Rebase: Social Capital System with Adaptive Supply

E. White
July 6, 2020

Abstract

Quantitative easing in various monetary systems concentrates the issuance of the currency into the accounts of few market participants, undermining the utility of the market distortions. Monetary policy has been unilateral, opaque, arbitrary and reactionary, leaving the market guessing at the whims of centralized authorities. On the contrary, transparent known supplies and issuance schedules, such as in digital commodities like Bitcoin or Ethereum, lead to complacency of the market participants in a disinflationary economy with poor velocity. An adaptive supply which updates at a greater frequency and is transparent and verifiable will offer an economic system and policy that is unparalleled across societies. In this paper, we introduce the concept of altering the monetary base through a process called *rebasing*, how a fair distribution of stimulus can inject capital into communities that have been underserved by prior monetary policy, and how community driven liquidity pools can be incentivized on a bonding curve.

1 Introduction

Quantitative easing ("QE") has been a primary policy tool over the 21st century by central banks to stimulate economic growth. The concept is to expand the monetary base by purchasing from a universe of eligible assets, such as government bonds, investment grade corporate bonds, mortgage backed securities and more. When the central bank purchases an asset, the prior owner of the asset has received new money created at the time of transaction. The goal is for the beneficiary to continue purchasing and investing with the new money in order for it to circulate in the economy. The incentives are misaligned for this to occur. Frequently, the beneficiaries are large publicly traded corporations, who purchase their own shares after having sold assets at a premium to the central bank. The market distortions of the central bank activity are now twice removed, with higher bond prices and higher share prices, despite the central bank never having purchased shares. Growth is still limited as the capital and credit is not extended to the productive economy at this stage, and the funnel to achieving the goal requires accompanying fiscal policy. Fiscal policy lacks consensus.

An innovation to avoid the burden of fiscal policy adjustments is to create a monetary system that more directly stimulates economic growth. The challenge has always been obtaining accurate data from the economy, which can be partially solved using a decentralized group of oracles, feeding data into the easing framework for immediate reaction. With this data, when demand in the economy outpaces supply of the monetary base, the system can "rebase" the monetary supply, increase the amount of currency everyone holds at once.[1] This is in direct contrast to quantitative easing where only the nearest credit worthy participants receive more currency, by already owning assets in the eligible universe, or by being considered credit worthy to create new eligible assets for sale.

Supply or demand shocks to the monetary base, as well as subsequent rapid rebasing, can result in high pricing volatility. The actual effect of pricing volatility for the currency holder is smoothed by a changing balance of the currency as a direct product of rebasing. The effect can be further smoothed by controlling the demand for the asset by incentivizing flows into community organized liquidity pools (LPs), a process which automatically rebalances the amount of liquidity on both sides of the exchange market, and locks the liquidity in place for varying terms, removing a potential seller and their increased supply from the market. Demand can therefore keep up with rapid and hyperinflation, as well as slow down, without leaving a market flooded with supply in its wake. The system reaches equilibrium faster.

[1] Evan Kuo, Brandon Iles, and Manny Rincon Cruz, *Ampleforth Original Whitepaper, (*Ampleforth Foundation, 2019)

2 How it works

The total supply expands and contracts based on an individual unit's relative value against a basket of currencies, aiming to retain a certain notional value, such as $1. For example, the Swiss Franc, CHF, has maintained near-parity with the US Dollar from time to time, via expansion and contraction of its money supply, coordinated by the Swiss National Bank manually. Our system adopts the same concept to automatically contract supply when under $1, proportionally deleting some of the money supply from all distinct holders' asset at set intervals, making the currency scarcer until it recovers a notional value of $1. When above $1, the system automatically expands the supply until it is no longer considered scarce and trades for $1 again. The owners of our asset should expect to have a predictable purchasing power and means of exchange over time, deterring rampant speculation and any expectation of profit. The system matches the demand with the supply.

In this kind of system, the supply adjustments are done programmatically in a process called "rebasing". As the monetary *base* is *re*-adjusted. The inputs to how a rebase occur can follow varying approaches. Some existing systems implement oracles to collect data outside of their asset's closed loop economy and feed that into the supply coordinator to determine how much to change the supply, if at all. The confidence in the data comes from using multiple independent oracles that have reached the same result. This is one approach. Another approach is to try to use inputs from within the economy. For a digital asset operating in a virtual machine, there are records of all states of the use. Therefore, the asset's own smart contract can attempt to calculate the supply changes based on activity, or at the very least verify information that the oracles convincingly input.

