Introducing the Poly, a novel single token stablecoin

Christopher Georgen[1], Kim Raath[1], and James Aman[1]

[1]Affiliation not available

November 25, 2018

Intro

In this paper, we introduce the Poly, the native currency of the Topl protocol. The design of this currency is informed in large part by what has come to be known as the Friedman rule[1] as well as the Seigniorage Shares model[2]. The first inspires our close consideration of the effects of inflation on individual economic actors, while the second serves as a starting point for our considerations on how to handle changes in currency supply, even though we abandon the signature two-token model of Seigniorage Shares.

Current Landscape

Although the space is still nascent, we can largely divide "stablecoin" efforts into three distinct groups: Homogeneous Collateral Coins, Heterogeneous Collateral Coins, and Seigniorage Shares. While the Poly can only be described as a derivative of the third model, we first introduce the other two models as points of contrast.

Homogeneous Collateral Coins

Stablecoins in this category are the simplest to design and understand since the asset whose price they are intended to track is also the asset held by the issuer as collateral. By example, we can imagine that we wish to issue a stablecoin that will always be worth 1 USD. To accomplish this, we could simply hold a number of actual USD as collateral that is always equal to the number of stablecoin units outstanding. Those familiar with the space should recognize this as the model used in Tether's USDT stablecoin.

Weakness

> These Homogeneous Collateral Coins have two major weaknesses. First, since collateral such as USD or gold cannot be held directly on a blockchain, there is still the custodial risk of the issuer. Users of such a coin must be able to trust that the issuer actually has the collateral they claim to possess. Second, it can be argued that systems in this category require an expensive and wasteful hoarding of assets, making such a system of money parasitic to the existing economy.[3]

Heterogeneous Collateral Coins

Instead of using the same asset as that of the tracked price, stablecoins of this variety use a different collateral asset. Usually, this is a cryptocurrency such as Ether or Bitcoin. The advantage of crypto-collateral is that there is never any risk that the issuer of the stablecoin does not have sufficient collateral to cover all outstanding liabilities.

Weaknesses

> Given that the collateral and tracked assets are not the same, an excess of collateral must be held to cover relative price swings. This is likely to aggravate any parasitic effects such a currency might have in comparison to homogeneous collateral coins. This required excess of collateral makes such approaches extremely expensive in practice while still likely insufficient to head off black swan events.

Seigniorage Shares

Often considered the most theoretical class of stablecoins, the systems that follow the Seigniorage Share model involve no use of collateral. Instead, they use a two-token system of shares and coins. A Seigniorage Share system begins with some number of coins, x, distributed across the ecosystem. When the price of the coin rises by $y\%$, $x \cdot y\%$ new coins are created. These new coins are distributed in some manner to holders of the second token, shares. Then in the event that the price of coins falls by $z\%$, new shares are created and sold in exchange for coins (which are then destroyed), until the number of coins falls by $x \cdot z\%$. The basic theory states that by increasing or decreasing the supply curve to match changes in demand, the price can be continually adjusted back to a single chosen equilibrium.[4]

It may be noticeable from the above description that, on one level, the Seigniorage Shares model closely resembles that of current fiat systems. In fiat systems, the money supply is increased or decreased through interactions with a limited list of "accounts". More specifically, money is injected into the economy only to banks which hold accounts with the Central Bank and to individuals or entities from whom the Central Bank purchases government securities. In a similar way, new coins in a Seigniorage Share system are only distributed to holders of shares. Additionally, in both systems, the injection group is likely to be the same. Since wealthier individuals are more likely to borrow from banks and purchase either government securities or seigniorage shares, new currency is likely to be injected to the same (wealthy) segment of society through a seigniorage shares system as in our current fiat systems.[5] Under assumptions of long-term economic growth (and a correspondingly increasing money supply), such systems will result in increased economic inequality because those individuals and entities most exposed to increases in currency supply are those least exposed to the wealth erosion produced by the corresponding inflation.[6]

