Cryptotokens and cryptocurrencies: the extensive margin.*

Andrea Canidio †

First version: July 13, 2020. This version: January 29, 2021. Please check here for the latest version.

Abstract

The supply of cryptotokens or cryptocurrencies can be indefinitely expanded on the *extensive margin* by introducing new cryptotokens and cryptocurrencies. Here we propose a theoretical model in which this extensive margin is endogenous. We do so by considering the choice of entry and subsequent competitive dynamics among blockchain-based decentralized digital platforms, each having an associated cryptotoken. We find that, if there are developers who can self-finance the development of their platforms, then the equilibrium is a monopoly in which a single platform (and a single token) enters the market. If these developers are absent, then entry is possible only by holding an Initial Coin Offering (ICO). We show that ICOs weaken incentives, because in equilibrium there is a strictly positive probability that a developer who held an ICO will then liquidate all his tokens and hence stop the development of his platform. This, however, stimulates entry because each developer might become a monopolist with strictly positive probability. We show that, under certain conditions, welfare is higher when multiple developers enter via ICOs than when a single developer self-finance the development of the platform.

JEL classification: D25, O31, L17, L26

Keywords: Blockchain, Cryptocurrencies, Cryptotokens, Initial Coin Offering (ICO), seigniorage, innovation, tournaments, entry.

*I am grateful to Matus Drgon, Christian Ewerhart, Antonio Fatas, Kenan Huremović, Marteen van Oordt, and participants to the Oligo Workshop 2020, European Economic Association Congress 2020, IMT Internal Seminar, the Third Toronto Fintech Conference for their comments and suggestions.

†IMT school of advanced studies, Lucca, Italy; andrea.canidio@imtlucca.it

1 Introduction

In the opening paragraph of "Bitcoin: A Peer-to-Peer Electronic Cash System" (the Bitcoin whitepaper) Nakamoto (2008) writes

> Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. [...] What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

After stating his objective, Nakamoto (2008) then proceeds to introduce two innovations. The first one is Bitcoin, a new digital currency. The second, more important, is the *bitcoin protocol*, an open-source software allowing a network of anonymous, selfish participant to maintain a record of Bitcoin transactions. Because these transactions are grouped into "blocks" that are then "chained" (i.e., linked) together to form an immutable history, this technology became known as blockchain. Importantly, the bitcoin protocol also regulates the total number of bitcoins in existence in every period, which is set to increase over time at a decreasing rate so to never exceed 21 millions. At the onset of Bitcoin (in early 2009), Nakamoto created and kept to himself approximately 1 million Bitcoin, before ceasing to contribute to the development of the Bitcoin protocol in mid-2010.

Enterprising developers soon realized that blockchain technology can be used to maintain not only records of Bitcoin transactions, but any type of record.[1] This led to the creation of hundreds other *decentralized digital platforms*—where a decentralized digital platform is the network of users of a given blockchain based-protocol. In addition to several other cryptocurrencies (such as Monero, ZCash, Litecoin, ...), there are now several decentralized computing platforms (see Ethereum, EOS, Car-

[1] Occasionally a distinction is made between blockchain and *decentralized ledger technologies*, where blockchain refers to a specific way of maintaining a decentralized ledger. This distinction is not relevant for the purpose of this paper. Another distinction is between "blockchain" meaning the technology, and "the blockchain" meaning a specific application of the blockchain technology, usually the Bitcoin blockchain. Here we always mean the technology.

dano, NEO, Algorand, ...);[2] decentralized real-time gross settlement platforms (see Ripple, Stellar); decentralized marketplaces for storage and hosting of files (see SIA, Filecoin, Storj) or for renting in/out CPU cycles (see Golem); generic e-commerce decentralized digital platforms (see Openbazaar); decentralized prediction markets (see Augur, Gnosis), financial exchanges (see 0xproject), and financial derivatives (see MakerDAO); and many more.

Importantly, a decentralized digital platform can function only if some of its users perform costly actions—mining being the prime example. These users must be adequately rewarded, which is achieved via the creation of a specific blockchain-based token. The protocol powering the decentralized digital platform automatically allocates new tokens to the users who perform such costly actions. At the same time, the protocol specifies that the token is necessary in order to use the corresponding platform—usually as its internal currency. Finally, the supply of tokens is finite in every period, and is pre-specified at the protocol level. As a consequence, to the extent that the platform is used, its associated token will have positive value and therefore can be used to create incentives at the protocol level.[3]

This, in turns, implies that tokens can also be used to generate *off-protocols* incentives. For exampe, tokens can be used to raise funds in an Initial Coin Offering (ICO). In an ICO, the developer of a blockchain-based decentralized digital platform sells some of the associated tokens to investors, in exchange for capital to be used for the development of the platform. The first notable ICO was that of Ethereum in 2014, raising USD 2.3 million in approximately 12 hours. ICO activity exploded in 2017 and, especially, in 2018, with ICOs raising more that USD 6 billion in a single month (July 2018, from Lyandres, Palazzo, and Rabetti, 2018).[4] Furthermore, the sale of tokens not sold at ICO allows the developers of decentralized digital platofrom to profit from their work, despite the fact that these plaforms are open source and

[2] A decentralized computing platform can be seen as an operating system running over a network of computers rather than a single machine. Developers can then create software (which in this context are smart contracts) that is executed by the network rather than by a single machine.

[3] For an economic analysis of these incentives for the case of Bitcoin, see, for example Biais, Bisiere, Bouvard, and Casamatta (2019) and Huberman, Leshno, and Moallemi (2017).

[4] For comparison, in 2016 total Venture Capital investment in Europe was USD 4.7 billion (OECD, 2017).

free to use. This novel business model is called *seigniorage*.[5]

The introduction of decentralized digital platforms and the explosion ICOs raised important concerns. One in particular is the fact that blockchain-based tokens are simultaneously performing many functions: they regulate access to decentralized digital platforms, they allow to raise financing, they generate profits. In a traditional platform, instead, each of these functions can be performed by a different instrument (prices, debt, and equity, respectively). Because of this, the incentives faced by the developers of decentralized digital platforms may be far from optimal.

This paper contributes to the understanding of these incentives by studying theoretically the entry of competing decentralized digital platforms in the same market. A market here is defined by all decentralized digital platforms that allow users to perform a given action. Examples are the market for cryptocurrencies (i.e. the set of decentralized digital platforms that can be used to send and receive crypto-tokens with money-like properties), the market for decentralized computing platforms (i.e., the set of decentralized digital platforms that can be used to run smart contracts), the market for decentralized exchanges of various types (i.e., the set of decentralized digital platforms that can be used to trade a given object—could be CPU cycles, personal data, or various digital objects). Competition among different blockchain-based decentralized digital platforms is assumed winner-take-all, which is justified by the presence of strong network externalities. Because to each decentralized digital platform entering the market is associated a specific crypto-token, in our model the number of crypto-tokens in existence is endogenous.

In the model, at the beginning of the game each developer decides whether to hold an ICO, and, immediately after, whether to pay an entry cost. In case a developer did not hold an ICO, this entry cost can only be paid using the developer's own resources. In case a developer held an ICO, this entry cost can be paid using both the developer's own resources and the proceedings from the ICO. Importantly, if a developer held an ICO, then in every subsequent period a frictionless market

[5] See Canidio (2018). Seigniorage are profits earned by issuing currency, and is clearly not a novel concept. What is novel in this context is the fact that seigniorage can be used to finance innovation. Note that Howell, Niessner, and Yermack (2018) and Amsden and Schweizer (2018) show that projects that go through an ICO sell only about half of their tokens at ICO, with the rest being kept by the founding team. This indicates that projects that go through an ICO expect to sell as many tokens at ICO as on the market post-ICO.

for tokens opens, in which investors and the developer can buy and sell tokens.[6] All developers who paid the entry cost exert effort in the development of their respective platforms. The developer who exerts the highest effort is the winner, and his platform is the one adopted by users. After the winner is determined, all developers liquidate their tokens and exit the game, while users continue using the winning platform indefinitely. Our measure of welfare is the volume of transactions occurring in each period on the winning platform, which depends on the effort exerted by the winning developer.

To start, we show that competition is beneficial: having multiple competitors always leads to higher welfare than having a single competitor, although increasing the number of competitors beyond 2 does not always increases welfare. This reflects both on the value of the winning platform and on the total value of all tokens associated with the competing platforms. Our second result is that, as it is often the case, outside financing (here in the form of an ICO) weakens incentives. This weakening of incentives here takes a specific form: if a market for tokens is present, then, in equilibrium, with strictly positive probability each developer will liquidate all his tokens and stop the development of the protocol.[7] The intuition is that, if investors expect a developer to hold on to his tokens, then they should also expect this developer to exert high effort in the future, which implies that the price of the token associated with the developer's platform should be high. But then, the developer should sell all his tokens, so to "cash in" on his future effort before exerting any. Similarly, if investors expect low effort tomorrow, then the price of the developer's token will be low, which implies that the developer should hold on to most of his tokens and exert high effort tomorrow. Each developer is therefore engaged in a anti-coordination game with investors, which implies that the equilibrium must be in mixed strategies: each developer sells all his tokens on the market with strictly positive probability, and holds on to as many tokens as possible otherwise.

[6] Usually, tokens sold at ICO start trading on specialized financial exchanges immediately after the end of the ICO. Sometimes a lockup mechanism prevents those tokens from being traded. This lockup period can last between a few months to a year. Note, however, that sophisticated investors can circumvent it via the creation of future markets. Also, the length of this lockup period is minimal relative to time required to develop the platform

[7] This result is already in Canidio (2018), who however considers a single developer.

An important implication is that, if there is a developer who paid the entry cost without holding an ICO, this developer will for sure reach the final stage of the game. In this case, competition ensures that a second developer who pays the entry cost will earn zero profits in the following period. Hence, no other developer will want to pay the entry cost. If instead all developers who paid the entry cost also held an ICO, then each of these developers may liquidate all his tokens before reaching the final stage of the game. That is, when paying the entry cost, each developer knows that, with strictly positive probability, he may be the only developer reaching the final stage of the game. In this case, multiple developers may find it profitable to pay the entry cost.

Building on the above insight, we then solve for the equilibrium number of entrants. Depending on the developers' initial wealth, there are three cases. In the first one, there are developers who can self-finance the entry cost. In this case, no ICO occurs in equilibrium and a single developer enters the market. In the second case, all developers are very poor relative to the cost of entry, and there are no ICOs nor entry. Intuitively, a developer who is very poor will need to sell many tokens at ICO to raise enough resources to then pay the entry cost. But this leaves this developer with few tokens, which means that his future profits in case he pays the entry cost are low. As a consequence, for this developer paying the entry cost may not be incentive compatible.

