
Management Science

Publication details, including instructions for authors and subscription information:
http://pubsonline.informs.org

# An Examination of Velocity and Initial Coin Offerings

Richard Holden, Anup Malani

To cite this article:
Richard Holden, Anup Malani (2022) An Examination of Velocity and Initial Coin Offerings. Management Science 68(12):9026-9041. https://doi.org/10.1287/mnsc.2022.4314

https://pubsonline.informs.org/journal/mnsc

MANAGEMENT SCIENCE
Vol. 68, No. 12, December 2022, pp. 9026–9041
ISSN 0025-1909 (print), ISSN 1526-5501 (online)

# An Examination of Velocity and Initial Coin Offerings

**Richard Holden,**[a,*] **Anup Malani**[b,c]

[a] Economics, University of New South Wales Business School, Sydney, New South Wales 2052, Australia; [b] University of Chicago Law School, Chicago, Illinois 60637; [c] National Bureau of Economic Research, Cambridge, Massachusetts 02138
*Corresponding author

**Contact:** richard.holden@unsw.edu.au, https://orcid.org/0000-0003-2293-6355 (RH); amalani@uchicago.edu (AM)

**Received:** October 12, 2021
**Revised:** January 5, 2022
**Accepted:** January 9, 2022
**Published Online in Articles in Advance:** March 1, 2022

https://doi.org/10.1287/mnsc.2022.4314



**Abstract.** Blockchain technology offers firms a novel method of raising capital via so-called initial coin offerings (ICOs). In the most common form of an ICO, a firm creates digital assets called "utility tokens" that are tracked on a blockchain-based ledger, requires that its product be purchased only with those tokens, and then, raises capital by selling these tokens to investors prior to creating any saleable product. (Some nonfungible tokens (NFTs) may function in a similar fashion.) We model a fundamental paradox with the use of ICOs involving utility tokens and similar structures. To increase capital raised by an ICO, the firm may attempt to reduce blockchain operating costs, thus expanding the quantity of goods sold. However, because of the mechanics of miner compensation, doing so increases the number of utility token transactions that take place in any time interval (i.e., increases token velocity and thus, the effective supply of tokens). By Fisher's equation, this lowers the dollar value of tokens and the amount investors are willing to pay for them. We show that this paradox limits the value of utility token ICOs as an alternative to traditional financing options. We discuss alternatives to and variations of utility tokens that can mitigate the conundrum and promote ICOs as a more viable form of financing.

**History:** Accepted by Joshua Gans, business strategy.

**Keywords:** blockchain • initial coin offerings • security token offerings • cryptoeconomics • utility token • equation of exchange • transactions costs • cryptocurrencies

## 1. Introduction

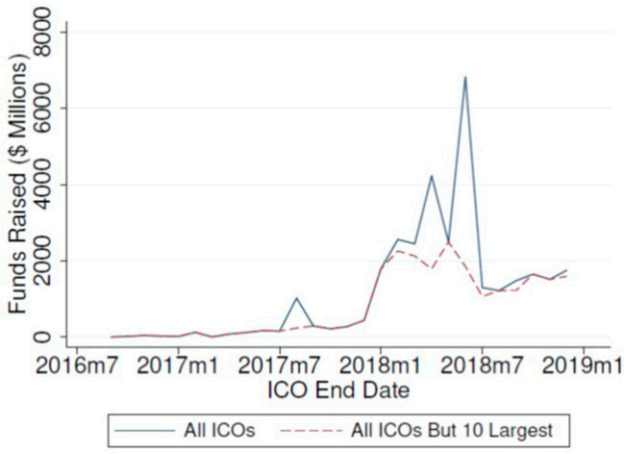
In the last six years, there has been a boom in investment in start-up projects that use blockchain, a new technology for creating digital ledgers that do not rely on a centralized authority to manage the ledger. The initial surge of investment came through a new vehicle for raising capital called an initial coin offering (ICO) (see Figure 1). Through December 2018, ICOs raised nearly $33.4 billion. In 2017 alone, even before the number of ICOs peaked, ICOs raised $6.5 billion, more than the total amount raised via venture capital investment in all internet projects. There was a crash in 2018 following regulatory attention from the U.S. Securities and Exchange Commission that wiped out the ICO market. However, investment in blockchain start-ups found another vehicle in 2021 with nonfungible tokens (NFTs). Although some of these were final sales of digital art (as opposed to digital currencies), others were sales of digital assets that entitled owners to additional services later, like many ICOs.[1] Moreover, ICOs are still possible, although they now require (costly) disclosures under the securities laws.

In an ICO, a firm raises capital for a project in three steps. First, it creates a digital asset, called a "token," that gives owners the right to some value from the firm's project. This value can either be the dividends of the firm (a "security" token) or rights to the firm's output (a "utility" token).[2] Second, the firm tracks the ownership of the token on a blockchain ledger. Third, the firm sells those tokens to investors. The proceeds of the sale are used to execute the project.

ICOs have become a popular method of raising capital owing to their advantages over traditional financing options. Beyond benefiting from the security and disintermediation of a blockchain ledger, ICOs also assist with coordination and first-mover problems in the face of network effects, which are particularly relevant for platform projects (Catalini and Gans 2018, Li and Mann 2018); they limit moral hazard created by sale of equity (Bocks et al. 2019), and although they are similar to other crowdfunding approaches, like Kickstarter, they also offer liquidity to investors by allowing for trade in the right over future goods (Howell et al 2019).

Understanding the role that ICOs can play as an alternative form of financing is important in determining not only the capital structure of firms but also, the degree to which firms are financially constrained, which in turn, affects their business strategy and ability to grow. Although ICOs have many advantages, there remains the primary question of how their capital-raising potential compares with traditional modes of finance. To what

**Figure 1.** (Color online) Capital Raised via ICOs




*Source.* Davydiuk et al. (2019).

extent do ICOs offer less restrictive financing? Additionally, what factors or trade-offs limit their efficacy as an alternative mode of finance?

In this paper, we consider the economics of ICOs that issue utility tokens and similar financing structures, including sales of NFTs that function like utility tokens. We focus on a particular unexpected trade-off faced by such ICOs that limits their ability to raise funds. To do this, we model two ways in which a firm can generate revenues from a project. One is to charge a fee (or markup over costs) for the output of the project. The other is to sell utility tokens that can later be exchanged for output. In either case, the firm can use revenues to finance the underlying project. In the case of fees, the firm can sell rights to the revenue from fees to investors ("traditional financing"). With funds from selling utility tokens, the firm can directly finance the project.

Setting the optimal fee is akin to the problem of setting a revenue-maximizing tax or choosing the optimal markup on costs. By contrast, the optimal utility token policy requires choosing a ledger technology that imposes some friction but not too much. The friction here refers to the cost—in effort and time—of validating transactions on a blockchain ledger (i.e., the cost of what is called "mining" in blockchain parlance). This, in turn, is determined by the "consensus protocol" used by the ledger. The most popular candidates are proof of work (PoW) and proof of stake (PoS).

Choosing the optimal level of friction involves what we call the ICO paradox. Setting too high a friction discourages sales. However, setting too low a friction increases the number of utility token transactions that take place in any time interval. In other words, it increases token velocity and thus, the effective supply of tokens (Fisher 1912). This, in turn, reduces the value of the token, despite offering a lower friction.

### 1.1. An Illustration

We can illustrate the basic economics behind our main result with a simple example. The key thing here is that consumer demand does not limit token velocity. Indeed, any finite velocity can be supported.

Consider a gym where the cost of producing service is \$10 per day. Suppose there are 10 people indexed from 1 to 20, and the willingness to pay (WTP) for person $i$ is $\$(i-1)$. This implies that 10 people have a WTP greater than or equal to cost and that 10 do not. Assuming a competitive market in daily gym access, the total value of output is $Q = \$100$ per day. Suppose that the owner issues 10 Gymtokens and only accepts these tokens as payment and that no other seller of any good takes Gymtokens as payment.

Imagine that each token can only be used once per day (i.e., velocity $V$ is one day per token). This velocity implies that the dollar-denominated price $P$ of each token is \$10. Market clearing requires that United States Dollar (USD)-denominated supply equals USD-denominated demand (i.e., $P \cdot M \cdot V = Q$). Plugging in $M = 10$, $V = 1$, and $Q = 100$ yields $P = \$10$.

Now suppose that velocity increases to two. Price falls to \$5, and the token price of gym access is two. However, there are still just 10 tokens, so only five customers can buy gym access at any given time. How is total daily demand of 10 customers met? Sequential purchase does the trick. The owner starts the day by selling 10 tokens in the market. The first five consumers buy the 10 tokens at \$2 per token for \$50, and they turn around and buy gym memberships with their tokens before noon. The owner is left with an additional 10 tokens to sell after noon to five more people, generating an additional \$50 in revenue. All 10 consumers get gym access, and the owner makes \$100 daily.

We can generalize to any velocity $V > 1$. The owner begins the day by selling 10 tokens. So, price of tokens falls to $\$(100/10V)$ per token. The token price of gym access per day is $V$ tokens. The first $10/V$ consumers buy the 10 tokens from the owner for $\$100/V$, turn around, and buy gym memberships before hour $24/V$, leaving the owner with an additional 10 tokens to sell at hour $24/V$ to $10/V$ people at $\$(10/V)$/token for an additional $100/V$. The process repeats until the end of the day. The owner makes \$100 through token sales.

This example illustrates that any finite velocity can be supported here. Moreover, the velocity can be more than the number of consumers—so demand does not limit velocity. We formalize this in Section 3.6, where we show that frictionless utility tokens have zero value in the limit.

