# Financial incentives for open source development: the case of Blockchain

Canidio, Andrea

IMT Lucca, INSEAD

2018

# Financial incentives for open source development: the case of Blockchain*

*Andrea Canidio* †

First version, March 20, 2018. This version: October 3, 2018. Please check here for the latest version.

#### Abstract

Unlike traditional open-source projects, developers of open-source blockchain-based projects can reap large financial rewards thanks to a modern form of seigniorage. I consider a developer working on an open-source blockchain-based software that can be used only in conjunction with a specific crypto-token. This token is first sold to investors via an Initial Coin Offering (ICO) and then traded on a frictionless financial market. In all equilibria of the game, 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.

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

**Keywords**: Blockchain, decentralized ledger technologies, Initial Coin Offering (ICO), seigniorage, innovation, incentives, open source

---

*I am grateful to Bruno Biais, Ennio Bilancini, Sylvain Chassang, Kenneth Corts, Antonio Fatas, Gur Huberman, Allistair Milne, Julien Prat, Massimo Riccaboni, Harald Uhlig, the participants of the INSEAD research symposium, INSEAD finance brownbag seminar, IMT brownbag seminar, 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, and EEA-ESEM conference for their comments and suggestions.

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

# 1 Introduction

This paper studies a new mechanism to finance innovation: seigniorage. Seigniorage allows the developer of an open-source blockchain-based software to earn a direct financial reward (in addition to indirect benefits derived from, for example, career concerns) via the creation of a token—itself a piece of open-source software—that must be used in conjunction with the software.

To illustrate, 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. A developer who creates the missing protocol can profit from his innovation by simultaneously creating a *token*, and by establishing that all exchanges that occur using the protocol must use this token.[1] The developer owns the initial stock of tokens so that, if the protocol is successful, there will be a positive demand for tokens, a positive price for tokens and positive profits earned by the developer.[2]

Blockchain enables this mechanism in three ways (see Section 1.1 for additional details on blockchain). First, it allows the developer to commit to a specific supply of tokens. Absent this commitment, because the marginal cost of creating electronic tokens is zero, the only possible equilibrium price for tokens is zero, leading to zero profits for the entrepreneur. Using blockchain technology, instead, the rules determining whether (and how) the supply of tokens increases over time can initially be specified within the software. If the software is open source, this commitment is credible because anybody can verify the software's source code.[3] Furthermore, blockchain can be used to specify that only a given token can be used to transact

[1] 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.

[2] Alfred Wenger, a prominent venture capitalist, provides one of the first descriptions of this mechanism: "You can think of these [tokens] like the tokens you might buy at a fair to get on a ride: different operators can have their own rides and set their own price in terms of tokens. You only need to buy tokens once (in exchange for fiat currency) and then can use them throughout the fair." See https://continuations.com/post/148098927445/crypto-tokens-and-the-coming-age-of-protocol.

[3] This implies that the development of a closed-source protocol cannot be financed via seigniorage, but only via a set of fees/prices (see Section 5.1 for a discussion).

using the protocol.[4] Finally, blockchain may be used to create the protocol.

This paper studies the incentives for innovation generated by seigniorage. I build a model in which, in every period, a developer exerts effort and invests in the development of a protocol. 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 both users of the protocol and investors are active. The developer can use the proceedings of the sale of tokens to either invest in the development of the protocol or to consume.

The first result of the paper 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 protocol, 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 protocol) or keeping a strictly positive amount of tokens (and therefore continuing the development of the protocol). The developer randomizes between these two options, in a way that leaves investors indifferent between purchasing tokens in any given period.

The equilibrium at ICO is instead in pure strategies. The important point is that, if the ICO is an auction, then the fraction of the total stock of tokens sold to investors is announced initially. Because the fraction kept by the developer determines his incentives to exert effort and invest in the development of the protocol, investors can anticipate the amount of development that will occur in the period following the ICO.

[4] Of course, it is always possible to modify the source code to accept a different token, therefore creating a "fork": a new protocol, with its own development, incompatible with the initial protocol.

In addition, both at ICO and post-ICO there may be multiple equilibria. Because of a cash constraint, the developer cannot invest in the development of the protocol 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 protocol. 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, at ICO there could be multiple pure-strategy Nash equilibria, while post-ICO there could be multiple mixed-strategy Nash equilibria.[5]

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 with positive probability he will sell all of his tokens and not develop the software. 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 protocol. As a consequence, the developer never wants to hold an ICO if his own assets are sufficient to finance the optimum level of investment in the development of the protocol, but may hold the ICO otherwise.

The equilibrium of the game is, in general, not efficient. The first source of inefficiency is that, as already discussed, the developer may need to sell some tokens to finance the development of the protocol, but doing so implies that in every subsequent period he will develop the protocol with probability less then one. But even assuming that the developer has sufficient funds to invest optimally, there is

[5] 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 is a coordination problem among users, possibly leading to the existence of 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.

a second, more subtle, source of inefficiency. The developer's 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 using the protocol during a given period of time.[6] Instead, in the first best, effort and investment should be set so as to maximize the *present discounted value* of the surplus generated by the protocol. That is, the fact that the protocol will be used and generate surplus over multiple periods is completely disregarded by the developer.

Furthermore, the fraction of tokens held by investors determines the sensitivity of the price of tokens to changes in the developer's effort and investment, and therefore whether the equilibrium level of effort and investment is above or below the efficient level. Back-of-the envelope calculations using data from the Ethereum blockchain suggest that, conditional on exerting positive effort, 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, which implies a very high sensitivity of the price of token to the developer's effort and investment.[7]

## 1.1 Blockchain-based protocols

The key premise of this paper is that blockchain can be the technological foundation of various other protocols. To illustrate this fact, it is useful to make an analogy between blockchain and the *Internet Protocol Suite*.

The Internet Protocol Suite (commonly known as TCP/IP) was developed in the late '60s and early '70s to allow for the decentralised *transmission* of data, that is, transmission of data via a network of computers in which no node is, individually, essential for the well functioning of the network. Financed by the Defense Advanced Research Projects Agency (DARPA), it had the goal of increasing military commu-

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

[7] 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.

nication resilience by moving from a hub-and-spoke model of communication to a complete (or mesh) network model of communication (see Figure 1).[8] The Internet Protocol Suite is the technological foundation of a second set of protocols, also called *application layer protocols*. Those protocols make use of TCP/IP to handle specific types of data in a specific context: HTTP for accessing web pages; SMTP, POP, and IMAP for sending and receiving emails; FTP for sending receiving files; and so on.

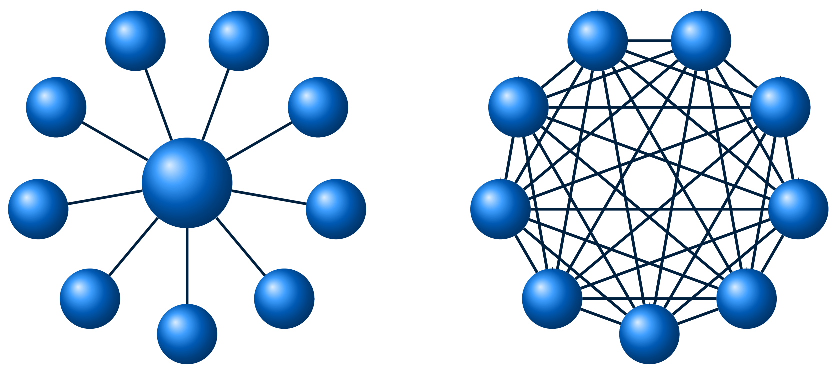


Fig. 1: Hub-and-spoke (left) and mesh (right)

Blockchain further expands the possible operations that can be performed by a network of computers in which no node is essential. Like TCP/IP, it allows for the decentralized transmission of data, but also permits the decentralized storage, verification and manipulation of data.[9] Blockchain is also similar to TCP/IP in that it provides the foundation for a number of other protocols. The most well-known is the Bitcoin protocol: a protocol allowing a network of computers to store data (how many Bitcoins each address owns), and to enforce specific rules regarding how these data can be manipulated (no double spending). The Bitcoin protocol is not only the oldest and most widely known application of blockchain technology, but also well illustrates an important point: absent blockchain technology, the same type of data can be maintained only within a traditional organization (typically a bank).

[8] See Hafner and Lyon (1998), in particular the description of the work of Paul Baran (pp 53-64).

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

Numerous other open-source blockchain-based protocols currently exist or are actively being developed. In addition to several cryptocurrencies (such as Monero, ZCash, Litecoin), there are protocols for building decentralized computing platforms that can run any application or software (see Ethereum, EOS, Cardano, NEO);[10] protocols for decentralized real-time gross settlement (see Ripple, Stellar); protocols enabling the creation of 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); protocols for generic e-commerce transactions (see Openbazaar); protocols creating fully decentralized prediction markets (see Augur, Gnosis), financial exchanges (see 0xproject), and financial derivatives (see MakerDAO); protocols allowing the existence of fully decentralized organizations (see Aragon) and virtual worlds (see Decentraland); and many more.[11]

## 1.2 Blockchain and Seigniorage

An important difference between the protocols built on TCP/IP and those built on blockchain is the way in which their developers are rewarded. The vast majority of protocols based on TCP/IP are open source, free to adopt and use. The contributors to these projects are not organized in a single, traditional company, but rather form a loosely-defined group around one (or multiple) project leader(s) and are based on open collaboration (as is typical of open source projects). They do not receive immediate, direct financial compensation for their contributions, and are motivated by career concerns (i.e., to increase their reputation and reap financial benefits in the future) and by non-monetary considerations (i.e., the pleasure of sharing, collaborating and contributing to a public good).

Instead, as already discussed in the Introduction, the development of blockchain-based protocols can leverage financial incentives via seigniorage. This is possible

[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] To my knowledge, the vast majority of blockchain projects are (or plan to be) open-source protocols, with only few exceptions, such as Iota (a protocol that is not fully open source) and Binance Coin (a token that works as a "voucher" to access Binance, a traditional exchange).

whenever the protocol must be used in conjunction with a token. In case of protocols creating decentralized marketplaces, the token is typically the currency used by the two sides of the market. In blockchain projects without this “marketplace” element, the use of the token can vary. For example, in the case of cryptocurrencies such as Bitcoin, there are two types of users: people who need to exchange Bitcoins, and those who use their computers to process these transactions, also called miners. The first “pays” the second in two ways. One is direct: the sender of bitcoins can pay a fee to process the transaction faster, and this fee is earned by the miner. 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.[12] A similar mechanism is used within decentralized computing platforms such as Ethereum, with the difference that miners do not only process transactions, but can perform any arbitrary operation on the data contained in the ledger.

