Financial incentives for the development of blockchain-based platforms

Canidio, Andrea

IMT Lucca

2018

Financial incentives for the development of blockchain-based platforms.*

Andrea Canidio †

First version, March 20, 2018. This version: October 27, 2020. Please check here for the latest version.

Abstract

A developer creates a new blockchain-based decentralized digital platform by investing resources and exerting costly effort. Performing exchanges on the platform is possible only by using a new crypto-token. The initial stock of this token is owned by the developer, who can sells some in an Initial Coin Offering (ICO), and more later on a frictionless financial market. I show that, if the developer raises funds via an ICO, then in every subsequent period with strictly positive probability he may liquidate his tokens and stop the development of the platform. Even if the developer does need to hold an ICO, the equilibrium will nonetheless be inefficient because the developer's payoff depends on the volume of transaction on the decentralized digital platform in each period. Instead, the social value of the platform depends on the present discounted value of the total surplus created. The developer's effort and investment could be above or below their optimal levels, depending on the discount factor and the elasticity of supply/demand of the users of the platform.

JEL classification: D25, O31, L17, L26, G23

Keywords: Blockchain, decentralized digital platforms, Initial Coin Offering (ICO), Tokenomics, seigniorage, innovation, incentives, open source.

---

*I am grateful to Bruno Biais, Ennio Bilancini, Sylvain Chassang, Lin William Cong, Kenneth Corts, Antonio Fatas, Gur Huberman, John Kuong, Jiasun Li, Allistair Milne, Julien Prat, Massimo Riccaboni, Harald Uhlig, the participants of the CoPFiR workshop on FinTech, Bank of Finland/CEPR Conference on Money in the Digital Age, ZEW conference on the Dynamics of Entrepreneurship, Annual Meeting of the Central Bank Research Association, 8th EIEF-Unibo-IGIER Bocconi Workshop on Industrial Organization, second Toronto FinTech Conference, Paris Tokenomics conference, seminar participants at the University of Bolzano for their comments and suggestions. This paper initially circulated under the title "Financial incentives for open source development: the case of Blockchain".

†IMT school of advanced studies, Lucca, Italy & INSEAD, Fontainebleau, France. andrea.canidio@imtlucca.it

1 Introduction

The astonishing rise of Initial Coin Offerings (ICOs) brought blockchain-based crypto-tokens to the forefront of the policy, academic, and regulatory debate. In an ICO, a startup (or loose groups of developers) raises capital by selling crypto-tokens to a wide pool of investors. 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, see Figure 1).[1] However, these extraordinary events partially obscured a crucial fact: that in the vast majority of cases, teams holding ICOs plan to profit from their work by selling more tokens at a later stage. That is, the sale of tokens constitutes not only an innovative fundraising mechanism, but also a novel way to profit from software development. This novel form of *seigniorage* is the dominant business model in the blockchain sector.[2]

To illustrate how seigniorage can provide incentives for innovation, consider a population of agents who wish to exchange either a good or a service, but are prevented from doing so by the lack of the required infrastructure. If this exchange can occur in electronic form, then the missing infrastructure may be a *protocol*, that is, the technical specifications governing the communication between machines. Suppose a developer creates the missing protocol and with it a *decentralized digital platform* (i.e., the peer-to-peer network of the users of the protocol). This developer can profit from his innovation by simultaneously creating a *token*, and by establishing that all exchanges that occur on the decentralized digital platform must use this token. The token is therefore the internal currency of the platform. The developer owns the initial stock of tokens so that, if the decentralized digital platform is successful, there will be a positive demand for tokens, a positive price for tokens and positive profits earned by the developer.

Blockchain enables seigniorage because it allows a developer to commit to a given supply of tokens. This is because the rules determining whether (and how) the supply of tokens increases over time can initially be specified within the protocol (see Section 2.1 for additional

[1] For comparison, in 2016 total Venture Capital investment in Europe was USD 4.7 billion (OECD, 2017). Note that, although far from its 2018 peak, ICOs continue to attract large investments. For example, between January 2020 and September 2020, despite the economic turmoil cause by the pandemic, 7 ICOs were able to raise more that 10M USD each, with one raising more than 100M USD (source: https://icodrops.com.)

[2] At the time of writing, among the top-30 tokens by market capitaliztion, 23 are associated with projects earning profits via seignorage. These tokens represent approximately 85% of the total crypto-market, with the rest comprised for the most part of stable coins (tokens that are supposed to maintain a stable value relative to a benchmark, for example the US dollar; data from www.coinmarketcap.com).

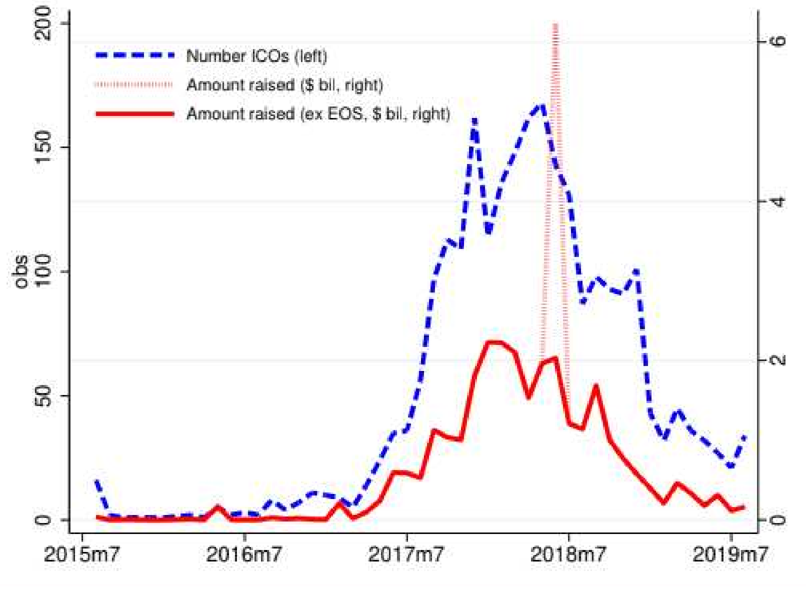

Fig. 1: From Lyandres, Palazzo, and Rabetti (2018) page 35: "This figure reports monthly values of the number of ICOs that are able to raise funds (dashed blue line, left axis) and the total amount raised across all ICOs each month (billions of dollars, right axis). The solid red line excludes the EOS ICO in June 2018, while the dotted red line includes it. Monthly observations go from August 2015 to August 2019. The observations reported for the month of August 2015 group all ICOs up to August 2015.".

details on blockchain). If the protocol is open source—that is, its source code is publicly available—this commitment is credible because anybody can verify the monetary policy specified by the protocol. Of course, this type of commitment could be achieved by other means, for example by complex institutional design (e.g., creating a "central bank") or by building reputation over time. But these alternatives are very expensive and not widely available.[3] Blockchain instead generates commitment by computer code. The downside is, however, that blockchain-based protocols (like all open-source software) must be free to use.[4] Hence, seigniorage is incompatible with traditional pricing.

In this paper I study a developer's incentives to create a decentralized digital platform. I do so by building a model in which a developer can sell tokens both to raise funds and to then profit from his/her work. Crucially, the quality of the decentralized digital platform is

[3] As a consequence, the only notable example of non-blockchain electronic currency that is freely exchangeable with dollars is the Linden Dollar (the currency of the game Second Life). Other non-blockchain electronic currencies are those of online games like World of Warcraft. These currencies cannot be freely exchanged with dollars.

[4] This follows from Bertrand competition: if an open-source software is not free, a competitor or a group of users could, at zero cost, launch an exact replica of the same software having lower or zero prices.

endogenous: in every period, the developer exerts effort and invests in the development of the platform, therefore improving its quality. Initially, the developer owns the entire stock of tokens, and can sell some to investors via an Initial Coin Offering (ICO), modeled as an auction. Subsequently, in every period, he can sell (or buy) tokens on a frictionless financial market on which investors are also active.[5] The developer can use the proceedings of the sale of tokens to either invest in the development of the platform or to consume.

The first result is that, if investors are price takers, then in any post-ICO period there is an anti-coordination problem. If investors expect the developer to develop the platform in the future, this expectation should be priced into the token's current price. But if this is the case, then the developer is strictly better off by selling all of his tokens, which allows him to "cash in" on future developments without doing any work. On the other hand, if investors expect no development to occur, the price of the token will be low. The developer should hold onto as many tokens as possible, exert effort and invest in the development of the platform, so to increase the future price of the token. In every post-ICO period, therefore, the equilibrium is in mixed strategy: the price of the token is such that the developer is indifferent between selling all of his tokens (and therefore not developing the platform) or keeping a strictly positive amount of tokens (and therefore continuing the development of the platform). The developer randomizes between these two options, in a way that leaves investors indifferent between purchasing tokens in any given period.

When choosing whether and when to hold an ICO, the developer is therefore facing a tradeoff. If he holds an ICO, in every subsequent period he may sell all of his tokens and not develop the platform. Postponing the ICO, therefore, prevents the creation of a market for tokens and works as a commitment device, because the developer will hold all of his tokens for certain and set the corresponding level of effort and investment. However, if the developer does not sell tokens at ICO, he may lack the funds to invest in the development of the platform. As a consequence, the developer never wants to hold an ICO if his own assets are sufficient to finance the optimum level of investment, but may hold an ICO otherwise.

The model delivers two main insights. The first one is that, as with other forms of external financing, selling some tokens at ICO weakens the developer's future incentives to

[5] This feature of the model is justified by the observation that, absent a market for tokens, users could not use the platform. This is one of the distinguishing features of tokens relative to other forms of financing, such as, for example, equity. In a traditional business financed via equity, instead, trading equities can be made more or less liquid for the company founders and managers (for example via provisions in the shareholders agreement), independently from the ability of consumers to use the product.

develop the platform, and therefore leads to inefficiencies. The interesting part of this result is the specific form of this inefficiency: in every period after the ICO the developer may sell all his tokens and stop the development of the platform. The second insight is more subtle but more interesting. Even assuming that the developer can develop the decentralized digital platform using exclusively his own funds (so that the first source of inefficiency is absent), his level of effort and investment are set so as to maximize the value of his stock of tokens. This value depends on the volume of the transaction occurring on the platform during a given period of time.[6] Instead, in the first best, effort and investment should be set so as to maximize the present discounted value of the surplus generated by the platform.

Interestingly, the level of effort and investment set by the developer may be above or below their first best levels. This depends on the discount factor and on the distribution of the willingness to sell and to buy of the users using the platform to transact with each other. The developer disregards the fact that the platform will be used and generate surplus over multiple periods. Hence, if the discount factor is high (i.e., future payoffs have a large present discounted value) then effort and investment are more likely to be below their first best levels. In addition, when the elasticity of demand and supply on the platform are high, total surplus is low, and with it the social return of effort and investments. In this case, the equilibrium effort and investment are above their optimal level. On the other hand, if these elasticities are high, the equilibrium effort and investment are below their optimal levels.[7]

The model delivers a number of other interesting results. For example, post-ICO there may be multiple equilibria. Because of a cash constraint, the developer cannot invest in the development of the platform more than his assets. It follows that the developer may sell some of his tokens, as a way of accumulating assets to finance the future development of the platform. The number of tokens that the developer needs to sell in order to finance future investments depends on the current price for tokens, therefore generating a coordination problem. If the price is high, the developer needs to sell fewer tokens, and his incentives to invest and develop the software in the future are high. This, in turn, justifies the high price for tokens today. If instead the price today is low, in order to finance future development,

[6] This will result from an application of the equation of exchange, usually employed to link a country's price level, real GDP, money supply and velocity of money.

[7] Interestingly, the elasticity of demand and supply also determine the choice between creating a traditional platform or a decentralized digital platform, which I consider in an extension (Section 6.1). If the developer creates a traditional platform, he will then earn a fraction of the surplus created (could be the totality if he can perfectly price discriminate). If the elasticity of supply/demand are high, total surplus will be low and the developer will prefer to create a decentralized digital platform. This seems to suggest that conditional on creating a decentralized digital platform, effort and investment should be above their efficient levels.

the developer needs to sell more tokens. But then his incentives to develop the software will be low, which justifies the fact that the price is low today. Therefore, post-ICO there could be multiple mixed-strategy Nash equilibria.[8]

The remainder of the paper is organized as follows. The next Section provides the reader with the necessary background information on blockchain, ICOs and seigniorage, and also discusses the relevant literature. Section 3 presents a model of seigniorage. Section 4 solves for its equilibrium. Section 5 illustrates the first best of the model and compares it to its equilibrium. Section 6 discusses some extensions to the model, such as the possibility of creating a traditional platform (instead of a decentralized digital platform) and the possibility of raising funds from a Venture Capitalists (instead of via an ICO). Section 7 concludes. Unless otherwise noted, all proofs and mathematical derivations missing from the text are in the Appendix.

