Cryptoasset valuation techniques

Lanre Ige

Researcher and Content Manager @Mosaic.io | @LanrayIge

Thanks to Andrew Hawley and Dr Garrick Hileman for comments.

Introduction

There is growing interest in cryptoasset valuation techniques and frameworks. In this article I will briefly review various valuation frameworks and critique their assumptions and findings. Specifically, I examine:

1. Adam Hayes's cost of production method
2. Ken Alabi's Metcalfe's Law framework
3. Chris Burniske's use of the Equation of Exchange
4. Comparables such as the Network Value to Transactions ratio

1. Hayes's Cost of Production method

Overview

One interesting and intuitive approach to cryptoasset valuation has been the Cost of Production method by Adam Hayes[1]. He argues that the cost of production price of a single bitcoin can represent a value around which the market price of a bitcoin will gravitate. Bitcoin mining requires miners to expend computation effort to successfully carry out Bitcoin's Proof of Work (PoW) algorithm; this, in turn, requires electrical consumption for operation. One can model bitcoin production as a competitive market, therefore, where miners produce (or should produce) until their marginal costs equal their marginal product.

Miners are driven by the expectation of profit.[2] They compete against other profit motivated miners and the greater the computational effort of a given miner, the greater the probability of a miner successfully mining a given block and being rewarded with bitcoins.[3] Moreover, the probability of a miner successfully mining a block also depends on the current mining difficulty which the Bitcoin network adjusts dynamically (every 2016 blocks) to always ensure that a block is mined once every ten minutes on average.

[1] Hayes, Adam (2015) "A cost of production model for bitcoin." http://www.economicpolicyresearch.org/econ/2015/NSSR_WP_052015.pdf

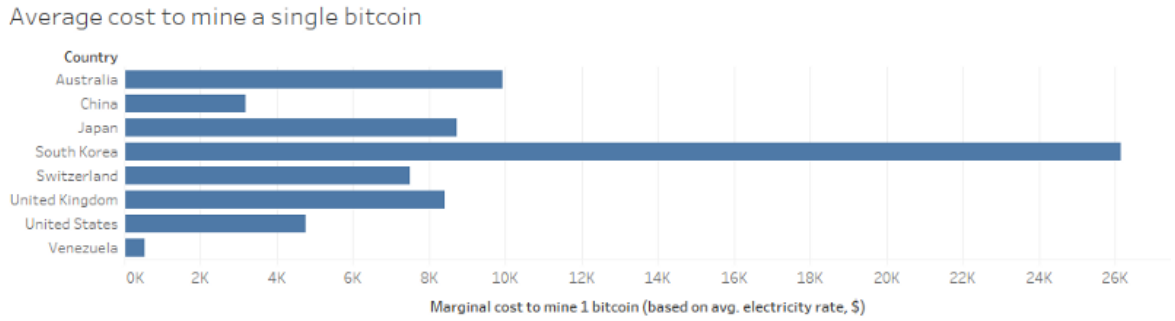
[2] A rational miner would only produce bitcoin if they expect themselves to profit from doing so.

[3] The computational effort exerted by miners can be measured in Gigahashes per second (GH/s).

Per unit mining effort has a fixed sunk cost associated with the purchase, transport, and installation of mining hardware. In addition, there is the variable cost of electricity consumption.[4] Hayes claims, therefore, that the important variables in determining whether a miner decides to mine or not are:

1. Cost of electricity (cents per kilowatt-hour)
2. Energy consumption per unit of mining effort (watts per GH/s)
3. The market price of bitcoin
4. The current level of mining difficulty

A rational miner will undertake mining if the marginal cost per day (electricity consumption) is less than or equal to the marginal product (number of bitcoin accrued per day on average, multiplied by the dollar price of bitcoin). If we assume that bitcoin production is a competitive commodity market, then we should expect marginal cost to equal marginal product for mining. The cost of product could be said to set a lower bound for the market price; a market price lower than this would force miners to stop mining. This does, however, discount subjective reasons for bitcoin mining – such as individual philosophical and socio-economic motivations, or even long-term economic goals. Here are diagrams illustrating the marginal cost of mining a single bitcoin for reference[5]:



Sum of Marginal cost to mine 1 bitcoin (based on avg. electricity rate, $) for each Country.

[4] If Bitcoin is viewed as a virtual commodity then the marginal cost of bitcoin production will play the principal role in value formation.

[5] https://www.elitefixtures.com/blog/post/2683/bitcoin-mining-costs-by-country/

Map based on Longitude (generated) and Latitude (generated). Size shows sum of Marginal cost to mine 1 bitcoin (based on avg. electricity rate, $). Details are shown for Country.

Profit per day model

Hayes models the economic decision a miner must make, where the inputs are the dollar price of electricity, the energy consumption per unit of mining power, the dollar price of bitcoins, and the expected production of bitcoins per day (derived to an extent from mining difficulty). In an earlier paper, Hayes[6] created a model to determine an estimate for mined bitcoin per day given mining difficulty and block reward per unit of hashing power:

$$(1) \qquad BTC/day^{*} = \left[\frac{(\beta \cdot \rho)}{(\delta \cdot 2^{32})} \div 3600\right] \cdot 24$$

Where:

- ***BTC / day**** is the expected amount of bitcoin a miner can expect to earn per day
- β is the block reward
- ρ is the hashing power employed by a miner
- δ is the mining difficulty
- **3600** refers the number of seconds in an hour and 24 to the number of hours in a day
- 2^{32} refers to the probability of any single hash solving the PoW for a given block.

[6] Hayes, Adam, The Decision to Produce Altcoins: Miners' Arbitrage in Cryptocurrency Markets (March 16, 2015) http://www.economicpolicyresearch.org/econ/2015/NSSR_WP_042015.pdf

The value of ρ will be taken as 14 terahashes per second (TH/s); for comparison, the total hashing power of the Bitcoin network is currently around 21,000,000 (TH/s)[7]. The current block reward is 12.5 bitcoin per block.

We can simplify the formula by summarizing the constants for daily time and successful mine probability with the term, θ, such that:

$$\theta = 24 \times 2^{32} / 3600 = 28,633,115.30667$$

Thus, we can rewrite (1) above as:

(2) $$BTC/day^{*} = \frac{\theta(\beta \cdot \rho)}{\delta}$$

And the cost of mining per day, E_{day}, can be expressed as:

(3) $$E_{day} = (price\ per\ kWh \cdot 24 \cdot W\ per\ GH/s) \cdot \left(\frac{hash\ power\ (in\ GH/s)}{1000}\right)$$

The marginal product of mining should theoretically, according to Hayes, equal its marginal cost in a competitive market which should, in turn, equal its selling price. Cost per day is expressed as $/day and mining production is expressed as BTC/day. Then $/BTC price is simply the ratio of the two. This price, p*, serves as a theoretically lower bound for the market price, below which a miner would operate at a marginal loss. Therefore, p* can be expressed as follows:

(4) $$p^{*} = \frac{E_{day}}{BTC/day^{*}}$$

Let us assume that the average electricity cost for the world is 11.5 cents per kilowatt- hour and the current average energy efficiency of ASIC mining hardware deployed is 0.1 J/GH[8]. Therefore:

- the average cost per day for an AntMiner S9 would be (0.115 x 24 x 0.1) · (14000 / 1000) which is $3.864 ($/day);

[7] See https://bitinfocharts.com/comparison/bitcoin-hashrate.html

[8] For an AntMiner S9

- the average cost per day for an AntMiner S9 would be (0.115 x 24 x 0.1) · (14000 / 1000) which is $3.864 ($/day);
- the number of bitcoins that 14,000 GH/s of mining would generate on an average day[9] would be Ƀ0.00314966676 (Ƀ/day); and
- the lower bound value of a bitcoin should be around 3.864/0.00314966676 which is $1226.80 ($/Ƀ).

According to Hayes, if the market price were to drop below this value miners would be operating at a marginal loss and halt production.

Other considerations

This analysis is an interesting approach to understanding the economic drivers underlying the price of a bitcoin. However, the Hayes model raises several concerns.