The most visible part of seigniorage is the Initial Coin Offering (ICO), where the developer sells tokens to investors and users for the first time. The first notable ICO was that of Ethereum in 2014, raising USD 2.3 million in approximately 12 hours. In a recent report, PwC estimates that in 2017 there were 552 ICOs raising a total of USD 7 billion (Diemers et al., 2018). The same report notes that the figures for 2018 are likely to be much larger: in the first five months of 2018 alone there were 537 ICOs raising USD 13.7 billion. For comparison, in 2016 total Venture Capital investment was USD 66.6 billion in the US and USD 4.7 billion in Europe (OECD, 2017). Interestingly, some analysts claim that about half of the ICOs launched in 2017 had already failed by early 2018.[13]

The less visible part of seigniorage is the sale on the open market of tokens that were not sold at ICO. With few exceptions,[14] either the sale of tokens on the open market is not disclosed, or it is discussed only within blog posts and informal communication.[15] More visible is the practice of rewarding suppliers using tokens.

[12] See also Huberman, Leshno, and Moallemi (2017).
[13] See http://fortune.com/2018/02/25/cryptocurrency-ico-collapse/.
[14] 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/.
[15] For example, see this blog post by the Ethereum foundation https://blog.ethereum.org/2016/01/07/2394/.

This is often referred to as “bug bounty programs” by which translators, coders, and marketers receive tokens for their work.

Despite this difference in visibility, recent work by Howell, Niessner, and Yermack (2018) and Amsden and Schweizer (2018) show that projects that go through an ICO sell only about half of their tokens at ICO, with the rest being kept by the founding team.[16] This indicates that for projects that go through an ICO, the two sides of seigniorage—the sale of tokens at ICO and the sale of tokens post-ICO—are comparable in terms of the number of tokens sold (or that are expected to be sold). Furthermore, it is not uncommon for some projects to skip the ICO stage and only sell tokens on the market, in a practice known as “airdrop”. This is typically the case for forks (i.e., derivations) of other projects, such as Stellar (a fork of Ripple and currently the sixth most valuable blockchain project by market capitalization), Bitcoin cash and Bitcoin Gold (forks of Bitcoin).[17]

## 1.3 Relevant literature

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

[16] More precisely, Howell et al. (2018) finds that 54% of tokens are sold at ICO, while Amsden and Schweizer (2018) put this number at 60%. Interestingly, Howell et al. (2018) also find that only about one third of the ICOs in their sample include vesting provisions that lock up the tokens not sold at ICO (or part of them) for some amount of time.

[17] Forks of existing projects typically distribute their tokens among the holders of the tokens associated with the project from which they are forking, sometimes creating additional tokens and allocating them to the founding team. For example, the developers behind Bitcoin Gold allocated to each Bitcoin holder an equal amount of Bitcoin Gold tokens, plus they created 100,000 new tokens and allocated them to themselves. Airdrops are becoming particularly popular with projects built on EOS, a decentralized computing platform (currently the fifth most valuable blockchain project by market capitalization). These projects distribute 20-30% of their tokens for free, wait for the token to start trading, and then sell part of their stock of tokens on financial exchanges. The goal seems to be to gain publicity, and to avoid the (few) legal constraints of an ICO. For more details on EOS airdrops, see https://hacked.com/everything-you-need-to-know-about-the-first-wave-of-eos-airdrops/.

Tirole, 2003); that is, whether the open source ethos will be compromised by the introduction of strong financial incentives.

Closely related is a recent literature building theoretical models of ICOs (see Sockin and Xiong, 2018; Li and Mann, 2018, Catalini and Gans, 2018; Chod and Lyandres, 2018). The main difference is that, in my model, the developer can sell tokens both at ICO and post-ICO. That is, these papers focus on a specific aspect of seigniorage (the ICO), while my goal is to capture it in its entirety. Of course, the converse is that these papers provide a more realistic and detailed description of how ICOs work, while here I simply assume that an ICO is an auction. A second important difference is that here the quality of the project is endogenous, which allows the study of the incentives for innovation generated by ICOs, and seigniorage more in general. With the exception of Chod and Lyandres (2018), all other papers building theoretical models of ICO, instead, take the quality of the project as given.

There is a small but growing literature studying 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 (2018), 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 in which the demand comes both from users and investors. The novelty with respect to their paper is that, here, the demand for tokens (originating from both investors and users) 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).[18]

[18] 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. I, instead, allow this demand to 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.

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

A line of literature that is also related is the one studying how the financial market may weaken incentive schemes faced by managers (see, for example, the seminal work by Diamond and Verrecchia, 1982 and the most recent Bisin, Gottardi, and Rampini, 2008; Acharya and Bisin, 2009). The reason is that, also in my model, the possibility of trading on the financial market reduces the incentives to exert effort and invest. The environment considered here is, however, different from the one in these papers, because there is no contract between the issuer of the currency (the developer) and those holding the currency (the investors). The developer's incentive problem depends on how the equilibrium price of the token is determined and how this price is affected by the developer's actions.

The remainder of the paper is organized as follows. Section 2 presents a model of seigniorage. Section 3 solves for its equilibrium. Section 4 illustrates the first best of the model and compares it to its equilibrium. Section 5 discusses some extensions to the model, and Section 6 concludes. Unless otherwise noted, all proofs and mathematical derivations missing from the text are in the Appendix.

## 2 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

[19] See, for example "Could a gigantic nonsovereign like Facebook someday launch a real currency to compete with the dollar, euro, yen and the like?" by Matthew Yglesias on Slate, February 29, 2012 (available at http://www.slate.com/articles/business/cashless_society/2012/02/facebook_credits_how_the_social_network_s_currency_could_compete_with_dollars_and_euros_.html).

protocol, which can be used by users to transact with each other. The development of the protocol lasts $T$ periods, after which the developer exits the game and the protocol continues being used indefinitely. At the beginning of the game, the developer establishes that all transactions using the protocol must be conducted using a specific token, with total supply $M$, fully owned by the developer.

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.[20] 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, next a frictionless market for tokens opens and then users can use the protocol. In every period after the developer exits (that is, in every $t > T$), first the market for tokens opens and then users use the protocol. See Figure 2 for a graphical representation of the timeline.

**Investors.** Investors are risk-neutral profit maximizers with no cash constraints. They can purchase tokens in every period and sell them during any subsequent period. Importantly, when buying or selling tokens on the market, they are price takers: their net demand for tokens in period $t$ depends on the sequence of token prices from period $t$ onward, which they take as given. Investors do not discount the future, and 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, therefore, 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.

**Users.** In every period $t \geq t_o$, there is a market for tokens, in which users can purchase tokens to be used with the protocol. The total value of all exchanges occurring using the protocol during a given period is the *value of the protocol* and

[20] As we will see when solving for the equilibrium, the important element of an auction is that the developer specifies in advance what share of the total stock of tokens will be sold and what share will be kept by the developer. Hence, despite the fact that not all ICOs are auctions (see, for example, the practice of holding *uncapped ICOs* in which the token's price is fixed and the number of tokens sold is determined in equilibrium), the results derived in this paper extend to other types of ICOs, as long as these shares are specified in advance.

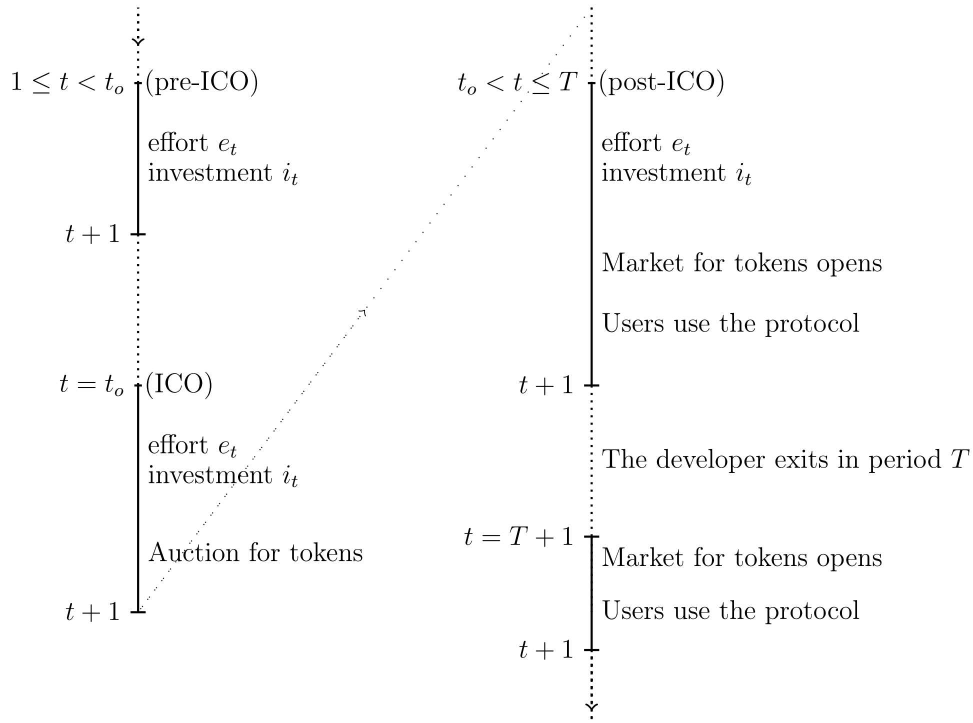



Fig. 2: Timeline

is defined as:

$$V_t = \sum_{s=1}^{t} f(e_s, i_s), \tag{1}$$

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.[21] This implies that those who use the protocol to purchase goods and services in period $t$ have a demand for tokens in period $t$ equal to $\frac{V_t}{p_t}$. Instead, those who use the protocol to sell goods or services in period $t$ have a supply of tokens in period $t+1$ equal to $\frac{V_t}{p_t}$.[22]

[21] That is, the velocity of the token is 1. Assuming a different velocity will introduce an additional parameter without affecting the results.