2 Background and relevant literature

2.1 Blockchain-based decentralized digital platforms and seigniorage

In his seminal paper, Nakamoto (2008) introduced 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 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.

Shortly after the introduction of Bitcoin, it became apparent that blockchain can be used to maintain any type of record, not only financial records. It therefore quickly became

[8] Clearly, if there are network effects, then there is an additional coordination problem: for a given sequence of effort and investment by the developer, there could be both a "high adoption" and a "low adoption" equilibrium. The novelty here is that, for a given adoption equilibrium, there are multiple equilibrium sequences of effort and investment arising from a coordination problem between investors and the developer.

the technological foundation of various other decentralized digital platform. In addition to several cryptocurrencies (such as Monero, ZCash, Litecoin), there are now several decentralized computing platforms (see Ethereum, EOS, Cardano, NEO);[9] decentralized platforms for real-time gross settlement (see Ripple, Stellar); decentralized marketplaces for storage and hosting of files (see SIA, Filecoin, Storj), for renting in/out CPU cycles (see Golem), for event or concert tickets (see Aventus), for e-books (see Publica); decentralized prediction markets (see Augur, Gnosis); decentralized financial exchanges (see 0xproject); and many more.

As already discussed, each platform must be used in conjunction with a specific token. In case of decentralized marketplaces, the token is typically the internal currency of the marketplace. Similarly, within decentralized computing platforms (e.g., Ethereum), the protocol native token (e.g., Ether) must be used to pay miners or validators for executing some piece of software (called smart contracts). In the case of cryptocurrencies such as Bitcoin, people who need to exchange Bitcoins reward those who process these transactions (called, again, miners) in two ways. One is direct: the sender can directly pay some Bitcoins to the miner to process his transaction faster. The second is indirect: the network awards miners with new bitcoins for their work. Because of its effect on the price, this increase in the supply of bitcoins amounts to a transfer from the holders of bitcoins to the miners.[10] In other blockchain-based decentralized digital platforms, the use of the token can be the most diverse and the most complex.

If the token is necessary to use a decentralized digital platform, this token has positive value as long as this platform is expected to have some usage in the future. Given this, the developers behind a platform can sell some tokens to investors before completing its development. One way to sell a token is via an ICO, which are typically well advertised. Usually, tokens sold at ICO start trading on specialized financial exchanges shortly after the end of the ICO.[11] Importantly, developers can use these same exchanges to sell additional

[9] A decentralized computing platforms can be seen as a virtual machine running over a network rather than a single server. Developers can then create software (which in this context are smart contracts) that is executed by the network as a whole rather than by a single machine.

[10] See also Huberman, Leshno, and Moallemi (2017) and Easley, O'Hara, and Basu (2019).

[11] Some ICOs "lock" their tokens for a period raging from few months to 2 years. During this period, investors cannot trade tokens, although the emergence of future markets allowed sophisticated investors to circumvent this limitation. At the expiration of the "lock" period—usually well before the development of the platform is completed—trading tokens on specialized financial exchanges becomes possible. Note that, to the extent that investors value liquidity, "locking" tokens impose a cost on them. It is possible that "locking" tokens for too long may prevent a developer from raising sufficient funds at ICO.

tokens after the ICO. With few exceptions,[12] either token sales on the open market are not disclosed, or they are discussed only within blog posts and informal communication.[13] Despite the difference in visibility between these two ways of selling tokens Howell, Niessner, and Yermack (2019) 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.

2.2 Relevant literature

This paper is closely related to corporate finance literature studying "large shareholders". In particular DeMarzo and Urošević (2006) consider a large shareholder who can exert effort to improve the performance of a firm, and is active on the market together with a mass of small investors. They find that, in equilibrium, the large shareholder will inefficiently liquidate his holdings (either immediately or slowly over time). Also, they show that the large shareholder may benefit from committing to a holding schedule. This is similar to what happens in my model, in which, in equilibrium, the developer liquidates all tokens with positive probability and, anticipating this, he may postpone the ICO. There are, however, a number of differences between the problem studied here and that in DeMarzo and Urošević (2006). The most prominent is that, here, the developer may sell tokens to raise funds to invest in the development of the platform, in which case selling tokens increases the value of the platform and its associated token. In DeMarzo and Urošević (2006), there is no such investment and therefore selling shares always decreases the "large shareholders" effort and the share price.[14]

We contribute to the literature on blockchain-based decentralized digital platforms by studying the incentives faced by the creators of such platforms. We do so by assuming that tokens are both a mean to raise funds and a mean to earn a profit, and that the quality of

[12] For example, Ripple announces in advance a schedule for selling parts of its XRP stock, see https://ripple.com/insights/q1-2018-xrp-markets-report/ (accessed on July 24, 2020).

[13] For example, see this blog post by the Ethereum foundation https://blog.ethereum.org/2016/01/07/2394/ (accessed on July 24, 2020).

[14] Also, from the modeling viewpoint, DeMarzo and Urošević (2006) assume symmetric information between the large shareholder and investors, and hence abstract away from the most obvious sources of inefficiencies. Here I make the same assumption. However, DeMarzo and Urošević (2006) assume that, in each period, first the large shareholder chooses his shareholding, then investors set their demand/supply. They then consider arbitrarily small periods, i.e., a continuous-time model. Here instead the developer and investors set their demand/supply for tokens simultaneous, but the timing is discrete.

the platform depends on the developer's effort and investment.

With this respect, the most closely related papers 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 their model, the optimal monetary policy may require the owner to buy back tokens, which can be done by raising costly external financing. The main result is that, to avoid incurring such cost, the platform owner will create *fewer* tokens than optimal. In Goldstein, Gupta, and Sverchkov (2019) an entrepreneur chooses whether to create a decentralized digital platform or a traditional platform. If the entrepreneur creates a decentralized digital platform he will hold an ICO and then sell additional tokens over time. In this case, Goldstein et al. (2019) find that the entrepreneur optimally releases tokens over time rather than all at once. Their main result is that creating a decentralized digital platform allows the entrepreneur to commit to decentralization and competitive pricing rather than monopoly pricing. Hence, if the distortion introduced by monopoly pricing (in terms of reduction of equilibrium quantity exchanged) is large, the entrepreneur will prefer to create a decentralized digital platform.

In contrast to both Cong et al. (2019) and Goldstein et al. (2019), I find that the developer (also the entrepreneur and the platform owner) may sell *too many* tokens (that is, all of them) on the market. The reason for this difference is that, in the model presented here, the developer chooses not only how many tokens to sell, but also how much effort to exert in the development the decentralized digital platform[15] I also consider the choice between creating a traditional platform (and hence charge monopoly pricing) and a decentralized digital platform (Section 6.1). I find results that are in line with Goldstein et al. (2019), but with some important differences. In particular, I provide conditions under which a non-distortionary monopolist (i.e., a monopolist who can perfectly price discriminate) may prefer to create a decentralized digital platforms. Hence, market distortions only partially explain the choice between a traditional and a decentralized platform.

The rest of the literature studying blockchain tokens has focused on the ICO. This literature can be divided into two parts. Most closely related are papers studying the role of tokens in decentralized digital platforms. Sockin and Xiong (2018), Cong, Li, and Wang

[15] Both Goldstein et al. (2019) and Cong et al. (2019) abstract away from such effort. Note also how the results in DeMarzo and Urošević (2006) (discussed earlier) also suggest that when a large "insider" can both exert effort and trade on the market, in equilibrium he will sell too many tokens than optimal.

(forthcoming), Bakos and Halaburda (2018), and Li and Mann (2018) argue that because of network externalities there could be coordination failures in the adoption of a decentralized digital platform. They study the role of tokens and they way they are sold in achieving the high-adoption equilibrium. A second strand of literature has studied ICOs held by startups 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 combination of both. This use of blockchain-based tokens is studied in Catalini and Gans (2018), Chod and Lyandres (forthcoming), Garratt and van Oordt (2019), Malinova and Park (2018).

There is a growing literature building economic models to study how blockchain works (see, for example Catalini and Gans, 2016; Huberman, Leshno, and Moallemi, 2017; Dimitri, 2017; Prat and Walter, 2018; Ma, Gans, and Tourky, 2018; Budish, 2018). Within this literature, closely related is Biais, Bisiere, Bouvard, and Casamatta (2019), in which the price of a token and incentives of Bitcoin miners are determined in the equilibrium of a game-theoretic model. Also in my paper, prices and incentives are determined in equilibrium, but the interest is in the incentives to develop the decentralized digital platform rather than processing transactions. The portion of the model that determines the equilibrium price of the token borrows heavily from Athey, Parashkevov, Sarukkai, and Xia (2017), who propose an equilibrium model of the price of Bitcoin. The novelty with respect to their paper is that, here, the demand for tokens is a function of the developer's effort and investment, while the "quality" of the Bitcoin protocol is taken as given in their model (but is unknown and therefore discovered over time).

Gans and Halaburda (2015) study platform-based digital currencies, such as Facebook credits and Amazon coins. These currencies share some similarities with the tokens discussed in the Introduction, because they can be used to perform exchanges on a specific platform. They are, however, controlled by their respective platforms, which decide on their supply and the extent to which they can be traded or exchanged. This may explain why, despite some initial concerns,[16] these currencies have neither gained wide adoption, nor generated significant profits for the platform issuing them.

[16] See, for example "Could Facebook Credits ever compete with dollars and euros?" by Matthew Yglesias on Slate, February 29, 2012 (available at https://slate.com/business/2012/02/facebook-credits-how-the-social-networks-currency-could-compete-with-dollars-and-euros.html, accessed on July 24, 2020).

Finally, this paper contributes to the literature on innovation and incentives, in particular to the literature studying the motivation behind contributions to open-source software (see the seminal paper by Lerner and Tirole, 2002). In this respect, I show that open source—with its organizational structure and ethos—can coexist with strong financial incentives. Of course, an open question not addressed here is whether or not financial rewards will crowd out other motives (see, for example, Benabou and Tirole, 2003); that is, whether the open source ethos will be compromised by the introduction of strong financial incentives.

3 The model

The economy is composed of a developer, a large mass of risk-neutral price-taking investors and a large mass of users. At the beginning of every period $1 \leq t \leq T$, the developer exerts effort e_t and invests i_t into the development of a blockchain-based decentralized digital platform. The development of the protocol lasts T periods, after which the developer exits the game and users start using the decentralized digital platform. The decentralized digital platform can be used indefinitely. At the beginning of the game, the developer establishes that all transactions on the decentralized digital platform must be conducted using a specific token, with total supply M, fully owned by the developer. There is a common time-discount factor $\beta \in (0, 1)$

In period $t_o \leq T$, the developer sells some tokens to investors via an auction. This stage is the ICO (Initial Coin Offering) stage, and its date t_o is chosen by the developer. In each period after the ICO, but before the developer exits the game (that is, in every $t \in \{t_o + 1, ..., T\}$), first the developer exerts effort and invests, then a frictionless market for tokens opens. In every period after the developer exits (that is, in every $t > T$), first the market for tokens opens and then users use the platform. See Figure 2 for a graphical representation of the timeline.

Investors and the developer can also hold a risk-free asset yielding a per-period gross return $R \geq 1$. For ease of derivations, I assume that $R = \frac{1}{\beta}$.[17]

[17] Hence, R is the steady-state rate of return of the Ramsey-Cass-Koopmans growth model (with no population growth or exogenous productivity growth). As we will see, this assumption is not essential for the results but simplifies their derivation. Furthermore, although the model is solved in partial equilibrium (i.e., for given R), it is useful to discuss the general equilibrium consequences of the creation of the platform (see the Conclusion).