The last case occurs for intermediate levels of wealth: developers are poor but not so poor to be unable to hold an ICO. We solve this case by assuming that all developers have the same initial wealth. We show that there is an equilibrium in which no ICO occurs, together with an equilibrium in which there are multiple ICOs. The reason is that, if investors believe that the developer will not have the incentive to pay the entry cost, then they will be unwilling to purchase tokens at ICO, which implies that the developer will indeed be unable to pay the entry cost. If investors instead expect high effort in the future, the price of the token will be high. Each developer will be able to keep a large amount of tokens at ICO (while simultaneously paying the entry cost), which implies that future effort will be high.

We then compare welfare in the three cases above. Clearly, the lowest level of welfare is achieved when all developers are extremely poor (case 2 above), or when

developers have an intermediate level of wealth but an inferior equilibrium with no ICOs nor entry emerges (case 3 above). However, the comparison between the case with no ICO and monopoly (case 1 above) and the case of multiple ICOs (case 3 above) is ambiguous. In case 1, a single developer will enter the market and reach the final stage of the game with probability 1. In case 3, multiple developers enter the market. Each of them has some probability of exiting the market prematurely. But it is also possible that multiple developers reach the final stage of the game—in which case competition guarantees a higher level of effort than in case 1. We show that, relative to no ICO and a monopoly, welfare is higher with multpile ICOs whenever developers are not too poor—that is, outside financing is present but limited. An interesting corollary is that increasing the cost of entering into the market may increase welfare. If the cost is such that some developers can pay it using their own funds, then in equilibrium there is a monopoly. If the cost increases (via, for example, a tax) then all developers may need to resort to an ICO to be able to pay it. This generates competition and, if this tax is not too large, also increases welfare relative to the monopoly case.

Literature

Competition, cryptocurrencies, and crypto-tokens. To the best of our knowledge, ours is the first paper to study entry and competition among decentralized digital platforms. However, few existing papers investigate related questions. For example, Gandal and Halaburda (2016) study empirically the price movements of various cryptocurrencies between May 2013 and July 2014. They find evidence of strong network effects and winner-take-all dynamics toward the end of their sample period, but not at the beginning. Also closely related are general-equilibrium models of competition between traditional currencies and cryptocurrencies (see Garratt and Wallace, 2018, Schilling and Uhlig, 2019, Benigno, Schilling, and Uhlig, 2019). Importantly for our purposes, these papers take as given both the choice of entry and the overall "quality" of these currencies. In addition, they focus exclusively on cryptocurrencies.

Tokens and decentralized digital platforms. The literature studying tokens and decentralized digital platforms has so far largely ignored the choice of entry of decentralize digital platform and the subsequent competitive dynamics.

Within this literature, the most closely related paper is a previous work of ours (Canidio, 2018), in which a developer can exert effort and invest funds in the development of a decentralized digital platform over several periods. The developer holds the initial stock of tokens and can choose when to hold an ICO. Following the ICO, in every period there is a frictionless market for tokens where investors and the developer himself can trade tokens. Relative to Canidio (2018), here we allow the developers to invest and exert effort only once. Also, the choice of when to hold the ICO is simplified to two options: either initially or before exiting the game. Of course, here the number of developers is endogenous and could be greater than one, while in Canidio (2018) there is a unique developer.

Also closely related are Cong, Li, and Wang (2019) and Goldstein, Gupta, and Sverchkov (2019). Cong, Li, and Wang (2019) build a model in which the owner of a decentralized digital platform continuously creates new tokens which can be either sold (and the proceedings consumed) or used to pay workers who will improve the value of the platform. In Goldstein, Gupta, and Sverchkov (2019) an entrepreneur chooses whether to create a decentralized digital platform or a traditional platform. Their main result is that creating a decentralized digital platform generates competition among the users of the (unique) platform. Here instead we study competition among platforms.

Sockin and Xiong (2018), Cong, Li, and Wang (2018), Bakos and Halaburda (2018), and Li and Mann (2018) consider a single decentralized digital platform, and argue that because of network externalities there could be coordination failures in its adoption. They study the role of tokens and they way they are sold in achieving the high-adoption equilibrium. Finally, a number of authors have studied ICOs held by firms that are not building decentralized digital platforms and may even completely unrelated to blockchain. In this case, a token may represent a voucher and therefore give the right to acquire a good or a service from the issuer, or may represent a claim on a business' revenues, or a claim on a business' profits. This use of blockchain-based tokens is studied in Catalini and Gans (2018), Chod and Lyandres (2018) and

Garratt and van Oordt (2019), Malinova and Park (2018). Again, all these papers study this problem by considering a single firm.

Contest theory and platform competition. The core of our model is a winner-take-all contest with asymmetric players and valuable effort. The main theoretical reference is therefore Siegel (2014), who provides conditions under which these types of contests have an equilibrium, and show that the equilibrium payoffs of all participants is the same in all equilibria of the game.

Finally, the literature studying competitions among (traditional) platforms has focused mostly on the resulting equilibrium prices (see, for example, the seminal work by Rochet and Tirole, 2003, Armstrong, 2006, and Caillaud and Jullien, 2003). Here this issue is not present because decentralized digital platforms are free provided that the corresponding tokens is used. Hence, profits are generated exclusively by the sale of tokens. Despite this, our research question is related to Kristiansen and Thum (1997), who study R&D choice when there are network externalities. In their model, however, network extrnalities are at the market level—users benefit of using a product depends on the total number of users of all products in the market—while here the user of each platform cannot interact with users on a different platform.

2 The Model

The economy is composed of a large mass of developers, a large mass of risk-neutral price-taking investors, and a large mass of users. Developers are heterogeneous in their initial wealth a^i, but are identical in all other respects. Each developer i entering the market creates his own platform (also indexed by i) and establishes that all transactions using his/her platform must be conducted using a specific token (also indexed by i) with total supply M, fully owned by the developer at the beginning of the game.[8] The development of the protocol lasts 2 periods. In the first one, each developer invests $I^i \in \{0, C\}$, where we interpret $C > 0$ as a market-entry cost. In the second one, each developer exerts effort e^i, which is productive only if he/she

[8] As we will show later, equilibrium actions, payoffs and prices are independent of M, provided that it is strictly positive and finite. We therefore treat M as a parameter common to all developers rather that a choice variable.

previously paid the entry cost. All developers exit the game at the end of period 2.

Each developer can choose to hold an ICO either at the beginning of the game (in period $t = 0$) or before exiting the game (in period $t = 2$). An ICO is modeled as an auction, in which a developer sells some tokens to investors. If developer i held an ICO in period t, then at the end of every subsequent period a frictionless market for token i opens. In this market, investors and developer i can trade token i. Developers and investors can also hold a risk-free asset yielding a per-period gross return $R \geq 1$.

From period 3 onward, all users adopt a single decentralized digital platform. We call such platform the winning platform w, which we define in the next paragraph. More precisely, in every $t > 3$ first the market for token w opens and then users use the winning platform. See Figure 1 for a graphical representation of the timeline.

Investors. Investors are risk-neutral profit maximizers with no cash constraints. They can purchase tokens in every period and sell them during any subsequent period. Importantly, when buying or selling tokens on the market, they are price takers: their net demand for tokens in period t depends on the sequence of token prices from period t onward, which they take as given.

Call p_t^i the price of token i in period t, which could be determined on the market or in an ICO. Investors are indifferent between purchasing any amount of tokens i in period t whenever they expect the token to yield the risk-free return, that is whenever $p_t^i = \max_{s>t} \left\{ E[\frac{p_s^i}{R^{s-t}}] \right\}$. If instead $p_t^i > \max_{s>t} \left\{ E[\frac{p_s^i}{R^{s-t}}] \right\}$, then the investors' demand for tokens i in period t is zero. Finally, if $p_t^i < \max_{s>t} \left\{ E[\frac{p_s^i}{R^{s-t}}] \right\}$, then the investors' demand for token i in period t is not defined.

Users. Because of network externalities, from $t = 3$ onward, all user will use the winning platform to transact with each other. To do so, in every period they first purchase token w, and then use it to transact with other users on platform w. The total value (in US dollars) of all exchanges occurring on the wining platform during a given period is the *value of the winning platform* and is equal to the developer's effort e^w. This assumption is meant to capture in a parsimonious way the fact that the developer's effort generates an improvement of the platform (i.e., lower

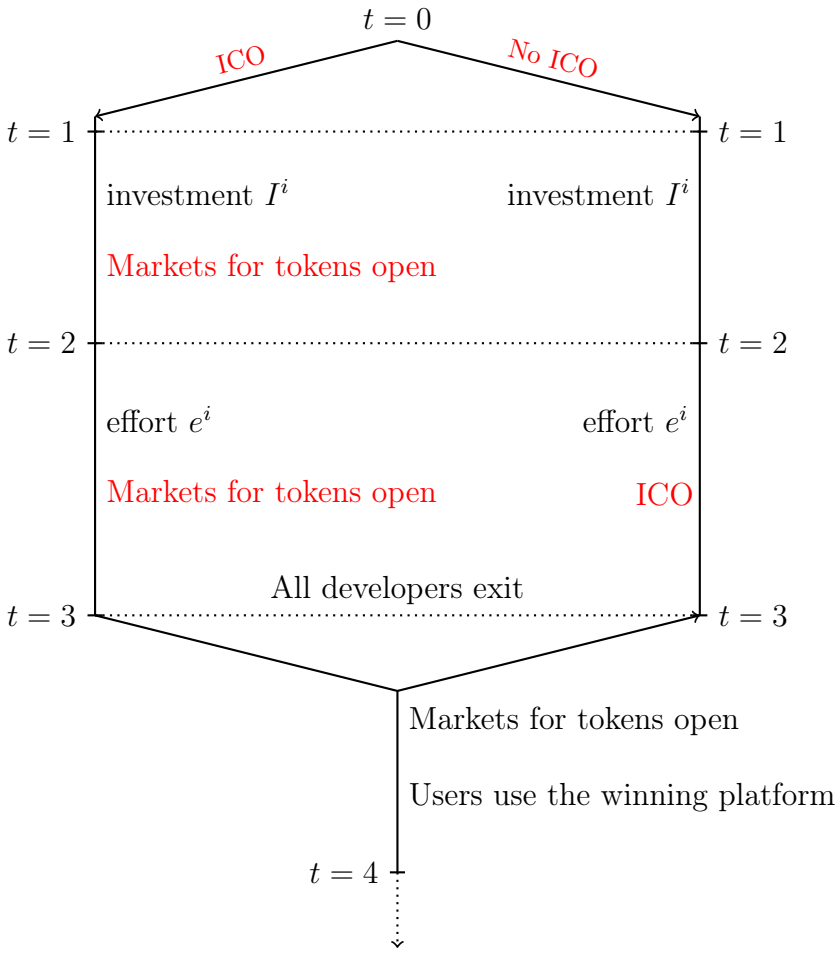

Fig. 1: Timeline

transaction costs, enhanced ease of use, increased security and reliability), which in turns allows more users to use the platform and perform more/larger transactions.

