PeerFed: A Self-Stabilizing Peer-to-Peer Monetary System

Joshua Doman
joshsdoman@gmail.com

Abstract. A stabilizing monetary policy is necessary for a peer-to-peer system like Bitcoin to maintain a consistent unit of value. This paper presents a peer-to-peer system that is self-stabilizing in an efficient market, with no trusted third parties, external peg, or other dependencies. The system consists of two convertible assets, interest-bearing cash and a paid-in-kind perpetual bond. The market sets the interest rate by converting between cash and bonds, and a constant sum-of-squares conversion rule ensures the aggregate nominal value of the system approximates an infinite-period paid-in-kind perpetuity. As such, the nominal value of the system rises when the interest rate falls, falls when the interest rate rises, and grows at the interest rate at all other times. In equilibrium, the interest rate is the real opportunity cost of capital of the system, and if the market is efficient, the system's nominal and real value are kept in sync, stabilizing the real value of cash.

1. Introduction

Recent monetary instability highlights the need for a credibly-neutral, self-stabilizing monetary system that is independent of trusted third parties. Satoshi Nakomoto solved the double-spending problem with the creation of Bitcoin, but the lack of a stabilizing monetary policy limits Bitcoin's use.[1] Nakamoto acknowledged this limitation but did not know of a solution:

> "There is nobody to act as central bank or federal reserve to adjust the money supply as the population of users grows. That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things. If there was some clever way, ... the rules could have been programmed for that."[2]

To solve this problem, we need a model for how demand behaves in an efficient market. We can then design a mechanism that automatically responds to changes in demand. In this paper, I show that an infinite-period paid-in-kind perpetuity is the appropriate model. This means that in an efficient market, change in demand is a function of the real opportunity cost of capital, or the real rate of return that could be earned elsewhere in the market investing at a similar level of risk.

Informed by this model, I present a system consisting of two convertible assets, interest-bearing cash and a paid-in-kind perpetual bond, which accrues interest at the same rate as cash but in the form of additional bonds. The market sets the interest rate by converting between cash and bonds, and a constant sum-of-squares conversion rule ensures that the conversion rate equals their relative market price and that the yield on cash and bonds is the same.

I assert that the value maximizing strategy is for the nominal and real value of the system to grow at the same rate, so that the expected rate of change in the real value of cash is zero. This means that in equilibrium, the interest rate is the real opportunity cost of capital. In an efficient market, the aggregate nominal value approximates an infinite-period paid-in-kind perpetuity, mirroring changes in the real value of the system and keeping the real value of cash approximately the same. In practice, the degree to which the system is self-stabilizing is a function of the efficiency of market forces. At the limit where the market is perfectly efficient, cash is an ideal unit of account and store of value, and the interest rate approximates the real risk-free rate.

Being oracle-free, there are multiple ways to implement the system. In the spirit of adhering as closely as possible to Nakamoto's original design, I describe a modified version of Bitcoin with a suitable issuance schedule for block rewards. Alternatively, the system could be implemented as a smart contract on Ethereum, a meta-protocol like BRC-20 on Bitcoin, or even as a hard fork of the existing Bitcoin ledger.[3][4] Different implementations have different drawbacks, and the optimal implementation is left for future debate.

2. Assumptions

I evaluate the system under the usual behavioral assumptions that investors prefer more wealth to less, prices are determined in the market such that perfect substitutes are valued identically, and dominant assets do not to exist.[5] I also assume no transaction costs, equal access to information for all investors, and a flat term structure for real interest rates. Finally, I make the following assumptions about the system:

(1) The aggregate real value of cash and bonds is irrespective of their relative quantity, just as the value of a firm is irrespective of the relative quantity of preferred and common stock.[6]
(2) The aggregate value of the system is non-zero.
(3) The value-maximizing strategy for investors is to keep the system in equilibrium, such that the expected rate of change in the real value of cash is zero.

3. The Real Value of the System

We start by considering a hypothetical perpetuity with an expected real cash flow of C per year. Let r_{real} be the real opportunity cost of capital of the perpetuity. By the perpetuity formula, its present value in real terms is C/r_{real}, as is its expected value in all future periods.

