Financial incentives for the development of blockchain-based platforms

Canidio, Andrea

IMT Lucca, INSEAD

2018

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

Andrea Canidio †

First version, March 20, 2018. This version: July 28, 2020. Please check here for the latest version.

Abstract

I consider a developer creating a new blockchain-based decentralized digital platform. Users can perform exchanges on the decentralized digital platform only by using a specific crypto-token. The entire stock of this token is initially owned by the developer, who can sell some in an Initial Coin Offering (ICO) to raise funds. Novel with respect to the literature, the developer can also sell tokens later on a frictionless financial market. I show that, if the developer raises funds in an ICO, in each post-ICO period there is a positive probability that the developer sells all of his tokens on the market and, as a consequence, no development occurs. If the developer does not need to raise funds via an ICO, the equilibrium will nonetheless be inefficient because the developer's payoff depends on the surplus generated by the decentralized digital platform in a given period (when he expects to sell his tokens). He therefore fails to internalize that the decentralized digital platform will be used (and generate surplus) over multiple periods.

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. An ICO is a form or crowd-funding in which startups (or loose groups of developers) raise capital by selling crypto-tokens. 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). For comparison, in 2016 total Venture Capital investment in Europe was USD 4.7 billion (OECD, 2017).

These extraordinary events partially obscured a crucial fact: that in the vast majority of cases, teams going through an ICO 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. I call the sale of tokens as a mean to earn profits *seigniorage*.[1] Seigniorage is the dominant business model in the blockchain sector, covering the largest ICOs to date and approximately 90% of the total crypto-market.[2]

To illustrate how seigniorage works, 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 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.[3] 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.

[1] Seigniorage is defined as the profits earned by issuing currency, and is a well known concept from monetary economics. What is novel here is that, thanks to blockchain technology, it can be used to create incentives for innovation.

[2] At the time of writing, among the top-30 tokens by market capitaliztion, 22 are tokens associated with open-source blockchain-based decentralized digital platforms earning profits via seignorage. These 28 tokens represent approximately 90% of the total crypto-market (data from www.coinmarketcap.com).

[3] Prices could be expressed in fiat currency (that is, in some numeraire). The important point is that they need to be settled using the token.

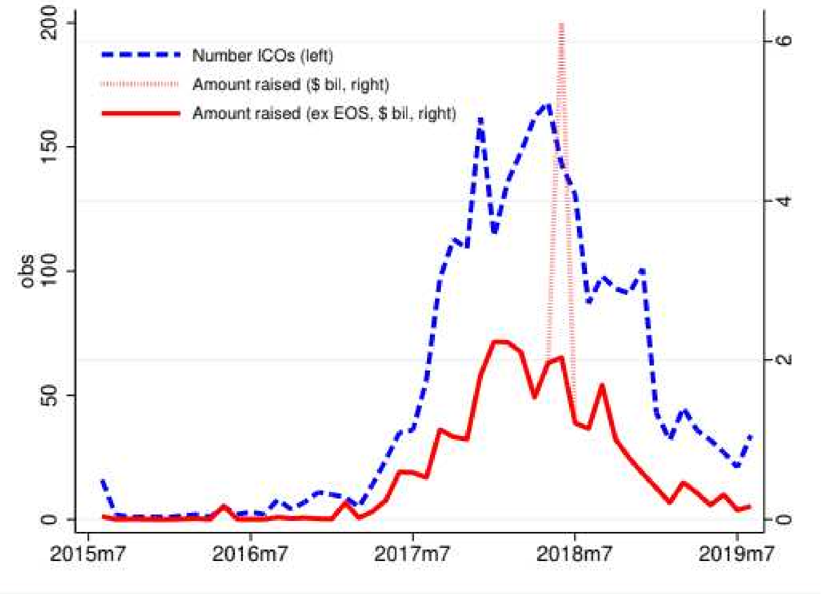

Fig. 1: From Lyandres, Palazzo, and Rabetti (2018) page 35: “This figure reports monthly values of the number of ICOs that are able to raise funds (dashed blue line, left axis) and the total amount raised across all ICOs each month (billions of dollars, right axis). The solid red line excludes the EOS 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.”.

Blockchain enables seigniorage because it allows the 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 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.[4] Blockchain instead generates commitment by computer code. Note, however, that open-source software (including blockchain-based protocols) must be free to use.[5] This

[4] 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.

[5] This follows from Bertrand competition: if an open-source software is not free, a competitor or a group

implies that seigniorage is incompatible with traditional pricing.

I build a model in which a developer can sell tokens both to raise funds and to then profit from his/her work. More precisely, in every period, a developer exerts effort and invests in the development of a blockchain-based decentralized digital platform. 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 market for tokens in which investors are active.[6] 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 software 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

of users could, at zero cost, launch an exact replica of the same software having lower or zero prices.

[6] 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.

are sufficient to finance the optimum level of investment, but may hold the 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 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.[7] 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. That is, the fact that the platform will be used and generate surplus over multiple periods is completely disregarded by the developer.

