zBTC: A Stable Reserve Currency Backed by Bitcoin

Foundation Crypto Labs
https://github.com/FoundationCryptoLabs

Abstract: We set out to create a bitcoin-backed reserve currency that is both highly stable and highly inflation resistant. This is in contrast with bitcoin, which is highly inflation resistant but also volatile; and USD, which is stable in the short term, but loses purchasing power in the medium to long term. All else being equal, the factors that make something a good store of value also make something a good unit of account. Per contra, an asset that doesn't store value well (in the short, medium, or long term) does not serve as an effective unit of account for those specific time-frames. To solve this, we utilise a scarce collateral (BTC) to algorithmically back stable zBTC and make it redeemable for a stable yet appreciating value at all given times. zBTC (EVI DAO) is a capital-efficient stablecoin system with a redemption price that shows little downward volatility but significant upward volatility. zBTC is deployed on RootStock, and thus matches the security of the Bitcoin network itself without any further assumptions.

1.0 Introduction - Stablecoin Design

Popular digital assets such as Bitcoin (BTC) and Ether (ETH) are too volatile to be used as everyday currency. The value of a bitcoin often experiences large fluctuations, rising or falling by as much as 25% in a single day and occasionally rising over 300% in a month. Stablecoins represent a new era of possibilities in terms of financial engineering, as collateral-backed assets can be designed to algorithmically adjust redemption rates based on novel models.

Two existing collateralised stablecoin models are MCD (DAI) and FLX (RAI). DAI utilises a *fixed USD peg* - which by definition is stable in USD terms only. Stablecoins like DAI suffer from loss of purchasing power, when they are diluted alongside USD by fiscal measures which cause USD inflation. There is no in-built mechanism to change the peg to account for inflation - meaning that DAI is innately dependent on USDs stability in global markets.

In contrast, RAI utilises a *floating peg* system, which allows its redemption price to change in USD terms, as dictated by market forces.

This allows RAI to be potentially inflation resistant. An advantage of RAI is that it uses only decentralised collateral, namely ETH. However, RAI does not have any explicit mechanism forcing/incentivising any change in the redemption price; such change is merely permitted and implicit in the protocol. In practice, this has brought RAI closer to behaving like a USD pegged stable coin rather than an inflation resistant asset, as its redemption price has remained virtually constant since launch.[1]

We approach this problem by designing an *explicit peg* to an algorithmic measure of stable/appreciating purchasing power, instead of pegging directly to USD (loses purchasing power), or a scarce asset like BTC (too volatile). An explicit and autonomous redemption price adjustment mechanism, offers a practical way for ensuring mid-and-long term value appreciation of the asset. However such a mechanism must be chosen carefully, to avoid collateral insufficiency issues.[2]

2.0 Monetary Assets

The analysis of the behaviour of price action of different monetary commodities (like gold, btc, and EUR), as it relates to supply and demand shocks, shows us some clear trade-offs that are at play in monetary asset selection/design.

On the one hand, assets with fixed supply (like land) or (physically) limited supply growth (btc, gold) show great resistance to mid-to-long term inflation of other monetary assets like fiat currency. On the other hand, the very inflexibility of supply that makes them good long term holders of value, makes them bad at absorbing short-term demand and supply shocks.

The classic example is bitcoin halving. As demand either remains constant or increases, while supply drops suddenly every 4 years, a dramatic shift is produced in the demand-supply equation, with a lot of ensuing volatility. Typically, the value eventually settles at a higher place

---

[1] RAI founders also admit that without explicit mechanisms to adjust redemption price, it is perhaps likely that RAI will also behave like a pegged coin, similar to DAI.

