An Empirical Analysis on Algorithmic Stablecoins

Mark Zhang
UC Berkeley
Berkeley, CA
ziyaoz@berkeley.edu

Kunaal Sundara
UC Berkeley
Berkeley, CA
kunaalsundara@berkeley.edu

Danny Halawi
UC Berkeley
Berkeley, CA
dhalawi@berkeley.edu

Yizhuo Miao
UC Berkeley
Berkeley, CA
miaoyizhuo@berkeley.edu

Yingge Yan
UC Berkeley
Berkeley, CA
yingge_yan@berkeley.edu

ABSTRACT

We propose a system and threat model for algorithmic stablecoins and apply it to various coins to analyze their stability and security. We also create a novel volatility metric to help us compare different algorithmic stablecoins. Finally, we compare various stablecoins in terms of their market cap, volume, holder statistics, and volatility.

1 INTRODUCTION AND PROBLEM DEFINITION

A stablecoin is a cryptocurrency with a fixed price. In order to build up a modern decentralized finance system on the blockchain, there needs to be a stable medium of exchange, a truly stable currency. Traditional stable coins (e.g. USDT, USDC) claim to use fiat currencies as collateral and are minted by a central party mostly at will. As a result, they can create systematic risk for the entire defi ecosystem in case one of these stablecoin issuers fail. On the other hand, algorithmic stable coins react to market events stipulated in code to maintain their peg, offering better transparency and are more decentralized. However, depegged algorithmic stable coins are very common. Therefore, we seek to answer the question of how existing algorithmic stable coins compare with each other and whether we could have a truly stable algorithmic stable coin that's free from the risks of depegging.

In this paper, we focus on algorithmic stable coins pegged to USD, though our analysis could be easily extended to stable coins pegged to another fiat currency or cryptocurrency. The list stable coins we are analyzing include: AmpleForth, Basis Cash, and Terra (with FRAX in the appendix).

2 RELATED WORKS

In [14], the authors examine stablecoins to answer the question of whether algorithmic stablecoins are volatile by design and in practice. The paper introduces a modeling framework that allows for a complete representation of a stablecoin by a network of timed automata consisting of the protocol, expansion, contraction, seller, buyer, and DEX. Each timed automata has a set of states and actions which describe how the stablecoin adjusts due to its price. The network also communicates through channels which trigger state transitions such as expansion and contraction. In order to verify the stability of a stablecoin, Zhao et al. check the "expansion-validity" and "contraction-validity" of the model. Essentially, the model must ensure that when a stablecoin's expansion is enforced, the DEX should not stay in a state where the stablecoin would be bought and vice-versa for contraction-validity. Through this modeling and verification process, the authors find that Basis cash violates expansion and contraction validity under two circumstances which were then observed on the blockchain and caused the price of Basis Cash to deviate far from the peg. We have attempted to use a similar approach to model stablecoines other than Basis Cash. However, we had limit success applying the timed-automata abstraction as a generalised framework to other stablecoin algorithms, so we demonstrate another approach in this particular paper.

In [10], Klages-Mundt et al. proposes that a non-custodial stablecoin system may have the following components: primary value, risk absorbers, stablecoin holders, issuance, governance, data feed, and miners. We will follow this general model but develop it further in our analysis (see section 3). Another useful observation in the paper is that "at some level, confidence in something seems unavoidable as a source of value in a monetary system." We agree with this conclusion, and thus plan to only describe the primary value of an algorithmic stablecoin in a qualitative manner while focusing our modeling efforts on issuance/deleveraging, risk absorbers, and stablecoin holders.

In [13], Robert Sams proposes that the purchasing power of a coin P is a function of coin demand CD and the quantity of coin supply Q.

$$P = \frac{CD}{Q} \tag{1}$$

This is the foundational assumption we make in our analysis of algorithmic stablecoins - by changing the quantity of the supply of stablecoins according to this formula, stablecoins can meet the fluctuating coin demand while maintaining a stable price. However, this is not a new concept. The quantity theory of money is a classic economic theory dating back to Nicolaus Copernicus [12]. Due to time and space constraints we will not dive deep into justifying this theory, though we do acknowledge that more sophisticated monetary models could improve our analysis in future work.