Interestingly, the level of effort and investment set by the developer may be above or below their first best levels. This will be determined by a parameter in the model measuring the speculative demand for tokens—that is, the investors' demand for tokens driven by the expectation that other investors will demand tokens in the future. The speculative demand determines the sensitivity of the price of tokens to changes in the developer's effort and investment, which therefore will be higher when speculation is more intense. Back-of-the envelope calculations using data from Ethereum suggest that the equilibrium level of effort and investment is above the welfare-maximizing level. This is due to the fact that, at present, only a small fraction of tokens is used by users, with the vast majority being held by investors.[8]

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

[7] 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.

[8] This result is subject to many caveats. The main one is that over- or under-provision of effort and investment should emerge as a function of the fraction of tokens held by investors *in the long run*, that is, when the software is mature and all major developments stop. Arguably, no blockchain project has yet reached this stage. I will argue that, at present, the best candidate for such an analysis is Ethereum, because among the oldest and better established projects, it is the one in which it is easier to identify the fraction of tokens used vs kept by investors.

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, 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.[9]

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 using monopoly pricing (instead of seigniorage) 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 ap-

[9] 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.

proximately 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 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 that can run any application or software (see Ethereum, EOS, Cardano, NEO);[10] 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 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.[11] 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. ICOs are typically well advertised and, as already discussed in the introduction, sales of tokens at ICOs exploded in 2017 and 2018.[12] But tokens can be sold also on the open market, possibly after the ICO. With few

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

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

[12] Usually, tokens sold at ICO start trading on specialized financial exchanges shortly after the end of

exceptions,[13] either token sales on the open market are not disclosed, or they are discussed only within blog posts and informal communication.[14] Despite the difference in visibility between these two ways of selling tokens, recent work by 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

The novelty of this paper with respect to the existing literature studying blockchain-based decentralized digital platforms is that, in the model, tokens are both a mean to raise funds and a mean to earn a profit.

Cong, Li, and Wang (2019) build a model in which tokens can be sold to earn a profit (but not to raise funds). In their model, 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. Interestingly, in my model there is the opposite result: the developer (also 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 has a finite lifespan and chooses how much effort to exert in the development the decentralized digital platform. In Cong et al. (2019) instead there is no such effort and the platform owner has an infinite life. In my opinion, these differences reflect the models' different objectives. If the purpose is to study the creation of the platform, then assuming a finite

the ICO. However, 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.

[13] 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).

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

number of development periods and costly effort is reasonable. If the purpose is to study the maintenance of such platform, then assuming an infinite horizon while abstracting away from effort is also reasonable.[15]

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 (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). In those models, the seller of a token also sells a product or a service, which is what generates a profits. That is, the token only serves as fundraising tool.

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 miners (i.e., the computers that process transactions and therefore constitute the nodes of the Bitcoin blockchain) 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 protocol 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

[15] Note also that Cong et al. (2019) allows the platform owner to create and distribute new tokens in every period, while here the developer creates the initial stock of tokens initially and then, in every period, decides how many tokens to sell. Again, if the lifespan of the platform owner/developer is finite then, in both cases, the platform owner/developer creates and sells a finite amount of tokens. These two assumptions are instead clearly different if the lifespan of the platform owner/developer is infinite.

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).[16]

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,[17] these currencies have neither gained wide adoption, nor generated significant profits for the platform issuing them.

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 starts 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.

[16] A second, more technical, difference is that Athey et al. (2017) assume that the demand for Bitcoins by investors is zero in the long run. In my model, instead, the long-run demand for tokens by investors is a parameter that could be positive. Indeed, the fraction of tokens held by investors in the long run will be an important determinant of the equilibrium of the model and of its efficiency properties.

[17] 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).

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.

