The ICO Explosion: A Primer

Grant Hummer leads the SF Ethereum Developers Meetup and has been a cryptocurrency enthusiast since 2011. Follow him on twitter @granthummer

If you've been following recent news headlines, you may have noticed an uptick in the number of articles discussing blockchain technology, and more specifically, the emergence of a new venture funding model based on that technology: the token sale. But first, a brief explanation of blockchains.

Blockchain technology was first unveiled to the world in 2009 with the release of Bitcoin. Bitcoin was and is the first widely used digital asset in history. As of early July 2017, Bitcoin has a market cap of ~$42 billion. Bitcoin runs on a peer-to-peer network, and transactions take place between users directly, without an intermediary. These transactions are verified by network nodes and recorded in a public distributed ledger called a *blockchain*. Since the system works without a central repository or single administrator, Bitcoin is often called the first decentralized digital currency.

Besides being created as a reward for mining, Bitcoin can be exchanged for other currencies, products, and services in legal or black markets. One of Bitcoin's drawbacks (which some people would argue is actually a strength) is that it's only usable for simple payments - users who wish to engage in more complex decentralized transactions can't do so without building unwieldy Rube Goldberg-esque solutions atop Bitcoin's relatively static code base.

Enter Ethereum, another blockchain platform with a market cap of ~$25 billion as of early July 2017. Ethereum is the brainchild of Vitalik Buterin, a 23-year old wunderkind who conceived of the idea after noticing that many of the 'more flexible' Bitcoin competitor blockchains suffered in that they were perfectly fine for use cases A, B and C, but when a developer wanted to code D he was out of luck. Vitalik therefore went for the mother of all abstractions and created a Turing complete blockchain platform, meaning that any kind of code can be executed on it.

In particular, Ethereum enables the use of *smart contracts*, which are like traditional web applications akin to Facebook and Spotify, except they run in a completely decentralized manner, which enables trustless computation and could potentially unlock hundreds of billions of dollars (or more) in cost efficiencies as middlemen in a variety of industries are disintermediated. Smart contracts are somewhat akin to the deist theological model of the universe - an enlightened creator sculpts an ecosystem and then optionally relinquishes control and lets it run on its own momentum, such that nobody can control it and thus everybody can trust that it will act in a predictable manner.

Some smart contract projects can become quite complex, often to the point of becoming platforms in and of themselves. An emerging trend in these smart contract platforms is the issuance and use of *tokens*. In the ideal scenario, tokens derive their underlying value from some use case which is endogenous to the smart contract platform in question and that isn't just a revenue stream from a centralized entity. (Many do not abide by this standard however, and are for lack of a better phrase glorified scams at worst or Howey Test violating unregistered securities at best.)

As a quick example of what I consider to be one of the more legitimate tokens, Brendan Eich, the creator of the Javascript programming language, the Firefox web browser, and the Mozilla Foundation, is working on an Ethereum-based project called the Basic Attention Token (BAT). The purpose of the BAT is to fix online advertising, which has become plagued in recent years with value-leeching middlemen engaging in large-scale privacy violating schemes and cross site user tracking. The BAT enables advertisers to make micropayments directly to publishers in exchange for giving them users' attention. Additionally, users themselves can profit in exchange for their attention, such as by sitting through a 2-minute video and being paid a small cut of the revenue for that impression in BAT tokens. The BAT white paper is a good example of a token project and can be found at http://basicattentiontoken.org/

This all leads to what many people consider the hottest trend in the blockchain space: ICOs, or initial coin offerings. ICOs are a new type of crowdfunding model for primarily Ethereum-based projects that want to issue tokens to users. The premise is simple - users send one of the larger, more established cryptocurrencies (such as Bitcoin or Ethereum) to the project in question, and the project then gives the user some amount of tokens in proportion to how much cryptocurrency was sent in.

There's no real legal framework in place for ICOs, leading to a wild west like gold rush of global capital pouring into these projects, many of which have dubious investment pitches and little to no actual invented product - at this point, the market consists mostly of white papers and dreams. And yet… for all the pets.com style disasters which will undoubtedly unfold, there may also be a new Amazon or Google among the litter.

All that being said, it appears that most ICO funding mainly consists of investors who are either trying to ride the cryptocurrency bubble in a 'greater fool' game of musicals chairs, or who are naive about blockchain investing and don’t know how to properly price the risk they’re taking with their capital. For instance, one of the basic tenets of investing in any ICO is the understanding that the smart contract project might fail for reasons that have nothing to do with the project itself - it could fail because Ethereum (the platform the smart contract is deployed atop of) fails - a distinct possibility given that the Ethereum network can only perform 15 transactions per second. Bitcoin is hamstrung at 4 transactions per second. Visa, by contrast, can perform up to 56,000 transactions per second.

Additionally, there’s the risk that with any new major updates to the Ethereum protocol, a bug will be introduced which could bring down the entire network. Imagine having to roll back the *entire Internet* for a day because a Russian hacker found a bug buried somewhere in millions of lines of code. This of course wouldn’t happen to the real Internet, but is an ever-present, unappreciated risk with blockchains. The core Ethereum developers are aware of these issues and are working as hard as they can to scale the network while maintaining security. That being said, Ethereum and its ICOs have a long hill to climb before the dream of trustless computing becomes a reality.