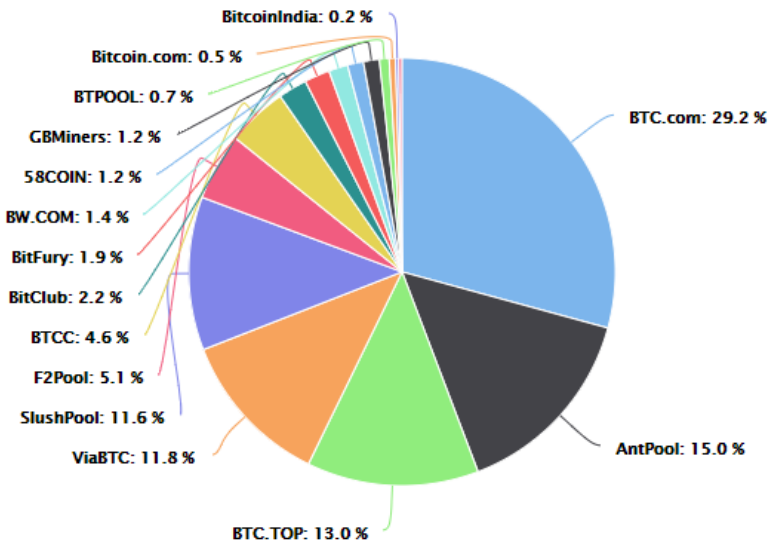
1. Transaction fees

The first concern is that Hayes fails to address the effect transaction fees accrued by miners may have on their incentives. Miners are rewarded in bitcoin but also in transaction fees paid by those who use the network. The average Bitcoin transaction fee stands at around 2.673 USD[10], and with the average number of transactions per block currently sitting at around 850, successful miners of a given block can expect to receive around $2,000 in transaction fees. This will only make a small difference to the lower bound of the bitcoin price calculation, given that $2,000 is around 1.5% of the USD price of bitcoin a successful miner currently receives. However, it is not inconceivable for future bitcoin transaction fees to be 20x what they currently are, given that they peaked at an average of $55 in December[11]. At the same time in December, the average number of transactions per block was around 2,450. Here the total transaction fees in USD represented a much higher percentage of the total mining reward (transaction fees + block reward); in such a situation it becomes much more important for the model to consider accounting for transaction fees.

2. Mining centralization

Another concern I have with Hayes's model is his assumption that bitcoin mining is a competitive pursuit. The top five bitcoin mining pools currently command 74% of the network's total hashing power. See the pie chart below[12]:

[9] See here https://bitcoinwisdom.com/bitcoin/difficulty for details for current mining difficulty
[10] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html as of 26/02/18 15:18 UTC
[11] https://bitinfocharts.com/comparison/bitcoin-transactionfees.html
[12] https://btc.com/stats/pool



The current state of the bitcoin mining market is more aptly described as oligopolistic than (perfectly) competitive. Several of the findings in a 2018 paper[13] – which studied the distribution of mining power on the Bitcoin network – are useful in understanding bitcoin mining centralization. Moreover, the top four Bitcoin miners have more than 53% of the average mining power. Going further, 90% of the mining power of Bitcoin is controlled by only 16 miners; though this is tempered by the fact that the largest miners are all mining pools whose participants do have the ability to move to competing pools.
The point should be clear that Hayes' assumption of perfect competition, and therefore his argument for the price of a bitcoin being set where the marginal product of mining is equal to the marginal cost, is shaky at best. Bitcoin miners offer an identical product – electricity – and are price takers, but the economies of scale that are present (due to the high cost of ASIC mining rigs and Bitmain's monopoly on their production) have led to a degree of centralization. Although there isn't a single framework to describe oligopolistic markets, further work could be done in this area with some commonly used models like Cournot-Nash, Bertrand, or Kinked Demand.

3. Mining centralization

One final, especially interesting variable highlighted by Hayes is that of mining difficulty, δ. To keep the rate of bitcoin creation relatively consistent, mining difficulty adjusts every 2016 blocks according to the overall hash power of current miners. Therefore, mining difficulty can be said to be a function of the total hash power of bitcoin mining[14] , P, such that:

$$\delta = f(P) + Z$$

[13] Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert van Renesse, and Emin Gün Sirer "Decentralized in Bitcoin and Ethereum Networks" (2018) https://arxiv.org/pdf/1801.03998.pdf
[14] Note that an average individual miner's hash power was notated by Hayes as ρ.

where Z is white noise representing the mining difficulty deviation (from ideal difficulty for the given hash power) from the 2016-block delay.

Interestingly, the total hash power of mining is a function of the (1) bitcoin price, (2) macroeconomic circumstance (a nation-state banning cryptocurrencies or positive legal change, for example), and (3) technological advancements (improvements in ASIC quality, for example). With regards to (1), one may notice the slightly circular (or at the very least recursive) nature of Hayes's bitcoin price framework. The lower bound of the bitcoin price depends partially on mining difficulty, which in turn depends on total mining hash power, which in turn depends on the bitcoin price. Bitcoin mining displays a reflexive relationship with its price. This is not necessarily a problem, but it does leave us wondering whether there is a more fundamental way (based on exogenous factors) to measure cryptoassets like bitcoin.

Application to other cryptoassets

As a final note on this framework, it is unclear how well that this can be applied to other cryptoassets. Some cryptoassets (e.g., Delegated Proof of Stake projects, future Proof of Stake implementations for Ethereum) do not use electricity-based mining; while there isn't a specific timeline on a Proof of Stake consensus algorithm implementation for Ethereum, the ultimate aim is to transition to Proof of Stake.

2. Metcalfe's Law

Ken Alabi[15] argues that the value of certain cryptoasset networks (such as Bitcoin, Ethereum, and Dash) can be modelled using Metcalfe's Law. Metcalfe's Law says that the value of a network is proportional to the number of its nodes or end users. More specifically, the value of the network is proportional to the square of the nodes of the network ($V \propto N^2$) where V is the network value and N is number of nodes.

The relationship between network value and size is known as the network effect. Metcalfe's Law can be formalized as:

$$V(N) = k \cdot N^2 \tag{1}$$

Alabi's study was subject to the following parameters:

i. The network value is modelled by the price of the network's digital currency. Price and market capitalization (or network value) have a direct relationship so they can be used interchangeably.

ii. The number of end users is the number of unique addresses participating in the network per day.

[15] Alabi, Ken. (2017) "Digital blockchain networks appear to be following Metcalfe's Law." Electronic Commerce Research and Applications 24: 23-29.

iii. The price curve on the network will contain bubbles and bursts – noise deviating from the mean – that should be filtered out to ascertain the 'true model of growth and value of the network'.

iv. Network growth (under Metcalfe's Law) begins once critical mass is reached. Critical mass is defined as the threshold number of users from which the network becomes viral.

The growth function used within Alabi's model begins with exponential growth, saturation, and then exponential deceleration. The function takes the form:

(2) $$N(t) = \frac{p}{1+e^{-v(t-t_m)}}$$

In the above equation, *t* is defined as time and *tm* is the time when user growth is at its peak growth; here $N = p/2$. Moreover, p is defined as the upper limit on the network's users and v is the virality of the network, how fast it's growing.

None of the popular cryptoassets have yet reached a point of stagnation in their adoption. As a result, Alabi only models the initial growth of the network.

Alabi's rationale for his growth function

Cryptoasset growth, currently, is driven by users' expectation of their future utility – or their discounted expected utility value. Users then communicate the value proposition for a given cryptoasset to their peers in the same way they would for a new social network. If *N* is the number of people with a given cryptoasset at time *t*, then at time $t + t$ the $N(t + t)$ should be proportional to $N(t)$.