In established rebasing monetary supply formulas,[2] the following occurs, at a set known interval, such as daily.

Notional price/unit	Rebase %
$1	0%
$1.10	1%
$1.20	2%
⋮	⋮
$2.00	10%
$3.00	20%
$4.00	30%
⋮	⋮
$10	90%
$11	100%
$12	110%
⋮	⋮
$$n$	$(n * .1) - .1$

The goal after each positive rebase is for supply to outpace demand, eventually, by automated, programmatic, massive inflation. When an equilibrium is reached, the correct money supply will be found to accommodate the market.

Under $1, negative rebases occur, causing steady deflation. During periods of contraction the system still seeks to match the supply with

[2] $((Or - Pt) / Pt) / 10$ where Or is the rate provided by the oracles, and Pt is the target price.

lowered demand. It should be noted that the target price is the midpoint of a range of values where supply-wide rebases do not occur, and the target price itself can be adjusted.

The general adjustments toward a target price can create an asset uncorrelated with general market sentiment, across the universe of markets and distinct asset classes. An asset of these qualities can be a meta-portfolio hedge, meta-currency[3] due to its stability seeking mechanisms, and also act as collateral for other financial products and *yield farming*, as this paper will later discuss. Uncorrelated assets are often coveted additions to portfolios as they are few and far between and not much capital can be deployed towards them. The rebasing mechanism provides no limitation[4] on total notional value, while the necessary high inflation offers no negative benefits for the economy.

The goal of the system and internal algorithm is to reach an equilibrium in supply and demand, and have its monetary base equal to the notional size of a collection of assets surrounding it, which can be smaller or greater than what a central authority may have initially valued the system as. It can reach the target price with a much lower notional value, after prolonged periods of negative rebasing, and also with a much higher notional value after prolonged periods of positive rebasing due to market forces requiring higher inflation to meet equilibrium.

An asset tied to this system in a small market may experience periods of volatility as it searches for equilibrium. Whereas, a Central Bank Digital Currency (CBDC) using this system would experience the necessary inflation or deflation via the minute adjustments required to maintain its target price, due to representing much larger and known economic output from the onset.

The system uses an internal currency to manage the state of the balances of all addresses. This reduces or removes the need to transfer the updated balances to each address individually to accomplish the supply updates, significantly reducing the cost to operating the system. Instead, when an address' balance is queried, the correct registers are accessed reflecting the proper balance, and when an address transfers any of the asset, that portion of the total balance is subtracted from the sender and added to the destination address, as one would expect but implemented to accommodate adaptive supply changes.

[3] Digital meta-currencies in virtual machines are referred to as "stablecoins"
[4] Different virtual machines have different maximum values. The Ethereum Virtual Machine uses unsigned integers which have a maximum value.

3 Stimulus

In addition to the system wide supply rebase, directed stimulus can be targeted at owners of the asset, to ensure there are no underserviced areas of the economy, rebalancing capital towards an egalitarian society.

An updated rebase function within a virtual machine can use the hashes of saved states – ie. recent block hashes in a blockchain – as random entropy in deciding which account balances should be increased with an extra rebase.

This aspect of the money supply can be conditional on whether there are system wide positive rebases occurring, or negative rebases occurring, both or none at all. The addition of this aspect of rebasing can help end periods of deflation faster and return stability and predictability to the system.

In a blockchain implementation with a virtual machine, such as the Ethereum Virtual Machine (EVM), all distinct owners of the asset have accounts with a hash. The namespace of the hash overlaps with the namespace of the block hashes, so the system can look for similarities at the time of rebase to determine if any particular account should report a larger balance. Any implementation should consider the possibilities of gaming the system, during development. An example implementation involves taking the last two characters from one of the last 128 block hashes, and giving rebases to addresses that have the same two characters. A limited set of block hashes does not require external input from oracles, making a fundamentally more robust and autonomous system than one reliant on the timely availability of third parties.