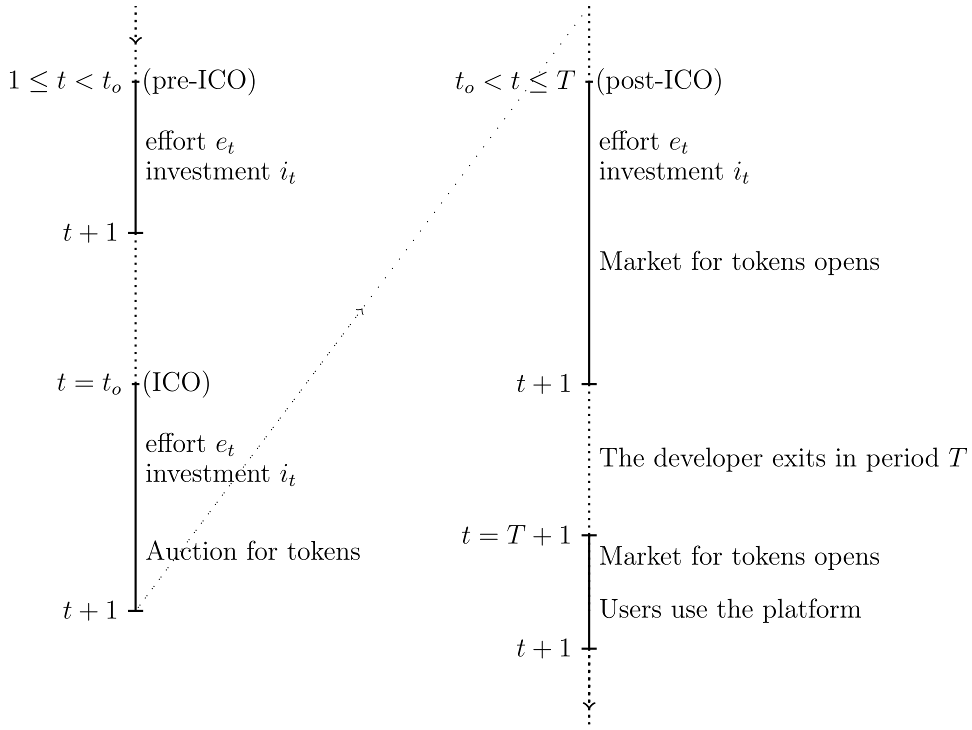

Fig. 2: Timeline

Investors. Investors are risk-neutral profit maximizers with no cash constraints. They can purchase tokens in every period and sell them during any subsequent period. Importantly, when buying or selling tokens on the market, they are price takers: their net demand for tokens in period t depends on the sequence of token prices from period t onward, which they take as given. Investors do not discount the future. They are indifferent between purchasing any amount of tokens in period t whenever $p_t = \bar{p}_t \equiv \max_{s>t} \{E[p_s]\}$, where $\bar{p}_t$ is the largest future expected price. If instead $p_t > \bar{p}$, then the investors' demand for tokens in period t is zero. Finally, if $p_t < \bar{p}$, 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, with $Q_1 = M$. Call:

$$A_t \equiv A_0 + \sum_{s=1}^{t-1} [(Q_s - Q_{s+1}) \cdot p_s - i_s] = A_{t-1} - i_{t-1} + p_{t-1}(Q_{t-1} - Q_t)$$

the total resources available to the developer at the beginning of period t, where A_0 is the developer's initial assets (cash) and the rest are resources earned from the sale of tokens in previous periods, net of the investments made. To account for the fact that during periods $t < t_o$ the developer cannot sell tokens, I impose that $p_t \equiv 0$ for all $t < t_o$. Intuitively, in any $t < t_o$ the developer cannot sell tokens but can destroy them, which is equivalent to selling them at price zero. Of course, this will not happen in equilibrium.

In every period, the developer maximizes his end-of-life assets A_{T+1} minus the disutility of effort. He faces a per-period feasibility constraint determining the largest investment that can be made:

$$i_t \leq A_t.$$

He also faces a per-period cash constraint establishing an upper bound to the amount of tokens that he can purchase on the market as a function of his period-t assets and his period-t investment:

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

Note that the cash constraint is always tighter than the feasibility constraint, which can therefore be disregarded.

Similar to investors, the developer does not discount the future either. Hence, his problem can be rewritten in recursive form as, for $t < T$:

$$\begin{aligned} U_t(Q_t, A_t) \equiv \max_{Q_t, e_t, i_t} \Big\{ &-\frac{1}{2}e_t^2 + U_{t+1}(Q_{t+1}, A_t + (Q_t - Q_{t+1}) \cdot p_t - i_t) + \\ &\lambda_t(A_t - i_t - p_t \max\{Q_{t+1} - Q_t, 0\}) \Big\}, \end{aligned}$$

and for $t = T$:

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

where λ_t is the Lagrange multiplier associated with the period-t cash constraint. 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. To do so, in every period they first purchase tokens and then use them to transact on the decentralized digital platform. The total value (in US dollars) of all exchanges occurring on the decentralized digital platform during a given period is the *value of the decentralized digital platform* and is defined as:

$$V_T = \sum_{s=1}^{T} f(e_s, i_s), \tag{2}$$

where $f(.,.)$ is increasing in both arguments, concave in e_t, with $\lim_{i\to\infty}\left\{\frac{\partial f(e_t,i_t)}{\partial i_t}\right\} = 0$ for all e_t. For ease of notation, I assume that each user can access the market for tokens only once in every period.[18] 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 $\frac{V_T}{p_t}$.

Equation (2) 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.[19]

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

[19] 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

4 Solution

4.1 Periods $t \geq T$

I start by solving for the price of the token from period T onward, using the behavior of users (as captured by equation 2) and an appropriate equilibrium selection criterion (introduced below).

The fact that no development is possible after period T implies that the price of the token must be constant from period T onward. Investors are therefore indifferent between holding cash and holding the token, which implies that there are multiple equilibria: the price of the token will depend on the stock of tokens held by the investors, who are indifferent between holding any level of tokens.[20] To break this indeterminacy, I impose the following assumption:

Assumption 1. *In equilibrium, the stock of tokens held by investors from period $t \geq T$ is $\gamma \cdot M$ for $\gamma \in [0, 1)$.*

That is, out of the many equilibria possible, I am interested here in those in which the demand for tokens by investors is a constant fraction of the stock of tokens M.

