The Util: A Standard of Deferred Payment for the Bitcoin Economy

Joshua Doman
joshsdoman@gmail.com
theutil.org

Abstract. A monetary system where the price of money is set directly by the market would be less disposed to asset pricing bubbles and monetary inflation. Many see Bitcoin as the basis for this monetary system, but Bitcoin's fixed supply makes BTC a poor standard of deferred payment, as its future purchasing power is inherently uncertain. In this paper, we argue that bitcoin's long-term value in real terms is an algorithmic function of its required real rate of return, which will eventually converge to the global real rate of interest. An estimate for this rate of return could therefore be used to define a new unit of BTC, which reflects a consistent amount of value in real terms. We call this unit of account the "util." We propose a purely peer-to-peer mechanism to continuously estimate Bitcoin's expected real rate of return. The mechanism consists of two convertible assets, Tighten and Ease. Users convert between them according to a constant sum-of-squares invariant, and the relative quantity determines the estimated rate. By pricing Tighten and Ease optimally, the market sets the interest rate in the economy such that the number of "utils" per BTC expands and contracts with long-term demand, making it suitable for transactions where payment is due in the future.

1. Introduction

Economic prosperity depends on sound monetary policy and a good standard of deferred payment. In transactions where payment is due in the future (wages, subscriptions, purchases made on credit, etc.), it is desirable to use a unit of account whose future value is as certain as possible. In the US, this standard is the US dollar, and the responsibility for its stability is given to the Federal Reserve, which manages its value through its control of short-term interest rates.

Unfortunately, central banks often get it wrong, limited by poor data and the human judgment of a handful of experts. This can have disastrous economic consequences. By distorting the true cost of capital, central banks can induce asset pricing bubbles, like the "Everything Bubble" of 2021. This leads to distorted economic activity, and when the bubble inevitably bursts, investors and consumers get hurt.

What is needed is a monetary system where the price of money is set by the market, and not a central bank. With a fixed supply and global liquidity, Bitcoin is the ideal candidate for this monetary system.[1] Bitcoin's fixed supply, however, makes BTC a poor standard of deferred payments, because its future purchasing power will always be uncertain.

In this paper, we focus solely on the eventual steady-state equilibrium, where all 21 million bitcoin have been mined and its aggregate value relative to global wealth is well-established.

What we argue is that in this eventual equilibrium, Bitcoin's value in real terms can be modeled as an algorithmic function of a single variable, its required real rate of return. This reflects the expected return that the marginal investor requires to invest in the asset, given the opportunity set that exists elsewhere in the market. This is likely to converge to the global real rate of interest, in the eventual steady-state equilibrium.

This model likens bitcoin to a risk-free perpetual bond that forever defers payment. Using this model and an estimate of bitcoin's required real rate of return, we can define a unit of BTC that reflects a consistent amount of value in real terms. We call this unit of account the "util."

Estimating bitcoin's required return is not a trivial task, and it is in some ways more art than science. To do so continuously and in a peer-to-peer fashion, we propose a mechanism consisting of two convertible assets, Tighten and Ease. Users freely convert between them according to a constant sum-of-squares conversion rule, akin to the constant product rule used by Uniswap.[2] The relative quantity, which reflects the relative price of Tighten and Ease, determines the estimated rate of return and the number of "utils" per BTC, giving the market a way to continuously set monetary policy.

To manipulate the system, an attacker must acquire a near-majority of the aggregate value of Tighten and Ease. The value of Tighten and Ease depends on the success of the "util" as a standard of deferred payment, so holders are incentivized to set bitcoin's estimated rate of return as close to the expected rate as possible.

Being oracle-free, there are multiple ways to implement this protocol. The optimal implementation is likely a minimal meta-protocol running directly on Bitcoin, like the Runes protocol proposed by Casey Rodarmor.[3] Due to the complexity of implementation, however, it may make sense to initially deploy on Rootstock, an EVM sidechain merged-mined with Bitcoin.[4] Balances can later be forked so that the protocol runs directly on Bitcoin.

2. Why Bitcoin

Bitcoin represents a leap forward in monetary technology. At its simplest, it is a digital asset with a game theoretically finite supply, which is impractical to confiscate and saleable at any point in time anywhere in the world.[5] Lacking cash flows or implicit utility, its aggregate value relative to global wealth is purely a function of human choice.

Is it in the interest of humanity to assign purchasing power to bitcoin? Consider an island with a thriving self-sufficient barter economy. On this island, there are commercial enterprises, which produce many types of goods and services that are valued by the local population. There is an active stock exchange, where individuals can purchase shares in any enterprise on the island, and entrepreneurial individuals create new enterprises on a regular basis. Now, suppose that bitcoin is introduced to the island and given to each individual proportionally to their share of overall wealth. If the islanders assign to bitcoin a fixed percentage of the wealth on the island, no islander is worse off. In fact, the task of saving for future consumption becomes radically easier. Rather than investing in a diversified basket of every asset on the island, an islander need only save in bitcoin, and they will retain their share of the island's overall wealth.