Notice also that it is *not* the case that for any finite velocity $V$, the value of all tokens have to be the same as market demand $Q$ for gyms (e.g., \$100 per day). The reason is that the owners of coins purchased in an ICO (i.e., the investors in the ICO) can only sell the tokens once. They only gain $P \times M$, not $P \times M \times V$. The latter would be equal to $Q$. However, the former is equal to $Q/V < Q$ for $V > 1$. One must not confuse stock with tokens. Stock ownership is the right to all future dividends. However, utility token ownership is only the right to one trade of tokens for gym membership, not all the trades required to clear the gym market in a day, let alone for all time.

### 1.2. Related Literature

The ICO paradox—that lowering trading frictions reduces the market capitalization of utility tokens—is reminiscent of the "Grossman–Stiglitz paradox" on the impossibility of informationally efficient markets when there are positive costs to information acquisition (Grossman and Stiglitz 1976, 1980).[3] In that environment, if markets are informationally efficient, those who acquire information cannot receive a payoff for so doing. Yet, this deters them from paying the cost of information acquisition, thereby making markets informationally inefficient. Thus, an interior amount of informational efficiency arises in equilibrium. So, too, it is with utility tokens, where an interior amount of transaction costs/frictions must arise for the tokens to be worth issuing in the first place. At least, this must hold in any rational asset-pricing equilibrium. This inefficiency requirement puts an upper bound on the value of utility tokens themselves, thus limiting the viability of utility token ICOs as an alternative form of financing.

We are not the first to raise this paradox, which has previously been called the velocity problem. Vitalik Buterin (2017), the founder of Ethereum, mentioned it in an early blog post.[4] However, we believe we are the first to connect the paradox to the economics of the underlying project that the firm seeks to finance (i.e., find the optimal behavior of the firm given the paradox).[5] This is important as it helps trace the paradox back to basic economic phenomena, such as the supply and demand functions for the underlying project's output. We also believe we are the first to formally compare ICOs with alternative methods of financing while considering the impact of the ICO paradox. This comparison is made possible by modeling the underlying economics and is vital to understanding the potential for ICOs to persevere as an alternative form of financing and the circumstances in which it may be most effective.

After examining the optimal fee (or markup) and the optimal friction for utility tokens, we determine which approach provides higher revenues and therefore, less constrained finance. Surprisingly, a utility token ICO makes more sense the less technologically efficient the underlying ledger technology is. If the technology has too little friction, the utility token price will be too low to generate revenues in excess of the simpler fee-based revenue model.[6]

Our final contribution is that we use our economic model of the underlying project and of the price of tokens to help inform technological discussions about how to improve blockchains to mitigate the velocity problem and thus, increase the total amount that can be raised via ICOs. Samani (2018) attempts to do this, but without a model of the value of the underlying project, not all of the recommended methods can avoid the ICO paradox. Moreover, the economic model reveals some new techniques for avoiding the paradox.

We note that a majority of ICOs use the existing Ethereum blockchain through ERC-20 tokens (Howell et al. 2019), constraining their choices in relation to the consensus protocol, which is central to our theory. Our findings suggest that the lack of control over consensus protocol is likely to lead to a level of friction that is not optimal from the firm's perspective. However, the reduced setup costs associated with an off-the-shelf token (as well as the consistency of the standard) account for the persisting use of ERC-20 tokens.

The discussion in this paper has applications to financing outside the blockchain sector. Although utility token ICOs are typically used to fund underlying projects that themselves use blockchain technology, they can also be used to fund projects unrelated to blockchain.[7] Indeed, firms can issue the equivalent of utility tokens without a blockchain at all (i.e., not even use blockchain for the financing).

Although it is true that selling rights to the revenue from either a fee-based or a utility token model can be used to finance the project, this paper does not examine whether it is better to sell rights to these revenue streams or to have an initial public offering (IPO) of equity. Either revenue model can support an IPO to raise capital to begin the project; one could sell net profits after raising revenue either via a transaction fee or via sale of utility tokens. The main difference between selling revenue streams and selling profits streams (i.e., equity) is that the latter shares costs with investors. For a direct comparison of ICOs and IPOs, see Catalini and Gans (2018). We do not model the firm's management of the cost side of its business and therefore, do not have anything to say about selling revenue versus profit rights.

Our paper contributes to a growing literature on ICOs. Much of that literature is empirical. It either describes the return to ICOs (Benedetti and Kostovetsky 2018), as compared with IPOs (Hu et al. 2019, Garratt and van Oordt 2021) or non-ICO cryptocurrencies (Dittmar and

Wu 2018), or examines correlates of more successful ICOs (Momtaz 2018, Davydiuk et al. 2019, Howell et al. 2019). One strand of the theoretical literature explains the rationale for ICOs. For example, they solve the first-mover problem that can scuttle platforms that depend on network effects to succeed (Li and Mann 2018), help internalize the total consumer surplus created by entrepreneurs (Lee and Parlour 2018), or limit the moral hazard created by sale of equity (Bocks et al. 2019). Another strand examines how utility tokens for a platform are priced (Cong et al. 2018).

A third strand, which includes our paper, examines weaknesses of ICOs. Many of these papers focus on the incentive problems that ICOs create for entrepreneurs (Canidio 2018, Chod and Lyandres 2018, Sockin and Xiong 2018, Garratt and van Oordt 2021) and possible solutions to such incentive problems (Malinova and Park 2018). The paper closest in spirit to ours is Catalini and Gans (2018), which provides practical advice, such as the value of entrepreneurs retaining tokens to limit moral hazard and the constraint that a fixed supply monetary policy imposes on future fundraising. Likewise, this paper examines how token velocity can limit the revenue that firms can earn selling utility tokens and thus, the capital that these firms can access for finance as well as what sort of technology can mitigate that effect.

Section 2 provides background on the mechanics of blockchain and ICOs. Section 3 presents an economic model of a market platform that can raise capital either by selling rights to future revenue from charging a transaction fee or by undertaking an ICO. In the main text, we specify that the project establishes a market for the trade in some good between consumers and other producers. In the appendix, we extend the model to a simpler case where the project itself produces some good. Finally, Section 4 discusses different technological modifications to utility tokens and their potential to mitigate the velocity problem.

## 2. Background on Blockchain, Utility Tokens, and ICOs

### 2.1. Purpose of and Trust in Blockchain Ledgers

Blockchain is a technology for creating digital ledgers for tracking facts (e.g., ownership of digital assets) that can be trusted even though there is no central authority maintaining the ledger. The main alternative is ledgers maintained by a central authority, such as a government or a bank. Blockchain is useful when the central authority maintaining the alternative ledger is not trustworthy or charges too high a price for maintaining the ledger. In such cases, users may want a ledger that eliminates manipulation by (or cuts out completely) the existing intermediaries.

Blockchain utilizes computer algorithms that distribute the task of maintaining a ledger to a large number of entities in a manner that, in theory, gives those entities an incentive not to manipulate the ledger. In a well-functioning blockchain-based ledger, parties can trust the "miners" to honestly maintain the network because properly maintaining the network attracts a reward, manipulating the network is costly, and the rewards and costs are such that the return to maintenance is greater than the return to manipulation. Although this incentive scheme may make blockchain trustworthy, it also drives the major cost to users from blockchain ledger: miner compensation.

### 2.2. Mechanics of Miner Compensation

There are many ways to build a blockchain. To illustrate their commonalities, we describe the two most widely used algorithms for ensuring the trustworthiness of a decentralized ledger: PoW and PoS. PoW is the algorithm at the heart of Bitcoin, the first and largest blockchain ledger ever deployed.[8] PoS is the algorithm that Ethereum is currently transitioning to.[9]

In the Bitcoin blockchain, miners solve a computational problem that depends on the publicly announced transactions that are to be included on the ledger. The first miner to solve the puzzle earns the right to record those announced transactions (called a block of transactions) onto the ledger (which is a chain of blocks and hence, also called a blockchain). They are also compensated with a reward. The amount of the reward must be greater than the cost of attempting to solve the puzzle (in electricity and computational capital) times the probability of being the first to do so.

A selfish miner may attempt to record transactions that did not take place to enrich themselves. For fraudulent transactions to be accepted by the network, they must be incorporated into the longest existing chain. This can only be guaranteed when the selfish miner commands the majority of the computing power of the network so as to outpace the rest of the network in solving the computational problems associated with their version of the chain (Nakamoto 2008). The cost of acquiring enough computation power on the Bitcoin network to engage in a "51% attack" is over U.S. $1.4 billion and would consume as much electricity as the country of Morocco does in a typical year (Moos 2018). This prohibitive cost arguably ensures that blockchains can be trusted by parties, even though they do not rely on trusted central authority.[10]

PoW has been criticized because the amount of electricity required to power miners' computers is very large. It is estimated that maintaining the Bitcoin blockchain consumed as much electricity in 2018 as did all of Ireland that year. Putting aside the social

cost of this energy consumption, this criticism can be treated as a complaint about the transaction costs of Bitcoin and PoW.[11] Because miners must be compensated for their electricity consumption, high electricity consumption means high miner rewards. To address this problem, computer scientists have proposed alternative consensus protocols to generate trust in a decentralized ledger. The alternative that has received the most attention is PoS.

In this algorithm, instead of solving a puzzle for the right to record new transactions to the blockchain, miners bet or stake digital tokens issued by the network. On the Ethereum blockchain, which is in the midst of moving a PoW to a PoS algorithm, the token is called an Ether.[12] A miner's chance of being selected by the network to record the next set of transactions is proportional to the amount of tokens she stakes. A miner who is selected to record the next block obtains a reward.[13]

Engaging in a 51% attack under PoS is also costly, as it requires purchasing (or at least borrowing) the majority of the existing tokens. Depending on the value of the total stock of tokens, this can be many times more costly than a 51% attack under the PoW algorithm.[14] PoS often contains additional security mechanisms, requiring miners to stake their coins for a period of time and to relinquish their staked coins if they are found to have manipulated the blockchain. The larger the stakes are and the longer they are held in escrow, the greater the incentive for miners to behave as desired.