The term $\gamma \cdot M$ therefore represents the "speculative" demand for tokens: the demand for tokens driven by the expectation that future investors will also demand $\gamma \cdot M$. Next to this demand, in every period there is a demand and a supply for tokens originating from users. Because the stock of tokens available to users is $(1 - \gamma) \cdot M$, the price for tokens must solve:

$$p_T = \frac{V_T}{(1-\gamma)M}. \tag{3}$$

The above equation 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 $(1 - \gamma)M$) 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

the value of the decentralized digital platform.

[20] This is a version of a well know result: the indeterminacy of equilibrium exchange rate by Kareken and Wallace (1981). See also example 4.1 in Santos and Woodford (1997), where an overlapping generation model with two types of money is considered, and the indeterminacy of the exchange rate between the two types of money is established.

his token — is 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.[21]

4.2 The developer's problem

We start by deriving a useful lemma. This lemma is based on the observation that, in equilibrium, the expected price of tokens must be constant over time.

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

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

An important observation is that what is known by investors—and hence is used to compute the expectation about the developer 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 p_t and $\bar{p}_t$, and not on the quantity of tokens sold by the developer in period t.[22] 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 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 developers' 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.*

[21] Using the equation of exchange to derive the price of the token is convenient but is not essential. All the results derived below are robust to different assumptions about what happens from period T onward (i.e., different assumptions regarding the demand and supply of tokens by users or investors, or about the velocity of the token), provided that p_T is increasing in the sequence of effort and investments made by the developer. Otherwise, the developer has no incentives to exert effort and invest, and the equilibrium is a trivial one in which no development occurs.

[22] 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.

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_0 are sufficient to cover the optimal level of investment in every period. In this case, the cash constraint is never binding and 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 utility can be written as, for $t \leq T-1$:

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

and for $t = T$:

$$\tilde{U}_T(Q_T) \equiv \max_{e_T, i_T} \left\{ Q_T \cdot p_T - i_T - \frac{1}{2}e_T^2 \right\}.$$

Note that $(Q_t - Q_{t+1}) \cdot p_t - i_t$ is the cash generated in period t, net of investment. Because there is no discounting and the cash constraint is never binding, I can include this cash in period-t utility function (i.e., the period in which it is generated), even if it is consumed in period T.

We use Lemma 1 to compute optimal effort and optimal investment in any period t:[23]

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

$$i^*(Q_t) \equiv \text{argmax}_{i_t} \left\{ f(e^*(Q_t), i_t) \frac{Q_t}{(1-\gamma)M} - i_t \right\}. \tag{6}$$

Hence, optimal effort and investment depend exclusively on Q_t and not on the specific time period t. The reason is that, by Lemma 1, effort and investment in period t increase the price of tokens in every subsequent period. Hence, the benefit of exerting effort and investing is the same no matter when the developer plans to sell his tokens.[24]

Furthermore, Q_t and e_t are complements in the developer's objective function. This,

[23] 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.

[24] For future reference, note that this logic does not necessary extend to the poor developer case. The reason is that the level of investment chosen in a given period may determine whether the cash constraint is binding.

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 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*

$$\alpha = (1-\gamma)\,\frac{(e^*(M))^2/2 + i^*(M)}{f(e^*(M), i^*(M))} \tag{7}$$

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

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

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:

$$M \cdot \frac{f(e^*(M), i^*(M))}{(1-\gamma)M},$$

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:

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

with probability:

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

and will decrease by:

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

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 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 less than one.

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

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

If instead the ICO happens in period $T-1$ or in period T, the developer's payoff is[25]

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

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

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

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 exert high effort and investment in all future period. 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 $A_0 \geq T \cdot i^{*}(M)$.*

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

[25] 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.

and, as a consequence, $p_t M$ are independent from M. The developer's utility is therefore independent from M for any t_o.

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 $A_0 < T \cdot i^*(M)$: 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. Hence, i is an essential input in the development of the protocol, because effort is productive only if $i \geq \bar{i}$. However, investing more that $\bar{i}$ is also not productive. 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:

$$\bar{i} < \frac{1}{2}\left(\frac{1}{1-\gamma}\right)^2, \tag{A2}$$

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*

$$e^*(Q_t, A_t) \equiv \begin{cases} \frac{Q_t}{(1-\gamma)M} & \textit{if } i_t \geq \bar{i} \\ 0 & \textit{otherwise} \end{cases} \tag{9}$$

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

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.*[26] *Such equilibrium exists if and only if*

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

- *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*

$$\alpha = \frac{1}{2} + \bar{i}(1-\gamma)^2.$$

Such equilibrium exists if and only if

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

- *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*

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

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

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

lies in $\left[(1-\gamma)M\sqrt{2\bar{i}}, M\right]$.

An equilibrium always exists. If $A_{T-1} - i_{T-1} \geq \bar{i}$, either a "high" equilibrium or a "medium"

[26] 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.

equilibrium exist. If $A_{T-1}-i_{T-1} < \bar{i}$ 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. 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 $Q^*_{t+1} < (1-\gamma)M\sqrt{2\bar{i}}$) 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 $A_t - i_t < \bar{i}$, after investing 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 $A_t - i_t \geq \bar{i}$, after investing 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 in general possible to write down a 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, so that, in equilibrium, $Q_{t_o+1} = 0$.