Now, let's suppose this perpetuity is paid-in-kind for the first period. This means that instead of receiving C cash, r_{real} additional perpetuities are received, which are expected to be of equal value to the real cash flow C. This does not change the present value of the perpetuity, so its value is still C/r_{real}. If we suppose the perpetuity is paid-in-kind for N periods, this would still be the case, but we we would expect to have $(1+r_{real})^N$ perpetuities after N periods. At the limit where N approaches infinity, the present value is still C/r_{real}, and the quantity of perpetuities held forever compounds at the r_{real} in each period.

Let's now consider a hypothetical monetary system where every currency unit forever accrues interest at its real opportunity cost of capital. If $r_{real} = 1\%$, for instance, every holder sees their balance grow at a rate of 1% per year. If r_{real} changes to 2%, balances grow at a rate of 2% per year, and so forth. We observe that this asset is identical to our infinite-period paid-in-kind

perpetuity. We have simply replaced the word "perpetuity" with "currency unit." Provided the currency has value, its real present value takes the form of C/r_{real}, for some C and some r_{real}.

We can thus describe how r_{real} relates to the change in the aggregate real value of the monetary system. Specifically, we consider a monetary system where all currency units already exist and currency units cannot be destroyed. The aggregate value of this monetary system is simply the quantity of currency units Q multiplied by C/r_{real}. The quantity of currency units compounds at r_{real} continuously, so the aggregate real value does as well.

Let Q_0 be the initial quantity of currency units and let $r_{real}(t)$ be the real opportunity cost of capital at time t. We can model the real value of the system $V_{real}(t)$ as:

$$V_{real}(t) = \frac{Q_0 \cdot C}{r_{real}(t)} \cdot e^{f(t)}$$
$$\text{where} \quad f(t) = \int_0^t r_{real}(t')dt'$$

In this system, where each currency unit accrues interest at r_{real}, the expected rate of change in the real value of a currency unit is zero. However, the value of a currency unit will change if r_{real} changes. If r_{real} doubles, for instance, its value will fall by half. This inherently makes the currency risky and thus unsuitable as money. This system is also impractical without a way to measure r_{real}. The described monetary system solves these two problems.

4. The Monetary System

Let two assets be issued. Let's call one cash and the other a perpetual bond. Let M be the supply of cash, and let B be the supply of bonds.

(1) Continuously compound M and B at an annualized interest rate r, where $r = M/B$. Distribute new supply on a pro rata basis to cash and bond holders, respectively.

(2) Let cash and bonds be freely convertible, such that $M^2 + B^2 = (M + \Delta M)^2 + (B + \Delta B)^2$, where ΔM and ΔB is the change in the cash and bond supply due to the conversion.

5. The Conversion Rate

Inspired by the constant function automated market maker Uniswap,[7] the constant sum-of-squares conversion rule ensures the marginal conversion rate from bonds to cash always equals $1/r$. The conversion invariant can be described as $M^2 + B^2 = K^2$, where K is some constant during the conversion. We observe that the marginal bond dB can be converted to cash at B/M, which equals $1/r$:

$$\begin{aligned} -\frac{dM}{dB} &= -\frac{d}{dB}\left(\sqrt{K^2 - B^2}\right) && \text{(since } M = \sqrt{K^2 - B^2}\text{)} \\ &= \frac{B}{\sqrt{K^2 - B^2}} \\ &= \frac{B}{M} \end{aligned}$$

Assuming no arbitrage or conversion costs, this conversion rate equals the nominal price of a bond in the open market. To illustrate, suppose that B/M is not the market price. Without loss of generality, let's assume the nominal price is above B/M. By symmetry, the conversion rate from

cash to bonds is M/B. Arbitrageurs can purchase cash, convert to bonds starting at M/B, and sell them in the market for a profit. Doing so will increase B and decrease M, causing B/M to rise. This will continue until B/M equals the fair market price.

6. Yield Equivalence

A bond returns additional bonds at the rate $r = M/B$, each of which is worth B/M cash, so the bond is expected to return nominal value at a rate of one unit of cash per year in perpetuity. The nominal yield on the bond is therefore $1/P$, where P is its nominal price. The nominal yield on cash is $r = M/B$ and $P = B/M$, so the yield on cash and bonds is the same. Having the same rate of return, cash and bonds have the same opportunity cost of capital in an efficient market.