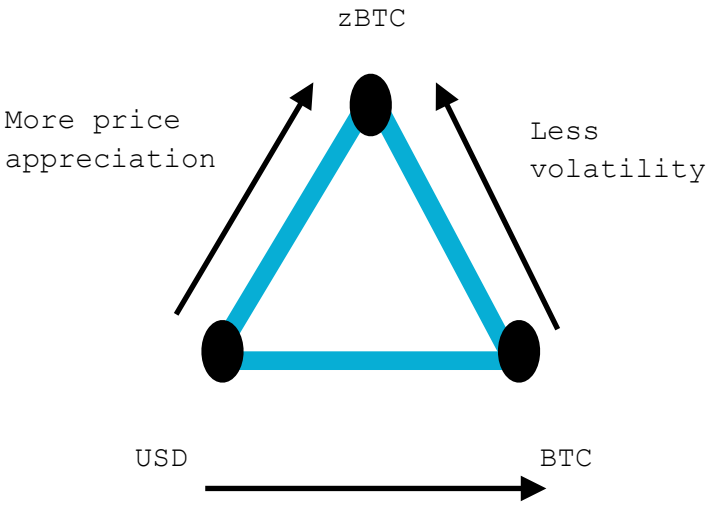
[2] In theory, you could define a coin with a USD redemption price that rises say 200% every year. However, practically speaking, such a model would very quickly run into collateral sufficiency issues, barring major bull runs in the associated collateral.
We discuss this tradeoff further in Appendix-B, by backtesting various redemption rate models for volatility and collateral sufficiency.

than pre-halving, however this is achieved only after a series of rises and 'dips', characteristic of free market price-discovery of a scarce asset. Arguably, this series of supply shocks may diminish between 2028 -2040 as available supply from mining drops below that available from other sources. However even if that happens, bitcoin will still potentially be subject to short term demand-shocks, with sudden buying or selling affecting the price as the supply cannot change to accommodate the extra/reduced demand, so it must be reflected in the price.

Designing an ideal "stable" asset thus requires supply flexibility to cope with short-term flux in demand, while maintaining steady purchasing power in the short, medium, and long term.

It is hard to have commercial certainty when BTC price has ranged from $20K to $66K in the same year, and when downward volatility of >20% is considered commonplace. On the other hand, if the short term volatility of bitcoin was somehow tempered, and instead only the slower, more certain price appreciation captured, that would make it an excellent Store of value across time frames, and thus a great unit of account.

USD currently represents good very-short-term stability, and reasonable medium term stability, but poor long term stability in purchasing power. You can be almost certain that you can buy the same bread for the same USD price tomorrow, but the certainty reduces (mostly towards loss of value) the longer you wait. Estimates of annual inflation range from 6% overall to over 12% in metros bear out that USD is not a good store-of-purchasing-power in the mid-to-long term.
The Volatility-Appreciation trade off looks something like this:



3.0 Analysis of Redemption Rate Models

3.1 Goals

The main goals of the zBTC Stablecoin system are optimising for a stable store of value across time-frames, plus offering users stable USD appreciation. Essentially, for such a stable/reserve currency model to be successful, the following are required, or desirable -

1. Low Downward volatility - first and foremost, for people to hold a "stable" asset, they expect that they will not incur a significant (permanent or impermanent) loss when they choose to liquidate the asset.*

   *"Significant loss" can be defined as anything from -0.05% to -5% in USD terms. However, even assets stable in fiat-denominated market price, like USDC or DAI, can and do suffer from loss of purchasing power, when they are diluted alongside USD by fiscal measures. This problem takes us to Point number 2-
2. Inflation Resistance - While downward volatility is the anathema of a stable coin, a certain amount of upward-only volatility is desirable (as measured in fiat denominated terms), such that the purchasing power of the stable coin either remains the same or rises with time.
3. Collateral Efficiency - Collateral Sufficiency refers to the relationship between the stable asset's redemption price; and the amount of collateral available to redeem it. Collateral ratios range from 150% to 300% for more volatile collateral like BTC and ETH; the goal being that sufficient collateral must exist even during periods of downwards volatility to allow the stables to continue being redeemed at the redemption price. This ensures that their stability is not affected. Alternatively, the goal is that a sufficient buffer should exist such that the collateral can be liquidated in periods of downward volatility well before it crashes below the value required to redeem all outstanding stable asset coins.
4. Price Appreciation - All the above being equal, users will favour the asset that shows the maximum increase in purchasing power, over the medium-to-long term. Assuming equal safety from downward volatility, the asset that shows the most price appreciation is the best.