Bitcoin is valued by the market today out of the expectation that this use case will cause it to be valued in the eventual steady-state equilibrium, when all 21 million bitcoin have been mined. If bitcoin in equilibrium represents some fixed percentage of global wealth, its value will be

primarily a function of the global real rate of interest. A good standard of deferred payment could therefore be defined by accurately estimating this rate. In the following sections, we present a model for thinking about bitcoin's value in the steady-state equilibrium.

3. A Primer on the Valuation of Perpetual Bonds

In this paper, we model bitcoin as a risk-free perpetual bond that forever defers payment. For this reason, it is necessary to review how perpetual bonds are valued. Specifically, we consider a perpetual bond that forever returns a constant amount of value in real terms.

Let's define an imaginary currency unit, called the "util," which has precisely the same value in real terms at all points in time. Now, consider a hypothetical risk-free bond, which returns 1 util per year, in perpetuity. How many utils is this bond worth today?

To calculate the present value of each coupon payment, we must discount it by the appropriate discount rate r. This is determined by the rate of return we could receive elsewhere in the market investing at an equivalent level of risk. To obtain the present value of 1 util received t periods in the future, we discount at $1/(1+r)^t$. The present value of our perpetual bond is therefore:

$$\begin{aligned} PV_{bond} &= \frac{1}{1+r} + \frac{1}{(1+r)^2} + \frac{1}{(1+r)^3} + ... \\ &= \frac{1}{r} \end{aligned} \tag{1}$$

4. Valuing a Deferred Perpetual Bond

Now, let's suppose our perpetual bond defers payment for the first period. This means that instead of receiving one util, we receive new bonds of equal value. Since the value of a perpetual bond is $1/r$, we receive r new bonds at $t = 1$. These bonds are expected to be worth 1 util, so this does not change the value of what we hold at $t = 0$:

$$PV_{deferred} = \frac{1}{r} \tag{2}$$

In short, we expect to receive an equivalent amount of value each period, so the value of what we hold today does not change. Let's now suppose that we defer payment until the Nth period. Each period, our bond holdings accrue "interest" at the discount rate r, so we expect to receive the same amount of value each period. Thus, the value of what we hold at $t = 0$ remains $1/r$.

Nothing changes at the limit where N approaches infinity. In the next section, we'll show how this allows us to model the value of bitcoin in terms of the discount rate r.

5. A Valuation Model for Bitcoin

Let's suppose bitcoin's required real rate of return is r. In equilibrium, this is the same as bitcoin's expected real rate of return.

Let's define an intermediate denomination of bitcoin, which we'll call the "e-bond." Initially, there is one e-bond per bitcoin, but every second, the number of e-bonds per bitcoin q grows at bitcoin's required real rate of return $r(t)$:

$$\frac{dq}{dt} = r(t) \tag{3}$$

As a purely illustrative example, suppose 1 bitcoin at $t = 0$ equates to 100 e-bonds and $r = 1\%$ per second. In one second, holding 1 bitcoin equates to holding 101 e-bonds. If r increases, the number of e-bonds per bitcoin grows at a faster rate, and vice versa. This is purely accounting. Holding e-bonds is no different than holding bitcoin. It is simply a different denomination.

The concept of e-bonds is important because it provides a bridge to our perpetual bond. The number of e-bonds per bitcoin grows at the same rate as bitcoin's expected real rate of return, so like a perpetual bond, we expect the value of an e-bond to remain the same in real terms if we do not expect r to change.

The value of an e-bond is not fixed, however. If the value of bitcoin falls, the value of an e-bond will also fall. There is a direct relationship, however, between the value of an e-bond and bitcoin's discount rate r.

E-bonds forever accrue interest at the discount rate r, just like the deferred perpetual bond where the number of deferral periods N approaches infinity. Thus, the present value of 1 e-bond is inversely proportional to bitcoin's discount rate:

$$PV_{e-bond} \propto 1/r \tag{4}$$

Combining (3) and (4), we obtain a deterministic algorithm for the number of e-bonds per bitcoin and the number of utils per e-bond as a function of r and t. We therefore have a model for how the number of utils per bitcoin changes over time, in the steady-state equilibrium.