Alabi states that this can be written as:

(3) $$\partial n \; / \; \partial t \; = \; vN$$

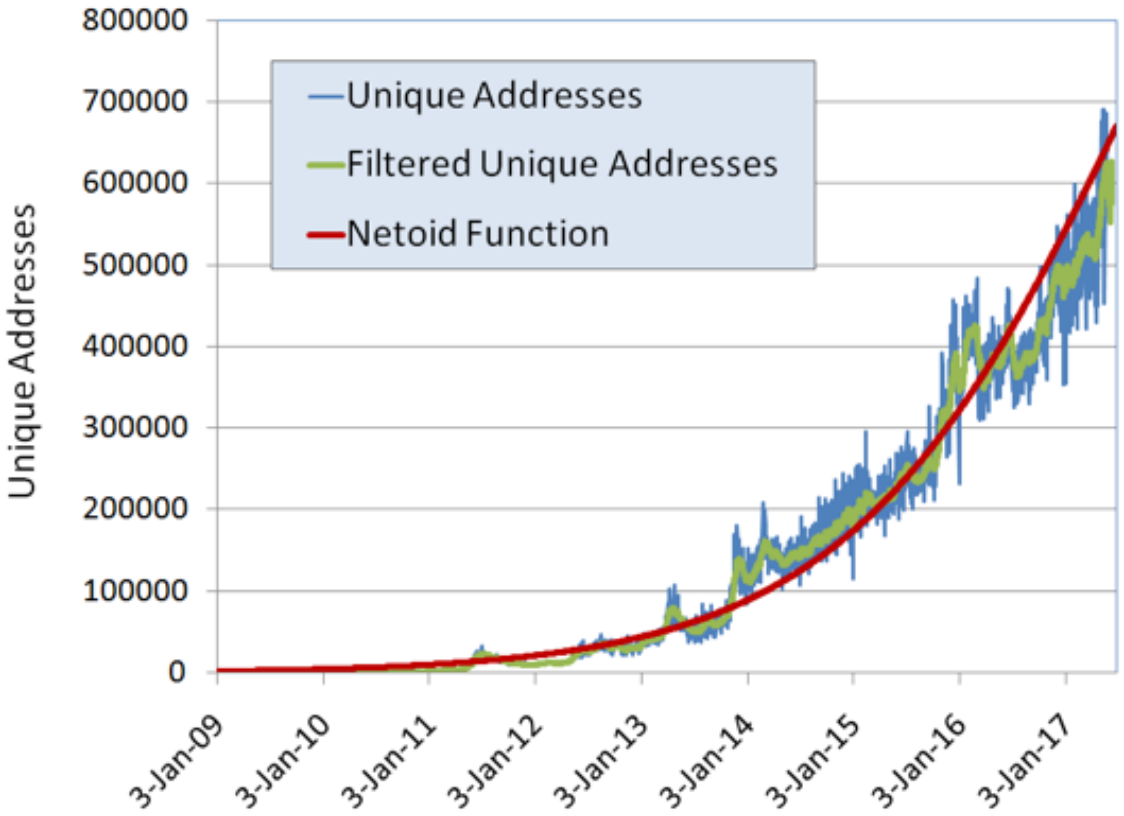
This equation then has solutions of the form[16]:

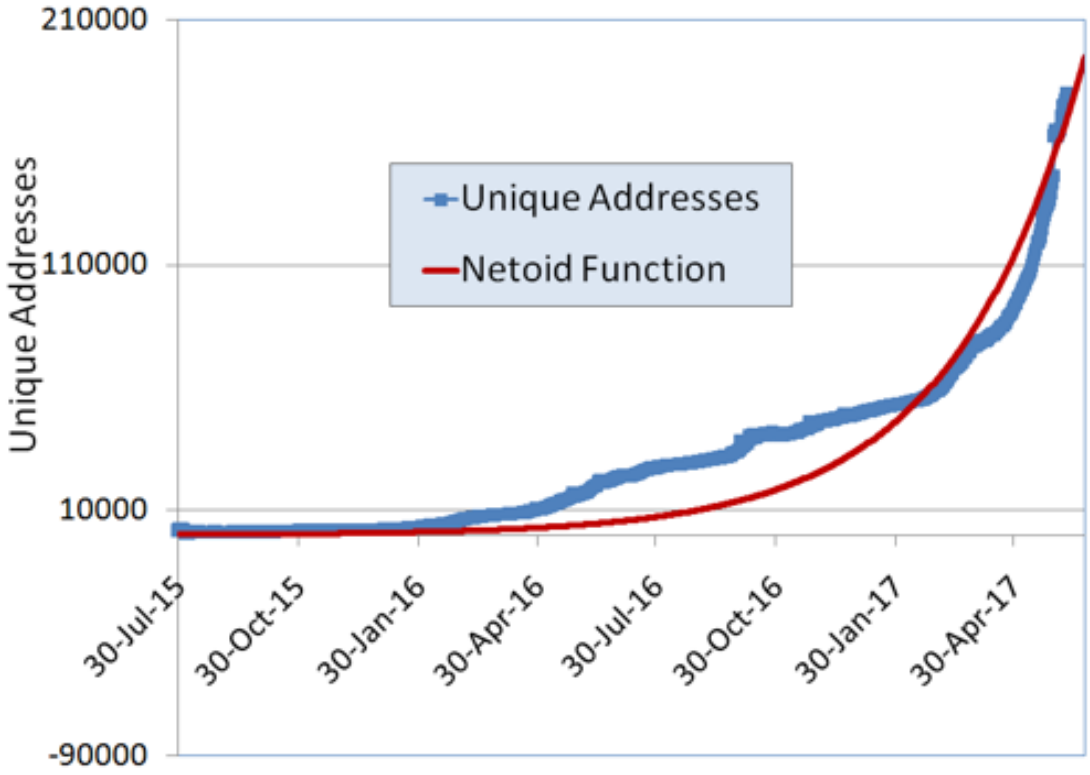
(4) $$N(t) = N_0 e^{vt}$$

The following graphs show Alabi's comparisons of his growth function with the growth in unique addresses carrying out transactions per day on the Bitcoin and Ethereum networks respectively[17]:

[16] In general, $y(x) = Ce^{kx}$ is a solution to the differential solution $\frac{dy}{dx} = ky$ where *C* is a constant.

[17] https://medium.com/@alabs.ken/a-macro-mathematical-model-for-the-observed-value-of-digital-blockchain-networks-23cc8e0dc7ea


800000
700000
600000
500000
400000
300000
200000
100000
0
Unique Addresses
Unique Addresses
Filtered Unique Addresses
Netoid Function
3-Jan-09
3-Jan-10
3-Jan-11
3-Jan-12
3-Jan-13
3-Jan-14
3-Jan-15
3-Jan-16
3-Jan-17

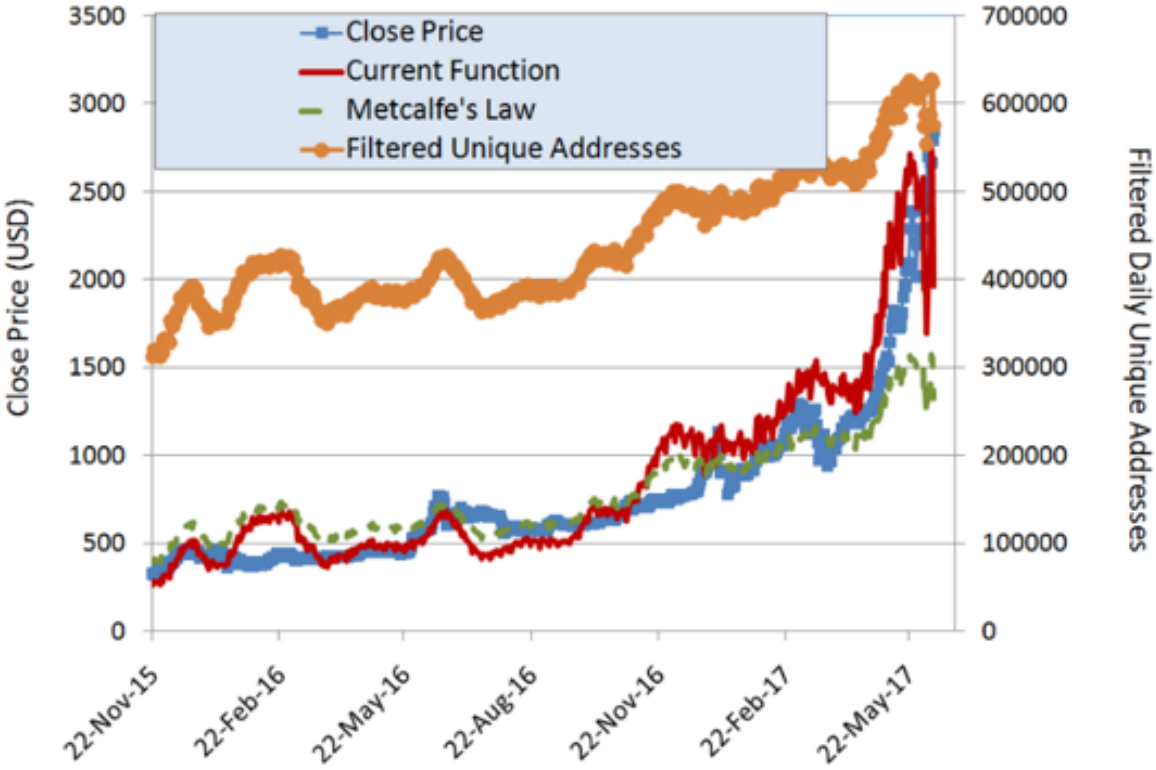

210000
110000
10000
-90000
Unique Addresses
Unique Addresses
Netoid Function
30-Jul-15
30-Oct-15
30-Jan-16
30-Apr-16
30-Jul-16
30-Oct-16
30-Jan-17
30-Apr-17

