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 †

Preliminary, please check here for the latest version. This version: March 19, 2018.

Abstract

Unlike traditional open-source projects, developers of open-source blockchain-based projects can reap large financial rewards thanks to a modern form of *seignorage*. I study to what extent this novel form of financing generates incentives to innovate. I consider a developer working on an open-source blockchain-based protocol that can be used only in conjunction with a protocol-specific crypto-token. This token is first sold to investors via an auction (the ICO phase) and then traded on a frictionless financial market. I establish that seignorage is effective at providing capital and at generating incentives to develop the protocol. Its effectiveness is however limited by the fact that, in all equilibria of the game, in each post-ICO period there is a positive probability that the developer sells all his tokens and, as a consequence, no development occurs.

JEL classification: D25, O31, L17, L22, L26, E42, E51,

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

1 Introduction

This paper studies a new mechanism for the financing of software development: seignorage. Seignorage allows the developer of a blockchain-based open-source software to rip a direct financial benefit (in addition to indirect benefits derived from,

*I'm are grateful to Ennio Bilancini, Antonio Fatas, Massimo Riccaboni, the participants to the INSEAD research symposium, IMT brownbag seminar, for their comments and suggestions.

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

for example, career concerns)[1] via the creation of a token that must be used in conjunction with the software.

Historically, seigniorage are profits earned by a government by issuing a currency. As the economic activity within a country increases, the value of the currency used in this country also increases, and with it the profit earned by the government issuing this currency. The same mechanism allows developers of open-source blockchain-based projects to benefit from their work. As an illustration, consider a population of agents who wishes to transact but are prevented from doing so for lack of the required infrastructure. For example, these agents may want to exchange a physical good, but there may be no legal system, no agreed upon units of measurement, no security. Alternatively, the exchange may be between computers, in which case the technical specifications governing the communication between machines may be missing. An entrepreneur may decide to invest resources and create this missing infrastructure, and, with it, a market. One way to profit from this investment is to create a *token*, and establish that all exchanges occurring within the market must use this token. All prices within the market can be expressed in fiat currency (that is, in some numeraire), but must be paid using the token. The entrepreneur owns the initial stock of tokens and can credibly commit to limit their supply. It follows that if the market is successful, there will be a positive demand for these tokens, a positive price for tokens, and positive profits earned by the entrepreneur.

The way blockchain allows for the creation of this infrastructure and the ability of the entrepreneur to extract profits is threefold (see Section 1 for some details of how blockchain works). First, blockchain technology can be used to create the infrastructure and therefore the marketplace.[2] Second, the rules determining whether

[1] On the motivation of contributors to open source projects, see the seminal work by Lerner and Tirole (2002).

[2] It may appear that not all blockchain projects have this "marketplace" element. For example, the existence of "two sides who want to transact" is not immediately evident when considering the Bitcoin protocol. However, also in this case there are two sides: people who need to exchange bitcoins, and those who use their computers to process these transactions also called miners. Users of bitcoins "pay" the miners 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 new bitcoins for their work. Because of its effect on the price, this increase in the supply of bitcoins amounts to a transfers from the holders of bitcoins to the miners. See also Huberman, Leshno, and Moallemi (2017). The case of Bitcoin also illustrates another point: that the mechanism by which one side of the market rewards the other may not be a market-clearing price. This aspect, however, will not be relevant here.

(and how) the supply of tokens increases over time can be fully specified initially and cannot be manipulated afterward. That is, using blockchain technology the entrepreneurs can commit to a specific supply of tokens. Finally, the fact that a given token is necessary to transact is also specified within the protocol. That is, it is not possible to use the same protocol with a different token.[3]

This paper studies theoretically seignorage as a form of financing for open-source software, both in its ability to generate incentives for innovation beyond those already discussed in the literature on open source software, and in its ability to provide capital to be invested in the development of the software. I build a model in which, in every period, a developer exerts effort and invests in the development of a software. Initially, the developer owns the entire stock of tokens, and can sell some to investors via an auction (also called Initial Coin Offering—ICO). Subsequently, in every period he can sell or buy tokens on a frictionless market for tokens, in which both users of the software and investors are active. The developer can use the proceedings of the sale of tokens to either invest in the development of the software or to consume.

The main insight 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 his tokens, which allows him to "cash in" on the future development without doing any. On the other hand, if investors expect no development to occur, the price of the token will be low. The developer should hold on 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 his tokens (and therefore stop 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 supply of tokens sold

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

by the developer is announced initially. Because the incentives to exert effort and invest in the development of the software increase with the share of tokens held by the developer, investors can anticipate the amount of development that will occur in the period following the ICO, which will be reflected in the price of the token at ICO.

In addition, both at ICO and post-ICO there may be a coordination problem. Because of a cash constraint, in every period the developer cannot invest in the development of the software more than his assets. It follows that the developer may sell some of his tokens, as a way to accumulate assets and finance the future development of the software. 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 few 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 many 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.[4]

When choosing whether and when to hold an ICO the developer is therefore facing a tradeoff. If he holds an ICO, in all subsequent periods he may sell all his tokens and therefore 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 his tokens for sure and set the corresponding level of effort and investment. On the other hand, if the developer does not sell tokens at ICO he may lack the funds to invest efficiently 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 as soon as his own funds are not sufficient to achieve the efficient level of investment.

[4] Clearly, if there are network effects, then there is an additional coordination problem: for 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 "low adoption" equilibria. The novelty here is that fixing one of the adoption equilibria, there are multiple equilibrium sequence of effort and investment arising from a coordination problem between investors and the developer.

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). With this respect, I show that open source—with its organizational structure and ethos—can coexist with strong financial incentives. Of course, an open question that I do not address here is whether financial rewards will crowd out other motives (see, for example, Benabou and Tirole, 2003), that is, whether the open source ethos will be compromised by the introduction of strong financial incentives.

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

There is a small but growing literature studying specific blockchain-based projects, mostly bitcoin and its blockchain (see, for example Athey, Parashkevov, Sarukkai, and Xia, 2017, Huberman, Leshno, and Moallemi, 2017, Dimitri, 2017, Biais, Bisiere, Bouvard, and Casamatta, 2018, Prat and Walter, 2018, Ma, Gans, and Tourky, 2018). Catalini and Gans (2016) discusses the broader economic implications of blockchain (that is, beyond specific projects). These papers do not discuss seignorage as a way to finance blockchain-based projects.

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 I'm considering here is however different from the one considered in these papers, because a token is a currency that may be used in the

[5] 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).

future and hence acquire value. That is, there is no contract between the issuer of the currency (the developer) and those holding the currency (the investors).

The remainder of the paper is organized as follows. Because seignorage as a mechanism for financing innovation is specific to blockchain-based projects, the next section provides some background on blockchain. Section 3 presents a model of seignorage, which is solved in Section 4. Section 5 discusses some extensions to the model. Section 6 concludes. Unless otherwise noted, all proofs and mathematical derivations missing from the text are in appendix.

2 Blockchain

Blockchain is better understood in relation to Internet. The *Internet protocol suite* (commonly known as TCP/IP) was developed in the late '60 and early '70 to allow for the decentralized *transmission* of data, that is, transmission of data via a network of computers in which no node is, individually, essential to the well functioning of the network. It is the technological foundation of a second set of protocols (also called *application layer protocols*) handling specific types of data: HTTP for accessing web pages; SMTP, POP, and IMAP for sending and receiving emails; FTP for sending receiving files; and so on.

Blockchain is a recent innovation that further expands the operations that can be performed by a network of computers. It is a protocol that allows for the decentralized transmission of data (as does the Internet protocol suite), as well as for the decentralized *storage, verification, manipulation* of data.[6] Similarly to the way the Internet protocol suite is the foundation of a number of application-layer protocols, blockchain is the technological foundation of a number of application-layer protocols. The most well-known is the Bitcoin protocol: a protocol allowing a network of computers to store data (how many Bitcoin each address owns) and to enforce specific rules regarding how these data can be manipulated (no double spending). Numerous other blockchain-based protocols currently exist or are being actively developed. For example, protocols for building applications that can run on a decentralized network

[6] Sometimes a distinction is made between blockchain and *decentralized ledger technologies*, where blockchain refers to a specific way to maintain 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.