We abstract away from possible coordination failures by assuming that users use the platform with the highest value, so that

$$w \equiv \text{argmax}_i\{e^i\}$$

In case more then one platform have the same, highest value, then a tie breaking rule determines which platform is the winner (the exact nature of this tie breaking rule is irrelevant for the calculations below).

Finally, each user can access the market for tokens only once in every period.[9] This implies that, in every $t \geq 3$, those who use the winning protocol to purchase goods and services have a demand for tokens equal to $\frac{e^w}{p_t^w}$, while those who use the protocol to sell goods or services have a supply of tokens in period $t+1$ equal, again, to $\frac{e^w}{p_t^w}$.

The developers. Call Q_t^i the stock of token i held by developer i at the beginning of period t. Each developer maximizes the total cash at the end of life minus a cost of effort $\frac{(e^i)^2}{2}$.

It follows that, in period 2, a developer sets effort e^i so to maximize

$$U_2^i \equiv p_2^i Q_2^i - \frac{(e^i)^2}{2}.$$

Given this, in period 1 each developer chooses $Q_2^i \in [0, M]$ and $I^i \in \{0, C\}$ so to maximize

$$U_1^i \equiv U_2^i + \left((a^i + p_0^i(M - Q_1^i))R - I^i - p_1^i(Q_2^i - Q_1^i)\right) R$$

subject to a cash constraint

$$(a^i + p_0^i(M - Q_1^i))R \leq I^i + \max\left\{p_1^i(Q_2^i - Q_1^i), 0\right\}. \tag{1}$$

Note that $p_0^i(M - Q_1^i)$ are the proceeds of the ICO, invested in the risk free asset in period 0 together with the initial wealth. Hence, the term $(a^i + p_0^i(M - Q_1^i))R$ represents the developer's wealth at the beginning of period 1. Note also that if $p_1^i(Q_2^i - Q_1^i) > 0$, then this term represents the resources spent by the developer to purchase his own token on the market in period 1 (which matters for the cash

[9] That is, the winning token has velocity 1. Assuming a different, exogenous velocity will introduce an additional parameter without affecting the results. The velocity of tokens could, however, be endogenous as in Prat, Danos, and Marcassa (2019). As we will see later, the important element here is that the price of the winning token increases with the effort exerted by the winning developer. We believe that this result (and, as a consequence, all results presented here) extends to the case in which the velocity of the token is endogenous. Endogenizing the velocity of the token however opens the possibility that developers may try to manipulate the price of tokens by taking actions that do not affect the value of their platform but rather the velocity of the related token. We plan to explore this possibility in future work.

constraint).[10] If instead $p_1^i(Q_2^i - Q_1^i) < 0$ then this term represents the resources earned by selling additional tokens on the market in period 1.

The cash constraint therefore says that the agent wealth at the beginning of period 1 cannot exceed the amount invested I^i plus the amount spent to purchase tokens on the market. Also, the term $(a^i + p_0^i(M - Q_1^i))R - I^i - p_1^i(Q_2^i - Q_1^i)$ is the developer's total wealth at the end of period 1, after choosing $Q_2^i \in [0, M]$ and $I^i \in \{0, C\}$. This wealth earns the risk-free return and is consumed at the end of period 2. Finally, if there was no ICO in period 0, then the period-1 maximization problem is subject to the additional feasibility constraint $Q_1^i \equiv M$.

In period 0, the developer chooses whether to hold an ICO and how many tokens to sell at ICO so to maximize his continuation utility U_1^i. We assume full information, so that whether a developer paid the entry cost, his/her effort, and his/her token holdings are observable by investors, users, and other developers.

Equilibrium. We solve the model by backward induction, starting from the price of the winning token, then moving to solving for the equilibrium effort, the market equilibrium in period 1 (if an ICO occurred), the choice of paying the entry cost, and finally the choice of whether to hold an ICO.

As we will see, at each stage there may be multiple equilibria. When this is the case, we apply a forward induction refinement: at the beginning of the subgame, we allow a single developer to take a useless-but-costly action, which is observable by other developers but not by investors nor users.[11] Ben-Porath and Dekel (1992) show that this developer is able to "signal his future action." The intuition is that, by bearing an additional cost, this developer can credibly commit to choosing the equilibrium strategy of his preferred equilibrium. Because the other developers ob-

[10] This possibility emerges because, at ICO, a developer could sell more tokens than what necessary to pay the entry cost, invest the proceeding in the risk free asset and then purchase back some of his tokens on the market in period 1. As we will show later, without loss of generality, we can focus on equilibria in which this never happens. The reason is that, in equilibrium, the return on holding tokens is the same as holding the risk free asset.

[11] In the literature, this a useless-but-costly action is usually assumed to be "money burning". The problem with this interpretation is that if a developer's cash constraint is binding, then this developer has no money to burn. The forward induction logic, however, applies to any form of action that generates a cost to the player but has no impact on the payoffs of the game. For example, there could be a second dimension of effort that has no impact neither on quality of the decentralized platform but is nonetheless observed by the other developers.

serve this, they will therefore coordinate on the equilibrium chosen by the developer who took the costly action. Interestingly, this works also if no useless-but-costly action is taken on the equilibrium path. Also, these actions are not observable by investors and hence can be used only to coordinate the equilibrium strategies of developers, and not to manipulate the price of the token (which depends on the investors' beliefs over the developers future actions).

For each developer, therefore, the possibility of taking a useless-but-costly action restricts the set of possible equilibria to a subsect of the full set of equilibria. In our refinement, we consider the union of these subsets. That is, we check, for each developer, which equilibria are eliminated when only this developer is allowed to take a useless-but-costly action, and then consider all the surviving equilibria as plausible.[12] If multiple equilibria survive this refinement, then we focus on the symmetric equilibrium: the equilibrium in which identical developers play identical equilibrium strategies.

3 Solution

3.1 Price of tokens from period 2 onward

We start by solving for the price of the token associated with the winning platform. The fact that no development is possible after period 2 implies that the price of the token associated with the winning platform must be constant from period 2 onward. Investors are therefore unwilling to hold any token. Because the demand for tokens originates exclusively from users, from period 2 onward the price of the winning token is:

$$p_2^w = \frac{e^w}{M}. \tag{2}$$

Note that the above equation is a version of the equation of exchange, used in macroeconomics to link money supply (here M), economic activity (here e^w), price

[12] When multiple players are allowed to useless-but-costly actions, then Ben-Porath and Dekel (1992) show that their ability to select an equilibrium depends on the order in which those actions are taken.

level, and velocity of money (here assumed 1).[13] With respect to the non-winning platforms, because they are not used, their associated tokens have prices equal to zero.

Before continuing with the derivation of the solution, an important observation. The presence of the investors guarantees that, if a token is traded on the market in period 1, in equilibrium it must be that

$$p_1^i = \frac{E[e^i]}{R \cdot M} \cdot \text{pr}\{i = w\},$$

and if a token is sold at ICO in period 0, in equilibrium it must be that

$$p_0^i = \frac{E[e^i]}{R^2 \cdot M} \cdot \text{pr}\{i = w\}.$$

The important observation is that what is known by investors and hence is used to compute the expectation changes from period 0 to period 1. In an ICO, the developer announces the supply of tokens and investors submit bids. The developer's announcement is used to compute the expectation, and hence determines the token price at ICO. On the market, instead, investors are price takers, which implies that their demand for tokens depends exclusively on p_1 and $E[p_2]$, and not on the quantity of tokens sold by the developer in period 1.[14] To say it differently, in period 1 investors form an expectation with respect to future effort that does not depend on period-1 supply of tokens. This expectation is correct in equilibrium (that is, for the equilibrium supply of tokens in period 1 and subsequent effort) but will not react to deviations from the equilibrium. From the developers view point, therefore, the supply of tokens in period 1 does not affect the equilibrium price for tokens *in that period*. However, as we will see, the supply of tokens in period 1 determines the developers' effort, and hence the price of the token in period 2.

[13] Using the the equation of exchange to determine the price of cryptocurrencies is also in Bolt and Van Oordt (2020).

[14] Of course, the equilibrium price will be such that demand equals supply; the point is simply that in a price-taking environment the demand cannot be a function of the supply.

3.2 Equilibrium effort

Consider the choice of effort in period 2. We order the developers so that the first $n \geq 0$ are that active ones, that is, those who paid the entry cost. Of those, the first $r \in \{0, ..., n\}$ are $r$rich: they paid the entry cost without holding the ICO in period 0. The subsequent $n - r$ are poor: they paid the entry cost and held the ICO in period 0.

In period 2 all developers will sell their entire stock of tokens. Given this, when choosing the optimal level of effort, developer $i \leq n$ chooses e^i to maximize

$$\begin{cases} \frac{Q_2^i \cdot e^i}{M} - \frac{(e^i)^2}{2} & \text{if } e^i > e^j \ \forall j \neq i \\ -\frac{(e^i)^2}{2} & \text{otherwise} \end{cases}$$

The developers are therefore engaged in an asymmetric contest with productive effort, as studied in Siegel (2014). Note that $\frac{Q_2^i}{M}$ is the optimal effort whenever developer i expects to win with probability one. Instead $\frac{2Q_2^i}{M}$ is the effort level at which a developer's utility is zero even if he wins with probability 1. Call the developer with the highest Q_2^i the $l$eader and the developer with the second-highest Q_2^i the $f$ollower.[15] Define $Q^l \equiv \max_i Q_2^i$ and $Q^f \equiv \max_{i \neq l} Q_2^i$ as the tokens held by leader and follower, respectively.

When $2Q^f \leq Q^l$ the leader's unconstrained optimal effort is larger then the follower's largest possible effort. In this case, in the unique equilibrium of the game, the leader will set effort equal to his unconditional optimal level and earn

$$\frac{1}{2}\left(\frac{Q^l}{M}\right)^2,$$

while all other developers earn zero. If instead $2Q_2^f > Q^l$, then the leader's unconstrained optimal effort is strictly below the follower's largest possible effort. In this case, there are multiple mixed-strategy equilibria. However, by Theorem 1 in Siegel

[15] Whenever leader and follower have the same Q_2^i, we say that there are multiple leaders. Although we do not explicitly mention it, our results extend to this case as well. See, in particular, Equation (3) in Proposition 1.

(2014), in every equilibrium of the game the leader's utility is

$$\frac{2Q^f\left(Q^l - Q^f\right)}{M^2}.$$

That is, the leader's utility is equal to the utility he would achieve if he'd set his effort equal to the follower's largest possible effort.[16] Also here, the utility of all other developers is zero. The following proposition summarizes these results.