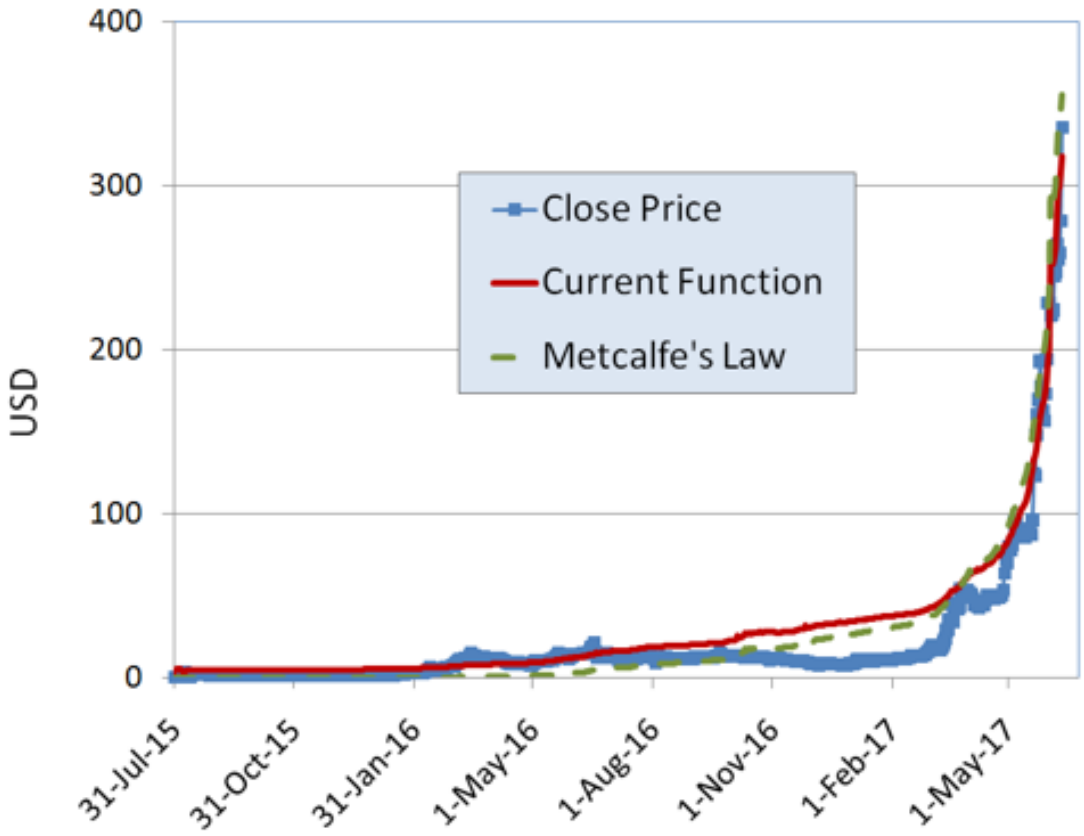
Under this model – and assuming the model continues to hold – Tm for Bitcoin would be achieved around October 2017, and in August 2018 for Ethereum. The Root-mean- square deviation for Metcalfe's law compared to live data for Bitcoin was 7.6% and 4.1% for Ethereum. We can then model, according to Alabi, the network value of the same cryptoassets by using the following formula:

$$V(N)=Ce^{\lambda \bar{N}^m} \quad (5)$$

For Bitcoin, Alabi estimates the growth amplitude parameter v to be 4×10^{-9}, m = 0.5, λ = 0.01, and C = 1. For Ethereum, Alabi estimates the growth amplitude parameter v to be 2.8×10^{-9}, m = 0.5, λ = 0.02, and C = 6.

Consider the comparison of Bitcoin and Ethereum's closing price to that proposed by the models:





Here the Root-mean-square deviation was 7.7% for Bitcoin and 4.3% for Ethereum when compared to the close price at the latest data point. In all Alabi's growth models, m = 0.5 so we can rewrite the network value function as:

(6) $$V(N)=Ce^{\lambda\sqrt{N}}$$

If we let $\gamma = \lambda^2$ then we can rewrite (6) as:

(7) $$V(N)=Ce^{\sqrt{\gamma N}}$$

Is Metcalfe's Law valid?

A common criticism[18] of valuation methodologies that use Metcalfe's Law is the claim that Metcalfe's Law is not a good estimate for the value of networks. To get an understanding of on what grounds would make such an argument it is useful to compare the most common network models[19]:

> **Metcalfe's Law (** $V(N) = k_M \cdot N^2$ **)**: as more individuals join a network, each adds to the overall network value in a non-linearly fashion. The mathematics behind the law is based on pair-wise connections apparent in systems like

[18] See Odlyzko and Tilly (2005) A refutation of Metcalfe's Law and a better estimate for the value of networks and network interconnections. (Unpublished manuscript.) http://www.dtc.umn.edu/~odlyzko/doc/metcalfe.pdf

[19] This section borrows from Peterson (2017) – Metcalfe's Law as a Model for Bitcoin's Value

telephone networks; for example, if there are 5 people with telephones, there can be a maximum of 10 connections (4 + 3 + 2 + 1) – assuming equality among the members' network connections.

The value of the network is derived from the sum of all possible pairings between users and is therefore generalized for n users as:

$$\frac{n(n-1)}{2}$$

Sarnoff's Law ($V(N) = k_s \cdot N$ **)**: the value of a (broadcast) network is directly proportional to the number of viewers. Value is created through the network's one-to-many relationship and not peer-to-peer.

Reed's Law ($V(N) = k_R \cdot 2^N$ **)**: the utility of large networks scales exponentially with the size of the network. This is because the number of possible sub-groups of network participants is generalized as:

$$2^n - n - 1$$

Odlyzko's Law ($V(N) = k_O \cdot N\mathrm{Log}_e(N)$ **)**: the growth rate of the network decreases as new members join because the most valuable links are likely to be formed early on.

Critics of Metcalfe's Law suggest that one of the other laws may more accurately reflect the Bitcoin networks. Reed's Law, however, seems undoubtedly to be a worse fit than Metcalfe's Law given that the concept of 'sub-groups' isn't coherent in the simple Bitcoin financial transaction network. Moreover, Sarnoff's Law seems too conservative since it seems to imply that the sum of individual disconnected notes in a cryptoasset are equal to a single network constituted of each node. Such an argument seems nonsensical, since there are undoubtedly some network effects present on cryptoasset networks and they do influence the value (especially the fundamental financial value) of said network.

This leaves us with Metcalfe's Law and Odlyzko's Law. The crucial difference between the two is that the former assumes homogeneity between the value added for each new node introduced to the network whilst the latter assumes diminishing returns to value for newer nodes. Odlyzko and Tilly (2005) suggest that Metcalfe's Law "provides irresistible incentives for all networks relying on the same technology to merge" and this conclusion is divorced from the reality of modern networks, thus untenable.

We can apply similar logic to cryptoasset network forks. Consider a single network with n members. The network's participants decide to fork, such that the first network has users and the second users. Therefore, and so their combined value would be compared to the value - - of the original network unforked.

We can apply similar logic to cryptoasset network forks. Consider a single network with n members. The network's participants decide to fork, such that the first network has $\frac{9n}{10}$ users and the second $\frac{n}{10}$ users. Therefore, $V(n_1) = k \cdot \frac{81n^2}{100}$ and $V(n_2) = k \cdot \frac{n^2}{10}$ so their combined value would be $2k \cdot \frac{91n^2}{100}$ compared to the value - $k \cdot n^2$ - of the original network unforked.

When we solve for forking transaction costs, ∂, (where $\partial < 0$) and assume that the cumulative value of the forked networks (accounting for transaction costs) are greater than that of the original network, then we see that $|\partial| > 1.82k \cdot n^2$. This implies that the transaction costs of forking a cryptoasset are likely quite large since k is likely much larger than $\frac{1}{n^2}$ for large values of n.

