphone manufacturer (which also assembles the vast majority of Apple iPhones), as its main supplier. As such, the risk of failure was arguably quite low. Indeed, the company went on to successfully produce their products and made them available to consumers. However, despite successful production and a very impressive ICO outcome in terms of total funds raised, the company's token market price dropped significantly in the months and years post ICO, because, among other things, customer demand for their product fell well short of expectations. In other words, demand uncertainty can have a first-order effect on the token's market value. Nonetheless, for completeness, we also extend the base model to consider technology risk, and show it leads to additional insights.

Contributions Using this relatively simple and flexible model, we derive the optimal ICO price, token cap and production strategy as a function of operational and demand characteristics, for both utility-based and equity-based coin offerings. We find that, despite rampant moral hazard, both types of ICOs can be successful under the right conditions.

Focusing first on utility ICOs, we show that these are analogous to a form of *revenue-sharing* contract between the firm and speculators, and we identify four key factors that are required for the success of an ICO: i) the existence of a liquid secondary market for the tokens, which provides an "exit ramp" for speculators, incentivizing them to participate in the ICO even when they might otherwise not be interested in consuming the firm's products; ii) a minimum price-cost ratio of 2 (i.e., a 50% margin, or 100% markup) to provide enough incentive for the company to pursue production; iii) a minimum amount of tokens to be sold during the ICO, termed the "critical mass" condition, which ensures speculators break even in expectation; and iv) a maximum amount of tokens to be sold during the ICO, which defines a "misconduct threshold". Interestingly, when excessive funds beyond this threshold are raised (e.g., from over-optimistic investors) the firm is actually discouraged from pursuing production ex-post given it does not have enough "skin" left in the game. This provides a possible explanation for the loss of motivation or productivity post ICO of some well-funded startups in practice. While conditions i)-iv) suffice to prevent total market breakdown, they do not fully eliminate the adverse effects of moral hazard. Rather, in equilibrium, these lead to agency costs, underproduction and lower-than-optimal profits versus first best. Importantly, we show how these inefficiencies fade as expected demand and product margins increase, and/or as demand volatility decreases.

We then turn attention to ICOs with equity tokens (STOs)[4]. Although STOs have a relatively smaller market compared to ICOs, they gained much popularity in 2018, with total volume being almost seven times that of 2017 (from \$65.59 million in 2017 to \$434.95 million in 2018) (Blockstate 2020). Unlike utility tokens that can be exchanged for the firm's products, equity tokens simply represent a share of an underlying asset, which in our model takes the form of a *profit-sharing* contract. Therefore, equity tokens are closely related to traditional equity stakes, though without voting rights. We show that, even though moral hazard and the inefficiencies it generates cannot be fully eliminated in this setting, these inefficiencies are less prominent compared to utility token offerings, as long as profit-sharing can be credibly implemented, e.g., using auto-executable smart contracts. Assuming the latter holds, equity-type ICOs also have the advantage of not requiring a liquid secondary market for the tokens, as speculators can instead rely on smart contracts to receive their share of future cash flow and effectively "exit" the deal. Importantly, the advantage of equity tokens stems from their inherent ability to better align incentives, and hence continues to hold even in unregulated environments.[5]

Finally, we extend the model in two separate dimensions: i) We add the possibility of production failure to capture situations in which the firm's technology is risky and manufacturing success is not guaranteed. We find that this additional source of risk incentivizes the firm to keep a fraction of the ICO proceeds in a reserve fund to provide coverage in case production fails. This, in turn, can significantly exacerbate the moral hazard problem, reducing the chance of ICO success. ii) We then make speculators utility more realistic by assuming speculators require a minimum amount of expected return to invest in the ICO (the base model assumes their outside option is zero). We show that, consistent with practice, this assumption creates a wedge between the ICO's token price and the secondary market price, ex-post production.

[4]Throughout the paper, we use "STOs" and "ICOs with equity tokens" interchangeably.

[5]In our model, assuming regulation can effectively alleviate moral hazard, both ICOs and STOs reduce to the first best financing case without frictions.

ICOs vs Crowdfunding Our model distinguishes ICOs from other early-stage financing methods by capturing several of their unique features, including the fundraising mechanism and the issuance of tokens, the existence of a peer-to-peer secondary market, and the nature of investors. In contrast to reward-based crowdfunding,[6] for instance, there is no intermediary platform imposing a fundraising mechanism (e.g., Kickstarter uses and all-or-nothing mechanism). Rather, firms running ICOs have to determine how many tokens to issue/sell during the initial round in addition to how many products to make. Another important difference that we highlight is that tokens allow the firm to disperse downside risks of future demand among the token holders, whereas in reward-based crowdfunding, campaign backers typically share downside risk only in terms of product failure (not in terms of future demand uncertainty). Finally, we show that the existence of the secondary market for the tokens is crucial in incentivizing investors to participate in utility-type ICOs, an important feature missing from crowdfunding. We refer the readers to §5 for a more detailed discussion and Table 1 for a summary comparison to other financing methods.

Literature Review The literature on ICOs is new but rapidly growing. On the theory side, several papers study ICOs in a business-to-customer setting, like we do. Catalini and Gans (2018) propose analysis of an ICO mechanism whereby the token value is derived from buyer competition. Malinova and Park (2018) suggest a variation on the traditional ICO mechanism that can mitigate certain forms of entrepreneurial moral hazard. Chod and Lyandres (2018) compare ICOs to VC financing. Relatedly, several papers focus on ICOs for peer-to-peer type platforms where network effects can be central. For example, Li and Mann (2018) and Bakos and Halaburda (2018) demonstrate that ICOs can serve as a coordination device among platform users. In a dynamic setting, Cong et al. (2018) consider token pricing and user adoption with inter-temporal feedback effects. Gryglewicz et al. (2019) study both ICOs and STOs in the absence of cash diversion. To the best of our knowledge, ours is the first paper to consider more specifically the question of asset tokenization. In particular, we study how firms should jointly optimize ICO design and firm operating decisions, including sales cap, token pricing and production quantity, in the presence of strategic investors under customer demand uncertainty, and we compare utility and equity (STO) token issuance in this context.

On the empirical side, Fahlenbrach and Frattaroli (2019) study the nature of ICO investors and show that many of them sell their tokens on the secondary market—a stylized fact that we rely on in our model of speculation. Relatedly, several other papers study determinants of ICO

[6] Refer to Section 5 for a discussion on the differences. For recent papers on crowdfunding, see Alaei et al. (2016), Babich et al. (2019), Belavina et al. (2019), Chakraborty and Swinney (2017), Chakraborty and Swinney (2018), Fatehi et al. (2017), Xu and Zhang (2018), Xu et al. (2018).

success and for instance, find a positive relationship with the amount of information disclosed to investors (de Jong et al. 2018, Howell et al. 2018), and with access to additional service (Adhami et al. 2018). Other studies examine differences and similarities between ICOs and IPOs, such as Benedetti and Kostovetsky (2018) and Lyandres et al. (2019), and we contribute to this debate through our comparison between utility and equity tokens.

More broadly, this paper contributes to the strand of literature at the interface of operations and finance that studies, among other things, different ways of financing inventory. Earlier works include Babich and Sobel (2004), Buzacott and Zhang (2004), Boyabatlı and Toktay (2011), Kouvelis and Zhao (2012), and Yang and Birge (2013), see Kouvelis et al. (2011) for a review of this literature. More recent papers include Boyabatlı et al. (2015), Yang et al. (2016), Iancu et al. (2016), Alan and Gaur (2018), Chod et al. (2019a).

Finally, the paper also contributes to a growing theoretical literature studying the economics of blockchain-based systems, see e.g., Biais et al. (2017), Chod et al. (2019b), Cong et al. (2018), Hinzen et al. (2019), Pagnotta (2018), Pagnotta and Buraschi (2018), Rosu and Saleh (2019), Tsoukalas and Falk (2019), and references therein.

Here and below, we first develop in §2 and solve in §3 the case of utility tokens, before examining equity tokens in §4.

2 Model: ICOs with Utility Tokens

Consider an economy with three types of agents: i) a monopolist product market firm, ii) investors termed speculators, and iii) product customers. The economy has three periods: i) The first period, termed "ICO", is the fundraising phase containing the firm's white paper that includes contract terms and the (utility) token crowdsale; ii) the second period, termed "production", covers firm's production decisions in the face of uncertain customer demand; iii) the third period, termed "market", covers the realization of customer demand, and market clearing for the product and any remaining tokens. The firm participates in all three periods. Speculators participate in the ICO and the market periods. Customers participate only in the market period.

Firm The firm has no initial wealth and seeks to finance production through a "capped" ICO. The firm has a finite supply of m total tokens that are redeemable against its future output (if any). In the ICO period, the firm maximizes its profits by choosing i) the ICO "cap", $n \leq m$, that is, the maximum number of tokens to sell ("float") to speculators in the ICO period, and ii) the ICO token price τ (in dollars per token). Subsequently, in the production period, the firm has the option to use any amount of funds raised through the ICO to finance the production of its output. To this end, the firm maximizes its total wealth, through a newsvendor-type production function (Arrow et al. 1951), by choosing quantity $Q \geq 0$ of a product with unit cost c (in dollars per unit) that it can later sell in the market period at a price p (in tokens per unit), in the face of uncertain customer demand D. To capture the lack of regulation in the current environment, we assume that the firm could divert all or a portion of the funds raised through the ICO, rather than engage in production (moral hazard).

In the final market period, demand is realized and the product is launched. The product can only be purchased using the firm's tokens—a restriction that has two consequences: i) it endows tokens with (potential) value ii) it implies price p represents the exchange rate between tokens and units. The firm competes with speculators to sell any remaining tokens it has post-ICO to product customers, e.g., through a "secondary" offering round. As opposed to the ICO round, there is no uncertainty in the secondary offering round as production is finished and demand is already realized. The equilibrium token price τ_{eq} (in dollars per token) as well as the product price p (in tokens per unit) are then derived through a market clearing condition, described below. Once the market clears, tokens have no residual value (since there is only a single production round and the tokens have no use on any other platform) and the game ends. We provide more details of the tokens' features and discuss their implications for speculators and customers in Appendix A.1.

To recap, the firm's decisions are the number of tokens to make available in the ICO to speculators n, the ICO token price τ, and how production quantity Q.

Speculators Let z denote the total number of speculators with $z \gg m$ reflecting that ICOs have low barriers to entry. Speculators are risk-neutral, arrive simultaneously, and can each try to purchase a single token in the ICO at the price set by the firm, τ, that they expect to subsequently sell in the market period at an equilibrium price $\mathbb{E}[\tau_{eq}]$, where $\mathbb{E}$ is the expectation operator. If demand for tokens exceeds token supply in the ICO, speculators are randomly allocated token purchase rights. Speculators' expected profit u depends, among other things, on the expected price difference $\mathbb{E}[\tau_{eq}] - \tau$, denoted Δ, and on the total number of speculators that purchase tokens in the ICO, denoted s; formally:

$$u(s) = \frac{s}{z}\Delta(s), \quad \text{with} \quad \Delta(s) = \mathbb{E}[\tau_{eq}(s)] - \tau, \tag{1}$$

where the ratio s/z reflects random assignment of token purchase rights. We emphasize that the number of speculators s will be determined endogenously in equilibrium, and as we shall show later on, this number depends on the ICO cap n and the ICO token price τ. A necessary condition for $s(\tau, n) > 0$ speculators to participate in the ICO is

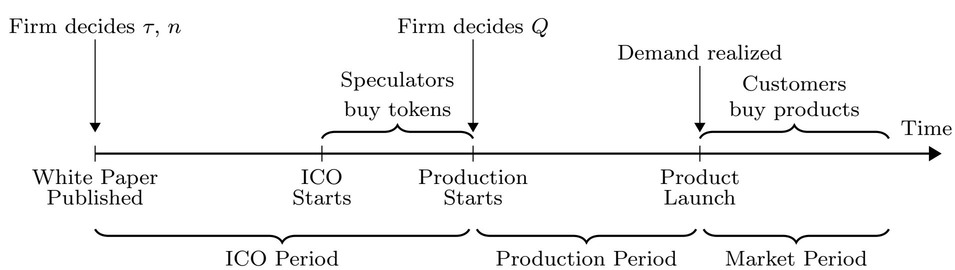
$$u(s(\tau, n)) \geq 0 \quad \text{(participation constraint).} \tag{2}$$

Note, as we show in Appendix B.2, assuming sequential rather that simultaneous arrival of speculators does not impact the results of the paper. The proofs are written to cover both cases. Also note that the model readily extends to the case in which speculators are given the additional option of using their tokens to purchase the firm's product rather than selling their tokens to product customers.

Product Customers Customers who join the market after the product launch have a homogeneous willingness-to-pay v (dollars per unit) for the product that is strictly greater than the production cost c. As we shall see later on, v plays a critical role in the market clearing condition. Customers can buy tokens directly from the firm (if it has any tokens remaining in the market period) or from speculators, and they can redeem the tokens for the products. The demand for the product D is stochastic and we denote the cumulative distribution function of demand by $F(\cdot)$. For ease of analysis, we assume that $F(\cdot)$ is continuous and $F^{-1}(0) = 0$.

We summarize the timeline in Figure 1 below.

Figure 1: Sequence of Events



Market Clearing Clearing occurs in the market period. Recall that the customers have a constant willingness-to-pay v (dollars per unit). This means that the dollar-denominated price of the product charged by the firm, which is equal to the product of the token-denominated price of the product p (tokens per unit) and the equilibrium market token price τ_{eq} (dollars per token), is at most v. Since the firm is a monopolist, it sets the dollar-denominated price to be exactly v, i.e., $p \cdot \tau_{eq} = v$. Therefore, p and τ_{eq} have an inverse relationship, and we have the following lemma due to the law of supply and demand.

Lemma 1. (Equilibrium Prices)

i) The equilibrium token-denominated price of the product is $p = m/\min\{Q, D\}$.

ii) The equilibrium token price in the market period is given by $\tau_{eq} = \frac{v}{m}\min\{Q, D\}$.

Part (i) of Lemma 1 implies that there are no idle tokens in the market period—the total token supply m can be redeemed for an amount $\min\{Q, D\}$ of products. Part (ii) implies the market clears. Specifically, customers' valuation for the total token supply equals their willingness-to-pay for all products that are purchased using these tokens, i.e., $\tau_{eq}\, m = v \min\{Q, D\}$. This equation addresses one of the most frequently asked questions regarding utility-based ICOs—what gives tokens their ultimate value? In our model, the value of platform-specific tokens depends positively on three factors: the quality of the product reflected by the customers' willingness-to-pay, the sales volume determined by the supply and demand for the products and the scarcity of tokens inversely determined by the total supply, m.

Firm's optimization problem The firm maximizes its expected dollar-denominated wealth at the end of the market period, denoted by Π, which consists of three terms: i) the total funds raised during the ICO, $\tau s(\tau, n)$, plus ii) the expected total funds raised in the secondary offering, $(m - s(\tau, n))\mathbb{E}[\tau_{eq}]$, minus iii) production costs $c\,Q$. The constraints are i) that production is funded by funds raised in the ICO, i.e., $c\,Q \leq \tau s(\tau, n)$, ii) that speculators participate in the ICO, i.e., $u(s(\tau, n)) \geq 0$, and iii) that the token value τ_{eq} is given by the market clearing condition in Lemma 1(ii). All together, the firm's optimization problem can be formally written as:

$$\max_{\tau,\, n} \left\{ \tau\, s(\tau, n) + \max_{Q} \left\{ (m - s(\tau, n))\, \mathbb{E}[\tau_{eq}(Q)] - c\, Q \right\} \right\} \tag{3}$$

subject to

$$\tau\, s(\tau, n) - c\, Q \geq 0, \qquad \text{(ICO funds cover production costs)}$$

$$u(s(\tau, n)) \geq 0, \qquad \text{(speculators' participation constraint)}$$

$$\tau_{eq}(Q) = \frac{v}{m}\,\mathbb{E}[\min\{Q, D\}]. \qquad \text{(market clearing)}$$

Recall that $s(\tau, n)$ is an equilibrium quantity, and we will show later how it depends on the firm's decisions variables, τ and n, and on Q (which itself depends on s, and hence τ and n).

3 Analysis: ICOs with Utility Tokens

In this section, we find the subgame perfect equilibrium using backward induction. We first consider (§3.1) the firm's last decision, the production quantity for fixed token price τ and ICO cap n, based on which we examine the speculators' equilibrium behavior (Section 3.2). We then calculate the optimal token price τ^* and ICO cap n^* (§3.3). Lastly, we present and discuss the equilibrium results in §3.4.

3.1 Optimal Production Quantity

We first consider the firm's last decision—the production quantity $Q(\tau, n, s(\tau, n))$, for fixed token price τ and ICO cap n. Here and below, we drop when possible the fixed arguments τ and n to ease exposition.

Proposition 1. (Optimal Production Quantity)
For a fixed token price τ, ICO cap n and number of speculators s, the firm's optimal production quantity $Q^*(s)$ is as follows.

i) If $0 < s < m\left(1 - \frac{c}{v}\right)$, then $Q^*(s) = \min\left\{F^{-1}\left(1 - \frac{m}{(m-s)}\frac{c}{v}\right), \frac{\tau s}{c}\right\}$.

ii) If $s = 0$ or $s \geq m\left(1 - \frac{c}{v}\right)$, then $Q^*(s) = 0$.

