Alchemy Capital

Investment Thesis

Kevin Xu

April 2018

Introduction

When citing the benefits of blockchain technology, people often talk about the data integrity, disintermediation, and removal of central authorities. However, I believe the biggest benefit is one that is rarely mentioned: data changing from being a privately owned asset to a publicly shared resource. In a blockchain, each participant has an equal opportunity to access and change the underlying data. This is a huge paradigm shift that will significantly impact the way we interact with our applications and build our systems in the future, by drastically reducing cost to market for new startups and creating possibilities for entirely new business models.

Today, the baseline cost of entry to the market for tech startups is to build out their own data infrastructure and deploy it to servers. However, many of the software components they build in the process are redundant. User accounts, authentication portals, payment processing, and reputation systems are just a few of common features that need to be built and rebuilt across many application stacks. As a result, every time a new application is developed, the startup behind it must dedicate significant resources to effectively reinvent the wheel.

To further complicate things, each startup must build their own network and marketplace to compete successfully. They must seed their platform with users, drivers, homes, content—whatever drives the network effects. Network effects are non existent on empty platforms, so startups subsidize their network in order to grow and scale their platform. This is incredibly expensive, and the reason many startups choose to raise a lot of capital while operating at significant losses for years in pursuit of network growth.

Because of these costs, entries to barrier are high for a technology company to compete with incumbents. Blockchain technology—specifically, sharing data resources—changes all of this, by abstracting away technological redundancies and aggregating all the network effects into what is essentially a public utility.

Throughout history, marginal costs go down as business concerns become abstracted into a third party services that use economies of scale to create cost efficient alternatives. One

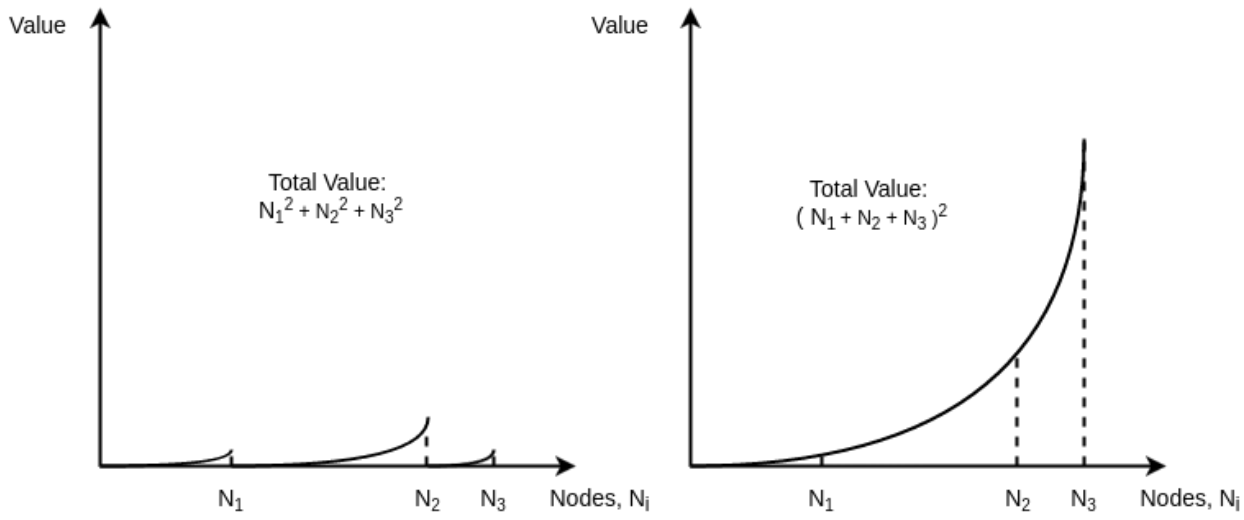
example of this is Amazon's fulfillment service for online ecommerce: by shipping on behalf of all the stores using their service, Amazon can coordinate logistics to create more efficient distribution channels than any individual business could do on its own. This in turn reduces the operational costs for any online retail business that uses it. Cloud infrastructure is another example—by abstracting away the responsibilities of physical server management, startups can save significantly on the costs of deploying software.

Blockchain technology, similarly, abstracts away the costs of building and maintaining the data layer for a given business vertical with protocols. Startups using a shared blockchain protocol avoid needing to build proprietary backend solutions, deploying servers, or aggregating network effects, because it is all handled within smart contracts on the blockchain infrastructure. This drastically decreases the cost to market for new startups, allowing them to focus purely on the building better service layers for end users.

Applications on a shared protocol have equal access to the underlying data, meaning that they get no competitive advantages from network effects. Rather, they compete on margins, since everyone using the same protocol has relatively the same marginal cost. This means that in order to be successful, startups using the same protocol must find innovative market niches and provide the best services.

This is similar to how telephone networks operate today: any phone, regardless of service provider, is able to call any other phone. This is the case because telecom companies know it is vastly more valuable to their customers if phone calls are platform agnostic. Telephones, regardless of the service provider, would be significantly less valuable if Verizon phone calls were restricted to other Verizon phones, or if AT&T used their own phone numbering system.