For example, given a block hash of:

0xa38e6f5d699d8480e1c710077b0d27e7cba1a21af372fcece9b788936607b0**01**

The system checks its registry of all account hashes ending in the same last two characters. As hashes follow hexadecimal, there are 256 possibilities of registers.

```
[00]    => [0x5a0b54d5dc17e0aadc383d2db43b0a0d3e029c00], [0x3767c58b49d2B476ec8C8a411795d5c8caAAd300] ...
[01]    => [0xa10ae543db5d967a73e9abcc69c81a18a7fc0a01], [0x257b97745af59dc97b5ebe6caa598cc611bda601] …
 .
 .
 .
[ff]    => [0xea674fdde714fd979de3edf0f56aa9716b898eff], [0x707191c63c30337ed701a99a529f24cffa4e22ff] …
```

All addresses in the table named [01] now have the larger rebase,[5] whoever owns each address can now spend and invest with a greater amount of currency. A more efficient implementation may be possible, and this example is for illustrative purposes only, implementation is dependent on the stack size of the virtual machine.

[5] The registry more accurately exists as a map or a hashtable.

The imagined data structure should not be computationally expensive, lowering transaction costs to update the state of the EVM across nodes. The smart contract can have a multidimensional mapping, or 256 individual maps. Each key is populated by the address the first time or whenever a transaction is made to that address, requiring a modified *transfer()* function, according to fungible asset protocols.[6]

Using the concept of inheritance, the *transfer()* function can conform to the protocol standard, while extending its functionality. Careful considerations must be made to ensure predictable transfer fees, as well as low transfer fees comparable to the default.

With the above implementation, miners and validators are in the prime position to attempt to gain an advantage, specifically by attempting to manipulate the block hash created at the time of rebase to match their own address. This is why the program can choose a block hash from the last 128 blocks, or a combination of the last blocks, using additional entropy. This makes it further unlikely that any one miner, or attacker, can have an advantage. There are many implementations to solving entropy, and with the use of a proxy contract, the actual digital asset can be upgraded seamlessly, as soon as any gaming or vulnerability is found.

One way to increase demand to offset the inflationary pressure is by incentivizing participants to spread the amount of their holdings across the 256 combinations of addresses. There is daily pressure to own more of the asset, and daily pressure to keep the asset.

Additional stimulus to unpredictable segments of the economy can require further smoothing of the supply to control inflation, as this exists outside of the general step function of adaptive easing. Growing utility to keep the supply low, even in the expansion of the monetary base, can allow demand to keep up in the face of steady inflation.

[6] ERC20 protocol is the “fungible token standard”, usable in any EVM and other systems.

4 Farm

Productive capital is the backbone to any economy. Community organized liquidity pools (LPs)[7] encourage price discovery across a variety of assets, currencies and other mediums of exchange. Some economic systems attempt to incentivize a single LP, amongst digital asset traders this has been called "yield farming", which is a redundant skeuomorph to "farming". Earning a yield from participating in a LP attracts productive capital, while also constricting the supply for varying lengths of time or indefinitely.

Incentivizing a *single* LP to attract farmers has the same issues as centralized monetary policy: a single sector of the economy is the beneficiary of a stimulus, while there are underserved aspects of the economy completely neglected. The central authority has to use its own allocation of the currency at arbitrary amounts, or create new currency at arbitrary amounts, undermining its own monetary policy or the trust in that authority.

A solution is to propose a Decentralized Autonomous Organization (DAO) which incentivizes *many* LPs, ideally as they are formed, or as they are voted on by the community. In this system, the DAO is called a "farm", as it generates new plots for harvest. The farm incentivizes an indefinite number of LPs.

