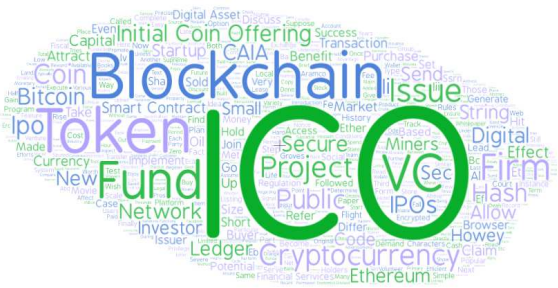
Initial Coin Offerings

Hossein Kazemi
CAIA Association & Isenberg School of Management, University of Masschusetts

May 30, 2018



1. Introduction

In the late 1940s, W.J. Howey company owned a hotel and large tracts of orange groves in Florida. It devised a plan to sell portions of the groves to the public, whereby buyers would receive ownership of a piece of land for a set price with the option to lease the property back to Howey. The lease agreement entitled the owners to a share of profits generated by Howey through its management of the orange groves. The U.S. Securities and Exchange Commission sued Howey, claiming that the sale contracts were in fact securities that it was offering to the public, and, therefore, they should have been registered with the SEC. The U.S. Supreme Court sided with the SEC, and since then firms that wish to raise funds from the public have had to register their offerings with the SEC if the sales met the standards set by the Supreme Court. However, technology has caught up with the Supreme Court ruling, creating a vehicle through which a variety of for-profit and not-for-profit entities can raise substantial amounts of funds from the public without violating the SEC regulations. Initial coin offerings (ICOs), or more precisely, blockchain-based tokens, represent this vehicle.

In the following pages, first, I will give a brief introduction to blockchain. Next, I will explain the differences between cryptocurrencies and tokens followed by an introduction to ICOs and the process of issuing ICOs. Finally, I will discuss the relationship between ICOs and VC investing.

2. Blockchain

A blockchain is a ledger that can contain various types of information. For this essay I use the term blockchain to refer to public ledgers that can be accessed without permission from a central authority. Bitcoin blockchain is such a ledger.

A blockchain can contain information about ownership of assets, instructions about performing specific tasks in response to a certain signal, rights and privileges of asset owners and asset issuers, and so on. Since it is a permission-less public ledger, there must be a mechanism to prevent

unauthorized changes to the ledger. The current mechanism gives a group of volunteers (i.e., miners) the incentive so that through a consensus process they verify that only legitimate changes are recorded on the ledger. The key is the incentive mechanism, which creates the conditions such that a large group of people volunteer to spend time and money to verify the changes. The mechanism has a built-in incentive so that fraudulent entries into the blockchain are not approved by a majority of volunteers.

One major advantage of blockchain is that the history of the system and all transactions completed through that system are saved securely, and no changes can be made unless 51% of the miners approve the change. Most blockchains use encryption discussed below to secure and verify the authenticity of the changes that enter the blockchain. The following is an example of how encryption can secure a blockchain:

- Go to this website https://passwordsgenerator.net/sha256-hash-generator/
- Type "CAIA Association owns 10 bitcoins" in the window and hit the enter key.
- Below the window, you will see "SHA256 Hash of your string:" The string shown will be:

  191561C5ECA2B17FE6D8430BC6B001B59EB12E21E80F172D4DDE200B554102BC

- Hit the enter key and copy and paste this string into the original window below "CAIA Association owns 10 bitcoins" and then type below it the phrase "CAIA Association paid Hossein 2 bitcoins" and hit the enter key. Now the encrypted string should read:

  01A9647724B73D89956A4A49B41F1ABD4BA217EF27156B2948D5865F9852B31E

We have now created a crude blockchain. Going forward, this last string can serve as a check on the integrity of the blockchain.