Given the open source nature of most cryptoasset networks and the ease with which a developer can fork a given network, such a claim seems unlikely. Under Odlyzko's law, the transaction costs of forking would be much smaller and scale logarithmically with the cryptoasset network's number of users.

This implies that early cryptoasset networks may face large transaction costs to fork (relative to their overall value) but more mature ones would not. Based off the 'digital gold' investment thesis of a cryptoasset like Bitcoin, Odlyzko's Law seems like a much more appropriate model for network value. Perhaps, Metcalfe's Law will be more appropriate for a strictly medium-of-exchange cryptoasset where there are likely to be greater network effects and the value added by each node in the network is more evenly distributed.

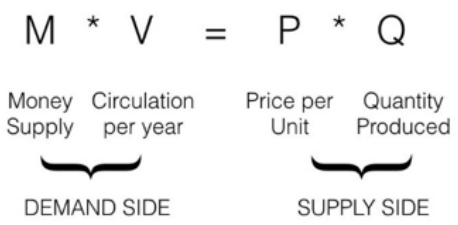
An observation made by Alabi is that his proposed model of $V(N)=Ce^{\sqrt{\gamma N}}$ does not result in a 'pre-ordained exponent' in the same way N2 does. Exponential growth is not guaranteed with N, which is essentially what the criticism in the previous section had been. γ can be changed to match the fundamentals of a given cryptoasset network.

3. Burniske's Equation of Exchange

Chris Burniske has pioneered a method[20] for valuing cryptoassets based on Irving Fisher's Equation of Exchange formula. In the words of Alex Evans[21], the utility value of cryptoassets can be derived by "(a) forecasting demand for the underlying resource that a network provisions and (b) dividing this figure by the monetary base available for its fulfilment to obtain per-unit utility value."

[20] https://medium.com/@cburniske/cryptoasset-valuations-ac83479ffca7
[21] https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f

In this model, a cryptoasset serves as a currency in the underlying protocol economy it supports. Given that the equation of exchange has traditionally been used to understand the flow of money necessary to sustain an economy, it naturally should work in crypto-economies as well. The equation is as follows:



Source: Austere Capital

Where:

- M is the total nominal amount of money supply in circulation
- V is the velocity of money – the number of times a currency changes hands within a given time-period
- P is the price level, and
- Q is an index of real expenditures on newly produced goods and services.

However, when applied to cryptoasset networks, Burniske alters the definitions slightly such that:

- M is size of the asset base
- V is the velocity of the asset – the number of times the token is spent on the resource provisioned by the network
- P is the price of the digital resource being provisioned, and
- Q is the quantity of the digital resource being provisioned.

A valuation for a cryptoasset can thus be ascertained by solving for M, where

$$M = \frac{PQ}{V}$$

Therefore, M is the size of the monetary base necessary to support a cryptoasset network of size PQ at velocity V.

Firstly, consider a valuation for Filecoin; P here would be the price per gigabyte of storage provisioned ($/GB). Q would be the quantity of said resource. PQ can thus be said to be the GDP of the Filecoin economy. Velocity of an asset can be found by dividing PQ by M. Burniske calculated Bitcoin to have a velocity of around 6.5 in 2016. This means on average Bitcoin changed hands 6.5 times. You can have a look

at Burniske's model[22] to get a full understanding of how this valuation method is applied. Using the Equation of Exchange formula and total addressable market (TAM) analysis, one can determine the current utility value of a cryptoassets. A TAM analysis is a top-down approach which begins with the estimate of the market's total size and then ascertains what share of the market the cryptoasset network could potentially obtain. The total market price consists of current utility value and discounted future expectations of the cryptoasset network's key drivers in subsequent years. TAM analyses used in cryptoasset valuations often rely on an asset rotation thesis such as that seen in Grayscale's Zcash investment paper[23].

Claims of circularity

Recently, there has been some interesting criticism of Chris Burniske's MV = PQ formulation; one notable example is that by Austere Capital. Their criticisms can be summarized as follows:

(a) The model relies on arbitrary assumptions of token velocity
(b) The model relies on a circularity to determine the token/USD price

(a) Token Velocity

Token velocity is a large determinant of the value of a token; one can see token velocity as having an inversely proportional relationship to its value[24]. All other things being equal, the longer people hold a token for, the higher its price. Burniske gives the following example: consider an economy with transaction activity of $100 billion for the year and the coins circulate within said economy 10 times within that year. The collective value of the coins is $10 billion; if they had circulated 100 times, then the coins would have been worth $1 billion.

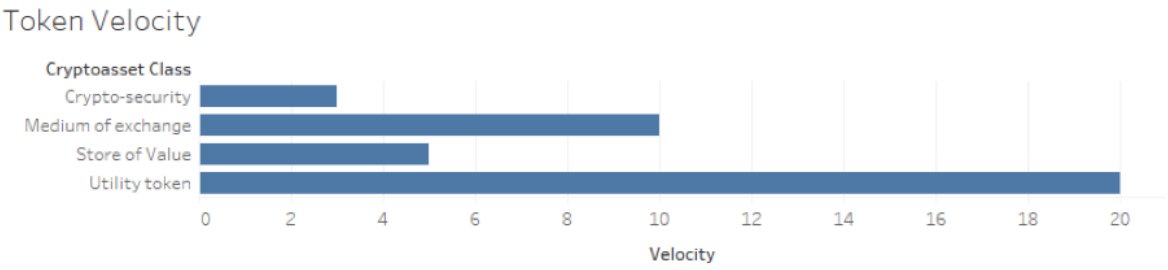
Austere Capital's claim[25] is that "an arbitrary assumption of V, made with no regard to the token model or economic incentives of token holders, has since become the norm in this kind of analysis." At least within Burniske's article, there is a relatively considered approach to the velocity of Bitcoin, done by re-arranging MV = PQ as V = PQ/M. Velocity is then calculated by dividing Bitcoin's average transactional value per day, which is then divided by its asset base.

While there is no 'perfect' way to estimate token velocity, it may be helpful to estimate it via classifications of different cryptoassets. 'Store of value' and 'Privacy coins' like Monero, Bitcoin, Zcash, Litecoin, & Dash are all likely to have similar token velocities since they purport to perform similar functions. While on the other hand, medium of exchange and stable coins could be expected to have much

[22] https://docs.google.com/spreadsheets/d/1ng4vv3TUE0DoB12diyc8nRfZuAN13k3aRR30gmuKM2Y/edit?usp=sharing
[23] https://grayscale.co/zcash-investment-thesis/
[24] James Kilroe has published a useful overview of the importance of token velocity https://medium.com/newtown-partners/velocity-of-tokens-26b313303b77
[25] https://medium.com/@brian.koralewski/mv-p-que-love-and-circularity-in-the-time-of-crypto-2b84074fa2d2

higher token velocities since they are, or tend to be, used as everyday transactional mediums.

We could assign multiples to different cryptoasset subsets and estimate velocity that way. Whilst this method is far from perfect, it would be an improvement on the current ad-hoc way of calculating velocity. I've shown a very basic example of this method below:



One attempt to estimate bitcoin's velocity can be found in a paper by Blocksci[26]. The method is as follows:

1. Compute the total value of transactions outputs monthly and divide it by the total value of the money supply
2. Eliminate outputs controlled by an address linked to one of the input addresses. Doing this eliminates change outputs and transactions by entities simple 'shuffling money around'
3. Eliminate outputs that are then spent within less than k blocks (where k = 4 in this case). Blocksci found that such transactions are likely to be carried out by addresses controlled by the same entity.

Based on these heuristics, the velocity of Bitcoin works out to be 1.4 per month. If this were to remain constant over a 12-month window, then yearly bitcoin velocity would be 16.8 which is much higher than Burniske's estimate.

Velocity is fundamentally a difficult concept to measure or even estimate; Alex Evans[27] summarizes the problems surrounding the concept well:

- Velocity is often used as a catch-all to help balance both sides of the equation of exchange; it simply represents the estimation error of the other variables in the model. To avoid being tautological, velocity needs to be measured separately from the other variables and its fluctuations projected over time.

- Velocity only matters in comparison to the growth or decline in PQ. The velocity thesis – if velocity grows fasters than PQ, token utility value declines – can be derived from this.

[26] Blocksci: Design and applications of a blockchain analysis platform. https://arxiv.org/pdf/1709.02489.pdf
[27] https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f

- Velocity suppression mechanisms such as staking and mint-and-burn are only useful to the extent that they genuinely improve governance and user experience.