Proposition 1 (Period 2 utility)**.** *Define* $\mathbf{Q}^i = \max_{j\neq i}\{Q_2^j\}$*. In all equilibria of the period-2 effort game, developer* i*'s utility is*

$$U_2^*(Q_2^i, \mathbf{Q}^i) = \begin{cases} 0 & \text{if } \mathbf{Q}^i \geq Q_2^i \\ \frac{2\mathbf{Q}^i\left(Q_2^i - \mathbf{Q}^i\right)}{M^2} & \text{if } \mathbf{Q}^i < Q_2^i < 2\mathbf{Q}^i \\ \frac{1}{2}\left(\frac{Q_2^i}{M}\right)^2 & \text{otherwise .} \end{cases} \tag{3}$$

Proof. By direct application of Siegel (2014), Theorem 1. □

See Figure 2. For future reference, note that, given the shape of $U_2^*(Q^i, \mathbf{Q}^i)$, randomizing over values of Q_2^i makes the developer better off, strictly so when i could be both a leader and a follower depending on the realization Q_2^i.

To derive the equilibrium period-2 prices of tokens, we again distinguish between two cases. As already mentioned, if $2Q^f \leq Q^l$ there is a unique equilibrium in pure strategy: the leader sets effort equal to $\frac{Q^l}{M}$ and wins with probability 1; all other developers set effort equal to zero. The leader's token price is

$$p_2^l = \frac{Q^l}{M^2}.$$

All other developers' tokens have price equal to zero.

If instead $2Q^f > Q^l$, then multiple, mixed strategies Nash equilibria exist. To each equilibrium of the game corresponds the same equilibrium payoffs, but a different distribution of effort by leader and follower, and expected prices of tokens

[16] This result is also in Siegel (2009), in which however only non-productive effort is considered. Siegel (2014) extends these results to cases in which, over some range, the "prize" to be won by a player may be increasing in this player's effort. Note also that the fact that the equilibrium payoffs are the same in all equilibria implies that our forward-looking equilibrium refinement is mute.

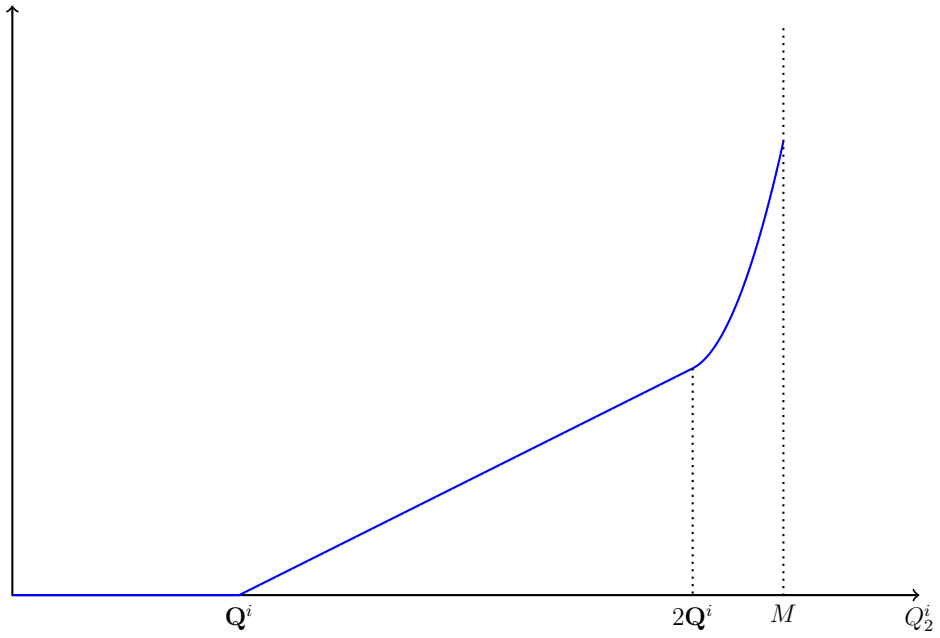

Fig. 2: Player i's payoff in period 2, as a function of Q_2^i.

(where the expectation is taken at the beginning of period 2 with respect to effort). Deriving the full set of equilibrium effort is, in general, quite convoluted. However, there is a particular case that will be relevant on the equilibrium path and that we can explicitly solve: the case in which either a developer holds a given amount of tokens, or he holds no tokens.

Proposition 2 (Prices in period 2)**.** *Suppose that for $i \leq k \leq n$ we have $Q^i = Q^l$, while for $k < i \leq n$ we have $Q^i = 0$. If $k \geq 2$, then set of equilibria of the game can be characterized by a $z \in \{2, ..., k\}$ such that z developers randomize over $\left[0, \frac{2Q^l}{M}\right]$, while the remaining developers set effort equal to zero with probability 1. Furthermore, the expected value of the winning platform is:*

$$E[e^w] = \frac{z}{2z-1}\left(\frac{2Q^l}{M}\right),$$

where the expectation is taken at the beginning of period 2, before effort is set. If $i \leq z$ then

$$E[p_2^i] = \frac{1}{2z-1}\left(\frac{2Q^l}{M^2}\right),$$

otherwise $E[p_2^i] = 0$.

An important consequence of the above proposition is that, going from a single active developer to multiple active developers always increases the value of the winning platform: that is, in any equilibrium with $k \geq 2$ the expected value of the winning platform is larger than with $k = 1$. Conditional on having more than 2 active developers, the value of the winning platform is maximized when only two developers take part in the competition, while all other developers set effort equal to zero.

As already discussed, here we focus on the symmetric equilibrium. In this equilibrium, whenever there are $k > 1$ leaders and all other developers have zero tokens, then all k developers randomize. The value of the winning platform is given in Proposition 2, for the case $z = k$. If instead $k = 1$ the unique leader sets effort equal to $\frac{Q^l}{M}$ with probability 1. Finally, if $k = 0$ then no developer will exert effort and the value of the winning platform will be zero. We can therefore write the expected value of the winning platform in the symmetric equilibrium as a function of k as:

$$E[e^w] = \frac{2k}{2k - \mathbb{1}\{k \neq 1\}} \left(\frac{Q^l}{M}\right). \tag{4}$$

where $\mathbb{1}$ is the indicator function, so that $\mathbb{1}\{k \neq 1\}$ takes value 1 if $k > 1$ or $k = 0$, and zero if $k = 1$. We can similarly write the price of tokens in the symmetric equilibrium as:

$$E[p_2^i] = \begin{cases} \frac{2}{2k - \mathbb{1}\{k \neq 1\}} \left(\frac{Q^l}{M^2}\right) & \text{if } i \leq k \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

In this class of equilibria, competition has a non-monotonic effect on the value of the winning platform: the expected value of the winning platform increases with k for $k \leq 2$, but decreases with k for $k \geq 2$. Finally, a fact that we will use extensively is that the expected value of all tokens is equal to the expected value of the winning platform, that is:

$$M \sum_i E[p_2^i] = E[e^w]. \tag{6}$$

3.3 Sale of tokens in period 1

Consider now the choice of Q_2^i, that is, for the developers who held an ICO, how many tokens to sell on the market in period 1. For given p_1^i, this choice solves

$$\max_{Q_2^i \in [0, \bar{Q}^i]} \left\{ p_1^i (Q_1^i - Q_2^i) R + E\left[U_2^*(Q_2^i, \mathbf{Q}^i) \right] \right\}$$

where

$$\bar{Q}^i = \max\{Q_1^i \leq M | \ \ (a^i + p_0^i (M - Q_1^i)) R \leq I^i + \max\{p_1^i (Q_2^i - Q_1^i), 0\}\} \tag{7}$$

that is, $\bar{Q}^i$ is the largest $Q_2^i \leq M$ satisfying the developer's cash constraint (1). Note that $p_1^i (Q_1^i - Q_2^i)$ is the amount earned by selling tokens in period 1, while $E\left[U_2^*(Q_2^i, \mathbf{Q}^i)\right]$ is developer i's expected period 2 utility (as defined in Proposition 3), where the expectation is taken with respect to $\mathbf{Q}^i$ (developer i's opponents may be randomizing).

The fist observation is that if there is at least one rich developer $j \leq r$, then for all other developers $i \neq j$ we have $\mathbf{Q}^i = M$ and their continuation utility is zero. In this case, all tokens that are traded in period 1 (those belonging to poor developers) must have price equal to zero, as the next proposition shows.

Proposition 3. *Suppose that $r > 0$. Then, in equilibrium, every developer $i \in \{r+1, ..., n\}$ chooses $Q_2^i = 0$ so that $e^i = 0$ and $p_1^i = p_2^i = 0$.*

The intuition for the above result is quite straightforward. If developer i holds enough tokens in period 2, he may be expected to set strictly positive effort with some probability. But then, the period-1 price of his token should be strictly positive. This, however, cannot be an equilibrium: if $\mathbf{Q}^i = M$, developer i is better off selling all his tokens in period 1 (and earn strictly positive payoff) rather than holding tokens until period 2 (and earn zero). In equilibrium, therefore, it must be that $Q_2^i = 0$, so that effort is zero in period 2.[17]

[17] Note that effort could be zero also if $Q_2^i > 0$ but low. Hence, whereas period-2 effort, period 1 price and period 2 price are zero in every equilibrium, the equilibrium token holding is not uniquely identified.

By the above proposition, only rich developers will be active on the market in period 2. Proposition 2 then directly implies the following corollary.

Corollary 1. *If $r > 0$, then in a symmetric equilibrium the expected value of the winning platform is given by* (4) *and the price of tokens is given by* (5)*, with $k = r$ and $Q^l = M$.*

Consider now the case $r = 0$ and $n > 0$, that is, all active developers are poor. Two observations are important here. First, because $U_2^*(Q_2^i, \mathbf{Q}^i)$ is convex in Q_2^i, also $E\left[U_2^*(Q_2^i, \mathbf{Q}^i)\right]$ is convex in Q_2^i, strictly so if developer i is the only leader for some Q_2^i and some realizations of $\mathbf{Q}^i$.[18] This implies that the developer's maximization problem can only have corner solutions: he sets either $Q_2^i = 0$, or $Q_2^i = \bar{Q}^i$ (as defined in 7), or he randomizes between these two values.

Second, p_1^i must be such that investors are indifferent between purchasing tokens or the risk free asset. This gives rise to an anti-coordination problem between investors and each developer. The reason is that if investors expect developer i to hold on to his tokens and exert high effort tomorrow, this should already be priced into p_1^i. But then this developer should sell all his tokens in period 1 and invest in the risk free asset. This way, he can benefit from his future effort without exerting any. Similarly, if investors expect a developer to hold no tokens in period 2, then the period-1 price of this token should be zero. But then, as long as this developer can be the leader with positive probability in period 2, such developer should hold on to all his tokens.