The key to the encryption method used here (SHA256) is that no matter how long or how short the text in the window is, the string (i.e., "hash") will be 64 characters long. One can upload all the books in the local library or the entire history of all bitcoin transactions into that window and the "hash" of each one would be a unique string of 64 characters. Even if one letter in one of those books is changed or just a zero is added to a bitcoin transaction that took place years ago, the entire hash will change unpredictably. Therefore, if we have the hash of the verified history of all bitcoin transactions up to now and someone presents us with a copy of the public ledger, it will take us a few seconds to determine if that ledger has been altered. All we need to do is to compare the hash we have with the hash of the ledger being presented.

In our example if someone tries to change the original statement to "CAIA Association own 9 bitcoins," the resulting string will change since it is a unique representation of the input. No other input would generate the same string. Therefore, the public will realize that someone has made an unauthorized change to the previous version of the blockchain. The role of the miners is to find a set of characters called "nonce" such that when added to the above blockchain, the resulting hash will have a pre-determined property (e.g., the first *n* characters must be zeros). For their efforts, the miners are rewarded with cryptocurrencies. There is no known formula for finding the nonce and only brute force can find the right nonce.

Since the ledger is public, everyone can see who owns what. As a result, the blockchain and internet allow global transfers of digital assets like bitcoin. Similar to emailing, you can send a digital asset to another party by letting the network that monitors and secures the blockchain know that you have transferred the ownership of the asset to someone else. You need a password (i.e., a private key) to start the transfer of the ownership to someone else. The blockchain maintains a record of who owns these digital assets at any point in time and no centralized authority, like a central bank or a centralized exchange, is needed to verify the transactions. In theory, we can use the blockchain technology to trade stocks and bonds, but the efficiency gains are not there yet to implement this technology on a large scale. Below we discuss one particular application of the blockchain technology: issuing and tracking of tokens.

As I discuss below, tokens have been around for a long time (almost as long as capitalism has existed), and entities have used various forms of tokens to raise funds. What has changed in recent years is the use of the blockchain technology in creating, tracking and trading of tokens.

3. Tokens and Cryptocurrencies

Tokens and cryptocurrencies are different. Both could be based on a particular blockchain (i.e., a given ledger), but they serve different functions. First, every blockchain has its own cryptocurrency. This is needed to reward the miners who verify and secure changes in the blockchain. The most famous blockchain is the Bitcoin blockchain and bitcoin is its cryptocurrency. Ethereum is another blockchain with its own currency called ether.

Cryptocurrencies have limited use. You can use them as a means of payment and a store of value. Once you own a cryptocurrency, you can do three things: (a) hold it, (b) spend it to purchase an item or (c) use it to gain access to the underlying blockchain system. Bitcoin and ether are cryptocurrencies.

Tokens may have nothing in common with cryptocurrencies. In fact, a token need not be based on a blockchain. For example, a casino chip is a token. It allows you to take part in a game. You can trade it, but there is no point in holding it because its value will not appreciate. A ticket to a movie is also a token, which can be traded and may appreciate in value if the movie is popular. Stock certificates are also tokens and so are the tickets to enter Disney World.

We can see that tokens can serve a variety of functions and may possess several features not shared by cryptocurrencies. The primary contribution of the blockchain technology is that it has allowed a variety of entities to issue and track their tokens on a very large scale. The blockchain of choice for issuing tokens is Ethereum.

4. Ethereum Blockchain

It is hard to believe, but the Bitcoin blockchain is already becoming obsolete as it has limited uses beyond supporting bitcoin. Ethereum is a more advanced blockchain, which not only has its own currency – ether – but can hold and execute computer programs called “smart contracts.”

Smart contracts are software programs embedded in a blockchain that can receive or send assets and information if certain conditions are met. The transmission of information and assets by the smart contract is entirely pre-defined in the code and is autonomously triggered if certain conditions are met. For example, suppose an insurance company sells flight insurance where the payments are made through Ethereum blockchain. A customer will use a wallet on Ethereum to pay for flight insurance. The information is stored on the blockchain with a smart contract receiving information from a flight traffic database. If there is a delay, the smart contract will automatically execute some pre-defined instructions and send the amount of insurance to the customer's wallet. The insurance company AXA has already introduced such a contract.