(rather than on a specific computer, see Ethereum, Tezor, Ardor, NTX); protocols for decentralized real-time gross settlement (see Ripple, Stellar); protocols enabling the creation of decentralized marketplace for storage and hosting of files (see SIA, Filecoin, Storj) and for renting in/out CPU cycles (see Golem, Gridcoin); protocols creating fully decentralized prediction markets (see Augur, Gnosis, Stox), financial exchanges (see 0xproject), and financial derivatives (see MakerDAO); and many more.

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 opensource, 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 and are based on open collaboration (as typical of open source projects). They do not receive immediate, direct financial compensation for their contributions, and are motivated by career concerns (i.e. increase their reputation and reap a financial benefit in the future) and by non-monetary considerations (i.e. the pleasure of sharing, collaborating, contributing to a public good). Instead, as already discussed in the introduction, the development of blockchain-based protocols can leverage financial incentives via seignorage. The remainder of the paper studies the effectiveness of seignorage in generating incentives for innovation.

3 The model

The economy is composed of a developer, a large mass of risk-neutral price-taking investors, and a large mass of users. At the beginning of every period $t \geq 1$, the developer exerts effort e_t and invests i_t into the development of a Blockchain-based protocol. At the end of every period the developer consumes $c_t \geq 0$. The sequence of investment and effort determines the *value of the protocol* in each period t:

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

representing the total monetary value of the transactions made using the protocol during a given period. The function $f(.,.)$ 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. All transactions that use the protocol

must be conducted using a specific token, with total supply M, fully owned by the developer at the beginning of the game.

Note that, although quite general, the above specification 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 given sequence of effort and investment there are 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.[7]

Timeline. The development of the protocol lasts T periods, after which the developer exists the game and the protocol continues being used indefinitely. In period $t_o \leq T$, the developer sells some tokens to investors via an auction. I call this stage the ICO (Initial Coin Offering) stage, and I assume that its date t_o is chosen by the developer.[8] In each period $t \in \{t_o + 1, ..., T\}$, first the developer exerts effort and invests, and then a frictionless market for tokens opens. In period $t = T$, after the developer exerts effort and invests, and after the market for tokens has open, users can use the protocol. At the end of period T the developer exists the game. In every subsequent period (that is, in every $t > T$), first the market for tokens opens, and then users use the protocol. See Figure 1 for a graphical representation of the timeline.

Investors. Investors are risk-neutral profit maximizers with no cash constraints. They can purchase tokens in every period and sell them during any subsequence 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's prices from period t onward, which they take as given. Because they do not discount

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

[8] The important element of an auction is that the number of tokens sold is fixed initially by the auctioneer and the price is determined endogenously via the investors' bid. In practice, however, not all ICOs follow this format. See, for example, the practice of holding *uncapped ICOs* in which the token's price is fixed and the number of tokens sold initially is determined in equilibrium. The results derived in this paper do not extend to these types of ICOs.

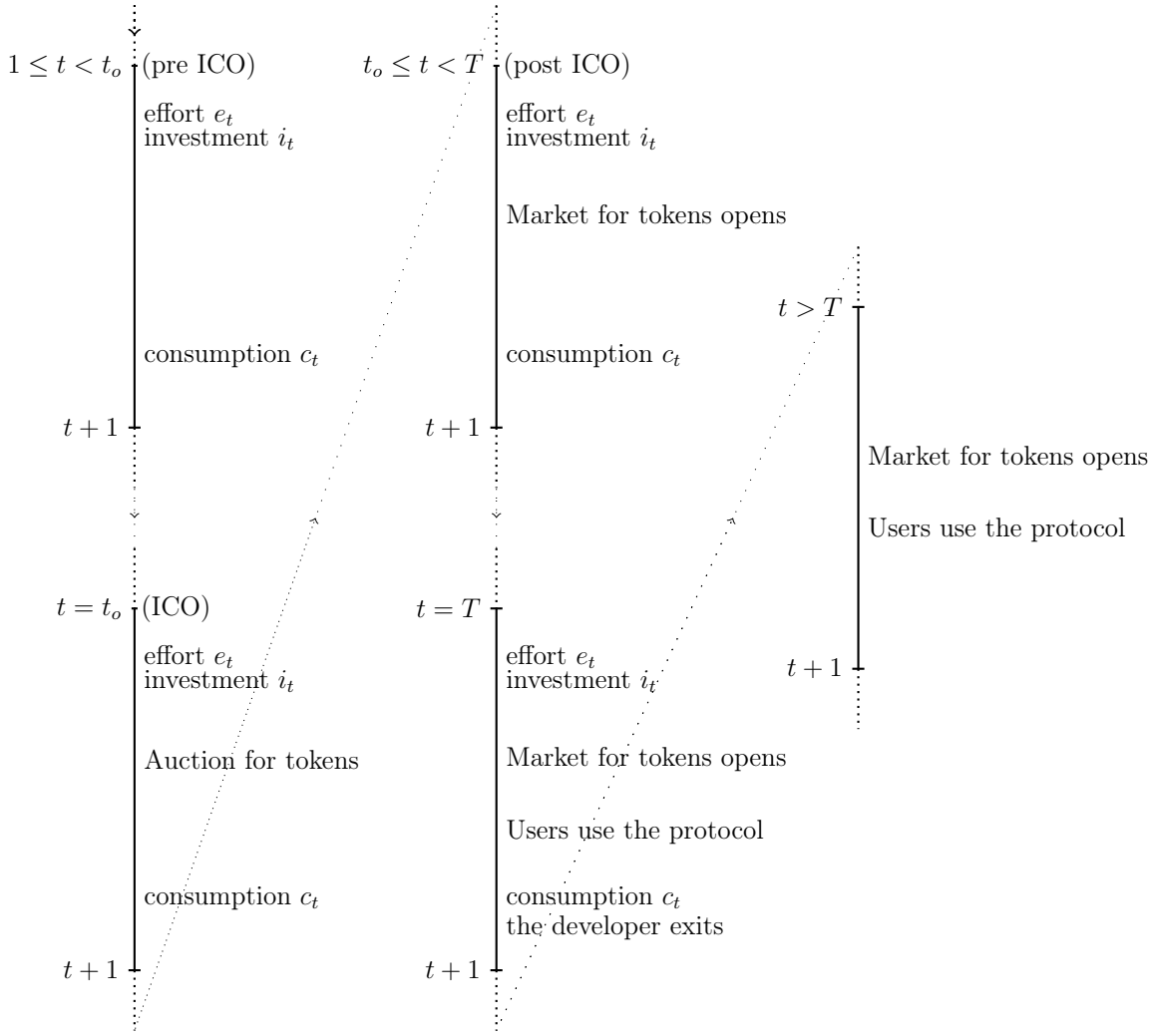


Fig. 1: Timeline

the future, investors 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.[9] Finally, if $p_t < \bar{p}$ then the investors' demand for token in period t is not

[9] I'm therefore abstracting away from short-selling. This is without loss of generality. The reason is that to short sell, an investor should borrow a token, sell it, and then return it to the owner in a later period. As I discuss in the next paragraph, users are prevented by assumption from deciding intertemporarily when they want to use the token, and hence cannot lend tokens. Furthermore, if the price is expected to drop, neither the developer nor other other investors will want to lend tokens, preferring instead to sell them when the price is high.

defined.

Users. In every period $t \geq T$ users use the protocol to exchange goods and services of value V_t. Given the assumed timing, 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 have a supply of tokens in period $t+1$ equal to $\frac{V_t}{p_t}$. The mass of users on the selling and buying side of the protocol are assumed constant.[10]

The developer. Call $Q_t \leq M$ the stock of tokens held by the developer at the beginning of period t, with $Q_0 = M$. Call

$$A_t \equiv a + \sum_{s=0}^{t-1} \left[(Q_s - Q_{s+1}) \cdot p_s - i_s \right] = A_{t-1} - i_{t-1} + p_{t-1}(Q_{t-1} - Q_t)$$

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

In period t, the developer's optimization problem is:

$$U_t(Q_t, A_t) \equiv \max_{\{Q_{t+1},\ldots\},\{e_t,e_{t+1},\ldots\},\{i_t,i_{t+1},\ldots\}} \left\{ \sum_{s=t}^{T} \left(c_s - \frac{1}{2} e_s^2 \right) \right\}$$

subject to the budget constraint:

$$c_t = A_t + (Q_t - Q_{t+1}) \cdot p_t - i_t \geq 0,$$

a feasibility constraint determining the largest investment that can be made:

$$i_t \leq A_t,$$

[10] It is important to point out that the same person could purchase tokens both to buy/sell using the protocol, and as investment. The important element is that the demand for tokens can be decomposed into two motives (i.e. usage and investment); the fact that each of this motive originates from a distinct type of agents is for ease of exposition.