3 APPROACH

3.1 Volatility Metric

Volatility is traditionally a metric which is used to measure the variation in the price of an asset over time. To analyze just how 'stable' existing stablecoins are, we developed a new volatility measurement for stablecoins and employed it on the historical price data for several stablecoins.

First, we attempted to use standard deviation from the stablecoin's peg as a naive volatility measure. However, we found that it resulted in numbers that were not meaningful when trying to assess stablecoins. We concluded that this naive measurement was inadequate due to two reasons. 1. Assets are not assigned a fixed price value and normal standard deviation calculations account for this by taking deviations from the mean value. 2. It weights values above and below the peg equally so it is skewed towards values greater than the peg (Ex. if a stablecoin pegged to $1 has a price close to 0, the deviation would be close to 1, but if the price was 10, the deviation would be 9). To remedy these issues, we created a new volatility calculation similar to our first approach, but for the deviations in the calculation, we now map prices greater than the peg : $[peg, \inf) \rightarrow [0, peg)$ and use the same deviations for prices below the peg.

Letting P be the stablecoin's peg, X_i, the price a given point, D_i be the deviation of the price after mapping, and N be the number of data points, we calculate V, the volatility, as follows:

$$D_i = \begin{cases} \frac{P(X_i - P)}{X_i} & X_i > P \\ P - X_i & X_i \leq P \end{cases} \tag{2}$$

$$V = \sqrt{\frac{\sum_{i=1}^{N} D_i^2}{N}} \tag{3}$$

Under this metric, a volatility close to 0 indicates that the coin is stable and remains close to its peg, while a volatility closer to 1 indicates that the coin is highly unstable and likely depegged. Lifetime volatility calculations for several stablecoins using the above metric are listed in Table 1. The highlighted rows indicate depegged stablecoins which we can see have much a higher volatility than the other stablecoins.

Table 1: Lifetime Volatility of Stablecoins

Stablecoin	Volatility
AMPL	0.26509
BAC	0.77613
FEI	0.06144
FRAX	0.00690
DSD	0.88080
DAI	0.01096
ESD	0.76482
RSV	0.02256
UST	0.00778

All values calculated using daily price data from CoinGecko as of Dec 12, 2021 [4]

3.2 System Model

First and foremost, we use the relationship (1) proposed by Sams [13] to simulate how prices move based on changes in the quantity of coin supply. In our analysis, we equate purchasing power P with the price of a coin in US dollars, since the purchasing power of USD remains relatively constant in at least the short to medium term, and because most of the stablecoins we investigate are pegged to the US dollar.

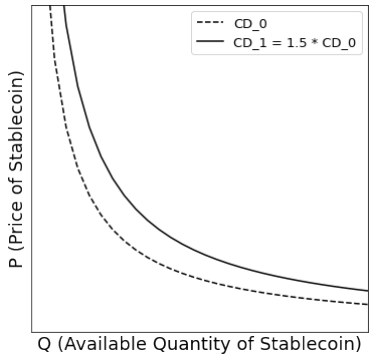


Figure 1: Shifting Coin Demand Causes Price Change

For example, as shown in Figure 1, when coin demand goes up, either P, Q, or both P and Q has to go up. An example used in Sams' paper is Bitcoin[13]. Since Bitcoin's Q is held constant, its price P will have to go up when coin demand goes up either due to economic growth or increased speculation interest. However, a stablecoin should be able to adjust its supply quantity Q so that price remains constant.