Part (i) of Proposition 1 shows that production can occur only if the number of speculators that purchased tokens in the ICO, is below a fraction $\left(1 - \frac{c}{v}\right)$ of all available tokens m. The first term inside the minimum operator, $F^{-1}\left(1 - \frac{cm}{(m-s)v}\right)$, is the unconstrained optimal production quantity; interestingly, this term decreases in the number of speculators s. The second term, $\frac{\tau s}{c}$, captures the firm's budget constraint, i.e., the production costs cannot exceed funds raised in the ICO, and this term is increasing in s.

Part (ii) of Proposition 1 shows that if more than a fraction $\left(1 - \frac{c}{v}\right)$ of all tokens have been sold in the ICO, the firm prefers not to use any of the funds raised for production, meaning, the firm "diverts" all money raised to its own pocket. We refer to this fraction (which also represents the product margin) as the firm's *misconduct fraction*,

$$1 - c/v. \tag{4}$$

Clearly, as the willingness-to-pay v increases relative to the production cost c, the misconduct fraction increases, making the abandonment of production less likely.

We clarify that this analysis does not suggest all crypto startups systematically divert funds. Rather, it provides an explanation for the loss of motivation or productivity of some well-funded startups based on pure profit maximization reasoning, due to moral hazard in the absence of regulatory controls.

3.2 Equilibrium Number of Speculators and Participation Constraint

Having derived the firm's optimal production quantity for a given ICO design τ, n, we next examine the implications on speculators.

Lemma 2. (Speculator Equilibrium Properties) *Given initial token price τ and the sales cap n,*

i) The number of speculators who purchase tokens is $s^*(\tau, n) = n \cdot \mathbb{1}_{\{u(n)\geq 0\}}$,

ii) $s^*(\tau, n) \in \left[0, m\left(1 - \frac{c}{v}\right)\right]$ such that complete fund diversion does not occur in equilibrium.

iii) Define $s_0(\tau) = \max\{0 < s \leq m : u(s) = 0\}$. If $s_0(\tau)$ exists, $s_0(\tau) < m\left(1 - \frac{c}{v}\right)$ and $u(s) < 0$ for all $s > s_0(\tau)$.

Lemma 2, part i) is a compact way to write that in equilibrium, the number of speculators purchasing tickets is equal to the ICO cap, as long as speculators' participation constraint is satisfied. This is because all speculators have the same expected profit, and hence, either n speculators will purchase tokens (if this expected profit is ≥ 0), or none will. Note, this result holds for sequential arrivals as well (see Appendix B.2).

Lemma 2, part ii) defines a lower and upper bound on the number of speculators that arises in equilibrium. The lower bound of zero is trivial. The upper bound is a consequence of the firm's misconduct threshold derived in Proposition 1, and captures the fact that in any equilibrium, speculators strategically prevent their funds from being completely diverted.

Lemma 2, part iii) is a necessary technical condition ensuring speculator participation constraint holds, and hence, the success of the ICO. In the Sections 3.3 and B.1, we show that the existence of $s_0(\tau)$ depends on τ, which in turn depends on n, and discuss the implications.

3.3 Optimal Token Price and ICO Cap

Given the optimal production quantity (§3.1) and speculators' equilibrium behavior (Section 3.2), we now examine how the firm sets the profit-maximizing ICO token cap n^* and initial token price τ^*.

We show in Lemma 2 in Section 3.2 that the number of speculators $s^*(\tau, n) \leq m\left(1 - \frac{c}{v}\right)$. Given the speculators participating in the ICO buy 1 token each, we need not consider the case in which tokens $n > m\left(1-\frac{c}{v}\right)$. We will first find the token price $\tau^*(n)$ for a given token cap $n \le m\left(1-\frac{c}{v}\right)$ and then maximize profit over the token cap n. The following Proposition guarantees the existence of a nonzero equilibrium token price τ^*.

Proposition 2. (Conditions for ICO Success)
The ICO succeeds if and only if

i) (critical mass condition) the firm sells more than $\frac{m\,c}{v}$ tokens in the ICO and,

ii) (price-cost ratio requirement) customers have a high willingness-to-pay such that $v > 2c$.

Part (i) of Proposition 2 shows that the firm should not set the ICO cap too low. Speculators expect non-negative returns only when more than a critical mass of tokens, $\frac{m\,c}{v}$, are sold in the ICO. This quantity increases in the production cost and decreases in customer willingness-to-pay. Recall from Section 3.2 that speculators would not invest more than the misconduct fraction. Combining these two results, we have that the ICO will only be successful when the misconduct fraction $m\left(1-\frac{c}{v}\right)$ is above the lower bound $\frac{m\,c}{v}$. This simplifies to the condition in Part (ii) of Proposition 2, $v > 2c$.

Next we find the optimal ICO token price $\tau^*(n)$ and the optimal ICO cap n^* assuming these two conditions are met. We show that for any fixed ICO cap n in the appropriate range ($n \in (\frac{m\,c}{v}, m\left(1-\frac{c}{v}\right))$), there exists a unique, positive and finite ICO token price $\tau^*(n)$ that maximizes (10) by extracting all utility from the speculators who participate strategically.

Given this result, we obtain a semi-closed-form solution of the optimal ICO cap n^*, and show that neither a small ICO cap that suppresses the production quantity nor a large cap that induces idle cash is profit-maximizing for the firm. The optimal ICO cap n^* allows the firm to raise just enough funds that can be credibly committed to production. We point interested readers to Appendix B.1 for detailed technical results.

3.4 The Equilibrium

Proposition 3. (Equilibrium Results)

i) If $v \le 2c$, then the ICO fails.

ii) If $v > 2c$, then there exists a unique equilibrium where

(a) the ICO cap n^* satisfies $n^* \in (\frac{m\,c}{v}, \frac{m}{2})$ and is uniquely determined by
$\frac{v\,n^*}{c\,m}\,\mathbb{E}[\min\{D, Q^*\}] = Q^*$,

(b) the ICO token price is $\tau^* = \frac{v}{m}\,\mathbb{E}[\min\{D, Q^*\}]$,

(c) the production quantity is $Q^* = F^{-1}\left(1 - \frac{m}{(m-n^*)}\frac{c}{v}\right)$,

(d) the number of speculators is $s^* = n^*$,

(e) the equilibrium token price is $\tau_{eq} = \frac{v}{m} \min\{Q^*, D\}$*, with* $\mathbb{E}[\tau_{eq}] = \tau^*$*,*

(f) the firm spends all funds raised through the ICO on production.

Several results are of interest here, starting with the failure condition in part (i) $v \leq 2c$, which says that the ICO does not raise any cash. Interestingly, this condition does not depend on customer demand characteristics. It simply defines the cutoff (in terms of margins) below which the firm would always prefer to fully divert funds, regardless of the distribution of future customer demand. Above that cutoff, however, how successful the ICO will be (e.g. how much money it will raise) depends critically on product and demand characteristics (e.g., expressions depend on c, v, F). The success condition in part (ii), $v > 2c$, implies that ICOs may be best suited for products with relatively high margins (above 50%).

Parts (ii)(a), (b) and (c) show the optimal ICO design and operating strategies. Part (a) links the ICO cap to operational and demand parameters, showing that these decisions become entangled under moral hazard, that is, ICO design parameters can no longer be set independently from the firm's operating strategy. Part (a) also suggests it is never optimal for the firm to sell more than half of its tokens ($m/2$) in the ICO. Note, this bound is unrelated to preserving majority control of the company. As the firm is not giving out equity with voting rights here, it always has full control, regardless of the number of utility tokens it gives out. Rather, this result is directly driven by moral hazard considerations. The more tokens the firm gives out in the ICO (ceteris paribus) the more money it may be able to raise initially. However, the fewer tokens it then has left to sell into the secondary market, i.e., the less "skin it has in the game", which reduces its incentive to invest the ICO proceeds into production after ICO funds are raised. The equilibrium n^* resolves this trade-off between cash "now" (in the ICO) versus cash "later" (in the secondary market).[7]

The remaining equilibrium quantities depend on this optimal ICO cap n^*. Since the total number of tokens available is kept constant, the ICO cap n^* is a proxy for the fraction of tokens sold during the ICO period. From parts (b) and (c), we can see that the more tokens the firm sells in the ICO, the lower the ICO token price and the firm's production quantity. The first effect is a direct consequence of speculators' participation constraint while the second effect reflects the aforementioned "skin-in-the-game" explanation.

While both the ICO cap n^* and the ICO token price τ^* combine to set the firm's total ICO

[7] If the firm were to sell more than $m/2$ tokens in the ICO, it would raise more cash than what could credibly be committed to production. The firm would then produce at the unconstrained optimal level and would be left with excess funds that it diverts to its pockets. However, these excess funds would be gained at the expense of a lower share of the future revenue (recall, the more tokens the firm sells to speculators in the ICO, the fewer tokens it leaves in the market period to sell to consumers). Overall, the firm would produce less and be less profitable. A detailed analysis is provided in Appendix C.

proceeds ($\tau^* n^*$), these two levers are not substitutes of each other; n^* determines, among other things, the optimal production level Q^*, the market equilibrium token price, and the firm's share of future revenue. Unlike n^*, τ^* uniquely determines speculators' utility and thus their participation constraint.

Part (d) shows that the ICO cap directly controls the number of speculators that will take part in the ICO.

Part (e) is a consequence of the market clearing mechanism (see Lemma 1) and the break-even condition for speculators. Note that the numerator of τ_{eq}, $v \min\{D, Q^*\}$, is simply the revenues generated after customer demand D is realized. Combining this with the fact that speculators' utility is a function of τ_{eq} brings to light the revenue sharing and demand risk sharing properties that utility tokens generate, discussed in the introduction. Importantly, traditional crowdfunding methods, such as reward-based crowdfunding do not typically enable this type of upside and downside sharing. We discuss the differences in more detail in Section 5.

Finally, part (f) says there is no cash diversion in equilibrium. Recall that we model an unregulated environment whereby the firm has the option to divert funds raised, but the conditions listed in Proposition 3 prevent such misconduct. Akin to the proverbial "carrot" and "stick" metaphor, when the product is profitable enough (captured by the high-margin requirement) and the firm has retained a substantial share of its tokens (captured by the misconduct fraction) that are to be monetized in the future, the firm is better off utilizing its resources on production to generate more cash "later". As such, despite the absence of regulation and intermediaries, utility ICOs can overcome moral hazard through a combination of the aforementioned factors. We refer readers to §5 for continued discussion.

3.5 ICO Agency Costs

A natural question that follows is just how well moral hazard is mitigated and what is the magnitude of agency costs in equilibrium. To answer this, we define the first-best benchmark as that of an ICO without any cash diversion. In this case, the separation theorem of Modigliani and Miller (1958) holds, implying that ICO design, and operating decisions can be optimized independently. It is relatively straightforward to show that the optimal production quantity reduces to that of Arrow et al. (1951) or more commonly referred to as the newsvendor quantity, which is simply given by

$$Q^{fb} = F^{-1}\left(1 - \frac{c}{v}\right).$$

In equilibrium, any firm in the range $v \in [c, \infty)$ would obtain financing and all funds raised in the ICO would be invested towards (some) production, meaning $\tau^{fb} n^{fb} = cQ^{fb}$, yielding an operating profit of Π^{fb}. We omit the corresponding expressions as they will not directly be useful for the comparison.

Proposition 4. (ICO vs First Best) *ICO financing under moral hazard leads to two types of underinvestment: First, profitable firms in the range $v \in [c, 2c]$ cannot get financed. Second, firms in the range $v \in [2c, \infty]$ that do get financed, suffer from underproduction ($Q^* \leq Q^{fb}$) and lower profits ($\Pi^* \leq \Pi^{fb}$) compared to first best.*

Proposition 4, shows that ICOs are a viable means of financing future assets, but this comes at a cost of lower production quantity, profit and flexibility in terms of margin. We evaluate the extent of these benefits and inefficiencies numerically in §3.6. Our numerical results show that in general, the production and profit gaps versus first best can be significant (50% or even more), but these gaps shrink when the market is bigger, more stable or (and) with a higher willingness-to-pay. Under the same market conditions, ICOs lead to lower profit variance, rendering firm profits less sensitive to demand uncertainty.

3.6 Numerical Experiments: ICOs with Utility Tokens

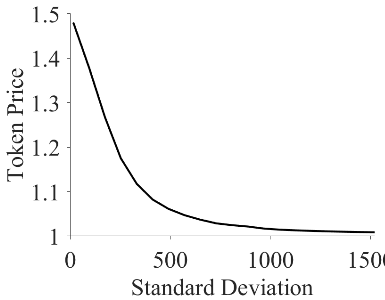
In this section, we provide a comparative-statics analysis through numerical experiment.[8] In particular, we focus on the impact of the mean and variance of demand and customers' willingness-to-pay.

Impact of mean demand

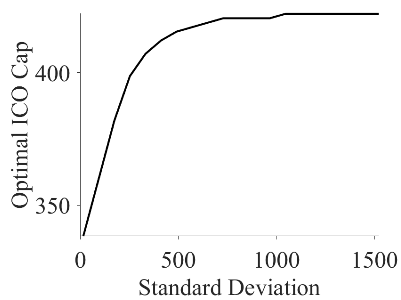
The impact of mean demand is relatively straightforward, and we omit the corresponding plots for brevity. In brief, our results demonstrate that, as mean demand increases, the firm increases the ICO token price while also selling fewer tokens to speculators, that is, it maintains a larger share of the tokens. Overall, the pricing effect dominates, that is, increasing mean demand allows the firm to raise more cash in the ICO, which, in turn, allows it to increase production and profit.

Impact of demand volatility

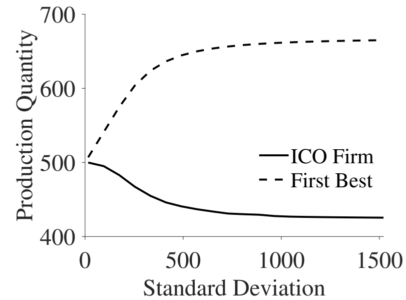
[8] In all of our numerical experiments throughout the paper, demand follows a truncated normal distribution distributed with mean μ, standard deviation σ, lower bound 1, upper bound 2μ. By default, the parameters are assigned values $\mu = 500$, $\sigma = 166$, $m = 1000$, $c = 1$ and $v = 3$. The price-cost ratio in our numerical experiments was calibrated to be close to the Honeypod example discussed in the introduction. Our numerical results are qualitatively robust to alternative distributions such as uniform distributions. For expositional clarity, we focus only on results under normal distributions in the paper.



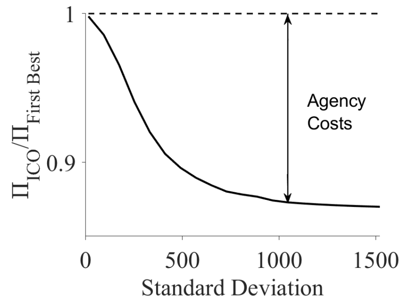
(a) Token Price vs Std



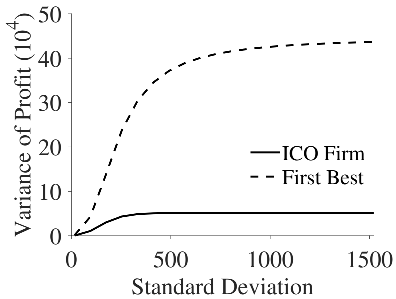
(b) ICO Cap vs Std



(c) Production Quantity vs Std



(d) Profit Ratio vs Std



(e) Variance of Profit vs Std

Figure 2: Impact of Standard Deviation (Std) of Demand

Figure 2 shows the impact of demand volatility (standard deviation) on token price (a), ICO cap (b), production quantity (c), profits (d), and profit variance (e).

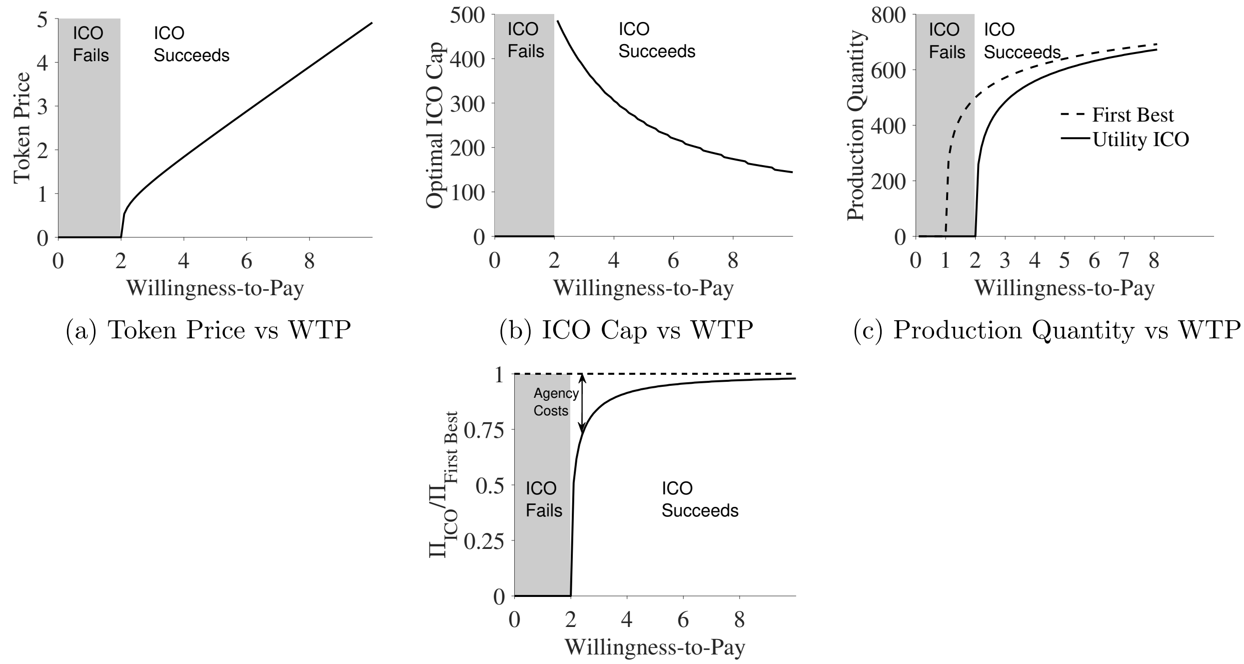
The key takeaways are that greater demand uncertainty leads to lower token prices (a) and requires the firm to give out more tokens in the ICO (b). It also hurts both the firm's ability to produce (c) and its profit (d). Moreover, Figure 2(d) also shows the profit gap between ICO financing and first best widens as demand volatility increases, suggesting that ICOs are better suited for products with a more predictable or stable customer base.