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

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

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

4 Solution

4.1 Periods $t \geq T$.

In this section I show that, given the set up of the model and an appropriate equilibrium selection criterion (which I introduce 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 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 happen from period T onward (for example, regarding the demand and supply of tokens by users or by investors), provided that under these different assumptions p_T is increasing in V_T.

The presence of the 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, here I am interested 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 token must solve:[11]

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

The important observation here 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.

4.2 The developer's problem.

The fact that the price of the token in period T is increasing in the sequence of effort and investments made by the developer generates the following tension. Investors are forward looking and are willing to purchase tokens in period $t < T$ at the same price that is expected in period T. But if the developer's future effort is already priced into todays' price, the developer may be better off by selling all his tokens—that is, to benefit from his future effort and investment before exerting any. This section shows that, as a consequence of this tension, the game has mixed strategy equilibria in which, in every period with some probability the developer sells all his tokens.

Because investors are price takers, their demand in period t depends 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.[12] The equilibrium sequence of prices starting from period t should, however, reflect effort and investments made prior to t, as well as the

[11] This expression is an application of the equation of exchange, usually employed to link a country's price level, real GDP, money supply and velocity of money. The simplification is that, in the application of this equation, I implicitly assume a velocity equal to 1: cash can be exchanged with the token only once in every period. Of course, if cash can be exchanged for tokens multiple times during a period, the same token can be used multiple times within the same period, which affects the way in which the stock of tokens maps into the price of tokens for given V_T. This would introduce an additional parameter that is, however, inconsequential with respect to subsequent derivations, and hence is omitted for ease of notation.

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

equilibrium sequence of future effort and investments. Hence, the investors' demand for tokens from period $t+1$ onward depends on the supply of tokens by the developer in period t, which determines the stock of tokens held by the developer from period $t+1$ onward, and his optimal future effort and investment. To say it differently, 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 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 distinguishing 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.

4.2.1 Rich developer.

If the cash constraint is never binding, the developer's problem can be written as

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

for $t \leq T-1$ and

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

Note that $(Q_t - Q_{t+1}) \cdot p_t - i_t$ is the cash generated in period t, net of investment. Without loss of generality, we can think of this cash as being consumed in period T. However, because it depends on actions taken in period t, it is included in period t's utility function.

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 the 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[13]

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

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

As long as either $e^*(Q_T)$ or $i^*(Q_T)$ are positive for some $Q_T \leq M$ (an assumption I maintain 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 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 his tokens (when p_{T-1} is high), or 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 at the beginning of period T.

Note, however, that if investors expect the developer to sell all 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. We therefore 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 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

[13] 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. They however may not be unique. In what follows, for ease of exposition I will implicitly assume that they are indeed unique, although none of the results depend on this assumption.

purchasing in period T or period $T-1$, it must be that

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

where α_{T-1} is the probability that the developer sells all 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 $M \cdot \frac{f(e^*(M),i^*(M))}{(1-\gamma)M}$ 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. The term $(e^*(M))^2/2 + i^*(M)$ is instead the cost generated by holding M tokens, coming from the additional effort and investment that the developer will exert in period T. Because effort and investment are chosen optimally, the benefit should be at least as large as the cost, we have that $\alpha_{T-1} \leq 1$.

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

Proposition 1 (Equilibrium for $t_o < t \leq T$)**.** *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*

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

   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 his tokens and selling all his tokens. But this also

implies that the agent is indifferent between selling all 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 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 characterize by the fact that tokens are sold via an auction. Hence, contrarily to all subsequent periods, in period t_o the price of 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

$$\begin{aligned}
&\max_{Q_{t_o+1}} \left\{ \tilde{U}_{t_o+1}(Q_{t_o+1}) + (M - Q_{t_o+1})p_{t_o} \right\} = \\
&\max_{Q_{t_o+1}} \left\{ \max_{e_{t_o+1}, i_{t_o+1}} \left\{ Q_{t_o+1} \cdot p_{t_o+1} - \frac{1}{2}e_{t_o+1}^2 - i_{t_o+1} \right\} + (M - Q_{t_o+1})p_{t_o+1} \right\} \leq \\
&\max_{Q_{t_o+1}} \left\{ \max_{e_{t_o+1}, i_{t_o+1}} \left\{ Q_{t_o+1} \cdot p_{t_o+1} - \frac{1}{2}e_{t_o+1}^2 - i_{t_o+1} + (M - Q_1)p_{t_o+1} \right\} \right\} \equiv \tilde{Q}_1(M)
\end{aligned}$$

where the first equality follows from writing $\tilde{U}_{t_o+1}(Q_{t_o+1})$ explicitly (under the assumption that the developer sells all his tokens in period 1). It follows that the

choice of how many tokens to sell at ICO only depends on 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 his tokens during the ICO, and then exists 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 token at ICO. It follows that $Q_{t_o+1} = M$ with probability 1. Effort and investment in all t_o are $e^*(M)$ and $i^*(M)$ with probability 1. If instead the ICO occurs at period T, then the developer sells all his tokens at ICO.*

Proof. In the text. □

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

It is immediate to check that optimal effort and investment between period 1 and t_{o+1} are, again, $e^*(M)$ 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 all his tokens 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 he will sell M tokens on the market in period T. If instead the ICO is in period T the developer sells all 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 token before period T and sells all his tokens in period T. As a consequence effort and investment are at their optimal level $e^*(M)$ 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 M. From (2) and (3) we know that the equilibrium sequence of investment and effort is also independent from M. By proposition 1, in every post-ICO period the value of all outstanding tokens $p_t M$ is independent from M. The developer's utility is therefore independent from M.

4.2.2 Poor developer

Suppose now that that $a < T \cdot i^*(M)$: the developer cannot invest efficiently in all periods, and the cash constraint could be binding. The developer's utility function can be rewritten in recursive form. For $t < T$:[14]

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

and for $t = T$:

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

where λ_t is the Lagrange multiplier associated with the period-t cash constraint.

I make two simplifying assumptions. The first one is that the developer is active only for three periods, that is $T = 3$.[15] Furthermore, to focus on the role of the cash constraint, I assume 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.

[14] Without loss of generality, I write the problem assuming that consumption occurs exclusively in period T.

[15] See Section 5.1 for a discussion of the case $T > 3$.

Given this, period-T effort and investment are[16]

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

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

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

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

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. □

I proceed by first solving the game for given t_o, that is, by assuming that the ICO occurs in period $T = 3$, $T - 1 = 2$ or $T - 2 = 1$. I then derive the optimal t_o.

[16] Again, I do not index optimal effort by T because I will show later that this function is time invariant. Optimal investment will, instead, depend on t so I maintain the time index.

Case 1: $t_o = 3$. If the ICO occurs in period 3, then optimal effort and investment in period $T = 3$ are $\{e^*(M), \bar{i}\}$ whenever $\bar{i} < A_3$ and $\{0, 0\}$ otherwise. The price of token is therefore:

$$\frac{f(e_1, i_1) + f(e_2, i_2)}{(1-\gamma)M} + \begin{cases} 0 & \text{if } A_3 < \bar{i} \\ \frac{g(e^*(M))}{(1-\gamma)M} & \text{otherwise} \end{cases}$$

In period 2, the choice of optimal investment affects A_3 and the period-3 optimal effort and investment. This is relevant whenever $\bar{i} \leq A_2 < 2\bar{i}$, that is, whenever period-2 assets are not sufficient to invest optimally both periods 2 and 3. It is quite immediate to see that, in this case, the final price is always $\frac{f(e_1,i_1)+g(e^*(M)}{(1-\gamma)M}$, independently from whether effort and investment are positive in period 2 or 3. The same logic applies to the choice of period-1 investment and effort: whenever $a < 3\bar{i}$, the developer will invest and exert positive effort only in some periods, but he is indifferent with respect to which ones.