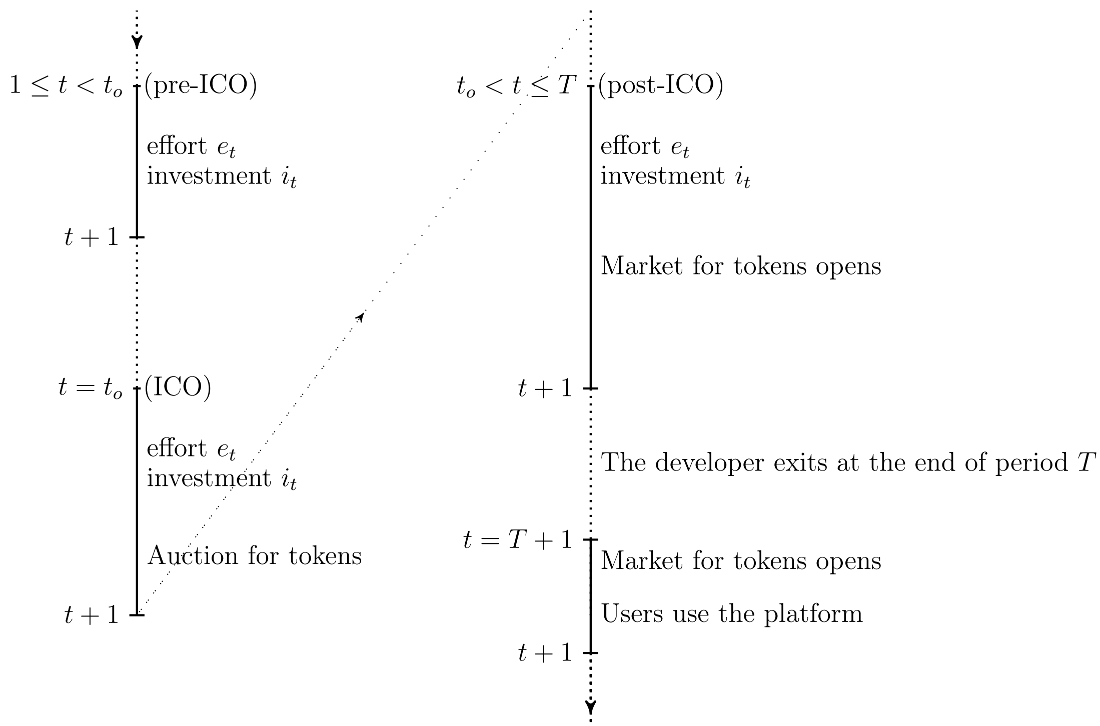

Fig. 2: Timeline

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

The developer. Call $Q_t \in [0, M]$ the stock of tokens held by the developer at the beginning of period t. Recursively define

$$A_t \equiv \left(A_{t-1} - i_{t-1} + p_{t-1}(Q_{t-1} - Q_t)\right) R$$

the total resources available to the developer at the beginning of period t, where A_1 is the developer's initial assets and the rest are resources earned from the sale of tokens in previous periods, net of the investments made. Note that if $p_{t-1}(Q_{t-1} - Q_t) > 0$ then this term represents the resources spent by the developer to purchase his own token on the market in period $t-1$. If instead $p_{t-1}(Q_{t-1} - Q_t) < 0$ then this term represents the resources earned by selling additional tokens on the market in period 1. At the end of each period, the available assets are invested at the risk-free rate.

The developer faces a per-period cash constraint establishing that the amount spent by the developer (either as investment or to purchase tokens on the market) cannot exceed his assets:

$$p_t \max\{Q_{t+1} - Q_t, 0\} + i_t \leq A_t. \tag{1}$$

Because the developer cannot sell tokens before holding an ICO, there is also a feasibility constraint

$$Q_t \equiv M \text{ for all } t \leq t_o.$$

In every period, the developer maximizes his assets at the end of period T (when he exits the game) minus the disutility of effort. His problem can be rewritten in recursive form as, for $t < T$:

$$U_t(Q_t, A_t) \equiv$$

$$\begin{cases} \max_{Q_t,e_t,i_t} \left\{-\frac{1}{2}e_t^2 + \beta U_{t+1}(Q_{t+1}, (A_t + (Q_t - Q_{t+1}) \cdot p_t - i_t)R) + \lambda_t(A_t - i_t - p_t \max\{Q_{t+1} - Q_t, 0\})\right\} \\ \qquad \text{if } t \geq t_o \\ \max_{e_t,i_t} \left\{-\frac{1}{2}e_t^2 + \beta U_{t+1}(M, (A_t - i_t)R)\right\}, \text{ otherwise} \end{cases}$$

where λ_t is the Lagrange multiplier associated with the period-t cash constraint. Because in period T the developer sells all his tokens for sure (either on the market or in an ICO) his period-T problem is:

$$U_T(Q_T, A_T) \equiv \max_{e_T,i_T} \left\{A_T + Q_T \cdot p_T - i_T - \frac{1}{2}e_T^2 + \lambda_T(A_T - i_T)\right\},$$

Finally, at the beginning of every period, if no ICO was held, the developer will decide whether to hold one. The sequence of effort, investments and Q_t are assumed observable by investors and users.

Users. In period T the development of the protocol stops, and users start using the decentralized digital platform. Call q the price of the good (or service) exchanged on the platform, expressed in fiat currency (for example USD). For ease of derivation, I introduce the following functional forms for the supply and the demand on the platforms:

Assumption 1. *The per-period demand and supply functions on the decentralized digital platform are, respectively:*

$$\tilde{D}(q) \sum_{t=1}^{T} \tau(e_t, i_t) \qquad\qquad \tilde{S}(q) \sum_{t=1}^{T} \tau(e_t, i_t).$$

$\tilde{S}(q)$ is strictly increasing, $\tilde{D}(q)$ is strictly decreasing, $\tau(.,.)$ is increasing in both arguments, concave in e_t, with $\lim_{i \to \infty} \left\{ \frac{\partial \tau(e_t, i_t)}{\partial i_t} \right\} = 0$ for all e_t, and with $\tau(0,0) = 0$.

Hence, effort and investments increase both supply and demand proportionally and by the same factor. The equilibrium price on the platform q^*, implicitly defined as

$$\tilde{D}(q^*) = \tilde{S}(q^*),$$

is independent of the sequence of effort and investment. The elasticity of demand and supply are independent of the developer's effort and investment. Effort and investment however determine the volume of exchanges occurring at price q^*. For ease of notation, I define

$$f(e_t, i_t) \equiv \tau(e_t, i_t) \tilde{D}(q^*) q^*,$$

so that the total value (in US dollars) of all exchanges occurring on the decentralized digital platform during a given period is

$$V_T \equiv \sum_{s=1}^{T} \tau(e_t, i_t) \tilde{D}(q^*) q^* = \sum_{s=1}^{T} f(e_s, i_s). \tag{2}$$

I call the above quantity the *value of the decentralized digital platform.*

Assumption 1 is meant to capture in a parsimonious way the fact that the developer's effort and investment generates an improvement of the protocol (i.e., lower transaction costs, more ease of use, increased security, and reliability), which in turns induces more users to use the platform to perform more/larger transactions. Being parsimonious, however, it also abstracts away from important elements. For example, because of network externalities, it is possible that for a given sequence of effort and investment there is both a "high adoption" equilibrium (in which the value of the decentralized digital platform is high) and a "low adoption" equilibrium (in which the value of the decentralized digital platform is low). With a minimal loss of generality, the reader can interpret V_T as the value of the decentralized digital platform in one of these equilibria, the one that the developer expects to emerge.[18]

Finally, each user can access the market for tokens only once in every period.[19] This implies that, in every $t > T$, those who use the protocol to purchase goods and services have a demand for tokens in period t equal to $\frac{V_T}{p_t}$, while those who use the protocol to sell goods or services have a supply of tokens in period $t+1$ equal, again, to $\frac{V_T}{p_t}$.

4 Solution

4.1 Periods $t \geq T$

I start by solving for the price of tokens from period T onward. The fact that no development is possible after period 2 implies that the price of tokens must be constant from period T onward. Investors are therefore unwilling to hold tokens, and the entire stock of tokens M is used by users to transact on the platform. Because in period $t \geq T$, the demand of tokens by users is $\frac{V_T}{p_t}$, the equilibrium price of tokens must be:

$$p_T = \frac{V_T}{M}. \tag{3}$$

Because the supply of tokens in all following period is again M, and the demand is again $\frac{V_T}{p_t}$, the above is the price of tokens in every period from T onward.

Equation 3 is an adaptation of the equation of exchange, which is usually employed to link a country's price level (here the price of the token relative to "fiat" currency), real GDP (here V_T), money supply (here the number of tokens available for transacting on the platform M) and velocity of money (here assumed equal to 1). For our purposes, the important implication is that V_T — and hence the price at which the developer can sell his token — is

[18] The loss of generality is that either the "high" or the "low" adoption equilibrium may not exist for some sequences of effort and investment, generating a discontinuity in the way effort and investment maps into the value of the decentralized digital platform.

[19] That is, the token has velocity 1. Assuming a different, exogenous velocity will introduce an additional parameter without affecting the results. See Prat, Danos, and Marcassa, 2019 for a model in which the velocity of the token in endogenous.

strictly increasing in the sequence of effort and investments made by the developer. As we will see, this motivates the developer to exert effort and invest.

4.2 The developer's problem

We start by deriving a useful lemma. This lemma is based on the observation that, in equilibrium, between period t_0 and T holding tokens must generate a return equal to the risk-free return R:

Lemma 1. *In equilibrium, in every period $t_o \leq t \leq T$, the price of tokens is*

$$p_t = \frac{E[p_T]}{R^{T-t}} = \frac{\sum_{s=1}^{t} f(e_s, i_s) + \sum_{s=t+1}^{T} E[f(e_s, i_s)]}{MR^{T-t}} \tag{4}$$

An important observation is that what is known by investors—and hence is used to compute the expectation about the developer's future effort and investment—depends on whether $t = t_o$ (i.e., the tokens are sold at ICO) or $t > t_o$ (i.e., the tokens are sold on the market). The ICO is modeled as an auction, in which the developer announces the supply of tokens and investors submit bids. The developer's announcement is used to compute the future expected effort and investment, and hence determines the token price at ICO. On the market, instead, investors are price takers, which implies that in every $t > t_o$ their demand for tokens depends exclusively on current and future (expected) prices, and not on the quantity of tokens sold by the developer in period t.[20] To say it differently, in period $t > t_o$ investors form an expectation with respect to future effort and investment. This expectation is correct in equilibrium (that is, for the equilibrium supply of tokens in period t) but will not react to deviations from the equilibrium. From the developer's view point, therefore, in every period $t > t_o$, the equilibrium price for tokens does not depend on the amount of tokens sold *in that period.* However, as we will see, the supply of tokens in period t determines the developer's effort and investment in period $t + 1$. Hence, the amount of tokens sold by the developer in a given period affect the price of tokens *in all subsequent periods.*

It is useful to solve the developer's problem by considering two cases. The first is the "rich developer" case, in which the developer's initial assets A_1 are sufficient to cover the optimal level of investment in every period. In this case, the cash constraint is never binding and

[20] 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.

can be ignored. The second case is that of a "poor developer", in which the cash constraint is binding for at least one period.

4.2.1 Rich developer

If the cash constraint is never binding, the developer's maximization problem does not depend on the assets available in every period. It is therefore possible to rewrite the objective function as, for $t \leq T-1$:

$$\tilde{U}_t(Q_t) \equiv \max_{Q_{t+1},e_t,i_t} \left\{ -\frac{1}{2}e_t^2 + \beta \tilde{U}_{t+1}(Q_{t+1}) \right\},$$

and for $t = T$:

$$\tilde{U}_T(Q_T) \equiv \max_{e_T,i_T} \left\{ \sum_{t=1}^{T-1} \left[(Q_t - Q_{t+1}) \cdot p_t - i_t \right] R^{T-t} + Q_T \cdot p_T - i_T - \frac{1}{2}e_T^2 \right\}.$$

Note that $\sum_{t=t_o}^{T-1} \left[(Q_t - Q_{t+1}) \cdot p_t - i_t \right]$ is the cash generated between period 1 and $T-1$ (net of investment) which is invested in the risk free asset. Because the developer liquidates all his tokens in period T, then $Q_T \cdot p_T - i_T$ is the cash generated in period T.

Lemma 1 allows to compute optimal effort and optimal investment in any period t:[21]

$$e^*(Q_t) \equiv \text{argmax}_e \left\{ f(e, i^*(Q_t)) \frac{Q_t}{M} - \frac{1}{2}e^2 \right\} \tag{5}$$

$$i^*(Q_t) \equiv \text{argmax}_i \left\{ f(e^*(Q_t), i) \frac{Q_t}{M} - i \right\}. \tag{6}$$

Note that, by Lemma 1, effort and investment in period t increase the price of tokens in every subsequent period, but because the price must increase at rate R, this effect is stronger in later periods. At the same time, because of discounting, payoffs earned in the distant future are less valuable from today's viewpoint. Because $\beta R = 1$ the two effects cancel out, so that optimal effort and investment depend exclusively on Q_t and not on the specific time period t.[22]

[21] Under the assumptions made on $f(.,.)$ optimal effort and investment must exist. However, they may not be unique. In what follows, for ease of exposition, I implicitly assume that they are indeed unique, although no result depends on this assumption.

[22] If instead $\beta R > 1$, for given token holdings, effort will be high in earlier periods and decrease over time, while if $\beta R < 1$ effort will be low in earlier periods and increase over time. This effect is purely mechanical,

Furthermore, Q_t and e_t are complements in the developer's objective function. This, by Topkis' theorem, implies that $e^*(Q_t)$ is an increasing function. Similarly, Q_t and i_t are complements in the developer's objective function, which implies that $i^*(Q_t)$ is an increasing function. At the same time, $e^*(0) = i^*(0) = 0$. There are therefore two possible cases. The first one is trivial: $e^*(Q_t)$ and $i^*(Q_t)$ are equal to zero for all $Q_t \leq M$. The second case is non-trivial: both $e^*(Q_t)$ and $i^*(Q_t)$ are increasing in Q_t, strictly so somewhere. In what follows, I focus exclusively on the non-trivial case.