[22] This is abstracting away from the fact that, from period-$t$ point of view, the price in period $t+1$ may be uncertain, which may affect the willingness to trade using the protocol and the value of the protocol. Introducing this additional complication does not change the equilibrium price for tokens and hence the developer's incentive to exert effort and invest. I will argue later that, because no development occurs past period $T$, the price of the token is constant from $T$ onward.

The key assumption is that the value of the protocol is increasing in the sequence of effort and investment. The developer's effort and investment improve the protocol, in the sense of reducing transaction costs, increasing ease of use, increasing security, and reliability. As a consequence, more users (both on the selling side and on the buying side) will use the protocol to perform more/larger transactions. The above specification, however, abstracts away from a possible coordination problem in the adoption phase of the protocol. That is, 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 protocol is high) and a "low adoption" equilibrium (in which the value of the protocol is low). With a minimal loss of generality, the reader can interpret $V_t$ as the value of the protocol in one of these equilibria, the one that the developer expects to emerge.[23] Finally, the above formulation implies that the token is used as a mean of exchange. If the token is necessary in order to use the protocol, but without being a means of exchange, then $V_t$ is a measure of token usage which is not necessarily equal to the value of the exchanges occurring using the protocol. All of the results presented are robust to this different interpretation, with the exception of the back-of-the envelope calculations in Sections 4 and 5.1.

**The developer.** Call $Q_t \leq M$ the stock of tokens held by the developer at the beginning of period $t$, with $Q_1 = M$. Call:

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

the total resources available to the developer at the beginning of period $t$, where $a$ is the developer's initial assets (cash) and the rest are resources earned from the sale

Furthermore, the value of the protocol from $T$ onward must be larger than the value of the protocol in any previous period. Because of the investors, the price of the token in every period before $T$ is equal to the expected price of the token at $T$, which implies that only the expected value of the protocol in period $T$ matters in equilibrium. This remains true when uncertainty depresses the usage of the protocol in periods before $T$.

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

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:

$$i_t \leq A_t,$$

and a per-period cash constraint determining the maximum amount of tokens that can be purchased by the developer:

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

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 $t < T$:

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

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 $\lambda_t$ 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 at the beginning of each period. The developer understands the price formation mechanism.

# 3 Solution

## 3.1 Periods $t \geq T$

In this section, I show that, given the setup of the model and an appropriate equilibrium selection criterion (introduced below), the price of the token in period $T$ is strictly increasing in the value of the protocol $V_T$—and hence in the sequence of effort and investments made by the developer. It is important to keep in mind, however, that the solution to the developer's problem will depend exclusively on the fact that $p_T$ is strictly increasing in $V_T$, while the details of how $V_T$ affects $p_T$ will be relevant only to derive closed-form solutions. That is, the model is robust to different assumptions about what happens from period $T$ onward (for example, regarding the demand and supply of tokens by users or investors), provided that under these different assumptions $p_T$ is increasing in $V_T$.

The presence of investors and 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.

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:

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

The important observation is that the price at which the developer can sell his tokens in period $T$ is strictly increasing in the value of the protocol $V_T$, and therefore in the prior sequence of effort and investments.

## 3.2 The developer's problem

In solving the developer's problem, the following observation will play a key role. Because investors are price takers, in every $t > t_o$ their demand for tokens depend exclusively on $p_t$ and $\bar{p}_t$ (the largest future price) and not on the quantity of tokens sold by the developer in period $t$.[24] In particular, if $p_t = \bar{p}_t$, then investors are indifferent between purchasing any amount of tokens. At the same time, the equilibrium price in period $t$ should reflect effort and investments made prior to $t$. Hence, because the instantaneous demand for tokens by investors is inelastic to the supply of tokens, in every period the developer can sell any amount of tokens at the market price. But because prices react to effort and investment which in turn depend on the stock of tokens held by the developer, the amount sold by the developer in each period will have an effect on future prices.

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 $a$ 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.

### 3.2.1 Rich developer

If the cash constraint is never binding, the developer's utility can be written as, for $t \leq T - 1$:

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

[24] 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.

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 $T$.

Consider the last period of the developer's life. The fact that $p_T$ increases in $e_T$ and $i_T$ immediately implies that $\tilde{U}_T(Q_T)$ is strictly convex. The argument is quite standard: if $e_T$ and $i_T$ were fixed, then $p_T$ would be fixed and $\tilde{U}_T(Q_T)$ would be linear in $Q_T$. However, the optimal $e_T$ and $i_T$ are:[25]

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

$$i^*(Q_T) \equiv \text{argmax}_i \left\{ f(e^*(Q_T), i) \frac{Q_T}{(1-\gamma)M} - i \right\}. \tag{3}$$

As long as either $e^*(Q_T)$ or $i^*(Q_T)$ are positive for some $Q_T \leq M$ (an assumption maintained in order to avoid trivialities), then optimal effort and investment react to changes in $Q_T$, which implies that $\tilde{U}_T(Q_T)$ must grow faster than linearly.

Consider now the choice of $Q_T$ in period $T-1$. For given $e_{T-1}$ and $i_{T-1}$, the developer chooses $Q_T$ so as to maximize $p_{T-1}(Q_{T-1} - Q_T) + \tilde{U}_T(Q_T)$, which is strictly convex in $Q_T$ because $\tilde{U}_T(Q_T)$ is strictly convex. It follows that, 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:

$$p_{T-1} = \frac{\tilde{U}_T(M)}{M} = \frac{V_{T-1} + f(e^*(M), i^*(M))}{(1-\gamma)M} - \frac{(e^*(M))^2/2 + i^*(M)}{M}, \tag{4}$$

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

[25] With a slight abuse of notation, I ignore the time index when writing optimal effort and optimal investment. I show below that these functions are, in fact, time invariant. Note also that, 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.

at the beginning of period $T$.

Note, however, that if investors expect the developer to sell all of his tokens, they should also expect no effort or investment in period $T$, and therefore $p_{T-1}$ should be low. If instead they expect the developer to set $Q_T = M$, they should expect maximum effort and investments in period $T$ and therefore $p_{T-1}$ should be high. 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 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 $\alpha_{T-1}$ is the probability that the developer sells all of his tokens in period $T-1$, which using (4) can be written as:

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

For intuition, note that $(e^*(M))^2/2 + i^*(M)$ is the cost generated by holding $M$ tokens, coming from the additional effort and investment that the developer will exert in period $T$. Instead:

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

is the benefit of setting $Q_T = M$, coming from the increase in the value of these tokens due to the developer's effort and investment in period $T$. $\alpha_{T-1}$ 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 $\alpha_{T-1} \leq 1$.

The following proposition shows that these results generalize to every period in which the market for tokens operates.

**Proposition 1** (Equilibrium post-ICO). *In every period $t \in \{t_o + 1, ..., T\}$:*

1. *Optimal effort and investment for given $Q_t$ are $e^*(Q_t)$ and $i^*(Q_t)$, given by* (2) *and* (3)*,*

2. *The developer sells all his tokens (so that $Q_{t+1} = 0$) with probability*

$$\alpha_t = \begin{cases} 1 & \textit{if } t = T \\ (1-\gamma)\frac{(e^*(M))^2/2 + i^*(M)}{f(e^*(M), i^*(M))} & \textit{otherwise} \end{cases} \tag{5}$$

   *and purchases all tokens (so that $Q_{t+1} = M$) with probability $1 - \alpha_t$,*

3. *The price of tokens as a function of past effort and investment is*

$$p_t = \frac{V_t + (1-\alpha_t)(T-t)f(e^*(M), i^*(M))}{(1-\gamma)M}. \tag{6}$$

The proposition is based on the fact that all $\tilde{U}_t(Q_t)$ are strictly convex and, therefore, in every period $t < T$ the equilibrium price must be such that the agent is indifferent between holding all of his tokens and selling all of his tokens. But this also implies that the agent is indifferent between selling all of his tokens in period $t$ or holding $M$ in every period until $T$. The benefit of exerting effort and of investing in a given period is therefore given by the resulting change in $p_T$, which is constant over time and given by (2) and (3).

Hence, whenever $Q_t = M$ the value of the protocol increases by $f(e^*(M), i^*(M))$ in period $t$, while if $Q_t = 0$ the value of the protocol does not change in period $t$. The probability that $Q_t = 0$ is such that investors are indifferent between holding the token at $t-1$ or at $t$, and is also constant over time. It follows that the price in period $t$ (Equation (6)) reflects past effort and past investment via the term $V_t$, as well as expected future effort and investment via the term $(1-\alpha_t)(T-t)f(e^*(M), i^*(M))$. This expression 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. Hence, contrary to all subsequent periods, in period $t_o$ the price of a token depends on the number of tokens sold, which is $M-Q_{t_o}$. 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:

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

where the first and the last equality follow from writing $\tilde{U}_{t_{o+1}}(Q_{t_{o+1}})$ explicitly (under the assumption that the developer sells all of his tokens in period $t_{o+1}$). 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 $t_{o+1}$. By choosing $Q_{t_{o+1}}=M$, the developer maximizes effort and investments in period $t_{o+1}$, and therefore the price in period $t_{o+1}$. If instead $t_o=T$, then the developer sells all of his tokens during the ICO, and then exits the game. The following proposition summarizes these observations.

**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.*

*Proof.* In the text. □

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 protocol is maximized when the developer holds $M$ tokens in every period until $T$, but this cannot happen in equilibrium. From period $t_{o+2}$ onward, the developer exerts effort and invests with probability less than one, which implies the following proposition:

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

*Proof.* In the text. □

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 $T$. As a consequence, 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 $a \geq T \cdot i^*(M)$.*

*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.

Finally, it is easy to check that the developers' utility does not depend on the total stock of tokens $M$. From (2) and (3) 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 5, also independent from $M$). This implies that $V_T$ and, as a consequence, $p_t M$ are independent from $M$. The developer's utility is therefore independent from $M$ for any $t_o$.

### 3.2.2 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: its 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 $a < T \cdot i^*(M)$: 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:

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

where $\mathbb{1}\{\}$ is the indicator function, and $g(e)$ is strictly increasing and strictly concave. 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.

