CRYPTO LEADERS SINCE 2014

New Frontiers™

ALGORITHMIC STABLECOINS: RAI FRAX AND FEI

Kent Barton

Head of Research and Development, ShapeShift

ShapeShift

Foreword

Stablecoins are the lifeblood of decentralized finance (DeFi). While ETH and other volatile assets collateralize much of the lending that makes DeFi possible, non-volatile alternatives make it far easier to use. Whether it's providing liquidity in an Automated Money Maker (AMM) pool or simply earning yield in a stable asset, the predictable base value offered by the likes of DAI and USDC have played a leading role in DeFi's meteoric rise.

All stablecoins, however, are not created equal. Each project has its own mechanism to reduce volatility, exposes holders to a unique set of risks, and occupies its own space on the spectrum of decentralization.

Where initial efforts to create stablecoins employed an easy-to-understand "lock up a dollar and we'll mint a digital dollar" approach, the design space expanded in a dramatic way with the rise of MakerDAO and DAI—a decentralized alternative that relied on crypto-based collateral rather than locked-up fiat. Over the past year we've seen another wave of stablecoin innovation. This time the experimentation is centered around algorithms that automatically adjust an asset's supply (and other important parameters) in order to reduce volatility. This report will take a closer look at three of these newer alternatives: RAI, FRAX, and FEI. How do they maintain stability? What's their take on governance? What are their potential risks? Can they find a product/market fit in an ecosystem that's already crowded with existing incumbents?

Stablecoin experimentation is happening in real-time with billions of dollars at stake in this vast permissionless lab we call DeFi. Let's crack open the door to the labs and see what's cracking . . .

Kent Barton
Head of Research and Development, ShapeShift

Table of Contents

01 Types of Stablecoins

Types of Stablecoins

Before delving into RAI, FRAX, and FEI, let's briefly examine the broader categories of stablecoins: their algorithmic approach has some crucial differences versus other implementations.

Fiat-Backed

You send me a dollar. I mint you a dollar on the blockchain. Easy peasy—and it's an approach that's been leveraged to great effect by Tether (USDT) and Circle (USDC).

For all its simplicity, there are also a few problems with fiat-backed stablecoins. For starters, you're inherently trusting a third party to hold enough funds to back the asset's total supply. As we've seen with the ceaseless Tether criticism for several years, it's hard to allay these concerns when you're relying solely on the credibility of the stablecoin-minter, or on the opinions of a third-party auditor.

In addition to the risk that your "fully backed" stablecoin has devolved into the fractional-reserve morass, there are also centralization risks. For instance, the entity that mints USDC has the ability to blacklist transactions. While this may be a desirable trait from the standpoint of regulatory adoption, it's also anathema to the fundamentals of permissionless and unstoppable wealth transfer that make crypto so powerful.

Crypto-Collateralized

MakerDAO changed the stablecoin game with DAI. The concept is simple: use crypto-native assets as collateral, which is in turn used to mint a stablecoin. While initially DAI could only be collateralized with ETH, the introduction of multi-collateral DAI (MCD) gave users the ability to lock up a variety of other ERC-20s as well.

By market cap, DAI is the largest decentralized stablecoin. It has a good amount of the ol' Lindy effect going on, with its track record of (pretty good) stability and widespread adoption in the DeFi space. Its reliability can be partially chalked up to over-collateralization: in order to ensure that there are sufficient funds to back DAI, users must provide at least $150 of collateral for every $100 of DAI they recieve. In practice, this means that there's plenty of slack in the system to compensate for the wild volatility of ETH and other MCD ERC-20s.

DAI is not without its downsides. For starters, it's capital-intensive; there's an opportunity cost associated with that extra 50% that

needs to be locked up in order to receive a DAI loan. Additionally, it's arguably too reliant on governance to define important parameters like the protocol's debt ceiling and which ERC-20s can be used in MCD. For those who are skeptical of human intervention, more governance translates to a larger attack surface.

The system is also not immune to wild price swings and steep increases in Ethereum gas prices; during the COVID-inspired "Black Thursday," rapid liquidations led to over $5 million in DAI being uncollateralized. There were brief discussions of an emergency shutdown (a disastrous scenario) before an alternate solution entailing debt auctions was enacted. Although MakerDAO became stronger as a result of Black Thursday (earning it some serious anti-fragility street cred), it's impossible to completely eliminate the systemic risk that stems from highly volatile collateral.