An important note to make here is that we understand and respect the investment being made by seigniorage shareholders. The above criticism on grounds of increasing inequality are meant not to argue that those who make such investments and accept increased risk are not entitled to the appropriate returns. Rather, we merely argue that such a system itself is flawed and detrimental to society. For this reason, we propose an alternative.[7]

Poly Proposal

We herein propose a new model of stable currency built on the tri-pillars of Fisher's Equation of Exchange, the robust asset tracking ability of blockchain systems, and the ideal of equitable seigniorage. At the most

basic level, this model resembles that of the seigniorage shares model in that it increases or decreases the currency supply as necessary and excludes the use of any collateral. However, our model diverges from seigniorage share efforts and more closely resembles fiat systems in that it considers both volatility control and economic stimulus (or impedance) as motivating factors for adjusting currency supply. Finally, the Poly is designed to follow an novel distribution scheme in its seigniorage, incorporating concerns regarding systematic and unnecessary drivers of inequality.

Protocol Requirements

Before introducing the specific mechanisms of the Poly currency system, it is necessary to outline the requirements of the Protocol through which the Poly will be offered as a currency.

1. Transactions must be carried out and stored on a blockchain ledger.
2. The blockchain ledger must be able to uniquely identify assets from each other based on their history, with the ledger having a UTXO (or similar) model.
3. All transfers involving financial assets or transactions must be marked as such.
4. Fees on transactions must be applied as a percentage of the price, in Polys, of the involved transfer.
5. The mechanism responsible for adjusting the supply of Polys must have access to transaction and transaction fee data.
6. Polys collected as transaction fees must be capable of being "locked up" for a specified period of time.

The reason for each of these above requirements will be covered through our introduction of the Poly system.

Tracking the Equation of Exchange

Resting at the base of nearly all attempts at monetary policy is Irving Fisher's algebraic formulation of the Equation of Exchange:

$$M \cdot V = P \cdot T$$

where for a given economy, over some period t, and ignoring any short term effects,

- M is the total supply of money in circulation,
- V is the average number of times money will be transacted with,
- P is the price level,
- T is the real value of all transactions over some period.

When stripped of assumed relationships involving interest rates and endogenous versus exogenous supply's of money, this formula becomes nearly tautological, but is nevertheless illustrative and useful.

Seigniorage Shares

The seigniorage shares model was built with explicit reference to the Equation of Exchange. It's author, Robert Sams, stated the system's basic rule as follows:

> [A]t the end of some pre-defined interval of time, if the change in coin price over the interval is $x\%$, change coin supply by $x\%$.

This rule relies on a rearrangement of the Equation of Exchange to $M = P \cdot T/V$ and assumes—as is done in most iterations of the Quantity Theory of Money—that to the extent there even exist any relation

between M or P and T/V, it can be ignored. While the above rule is likely valid, at least in a long term sense, it illustrates a focus on stability at the expense of good monetary policy. Looking only the price level, the seigniorage shares model neglects to account for times when an economy may need to be stimulated or impeded by altering the monetary supply based on factors other than the explicit price level.

Poly

In contrast with the seigniorage shares model, the Poly system alters its currency supply not based on the explicit price level but rather on the real value of its associated economy, T, and the velocity of currency movement, V. By ignoring explicit price levels directly, we both respect Goodhart's law and circumvent two major issues. Moreover, we hope establish the Poly not as a blockchain representation of another (fiat) currency but rather as a independent currency unto itself.

The first of these two issues is a weakness of the seigniorage share model back in its original elucidation. This is the problem of accurately and trustlessly[8] measuring the price level. Given that both methods of trustless information gathering, Distributed Oracles and Schelling points, have still yet to be robustly tested and have known weaknesses,[9] the avoidance of relying on a feed on the price level offers a distinct advantage. The second problem we seek to address is that price levels are often "sticky" and fail to adjust in the short term, in fiat systems, this results in situations in which Central Banks are forced to estimate future price levels to determine present policy.