7. The Nominal Value of the System

The aggregate nominal value of the system is the sum of the quantity of cash M and the quantity of bonds B times the bond price B/M:

$$V_{nominal} = M + B \cdot \frac{B}{M}$$

Applying the conversion invariant and rewriting in terms of M and the invariant K, we have:

$$V_{nominal} = \frac{M^2 + B^2}{M} = \frac{K^2}{M}$$

Using the relationship $r = M/B$, we can rewrite M in terms of K and r:

$$M^2 + B^2 = K^2 \implies M^2 + \frac{M^2}{r^2} = K^2 \implies M = \frac{Kr}{\sqrt{1+r^2}}$$

Substituting and simplifying, we obtain the result:

$$\begin{aligned} V_{nominal} &= \frac{K^2}{Kr} \cdot \sqrt{1+r^2} \\ &= \frac{K}{r} \cdot \sqrt{1+r^2} \end{aligned}$$

If r is small, the square root term can be ignored, and we see that the nominal value of the system is approximately K divided by the interest rate.

$$V_{nominal} \approx \frac{K}{r} \qquad (\text{if } r \ll 1)$$

Since M and B compound at r, K compounds at r. Let K_0 be the initial invariant and let $r(t)$ be the interest rate at time t. Assuming continuous interest, we can model the approximate nominal value of the system with respect to time t:

$$V_{nominal}(t) \approx \frac{K_0}{r(t)} \cdot e^{f(t)}$$

$$\text{where} \quad f(t) = \int_0^t r(t')dt'$$

Thus, the nominal value of the system approximates an infinite-period paid-in-kind perpetuity with an opportunity cost of capital of r when r is small.

8. The Optimal Interest Rate

Like any asset, there is some real rate of return r_{real} required by the market to invest in the system given it's riskiness. This equals the real opportunity cost of capital in an efficient market. Earlier, we describe with respect to time t the aggregate real value of a single currency system where each currency unit accrues interest at its real opportunity cost of capital r_{real}. We assert that the aggregate value of a system where every currency unit accrues interest is identical to one where no currency unit accrues interest and that the value of our dual-claim system is identical to one with only one claim against it. Therefore, the infinite-period paid-in-kind perpetuity, discounted at r_{real}, is an appropriate valuation model for our system.

We therefore reason that r_{real} is the optimal interest rate. At this rate, the nominal value of cash and bonds grows at the same rate as the real rate of return of the system, and the rate of change in the real value of cash is zero. This is a desirable property in a unit of account and optimal for this monetary system, which otherwise lacks intrinsic value. While inflation may be desirable in some monetary systems, it serves no economic purposes in this one because the real rate of return on cash and bonds is irrespective of inflation expectations.

9. Proof of Equilibrium

We prove that $r = r_{real}$ in equilibrium via the criterion of dominance. The proof is inspired by Ingersoll's proof that a convertible security with constant conversion terms will not be converted prior to maturity.[5] Suppose $r < r_{real}$ and consider the following two portfolios. Portfolio I consists of all M cash and some amount of bonds b. Portfolio II is identical, except the bonds b are immediately converted to cash. b is chosen such that $r = r_{real}$ after converting.

Since we own all the cash, we can convert back from II to I at any time if needed. II is therefore no riskier than I. $r = r_{real}$ is the value maximizing strategy, so if r_{real} stays the same, Portfolio II outperforms Portfolio I. While Portfolio I could convert to cash at a later date, it faces the non-zero probability that other bondholders convert first, leaving it with less nominal value than Portfolio II. Thus, Portfolio II outperforms Portfolio I in some future states and performs equally to I in all other states, making it the dominant portfolio. Since the cost of the two portfolios is the same, Portfolio I will not exist under no dominance. Thus, $r \not< r_{real}$. Without loss of generality, by reversing the portfolio construction, we prove that $r \not> r_{real}$. QED.

10. On the Stability of Cash

The value of cash is determined by the nominal value of the system relative to its real value. We assert that in a mature economy using this monetary system, the equilibrium interest rate is much less than 100%. As such, given $r = r_{real}$ under our market assumptions, the nominal value of the system approximately mirrors any change in its real value, keeping the real value of cash approximately the same when r_{real} changes.

In practice, the stability of the system is dependent on the efficiency of market forces. Market participants will buy, sell, and convert cash and bonds in accordance with their perspective on r_{real}. As such, r will reflect market consensus for r_{real}. The extent to which $r = r_{real}$ determines the stability of cash and thus the riskiness of the system. For this reason, cash will not be initially stable, but as capital markets develop and market efficiency improves, r will become more

accurate, causing the riskiness of investing in the system to fall. At the limit where the market is perfectly efficient, cash becomes a risk-free asset, and r_{real} equals the real risk-free rate r_f.