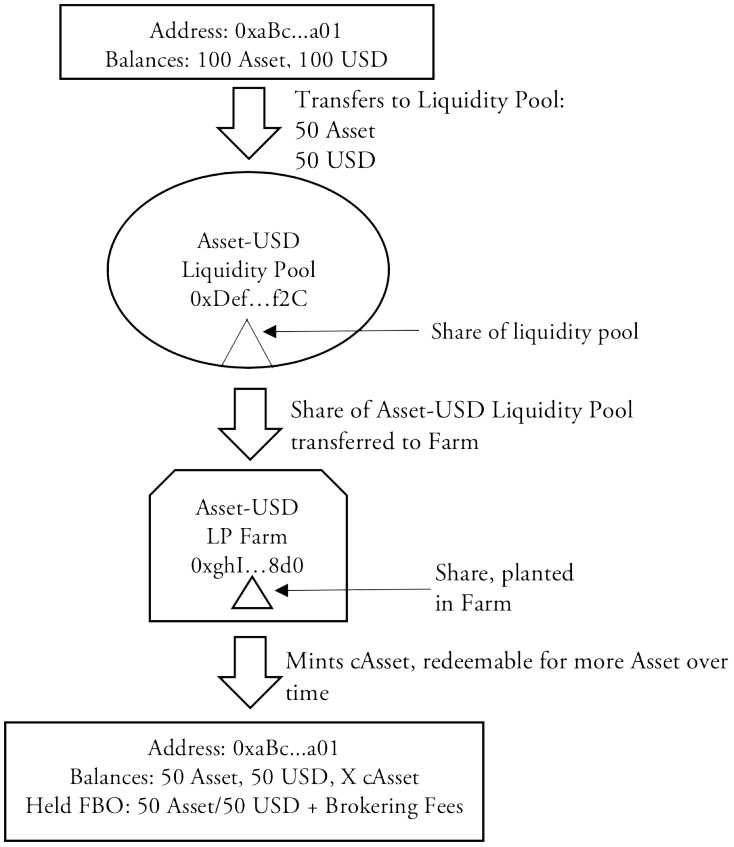
In one implementation, a benevolent organization slowly pays yield to farmers that stake their share of a single LP, paid from the organization's own excess allocation of the asset. The organization cannot continue to do so indefinitely, while yields become less attractive quickly as farmers crowd the market.

In a superior implementation, the farm keeps track of *all* LPs, and allows farmers to plant their stake in each LP. In exchange for planting, they receive a new asset (cAsset, or Asset_c) that is exchangeable for more of an underlying asset over time, priced on a time-based bonding curve. This functions analogously to interest, but removes the need for continually transferring interest payments, lowering the costs of the economy. Non-interest-based returns are compatible with a broad range of cultural and regulatory environments. Redeeming a cAsset mints the appropriate quantity of the primary system asset[8] and the velocity can be further limited by

[7] Prospective purchasers of an asset and ecosystem built to this model should understand that liquidity pools and secondary markets may not form, or may not always have liquidity. Purchasers cannot be construed to have an expectation of liquidity.

[8] The Farm autonomously incentivizes the creation of staking markets, and autonomously issues time bonded assets, redeemable for more of the underlying asset over time. Purchasers of the underlying asset cannot be construed to have an expectation of profit by merely purchasing the underlying asset, or by hypothetical and optional use cases. Liquidity pools are third party contracts, deployed by a different factory DAO, populated by the community. Their stake in the LP is transformable into a bonded asset, autonomously by the Farm.

deterring early withdrawals from the farm, restricting withdrawals, penalizing early withdrawals, or a combination thereof.



The example above demonstrates with a portfolio of Asset and USD[9] that one address owner can deploy productive capital and earn in a variety of ways. The productive capital helps the ecosystem by providing liquidity without any assurance of liquidity from a benevolent organization or issuer, while earning brokering fees from other's use of the LP, and also from the time-based bonded curve cAsset. Putting their supply of the asset to use disincentivizes the desire to sell and can help deter a prolonged period of negative rebases. In exchange, they create the bearer cAsset which can be further independently spent for goods and services, or invested in opportunities outside of the system.

Additionally, all distinct addresses are subject to the normal rebase, as well as the stimulus rebase, distributing the opportunities for the farmer. If the farmer had a portfolio of other assets, such as EUR, they could also create or join an Asset-EUR LP, and Asset-EUR LP farm, or the same with other portfolio assets. If farm creation is not automatic, farm governance can be added to allow participants to vote on the addition of LP contract shares to be included in farm contract recognition.

[9] The wrapping and tokenization concepts allow for surrogates of assets outside of the monetary system to be traded against each other.

5 Conclusion

Adaptive supply and stimulus, dictated autonomously by the rebasing concept, can offer an alternative to the need for benevolent organizations unilaterally stewarding and altering the money supply. The effects of programmatic rebasing can be further lessened by providing a Decentralized Autonomous Organization for productive capital as new supply enters the market during periods of inflation, or reducing prolonged periods of deflation.

As demonstrated, the rebasing functionality also creates an uncorrelated asset which can be deployed for a variety of purposes, including a system for Central Bank Digital Currencies that unburdens the Central Bank from unilateral monetary policy decisions to meet inflation targets. An uncorrelated asset deployed by a community can complement the universe of assets, and supersede the need for Central Bank Digital Currencies entirely.

Aligning the incentives for community provided liquidity assist the rebasing step functions in reducing the volatility in notional value as the system seeks equilibrium.