Because of this we, propose to adjust the currency supply not based on total P but rather on quantity $T_{real}/V\ dt$, where T_{real} represents the value of all non-financial transactions in our economy.[10] The measurement of this ratio as a function of time offers two advantages. First, as defined in our protocol requirements, this information is endogenous to the system and therefore does not rely on any trusted or complex price feeds. Second, by measuring the change in this ratio over time we can effectively measure any changes to the economy and, perhaps more uniquely, whether they are driven by financial or productive considerations. Based upon the changes in $T_{real}/V\ dt$, we propose the following rule.

$$T_{real}/V dt = \Delta M$$

In this equation we can see that, when Vmoves faster than T_{real}, we are faced with inverse change in the money supply, M. This is desired since growth in V exceeding T_{real} is very likely a sign of asset bubbles or other economic overheating. On the other hand, V decreasing faster than T_{real} is a likely indicator of a financial crash. Finally, any changes in T_{real} unmatched by changes in V should be taken as signs of real economic change which should be matched by changes in the money supply to allow the velocity of money to return to its previous equilibrium.

Calculating M dt

Having decided upon a rule upon which to base changes in our money supply we must now determine how to obtain our necessary inputs and how to distribute money into or remove money from the economy.

Determining Inputs

Turning first to the issue of obtaining $T_{real}/V\ dt$, we can quickly see that only one piece of this will prove difficult, the calculation of $T_{real}\ dt$.[11] Interestingly, since we have required that we can precisely measure all

other variables in the equation of exchange, we could quite easily solve for T. However, this would provide us no insight into the financial and non-financial makeup of our total transaction value. To accomplish this, we must first calculate a price level for non-financial assets:

1. In a given period t_0, we analyze our transaction data to determine the n most valuable assets by total volume, which also occupy places among the m most valuable assets by total volume in period t_{-1}. We denote this basket as $B_0\left(P_0\right)$.
2. The total value and proportionate makeup of this basket in period t_{-1} is then scaled to match that found in period t_0 and denoted as $B_{-1}\left(P_{-1}\right)$.
3. Taking the ratio $B_0\left(P_0\right)\ /\ B_{-1}\left(P_{-1}\right)$, we multiply it by the total value of all non-financial transactions in period t_{-1}, $T_{nf,-1}P_{nf,-1} \cdot \left(B_0\left(P_0\right)\ /\ B_{-1}\left(P_{-1}\right)\right)$, to obtain $T_{nf,-1}P_{nf,0}$.
4. Finally, we calculate $T_{nf,0}P_{nf,0} - T_{nf,-1}P_{nf,0}$. Since the price level in both terms is now identical it can be ignored and we have therefore obtained $T_{nf,0} - T_{nf,-1} = T_{nf}\ dt$.

Distributing M dt

Having successfully extracted $T_{real}/V\ dt$, we must now determine how to distribute changes in the money supply when necessary. The first determination that must be made towards the adjustment of our currency supply that of the relevant time frames. Each supply adjustment requires three time periods, two to calculate movement in $T_{real}/V\ dt$ and one to adjust the supply. As described above, we utilize periods t_{-1} and t_0 to calculate the necessary adjustment. Once we have determined the required ΔM, we adjust our supply in period t_1. For simplicity, we propose that as this cycle iterates, it always begins with period t_{i+1}, where t_i was the distribution period of the previous cycle.

Having defined our three step process, let us first consider the case where ΔM is positive. In these scenarios, ΔM will be distributed pro rata to each existing positive Poly balance. Importantly, this distribution will be randomly distributed in time over the period t_1 in order to avoid excessive market activity attempting to benefit from known supply adjustments. Turning now to cases where ΔM is negative, we are faced with a more challenging problem, how to contract the money supply. Leveraging the fact that the movement of funds and value through the described Protocol must be paid in Polys, we propose that in times of monetary contraction, transaction fees are increased and the Polys collected as fees are not immediately transferable. The specific algorithms of this process are still being tested in simulations.