We can then incorporate this relationship into the stablecoin model proposed by [10]. Furthermore, we divide their

model into two parts: system model and threat model. The system model includes the most important factors that determine the stability of an algorithmic stablecoin, whereas the threat model determines whether a given implementation of a stablecoin will be successful given a sound system model. Our system model is thus the following:

(1) **Primary value**: how does the stablecoin justify its worth. This factor directly affects coin demand. When the primary value is regarded by the market as tangible and stable, bank-runs would rarely happen, and CD remains relatively stable as well. However, if the primary value of a stablecoin has too many unknowns for the market to value it efficiently, CD may change very rapidly following changes in market sentiment, creating challenges for the issuance and deleveraging mechanism of the stablecoin. Primary value can also affect how easy the deleveraging process is through the existence, non-existence, and types of collateral of a given stablecoin. For example, if a stablecoin's primary value is derived from its easily redeemable USD collateral, then the process of deleveraging would be very straightforward: people trade their stablecoins for USD, and Q is decreased. However, as we explore later in this paper, if a stablecoin's primary value is derived from a less tangible source, it is harder to align the incentives in a deleveraging.
(2) **Issuance**: When CD goes up, how to increase Q. The stablecoin can choose the evenly split the newly minted coins to all stablecoin holders (e.g. AmpleForth), or it can prioritize a particular group (e.g. bond holders) over others (e.g. Basis Cash).
(3) **Deleveraging**: When CD goes down, how to decrease Q. Deleveraging means "the act or process of paying off or reducing debt [5]." Here, the subject of deleveraging is the entity that issues the algorithmic stablecoins. This could be a real person, a company (e.g. Coinbase for USDC, Tether for USDT), or a smart contract (for the majority of algorithmic stablecoins). In the event that CD goes down, that entity would need to reduce the supply Q of the stablecoin by reducing its debt (issued stablecoins) in exchange to selling some other asset.
(4) **Risk Absorbers**: Who are they, and how are they incentivized?

3.3 Threat Model

We categorize the following components as security characteristics of a stablecoin that are critical but not essential for whether a stablecoin is stable.

(1) Governance
(2) Data Feed
(3) Consensus Layer Security (miners)

All of those three factors are critical to an algorithmic stablecoin's success and are by no means easy to get right individually, let alone all at the same time. However, we argue that by considering all those three components in our threat model in their ideal form we could simplify our initial analysis while still producing useful results. We will later proceed to consider all six factors and what their interactions imply on a given algorithmic stablecoin's stability.

4 STABLECOIN SYSTEM MODELS

4.1 AmpleForth

AmpleForth is a so-called rebase token, meaning that its supply changes directly by reducing or increasing the amount of tokens held by all accounts proportionally. It is worth noting that AmpleForth is not pegged to the current dollar, but instead to the to the 2019 US dollar based on reports from a CPI (consumer index) oracle. [8]

4.1.1 Primary Value. AmpleForth does not have any collateral, so its primary value is mostly derived in its utility, which is providing a decentralized, stable unit of denomination for smart contracts.

4.1.2 Constants [8]. The following parameters are constants in the issuance and deleveraging algorithms:

(1) `deviation_threshold`: only adjust supply if the price of AMPL deviates from its target by > the `deviation_threshold`. It's currently set to 5%.
(2) `reaction_lag`: If the price of AMPL is x% above the target, the policy adjusts supply by $\frac{x}{\texttt{reaction\_lag}}$ %. It's currently set to 10.

4.1.3 Issuance [8].

```
if (oracle_price > cpi_oracle_price +
    ↪ deviation_threshold)
       all_wallets *= 1 + (deviation/
           ↪ reaction_lag)
```

4.1.4 Deleveraging [8].

```
if (oracle_price < cpi_oracle_price -
    ↪ deviation_threshold)
       all_wallets *= 1 - (deviation/
           ↪ reaction_lag)
```

4.1.5 Risk Absorbers. The AMPL holders are also risk absorbers. Because AmpleForth directly changes the amount of coins held in all wallets based on the current price, the stablecoin holders are risk absorbers.

4.1.6 Simulations and Analysis. Here, we model the how the AmpleForth algorithm adjusts the coin supply in response to a change in coin demand CD. In Figure 2, we show the deleveraging process for AMPL, and in Figure 7, we show its issuance process. We demonstrate that assuming CD doesn't change after the initial adjustment, the AmpleForth algorithm is able to move P back to 1$ by gradually adjusting Q.