(b) Apparent Circularity

Secondly, Austere Capital argue that there is a circularity at the center of the cryptoasset MV = PQ (Burniske's formulation). To quote Austere: "A distributed network is expected to generate USD revenues by buying and selling tokens at the traded token/USD price all year long. The crypto MV = PQ equation turns right around and **uses this very USD revenue** figure to try to determine a target token/USD price."

This analysis seems to argue that the MV=PQ fails because it uses a dollar denomination. This is because the heart of their analysis seems to be a conflation between the 'P' in MV=PQ, which represents the price of the good provisioned ($/GB in Filecoin's case) and the price of the underlying token. The latter is found by solving for M = PQ/V and then dividing M by the circulating token supply.

Taking a note from Warren Weber's article[28] on the matter, we can write the equation as MZVZ = PZQZ. PZ is the price of a unit in QZ in terms of ZZZ (ZZZ/unit of QZ) — **it is not the price of USD in terms of ZZZ or the price of ZZZ in USD**. A lot of misunderstanding around the Equation of Exchange applied to cryptoassets comes from a failure to understand this point.

Burniske's MV = PQ equation has the habit of being misunderstood by some of its readers, which unfortunately prevents more research efforts being focused on some of the actual – and interesting – problems his methodology shines a light on (e.g., token velocity, discount rates, the relationship between each of its moving parts).

Discount Rates for Equation of Exchange valuations

In traditional finance, discount rates are used to determine what future cash flows of a company are worth today. In the context of cryptoassets, we discount the future expected utility value to the present, and the discount rate is used to account for the risk of our expectation not panning out as expected. The crucial difference is that equity discounting is accumulative whilst cryptoasset discounting isn't. For his bandwidth utility token, Burniske uses a discount rate of 40%; this rate was heuristically chosen by multiplying the discount rate used by risky equities with high WACCs[29] by 3-5x.

[28] https://blog.coinfund.io/the-quantity-theory-of-money-for-tokens-dbfbc5472423

[29] The proportionate minimum after-tax required rate of return which a company must earn for all its security holders.

There are further interesting questions to be asked about how discount rates may change depending on the profile of an investor[30] (crypto-only fund vs. partial crypto, partial-equity fund) as Boris Hristov has argued[31]. For example, a fund which raises money via token sale and then returns money to LPs in tokens may prefer to use a cryptoasset-based CAPM to decide the appropriate discount rate. There currently isn't enough talk on the topic but I imagine there will be more articles and papers appearing in coming years.

Alternative absolute value methodologies

Burniske's approach is interesting since it argues for a fundamental value approach to cryptoasset investment. While he argues that one should take the price targets gathered from the model with a pinch of salt, fundamental valuation frameworks do help in understanding the economic drivers which should power a cryptoasset network.

In a similar fashion, Alex Evans[32] from Lowe's Ventures posits an alternative but similar framework. He models a utility token VOLT used to buy electricity. The model economy has one good (electricity) and two assets: VOLT and a store-of-value asset with a given expected rate of annual return. Users start with a holding of the store-of-value at the start of the year and must transfer their holdings to VOLT to finance their consumption of electricity which incurs transaction costs.

Money demanded is modelled using the Baumol-Tobin approach[33]. The model relies on the trade-off between liquidity provided by holding a medium-of-exchange money and the interest lost by holding assets in the non-interest-bearing money. The variables behind money demand are therefore the nominal interest rate, the level of income corresponding to the amount of desired transactions, and the transaction costs of transferring one's wealth between liquid money and interest-bearing assets.

I expand on both the Baumol-Tobin and Evans' approach in Fig. 1 and 2 in the appendix. The Evans framework gives velocity as two times the optimal number of transfers in the economy, 2N. If a user transferred a balance from their store of value at the start of the year, each VOLT token would change hands twice: firstly, SoV – VOLT and secondly, VOLT – electricity.

The rest of the model[34] outlines various projections of the VOLT economy in a similar way to Chris Burniske's article so there's no need to cover it here in any depth. However, there are two interesting calculations to note: transaction costs and token velocity. Evans assumes transaction costs in the initial year of the economy to be $20 per transfer. This number should account for network fees (gas

[30] https://medium.com/@hristovbz/thoughts-on-token-valuation-dynamics-9ecb979b7b65
[31] https://medium.com/@hristovbz/
[32] Ibid fn 21
[33] See http://homepage.ntu.edu.tw/~nankuang/Baumol-Tobin%20Model.pdf for a more thorough explanation.
[34] https://docs.google.com/spreadsheets/d/1a1SzF2H1Y3twTvqAlGAwm8Q2jG-CPnP1Q-7qopN-4LE/edit

costs[35] for example), exchange fees and spreads, asset instability fees, taxation fees, time lost waiting for block confirmations, mental transaction costs[36], etc. He models transaction costs on the thesis that (most) utility token values will collapse alongside transaction costs in the future. Therefore, they decline slowly initially but decline aggressively within the next 5 years, coinciding with mainstream adoption of the VOLT token. By the time the VOLT economy is fully saturated, transaction costs will be equal to $0.36. Using the *Velocity = 2N* identity seems to support the velocity thesis' core prediction as utility value of the VOLT token is expected to peak in 2025 and then declines thereafter, despite the continued growth of the VOLT GDP.

The long-term property of token velocity can also be derived from our money demand equation. Log-linearizing Evans' money demand formula gets us:

$ln M^{d^*} = \frac{1}{2} ln Y + \frac{1}{2} ln C - \frac{1}{2} ln R - ln\sqrt{2}$. The money demand elasticity of total spending, Y, is 0.5. This means that transaction demand for money is subject to economies of scale and as total spending increases, money demand increases less proportionally. Consequently, this must mean that token velocity must increase in the long-term as total spending within the crypto-economy increases. Overall, Evans' new model produces some interesting results and a different way to look at the drivers of cryptoasset economies – namely the importance of modelling transaction costs and endogenous token velocity.

Mature equilibriums

One of the more thought out articles on cryptoasset valuations is by John Pfeffer[37]. Pfeffer covers a range of topics such as bitcoin valuations, utility token velocity, and the effect of a Proof of Stake consensus algorithm on the price of ether. However, I tend to disagree with several of Pfeffer's claims. Examining my concerns may reveal new insights into the world of cryptoasset valuations.

First, one of the axioms of Pfeffer's essay is the belief that PQ within the MV = PQ equation should be equal to the total cost of computing resources the blockchain protocol consumes. Let's lay out his argument:

1. A given protocol is analogous to a simple economy.
2. The GDP of the company is the aggregate cost of the computing resources needed to maintain its blockchain (in a mature equilibrium).
3. For utility tokens without in-build price decoupling mechanisms like Ethereum's GASPRICE, one of three things will happen: a) the token's price trades to a level where the network takes no economic rent; b) the network forks into a less rent-seeking network until eventually no

[35] https://ethgasstation.info/
[36] http://nakamotoinstitute.org/static/docs/micropayments-and-mental-transaction-costs.pdf
[37] https://s3.eu-west-2.amazonaws.com/john-pfeffer/An+Investor%27s+Take+on+Cryptoassets+v6.pdf

economic rent is reached; c) the network's adoption is limited to the highest-value uses cases until a) or b) occurs.
4. Because of (3) the economic equilibrium of the network must be near marginal revenue = marginal cost for the mining industry to maintain the blockchain in question.

I agree with (1) and the previous examples I've given rely on this assumption. However, I don't fully understand (2), therefore let's dive deeper to understand why.

Many of Pfeffer's comments relate to Bitcoin's place as a store of value. He argues that the economic drivers behind a cryptoasset store of value will be very different from a utility protocol in equilibrium. To quote him: "a 'mature equilibrium' utility protocol 'either has extremely high velocity or we see them reduced to computational functionality that is disaggregated from means of exchange (for non-compute economic activity) and monetary store of value"[38]. We can define an equilibrium as follows:

- There is a mainstream, institutional acceptance of cryptoassets as a core monetary store of value
- Markets value cryptoassets based on 'significant realized user penetration'
- Cryptoasset and blockchain networks are perfectly competitive and take no economic rent; this is because of the eventual ease with which users will be able to switch platforms, move around capital (through decentralized exchanges & atomic swaps), and fork rent-seeking protocols.

Pfeffer argues that:

The value of utility tokens will equal the computational power expended by their respective networks in the long-term.

