Vanderbilt University Department of Economics Working Paper Series
Nashville, TN 37235-1819

Vanderbilt University Department of Economics Working Papers 17-00008

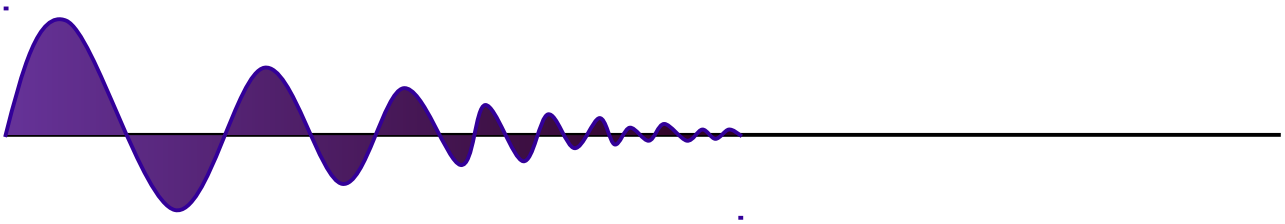
Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings

John P. Conley
Vanderbilt University

Abstract

Blockchain startups have embraced initial coin offerings (ICOs) as a vehicle to raise early capital. The crypto-tokens offered in these sales are intended to fill a widely varied set of roles on different platforms. Some tokens are similar to currencies, others are more like securities, and others have properties that are entirely new. Each company's technological vision calls for a token with unique properties and uses. The main point of this paper is that designing a successful token must take into account certain aspects of monetary theory, financial economics, and game theory. Failing to do so can put an otherwise excellent project at risk. We also explore what economics tells us about how to assess the value of tokens offered for sale, how startups should structure their ICOs, and what the implications of assigning various roles to tokens on a platform might be.

This paper was completed while the author was visiting researcher at Microsoft Research. I would like to thank Microsoft for their hospitality. The author takes sole responsibility for the content of this paper.
Citation: John P. Conley, (2017) "Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings", *Vanderbilt University Department of Economics Working Papers*, VUECON-17-00008.
Contact: John P. Conley - j.p.conley@vanderbilt.edu.
Submitted: June 06, 2017. **Published:** June 06, 2017.
URL:http://www.accessecon.com/Pubs/VUECON/VUECON-17-00008.pdf



Blockchain and the Economics of Crypto-tokens and Initial Coin Offerings[1]

John P. Conley[2]

Vanderbilt University

June 2017

Abstract

Blockchain startups have embraced initial coin offerings (ICOs) as a vehicle to raise early capital. The crypto-tokens offered in these sales are intended to fill a widely varied set of roles on different platforms. Some tokens are similar to currencies, others are more like securities, and others have properties that are entirely new. Each company's technological vision calls for a token with unique properties and uses. The main point of this paper is that designing a successful token must take into account certain aspects of monetary theory, financial economics, and game theory. Failing to do so can put an otherwise excellent project at risk. We also explore what economics tells us about how to assess the value of tokens offered for sale, how startups should structure their ICOs, and what the implications of assigning various roles to tokens on a platform might be.

1 This paper was completed while the author was visiting researcher at Microsoft Research. I would like to thank Microsoft for their hospitality. The author takes sole responsibility for the content of this paper.

2 j.p.conley@vanderbilt.edu.

John P. Conley
Department of Economics
Vanderbilt University
Nashville, TN, 37235

jpc@jpconley.com
http://jpconley.wordpress.com/

Introduction

Blockchains are distributed, append only ledgers, usually validated using some type of consensus mechanism. They can record time-stamped, digitally signed, records of any kind, and make them immutable. Blockchains can be configured to preserve the anonymity of its users, and if copies of the ledger are widely distributed, censuring the record is difficult. Neither access to, nor validation of, records in a blockchain require trust in the good behavior of any central authority.

One of the earliest uses of a blockchain was Bitcoin. Bitcoin's public ledger maintains a complete history of the ownership of every unit of the cryptocurrency ever created on the chain. In recent years, hundreds of startups have emerged that use blockchains in a variety new and innovative ways. Examples include facilitating bank settlements (Ripple), creating markets for unused computer resources (Golem and MaidSafe), and prediction and wagering platforms (Augur, Gnosis, and FirstBlood), among many others.