To solve for the optimal choice of Q_{t+1}, as a preliminary step I characterize the shape of $\tilde{U}(Q_t)$.

Lemma 2. *For all* $t \in \{t_o, ..., T\}$

$$\frac{\partial^2 \tilde{U}(Q_t)}{\partial Q_t^2} \geq 0,$$

with strict inequality for some $Q_t \leq M$.

Hence, in every period, the developer's utility function is convex in Q_t, strictly so somewhere. For intuition, note that if the price of tokens is constant in every period, then $\forall t \in \{t_o, ...T\}$, $\tilde{U}(Q_t)$ grows linearly in Q_t. However, we know that as Q_t increases effort and investment will also increase, and with them the price of tokens. Because effort and investment are chosen optimally, $\tilde{U}(Q_t)$ must grow faster than linearly in Q_t.

Consider now the choice of how many tokens to sell on the market. In period T, quite trivially, the developer will sell all his tokens at price given by (3). Consider therefore a period $t \in \{t_o + 1, ..., T - 1\}$. In such period, the developer can sell any amount of tokens at the equilibrium market price p_t. Hence, the instantaneous opportunity cost of holding (i.e., not selling) tokens is linear. By the above lemma, the continuation value of holding tokens is instead positive and convex (strictly so somewhere). It follows that, in every $t \in \{t_o + 1, ..., T - 1\}$ the optimal choice of Q_{t+1} must be a corner solution: either the developer sells all his tokens (i.e. $Q_{t+1} = 0$), or the developer holds on to all his tokens (i.e. $Q_{t+1} = M$), or he randomizes between these two options.

Note, however, that if in equilibrium we have $Q_{t+1} = 0$ with probability 1, then investors should expect no effort nor investment in the following period. This implies that p_t should be low. But if p_t is low, then the developer is better off to hold on to his tokens until next period (i.e. choose $Q_{t+1} = M$). If instead in equilibrium we have $Q_{t+1} = M$ with probability 1, then investors expect high effort and investment in the future. In this case, today's price

which is why I focus on the case $\beta R = 1$.

for tokens will incorporate this expectation. The developer should sell all his tokens today so to benefit from the expectation of his future effort and investment without actually exerting any effort or making any investment. Thus, we have an anti-coordination problem, which implies that the unique equilibrium is in mixed strategy: the price will be such that the developer is indifferent, and will randomize between $Q_{t+1} = 0$ and $Q_{t+1} = M$, as the next proposition shows.

Proposition 1 (Equilibrium post-ICO)**.** *In every period $t \in \{t_o+1, ..., T-1\}$ the developer sells all his tokens (so that $Q_{t+1} = 0$) with probability*

$$\alpha = \frac{(e^*(M))^2/2 + i^*(M)}{f(e^*(M), i^*(M))} \tag{7}$$

and purchases all tokens (so that $Q_{t+1} = M$) with probability $1-\alpha$. The price of tokens as a function of past effort and investment is

$$p_t = \frac{\sum_{s=1}^{t} f(e_s, i_s) + (1-\alpha)(T-t) f(e^*(M), i^*(M))}{R^{T-t} M}. \tag{8}$$

For intuition, note that $(e^*(M))^2/2 + i^*(M)$ is the cost generated by holding M tokens in period t, coming from the additional effort and investment that the developer will exert in period $t+1$. Instead, $f(e^*(M), i^*(M))$ is the benefit of holding M tokens in period t, coming from the increase in the value of these tokens due to the developer's effort and investment in period $t+1$. α is therefore equal to the ratio between cost and benefit of holding M tokens in period T. Because effort and investment are chosen optimally, the benefit should be at least as large as the cost, and therefore $\alpha \leq 1$.

Equation (8) can also be interpreted as the law of motion of the price, because it implies that, in every period $t \leq T$, the price of token will increase by:

$$\frac{(e^*(M))^2/2 + i^*(M)}{M \cdot R},$$

with probability:

$$1 - \frac{e^*(M))^2/2 + i^*(M)}{f(e^*(M), i^*(M))},$$

and will decrease by:

$$\frac{1}{M \cdot R}\left(f(e^*(M), i^*(M)) - (e^*(M))^2/2 + i^*(M))\right),$$

otherwise.

Period t_o (the ICO) is characterized by the fact that tokens are sold via an auction. Again, if $t_o = T$ then the developer will sell all his tokens at price given by (3). If instead $t_o < T$, at ICO (and contrary to all subsequent periods) the price of a token depends on the number of tokens sold, which is $M - Q_{t_o}$. The next proposition shows that, if $t_o < T$, then the developer chooses not to sell any token at ICO. The intuition is quite straightforward: the more tokens the developer sells at ICO, the lower future effort and investment will be. Because investors must be indifferent between purchasing at ICO or in the subsequent period, this implies that selling tokens at ICO lowers the price of the token at ICO and in all subsequent periods.

Proposition 2 (Equilibrium at t_o)**.** *If the ICO occurs before T, then the developer does not sell any tokens at ICO. It follows that $Q_{t_o+1} = M$ with probability 1. Effort and investment in all $t \leq t_o + 1$ are $e^*(M)$ and $i^*(M)$ with probability 1. If instead the ICO occurs at period T, then the developer sells all of his tokens at ICO.*

Period $t_o + 1$ is therefore the only period in which the market for tokens is open and the developer contributes to the development of the protocol with probability 1.

With respect to the optimal timing of the ICO, the previous proposition shows that optimal effort and investment between period 1 and $t_o + 1$ are $e^*(M)$ and $i^*(M)$. In all subsequent periods, instead, the existence of the market for tokens creates a commitment problem: the value of the decentralized digital platform is maximized when the developer holds M tokens in every period until T. In equilibrium, instead, from period $t_o + 2$ onward the developer exerts effort and invests with probability $1 - \alpha < 1$. Hence, if the ICO occurs in period $t_o < T - 1$, then, from period $t \leq t_o$ viewpoint, the developer's expected payoff is

$$V_{t-1}+\sum_{s=t}^{t_o+1}\left(f\left(e^*(M),i^*(M)\right)-1-\beta^{s-t}\frac{(e^*(M))^2}{2}\right)+(1-\alpha)\sum_{s=t_o+2}^{T}\left(f\left(e^*(M),i^*(M)\right)-1-\beta^{s-t}\frac{(e^*(M))^2}{2}\right).$$

If instead the ICO happens in period $T - 1$ or in period T, the developer's payoff is[23]

$$V_{t-1}+\sum_{s=t}^{T}\left(f\left(e^*(M),i^*(M)\right)-1-\beta^{s-t}\frac{(e^*(M))^2}{2}\right)$$

[23] Note that if the ICO is held in period $T - 1$, the developer will auction off 0 tokens, and will sell M tokens on the market in period T. If instead the ICO is in period T, the developer will sell all of his tokens via the auction. Holding the ICO in period $T - 1$ or period T, therefore, achieves the same outcome: the developer does not sell any tokens before period T and sells all of his tokens in period T.

Because effort and investment are chosen optimally, it must be that

$$f\left(e^{*}(M), i^{*}(M)\right) > \frac{\left(e^{*}(M)\right)^{2}}{2} + 1,$$

which implies that the developer's payoffs is maximized when the ICO is postponed to either period T or period $T-1$. The following proposition summarizes these observations.

Proposition 3 (Equilibrium t_o). *The developer holds the ICO either in period T or in period $T-1$.*

Proof. In the text. □

By postponing the ICO, the developer can commit to set high effort and investment in all future periods. Doing so maximizes the value of the decentralized digital platform and also the value of the developer's stock of tokens. As a consequence, in equilibrium, effort and investment are $e^{*}(M)$ and $i^{*}(M)$ with probability 1 in every period.

Corollary 1. *The cash constraint is never binding (and hence we are in the "rich developer" case) if and only if $A_1 \geq \sum_{t=1}^{T} \frac{i^{*}(M)}{R^{t-1}}$.*

Proof. Immediate from the above Proposition. □

That is, we are in the "rich developer" case whenever the developer does not need to sell tokens to finance the optimal amount of investment for T periods.

A final observation is that neither the developers' utility nor the value of the platform depend on the total stock of tokens M. From (5) and (6) we know that the equilibrium sequence of effort and investment depends on M exclusively via the share of tokens held by the developer. This share is 1 for $t \leq t_o$, and can be either 1 or 0 for $t_o < t \leq T$ (with the probability of being 1 or 0 given by 7, also independent from M). This implies that V_T and, as a consequence, $p_t M$ are independent from M. The developer's utility is therefore independent of M.

4.2.2 Poor developer

The rich developer case focuses on one side of seigniorage: the incentives provided to the developer. It shows that the developer will hold the ICO just before exiting the game, as a way to commit to the highest level of effort and investment in every period. There is, however, a second side of seigniorage: the ability to channel funds from investors to the developer, to be then used in the development of the protocol. I now introduce this aspect into the model by assuming that the developer is "poor", in the sense that $A_1 < \sum_{t=1}^{T} \frac{i^*(M)}{R^{t-1}}$: the developer cannot invest efficiently in all periods, and the cash constraint could be binding.

To focus on the role of the cash constraint, I introduce the following functional form:

$$f(e,i) \equiv e \cdot \mathbb{1}\{i \geq \bar{i}\}, \tag{A1}$$

where $\mathbb{1}\{\}$ is the indicator function. The choice of optimal investment, therefore, simplifies to the choice between two levels: $\bar{i}$ and 0. If there is positive investment, then effort increases the value of the decentralized digital platform linearly. I furthermore assume that the fixed cost is not too large:

$$\bar{i} < \frac{1}{2}. \tag{A2}$$

As it will become clear later, the above assumption eliminates trivial equilibria in which there is never positive effort nor investment.

The next proposition shows that, also here, in all post-ICO periods (except for T) the equilibrium is in mixed strategies.

Proposition 4 (Equilibrium post-ICO)**.** *In every period $t \in \{t_o+1, ..., T\}$ the developer sets effort and investment equal to*

$$e^*(Q_t, A_t) \equiv \begin{cases} \frac{Q_t}{M} & \text{if } i_t \geq \bar{i} \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

$$i^*(Q_t, A_t) \equiv \begin{cases} \bar{i} & \text{if } \bar{i} \leq \frac{1}{2}\left(\frac{Q_t}{M}\right)^2 \text{ and } \bar{i} \leq A_t \\ 0 & \text{otherwise.} \end{cases} \tag{10}$$

In period T the developer sells all his tokens with probability 1. In periods $t \in \{t_o+1, ..., T-1\}$, instead, there are several possible equilibria:

- *There is a "low" equilibrium in which the developer chooses $Q_{t+1} = 0$, so that subsequent* *effort and investment are zero.*[24] *Such equilibrium exists if and only if*

$$V_t \left(\frac{Q_t}{M} - \sqrt{2\bar{i}} \right) < \bar{i} + R(i^*(Q_t, A_t) - A_t).$$

- *There is a "high" equilibrium in which the developer sells all his tokens (so that* $Q_{t+1} = 0$*) with probability* α *and holds on to all his tokens (so that* $Q_{t+1} = M$*) with probability* $1 - \alpha$*, where*

$$\alpha = \frac{1}{2} + \bar{i}.$$

Such equilibrium exists if and only if

$$\left(V_t + \frac{1}{2} - \bar{i} \right) \left(1 - \frac{Q_t}{M} \right) \leq R(A_t - i^*(Q_t, A_t)) - \bar{i}.$$

- *There is a "medium" equilibrium in which the developer chooses* $Q_{t+1} = 0$ *with probability* α *and* $Q_{t+1} = Q^*_{t+1} < M$ *with probability* $1 - \alpha$*, where*

$$\alpha = \frac{1}{2} + \bar{i} \left(\frac{M}{Q^*_{t+1}} \right)^2.$$

Such equilibrium exists if and only if Q^*_{t+1} *solution to*

$$Q^*_{t+1} = Q_t - \frac{\bar{i} + R(i^*(Q_t, A_t) - A_t)}{\frac{V_t}{M} + \frac{Q^*_{t+1}}{2M^2} - \frac{\bar{i}}{Q^*_{t+1}}}$$

lies in $\left[M\sqrt{2\bar{i}}, M \right]$.

An equilibrium always exists. If $R(A_t - i^*(Q_t, A_t)) \geq \bar{i}$*, the equilibrium is unique, and is either a "high" equilibrium or a "medium" equilibrium. If* $R(A_t - i^*(Q_t, A_t)) < \bar{i}$ *instead there can be multiple equilibria: a low equilibrium as well as multiple "medium" equilibra might exist.*

Also here, when the market for tokens is open, there is the same anti-coordination problem discussed in the "rich developer" case. If investors expect the developer to hold a sufficient number of tokens for sure, then the current price should reflect future effort and investment.