3.2 SMA1458

After backtesting a number of models, we found that the 4-year Simple Moving Average (SMA4 - green in fig. 1) represents an excellent tradeoff of the 3 goals described above. It illustrates a capital-efficient way to redeem a stable coin at a value that shows little downward volatility but significant upward appreciation in the medium to long term. You can see Appendix-B for an outline of possible redemption rate models studied, and why we settled upon the SMA4 of the BTC/USD exchange rate as the ideal redemption rate model.

Fig 1: BTC/USD exchange rate and SMA1458 over time - log scale.

4.0 zBTC Stablecoin System (XSS)

EVI DAO is a protocol on Rootstock that backs and stabilises the value of zBTC through a dynamic system of Collateralized Debt Positions (CDPs), algorithmic redemption rate adjustments, and autonomous feedback mechanisms. EVI enables anyone to leverage their Bitcoin assets to generate stable zBTC on the EVI Platform.

4.1 Redemption rate

zBTC is a stable version of BTC. Each zBTC is *backed* by at least one full BTC, however it is only redeemable for a part of a BTC based on the current redemption rate. The redemption rate is based on the 1458-day Simple Moving Average of the BTC/USD exchange rate, computed as follows:

$$\text{SMA1458} = \sum_{i=1day}^{1458} /1458$$

$$\Rightarrow SMA = (day1 + day2 + \ldots + day1458)/1458$$

Where:
t= Date of calculation
i=1 => t-1 days BTC/USD exchange rate (day1)
i=2 => t-2 days BTC/USD exchange rate (day2)
…
i=1458 => t-1458 days' BTC/USD exchange rate (day1458)

The SMA1458 redemption rate is dynamically updated every 24 hours, based on the new sliding window for calculation.

zBTC can be understood as a slower, up-only version of BTC. Instead of significantly fluctuating like BTC, it aims to maintain a stable exchange rate that rises slowly with time, as bitcoin gets more valuable after each halving. If BTC price were to stabilise someday, zBTC price would eventually stabilise at a similar value - however the zBTC would be more immune to demand/supply shocks affecting BTC price, even in such a scenario.

We rely on the BTC-USD oracle for all our calculations. While the redemption rate at any point is calculated in USD terms, the redemption itself happens in BTC. Similar to Reflexer protocol, we follow the principle of governance minimisation, and focus on making important protocol decisions via algorithms rather than people wherever possible.

Notably, zBTC collateral requirements are denominated in BTC instead of USD - eliminating the need for automatic liquidations, while maintaining collateral sufficiency using a probabilistic model. This leads to higher

incentives to deposit collateral and mint zBTC, as there is no risk of collateral being liquidated.

4.2 The CDP interaction process

The zBTC system lets you open Collateralized Debt Positions (CDPs) using Bitcoin[3] as collateral, at the current collateralization ratio. CDPs hold collateral assets deposited by a user and permit this user to generate zBTC, but generating also accrues debt. This debt effectively locks the deposited collateral assets inside the CDP until it is later covered by paying back an equivalent amount of zBTC, at which point the owner can again withdraw their collateral. Active CDPs are collateralized in excess, meaning that the value of the collateral is higher than the redemption rate of the debt. This ensures that the stable assets (zBTC) can be redeemed for BTC at the prevailing stated redemption price at all times.

- Step 1: Depositing collateral

The CDP user sends a transaction to deposit collateral for minting zBTC. At this point the CDP is considered collateralized.

- Step 2: Generating zBTC from the collateralized CDP

The CDP user then sends a transaction to mint the amount of zBTC they want from the CDP, and in return the CDP accrues an equivalent amount of debt, locking them out of access to the collateral until the outstanding debt is paid.

- Step 3: Paying down the debt and zBTC Savings Rate.

When the user wants to retrieve their collateral, they have to pay down the debt in the CDP, plus the Stability fee that continuously accrue on the debt over time. Once the user sends the requisite zBTC to the CDP, paying down the debt and Stability Fee, the CDP becomes debt free.

- Step 4: Withdrawing collateral

With the Debt and Stability Fee paid down, the CDP user can freely retrieve all or some of their collateral back to their wallet by sending a transaction to EVI.