The cost of PoS, like that of PoW, is the amount that miners have to be compensated for to maintain the network. This is increasing in the amount that has to be staked to ensure a given probability of winning the rights to record the next block and how long staked tokens are held in escrow. Because a miner does not have access to her tokens when in escrow, the longer the escrow period, the larger the lost time value of money because of escrow, and therefore, the higher the required compensation is.[15]

### 2.3. Lower Miner Compensation Associated with Higher Velocity

In this section, we explain the basic empirical relationship that drives the ICO paradox; attempts to reduce miner compensation under either PoW or PoS increases transaction velocity on a blockchain ledger (i.e., the number of transactions that the digital ledger can record in a given interval of time).

This relationship is easy to explain for PoW. Because harder computational puzzles require more computing power and thus, electricity to solve, they also require greater compensation for miners. Because more difficult puzzles also require more time to solve, all else held constant, there is a positive correlation between the time required to validate and record a transaction and the required compensation for miners.[16]

This negative relationship exists in PoS, but it is not mediated by validation time. It is driven by the fact that PoS ensures trust, in part, by requiring miners to stake their tokens for a period of time. The larger the amount of time is that miners must stake tokens, the more miners must be compensated for not being able to use those coins for some other investment. However, the larger the amount of time staked tokens are in escrow, the lower the number of tokens available for transactions is, and thus, the lower the potential number of transactions is for the average token.[17]

In the previous section, we offered one reason why a blockchain consensus protocol may not want to reduce miner compensation, namely that it would reduce trust in the network. Holding trust constant, the negative relationship between miner compensation and token velocity provides a second reason why the protocol may not want to reduce compensation; lower velocity undermines the use of ICOs with utility tokens to raise capital.

### 2.4. Utility Tokens and Initial Coin Offerings

Setting up a blockchain entails development costs. Most significantly, software engineers must be hired to write the code to create and operate the blockchain. These start-up costs can be financed in traditional ways (e.g., loans or sales of equity). To be clear, these costs are not unique to blockchain. Setting up a ledger using any method entails some development costs. In this section, we discuss the use of blockchain ledgers to finance start-up costs. It is important to clarify, however, that this use of blockchains can be attached to any project requiring start-up funds whether that underlying project also uses blockchains for some other purpose or not. For example, it is possible for Filecoin to raise capital for its blockchain-based marketplace for data storage[18] and for Agenus, a pharmaceutical company, to raise capital to fund its new biotech products,[19] each using blockchain technology.

Recall that a blockchain can be used to track ownership of a digital asset. A firm seeking capital could, therefore, create a digital asset that represents rights to some value it will subsequently create after it is up and running and sell those right to investors in return for cash.

On a blockchain, rights to a firm's value creation generally take two forms, each called a token. The first is called a "security" token. This token represents rights to the firm's profits or dividends and is akin to equity. The token can be exchanged on a blockchain just as equity is traded on a stock exchange's servers. The second type of token, which is the subject of this paper, is called a "utility" token. This token obtains value from

the requirement—imposed by the firm—that goods or services created by its project can only be purchased using the token. Notable examples of utility tokens are tokens issued by Filecoin, which operates a marketplace for the exchange of hard drive space; Golem, which operates a platform for the exchange of cloud computing resources; and Basic Attention Token, which offers a marketplace for the exchange of access to eyeballs for marketers.[20]

This last requirement means that the value of a utility token (and thus, its capital-raising potential) is proportional to the total revenue—rather than the profit—generated by the project the firm seeks to finance. To understand why, consider a simple example. Suppose the firm's project produces a widget, but the widget must be purchased using the firm's utility token, which for fun, we will call a "wicket." Suppose the market price of a widget is \$3, that the firm is able to sell 10 widgets, and that the firm creates only 20 wickets. Because all purchases of widgets from the firms must take place in wickets, the value of the 20 wickets must be equal to the dollar value of the 10 wickets people want to buy from the firm. This implies that the value of each wicket is \$30/20 (i.e., equal to total firm revenues (in dollars) divided by the number of minted tokens). In our model, we will show that this simple characterization of wicket price is not exactly right because it does not indicate the time period within which the firm's 10 sales take place. However, to the extent that the example shows that token value is proportional to revenue, it is correct.

Regardless of whether a firm issues a security token or a utility token, it can sell that token to investors even before it completes the underlying project. The capital raised from the sale can then be used to finance that underlying project. This process is called an ICO.[21] It is called an ICO to evoke the idea of an initial public offering for equity security on a stock exchange. However, the similarities are limited. Whereas an IPO involves the sale of stock to the public, an ICO also refers to sales of utility tokens only to a small group of private investors. That said, many of the largest ICOs have involved token sales to the public. Although the largest IPOs raise billions of dollars, the largest ICOs are also significant. The top 10 highest-grossing ICOs, listed in Figure 2, have collectively raised \$7.6 billion.

## 3. Model of Financing a Platform with an ICO

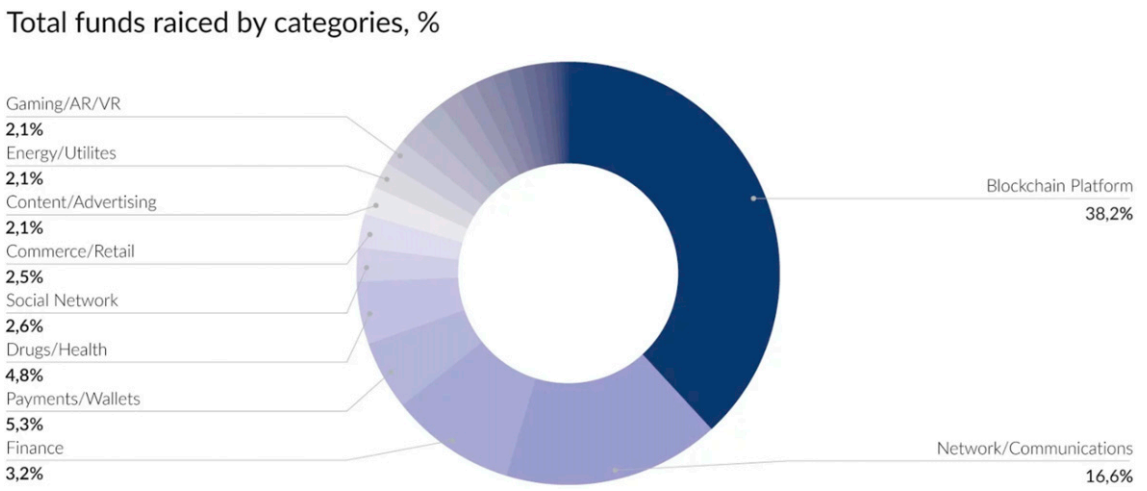
We model a firm that has an underlying project that provides a platform for the trade of a good. In the appendix, we offer an alternative model of a firm with a project that supplies a good rather than a platform for trade in that good. We focus on a platform here because it seems that platform producers are the most significant users of ICOs, at least in terms of capital raised (see Figure 3). So, our firm is neither a consumer nor producer of the good; instead, it provides a

**Figure 2.** Top 10 ICOs by Amount Raised

| Promoter | Amount raised | ICO Dates | Project |
|---|---|---|---|
| EOS | \$4.1 billion | 6/26/17 - 6/18/18 | Smart Contracts |
| Telegram | \$1.7 billion | 01/18 - 02/18 | Encrypted Messaging & Blockchain Ecosystem |
| Dragon | \$320 million | 02/15/18 - 03/15/2018 | Decentralized Currency for Casinos |
| Huobi | \$300 million | 01/24/18 - 02/28/18 | Cryptocurrency Exchange |
| Hdac | \$258 million | 11/27/17 - 12/22/17 | IoT Contract & Payment Platform |
| Filecoin | \$257 million | 08/10/17 - 09/10/17 | Decentralized Cloud Storage |
| Tezos | \$232 million | 07/01/17 - 07/14/17 | Self-Amending Distributed Ledger |
| Sirin Labs | \$158 million | 12/16/17 - 12/26/17 | Open-Source Blockchain Smartphone |
| Bancor | \$153 million | 12/6/17 | Prediction Markets |
| The DAO | \$152 million | 05/01/17 - 05/28/17 | Decentralized VC |

*Source.* https://www.bitcoinmarketjournal.com/biggest-icos/.
*Note.* IoT, Internet of Things; VC, Venture Capital.

**Figure 3.** (Color online) Capital Raised via ICOs




*Source.* https://cointelegraph.com/news/from-2-9-billion-in-a-month-to-hundreds-dead-trends-of-the-rollercoaster-ico-market-in-18-months.
*Note.* AR, Augmented Reality; VR, Virtual Reality.



marketplace in which consumers and producers can exchange the good with fewer transactions costs.

We will first model the exchange of the underlying good and associated transaction costs before the firm creates its platform. Then, we explore two alternative forms of financing the firm's platform project—"traditional" financing (selling rights to future income from transaction fees) and an ICO of utility tokens. Under the ICO, the proceeds from sale of the tokens act as both the capital to invest in the project and the revenue from the project itself. In Sections 3.6 and 3.7, we model the price of tokens issued in the ICO and demonstrate the paradox that is the main insight of this paper. Finally, we compare the two financing models and their implications for equilibrium price and quantity of the underlying good.