There was no apparent token associated with the flight insurance example provided above. In most cases, a firm may create its own token to facilitate the sale of its products or services to the public. For example, suppose a group of movie theaters decide to pre-sell tickets to the next Marvel Studios' movie by issuing the tickets through the Ethereum blockchain. A simple smart contract is placed on the blockchain. Every time a payment is received by a designated account that is on the blockchain, the program is executed, sending the correct number of digital tickets to the buyer's account on the blockchain. The owners of these digital tickets may trade them for other tickets or to sell them to people looking to buy tickets. All these transactions are recorded on the blockchain. This will not be a smart way of issuing tickets as the issuers will need to compensate the miners for securing the history of transactions and the digital tokens have a limited life. Besides, there are more efficient ways of implementing this pre-sale.

Issuing a new token on Ethereum blockchain is exceedingly simple and can be implemented in less than an hour! Getting people to buy your token is another matter. However, interesting and promising projects can use Ethereum tokens to raise a substantial amount of funds in a short period. According to Coindesk, the total amount of ICOs issued in the first quarter of 2018 was $6.3 billion. This is slightly less than half the size of the US IPO market and about one-third the size of venture capital funds allocated during the same period. In short, the ICO market is becoming very large.

5. Initial Coin Offerings

Despite their name, ICOs differ from IPOs. In case of an IPO, shares of a startup company are sold to the public. These shares will represent claims on the firm's assets, and investors are owners of the firm with certain rights and privileges. Once the IPO is completed and necessary funds are raised, the firm will not directly benefit from a rise in the value of its shares unless it does a secondary offering and issue additional shares.

Most ICOs are like crowdfunding done on Kickstarter for example. The firm issues its own digital currency, which can access the services offered by the firm. Not only the firm can raise cash to fund its operations, but it will benefit if the value of its currency increases through time. For example, suppose a firm creates a new social networking platform similar to Facebook. It issues its own digital currency and stipulates that anyone who wishes to join the platform must pay a small fee using the digital currency that the firm has issued. Suppose each token is worth $0.01 at the beginning and its costs one token to join the network. Every time someone joins the network, the firm will receive a token which it can then sell for cash or use it to pay for its employees'

salary. If the network becomes popular, the value of the token may increase to, say, $0.1. While the firm still requires one token for joining its network, those tokens are worth ten times more.

Similar to other commodities, the price of a token issued through an ICOs will depend on its demand and supply. The issuing firm can undertake certain actions to affect both and thus increase the value of the token. Policies or actions that directly affect the supply of the tokens are referred to as money policies while those that directly affect the demand for the tokens are referred to fiscal policies.

ICOs Monetary Policy: This refers to the management of the supply of the tokens. Continuing with our social networking example, we need to determine the volume of the coins to be sold and whether the entire supply will be offered to the public or a portion will be kept at the firm. For instance, in 2017 Gnosis, a prediction market platform, used an ICO to raise $12 million in less than 15 minutes. However, the coins sold to the public made up only 5% of the entire supply. The remaining 95% was held Gnosis, which implies a market cap of $300 for the ICO. The monetary policy of a token should communicate to outsiders the issuer's policy regarding current and future supplies of the tokens. If only a fraction of the tokens is offered to the public, the remaining tokens are typically stored in an escrow account with the future sales of these token normally tied to operating expenses of the issuer.

ICOs Fiscal Policy. While the monetary policy deals with the supply of the tokens, the fiscal policy deals with the benefits received by token holders. These policies increase the attractiveness of the tokens. For instance, the firm may accept other currencies for its service but to offer a discount to those who use its token to purchase the service. Improving the efficiency of the underlying project will be the most important benefit that the firm can provide for its token holders and here lies one of the fundamental aspects of the token economics. As the firm works to improve its product (e.g., our social network project offers new features), demand for its tokens will increase leading to a rise in the price of its token. This will benefit both the firm and the token holders. In other words, there is a strong alignment of incentives in this tokenized economy.