Lemma 2. *Whenever $t_o = 3$, the final value of the protocol is $V_3 = n \cdot e^*(M)$, where $n \equiv argmax_{k \leq 3}\{k \cdot \bar{i} \leq a\}$.*

Proof. In the text. □

Case 2: $t_o = 2$. If the ICO occurs in period 2, then the developer can finance some of its period 3 investment by selling tokens in period 2. Remember that, in equilibrium, the price of tokens at ICO p_2 must be equal to p_3. Hence, for given $M - Q_3$ (i.e., tokens sold at ICO) the price for tokens will be

$$p_3 = \frac{f(e_1, i_1) + f(e_2, i_2)}{(1-\gamma)M} + \begin{cases} 0 & \text{if } A_2 - i_2 + p_3(M - Q_3) < \bar{i} \\ \frac{g(e^*(M))}{(1-\gamma)M} & \text{otherwise} \end{cases} \tag{9}$$

Whenever $A_2 - i_2 < \bar{i}$ (that is, whenever the developer does not have enough own funds to finance period-3 investment), both LHS and RHS of (9) depend on p_3, and therefore for given Q_3 there are multiple equilibrium p_3. For intuition, suppose that the developer announces the sale of $M - Q_3$ tokens at ICO. If investors expect p_3 to be low, they will drive down p_2 (the price at ICO), which implies that the level of investment achievable in period 3 by selling $M - Q_3$ at ICO may be below $\bar{i}$, which justifies the initial expectation. If instead investors expect p_3 to be high, in equilibrium p_2 will also be high, which implies that the level of investment achievable

in period 3 by selling $M-Q_3$ tokens at ICO may be above $\bar{i}$, which justifies the initial expectation. This can be interpreted as a coordination problem among investors. For given action taken by the developer in period 2, investors may coordinate on a "high" equilibrium that leads to high effort and investment in period 3, or on a "low" equilibrium leading to "low" (or no) development in period 3. Call $p(Q_3)$ the correspondence mapping Q_3 to the equilibrium p_3. We therefore have:

$$p(Q_3) = \begin{cases} \frac{f(e_1,i_1)+f(e_2,i_2)}{(1-\gamma)M} & \text{if } \frac{\bar{i}+i_2-A_2}{M-Q_3} < \frac{f(e_1,i_1)+f(e_2,i_2)+g(e^*(Q_3))}{(1-\gamma)M} \\ \frac{f(e_1,i_1)+f(e_2,i_2)+g(e^*(Q_3))}{(1-\gamma)M} & \text{if } \frac{\bar{i}+i_2-A_2}{M-Q_3} > \frac{f(e_1,i_1)+f(e_2,i_2)}{(1-\gamma)M} \\ \left\{ \frac{f(e_1,i_1)+f(e_2,i_2)}{(1-\gamma)M}, \frac{f(e_1,i_1)+f(e_2,i_2)+g(e^*(Q_3))}{(1-\gamma)M} \right\} & \text{otherwise} \end{cases}$$

Figure 2 plots $p(Q_3)$. Note that, even if investors can coordinate on one of the

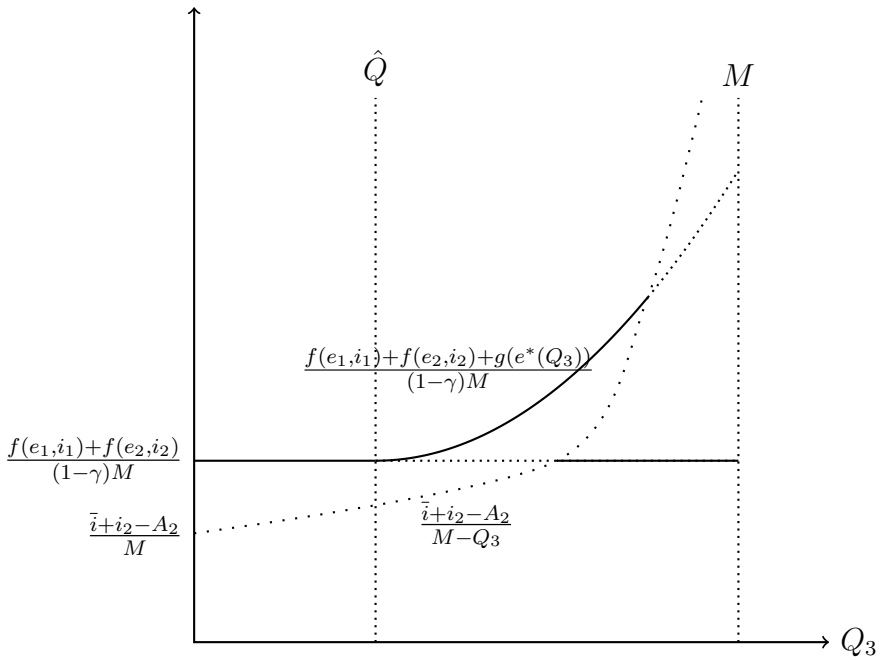


Fig. 2: $p(Q_3)$ whenever $\bar{i} + i_2 > A_2$.

two equilibria so $p(Q_3)$ is a function, this function would be discontinuous and non monotonic.

The choice of Q_3 maximizes the continuation value:

$$U_3(Q_3, A_2 + (M - Q_3) \cdot p(Q_3) - i_2)$$

The important observation is that Q_3 determines the assets available in the following period. Therefore, by Lemma 1, the continuation value

$$U_3(Q_3, A_2 + (M - Q_3) \cdot p(Q_3) - i_2)$$

is strictly convex in Q_3 only for

$$\hat{Q} \leq Q_3 \leq Q_2 - \frac{i_2 + \bar{i} - A_2}{p(Q_3)}$$

and is linearly increasing in Q_3 otherwise, with a downward discontinuity at $M - \frac{i_2+\bar{i}-A_2}{p(Q_3)}$, given by the minimum number of tokens that the developer needs to sell in order to achieve $\bar{i}$ in period 3. Of course, because $p(Q_3)$ is a correspondence, the point of discontinuity of the continuation value depends on which equilibrium is expected to emerge. See Figure 3 for a graphical representation.

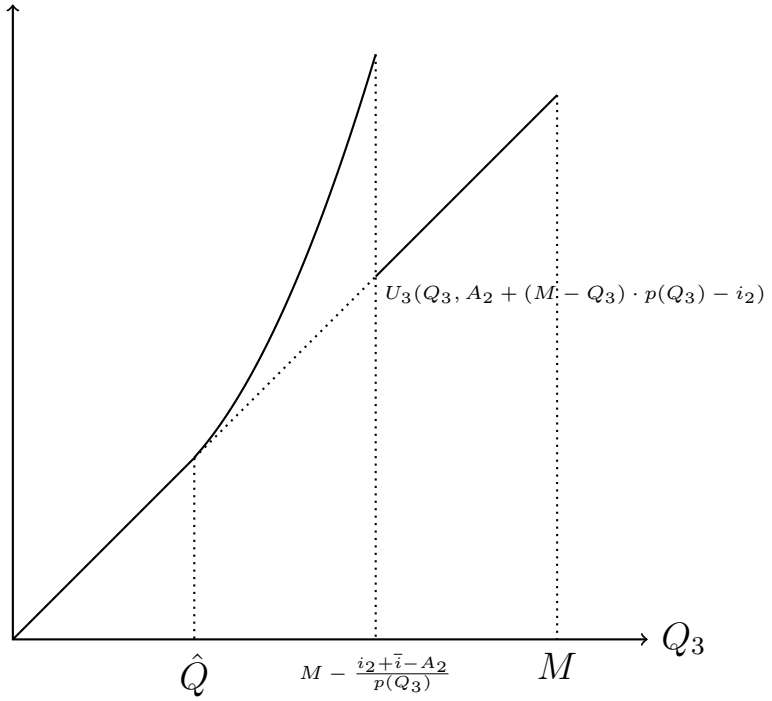


Fig. 3: Continuation value as a function of Q_3.

Lemma 3. *Define*

$$Q_3^* = M - \frac{\max\{i_2 + \bar{i} - A_2, 0\}}{p(Q_3^*)} \tag{10}$$

as the largest Q_3 such that the developer can invest $\bar{i}$ in period 3. If $Q_3^* > \hat{Q}$ the developer chooses $Q_3 = Q_3^*$; there are positive investment and effort in period 3. If instead $Q_3^* \leq \hat{Q}$ then the developer is indifferent between any Q_3; there are no investment nor effort in period 3. When $A_2 - i_2 < \bar{i}$ multiple equilibria are possible and Q_3^* may not be unique. When $A_2 - i_2 \geq \bar{i}$ the equilibrium is unique and $Q_3^* = M$.