These two observations imply that, in equilibrium, all developers will randomize between holding the maximum amount of tokens (and therefore putting high effort in the following period) or no tokens (and therefore putting no effort in the following period), as the next proposition shows.[19]

[18] To see this, consider a specific Q_2^i and $\mathbf{Q}^i$. By Proposition 1, we can write $\alpha U_2(x, \mathbf{Q}^i) + (1 - \alpha)U_2(y, \mathbf{Q}^i) \geq U_2(\alpha x + (1-\alpha)y, \mathbf{Q}^i)$ for all $x, y \in [0, Q_1^i]$ and $\alpha \in [0, 1]$. Furthermore, the inequality will be strict if i is the leader at x but not at y (or vice versa). To establish that $E\left[U_2^*(Q_2^i, \mathbf{Q}^i)\right]$ is convex, it is enough to integrate both sides over the possible values of $\mathbf{Q}^i$.

[19] A note on our forward-looking equilibrium selection criterion. In every possible equilibria, developers are indifferent between selling all their tokens or holding on to all their tokens. Hence, in all equilibria, a developer i's payoff is equal to $p_1^i Q_1^i R$ (i.e., what he would earn if he sold all his tokens in period 1). Because, by assumption, the useless-but-costly action is not observable by investors, this action does not affect the period 1 market price. It follows that, given such prices,

Proposition 4 (Market equilibrium in period 1)**.** *Suppose $r = 0$ and $n > 0$ (that is, only poor developers are present). In the period-1 market equilibrium all developers randomize between 0 and $\bar{Q}^i$, where $\bar{Q}^i$ is the largest $Q_2^i \leq M$ satisfying the developer's cash constraint* (1) *(see 7).*

If, furthermore, all developers are identical (i.e. same Q_1^i and same $\bar{Q}^i$), then in the symmetric equilibrium the probability that each developer sets $Q_2^i = 0$ is $\tau(n)$, implicitly defined as

$$\tau(n) \equiv \tau : \quad \frac{1}{2} = (1-\tau) \sum_{j=0}^{n-1} \binom{n-1}{j} \left(\frac{1-\tau}{\tau}\right)^j \frac{2}{2(j+1) - \mathbb{1}\{j \neq 0\}} \tag{8}$$

The corresponding period-1 prices are

$$p_1^i = \frac{1}{R} \frac{E\left[U_2(\bar{Q}^i, \mathbf{Q}^i)\right]}{\bar{Q}^i} = \frac{\tau(n)^{n-1}}{R} \cdot \frac{1}{2} \frac{\bar{Q}^i}{M^2}$$

The corresponding value of the winning platform is:[20]

$$E[e^w] = n\tau(n)^{n-1} \cdot \frac{1}{2} \frac{\bar{Q}^i}{M}$$

Note that, by equation 8, $\tau(n)$ increases with n. Hence, as the number of competitors in the market increases, in the symmetric equilibrium the probability that a single developer liquidates all his token increases. This has an ambiguous effect on the equilibrium prices: from the point of view of a given developer, it is now more likely that a given opponent liquidates his tokens, but the number of opponents increases. Similarly, changes in n have an ambiguous effect on the value of the winning platform. We therefore resort to numerical calculations, reported in Table 1.

The first order effects is that, as the number of competitors increases, the probability that all developers but one liquidate their tokens decreases. This in turns decreases the price of each individual token because each developer is more likely to have a competitor and, in equilibrium, this developer must be indifferent between

all equilibria yield the same payoffs to all developers, and hence our forward-looking equilibrium refinement is mute.

[20] The expectation here is taken after the developers paid the entry cost, before the market opens.

$Q_2^i = 0$ and $Q_2^i = \bar{Q}^i$. The calculations also show that the expected value of the winning platform is monotonically increasing with n. Hence, if all developers are poor, competition is always beneficial. This is in sharp contrast with the case $r > 0$ in which, as we saw, the value of the winning platform is maximized at $r = 2$.

A related observation is that, by Proposition 3, if $r = 1$ then the value of the winning platform will be 1. It is possible, therefore, that the value of the winning platform is greater when there are sufficiently many poor developers and no rich developers.[21] If instead there are two developers who did not hold an ICO, then the value of the winning platform will be 2, which is always above the value of the winning platform when any numbers of developers held an ICO. Intuitively, relative to a situation in which a single developer self-financed the entry cost, having multiple ICOs implies two things. On the one hand, there could be multiple competitors in period 2, which increases expected effort. On the other hand, in equilibrium it is possible that all developers liquidate their tokens. If sufficiently many developers held an ICO, the first effect dominates, which implies that it is better to have several developers who held an ICO. Of course, if there are two developers who did not hold an ICO, then we have the best of both words: competition will push these developers to exert effort, but without the risk that they liquidate all their tokens in period 1. We summarize these observations in the following remark.

Remark 1. *The value of the winning platform is the largest possible when $r = 2$ (i.e., there are two rich developers). If $\bar{Q}$ is sufficiently large, then the value of the winning protocol is greater with $r = 0$ and n sufficiently large (i.e., no rich developers but sufficiently many poor developers), then with $r = 1$ (i.e., a single rich developer).*

3.4 Period 1: entry cost.

Consider now the choice of paying the entry cost. It is useful to reorder the developers in the following way. The first $\tilde{n} \geq 0$ developers have enough funds to pay the entry cost. Of those, the first $\tilde{r} \geq 0$ did not hold an ICO so that, by definition

[21] In particular, this would be the case if there are no rich developers, at least 12 poor developers, and for these developers $\bar{Q}$ is either greater or sufficiently close to M.

n	$\tau(n)$	$\tau(n)^{n-1}$	$n\tau(n)^{n-1}$
1	1/2	1	1
2	0.6375	0.6375	1.274
3	0.6976	0.4866	1.46
4	0.7353	0.3975	1.5902
5	0.7622	0.3375	1.6874
6	0.7827	0.2938	1.763
7	0.7992	0.2605	1.8234
8	0.8127	0.2341	1.8728
9	0.8241	0.2127	1.914
10	0.8339	0.1949	1.949
11	0.8423	0.1799	1.9788
12	0.85	0.167	2.0044
13	0.8565	0.1559	2.0272
20	0.8888	0.1064	2.1284
30	0.9138	0.0731	2.1944
100	0.9625	0.0227	2.2672

Tab. 1: Probability of liquidating all tokens ($\tau(n)$), price of each token ($\propto \tau(n)^{n-1}$) and expected value of the winning platform ($\propto n\tau(n)^{n-1}$) as a function of n. Symmetric equilibrium for $r = 0$.

$Q_1^i = M$ for $i \leq \tilde{r}$. The remaining developers held an ICO and therefore have $\bar{Q}_i \leq M$.[22]

Suppose $\tilde{r} > 0$. If

$$\frac{1}{2} \geq C \cdot R, \tag{9}$$

then entry by at least one developer $i \leq \tilde{r}$ is profitable. In this case, there are $\tilde{r}$ equilibria in which a single developer $i \leq \tilde{r}$ pays the entry cost. There are also equilibria in mixed strategy in which multiple developers randomize between paying the entry cost or not. It is clear however that these equilibria do not survive our forward-induction refinement: by taking a useless-but-costly action a developer $i \leq \tilde{r}$ can signal its intention to pay the entry cost with probability one, therefore deterring all other developers from paying the entry cost.[23] We summarize these observation in the following proposition (we omit its proof).

Proposition 5. *Suppose $\tilde{r} > 0$. If*

$$\frac{1}{2} \geq C \cdot R \tag{10}$$

Then the equilibria robust to our forward-looking refinement are those in which only a single developer $i \leq \tilde{r}$ pays the entry cost. The value of the winning protocol is therefore:

$$e^w = 1.$$

If (10) *is violated, then in equilibrium no developer pays the entry cost.*

From now on, we always assume that (10) holds.

If instead $\tilde{r} = 0$, by Proposition 3, if a single developer i pays the entry cost, his subsequent payoff is

$$\frac{1}{2R}\left(\frac{\bar{Q}^i}{M}\right)^2.$$

[22] Note that, if a developer held an ICO and $\bar{Q}_i = M$, this developer was rich enough to pay the fixed cost without holding an ICO. We show later that, in equilibrium, no developer who is rich enough to pay the fixed cost holds an ICO. Hence, on the equilibrium path, for all developers who held an ICO we have $\bar{Q}_i < M$.

[23] Note that if a developer j with $\tilde{r} < j \leq \tilde{n}$ signals his intention to pay the fixed cost in the same way, a developer $i \leq \tilde{r}$ will still find it profitable to enter. The reason is that, by Proposition 3, if both i and j pay the fixed cost, j will liquidate all his tokens on the market and never reach period 2.

Hence, entry can occur if and only if

$$\frac{1}{2}\left(\frac{\max_i\{\bar{Q}^i\}}{M}\right)^2 \geq C \cdot R, \tag{11}$$

Suppose now that (11) holds and assume that all developers are identical. In this case, if all $\tilde{n}$ developers pay the entry cost, each of them will earn

$$\frac{\tau(\tilde{n})^{\tilde{n}-1}}{R} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2.$$

This immediately implies that if

$$\tau(\tilde{n})^{\tilde{n}-1} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2 \geq C \cdot R \tag{12}$$

in equilibrium all developers with enough resources pay the entry cost with probability one. However if

$$\tau(\tilde{n})^{\tilde{n}-1} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2 < C \cdot R, \tag{13}$$

then, again, if all developers with enough resources pay the fixed cost, then profits will be negative. Hence, the only equilibrium surviving our forward-induction refinement is one in which $\hat{n}(\bar{Q})$ developers pay the entry cost, where

$$\hat{n}(\bar{Q}) \equiv \max\left\{n | \tau(n)^{n-1} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2 \geq C \cdot R\right\} \tag{14}$$

The following proposition summarizes these observations (we omit its proof).

Proposition 6. *Suppose that $\tilde{r} = 0$, that* (11) *holds, and that all developers are identical. In the equilibrium robust to our forward-looking refinement $n = \min\{\tilde{n}, \hat{n}(\bar{Q})\}$ developers pay the entry cost.*

It is interesting to note that the above equilibrium may not be the only one surviving our forward looking refinement. If

$$\tau(\hat{n}(\bar{Q}))^{\hat{n}(\bar{Q})-1} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2 = C \cdot R$$

then there are also equilibria in which $\hat{n}(\bar{Q}) - 1$ pay the entry cost for sure, and an additional developer randomizes. We have not expicitly mentioned them because, when considering the ICO stage, these equilibria are never reached. For a more detailed discussion, see the Mathematical appendix, Remark on Proposition 6.

By Proposition 3, therefore, as long as $\tilde{n} < \hat{n}(\bar{Q})$, increasing $\tilde{n}$ increases the expected value of the winning protocol and the sum of the token prices, while decreasing the price of each individual token. If instead $\tilde{n} > \hat{n}(\bar{Q})$, then the equilibrium level of entry (and hence the value of the winning protocol and the prices of tokens) are independent of $\tilde{n}$.