Most dispute's in Pfeffer's paper can be boiled down to two issues:

1. he overestimates the extent to which forks will be motivated by cost-minimization and the ease with which users/developers will be able to switch between cryptoasset/blockchain networks and protocols; and
2. he does not account for the range of 'velocity-sink' utility tokens which users may value above the immediate computational cost expended by them (i.e. governance tokens).

On (1), Pfeffer argues that given blockchain protocols' open-source (generally) nature and thus the ease with which they can be forked into functionally identical blockchains, it is likely that the cryptoasset market will become perfectly

[38] https://medium.com/john-pfeffer/an-institutional-investors-take-on-cryptoassets-690421158904

competitive in the long term. Moreover, competition between similar protocols is likely to be fierce in the future. He gives the example of Kik considering migrating its network from Ethereum to another blockchain because of transaction fees. While it is impossible to know for certain, most forks on popular protocols have been motivated by philosophical disputes (ETH/ETC or BTC/BCH), rather than cost-minimization generally; so I'm not convinced as to how widespread cost-minimization forks will be.

Pfeffer would likely argue in response that (a) this will likely change in the future, and (b) the Bitcoin Cash fork to an extent can be seen, to an extent, be driven by cost-minimization efforts through increased block-sizes and reduced transaction fees. However, the primary motivation for the Bitcoin Cash fork was over the primary use case of Bitcoin (medium of exchange vs. store of value); I don't believe that either side based their arguments on claims of their interlocutor rent-seeking.

In regards to (b), this is a slightly more interesting point since there isn't much evidence for or against it. We must wait to see how efficient forking, token exchange, and cross-blockchain interactions become on blockchain networks. I imagine, however, that developers (the ones who ultimately decide if a chain forks and support subsequent development) may continue to develop on a supposedly 'rent-seeking' chain if they believe other, less quantifiable attributes give it value (e.g., quality of developers, overall philosophy and culture). Even if non-technical users would support a hypothetical fork because of its reduced fees, the decision comes down to developers to build on this new fork and miners to provide their computational resources. These reasons could limit the ability of a blockchain network to reach 'mature equilibrium' within the next 20-30 years, if ever.

For example, consider whether John Barlow's vision for the internet has truly become a reality? Have we really created a world where "anyone, anywhere may express his or her beliefs … without fear of being coerced into silence or conformity?"[39]. Coincidentally I do think blockchain networks will help move the internet closer to what John Barlow envisioned; however, we must not discount the ability of humans to introduce inefficiencies and unwanted attributes into systems for our various irrational, very human reasons. This has been the case with the development of the internet following the publication of John Barlow's 'A declaration of the independence of cyberspace' and it will likely be the same for blockchain networks.

Secondly, with (2) I believe Pfeffer underestimates the extent to which future developers of utility tokens will introduce velocity sinks[40] (for better or worse) which may help prop up a token's value even in a 'mature equilibrium'. There will be many utility tokens which have semi-governance properties (e.g., curation of content on a platform[41] or control of certain parameters within the token economy)

[39] https://www.eff.org/cyberspace-independence

[40] https://medium.com/blockchannel/on-value-velocity-and-monetary-theory-a-new-approach-to-cryptoasset-valuations-32c9b22e3b6f

[41] https://medium.com/@ilovebagels/token-curated-registries-1-0-61a232f8dac7

and they can still have justifiable value in a 'mature equilibrium'. I do agree that many cryptoassets, that have simply been used as fundraising mechanisms and currently only act as mediums of exchange within their native network, will likely have no value in the long term. However, utility tokens can certainly be a lot more than just native mediums of exchange.

On staking

Pfeffer argues that a move from proof-of-work to a proof-of-stake consensus algorithm will lead to a 'commensurate reduction in the PQ of the network'. Moreover, the additional cost in the form of a 'capital charge from acquiring and immobilizing' ether will be added to PQ, making it more expensive compared to a non-staking protocol.

These comments seem odd. He argues that, ceteris paribus, a move from proof-of-work to proof-of-stake will be more expensive for miners. See the following quote:

> *"... let's layer on the idea that in order to participate in mining and the associated revenues,* ***on top of paying for processing power, storage, bandwidth and energy****, you must now bear an additional cost in the form of a* ***capital charge from acquiring and immobilising an amount of the native cryptoasset****. This capital charge on immobilised cryptoasset is added to PQ, making the protocol in question more expensive to use than an equivalent utility protocol that doesn't require staking (or where staking is less expensive because the native cryptoasset is cheaper)" – John Pfeffer*

It should be clear that a successful implementation of Proof-of-Stake such as Casper[42] would be much cheaper for miners (in terms of processing power, storage, bandwidth, and energy consumption) than an equivalent Proof-of-Work algorithm. Moreover, if we are under the assumption of a 'mature equilibrium – as Pfeffer's paper is – then the cost incurred for acquiring and immobilizing an amount of native cryptoasset would be minimal. Instead, there are two potential costs for a proof-of-stake miner: (i) the opportunity cost of immobilizing the native cryptoasset instead of investing/using it in some other way; (ii) punishments (by taking away a portion of the staker's deposit) for validators who misbehave (i.e., Safety Faults - creating blocks on multiple or the wrong chain[s] and Liveness Faults – network latency, preparing different hashes from the majority of validators, etc.). Proof-of-stake consensus algorithms like Casper are based on the belief that the economics of proof-of-work can be replicated in a proof-of-stake system. While the penalties within a proof-of-work system can only be properly measured externally (in electricity spent or hardware rented), in proof-of-stake systems penalties can be defined explicitly.

I don't believe a switch to a proof-of-stake consensus algorithm will likely make a large direct difference to the value of the Ethereum network. While a percentage of

[42] See: https://github.com/ethereum/research/tree/master/papers/casper-economics

ether may be locked up in staking contracts (and therefore have an extremely low velocity), this may simply mean that the velocity of non-staked ether may just increase proportionally. However, there remains the possibility that, depending on the how Casper is rolled out, that demand for ether increases by some amount and miners buy up quantities to benefit from early proof-of-stake rewards; moreover, there may be philosophical or socio-economic factors (such as activist forks in protest of Casper) that affect the ether price indirectly.

4. Comparables

In this section I look at comparables. With this methodology, we need to identify a value relevant metric from one protocol, and then use it to value another protocol such as[43]:

$$\frac{Value_i}{Attribute_i} = \frac{Value_j}{Attribute_j}$$

Here, "i" is the comparable protocol and "j" is the protocol we are trying to value. Alternatively, we can compare a single asset over time:

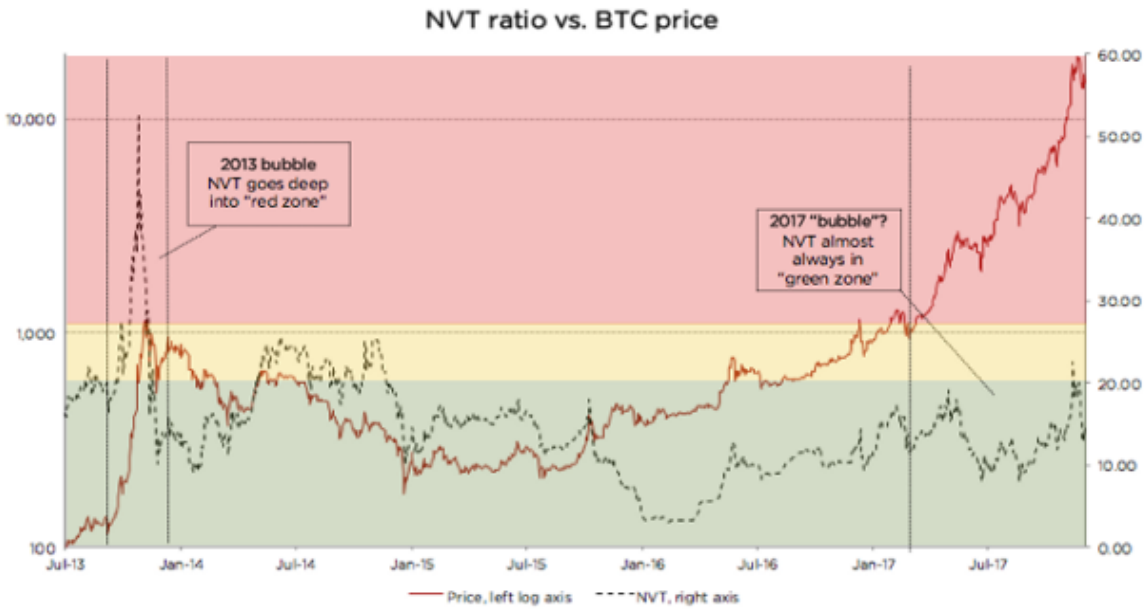
$$\frac{Value_t}{Attribute_t} = \frac{Value_{t+1}}{Attribute_{t+1}}$$