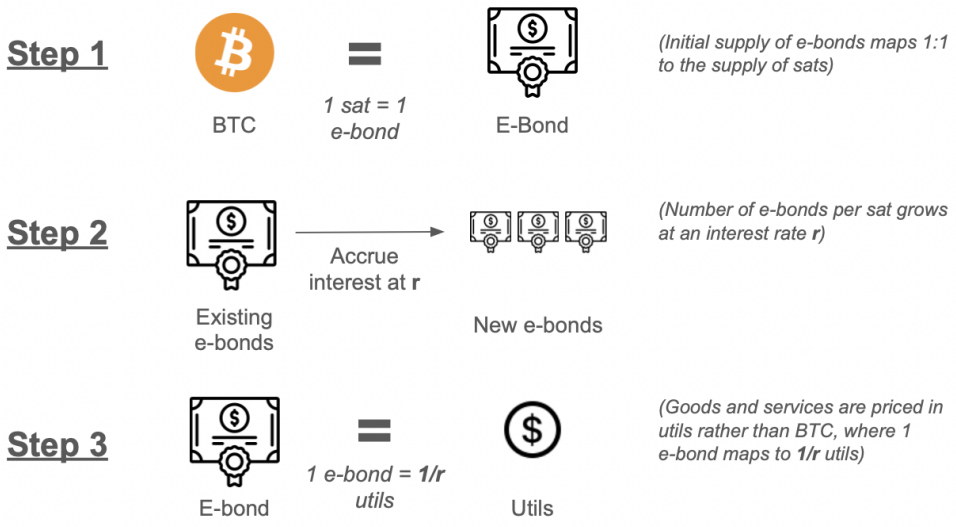


Fig. 1. The relationship between r and the number of "utils" per BTC

Where are we going with this? Provided an accurate estimate of r, we can create a real-life version of the util. First, we define 1 e-bond as 1 sat, the smallest denomination of bitcoin. Next, we compound the number of e-bonds per sat at r. Finally, we define 1 e-bond to be $1/r$ utils. The value of the "util" will then remain approximately the same in real terms at all points in time.

6. A Mechanism to Estimate r

For the "util" to exist, a governance mechanism is needed to determine r. Setting r is more art than science, but the objective should be to achieve price stability in the "util" economy, without introducing trusted third parties. In this section, we propose a mechanism to set r continuously,

controlled via the relative quantity of two convertible assets, Tighten and Ease.

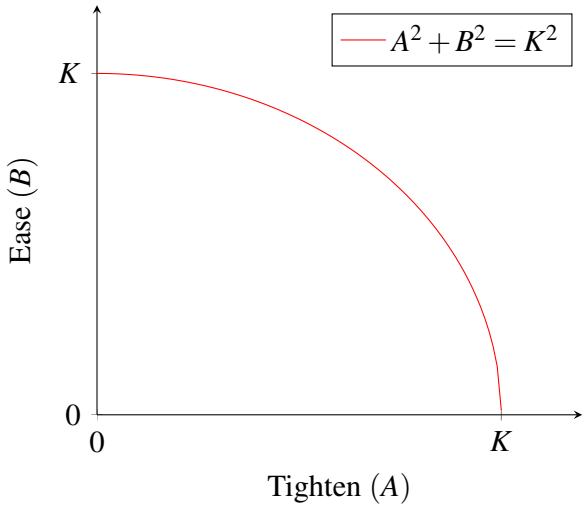
Let A be the outstanding quantity of Tighten, and let B the outstanding quantity of Ease. We define r in terms of A and B, such that $r = 0$ when $A = B$:

$$r = \frac{A - B}{A + B} \tag{5}$$

Users can freely convert between the two assets, according to the invariant:

$$A^2 + B^2 = K^2 \tag{6}$$

where K is some constant. This is akin to the constant product rule used by Uniswap and ensures that the conversion rate moves against the trader as they convert.[6] Visually, conversions occur occur along a quarter-circle with radius K:



As we can see, the conversion rate worsens as Tighten is converted to Ease, and vice versa. The marginal conversion rate from Tighten to Ease at (A, B) is given by the negative slope of the curve, which is A/B:

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

By symmetry, the rate at which Ease can be converted to Tighten is B/A. Assuming no arbitrage or transaction costs, these conversion rates reflect the relative market price of Tighten and Ease. To illustrate, suppose that A/B is not the price of Tighten relative to Ease. Without loss of generality, let's assume the relative price is above A/B. Arbitrageurs can buy Ease, convert to Tighten at B/A, and sell in the market for a profit. Doing so will increase A and decrease B, causing A/B to rise. This will continue until A/B equals the relative market price.

For this reason, it is the relative price of Tighten and Ease that determines the value of r. Converting itself will not change r for very long, since arbitrageurs will reverse the conversion. For an attacker to artificially raise r, they must first acquire the entire supply of Tighten, which

will be a majority of the value of the system. Artificially lowering r is similarly expensive, requiring the attacker to purchase the entire supply of Ease.