Interestingly, (f) shows that the variance of profits is actually lower for an ICO-financed firm under moral hazard, a consequence of the ensuing underproduction as seen in (c).

Impact of customer willingness-to-pay

Figure 3 shows the impact of customer willingness-to-pay (wtp) on token price (a), ICO cap (b), production quantity (c), and profits (d). In all cases, the ICO fails if wtp is below 2 (given $c = 1$), reflecting the $v < 2c$ condition from Proposition 3.

Similar to a higher mean demand, a higher wtp boosts the token price (a) and allows the firm to raise more funds in the ICO while saving a larger fraction of tokens for itself (b). Moreover, a higher wtp leads to higher production, while also shrinking the gap to first best (c). Lastly, higher



(a) Token Price vs WTP

(b) ICO Cap vs WTP

(c) Production Quantity vs WTP

(d) Profit Ratio vs WTP

Figure 3: Impact of Willingness-to-Pay ($c = 1$)

wtp leads to lower agency costs as seen in (d). For lower values of wtp (close to 2), agency costs can entirely wipe out firm value.

4 Analysis: ICOs with Equity Tokens (STOs)

In this section, we consider a different type of ICO—one with equity, rather than utility, tokens (also referred to as STOs as mentioned earlier). Although most tokens offered so far have been utility tokens (through ICOs), STOs have become much more popular since 2018 (Blockstate 2020). Unlike ICOs, STOs are typically regulated, and in our model, one could interpret strict regulations as a restriction on the firm's ability to divert any funds raised. In turn, this implies the funds will be put towards production, in which case, we can show that financing frictions are alleviated, and the outcome reduces to that of Proposition 4, where the regulated STO is simply equivalent to first best financing.

A more meaningful setting is one in which STOs do not automatically imply the firm commits funds raised to production. For instance, this could be the case if there is no way to perfectly monitor the use of all funds, or, if monitoring is prohibitively costly to implement. A natural question that follows is whether then there is any difference between a utility ICO and an STO in this case. This section is devoted to answering this question.

4.1 Model & Equilibrium

The fund-raising mechanism with equity tokens follows that with utility tokens (Figure 1) but with two main differences. First, the fundamental value of equity tokens is backed by the firm's future profit, rather than its future revenue. Second, the equity tokens have no utility purposes—in the market period, the firm sells its products for cash and distributes its profit among the equity token holders in proportion to their token holdings. As a result, the firm, unlike a utility-token-issuing firm, does not need to sell the remaining tokens (i.e., tokens unsold in the ICO period) in the market period.

By definition, in the market period, the realized value of each equity token is

$$\tau_{eq,e} = \frac{1}{m} \cdot (v \, \min\{D, Q_e\} \, - \, c\, Q_e)^+ \, . \tag{5}$$

The firm maximizes its expected dollar-denominated wealth at the end of the market period, denoted by Π_e, which consists of three terms: i) the total funds raised during the ICO, $\tau_e \, s(\tau_e, n_e)$, plus ii) the expected total profit, $v \, \mathbb{E}\,[\min\{D, Q\}] \, - \, c\, Q$, minus iii) total payout to other token holders, $s(\tau_e, n_e) \, \mathbb{E}\,[\tau_{eq,e}]$. The objective function is as follows.

$$\max_{\tau_e,\, n_e} \left\{ \tau_e \, s(\tau_e, n_e) + \max_{Q_e} \, \left\{ (v \, \mathbb{E}\,[\min\{D, Q_e\}] \, - \, c\, Q_e) - \frac{s(\tau_e, n_e)}{m} \, \mathbb{E}\,[v \, \min\{D, Q_e\} \, - \, c\, Q_e]^+ \right\} \right\} \tag{6}$$

subject to

$\tau_e \, s(\tau_e, n_e) - c\, Q_e \geq 0,$ (ICO funds cover production costs)

$u(s(\tau_e, n_e)) \geq 0.$ (speculators' participation constraint)

The subgame perfect equilibrium is derived using backward induction.

First, we consider the optimal production quantity Q_e^* given fixed token price τ_e and ICO cap n_e. Let $Q_u^*(s)$ denote the optimal production quantity unconstrained by the budget.

Proposition 5. (Optimal Production Quantity with Equity Tokens)
For a fixed token price τ_e, ICO cap n_e and number of speculators $s \in (0, m)$, the firm's optimal

production quantity is $Q_e^*(s) = \min\left\{Q_u^*(s), \frac{\tau_e s}{c}\right\}$, *where* $Q_u^*(s) > 0$ *is the unique solution of*

$$(m-s)[(1-F(Q_u^*(s))\, v - c] = s\, c\, F\left(\frac{c}{v}\, Q_u^*(s)\right). \tag{7}$$

We show in the proof of Proposition 5 that for any positive number of speculators in equilibrium, there continues to be underproduction compared to first best, similar to the result obtained for utility tokens.

At this point, we make a regularity assumption on the demand distribution:[9] $f(x) < a^2 \cdot f(ax)$ for $a > 2$. Using the result of Proposition 5, we show next that successful ICOs with equity tokens require a larger fraction of the tokens to be sold during the ICO than those with utility tokens.

Proposition 6. (Conditions for ICO Success with Equity Tokens)
An ICO that issues equity tokens succeeds if and only if

i) (critical mass condition) the firm sells more than $\frac{c}{v-c}\, m$ *tokens in the ICO and,*

ii) (price-cost ratio requirement) customers have a high willingness-to-pay such that $v > 2c$.

Recall from Proposition 2 part (i) that with utility tokens, the minimum number of tokens needed for production is $\frac{c}{v}\, m$. Given $\frac{c}{v-c}\, m > \frac{c}{v}\, m$, this implies a more stringent critical mass condition for equity tokens, which also translates into a higher ICO cap in equilibrium (we verify this numerically in §4.2). Following part (i) and Proposition 5 that the firm should not sell all of its equity tokens, we need $\frac{c}{v-c}\, m < m$ for the existence of feasible n, which leads to part (ii). Comparing with Proposition 2 part (ii), we see that the price-cost ratio requirement is the same for both types of tokens. Therefore, while intuitively the equity tokens put an emphasis on "profit" by definition, they do not require a higher or lower profit margin of the product than the revenue-sharing utility tokens.

Lastly, we show that when the two conditions given by Proposition 6 are met, the firm sets the ICO token price such that the speculators' expected profit is zero—a similar result to Proposition 3(ii)(e).

Proposition 7. (Optimal ICO Equity Token Price)
When $v > 2c$, *for a given* $n_e \in (\frac{c}{v-c}\, m,\, m)$, *there exists a finite positive* $\tau_e^*(n_e)$ *uniquely determined by* $u(s^*(\tau_e^*(n_e))) = 0$.

In summary, our analytical results identify two key differences and two similarities between ICOs and STOs in the absence of regulations: i) STOs are associated with lower agency costs; ii)

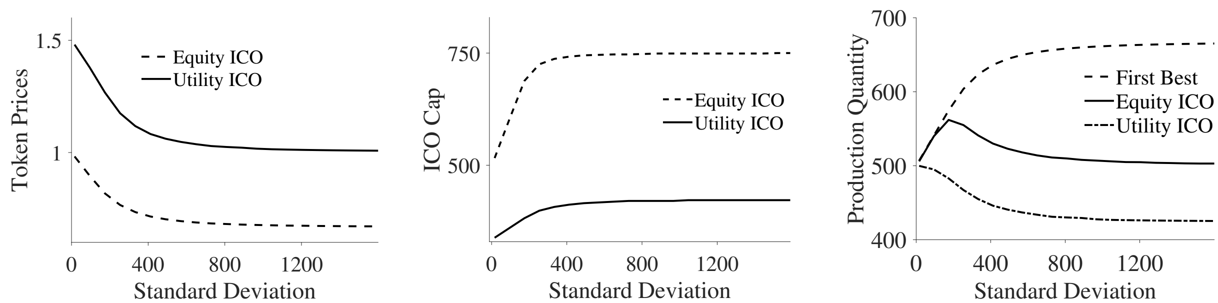
[9] This assumption is satisfied by distributions that do not contain sharp peaks such as uniform distributions and most normal distributions.

STOs require a larger ICO cap to be successful; iii) both require the same high-margin condition; iv) neither leaves any arbitrage opportunities for speculators. We study the rest of the equilibrium results numerically in §4.2.

4.2 Numerical Experiments: Comparing ICOs to STOs

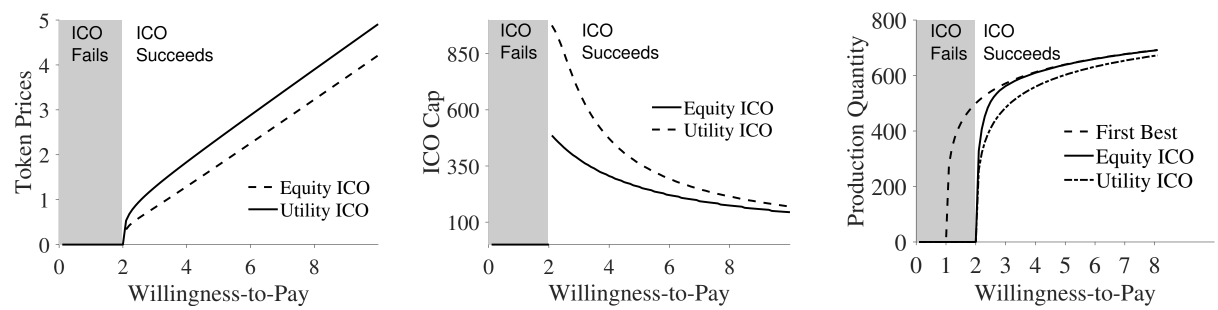
In this section, we numerically compare utility and equity token issuance, starting with sensitivity to customer demand volatility and customer wtp in Figures 4 and 5, respectively. In both figures, equity issuance is characterized by lower ICO token prices and higher ICO caps, that is, the firm retains fewer tokens.

Our analysis (Sections 3 and 4.1) shows that, there is underproduction under both utility and equity issuance. From figures 4(c) and 5(c) we see that good market conditions (low variance, high willingness-to-pay) reduce the extent of underproduction in both cases, and that underproduction is always less severe under equity issuance. By Proposition 3 (iii), this implies that equity issuance also leads to more total funds raised, for the same product and customer demand base.



(a) Token Prices vs Std (b) ICO Cap vs Std (c) Production Quantity vs Std

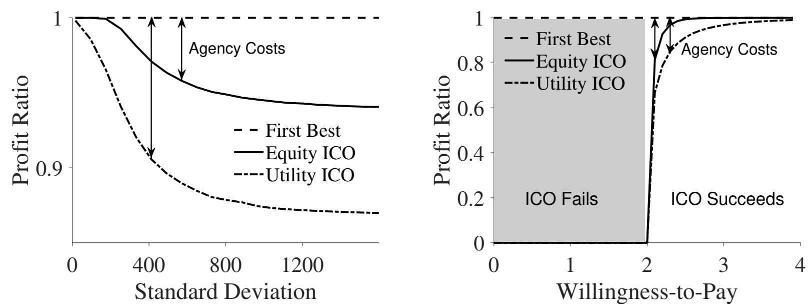
Figure 4: Impact of Demand Volatility on Coin Offering Design Parameters



(a) Token Prices vs WTP (b) ICO Cap vs WTP (c) Production Quantity vs WTP

Figure 5: Impact of Willingness-to-Pay on Coin Offering Design Parameters ($c = 1$)

Finally, Figure 6 shows that with a closer-to-optimal production quantity, the firm faces lower agency costs (a) and expects a higher total wealth (b) under equity issuance. In particular, when market conditions are better, equity tokens allow the firm to achieve a near-the-first-best outcome.



(a) Profit Ratio vs Std (b) Profit Ratio vs WTP

Figure 6: Comparison of Agency Costs

5 Discussion: ICOs vs Other Early-Stage Financing Methods

Our results suggest that ICOs have important differences compared to other forms of early-stage financing. We summarize some of these differences in Table 1. We also discuss in detail two distinct features that our results have highlighted, distinguishing ICOs from other early-stage financing methods: the existence of a secondary market and the issuance of tokens.

Table 1: Comparison of Early-Stage Financing Methods. (A checkmark ✓ indicates the feature is prominent, while ✗ indicates it is of second-order or non-existent. The dual notation ✓✗ indicates that the feature may or may not be of first order, depending on circumstance.)

	Bank	**VC**	**Crowdfunding**		**Coin Offering**	
			Reward	Equity	Utility	Equity
Upside through Profit Sharing	✗	✓	✗	✓	✗	✓
Upside through Revenue Sharing	✗	✗	✗	✗	✓	✗
Downside Demand Risk Sharing	✓	✓	✗	✓	✓	✓
Heavily Regulated	✓	✓	✗	✓	✗	✓✗
Voting/Control Rights	✓✗	✓	✗	✗	✗	✓✗
Funds from Retail Speculators	✗	✗	✗	✓	✓	✓
Funds from Retail Consumers	✗	✗	✓	✓	✓	✓
Secondary Trading	✗	✗	✗	✗	✓	✓

Table 1 contains a large amount of information, and we recommend it be read through bilateral column comparisons. The high-level takeaway from the table is that ICOs, be it utility or equity offerings, differ from each of the other alternative forms of financing in at least one crucial dimension (and more often than not, in several dimensions). We highlight two of these aspects next.

Implications of the existence of a secondary market

ICOs with utility tokens differ from all other financing methods because of their reliance on a secondary market for the tokens. This difference has two important implications.

(i) **Mitigation of moral hazard** The alternative financing methods listed in Table 1 address moral hazard in different ways. Banks, for instance, use interest rates and covenants (Iancu et al. 2016) and/or leverage collateral. VC firms directly monitor the progress of the funded company and invest in stages to keep the company under control (Cherif and Elouaer (2008); Wang and Zhou (2004)). In crowdfunding, moral hazard is often left unadressed, though more recently, some platforms like Indiegogo have started to use escrow accounts to mitigate it (Belavina et al. 2019).

In the case of utility-based ICOs, there typically exists no third party between the fundraising firm and its investors. Instead, moral hazard is addressed, among other things, via the existence of a peer-to-peer secondary market for the tokens. To see this, recall that in our model, the fraction of tokens sold during the ICO, in equilibrium, is below the misconduct fraction. This ensures that a rational firm would be active in production after the ICO. The firm's production effort is reflected in the secondary market token price, and the firm always prefers a higher market token price. We show that, when the willingness-to-pay for the product is high relative to the unit production cost, the firm's dominant strategy is to spend all cash raised on production (i.e., zero cash diversion), which leads to the highest possible token price. Thus, in contrast to the alternative financing methods mentioned above, the existence of a secondary market is crucial in mitigating moral hazard in the context of ICOs.

(ii) **The nature of investors** The ICO secondary peer-to-peer market allows all owners to jointly sell the tokens to those who desire them. As discussed in Appendix A.1, this implies that the investors (speculators) do not have to be the consumers of the firm's products. In contrast, entrepreneurs running traditional crowdfunding campaigns (e.g., on Kickstarter), pre-sell their products directly to early adopting customers during the fundraising stage implying that the majority, if not all, backers in crowdfunding campaigns are the actual product consumers. Given the different nature of investors, it is reasonable to argue that ICOs have access to a larger investor pool than the crowdfunding projects. Indeed, an average ICO project in 2018 was able to raise \$11.52 million (Cointelegraph 2019), which is closer to the average VC deal value in the same year (\$14.6 million) (PitchBook 2019) and far exceeding the crowdfunding average ($10k) (Kickstarter 2019).

Implications of the issuance of tokens

While both ICOs and crowdfunding raise funds through retail investors, the issuance of tokens further differentiates ICOs from crowdfunding. Our model shows that the utility tokens allow revenue sharing and equity tokens allow profit sharing among all token holders. In addition, the tokens dilute the impact of future demand on the firm by allowing the firm to disperse the downside risks of low demand realization among the investors. On the contrary, the backers of a crowdfunding campaign do not share such risks because a low demand in the crowdfunding aftermarket would hurt only the firm's profit. Of course, one exception to the latter point would be when backers are purchasing products that are sensitive to network effects. In this case, the less demand for the product, the lower the network effects, and the lower an individual backer's utility.

6 Extensions

Our base model (ICO with utility tokens) is flexible enough to be extended in different ways to fit a variety of practical situations. We provide two such extensions in this section.