Although a few of these startups are simply providers of alternative cryptocurrencies, the great majority use blockchain technology to intermediate new markets or make existing markets more efficient. Nevertheless, most include native crypto-tokens that play a wide range of roles. These tokens often serve as an internal unit of account to keep track of services such as validation and block-writing that users provide to the platform. or to intermediate transactions between buyers and sellers in the markets that the platforms support. However, tokens are sometimes given more creative uses such as helping to prevent spamming on the chain, providing proof of stake, or giving token holders certain types of privileged access, rights to a share of specific revenue streams, or rights to participate in the platform's development.

Regardless of their functions on the platform, crypto-tokens have also turned out to be a very successful way for startups to raise early financing. Instead of going to the expense of making an initial public offering (IPO) of stock or the trouble of convincing a venture capitalist to back the company, blockchain companies have started to make initial coin offerings (ICOs).

The typical pattern is for a startup to produce a white paper that describes their business model and technical approach. The white paper includes details about the functions that the tokens issued

during the ICO will perform and the process of token creation. It is important that the number of tokens created is limited and that these limits are clearly spelled out. The simplest way is to commit to premining a fixed number tokens and then never issuing tokens again, but more complicated approaches are common as well. The tokens are then offered for sale in an auction, and the proceeds are used to fund the project. About $\$250M$ was raised through ICOs in 2016,[3] This is a significant fraction of the $\$1.4B$ estimated to have been invested in blockchain companies in total that year.[4]

The legal status of ICOs is unsettled at this point. If crypto-tokens are a form of currency, then the issuing startup may need to comply with know your customer (KYC) and anti-money laundering (AML) rules.[5] On the other hand, if they are a form of stock or security, startups must comply with certain securities and exchange commission (SEC) regulations.[6] Conforming to either set of requirements is complex and expensive, but failure to to do so can have serious repercussions. In addition, imposing the necessary controls often runs contrary to the philosophy of freedom, anonymity, and privacy that drives many of the people involved in blockchain companies,

Whether crypto-tokens are currencies, securities, or something new entirely new also affects how they should be viewed from an economic standpoint. Although there is a well-developed body of theory in monetary and financial economies, how this might be applied to crypto-tokens and ICOs is only beginning to be explored. At this point, there is not much economic guidance about how potential investors should assess the value of tokens offered for sale, how startups should structure ICOs, and what the implications of assigning various roles to tokens on a platform might be. This paper is meant to be a first step toward building an economic framework that allows us to address questions like these.

---

3 https://www.smithandcrown.com/icos-crowdsale-history/

4 https://www.cryptocoinsnews.com/pwc-expert-1-4-billion-invested-blockchain-2016/

5 See http://kyc-chain.com/ for an example of a startup focused on these issues, and Marcel T. Rosner & Andrew Kang, *Understanding and Regulating Twenty-First Century Payment Systems: The Ripple Case Study*, 114 Mich. L. Rev. 649 (2016), available at: http://repository.law.umich.edu/mlr/vol114/iss4/4 for an interfering study of how Ripple went afoul of these requirements.

6 Interested reader may wish to see the following paper for more discussion: "A Securities Law Framework for Blockchain Tokens", available at:*https://www.coinbase.com/legal/securities-law-framework.pdf*

A Walk Down Monetary Lane

Let's begin by remembering the basic economics of money. First, what is it good for? Absolutely nothing. I'll say it again. Fiat currencies, such as US federal reserve notes, have no intrinsic value. They are simply pieces of paper that have been blessed by the Treasury Gods. Why are we willing to take these paper tokens in exchange for things of real value? Because we trust that others will take the same pieces of paper in exchange for things of value in the future. This leads to one of the fundamental rules of monetary theory:

Money is Trust.[7]

If we have this trust, money is a wonderful way to disintermediate markets and reduce transactions costs. If I can use money or other tokens as a **medium of exchange** I don't need to solve the **mutual coincidence of wants** problem. For example, if I want pack of cigarettes, I don't have to find a tobacco farmer who happens to want some of my goats. I can just sell my goats to anyone who wants them and then use the money I get to buy cigarettes. Personally, I think this is a very good thing. I find that it is surprisingly difficult to exchange economics lectures for Big Macs or gasoline.