Algorithmic

Over the past year, we've seen the most experimentation around algorithmic stablecoins. The basic notion here is that if a stablecoin protocol has the ability to automatically manage supply by minting and burning assets in response to market conditions, it can ensure that the asset remains close to its peg. This can lead to less reliance on governance, as well as lower collateralization requirements.

RAI, FRAX, and FEI all have algorithmic aspects (although as we'll see, they differ in important ways as well). They've all seen an enthusiastic reception in various parts of the crypto community, owing to their more capital-efficient approach. Another commonality is their usage of time-weighted oracles, pulling data from Uniswap. Time weighting makes it more difficult for attackers to manipulate prices, albeit at the cost of added latency to the price feed.

Note that the algorithmic and crypto-collateralized variants are not mutually exclusive: these stablecoins are collateralized to some extent, but also feature in-protocol mechanisms to manage supply and reduce volatility.

02 RAI

NEW FRONTIERS

RAI

Fiat-backed stablecoins do a wonderful job of reducing exposure to volatility in a common-sense way that everyone can understand.

But when you stop and think about it, there's also a giant elephant in the room. This is crypto! Aren't we supposed to be moving further away from reliance on fiat toward a bankless and blockchain-native world? If fiat is destined for the trash-heap of history, why are we so reliant on dollar-backed assets? Surely there must be a better way.

RAI addresses this elephant in the room with a stablecoin protocol that eschews fiat-pegging. Instead, it floats freely like real-world currencies, and uses an algorithm to reduce its volatility.

If this sounds a little hard to get your head around, you're not alone. Conceptually, this is much different than other stablecoin implementations. Let's take a closer look.

How It Works

In some respects, RAI is similar to MakerDAO's deprecated, single-collateral DAI. Users deposit ETH into a "safe" (similar to DAI vaults), at a minimum collateralization rate of just under 150%, and in turn receive RAI. If the safe's holdings fall under that collateral requirement, the position is liquidated and the debt is covered.

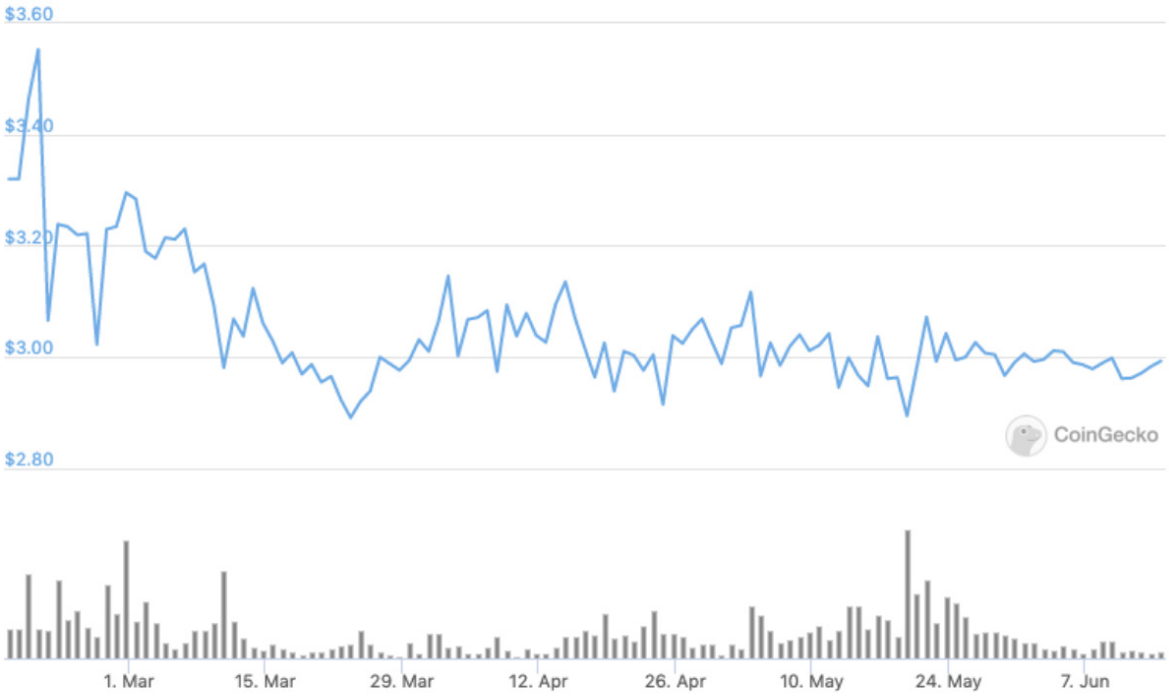
The key differentiator is RAI's peg—or lack thereof. Rather than attempt to remain stable relative to $1.00, RAI follows a "redemption price," which the protocol targets for secondary-market sales. This initial value was $3.14: a completely arbitrary price set by a community Twitter poll. The important thing here isn't the price itself, but rather RAI's ability to maintain stability versus the underlying asset (ETH) over time. Reflexer Labs (the creator of RAI) likes to describe the asset as a volatility-reduced version of ETH, which makes sense considering the latter token is the underlying collateral.