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

If $t_o < T$ and $A_{t_o} - i_{t_o} < \bar{i}$, then define $\tilde{Q}$ as the largest solution to

$$A_{t_o} + \left(M - \tilde{Q}\right) \cdot \left(\frac{V_{t_o}}{(1-\gamma)M} + \frac{\tilde{Q}}{((1-\gamma)M)^2}\right) - i_{t_o} = \bar{i}.$$

If $\tilde{Q} \in \left[(1-\gamma)M\sqrt{2\bar{i}}, M\right]$, 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 $\tilde{Q} < (1-\gamma)M\sqrt{2\bar{i}}$, 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, the price for tokens at ICO is decreasing in the amount of tokens sold at ICO. Also, by Lemma 1, in expectation the price of tokens is constant over time. Hence, the value of the stock of tokens M is decreasing in the amount of tokens sold at ICO.

This implies that the developer will want to sell as few tokens as possible at ICO. If $A_{t_o} - i_{t_o} \geq \bar{i}$, 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. If instead $A_{t_o} - i_{t_o} < \bar{i}$, 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 at

ICO. 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* $t_o = \max\{t | t \cdot \bar{i} \leq A_0\}$, *where* A_0 *are the developer's initial assets.*

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 protocol from period T onward, where the discount factor is that of users. I consider the social welfare generated by the platform in every period to be equal to the volume of transactions on the platform, that is V_T.[27]

The equilibrium of the game differs from the first best in several ways. As already discussed, if the developer is poor, he will hold the ICO after exhausting his own funds. This is, however, inefficient because, in every post-ICO period, the developer may set zero effort and zero investment, even if the social value of his effort and investment is strictly positive.

[27] Of course, more in general, the social welfare generated by the platform in every period should depend on the slope of the demand function of those on the buying side of the platform, and on the slope of the supply function of those on the selling side of the platform. It is quite easy to make assumptions on those slopes such that surplus is equal to V_T—for example, -1 and 1 for the slope of demand and supply respectively.

More interestingly, even assuming that the developer is rich, there is an additional source of inefficiency. The developer is setting effort and investment so as to maximize the value of the decentralized digital platform in period T—when he will exit the game—and completely disregards the fact that the protocol will generate value over multiple periods.

To see this, consider the rich developer case. Social welfare is:

$$\sum_{s=T}^{\infty} \beta^{s-T} V_T = \frac{V_T}{1-\beta},$$

where β is the users' discount factor. The choice of effort and investment that maximize social welfare is:

$$e^{**} \equiv \text{argmax}_e \left\{ \frac{f(e, i^{**})}{1-\beta} - \frac{1}{2}e^2 \right\} \tag{11}$$

$$i^{**} \equiv \text{argmax}_i \left\{ \frac{f(e^{**}, i)}{1-\beta} - i \right\}. \tag{12}$$

By comparing the above expression with the equilibrium level of effort and investment (equations 5 and 6), it is clear that equilibrium effort and investment will be below the efficient level if $\gamma < \beta$, and above the efficient level if $\gamma > \beta$.

To determine which case is more likely, I turn to some back-of-the-envelope calculations using data from Ethereum. Remember that γ is the fraction of tokens held by investors from period T onward. The empirical counterpart for γ is therefore the fraction of tokens held by investors when the project is mature and (major) developments no longer occur. This is a stage no blockchain-based protocol has yet reached. The best approximation possible is to consider some of the oldest, better established blockchain project, and calculate the fraction of the corresponding tokens kept by investors. However, with the exception of Ethereum, all oldest, better established blockchain-based protocols are digital currencies (such as Bitcoin), where only one operation is allowed: sending tokens. Because this operation is consistent both with investors' behavior and with usage (for example, sending remittances), it is very difficult to distinguish between users and investors.[28] Instead, Ethereum is the oldest and better established decentralized computing platform, used primarily to run software, which are in this context called *smart contracts*. The fraction of ETH (Ethereum native token) paid in fees is therefore a measure of the value of the decentralized digital platform V_t: the payments (in tokens) from users of Ethereum to the nodes maintaining the Ethereum

[28] For more details on these difficulties, see Athey et al. (2017).

network, performed in exchange for a service—executing a smart contract.[29]

After collecting data on the total fees paid on the Ethereum network,[30] what remains to do in order to derive γ is to define the length of a period. In the model, users can exchange fiat money for tokens once in every period. The empirical equivalent of a "period" is, therefore, the inverse of the velocity of ETH: the average number of days before a given token can be used again to pay a fee. Absent any good prior, I will consider different possible values, from one to 30 days.

I therefore compute the average value of:

$$1 - \frac{\text{total transaction fees collected over } n \text{ days}}{\text{total stock of ETH}},$$

for the year 2019, where the n goes from 1 to 30. This value corresponds to γ, under the assumption that a single period of the model corresponds to n days. I compare this value to the discount factor over n days, computed assuming a daily discount factor of 0.015% (approximately a 5% yearly discount factor). As Table 1 shows, for all values of n, the estimated γ is orders of magnitude above β. This is because the vast majority of ETH are held by investors and never used to pay fees. This suggests that the equilibrium effort and investment is above the efficient level.[31]

The above result is specific to the rich developer case. 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. By comparing the values for β and γ in Table 1 for $n = 10$, as long as the developer holds more than 0.15% of the share of tokens, he will set effort and investment above the social optimum. It seems likely, therefore, that conditional on exerting positive effort and investment, the level of effort and investments will be above the socially optimal level, even in the "poor developer" case.