Given this, period-T effort and investment are:

$$\hat{e}_T(Q_T, i_T) \equiv \begin{cases} e^*(Q_T) \equiv \text{argmax}_e \left\{ g(e)\frac{Q_T}{(1-\gamma)M} - \frac{1}{2}e^2 \right\} & \text{if } i_T \geq \bar{i} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

$$\hat{i}_T(Q_T, A_T) \equiv \begin{cases} \bar{i} & \text{if } \bar{i} \leq \max_e \left\{ g(e)\frac{Q_T}{(1-\gamma)M} - \frac{1}{2}e^2 \right\} \text{ and } \bar{i} \leq A_T \\ 0 & \text{otherwise.} \end{cases} \tag{8}$$

To avoid trivial equilibria in which there is never any effort or investment, I furthermore assume that:

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

that is: there is a level of $Q_T$ for which the developer will invest and exert positive effort whenever his assets are sufficient to do so. I call the threshold level $\hat{Q}$, implicitly defined as:

$$\hat{Q} \equiv Q: \quad \bar{i} = \max_e \left\{ g(e)\frac{Q}{(1-\gamma)M} - \frac{1}{2}e^2 \right\}. \tag{9}$$

In the remainder of this section, I fully solve for the equilibrium in periods $T$ and $T-1$, depending on whether the ICO happened in period $T$, $T-1$ or in any earlier period. I will only informally discuss the equilibrium in periods before $T-1$. Nonetheless, I will provide a characterization of the optimal timing of the ICO.

**Case 1:** $t_o = T$**.** If the ICO occurs in the last period, then optimal effort and investment in period $T$ are given by (7) and (8). The price of a token is therefore:

$$\frac{V_{T-1}}{(1-\gamma)M} + \begin{cases} 0 & \text{if } A_T < \bar{i} \\ \frac{g(e^*(M))}{(1-\gamma)M} & \text{otherwise.} \end{cases}$$

In period $T-1$, the choice of optimal investment affects $A_T$ and the period-T optimal effort and investment. This is relevant whenever $\bar{i} \leq A_{T-1} < 2\bar{i}$, that is, whenever assets in period $T-1$ are not sufficient to invest optimally in both period

$T-1$ and period $T$. It is immediately clear that, in this case, the final price is always $\frac{V_{T-2}+g(e^*(M))}{(1-\gamma)M}$, independent from whether effort and investment are positive in period $T-1$ or in period $T$. The same logic applies to the choice of investment and effort in any earlier period. Define:

$$n \equiv \text{argmax}_{k\in\{1,2,\dots,T\}}\{k \cdot \bar{i} \leq a\}, \tag{10}$$

as the number of periods in which the developer can invest efficiently using his initial assets exclusively. The above discussion implies that the developer will invest and exert effort for $n$ periods, and he is indifferent with respect to which ones. The following proposition summarizes these observations.

**Proposition 4** (ICO in period $T$)**.** *Whenever $t_o = T$, the final value of the protocol is $V_T = n \cdot e^*(M)$.*

*Proof.* In the text. □

**Case 2:** $t_o = T-1$. If the ICO occurs in period $T-1$, then the developer can finance some of the period $T$ investment by selling tokens in period $T-1$. Remember that, in equilibrium, the price of tokens at ICO $p_{T-1}$ must be equal to $p_T$. Hence, for given $M - Q_T$ (i.e., tokens sold at ICO), the price for tokens will be:

$$p_T = \frac{V_{T-1}}{(1-\gamma)M} + \begin{cases} 0 & \text{if } A_{T-1} - i_{T-1} + p_T(M-Q_T) < \bar{i} \\ \frac{g(e^*(Q_T))}{(1-\gamma)M} & \text{otherwise.} \end{cases} \tag{11}$$

Whenever $A_{T-1} - i_{T-1} < \bar{i}$ (that is, whenever the developer does not have enough own funds to invest in period $T$), both LHS and RHS of (11) depend on $p_T$, and therefore for given $Q_T$ there are multiple equilibrium $p_T$. For intuition, suppose that the developer announces the sale of $M - Q_T$ tokens at ICO. If investors expect $p_T$ to be low, they will drive down $p_{T-1}$ (the price at ICO), which implies that the level of investment achievable in period $T$ by selling $M - Q_T$ at ICO may be below $\bar{i}$, which justifies the initial expectation. If instead investors expect $p_T$ to be high, in equilibrium $p_{T-1}$ will also be high, which implies that the level of investment achievable in period $T$ by selling $M - Q_T$ tokens at ICO may be above $\bar{i}$, which justifies the initial expectation. This can be interpreted as a coordination problem among investors. For any number of tokens sold by the developer at ICO, investors may coordinate on a "high" equilibrium that leads to high effort and investment in period $T$, or on a "low" equilibrium leading to low (or no) effort and investment in period $T$. Call $p(Q_T)$ the correspondence mapping $Q_T$ to the equilibrium $p_T$. We therefore have (see also Figure 3):

$$p(Q_T) = \begin{cases} \frac{V_{T-1}}{(1-\gamma)M} & \text{if } \frac{\bar{i}+i_{T-1}-A_{T-1}}{M-Q_T} < \frac{V_{T-1}+g(e^*(Q_T))}{(1-\gamma)M} \\ \frac{V_{T-1}+g(e^*(Q_T))}{(1-\gamma)M} & \text{if } \frac{\bar{i}+i_{T-1}-A_{T-1}}{M-Q_T} > \frac{V_{T-1}}{(1-\gamma)M} \\ \left\{ \frac{V_{T-1}}{(1-\gamma)M}, \frac{V_{T-1}+g(e^*(Q_T))}{(1-\gamma)M} \right\} & \text{otherwise.} \end{cases}$$

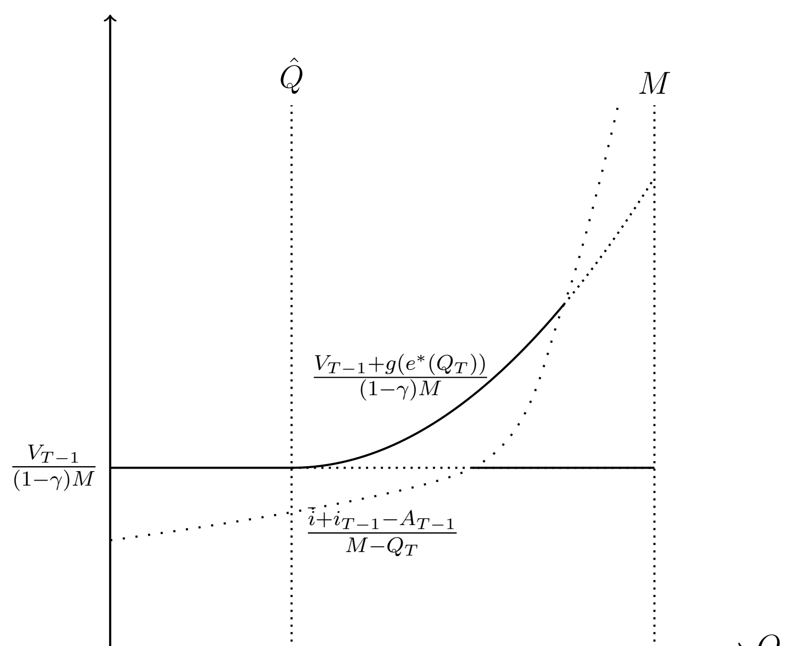



Fig. 3: $p(Q_T)$ whenever $\bar{i} + i_{T-1} > A_{T-1}$.

Given this, we can solve for the utility-maximizing $Q_T$. As a preliminary step, the next lemma shows that $U_T(Q_T, A_T)$ is convex in $Q_T$, provided that the developer has enough wealth to invest, and provided that he has enough "skin in the game" in the sense that $Q_T > \hat{Q}$.

**Lemma 1.** *$U_T(Q_T, A_T)$ 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 $Q_T \geq \hat{Q}$.*

*Proof.* By the same argument made in the previous case: $U_T(Q_T, A_T)$ is linear in $Q_T$ whenever optimal investment and effort do not change with $Q_T$, and is strictly convex whenever optimal investment and effort depend on $Q_T$. Similarly, $U_T(Q_T, A_T)$ is discontinuous in $A_T$ whenever the level of wealth allows for the optimal level of investment. □

Note, however, that $A_T$ is also a function of $Q_T$, because:

$$A_T = A_{T-1} + (M - Q_T) \cdot p_{T-1} - i_{T-1},$$

where $p_{T-1} \in p(Q_T)$ is the price of tokens at ICO. Hence, the choice of $Q_T$ determines both period $T$'s incentives to exert effort and whether the developer will have enough resources to invest. The next lemma shows that the continuation value is maximized at:

$$Q_T^* = M - \frac{\max\{i_{T-1} + \bar{i} - A_{T-1}, 0\}}{p_{T-1}}, \tag{12}$$

which is the largest $Q_T$ such that the developer can invest $\bar{i}$ in period $T$.

**Lemma 2** (Equilibrium in period $T-1$ for $t_o = T-1$)**.** *If $Q_T^* > \hat{Q}$ the developer chooses $Q_T = Q_T^*$; there is positive investment and effort in period $T$. If instead $Q_T^* \leq \hat{Q}$ then the developer is indifferent between any $Q_T$, and there is no investment or effort in period $T$. When $A_{T-1} - i_{T-1} < \bar{i}$ multiple equilibria are possible and $Q_T^*$ may not be unique. When $A_{T-1} - i_{T-1} \geq \bar{i}$ the equilibrium is unique and $Q_T^* = M$.*

For intuition, remember that the developer has incentives to invest and exert effort in period $T$ only if $Q_T > \hat{Q}$. Whether $Q_T > \hat{Q}$ is attainable depends on the cash constraint. If this constraint is tight, $Q_T^* \leq \hat{Q}$ and no level of $Q_T$ that allows for positive investment will generate sufficient incentives, and hence there will be no development in period $T$. If instead the cash constraint is sufficiently loose, then $Q_T^* > \hat{Q}$ and for some level of $Q_T$ there will be positive effort and investment in period $T$.

