FEBRUARY 13, 2018

NEW MODELS FOR UTILITY TOKENS

BY KYLE SAMANI

There are three types of cryptoassets: stores of value, security tokens, and utility tokens. General-purpose stores of value should be valued using the equation of exchange (https://en.wikipedia.org/wiki/Equation_of_exchange) because these currencies are independent monetary bases. Examples include Bitcoin (https://bitcoin.org/), Bitcoin Cash (https://www.bitcoincash.org/), Zcash (https://z.cash/), Dash (https://www.dash.org/), Monero (https://getmonero.org/), and Decred (https://www.decred.org/).

Although some may disagree, I also include the native tokens of smart contract platforms such as Ethereum (https://www.ethereum.org/), EOS (https://eos.io/), Dfinity (https://dfinity.org/), and Kadena (http://kadena.io/) in this category. Why? Because there's a real chance that the native token of a smart contract platform that becomes sufficiently useful will emerge as an independent store of value.

I won't touch on security tokens in this essay as traditional securities are widely understood. Moving securities onto a blockchain, while better than legacy systems in terms of settlement times and custodianship, doesn't change anything about the nature of the security itself.

This essay will focus on utility tokens.

Background

The vast majority of ICOs that launched in 2016 and 2017 were utility tokens that also acted as proprietary payment currencies. These include many of the highest-profile projects: Filecoin (https://filecoin.io/), Golem (https://golem.network/), 0x (https://0xproject.com/), Civic (https://www.civic.com/), Raiden (https://raiden.network/), Basic Attention Token (https://basicattentiontoken.org/), and more.

Each of these cryptocurrencies is presenting itself as a freestanding monetary base. Monetary bases should be valued using the equation of exchange (https://www.investopedia.com/terms/e/equation_of_exchange.asp): MV = PQ. Therefore M = PQ/V.

As I noted in Understanding Token Velocity (https://multicoin.capital/2017/12/08/understanding-token-velocity/), the V in the equation of exchange is a huge problem for basically all proprietary payment currencies. Proprietary payment currencies are, generally speaking, susceptible to the velocity problem, which will exert perpetual downwards price pressure. Due to this effect, I expect to see utility tokens that are just proprietary payment currencies exceed a velocity of 100. Velocities of 1,000 are even possible. As a point of reference, the USD M1 supply has a velocity of 5.5 (https://fred.stlouisfed.org/series/M1V).

Below I'll present two new token economic models that address the velocity problem for utility tokens. Both models are primarily designed to optimize for the following:

The price of the utility token should increase approximately linearly with usage of the network.

Of course, the corollary to this is that the price of the native token should decrease if usage of the network falls, or grows more slowly than previously forecast.

Work Tokens

Augur (https://augur.net/) is the pioneer of the work token model. Keep (https://keep.network/) is another example.

In the work token model, a service provider stakes (AKA bonding) the native token of the network to earn the right to perform work for the network. For services which are commodities such as Keep (off-chain private computation), Filecoin (distributed file storage), Livepeer (https://livepeer.org/) (distributed video encoding), Truebit (https://truebit.io/) (off-chain verifiable computation), and even "decentralized mechanical Turk" powered by humans such as Gems (https://gems.org/), the probability that a given service provider is awarded the next job is proportional to the number of tokens staked as a fraction of total tokens staked by all service providers.

The beauty of the work token model is that, absent any speculators, increased usage of the network will cause an increase in the price of the token. As demand for the service grows, more revenue will flow to service providers. Given a fixed supply of tokens, service providers will rationally pay more per token for the right to earn part of a growing cash flow stream.

Most work tokens systems enforce some sort of mechanism to penalize workers who fail to perform their job to some pre-specified standard. For example, in Filecoin, service providers contractually commit to storing some data for a period of time. During the life of the contract, service providers must lock up some number of Filecoin, and the file must be available 24/7 with some minimum bandwidth guarantee. If the service provider does not adhere to this standard, she's automatically penalized by the protocol, and some of her staked tokens are slashed (taken away).

The valuation model for work tokens is simple: net present value (https://www.investopedia.com/terms/n/npv.asp) (NPV).

Relative to the traditional "tokens as money" model, the work token model completely changes the terminal value calculation of a utility token. Let's consider Filecoin to highlight the magnitude of the discrepancy.

The Filecoin team has suggested that their target market is $110B (https://coinlist.co/assets/index/filecoin_index/Filecoin-Primer-c74e73db1d65598ca171397df9d219de6b7a7ef80a4886bb152c01883aea7e79.pdf) (page 16) in 2021. These figures are based on the legacy model of buying hard drives with the express intent of renting them out, rather than leveraging what is otherwise unused capacity. Filecoin is likely to offer to substantially lower unit prices. Let's be conservative and assume that Filecoin doesn't reduce prices at all.