### 3.1. Trade in the Underlying Good

Consider a marketplace for a good with many consumers and producers. Without loss of generality, we assume that each consumer buys just one unit of the good. This will help us relate quantity sold to token velocity. We assume that the supply side is competitive.[22]

We assume that, before our platform firm enters, trade in the preexisting marketplace entails some friction $F > 0$. This friction operates like a per-unit sales tax of $F$ would, except that proceeds are burned. This is our model of transactions costs. Let $(p_s(X^*(F,t)), p_d(X^*(F,t)), X^*(F,t))$ be equilibrium price producers receive, the equilibrium price consumers pay, and the amount consumers buy, respectively, in equilibrium in that marketplace at time $t$. Subscripts $d$ and $s$ indicate inverse demand and supply functions, respectively. Because trade in the underlying good is competitive and $F$ operates like a tax, $p_d(X^*(F,t)) = p_s(X^*(F,t)) + F$. Because it is not essential to our basic economic insight, we make Assumption 1.

**Assumption 1.** *Supply and demand curves are constant over time.*

This allows us to suppress the dependence of prices and quantity on $t$.

**Example 1.** Let us explore an example with linear demand and supply to be able to relate equilibrium values more transparently to the friction. Suppose that the demand curve is $X_d = a_0 - a_1 p_d$ and that the supply curve is $X_s = b_0 + b_1 p_s$ for all $t$. Equilibrium price and quantity with friction $F$ are found by setting $a_0 - a_1(p + F) = b_0 + b_1 p$. This yields an equilibrium producer price and quantity of

$$p_s(X^*(F)) = \frac{a_0 - b_0 - a_1 F}{a_1 + b_1} \qquad X^*(F) = \frac{a_1 b_0 + a_0 b_1 - a_1 b_1 F}{a_1 + b_1}. \tag{1}$$

Consumers face a price of $p_d(X^*(F)) = p_s(X^*(F)) + F$. The elasticity of equilibrium quantity with respect to friction is

$$\eta_{X^*F} = \frac{a_1 b_1 F}{a_1 b_0 + a_0 b_1 - a_1 b_1 F}, \tag{2}$$

which is increasing in frictions.

### 3.2. The Firm Offering a Market Platform

Assume that there is a monopolist firm[23] that has a technology that can reduce frictions in the exchange

of the underlying good. We assume that the technology can lower frictions to $f < F$.

To implement the technology, we assume the firm needs to pay a fixed cost of $I$ and that marginal cost of operating the marketplace is zero. Our assumption about marginal cost can be relaxed, again without affecting the qualitative results. This fixed cost will need to be financed, a topic we address later.

Importantly, we have not specified whether the platform technology (i.e., the underlying project that needs to be financed) employs blockchain or something else. The only substantive assumption we make about the platform technology is Assumption 2.

**Assumption 2.** *The cost of implementing that underlying project is the same regardless of what financing and revenue model the firm chooses.*

This assumption is not completely innocuous. The ubiquity of cash and credit card payment systems that would be used for transaction fees under the traditional financing model may result in fewer setup costs than a blockchain ledger for a utility token, especially where the underlying project itself is not based on blockchain technology. Additionally, firms opting to finance via an ICO may choose to utilize an existing blockchain like Ethereum (using an ERC-20 token).[24] In this case, the firm sacrifices control over the consensus protocol (a choice that we show is key to the success of an ICO) for reduced setup costs. Although our model does not account for this option, it does highlight that choosing an off-the-shelf consensus protocol entails its own costs that firms must weigh against the decreased setup costs.

### 3.3. Traditional Financing with Transaction Fees

We model two forms of finance for the platform-supplying firm. One form is to sell rights to future revenue, which is raised by a transaction fee, $k$, on each unit traded.[25] The other is to issue and sell utility tokens prior to implementing the project using a fraction of the proceeds as finance. Note that in our model, the means of financing and of gaining revenue are linked. Here, we consider the traditional finance with fee model. We assume that the fee is constant over time to simplify the analysis.

A transaction fee must be less than or equal to $F - f$; otherwise, consumers and producers will not use the firm's platform. The fee operates like a tax on transactions that increases the price that consumers pay and decreases equilibrium quantity to $p_d(X^*(f+k,t))$ and $X^*(f+k,t)$, respectively, where $p_d(X^*(F,t)) \geq p_d(X^*(f+k,t)) > p_d(X^*(f,t))$ and $X^*(F,t) \leq X^*(f+k,t) < X^*(f,t)$. The incidence of the fee and the reduction in trade depends on the elasticities of the demand and supply curve, as per usual tax incidence equations. The present value of total revenue is

$$k\int_0^\infty e^{-\delta t}X(f+k,t)dt,$$

where $\delta$ is the interest rate.

Following Assumption 1, we focus on the special case where demand is stable over time (i.e., $X(z,t) = X(z)$ for all $t$). Allowing demand to shift over time complicates the analysis in a manner that obscures the basic economics of raising revenue via transaction fees or sale of utility tokens. In this special case, the present value of total revenues from fees is

$$\left(\frac{k}{\delta}\right)X(f+k).$$

Recall that the firm needs to finance $I$. If the firm charges a fee, it can sell—in advance—rights to some of the stream of income from that fee to investors in return for capital to cover $I$. Let $\phi^{TF}$ be the fraction of transaction fee revenue sold to investors. The financing constraint is

$$\phi^{TF}\left(\frac{k}{\delta}\right)X(f+k) \geq I. \tag{3}$$

This constraint will always just bind as the firm has no reason to raise more capital than is required to launch the platform.

The firm's objective is to maximize profit from the fee subject to the constraint that it raises enough capital to fund implementation of the platform and does not drive away market participants. Assuming that the financing Constraint (3) just binds, the firm's problem can be written

$$\max_k (1-\phi^{TF})\left(\frac{k}{\delta}\right)X(f+k) \tag{4}$$

subject to

$$f + k \leq F. \tag{5}$$

Assuming that there is an internal solution, the optimal fee satisfies the condition that the elasticity of equilibrium quantity (not the demand curve) with respect to the fee $\eta_{x^*k}$ is equal to one:

$$X^*(f+k^*) = -k^*\frac{\partial X^*(f+k^*)}{\partial k^*} \leftrightarrow \eta_{X^*k}(f+k^*) = 1. \tag{6}$$

Intuitively, raising the fee by 1% increases revenue per transaction by 1% but also, decreases the number of transactions. The optimal fee balances those effects (i.e., sets the elasticity of the transaction effect equal to one).

If, at the $k^*$ that ensures that equilibrium quantity elasticity (with respect to $k$) is one, the firm cannot raise enough revenue to cover $I$, even after selling the rights to all fees (i.e., $\phi^{TF} = 1$), then the transaction fee model is not a viable revenue model because it cannot

finance the required start-up investment. If, at the $k^*$ that satisfies the condition that the market participation Constraint (5) binds, we have $k^* = F - f$.

**Example 2.** Suppose that demand and supply are linear as in Example 1. Using the market-clearing conditions from that example, the first-order condition for the firm's problem, assuming the financing constraint binds but the market participation constraint does not, is

$$k^* = \frac{1}{2}\left(\frac{a_0}{a_1} + \frac{b_0}{b_1} - f\right). \tag{7}$$

The optimal fee decreases as platform frictions rise.

### 3.4. Financing with Utility Token ICO

The second way for the platform firm to finance the project and earn revenue is to mint tokens, to require that all trade on the platform takes place in tokens, and to sell some or all of those tokens. This type of token is called a "utility token."[26] Because the tokens are required for trade, they may have value as a medium of exchange, a topic we consider in the next section. If tokens have value, the firm can allocate some of the minted tokens to itself and sell them for dollars. To focus on the nub of the problem (i.e., that choice of technology for the utility token ledger), we make Assumption 3.

**Assumption 3.** *The firm mints only $M$ tokens, and the firm chooses the technology for maintaining the blockchain ledger for utility tokens once and for all at the start of the project.*

Assuming that trade in tokens implies frictions $z$ in the trade of the underlying good,[27] the total value of tokens is $P(z,t)M$ at time $t$, where $P(z, t)$ is the price of a token at time $t$ given trading frictions $z$.

As with the traditional finance model, we will assume that both frictions are because of the requirement that consumers use utility tokens and consumer demand for the underlying good is stable. This will allow us to ignore questions such as when the firm should sell the tokens it has allocated to itself. These questions do not shed light on the core trade-offs between raising revenue with fees versus utility tokens. Indeed, we can assume that the platform firm sells all its tokens at $t = 0$ (i.e., at an ICO with some fraction $\phi^{UT}$ of the proceeds going toward financing $I$). The remaining proceeds can be considered as revenue. Going forward, therefore, we shall also suppress the dependence of price on time (i.e., we shall write $P(z,t) = P(z)$).

Note that, even if the firm requires a utility token be used to purchase the underlying good, the price of the good is set in dollars rather than tokens. Define $r(z)$ as the token-denominated price of the good. If $P(z)$ is the dollar value of a token, then $r(z)P(z)$ is the dollar price of the good to consumers. If $r(z)P(z) > p_d(X^*(z))$, the price of the good with friction $z$, producers will profitably lower their prices. If $r(z)P(z) < p_d(X^*(z))$, consumers will bid up the price to $p_d(X^*(z))$. (If there were no frictions in this model, the result would be obtained from a simple no-arbitrage condition.) Thus, we conclude that

$$r(z) = p_d(X^*(z))/P(z),$$

consistent with the main finding of Catalini and Gans (2018) regarding the setting of token-denominated prices.

The issuance of tokens is not without cost. Because utility tokens are issued on the blockchain, they entail a cost that depends on the consensus protocol. For example, with PoW, miners will have to expend energy to validate trades with tokens; consumers and producers will have to compensate miners for that electricity expenditure. With PoS, miners may have to stake (and thus, forego use of) tokens for some time to obtain the right to validate trades; they will have to be compensated for at least the time value of their staked money.