In this last case, multiple equilibria are possible. This is because the right hand side of (12) may be neither monotonic nor continuous (remember that $p_{T-1} \in p(Q_T)$). That is, even assuming that the investors can solve their coordination problem and therefore $p(Q_T)$ is a function and not a correspondence, there is an additional coordination problem between developer and investors giving rise to multiple equilibrium $Q_T^*$. Suppose that $A_{T-1} - i_{T-1} < \bar{i}$, so that the developer needs to sell some tokens at ICO in order to finance future development. If the price in period $T$ is expected to be high, so will be the price in period $T-1$ and, as a consequence, the developer needs to sell fewer tokens in order to achieve $i_T = \bar{i}$. Because he can hold a large fraction of tokens, future effort will be high, which implies that today's price for tokens should be high. Similarly, if period-$T$ price is expected to be low, price at ICO will be low, and the developer needs to sell a large fraction of his tokens, which implies that future effort will be low, as should today's price. If instead $A_{T-1} - i_{T-1} \geq \bar{i}$, then the developer does not need to sell any tokens to finance his future investment and, as a consequence, in the unique equilibrium $Q_T^* = M$.

Consider now optimal investment and effort in period $T-1$. It is easy to see that optimal effort is again given by (7). The choice of optimal investment, instead, has an inter-temporal element to consider: for given initial assets, the choice of period $T-1$ investment affects the equilibrium at ICO and therefore $Q_T^*$. This is relevant whenever $A_{T-1} < 2\bar{i}$, in which case the developer may choose not to invest in period $T-1$, so as to set $Q_T^* = M$.

It is, however, easy to show that postponing the investment is never optimal. Suppose that the developer has sufficient funds to invest in only one period. If the developer invests in period $T-1$, then total utility is:

$$\frac{V_{T-2} + g^*(M) + g^*(Q_T^*)}{(1-\gamma)M} M - \frac{1}{2}(e^*(M))^2 - \frac{1}{2}(e^*(g^*(Q_T^*))^2.$$

If instead the developer does not invest in $T-1$, he can set $Q_T = M$ and achieve utility:

$$\frac{V_{T-2} + g^*(M)}{(1-\gamma)M} M - (e^*(M))^2.$$

Comparing the above two expressions, it is clear that the developer is better off using his own funds for investing in period $T-1$, and then financing period-T investment via the sale of tokens at ICO. This reasoning extends to any period prior to the ICO, and therefore implies the following proposition.

**Proposition 5** (ICO in period 2)**.** *Whenever $t_o = T-1$, the final value of the protocol is:*

$$V_T = \begin{cases} 3g^*(M) & \text{if } a \geq 3\bar{i} \\ ng^*(M) + g^*(Q_T^*) & \text{otherwise,} \end{cases}$$

*where $n$ is defined in* (10) *and $Q_T^*$ is defined in* (12)*.*

*Proof.* In the text. □

**Case 3:** $t_o < T-1$. If the ICO occurred in period $t_o < T-1$, then in period $T-1$ there is a market for tokens. I start by considering the choice of $Q_T$, that is, how many tokens to sell or buy on the market in period $T-1$. For a given market price $p_{T-1}$, the developer's utility as a function of $Q_T$ is:

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

There are similarities with the previous case (i.e., the case of an ICO in period $T-1$). Also here, the choice of $Q_T$ determines the assets available in the following period. As a consequence, the continuation value:

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

is strictly convex in $Q_T$ only for:

$$\hat{Q} \leq Q_T \leq Q_T^*,$$

and is linearly increasing in $Q_T$ otherwise, with a downward discontinuity at $Q_T^*$ (where $Q_T^*$ is defined in (12)).

There are, however, two important differences with the previous case. The first one is that, here, the developer could have sold some tokens during a previous period, and therefore it is possible that $Q_{T-1} < M$. It follows that the cash constraint in period $T-1$ may be binding. In this respect, note that if the cash constraint in period $T-1$ is binding, then $A_T = 0$ and the cash constraint in period $T$ is binding. Conversely, if the period $T$ cash constraint is binding, we have $A_T = \bar{i}$, which implies that the period $T-1$ cash constraint is not binding. Hence, in solving for $Q_T$, the only constraint that needs to be taken into consideration is the period-$T$ cash constraint.

Second, and most importantly, because investors are price takers, then the market price in period $T-1$ does not depend on $Q_T$. Only period-$T$ price depends on $Q_T$, leading to the same type of anti-coordination problem discussed in the "rich developer" case.

**Lemma 3** (Equilibrium in period $T-1$ for $t_o < T-1$)**.** *If $Q_T^* \leq \hat{Q}$, then the developer is indifferent between holding any level of $Q_T$. Effort and investment in period $T$ are zero, so that $p_T = p_{T-1} = \frac{V_{T-1}}{(1-\gamma)M}$.*

*If instead $Q_T^* > \hat{Q}$, then, in equilibrium, the developer is indifferent between setting $Q_T = 0$ and setting $Q_T = Q_T^*$. He sets $Q_T = 0$ with probability:*

$$\alpha_{T-1} = \left(\frac{1}{2}(e^*(Q_T^*)^2 + \bar{i}\right)\left(Q_T^* \cdot \frac{g(e^*(Q_T^*)}{(1-\gamma)M}\right)^{-1}.$$

*The equilibrium price is:*

$$p_{T-1} = \frac{V_{T-1} + (1-\alpha_{T-1})g(e^*(Q_T^*))}{(1-\gamma)M}.$$

*If $A_{T-1} - i_{T-1} \leq \bar{i}$ multiple equilibria are possible, while if $A_{T-1} - i_{T-1} > \bar{i}$ the equilibrium is always unique.*

By comparing the above lemma with Lemma 2, we see that, whenever $Q^* > \hat{Q}$, if the market for tokens exists the equilibrium is in mixed strategies, while if the tokens are sold via an ICO the equilibrium is in pure strategies. The reason is that the presence of the market generates the same anti-coordination problem discussed in the previous section. The developer randomizes between selling everything and setting $Q_T = 0$ and holding the maximum number of tokens, which is the minimum between the one at which period-$T$ cash constraint is binding and $M$.

The other features of the equilibrium are similar. In particular, whenever $A_{T-1} - i_{T-1} \leq \bar{i}$ there could be multiple equilibria. There could be an equilibrium in which $p_{T-1}$ is high, which implies that the developer needs to sell only a few tokens to finance future investment, and therefore period-T effort is high. Next to this equilibrium, there could be one in which $p_{T-1}$ is low, which implies that the developer needs to sell many tokens to finance future investment, and therefore period-T effort is low. If, instead, $A_{T-1} - i_{T-1} > \bar{i}$, then the developer does not need to sell any tokens to achieve $i_T = \bar{i}$, and this coordination problem is absent. In case the market for tokens is open, there are therefore multiple mixed strategy equilibria, each corresponding to a different $Q_T^*$ and a different $p_{T-1}$.

Deriving the equilibrium in earlier periods is complicated by the fact that the choice of investment in every period affects the equilibrium in all subsequent periods. For example, the choice of $i_{T-1}$ affects $Q_T^*$. Hence, the developer may want to set $i_{T-1} = 0$ even if $A_{T-1} \geq \bar{i}$ and $Q_{T-1} > \hat{Q}$ so as to achieve a higher $Q_T^*$. Not only, but because there are multiple equilibrium $Q_T^*$, the choice of $i_{T-1}$ may determine what equilibrium emerges in the market for tokens. This difficulty extends to the choice of $Q_{T-2}$, because $Q_{T-2}$ determines $i_{T-1}$.

Despite these issues, it is possible to characterize the developer's choice of when to hold an ICO. The reason is that every time the market is open, there is the basic anti-coordination problem discussed earlier and the equilibrium is in mixed strategy. If instead the developer does not hold the ICO and has sufficient funds to invest $\bar{i}$, he will set a high level of effort and investments with probability 1. Hence, if the developer's funds are greater that $\bar{i}$, he will never want to hold the ICO. But if the developers funds are below $\bar{i}$, then no development will occur unless the developer holds the ICO. This observation implies the following proposition.

**Proposition 6.** *In equilibrium $t_o = n$, that is, the developer initially invests using his own funds, and holds the ICO as soon as his funds are below $\bar{i}$.*

*Proof.* In the text. □

To conclude, note that, also here, the developer's payoff does not depend on $M$. The reason is that, in each period, the developer's problem depends on $M$ only via the share of $M$ that he holds (see the optimal level of effort (2) and the incentive to set positive investment (9)). Therefore, in each period, the value of the protocol and the value of all outstanding tokens $p_t M$ depend on the share of tokens held by the developer in each period and not on $M$. In addition, in all cases analyzed, the equilibrium share of tokens held by the developer in a given period is either zero, $M$ or $Q_T^*$. It is easy to see that, if $p_t M$ is independent from $M$, so is $Q_T^*/M$, and therefore the equilibrium share of tokens held by the developer in each period is also independent from $M$.

## 4 First best

In the first best, effort and investment are set to maximize the present discounted value of the surplus generated by the protocol.[26] Furthermore, the ICO is held immediately so as to allow users to use the protocol from the very beginning.

The equilibrium of the game differs from the first best in several ways. As already discussed, in equilibrium the developer will want to hold the ICO only after exhausting his own funds. This is, however, inefficient because users are prevented from using the protocol before the ICO. The equilibrium post-ICO is also inefficient because the developer may set zero effort and zero investment, even if the social value of his effort and investment is strictly positive.

More interestingly, even assuming that the market for tokens exists so that users can use the protocol and that the developer will set positive effort and investment, there is an additional source of inefficiency. The developer is setting effort and investment so as to maximize the value of the protocol in period $T$, when he will exit the game. A minor observation is that the value of the protocol in a given period (i.e., the value of the transactions that occur using the protocol) is, in general, different from the social surplus generated by the protocol.[27] A more important observation is that, in its objective function, the developer completely disregards the fact that the protocol will generate value over multiple periods, instead focusing exclusively on the period in which he will sell all of his tokens and exit the game.

Whether the developer's effort and investment will be above or below their first

[26] The discount factor should be that of users.

[27] The social surplus depends on the equilibrium utility/profits of users on the buying and selling side of the protocol, as well as on their outside options.

best level is, however, ambiguous as it depends on $\gamma$, which determines the elasticity of the price of token to his effort and investment. If the speculative demand for tokens is sufficiently high, then the developer will exert effort and investment above the first best. If instead it is low, then the developer may exert effort and invest below the first best.

It is possible to resolve this ambiguity by introducing a few simplifying assumptions and performing some back-of-the-envelope calculations. Consider the rich developer case, and assume that the value of the protocol in a given period is a good approximation of the surplus generated in that period. Social welfare is therefore:[28]

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

where $\beta$ is the user's discount factor.