[24] The developer could also set Q_{t+1} small but not exactly zero. As long as the subsequent effort and investment are zero, this would also be an equilibrium.

But given this the developer should sell all his tokens today. Similarly, if investors expect the developer to sell all his tokens, the price of tokens should be low. But given this, the developer should hold on a positive amount of tokens. Hence, also here, in equilibrium the developer will randomize between selling all tokens and holding the maximum amount of tokens.

Here, however, the maximum amount of tokens the developer can keep may be determined by the cash constraint. If this constraint is binding, then $Q^*_{t+1} < M$ is the largest token holdings allowing the developer to invest optimally in the following period. Importantly, if Q^*_{t+1} is too low (more precisely $Q^*_{t+1} < M\sqrt{2\bar{i}}$) then a developer setting $Q_{t+1} = Q^*_{t+1}$ will not *want* to invest in period $t+1$ despite being able to do so.

The important observation is that Q^*_{t+1} may not be uniquely determined, and hence there could be multiple equilibria. When $R(A_t - i^*(Q_t, A_t)) < \bar{i}$, after investing optimally in period t, the developer does not have enough funds to invest also in period $t+1$. Hence, the developer needs to sell tokens on the market to be able to invest in the following period. In this case, there could be a "low" equilibrium next to multiple "medium" equilibria. This equilibrium multiplicity arises from a coordination problem between the developer and investors. There could be an equilibrium in which investors expect future effort to be high, driving up p_t. Given this, the developer will be able to finance future investments while simultaneously holding a large fraction of tokens (i.e., Q^*_{t+1} is high). As a consequence, future expected effort will be high. Next to this equilibrium, there could be one in which investors expect future effort to be low (or zero), which implies that p_t is low. In this equilibrium, the developer needs to sell many tokens to finance future investment (i.e., Q^*_{t+1} is low), and therefore future expected effort will be low or even zero.

If instead $R(A_t - i^*(Q_t, A_t)) \geq \bar{i}$, after investing optimally in period t, the developer has enough funds to invest also in period $t+1$. In this case, the developer may purchase additional tokens on the market. The equilibrium is always unique, and could be either a "high" equilibrium, or a "medium" equilibrium. Finally, note that because of this multiplicity of equilibria, it is not possible to write down the law of motion of the price for tokens. Such law of motion can be specified only by first defining which equilibrium is expected to emerge in every period.

Consider now period t_o (the ICO).

Proposition 5. *In every $t \leq t_o$, optimal effort and investment are again given by* (9) *and* (10).

If $t_o = T$, the developer sell all his tokens at ICO..

If $t_o < T$ and $R(A_{t_o} - i^*(Q_{t_o}, A_{t_o})) \geq \bar{i}$, then the developer does not sell any token at ICO, so that, in equilibrium, $Q_{t_o+1} = M$.

If $t_o < T$ and $R(A_{t_o} - i^*(Q_{t_o}, A_{t_o})) < \bar{i}$, then define $\tilde{Q}$ as the largest solution to

$$A_{t_o} + \frac{\left(M - \tilde{Q}\right)}{R^{T-t_o}} \cdot \left(\frac{V_{t_o}}{M} + \frac{\tilde{Q}}{M^2}\right) - i^*(Q_{t_o}, A_{t_o}) = \bar{i}R^{-1}.$$

If $\tilde{Q} \in \left[M\sqrt{2\bar{i}}, M\right]$, then in equilibrium $Q_{t_o+1} = \tilde{Q}$. Effort and investment will be strictly positive in period t_o+1. If instead either $\tilde{Q}$ does not exist or $\tilde{Q} < M\sqrt{2\bar{i}}$, then any $Q_{t_o+1} \leq M$ is an equilibrium. In this case, there is no effort nor investment in period $t_o + 1$.

Remember that, if $t_0 < T$, then there is at least one period of development after the ICO. Because effort and investments are increasing in the amount of tokens held by the developer, and the price at ICO is proportional to that in the following period, the price for tokens at ICO is decreasing in the amount of tokens sold at ICO. Hence, the value of the stock of tokens M is decreasing in the amount of tokens sold at ICO.

Hence, similarly to the rich developer case, the developer will want to sell as few tokens as possible at ICO. If $R(A_{t_o} - i_{t_o}) \geq \bar{i}$, then the developer will be able to invest optimally in period $t_o + 1$ without selling any token at ICO—which is therefore the equilibrium like in the rich developer case. If instead $R(A_{t_o} - i_{t_o}) < \bar{i}$, to invest optimally in the following period, the developer needs to sell some tokens at ICO. But if the amount of tokens to be sold is too large, then in the following period the developer has no incentive to invest. In this case, the only possible equilibrium is one in which there is no investment nor effort following the ICO.

Hence, similarly to the "rich developer" case, also here the equilibrium at ICO is unique and in pure strategy. Also, period $t_o + 1$ may be the only period in which the market for tokens is open and the developer invests and exerts effort with probability 1. However, here the ICO may be unsuccessful—in the sense that the developer is unable to raise funds. This is more likely to happen when the developer's own funds A_{t_o} are low, and the cost of investing $\bar{i}$ is large.

With respect to the timing of the ICO, if the developer has enough resources to invest, then the logic discussed in the "rich developer case" applies here as well: the developer will not hold an ICO so to optimally invest in every period. The developer will hold the ICO as soon as his resources are insufficient to invest, so to continue the development of the platform. I summarize this observation in the following remark.

Remark 1. *In equilibrium, the developer holds the ICO in period* $t_o = \max\{s | \sum_{t=1}^{s} \frac{\bar{i}}{R^t} \leq A_1\}$.

Hence, by Proposition 4, when the market for tokens is open, there can be a "medium" or a "low" equilibrium (or both) but never a "high" equilibrium. This implies that, for $t \leq t_o$ we have $Q_t^* = M$, while for $t > t_o$ we have $Q_t^* < M$.

Finally, also here the equilibrium is independent of M. The above remark shows that the timing of the ICO does not depend on M. Similarly (9) and (10) show that optimal effort and investment depend on the share of tokens held by the developer. Furthermore, the share of tokens held by the developer in equilibrium does not depend on M—see the definition of Q_{t+1}^* in Proposition 4 and the definition of $\tilde{Q}$ in Proposition 5. This implies that, in every period t, the value of the platform V_t as well as the total value of the stock of tokens $p_t \cdot M$ is independent of M.

5 First best

In the first best, effort and investment are set to maximize the present discounted value of the social welfare generated by the platform. Here we consider the social welfare generated by the platform in every period to be sum of producer and consumer surplus, that is:[25]

$$SUR = \sum_{t=1}^{T} \frac{f(e_t, i_t)}{\tilde{D}(q^*)q^*} \left(\int_{q^*}^{\infty} \tilde{D}(q)dq + \int_{0}^{q^*} \tilde{S}(q)dq \right).$$

Social welfare is therefore:

$$SW \equiv \frac{1}{1-\beta} SUR$$

There are a number of differences between the first best and the equilibrium. To start, the developer may be poor, in which case he may liquidate all his tokens and as a consequence exert no effort nor invest—which is inefficient. But even assuming that the developer is rich, a second source of inefficiency emerges. In the first best, the platform generates a benefit for its users in every period, and the social welfare is the present discounted value of this benefit.

[25] This is the case if users' utilities are quasilinear and the marketplace created by the decentralized digital platform is perfectly competitive.

However, because the developer can sell the same token only once, he will only consider the impact of his effort/investment on the volume of transactions in the period in which he plans to sell it. The developer is therefore shortsighted, because he only considers the impact of his action in period T rather than in all subsequent periods. Finally, the developer maximizes the value of the platform, which depends on the willingness to pay/sell of the marginal buyer/seller. Social welfare instead depends on the willingness to pay/sell of all market participants, including the infra-marginal ones. Depending on whether equilibrium effort and investment affect mostly the marginal or the inframarginal buyer/seller, equilibrium effort and investment could be above or below their first best level.

More formally, the private and social benefit of effort and investment are, respectively:

$$\frac{\partial V_T}{\partial e_t} = \frac{\partial f(e_t, i_t)}{\partial e_t} \qquad \frac{\partial V_T}{\partial i_t} = \frac{\partial f(e_t, i_t)}{\partial i_t}$$

$$\frac{\partial SW}{\partial e_t} = \frac{1}{1-\beta}\frac{\partial f(e_t, i_t)}{\partial e_t}\frac{\int_{q^*}^{\infty} \tilde{D}(q)dq + \int_0^{q^*} \tilde{S}(q)dq}{\tilde{D}(q^*)q^*} \qquad \frac{\partial SW}{\partial i_t} = \frac{1}{1-\beta}\frac{\partial f(e_t, i_t)}{\partial i_t}\frac{\int_{q^*}^{\infty} \tilde{D}(q)dq + \int_0^{q^*} \tilde{S}(q)dq}{\tilde{D}(q^*)q^*}.$$

Equilibrium effort and investment will be *above* their first best levels whenever

$$\int_{q^*}^{\infty} \tilde{D}(q)dq + \int_0^{q^*} \tilde{S}(q)dq < (1-\beta)\tilde{D}(q^*)q^*$$

or

$$SUR < (1-\beta)V_T,$$

and will be below otherwise.

Figure 3 illustrates the two cases. In both cases V_T is constant, but in the first one the demand and the supply are less elastic than in the second case. As a consequence, surplus is large in the first case, but small in the second one. As it is clear, if demand and supply are sufficiently elastic, surplus will be arbitrarily small, and hence equilibrium effort and investment will be above the efficient level. If instead they are sufficiently inelastic, surplus will be large and therefore equilibrium effort and investment will be below the efficient level. The following Proposition summarizes there observations (its proof is omitted).

Proposition 6. *Consider the rich developer case. For given $\tilde{D}(q^*)q^*$, if either β is sufficiently high or supply and demand are sufficiently inelastic, then equilibrium effort and investment will be inefficiently low. If instead β is sufficiently low and supply and demand are sufficiently elastic, then equilibrium effort and investment will be inefficiently high.*

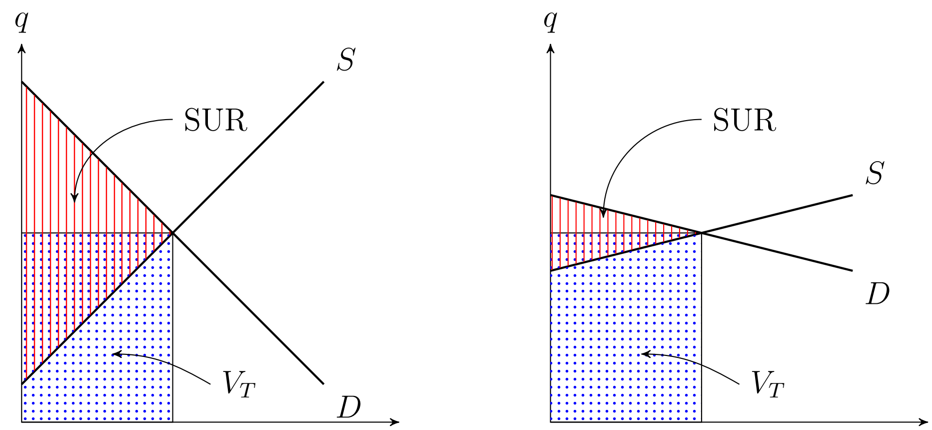

Fig. 3: Left panel: low elasticity of demand/supply, $CS > V_T$ and hence there is under-investment and under-provision of effort. Right panel: high elasticity of demand/supply, CS is arbitrarily small and hence there is over-investment and over-provision of effort.

To conclude, remember that in the poor developer case, after ICO, the developer invests and exerts effort with probability less than one. Furthermore, conditional on exerting effort, because in every period he holds less than the full stock of tokens, his level of effort and investment are lower than in the rich developer case. Hence, if there is under-provision of effort / under-investment when the developer is rich, the same holds when the developer is poor. But if there is over-provision of effort / over-investment when the developer is rich, this may not be the case when the developer is poor.

6 Discussion

6.1 Decentralized vs traditional platform

Suppose that the developer can choose between creating a standard platform or a decentralized digital platform. I start by considering an extreme case in which, if the developer creates a standard platform, he can then perfectly price discriminate: he can charge every seller his willingness to sell, and every buyer his willingness to buy. In this case, for given sequence of effort and investment, the market equilibrium is efficient, that is total surplus is maximized. The entire surplus is earned by the developer as profits, while buyers and sellers earn zero.

It turns out that, also in this extreme case, the developer may be better off creating a decentralized digital platform rather than a traditional platform. In case he creates a traditional platform, the developer payoff in period T is:

$$\frac{1}{1-\beta}SUR,$$

while in case he creates a decentralized digital platform his payoff in period T is V_T. The derivations in the previous section show that, for every sequence of effort and investment, SUR tends to zero as demand/supply become more elastic. In this case the developer is better off by creating a decentralized digital platform.