6.1 Technology Risk

Motivated by the Sirin Labs example discussed in the introduction, our base model assumes that the firm is able to successfully produce its product when it incurs the necessary production cost. However, recognizing that startups are inherently risky, here, we relax this assumption, and we add to the base ICO model the risk of production failure.

Let $\alpha \in (0, 1]$ denote the probability that the firm's technology leads to successful production and suppose that the value of α is common knowledge. The firm either successfully produces the decided quantity or ends up with zero acceptable products. We also assume that the firm finds out whether production has been successful at the end of the production period, after it has paid the necessary production cost for the decided quantity. In other words, the production cost is sunk regardless of the outcome of production.

Given such risks, the equilibrium token price is given by $\tau_{eq} = (1 - \alpha) \cdot \frac{v}{m} \min\{0, D\} + \alpha \cdot \frac{v}{m} \min\{Q, D\}$, and thus $\mathbb{E}[\tau_{eq}] = \alpha \cdot \frac{v}{m}\mathbb{E}[\min\{Q, D\}]$. The firm optimizes a modified objective function

$$\max_{\tau, n} \left\{ \tau\, s(\tau, n) + \max_{Q} \ \left[\alpha\,(m - s(\tau, n))\, \frac{v}{m}\, \mathbb{E}[\min\{Q, D\}] - c\, Q \right] \right\} \tag{8}$$

subject to

$\tau\, s(\tau, n) - c\, Q \geq 0,$ (ICO funds cover production costs)

$u(s(\tau, n)) \geq 0.$ (speculators' participation constraint)

We show next that riskier production intensifies the moral hazard problem.

Proposition 8. (Optimal Production Quantity under Risks of Production Failure)
Suppose the firm's production is successful with probability $\alpha \in (0, 1]$. For a fixed token price τ, ICO cap n and number of speculators s, the firm's optimal production quantity $Q^*(s)$ is as follows.

i) If $0 < s < m(1 - \frac{c}{\alpha v})$, then $Q^*(s) = \min\left\{ F^{-1}\left(1 - \frac{m}{\alpha(m-s)} \frac{c}{v}\right), \frac{\tau\, s}{c} \right\}$.

ii) If $s = 0$ or $s \geq m(1 - \frac{c}{\alpha v})$, then $Q^*(s) = 0$.

Proposition 8 shows that, given the same ICO token price and ICO cap, a lower success probability leads to lower production quantity. The firm is also more likely to give up production and divert funds when α is smaller because the misconduct fraction, $1 - \frac{c}{\alpha v}$, is lower. As a result, we show in Proposition 9 that ICOs are less likely to succeed under higher production risks.

Proposition 9. (Conditions for ICO Success under Risks of Production Failure)
Suppose the firm's production is successful with probability $\alpha \in (0, 1]$. Then, the ICO succeeds if and only if

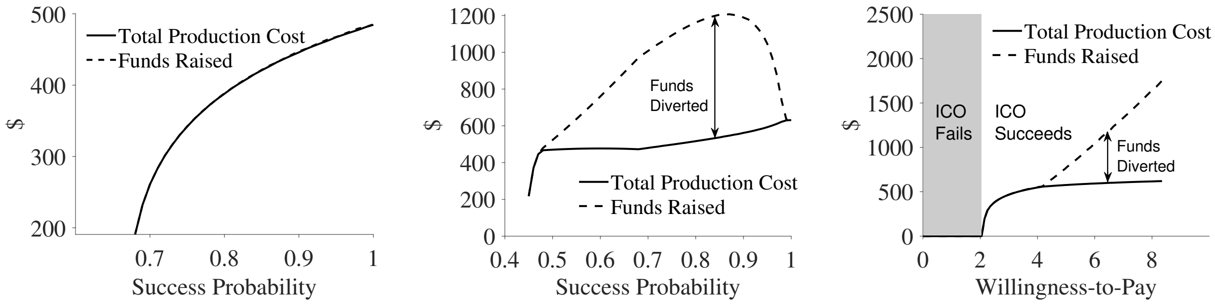
i) (critical mass condition) the firm sells more than $\frac{m\, c}{\alpha\, v}$ tokens in the ICO and,

ii) (price-cost ratio requirement) customers have a high willingness-to-pay such that $v > \frac{2c}{\alpha}$.

To obtain additional insights, we proceed to numerically examine the properties of the equilibrium under this technology risk extension.

Numerical Experiments: The Impact of Technology Risk

It can be readily checked that the firm's final wealth increases in the success probability. More interestingly, Figure 7 shows that the firm's optimal strategy varies for different values of α and v. Recall from Proposition 3 (iii) that, when there is no risk ($\alpha = 1$), the firm invests all money raised in production. For $\alpha < 1$, the firm does the same if either the risks are high or the willingness-to-pay is low (Figure 7 (a,b)). However, under more favorable conditions, i.e., low risk ($\alpha < 1$ but



(a) Funds Usage vs α ($v = 3$) (b) Funds Usage vs α ($v = 6$) (c) Funds Usage vs WTP ($\alpha = 0.95$, $c = 1$)

Figure 7: Funds Usage under Risks of Production Failure

close to 1) and high willingness-to-pay, the firm spends part of its funds raised on production and diverts the rest (Figure 7 (c)). Such practice guarantees that the firm ends up with non-negative final wealth even if production fails.

6.2 Outside Investment Options

We can account for the existence of other investment options (e.g., a savings account) by adding a generic investment option that returns $k > 0$ dollars per dollar investment.

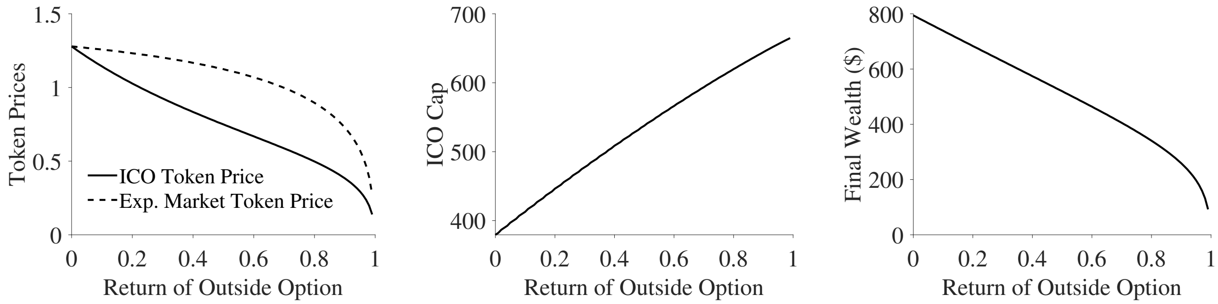
Suppose there exists a generic outside investment option that returns $k > 0$ dollars per dollar of investment. The outside option provides a new reference point when the speculators evaluate their ICO return. Let $\Delta_i(s)$ denote the expected profit improvement by investing in an ICO with utility tokens. Then,

$$\Delta_i(s) = \mathbb{E}[\tau_{eq}(s)] - \tau - \tau\, k = \mathbb{E}[\tau_{eq}(s)] - (k+1)\,\tau, \tag{9}$$

and the speculators' expected profit improvement is $u(s) = \frac{s}{z}\Delta_i(s)$. The firm optimizes the same objective function as in (3). Therefore, the misconduct fraction is unaffected by the presence of the outside option, and the optimal production quantity in the subgame still follows that in Proposition 1. However, we show below that a higher return of the outside option makes ICOs harder to succeed as it leads to more stringent success conditions.

Proposition 10. (Conditions for ICO Success with an Outside Investment Option)
In the presence of an outside investment option with return k per dollar invested, the ICO succeeds if and only if

i) (critical mass condition) the firm sells more than $(1+k)\frac{m\,c}{v}$ *tokens in the ICO and,*



(a) Token Prices vs k (b) ICO Cap vs k (c) Firm's Final Wealth vs k

Figure 8: Impact of Outside Investment Return on ICOs

ii) (price-cost ratio requirement) customers have a high willingness-to-pay such that $v > (2+k)c$.

Next, we show that the optimal ICO token price leads to zero expected profit improvement, i.e., the expected return of the tokens is equal to that of the outside investment option. In this case, since the outside option guarantees positive return, the expected market token price is higher than the ICO token price.

Proposition 11. (Optimal ICO Token Price with an Outside Investment Option)
When $v > (2+k)\,c$*, for a given* $n \in \left((1+k)\frac{m\,c}{v}, m\left(1-\frac{c}{v}\right)\right)$*, there exists a finite positive* $\tau^*(n)$ *uniquely determined by* $u(s^*(\tau^*(n))) = 0$.

To obtain additional insights, we proceed to numerically examine the properties of the equilibrium under this technology risk extension.

Numerical Experiments: The Impact of Outside Investment Options

Intuitively, a better-paying outside option makes ICOs less attractive in comparison. To incentivize the speculators to participate, the firm needs to make token trading more lucrative by either raising the expected market token price or by reducing the ICO token price. Since the former is difficult to achieve given that the customer demand distribution remains unchanged, the firm uses the latter. Our numerical results show that, as k increases, the ICO token price drops (Figure 8 (a)) and the firm sells more tokens during the ICO (Figure 8 (b)) to mitigate the loss in funds raised. A higher k also discourages production and hurts the firm's final wealth (Figure 8 (c)).

In §6.2, we show that the optimal ICO token price makes the expected return of the tokens equal to that of the outside option. This result can be readily checked in Figure 8 (a), where for any value of k, the difference of the token prices divided by the ICO token price is exactly k.

7 Conclusion

7.1 Empirical Predictions

Below, we provide a high-level, non-exhaustive list of some of the empirical predictions of the model. While these predictions are confined to the asset tokenization setting of the paper, they may remain true more generally. They are also subject to the limiting assumptions of the model, discussed in Section 7.2.

1. *ICO "success" (e.g., money raised, cash non-diversion, firm profit, ...) is:*
   (a) Positively correlated with product margins, expected customer demand, and secondary market liquidity
   (b) Negatively correlated with customer demand volatility, and technology/production risk.
2. *Tokens in secondary market:*
   (a) Token value in the secondary market is positively correlated with realized customer demand for the underlying product, revenues, and customer willingness-to-pay
   (b) Token turnover post ICO is positively correlated with secondary market liquidity
3. *Compared to utility-based issuance, equity-based issuance involves:*
   (a) lower: agency costs, token turnover, ICO token prices, cash diversion
   (b) higher: funds raised, investment in production, tokens issued, firm profits
4. *Compared to (reward-based) crowdfunding, ICOs:*
   (a) raise more funds on average, but are better suited for higher-margin products
   (b) attract more speculative investment

7.2 Limitations

As one of the first papers to study the implications of ICOs for asset tokenization, the model we develop has of course some limitations that could represent interesting research opportunities.

Several assumptions in our model could be relaxed to capture more realistic settings. For instance, the tokens could be used for purposes other than to purchase physical goods; customer willingness-to-pay and demand could be affected by quite a few factors that we do not capture, including network effects; the success of the ICO could be informative about future demand in a multi-period setting; investors could have heterogeneous beliefs about product quality; customers could have different valuations for the same product; firms, investors and/or customers could be risk averse or risk seeking, etc.

Finally, like some of the extant literature considering strategic customer behavior (Cachon and Swinney 2011, Belavina et al. 2019), our model assumes strategic customers with known and homogeneous willingness-to-pay. In reality, customer wtp could be i) uncertain and ii) heterogeneous. Our existing model can readily incorporate a relaxation of i) by replacing v with $E[v]$.[10] However, relaxing assumption ii) would generate at least two complications in our setting that would go beyond the scope of the paper: the first would be the need to specify a doubly stochastic model of customer demand, that is, the firm's demand beliefs would need to be specified for every possible customer type; the second would be the need to develop a more elaborate model of secondary market clearing for crypto-currency exchanges. We believe these, as well as the other aforementioned extensions above, to be interesting directions for future research.

References

Adhami S, Giudici G, Martinazzi S (2018) Why do businesses go crypto? an empirical analysis of initial coin offerings. *Journal of Economics and Business* .

Alaei S, Malekian A, Mostagir M (2016) A dynamic model of crowdfunding. *Available at SSRN* .

Alan Y, Gaur V (2018) Operational investment and capital structure under asset-based lending. *M&SOM* .

Arrow KJ, Harris T, Marschak J (1951) Optimal inventory policy. *Econometrica: Journal of the Econometric Society* 250–272.

Babich V, Marinesi S, Tsoukalas G (2019) Does crowdfunding benefit entrepreneurs and venture capital investors? M&SOM, forthcoming.

Babich V, Sobel MJ (2004) Pre-ipo operational and financial decisions. *Management Science* 50(7):935–948.

Bakos Y, Halaburda H (2018) The role of cryptographic tokens and ICOs in fostering platform adoption. Working paper.

Bananacoin (2018) Bananacoin official website. https://bananacoin.io/, last accessed on 06/22/2020.

Belavina E, Marinesi S, Tsoukalas G (2019) Rethinking crowdfunding platform design: mechanisms to deter misconduct and improve efficiency. *Management Science, forthcoming* .

Benedetti H, Kostovetsky L (2018) Digital tulips? returns to investors in initial coin offerings. Working paper.

Biais B, Bisiere C, Bouvard M, Casamatta C (2017) The blockchain folk theorem. Toulouse School of Economics, TSE-817 Working Paper.

Blockstate (2020) Global sto study. https://blockstate.com/global-sto-study-en/, last accessed on 06/22/2020.

Boyabatlı O, Leng T, Toktay LB (2015) The impact of budget constraints on flexible vs. dedicated technology choice. *Management Science* 62(1):225–244.

Boyabatlı O, Toktay LB (2011) Stochastic capacity investment and flexible vs. dedicated technology choice in imperfect capital markets. *Management Science* 57(12):2163–2179.

Buzacott JA, Zhang RQ (2004) Inventory management with asset-based financing. *Management Science* 50(9):1274–1292.

[10]This is the case because the token exchange rate is set via the market clearing condition, which occurs after demand is realized and uncertainty has been resolved.

Cachon GP, Swinney R (2009) Purchasing, pricing, and quick response in the presence of strategic consumers. *Management Science* 55(3):497–511.

Cachon GP, Swinney R (2011) The value of fast fashion: Quick response, enhanced design, and strategic consumer behavior. *Management science* 57(4):778–795.

Catalini C, Gans JS (2018) Initial coin offerings and the value of crypto tokens. Working paper.

Chakraborty S, Swinney R (2017) Sigkonaling to the crowd: Private quality information and rewards-based crowdfunding. Working paper.

Chakraborty S, Swinney R (2018) Designing rewards-based crowdfunding campaigns for strategic contributors. *Available at SSRN 3240094* .

Cherif M, Elouaer S (2008) Venture capital financing: A theoretical model. *The Journal of Applied Business and Economics* 8(1):56.

Chod J, Lyandres E (2018) A theory of ICOs: Diversification, agency, and information asymmetry. Working paper.

Chod J, Trichakis N, Tsoukalas G (2019a) Supplier diversification under buyer risk. *Management Science* .

Chod J, Trichakis N, Tsoukalas G, Aspegren H, Weber M (2019b) On the financing benefits of supply chain transparency and blockchain adoption. *Management Science* .

Cong LW, Li Y, Wang N (2018) Tokenomics: Dynamic adoption and valuation. Working paper.

CryptoGlobe (2018) Only 13% of ico's have a running product, ernst & young report shows. https://www.cryptoglobe.com/latest/2018/10/13-of-icos-have-a-running-product-86-are-below-ico-price-finds-ernst-young/, last accessed on 06/22/2020.

Dana Jr JD, Petruzzi NC (2001) Note: The newsvendor model with endogenous demand. *Management Science* 47(11):1488–1497.

de Jong A, Roosenboom P, van der Kolk T (2018) What determines success in initial coin offerings? *Available at SSRN 3250035* .

Fahlenbrach R, Frattaroli M (2019) ICO investors. *European Corporate Governance Institute-Finance Working Paper* (618).

Fatehi S, Wagner MR, et al. (2017) Crowdfunding via revenue-sharing contracts. *Foundations and Trends® in Technology, Information and Operations Management* 10(3-4):407–424.

Forbes (2018) ICOs were 45% of IPOs in Q2 2018, as cryptos disrupt investment banks. https://www.forbes.com/sites/caitlinlong/2018/07/22/icos-were-45-of-ipos-in-q2-2018-as-cryptos-disrupt-investment-banks/#d55f013794c2, last accessed 06/22/2020.

Gryglewicz S, Mayer S, Morellec E (2019) Optimal financing with tokens. *Swiss Finance Institute Research Paper* (19-78).

Hinzen FJ, John K, Saleh F (2019) Bitcoin's fatal flaw: The limited adoption problem. *SSRN (3334262)* .

Honeypod (2018) Honeypod white paper. https://docsend.com/view/6w2kpua, last accessed on 06/22/2020.

Howell ST, Niessner M, Yermack D (2018) Initial coin offerings: Financing growth with cryptocurrency token sales. Working paper.

Iancu DA, Trichakis N, Tsoukalas G (2016) Is operating flexibility harmful under debt? *Management Science* 63(6):1730–1761.

Khatri Y (2019) Colorado senators file bill to exempt cryptos from securities laws. https://www.coindesk.com/colorado-senators-file-bill-to-exempt-cryptos-from-securities-laws, last accessed on 06/22/2020.

Kouvelis P, Dong L, Boyabatli O, Li R (2011) *Handbook of integrated risk management in global supply chains*, volume 1 (John Wiley & Sons).