The key choice for a firm hoping to issue utility tokens is what consensus protocol (i.e., technology) to use. This can be parameterized as a choice over the variables $s$, which is the time for validating a transaction on the blockchain, and $\theta$, which are features of the technology other than $s$. Choice of time affects miner compensation according to $d(s,\theta)$, where $\partial d(s,\theta)/\partial s \geq 0$ because more time to validate a block means either more energy under PoW (with more complex problems for mining computers to solve) or more time tokens are staked under PoS.[28] To allow us to invert $d(s,\theta)$ for expositional convenience, we shall assume that $d$ is strictly monotonic in $s$. Technology features $\theta$ can change the compensation required for any given validation time.[29]

Miner compensation functions like the transaction fee in the previous revenue model, except that the proceeds go to miners rather than the platform firm.[30] Miner compensation, therefore, raises the friction to trade from $f$ to $f + d(s,\theta)$. Just as greater fees increase consumer price and lower quantity in equilibrium, so too does greater compensation.

**Assumption 4.** *Without loss of generality, we assume* $d(0,\theta) = 0$.

If miner costs are positive even when validation time is zero, we can simply fold that into frictions $f$ when determining optimal technological choice under the utility token model. These miner costs would affect comparison of traditional financing and ICO financing but are not relevant to the basic economic difference between the two models, so we ignore them.

Critical to our analysis is the inverse relationship between validation time per transaction $s$ and the velocity of tokens, defined as the number of transactions of a given token in a period of time. Specifically,

$$V(s) = 1/s.$$

Velocity falls in the time required for validation. Moreover, as validation time goes to zero,[31] velocity becomes infinite.[32]

### 3.5. Pricing Utility Tokens with the Equation of Exchange

In order to derive the firm's optimal token policy, we need to price tokens. To do that, we use Fisher's equation of exchange, which in this context, says that the equilibrium price of a token is that which equates the demand and supply of that token.

Under the utility token ICO financing model, the underlying good must be purchased with tokens. Thus, the demand for tokens at a given point in time is, in dollar terms, equal to total consumer expenditure, $D = p_d(X^*(f+d))X^*(f+d)$.[33] (For readability, we have suppressed the dependence of $d$ on $s$ and $\theta$.)

The dollar-denominated supply of tokens $S$ is a product of the total stock of tokens minted and available for circulation and the velocity of those tokens, $V(s)$. Velocity (i.e., transactions per period) ensures that the units of supply are measured per period of time.

The equilibrium price that equates supply and demand for tokens in a period is

$$D = p_d(X^*(f+d))X^*(f+d) = PMV(s) = S \leftrightarrow P(d) = \frac{p_d(X^*(f+d))X^*(f+d)}{MV(s)}. \tag{8}$$

Token price is increasing in the value of transactions on the platform in a given period and decreasing in the effective supply of tokens on the market that period.

### 3.6. Frictionless Utility Tokens Have Zero Value

Here, we demonstrate a basic problem for utility tokens (and thereby, hint at a paradox for ICOs in the next section). If the firm chooses a consensus protocol for utility tokens that implicitly sets transaction time $s$ too low and thus, velocity too high, the token price will be zero.[34]

To see this, we make the dependency of miner compensation $d$ on validation time $s$ explicit and take the limit of token price $P$ as validation time $s$ goes to zero. From (8), this is

$$\lim_{s\to 0} P(d(s,\theta)) = \frac{1}{M}\cdot\frac{\lim_{s\to 0}[p_d(X^*(f+d(s,\theta)))X^*(f+d(s,\theta))]}{\lim_{s\to 0} V(s)}. \tag{9}$$

We already know the limit of revenue as frictions go to zero: $\lim_{s\to 0} p_d(X^*(f+d(s,\theta)))X^*(f+d(s,\theta)) = p_d(X^*(f))X^*(f) > 0$. The limit of velocity as friction goes to zero is infinity: $\lim_{s\to 0} V(s) = \lim_{s\to 0} 1/s = \infty$. With no friction, tokens can circulate an infinite number of times in any time interval. Together, these results imply that $\lim_{s\to 0} P = 0$.

### 3.7. Optimal Friction with Utility Tokens and the ICO Paradox

Assuming that the financing constraint binds (i.e., $\phi^{UT} p(d(s,\theta))M = I$), the firm's problem is to choose a quantity of tokens $M$ and validation time $s$ so as to maximize surplus funds raised beyond the required amount for financing (i.e., maximize revenue):

$$\max_{M,s}(1-\phi^{UT})P(d(s,\theta))M \tag{10}$$

subject to the market participation constraint

$$f + d(s,\theta) \le F \tag{11}$$

and the equation of exchange in (8). We do not worry about whether the firm maximizes token price now or at some future date $t$ because (a) token price is driven by demand for the underlying good and we assumed that (Assumption 1) demand is fixed over time and (b) we assumed (Assumption 3) that choice of consensus protocols is fixed at the start. Adding a dynamic choice of technology will not aid our intuition about the choice between financing models.

Plugging in the equation of exchange for $P$ reveals that $M$ cancels out. The choice of $M$ is arbitrary from an economic perspective; more tokens lower the per-token price to exactly compensate. Because $d(s,\theta)$ is assumed strongly (rather than merely weakly) monotonic in $s$, we can write validation time as a function of compensation: $s(d;\theta)$. Now, the objective function is

$$\max_{d}(1-\phi^{UT})\frac{p_d(X^*(f+d))X^*(f+d)}{V(s(d))}, \tag{12}$$

where we have suppressed the dependence of $d$ on $\theta$ for expositional ease.

If the financing and participation constraints do not bind, one can take logs of the objective function before maximizing and write the first-order condition as

$$\eta_{p_d X^*}(X^*(f+d^*))\eta_{X^* d}(f+d^*) + \eta_{Vd}(d^*) = \eta_{X^* d}(f+d^*). \tag{13}$$

Intuitively, the marginal benefits of higher miner compensation are an increase in the price consumers pay and a reduction in velocity, both of which increase token price both on the left-hand side. The marginal cost is lower equilibrium quantity purchased on the right-hand side. Optimal miner compensation (equivalently transaction time) balances these two.

The last equation illustrates the basic ICO paradox. If a firm wants to raise capital and revenue via an ICO, it needs to promise investors that their tokens will have positive value. It can generate some value by lowering friction from $F$ to $f + d$. However, if it tries to grow the market further by lowering $d$ (i.e., reducing frictions from utility token exchange), then it faces a headwind from token velocity. If the elasticity of the revenue effect ($\eta_{p_d}\eta_{X^*d} - \eta_{X^*d}$) is smaller than the elasticity of the latter velocity effect ($\eta_{Vd}$), then paradoxically, improving the efficiency of the utility token will decrease token price even as it increases trades on the platform. Whether this is the case is an empirical question that will vary by market, as it depends on the elasticity of equilibrium price and quantity for the underlying good, and the technology because it also depends on the relationship between validation time, miner compensation, and token velocity.

We can rearrange the expression to compare it with (6), the first-order condition for the traditional finance with transaction fee model:

$$\eta_{X^*d}(f + d^*) = \frac{\eta_{Vd}(d^*)}{1 - \eta_{p_dX^*}(X^*(f + d^*))}, \tag{14}$$

where $\eta_{ab}$ is the elasticity of $a$ with respect to $b$ and $p_d$ is the demand function for the underlying good.

There are two implications. First, the firm will set miner compensation where demand elasticity is less than one. Because the equilibrium quantity falls in the amount of transactions costs, the elasticity (which is customarily as a positive number) is on the left-hand side. For the right-hand side to correspondingly be positive, it must be that $\eta_{p_d} < 1$. Intuitively, if the firm increased miner compensation where demand elasticity was high, the loss from lower quantity would swamp the increased revenue from higher price.

Second, the utility token problem is more complicated than the traditional finance model, which simply sets the elasticity of equilibrium quantity with respect to the transaction fee equal to one. The firm has to have knowledge about consumer demand and technology.

**Example 3.** We derive optimal miner compensation assuming linear demand and supply. Equilibrium price and quantity are obtained from the formulas derived in Example 1 by replacing $F$ with $f + d^*$. We assume that miner fees are linear in validation time: $d = \theta s$, where $\theta > 0$. Together, this implies that total revenue under the ICO is

$$R_{UT} = P^*M = \frac{p_d^* X_d}{\theta / d^*} = \frac{d^*(a_0 - b_0 + b_1(f + d^*))(a_1 b_0 + a_0 b_1 - a_1 b_1^2(f + d^*))}{(a_1 + b_1)^2 \theta}.$$

Under our assumption about miner fees, $\eta_{Vd} = 1$. Using the first-order condition for $d^*$ under ICO financing, we find that $d^*$ is the solution to the following quadratic equation: $k_2(d^*)^2 + k_1 d^* + k_0 = 0$, where

$$k_2 = a_1 b_1^2$$
$$k_1 = 4a_1 b_0 b_1 - 2a_0 a_1 b_1 + a_0 a_1 b_1^2$$
$$k_0 = a_0 a_1 b_0 + a_0^2 b_1 - a_1 b_0^2 - a_0 b_0 b_1 + a_0 a_1 b_1 f + 2a_1 b_0 b_1 f + a_0 b_1^2 f - a_1 b_1 f^2.$$

### 3.8. Comparing Modes of Finance

We can compare the two financing models by comparing their objective functions (i.e., the present value of revenues associated with each). This represents a comparison of the upper bound with the amount of capital that can be raised for each mode of finance. The ratio of utility token (ICO financing) and transaction fee revenues (traditional financing) at any given level of transaction cost $f + w$ is

$$\frac{R^{UT}}{R^{TF}}(w) = \frac{p_d(X^*(f + w))X^*(f + w)}{V(s(w))} \frac{1}{wX^*(f + w)} = \frac{p_d(X^*(f + w))}{w} \frac{1}{V(s(w))}. \tag{15}$$

We use two observations to leverage this ratio to discriminate between the financing models. First, if we evaluate this ratio at the optimal transaction fee $w = k^*$ ($w = d^*$) and find that it is greater (less) than one, then ICO financing (traditional financing) must generate more revenue than the maximal revenue under traditional financing (ICO financing). Second, the ratio of revenue from ICO financing to traditional financing is decreasing in token velocity.