Filecoin, using the "token as money" model, will have a high velocity. The velocity will not approach infinity—there is an upper limit because storage providers in the Filecoin network must post a deposit before storing files. The exact mechanics of this staking system are not yet set. Regardless, this mechanism guarantees some upper bound on the velocity of Filecoin tokens (similarly, transaction fees also impose some upper bound; however, that upper bound is likely to be so high as to be irrelevant in the context of this essay).

The velocity of the USD M1 is about 5.5 (https://fred.stlouisfed.org/series/M1V). Prior to the financial crisis (in which the Federal Reserve approximately doubled the money supply), the velocity was about 10. But 10 isn't a realistic assumption for Filecoin. Given that Filecoin isn't intended to be general-purpose money, and that there's not a compelling motivation to hold Filecoin beyond the minimum staking requirements, I'll assume 3-10x higher velocity than USD M1. This implies a velocity of 30-100.

The terminal value for Filecoin—assuming 100% market saturation— is therefore somewhere in the range of $1.1B-$3.6B ($110B/100 and $110B/30).

Now, let's consider Filecoin's potential terminal value in the work token model. Terminal value can be calculated as cash flow / discount rate. Assuming a discount rate of 40% (http://people.stern.nyu.edu/adamodar/pdfiles/papers/younggrowth.pdf) and operating margins of 50%*, the potential terminal value of Filecoin is $110B x 50% / 40% = $137.5B.

The work token model captures ~100x more value than the proprietary payment currency model.

How is this possible?

Considering utility tokens as a proprietary payment currency, terminal value will trend towards a value that's a fraction of transaction volume. Why? Because, per the equation of exchange, M = PQ/V, and assuming a V > 1, M must be less than PQ.

On the other hand, if you instead use a utility token as a right to perform work on behalf of the network, it becomes valued at a multiple of the operating cash flows that the system generates rather than as a fraction of revenues paid to service providers**. Moreover, in the work token model, as a network grows and matures, it will de-risk, decreasing the discount rate, and ultimately increasing the terminal value (this actually implies that total token value should grow super-linearly relative to transaction throughput).

The work token model only works if the service being provided is a pure commodity. If suppliers compete on other variables, such as marketing, customer service, go-to-market strategies, etc. then the work token model doesn't work. The work-token model is predicated on assigning new jobs to service providers based on their staked tokens. This is not amenable to service providers who must actively compete for customers. In these types of networks, another model is necessary.

Burn-And-Mint Equilibrium

Factom (http://factom.com) is the pioneer of the burn-and-mint equilibrium (BME) model, and is to the best of my knowledge the only token with a substantial network value that implements this model. (Factom is providing a commodity service that could be implemented as a work token; however, they chose to implement BME instead.)

In the BME model, unlike the work token model, tokens are a proprietary payment currency. But unlike traditional proprietary payment currencies, users who want to use a service do not directly pay a counterparty to use the service. Rather, users burn tokens.

Yes, the customer burns the money.

When the customer burns the money, they do so in the name of the service provider. That is, the customer publicly acknowledges (on chain) that the service provider did the work for the money that was burned.

The amount of token burned to access the underlying service should be denominated in USD. For example, in Factom, the cost of committing an entry to the Factom blockchain is $.001, regardless of the price of Factoids (FCT) in USD.

Independently of the token burning process, the protocol should mint X new tokens per time period, and allocate those tokens to service providers ratably: If 1 of 50 tokens burned during a token minting period were in the name of Service Provider A, then Service Provider A should receive 2% of newly minted tokens.

Note that X does not have to be static. It can be variable, so long as X is not a function of burned tokens (this would create circular logic, and ultimately defeat the purpose of BME).

On the surface, it seems like this model could create scenarios in which service providers are under or overpaid. However, in practice, if the system is running near equilibrium state, then service providers will be paid the appropriate amount.

Also note that in the case of Factom, service providers and block producers are the same. For ERC20 tokens, this is by definition not true since the Ethereum network abstracts block production. However, the BME model can be adopted for ERC20 tokens.

Like the work token model, the BME model creates a model in which linear growth in usage of the network causes linear, non-speculative growth in the value of the token.

Let's walk through an example that assumes no market speculators. I'll assume the following:

Tokens minted per month: 10,000

Cost of token in USD: $10.00

Unit cost of service: $.001

The system will be in equilibrium—meaning that the number of tokens in circulation remains unchanged— if 10,000 tokens are burned per month. Since the cost of using the service is $.001, the system will be in equilibrium if the service is used (10,000 * 10)/.001 = 100,000,000 times per month. If usage grows and 15,000 tokens are burned in a month, then total supply will decrease, creating upwards price pressure. This upwards price pressure means fewer tokens need to be burned to purchase the same amount of service from the network, bringing the system back into equilibrium.