Kouvelis P, Zhao W (2012) Financing the newsvendor: supplier vs. bank, and the structure of optimal trade credit contracts. *Operations Research* 60(3):566–580.

Li J, Mann W (2018) Initial coin offering and platform building. Working paper.

Lyandres E, Palazzo B, Rabetti D (2019) Do tokens behave like securities? an anatomy of initial coin offerings. *SSRN Electronic Journal* .

Malinova K, Park A (2018) Tokenomics: when tokens beat equity. *Available at SSRN* .

CB Insights (2018) Venture capital funding report q2 2018. https://www.cbinsights.com/research/report/venture-capital-q2-2018/, last accessed on 06/22/2020.

Cointelegraph (2019) ICO markets 2018 vs 2017: Trends, capitalization, localization, industries, success rate. https://cointelegraph.com/news/ico-market-2018-vs-2017-trends-capitalization-localization-industries-success-rate, last accessed on 06/22/2020.

Kickstarter (2019) Kickstarter stats. https://www.kickstarter.com/help/stats, last accessed on 06/22/2020.

PitchBook (2019) 18 charts to illustrate us vc in 2018. https://pitchbook.com/news/articles/18-charts-to-illustrate-us-vc-in-2018, last accessed on 06/22/2020.

Sirin Labs (2019) Sirin labs official website. https://sirinlabs.com/, last accessed on 06/22/2020.

Memoria F (2018) $9 million: Ether stolen from coindash ICO after website compromise. https://www.ccn.com/110991-2/, last accessed on 06/22/2020.

Milner JM, Kouvelis P (2007) Inventory, speculation, and sourcing strategies in the presence of online exchanges. *Manufacturing & Service Operations Management* 9(3):312–331.

Modigliani F, Miller MH (1958) The cost of capital, corporation finance and the theory of investment. *The American economic review* 48(3):261–297.

Pagnotta E, Buraschi A (2018) An equilibrium valuation of bitcoin and decentralized network assets. *Available at SSRN 3142022* .

Pagnotta ES (2018) Bitcoin as decentralized money: prices, mining, and network security. *SSRN (3264448)* .

Papanastasiou Y, Savva N (2016) Dynamic pricing in the presence of social learning and strategic consumers. *Management Science* 63(4):919–939.

Pozzi D (2018) September ICO market overview: Trends, capitalization, localization. https://cointelegraph.com/news/september-ico-market-overview-trends-capitalization-localization, last accessed on 06/22/2020.

Rosu I, Saleh F (2019) Evolution of shares in a proof-of-stake cryptocurrency. *Working Paper* .

Seth S (2018) 50% of ICOs failed to raise funds since 2017: Report. https://www.investopedia.com/news/50-icos-failed-raise-funds-2017-report/, last accessed on 06/22/2020.

Shifflett S, Jones C (2018) Buyer beware: Hundreds of bitcoin wannabes show hallmarks of fraud. https://www.wsj.com/articles/buyer-beware-hundreds-of-bitcoin-wannabes-show-hallmarks-of-fraud-1526573115, last accessed on 06/22/2020.

Su X (2010) Optimal pricing with speculators and strategic consumers. *Management Science* 56(1):25–40.

Thomson D (2018) US IPO activity showed continued strength: Q2 2018 capital markets watch. http://usblogs.pwc.com/deals/q2-2018-capital-markets-watch/, last accessed on 06/22/2020.

Tsoukalas G, Falk BH (2019) Token-weighted crowdsourcing. *Management Science* .

Wang S, Zhou H (2004) Staged financing in venture capital: moral hazard and risks. *Journal of corporate finance* 10(1):131–155.

Xu F, Guo X, Xiao G, Zhang F (2018) Crowdfunding or bank financing: Effects of market uncertainty and word-of-mouth communication. Working paper.

Xu F, Zhang F (2018) Crowdfunding under social learning and network externalities. Working paper.

Yang SA, Bakshi N, Chen C (2016) Cancelability in trade credit insurance. Working paper.

Yang SA, Birge JR (2013) How inventory is (should be) financed: Trade credit in supply chains with demand uncertainty and costs of financial distress. Working paper.

Appendix:
Initial Coin Offerings, Speculation, and Asset Tokenization

Jingxing (Rowena) Gan, Gerry Tsoukalas and Serguei Netessine*

June 28, 2020

A Additional Discussions and Results

A.1 Utility Tokens and the Token Buyers

In this section, we elaborate on two important features of tokens and the role of the token buyers (the speculators and the customers).

First, tokens play a dual role: as of today, most tokens in the market have been considered as both utility and security.[1] The "security" aspect results from the tradable feature of the tokens. The "utility" aspect comes from the fact that the fundamental value of these tokens lies in the economic value of the products or services that they are redeemable for. However, most projects do not have any products at the time of the ICO. In 2017, for instance, 87% of ICOs did not yet have a running product (CryptoGlobe 2018). To capture these features, we model tokens that start out as pure securities and only after product launch become utility tokens. Such tokens appeal to two groups of token buyers: those who see tokens as securities purchase the tokens in the ICO period (before product launch),[2] whereas those who wish to consume the products buy tokens in the market period (after product launch). Therefore, we refer to the token buyers in the ICO period and those in the market period as *speculators* and *customers* respectively.

The second feature is that the tokens issued by the firm can only be redeemed on the firm's own platform and are the only viable method of payment for the its products. By restricting the method of payment, the firm ties the value of the tokens to the economic value of the products. This, together with the existence of a secondary market to trade the tokens, incentivize speculators

*OID Department, The Wharton School, University of Pennsylvania, Philadelphia, PA 19104. Gan: ganj@wharton.upenn.edu, Tsoukalas: gtsouk@wharton.upenn.edu, Netessine: netessin@wharton.upenn.edu

[1]The regulatory environment is still uncertain but efforts are being made to pass bills that would distinguish tokens from securities like stocks (Khatri 2019).

[2]Technically, those who see tokens as securities may purchase tokens whenever they feel optimistic about the potential return. However, we model a firm that plans one round of production and product sale and the market token price in the market period is an equilibrium quantity that does not change during that period. Therefore, it only makes sense for this group of token buyers to come in the ICO period.

to purchase tokens in the ICO, even if they are not interested in subsequently consuming the product themselves.

At the same time, the fact that the tokens have no use on other platforms has a few implications. First, it means that the token value solely depends on the consumption of products of this particular platform. Second, after the firm ends production, the speculators have no reason to hold the tokens and the customers do not buy more tokens than needed. Third, redeemed tokens retain no value if no further production is planned. Last, since we only consider one round of production, this suggests that the tokens are for one-time use only and the firm cannot resell the redeemed tokens for more cash.

A.2 Example: Honeypod Whitepaper

Honeypod (Honeypod 2018) aims to produce a hardware that serves as the main hub that interconnects various devices and provides traffic filtering. The company claims that they have mature products that are ready for mass production before token crowdsale.

Parameters captured by our model include

1. Hard cap ($m = 200,000,000$).
2. ICO sales cap/soft cap ($n = 40,000,000$).
3. Fixed token price of during public token sale ($\tau = \$0.05$).
4. Customers' willingness to pay ($v = \$99$).
5. Manufacturing cost ($c = \$32$).
6. Production quantity over 12 months ($Q = 50,000$).

Parameters not captured by our model include

1. Four tiers of fixed token prices during private token sale ($\$0.02, \$0.025, \$0.03, \$0.035$).
2. Other use of funds from the token sale (e.g. 25% on maintenance, R&D).

Parameters in our model that are not mentioned in the white paper include

1. Aggregate demand (D).

B Technical Results

B.1 Optimal Token Price and ICO Cap

Given the optimal production quantity and speculators' equilibrium behavior, we now examine how the firm sets the profit-maximizing ICO token cap n^* and initial token price τ^*.

From Lemma 2, the number of speculators $s^*(\tau, n) \leq m\left(1 - \frac{c}{v}\right)$, and given speculators participating in the ICO buy 1 token each, we need not consider the case in which tokens $n > m\left(1 - \frac{c}{v}\right)$. We will first find the token price $\tau^*(n)$ for a given token cap $n \leq m\left(1 - \frac{c}{v}\right)$ and then maximize profit over the token cap n.

For a fixed n, the platform's optimization problem (3) can be written as a maximization problem over τ subject to speculators' participation constraint. In particular, the optimization problem is

$$\max_{\tau \geq 0} \Pi = \tau(n)\, s^*(\tau, n) - c\, Q^*(s^*(\tau, n)) + (m - s^*(\tau, n))\, \mathbb{E}[\tau_{eq}(s^*(\tau, n))], \tag{10}$$

subject to $u(s^*(\tau, n)) \geq 0$ and $Q^*(s^*(\tau, n)) = \min\left\{F^{-1}\left(1 - \frac{cm}{(m - s^*(\tau,n))v}\right), \frac{\tau\, s^*(\tau,n)}{c}\right\}$ (from Proposition 1). Proposition 2 (see Section 3.3) guarantees the existence of a nonzero equilibrium token price τ^*.

Next we find the optimal ICO token price $\tau^*(n)$ assuming the two conditions in Proposition 2 are met. Before stating the proposition, we impose an additional technical condition on the demand distribution to guarantee equilibrium uniqueness[3]: $\frac{f'(F^{-1}(y))}{(f(F^{-1}(y)))^2} > -\frac{3v}{c} \cdot k \cdot \frac{1-k}{2k-1}$ where $k = 1 - \frac{c}{(1-y)v}$ and $y \in [0, 1 - \frac{2c}{v})$.

Proposition 12. (Optimal ICO Token Price)
When $v > 2c$,

- *i) For a given $n \in (\frac{m\,c}{v}, m\left(1 - \frac{c}{v}\right)]$, there exists a finite positive $\tau^*(n)$ uniquely determined by $u(s^*(\tau^*(n))) = 0$.*
- *ii) There exists a unique $\hat{n} \in (\frac{m\,c}{v}, \frac{m}{2})$ such that*
  - *for $n \in \left[\frac{m\,c}{v}, \hat{n}\right)$, $\tau^*(n)$ is the unique solution of $\tau^*(n) = \frac{v}{m}\,\mathbb{E}\left[\min\left\{D, \frac{\tau^*(n)\,n}{c}\right\}\right]$;*
  - *for $n \in \left[\hat{n}, m\left(1 - \frac{c}{v}\right)\right]$, $\tau^*(n) = \frac{v}{m}\,\mathbb{E}\left[\min\left\{D, F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)\right\}\right]$.*

Part (i) of Proposition 12 shows that when the price-cost ratio is high enough, for any fixed ICO cap n in the appropriate range as suggested by Proposition 2 (i), there exists a unique, positive and finite ICO token price $\tau^*(n)$ that maximizes (10) by extracting all utility from the speculators who participate strategically according to Lemma 2. By (1), this implies that the expected equilibrium token price in the market period is equal to the optimal ICO token price, i.e., $\mathbb{E}[\tau_{eq}(s(\tau^*(n), n)] = \tau^*(n)$. We then solve $u(s^*(\tau^*(n))) = 0$ using Lemma 1 (ii) and Proposition 1 (i) and obtain part (ii) of Proposition 12. Recall that the term $\frac{\tau^*(n)\,n}{c}$ reflects the budget constraint and $F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)$ is the constrained optimal production quantity. Therefore, part (ii) of

[3]One can readily check analytically or numerically) that this sufficient condition is generally satisfied for some common distributions such as uniform and normal. All numerical results presented in the paper satisfy this condition.

Proposition 12 suggests that the firm, upon setting the optimal ICO token price, spends all funds raised on production when the ICO cap n is small but produces an optimal quantity without using all the funds when n is large or $\frac{n}{m}$ is closer to the misconduct fraction.

Knowing $\tau^*(n)$, $s^*(\tau^*(n), n)$ and $Q^*(s^*(\tau^*(n), n))$, the firm's optimization problem reduces to a maximization problem over the ICO cap n given by

$$\begin{aligned} \max_{\frac{mc}{v} < n \leq m\left(1-\frac{c}{v}\right)} \Pi \;&=\; \tau^*(n)\, s^*(\tau^*(n), n) \;-\; c\, Q^*(s^*(\tau^*(n), n)) \\ &\quad + (m - s^*(\tau^*(n), n))\, \mathbb{E}[\tau_{eq}(s^*(\tau^*(n), n))] \end{aligned} \tag{11}$$

where $s^*(\tau(n), n) \;=\; n$, $Q^*(s^*(\tau(n), n)) \;=\; \min\left\{F^{-1}(1 - \frac{cm}{(m-n)v}), \frac{\tau^*(n)\, n}{c}\right\}$ and $\tau^*(n)$ is given by Proposition 12 part ii).

This leads to the following result.

Proposition 13. (Equilibrium ICO Cap) *When $v > 2c$, the unique optimal ICO cap $n^* \in (\frac{m\,c}{v}, \frac{m}{2})$ equals the threshold $\hat{n}$ in Proposition 12 ii), and is the solution to the following equation:*

$$\frac{v\, n^*}{c\, m}\, \mathbb{E}\left[\min\left\{D, F^{-1}(1 - \frac{c\, m}{(m - n^*)v})\right\}\right] = F^{-1}\left(1 - \frac{c\, m}{(m - n^*)v}\right).$$

Proposition 13 tells us that neither a small ICO cap that suppresses the production quantity nor a large cap that induces idle cash is profit-maximizing for the firm. The optimal ICO cap n^* allows the firm to raise just enough funds that can be credibly committed to production, and here we provide a semi-closed-form solution of n^*.

B.2 Sequential Arrival of Speculators

In this section, we assume that the z speculators arrive sequentially during the ICO period and observe the number of tokens sold before their arrival, rather than showing up simultaneously. Tokens are sold on a first-come, first-served basis and each speculator buys either zero or one token based on the expected profit of their purchase. We will show that while this alternative assumption on the speculators' arrival changes one of the intermediate results, it leads to the same equilibrium results as in the rest of the paper.

Suppose the first s speculators will buy one token each. Then anyone who arrives later than the $s - th$ speculator will not buy any token and thus obtains zero utility. In this section, we focus on the earliest s arrivers. The expected profit of such a speculator given there s tokens will be sold by the end of the ICO is given by

$$u(s) = \Delta(s)\mathbb{1}_{\{s>0\}}, \tag{12}$$

where $\Delta(s)$, by (1), Lemma 1 and Proposition 1, is

$$\Delta(s) = \frac{v}{m}\,\mathbb{E}\left[\min\left\{D, F^{-1}\left(1 - \frac{cm}{(m-s)v}\right), \frac{\tau\, s}{c}\right\} \cdot \mathbb{1}_{\left\{s<m\left(1-\frac{c}{v}\right)\right\}}\right] - \tau. \tag{13}$$

The participation constraint requires that $u(s) \geq 0$. From (13) we immediately know that the equilibrium number of speculators will never be $m\left(1 - \frac{c}{v}\right)$ or beyond because $u(s) = -\tau < 0$ for $s \geq m\left(1 - \frac{c}{v}\right)$. Therefore, the speculators who arrive sequentially would collectively buy under the misconduct fraction.

Since $u(s)$ and $\Delta(s)$ have the same sign for $s > 0$, Lemma 2 part iii) still holds. Lemma 2 part iii) tells us that when the speculators arrive sequentially, there will be exactly $s_0(\tau)$ speculators without the sales cap n. However, note that $s_0(\tau)$ is not necessarily the utility-maximizing s because the early speculators cannot stop those who arrive later from buying more tokens unless it is no longer profitable to do so.

So far there are two upper bounds of the equilibrium number of speculators s^*: the sales cap, n, and $s_0(\tau)$[4]. We express s^* in terms of these two upper bounds in the following proposition.

Proposition 14. (Equilibrium Number of Sequentially Arriving Speculators)
Given initial token price τ and the sales cap n, the equilibrium number of speculators is given by

$$s^*(\tau, n) = \min\left\{s_0(\tau), n\right\} \tag{14}$$

provided that $s_0(\tau)$ exists and

$$u(s^*) \geq 0. \tag{15}$$

If $s_0(\tau)$ does not exist or $u(\min\{s_0(\tau), n\}) < 0$, then there will be no speculators and thus ICO fails.

Note that the expression of $u(s)$ with simultaneous arrivals given by (1) and that with sequential arrivals given by (12) have the same sign, albeit differing by a scale of s/z for $s > 0$. Since the magnitude of the speculators' profit does not affect their purchase decision or the firm's profit, Propositions 2 - 4 and Proposition 3 (iii) hold for both arrival assumptions. Details can be found

[4]In this section, we assume that $s_0(\tau)$ exists because its existence is necessary for $u(s^*) \geq 0$ for some $s > 0$. We show that the existence of $s_0(\tau)$ depends on both τ and n and discuss the conditions (the critical mass condition and a high willingness-to-pay) in Section 3.3.

in Appendix C.

Moreover, following Proposition 3, we can show that setting a sales cap is not needed when the customers observe their arrival sequence.

Corollary 1. *When $v > 2c$, in equilibrium we have $n^* = s_0(\tau^*(n^*))$.*

By Corollary 1, the optimal ICO sales cap is equal to the equilibrium number of speculators who would participate even when the cap is unannounced. Therefore, to reach the target level of token sales n^* that eventually induces maximum expected profit, it suffices to set the ICO token price to be $\tau^*(n^*)$.