The choice of effort and investment that maximize social welfare is:

$$e^{**} \equiv \text{argmax}_e \left\{ \frac{f(e, i^{**})}{1-\beta} - \frac{1}{2}e^2 \right\} \tag{13}$$

$$i^{**} \equiv \text{argmax}_i \left\{ \frac{f(e^{**}, i)}{1-\beta} - i \right\}. \tag{14}$$

By comparing the above expression with the equilibrium level of effort and investment (equations (2) and (3) for $Q_T = M$), it is clear that equilibrium effort and investment will be below the efficient level if $\gamma < \beta$, and above the efficient level if $\gamma > \beta$.

Remember that $\gamma$ is the fraction of tokens held by investors in period $T$ when the developer exits the game. The fraction of tokens held by investors before $T$ could be much higher, even close to 100% in early periods. The empirical counterpart for $\gamma$ is therefore the fraction of tokens held by investors when the project is mature and (major) developments no longer occur, which is a stage no blockchain-based

[28] This expression assumes that the protocol will not be used before $T$. It is therefore a measure of welfare in a "constrained" first best, in which the timing of the ICO cannot be changed. Of course, the value generated by the platform before $T$ is second order relative to the value generated by the platform from $T$ onward. We can, therefore, also think of this expression as an approximation of the unconstrained social welfare.

protocol has yet reached.

In my opinion, at present the best possible estimate for $\gamma$ comes by looking at Ethereum. 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.[29] Instead, Ethereum is a decentralized computing platform and is 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 protocol $V_t$: the payments (in tokens) from users of Ethereum to the nodes maintaining the Ethereum network, performed in exchange for a service—executing a smart contract.[30]

After collecting data on the total fees paid on the Ethereum network,[31] what remains to do in order to derive $\gamma$ 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 average number of days before a given token can be used again to pay a fee (that is, the inverse of the velocity of ETH). Absent any good prior, I will consider different options, 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 first six months of 2018, where the $n$ goes from 1 to 30. This value corresponds to $\gamma$, 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 $\gamma$ is orders of magnitude above $\beta$, which suggests that the equilibrium effort and investment is above the efficient level.[32]

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

[30] 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.

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

[32] In these calculations, I considered the total stock of ETH as the total number of ETH at the

| $n$ | $\gamma$ | $\beta$ |
|---|---|---|
| 1 | 0,99999 | 0,00015 |
| 2 | 0,99998 | 0,00030 |
| 3 | 0,99998 | 0,00045 |
| 4 | 0,99997 | 0,00060 |
| 5 | 0,99996 | 0,00075 |
| 6 | 0,99996 | 0,00090 |
| 7 | 0,99995 | 0,00105 |
| 8 | 0,99994 | 0,00120 |
| 9 | 0,99994 | 0,00135 |
| 10 | 0,99993 | 0,00150 |
| 20 | 0.99989 | 0.00300 |
| 30 | 0.99986 | 0.00451 |

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

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 $\beta$ and $\gamma$ 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.

# 5 Discussion

## 5.1 Seigniorage vs monopoly pricing

It is possible to compare seigniorage with more standard mechanisms, such as establishing a set of fees/prices for using the protocol. Profits generated via seigniorage

end of the period (that is, end of June 2018). The conclusion remains the same if I were to consider the total number of ETH at the beginning of January 2018, or the average total number of ETH over this period.

depend on the value of the protocol in the moment at which the developer sells his tokens. Under standard monopoly pricing, instead, the monopolist is able, in every period, to capture only a fraction of the value of the protocol (which will depend on the elasticity of supply and demand). But the monopolist is able to earn profits in every period; not only in one period.

Profits under seigniorage therefore depend on the value of the protocol in a given period, while profits under standard monopoly pricing will accrue in every period. Which one is larger is, again, ambiguous and crucially depends on $\gamma$: the speculative demand for tokens. It is always possible to find a large enough $\gamma$ such that profits under seigniorage are greater than profits under monopoly pricing. For low $\gamma$, however, the ranking may reverse.

The same back-of-the envelope calculations reported in Table 1 are useful also here. Call $\tau$ the fraction of total value lost as deadweight loss caused by monopoly pricing, and $\nu$ the fraction of the remaining value that is captured by the monopolist in every period. 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:

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

The above inequality can be satisfied only if $\beta > \gamma$. However, the above calculations suggest that this inequality does not hold empirically, and hence profits under seigniorage are larger than profits under monopoly pricing for any value of $\nu$ and $\tau$.

## 5.2 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. The price in every period is equal to the expected price tomorrow, which depends on the developer's expected contribution to the protocol. 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.[33]

The important observation is that, if at ICO the productivity of the developer is unknown to investors, it will nonetheless 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.

Less obvious is the impact of asymmetric information on the timing of the ICO. A developer of ability greater than the investors' expectation may benefit from anticipating the ICO, because he expects to exert effort and invest in the development of the protocol with probability 1 for a few periods post-ICO. But if this is the case, then investors should infer that a developer holding an ICO early is of high ability. This, clearly, cannot be an equilibrium because, now, the high-ability developer no longer benefits from anticipating the ICO. The full analysis of this problem is left for future work.

## 5.3 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 protocol 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

[33] The same argument can be made about wealth. If the developer's wealth is private information and affects the development of the protocol, then a developer who is richer than the market expectation about his wealth will want to purchase all tokens and develop with probability one. Otherwise he will sell all tokens and not develop.

that the developer with the largest $q^i_{t+1}$ is indifferent between holding all tokens or no tokens.[34] If, furthermore, $\max_j q^j_t$ 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 protocol.

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 he 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 in the development of the protocol. The identity of the developer that, in every period, develops the protocol (with some probability) depends partly on productivity and partly on wealth.

## 5.4 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 protocol (and the developer's payoff) is always higher in the rich developer case. This observation suggests that an external in-

[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.

vestor (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. Under perfect contracting, therefore, in the poor developer case the traditional investor would always provide funds to the developer. Traditional financing and seigniorage are, in this case, complementary. If instead the investors and the developer are constrained in the type of contracts they can sign, then the external investor may not provide funds.[35]

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 $\rho$ at ICO. It is quite easy to see that 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* the level of effort and investment will be lower, because the developer anticipates that his payoff will be $(1-\rho)Mp_T$. Clearly, there are cases in which the outside investment will not happen.[36]

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 protocol increases (relative to no outside investment). But contractual frictions may prevent the traditional investor and the developer from finding an agreement, even when such an agreement would be welfare-maximizing.

[35] 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/ and https://www.bloomberg.com/news/articles/2017-10-03/hedge-funds-flip-icos-leaving-other-investors-holding-the-bag. See also a recent paper by Chod and Lyandres (2018), 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.

[36] For example, if the developer already has enough funds to invest efficiently in the first $T-1$ periods (so that the need for external funds is small) and $T$ is very large (so that the drop in effort and investment may be small in every single period but have a large effect on the value of the protocol), then the developer and the investor may not sign a contract.

## 6 Conclusion

This paper studies a novel form of financing for open-source software development: seigniorage. I show that seigniorage is effective at generating incentives and providing financial resources for the development of open-source blockchain-based protocols. Its effectiveness is, however, limited by the fact that whenever a market for tokens exists, in equilibrium there is a positive probability that the developer will sell all of his tokens and that, as a consequence, no development will occur. I also argue that the equilibrium will be inefficient, because the developer's objective is to maximize the value of the protocol in a single period (when he expects to leave the game), and does not internalize the fact that the protocol generates value over multiple periods.

The paper shows that, thanks to seigniorage, the developer earns positive profits, users enjoy the full surplus generated by the protocol, while at the same time investors are left indifferent. Some readers may therefore wonder if seigniorage is magic. 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.[37] Initial holders of cash are therefore made worse off by the introduction of the token. In this general-equilibrium framework, the developer should anticipate that an increase in the value of the protocol 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.

The model abstracts away from a few important elements. The first one is asymmetry of information. This is an intentional feature of the model, and illustrates the fact that the failure to develop a project following an ICO should not be considered exclusively as the result of deception and fraud. Nonetheless, how asymmetry

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

of information changes the equilibrium of the model is an important question. As discussed in the text, the post-ICO equilibrium only marginally changes with the introduction of asymmetric information. The choice of the timing of the ICO is instead likely to be affected in a non-trivial way, especially if an outside investor is present.

The model also abstracts away from competition, either from other open-source blockchain-based protocols or traditional companies. Remember that, in the model, users enjoy the full surplus generated by the protocol. Hence, a competing open-source blockchain-based protocol (or a traditional company) can attract users only if it can generate a higher surplus, either by providing a better technological solution or by attracting a larger user base. This could affect the timing of the ICO. If there are "winner takes all" dynamics and network effects, it is conceivable that the developer will want to anticipate the ICO, so as to build a sufficiently large user base and prevent the entrance of competitors. However, assuming that the source code is disclosed at ICO, holding an ICO earlier also gives the opportunity for competitors to copy the code and imitate some features. The full treatment of asymmetry of both information and competition is also left for future work.

# A Mathematical appendix

*Proof of Proposition 1.* In the text I show that if $\tilde{U}_T(Q_T)$ is strictly increasing and convex, strictly so for some $Q_T$. 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:

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

that is, I can write the utility in period $T-1$ assuming that the developer sells all of his tokens in period $T$. Again, because effort and investment affect $p_T$, then $\tilde{U}_{T-1}(Q_{T-1})$ is strictly increasing and convex (strictly so somewhere). Again, in equilibrium, in period $T-2$ the developer is indifferent between selling all of his tokens or keeping all of his tokens. Therefore, I can write:

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

which is strictly increasing and convex (strictly so somewhere). Repeating the same argument implies that all $\tilde{U}_t(Q_t)$ are strictly increasing and convex (strictly so somewhere), and therefore in every period the only possible equilibrium is one in which the developer is indifferent between selling all of his tokens or purchasing all tokens. All $\tilde{U}_t(Q_t)$ can be written as:

$$\tilde{U}_t(Q_t) = \max_{e_t, i_t, e_{t+1}, i_{t+1}, \ldots, e_T, i_T} \left\{ -\sum_{s=t}^{T} i_s - \sum_{s=t}^{T} \frac{e_s^2}{2} + Q_{t-1} \cdot p_T \right\},$$

which implies that, in every period, optimal effort and investment are again given by (2) and (3).