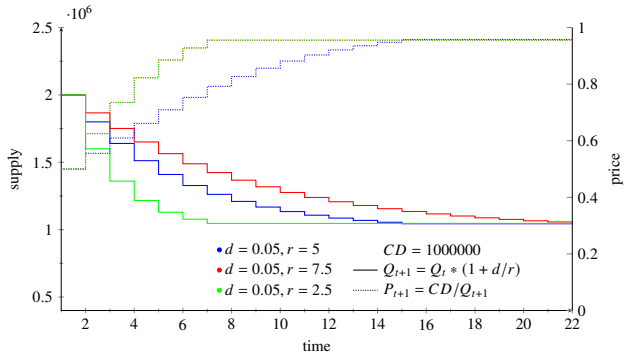


Figure 2: AmpleForth Deleveraging Simulation

4.2 Basis Cash

Basis Cash uses a similar mechanism to the seigniorage shares described by [13] to incentives risk-taking. When the price of basis cash falls, basis bonds are issued at a discount to speculators, who can then redeem their bonds when the price of basis cash rise back up.

4.2.1 Primary Value. Like AmpleForth, Basis Cash does not require any collatoral. While AmpleForth aims to provide a decentralized and stable unit of denomination for smart contracts, basis cash aims to be a more general purpose stablecoin that can be both used in smart contracts and fulfill other functions of money, such as a store of value. However, basis cash is currently depegged and trading at $0.03 [2].

4.2.2 Constants.

(1) `deviation_threshold`: The threshold that triggers either issuance or deleveraging. It's currently set to 5%.

4.2.3 Issuance [3].

```
if (oracle_price > (1 + deviation_threshold) DAI
    ↪ )
    amount = deviation * total_supply
        if (treasury_balance > 1,000)
            mint(boardroom, amount)
        else
            mint(treasury, amount)
```

Here, the treasury and the boardroom are both smart contracts. Coins stored in the treasury can be redeemed by basis bond holders with a 1:1 ratio if `oracle_price` is above 1 DAI, whereas coins stored in the boardroom are evenly distributed to all basis share holders based on how many shares they hold.

4.2.4 Deleveraging [3]. Basis bonds can be bought at any time for a price of `oracle_price` BAC, making the effective price of basis bond $\texttt{oracle\_price}^2$ DAI. The intention is to incentivize speculators by giving them a discount for basis bonds in exchange for basis cash.

4.2.5 Risk Absorbers. The risk absorbers are owners of basis bonds, since they bear the risk of not being able to redeem their basis bonds for basis cash. Given that basis share holders don't participate in the deleveraging process, they only reap the benefits of issuance without directly absorbing risk.

4.2.6 Simulations and Analysis. The issuance mechanism for Basis Cash, although different mechanistically, behaves similarly to the issuance mechanism that of AmpleForth - the supply of the coin increases linearly with a damping factor set in the protocol. What's interesting about Basis its deleveraging mechanism - it sells bonds to speculators in exchange for BasisCash at a discount that can be later redeemed as Basis Cash. However, this mechanism has a fatal flaw, in that the protocol has no control over the speculation interest of the market. Furthermore, the speculation interest is only strong if BasisCash grows consistently in its market cap because bonds are only worth something if they can be redeemed back to BasisCash in the future. With these two factors combined, even a small slump in the market sentiment towards BasisCash could lead to a deleveraging spiral that ultimately depegs the stablecoin. In Figure 3, we set a maximum demand for Basis Bonds (reflected by the red line for the lowest supply level that the protocol can deleverage to). As shown in the graph, the price falls short of $1 when there is not enough speculation demand.

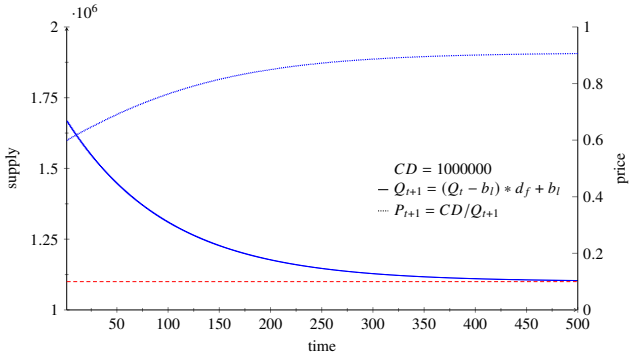


Figure 3: Basis Cash Deleveraging Simulation

4.3 Terra

Terra achieves price stability through an elastic money supply which is enabled by stable mining incentives. The protocol issues Terra currencies pegged to USD, EUR, CNY, JPY, GBP, KRW, and the IMF SDR. TerraSDR is the flagship currency of this family since it exhibits the lowest volatility against any of the individual fiat currencies (Kereiakes, 2018). The Terra protocol runs proof of stake where miners stake a native cryptocurrency, Luna.