5.0 EVI DAO Governance Model

EVI DAO token holders will control the key system variable, XSR savings rate, as an added mechanism to maintain zBTC stability. EVI DAO earns a

[3] RBTC or Rootstock native Bitcoin is the actual collateral used for creating CDPs. RBTC is 1:1 pegged to BTC.

portion of the XSR savings rate paid by borrowers. Thus the incentives of EVI token holders aligns with that of zBTC protocol - that is to maximise usage (and resulting XSR revenue) by ensuring stability around the peg.

5.1 zBTC savings rate (XSR)

zBTC savings rate is controlled by governance, as an additional means of securing the peg besides the redemption rate. If zBTC starts trading above the redemption rate, the XSR can be increased to incentivise more BTC to be locked up, which causes the zBTC supply to inflate, eventually bringing down the price to the redemption rate. The XSR fixed by Governance can be set higher than in liquidation based protocols like MCD or FLX, as the risk of liquidation is now eliminated - increasing long term protocol revenues and reserves.

5.2 Price Stability

The redemption rate serves as the floor of the trading price for zBTC. To prevent upward volatility and speculation beyond the redemption rate, the following mechanisms are in place:

First, Arbitrageurs expecting the price to drop down to the redemption rate, can exploit the difference in price by borrowing more zBTC when the market price is above the redemption rate, and returning the debt when the market price drops to the redemption rate. In this way they will expand zBTC supply and quickly drop the price to the redemption rate.

Second, in case of sustained market prices above the redemption rate, EVI Token holders may vote to reduce the zBTC savings rate, making it cheaper to borrow zBTC and consequently expanding the supply. Notably, in many cases, just the anticipation of such an action may be sufficient to motivate arbitrageurs to bring down the price as described above.

Conversely, if the zBTC token is trading at or close to the redemption rate for sustained periods, EVI holders may vote to slowly increase XSR to maximise system revenue as well as provide a cushion for future rate drops in case of upwards volatility. The function of EVI DAO in this way mirrors that of a central bank.

5.3 Relationship with Bitcoin

zBTC is a derivative product of BTC. As such, both will have a highly symbiotic relationship. zBTC offers a stable way for millions of investors to hold BTC in the medium or short run, absent the extreme volatility that has so far kept a large proportion of users from full adoption. As demand for zBTC rises, so will the demand for BTC to lock up more collateral and mint more zBTC. Conversely, rise in price of BTC will slowly translate to increasing demand for zBTC due to stable increase in value, completing the adoption loop.

6.0 Conclusion

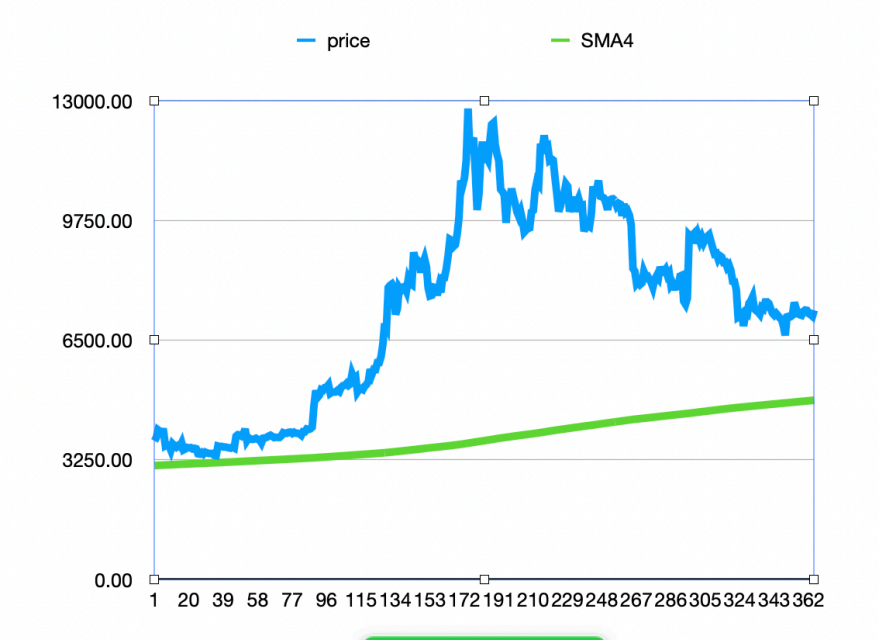
We present the first stablecoin system with a dynamic redemption price model, the zBTC Stablecoin System. We propose using the 1458-day simple moving price of BTC/USD exchange rate as the dynamic redemption price, due to its historical stability. This is aimed at solving the twin problems of inflation of current stable assets (USDC, DAI, RAI), as well as high volatility in appreciating assets (BTC). zBTC protocol is governed by the EVI DAO, which sets the XSR savings rate as a further mechanism to stabilise price and earn protocol revenue.