3.5 Period 0: the ICO.

To start, suppose $\tilde{r} > 0$: some developers have enough own resources to pay the entry cost without holding an ICO. The following Lemma follows directly from Proposition 5.

Lemma 1. *Suppose $\tilde{r} > 0$, that is, $\max\{a_i\} \geq \frac{C}{R}$. In this case there is no ICO in period 0.*[24] *In the subsequent period a single developer $i \leq \tilde{r}$ pays the entry cost. The expected value of the winning platform is $e^w = 1$.*

Hence, the presence of even a single developer who is sufficiently rich effectively prevents all other developers from raising funds at ICO. The equilibrium outcome is therefore a monopoly.

Suppose no developer has enough resources to pay the entry cost C. Note that, because the ICO is modeled as an auction, first investors learn Q_1^i, and then they form an expectation with respect to the developer's behavior in period 1 and hence about p_1^i. For investors to be indifferent, it must be that:

$$p_0^i = \frac{p_1^i}{R}.$$

Furthermore, a developer holding the ICO should raise sufficient funds to pay

[24] More precisely, there could be ICOs with equilibrium price equal to zero. We consider this possibility as equivalent to "no ICO".

the entry cost[25]

$$(a^i + p_0^i(M - Q_1^i))R = C. \tag{15}$$

Finally, the investors' expectation with respect to the developer's behavior in period 1 should be correct. For example, if investors expect developer i to pay the entry cost, then p_1^0 should reflect this. In equilibrium, the developer should be able to sell sufficiently few tokens at p_1^0 so to be willing to pay the entry cost in period 1.

The next proposition uses these three conditions to characterize the equilibrium.

Proposition 7. *Suppose* $\max_i\{a^i\} < \frac{C}{R}$. *There is always an equilibrium in which there is no ICOs nor entry in equilibrium.*

Suppose furthermore that all developers are identical, that is $a^i = a$ *for all* i. *Define:*

$$p_1^i(Q_1^*) \equiv \frac{1}{R}\tau(\hat{n}(Q_1^*))^{\hat{n}(Q_1^*)-1} \cdot \frac{1}{2}\frac{Q_1^*}{M^2}.$$

Then any $Q_1^* \geq M\sqrt{2C}$ *solution to:*

$$Q_1^* = M - \frac{C - aR}{p_1^i(Q_1^*)}, \tag{16}$$

is an equilibrium in which $\tilde{n}(Q_1^*)$ *developers hold an ICO, each of them selling* $M - Q_1^*$ *tokens.*

For intuition, note that $p_1^i(Q_1^*)$ is the price for tokens in period 1, when all developers holding an ICO sell $M - Q_1^*$ tokens and, as a consequence, $\hat{n}(Q_1^*)$ developer pay the fixed cost. Note also that, as Q_1^* increases, if $\hat{n}(Q_1^*)$ stays constant then $p_1^i(Q_1^*)$ will increase. It is however possible that increasing Q_1^* leads to an increase in the number of competitors $\hat{n}(Q_1^*)$ and to a discontinuous drop in $p_1^i(Q_1^*)$. Condition (16) comes from (15) and guarantees that, at ICO price equal to $p_1^i(Q_1^*)/R$, a developer selling $M - Q_1^*$ tokens raises enough money to pay the fixed cost in the following

[25] A technical note. A developer could sell at ICO more tokens that what required to pay the entry cost, and then use the extra funds to invest in the risk-free asset and then, possibly, purchase back his tokens in period 1. These extra funds yield a return R, which in equilibrium is equal to the return on tokens. Hence, developers are indifferent between selling extra tokens or not. Furthermore, Proposition 4 shows that p_1^i depends on $\bar{Q}^i$. By definition, $\bar{Q}^i$ is the largest number of tokens that a developer can purchase in period 1 given his cash constraint (1), and is the same independently of whether the developer sells extra tokens in period 0. For ease of exposition, here we focus on the equilibria in which no extra tokens are sold at ICO.

period. Finally, the condition $Q_1^* \geq M\sqrt{2C}$ guarantees that (11) holds at Q_1^*, and hence it is incentive compatible for at least one developer having enough funds to actually pay the fixed cost.

There are therefore multiple equilibria. One source of equilibrium multiplicity are off equilibrium beliefs: if investors believe that no developer will pay the entry cost in the future, then it is not possible to raise funds at ICO. This is always an equilibrium because no developer is given the chance to invest, and hence investors' beliefs cannot be shown to be incorrect.

Furthermore, an equilibrium with ICOs may or may not exist. This may happen for two reasons. Note that the largest possible value of Q_1^* is M, and at this value we have

$$Q_1^* > M - \frac{C - aR}{p_1^i(Q_1^*) \cdot Q_1^*}.$$

Hence, the equilibrium with ICO may fail to exist because, for all $Q_1^* \geq M\sqrt{2C}$ we have

$$Q_1^* > M - \frac{C - aR}{p_1^i(Q_1^*) \cdot Q_1^*}.$$

Clearly, this situation is more likely to emerge when $C - aR$ is large, and never emerges when $C - aR$ is sufficiently small. Hence, if developers are too poor, there is no equilibrium with ICO. In this case, developers can raise enough funds to pay the fixed cost only by selling many tokens. But by doing so they have no more incentive to pay the fixed cost in the following period.

An equilibrium with ICO may fail to exist also because of an integer problem: there are value of Q_1^* such that

$$Q_1^* < M - \frac{C - aR}{p_1^i(Q_1^*) \cdot Q_1^*}.$$

but because $\hat{n}(Q_1^*)$ jumps discontinuously at some values of Q_1^* equation (16) never holds. In this case, it is possible to show that an equilibrium with ICO exists provided that a public randomization device is available.[26]

[26] In such equilibrium, each of $\hat{n}(Q_1^*)$ developers announces how many tokens to sell at ICO and investors then submit bids. Each developer may then cancel the ICO (in which case investors do not pay anything). After the bids are submitted, a fair public randomization device is used to identify a single developer among the $\hat{n}(Q_1^*)$, who will then randomize between canceling his

Finally, note that (16) may have multiple solutions and hence there could be multiple equilibria with ICOs. The intuition here is the following. As Q_1^* increases, as long as $\hat{n}(Q_1^*)$ does not change the corresponding token price $p_1^i(Q_1^*)$ will increase. This is because investors expect higher effort in the future, and hence are willing to pay a larger price. But if this is the case, then the developer needs to sell fewer tokens at ICO in order to pay the entry cost, which implies that his future effort will be high. Conversely, if Q_1^* is low, then $p_1^i(Q_1^*)$ will be low, in which case the developer will need to sell many tokens to cover the entry cost. This can be seen as a coordination problem between investors and developers. This logic is mitigated (but not fully eliminated) by the fact that, as Q_1^* increases $\hat{n}(Q_1^*)$ may also increase. In this case, additional competition will drive the price of each token down.

4 Welfare

Our measure of welfare is the expected value of the winning protocol. As already discussed, if there is at least one developer with enough resources to pay the entry cost, then a single developer will enter and the equilibrium value of the winning protocol is 1.

If instead there is no developer who can pay the entry cost, then, by Proposition 3 the expected value of the winning protocol is

$$E[e^w] = \tilde{n}(Q_1^*)\tau(\tilde{n}(Q_1^*))^{\tilde{n}(Q_1^*)-1} \cdot \frac{1}{2}\frac{Q_1^*}{M}$$

where Q_1^* is defined in (16). If, furthermore, we have $a \to \frac{C}{R}$ then $Q_1^* \to M$ and

$$E[e^w] \to \tilde{n}(M)\tau(\tilde{n}(M))^{\tilde{n}(M)-1} \cdot \frac{1}{2}$$

In this case, welfare with ICOs is larger than welfare without ICOs as long as $\tilde{n}(M)\tau(\tilde{n}(M))^{\tilde{n}(M)-1} > 2$ or $\tilde{n}(M) \geq 12$ (see Table 1). By definition of $\tilde{n}(M)$, this would indeed be the case if, for example, C is sufficiently low.

The key observation is that, despite the fact that ICOs decrease each developers'

ICO or not. Note also that this equilibrium is strictly preferred by all $\hat{n}(Q_1^*)$ developers to the equilibrium with no ICOs. See the proof of the proposition for more details.

incentive, they also stimulate entry. Overall, welfare will be higher with ICOs (than without) when the loss of incentives is contained (because Q_1^* is sufficiently large) and when ICOs allow sufficiently many developers to enter. An interesting implication is that welfare is non-monotonic in the cost of entry: welfare may be higher when C is high (and hence ICO occur in equilibrium) than when C is low (and hence no ICO occurs in equilibrium).

5 Conclusion

ICOs have received a number of criticism, both in the popular press and in the academic domain. In particular, Canidio (2018) considers a single developer and shows that ICOs, like all forms of outside financing weakens incentives. Specific to this environment, if a developer holds an ICO, then in all subsequent periods there is a positive probability that this developer will liquidate all his tokens and stop the development of his decentralized digital platform—essentially, this developer may exit the market prematurely. Here we show that this result is robust to the introduction of multiple developers. However, precisely because of that, then ICOs stimulate entry.[27] This has a positive effect, because entry stimulates competition and effort.

From the view point of the regulator, our model highlights two things. First, there could be equilibria with ICOs and entry next to equilibria without ICOs. Hence, the regulator's role could be to help achieve the equilibrium with ICOs and entry. Second, as already discussed, welfare is sometimes larger when there is entry with ICOs than without ICOs. This implies that a regulator may want to increase the cost of entry (possibly via a tax), so to induce developers to hold ICOs and hence stimulate entry.

We believe that the model can be extended in several directions. For example, there could be a second dimension of effort (for example, marketing effort) affecting the probability that a platform is the winning platform, without changing its under-

[27] It is important to stress that, whereas all forms of external financing weaken incentives, not all forms of external financing stimulate entry. So, for example, external financing in the form of a sale of equity weakens incentives because it reduces effort, which however will be exerted with probability 1. In this case only one developer will enter the market because a second developer will for sure earn zero profits., which is the same with or without external financing.

lying platform. This effort is therefore welfare reducing, because it may induce users to adopt an inferior platform. Introducing this second dimension of effort may make competition less desirable. The reason is that, when a single developer pays the entry cost, all effort is productive. When multiple developers are present, however, some effort may be unproductive. Studying the competitive dynamics and welfare properties of the equilibrium under this different assumption is left for future work.

A Mathematical Appendix

Proof of Proposition 2. A player's equilibrium strategy is a function $F^i(x) = \text{pr}\{e^i \leq x\}$, representing the probability that developer i chooses effort level below a given threshold x. Remember that the existence of the equilibrium is already in Siegel (2014). The goal here is to derive the equilibrium strategies, for then determining the equilibrium prices and equilibrium value of the winning platform.