4.3.1 Primary Value [9]. Terra is price stable, growth driven, and promotes stable mining incentives. Like AmpleForth and Basis Cash, it does not require any collateral.

4.3.2 Constants [9]. Terra price making is financed through the Luna cryptocurrency. That is, for one to buy 1 TerraSDR, the protocol first mints and sells Luna worth 1 SDR. Then, the Luna (in the amount worth 1 SDR) is exchanged for 1 TerraSDR, so the protocol earns Luna in exchange for TerraSDR. Since Luna is minted to match Terra offers, the volatility is moved from Terra price to Luna supply. The Luna dilution can present a problem for miners, since their Luna stakes are worth a smaller portion of total available mining power. To mitigate this, the system burns a subset of the Luna it has earned during expansions until the Luna supply has reached its 1 billion equilibrium issuance.

4.3.3 Issuance [9]. If one were to expand money supply, all conditions held equal, Terra believes it would result in lower currency price levels. In particular, when price levels are rising above the target, then increasing money supply will return price levels to normal.

> When TerraSDR's price > 1 SDR, users and arbitrageurs can send 1 SDR's worth of Luna to the system and receive 1 TerraSDR.

4.3.4 Deleveraging [9]. If one were to contract money supply, all conditions held equal, Terra believes it would result in higher currency price levels. In particular, when price levels are falling below the target, then reducing money supply will return price levels to normalcy.

> When TerraSDR's price < 1 SDR, users and arbitrageurs can send 1 TerraSDR to the system and receive 1 SDR's worth of Luna.

4.3.5 Risk Absorbers [9]. Terra miners absorb volatility in Terra supply. During a contraction, the system mints and auctions more mining power (mints Luna) to buy back and burn Terra. This temporarily results in mining power dilution; therefore, in the short term, miners absorb Terra contraction cost. In the mid to long term, however, miners are compensated. First, the system continues to buy back mining power (burns Luna) until a fixed target supply is reached, hence creating long term dependability on available mining power. Secondly, the system increases mining rewards.
In order to create mining demand that is long-term stable, the protocol creates predictable rewards. Profit or loss for a unit of mining power abides by the following equation:

$$P(t) = \frac{TotalRewards(t)}{LunaSupply(t)} - UnitMiningCost(t) \quad (4)$$

To achieve predictable awards, the protocol adjusts both transaction fees and the rate of Luna burn to oppose changes in unit mining rewards. Sensibly, adjusting the transaction fees will affect total rewards, and adjusting the rate of Luna burn will affect Luna supply, which are the two factors determining unit mining rewards.

> If unit mining rewards are increasing:
> - decrease fees
> - decrease Luna burn
>
> If unit mining rewards are decreasing:
> - increase fees
> - increase Luna burn

5 THREAT MODELING

Due to constraints in both space and time, we look at one particular instance of insecure stablecoin design - AmpleForth's governance mechanism. On paper, AmpleForth is governed in a decentralized manner by FORTH token owners, and anyone who interacted with the protocol before 03/30/21 can claim a share of the FORTH token [1]. However, the smart contract on-chain shows that AmpleForth is ultimately controlled by undisclosed addresses. According to EtherScan [6], the AMPL token contract is an OpenZeppelin Unstructured Storage Proxy [11], which means it allows the owners of the storage proxy to upgrade the underlying contract at any time. Digging deeper, we see that the owner of the AMPL contract[1] is a MultiSigWallet[2], which in turn has three owners. None of these owners are smart contracts act on behalf of FORTH owners. Instead, they are individual addresses. Given that this MultiSigWallet is currently set require 2 approving owners for it to send a transaction, in the case that any 2 of the owners' accounts get compromised, or if any 2 of the owners decide to collude, the AMPL forth contract could be replaced with something entirely different. In terms of decentralization, AMPL appears to be no better than traditional collateral based stablecoins like USDT and USDC.