If we are lucky enough to have a currency that has a relatively stable value over time, it can also be used as a **store of value**. I can sell a goat for 10 units of currency today, put them under my mattress, and then buy cigarettes as I need them. On the other hand, if I expected the value of money to fall over time, I would avoid holding it. I would sell only as many goats as I needed to satisfy my immediate needs and use the money I received as quickly as I could.

Valuing Tokens

As we say above, crypto-tokens are not exactly currency, and not exactly securities. They can incorporate aspects of both, and also have characteristics that are entirely new. In addition, the

7 I am also told that "Microsoft Runs of Trust", which, I guess, means that Microsoft runs on money. In a real sense this is true. Trust in the continuing value of something makes it worth owning, holding, and paying for. Trust is valuable and Microsoft runs only if it creates value.

crypto-tokens we see in the wild are extremely diverse, combining uses and traits in many variations. Given this, how do we figure out what tokens are worth? Let's begin with five basic valuation models.

Quantity Theory of Money

If tokens are currency, then the classic quantity theory of money (QTM) applies. This is an **accounting identity** that says that the value of transactions in a period (T) equals the amount of money in the economy (M) times its velocity (V) (which is the number of times a unit of currency changes hands in a given period):

$$T = MV.$$

This means that if there are a total M tokens issued, they must each have a value of $\frac{T}{MV}$.

Present Value

If tokens are a security, then their value must be equal to the present value (PV) of the associated flow of dividends. To take the simplest case, suppose a token holder can expect the following stream of profits: $\pi \equiv \{\pi_1, \pi_2, \ldots, \pi_T\}$. Suppose the opportunity cost of capital is $r\%$ (meaning that r is the rate of return that can be earned on the next best investment available). Then the value of the token must be:

$$\sum_{t=1}^{T} (1-r)^t \pi_t.$$

If the token sold for any other price, it would be either a better or worse investment than the next best alternative. Demand and price would therefore go up or down to the point where the tokens returned exactly $r\%$.

Efficient Market Theory

Efficient market theory (EFT) says that the best predictor of tomorrow's price is today's price. Put another way, the current price of any a security or currency should incorporate all publicly available information that might affect it.[8] More formally:

$$p_t = E(p_{t+1}).$$

Suppose that the price of a security today was lower than its expected price tomorrow. Then you could buy it today, hold it, and sell it tomorrow at a profit. Since this arbitrage is available to anyone, today's price would necessity be driven up to equal tomorrow's expected price.[9]

Behavioral

In some cases, we find that agents don't follow what we might call strictly rational behavior patterns. A good example of this phenomenon is called "framing". It turns out that if workers are given an opportunity to opt-in a 401k plan by their employers, very few do. On the other hand, if workers are given an opportunity to-opt out of such a plan, most do not. Whether it is optimal for a worker to save for retirement does not change with the way this default is set, but behavior nevertheless does. In blockchain space, crypto-tokens are new and cool. Stocks and securities are old and boring. It might be that agents are willing to pay more to participate in a company through an ICO than an IPO. What does this mean for the value of tokens:

$$p = ?.$$

In other words, we don't exactly know. Anything is possible. Behavioralists are sometimes accused of telling "just so stories". At root, the claim is that agents do what they do, because they do what they do. Despite this, experiments clearly support the conclusion that agents' actions are inconsistent with conventional notions of rational optimization in certain situations. To the extent that we

8 This statement of EFT is a little stark. First, as new information becomes public, both the future and the current price adjust to take into account any effect it might have on the underlying value of a security. If a company patents an invention, profits would be expected to go up, and so prices would adjust to a new, higher, PV. Second, this does does not account for any risk premium. Third, this assumes the stream of profits or value a security produces is constant. It is easy to modify the EFT to account for variable steams. Forth, if the time horizon between "today" and "tomorrow" is nontrivial, then discounting future prices using the opportunity cost of capital may need to be added.