A couple of preliminary observations. First, there cannot be a pure strategy equilibrium and hence at least two players must randomize over positive effort values. We say that developers $i \leq z$ with $2 \leq z \leq k$ set strictly positive effort with strictly positive probability, while the other developers set effort equal to zero. Hence, for $i > z$ we have $F^i(x) = 1$ for all $x \geq 0$. The second observation is that, for every $i \leq z$ and possible equilibrium effort level $x > 0$, the developer earns zero expected utility, and hence

$$\text{pr}\{x > \max_{j \neq i}\{e^j\}\}\frac{Q^l}{M} = \frac{x}{2}.$$

Note that

$$\text{pr}\{x > \max_{j \neq i}\{e_j\}\} = \prod_{j \neq i} F^j(x),$$

so that developer i earns zero profits by choosing effort x if and only if:

$$\prod_{j \neq i} F^j(x) = x\frac{M}{2Q^l} \tag{17}$$

Consider an equilibrium. For this equilibrium, write the CDF of $e^w = \max_i\{e^i\}$

as

$$F^w(x) = \prod_j F^j(x) = F^i(x) \prod_{j \neq i} F^j(x) = xF^i(x) \frac{M}{2Q^l},$$

where the first equality follows from the fact that the probability that the maximum of multiple random variables is below a given threshold is equal to the probability that *all* these random variables are below this same threshold.

The above expression implies that for $i, j \leq z$ we have $F_i(x) = F_j(x) \equiv F(x)$. That is, if two leaders i and j set strictly positive effort with strictly positive probability, their equilibrium strategies must be the same. Knowing this, by (17), we have that

$$F(x) = \left(x \frac{M}{2Q^l} \right)^{\frac{1}{z-1}}$$

Hence, for every z such that $2 \leq z \leq k$ we can compute

$$F^w(x) = \left(x \frac{(1-\gamma)M}{2Q^l} \right)^{\frac{z}{z-1}}$$

$$f^w(x) = \frac{z}{z-1} x^{\frac{1}{z-1}} \left(\frac{M}{2Q^l} \right)^{\frac{z}{z-1}}$$

$$E[e^w] = \frac{z}{z-1} \left(\frac{M}{2Q^l} \right)^{\frac{z}{z-1}} \int_0^{\frac{2Q^l}{M}} x^{\frac{z}{z-1}} dx = \frac{z}{z-1} \left(\frac{M}{2Q^l} \right)^{\frac{z}{z-1}} \frac{z-1}{2z-1} \left(\frac{2Q^l}{M} \right)^{\frac{2z-1}{z-1}}$$

$$= \frac{z}{2z-1} \left(\frac{2Q^l}{M} \right).$$

Note that, because all developer $i \leq z$ have the same strategy, they must have the same probability of succeeding. Hence, the price of each token $i \leq z$ is

$$E[p_2^i] = \frac{1}{2z-1} \left(\frac{2Q^l}{(1-\gamma)^2 M^2} \right)$$

□

Proof of Proposition 3. Consider a poor developer i. Suppose that, in equilibrium Q_2^i is sufficiently large so that i's expected effort is strictly positive, either because he is the follower in a mixed strategy equilibrium, or because he is one of multiple leaders. If there is also a rich developer, however, developer i's continuation utility

is zero. But because expected effort is strictly positive, then $p_1^i > 0$. This cannot be an equilibrium because, clearly, if $p_1^i > 0$ the developer is better off to sell all his tokens in period 1 and exert no effort in period 2.

Hence, in equilibrium Q_2^i must be such that period-2 effort is zero and hence $p_1^i = 0$. Clearly, $Q_2^i = 0$ is an equilibrium.

□

Proof of Proposition 4. Suppose $Q_1^i > 0$ for some i.

Step 1: in equilibrium, at least one developer earns strictly positive profits. In any equilibrium, there must exist a developer y with $Q_1^y > 0$ who earns strictly positive profits. Suppose not. In this case, the only possible equilibrium is one in which $p_1^i = 0$ for all i. The reason is the same discussed in the proof of Proposition 3: if period 1 prices were positive, then developers would be better off to sell all their tokens in period 1, which cannot be an equilibrium. But because there are no rich developers, $p_1^i = 0$ for all i is not an equilibrium either. The reason is that a single developer could hold on to his tokens, become the unique leader in the following period and earn strictly positive profits.

Step 2: in equilibrium, the developer earning strictly positive profits randomizes. If developer y earns strictly positive profits, then he is the unique leader for some Q_2^y and some (or all) realizations of $\mathbf{Q}^y$. For given investors' belief about period-2 effort (and period-2 prices) period-1 prices are fully determined and equal to $p_1^y = E[e^y]\text{pr}\{y = w\}/R$. Hence, developer y's objective function is convex (strictly so somewhere) in Q_2^y, and his maximization problem must have a corner solution. Therefore, we can represent each developer's equilibrium strategy by $\tau_y \in [0, 1]$ the probability that developer y sets $Q_2^y = 0$, with $1 - \tau_y$ being the probability that the developer sets $Q_2^y = \bar{Q}^y$.

Consider now the investors. If in equilibrium $\tau^y = 0$, then, with probability 1, effort will be high in period 2. This effort will be priced into period 1 price. But given this, the developer should sell all his tokens and invest in the risk-free asset. This way, he can benefit from his future effort before exerting any, and hence without paying the cost of effort. This establishes that, in any equilibrium, it must

be that $\tau^y > 0$. If, in equilibrium, $\tau^y = 1$, then because $e_2^y = 0$, the period 1 price of token y is zero. The developer can earn the exact same payoff by holding on to his token until period 2 and setting $e_2^y = 0$. He can do strictly better if he holds on to his token until period 2 and sets e_2^y optimally. Hence $\tau^y = 1$ cannot be an equilibrium.

Hence, in equilibrium it must be that $\tau_y \in (0, 1)$, which can only be the case if developer y is indifferent between setting $Q_2^y = 0$ and $Q_2^y = \bar{Q}^y$, which is equivalent to:

$$p_1^y Q_1^y R = E\left[U_2(\bar{Q}^y, \mathbf{Q}^y)\right] - p_1^y \left(\bar{Q}^y - Q_1^y\right) R$$

so that

$$p_1^y R = \frac{E\left[U_2(\bar{Q}^y, \mathbf{Q}^y)\right]}{\bar{Q}^y}.$$

Step 3: all developers with $Q_1^i > 0$ randomize. Conditional on developer y liquidating all his tokens, by repeating the same argument in Step 1, there must be another developer x that will be the unique leader for some Q_2^x and some realizations of $\mathbf{Q}^x$. By step 2 above, this developer must randomize between $Q_2^x = 0$ and $Q_2^x = \bar{Q}^x$.

By repeating the same argument, every developer with $Q_1^i > 0$ has a strictly positive probability of being the unique leader in period 2 for some Q_2^i. This probability is equal to the probability that all other developers sell all their tokens in period 1. Hence, in equilibrium every developer with $Q_1^i > 0$ must randomize between $Q_2^i = 0$ and $Q_2^i = \bar{Q}^i$.

Step 4: characterization of the equilibrium probabilities for the case of identical developers. To characterize the equilibrium probabilities, assume that all developers are identical (so that $\bar{Q}^i = \bar{Q}$ for all i) and consider the symmetric equilibrium. In this case, a developer is indifferent between holding zero tokens and holding $\bar{Q}$ whenever

$$p_1^i R = \frac{E\left[U_2(\bar{Q}, \mathbf{Q})\right]}{\bar{Q}} = \tau^{n-1} \cdot \frac{1}{2} \frac{\bar{Q}}{M^2}$$

At the same time, by (5), for investors to be indifferent it must be that

$$p_1^i R = (1-\tau)\sum_{j=0}^{n-1}\binom{n-1}{j}(1-\tau)^j\tau^{n-1-j}\cdot\frac{\bar{Q}}{M^2}\cdot\frac{2}{2(j+1)-\mathbb{1}\{j>0\}}$$

where $\binom{n-1}{j}(1-\tau)^j\tau^{n-j-1}$ is the probability that, among all developers other than i, there are j developers who do not liquidate their tokens. Because $(1-\tau)$ is the probability that developer i did not liquidate his token, the entire expression

$$(1-\tau)\binom{n-1}{j}(1-\tau)^j\tau^{n-1-j}$$

is the probability that player i and j other developers did not liquidate their tokens, and hence in the following period there are $j+1$ leaders with $\bar{Q}$ tokens. By using the above two expressions for p_1^i, we establish that τ is implicitly determined by

$$\frac{1}{2} = (1-\tau)\sum_{j=0}^{n-1}\binom{n-1}{j}\left(\frac{1-\tau}{\tau}\right)^j\frac{2}{2(j+1)-\mathbb{1}\{j>0\}}$$

Note that the RHS of the above expression is strictly decreasing in τ, goes to infinity for $\tau\to 0$ and to zero for $\tau\to 1$. It follows that the above expression has a unique solution. Furthermore, because the RHS of the above expression is strictly increasing in n, the equilibrium τ must be increasing in n.

Finally, by (6), the expected value of the winning platform is

$$E[e^w] = nE[p_2^i]M = np_1^i RM = n\tau^{n-1}\cdot\frac{\bar{Q}}{2M}$$

where the last equality follows from the expression for $p_1^i R$ derived earlier.

□

Remark on Proposition 6. To characterize the full set of equilibria, Proposition 6 should be modified in the following way:

Proposition 8. *Suppose that $\tilde{r}=0$, that (11) holds, and that all developers are identical. The equilibria robust to our forward-looking refinement are:*

- *if either* $\tilde{n} < \hat{n}(\bar{Q})$ *or*

$$\tau(\hat{n}(\bar{Q}))^{\hat{n}(\bar{Q})-1} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2 > C \cdot R$$

then n *developers pay the entry cost, where* $n = \min\{\tilde{n}, \hat{n}(\bar{Q})\}$.

- *if* $\tilde{n} \geq \hat{n}(\bar{Q})$ *and*

$$\tau(\hat{n}(\bar{Q}))^{\hat{n}(\bar{Q})-1} \cdot \frac{1}{2}\left(\frac{\bar{Q}}{M}\right)^2 = C \cdot R$$

then in all equilibria $\hat{n}(\bar{Q})-1$ *developers enter with probability 1, while a single additional developer enters with probability between 0 and 1 (included).*

It is therefore possible that when $\hat{n}(\bar{Q})-1$ developers enter they all earn positive profits, but if an additional developer enters all developers earn zero profits (in the sense that their continuation utility equals C). This additional developer is therefore indifferent between entering or not and, in equilibrium, may randomize. Note also that this equilibrium survives our forward looking refinement because the additional developer is indifferent between entering or nor—even if he knows for sure that the other $\hat{n}(\bar{Q}) - 1$ developers will enter for sure. Note also that when $\tilde{n} \geq \hat{n}(\bar{Q})$ there is no symmetric equilibrium because all developers are identical but some developer will pay the entry cost and some will not.