[1] 0xD46bA6D942050d489DBd938a2C909A5d5039A161
[2] 0xa847dc227D3F3e86Fa01406279C1E88cb6950c3A

6 CROSS SECTIONAL COMPARISONS

6.1 Market Cap [4]

Of the stablecoins we looked at, FRAX is in lead with 1480 million in market cap; AmpleForth has 216 millions; Fei has 425 millions; Basic Cash has a tiny market cap relatively speaking, at 1.8 million.

6.2 Volume [4]

Two stablecoins with similar market caps can have vastly different trading volumes. AmpleForth does not have the largest market cap, yet it has the most volume traded in the last 24 hour window, at 297 million. Its volume to market ratio is at 1.375. All the other stablecoins have relatively small volume to market cap ratio. Fei is at 0.128 with 54.5 millions daily volume. Both Basis Cash and FRAX have less than 5% volume to market cap ratio. Given that crytocurrencies are not regulated for wash trading, it is possible that AmpleForth is being wash traded, though we should look at volume to market ratios for more coins to understand this issue better. Another explanation to its high volume could be its usage as a unit of denomination in smart contracts, in which case contracts do not hold AmpleForth long term and instead trade the coin to something else right away to avoid volatility.

6.3 Holder Statistics

We look at other holder statistics from on-chain analytics. Specifically, we look at the number of holder addresses, daily active addresses, and holdings by top 3 addresses. The last parameter reflects how concentrated the market is, and therefore how susceptible it is to attacks and market manipulations. AmpleForth has the most address holders, the most daily active address, and also the least concentrated market reflected in the holdings by top 3 addresses.

6.4 Volatility

For comparison, we graph the weekly volatility of the four stablecoin's we analyze in this paper in Figure **??**. We see that BAC's graph approaches a value of 1 over time due to its depegged status, while FRAX and FEI stay near a volatility of 0. AMPL has a large variance in weekly volatility overtime which could indicate shortcomings in its stabilization algorithm.

As Of December 12, 2021				
Stablecoin	AmpleForth	Basic Cash	Fei	FRAX
Number of Holder Addresses	29378	2864	4432	6108
Daily Active Addresses	299	10		82
Holdings by Top 3 Address (%)	37.91	83.52	60.14	71.04
Market Cap (millions)	216	1.8	425	1480
Volume (millions)	297	0.07	54.5	25.6
Vol/Market Cap	1.375	0.04	0.128	0.017

7 EVALUATION

7.1 Volatility Metric

To evaluate our volatility metric, we asked the question of whether the market agrees with the metric. We expected that the lower volatility of a stablecoin, the higher the market cap, since when a user is deciding on a stablecoin to use, they would want the most stable unit available. For the four coins in our analysis, this is indeed the case, with FRAX having the lowest volatility and highest market cap.

We also expected the amount of collateralization to determine a coin's stability, but our volatility measure did not agree. Although FRAX is only partially collateralized, it has a lower volatility with our measure compared to FEI which is over-collarteralized. These findings possibly provide an important insight - that an algorithmic stablecoin's issuance/deleveraging mechanisms can outweigh the amount of collateralization.

7.2 System & Threat Model

We successfully demonstrated the versatility of our system model by applying it to a variety of algorithmic stablecoins and generating useful predictions. Though threat modeling was not a large focus of this paper, we demonstrated that our threat model is a useful tool when analyzing the security of stablecoins by showing one security flaw that we found in AMPL.

8 CONCLUSION

Although we did not arrive at the ultimate algorithmic stablecoin that is free from depegging, we got closer to that goal by comparing various stableocoins, creating a novel volatility metric, and proposing both a system and a threat model. For future work, we think it's beneficial to look at different models of monetary policy and their impact on how the market increase to supply changes in stablecoins, and to apply our system and threat model to more algorithmic stablecoins.