The same system works in reverse: If usage slows and more tokens are minted than burned in a given month, supply increases, creating downwards price pressure, meaning more tokens have to be burned for the same amount of service, bringing the system back to equilibrium.

This model assumes that both consumers and service providers never want to actually hold the proprietary payment currency. Rather, this model assumes that service providers only want to hold general purpose currencies.

Note that this model doesn't require that the service being provided is a commodity. The ratable redistribution of newly minted tokens allows service providers to price their service however they see fit.

Given that there will always be excess supply floating in the market as Menger Goods (http://unenumerated.blogspot.com/2016/02/two-malthusian-scares.html), there isn't a universal formula model that can be used to calculate non-speculative value. Regardless, the following can be generalized:

Price should increase if # of tokens burned > # of tokens of minted

Price should decrease if # of tokens burned < # of tokens of minted

When To Use Each Model

Given that work tokens capture far more value than BME tokens, teams should try to implement work tokens whenever possible. However, the work token is not universally applicable. Work tokens are applicable for most decentralized cloud services such as Filecoin, Keep, Truebit, and Livepeer. These services can use the work token model because they provide undifferentiated commodity services. Additionally, work tokens can be used for services that require human input such as Augur or Gems.

Even systems like Filecoin that offer different levels of service—e.g., amount of redundancy—can adopt the work token model.

Most other services should use the BME model: Civic, Golem, Raiden, Basic Attention Token (BAT), 0x, etc. In these models, service providers aren't providing a pure commodity. They're competing on variables that are out of band relative to the protocol itself. Service providers on the Civic network compete on business development and partnership development. 0x relayers compete on UX, quality of API, SLAs, tokens listed, and more. Web publishers compete on differentiated content in the BAT network.

ICOs and Token Distribution

For tokens that employ the work token model, development teams don't really need to worry about token distribution. Why? Because end users don't ever need to purchase the token. Service providers seeking yield on underutilized computing/storage/bandwidth resources will figure out how to make money on underutilized hardware relatively quickly. Services like AwesomeMiner (http://www.awesomeminer.com/) will emerge for work token-based staking protocols that dynamically allocate one's resources to the most profitable network. 1protocol (https://1protocol.com/) is already working on this.

Unfortunately, the BME model doesn't provide this same benefit. Systems that implement the BME model will still need to get their tokens in the hands of millions of people so that end users can use the service.

Pricing (Of Services)

In systems using work-tokens, the unit price of the service needs to be set at the network level. Individual service providers cannot set pricing. Relative to the free-market approach of Filecoin (every miner sets her own price in a hyper-competitive market), this sounds worse. However, in practice, there will be competition, not between providers in the same network, but among providers across different networks. This is similar to how Amazon and Google set prices for storing 1GB of data in their respective cloud offerings.

In systems implementing BME, every service provider can set her own price.

Governance

For tokens that implement the generic "tokens as money" model, many entrepreneurs assume that users will have a say in governance. This is unlikely to be true in practice. Because of the velocity problem, consumers won't hold tokens, so they're unlikely to vote in stake-based governance models. Why spend time voting on governance issues when you only intend to hold the token for ten seconds at a time?

The work token model embraces this truth by moving stake-based voting exclusively to the supply side of the market. This feels a lot more like decentralized equity in the sense that traditional equity holders vote on what the company (supply side) should do in the context of a competitive marketplace.

In the BME model, tokens are still acting as money. It's unclear how the BME will impact stake-based voting governance, if at all, relative to the proprietary payment currencies that don't implement BME.

Network Effects

Neither of these models should materially affect network effects relative to the generic "tokens as money" model. Network effects for utility tokens are not based on liquidity of the token itself. They're based on the intrinsic nature of the protocol. For example, the network effect in 0x isn't the liquidity between ETH and ZRX, but rather the network effect of the global liquidity pool of all trading pairs using the 0x protocol. If ZRX tokens adopt the BME model, the global liquidity pool will remain unchanged. Similarly, the network effect of Filecoin, which should be approximately log(n) (due to decreasing value per marginal miner as you approach global saturation), should not be materially different as a work token versus proprietary payment currency.

Scaling Work Token Networks

In the work token model, some interesting phenomena emerge as the network grows in usage and value.

Let's say that at time of network launch, I own 1% of all Keep tokens, that the entire Keep network can be powered by 300 mid-range AWS servers, and that there are no market speculators. In order to perform this work, I need 3 mid-range AWS servers. Let's then say that, over the next year, demand for Keep tokens grows 100x, and that I don't sell any tokens. In order to service that demand I'll need to manage 300 servers.

But I don't want to manage 300 servers. That's just too complicated for me.

What now? I can just sell my tokens on the open market. The market should rationally value the tokens at 100x what they were valued at a year ago, because the cash flows going through the network are 100x what they were a year ago.