[29] As in the Bitcoin network, these nodes also earn a "per-block" reward. In the case of Ethereum, however, this reward is a much smaller component of the node's total payoff. As a consequence, performing any operation on the Ethereum network requires the payment of a fee.

[30] Easily downloadable from several sources, such as https://etherscan.io/chart/transactionfee

[31] In these calculations, I considered the total stock of ETH as the total number of ETH in existence at the end of year 2019 (that is, 1,577,750,400). The conclusion remains the same if I were to consider the total number of ETH in existence at the beginning of 2019 (that is, 1,546,300,800).

n	γ	β
1	$\approx$1	0,00015
2	0,999999	0,00030
3	0,999999	0,00045
4	0,999999	0,00060
5	0,999999	0,00075
6	0,999998	0,00090
7	0,999998	0,00105
8	0,999997	0,00120
9	0,999997	0,00135
10	0,999997	0,00150
20	0.999993	0.00300
30	0.999990	0.00451

Tab. 1: Data from https://etherscan.io/chart, elaborated by the author

6 Discussion

6.1 Seigniorage vs monopoly pricing

It is possible to compare seigniorage with more standard pricing. Profits generated via seigniorage depend on the value of the decentralized digital platform in the moment at which the developer sells his tokens. Under standard monopoly pricing, the monopolist captures a fraction of the value of the decentralized digital platform *in every period;* not only in one period.

The same back-of-the envelope calculations reported in Table 1 allow to compare profits under seigniorage with profits under monopoly pricing. Call τ the fraction of total value lost as deadweight loss caused by monopoly pricing, and ν the fraction of the remaining value that is captured by the monopolist in every period.[32] Profits earned via monopoly pricing from period T onward are therefore:

$$\sum_{s=T}^{\infty} \beta^{s-T} \nu(1-\tau)V_T = \frac{\nu(1-\tau)V_T}{1-\beta},$$

which are greater than profits earned via seigniorage if and only if:

$$\nu(1-\tau) \geq \frac{1-\beta}{1-\gamma}.$$

[32] There two parameters depend on the elasticity of supply/demand of those using the platform to sell/buy.

The above inequality can be satisfied only if $\beta > \gamma$. However, Table 1 suggests that, empirically, $\gamma > \beta$. This implies that profits under seigniorage are larger than profits under monopoly pricing for any value of ν and τ.

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, and by doing so generate extra surplus.[33] 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 *in every period of development* the level of effort and investment will be reduced, because the

[33] 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.

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), in every period t the equilibrium price of the token must be such that the developer with the largest q_{t+1}^i is indifferent between holding all tokens or no tokens.[34] 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, introducing the token increases the supply of money in the economy by an amount equal to the value of the stock of tokens (which is also the developer's profits), leading to an increase in the economy-wide price level.[35] Initial holders of cash are therefore

[34] 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.

[35] 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).

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.) The effect of the developer's effort on the economy-wide price level 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.[36] 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. 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 the 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

[36] 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.

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

Hence, in every period $t \leq T$, in equilibrium the sequence of future expected prices must be constant. We can therefore write the price of tokens in every period as $p_t = E[p_T]$. 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 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 (when p_{T-1} is high), purchase as many tokens as possible (when p_{T-1} is low), or be indifferent between these two options. The price at which the developer is indifferent is:

$$p_{T-1} = \frac{\tilde{U}_T(M)}{M} = \frac{V_{T-1} + f(e^*(M), i^*(M))}{(1-\gamma)M} - \frac{(e^*(M))^2/2 + i^*(M)}{M}, \qquad (13)$$

where $\frac{V_{T-1}+f(e^*(M),i^*(M))}{(1-\gamma)M}$ 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 $\frac{V_{T-1}}{(1-\gamma)M}$. If instead the developer purchases M tokens in period $T-1$, then $p_T = \frac{V_{T-1}+f(e^*(M),i^*(M))}{(1-\gamma)M}$. Because investors must be indifferent between purchasing in period T or period $T-1$, it must be that:

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

where α_{T-1} is the probability that the developer sells all of his tokens in period $T-1$, which using (13) can be written as:

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

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:

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

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

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

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

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

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

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

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 $p_{t_o} = p_{t_o+1}$. Hence, whenever $t_o < T$, the developer's problem at ICO can be written as:

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

where the first and the last equality follow from writing $\tilde{U}_{t_{o+1}}(Q_{t_{o+1}})$ explicitly.[37] The developer therefore anticipates that the price of tokens will be the same at ICO and in the following period, independently from how many token he sells. The number of tokens sold, however, determines the equilibrium level of effort and investment in period t_{o+1}. □

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 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 $T-1$.

[37] 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.