9 The possibility of selling short prevents today's price from being higher than the expected price tomorrow.

can find rules that describe systematic and predictable, although, non-rational, behavior, economics can still be of use. Unfortunately, this is difficult to do in new situations such as blockchain startups and ICOs.

Metagame Value

Whatever the value of token might be in the context of its intended use, it may be more valuable when repurposed in some way. For example, a run-down, firetrap, apartment building might have an extremely low rental income stream and need lots of work to meet code. The PV calculation suggests that the apartment building should sell for a correspondingly low price. However, if the building could be torn down and the land repurposed for a new condominium complex, it would be worth far more to a developer. Startups should be careful to think about how the functions and attributes they give their tokens could be used for unintended purposes that might harm their platforms or benefit their competitors.

Summary

So which of these ways to value tokens is correct? In principle, all of them could be at the same time. The QTM only applies to tokens with transactional uses, but EMT and PV always hold. the QTM is simply an accounting identity, so token value automatically adjusts to make it true. EMT is just a no-arbitrage condition. It pins down relative prices over time, but does not imply any specific absolute price. PV gives a lower bound on on absolute prices. Token prices cannot drop below this because then tokens would be a better investment than any other alternative. On the other hand, if tokens have a use value as a currency or proof of stake, for example, there is every reason that token values might be above the PV of profits. In the same way, behavioral and metagame factors, if they exist, also provide lower bounds on token value.

Properties of Crypto-tokens

Various startups have devised crypto-tokens with an array of characteristics. No two tokens seem to be exactly alike. Still, most combine four basic elements in different proportions. Below, we consider these elements one by one to see how each should influence token value.

Transactional Currency

Bitcoin, the father of us all, is a purely transactional currency. As such, its value must satisfy the QTM. All tokens that serve even in part as transactional currencies must satisfy the QTM equation as well.

In the real world, the velocity of fiat currencies is limited by fractional reserve requirements and the physical and electronic delays involved in making transactions. In principle, a crypto-token could change hands each time the ledger is updated. This would be 144 times per day for bitcoin and thousands of times per day for Ripple. The daily value of bitcoin transactions is currently around $\$400M$ and about $16M$ bitcoins exist. At maximum velocity, $2.3B$ transactions could take place per day. This means that bitcoins could support $\$400M$ in transactions if they were worth as little as $¢17$. Given that bitcoins are actually worth about $\$1100$, the quantity theory of money equation tells us that velocity must be $.023$. This means that about 2% of bitcoins change hands once per day, or equivalently, each bitcoin changes hands once every 44 days.

Why don't bitcoins circulate faster? One reason is that the transactions cost of converting bitcoins to dollar deposits range from 1.5% to 4%. Jumping in and out of bitcoin quickly is expensive. If a user is likely to need to bitcoins for purchases in the future, it may be better to hold them. Unfortunately, this exposes the user to exchange rate risk, and bitcoin is notoriously volatile. Of course, users may also benefit from these swings in value, so bitcoin must also be compared to other potential investment vehicles.

Given this, how should we value bitcoin? The QTM implies a floor price of $¢17$, but how much higher could the price be? Suppose that the stock market paid an average return of 7% and that bitcoins were worth $\$1000$. What conditions would we need to make this an equilibrium? If agents expected bitcoin to increase in value at a rate of 7%, per year as well, they would be indifferent between holding bitcoins and stocks. A price of $\$1000$ today, $\$1070$ next year, and so on, would therefore be an equilibrium. Of course, a price of $\$2000$ today, $\$2140$ next year, etc. would also be an equilibrium. We will see below that is an example of a more fundamental problem.

Suppose instead that we expected a zero rate of increase in the bitcoin price. Using bitcoin still offers several advantages, not the least of which is privacy. Holding bitcoin for 78 days instead of putting the same dollars to work in the stock market has an opportunity cost of 1.5%. Agents who expected to transact at least this often would be better off holding bitcoins than converting them to cash and then back into bitcoins when needed. What this means is that if agents expected to need bitcoins every 44 days, for example, and $\$400M$ in transactions took place on an average day, then a price of $\$1100$ for all time would be an equilibrium. This would be consistent with the QTM and the no-arbitrage conditions implied by PV and EFT equations that make agents willing to hold bitcoin for up to 78 days.