Furthermore, for the agent to be indifferent, in every period the price must be $p_t = \frac{\tilde{U}_{t+1}(M)}{M}$. Writing the utility function in period $t+1$ as above, and using optimal effort and investment, we get:

$$p_t = \frac{V_t + (T-t) f(e^*(M), i^*(M))}{(1-\gamma)M} - (T-t)\frac{e^*(M)^2/2 + i^*(M)}{M}. \tag{15}$$

It follows that if $Q_t = M$, then:

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

if instead $Q_t = 0$, then:

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

Call $\alpha_{t-1}$ the probability that in period $t-1$ the developer sells all of his tokens. Because investors must be willing to hold tokens between the two periods, it must be that:

$$\begin{aligned} p_{t-1} =& \frac{V_{t-1} + (T-t+1) f(e^*(M), i^*(M))}{(1-\gamma)M} - (T-t+1)\frac{e^*(M)^2/2 + i^*(M)}{M} = \\ &\alpha_{t-1}\left(\frac{V_{t-1} + (T-t) f(e^*(M), i^*(M))}{(1-\gamma)M} - (T-t)\frac{e^*(M)^2/2 + i^*(M)}{M}\right) + \\ &(1-\alpha_{t-1})\left(\frac{V_{t-1} + (T-t+1) f(e^*(M), i^*(M))}{(1-\gamma)M} - (T-t)\frac{e^*(M)^2/2 + i^*(M)}{M}\right). \end{aligned}$$

Solving for $\alpha_{t-1}$ yields:

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

Finally, the above expression can be used to further simplify (15) and achieve (6).

□

*Proof of Lemma 2.* As discussed in the text, the choice of $Q_T$ maximizes the continuation value:

$$U_T(Q_T, A_{T-1} + (M - Q_T)\cdot p_T^* - i_{T-1}),$$

where $p_T^* \in p(Q_T)$ depends on which equilibrium is expected to emerge in period $T$. The important observation is that $Q_T$ determines the assets available in the following period. Therefore, by Lemma 1, the continuation value is strictly convex in $Q_T$ for:

$$\hat{Q} \le Q_T \le Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{p_T},$$

and is linearly increasing in $Q_T$ otherwise, with a downward discontinuity at $M - \frac{i_{T-1}+\bar{i}-A_{T-1}}{p_T}$, given by the minimum number of tokens that the developer needs to sell in order to achieve $\bar{i}$ in period $T$. See Figure 4 for a graphical representation.

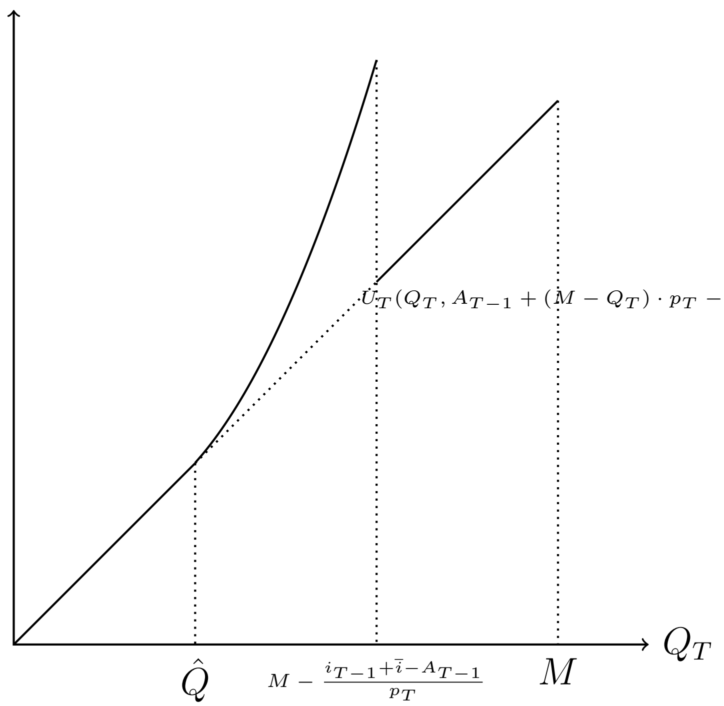



Fig. 4: Continuation value as a function of $Q_T$.

Suppose that the "high" equilibrium is expected to emerge, so that $p_T = \max\{p(Q_T)\}$. The discontinuity is at:

$$\tilde{Q}'_T \equiv Q_T : \frac{\bar{i} + i_{T-1} - A_{T-1}}{M - Q_T} = \frac{V_{T-1} + g(e^*(Q_T))}{(1-\gamma)M},$$

generating a continuation utility:

$$\frac{V_{T-1} + g(e^*(\min\{\tilde{Q}'_T, M\}))}{(1-\gamma)M} M - \frac{1}{2}(e^*(\min\{\tilde{Q}'_T, M\}))^2.$$

If the "low" equilibrium is expected to emerge, then the discontinuity is at:

$$\tilde{Q}''_T = M - \frac{\left(\bar{i} + i_{T-1} - A_{T-1}\right)(1-\gamma)M}{f(e_{T-2}, i_{T-2}) + f(e_{T-1}, i_{T-1})},$$

generating a continuation utility:

$$\frac{V_{T-1} + g(e^*(\min\{\tilde{Q}''_T, M\}))}{(1-\gamma)M} M - \frac{1}{2}(e^*(\min\{\tilde{Q}''_T, M\}))^2.$$

Because period $T$ effort is chosen optimally, it must be that:

$$\frac{g(e^*(\min\{\tilde{Q}'_T, M\}))}{(1-\gamma)M} M \geq \frac{1}{2}(e^*(\min\{\tilde{Q}'_T, M\}))^2,$$

and:

$$\frac{g(e^*(\min\{\tilde{Q}''_T, M\}))}{(1-\gamma)M} M \geq \frac{1}{2}(e^*(\min\{\tilde{Q}''_T, M\}))^2,$$

which implies that the two continuation utilities (the one with threshold $\tilde{Q}'_T$ and the one with threshold $\tilde{Q}''_T$) are greater than the continuation utility when the developer holds $Q_T = M$ and no investment occurs:

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

Hence, holding either $\tilde{Q}'_T$ or $\hat{Q}''_T$ is preferred to holding the entire stock of tokens $M$ and not investing. The continuation utility is therefore maximized at either $\tilde{Q}'_T$ or $\hat{Q}''_T$, depending on what equilibrium is expected to emerge in period $T$. $\square$

*Proof of Lemma 3.* Remember that $Q^*_T$ is the largest possible $Q_T$ such that the period-$T$ constraint is not binding. It follows that, as already discussed, if $Q^*_T \leq \hat{Q}$ then the continuation value is linear in $Q_T$ because there is no $Q_T$ for which the developer will exert effort in period $T$.

If instead $Q^*_T > \hat{Q}$ then the continuation value is somewhere strictly convex in $Q_T$ for $Q_T \leq Q^*_T$. In this case, there is the same anti-coordination problem discussed for the "rich developer" case and the equilibrium is in mixed strategies. The developer must be indifferent between $Q_T = 0$ and $Q^*_T$.

The price at which the developer is indifferent is:

$$p_{T-1} = \frac{U_T(Q^*_T, A_{T-1} + (Q_{T-1} - Q^*_T) \cdot p_{T-1} - i_{T-1})}{Q^*_T} = \frac{Q^*_T \left(\frac{V_{T-1} + g(e^*(Q^*_T, \bar{i})}{(1-\gamma)M}\right) - \frac{1}{2}(e^*(Q^*_T, \bar{i})^2 - \bar{i}}{Q^*_T}.$$

Furthermore, investors must be indifferent between holding tokens in period $T$ and in period $T-1$, which implies that:

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

where $\alpha_{T-1}$ is the probability that the developer sells all his tokens in period $T-1$. Combining the above two expressions and solving for $\alpha_{T-1}$ yield the expression in the proposition.

For existence and (sometimes) uniqueness of the equilibrium, without loss of generality, assume that whenever $Q^* \leq \hat{Q}$ the agent randomizes between $\max\{Q_T^*, M\}$ and 0. In case the developer holds a positive amount of tokens, this amount can be written as a function of $p_{T-1}$:

$$Q(p) \equiv \begin{cases} \min\left\{Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{p}, M\right\} & \text{if } Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{p} > 0 \\ 0 & \text{otherwise.} \end{cases}$$

The above expression is increasing whenever $A_{T-1} - i_{T-1} \leq \bar{i}$ (that is, when the developer needs to sell some tokens in period $T-1$ to invest $i_T = \bar{i}$), and is decreasing otherwise.

Similarly, call $p(Q)$ the equilibrium $p_{T-1}$ as a function of the number of tokens held by the developer in case he holds a positive number of tokens. I distinguish between two cases. Whenever $A_{T-1} - i_{T-1} < \bar{i}$ (that is, whenever the developer needs to sell some tokens in period $T-1$ to invest $i_T = \bar{i}$), we have:

$$p(Q) \equiv \frac{V_{T-1}}{(1-\gamma)M} + \begin{cases} 0 & \text{if either } Q \leq \hat{Q} \text{ or } Q > Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{\frac{V_{T-1}}{(1-\gamma)M}} \\ \frac{(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} & \text{if } \hat{Q} \leq Q \leq Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{\frac{V_{T-1}+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}}, \end{cases}$$

where:

$$\alpha(Q) \equiv \left(\frac{1}{2}(e^*(Q, i^*(Q, A_T)))^2 + i^*(Q, A_T)\right)\left(Q \cdot \frac{g(e^*(Q, i^*(Q, A_T)))}{(1-\gamma)M}\right)^{-1}.$$

Because:

$$Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{\frac{V_{T-1}}{(1-\gamma)M}} < Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{\frac{V_{T-1}+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}},$$

for all $Q$, the case $A_{T-1} - i_{T-1} < \bar{i}$ can be split into three subcases:

1. Whenever $Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{\frac{V_{T-1}}{(1-\gamma)M}} > \hat{Q}$ then for some $Q$ we have:

   $$p(Q) = \left\{ \frac{V_{T-1}}{(1-\gamma)M}, \frac{V_{T-1} + (1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} \right\}.$$

   That is, there are situations in which for given $Q_T^*$, if $p_{T-1}$ is low the developer will not have enough funds to finance investment in period $T$, and therefore no development will occur. If instead $p_{T-1}$ is high, there is a positive probability that the developer will invest and exert effort in period $T$. Again, this situation can be seen as a coordination problem among investors. For given action taken by the developer in period $T-1$, investors can coordinate on a "high" equilibrium that leads to effort and investment in period $T$ with positive probability, or a "low" equilibrium leading to no development in period $T$.