Conclusion

Although significant work remains, including the calculation of ideal values for key variables introduced, we believe that the Poly represents a promising new model of currency. First, as a single token stablecoin system, the Poly is designed to be free of well-known concerns involving the use of collateral as well as the lesser known problem of inequality created in multi-token systems. Second, by relying on endogenous information involving transaction value and velocity instead of on external price feeds, the Poly is first and foremost a new currency unto itself, not a crypto-peg to an existing currency. Taken together, these two considerations lead us to an optimistic assessment of the unique potential of the Poly.

1. M. Friedman (1969), *The Optimum Quantity of Money,* Macmillan
2. https://github.com/rmsams/stablecoins/blob/master/paper.pdf
3. This point depends largely on the specific assets chosen as collateral and the method of implementation and whether or not these assets were already being held for another purpose. We have in fact even written a cursory proposal suggesting this criticism can be circumvented.
4. By introducing an additional third token, certain groups have attempted to conduct ICOs for such systems. While it is creative and occasionally profitable for the issuer, such a modification does nothing to improve upon the model and is more likely to prove detrimental. This is due to the fact that the third token exists merely to collect newly distributed coins in the event that their are no shares outstanding. Since we do not believe that there are any reasonable equilibrium states where such a scenario will occur, we perceive this third class of token to be merely a fundraising tool that may even weaken demand for shares.
5. It follows from the simple fact that those with higher incomes can and do allocate a greater percentage of their incomes to financial assets that Seigniorage Shares will be disproportionately held by wealthier individuals. However, understanding this the analogous mechanism for fiat systems is slightly more involved. First, we must recognize that as household income increases so too does the income to debt ratio. Second, we note that the manipulation of interest rates is the primary method by which money supply is adjusted in fiat systems. Therefore, since those with higher incomes carry high debt loads, they are more directly affected by changes in monetary supply through interest rate manipulation. Moreover, as is the case with Seigniorage Shares, wealthy individuals are more likely to hold national bonds, which produce yields that closely track inflation.
6. The relationship between one's exposure to growth in currency supply and inflation can be understood as follows. As new money is issued into an economy, prices are driven up, or at least prevented from falling as they would have otherwise. While we can assume that everyone is equally exposed to this price increase, we other effects of new currency creation are not equally distributed. In the case of Seigniorage Shares, the additional currency issued serves to offset any losses incurred as a result of increasing prices for anyone holding shares. In fiat systems, it is the decreased cost of borrowing that serves to offset losses due to inflation. However, this offsetting benefit is distributed only according to one's debt level, which again is a function of one's income and wealth.
7. It is important to note however, that the argument for rewarding individuals for taking increased risk only applies in the case of Seigniorage Shares and not in fiat systems since government bonds (at least in countries such as the US, Canada, EU, and UK) are considered "risk-free".
8. The element of trustlessness is one of critical importance to the blockchain ethos and represents one of the core motives behind its creation and adoption.
9. More specifically, Distributed Oracles suffer from the need for complex governance and dispute periods to protect against misbehavior by a minority group and lack of sufficient participation by the majority. On the other hand, Schelling Points are still largely theoretical and while they work well for extremely simple questions, determining price levels may still be beyond their scope.
10. By non-financial transactions, we refer to all services and goods, excluding financial assets such as stocks, bonds, options, and currency instruments. We exclude financial transactions here to allow for the detection of financial crashes and asset bubbles. Exerting opposing pressure to which will be a critical task of the subsequent changes in Poly supply.
11. Note that the velocity can be trivially extracted from our Protocol as specified in Protocol Requirement 2. More specifically, this could be measured directly by randomly selecting individual Polys, looking at how often they changed hands, and averaging the individual results.