As we see, even if the QTM, PV, and EFT conditions are all satisfied, we still are not able to pin down the price of crypto-tokens. Even worse, transactional tokens are subject to same the potential for bubbles and value collapse as any other fiat currency. Consider the following scenario:

- A startup sells 1M tokens in an ICO. Several big, sophisticated investors (BSIs) take large positions. (In most token markets, relatively little is in active circulation. Most tokens seem to be held by investors or speculators.)

- Suppose that one of these BSIs decides to sell his tokens and dumps his 3% of the total token stock on the market all at once. This might double the number of tokens in active circulation. The price of tokens falls as a result.

- If all the rest of the tokens were held by BSIs, this might be the end of it. Each of the other BSIs would regret that he did not sell before the price drop, but realize that it is too late to do anything about it.

- However, if a fraction of the tokens were held by small unsophisticated investors (SUIs), they might see the price drop and react by dumping their own tokens. Get out while the getting is good!

- The BSIs would anticipate the behavior of the SUIs. They would respond by dumping their tokens as soon as they saw the first BSI do so in order to beat the additional price drop caused by the SUIs' reaction.

The result is a catastrophic fall in the token price and a loss of confidence in the platform. Even if investors expect the price to rebound, they would still be better off selling before the price drop and then buying the tokens back in the trough.

This scenario does not violate any of our three valuation models since the price drop was not anticipated in advance. In other words, these three equations allow for an almost arbitrary base price of tokens, and unexpected jumps in price in themselves do not produce disequilibrium. For example, if investors found that the price of bitcoin had halved overnight but still expected them to appreciate at 7% in the future, they would have no reason to change their positions.

What's going on here? It turns out that there are **multiple equilibrium** in any currency or token market. In fact, there are an infinite number of potential equilibrium prices. The three equations place some limits on the possibilities, but they fail to pin prices down. Which of these equilibria emerges in the real life depends critically on the expectations and beliefs of the agents holding the currency. So what is the best advice to a company considering a coin offering?:

> *Do not meddle in the affairs of wizards, for they are subtle and quick to anger,*

or as Alan Greenspan put it:

> *I guess I should warn you, if I turn out to be particularly clear, you've probably misunderstood what I've said.*

Monetary authorities in the real world work very hard to stabilize prices and manage expectations. They have the advantage of very large scale and lots of expertise. Nevertheless, George Soros and other speculators managed to force the UK out of the European Rate Mechanism in 1992 costing the country billions of pounds. The Latin American Crisis of 1994 and the Asian Crisis of 1997 are other examples of large scale currency crashes. More recent examples include the Venezuelan Bolivar fuerte now trading at 4000 to the USD, and the Zimbabwean dollar which last traded at 35 quadrillion Zimbabwean to the USD. The point is that even with scale and a carefully implemented monetary policy, bubbles, collapses, and manipulation by speculators for their own profit, are possible and even likely. For an ICO with a total capitalization of $\$25M$ or even $\$100M$, and a company more focused on its technology than its monetary system, this is dangerous territory.

One clear lesson that emerges from history is that seigniorage is very poor way to fund spending. Governments can always print more fiat currency and this leads to inflation, a loss of confidence in financial markets, bubbles, and sometimes currency collapse.

ICOs generally issue a fixed number of premined coins. In some cases, more are issued on a fixed schedule, when benchmarks are achieved, or as a result of mining, forging or other user activities. Sounds good, right? Startups are pledged not to dilute their monetary base. What could possibly go wrong?

One significant problem is that in most ICOs, the company's founders retain a share of the coins. Coin endowments for software development and even non-profit portions of a project are often made as well. About 20% of the total seems to be a typical fraction of coins that get held back (although about 70% of Ripple coins are held by Ripple Labs and associated groups and people).