The possibility of multiple equilibria arises from the fact that the right hand side of (10) may be neither monotonic nor continuous. That is, even assuming that the investors can solve their coordination problem and therefore $p(Q_3)$ is unique, there is an additional coordination problem between developer and investors giving rise to multiple equilibrium Q_3^*. Suppose that $A_2 - i_2 < \bar{i}$, so that the developer needs to sell some tokens at ICO in order to finance future development. If the price in period 3 is expected to be high, so will be period-2 price and, as a consequence, the developer needs to sell fewer tokens in order to achieve $i_3 = \bar{i}$. Because he can hold a large fraction of tokens, future effort will be high, which implies that today's price for token should be large. Similarly, if period-3 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, and so is today's price. If instead $A_2 - i_2 \geq \bar{i}$ then the developer does not need to sell any token to finance his future investment and, as a consequence, in the unique equilibrium $Q_3^* = M$.

Consider now optimal investment and effort in period 1 and 2. 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 1 and period 2 investment affects the equilibrium at ICO and therefore Q_3^*. This is relevant whenever $a < 2\bar{i}$, in which case the developer may choose not to invest in periods 1 or 2, so to set $Q_3 = M$.

It is, however, easy to show that postponing investment is never optimal. Suppose that $2\bar{i} \leq a < 3\bar{i}$. If the developer invests in the first two periods, then total utility is

$$\frac{2 \cdot g^*(M) + g^*(Q_3^*)}{(1-\gamma)M} M - (e^*(M))^2 - \frac{1}{2}(e^*(g^*(Q_3^*))^2.$$

if instead the developer does not invest in either period 1 or 2, he can set $Q_3 = M$ and achieve utility

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

Comparing the above two expressions, it is clear that the developer is better off by

using his own funds for investing in period 1 and 2, and then financing period-3 investment via the sale of tokens at ICO.

Lemma 4. *In equilibrium, the value of the protocol in period $T = 3$ is*

$$V_3 = \begin{cases} 3g^*(M) & \text{if } a \geq 3\bar{i} \\ ng^*(M) + g^*(Q_3^*) & \text{otherwise} \end{cases}$$

where $n \equiv argmax_{k \leq 2}\{k \cdot \bar{i} \leq a\}$ and Q_3^* is defined in Lemma 3.

Proof. In the text. □

Corollary 2. *The developer prefers to hold the ICO in period 2 than in period 3, strictly so when $a < 3\bar{i}$.*

Remember that in the "rich developer" case, the developer is indifferent between holding the ICO in the last period or the previous one because, in either case, he will not sell any token before period T. If instead the developer does not have enough funds to finance the efficient level of investment in all periods, he strictly prefers to hold the ICO in the second to last period of the game. Doing so, he can raise some funds at ICO and invest efficiently in the last period of the game.

Case 3: $t_o = 1$. If the ICO occurred in period 1, then in period 2 there is a market for tokens. Let's start by considering the choice of Q_3, that is, of how many tokens to sell or buy in period 2. For given p_2, the continuation utility as a function of Q_3 is:

$$U_3(Q_3, A_2 + (Q_2 - Q_3) \cdot p_2 - i_2) + \lambda_2(A_2 - i_2 - p_2 \max\{Q_3 - Q_2, 0\})$$

There are similarities with the previous case (i.e., the case of an ICO in period 2). Also here the choice of Q_3 determines the assets available in the following period. As a consequence, the continuation value

$$U_3(Q_3, A_2 + (Q_2 - Q_3) \cdot p_2 - i_2)$$

is strictly convex in Q_3 only for

$$\hat{Q} \leq Q_3 \leq Q_2 - \frac{i_2 + \bar{i} - A_2}{p_2}$$

and is linearly increasing in Q_3 otherwise, with a downward discontinuity at $Q_2 - \frac{i_2 + \bar{i} - A_2}{p_2}$.

There are however two important differences with the previous case. The first one is that, here, the developer could have sold some tokens at ICO, and therefore it is possible that $Q_2 < M$. It follows that the period-2 cash constraint may be binding. With this respect, note that if the cash constraint in period 2 is binding, then $A_3 = 0$ and the cash constraint in period 3 is binding. Conversely, if the period 3 cash constraint is binding we have $A_3 = \bar{i}$, which implies that the period 2 cash constraint is not binding. Hence, in solving for Q_3, the only constraint that needs to be taken into consideration is the period-3 cash constraint.

Second, and most importantly, because investors are price takers, then the market price in period 2 does not depend on Q_3. Only period-3 price depends on Q_3, leading to the same type of anti-coordination problem discussed in the "rich developer" case.

Proposition 4 (Equilibrium in period 2)**.** *Define*

$$Q_3^* \equiv \min\left\{Q_2 - \frac{i_2 + \bar{i} - A_2}{p_2}, M\right\}.$$

as the largest Q_3 that allows the developer to set $i_3 = \bar{i}$. If $Q^* \leq \hat{Q}$, then the developer is indifferent between holding any level of Q_3. Effort and investment in period 3 are zero, so that $p_3 = p_2 = \frac{V_2}{(1-\gamma)M}$.

If instead $Q^* > \hat{Q}$, then, in equilibrium, the developer is indifferent between setting $Q_3 = 0$ and setting $Q_3 = Q_3^*$. He sets $Q_3 = 0$ with probability

$$\alpha_2 = \left(\frac{1}{2}(e^*(Q_3^*)^2 + \bar{i}\right)\left(Q_3^* \cdot \frac{g(e^*(Q_3^*)}{(1-\gamma)M}\right)^{-1}$$

The equilibrium price is

$$p_2 = \frac{V_2 + (1-\alpha_2)g(e^*(Q_3^*))}{(1-\gamma)M}$$

The equilibrium always exists. If $A_2 - i_2 \leq \bar{i}$ multiple equilibria are possible, while if $A_2 - i_2 > \bar{i}$ the equilibrium is always unique.

For intuition, remember that the developer has incentives to invest and exert effort in period 3 only if $Q_3 > \hat{Q}$. Whether $Q_3 > \hat{Q}$ is attainable depends on the cash constraint. If this constraint is tight, $Q_3 \leq \hat{Q}$ and no level of Q_3 that is attainable will generate sufficient incentives and hence there will be no development

in period 3. If instead the cash constraint is sufficiently loose, then $Q_3 > \hat{Q}$ and for some level of Q_3 there will be positive effort and investment in period 3. In this case, there is the same anti-coordination problem discussed in the previous section. The equilibrium is again in mixed strategies, with the developer either selling everything and setting $Q_3 = 0$ or holding the maximum number of tokens, which is the minimum between the one at which period-3 cash constraint is binding and M.

Interestingly, next to this anti-coordination problem here there is the same coordination problem discussed for the case $t_o = 2$. Whenever $A_2 - i_2 \leq \bar{i}$, there could be an equilibrium in which p_2 is high, which implies that the developer needs to sell few tokens to finance future investment, and therefore period-3 effort is high. Next to this equilibrium, there could be one in which p_2 is low, which implies that the developer needs to sell many tokens to finance future investment, and therefore period-3 effort is low. We therefore could have multiple mixed strategy equilibria, each of them corresponding to a different Q_3^* and a different p_2.

To illustrate the possibility of multiple mixed-strategy equilibria, assume that no development occurred before period 3 (so that $V_2 = 0$), and that $A_2 = 0$. If p_2 is zero, then the developer cannot make any investment in period 3. Effort will be zero and therefore there will be no development in period T, which implies that $p_2 = 0$ is an equilibrium.[17] If instead p_2 is strictly positive, then by selling some tokens the developer can finance future investment and generate positive future effort. For $\bar{i}$ sufficiently low, a second equilibrium in which $Q_3^* > 0$ and development occurs with positive probability exists.

If instead $A_2 - i_2 > \bar{i}$ then the developer does not need to sell any token to achieve $i_3 = \bar{i}$, and the coordination problem discussed above is absent. The price for tokens determines how many additional tokens the developer can purchase and therefore future effort. If the price is low then he will be able to purchase many tokens and his future effort will be high. But then today's price should be large. Similarly, if the price in period 2 is high, then the developer cannot purchase many additional tokens, and future effort will be low, which implies that period 2's price should be low. There is a unique price such that investors expectation coincide with the developer's actions, and therefore there is a unique mixed strategy equilibrium.