REFERENCES

[1] AmpleForth. [n. d.]. Ampleforth Governance. ([n. d.]). https://www.ampleforth.org/governance/claim/

[2] Basis Cash. [n. d.]. Basis Cash. ([n. d.]). https://app.basis.cash/

[3] Basis Cash. 2021. Stabilization Mechanism - Basis Cash. (2021). https://docs.basis.cash/mechanisms/stabilization-mechanism

[4] CoinGecko.com. 2021. CoinGecko. (2021). https://www.coingecko.com/

[5] Dictionary.com. [n. d.]. Definition of deleveraging | Dictionary.com. ([n. d.]). https://www.dictionary.com/browse/deleveraging

[6] etherscan.io. [n. d.]. Ampleforth: AMPL Token | 0xd46ba6d942050d489dbd938a2c909a5d5039a161. ([n. d.]). https://etherscan.io/address/0xd46ba6d942050d489dbd938a2c909a5d5039a161

[7] Frax Finance. 2021. Frax: Fractional-Algorithmic Stablecoin Protocol. (2021). https://docs.frax.finance/

[8] Evan K., Manny R., and Nithin K. 2021. Ampleforth Network Durability - FAQ. (2021). https://faq.ampleforth.org/durability/

[9] Evan Kereiakes, Do Kwon, Marco Maggio, and Nicholas Platias. 2019. Terra Money: Stability and Adoption. (2019). https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf

[10] Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. 2020. Stablecoins 2.0: Economic Foundations and Risk-based Models. *SSRN Electronic Journal* (2020). https://doi.org/10.2139/ssrn.3633542

[11] OpenZeppelin. [n. d.]. Proxy Upgrade Pattern - OpenZeppelin Docs. ([n. d.]). https://docs.openzeppelin.com/upgrades-plugins/1.x/proxies

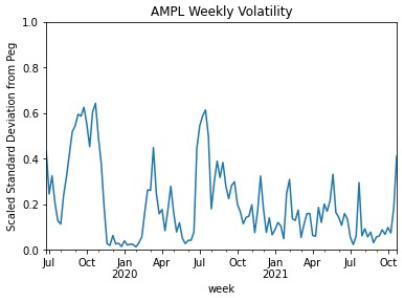
[12] Murray Rothbard. 2010. Copernicus and the Quantity Theory of Money | Murray N. Rothbard. (01 2010). https://mises.org/library/copernicus-and-quantity-theory-money

[13] Robert Sams. 2014. A Note on Cryptocurrency Stabilisation: Seigniorage Shares. (10 2014). https://blog.bitmex.com/wp-content/uploads/2018/06/A-Note-on-Cryptocurrency-Stabilisation-Seigniorage-Shares.pdf

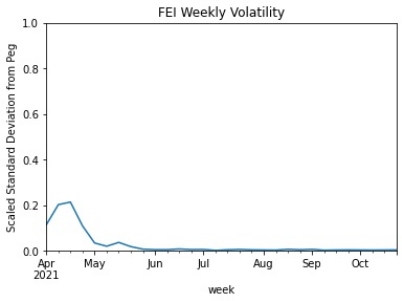
[14] Wenqi Zhao, Hui Li, and Yuming Yuan. 2021. Understand Volatility of Algorithmic Stablecoin: Modeling, Verification and Empirical Analysis. (2021). arXiv:cs.CR/2101.08423