These observations lead to the following proposition, which suggests that the velocity of transactions determines which traditional financing is optimal.

**Proposition 1.** (a) *The utility token ICO model generates more revenue if* $V(s(k^*)) < p_d(X^*(f + k^*))/k^*$. (b) *The traditional financing with transaction fee model generates more revenue if* $V(s(d^*)) > p_d(X^*(f + d^*))/d^*$.

This implies that if velocity is sufficiently low, then the ICO model is preferable and vice versa.

Unsurprisingly, whether the firm chooses to pursue an ICO for financing depends critically on the consensus protocol the firm chooses. The ICO firm will want to search for an available protocol that lowers $\eta_{sd}$, the elasticity of validation time on miner compensation, as that reduces the ICO paradox. To see why, think of the ICO firm's problem as maximizing token price via choice of miner compensation. The ICO paradox is that lowering compensation to increase equilibrium revenue also increases velocity, lowering price. The

latter effect is driven by the fact that lower compensation means less validation time. This drag on token price is mitigated, however, if the firm chooses a technology where validation time is not responsive to miner compensation (i.e., low $\eta_{sd}$).

**Example 4.** Let us examine whether a firm facing linear supply and demand is better off with a fee or an ICO. To answer this questions, we again assume that miner fees are linear in validation time: $d = \theta s$, where $\theta > 0$. Plugging in revenue from each model into (15) yields

$$\frac{R^{UT}}{R^{TF}}(w) = \frac{a_0 - b_0 + b_1(f + w)}{\theta(a_1 + b_1)}.$$

Using the formula for $k^*$ from Example 2 and the proposition, we see that the ICO model will be superior if $X^*(f) < 2(a_0 - \theta a_1)$ (i.e., if quantity when there is no fee is sufficiently small). In that case, the return to the traditional financing with transaction fee model, where revenue is the fee times quantity, is low because quantity is low with no fee, and a fee only lowers quantity further.

We can use the formula for $d^*$ from Example 3 and the proposition to determine when the transaction fee model is superior. The formulas are complicated and offer no insight about $d^*$ levels. However, they do suggest that if

$$\theta > \frac{a_0 - b_0 + b_1(f + d^*(a_0, a_1, b_0, b_1, f))}{a_1 + b_1},$$

the transaction fee model is superior. We get this condition because $d^*$ does not depend on $\theta$. When $\theta$ is sufficiently large, although the price of tokens is higher, the quantity of sales is sufficiently suppressed that quantity of trade in the underlying good is very low, lowering the market cap of tokens.

## 4. Moving out the Technological Frontier

In this section, we examine ways to reduce the cost of using utility tokens to raise capital and thus, make it a more competitive way of raising capital relative to traditional methods. Specifically, we explore techniques to reduce velocity conditional on miner compensation. We do this assuming either that the firm has decided to finance its platform using an ICO rather than selling rights to revenues from transaction fees or that the firm might choose an ICO over traditional financing if it can increase the price of tokens. Of the three approaches we explore, only one—*burn and mint*—holds promise as a way to mitigate the paradox and increase the total amount raised via an ICO.

Before we proceed, it should be noted that the firm that does not utilize the same blockchain to reduce frictions to $f$ on its platform as it does for its ICO could always raise ICO token value by lowering $f$ further. In other words, the ICO paradox pertains to attempts to raise revenue by lowering the frictions associated with utility tokens, not necessarily the platform generally.

### 4.1. Tokenize Transaction Fees

One possible approach is to pursue the transaction fee model but to tokenize the fee. Specifically, the firm can require that the fee be paid not in dollars but in newly created tokens.

Before we explain why this will not work, one should ask why the firm would want to tokenize the fee rather than collecting it directly in dollars. It is not obvious that the issues of trust or costs that typically motivate the use of blockchain based ledgers over centralized ones apply in the context of collecting fees. Moreover, tokenizing fees will actually increase overall fees because validating the payment of the fee via a blockchain would require compensating miners. Finally, tokenizing the transaction fee means the firm is selling a right to the fee rather than a right to the full price of the underlying good. This lowers the overall amount of funds that can be raised by selling tokens.

Even ignoring these issues, tokenizing fees may exacerbate the negative relationship between lower miner compensation and higher velocity. The price of a token that must be used to pay the transaction fee is

$$P = \frac{fX^*(f + k + d(k))}{MV(d(k))}, \tag{16}$$

where $d(k)$ is the compensation required to induce miners to validate fee payment $k$ made in tokens. As before, lower miner compensation increases velocity. Before, the compensating benefit was that the numerator would rise because lower miner payment would increase both equilibrium good price and quantity. Now, however, the benefit is smaller because the numerator only includes equilibrium quantity, not price.

The benefit of lowering miner compensation would be greater if the transaction fee was a percentage of the equilibrium good price. However, even then, this change would simply move the firm closer to the case where it tokenized payment for the good. It would not obviously improve the firm's position relative to that case.

### 4.2. Work Token: Requiring Miners to Hold Utility Tokens

A second approach is that the firm uses PoS and requires miners to stake tokens that are used for goods payments to earn the right to write the next block (Samani 2018). A number of existing projects, including Augur (a prediction market),[35] Keep (off-chain private data storage),[36] Livepeer (video services marketplace),[37] Truebit (off-chain computation),[38] and

Gems (decentralized mechanical Turk),[39] use this work token tactic.

To a large extent, the existing model already captures this approach to lowering the ratio of transactions costs to velocity. As we pointed out in Section 2.2, PoS lowers transactions costs relative to PoW. Whether it offers a better ratio of miner costs to velocity is uncertain. The ratio depends on the duration of time that miners must stake tokens, which is an open variable. In any case, PoS does not escape the negative relationship between miner compensation and velocity because miner compensation and velocity are both driven (although in opposite directions) by the amount of time miners have to stake their tokens. The longer a miner must stake tokens, the larger the compensation she will demand because of the time value of money. However, the longer the time tokens must be staked, the fewer tokens are available for transacting, thus reducing velocity. Fanti et al. (2019) examine how this requirement to hold tokens affects token price using the equation of exchange.[40]

A variant of standard work tokens is to create two tokens, one to pay for the underlying good and the other that miners must stake to obtain the right to record the next block. The reward that the winning miner gets is paid in the first token, the one used to buy the underlying good. The ICO would focus on sale of the miner token. This modification is similar to tokenization of the transaction fees and does not obviously improve matters.

### 4.3. Burn and Mint: Platform Holds Tokens Between Transactions

A final and more promising approach to improving the value of utility tokens is to destroy utility tokens that are used to pay for the underlying good and remint them after some delay (Lau 2018, Samani 2018). Projects, such as Factom[41] and Gnosis/Spankchain (platform for adult entertainment videos),[42] use this burn and mint tactic.

The key value of burn and mint is that introducing a delay between the use of a token to purchase a good and the time it is reintroduced to the market functionally increases validation time but does not require an increase in miner compensation because the network holds the token from the market *after* the miner has been paid. In other words, it lowers the denominator of (8) without affecting the numerator.

## 5. Conclusion

This paper has examined the economic choice between traditional financing with a transaction-fee revenue model and an ICO of a utility token for a marketplace (which is equivalent to a markup versus utility token for a product supplier). We characterized the optimal fee and revenue from the transaction-fee model and showed that the comparative value of an ICO as a mode of financing depends on the friction in the underlying blockchain technology used to track tokens. In the process of doing so, we illustrated the ICO paradox or velocity problem; lowering the costs of operating the blockchain ledger too far actually reduces the price of individual tokens and thus, the value of an ICO of utility tokens.

We compared the two models and demonstrated that the choice of finance depends on the extent of frictions and the amount of trade on the marketplace. Specifically, too high a level of frictions makes an ICO inferior. This suggests that for an ICO to work, blockchain frictions can be neither too low nor too high. Moreover, if the price of products sold on the marketplace is too high and thus, the quantity of trade on the marketplace is too low, traditional financing is inferior.

Finally, we examined different types of blockchain consensus protocols that would allow a firm to better control frictions and thus, optimize the market capitalization of all tokens. We showed that tokenizing transaction fees exacerbates the negative relationship between lower miner compensation and higher velocity, whereas the work token model is just a variant of PoS and does not solve the velocity problem. A more promising option is burn and mint, which allows the firm to directly control velocity without affecting miner compensation. This decoupling allows the miner fee to stay low so as to support the quantity of trade but the velocity to be low to support the token price.

There are limitations to our model. Notably, we assumed that demand is constant, which allowed us to sidestep issues such as the timing of sale. We leave it to future work to relax these assumptions. In practice, firms that conduct ICOs with utility tokens face difficult decisions on whether and when to hold tokens or liquidate them. Because token prices can vary, these choices can dramatically affect the purchasing power of capital raised.