Period-T effort and investment are:

$$e_T^*(Q_T, A_T) \equiv \begin{cases} \frac{Q_T}{(1-\gamma)M} & \text{if } i_T \geq \bar{i} \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

$$i_T^*(Q_T, A_T) \equiv \begin{cases} \bar{i} & \text{if } \bar{i} \leq \frac{1}{2}\left(\frac{Q_T}{(1-\gamma)M}\right)^2 \text{ and } \bar{i} \leq A_T \\ 0 & \text{otherwise.} \end{cases} \tag{15}$$

Define:

$$\hat{Q} \equiv (1-\gamma)M\sqrt{2\bar{i}}, \tag{16}$$

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:[38]

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

where

$$\begin{aligned} &U_T(Q_T, A_{T-1} + (Q_{T-1} - Q_T) \cdot p_{T-1} - i_{T-1}) = \\ &\begin{cases} Q_T \frac{V_{T-1}}{(1-\gamma)M} + \frac{1}{2}\left(\frac{Q_T}{(1-\gamma)M}\right)^2 + A_{T-1} + (Q_{T-1} - Q_T) \cdot p_{T-1} - i_{T-1} - \bar{i} & \text{if } Q_T \geq \hat{Q} \\ & \text{and } A_{T-1} + (Q_{T-1} - Q_T) \cdot p_{T-1} - i_{T-1} \geq \bar{i} \\ Q_T \frac{V_{T-1}}{(1-\gamma)M} + A_{T-1} + (Q_{T-1} - Q_T) \cdot p_{T-1} - i_{T-1} & \text{otherwise,} \end{cases} \end{aligned} \tag{17}$$

and λ_{T-1} is the Lagrange multiplier of the cash constraint, which establishes an upper bound to the number of tokens that the developer can purchase on the market in period $T-1$.

Define Q_T^* as the largest Q_T such that the developer can invest $\bar{i}$ in period T: that is,

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

the largest Q_T such that $A_T = A_{T-1} + (Q_{T-1} - Q_T) \cdot p_{T-1} - i_{T-1}$ is at least $\bar{i}$:

$$Q_T^* \equiv Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{p_{T-1}} \tag{18}$$

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

Note also that if $A_{T-1} - i_{T-1} \geq \bar{i}$, 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 $A_{T-1} - i_{T-1} < \bar{i}$ (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.

I now derive the three possible equilibria of the game

"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:

$$p_{T-1} = \frac{U_T(M, A_T)}{M} = \frac{V_{T-1}}{(1-\gamma)M} + \frac{1}{2(1-\gamma)^2 M} - \frac{\bar{i}}{M} \tag{19}$$

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

$$p_{T-1} = \alpha_{T-1} \frac{V_{T-1}}{(1-\gamma)M} + (1 - \alpha_{T-1}) \left(\frac{V_{T-1}}{(1-\gamma)M} + \frac{1}{(1-\gamma)^2 M} \right) \tag{20}$$

Putting the above two expressions together we get:

$$\alpha_{T-1} = \frac{1}{2} + \bar{i}(1-\gamma)^2$$

This is indeed an equilibrium if:

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

or

$$\left(\frac{V_{T-1}}{(1-\gamma)} + \frac{1}{2(1-\gamma)^2} - \bar{i} \right) \left(1 - \frac{Q_{T-1}}{M} \right) \leq A_{T-1} - i_{T-1} - \bar{i} \tag{21}$$

Note that the above is possible only if $A_{T-1} - i_{T-1} > \bar{i}$, that is, the agent wealth is sufficient to invest $\bar{i}$.

"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

$$p_{T-1} = p_T = \frac{V_{T-1}}{(1-\gamma)M}.$$

At such price, we have

$$Q_T^* \equiv Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{\frac{V_{T-1}}{(1-\gamma)M}}$$

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 (16) and (18), becomes:

$$V_{T-1} \left(\frac{Q_{T-1}}{(1-\gamma)M} - \sqrt{2\bar{i}} \right) < i_{T-1} + \bar{i} - A_{T-1}. \tag{22}$$

Note that the above equilibrium can exist only if $A_{T-1} - i_{T-1} < \bar{i}$, that is, the agent wealth is not sufficient to invest $\bar{i}$.

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

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

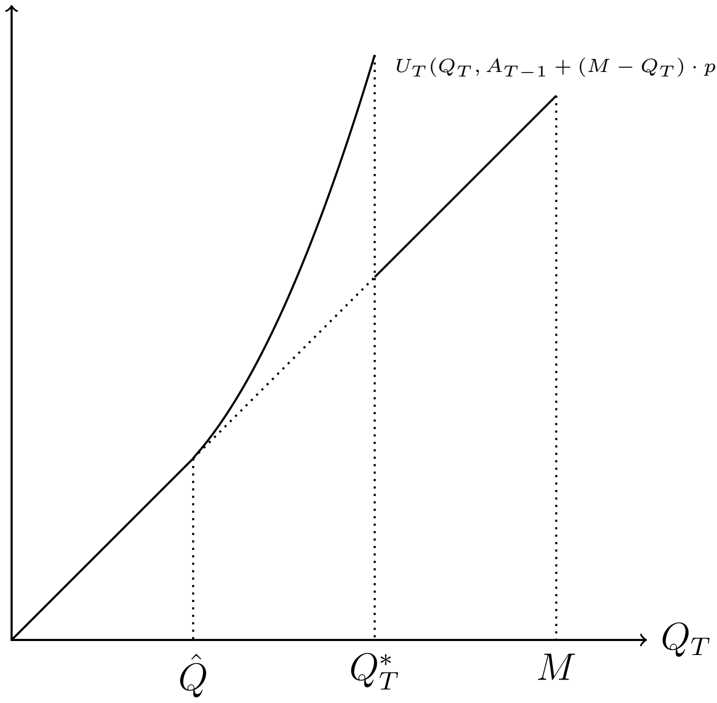

Fig. 3: Continuation value as a function of Q_T.