If the network grows faster than I can grow as a service provider, that's ok. I can just sell my tokens to someone else. I may even be able to lend out my tokens to someone else by using 1protocol or something similar.

Synthetic Tokens

Nothing about either of these models assumes that a given token exists on a single smart contract platform. Both the work token and BME models are compatible with synthetic tokens that live across chains as described in The Smart Contract Network Effect Fallacy (https://multicoin.capital/smart-contract-network-effect-fallacy/).

Conclusion

For the first time, Ethereum provides a canvas for developers, service providers, and consumers to transact using programmable money. Work tokens and the BME model are just two examples of the opportunities created by programmable money. The design space for programmable money is wide open and totally unexplored. New models and mechanics will emerge.

As the crypto ecosystem matures, developers will experiment, tweaking and building on the ideas presented in this essay. As they do, they'll find new and creative ways to capture value in the native tokens of their networks without degrading user experience.

Lastly, I welcome your feedback. Please email research@multicoin.capital (mailto:research@multicoin.capital) with questions and ideas. I presented a tremendous amount of material in this essay. I look forward to learning from the public and iterating on the ideas and designs presented in this essay.

Thanks to Tushar Jain and Myles Snider (Multicoin Capital), Matt Luongo and James Prestwich (Keep), Jon Choi (Ethereum Foundation), Will Peets (Passport Capital), Matt Huang (Sequoia), Gustav Simonsson (Orchid), and the others who provided input on this essay.

End Notes

* Although 50% operating margins are high for a hardware business, Filecoin differs in that there is no hardware cost since the hardware was otherwise going to generate $0 revenue. Also, most service providers in the Filecoin network are unlikely to have any overhead (no rent, no employees, etc.)

** Note that this is not a "like-to-like" comparison. It's comparing apples-to-oranges. "Tokens as money" are valued as a fraction of revenue paid to service providers, whereas work tokens are valued as a multiple of cash flows. Cash flows are inclusive of operating expenses. Revenues paid to service provider are not.

A bug in BME: There is one problem with the BME model: arbitrageurs. This problem is best understood using a simple example. Let's say that a protocol implementing BME mints 100 tokens per 24 hour period. If, at 23 hours and 50 minutes, only 50 tokens have been organically burned, arbitrageurs are incentivized to arbitrarily burn up to 49 additional tokens in their own name, as they're guaranteed a positive ROI.

This is problematic because this means that the tokens implementing BME will be perpetually deflationary. Arbitrageurs guarantee that the supply will never inflate, even if organic demand for usage of the service decreases.

You can reduce the scope of this problem by reducing the time interval to a single block, which is about 15 seconds in Ethereum. Using a time period of a single block, arbitrageurs have nothing to arbitrage. However, with a minting schedule this short, miners are incentivized to act as arbitrageurs as described above by manipulating (https://blog.keep.network/miners-arent-your-friends-cde9b6e0e9ac) transaction ordering in blocks.

A solution to this problem is to use a commit/reveal scheme (https://en.wikipedia.org/wiki/Commitment_scheme#Bit-commitment_in_the_random_oracle_model). Will Warren of 0x describes commit-reveal schemes in this (https://blog.0xproject.com/front-running-griefing-and-the-perils-of-virtual-settlement-part-2-921b00109e21) essay. In the future, this may be addressable using zk-SNARKs.

Factom doesn't have to deal with this problem because Factom uses a federated network model in which there are a fixed number of known service providers. Also, each federated server is guaranteed equal payment.

(https://www.facebook.com/sharer/sharer.php?u=https://multicoin.capital/2018/02/13/new-models-utility-tokens/)
(https://twitter.com/home?status=Check out this great post by Kyle Samani https://multicoin.capital/2018/02/13/new-models-utility-tokens/)
(https://www.linkedin.com/shareArticle?mini=true&url=https://multicoin.capital/2018/02/13/new-models-utility-tokens/&title=New Models For Utility Tokens&summary=&source=)

BROWSE CATEGORIES

(https://multicoin.capital/category/crypto-insights/)

Crypto Insights (https://multicoin.capital/category/crypto-insights/)

(https://multicoin.capital/category/asset-valuations/)

Asset Valuations (https://multicoin.capital/category/asset-valuations)

(https://multicoin.capital/category/news/)

News (https://multicoin.capital/category/news/)

‹ Previous (https://multicoin.capital/2018/01/27/opportunity-interoperable-chains-chains/)

(https://multicoin.capital/?blog)

SUBSCRIBE FOR THE BEST RESEARCH AND INSIGHTS IN CRYPTO

Email address... SUBSCRIBE

(http://angel.co/multicoin-capital)

(https://twitter.com/multicoincap)

in (https://www.linkedin.com/company/24776833/)