C Proofs

Proof of Lemma 1

i) First note that the customers have a fixed willingness-to-pay v that is equal to $p \cdot \tau_{eq}$. Suppose $p > m/\min\{Q, D\}$, then the demand of tokens $p \cdot \min\{Q, D\}$ exceeds the supply of tokens, m. This will drive the price of the token up, resulting in a decrease in the token-denominated price. In other words, τ_{eq} will increase and p will decrease. Similarly, if $p < m/\min\{Q, D\}$, then the demand of tokens is less than the supply of tokens, which induces an increase in p. Therefore, in equilibrium, demand of tokens is equal to its supply, i.e., $p \cdot \min\{Q, D\} = m$.

ii) The result follows immediately from $\tau_{eq} = v/p$ and Part (i).

□

Proof of Proposition 1

Taking derivative with respect to Q and applying Lemma 1,

$$\begin{aligned}
\frac{d\Pi}{dQ} &= -c + (m-s)\,\frac{d}{dQ}\frac{v\mathbb{E}[\min\{Q, D\}]}{m} \\
&= -c + (m-s)\,\frac{v}{m}(1 - F(Q)) \\
&= [(m-s)\,\frac{v}{m} - c] - (m-s)\,\frac{v}{m}F(Q)
\end{aligned} \tag{16}$$

By (16), $\frac{d\Pi}{dQ} < 0$ when $(m-s)\frac{v}{m} - c < 0$, i.e., $s > m\left(1 - \frac{c}{v}\right)$. On the other hand, when $s \leq m\left(1 - \frac{c}{v}\right)$, ignoring the budget constraint and setting $\frac{d\Pi}{dQ} = 0$, we get $Q^*_{unconstrained}(s) = F^{-1}(1 - \frac{cm}{(m-s)v})$. Since $\frac{d^2\Pi}{dQ^2} = -(m-s)\frac{v}{m}f(Q) < 0$, the profit function is concave in Q and $Q^*_{unconstrained}$ is a maximum. Hence the firm's optimal production quantity is given by

$$Q^*(s) = \min\left\{F^{-1}(1 - \frac{cm}{(m-s)v}), \frac{\tau\, s}{c}\right\} \cdot \mathbb{1}_{\left\{s \leq m\left(1 - \frac{c}{v}\right)\right\}}. \tag{17}$$

$\square$

Proof of Lemma 2

i) See the main text.

ii) Complete cash diversion means $Q^*(s) = 0$. By (17), we know that $Q^*(s) = 0$ when $s = 0$ or $s \geq m\left(1 - \frac{c}{v}\right)$, because $F^{-1}(1 - \frac{cm}{(m-s)v})$ strictly decreases in s while $\frac{\tau s}{c}$ strictly increases in s.

iii) Fix τ and n. Recall that by (1) that $u(s)$ and $\Delta(s)$ have the same sign. Therefore, we can also express $s_0(\tau)$ as $\max\{s \geq 0 : \Delta(s) = 0\}$. We now examine the behavior of $\Delta(s)$ as a function of s:

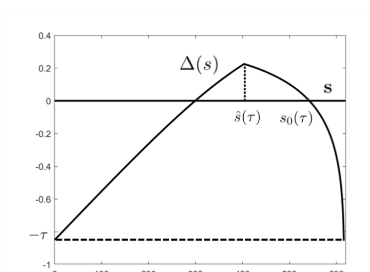
$$\left.\frac{d\Delta(s)}{ds}\right|_{s<m\left(1-\frac{c}{v}\right)} = \frac{v}{m}\left[1 - F(Q^*(s))\right] \left.\frac{dQ^*(s)}{ds}\right|_{s<m\left(1-\frac{c}{v}\right)}, \tag{18}$$

where

$$\left.\frac{dQ^*(s)}{ds}\right|_{s\leq m\left(1-\frac{c}{v}\right)} = \begin{cases} -\frac{cm}{f(Q^*(s))(m-s)^2\,v} & \text{if } F^{-1}(1 - \frac{cm}{(m-s)v}) \leq \frac{\tau s}{c} \\ \frac{\tau}{c} & \text{otherwise} \end{cases}. \tag{19}$$

Ignoring the sales cap n for the moment, note that for $s \in [0, m\left(1 - \frac{c}{v}\right)]$, $F^{-1}(1 - \frac{cm}{(m-s)v})$ monotonically decreases in s whereas $\frac{\tau s}{c}$ linearly increases in s. Also, $F^{-1}(1 - \frac{cm}{(m-s)v})\big|_{s=0} = F^{-1}(1 - \frac{c}{v}) > 0 = \frac{\tau s}{c}\big|_{s=0}$ and $F^{-1}(1 - \frac{cm}{(m-s)v})\big|_{s=m\left(1-\frac{c}{v}\right)} = 0 < \frac{\tau s}{c}\big|_{s=m\left(1-\frac{c}{v}\right)}$. Therefore, for any fixed τ, there exists one and only one $\hat{s}(\tau)$ that satisfies $F^{-1}(1 - \frac{cm}{(m-\hat{s}(\tau)v}) = \frac{\tau\,\hat{s}(\tau)}{c}$. By (19), $Q^*(s)$ increases in s for $s \in [0, \hat{s}(\tau))$ and decreases in s for $s \in (\hat{s}(\tau), m\left(1 - \frac{c}{v}\right))$, and is thus maximized at $\hat{s}(\tau)$. Therefore, (18) is positive for all $s \in [0, \hat{s}(\tau))$ and negative for all $s \in (\hat{s}(\tau), m\left(1 - \frac{c}{v}\right))$ and $\hat{s}(\tau)$ maximizes $\Delta(s)$. Now note that $\Delta(0) = 0 - \tau = -\tau$ and $\Delta(m\left(1 - \frac{c}{v}\right)) = 0 - \tau = -\tau$. This shows that $s_0(\tau) \in [\hat{s}(\tau), m\left(1 - \frac{c}{v}\right))$ if it exists. Figure 9 illustrates the relationships between the quantities mentioned above when demand is normally distributed.

Figure 9: $\Delta(s)$ vs s, assuming existence of $s_0(\tau)$



$\square$

Proof of Proposition 2

i) For an ICO to succeed, there must be a positive number of speculators who invest. Therefore, the firm needs to set a (τ, n) pair that satisfies the speculators' participation constraint. Consider a fixed $n > 0$. A necessary condition for this n to induce a successful ICO is that there exists $\tau > 0$ such that $s^*(\tau, n) > 0$ and $u(s^*(\tau, n)) \geq 0$, which is a necessary condition for the existence of $s_0(\tau)$. Therefore, we will characterize such n while assuming the existence of $s_0(\tau)$.

Now, for the fixed $n > 0$, we divide the space of possible τ into two partitions, $T_1 = \{\tau \geq 0 : s_0(\tau) < n\}$ and $T_2 = \{\tau \geq 0 : s_0(\tau) \geq n\}$, and in each partition look for eligible $\tau > 0$, i.e., $s^*(\tau, n) > 0$ and $u(s^*(\tau, n)) \geq 0$.

(*Simultaneous,* T_1) When $n > s_0(\tau)$, with simultaneous arrival $s^* = 0$. Therefore, there is no eligible $\tau > 0$ in T_1.

(*Simultaneous,* T_2) Now we consider T_2 where $0 < n \leq s_0(\tau)$. First note that when $\tau = 0$, the firm raises no money and thus produces $Q^* = 0$. Therefore $u(s^*(0, n)) = 0$ and $0 \in T_2$. To find out if an eligible $\tau > 0$ exists in T_2, we need to know how $u(s^*(\tau, n))$ changes in $\tau \in T_2$. Under simultaneous arrivals, by (1) and (13) we have

$$
\begin{aligned}
\left.\frac{du(s^*(\tau,n))}{d\tau}\right|_{\tau\in T_2} &= \frac{d}{d\tau}\left[\frac{n}{z}\Delta(n)\right] \\
&= \frac{n}{z}\left[\frac{v}{m}\frac{d}{d\tau}\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{cm}{(m-n)v}), \frac{\tau\, n}{c}\right\}] - 1\right] \\
&= \frac{n}{z}\left[\frac{v}{m}\frac{d}{d\tau}\mathbb{E}[\min\left\{D, \frac{\tau\, n}{c}\right\}]\cdot \mathbb{1}_{\{F^{-1}(1-\frac{cm}{(m-n)v})\geq \frac{\tau\, n}{c}\}}\right] \\
&\quad + \frac{n}{z}\left[\frac{v}{m}\frac{d}{d\tau}\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{cm}{(m-n)v})\right\}]\cdot \mathbb{1}_{\{F^{-1}(1-\frac{cm}{(m-n)v})< \frac{\tau\, n}{c}\}} - 1\right] \\
&= \frac{n}{z}\left[\frac{v}{m}(1-F(\frac{\tau\, n}{c}))\,\frac{n}{c}\cdot \mathbb{1}_{\{\tau\leq \frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})\}}\right] \\
&\quad + \frac{n}{z}\left[\frac{v}{m}(1-F(F^{-1}(1-\frac{cm}{(m-n)v})))\cdot 0\cdot \mathbb{1}_{\{\tau> \frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})\}} - 1\right] \\
&= \frac{n}{z}\left[\frac{v}{m}(1-F(\frac{\tau\, n}{c}))\,\frac{n}{c}\cdot \mathbb{1}_{\{\tau\leq \frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})\}} - 1\right]. \qquad (20)
\end{aligned}
$$

By the analysis of T_1 and (20), for $\tau > \frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})$, the speculators' profit would either remain the same (if $\tau \in T_1$) or keep decreasing in τ (if $\tau \in T_2$) as $\frac{du(s^*(\tau,n))}{d\tau}|_{\tau\in T_2} = -\frac{n}{z} < 0$. For $\tau \leq \frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})$, $u(s^*(\tau, n)$ is either zero (if $\tau \in T_1$) or keeps decreasing in τ (if $\tau \in T_2$) as $(1 - F(\frac{\tau\, n}{c})$ decreases in τ. Hence, to guarantee a positive number of speculators and thus non-negative profit, it is necessary and sufficient for the platform to set n such that $\frac{du(s^*(\tau,n))}{d\tau}\Big|_{\tau=0} = \frac{n}{z}\left[\frac{v}{m}\,(1-F(\frac{0\cdot n}{c}))\,\frac{n}{c}-1\right] > 0$, i.e., $n > \frac{m\,c}{v}$. In this case, $\exists \tau > 0$ s.t. $u(s^*(\tau,n)) > 0$. Note that by definition of $s_0(\tau)$, it must be that $s^*(\tau,n) < s_0(\tau)$ and thus $n < s_0(\tau)$, which means that this τ is indeed in T_2.

(*Sequential*) Consider the sequential arrivals assumption.

When $n > s_0(\tau)$, $s^*(\tau,n) = \min\{s_0(\tau), n\} = s_0(\tau)$ and $u(s^*(\tau,n)) = 0$. Ostensibly, there exists eligible τ's in T_1. However, we have assumed the existence of $s_0(\tau)$ and we need to make sure that it still holds. The existence of $s_0(\tau)$ depends on the behavior of $u(s^*(\tau,n))$ for $\tau \in T_2$. By (13) and (12), we have

$$\begin{aligned}\frac{du(s^*(\tau,n))}{d\tau}\Bigg|_{\tau\in T_2} &= \frac{d}{d\tau}\Delta(n) \\ &= \frac{v}{m}\,(1-F(\frac{\tau\, n}{c}))\,\frac{n}{c}\cdot \mathbb{1}_{\{\tau\le\frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})\}} - 1. \end{aligned} \tag{21}$$

Note that (21) only differs from (20) by a scale of $\frac{n}{z}$. We then follow a similar argument as in part (*Simultaneous, T_2*) to show that $s_0(\tau)$ exists if and only if $n > \frac{m\,c}{v}$.

ii) By Part (i), $s^* \ge \frac{m\,c}{v}$. On the other hand, we showed in Section 3.2 that $s^* < m\left(1-\frac{c}{v}\right)$. Therefore, the ICO fails if $m\left(1-\frac{c}{v}\right) \le \frac{m\,c}{v}$, i.e., $v \le 2c$.

□

Proof of Proposition 3

i) Shown by Proposition 2.

ii) (a) Shown by Proposition 13.

(b) By Proposition 12, we know that there exists a unique $\hat{n} \in (\frac{m\,c}{v}, \frac{m}{2})$ such that the following holds:

- $\frac{v\,\hat{n}}{c\,m}\,\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{c\,m}{(m-\hat{n})v})\right\}] = F^{-1}(1-\frac{c\,m}{(m-\hat{n})v})$;
- $F^{-1}(1-\frac{c\,m}{(m-\hat{n})v}) = \frac{\tau^*(\hat{n})\hat{n}}{c}$.

We show in the proof of Proposition 13 that this $\hat{n}$ is a global maximum point, which we call n^*. Hence, $\frac{v\,n^*}{c\,m}\,\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{c\,m}{(m-n^*)v})\right\}] = \frac{\tau^*(n^*)n^*}{c}$, and the ICO token price is $\tau^* = \frac{v}{m}\,\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{c\,m}{(m-n^*)v})\right\}]$.

(c) By Lemma 2, $s^*(\tau^*, n^*) = n^*\cdot\mathbb{1}_{\{u(n^*)\ge 0\}}$. By definition of τ^* as in Proposition 12 part (i), we know that $u(n^*) = u(n^*, n^*, \tau^*) \ge 0$. The result follows.

(d) Following the proof of part (b) and substituting n^* and τ^* into Proposition 1 part (i), we have $Q^* = \min\left\{F^{-1}(1-\frac{c\,m}{(m-n^*)v}), \frac{\tau^* n^*}{c}\right\} = F^{-1}(1-\frac{c\,m}{(m-n^*)v})$.

(e) By definition of τ^* as in Proposition 12 part (i), we have $\mathbb{E}[\tau_{eq}] = \tau^*$. We obtain the result by part (b).

iii) By part (a), (b) and (e) of Proposition 3, we have $n^* \cdot \tau^* = Q^* \cdot c$.

$\square$

Proof of Proposition 4

i) We show in Proposition 3 that an ICO is only viable when $v > 2c$.

ii) **Lower production level.** The ICO newsvendor's profit is given by $\Pi_{ICO} = \tau^* s^* - c\, Q^* + (m - s^*)\, \mathbb{E}[\tau_{eq}]$. By Proposition 3, $\tau^* = \mathbb{E}[\tau_{eq}]$, therefore

$$\begin{aligned} \Pi_{ICO} &= m\, \mathbb{E}[\tau_{eq}] - c\, Q^* \\ &= v\, \mathbb{E}[\min \left\{ D, F^{-1}(1 - \frac{c\, m}{(m-n^*)v}) \right\}] - c\, F^{-1}(1 - \frac{c\, m}{(m-n^*)v}) \\ &= \Pi_{traditional}(F^{-1}(1 - \frac{c\, m}{(m-n^*)v})) \end{aligned} \tag{22}$$

where $\Pi_{traditional}$ is the profit function of a traditional newsvendor defined as $\Pi_{traditional}(Q) = v\, \mathbb{E}[\min\{D, Q\}] - c\, Q$. We know that $\Pi_{traditional}(Q)$ is maximized by $F^{-1}(1 - \frac{c}{v})$ which is greater than $F^{-1}(1 - \frac{c\, m}{(m-n^*)v})$ by part (ii). Therefore $\Pi_{traditional}(F^{-1}(1 - \frac{c\, m}{(m-n^*)v})) < \Pi_{traditional}(F^{-1}(1 - \frac{c}{v}))$.

Smaller profit. By Proposition 3, $Q^*_{ICO} = F^{-1}(1 - \frac{c\, m}{(m-n^*)v})$. The optimal production quantity of a traditional newsvendor is $F^{-1}(1 - \frac{c}{v})$. Since $\frac{m}{m-n^*} > 1$ and F^{-1} is an increasing function, we have $F^{-1}(1 - \frac{c\, m}{(m-n^*)v}) < F^{-1}(1 - \frac{c}{v})$.

$\square$

Proof of Proposition 5

Let Π_e denote the expected final wealth of the firm that issues equity tokens. Ignoring the budget constraint for the moment and taking derivative of Π_e with respect to Q, by (6),

$$\begin{aligned} \frac{d\Pi_e}{dQ} &= v\,[1 - F(Q)] - c - \frac{s}{m} \frac{d}{dQ} \mathbb{E}[v \min\{Q, D\} - c\, Q]^+ \\ &= v\,[1 - F(Q)] - c - \frac{s}{m} \frac{d}{dQ} \left[(v - c)\, Q\, [1 - F(Q)] + \int_{\frac{c}{v}Q}^{Q} (v\, x - c\, Q) f(x) dx \right] \\ &= v\,[1 - F(Q)] - c - \frac{s}{m} \left[v\,[1 - F(Q)] - c + c\, F\left(\frac{c}{v}Q\right) \right] \\ &= \frac{m - s}{m}\, [v\,[1 - F(Q)] - c] - \frac{s\, c}{m} F\left(\frac{c}{v}Q\right). \end{aligned} \tag{23}$$

By (23), for $s \in (0, m)$, $\frac{d\Pi_e}{dQ}\big|_{Q=0} = \frac{m-s}{m}(v-c) - 0 > 0$ and $\frac{d^2\Pi_e}{dQ^2}\big|_{Q>0} = \frac{m-s}{m}[-f(Q)v] - \frac{s\, c}{m} \cdot \frac{c}{v}\, f\left(\frac{c}{v}Q\right) < 0$. Therefore, there exists a unique unconstrained optimal production quantity, denoted by $Q^*_u(s)$, such that $\frac{d\Pi_e}{dQ}\big|_{Q=Q_u^*(s)} = 0$, i.e.,

$$\frac{m-s}{m}\,\left[v\left[1-F(Q_u^*(s))\right]-c\right] \;=\; \frac{s\,c}{m}\,F\left(\frac{c}{v}Q_u^*(s)\right). \tag{24}$$

Next, we show that $\frac{dQ_u^*(s)}{ds} < 0$. Differentiating (24) with respect to s, we get

$$-\,(v-c) + v\,F(Q_u^*(s)) - c\,F\left(\frac{c}{v}Q_u^*(s)\right) \;=\; \left[(m-s)v\,f(Q_u^*(s)) + s\,c\,f\left(\frac{c}{v}Q_u^*(s)\right)\cdot\frac{c}{v}\right]\frac{dQ_u^*(s)}{ds}. \tag{25}$$

By (24), the left-hand side of (25) equals $-\frac{m}{s}[v\,(1-F(Q_u^*(s))) - c$, which is negative. Since the coefficient of $\frac{dQ_u^*(s)}{ds}$ on the right-hand side of (25) is positive, $\frac{dQ_u^*(s)}{ds}$ must be negative.