Consider now the choice of optimal effort and investment in period 2. Because

[17] Interestingly, the equilibrium is in pure strategy. This is the degenerate case of the more general class of equilibria described in Proposition 4.

the developer is indifferent between selling all his tokens in period 2 or holding Q_3^*, I can write

$$U_2(Q_2, A_2) = Q_2 p_2 - \frac{1}{2}e^2 + i_2 + \lambda_2(A_2 - i_2)$$

where $A_2 = a - i_1$ and

$$\begin{aligned} p_2 &= \frac{V_2 + (1-\alpha_2)g(e^*(Q_3^*))}{(1-\gamma)M} \\ &= \frac{V_1 + f(e_2, i_2) + g(e^*(Q_3^*))}{(1-\gamma)M} + \begin{cases} \frac{g(e^*(Q_3^*))}{(1-\gamma)M} - \frac{\frac{1}{2}\left(e^*(Q_3^*)\right)^2 + \bar{i}}{Q_3^*} & \text{if } Q_3^* > \hat{Q} \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

The choice of optimal e_2 is again given by (7). The choice of optimal i_2 instead has an additional consideration because the choice of i_2 affects Q_3^*. That is, the developer may want to set $i_2 = 0$ even if $A_2 \geq \bar{i}$ and $Q_2 > \hat{Q}$ so to achieve a higher Q_3. Without solving the full problem, I simply note that, because of these intertemporal considerations, the optimal i_2 is different from (8). Despite this, it is possible to characterize the developer's choice of Q_2, that is, how many tokens to sell at ICO.

Proposition 5. *At ICO, the developer sells just enough token so that $i_2 = \bar{i}$. If investment is always zero for all Q_2, than the agent is indifferent between any Q_2. There could be multiple equilibria.*

The above proposition is based on the fact that, for given i_2, the developer will undo in period 2 whatever choice was made at ICO. The reason is that the price at ICO must be equal to the price post ICO, and therefore the developer is indifferent between selling tokens at ICO or during the following period. It follows that the choice of how many tokens to sell at ICO affects exclusively effort and investment in the following period.

We can now compare the equilibrium in case $t_o = 2$ and $t_o = 1$. In making this comparison, the important observation is that when $t_o = 1$ development in period 3 will happen only with probability between zero and one. Let us assume that $a > \bar{i}$ so that the developer can self finance investment in period 1 (the argument is the same for the other case). In case $t_o = 2$ and $a \geq 2\bar{i}$, the developer will set $i_1 = i_2 = i_3 = \bar{i}$ with probability 1, and therefore $t_o = 2$ is preferred to $t_o = 3$. If instead $a < 2\bar{i}$, then when $t_o = 2$ the developer will invest for sure in periods 1 and 3 (or 2 and 3) and will not invest in remaining period. If instead $t_o = 2$, the developer will invest for sure in periods 1 and 2, and will invest with positive probability in period 3.

Proposition 6. *If $a \geq 2\bar{i}$ then the developer holds the ICO in period 2. Otherwise the developer holds the ICO in period 1.*

Proof. In the text. □

To summarize, the developer uses his own resources to invest until they are depleted, and only after they are depleted he will hold the ICO.

To conclude, note that, also here, the developer's payoff does not depend on M. Fix for every period the share of the total stock of tokens held by the developer. Given this sequence, the level of effort and the incentive to set positive investment in every period are independent from M. This also implies that, the value of all outstanding tokens $p_t M$ does not depend on M but only on the share of tokens held by the developer in every period. In addition, Lemma 3, Proposition 4 and 5, show that the equilibrium share of tokens held by the developer in a given period depends on the share of tokens held in the previous period and on the total value of outstanding tokens. All the relevant quantities are, therefore, invariant to changes in M.

5 Discussion

5.1 Poor developer, $T > 3$.

In the poor developer case, whenever $T > 3$ and the ICO happens in period T, $T-1$ or $T-2$, all results derived for the case $T = 3$ continue to hold. Whenever the ICO occurs before period $T-2$, the only difference with the case $T = 3$ is that the market for tokens will be open for additional periods. Note, however, that the basic anti-coordination problem discussed earlier applies during these periods as well: any time before T in which the market for tokens is open the equilibrium is in mixed strategy, and the probability that the developer develops the platform in the following period is less than 1. If instead the developer does not hold the ICO and has sufficient funds to invest $\bar{i}$, he can achieve the efficient level of effort and investments. This observation implies that Proposition 6 holds also for $T > 3$: in equilibrium the developer uses his own resources to invest until they are depleted, and only then holds the ICO.

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 token is open, for given price for token there is a threshold productivity above which the developer wants to hold all tokens, 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 token 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.[18]

The important observation is that the productivity of the developer is 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.

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 that the developer with the largest q_{t+1}^i is indifferent between holding all tokens or no tokens.[19] If, furthermore, $\max_j q_t^j$ is constant over time, then the model is

[18] 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.

[19] 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. But then this developer's contribution to the protocol should already be accounted for in the current price, which implies that this developer strictly prefers to sell all his token, leading to a contradiction.

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 of effort and investment in every period, but he may not be the most productive developer who could work on the project.

If instead some developer 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 developer that, in equilibrium, develops the protocol with positive probability in every period depends partly on productivity and partly on wealth. The full exploration of this case is left for future work.

5.4 Total stock of tokens

The fact that M does not play any role in the developer's problem depends crucially on the assumption that, from period T onward, investors hold $\gamma \cdot M$ tokens. Suppose instead that investors hold a constant amount of tokens I in every period. It is easy to see that by choosing M, the developer can effectively choose the parameter γ, which therefore becomes endogenous. The developer will want to set this parameter as high as possible (and therefore set M as low as possible), so to increase p_T for given V_T. Of course, under this alternative assumption the developer's problem has no solution. But the point here is simply to illustrate the fact that, in general, the way the speculative demand for tokens is determined will affect the choice of M.

6 Conclusion

This paper studies a novel form of financing for open-source software development: seignorage. I show that seignorage is effective at generating incentives and providing financial resources for the development of blockchain-based software. Its effective-

ness 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 his tokens and that, as a consequence, no development will occur.

Importantly, in the "rich developer" case the developer uses his own resources to finance the investment in the protocol, so that seignorage plays a role exclusively because it generates profits and provides incentives. In the "poor developer" case, seignorage 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 seignorage 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 investor (call it a *traditional investor*) could provide capital to the developer so to move from the "poor developer" to the "rich developer" case, and by doing so generate extra surplus.

There could be significant constraints to the parties ability to share this surplus, which may reduce the scope of a traditional investment. For example, if the developer can default on his liabilities at no cost, then the traditional investor will not want to contribute funds to the development of the protocol. Also, as discussed in Section 5.3, there could be multiple developers, each of them working on the protocol few periods and then abandoning it (as it is often the case with open source projects), in which case it may be unfeasible to contract with all developers. Studying the constraints that, in this environment, prevent perfect contracting between a traditional investor and a developer (or multiple developers), and comparing seignorage with traditional financing is left for future work.

Mathematical appendix

Proof of Proposition 1. In the text I show that if $\tilde{U}_T(Q_T)$ is strictly convex, then $\tilde{U}_{T-1}(Q_{T-1})$ is also strictly convex. It is easy to check that the argument applies to all t: if $\tilde{U}_{t+1}(Q_{t+1})$ is strictly convex then also $\tilde{U}_t(Q_t)$ is strictly convex. By induction therefore all $\tilde{U}_t(Q_t)$ are strictly convex. Hence, in every period the only possible equilibrium is one in which the developer is indifferent between selling all his tokens or purchasing all tokens, and the price must be $p_t = \frac{\tilde{U}_{t+1}(M)}{M}$.