Given that only a small percentage of a typical startup's tokens actually circulate, 20% might represent a multiple of this active stock. Even worse, selling these held-back tokens can easily be taken as a signal that the management team is losing confidence and cashing out, or that the project is costing more than anticipated. (Expectations, remember?) For these reasons, it is far better to sell all the tokens in the ICO and instead put 20% of the proceeds in an account to pay for development or whatever other purposes are thought necessary. Founders should be compensated with stock or profit shares, or even with salaries drawn from the proceeds of token sale. Holding back tokens is inherently destabilizing and is probably the worst way to incentivize the founders and developers.

An even better idea would be to hold back some of the cash from the ICO to prop up the token's value and maintain investor confidence should it become necessary. As George Soros taught the UK, this can be dangerous or impossible, but such policies have often been successful as well.

Profit Sharing

A major reason for the volatility seen in crypto-token prices is that there is nothing that ties down their value if they are only used as a medium of exchange.

In contrast, conventional stocks and securities dole out non-retained profits in the form of dividends in proportion to stock ownership share. Retained profits are reinvested in the firm and management has a fiduciary duty to do so in a way that maximizes shareholder value. If managers are doing their job, reinvestment only takes place when it returns more to stockholders in future profits than they could make by investing these profits on their own in other companies. Securities derive their value from these current and future dividend streams. Investors may disagree about the future profitability of any given company, but SEC rules are focused on setting up reporting and accounting practices to generate transparency and to allow investors to make good assessments about a company's prospects.

So what if a startup issues tokens that are used to share out profits instead of for transactions on the platform? If this were done under the same rules that apply to securities, then the founders would simply be selling a part of their capitalized stream of profits. If the tokens were also used for transactions, the QTM would apply as well, but the PV of profits would create a lower bound on the value of the tokens.

Unfortunately, the way that many ICOs take place leaves investors uncertain about how to estimate revenue streams. Some startups launch without a producing a white paper that outlines the business model and technology in detail. Even when a white paper exists, it is not always clear exactly what revenue streams token owners will share in.[10] In addition, a platform may evolve, the focus of the business may change, and even if the original revenue sharing rules are maintained, the profit stream from the legacy use case may dry up. On the other hand, if profits themselves are to be shared, then it needs to be clear what profits are. Founders could pay themselves salaries that use up any part of the difference between revenues and expenses they choose and give only a small residual to shareholders. Founders could count hot-tubs, karaoke nights and attendance at burning man as expenses, or just reinvest everything in the company. This might increase the value of the company for the founders, but it would not be reflected in the value of the tokens.

10For example, a share of jury fees might be promised, but the fee itself left unspecified. It can be hard to figure out if the fee or share might be changed somehow in the future. All this is in addition to the fundamental uncertainty about what volume of traffic a startup is likely to see once it launches. As a result, the revenue stream going to token holders is often a promise times an unknown times a guess.

In normal situations, the effect of this lack of information is investor uncertainty and an increase in perceived risk. Investors expect to be compensated for risk, and so the willingness to pay for a share of profits is lower than it might otherwise be. The result is that any public offering will raise less money for the company. This is exactly why firms involved in IPOs try to be as clear and convincing about their prospects as possible.

In the case of blockchain companies and ICOs, however, things might be a bit different. A lack of clarity simply creates uncertainty. It may be that investors end up overestimating instead of underestimating a company's future revenues. If the overestimate is large enough, it could more than offset the uncertainty discount. Thus, the real question for firms considering ICOs is what sorts of disclosures tend to raise investor estimates of returns, and when will investors fill in omitted details with overly optimistic guesses.

Tokens are new thing. Investors don't have much experience with them so they may not be very good and estimating their value. In addition, blockchain is a relatively new technology and there is a great deal of uncertainly over how much potential for profit there is and which sectors are the right ones to invest in.