□

Proof of Proposition 6

i) To make the ICO successful, the firm needs to set a (τ_e, n_e) pair such that a positive number of speculators participate in the ICO, i.e., $s(\tau_e, n_e) > 0$, which requires the participation constraint.

We first evaluate the behavior of $\Delta(s(\tau_e, n_e))$. Now, $\Delta(s(\tau_e, n_e)) = \frac{1}{m}\mathbb{E}[v\min\{Q_e^*(s(\tau_e, n_e)), D\} - c\,Q_e^*(s(\tau_e, n_e))]^+ - \tau_e$. For a fixed τ_e,

$$\begin{aligned}
\frac{d\Delta(s)}{ds} &= \frac{1}{m}\,\frac{\partial}{\partial Q_e^*(s)}\mathbb{E}[v\min\{Q_e^*(s), D\} - c\,Q_e^*(s)]^+\,\frac{dQ_e^*(s)}{ds} \\
&= \frac{1}{m}\,\left\{v\left[1-F(Q_e^*(s))\right] - c + c\,F\left(\frac{c}{v}Q_e^*(s)\right)\right\}\,\frac{dQ_e^*(s)}{ds}.
\end{aligned} \tag{26}$$

Following similar arguments as in Lemma 2 (iii) and the regularity assumption that $f(x) < a^2\cdot f(ax)$ for $a > 2$, we can show that $v\left[1-F(Q_e^*(s))\right] - c + c\,F\left(\frac{c}{v}Q_e^*(s)\right) > 0$ for all s. This, given that $\frac{dQ_u^*(s)}{ds} < 0$, means that there exists a unique $\hat{s}(\tau_e)$ that satisfies $Q_u^*(s) = \frac{\tau_e\,\hat{s}(\tau_e)}{c}$ and $\hat{s}$ maximizes $\Delta(s)$.

Next, following the argument in Proposition 2 (i), we have

$$\begin{aligned}
\frac{du(s^*(\tau_e, n_e))}{d\tau_e}\bigg|_{\tau_e\in T_2} &= \frac{d}{d\tau_e}\left[\frac{n_e}{z}\Delta(n_e)\right] \\
&= \frac{n_e}{z}\left[\frac{1}{m}\,\frac{d}{d\tau_e}\mathbb{E}[v\min\{Q_e^*(n_e), D\} - c\,Q_e^*(n_e)]^+ - 1\right] \\
&= \frac{n_e}{z}\left[\frac{1}{m}\,\frac{\partial}{\partial Q_e^*}\mathbb{E}[v\min\{Q_e^*(n_e), D\} - c\,Q_e^*(n_e)]^+\,\frac{dQ_e^*}{d\tau_e} - 1\right] \\
&= \frac{n_e}{z}\left[\frac{1}{m}\,\left\{v\left[1-F(Q_e^*(n_e))\right] - c + c\,F\left(\frac{c}{v}Q_e^*(n_e)\right)\right\}\,\frac{dQ_e^*}{d\tau_e} - 1\right]
\end{aligned} \tag{27}$$

Again, the firm needs $\frac{du(s^*(\tau_e,n_e))}{d\tau_e}\Big|_{\tau_e=0} = \frac{n_e}{z}\left[\frac{1}{m}\,\{v-c+0\}\,\frac{n_e}{c}-1\right] > 0$, i.e., $n_e > \frac{c}{v-c}\,m$.

ii) Since we need $n_e < m$, by part (i), we must have $1 > \frac{c}{v-c}$, i.e., $v > 2c$.

$\square$

Proof of Proposition 7

For a fixed n_e, $\frac{d\Pi_e}{d\tau_e} = \frac{\partial\Pi_e}{\partial\tau_e} + \frac{\partial\Pi_e}{\partial Q_e^*}\frac{dQ_e^*}{d\tau_e} = n_e + \frac{\partial\Pi_e}{\partial Q_e^*}\frac{dQ_e^*}{d\tau_e}$. Note that $\frac{\partial\Pi_e}{\partial Q_e^*} > 0$ because $Q_e^* \leq Q_u^*$, and $\frac{dQ_e^*}{d\tau_e} = \frac{n_e}{c}$ or 0. Therefore, we know that $\frac{d\Pi_e}{d\tau_e} > 0$. Given that τ_e^* must satisfy the participation constraint, we have $u(s^*(\tau_e^*(n_e))) = 0$. By (27), we know that such τ_e^* is finite. Lastly, since $u(s^*(\tau_e, n_e)$ is linear in τ_e, $\tau_e^*(n_e)$ must be unique.

$\square$

Proof of Proposition 8

Differentiate (8) with respect to Q,

$$\frac{d\Pi}{dQ} \;=\; [(m-s)\,\frac{\alpha\, v}{m}\, -\, c\,] \,-\, \alpha\,(m-s)\,\frac{v}{m}F(Q) \tag{28}$$

By (28), $\frac{d\Pi}{dQ} < 0$ when $\alpha(m-s)\,\frac{v}{m} - c < 0$, i.e., $s > m(1-\frac{c}{\alpha\, v})$. On the other hand, when $s \leq m(1-\frac{c}{\alpha\, v})$, ignoring the budget constraint and setting $\frac{d\Pi}{dQ} = 0$, we get $Q^*_{unconstrained}(s) = F^{-1}(1-\frac{cm}{\alpha(m-s)v})$. Since $\frac{d^2\Pi}{dQ^2} = -\,\alpha\,(m-s)\,\frac{v}{m}f(Q) < 0$, the profit function is concave in Q and $Q^*_{unconstrained}$ is a maximum. Hence the firm's optimal production quantity is given by

$$Q^*(s) = \min\left\{F^{-1}(1-\frac{cm}{\alpha\,(m-s)v}), \frac{\tau\, s}{c}\right\}\cdot \mathbb{1}_{\left\{s\leq m(1-\frac{c}{\alpha\, v})\right\}}. \tag{29}$$

$\square$

Proof of Proposition 9

i) We substitute the new definition of the market equilibrium token price, $\tau_{eq} = \alpha\cdot\frac{v}{m}\min\{Q, D\}$, into (1), and then follow similar arguments in the proofs of Lemma 2(iii) and Proposition 2. Applying (29), we have

$$\begin{aligned} \frac{du(s^*(\tau,n))}{d\tau}\bigg|_{\tau\in T_2} &= \frac{d}{d\tau}\left[\frac{n}{z}\Delta(n)\right] \\ &= \frac{n}{z}\left[\frac{\alpha\, v}{m}\,(1-F(\frac{\tau\, n}{c}))\,\frac{n}{c}\cdot \mathbb{1}_{\{\tau\leq\frac{c}{n}F^{-1}(1-\frac{cm}{\alpha\,(m-n)v})\}} - 1\right]. \end{aligned} \tag{30}$$

By the analysis of T_1 and (30), for $\tau > \frac{c}{n}F^{-1}(1-\frac{cm}{\alpha(m-n)v})$, the speculators' profit would either remain the same (if $\tau \in T_1$) or keep decreasing in τ (if $\tau \in T_2$) as $\frac{du(s^*(\tau,n))}{d\tau}|_{\tau\in T_2} = -\frac{n}{z} < 0$. For $\tau \leq \frac{c}{n}F^{-1}(1-\frac{cm}{\alpha(m-n)v})$, $u(s^*(\tau,n))$ is either zero (if $\tau \in T_1$) or keeps decreasing in τ (if

$\tau \in T_2$) as $(1 - F(\frac{\tau\, n}{c})$ decreases in τ. Hence, to guarantee a positive number of speculators and thus non-negative profit, it is necessary and sufficient for the platform to set n such that $\frac{du(s^*(\tau,n))}{d\tau}\Big|_{\tau=0} = \frac{n}{z}\left[\frac{\alpha v}{m}\left(1 - F(\frac{0\cdot n}{c})\right)\frac{n}{c} - 1\right] > 0$, i.e., $n > \frac{m\,c}{\alpha v}$. In this case, $\exists \tau > 0$ s.t. $u(s^*(\tau,n)) > 0$. Note that by definition of $s_0(\tau)$, it must be that $s^*(\tau,n) < s_0(\tau)$ and thus $n < s_0(\tau)$, which means that this τ is indeed in T_2.

ii) By Part (i), $s^* \geq \frac{m\,c}{\alpha v}$. On the other hand, we showed in §6.1 that $s^* < m(1 - \frac{c}{\alpha\, v})$. Therefore, the ICO fails if $m(1 - \frac{c}{\alpha\, v}) \leq \frac{m\,c}{\alpha\, v}$, i.e., $v \leq \frac{2c}{\alpha}$.

□

Proof of Proposition 10

i) We substitute the new definition of the expected profit given by (9) into (1), and then follow similar arguments in the proofs of Lemma 2(iii) and Proposition 2.

Applying (17), we have

$$\begin{aligned}\frac{du(s^*(\tau,n))}{d\tau}\bigg|_{\tau\in T_2} &= \frac{d}{d\tau}\left[\frac{n}{z}\Delta(n)\right] \\ &= \frac{n}{z}\left[\frac{v}{m}\left(1 - F(\frac{\tau\, n}{c})\right)\frac{n}{c}\cdot \mathbb{1}_{\{\tau \leq \frac{c}{n}F^{-1}(1-\frac{cm}{(m-n)v})\}} - (1+k)\right]. \end{aligned} \quad (31)$$

By the analysis of T_1 and (31), for $\tau > \frac{c}{n}F^{-1}(1 - \frac{cm}{(m-n)v})$, the speculators' profit would either remain the same (if $\tau \in T_1$) or keep decreasing in τ (if $\tau \in T_2$) as $\frac{du(s^*(\tau,n))}{d\tau}|_{\tau\in T_2} = -\frac{n}{z}(1+k) < 0$. For $\tau \leq \frac{c}{n}F^{-1}(1 - \frac{cm}{(m-n)v})$, $u(s^*(\tau,n))$ is either zero (if $\tau \in T_1$) or keeps decreasing in τ (if $\tau \in T_2$) as $(1 - F(\frac{\tau\, n}{c})$ decreases in τ. Hence, to guarantee a positive number of speculators and thus non-negative profit, it is necessary and sufficient for the platform to set n such that $\frac{du(s^*(\tau,n))}{d\tau}\Big|_{\tau=0} = \frac{n}{z}\left[\frac{v}{m}\left(1 - F(\frac{0\cdot n}{c})\right)\frac{n}{c} - (1+k)\right] > 0$, i.e., $n > \frac{m\,c}{v}(1+k)$. In this case, $\exists \tau > 0$ s.t. $u(s^*(\tau,n)) > 0$. Note that by definition of $s_0(\tau)$, it must be that $s^*(\tau,n) < s_0(\tau)$ and thus $n < s_0(\tau)$, which means that this τ is indeed in T_2.

ii) By Part (i), $s^* \geq \frac{m\,c}{v}(1+k)$. On the other hand, we showed in §6.2 that $s^* < m\left(1 - \frac{c}{v}\right)$. Therefore, the ICO fails if $m\left(1 - \frac{c}{v}\right) \leq \frac{m\,c}{v}(1+k)$, i.e., $v \leq (2+k)c$.

□

Proof of Proposition 11

Since the firm's objective function remains unchanged by adding the outside option, the proof of this proposition resembles that of Proposition 12 (i). □

Proof of Proposition 12

i) First note that by Lemma 2 or (14), for each τ, it is redundant to consider $n > s_0(\tau)$. Therefore, for each n, we can restrict our attention to the set $T_r = \{\tau > 0 : s_0(\tau) \geq n\}$.

When $n \leq s_0(\tau)$, we have $s^*(\tau, n) = n$. We will first find $\tau^*(n) \in \mathbb{R}^+$ that maximizes (10) evaluated at $s^*(\tau, n) = n$ and then show that this $\tau^*(n)$ is in T_r. Since $T_r \subset \mathbb{R}^+$, this $\tau^*(n)$ must maximize (10) over T_r.

Substituting $s^*(\tau, n) = n$ into (10) and differentiating with respect to τ,

$$\begin{aligned}
\frac{d\Pi}{d\tau} &= n - c\,\frac{dQ^*(n)}{d\tau} + (m-n)\,\frac{v}{m}\,\frac{d}{d\tau}\mathbb{E}[\min\{D, Q^*(n)\}] \\
&= n - c\,\frac{dQ^*(n)}{d\tau} + (m-n)\,\frac{v}{m}\,(1 - F(Q^*(n)))\,\frac{dQ^*(n)}{d\tau} \\
&= n + \left[(m-n)\,\frac{v}{m}\,(1 - F(Q^*(n))) - c\right]\frac{dQ^*(n)}{d\tau} \\
&= n + \left[(m-n)\,\frac{v}{m}\,(1 - F(Q^*(n))) - c\right]\mathbb{1}_{\{F^{-1}(1-\frac{cm}{(m-n)v}) \geq \frac{\tau n}{c}\}}\,\frac{n}{c} \\
&= \begin{cases} n + \left[(m-n)\,\frac{v}{m}\,(1 - F(Q^*(n))) - c\right]\frac{n}{c} & \text{if } F^{-1}(1 - \frac{cm}{(m-n)v}) \geq \frac{\tau n}{c} \\ n & \text{otherwise} \end{cases}.
\end{aligned} \tag{32}$$

Note that $F^{-1}(1-\frac{cm}{(m-n)v}) \geq \frac{\tau n}{c}$ means $(m-n)\,\frac{v}{m}\,(1-F(Q^*(n)))-c \geq 0$. Therefore, $\frac{d\Pi}{d\tau} > 0$ for all τ, implying that for a given n, the optimal initial token price $\tau^*(n)$ is given by

$$\tau^*(n) = \max\{\tau : u(s^*(\tau, n)) = \mathbb{E}[\tau_{eq}(Q^*(n))] - \tau \geq 0\}. \tag{33}$$

Consider some $n \in (\frac{m\,c}{v},\, m\left(1 - \frac{c}{v}\right)]$ and we know by (20) that $\frac{du(s^*(\tau,n))}{d\tau} > 0$ for $\tau \in [0, \tilde{\tau})$ for some $0 < \tilde{\tau} < \frac{c}{n}F^{-1}(1 - \frac{cm}{(m-n)v})$ such that $\frac{du(s^*(\tau,n))}{d\tau}\big|_{\tau=\tilde{\tau}} = 0$. Given that $u(s^*(0, n)) = 0$, by definition of τ^* given by (33), we must have $\tau^*(n) > \tilde{\tau} > 0$. We also know that $\tau^*(n) < \infty$ because by (20), the speculators' profit will eventually go negative as τ increases given that $\frac{du(s^*(\tau,n))}{d\tau} < 0$ when $\tau > \frac{c}{n}F^{-1}(1 - \frac{cm}{(m-n)v})$. Therefore, $\tau^*(n) = \max\{\tau : u(s^*(\tau, n)) = 0\}$. Since $u(s^*(\tau, n)) \geq 0$ for all $\tau \in [0, \tau^*(n)]$ and decreases linearly in τ for $\tau > \tau^*(n)$, the equation $u(s^*(\tau, n)) = 0$ has one and only one nonzero solution. We can thus simplify the definition by writing $\tau^*(n) = \{\tau > 0 : u(s^*(\tau, n)) = 0\}$.

Last, this new definition of $\tau^*(n)$ makes sure that $n \leq s_0(\tau^*(n))$ because $s_0(\tau^*(n))$ is the largest s that gives $u(s) = 0$ by definition. Therefore, $s^*(\tau, n) = n$ still holds. We can then solve $u(s^*(\tau, n)) = \frac{s^*(\tau,n)}{z}\Delta(s^*(\tau, n))$ or equivalently $\Delta(s^*(\tau, n)) = \frac{v}{m}\,\mathbb{E}[\min\left\{D, F^{-1}(1 - \frac{cm}{(m-n)v}), \frac{\tau n}{c}\right\}] - \tau = 0$.

ii) For a fixed $n \in (\frac{m\,c}{v},\, m\left(1 - \frac{c}{v}\right)]$, we define

- $\tau_1(n) = \frac{v}{m}\,\mathbb{E}[\min\left\{D, F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)\right\}]$;
- $\tau_2(n) : \{\tau > 0 : \phi(\tau) = \frac{v}{m}\,\mathbb{E}[\min\left\{D, \frac{\tau n}{c}\right\}] - \tau = 0\}$.