If, in equilibrium, $\hat{n}(\bar{Q})-1$ developers enter for sure with an additional developer randomizing, then the expected period-1 price of token $i \leq \hat{n}(\bar{Q}) - 1$ is

$$E[p_1^i] \in \left[\frac{\tau(\hat{n}(\bar{Q})-1)^{\hat{n}(\bar{Q})-2}}{R} \cdot \frac{1}{2}\frac{\bar{Q}}{(M)^2}, \frac{\tau(\hat{n}(\bar{Q}))^{\hat{n}(\bar{Q})-1}}{R} \cdot \frac{1}{2}\frac{\bar{Q}}{(M)^2}\right], \tag{18}$$

that is, depending on how the additional developer randomizes, any $E[p_1^i]$ within the above interval can emerge in equilibrium. The $\hat{n}(\bar{Q})$th developer, instead, randomized and therefore we have

$$E[p_1^{\hat{n}(\bar{Q})}] \in \left[0, \frac{\tau(\hat{n}(\bar{Q}))^{\hat{n}(\bar{Q})-1}}{R} \cdot \frac{1}{2}\frac{\bar{Q}}{(M)^2}\right] \tag{19}$$

The problem with this equilibrium is that, from period 0 viewpoint, it implies

that $\hat{n}(\bar{Q})$ identical developers are able to raise funds at ICO, but not all at the same price. But this cannot happen in equilibrium: identical developers cannot all raise $\frac{C}{R} - a$ at ICO by selling he same amount of tokens but at different prices. □

Proof of Lemma 1. By Proposition 5 we know that if every developer $i \leq \tilde{r}$ holds an ICO, then a single developer $j \leq \tilde{r}$ is better off to not hold the ICO and conquer the entire market. Hence there is no equilibrium in which every developer $i \leq \tilde{r}$ holds an ICO.

Given that at least one developer $i \leq \tilde{r}$ does not hold an ICO, then no other developer can sell tokens at ICO at a strictly positive price. That is because, by Proposition 3, their token will be worth zero in the following period.

If at least one developer $i \leq \tilde{r}$ does not hold an ICO, all other developers are indifferent between not holding an ICO and holding an ICO in which their tokens are sold at zero price. In the symmetric equilibrium no developer $i \leq \tilde{r}$ holds an ICO. The other developers $i \geq \tilde{r}$ may break their indifference either way.

The lemma follows by considering the case of "ICO with price zero" equivalent to "no ICO". □

Proof of Proposition 7. Suppose investors expect that, if a developer raises enough funds to pay the entry cost, then (11) will be violated in period 1. Then $p_0^i = p_1^i = 0$. No developer is able to raise funds at ICO. Although whether (**??**) holds or not is never observed (i.e., the investors beliefs are off equilibrium), no ICO is indeed an equilibrium.

Suppose investors expect (11) holds. Again, we focus on the symmetric equilibrium, in which all firms holding an ICO sells the same number of tokens. Call n^* and $Q_1^* < M$ the equilibrium number of firms holding an ICO and number of tokens not sold at ICO, respectively. Note that, for given Q_1^*, it must be that $n^* = \hat{n}(Q_1^*)$ (where $\hat{n}()$ is defined in 14). If $n^* > \hat{n}(Q_1^*)$ then some of the developers holding the ICO will not pay the entry cost, which quickly leads to a contradiction (these developers should not be able to raise funds at ICO in the first place); if $n^* < \hat{n}(Q_1^*)$ then some developers who are not holding an ICO could successfully hold one, pay the entry cost and earn positive profits in equilibrium. It follows that $n^* = \hat{n}(Q_1^*)$ is a piecewise increasing function of Q_1^*.

For given Q_1^*, therefore, we have a unique $n^* = \hat{n}(Q_1^*)$. We can therefore define

$$p_1^i(Q_1^*) \equiv \frac{\tau(\hat{n}(Q_1^*))^{\hat{n}(Q_1^*)-1}}{R} \cdot \frac{1}{2}\frac{Q_1^*}{M^2}.$$

as the period-1 price as a function of Q_1^*. Note that if Q_1^* increases without changing $n^* = \hat{n}(Q_1^*)$, then the corresponding price $p_1^i(Q_1^*)$ increases as well. As Q_1^* increases further, however, $n^* = \tilde{n}$ may also increase. At such Q_1^*, $p_1^i(Q_1^*)$ has a downward discontinuity.

Knowing this, using (15) together with the fact that $p_0 = \frac{p_1}{R}$, we can characterize the equilibrium by the following equation

$$Q_1^* = M - \frac{C - aR}{p_1^i(Q_1^*)},$$

If at Q_1^* solution to the above equation (11) holds, then such Q_1^* is an equilibrium. Note that (11) holds at Q_1^* if and only if $Q_1^* \geq M\sqrt{2C}$.

As discussed in the body of the text, the above equation may not have a solution (and hence an equilibrium with ICO may not exist) because of an integer problem: there exist an X such that

$$X > \lim_{Q_1^* \to X^-} \left\{ M - \frac{C - aR}{p_1^i(Q_1^*)} \right\}$$

but

$$X < M - \frac{C - aR}{p_1^i(X)}.$$

In this case, there is an equilibrium in which:

- $\tilde{n}(X)$ developers announce the sale of $M - X$ tokens at ICO. Investors submit bids.
- using a fair public randomization device, a single developer is selected. This developer then will cancel the ICO with some probability. If the ICO is canceled, then investors do not have to pay anything.

To start, note that each developer has the same probability of canceling his ICO, and hence investors should submit the same bids to all developers. It follows that the

equilibrium ICO price is the same for all developers who run an ICO. Furthermore, there exists a probability of canceling the ICO such that

$$X = M - \frac{C - aR}{p_1^i(X)}.$$

and hence the price of the token is such that if all $\hat{n}(X)$ developers hold an ICO, they all raise enough funds to pay the entry cost.

Finally, by definition, X is such that $\hat{n}(X)$ developers finds it (weakly) profitable to pay the fixed cost. However, at any $Q_1 < X$ we have that strictly fewer than $\hat{n}(X)$ developers find it profitable to pay the fixed cost. By definition of $\hat{n}(.)$, this implies that

$$\tau(\hat{n}(X))^{\hat{n}(X)-1} \cdot \frac{1}{2}\left(\frac{X}{M}\right)^2 = C \cdot R.$$

Hence, all $\tilde{n}(X)$ developers will pay the entry cost in period 1, but they all make zero profits. This implies that knowing that the other $X - 1$ developers will hold the ICO for sure, developer X is indifferent between holding it or not, and hence may randomize. The other $X - 1$ developers earn positive expected profits (because with some probability there will not be an additional ICO) and hence they strictly prefer to run the ICO for sure.

□

References

Amsden, R. and D. Schweizer (2018). Are blockchain crowdsales the new'gold rush'? success determinants of initial coin offerings. *working paper*.

Armstrong, M. (2006). Competition in two-sided markets. *The RAND Journal of Economics 37*(3), 668–691.

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

Ben-Porath, E. and E. Dekel (1992). Signaling future actions and the potential for sacrifice. *Journal of Economic Theory 57*(1), 36–51.

Benigno, P., L. M. Schilling, and H. Uhlig (2019). Cryptocurrencies, currency competition, and the impossible trinity. Technical report, National Bureau of Economic Research.

Biais, B., C. Bisiere, M. Bouvard, and C. Casamatta (2019). The blockchain folk theorem. *The Review of Financial Studies 32*(5), 1662–1715.

Bolt, W. and M. R. Van Oordt (2020). On the value of virtual currencies. *Journal of Money, Credit and Banking 52*(4), 835–862.

Caillaud, B. and B. Jullien (2003). Chicken & egg: Competition among intermediation service providers. *RAND journal of Economics*, 309–328.

Canidio, A. (2018). Financial incentives for open source development: the case of blockchain. *Working paper*.

Catalini, C. and J. S. Gans (2018). Initial coin offerings and the value of crypto tokens. Technical report, National Bureau of Economic Research.

Chod, J. and E. Lyandres (2018). A theory of icos: Diversification, agency, and information asymmetry. *working paper*.

Cong, L. W., Y. Li, and N. Wang (2018). Tokenomics: Dynamic adoption and valuation. *working paper*.

Cong, L. W., Y. Li, and N. Wang (2019). Tokenomics and platform finance. *working paper*.

Gandal, N. and H. Halaburda (2016). Can we predict the winner in a market with network effects? competition in cryptocurrency market. *Games 7*(3), 16.

Garratt, R. and M. R. van Oordt (2019). Entrepreneurial incentives and the role of initial coin offerings. *Working paper*.

Garratt, R. and N. Wallace (2018). Bitcoin 1, bitcoin 2,....: An experiment in privately issued outside monies. *Economic Inquiry 56*(3), 1887–1897.

Goldstein, I., D. Gupta, and R. Sverchkov (2019). Initial coin offerings as a commitment to competition. *Available at SSRN 3484627*.

Howell, S. T., M. Niessner, and D. Yermack (2018, June). Initial coin offerings: Financing growth with cryptocurrency token sales. Working Paper 24774, National Bureau of Economic Research.

Huberman, G., J. D. Leshno, and C. C. Moallemi (2017). Monopoly without a monopolist: An economic analysis of the bitcoin payment system. *CEPR discussion paper*.

Jönsson, S. and A. Schmutzler (2013). All-pay auctions: Implementation and optimality. *Available at SSRN 2205697*.

Katz, M. L., C. Shapiro, et al. (1985). Network externalities, competition, and compatibility. *American economic review 75*(3), 424–440.

Kristiansen, E. G. and M. Thum (1997). R&d incentives in compatible networks. *Journal of Economics 65*(1), 55–78.

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

Lyandres, E., B. Palazzo, and D. Rabetti (2018). Do tokens behave like securities? an anatomy of initial coin offerings. *Working Paper*.

Malinova, K. and A. Park (2018). Tokenomics: when tokens beat equity. *Working paper*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. (last accesed April 20, 2020).

OECD (2017). Venture capital investments. In E. O. Paris (Ed.), *Entrepreneurship at a Glance 2017*.

Olszewski, W., R. Siegel, et al. (2019). Performance-maximizing large contests. *Theoretical Economics*.

Prat, J., V. Danos, and S. Marcassa (2019). Fundamental pricing of utility tokens. Technical report.

Rochet, J.-C. and J. Tirole (2003). Platform competition in two-sided markets. *Journal of the european economic association 1*(4), 990–1029.

Schilling, L. and H. Uhlig (2019). Some simple bitcoin economics. *Journal of Monetary Economics 106*, 16–26.

Siegel, R. (2009). All-pay contests. *Econometrica 77*(1), 71–92.

Siegel, R. (2014). Contests with productive effort. *International Journal of Game Theory 43*(3), 515–523.

Sockin, M. and W. Xiong (2018). A model of cryptocurrencies. *Working paper*.