The fact that in every period t the developer is indifferent between setting $Q_{t+1} = 0$ and $Q_{t+1} = M$ implies that the developer is indifferent between holding zero tokens from period t onward, or holding M tokens from period t onward. Using this fact, I can write the developer's utility as the payoff achieved in case he sells all his tokens in period t and never purchase them anymore, so that the choice of effort and investment in period t solves:

$$\max_{e_t, i_t} \left\{ Q_t p_t - \frac{1}{2} e_t^2 - i_t \right\}$$

Furthermore, I can write the price of the token in period t as

$$p_t = \frac{\tilde{U}_{t+1}(M)}{M} = \frac{V_t + \sum_{s=t+1}^{T} f(e_s^*(M), i_s^*(M))}{(1-\gamma)M} - \frac{\sum_{s=t+1}^{T} e_s^*(M)^2/2 + i_s^*(M)}{M} \quad (11)$$

where I used the fact that the $\tilde{U}_{t+1}(M)$ can be written as the utility that the agent will earn if he holds M tokens until the last period, so that $e_t^*(M), i_t^*(M)$ are optimal effort and investment in period t conditional on holding all tokens, and $\frac{V_t + \sum_{s=t+1}^{T} f(e_s^*(M), i_s^*(M))}{(1-\gamma)M}$ is the resulting p_T. Using the above expression, optimal effort and optimal investment in period t solve:

$$\max_{e_t, i_t} \left\{ Q_t \left(\frac{V_{t-1} + f(e_t, i_t) + \sum_{s=t+1}^{T} f(e_s^*(M), i_s^*(M))}{(1-\gamma)M} - \frac{\sum_{s=t+1}^{T} e_s^*(M)^2/2 + i_s^*(M)}{M} \right) - \frac{1}{2} e_t^2 - i_t \right\}$$

It is easy to check that optimal effort and investment are again given by (2) and (3). Because optimal effort an investment in every period t do not depend on t, we can rewrite (11) as

$$p_t = \frac{V_t + (T-t) f(e^*(M), i^*(M))}{(1-\gamma)M} - (T-t) \frac{e^*(M)^2/2 + i^*(M)}{M} \quad (12)$$

Finally, from the above expression, 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 α_{t-1} the probability that in period $t-1$ the developer sells all 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 α_{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 (12) and achieve (6). □

Proof of Lemma 3. Suppose $p(Q_3)$ is a correspondence, and that the "high" equilibrium is expected to emerge. The discontinuity is at

$$\tilde{Q}'_3 \equiv Q_3 : \frac{\bar{i} + i_2 - A_2}{M - Q_3} = \frac{f(e_1, i_1) + f(e_2, i_2) + g(e^*(Q_3))}{(1-\gamma)M}$$

generating a continuation utility:

$$\frac{f(e_1, i_1) + f(e_2, i_2) + g(e^*(\min\{\tilde{Q}'_3, M\}))}{(1-\gamma)M}M - \frac{1}{2}(e^*(\min\{\tilde{Q}'_3, M\}))^2$$

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

$$\tilde{Q}''_3 = M - \frac{\left(\bar{i} + i_2 - A_2\right)(1-\gamma)M}{f(e_1, i_1) + f(e_2, i_2)}$$

generating a continuation utility:

$$\frac{f(e_1, i_1) + f(e_2, i_2) + g(e^*(\min\{\tilde{Q}''_3, M\}))}{(1-\gamma)M}M - \frac{1}{2}(e^*(\min\{\tilde{Q}''_3, M\}))^2$$

Because period 3 effort is chosen optimally, it must be that

$$\frac{g(e^*(\min\{\tilde{Q}_3', M\}))}{(1-\gamma)M} M \geq \frac{1}{2}(e^*(\min\{\tilde{Q}_3', M\}))^2$$

and

$$\frac{g(e^*(\min\{\tilde{Q}_3'', M\}))}{(1-\gamma)M} M \geq \frac{1}{2}(e^*(\min\{\tilde{Q}_3'', M\}))^2$$

which implies that the two continuation utilities (the one with threshold $\tilde{Q}_3'$ and the one with threshold $\tilde{Q}_3''$) are greater than the continuation utility when the developer holds $Q_3 = M$ and no investment occurs:

$$\frac{f(e_1, i_1) + f(e_2, i_2)}{(1-\gamma)M} M$$

Hence holding either $\tilde{Q}_3'$ or $\hat{Q}_3''$ is preferred to holding the entire stock of tokens M and not investing. □

Proof of Proposition 4. In the text, I argue that when $Q^* \leq \hat{Q}$ then the continuation value is linear in Q_3 because there is no Q_3 for which the developer will exert effort in period 3.

If instead $Q^* > \hat{Q}$ then the continuation value is somewhere strictly convex in Q_3. 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 $Q_3 = 0$ and the largest possible Q_3 such that the period-3 constraint is not binding, that is

$$Q_3^* = \min\left\{Q_2 + \frac{A_2 - i_2 - \bar{i}}{p_2}, M\right\}.$$

The price at which the developer is indifferent is:

$$p_2 = \frac{U_3(Q_3^*, A_2 + (Q_2 - Q_3^*) \cdot p_2 - i_2)}{Q_3^*} = \frac{Q_3^* \left(\frac{V_2 + g(e^*(Q_3^*, \bar{i})}{(1-\gamma)M}\right) - \frac{1}{2}(e^*(Q_3^*, \bar{i})^2 - \bar{i}}{Q_3^*}$$

Furthermore, investors must be indifferent between holding tokens in period 3 and in period 2, which implies that

$$p_2 = \frac{V_2 + (1-\alpha_2) g(e^*(Q_3^*, \bar{i}))}{(1-\gamma)M}$$

where α_2 is the probability that the developer sells all his tokens in period 2. Combining the above two expressions and solving for α_2 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 $\max\{Q_3^*, M\}$ and 0. Define Q_3^* as a function of p_2 by:

$$Q(p) \equiv \begin{cases} \min\left\{Q_2 - \frac{i_2+\bar{i}-A_2}{p}, M\right\} & \text{if } Q_2 - \frac{i_2+\bar{i}-A_2}{p} > 0 \\ 0 & \text{otherwise,} \end{cases}$$

which is increasing whenever $A_2 - i_2 \leq \bar{i}$ (that is, when the developer needs to sell some tokens in period 2 to invest $i_3 = \bar{i}$), and is decreasing otherwise.

Similarly define the equilibrium p_2 as a function of Q_3^* by:

$$p(Q) \equiv \frac{V_2 + (1-\alpha(Q))g(e^*(Q), i^*(Q, A_3))\{i^*(Q) \geq \bar{i}\}}{(1-\gamma)M}$$

where

$$\alpha(Q) \equiv \left(\frac{1}{2}(e^*(Q, i^*(Q, A_3)))^2 + i^*(Q, A_3)\right)\left(Q \cdot \frac{g(e^*(Q, i^*(Q, A_3)))}{(1-\gamma)M}\right)^{-1}$$

The complication here is that, for given Q, A_3 is itself a function of $p(Q)$, which implies that $p(Q)$ is a correspondence. The reason is the same discussed in the body of the paper for the case $t_o = 2$: if the developer needs to sell some tokens to invest in period 3, then for given number of tokens sold, period-3 investment will be a function of the price at which the developer can sell these tokens. Hence, whenever $A_2 - i_2 < \bar{i}$ (that is, whenever the developer needs to sell some tokens in period 2 to invest $i_3 = \bar{i}$), we have

$$p(Q) \equiv \frac{V_2}{(1-\gamma)M} + \begin{cases} 0 & \text{if either } Q \leq \hat{Q} \text{ or } Q > Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2}{(1-\gamma)M}} \\ \frac{(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} & \text{if } \hat{Q} \leq Q \leq Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}} \end{cases}$$

because

$$Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2}{(1-\gamma)M}} < Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}}$$

for all Q, the case $A_2 - i_2 < \bar{i}$ can be split into three subcases:[20]

[20] The three cases emerge as a function of the three state variables Q_2, V_2 and $A_2 - i_2$. For ease of exposition, I describe them solely in terms of V_2, although for $Q_2 > \hat{Q}$ but sufficiently low, the three cases will indeed emerge as a function of V_2 exclusively.

1. ("high V_2") Whenever $Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2}{(1-\gamma)M}} > \hat{Q}$ then for some Q we have $p(Q) = \left\{\frac{V_2}{(1-\gamma)M}, \frac{V_2+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}\right\}$. That is, there are situations in which for given Q_3^*, if p_2 is low the developer will not have enough funds to finance investment in period 3, and therefore no development will occur. If instead p_2 is high there is positive probability that the developer will invest and exert effort in period 3. Again, this situation can be seen as a coordination problem among investors. For given action taken by the developer in period 2, investors can coordinate on a "high" equilibrium that leads to effort and investment in period 3 with positive probability, or a "low" equilibrium leading to no development in period 3.

2. ("low V_2") Whenever $Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2+(1-\alpha(M))g(e^*(M))}{(1-\gamma)M}} \leq \hat{Q}$, then there is no development in period 3 and $p(Q) = \frac{V_2}{(1-\gamma)M}$ for all Q.