If the developer/monopolist cannot perfectly price discriminate then two things will happen. First, the prices charged by the monopolist will be distortionary, and hence total surplus will decrease. At the same time, some buyers and sellers may earn positive payoffs. As a consequence, the monopolist's total profits are now below $\frac{1}{1-\beta}SUP$. The developer's payoff in case he creates a decentralized digital currency is again V_T. This implies that, again, the developer will prefer to crease a decentralized digital platform when the elasticity of demand and supply is high.[26]

I summarize these observations in the following remark:

Remark 2. *Suppose that the developer can choose between creating a decentralized digital platform and a traditional platform. If, after creating a traditional platform, he can perfectly price discriminate, then he will create a decentralized digital platform if and only if*

$$\frac{1}{1-\beta}SUR < V_T,$$

which is more likely to hold when supply and demand are elastic. If instead he cannot perfectly price discriminate, he will create a decentralized digital platform if the above condition holds, but also in cases in which the above condition is violated but SUR is sufficiently low.

Finally, note that Proposition 6 together with the above remark imply that, if the developer can perfectly price discriminate, upon observing the creation of a decentralized digital

[26] This is related but not identical to Goldstein et al. (2019), who argue that by creating a decentralized digital platform, an entrepreneur commits not to use his monopoly power to distort future allocation. The difference is that, here, also in case in which monopoly pricing is not distortionary (i.e., perfect price discrimination) the developer may prefer to create a decentralized digital platform. Hence, the distortion introduced by monopoly power explains only partially the choice of whether to have a decentralized digital platform or a monopoly. I believe this is due to the fact in Goldstein et al. (2019) the token price at the end of the developer's life is exogenously given, while here this price is endogenous and depends on the volume of transactions on the platforms.

platform, we should infer that effort and investment are above their efficient levels (at least in the rich developer case). If instead the developer cannot perfectly price discriminate, there are also cases in which a decentralized digital platform is created and then there is under-provision of effort and investment.

6.2 Traditional investor

In the rich developer case, the developer uses his own resources to finance the investment in the protocol, so that seigniorage plays a role exclusively because it generates profits and provides incentives. In the poor developer case, seigniorage has the additional role of providing resources to be invested into the development of the protocol. The comparison between the two cases shows that the use of seigniorage to finance the investment in the protocol is a second-best response to the developer's lack of resource, because the value of the decentralized digital platform (and the developer's payoff) is always higher in the rich developer case.

This observation suggests that an external investor (call it a *traditional investor*, possibly a venture capital fund or a business angel) could provide capital to the developer so as to move from the poor developer to the rich developer case.[27] Under perfect contracting, therefore, in the poor developer case the traditional investor would always provide funds to the developer. If instead the traditional investor and the developer are constrained in the type of contracts they can sign—for example because effort is not contractible—then the external investor may not provide funds even if it is welfare improving to do so. In this case, the development of the platform can only be financed by holding an early ICO (i.e., an ICO before period $T-1$).

To illustrate this point, assume that the developer and the investor are limited to contracts of the following type: the investor provides an amount of cash equal to I at the beginning of the game, and receives a fraction of tokens ρ at ICO. If I is sufficiently large, such a contract has the advantage of postponing the ICO, and therefore extending the period in which the developer develops the protocol with probability 1. However, it also implies that

[27] Regarding the fact that traditional investors are investing in companies that subsequently run an ICO, see https://www.cbinsights.com/research/blockchain-ico-equity-financing-vc-investments/ (accessed on July 24, 2020) and https://www.bloomberg.com/news/articles/2017-10-03/hedge-funds-flip-icos-leaving-other-investors-holding-the-bag (accessed on July 24, 2020). See also a recent paper by Chod and Lyandres (ming), who compare traditional venture capital financing with financing via ICO under the assumption that they are perfect substitutes, and derive conditions under which one dominates the other.

in every period of development the level of effort and investment will be reduced, because the developer anticipates that his payoff will be $(1-\rho)Mp_T$. Clearly, there are cases in which the outside investment will not happen. For example, if the developer already has enough funds to invest efficiently in the first $T-2$ periods , then external financing allows to invest and exert effort with probability 1 in one extra period, at the expense of reducing the level of investment and effort during T periods. If T is very large, then the developer may choose to hold the ICO in period $T-2$ rather than accepting I from the external investor.

Overall, introducing a traditional investor is welfare-increasing: when a contract between the developer and the investor is signed, it must be the case that the value of the decentralized digital platform increases (relative to no outside investment). But contractual frictions may prevent the traditional investor and the developer from finding an agreement. In this case, the developer may hold an early ICO.

6.3 Asymmetric information

The results derived above largely extend to a situation in which the developer's productivity is private information. In this case, if the market for tokens is open, for a given price for tokens there is a threshold productivity above which the developer wants to hold all tokens, and below which the developer wants to sell all tokens. In every period, if the developer is more productive that the market expectation, he will purchase tokens and develop the protocol with probability 1. If the developer is less productive than the market expectation, he will sell all tokens and not develop the protocol.

The important observation is that the productivity of the developer will be revealed over time. In the moment it is fully revealed, the equilibrium of the game is again the one derived in the previous section. Asymmetry of information therefore implies that developers with above average productivity may contribute to the development of the protocol with probability 1 for some periods. Conversely, developers with below average productivity do not contribute to the protocols initially. After the developer's productivity is revealed, he will contribute with probability less than 1, as in the symmetric information case.

6.4 Multiple, heterogeneous developers

Suppose that there is a population of developers indexed by j, each characterized by a productivity parameter q_t^j (commonly known) so that effort and investment by developer j

in period t generates an increase in the value of the decentralized digital platform equal to $q_t^j f(e_t^j, i_t^j)$. If all developers are "rich" (that is, the cash constraint is never binding for any developer) and there is a market for tokens, then in every period t the equilibrium price must be such that the developer with the largest q_{t+1}^i is indifferent between holding all tokens or no tokens.[28] If, furthermore, $\max_j q_t^j$ is constant over time, then the model is formally identical to the one just solved. The only difference is its interpretation: in every period a different developer (the most productive in that period) may purchase tokens and contribute to the development of the platform.

Contrary to the case considered in the body of the text, now the existence of a market for tokens generates an allocative efficiency: the most productive developer works on the project in every period. Of course, as we already saw, this developer contributes to the project only with some probability. It follows that holding an ICO has an additional benefit because it allows the most productive developer to contribute to the project in every period. Absent the ICO, instead, the initial developer will set high effort and investment in every period, but this developer may not be the most productive developer who could work on the project.

If instead some developers are "poor" (i.e., the cash constraint may be binding), then the most productive developer in a given period may not have enough resources to purchase tokens and/or invest efficiently. The identity of the developer that, in every period, develops the platform (with some probability) depends partly on productivity and partly on wealth.

7 Conclusion

An attentive reader may have noticed a troubling aspect of the model. In equilibrium, the developer earns positive profits, users enjoy the full surplus generated by the platform, while at the same time investors are left indifferent. This implies that the sum of the players' payoffs exceeds the social surplus generated by the creation of the platform. While this result is correct, it is an artifact of the partial-equilibrium nature of the model. In a general equilibrium framework, from period T onward, introducing the token increases the supply of money in the economy by an amount equal to the value of the stock of tokens (which

[28] Suppose not: then the best developer strictly prefers to hold all tokens and exert the maximum level of effort and investment in the following period. However, in that case, this developer's contribution to the protocol should already be accounted for in the current price, which implies that he strictly prefers to sell all of his tokens, leading to a contradiction.

is also the developer's profits), leading to an increase in the economy-wide price level.[29] Initial holders of cash are therefore made worse off by the introduction of the token. In this general-equilibrium framework, the developer should anticipate that an increase in the value of the decentralized digital platform will lead to an increase both of the price of the token and of the economy-wide price level, therefore reducing the benefit of exerting effort and developing the protocol (relative to the partial-equilibrium case considered in the body of the paper.) Also, in general equilibrium, before period T the investment in tokens reduces the amount invested in the risk-free asset, therefore increasing its return. This implies that the developer's effort increases the return demanded by investors for holding tokens. The effect of the developer's effort on the economy-wide price level and on the risk-free return is, however, likely to be negligible and hence a partial-equilibrium analysis seems appropriate.

During the writing of the first version of this paper, there was a robust debate relative to whether tokens such as the ones studied in this paper (i.e., those associated with a decentralized digital platform, sometimes called *utility tokens*) should be considered securities, and hence subject to security regulation. Over the past few years most regulatory bodies started considering tokens associated with decentralized digital platform in the early development stage as securities, while tokens associated with decentralized digital platform that are already sufficiently functional as not securities.[30] The model suggests that the price of the token is less volatile and less dependent on the developer's actions after period T than before period T. Because period T marks the end of the development of the platform, the model provides support to the current regulatory stance.

The model abstracts away from competition, either from other open-source blockchain-based protocols or traditional companies. In ongoing work (Canidio, 2020), I consider a simplified version of the model presented here, in which multiple developers can hold ICOs and enter the market. In that model, the fact that developers hold an ICO (instead of using their own resources) encourages other developers to also hold ICOs and enter the market.

[29] For general equilibrium models in which the economy-wide price level depends on the presence of a cryptocurrency (Bitcoin), see Schilling and Uhlig (2019) and Garratt and Wallace (2018).

[30] For example, the Security and Exchange Commission (SEC) does not consider Bitcoin nor ETH securities, on the ground that, at this point, "there is no central party whose efforts are a key determining factor in the enterprise" (see https://www.cnbc.com/2018/06/14/bitcoin-and-ethereum-are-not-securities-but-some-cryptocurrencies-may-be-sec-official-says.html accessed on July 24, 2020). However, recent ICOs of tokens associated with platforms at a very early development stage have been prosecuted (see the case of Telegram's ICOs - https://www.sec.gov/news/press-release/2019-212 accessed on July 24, 2020). In most cases, this simply implies that it is not possible to sell tokens at ICO to people residing in the US.

Hence, despite the fact that ICOs weaken incentives, they also stimulate competition. Under some conditions, ICOs are welfare improving (relative to a situation in which the development of the platform is fully self financed).

The timing of the ICO is also likely to be affected by competition (an aspect not studies in Canidio, 2020). Remember that, in the model, users enjoy the full surplus generated by the protocol. Hence, a competing open-source blockchain-based protocol (or a traditional company) can attract users only if it can generate a higher surplus, either by providing a better technological solution or by attracting a larger user base. This could affect the timing of the ICO. If there are "winner takes all" dynamics and network effects, it is conceivable that the developer will want to anticipate the ICO, so as to build a sufficiently large user base and prevent the entrance of competitors. However, assuming that the source code is disclosed at ICO, holding an ICO earlier also gives the opportunity for competitors to copy the code and imitate some features. The full treatment of this case is left for future work.

A Mathematical appendix

Proof of Lemma 1. Consider period t such that $t_o \leq t < T$. Defined the *expected future normalized price* of tokens in period $t < s < T$ as $\tilde{p}_s = \frac{E[p_s]}{R^{s-t}}$.

If the expected future normalized price of tokens is strictly increasing anytime between t and T, then the demand for tokens is not defined in some periods, which cannot be an equilibrium. If the expected future normalized price for tokens is strictly decreasing over time but never increasing, then there is a period in which the expected future normalized price for tokens achieves a maximum. In this period, the demand for tokens from investors is zero, which implies that the maximum expected future normalized price for tokens between t and T must be zero. This is a contradiction because if the maximum expected future normalized price is zero, then the sequence of expected future normalized prices is constant at zero.

Hence, in every period $t \leq T$, in equilibrium the sequence of expected future normalized prices must be constant. We can therefore write the expected future normalized price as $\tilde{p}_t = E[\tilde{p}_T]$. Since the sequence of effort and investment from period 1 to t is known, the expectation is taken exclusively with respect to the future sequence of investments and effort, leading to equation (4).

□

Proof of Lemma 2. By the envelope theorem and Lemma 1, we can compute

$$\frac{\partial \tilde{U}(Q_t)}{\partial Q_t} = f(e^*(Q_t), i^*(Q_t)).$$

For Q_t such that both $e^*(Q_t)$ and $i^*(Q_t)$ are constant, we have that $\frac{\partial \tilde{U}(Q_t)}{\partial Q_t}$ is constant. For Q_t such that either $e^*(Q_t)$ or $i^*(Q_t)$ are strictly increasing, we have that $\frac{\partial \tilde{U}(Q_t)}{\partial Q_t}$ is strictly increasing. By assumption, there are $Q_t \leq M$ such that either $e^*(Q_t)$ or $i^*(Q_t)$ are strictly increasing. □

Proof of Proposition 1. I first show that the equilibrium in period $T-1$ is indeed in mixed strategies. I then use this fact to show that the equilibrium in all periods $t \in \{t_o+1, ..., T-1\}$ is in mixed strategies.