By part (i) we know that $\tau^*(n)$ is either equal to $\tau_1(n)$ or given by $\tau_2(n)$.

We first show that $\tau_2(n)$ is finite and unique. Consider $\phi(\tau) = \frac{v}{m}\,\mathbb{E}[\min\left\{D, \frac{\tau\, n}{c}\right\}] - \tau$ and $\phi'(\tau) = \frac{v}{m}\,\frac{n}{c}\,(1 - F(\frac{\tau\, n}{c})) - 1$. Note that $\phi(0) = 0$ and $\phi'(0) > 0$ since $n > \frac{m\,c}{v}$. For large τ, $\phi'(\tau) < 0$ as $\phi''(\tau) = -\frac{v}{m}\,\frac{n^2}{c^2}\,f(\frac{\tau\, n}{c}) < 0$ for all $\tau \geq 0$. Therefore, there exists exactly one $0 < \tau < \infty$, which is $\tau_2(n)$, that gives $\phi(\tau) = 0$. Also note that $\phi'(\tau_2(n)) < 0$ and we will use this result in the proof of Proposition 13.

Next, let's find out the expression of $\tau^*(n)$ for $n \in (\frac{m\,c}{v}, m\left(1 - \frac{c}{v}\right)]$. Let $g(n) = \frac{\tau_1(n)n}{c} - F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)$ and note that $g(n) > 0$ means $\tau^*(n) = \tau_1(n)$. If $g(n) = 0$, then $F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right) = \frac{\tau_1(n)n}{c}$ and thus $\mathbb{E}[\min\left\{D, F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)\right\}] = \mathbb{E}[\min\left\{D, \frac{\tau_2(n)n}{c}\right\}]$, which by definition implies that $\tau_1(n) = \tau_2(n) = \tau^*(n)$. Also, $g(n) < 0$ means $\tau^*(n) \neq \tau_1(n)$ and thus $\tau^*(n) = \tau_2(n)$. We will first look at $n \in (\frac{m\,c}{v}, \frac{m}{2}]$ and then $n \in (\frac{m}{2}, m\left(1 - \frac{c}{v}\right)]$ ($v > 2c$ guarantees that $\frac{m\,c}{v} < \frac{m}{2} < m\left(1 - \frac{c}{v}\right)$).
Consider $n \in (\frac{m\,c}{v}, \frac{m}{2}]$. Note that $g(\frac{m\,c}{v}) = \mathbb{E}[\min\left\{D, F^{-1}(\frac{v-2c}{v})\right\}] - F^{-1}(\frac{v-2c}{v}) < 0$ and we now show that $g(\frac{m}{2}) > 0$. Let $r = \frac{v}{c}$ and we know that $r > 2$. Define $\tilde{g}(r) = g(\frac{m}{2}) = \frac{v}{2c}\,\mathbb{E}[\min\left\{D, F^{-1}\left(1 - \frac{2c}{v}\right)\right\}] - F^{-1}\left(1 - \frac{2c}{v}\right) = \frac{r}{2}\,\mathbb{E}[\min\left\{D, F^{-1}\left(1 - \frac{2}{r}\right)\right\}] - F^{-1}\left(1 - \frac{2}{r}\right)$. When $r = 2$, $\tilde{g}(2) = 0$. For $r \geq 2$, $\tilde{g}(r)$ increases in r as $\tilde{g}'(r) = \frac{1}{2}\,\mathbb{E}[\min\left\{D, F^{-1}\left(1 - \frac{2}{r}\right)\right\}] + \frac{r}{2}\left[1 - FF^{-1}\left(1 - \frac{2}{r}\right)\right]\frac{d}{dr}F^{-1}\left(1 - \frac{2}{r}\right) - \frac{d}{dr}F^{-1}\left(1 - \frac{2}{r}\right) = \frac{1}{2}\,\mathbb{E}[\min\left\{D, F^{-1}\left(1 - \frac{2}{r}\right)\right\}] > 0$ for $r \geq 2$. Therefore, $g(\frac{m}{2}) = \tilde{g}(r) > 0$ for all $r > 2$.
Next note that

$$
\begin{aligned}
g'(n) &= \frac{\tau_1(n)}{c} + \frac{v\,n}{c\,m}(1 - FF^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right))\frac{d}{dn}F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)] \\
&\quad - \frac{d}{dn}F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right) \\
&= \frac{v}{cm}\,\mathbb{E}\left[\min\left\{D, F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right)\right\}\right] + \frac{2n-m}{m-n}\frac{d}{dn}F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right) \qquad (34)
\end{aligned}
$$

Since $\frac{d}{dn}F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right) < 0$, when $n \leq \frac{m}{2}$, $g'(n) > 0$. Therefore, there must exist a unique $\hat{n} \in (\frac{m\,c}{v}, \frac{m}{2})$ such that $g(\hat{n}) = 0$. This means that $\tau^*(n) = \tau_2(n)$ for $n \in (\frac{m\,c}{v}, \hat{n})$, $\tau^*(n) = \tau_1(n)$ for $n \in (\hat{n}, \frac{m}{2}]$, and $\tau^*(n) = \tau_1(n) = \tau_2(n)$ when $n = \hat{n}$.

For $n \in (\frac{m}{2}, m\left(1 - \frac{c}{v}\right)]$, we have $g(m\left(1 - \frac{c}{v}\right)) = \frac{v-c}{c}\mathbb{E}[\min\left\{D, F^{-1}(0)\right\}] - F^{-1}(0) = 0$ and $g'(m\left(1 - \frac{c}{v}\right)) = 0 + \frac{2n-m}{m-n}\frac{d}{dn}F^{-1}\left(1 - \frac{c\,m}{(m-n)v}\right) < 0$ by (34). Since we have shown that

$g(\frac{m}{2}) > 0$, there must be either zero or more than one $\hat{n} \in (\frac{m}{2},\, m\left(1-\frac{c}{v}\right))$ such that $g(\hat{n}) = 0$. To rule out multiple zeros in the range of $n \in (\frac{m}{2},\, m\left(1-\frac{c}{v}\right)]$, a sufficient condition is that $g''(n) < 0$ for $n \in (\frac{m}{2},\, m\left(1-\frac{c}{v}\right)]$. We can find $g''(n)$ from (34) and, after some algebra, simplify it as

$$g''(n) = -\frac{c\,m}{f(F^{-1}(y))(m-n)^4 v}\left[3n + \frac{(2n-m)cm}{(m-n)v} \cdot \frac{f'(F^{-1}(y)}{(f(F^{-1}(y))^2}\right], \tag{35}$$

where $y = 1 - \frac{c\,m}{(m-n)v}$.

Last, we find a sufficient condition for $g''(n) < 0$ for $n \in (\frac{m}{2},\, m\left(1-\frac{c}{v}\right)]$ or equivalently $y \in [0, 1-\frac{2c}{v})$. By (35), to make $g''(n) < 0$, it suffices to have $3n + \frac{(2n-m)cm}{(m-n)v} \cdot \frac{f'(F^{-1}(y)}{(f(F^{-1}(y))^2} > 0$, or

$$\frac{f'(F^{-1}(y)}{(f(F^{-1}(y))^2} > -\frac{3n(m-n)v}{(2n-m)cm}. \tag{36}$$

Let $\frac{n}{m} = k$. Then $k = 1 - \frac{c}{(1-y)v}$ and we look at $k \in (\frac{1}{2},\, 1-\frac{c}{v}]$. Then, the right hand side of (36) is equal to $-\frac{3v}{c} \cdot k \cdot \frac{1-k}{2k-1}$. Therefore, under our assumption, (36) holds.

□

Proof of Proposition 13

By Proposition 12, we know that there exists a unique $\hat{n} \in (\frac{m\,c}{v},\, \frac{m}{2})$ such that the following holds:

- $\frac{v\,\hat{n}}{c\,m}\,\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{c\,m}{(m-\hat{n})v})\right\}] = F^{-1}(1-\frac{c\,m}{(m-\hat{n})v})$;
- $F^{-1}(1-\frac{c\,m}{(m-\hat{n})v}) = \frac{\tau^*(\hat{n})\hat{n}}{c}$.

We will first show that this $\hat{n}$ is a local maximum point. Differentiating the objective function (11) with respect to n, we have

$$\frac{d\Pi}{dn} = \frac{d\tau^*(n)}{dn} \cdot n + \tau^*(n) \,-\, c\,\frac{dQ^*(n)}{dn} + (m-n)\,\frac{d\mathbb{E}[\tau_{eq}(n)]}{dn} \,-\, \mathbb{E}[\tau_{eq}(n)]. \tag{37}$$

By part (i), we know that $\tau^*(n) = \mathbb{E}[\tau_{eq}(n)]$ and consequently simplify (37) as

$$\begin{aligned}\frac{d\Pi}{dn} &= n\,\frac{d\tau^*(n)}{dn} \,-\, c\,\frac{dQ^*(n)}{dn} + (m-n)\,\frac{d\mathbb{E}[\tau_{eq}(n)]}{dn} \\ &= n\,\frac{d\tau^*(n)}{dn} \,-\, c\,\frac{dQ^*(n)}{dn} + (m-n)\frac{v}{m}(1-F(Q^*(n)))\frac{dQ^*(n)}{dn} \\ &= n\,\frac{d\tau^*(n)}{dn} \,+\, [(m-n)\frac{v}{m}(1-F(Q^*(n))) - c]\frac{dQ^*(n)}{dn}.\end{aligned} \tag{38}$$

Let's now evaluate $\frac{d\Pi}{dn}$ at $n = \hat{n}$. We know that $\tau^*(\hat{n}) = \frac{v}{m}\,\mathbb{E}[\min\left\{D, F^{-1}(1-\frac{c\,m}{(m-\hat{n})v})\right\}]$ and $Q^*(\hat{n}) = Q^*(\tau^*(\hat{n}),\hat{n}) = \min\left\{F^{-1}(1-\frac{cm}{(m-\hat{n})v}), \frac{\tau^*(\hat{n})\,\hat{n}}{c}\right\} = F^{-1}(1-\frac{cm}{(m-\hat{n})v})$. Therefore, $(m-$

$\hat{n})\frac{v}{m}(1-F(Q^*(\hat{n})))-c$ vanishes. Hence,

$$\begin{aligned}
\left.\frac{d\Pi}{dn}\right|_{n=\hat{n}} &= \hat{n}\left.\frac{d\tau^*(n)}{dn}\right|_{n=\hat{n}} + 0 \\
&= \frac{v\,\hat{n}}{m}(1-F(Q^*(\hat{n})))\left.\frac{dQ^*(n)}{dn}\right|_{n=\hat{n}} \\
&= \frac{c\,\hat{n}}{m-\hat{n}}\left.\frac{dQ^*(n)}{dn}\right|_{n=\hat{n}} \qquad (39)
\end{aligned}$$

$Q^*(n)$ is not differentiable at $n=\hat{n}$ and thus $\frac{dQ^*(n)}{dn}\big|_{n=\hat{n}}$ does not exist. However, we've shown in the proof of Lemma 2 part iii) that given $\tau^*(\hat{n})$, $\frac{dQ^*(\tau^*(\hat{n}),n)}{dn}\big|_{n<\hat{n}} > 0$ and $\frac{dQ^*(\tau^*(\hat{n}),n)}{dn}\big|_{n>\hat{n}} < 0$. Therefore we know that $\lim_{n\to\hat{n}^-}\frac{d\Pi}{dn} > 0$ and $\lim_{n\to\hat{n}^+}\frac{d\Pi}{dn} < 0$, suggesting that $\hat{n}$ maximizes profit locally.

Last, we will show that $\hat{n}$ is the global maximum point by showing that (38) is negative for $n \in (\hat{n}, m\left(1-\frac{c}{v}\right)]$ and positive for $[\frac{m\,c}{v},\hat{n})$.

For $n \in (\hat{n}, m\left(1-\frac{c}{v}\right)]$, we have $F^{-1}(1-\frac{cm}{(m-n)v}) < \frac{\tau^*(n)\,n}{c}$, $Q^*(n) = F^{-1}(1-\frac{cm}{(m-n)v})$ so $(m-n)\frac{v}{m}(1-F(Q^*(n)))-c=0$. Since $\frac{d\tau^*(n)}{dn} = \frac{v}{m}\frac{d}{dn}\mathbb{E}[\min\left\{D, F^{-1}\left(1-\frac{c\,m}{(m-n)v}\right)\right\}] < 0$, (38) is negative.

Now for $n \in (\frac{m\,c}{v},\hat{n})$, we have $F^{-1}(1-\frac{cm}{(m-n)v}) > \frac{\tau^*(n)\,n}{c}$ and $Q^*(n) = \frac{\tau^*(n)\,n}{c}$.

$$\begin{aligned}
\left.\frac{d\Pi}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} &= n\left.\frac{d\tau^*(n)}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} + \left[(m-n)\frac{v}{m}(1-F(Q^*(n)))-c\right]\left.\frac{dQ^*(n)}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} \\
&= \frac{n\,v}{m}\left[1-F(Q^*(\hat{n}))\right]\left.\frac{dQ^*(n)}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} \\
&\quad + \left[(m-n)\frac{v}{m}(1-F(Q^*(n)))-c\right]\left.\frac{dQ^*(n)}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} \\
&= \left[(m-n+n)\frac{v}{m}(1-F(Q^*(n)))-c\right]\left.\frac{dQ^*(n)}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} \\
&= \left[v\left[1-F(Q^*(n))\right]-c\right]\left.\frac{dQ^*(n)}{dn}\right|_{\frac{m\,c}{v}<n<\hat{n}} \qquad (40)
\end{aligned}$$

Note that

$$\begin{aligned}
v\left[1-F(Q^*(n))\right]-c &= v\left[1-F(\frac{\tau^*(n)\,n}{c})\right]-c \\
&> v\left[(1-F(F^{-1}(1-\frac{cm}{(m-n)v}))\right]-c \\
&= \frac{cm}{m-n}-c \\
&> 0. \qquad (41)
\end{aligned}$$

and $\frac{dQ^*(n)}{dn}\Big|_{\frac{mc}{v}<n<\hat{n}} = \frac{\tau^*(n)}{c} + \frac{n}{c}\frac{d\tau^*(n)}{dn}\Big|_{\frac{mc}{v}<n<\hat{n}}$. Therefore, to show that (40) is positive, it suffices to show $\frac{d\tau^*(n)}{dn}\Big|_{\frac{mc}{v}<n<\hat{n}} > 0$. By Proposition 12, when $\frac{mc}{v} < n < \hat{n}$, $\frac{d\tau^*(n)}{dn} = \frac{v}{m}(1 - F(\frac{\tau^*(n)\,n}{c}))\left[\frac{\tau^*(n)}{c} + \frac{n}{c}\frac{d\tau^*(n)}{dn}\right]$. Rearranging, we have

$$\frac{d\tau^*(n)}{dn} = -\frac{\frac{v}{m}(1 - F(\frac{\tau^*(n)\,n}{c}))\frac{\tau^*(n)}{c}}{\frac{v}{m}(1 - F(\frac{\tau^*(n)\,n}{c}))\frac{n}{c} - 1} \tag{42}$$

The denominator of (42) is equal to $\phi'(\tau^*(n))$ where ϕ is defined in the proof of Proposition 12 and we've shown that $\phi'(\tau^*(n)) < 0$. Therefore, (42) is positive and this completes the proof. □

Proof of Proposition 14

The case where $s_0(\tau)$ does not exist is trivial. Suppose that $s_0(\tau)$ exists. When $n > s_0(\tau)$, by Lemma 2 part iii), we know that $s^*(\tau, n) = s_0(\tau)$ under sequential arrival. Now consider the case $n \leq s_0(\tau)$. We show in the proof of Lemma 2 part iii) that $u(0) < 0$ and $u(s)$ is continuous and crosses zero at most once for $s \in [0, s_0(\tau))$. Therefore, if $u(n) < 0$, then $u(s) < 0$ for all $s \in [0, n]$. This means that no $s \leq \min\{s_0(\tau), n\}$ satisfies the participation constraint and hence $s^* = 0$. On the other hand, if $u(n) \geq 0$, then $s = n$ satisfies the participation constraint.

To see why (15) is a sufficient condition for s^* speculators, let's first consider the $s^* - th$ speculator that arrives after $s^* - 1$ other speculators have bought a token each. She knows that if she buys a token, then she will be the last person to do so — either because there is no extra token for sale ($s^* = n$) or buying tokens after her is no longer attractive ($s^* = m\left(1 - \frac{c}{v}\right)$). Therefore, (15) guarantees non-negative utility for her. Next, the $(s^* - 1) - th$ speculator knows that even if $u(s^* - 1) < 0$, buying a token now would induce the $s^* - th$ speculator to buy a token later, eventually resulting in non-negative rewards. By induction, we see that it is always optimal to buy a token for prior speculators.

□

Proof of Corollary 1

Substituting the expression of τ^* in Proposition 3 part c) into part a), we see that n^* and $\tau^*(n^*)$ satisfy $\frac{n^*}{c}\tau^*(n^*) = F^{-1}(1 - \frac{c\,m}{(m-n^*)v})$. Therefore, given $\tau^*(n^*)$, we know that $n^* = \hat{s}(\tau^*(n^*))$ where $\hat{s}(\tau)$ is the unique maximum point of $u(\tau, s)$ as defined in the proof of Lemma 2 part iii). Additionally, since $u(\tau^*(n^*), n^*) = 0$, we know that n^* is the only value of s such that $u(\tau^*(n^*), s) = 0$. Therefore, by definition of s_0, the result follows.

□