The reason for this is due to something called *Metcafe's Law*, which states that the effect of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). Since each new telephone added is more valuable than every other telephone added before it, the summed value of all the fragmented networks will never be larger than the value of those networks aggregated together, which the picture below describes.



Source: https://blog.0xproject.com/the-difference-between-app-coins-and-protocol-tokens-7281a428348c

As users join a network, they have low switching costs to other services within that network. As a result, while applications within a protocol compete with each other to provide the best services, more value accumulates at the protocol layer than to any individual application. Ultimately, applications using the same protocol are actually pooling their network effects to compete with incumbent networks trying to do the same thing.

In my opinion, the best investment opportunities currently in the space are protocol layer developments, and many smart investors have caught on. However, almost all these investors have employed the wrong strategy of acquiring and holding 'utility tokens' associated with these protocols, with false assumption that tokens are analogous to equity in the networks they power.

While protocols are the right investments, I believe that buying utility tokens directly is an inefficient allocation of capital that produces suboptimal returns in the long run. Any investor looking to hold utility tokens has a lack of understanding about their role in a network and what they should actually do. So, before explaining any further, I first need to share my philosophy on utility tokens.

The Role of the Utility Token

Utility tokens are a necessity for creating healthy and valuable blockchain protocols. The value of a blockchain protocol comes from its network effects, which is highly dependent on how the network is designed. Tokens shape the design of a network by attaching costs and rewards to specific behaviors, coordinating incentives across self-interested individuals to behave in ways that are beneficial to the network as a whole. Most importantly, utility tokens should exist only to provide incentives for systems that wouldn't work without them.

One utility token use case is for the tokens to bear the social cost of leveraging shared resources. Shared resources often run into a *tragedy of the commons* problem: an economic term where individual users acting in their own self-interest behave contrary to the common good by depleting or spoiling a shared resource through collective action. Shared protocols are a of shared resource, and are exposed to the same problem.

An example of this that exists today is email. The concept of 'email' is actually a shared protocol called SMTP that allows anyone to send messages to an email address. The shared resource in this network is attention—the time spent curating and evaluating each incoming message to see if it is worth opening. Since email senders don't incur the cost of the receiver's attention, they can send messages thinking about if receiver even wants to read it, resulting in tons of spam mail throughout the system.

Tokens on a blockchain protocol can fix this by representing the cost of our attention. Every time a sender sends an email, they must lock up an 'email utility token'. This token is unlocked and returned only if the message is opened within 15 days. Now with this mechanic, the cost of sending an email is dependent on the expectation of its recipient opening it. Spammers in this system will incur significant costs while normal users are relatively unaffected.

To improve on this further, senders can lock up additional tokens to signal importance. Email inboxes could then have an option to be sorted based on tokens locked: the more

urgent the message, the more the sender is willing to risk. This essentially creates a prediction market for the value of personal attention, with each unit of attention represented by a token.[1]

What is more important is the significance of *holding* these tokens. Having tokens grants a certain 'capacity of attention' that can be attached to outgoing messages at any given time. In this case, the most effective holders of these tokens are applications that run on the protocol, like a Gmail or Hotmail—or someone running a private server at home.

In this scenario, applications would most likely abstract all the token interaction away from the end users to reduce friction, just like how email clients abstract away SMTP today. They would buy the tokens on an exchange proportional to the scale they intend to serve, then take on the holding risk of the tokens. The services would pass on estimated 'unopened email' costs to their users in the form of monthly subscription fees and could even denominate the cost in USD and charge credit card—the user wouldn't even know there are tokens involved.

Another use case for utility tokens is to change the payout schemes for participants in a network. An example of this is a token that I designed for a decentralized poker platform called Virtue Poker. In this network, players are able to participate in peer-to-peer online poker without the need of a site to host and operate the game.

To prevent any cheating or malicious behavior, each table has an operator called a "justice." Justices are third-party nodes that anyone can run as software on their own computer, and they collect a portion of each pot as service fees, similar to table rake. Since the pot size is relative to the blinds of the table, justices make more money operating higher stakes games.

Tokens are essential to this system to function because in their absence, justices have the incentive to collude with players at their table. By using tokens to lock up value as a

[1] As a side note, it would be interesting to see the differences in the relative value of attention for different people, depending on their popularity. Public figures and company executives would probably see much higher 'bids' for their attention.

“security deposit”, proportional to the blinds of the game they operate, the incentives for justices change by eliminating any potential profit from cheating.

For example, operating $0.01/$0.02 games may require 5,000 staked tokens while $5.00/$10.00 games may require 100,000 staked tokens. As long as the value of tokens required to operate a game always supersedes the potential rewards from colluding, justices have more to lose than gain by misbehaving. In this context, the utility tokens most closely resemble a unitized license to lend computing resources to a decentralized poker platform, and secure the integrity of the platform.