A APPENDIX

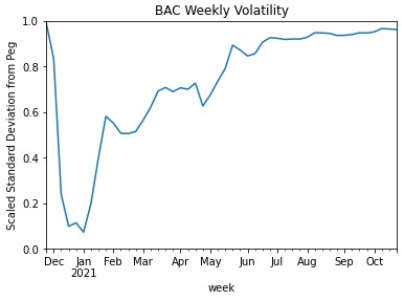
A.1 Additional Graphs



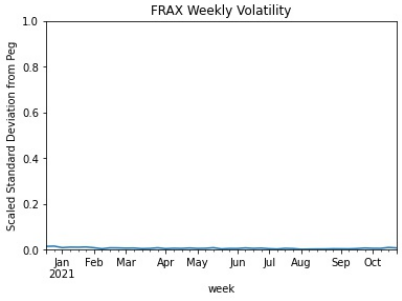
(a) AMPL Weekly Volatility



(b) FEI Weekly Volatility



(c) BAC Weekly Volatility



(d) FRAX Weekly Volatility

Figure 4: Weekly Volatility Charts

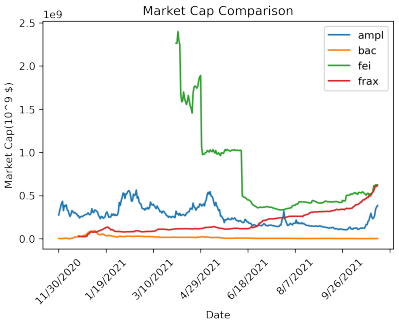


Figure 5: Market Cap Comparison [4]

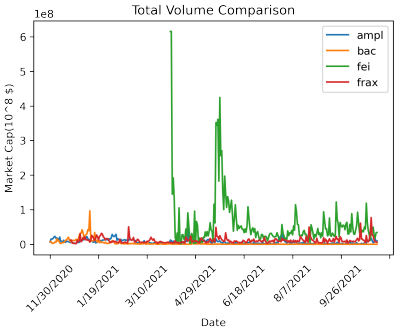


Figure 6: Volume Comparison [4]

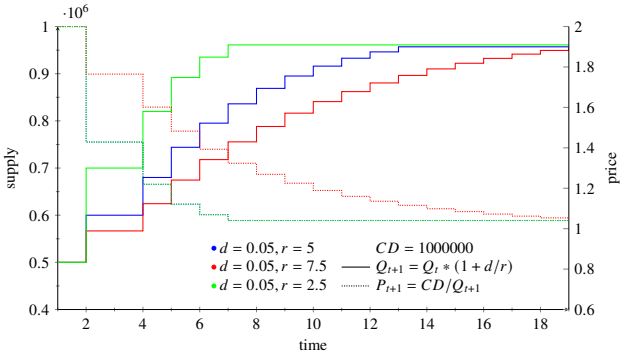


Figure 7: Issuance Simulation

A.2 FRAX [7]

Launched in December 2020, Frax pioneered the partially-collateralized algorithmic stablecoin model. The Frax stablecoin system consists of two tokens:

- FRAX - The stablecoin
- FXS - The utility token, which partially collateralizes the protocol.

The collateral vault initially holds just USDC.

A.2.1 Primary Value. FRAX is partially-collateralized. At launch the collateral ratio began at 100%, meaning that FRAX had a 1:1 backing with USDC. The collateral ratio today is 83.75%, meaning that FRAX is backed 83.75% by the collateral vault and 16.25% by FXS.

A.2.2 Constants.

(1) C_r: Collateral ratio. It's currently at 83.75%.
(2) P_y: The price in USD of collateral Y.
(3) P_z: The price in USD of FXS.

A.2.3 Issuance.
Suppose we are minting F units of Frax at a collateral ratio of C_r with Y units of the collateral asset. The system of equations below describes the minting functions of the FRAX protocal:

$$F = (Y \times P_y) + (Z \times P_z) \tag{5}$$

$$(1 - C_r) \times (Y \times P_y) = C_r \times (Z \times P_z) \tag{6}$$

A.2.4 Deleveraging.
Suppose we are redeeming F units of Frax at a collateral ratio of C_r. This process will transfer Y units of the collateral asset and Z units of FXS to the user:

$$Y = \frac{F \times C_r}{P_y} \tag{7}$$

$$Z = \frac{F \times (1 - C_r)}{P_z} \tag{8}$$

A.2.5 Risk Absorbers. The risk absorbers are traders who arbitrage FRAX when it's off its peg. FRAX can always be minted and redeemed for $1 of value. When the price of FRAX is above $1, a user can deposit $1 of value into the system to mint new FRAX. When the price of FRAX is below $1, a user can redeem FRAX for $1 of value from the system.

A.3 Problems with Basis Cash

(1) risk from DAI
(2) long-term supply that only increases
(3) MEV from people redeeming bonds