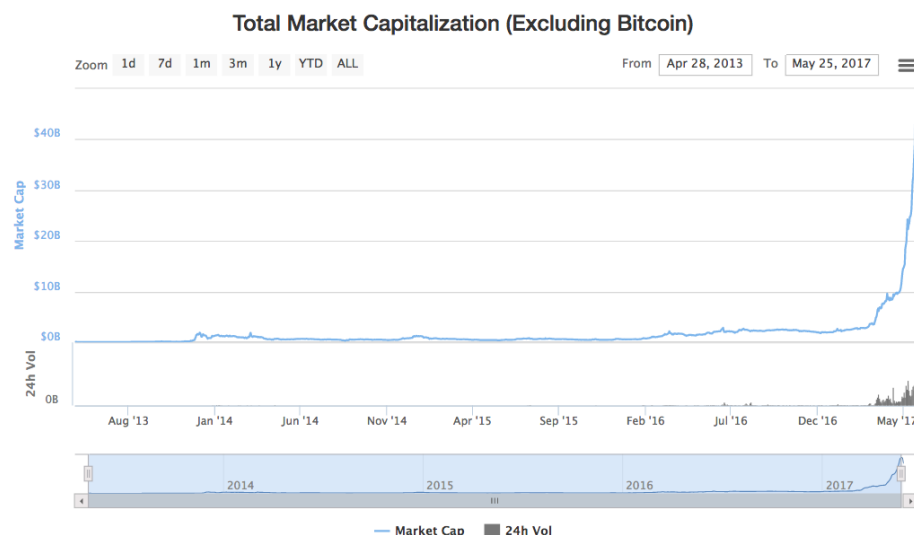Balaji S. Srinivasan [Follow]

CEO of Earn.com and Board Partner at a16z.com

May 27, 2017 · 11 min read

Thoughts on Tokens

Tokens are early today, but will transform technology tomorrow.

The exponential rise of non-Bitcoin tokens prior to the coming correction. Data from coinmarketcap.com/charts

In 2014, we wrote that "Bitcoin is more than money, and more than a protocol. It's a model and platform for true crowdfunding—open, distributed, and liquid all the way."

That new model is here, and it's based on the idea of an appcoin or token: a scarce digital asset based on underlying technology inspired by Bitcoin. While indisputably frothy, as of this writing the token sector sits at a combined market cap in the tens of billions. These new "fat protocols" may eventually create and capture more value than the last generation of Internet companies.

Here we discuss many concepts related to tokens, beginning with the basics for folks new to the space and then moving to advanced ideas.

The most important takehome is that tokens are not equity, but are more similar to paid API keys. Nevertheless, they may represent a >1000X improvement in the time-to-liquidity and a >100X improvement in the size of the buyer base relative to traditional means for US technology financing—like a Kickstarter on steroids. This in turn opens up the space for funding new kinds of projects previously off-limits to venture capital, including open source protocols and projects with fast 2X return potential.

But let's start with the basics first. Why now?

1. Tokens are possible because of four years of digital currency infrastructure

The last time the public at large heard much about digital currency was in late 2013 to early 2014, when the Bitcoin price last touched its then all-time high of $1242 dollars. Since then, several things happened:

- Bitcoin experienced a massive multi-year crash and recovery all the way down to $173 and back up to the recent all-time highs of $2800+

- Dozens of exchanges arose in many countries to facilitate the conversion of fiat currencies like dollars or yen into digital currencies like Bitcoin and Ethereum

- Major financial institutions began exploring the blockchain technology underpinning Bitcoin to build so-called "private blockchains" or distributed ledgers for internal or consortium use

- The programmable Ethereum blockchain launched, endured its own major crises, brought on major corporate support, and surged in value in early 2017

In 2013, the legality of digital currency was still in question, with many underline predicting death and others going so far as to call Bitcoin "evil". Those kneejerk headlines eventually gave way to Satoshi billboards in Davos and the Economist putting the technology behind Bitcoin on its cover.

By 2017, every major country has a digital currency exchange and every major financial institution has a team working on blockchains. The maturation of infrastructure and societal acceptance for digital currencies has set the stage for the next phase: internet-based crowdfunding of novel Bitcoin-like tokens for new applications.

2. Tokens vary in their underlying blockchains and codebases

To first order, a token is a digital asset that can be transferred (not simply copied) between two parties over the internet without requiring the consent of any other party. Bitcoin is the original token, with bitcoin transfers and issuances of new bitcoin recorded in the Bitcoin blockchain. Other tokens also have transfers and changes to their monetary base recorded in their own blockchains.

One key concept is that a token's codebase is different from its blockchain database. As an offline analogy, imagine if the US banking infrastructure was repurposed to manage Australian dollars: both are "dollars" and have a shared cultural origin, but a completely different monetary base. In the same way, two tokens may use similar codebases (monetary policies) but have different blockchain databases (monetary bases).

The success of Bitcoin inspired several different kinds of tokens:

- *Tokens based on new chains and forked Bitcoin code.* These were the first tokens. Some of these tokens, like Dogecoin, simply changed parameters in the Bitcoin codebase. Others like ZCash and Dash innovated on privacy-preserving features. Still others like Litecoin also began as simple tweaks to Bitcoin's code, but eventually became test grounds for new features. All of these tokens initiated

their own blockchains, completely separate from the Bitcoin blockchain.