In both the email and poker protocols, the tokens have a clear intrinsic value: the future discounted cash flows of all the fees collected by providing a service. However, that value is only attributable to those who actually provide *work* in the ecosystem. As a result, a speculator simply holding on to the token and not actually using it for its intended purpose will not be able to capture as much value from it as an actual user.

This makes sense, as real users will only purchase tokens if the value derived from it’s usage is worth more than cost to acquire it. By definition, users always derive more value from utility tokens than a passive speculator, because leveraging the value of the utility generate cash flows on top of the nominal cost of the token. By holding tokens and not using them, investors are not capitalizing on the potential of the assets they hold. It is comparable owning taxi medallions without operating taxis, or owning real estate without renting it out.

What is great is that the net present value of these tokens are strongly correlated with two things in particular: demand in the network and efficiency of the service provided. As demand in a network grows, existing services become more valuable. As more work is performed, more revenues are generated. The real financial opportunities from a blockchain protocol are in the services that can be provided, and how best to provide them—not in which tokens to buy.

Capturing Value from Shared Protocols

The main difference in my philosophy is that the price of the token should represent the cost to provide services on a network, rather than the total value that the network generates. As marginal costs decrease from technological advancements in blockchain infrastructure, the majority of the costs to enter a market will shift towards acquiring utility tokens for a protocol to be built on, rather than building redundant systems.

I also believe that revenue-generating service providers will be an important part of a decentralized protocol, despite the common belief that all middlemen will be disintermediated. Because the value of tokens increase with efficiency of use, companies will still exist by taking advantage of cost efficiencies through economies of scale. A company that runs Virtue Poker nodes can achieve significantly higher cash flows per token than a random guy with a computer because the company can optimize for server cost efficiencies and system uptime.

To speculate on the value of blockchain protocols, then, investors shouldn't purchase utility tokens directly. Rather, they should invest in the entities that use the tokens. Since properly designed tokens will be held, entities using a shared blockchain protocol will have an inventory of utility tokens. Investments made as normal equity into these companies still have exposure to the token appreciation via the balance sheet, but now also include the cash flows from using the token for its intended purpose.

Since the net present value of the tokens are dependent on their cash flows, they have the highest value when held by service providers with largest margins and highest uptime. As a result, even within a single utility token, there is a significant variance in investment opportunities, and identifying the best ones can result in significantly more returns.

Investment Strategy

The space is still nascent, and the best opportunities have yet to come. Competing protocol standards will arise and challenge incumbents, as philosophies and ideas are debated and implemented. In the end, the protocols that succeed are the ones able to find adoption

quickly and aggregate the most network effects. Ultimately, these depends on two things: cryptoeconomic design for long term stability of the network, and product and business execution from the founding team to grow it quickly.

Over the next 1-2 years, I will seed a portfolio with different blockchain protocols best positioned to disrupt their incumbents. Investments will be made as early as possible, at the ideation and development stage, where I can add the most value by being involved in the cryptoeconomic design and protocol architecture. I want to work with teams with strong executional capacity that have strategic partnerships or access to legacy networks to bootstrap usage of their protocol quickly.

As the market matures, and more service providers align themselves with certain protocols, I will prune the portfolio for protocols that taper off, and add exposure to the growing protocols by investing in other companies using the same token. I believe this is a good strategy for optimizing both risk and return: protocols that grow the most are most likely to grow more due to their network effects.

Ultimately, my goal is to separate each set of companies based on the token they use to create 'protocol indexes'—a diversified set of companies that generate separate revenue streams while holding the same utility tokens. Each index will serve as the investment vehicle for both the utility token value and operational fees, the same way a REIT is an investment vehicle for both real estate property value and management fees. For now, this might be a little far off, so this is where I'll end the summarization of my strategy.

Investable Assets and Security Tokens

One of the primary appeals of utility tokens to speculators is the instantaneous global liquidity. Traditional securities, especially equity private placements, do not have this luxury, and usually take years to exit. This is most likely why startups and investors alike have begun to prefer tokens over equity.

I believe tokens will still be used as a fundraising mechanism in the future, but in the form of tokenized securities rather than thinly disguised 'utility tokens'. Security tokens will be

issued and treated with the same regulations as securities, but have the liquidity properties of tokens. Any positions I take will be in security tokens, or future convertible to security tokens.

Security tokens will revolutionize financial markets in their own right, and these are the investment instruments that I'm most interested in. By being able to exist within smart contracts, entirely new financial models can be created. Revenue sharing agreements, tokenized balance sheets, and all sorts of debt instruments are the first possibilities that come to mind. Even dividends and yields can even be delivered directly to token addresses.

I see a future where tokens make applications better and investments more effective. In this world, users have more agency with their data, and investors have more opportunity with their capital. With my understanding of cryptoeconomics and finance, I believe I can make significant contributions towards building that world. If you share my vision and want to join me in my journey, please be in touch.

Thank you.