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 3). 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:

$$p_{T-1} = \frac{U_T(Q_T^*, \bar{i})}{Q_T^*} = \frac{V_{T-1}}{(1-\gamma)M} + \frac{Q_T^*}{2((1-\gamma)M)^2} - \frac{\bar{i}}{Q_T^*} \tag{23}$$

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

$$p_{T-1} = \alpha_{T-1}\frac{V_{T-1}}{(1-\gamma)M} + (1-\alpha_{T-1})\left(\frac{V_{T-1}}{(1-\gamma)M} + \frac{Q_T^*}{((1-\gamma)M)^2}\right) \tag{24}$$

Putting the above two expressions together we get:

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

By using (18) and (23), we can express Q_T^* as:

$$Q_T^* = Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{\frac{V_{T-1}}{(1-\gamma)M} + \frac{Q_T^*}{2((1-\gamma)M)^2} - \frac{\bar{i}}{Q_T^*}} \tag{25}$$

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 (25) is below its LHS at $Q_T^* = \hat{Q}$ if and only if (22) holds. At the same time the RHS of (25) is above its LHS at $Q_T^* = M$ if and only if (21) holds.

- by continuity, a "medium" equilibrium must exist whenever both (22) and (21) hold. A "medium" equilibrium must exist also when neither (22) nor (21) hold.

- In all other cases, such "medium' equilibrium may not exist. However, either a "low" or a "high" equilibrium will exist.

- $A_{T-1} - i_{T-1} \geq \bar{i}$, then the LHS of (25) is strictly increasing while its RHS is strictly decreasing. Furthermore, we established earlier that, in this case, (22) must be violated. Hence, a unique "medium" equilibrium exists if (21) is violated.

- $A_{T-1} - i_{T-1} < \bar{i}$. In this case, both the RHS and the LHS of (25) are strictly increasing. Furthermore, we established earlier that, (21) must be violated. Hence, if (22) is also violated, then there must be at least one "medium" equilibrium. If instead (22) holds (so that a "low" equilibrium exists) there could still be one (or more) "medium" equilibrium.

Hence, an equilibrium always exists. If $A_{T-1} - i_{T-1} \geq \bar{i}$, there can be either a "high" or a "medium" equilibrium. In this case, the equilibrium is unique. If $A_{T-1} - i_{T-1} < \bar{i}$, 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 (14) and (15). 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

$$\hat{Q} \equiv (1-\gamma)M\sqrt{2\bar{i}},$$

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

$$U_T(Q_{t_o+1}, A_{t_o} + (Q_{t_o} - Q_{t_o+1}) \cdot p_{t_o} - i_{t_o}).$$

There are two important differences with respect to the sale of tokens on the market (considered in the proof of Proposition 4). First, here, by definition, 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 $p_{t_o+1} = p_{t_o}$, 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.

We therefore have

$$U_T(Q_{t_o+1}, A_{t_o} + (Q_{t_o} - Q_{t_o+1}) \cdot p_{t_o} - i_{t_o}) = \begin{cases} M \cdot p_{t_o} - \frac{1}{2}\left(\frac{Q_{t_o+1}}{(1-\gamma)M}\right)^2 + A_{t_o} - i_{t_o} - \bar{i} & \text{if } Q_{t_o+1} \geq \hat{Q} \\ & \text{and } A_{t_o} + (M - Q_{t_o+1}) \cdot p_{t_o} - i_{T-1} \geq \bar{i} \\ M\frac{V_{T-1}}{(1-\gamma)M} + A_{T-1} - i_{T-1} & \text{otherwise} \end{cases} \tag{26}$$

where

$$p_{t_o} = \frac{V_{t_o}}{(1-\gamma)M} + \frac{Q_{t_o+1}}{((1-\gamma)M)^2}.$$

is the price at ICO (as well as after) in case there is positive investment and effort in period $t_o + 1$.

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

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

If this solution is greater or equal to M if and only if $A_{t_o} - i_{T-1} \geq \bar{i}$. 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 $A_{t_o} - i_{T-1} < \bar{i}$, 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.

□

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*.

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.

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*.

Kareken, J. and N. Wallace (1981). On the indeterminacy of equilibrium exchange rates. *The Quarterly Journal of Economics 96*(2), 207–222.

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*.

Santos, M. S. and M. Woodford (1997). Rational asset pricing bubbles. *Econometrica: Journal of the Econometric Society*, 19–57.

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*.