2. Whenever $Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{\frac{V_{T-1}+(1-\alpha(M))g(e^*(M))}{(1-\gamma)M}} \leq \hat{Q}$, then there is no development in period $T$ and $p(Q) = \frac{V_{T-1}}{(1-\gamma)M}$ for all $Q$.

3. In all other cases, $p(Q)$ is a function, which is equal to $\frac{V_{T-1}}{(1-\gamma)M}$ for $Q \leq \hat{Q}$ and to $\frac{V_{T-1}+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}$ otherwise. This function is continuous because, by definition of $\hat{Q}$, we have $e^*(Q,\bar{i})) = 0$.

Instead, whenever $A_{T-1} - i_{T-1} \geq \bar{i}$ (that is, whenever the developer has enough own funds to invest $i_T = \bar{i}$), then period $T$ investment does not depend on $p_{T-1}$ and therefore:

$$p(Q) \equiv \frac{V_{T-1}}{(1-\gamma)M} + \begin{cases} 0 & \text{if either } Q \leq \hat{Q} \\ \frac{(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} & \text{otherwise,} \end{cases}$$

which is a continuous function.

An important observation is that $p(Q)$ is strictly increasing whenever $Q$ is such that positive development is expected with some probability in period $T$, and is constant otherwise. To see this, use the definition of $\alpha(Q)$ to write:

$$Q \cdot \frac{g(e^*(Q,\bar{i}))}{(1-\gamma)M} - \frac{1}{2}(e^*(Q,\bar{i}))^2 - \bar{i} = (1-\alpha(Q))Q \cdot \frac{g(e^*(Q,\bar{i}))}{(1-\gamma)M}. \tag{16}$$

The LHS of (16) is equal to:

$$\max_e \left\{ Q \cdot \frac{g(e,\bar{i})}{(1-\gamma)M} - \frac{1}{2}e^2 \right\},$$

which is strictly increasing and strictly convex in $Q$. It follows that the RHS of (16) must also be strictly increasing and strictly convex in $Q$. This, in turn, implies that $p(Q)$ is strictly increasing whenever $Q$ is such that positive development is expected with some probability in period $T$, and is constant otherwise.

The equilibrium of the game is a $p^*$ such that $p^* = p(Q(p^*))$ and a $Q^* = Q(p^*)$. Figure 5 represents all possible cases. Whenever both $p(Q)$ and $Q(p)$ are continuous functions (when $A_{T-1} - i_{T-1} \geq \bar{i}$, and when $A_{T-1} - i_{T-1} < \bar{i}$ cases 2 and 3), the existence of the equilibrium is readily established. It is enough to note that the range of $p(Q)$ is a closed interval. Call this interval $[a, b]$. The equilibrium is the fixed point of the continuous function $p(Q(p))$ defined over $[a, b]$. Brower's fixed point theorem applies and the fixed point exists.

Whenever $p(Q)$ is a correspondence ($A_{T-1} - i_{T-1} < \bar{i}$, case 1) we know that for $\hat{Q} \leq Q \leq Q_{T-1} - \frac{i_{T-1}+\bar{i}-A_{T-1}}{\frac{V_{T-1}+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}}$ we have that $\frac{V_{T-1}+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} \in p(Q)$. Define the threshold value of $Q$:

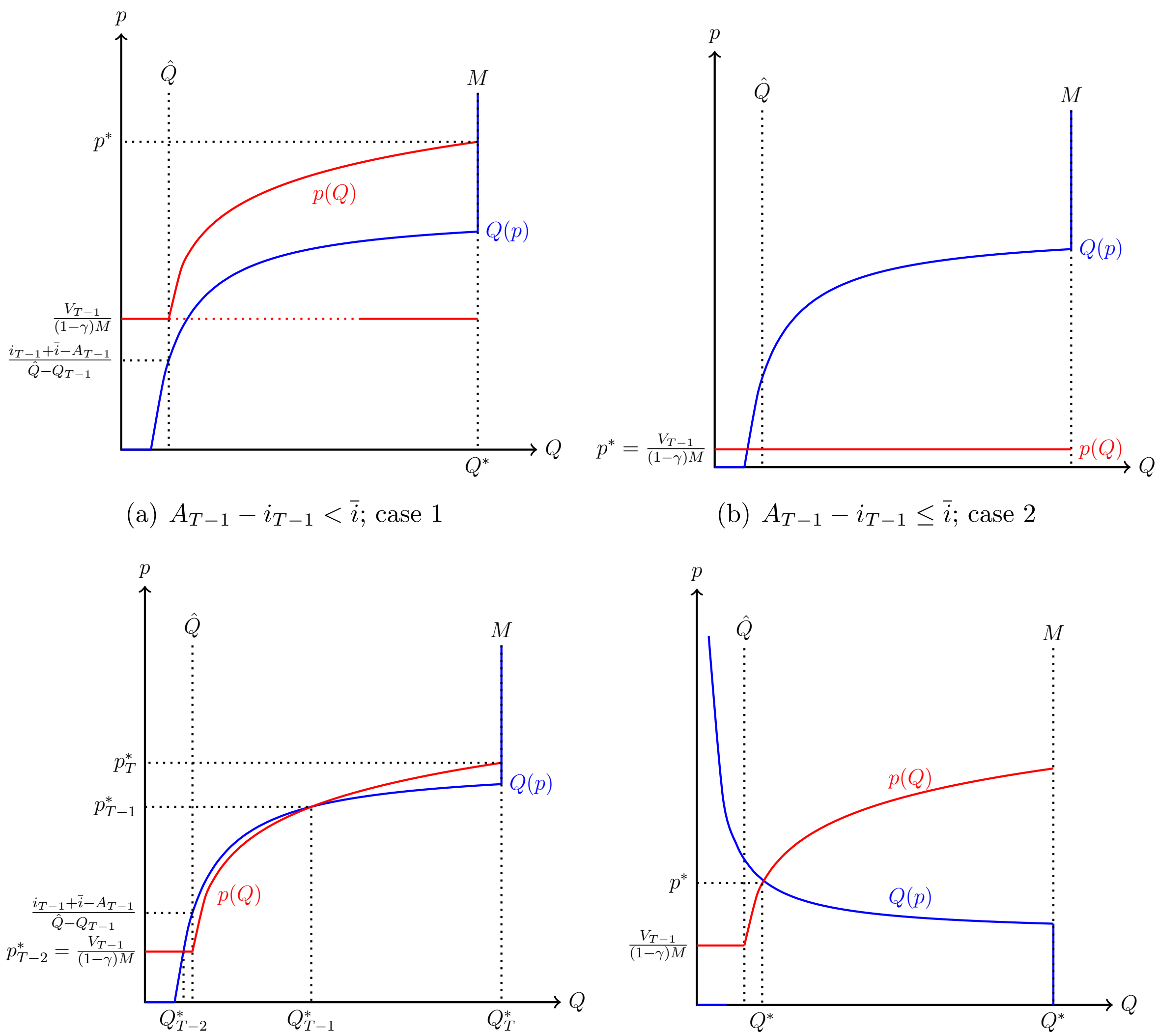
$$\tilde{Q} \equiv Q_{T-1} - \frac{i_{T-1} + \bar{i} - A_{T-1}}{\frac{V_{T-1}+(1-\alpha(\tilde{Q}))g(e^*(\tilde{Q},\bar{i}))}{(1-\gamma)M}},$$

and similarly the corresponding price:

$$\tilde{p} \equiv \frac{V_{T-1} + (1-\alpha(\tilde{Q}))g(e^*(\tilde{Q},\bar{i}))}{(1-\gamma)M} \in p(Q).$$

By definition of $Q(p)$ we have that $\tilde{Q} = Q(\tilde{p})$, which implies that $\{\tilde{Q}, \tilde{p}\}$ is an equilibrium.

As already discussed $p(Q)$ is weakly increasing. In case $A_{T-1} - i_{T-1} \geq \bar{i}$, $Q(p)$ is strictly decreasing, and the equilibrium is unique. The equilibrium is unique also when $A_{T-1} - i_{T-1} < \bar{i}$ case 2, because $p(Q)$ is constant and $Q(p)$ is increasing. In all other cases multiple equilibria are possible.




(a) $A_{T-1} - i_{T-1} < \bar{i}$; case 1

(b) $A_{T-1} - i_{T-1} \leq \bar{i}$; case 2

(c) $A_{T-1} - i_{T-1} \leq \bar{i}$; case 3

(d) $A_{T-1} - i_{T-1} > \bar{i}$

Fig. 5: Equilibrium in $T - 1$

$\square$

## References

Acharya, V. V. and A. Bisin (2009). Managerial hedging, equity ownership, and firm value. *The RAND Journal of Economics 40*(1), 47–77.

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*.

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 (2018). The blockchain folk theorem. *working paper*.

Bisin, A., P. Gottardi, and A. Rampini (2008). Managerial hedging and portfolio monitoring. *Journal of the European Economic Association 6*(1), 158–209.

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

Catalini, C. and J. S. Gans (2016, December). 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. Working Paper 24418, National Bureau of Economic Research.

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

Diamond, D. W. and R. E. Verrecchia (1982). Optimal managerial contracts and equilibrium security prices. *The Journal of Finance 37*(2), 275–287.

Diemers, D., H. Arslanian, G. McNamara, G. Dobrauz, and L. Wohlgemuth (2018). Initial coin offerings: A strategic perspective. *Strategy &*

*PwC*. Available at https://cryptovalley.swiss/wp-content/uploads/20180628_PwC-S-CVA-ICO-Report_EN.pdf.

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

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

Hafner, K. and M. Lyon (1998). *Where wizards stay up late: The origins of the Internet*. Simon and Schuster.

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

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

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). Initial coin offering and platform building. *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.

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

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

Schilling, L. and H. Uhlig (2018, April). Some simple bitcoin economics. Working Paper 24483, National Bureau of Economic Research.

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