APPENDIX A - Example Scenarios

This section demonstrates how zBTC will react in the following possible scenarios in terms of retaining stability and purchasing power.

1. USD Inflation, Volatile BTC appreciation

A good test case for this is the year 2019; where USD experienced approximately 6% inflation, and BTC appreciated about 100% with volatility throughout. As seen below, zBTC posts a smaller net gain of about 50%, without any volatility whatsoever.



2. BTC Crash

A good test case for this is the year 2018; where BTC had a sustained crash of about 50% with volatility throughout. As observed, the redemption rate of zBTC continues a slow but steady rise, without becoming under-collateralized at any point.

APPENDIX B: Analysis of Redemption Rate Models

Bitcoin's 13 year history provides rich data for calculating how various redemption rate algorithms would fare if they were collateralised by BTC. In short, it becomes clear that the algorithmic redemption price model must be dynamically linked to the current as well as historical BTC-USD exchange rate.

Other models independent of the exchange rate, such as static price appreciation models have numerous drawbacks. *First*, static price increase rate models do not dynamically adjust to changing inflation levels, and are likely to be left behind by runaway inflation. *Second,* small static price increases (eg. increase redemption price by 5-10% in USD terms annually) tend to under-utilise the full growth of the collateral asset, especially during bull runs. *Third*, larger static price increases (eg. increase redemption price by 20-50% in USD terms annually) is bound to run into collateral sufficiency issues, especially during bear runs.

Therefore for optimal use of the collateral asset's appreciation, whilst minimising collateral risk in depreciating conditions, requires linking the redemption price directly to the current and historic exchange rates. The Simple Moving Average (SMA) is one such effective measure that represents the long term trends of BTC/USD price with dampened volatility. The effective historical redemption rates for 3 different SMA models is shown below.