11. A Macroeconomic Thought Model

To ground our understanding, consider an economy using this monetary system where a new technology is introduced and the economy experiences a positive supply shock. For simplicity, let's assume $r_{real} = r_f$.

(1) With a positive supply shock, the investable opportunity set grows more attractive relative to risk-free assets, and r_f rises.
(2) With a higher r_f, the equilibrium interest rate rises, and bonds are converted to cash.
(3) With a higher interest rate, the aggregate nominal value of the system falls but grows at a faster rate. This reflects an economy with faster growth and less demand for risk-free assets.
(4) Conversely, if economic conditions reverse, the investable opportunity set grows less attractive, causing r_f to fall.
(5) This causes cash to be converted to bonds, increasing the aggregate nominal value of the system and slowing its rate of growth. This reflects an economy with slower growth and greater demand for risk-free assets.

12. A Blockchain Implementation

A modified version of Bitcoin can readily support this monetary system by internally representing ownership of "shares" of the cash and bond supply rather than ownership of cash and bonds directly. In this system, transaction outputs are denoted as cash or bond shares by a single byte, and the outstanding supply of cash and bond shares M_s and B_s is tracked in the header of each block. A computed scale factor F then determines the amount of cash or bonds that each share has a claim to at the start of the next block. Thus, the total supply of cash M and bonds B at the end of a block is simply the number of shares outstanding times the scale factor F:

$$M = M_s \cdot F$$
$$B = B_s \cdot F$$

The scale factor F is computed using the history of the chain. Starting at $F = 1$, the scale factor F compounds each block at the previous block's annualized interest rate $r = M_s/B_s$ divided by the average number of blocks per year. Since M_s and B_s scale by the same scale factor F, the interest rate r still equals M/B. Blocktime provides a trusted measure of time for the interest rate, and interest compounds nearly continuously, since blocks are produced every few minutes.

Users transfer cash or bonds by transferring the corresponding number of shares. This calculation can be abstracted away by the user's wallet, using the scale factor at the time the transaction is signed. Users convert between cash and bonds according to the invariant $M_s^2 + B_s^2 = C^2$, where C is some constant. The exact conversion rate depends on the ordering of conversions in the block, and M_s and B_s are internally updated after each conversion, with the final values being recorded. This conversion invariant is consistent with $M^2 + B^2 = K^2$, since F and C are the same before and after a conversion.

The format of a conversion is like that of a normal transaction, with the inputs and outputs

defining the maximum allowable input and minimum allowable output amounts. An unspendable output with a special opcode identifies the transaction as a conversion, and the output amount denotes the transaction fee. The remaining amount of the conversion appears as an extra output in the coinbase transaction, with the recipient address and remainder type (cash or bond) defined in the script following the previously mentioned opcode. This remainder would be subject to the coinbase maturity rule, but this is unavoidable since the final conversion rate is subject to block reorganizations.

Lastly, the block subsidy is split between cash and bond shares, such that if the block subsidy is R, the miner receives $M_s \cdot R/C$ cash shares and $B_s \cdot R/C$ bond shares each block (plus fees). This split avoids inadvertently changing the interest rate r and increases C, the fully converted supply of bond shares, by exactly R each block:

$$\begin{aligned}(M_s + M_S \cdot \frac{R}{C})^2 + (B_s + B_S \cdot \frac{R}{C})^2 &= M_s^2 \cdot (1+\frac{R}{C})^2 + B_s^2 \cdot (1+\frac{R}{C})^2 \\ &= (M_s^2 + B_s^2)(1+\frac{R}{C})^2 \\ &= C^2 \cdot (1+\frac{R}{C})^2 \\ &= (C+R)^2\end{aligned}$$

An issuance schedule like that of Bitcoin would halve R every four years, ensuring that the fully converted supply of bond shares increases deterministically and the terminal supply is finite. The following section explains why this issuance schedule does not affect the stability of the system.

13. On Issuance

13.1. On Deterministic Issuance in Bitcoin—In an efficient market, Bitcoin's deterministic issuance schedule has no impact on its monetary properties. A claim is just as risky as one in an identical system that issues all claims upfront, since future supply is just as certain and finite. The ownership percentage when all supply has been issued is the same and the required rate of return is identical, so the claim has the same present value and rate of return in the two systems.