If investors make systematic errors on the positive side, ICOs will benefit from something called the **winner's curse**. To understand this, suppose there are 100 potential investors, each with $\$1000$, who are considering an investment in a company issuing 10 tokens. If the company is in the well-understood old-tech sector, investor estimates of the PV of profits are uniformly distributed over a fairly narrow interval, $[900,1100]$. A typical outcome would be that the investor with the tenth highest PV estimate would be willing to pay $\$1080$ for the token. On the other hand, if the company is in the less well-understood blockchain sector, investor estimates of the PV of profits are uniformly distributed over a wider interval, $[0,1500]$. A typical outcome would be that the investor with the tenth highest PV estimate would be willing to pay $\$1350$ for the token. Thus, old-tech tokens (or stock) sell for less even though the lower bound on old-tech return is above the mean return to the blockchain company. If disclosure narrows the spread of the blockchain return estimates without raising the mean, the marginal investor will be willing to pay less, and the ICO will raise less money. If the mean of the distribution is the true expected return, it must be the case

that the "winners" who bought tokens are always paying too much, and thus, suffering from the winner's curse.

More generally, investors may think that blockchain and crypto-tokens are modern and sexy. They might be willing to pay more for a given revenue steam coming through tokens than from stock ownership. In other words, the framing of the offer may affect how much investors are willing to pay for same expected return. This is an example of behavioral economics driving value.

Voting Control

Stockholders typically are allowed to vote over who is on a company's board of directors in proportion to their holdings. This lets shareholders control who manages the company and to make sure that the company acts in the interests of shareholders by maximizing share value.

In the ICO world, token holders are sometimes given collective control over a variety of aspects of a project. For example, token owners might get to vote over fees for some subset of services or on some of the details of the protocols. They might be allowed to approve new stakeholders, new projects wishing to joining the platform, or even set the direction of future development.

Unfortunately, when any aspect of control is separated from profit sharing, serious incentive problems are created. Voters vote in their own interests. They may choose fees or protocols that maximize their own return but harm the ecosystem as a whole. They may choose directions for future development that benefit the use cases they have in mind, but are not of general interest. It is even possible that the tokens might be bought up by a competitor who then uses his power to weaken the company or move it into other less profitable markets. This might be relatively cheap to do since the tokens only capitalize whatever value the voting power might have and not the total value of future profits. This is an example of how tokens might have value in a metagame that is higher than their value within the platform.

Proof of Stake

Proof of stake can take many forms. In some cases, it includes a degree of voting control, perhaps over who is admitted to a trusted set of verifiers. In other cases, it serves a surety bond for the good behavior of agents charged with carrying out various functions on the platform. For example,

token holders might be required to form a consensus to verify things like who won a match in an online game or what the outcome was for a prediction market. Other examples include processing transactions or connecting users in markets. In most cases, some set of fees are paid to stakeholders in proportion to how much work is done and how many tokens are held.

How much should such tokens be worth? Token holders are apparently being asked to pay for the privilege of contributing their efforts to maintain the platform. All else equal, this makes the tokens less valuable. To be precise, tokens should be worth the present value of the expected fees less the cost of providing services to the platform. In effect, such tokens are selling jobs that have excessive salaries. For example, suppose that anyone could hire a crew for $\$100K$ to mow a golf course for a season. A corrupt city official offers a contract paying a fee of $\$250K$ to whomever offers the largest bribe. Clearly, the equilibrium value of the contract is $\$150K$ per year, which is less than the $\$250K$ fee paid to whomever buys the contract.

Burdening tokens with duties decreases their value. It is not clear that this is a good strategy for a startup. The services of token holders will all be provided in the future after the platform is launched and becomes established. However, the present value of the cost of these services gets deducted from the tokens at the time of the ICO. This is like a startup paying its expected electricity bill 20 years in advance instead of using the money to develop the platform more quickly.

To ICO or not to ICO

Should a startup use an ICO to fund itself? How do ICOs compare to other ways of getting funded?

Venture capital is one of the traditional ways to fund a startup. Convincing a VC to invest in a company with an unproven track record and an inexperienced team can be difficult. Even if the VC agrees, he will likely insist on getting a big share of the company and having control over many aspects of the firm's direction and management. This sort of adult supervision can benefit a company whose founders are more focused on the technology than the business, but it can also take all the fun out of a project.

IPOs are another traditional way to raise capital. Unfortunately, they are expensive. Doing an IPO costs a few million dollars plus about 7% of the capital raised. This is not a practical option for small companies seeking to raise modest amounts.