3. ("intermediate V_2") in all other cases, $p(Q)$ is a function, which is equal to $\frac{V_2}{(1-\gamma)M}$ for $Q \leq \hat{Q}$ and to $\frac{V_2+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}$ otherwise.

Instead, whenever $A_2 - i_2 \geq \bar{i}$ (that is, whenever the developer has enough own funds to invest $i_3 = \bar{i}$), then period 3 investment does not depend on p_2 and therefore

$$p(Q) \equiv \frac{V_2}{(1-\gamma)M} + \begin{cases} 0 & \text{if either } Q \leq \hat{Q} \\ \frac{(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} & \text{otherwise} \end{cases}$$

which is a continuous function.

By definition of $\alpha(Q)$, I can write

$$Q \cdot \frac{g(e^*(Q,\bar{i}))}{(1-\gamma)M} - \frac{1}{2}(e^*(Q,\bar{i}))^2 - \bar{i} = (1-\alpha(Q))Q \cdot \frac{g(e^*(Q,\bar{i}))}{(1-\gamma)M}. \tag{13}$$

The LHS of (13) 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 (13) 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 3, and is constant otherwise.

The equilibrium of the game is a p^* such that $p^* = p(Q(p^*))$ and a $Q^* = Q(p^*)$. Figure 4 represents all possible cases. Whenever both $p(Q)$ and $Q(p)$ are functions, 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 ($A_2 - i_2 < \bar{i}$, "high V_2" case) we know that for $\hat{Q} \leq Q \leq Q_2 - \frac{i_2+\bar{i}-A_2}{\frac{V_2+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M}}$ we have that $\frac{V_2+(1-\alpha(Q))g(e^*(Q,\bar{i}))}{(1-\gamma)M} \in p(Q)$. Define the threshold value of Q

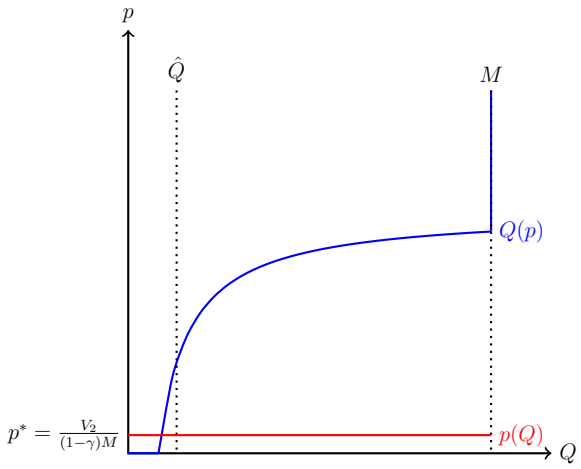
$$\tilde{Q} \equiv Q_2 - \frac{i_2 + \bar{i} - A_2}{\frac{V_2+(1-\alpha(\tilde{Q}))g(e^*(\tilde{Q},\bar{i}))}{(1-\gamma)M}}$$

and similarly the corresponding price

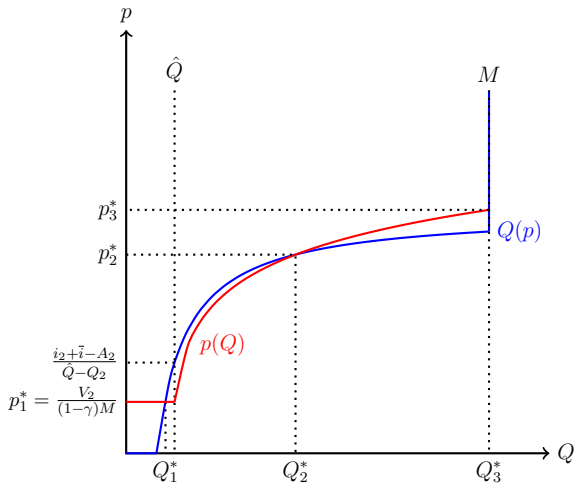
$$\tilde{p} \equiv \frac{V_2 + (1 - \alpha(\tilde{Q}))g(e^*(\tilde{Q}, \bar{i}))}{(1 - \gamma)M} \in p(Q)$$

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

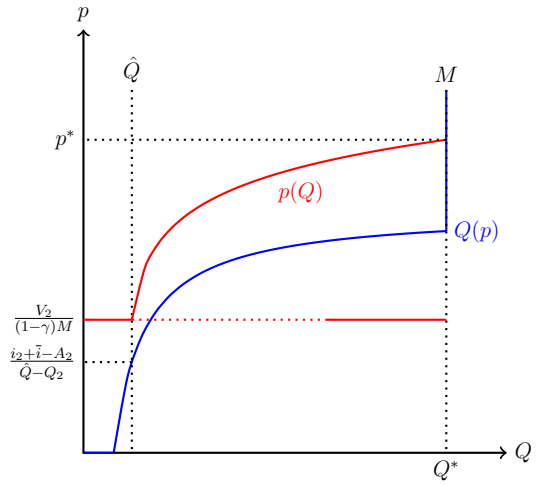
It is quite immediate to see that in case $A_2 - i_2 \geq \bar{i}$ the equilibrium is unique. The equilibrium is unique also in the "low V_2" case. In all other cases multiple equilibria are possible.



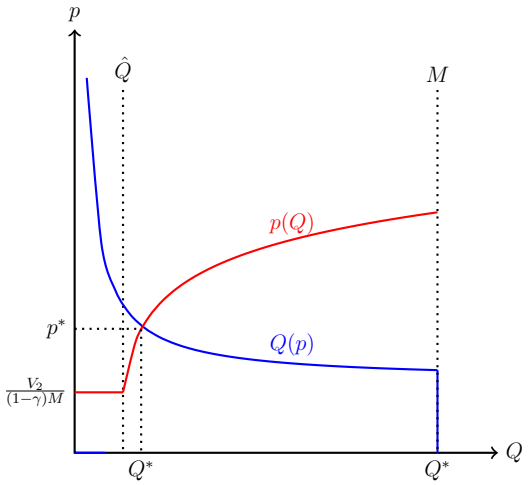
(a) $A_2 - i_2 \leq \bar{i}$; "low V_2" case.



(b) $A_2 - i_2 \leq \bar{i}$; "intermediate V_2" case; multiple equilibria



(c) $A_2 - i_2 < \bar{i}$; "high V_2" case.



(d) $A_2 - i_2 > \bar{i}$

Fig. 4: Equilibrium in 2.

□

Proof of Proposition 5. Write $A_2 = a - i_1 + p_1(M - Q_2)$, and note that in equilibrium $p_1 = p_2$, and hence

$$Q_3^* = \min\left\{M - \frac{i_2 + \bar{i} + i_1 - a}{p_2}, M\right\},$$

that is, independently from how many tokens are sold at ICO, in period 2 the

developer will sell/buy tokens so that Q_3^* is constant. Hence, the choice of Q_2 affects Q_3^* only via i_2.

Among the Q_2 such that $i_2 = 0$, the developer is indifferent between setting any Q_2, because Q_3^* is constant and so is period-3 effort and the final price. That is, any Q_2 such that $i_2 = 0$ generates utility Mp_2, where

$$p_2 = \left(\frac{V_1 + g(e^*(Q_3^*))}{(1-\gamma)M} - \frac{\frac{1}{2}\left(e^*(Q_3^*)\right)^2 + \bar{i}}{Q_3^*} \right)$$

with $Q_3^* = \min\left\{ M - \frac{\bar{i}+i_1-a}{p_2}, M \right\}$. Among the Q_2 such that $i_2 = \bar{i}$, the developer strictly prefers high Q_2, because they generate higher effort in period 2. Call Q_2^* the highest Q_2 for which $i_2 = \bar{i}$, and note that after setting $Q_2 = Q_2^*$ the fact that the agent chooses $i_2 = \bar{i}$ implies that the continuation payoff given $i_2 = \bar{i}$ is larger than the continuation payoff given $i_2 = 0$. The continuation payoff for given $i_2 = \bar{i}$ is itself increasing in Q_2 because it leads to higher period 2 effort but no changes in Q_3^*, leading to the following proposition. □

References

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

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. Technical report.

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

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

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

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.

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.

Ma, J., J. S. Gans, and R. Tourky (2018). Market structure in bitcoin mining. Technical report, NBER working paper.

Prat, J. and B. Walter (2018). An equilibrium model of the market for bitcoin mining. Technical report, CESifo Working Paper.