To illustrate, let $p(t)$ be the percentage of the monetary system that a claim owns at time t. The present value of this claim is simply the expected value of the Bitcoin monetary system at time t multiplied by $p(t)$ discounted by the real opportunity cost of capital r_{real}. The riskiness of investing in bitcoin is independent of how claims are distributed between now and time t, provided issuance remains deterministic, so r_{real} is unaffected by the distribution schedule. Thus, the present value of a claim would not change were all claims issued upfront, as long as the percentage owned at time t remains $p(t)$. This logic can naturally be extended to a sufficiently large t where p^* is the terminal ownership percentage. Thus, the present value of a claim is unaffected by the shape of the issuance schedule, putting aside security implications and the benefits of a fair initial distribution.

13.2. Impact on the Proposed Monetary System—Earlier sections in this paper described the stability of the monetary system under the assumption that cash and bonds are issued upfront. These arguments still hold for two reasons. First, the supply of cash and bonds is deterministic within any fixed interest rate environment r, ensuring that within that environment, cash and bonds behave as if supply is issued upfront. Second, the terminal ownership percentage p^* is

certain when the interest rate r is small. This reflects a successful steady-state monetary system where cash is nearly risk-free. At the limit where r approaches zero, all cash has been converted to bonds, and p^* is certain because the fully converted supply of bond shares is deterministic and finite.

14. On MEV

It should be noted that there exists the opportunity for miner-extractable-value (MEV) during the block creation process through the ordering of conversions. For example, miners can place their own conversions before and after a user's to maximize slippage and capture a portion of what would otherwise be their remainder, akin to a "sandwich attack" on an automated market maker (AMM). The difference is that unlike AMMs, which exist to facilitate swaps for users, the purpose of a conversion is solely to optimally set the interest rate, and the system is agnostic to how that occurs. Thus, such MEV should not be considered an attack but rather an acceptable source of additional revenue for miners. In the long-run, users that expect to be sandwiched may even choose to designate the miner as the recipient of their remainder to reduce their overall transaction fee.

15. Conclusion

For digital cash to be globally stable, the nominal value of the system must change to reflect changes in its real value. If the only asset is cash, changing the supply of cash is the only way to change the system's nominal value. Introducing a second asset to complement cash is part of the solution, but a system that increases the supply of cash in response to a sudden increase in demand is vulnerable to overexpansion. What's needed is a way for the nominal value of the system to increase without increasing the supply of cash, and vice-versa.

This paper presents a monetary system in which the interest rate, and not the supply of cash, is the primary determinant of the system's nominal value. The interest rate is set by the conversion rate between cash and bonds, and a constant sum-of-squares conversion rule incentivizes market participants to convert between them such that the conversion rate reflects their relative value. In equilibrium, the interest rate equals the real opportunity cost of capital of the system, and if the market is efficient, the value of cash is kept approximately the same. The rules comprising the monetary system are simple and consistent with financial economic theory. No oracle is required, and the system can be readily implemented in a peer-to-peer system, offering a path toward a consistent, credibly-neutral, and globally available unit of economic measurement.

Acknowledgements

I'd like to thank Alana Levin, Yuga Cohler, Alex Evans, Akshay Malhotra, and Oliver Xie for providing helpful comments on this paper.

Notes and References

[1] Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System." (2008) (accessed 17 June 2023) https://bitcoin.org/bitcoin.pdf.

[2] Quote available at https://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

[3] Wood, G., *et al.* "Ethereum: A secure decentralised generalised transaction ledger." *Ethereum project yellow paper* **151.2014** 1–32 (2014).

[4] Specification available at https://domo-2.gitbook.io/brc-20-experiment/.

[5] Ingersoll, J. E. "A contingent-claims valuation of convertible securities." *Journal of Financial Economics* **4.3** 289–321 (1977) doi:https://doi.org/10.1016/0304-405X(77)90004-6 URL https://www.sciencedirect.com/science/article/pii/0304405X77900046.

[6] Modigliani, F., Miller, M. H. "The Cost of Capital, Corporation Finance and the Theory of Investment." *The American Economic Review* **48.3** 261–297 (1958) URL http://www.jstor.org/stable/1809766.

[7] Angeris, G., Kao, H.-T., Chiang, R., Noyes, C., Chitra, T. "An Analysis of Uniswap markets." *Cryptoeconomic Systems* **0.1** https://doi.org/10.21428/58320208.c9738e64.