One example is the Network Value-to-Transactions (NVT) ratio. The definition is[44]:

$$NVT = \frac{Network\ Value}{Daily\ \ Transaction\ Volume}$$

The common argument is that the total value of transactions flowing through the cryptoasset network is a proxy for the utility derived from the network. Keep in mind that NVT considers on-chain transactions only, as trading activity on exchanges is speculative and therefore does not add utility to the network. Analysts such as Willy Woo have argued[45] that the NVT can be used to detect bitcoin price bubbles. This is nicely illustrated by the following diagram[46]:

[43] This formalization has been borrowed from Stephen McKeon's work on the topic.
[44] Daily transaction volume has been measured as a backward-facing moving average typically. There have been attempts to use forward and backward-moving averages, though we doubt that it's wise to use future input data whilst developing predictive models.
[45] https://www.forbes.com/sites/wwoo/2017/09/29/is-bitcoin-in-a-bubble-check-the-nvt-ratio/
[46] https://medium.com/cryptolab/https-medium-com-kalichkin-rethinking-nvt-ratio-2cf810df0ab0



We can gather a few ideas from the NVT framework:

1. High NVT ratio can indicate high speculative value.

   In the early years of the Bitcoin network, the markets valued the network high in comparison to the actual transaction value.

2. Therefore, we can use the NVT ratio to detect bubbles.

One can only determine a bubble after the peak when the market reassesses the new valuation and we see if the price consolidates or crashes. The **NVT Ratio isn't good at reliably determining a bubble ex-ante** but is very useful for discerning between a crash or a consolidation.

Price-to-Metcalfe Ratio

There are other comps. that may be useful in valuation analysis. One I came across recently was the Price-to-Metcalfe Ratio (PMR) formulated by Clearblocks[47]. Here they use an alteration of Metcalfe's Law (M2): $100 \times \frac{N^{1.5}}{S}$

Then PMR is defined as:

$$PMR = ln \frac{Daily\ USD\ Price}{30\text{-}Day\ MA\ of\ M2}$$

[47] https://medium.com/@clearblocks/valuing-bitcoin-and-ethereum-with-metcalfes-law-aaa743f469f6

Where:

- *30-Day MA* refers to a 30-day backwards-facing moving average of unique active addresses
- *N* is the number of active addresses, and
- *S* is current supply.

Clearblocks argue that PMR can be used as a strong leading indicator of both Bitcoin and Ethereum corrections. However, there's no clear reason why M2 is used instead of a more common formulation of Metcalfe's Law. Furthermore, both NVT and PMR cannot capture the value added by off-chain solutions such as Raiden, 0x or more general side-chains or state channels.

Reflexivity

Reflexivity is the concept that the price of an asset has an impact on its fundamentals. Coinmetrics has done work[48] which suggests that cryptoasset transaction volumes and prices both affect each other in a circular way. Changes in price can influence the fundamentals of a cryptoasset as it helps drive attention to it, helps support development initiatives, and makes mining (where it applies) more viable. Coinmetrics argue that this fact may mean that fundamental valuation frameworks are not entirely useful; instead, relative valuation metrics like the NVT ratio may work better. Further work needs to be done on cryptoasset reflexivity, although I note that there has been work done in the last few years to try to quantify financial asset reflexivity[49, 50, 51]. Some of the methods used could potentially be applied to the cryptoasset space.

For example, Filimonov and Sornette (2012) have done interesting work in quantifying reflexivity in financial markets. Their measure quantifies how much of an asset's price change is due to endogenous feedback processes, as opposed to exogenous market news. Reflexivity is therefore defined as the proportion of price moves due to endogenous interactions to the total number of price moves also including the impact of exogenous news. Much in the spirit of Soros' reflexivity principle, one could easily argue that this could help discern when agents are following naïve, trend-following forecasting rules and when they make price decisions based on the fundamentals of a cryptoasset. In such a case, we could use some of the other valuation frameworks in tandem – depending on the measured amount of reflexivity in the market at a given point.

[48] https://coinmetrics.io/mean-reversion-and-reflexivity/

[49] Cars Hommes (2013) Reflexivity, expectations feedback and almost self-fulfilling equilibria: economic theory, empirical evidence and laboratory experiments, Journal of Economic Methodology, 20:4, 406-419, DOI: 10.1080/1350178X.2013.859426

[50] George Soros (2013) Fallibility, reflexivity, and the human uncertainty principle, Journal of Economic Methodology, 20:4, 309-329, DOI: 10.1080/1350178X.2013.859415

[51] Filimonov, V., & Sornette, D. (2012). Quantifying reflexivity in financial markets: Toward a prediction of flash crashes. Physical Review E, 85(5), 056108.

Conclusion

This article has reviewed some of the current literature on cryptoasset valuations. Although I haven't been able to deal with everything in depth, I hope, at the very least, that my comments will help bring greater attention to the topic. While my aim was never to present or follow a singular theme throughout this essay, there have been certain strands of thought which I think are worth closer examination by others and myself. These include:

- **Cryptoasset price reflexivity**. Can we measure this? How do we account for this in our valuations (if we can)?
- **Cryptoasset velocity**. What is the best way to measure this? What effect will it have on the value of utility tokens in the long term? How does it change over time and what are the main drivers of this change?
- **Law-based relationship between N and value**. Is there a heuristic that can predict the value of a cryptoasset network (number of users => network value)? If so what form is it likely to take (exponential, logarithmic, etc.)
- **The effect of differing consensus algorithms**. What effect does a change of consensus algorithm have on a blockchain protocol's value?
- **Modelling money demand**. What are the best ways to measure cryptoasset money demand? Is this even necessary/important?
- **Mature equilibrium**. What are the features of a 'mature equilibrium' as hypothesized by John Pfeffer? Will this ever be reached?
- **Utility Tokens**. What future do they have?

Please leave comments on the medium article, send them to my twitter account, or email me.

Appendix

Figure 1: The Baumol-Tobin approach

The total number of times one must go to the bank is: $n = \frac{PY}{Z}$ and therefore transactional money demand (or average cash balance) is:

$$M^d = \frac{1}{2} \times \frac{PY}{n} = \frac{PY}{2n} = \frac{Z}{2}$$

The opportunity cost for holding cash is the amount of interest one would accrue if cash had been placed in an interest-bearing asset and is therefore:

$$i \times \frac{Z}{2} = i \times \frac{PY}{2n}$$

The transaction cost is $P\delta$. Therefore, the total costs of managing cash is:

$$TC = nP\delta + \frac{iPY}{2n}$$

We take the derivative of TC w.r.t n to find the point on the curve where total costs are minimized:

$$P\delta - \frac{iPY}{2n^2} = 0$$

The optimal numbers of trips to the bank is therefore: $n^* = \sqrt{\frac{iY}{2\delta}}$ and plugging n into our money demand equation gets us:

$$M^d = \frac{Z}{2} = \frac{PY}{2n} = P\sqrt{\frac{\delta Y}{2i}}$$

The Baumol-Tobin transactional demand identity equation can, therefore, be stated as:

$$\frac{M^d}{P} = \sqrt{\frac{\delta Y}{2i}}$$

Figure 2: The Evans Approach

Users pay *CN* in transaction fees and the average balance held in VOLT annually is:

$$\frac{Y}{2N}$$

The opportunity cost of keep balances in VOLT annually is, therefore: $\frac{RY}{2N}$

The total cost function is simply opportunity cost and transaction costs incurred:

$$TC = \frac{RY}{2N} + CN$$

Once again, we take the derivative of TC w.r.t to N and we get:

$$\frac{dTC}{dN} = -\frac{RY}{2N^2} + C$$

By setting this to zero and solving for N we can obtain the cost-minimizing N value:

$$N^* = \sqrt{\frac{RY}{2C}}$$

Finally, plugging this back into our original money demand equation gets us:

$$M^{d*} = \sqrt{\frac{YC}{2R}}$$

We can then formulate a definition for velocity independent of other monetary terms used in the equation of exchange. Velocity is defined as:

$$\frac{Y}{M^d} = Y \div \frac{Y}{2N} = 2N$$