"In the long run we are all dead. Economists set themselves too easy, too useless a task if in tempestuous seasons they can only tell us that when the storm is long past the ocean will be flat again."

- ***John Maynard Keynes***

Cryptocurrency Supply Algorithms and the Equation of Exchange

Although I am a proponent for Bitcoin, and view it as a good store-of-value, my belief is that all of the algorithms for cryptocurrency supply models that I have seen to date, are not amenable to creating a cryptocurrency useful as a general currency. That is as a means for exchange-of-value as opposed to store-of-value. The following is my brief description of the models that I am aware of, followed by an explanation of why I believe they are not useful for as general currencies. At the bottom I make a concluding remark on what I believe is a missing feature needed to realize a general currency.

Coin Supply Algorithms

N+1

In an N+1 algorithm, each time a block is produced, a constant incentive reward is added to the supply of coins. This means explicitly that the size of the coin supply will grow forever, unlimited. This sounds pretty good on the surface. If you are a miner, you are guaranteed that there will always be an incentive reward available for mining.

If we look at this from a total coin supply viewpoint, and a little highschool math, the normalized change in supply is:

$N+1/N$

We then want to ask the question, how fast is the coin supply changing, as N goes to infinity, since we are assuming that blocks are produced forever. This is:

$$\text{Lim } N \to \infty \quad N+1/N$$

Where N is the number of blocks produced. By L'Hôpital's rule for those that remember a little highschool calculus (I had to look it up), we can take the derivatives of the numerator and denominator which results in 1/1 = 1. In the limit at infinity, the coin supply is a constant value, even though theoretically it grows forever.

Since infinity is only theoretical, what does this look like for blockchain usecases:

To give a feel for it, imagine that we are at the following 4 stages: 10 blocks have been produced; 100 blocks have been produced; 1000 blocks have been produced; and 10000 blocks have been produced. Adding one reward at each stage gives the following percent change in coin supply:

1 - (10 + 1)/10 = 10%

1 – (100+1)/100 = 1%

1 – (1000+1)/1000 = .1%

1 – (10000+1)/10000 = .01%

This demonstrates that the change in coin supply quickly dwindles to an insignificant amount, even though it continues to grow forever. To put this another way, the addition of each new incentive reward quickly becomes a very small fraction of the total coin supply. The coin supply can be thought of as relatively constant.

N + M*N/2T or N(1+M/2T)

T is units of time in discrete steps, and M is the number of blocks produced at each step. This is essentially the Bitcoin model. To make this clearer let's assume that there is only 1 block produced at each step. This becomes N + N/2T or N(1+1/2T).

If we replace 2T with a new variable K, then this becomes:

N(1+1/K)

Where K increases forever. The summation of 1/K is the harmonic series and increases forever. Therefore, just like N+1 above, N(1+1/K) or N+N/K also increases forever. As with N+1, the rate of increase of the coin supply is then:

(N(1+1/K))/N

This is more simply 1 + 1/K. Thus, as K grows, we can see that the rate of increase tends towards zero as well. Further, since 1/K becomes a smaller and smaller fraction, eventually representing this as a value in a computer becomes impossible. For example, Bitcoin's smallest fraction is 1 satoshi. When 1/K becomes smaller than 1 satoshi it will no longer be possible to have an incentive reward for a single block produced.

Given that both coin supply algorithms tend towards a relatively constant supply, in terms of use as a currency, we can view both as essentially equivalent. The only difference is how fast the supply tends towards a constant value, where the Bitcoin model is faster.

N

A third coin supply algorithm is a simple constant amount created in the genesis block. The coins are usually distributed using an airdrop or similar model. Since coins are not being created, the coin supply is by definition constant. If the distribution model used is an incentive reward model to distribute from the pool of coins, it is indistinguishable from one of the above 2 models. If the distribution model is a one-time event, such that all the coins are distributed then there is no incentive reward model.

From a view point of use of currency all 3 models described above can be thought of as equivalent, given enough blocks have been produced for the first 2 models.

Marked To External Asset

There is fourth model for coin supply which is intended to mark the value of the coin to an external index of some kind. This may be a physical asset like an ounce of gold, or another commodity. In this model the coin can explicitly represent a unit of the external asset such as an ounce of gold. Regardless of whether the coin can be exchanged for the underlying asset or not, given that supply of commodities such as gold are constant following the same mining algorithms as above, the marked to asset model is a constant coin supply model. If the distribution model used is an incentive reward model, then it is similar to the third model.

Marked To Value Of External Asset

There is a fifth model for coin supply where the value of the coin is marked to the value of an external asset like the USD, instead of the supply of the external asset, as was the case for marking to a commodity. In this model, the coin supply is changed to reflect the exchange rate of the coin against the value of the external asset. The objective is to keep the exchange rate constant on average over time. For example: assuming the objective is a 1-to-1 exchange between the coin and the USD, then if the coin's value increases above the objective, more coins are printed, and vice-versa. That is, if the value of the coin decreases, given some means (i.e. burning), the coin supply is decreased to bring the exchange rate towards the objective.