Let's calculate the percentage of the value of the system that Ease represents at a given value of r. Let $x = A/B$, the relative price of Tighten to Ease. The percentage p of the value of the system that Ease represents is:

$$\begin{aligned} p &= \frac{B}{B + x \cdot A} \\ &= \frac{1}{1 + x^2} \end{aligned} \tag{7}$$

Using (5), we have $r = (x-1)/(1+x)$, or $x = (1+r)/(1-r)$. Substituting into (7) and simplifying, we obtain:

$$p = \frac{1}{2} - \frac{r}{1 + r^2} \tag{8}$$

Thus, if $r = 5\%$, an attacker must acquire 45% of the value of the system before they can lower the interest rate. If $r = 20\%$, they must acquire 31%, and so forth. In short, the system is secure as long as $1 - p(r)$ of the value of the system is held by "honest" actors, where r is the required real rate of return.

7. The Full Protocol

We need to make a few adjustments if we want to use this protocol in practice. First, we cannot allow r to be less than zero, since the discount rate of a perpetual bond is strictly positive. We therefore define r as:

$$r = \begin{cases} \frac{A-B}{A+B} & \text{if } A > B \\ 0 & \text{if } A \leq B \end{cases} \tag{9}$$

This value of r determines the rate at which the number of e-bonds per bitcoin grows, which is updated with every conversion. In contrast, the number of utils per e-bond $(1/r)$ is updated using the time-weighted average r over the previous 8 hours. If zero, the last well-defined value of r is used. This delay prevents manipulation and gives traders time to execute arbitrage.

Finally, the supply of Tighten and Ease is issued steadily over time, rather than all at once, to provide a fair initial distribution. Issuance occurs through 30-minute auctions, where the reward R is split between $A \cdot R/K$ Tighten and $B \cdot R/K$ Ease, starting at $R = 150$ and halving every 70,000 auctions. This prevents r from changing due to issuance and ensures that K, the maximum quantity of Tighten and Ease, never exceeds 21 million. Auction proceeds are sent to the miner of the block in which the auction is settled.

This protocol is straightforward to implement as a smart contract on an EVM sidechain like Rootstock, but the optimal long-term implementation is likely a meta-protocol running directly on Bitcoin. Implementing such a meta-protocol requires additional considerations, however, given Bitcoin's UTXO structure and 10-minute blocktimes. A full specification is beyond the scope of this paper but is intended in a future document.

8. A Macroeconomic Thought Model

To ground our understanding, consider an economy denominated in ”utils” where a new technology is introduced and the economy experiences a positive supply shock.

(1) With a positive supply shock, the investable opportunity set grows more attractive relative to bitcoin, causing the required rate of return to rise and demand for bitcoin to fall.
(2) With a higher required rate of return, Ease are converted to Tighten, and r rises.
(3) This causes the number of ”utils” per bitcoin to fall but grow 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 bitcoin's required rate of return to fall and demand to rise.
(5) With a lower required rate of return, Tighten are converted to Ease, and r falls.
(6) This causes the number of ”utils” per bitcoin to rise but grow at a slower rate, reflecting an economy with slower growth and more demand for risk-free assets.

9. Conclusion

For Bitcoin to be competitive as money, it needs a standard of deferred payment, which reflects a consistent amount of purchasing power in real terms. This requires an interest rate and a protocol to set monetary policy. While fiat monetary policy is set by a committee, ”util” monetary policy is set by the market. Anyone can influence monetary policy by buying or selling Tighten and Ease, democratizing a process that is opaque and somewhat arbitrary today.

The ”util” is an effective standard of deferred payment in the eventual steady-state equilibrium, where bitcoin's aggregate value reflects a consistent share of global wealth and the required return matches the global real rate of interest. The bitcoin market, however, likely remains decades away from this equilibrium. While the ”util” may prove useful as a way to denominate cross-border transactions, where payment is due years in the future, it will take time before it can substitute a fiat currency like USD as a way to denominate everyday transactions. What is exciting is the opportunity to define a globally consistent measure of bitcoin's economic value. This could facilitate global trade, ease the business cycle, and accelerate the adoption of Bitcoin as the global monetary standard.

Acknowledgments

Thank you to Yuga Cohler, Alana Levin, Patrick Lung, Akshay Malhotra, and others for helpful discussions during the development of 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] Adams, H., Zinsmeister, N., Robinson, D. H. "Uniswap v2 Core." (2020) URL https://uniswap.org/whitepaper.pdf.

[3] https://rodarmor.com/blog/runes/.

[4] https://www.the-blockchain.com/docs/Rootstock-WhitePaper-Overview.pdf.

[5] https://casebitcoin.com/docs/StoneRidge_2020_Shareholder_Letter.pdf.

[6] 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.