Consider the choice of Q_T in period $T-1$. As already discussed in the body of the text, the developer's problem has a corner solution: depending on p_{T-1}, the developer will either sell all of his tokens (and earn $Q_{T-1}p_{T-1}\beta R$), purchase as many tokens as possible (and earn

$\beta\tilde{U}(M) - (M - Q_{T-1})p_{T-1}\beta R)$, or be indifferent between these two options. Using the fact that $\beta R = 1$, the price at which the developer is indifferent is:

$$Rp_{T-1} = \frac{\tilde{U}_T(M)}{M} = \frac{V_{T-1} + f(e^*(M), i^*(M))}{M} - \frac{(e^*(M))^2/2 + i^*(M)}{M}, \tag{11}$$

where $\frac{V_{T-1}+f(e^*(M),i^*(M))}{M}$ is the period T price in case the developer holds M tokens at the beginning of period T.

As already discussed in the body of the text, we have an anti-coordination problem between investors and the developer, which implies that the unique equilibrium is in mixed strategy: the price will be such that the developer is indifferent, and the developer will randomize between $Q_T = 0$ and $Q_T = M$. More precisely, if the developer sells all of his tokens in period $T - 1$, then the price in period T will be $\frac{V_{T-1}}{M}$. If instead the developer purchases M tokens in period $T - 1$, then $p_T = \frac{V_{T-1}+f(e^*(M),i^*(M))}{M}$. Because investors must be indifferent between purchasing in period T or period $T - 1$, it must be that:

$$Rp_{T-1} = \frac{V_{T-1}}{M} + (1 - \alpha_{T-1})\frac{f(e^*(M), i^*(M))}{M},$$

where α_{T-1} is the probability that the developer sells all of his tokens in period $T - 1$, which using (11) can be written as:

$$\alpha_{T-1} = \frac{(e^*(M))^2/2 + i^*(M)}{f(e^*(M), i^*(M))}.$$

Therefore, in equilibrium, in period $T - 1$ the developer is indifferent between selling all of his tokens or keeping all of his tokens. It follows that I can write:

$$\tilde{U}_{T-1}(Q_{T-1}) = \max_{e_{T-1}, i_{T-1}, e_T, i_T} \left\{ -i_{T-1} - \frac{e^2_{T-1}}{2} + Q_{t-1} \cdot p_{T-1} \right\},$$

that is, I can write the utility in period $T - 1$ assuming that the developer sells all of his tokens in period $T - 1$. This immediately implies that the problem in period $T - 2$ is identical to the problem in period $T - 1$. That is, in period $T - 2$ the developer is indifferent between $Q_{T-1} = 0$ and $Q_{T-1} = M$ whenever

$$Rp_{T-2} = \frac{\tilde{U}_{T-1}(M)}{M} = \frac{V_{T-2} + f(e^*(M), i^*(M))}{M} - \frac{(e^*(M))^2/2 + i^*(M)}{M},$$

and investors are indifferent between purchasing in period $T-2$ or $T-1$ whenever

$$Rp_{T-1} = \frac{V_{T-2}}{M} + (1-\alpha_{T-2})\frac{f(e^*(M), i^*(M))}{M}.$$

Using the above two expression to solve for α_{T-2} we again get

$$\alpha_{T-2} = \alpha_{T-1} = \frac{(e^*(M))^2/2 + i^*(M)}{f(e^*(M), i^*(M))}.$$

The statement of the proposition follows by applying the same argument recursively to all periods after the ICO. □

Proof of Proposition 2. Again, in equilibrium, investors must be indifferent, and therefore, for any number of tokens sold at ICO, it must be that $p_{t_o} = \frac{p_{t_o+1}}{R}$. Hence, whenever $t_o < T$, the developer's problem at ICO can be written as:

$$\begin{aligned}
&\max_{Q_{t_o+1}} \left\{(M - Q_{t_o+1})p_{t_o} + \beta\tilde{U}_{t_o+1}(Q_{t_o+1})\right\} = \\
&\max_{Q_{t_o+1}} \left\{(M - Q_{t_o+1})\frac{p_{t_o+1}}{R} + \beta \max_{e_{t_o+1}, i_{t_o+1}} \left\{Q_{t_o+1}\cdot p_{t_o+1} - \frac{1}{2}e^2_{t_o+1} - i_{t_o+1}\right\}\right\} \leq \\
&\max_{Q_{t_o+1}} \left\{\max_{e_{t_o+1}, i_{t_o+1}} \left\{\beta\cdot Q_{t_o+1}\cdot p_{t_o+1} - \beta\cdot\frac{1}{2}e^2_{t_o+1} - \beta\cdot i_{t_o+1} + (M - Q_{t_{o+1}})\frac{p_{t_o+1}}{R}\right\}\right\} = \\
&\max_{e_{t_o+1}, i_{t_o+1}} \left\{\beta M\cdot p_{t_o+1} - \beta\frac{1}{2}e^2_{t_o+1} - \beta i_{t_o+1}\right\} = \beta\tilde{U}_{t_o+1}(M),
\end{aligned}$$

where the first and the last equality follow from writing $\tilde{U}_{t_{o+1}}(Q_{t_{o+1}})$ explicitly.[31] The developer therefore anticipates that the price of tokens at ICO will be proportional to the price of tokens in the following period, independently from how many token he sells at ICO. The number of tokens sold, however, determines the equilibrium level of effort and investment in period t_{o+1}, and hence the price both at ICO and in the following period. This price is maximized when no tokens are sold at ICO, and hence effort and investment in period t_{o+1} are at their maximum level. □

Proof or Proposition 4. I follow the same steps described in the proof of Proposition 1. First, I consider period $T-1$, derive optimal effort and investment and show that the equilibrium

[31] Remember that in every post ICO period the developer is indifferent between selling all his tokens or holding all tokens. Hence the utility in period t_o+1 is equal to the utility the developer earns if he sells all of his tokens in period t_{o+1} and never purchases them again.

must be in mixed strategy. Then, I argue that the equilibrium in all periods $t \in \{t_o + 1, ..., T-2\}$ is identical to that in period $T-1$.

Period-T effort and investment are:

$$e^*_T(Q_T, A_T) \equiv \begin{cases} \frac{Q_T}{M} & \text{if } i_T \geq \bar{i} \\ 0 & \text{otherwise} \end{cases} \tag{12}$$

$$i^*_T(Q_T, A_T) \equiv \begin{cases} \bar{i} & \text{if } \bar{i} \leq \frac{1}{2}\left(\frac{Q_T}{M}\right)^2 \text{ and } \bar{i} \leq A_T \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

Define:

$$\hat{Q} \equiv M\sqrt{2\bar{i}}, \tag{14}$$

so that the developer invests whenever $\bar{i} \leq A_T$ and $Q_T \geq \hat{Q}$, and will not invest otherwise. Note that, by (A2), we have $\hat{Q} < M$. Given this, it is immediate to check that $U_T(Q_T, A_T)$ is strictly convex in Q_T whenever $\bar{i} \leq A_T$ and $Q_T \geq \hat{Q}$, and is otherwise linear in Q_T. $U_T(Q_T, A_T)$ is linearly increasing in A_T with slope 1 (corresponding to the marginal utility of consumption), and has an upward discontinuity at $A_T = \bar{i}$ if and only if $Q_T \geq \hat{Q}$.

Consider now the choice of Q_T in period $T-1$. For a given market price p_{T-1}, the developer's utility as a function of Q_T is:[32]

$$\beta U_T\left(Q_T, A_T\right) + \lambda_{T-1}(A_{T-1} - i_{T-1} - p_{T-1}\max\left\{Q_T - Q_{T-1}, 0\right\}).$$

where λ_{T-1} is the Lagrange multiplier of the cash constraint, A_T are the assets available at the beginning of period T:

$$A_T = R\left(A_{T-1} + \left(Q_{T-1} - Q_T\right) \cdot p_{T-1} - i_{T-1}\right),$$

[32] The utility in period $T-1$ also depends on effort exerted in that period, which is sunk when Q_T is chosen.

and therefore

$$
U_T(Q_T, A_T) = \begin{cases} Q_T \frac{V_{T-1}}{M} + \frac{1}{2}\left(\frac{Q_T}{M}\right)^2 + A_{T-1}R + (Q_{T-1} - Q_T)\cdot p_{T-1}R - i_{T-1}R - \bar{i} & \text{if } Q_T \geq \hat{Q} \\ & \text{and } R(A_{T-1} + (Q_{T-1} - Q_T)\cdot p_{T-1} - i_{T-1}) \geq \bar{i} \\ Q_T \frac{V_{T-1}}{M} + A_{T-1}R + (Q_{T-1} - Q_T)\cdot p_{T-1}R - i_{T-1}R & \text{otherwise,} \end{cases} \tag{15}
$$

Define Q_T^* as the largest Q_T such that the developer can invest $\bar{i}$ in period T: that is, the largest Q_T such that $A_T = R\left(A_{T-1} + (Q_{T-1} - Q_T)\cdot p_{T-1} - i_{T-1}\right)$ is at least $\bar{i}$:

$$
Q_T^* \equiv Q_{T-1} - \frac{i_{T-1} + \bar{i}R^{-1} - A_{T-1}}{p_{T-1}} \tag{16}
$$

Note that there are three possibilities:

1. Q_T^* may be greater than M, in which case, for given p_{T-1}, the developer is able to hold on to the entire stock of tokens and still invest $\bar{i}$ in the following period.

2. $Q_T^* > 0$ may not exist, which implies that, at a given p_{T-1}, it is not possible for the developer to raise enough to then invest $\bar{i}$

3. for given P_{T-1}, $Q_T^* \in [0, M]$. In this case, note that if the developer sets $Q_T = Q_T^*$ then $A_T = R\left(A_{T-1} + (Q_{T-1} - Q_T)\cdot p_{T-1} - i_{T-1}\right) = \bar{i}$, which implies that $Q_T = Q_T^*$ satisfies the period $T-1$ cash constrain.

Note also that if $R(A_{T-1} - i_{T-1}) \geq \bar{i}$, then for given investment in period $T-1$, the developer's remaining funds are sufficient to invest in period T. In this case $Q_T^* \geq Q_{T-1}$, that is, the developer can purchase additional tokens on the market and still be able to invest in period T. Hence, we must be either in case 1 or 3 above. On the other hand, when $R(A_{T-1} - i_{T-1}) < \bar{i}$ (i.e. the developer's remaining funds are insufficient to invest in period T), then necessarily $Q_T^* < Q_{T-1}$: the developer needs to sell some token in period $T-1$ in order to invest in period T. Hence, we must be either in case 2 or 3 above.

In the above derivations, p_{T-1} is taken as given. In equilibrium, however, the price of tokens in every period is endogenous and depends on the investors beliefs about the developer's behavior. By using the fact p_{T-1} depends on Q_T, I can derive the equilibrium of the game. It turns out, that there are three possible equilibria.

“high” equilibrium ($Q_T^* \geq M$) This case is identical to the “rich developer” case. The developer’s continuation value is strictly increasing, and strictly convex for $Q_T \geq \hat{Q}$. Again, in equilibrium the developer randomizes between $Q_T = 0$ and $Q_T = M$.

For the developer to be indifferent, it must be that:

$$p_{T-1}R = \frac{U_T(M, A_T)}{M} = \frac{1}{M}\left(V_{T-1} + \frac{1}{2} - \bar{i}\right) \tag{17}$$

For investors to be indifferent, the developer should sell all his tokens with probability α_{T-1} such that

$$p_{T-1}R = \alpha_{T-1}\frac{V_{T-1}}{M} + (1-\alpha_{T-1})\frac{V_{T-1}+1}{M} = \frac{V_{T-1}}{M} + \frac{1-\alpha_{T-1}}{M} \tag{18}$$

Putting the above two expressions together we get:

$$\alpha_{T-1} = \frac{1}{2} + \bar{i}$$

This is indeed an equilibrium if:

$$Q_T^* = Q_{T-1} - \frac{i_{T-1} + \bar{i}R^{-1} - A_{T-1}}{\frac{1}{MR}\left(V_{T-1} + \frac{1}{2} - \bar{i}\right)} \geq M$$

or

$$\left(V_{T-1} + \frac{1}{2} - \bar{i}\right)\left(1 - \frac{Q_{T-1}}{M}\right) \leq R(A_{T-1} - i_{T-1}) - \bar{i} \tag{19}$$

Note that the above is possible only if $R(A_{T-1} - i_{T-1}) > \bar{i}$, that is, the developer does not need to sell tokens on the market in period $T-1$ to be able to invest in period T.