In this model, the coin supply is not fixed but varies with exchange rate. To the extent that the value of the external asset is relatively constant, and the value of the coin is relatively constant the coin supply will be relatively constant.

Although marking to the USD would seem to be a good idea, given that it is called a "reserve currency", the USD is intentionally subject to inflation, theoretically, the coin to USD exchange will continue to decrease, requiring the coin supply to be decreased to maintain the objective of a constant exchange rate. Over time, this model can be viewed as decreasing the coin supply if marked to an inflationary external asset value.

Comparing Coin Supply Models

In summary, of the five models described above, four of them are essentially variations on a constant coin supply using various means to distribute the coin, while the fifth tries to keep the value of the coin constant against an external asset value, by managing the supply of the coin.

The equation of exchange: $M * V = P * Y$[1] tells us that if the amount of money supply, M, (i.e. the coin supply) is constant, and the velocity of money is relatively constant, then an increase in demands for goods (Y), will cause a decrease in the price (P), price deflation. That is, with a fixed coin supply the price of goods is expected to drop, thus increasing the value of the coin. Bitcoin's increase in value is an example of this. (The Bitcoin ledger does not have a means to determine either prices (P) or goods (Y).

[1] https://en.wikipedia.org/wiki/Equation_of_exchange

Instead I am inferring from the increase in value of bitcoins that an increase in demand for Y is occurring. There are possible other explanations.)

However, it should be noted that in order for the equation of exchange to be valid, the assumption of the velocity of money being relatively constant must hold. If holders of the coin stop using it as a currency for the exchange of value, then the M * V = M * 0 = 0. There is no price in that coin for any goods or services. That is, the value of the coin collapses.

Conversely, if the velocity of the coin were to increase significantly, then this creates effectively more available coin, resulting in the price (P) of the goods and services (Y) to increase. This causes price inflation, which encourages coin holders to spend their coin as fast as possible to avoid losing value in the coin. As the price of goods becomes excessive, people shift from the coin to other forms of currency. As this happens, once more a collapse happens.

At an equilibrium point, the coin supply is constant, the velocity is constant, the demand for goods and services is constant, and therefore the price would be constant. At such an equilibrium point, a constant coin supply would be ideal. However, we can observe throughout history that such an equilibrium point is never reached.

Given any sort of constant coin supply, the value of the coin is expected to vary unpredictably and often wildly. Of the 5 models, the first 4 will always be subject to this. Although this may be interesting for speculators, usefulness for general currency is questionable.

The fifth model is to manage the coin supply against an external asset value. In essence this is a substitution of the coin for the asset. Provided that the coin supply can be managed to reflect the objective exchange rate, the value of the coin should be stable relative to the stability of the external asset value.

However, in my opinion, this marking of value does not take into account exchanges that are wholly internal to the coin and its blockchain. The transfer of a coin balance from one account to another implies an exchange of value, thus the equation of exchange applies internally to the blockchain. This exchange of value is independent of the exchange rate of the coin value versus the external asset value. Thus, the coin supply can be seen as independent of the exchange of value on the blockchain.

Given this assumption, we can make the simplifying assumption that the coin supply is relatively constant with respect to the exchange of value on the blockchain. As a result, one would expect that even though the coin supply is managed against the exchange rate with an external asset, its value can still fluctuate wildly, beyond the ability of coin supply management to compensate. This in turn, will impact the exchange rate, destroying the intended objective.

As a natural consequence, even with the approach of marking the value of the coin to an external asset value, such as the USD, the expected volatility limits the usefulness of the coin as a currency.

Towards A General Currency

As stated in the introduction, I believe that none of the cryptocurrency models described are viable for use as general currencies. In my opinion, my brief non-rigorous analysis above demonstrates this likely to be true. The question remains, what else is needed to create a cryptocurrency that is viable as a general currency.

The equation of exchange shows us what is missing directly: In the equation M * V = P * Y, we can say that on every blockchain we can know the values of M and V directly. The account ledger explicitly shows us this, (ignoring encrypted exchanges). What we do not know is the other side of the equation. We do not know either price (P) or goods and services (Y) for any exchanges that are internal to the blockchain, that is between accounts on the blockchain.

If we compare cryptocurrencies with national fiat currencies, and cryptocurrency exchanges with foreign exchanges, we can see that the foreign exchanges relate the difference in prices in related economies. In comparison, the cryptocurrency exchanges appear to only relate the difference in demand for the cryptocurrencies themselves. This demand only manifests itself during the exchange of cryptocurrencies for each other, and between fiat and cryptocurrencies and vice-versa.

It is my position that because the internal use of cryptocurrencies on their own blockchains is currently hidden, none of the above coin supply models will create a currency stable enough to be useful as a general currency. If/when a cryptocurrency model is created that takes into account the currently hidden internal exchange of value, then we will have realized a general currency.