6. Life-Cycle of an ICO

Let's consider the steps typically taken to issue a token on Ethereum's blockchain. Throughout we assume that the developers have already ensured that the ICO does not violate local rules and regulations regarding the issuance of securities to the public. For instance, in the US the crucial step is to apply the Howey Test to ensure that the project's token does not fall under the legal definition of a security, and is, therefore, subject to securities regulation. The four main parts of the Howey Test are (i) there is an investment of money, (ii) profits are expected, (iii) money investment is a common enterprise, and (iv) any profits come from the efforts of a promoter or a third party. The feature that most projects exploit to pass the Howey Test is that they make a decentralized cryptocurrency equivalent to a currency (or simply cash) with no central owner. Assuming that the project complies with local rules and regulations, let's consider the next steps.

Project: The very first step is to have a project that is worth funding. Let's assume that our project is to develop an open source web browser where all advertisements are removed from websites

that one visits while using this browser. To use this web browser, users will have to pay the developers one token, which is then used to pay the owners of the websites. We believe people will pay a small fee to use a browser that filters out all advertisements. Notice that our entity could be a not-for-profit organization. Some initial funding from angel investors or founders is needed to kick-start the project.

Whitepaper: The developers write and distribute a whitepaper describing the project. The whitepaper also describes the rights of token-buyers and the responsibilities of the entity. For example, the paper will state whether the supply of the token to be issued will be fixed or not. If not, a precise schedule regarding the future issuance of new tokens should be presented. Most tokens enjoy a network effect. The value of the network and its associated token will increase in value the more people use the network. In our case, as more people use this web browser, more websites are likely to agree to removing their advertisements for receiving a token every time one of our users accesses their website.

Roadshow: The developer team will go on the road to present the idea to potential buyers. Facebook, Twitter, Reddit, and other social networks will promote the idea and get people excited about the project.

Pre-ICO: Most projects implement a Pre-ICO. During a Pre-ICO, a fraction of the funds needed to support the project is raised. The early adopters and influential people in the industry are provided with cheaper tokens to increase the chance of success. The funds raised through Pre-ICO might be enough to pay for the cost of the initial development, the road show and the promotion. Some argue that the Pre-ICO also provides the developer team with information about the potential fair price of the token that will be issued to the public.

ICO: As mentioned above, the most popular platform for issuing tokens is Ethereum. Using Ethereum network to issue tokens is simple, and a tech-savvy person can complete the entire process in about 30 minutes! First, we must create a digital wallet on Ethereum (see www.ethereum.org/). Second, we download the code for smart contracts on Ethereum (the code is about 100 lines). The technical name for the code is *Ethereum Request for Comment 20* or ERC20. Third, we make some small edits in the program's parameters so that it will contain the information about our token (e.g., name, size, deadlines, etc.). We need to have some ethers to pay Ethereum for the privilege of using the network. Finally, the revised code is uploaded to Ethereum. We are ready to sell our coins! The mechanics of the actual ICO are almost as easy as emailing. The project creates an address to which the funds (in the form of other cryptocurrencies) will be sent. Investors will then send funds to the address and receive the equivalent amounts of the tokens.

Listing: A critical ingredient for making the ICO a success is its listing on one of the cryptocurrency exchanges (e.g., Coinbase or Kraken). The listing ensures that investors can trade their tokens with varying degrees of liquidity. The listing also contributes to the price discovery process. Increased liquidity will encourage others to use the token to purchase the services provided by the original project, contributing to the network effect.

7. ICO and VC Industry

ICOs have emerged as a popular funding tool for startups in the technology sector. They offer advantages to digital projects that traditional venture capital firms cannot. In particular, ICOs help attract developers and users of the product even when the project still is in its infancy. As we have seen, ICOs are low-cost options that do not dilute ownership, require no intermediaries, and can be completed quickly compared to the time to raise traditional venture capital.