We also gloss over the connection between financing and the accompanying revenue model. As we mentioned, there are many ways to finance a project. Although utility token models are naturally connected to ICOs, it is theoretically possible to issue such tokens, put them in a vehicle, and then, sell equity in that vehicle. Likewise, one could take IOUs from a transaction fee model, create an asset-backed token, and then, conduct an ICO for that token. There may also be important tax implications connected to this decision. We leave it to future economic and legal research to consider these topics.

The conclusions we draw, as well as this future research, have important implications for management strategy. They directly affect decisions about revenue generation and financial structure. They might also indirectly affect choices over blockchain technology,

which impact finance and revenue. Finally, the amount of revenue that firms receive and capital they have access to will affect a litany of other decisions the firm makes, including marketing and technology adoption.

## Acknowledgments

Th authors thank Zhiguo He and Stacy Rosenbaum for helpful comments. Chris Burnitt and D. J. Thornton provided exceptional research assistance.

## Appendix. Modeling the Supplier of a Good

In the main text, we model a firm that is a monopoly provider of a platform for the sale of a good. In this appendix, we show that model is nearly isomorphic with a model of a monopolistic firm that directly supplies a good (rather than a platform for the sale of that good). We also examine the case of a competitive supplier, which also maps onto a model of a competitive platform.

### A Monopolistic Supplier

We first consider a firm that is a monopolistic supplier of a good. We assume that there is some cost $F$ to selling the good for cash or credit card payments. For example, cash may be hard to transport and keep secure, and credit cards may charge a fee. Moreover, we assume that selling the good via a new technology, such as blockchain, reduces costs to $f < F$. Let $(p_s(X^*(F)), p_d(X^*(F)), X^*(F))$ now be the equilibrium price producers receive, the equilibrium price consumers pay, and the amount consumers buy, respectively, in a monopolistic market if the firm was not to use, for example, blockchain to sell its good.

If the firm was to use the new technology but use a transaction fee revenue model to make revenue and sell a portion of those fees to raise capital for investment, then its maximization problem would look just like that in (4) subject to the financing Constraint (3) and the market participation Constraint (5). Assuming no corner solution, the optimal fee $k^*$ is given by (6). If the firm was to use utility tokens to raise revenue, its maximization problem would be the same as in (12) subject to the financing constraint $\phi^{UT} PS \geq I$. Assuming there is no corner solution, (14) defines the optimal miner compensation $s^*$. Given this, we can use the analysis in Section 3.8 to compare the merits of the two revenue models.

### A Competitive Supplier

Now, consider a firm that supplies a good in a competitive market. Define $F$ and $f$ as in the last section. Let $(p_s(X^*(F)), p_d(X^*(F)), X^*(F))$ now be the equilibrium price producers receive, the equilibrium price consumers pay, and the amount consumers buy, respectively, in a competitive market if the firm was not to use, for example, blockchain to sell its good.

We first examine the optimal fee in a transaction fee revenue model. We can think of $F - f$ as the firm's cost advantage relative to other competing firms. Because this market is competitive, the firm can charge a fee equal to $k^* = F - f$ without losing market share. In other words, we would get the same fee as the corner solution to the maximization problem in (4) subject to the constraints in (3) and (5) if the market participation Constraint (5) was binding. Although a monopolistic supplier such as that in the previous section may sell the good at a higher price, it absorbs some of the burden of the selling fee, whether it is $F$ or $f$, depending on the firm's technology. By contrast, the competitive firm passes that fee on entirely.

If the firm employs a utility token ICO financing model, its maximization problem would be the same as in (12) subject to the financing constraint $\phi^{UT} pS \geq I$. Assuming there is no corner solution, (14) defines the optimal miner compensation $d^*$. Recall that, whereas the transaction fee model imposes a fee $k^* = F - f$ on top of $f$ so that the consumer faces the competitive price, the utility token ICO model imposes a miner compensation cost $d$ on top of $f$. If $d$ is less than $F - f$, the firm can raise $d$ without losing any sales. Moreover, because higher $d$ is achieved by increasing the validation time $s$ and because increasing $s$ lowers $V(s)$ and thereby, increases the price of tokens under the equation of exchange (8), the firm's optimal strategy is to set $d = d^*$ such that $d^* = F - f$. This implies a token price of $p_s(X^*(F))X^*(F)/V(s^*)$.

To compare the two financing models in the competitive supplier case, we now need to compare revenue from the transaction fee model, $(F - f)X^*(F)$, with revenue from the utility token model, $p_d(X^*(F))X^*(F)/V(s^*)$. The transaction fee model raises more revenue if $(F - f)/p_d(X^*(F)) > s^*$ (i.e., the cost advantage or markup as a percentage of price is greater than the time required for each transaction (one over velocity)). Let $\tilde{s}$ be the validation time that ensures $F - f = p_d(X^*(F))/V(\tilde{s})$. If the optimal $s^*$ in the utility token model is greater than $\tilde{s}$, then the utility token model is better because $V'(s) < 0$, so

$$p_d(X^*(F))/V(s^*) > p_d(X^*(F))/V(\tilde{s}) = F - f.$$

That is, if validation technology is sufficiently good that, to increase miner compensation to eat up the firm's cost advantage decreases velocity a lot, then the utility model is worthwhile.

## Endnotes

[1] For example, Unlock protocol (https://unlock-protocol.com/) sells NFTs that provide ad-free versions of the Forbes website.

[2] ICOs involving utility tokens are sometimes called utility coin offerings.

[3] See also Gibbons et al. (2012) for a related rational expectations equilibrium model for goods markets and organizations.

[4] See also blog posts by Pfeffer (2017), Selkis (2018), and Xu (2018). Samani (2017) expands on the use of Fisher's equation to describe the velocity problem, and Locklin (2018) points out some errors in Samani's formulas. Locklin's criticisms do not apply to our model because we assume that all consumers and producers are homogeneous.

[5] The work closest in spirit to ours is a blog post by Evans (2018), which provides a simulation involving the sale of tokens used to purchase a good. It is not accompanied by a general model about the sale or market in the underlying good.

[6] Nothing stops consumers or the firm from using an existing digital currency blockchain, such as Bitcoin, to send or receive this fee. We ignore that option because it is orthogonal to the core economic question of whether the firm should issue utility tokens to raise revenue and capital.

[7] Examples include Telegram's attempted ICO (https://bitcoinist.com/telegram-crypto-exchange-liquid-ico-gram/) and Nagritech (https://nagricoin.io/).

[8] As of March 22, 2021, the market capitalization of Bitcoin was roughly U.S. $1 trillion. The next closest blockchain token is Ethereum, valued at around $200 billion. See https://coinmarketcap.com/.

[9] There are a number of other blockchains that already use PoS, including Peercoin, Decred, Neo, Navvcoin, Reddcoin, PivX, Tendermint, and Dash.

[10] Often, blockchains are called trustless rather than trustworthy. This is not because they are not trustworthy but because they do not require trust in a central authority.

[11] There are consensus protocols that have miners solve socially useful computational problems so as to reduce the social costs of PoW-style mining. These include proof of exercise (Shoker 2017) and proof of useful work (Ball et al. 2017). However, these alternatives do not change the private costs of mining.

[12] See discussion of Casper at https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs.

[13] Here, we provide a description of a simpler version of PoS than that which Ethereum employs. Ethereum actually employs a Byzantine fault-tolerant version that resembles delegated PoS. See https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQs for a more complete description of Ethereum's implementation of PoS.

[14] As of March 22, 2021, the market capitalization of Ethereum is about U.S. $200 billion, requiring control of at least $100 billion worth of Ether to launch a 51% attack. See https://coinmarketcap.com/.

[15] See "What about capital lockup costs?" at https://eth.wiki/en/concepts/proof-of-stake-faqs.

[16] For a more thorough microfounding of miner behavior, see Ma et al. (2018). Note, however, that in faithfully modeling the Bitcoin protocol, their model does not hold important factors constant, such as security of the network (represented by the amount of computational power, 51% of which is required to cheat the network).

[17] This discussion suggests that miner compensation is fixed purely by technology. Depending on the consensus protocol and the rule of the platform, it can also be driven by demand for transactions. If consumers can compete for access to miners to record transactions, then the choice of consensus protocol and the parameters chosen—difficulty level and escrow time—can be thought of as determining the supply curve for mining. For a given demand curve for transactions, the intersection of the supply and demand determines an equilibrium transaction cost. When the demand curve shifts out, however, miner compensation may rise if the protocol and platform permit it. This will be reflected in the transaction fee. The platform changes the parameters of the consensus protocol (e.g., increasing difficulty level) that will shift the supply curve. If the supply curve shifts in, then again, miner compensation will rise. This equilibrium model of miner compensation does not change the basic economics. Technological parameters in the consensus protocol that shift out supply will tend to reduce miner compensation and thus, increase the number of transactions per period conditional on a given demand curve for transactions, increasing velocity.

[18] See https://filecoin.io/.

[19] See http://agenusbio.com/wp-content/uploads/2019/02/BEST-FINAL.pdf.

[20] See https://filecoin.io/, https://golem.network/, and https://basicattentiontoken.org/.

[21] J. R. Willet is credited with the idea of an ICO. He conducted the very first ICO for Mastercoin in 2014. See https://www.forbes.com/sites/laurashin/2017/09/21/heres-the-man-who-created-icos-and-this-is-the-new-token-hes-backing/#563df1731183.

[22] If the supply side for the good is monopolistic, the firm that provides the marketplace likely would be bought by the sole supplier of the good, and this model would look like a good supplier that conducts an ICO. We leave that model for the appendix.

[23] If the platform market was competitive, the analysis would look like that for the competitive supplier, which we discuss briefly in the appendix. Applying that discussion to platforms would reveal that, because platforms are competitive, the transaction fees they can charge would be driven by the market price of the platforms rather than the sort of optimization in Section 3.3.