- *Tokens based on new chains and new code.* The next step was the creation of tokens based on wholly new codebases, of which the most prominent example is Ethereum. Ethereum is Bitcoin-inspired but has its own blockchain and was engineered from the ground up to be more programmable. Though this comes with an increased attack surface, it also comes with new capabilities.

- *Tokens based on forked chains and forked code.* The most important example here is Ethereum Classic, which was based on a hard fork of the Ethereum blockchain that occurred after a security issue was used to exploit a large smart contract. That sounds technical, but essentially what happened is that a crisis caused the Ethereum community to split 90/10 with two different go-forward monetary policies for each group. A real world example would be if all the citizens of the US who disagreed with the 2008 bailouts changed in their dollars for "classic dollars" and adopted a different Fed.

- *Tokens issued on top of the Ethereum blockchain.* Examples include Golem and Gnosis, all based on ERC20 tokens issued on top of Ethereum.

In general, it is technically challenging to launch wholly new tokens on new codebases, but much easier to launch new tokens through Bitcoin forks or Ethereum-based ERC20 tokens.

The latter deserves particular mention, as Ethereum makes it so simple to issue these tokens that they are the first example in the Ethereum tutorial! Nevertheless, the ease with which Ethereum-based tokens can be created does not mean they are inherently useless. Often these tokens are a sort of public IOU intended for redemption in a future new chain, or some other digital good.

3. Token buyers are buying private keys

When a new token is created, it is often pre-mined, sold in a crowdsale/token launch, or both. Here, "pre-mining" refers to allocating a portion of the tokens for the token creators and related parties. A "crowdsale" refers to a Kickstarter-style crowdfunding in which internet users at large have the opportunity to purchase tokens.

Given that tokens are digital, what do token buyers actually buy? The essence of what they buy is a private key. For Bitcoin, this looks something like this:

```
5Kb8kLf9zgWQnogidDA76MzPL6TsZZY36hWXMssSzNydYXYB9KF
```

For Ethereum, it looks something like this:

```
3a1076bf45ab87712ad64ccb3b10217737f7faacbf2872e88fdd9a537d8
fe266
```

You can think of a private key as being similar to a password. Just like your private password grants you access to the email stored on a centralized cloud database like Gmail, your private key grants you access to the digital token stored on a decentralized blockchain database like Ethereum or Bitcoin.

There is one major difference, however: unlike a password, neither you nor anyone else can reset your private key if you lose it. If you have the private key, you have possession of your tokens. If you do not, you have lost access.

4. Tokens are analogous to paid API keys

The best existing analogy for tokens may be the concept of a paid API key. For example, when you buy an API key from Amazon Web Services for dollars, you can redeem that API key for time on Amazon's cloud. The purchase of a token like ether is similar, in that you can redeem ETH for compute time on the decentralized Ethereum compute network.

This redemption value gives tokens inherent utility.

Tokens are similar to API keys in another respect: if someone gains access to your Amazon API keys, they can bill your Amazon account. Similarly, if someone sees the private keys for your tokens, they can take your digital currency. Unlike traditional API keys, though, tokens can be transferred to other parties without the consent of the API key issuer.

So, tokens are inherently useful. And tokens are tradeable. As such, tokens have a price.

5. Tokens are a new model for technology, not just startups

Because tokens have a price, they can be issued and sold *en masse* at the inception of a new protocol to fund its development, similar to the way startups have used Kickstarter to fund product development.

The money is typically received in digital currency form and goes to the organization issuing the tokens, which can be a traditional company or an open source project funded entirely through a blockchain.

In the same way that boosting sales is an alternative to raising money, token launches can be an alternative to traditional equity-based financings—and can provide a way to fund previously unfundable shared infrastructure, like open source. A word of caution, though: read these three posts and consult a good lawyer before embarking on a token launch!

6. Tokens are a non-dilutive alternative to traditional financing

Tokens aren't equity, because they have intrinsic use and because they are non-dilutive to the company's capitalization table. A token sale is more similar to a Kickstarter sale of paid API keys than equity crowdfunding.

However, when considered as an alternative to classic equity financing, token sales yield a >100X increase in the available base of buyers and a >1000X improvement in the time to liquidity over traditional methods for startup finance. The three reasons why: a 30X increase in US buyers, a 20–25X increase in international buyers, and a 1000X improvement in time-to-liquidity.

7. Tokens can be bought by any American (>30X increase in buyers)

A token launch differs from an equity sale—the latter is regulated by the 1934 Act, while the former is more similar to a sale of API keys.

While equities can only be sold in the US to so-called "accredited investors" (the 3% of adults with >\$1 million in net worth), the US could not restrict the sale of API keys to accredited investors alone without crippling its IT industry. Thus, if tokens (like API keys) can be sold to 100% of the American population, it would represent an increase of 33x in the available US buyer base relative to a traditional equity financing for a US startup.