A Reg A+ IPO on the Over the Counter - Alternative Trading System is less traditional possibility. These stocks are traded on a separate OTC market and are subject to a few more constraints than stocks traded on the NYSE or Nasdaq. Companies can raise up to $\$50M$ this way and the costs of an OTC IPO are on the scale of $\$100K$. Reg A+ IPOs are regulated by the SEC and companies are required to abide by a set of standard reporting and operating rules. Several blockchain companies are listed on the OTC market including First Bitcoin Capital Corp, which currently has a market cap of about $\$100M$. Although IPOs like this are feasible for small startups, they do require considerable effort and compliance with SEC regulations. Also, stocks are not as fun as tokens.

ICOs, on the other hand, are easy to do for blockchain startups. They raise money quickly, and the money comes with few strings attached. As long as people are willing to invest this way, it is hard to argue that companies should not take advantage. Although one has to be careful about currency and securities law, this has been a largely theoretical concern for small startups so far.

Lessons

For Startups:

1. Monetary systems are hard to run and inherently unstable. There are multiple equilibria in money markets, and so it is simply not accurate to say that the value of a token will increase in proportion to platform use.

2. Consider setting aside a fund to stabilize token prices, especially if the token is primarily a transactional currency.

3. Don't hold back tokens in an ICO.

4. Avoid burdening token holders with work. Pay for work separately.

5. If token holders can control any aspect of your platform, be aware that they will use this power to further their own interests and not the ecosystem's. Think about their incentives within the platform and also how hostile actors might use such power to profit in the metagame.

6. Startups don't have to disclose or commit to anything when launching an ICO. Being free of constraints allows more flexibility. All else equal, this is a good thing, especially in a dynamic market like blockchain.

7. In general, making the value proposition clear to investors increases their willingness to pay for tokens (or securities). To the extent that you are committed to a plan and believe it to be a good one, you should disclose, explain, and bind yourself as much as you can.

For Investors:

1. Counting on token value appreciation to justify buying into an ICO is not a good long-run strategy. Prices of transactional tokens are built on expectations of future prices and such expectations are fragile.

2. The fact that the price of the tokens in your portfolio seems to keep going up does not mean that you have made good bets. It means that you have gotten lucky. Examples of markets where the bubble eventually burst are too numerous to mention.

3. Tokens that come with claims on clearly laid out revenue streams are a safer investment, especially if you think the business model and technology of a firm are sound.

4. Tokens almost never come with full voting control over a company. Since you are dependent on the choices made by the founders, make sure that their incentives align with yours, and that the commitments they have made to token holders cannot be diluted or ignored.

5. On the other hand, make sure that the interests of the other voting token holders agree with yours on the dimensions they control.

6. A confusing, incomplete, or nonexistent white paper could signal a lack of clear vision on the part of the founders, that a project is immature, or that the company hopes you will invest without it having to disclose or promise very much. It is hard to find a good interpretation for such a lack of clarity or transparency.

7. There is no number seven.

Conclusion

Without question, blockchain is a game-changing technology. We are still in the very early stages of figuring out how it will be used. Many startups are working in a variety of creative ways to bring applications to markets. Most of them will probably fail. Blockchain applications seem to exhibit significant network externalities and this tends to make for a winner-take-all environment. There will be winners, however, and their impact is likely to be huge.

ICOs are a kind of wild west of crowd funding at the moment. We see a lot of exuberance and what macroeconomists call "animal spirits". The fact that ICOs allow relatively small startups to raise a few million dollars quickly and with few transactions costs is a probably a good thing. Blockchains are new and having many firms at work exploring the possibilities of this technology will only bring its benefits to market sooner. If investors are willing to foot the bill for this public good despite the risks, then so much the better.

The main point of this paper is that designing a successful token must take into account aspects of monetary theory, financial economics, and game theory. Failing to do so can put an otherwise excellent project at risk. Each company's technological vision may call for a token with unique properties and uses. We hope that this paper provides a framework that allows companies to follow their vision while avoiding structural mistakes that might be harmful to their chances of ultimate success.