[24] This is a popular choice for ICOs. Howell et al. (2019) find that 73% of ICOs in their study used ERC-20 tokens.

[25] Alternatively, one could model the firm as choosing a fee that is a percentage $\pi$ of the good price, in which case, for example, $k = \pi p_s(f)$. We believe that our simpler model yields qualitatively the same insight into revenue generation and financing.

[26] This can be done on the firm's own blockchain or on, for example, Ethereum blockchain using an ERC-20 token. Although not presently important, our results will show that choosing an existing blockchain will likely entail its own cost because of the lack of control over the consensus protocol.

[27] This includes $f$ and frictions added by the trade in tokens.

[28] For example, the firm could decrease $s$ by increasing the block size. This allows more transactions per block. That means that in any given time period required to validate the block, there are more transactions validated. Because miner compensation is keyed to time rather than number of transactions, the amount of miner compensation per transaction would decrease.

[29] For example, if the monetary policy requires voluntary transaction fees and consumers and producers offer transaction fees for token trade validation that are proportional to token price, then an increase in the price of token will increase transaction fees, even though it has no effect on the time to validation.

[30] It does not qualitatively make a difference if the platform actually used utility tokens to reduce frictions $f$ and not just $d$. In that case, we would replace $f$ with $d$. Whether the firm uses utility tokens to reduce frictions $f$ or not, we will show that the firm must introduce frictions in the trade of utility tokens to ensure a positive price for tokens. When the firm uses utility tokens to reduce frictions, that just means the firm has to raise frictions $f$ above zero if they use utility tokens to earn revenue.

[31] This can be illustrated with a simple thought experiment. The case where $s$ is zero is akin to the case where any given interval of time $t$ can be divided into infinite subintervals and each token is traded once in each subinterval. Suppose the equilibrium quantity consumed and price (for consumers) at time $t$ is $(X, p_d)$. As we shall show, $r = (p_d + d(s))/P$ is the price per unit of good denominated in tokens. The total number of token trades required to purchase $X$ units of the good in interval $t$ is then $2 \cdot rX$. In the first $2 \cdot rX/M$ subintervals, let market participants use the available $M$ tokens to complete all trades required for purchasing goods. In each remaining subinterval, let the producers, who hold all tokens after selling goods, exchange each token twice among themselves so that each producer holds the same number of tokens that they received from consumers. Because there are infinite numbers of subintervals, there are infinite numbers of trades per token at $t$ (i.e., velocity is infinite).

[32] Note that in our model, there is no scope for holding tokens for the purpose of speculation because token price is constant over time. In reality, holding of tokens would result in longer times between when a token is received and next spent on average, thus affecting how much the firm can actually control velocity. Let $h(s)$

be average holding time, which may vary with validation time. Then, velocity will be given by $V(s) = 1/(h(s) + s)$. As long as $h(s)$ is nondecreasing in $s$ (i.e., investors do not hold longer tokens that have shorter validation times), the analysis will be substantively the same. If $h(0) > 0$, then the limit analysis in Section 3.6 no longer applies directly as it effectively puts an upper bound on velocity, but the intuition at the core of the ICO paradox presented in Section 3.7 remains unchanged.

[33] We assume miners are paid in tokens as well, as is often the case.

[34] As discussed in a previous footnote, if average holding time of a token is always positive (say, because owners of the token expect the price of the token to rise), then this result does not hold because $\lim_{s\to 0} V(s) = \lim_{s\to 0} 1/(h(s) + s) = 1/(h(0))$, where $h(0) > 0$. Importantly, however, the trade-off at the heart of the ICO paradox discussed in Section 3.7 remains applicable.

[35] See https://www.augur.net/.

[36] See https://keep.network/.

[37] See https://livepeer.org/.

[38] See https://truebit.io/.

[39] See https://expand.org/.

[40] In theory, PoW could use a similar tactic as work tokens in PoS. The firm would pay miners in tokens but require that those tokens be held in escrow for some period of time, taking them out of circulation. However, the longer this periodis, the more miners will have to be compensated because of the time value of money.

[41] Factom pioneered burn and mint. See https://accumulatenetwork.io/?utm_source=next.36kr.com.

[42] See https://www.spankstream.com/. See Lau (2018) for differences between Factom and the Gnosis/Spankchain implementations of burn and mint.

## References

Ball M, Rosen A, Sabin M, Vasudevan PN (2017) Proofs of useful work. IACR Cryptology ePrint Archive, 2017:203.

Benedetti H, Kostovetsky L (2018) Digital tulips? Returns to investors in initial coin offerings. Returns to Investors in Initial Coin Offerings (May 20, 2018).

Bocks K, Haas C, Heyden T (2019) A theory on pre-ICO venture capital involvement. Preprint, submitted January, https://doi.org/10.2139/ssrn.3402623.

Buterin V (2017) On medium-of-exchange token valuations. Accessed February 17, 2022, https://vitalik.ca/general/2017/10/17/moe.html.

Canidio A (2018) Financial incentives for open source development: The case of blockchain.

Catalini C, Gans JS (2018) Initial coin offerings and the value of crypto tokens. NBER Working Paper No. 24418, National Bureau of Economic Research, Cambridge, MA.

Chod J, Lyandres E (2018) A theory of ICOs: Diversification, agency, and information asymmetry. Agency and Information Asymmetry (July 18, 2018).

Cong LW, He Z, Li J (2018) Decentralized mining in centralized pools.

Davydiuk T, Gupta D, Rosen S (2019) De-crypto-ing signals in initial coin offerings: Evidence of rational token retention. Preprint, submitted Decenver 6, 2018, https://ssrn.com/abstract=3286835.

Dittmar RF, Wu DA (2018) Returns to initial coin offerings: An empirical examination. Preprint, submitted November 14, https://ssrn.com/abstract=3259182.

Evans A (2018) On value, velocity and monetary theory: A new approach to cryptoasset valuations. Accessed February 17, 2022, https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f.

Fanti G, Kogan L, Viswanath P (2019) Economics of proof-of-stake payment systems.

Fisher I (1912) *The Purchasing Power of Money: Its Determination and Relation to Credit Interest and Crises* (The MacMillan Company, New York).

Garratt R, van Oordt MRC (2021) Entrepreneurial incentives and the role of initial coin offerings. *J. Econom. Dynamics Control*, ePub ahead of print June 12, https://doi.org/10.1016/j.jedc.2021.104171.

Gibbons R, Holden R, Powell M (2012) Organization and information: Firms' governance choices in rational-expectations equilibrium. *Quart. J. Econom.* 127(4):1813–1841.

Grossman SJ, Stiglitz JE (1976) Information and competitive price systems. *Amer. Econom. Rev.* 66(2):246–253.

Grossman SJ, Stiglitz JE (1980) On the impossibility of informationally efficient markets. *Amer. Econom. Rev.* 70(3):393–408.

Howell ST, Niessner M, Yermack D (2019) Initial coin offerings: Financing growth with cryptocurrency token sales. *Rev. Financial Stud.* 33(9):3925–3974.

Hu AS, Parlour CA, Rajan U (2019) Cryptocurrencies: Stylized facts on a new investible instrument. *Financial Management* 48(4):1049–1068.

Lau W (2018) On the velocity problem for cryptoasset value. *Medium* (February 23), https://medium.com/thoughtchains/on-the-velocity-problem-for-cryptoasset-value-aad235694211.

Lee J, Parlour CA (2018) Crowdfunding, initial coin offerings, and consumer surplus. Preprint, submitted December 28, https://ssrn.com/abstract=3300297.

Li J, Mann W (2018) Initial coin offering and platform building. Preprint, submitted December 18, 2017, https://dx.doi.org/10.2139/ssrn.3088726.

Locklin S (2018) Token economics: Considering "token velocity." Accessed February 17, 2022, https://basicattentiontoken.org/token-economics-considering-token-velocity/token-econ_1.pdf.

Ma J, Gans JS, Tourky R (2018) Market structure in bitcoin mining. Preprint, submitted January 23, http://dx.doi.org/10.2139/ssrn.3103104.

Malinova K, Park A (2018) Tokenomics: When tokens beat equity. Preprint, submitted December 2, http://dx.doi.org/10.2139/ssrn.3286825.

Momtaz PP (2018) Initial coin offerings, asymmetric information, and loyal CEOs. Asymmetric information and loyal CEOs (July 12, 2018).

Moos M (2018) Analysis: Bitcoin costs $1.4 billion to 51% attack, consumes as much electricity as Morocco. *Cryptoslate* (November 29), https://cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/.

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system.

Pfeffer J (2017) An (institutional) investor's take on cryptoassets. Accessed February 17, 2022, https://s3.eu-west-2.amazonaws.com/john-pfeffer/An+Investor\%27s+Take+on+Cryptoassets+v6.pdf.

Samani K (2017) Understanding token velocity.

Samani K (2018) New models for utility tokens. *Medium* (February 13), https://medium.com/multicoin-capital/new-models-for-utility-tokens-d26c12ec00c5.

Selkis R (2018) 95 crypto theses for 2018. *Medium* (January 2), https://medium.com/@twobitidiot/95-crypto-theses-for-2018-ca7b74f8abcf.

Shoker A (2017) Sustainable blockchain through proof of exercise. *2017 IEEE 16th Internat. Sympos. Network Comput. Appl. (NCA)* (IEEE, Washington, DC), 1–9.

Sockin M, Xiong W (2018) A model of cryptocurrencies. Working paper, Princeton University, Princeton, NJ.

Xu K (2018) Not a velocity problem: My perspective on payment tokens. *Medium* (April 8), https://1kevinxu1.medium.com/not-a-velocity-problem-my-perspective-on-payment-tokens-9179120d5671.