“low” equilibrium (either $Q_T^* > 0$ does not exist or $Q_T^* < \hat{Q}$) In this case, there is no Q_T for which there will be positive effort and investment in the future. The equilibrium price is

$$p_{T-1}R = p_T = \frac{V_{T-1}}{M}.$$

At such price, we have

$$Q_T^* \equiv Q_{T-1} - \frac{i_{T-1} + \bar{i}R^{-1} - A_{T-1}}{\frac{V_{T-1}}{MR}}$$

which always exist but may be negative. Because $\hat{Q} > 0$, then, the "low" equilibrium exists if and only if $Q_T^* < \hat{Q}$, which using (14) and (16), becomes:

$$V_{T-1}\left(\frac{Q_{T-1}}{1M} - \sqrt{2\bar{i}}\right) < \bar{i} + R(i_{T-1} - A_{T-1}). \tag{20}$$

Note that the above equilibrium can exist only if $R(A_{T-1} - i_{T-1}) < \bar{i}$, that is, if the developer does not sell tokens in period $T-1$ he will be unable to invest in period T.

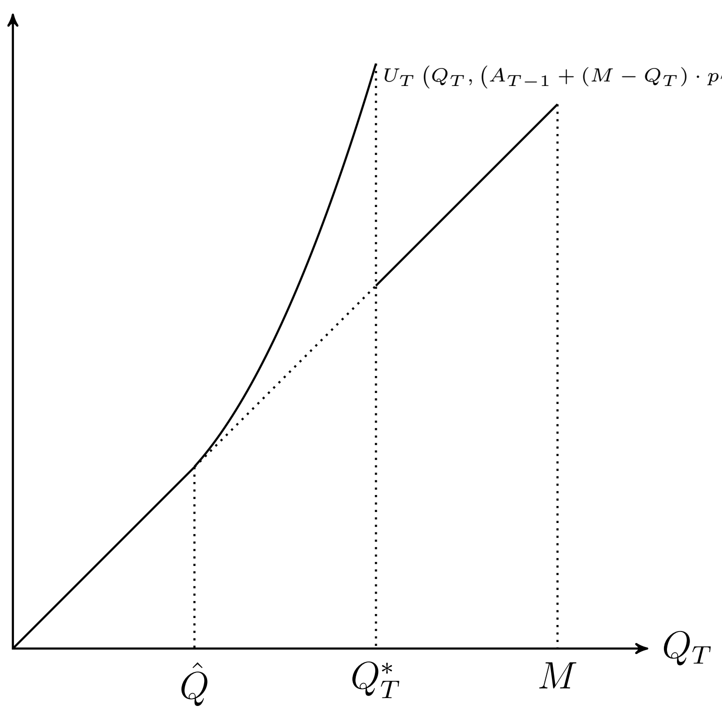

Fig. 4: Continuation value as a function of Q_T.

"medium" equilibrium ($Q_T^* \in [\hat{Q}, M]$) In this case, the previous discussion implies that the continuation value

$$U_T\left(Q_T, R\left(A_{T-1} + (Q_{T-1} - Q_T)\cdot p_{T-1} - i_{T-1}\right)\right),$$

is strictly convex in Q_T for $Q_t \in [\hat{Q}, Q_T^*]$ and is linearly increasing in Q_T for $Q_t \notin [\hat{Q}, Q_T^*]$. Furthermore, if $\hat{Q} < Q_T^*$ then the continuation value has a downward discontinuity at Q_T^* (see Figure 4). The argument presented for the "rich developer" case applies here as well:

the only possible equilibrium is one in which the developer randomizes between $Q_T = 0$ and $Q_T = Q_T^*$. For the developer to be indifferent, it must be that:

$$p_{T-1}R = \frac{U_T(Q_T^*, \bar{i})}{Q_T^*} = \frac{V_{T-1}}{M} + \frac{Q_T^*}{2M^2} - \frac{\bar{i}}{Q_T^*} \tag{21}$$

For investors to be indifferent, the developer should sell all his tokens with probability α_{T-1} such that

$$p_{T-1}R = \alpha_{T-1}\frac{V_{T-1}}{M} + (1-\alpha_{T-1})\left(\frac{V_{T-1}}{M} + \frac{Q_T^*}{M^2}\right) \tag{22}$$

Putting the above two expressions together we get:

$$\alpha_{T-1} = \frac{1}{2} + \bar{i}\left(\frac{M}{Q^*}\right)^2$$

By using (16) and (21), we can express Q_T^* as:

$$Q_T^* = Q_{T-1} - \frac{\bar{i} + R(i_{T-1} - A_{T-1})}{\frac{V_{T-1}}{M} + \frac{Q_T^*}{2M^2} - \frac{\bar{i}}{Q_T^*}} \tag{23}$$

Hence, such "medium" equilibrium exists if and only if the solution to the above equation is in $[\hat{Q}, M]$.

A few relevant observations:

- it is easy to check that, the RHS of (23) is below its LHS at $Q_T^* = \hat{Q}$ if and only if (20) holds. At the same time the RHS of (23) is above its LHS at $Q_T^* = M$ if and only if (19) holds.
- by continuity, a "medium" equilibrium must exist whenever both (20) and (19) hold. A "medium" equilibrium must exist also when neither (20) nor (19) hold.
- In all other cases, such "medium' equilibrium may not exist. However, either a "low" or a "high" equilibrium will exist.
- $R(A_{T-1} - i_{T-1}) \geq \bar{i}$, then the LHS of (23) is strictly increasing while its RHS is strictly decreasing. Furthermore, we established earlier that, in this case, (20) must be violated. Hence, a unique "medium" equilibrium exists if (19) is violated.
- $R(A_{T-1} - i_{T-1}) < \bar{i}$. In this case, both the RHS and the LHS of (23) are strictly increasing. Furthermore, we established earlier that (19) must be violated. Hence,

if (20) is also violated, then there must be at least one "medium" equilibrium. If instead (20) holds (so that a "low" equilibrium exists) there could still be one (or more) "medium" equilibrium.

Hence, an equilibrium always exists. If $R(A_{T-1} - i_{T-1}) \geq \bar{i}$, there can be either a "high" or a "medium" equilibrium. In this case, the equilibrium is unique. If $R(A_{T-1} - i_{T-1}) < \bar{i}$, there can be multiple equilibria: there can be both a low and multiple medium equilibria.

Finally, to derive the equilibrium in previous periods, I employ the same argument presented in the proof of Proposition 1. In equilibrium, the developer's continuation utility is equal to the utility he would get if he was to sell all his tokens in period $T-1$. In previous periods, therefore, the developer will behave as if his last period of development was $T-1$. Optimal effort and investment in period $T-1$ are, again, given by (12) and (13). But then, the equilibrium in period $T-2$ when choosing Q_{T-1} is again in mixed strategy, and is identical to the one derived earlier. A recursive argument implies that, in every period post-ICO, the developer will behave as if the following period was the last period of development. Hence, the set of equilibria is the same in every post-ICO period.

□

Proof of Proposition 5. Proposition 4 implies that, from period t_o view point, the developer's continuation utility is equal to the utility he would earn if he was to sell all his tokens in period t_o+1 and never purchase them again. This implies that optimal effort and investment in period t_o+1 are given, again, by (9) and (10). Also here, I define

$$\hat{Q} \equiv M\sqrt{2\bar{i}},$$

as the minimum token holdings such that the developer will want to invest.

At ICO, the developer chooses Q_{t_o+1} (i.e., the amount of tokens not to sell) so to maximize

$$\beta U_{t_o+1}\left(Q_{t_o+1}, R\left(A_{t_o} + (M - Q_{t_o+1}) \cdot p_{t_o} - i_{t_o}\right)\right).$$

There are two important differences with respect to the sale of tokens on the market (considered in the proof of Proposition 4). First, here the period-t_o cash constraint is not binding, the reason being that at ICO the developer is, by definition, a net seller. Second, when selling on the market, the developer takes as given the price of tokens (which depends on investor's expectations relative to his future effort). At ICO, instead, the price of tokens is set after the developer announces how many tokens to sell. Hence, because $p_{t_o+1} = Rp_{t_o}$, then the price at which the developer can sell his tokens (either at ICO or in the following period) reacts to the number of tokens sold.

When choosing how many tokens to sell, the developer maximizes:[33]

$$\beta U_{t_o}\left(Q_{t_o+1}, R\left(A_{t_o}+\left(Q_{t_o}-Q_{t_o+1}\right)\cdot p_{t_o}-i_{t_o}\right)\right)=\begin{cases} M\cdot p_{t_o}-\frac{1}{2}\left(\frac{Q_{t_o+1}}{M}\right)^2+\left(A_{t_o}-i_{t_o}\right)-\beta\bar{i} & \text{if } Q_{t_o+1}\geq\hat{Q} \\ & \text{and } A_{t_o}+\left(M-Q_{t_o+1}\right)\cdot p_{t_o}-i_{T-1}\geq\bar{i}R^{-1} \\ M\frac{V_{T-1}}{MR^{T-t_o}}+A_{T-1}-i_{T-1} & \text{otherwise} \end{cases} \tag{24}$$

where

$$p_{t_o}=\frac{1}{R^{T-t_o}}\left(\frac{V_{t_o}}{M}+\frac{Q_{t_o+1}}{M^2}\right).$$

is the price at ICO in case there is positive investment and effort in the following period (but no investment nor effort afterward). Instead, $\frac{V_{T-1}}{MR^{T-t_o-1}}$ is the price of tokens in period t_o+1 assuming no effort nor investment in period t_o+1 and in all subsequent periods.

It is easy to check that the above continuation value is strictly increasing in Q_{t_o+1} as long as the developer will be able to invest in the following period. That is, anticipating that the amount of tokens not sold increases the price at which the developer can sell his tokens, the developer will want to sell fewer tokens possible. The optimal Q_{t_o+1} therefore is the largest solution to

$$A_{t_o}+\frac{\left(M-Q_{t_o+1}\right)}{R^{T-t_o}}\cdot\left(\frac{V_{t_o}}{M}+\frac{Q_{t_o+1}}{M^2}\right)-i_{T-1}=\bar{i}R^{-1}$$

If this solution is greater or equal to M if and only if $A_{t_o}-i_{T-1}\geq\bar{i}R^{-1}$. In this case, then the developer will set $Q_{t_o+1}=M$ (i.e., he will not sell any token at ICO).

If instead $A_{t_o}-i_{T-1}<\bar{i}R{-}1$, then the largest solution to the above equation will be lower than M (if it exist). If it does not exist or is below $\hat{Q}$, then it is not possible to raise sufficient funds at ICO so to able to invest in the following period. In this case, the developer is indifferent between any $Q_{t_o+1}\leq M$. If instead the largest solution to the above equation is in $[\hat{Q}, M]$, then it will be the equilibrium.

□

[33] Again, I use the fact that the developer's continuation utility in period t_o+1 is equal to his payoff in case he sells all his tokens in that period.

References

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

Athey, S., I. Parashkevov, V. Sarukkai, and J. Xia (2017). Bitcoin pricing, adoption, and usage: Theory and evidence. *SIEPR working paper*.

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

Benabou, R. and J. Tirole (2003). Intrinsic and extrinsic motivation. *The review of economic studies 70*(3), 489–520.

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

Budish, E. (2018). The economic limits of bitcoin and the blockchain. Working Paper 24717, National Bureau of Economic Research.

Canidio, A. (2020). Cryptotokens and cryptocurrencies: the extensive margin. *working paper*.

Catalini, C. and J. S. Gans (2016). Some simple economics of the blockchain. Working Paper 22952, National Bureau of Economic Research.

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 (forthcoming). A theory of icos: Diversification, agency, and information asymmetry. *Management Science*.

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

Cong, L. W., Y. Li, and N. Wang (forthcoming). Tokenomics: Dynamic adoption and valuation. *Review of Financial Studies*.

DeMarzo, P. M. and B. Urošević (2006). Ownership dynamics and asset pricing with a large shareholder. *Journal of political Economy 114*(4), 774–815.

Dimitri, N. (2017). Bitcoin mining as a contest. *Ledger 2*, 31–37.

Easley, D., M. O'Hara, and S. Basu (2019). From mining to markets: The evolution of bitcoin transaction fees. *Journal of Financial Economics 134*(1), 91–109.

Gans, J. S. and H. Halaburda (2015). Some economics of private digital currency. In *Economic Analysis of the Digital Economy*, pp. 257–276. University of Chicago Press.

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 (2019, 11). Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales. *The Review of Financial Studies*.

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*.

Lerner, J. and J. Tirole (2002). Some simple economics of open source. *The journal of industrial economics 50*(2), 197–234.

Li, J. and W. Mann (2018). Digital tokens and platform building. *Working paper*.

Lyandres, E., B. Palazzo, and D. Rabetti (2018). Ico success and post-ico performance. *Working Paper*.

Ma, J., J. S. Gans, and R. Tourky (2018, January). Market structure in bitcoin mining. Working Paper 24242, National Bureau of Economic Research.

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*.

Prat, J., V. Danos, and S. Marcassa (2019). Fundamental pricing of utility tokens. *working paper*.

Prat, J. and B. Walter (2018). An equilibrium model of the market for bitcoin mining. *working paper*.

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

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