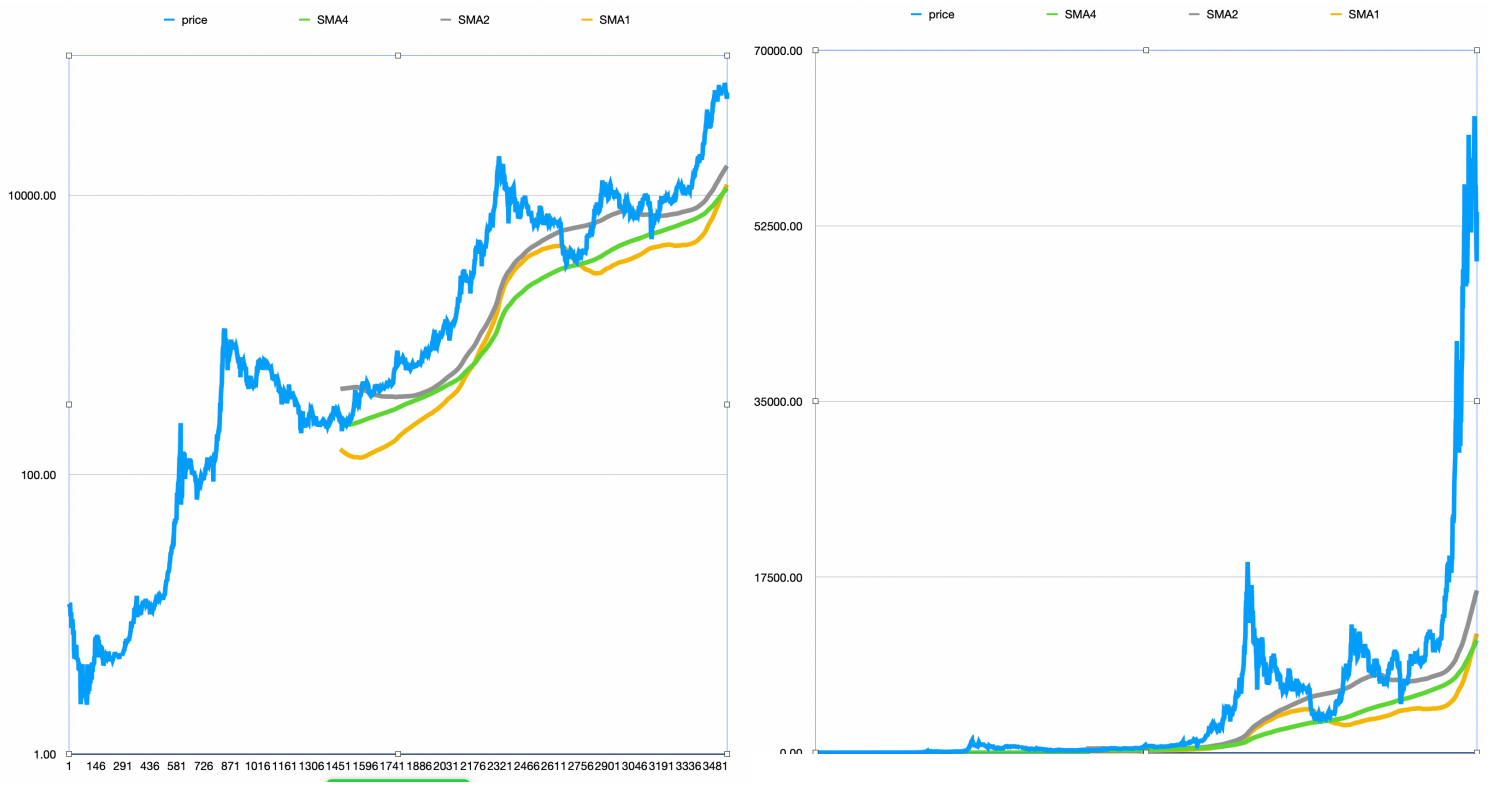


Fig. 3: Possible Redemption Rate Models.(Left)-Log Scale; (Right)- linear scale.

In Fig(1), note that whenever the redemption price (gray, green, yellow) crosses the exchange rate (blue), the coin would run into collateral sufficiency issues, as the redemption price for 1 zBTC becomes greater than the collateral (1 btc). In this fashion, the SMA1 and SMA2 run into collateral sufficiency issues; moreover SMA2 in particular shows significant downwards volatility, making it unsuitable for use as a stable coin redemption rate.[4]

After backtesting a number of models, we found that the 4-year Simple Moving Average (SMA4 - green in fig. 1) represents an excellent tradeoff of the 3 goals described above. It illustrates a capital-efficient way to redeem a stable coin at a value that shows little downward volatility but significant upward appreciation in the medium to long term. This is for two reasons:

[4] Dataset and a python codebase to replicate figure-1 is provided in the FoundationCryptoLabs/Redemption-Modelling Repo. For an interactive graph visit: https://stats.buybitcoinworldwide.com/sma1458/

1. Historically, spot/nominal BTC has never dropped significantly under the SMA4. This ensures collateral sufficiency, in that 1 zBTC can always be redeemed at the stated redemption rate, as long as it is collateralised by at least 1 BTC - and as long as the price stays within these very broad, historically tested parameters. Further, the fact that BTC price is almost always above the SMA4, means that the SMA4 displays upwards-only volatility, perfect for inflation resistance.
2. Subject to (1), the SMA4 also displays strong price appreciation, compared to any other stable redemption rate. Therefore, it is a prime candidate for a stable yet appreciating asset.

The redemption rate can be thought of as the slowly rising floor of BTC prices. While we cannot predict the exact volatility of BTC/USD exchange rate, it is possible to predict, with a high degree of probabilistic certainty, a minimum price below which BTC is exceedingly unlikely to drop.