ICOs are not viable fund-raising options for most startups. Firms that sell their services through online sites and enjoy a network effect appear to be prime candidates for ICOs. Several firms have tried to get on the bandwagon and take advantage of the hype surrounding ICOs. For instance, recently, ARAMCO, the state-owned oil company of Saudi Arabia, conducted an ICO where the tokens representing a claim to oil extracted by ARAMCO were issued. It is hard to see why ARAMCO Coins should be successful. Why would one need to purchase a token representing a claim to a barrel of oil when such investments can be done through available securities? Further, there is no incentive by token holders to increase their use of the token and the network as it will have no impact on the value of the tokens – there is no network effect. Finally, ARAMCO has to maintain the blockchain, which defeats the whole purpose of having a decentralized ledger. If a public ledger is to be used, then someone must pay the miners to secure the ledger.

Pros and Cons of ICOs: ICOs make it easy for the right startup to raise funds on a large scale in a short time. Almost every person on the Earth can become an investor in a project funded through an ICO. The size threshold for conducting an ICO is low. Even the smallest startups may raise funds through an ICO. The potential network effect will be small if the firm plans to remain small and therefore coins may have to be sold at deep discounts.

Transparency and security are the primary disadvantages of ICOs. Many projects are nothing, but a vague idea presented as a whitepaper. The ease with which ICOs can be implemented has attracted many fraudulent activities. This may lead to severe adverse selection problem such that investors will reduce the average price they are willing to pay for tokens, making the ICO an inefficient mechanism. Also, regulatory obstacles may increase, making the ICO process more costly.

Pros and Cons of VC: VC funding is available for almost any economically viable project. VC funding is more than just funding. Specialized VCs provide expertise and connections that are not available through the ICO channel. The long process of obtaining VC funding allows investors to perform due diligence, which would attract additional investors who use the reputation of the initial VC investors as a signal about the quality of the underlying investment.

While startups funded with ICOs may be under pressure to show results and profits rather quickly, VC investors are far more patient and hence enable developers to focus on the long-term strategic aspect of the project.

The primary shortcoming of VC is that less than 1% of startups are funded by VCs. VC funds make lumpy investments, and, therefore, cannot hold fully diversified portfolios of 1000s or even 100s of startups. As a result, VC funds have a very high threshold for return, leading them to reject

many promising projects. Therefore, the time and energy spent on attracting VC investors are wasted in most cases.

ICO + VC Model: A new form of startup funding is emerging. For some projects, a combination of ICO and VC funding could represent the most promising way of raising the funds, generating enthusiasm among potential customers, and using the expertise and the connections provided by VCs. VC funds are increasingly interested in taking part in Pre-ICO transactions. This will allow them to purchase tokens at a discount and because of their reputation, their Pre-ICO participation will increase the potential demand for the eventual ICO. Further, a successful ICO is likely to lead to a more successful eventual IPO.

8. Further Readings

- https://hackernoon.com/ contains a wealth of practical information about blockchain, bitcoin and ICOs.
- http://www.ssrn.com/ contains numerous academic papers on the same topics.
- The following sources are recommended:
    - "The Token Handbook," David Siegel, 2017, https://hackernoon.com/the-token-handbook-a80244a6aacb
    - "Some Simple Economics of Blockchain," C. Catalini et al., 2016, MIT Sloan Research Paper No. 5191-16. https://ssrn.com/abstract=2874598
    - "Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets," J. Rohr and W. Aaron, 2017, Cardozo Legal Studies Research Paper No. 527. https://ssrn.com/abstract=3048104
    - "Initial Coin Offerings", P. Momtaz, 2018, https://ssrn.com/abstract=3166709
    - "Bitcoin and Cryptocurrency Technology," A. Narayanan et al., 2016, Princeton University Press.