Do note, however: some people might want to issue a token and explicitly advertise it as a way to share in the profits of their efforts as a company. For example, the issuer might want to make token holders entitled to corporate dividends and voting rights, or make the company's total ownership stock denominated in tokens. In these cases, we really are talking about tokenized equity (namely securities issuance), which is very different than the appcoin examples we've discussed. Don't issue tokenized equity unless you want to be limited to accredited investors

under US securities laws. The critical distinction is whether the token is simply a useful and tradable digital item like a paid API key. Again: read these three posts and consult a good lawyer before embarking on a token launch!

8. Tokens can be sold internationally over the internet (~20–25X increase in buyers)

Token launches are typically international affairs, with digital currency transfers coming in from all over the world. New bank accounts receiving thousands of wires from all over the world in minutes for millions of dollars would likely be frozen, but a token sale paid in digital currency is always open for business. Given that the US is only ~4–5% of world population, the international availability provides another factor of 20–25X in the available buyer base.

9. Tokens have a liquidity premium (>1000X improvement in time-to-liquidity)

A token has a price immediately upon its sale, and that price floats freely in a global 24/7 market. This is quite different from equity. While it can take 10 years for equity to become liquid in an exit, you can in theory sell a token within 10 minutes—though founders can and should cryptographically lock up tokens to discourage short-term speculation.

Whether or not you choose to sell or use your tokens, the ratio between 10 years and 10 minutes to get the option of liquidity is up to a 500,000X speedup in time, though of course any appreciation in value is likely to be larger and more sustainable over a 10 year window.

This huge liquidity premium alone would cause tokens to predominate whenever they are legally and technically feasible, because the time to liquidity enters inversely in the exponent of the compound annual growth rate. Fast liquidity permits reinvestment in new tokens permits faster growth.

10. Tokens will decentralize the process of funding technology

Because token launches can occur in any country, the importance of coming to the United States in general or Silicon Valley / Wall Street in particular to raise financing will diminish. Silicon Valley will likely remain the world's leading technology capital, but it will not be necessary to physically travel to the United States as it was for a previous generation of technologists.

11. Tokens enable a new business model: better-than-free

Large technology companies like Google and Facebook offer extremely valuable free products. Despite this, they have sometimes come under fire for making billions of dollars while early adopters only receive the free service.

After the early kinks are worked out, the token launch model will provide a technically feasible way for tech companies (and open source projects in general) to spread the wealth and align their userbase behind their success. This is a better-than-free business model, where users make money for being early adopters. Kik is the first example of this, but expect to see more.

12. Token buyers will be to investors what bloggers/tweeters are to journalists

Tokens will break down the barrier between professional investors and token buyers in the same way that the internet brought down the barrier between professional journalists and tweeters and bloggers.

This will have several implications:

- The internet allowed anyone to become an amateur journalist. Now, millions of people will become amateur investors.

- As with journalism, some of these amateurs will do extremely well, and will use their token-buying track-record to break into professional leagues.

- Just like it eventually became a professional requirement for journalists to use Twitter, investors of every size from seed funds to hedge funds will get into token buying.

- New tools analogous to Blogger and Twitter will be developed that make it easy for people to use, buy, sell, and discuss tokens with others.

We don't yet have a term for this, but perhaps it will be "commercial media" by analogy to "social media".

13. Tokens further increase the primacy of the technologist over the traditional executive

Since the rise of Bill Gates in the late 70s, there has been a trend towards ever more tech-savvy senior executives. This trend is going to accelerate with token sales, as folks who are even more predisposed to the pure computer science end of the spectrum end up founding valuable protocols. Many successful token founders will have skillsets more similar to open source developers than traditional executives.

14. Tokens mean instant custody without intermediaries

Because token buyers need only hold private keys to guarantee custody, it changes our notion of property rights. For tokens, the final arbiter of who possesses what property is not a national court system but an international blockchain. While there will be many contentious edge cases to work through, over time blockchains will provide "rule-of-law-as-a-service" as an international, programmable complement to the Delaware Chancery Court.

15. Tokens may be generalizable to every tech company through paid logins

Can the token model can be extended beyond pure protocols like Bitcoin, Ethereum, or ZCash? It's not hard to imagine selling tokens as tickets—for access to logins, to car-rides, to future products. Or distributing them as rewards to the authors who power social networks and the drivers who power ride-sharing networks. Eventually, tokens can be extended to hardware as well: every time someone buys a slot in line for a Tesla Model 3 or re-sells a ticket, they're exchanging a primitive token. But the model will need to work for protocols first before being generalized.

Conclusion

The token space is very early, and is likely to experience a dramatic correction over the next few weeks. To deal with the coming profusion of tokens we will need review sites like Coinlist, portfolio management tools like Prism, exchanges like GDAX, and many other pieces of supporting technical and legal infrastructure.

But the world has changed. Tokens represent a 1000X improvement over the status quo, and those don't come around very often.

PS: If you thought this post was interesting, go join the list at Earn.com/digital-currency/join. You'll get notified of several upcoming token launches.

Thanks to my friend and colleague Naval Ravikant for helping think through many of the ideas in this post! Go follow him on Twitter at @naval.