But wait . . . if RAI started off with a dollar-based peg, isn't this just an indirect way of, well, pegging to the dollar, similar to what some fiat currencies do? The key distinction here is that RAI floats freely over time, and might eventually drift far off that initial value; there's no algorithmic design to bring it back to $3.14. The value of RAI is a reduction in volatility, rather than a stable peg. So there's an inherent trade-off here; you might be less sure that RAI can be exchanged for a certain amount of dollars in a year or two, but you can be reasonably sure that it will remain stable over shorter time periods. Thus, RAI appears to be a better choice for traders than long-term holders.

RAI's algorithm is dedicated by a "PID controller" (the term might be familiar to those of you who fly quadcopters), which takes an input of RAI's current price, then adjusts supply based on that price in a continuous feedback loop. (This system gets quite complex, and is described by RAI co-creator Stefan Ionescu here.) The main takeaway here is that these parameters are all hard-coded in the protocol and designed to react automatically to market data without requiring direct human intervention.

RAI also features an "ungovernance token" called FLX that's designed to both act as a backstop source of lending capital and facilitate the gradual removal of human-guided decision-making.

And how has RAI performed in its efforts to reduce volatility? Not too bad, in fact!



Source: Coingecko.com.

Following initial wide price swings, RAI has settled into a reasonably narrow range that reflects very little of ETH's endless volatility. While this stability doesn't come close to fiat-pegged variants such as DAI and USDC, RAI does seem to be succeeding in its mission to provide a reduced-volatility asset that's both decentralized and not pegged to the dollar.

RAI Governance

In addition to opting for a "self-peg" over a fiat peg, RAI also differs sharply from DAI with respect to governance. Its roadmap specifically outlines dates for taking governance out of the equation in 2022, with the goal of removing most parameters from the voting process. This includes questions like "which other collateral types should be added," and, "how should liquidation mechanisms be changed over time?" The goal is a laudable one, although possibly a bit too optimistic given the necessity to tweak parameters when you're experimenting with an entirely new type of stablecoin in a highly volatile market. Nonetheless, RAI's approach offers a stark contrast to DAI and its heavy reliance on governance. Whether that's a good thing or bad thing remains to be seen. In any case, it's nice to see a variety of implementations being offered to crypto users.

Risks

RAI's overcollateralization means that the obvious risk—the protocol having insufficient backing—is largely mitigated. The potential pitfalls lie more in the protocol's code itself; in addition to the underlying smart contract risk that any algorithmic stablecoin presents, the complexity of the PID controller could pose some problems.

For all its clever design and early success, there is no history of reliable PID controller functionality in a variety of market conditions; RAI is treading new ground here. Would the system be able to maintain volatility-reduction in a Black Thursday-esque tsunami of selling? Could high gas prices prevent a timely management of liquidity? We won't have firm answers until RAI has proven itself capable of dealing with crypto's wild volatility.

03 FRAX

NEW FRONTIERS

FRAX

As we discussed previously, DAI, the current leader of the decentralized stablecoin pack, comes with a notable downside: its over-collateralization requirements are not capital-efficient.

On the other hand, not enough collateral could lead to a platform that's insufficiently backed, leading to a precarious house-of-cards scenario.

FRAX is predicated on the notion that a stablecoin can be both partially collateralized and secure, thanks to a system that relies on arbitrage.

How It Works

FRAX is collateralized by USDC at a ratio such that its total USDC backing is always less than the total supply of FRAX.

Right off the bat, then, we have two notable differentiators versus DAI and RAI; in addition to being under-collateralized, it uses USDC, a centralized stablecoin, rather than ETH.

The protocol is algorithmically designed to observe the market price of FRAX, then make adjustments depending on its deviation from the desired $1.00 peg. If FRAX is below $1.00, the collateralization ratio increases, and traders can purchase the token at a discount to its redemption price, pocketing the difference in a straightforward arbitrage. If FRAX rises above its peg, the collateralization ratio decreases, traders can mint FRAX with USDC, and then sell that FRAX—resulting in the market price moving closer to the peg.

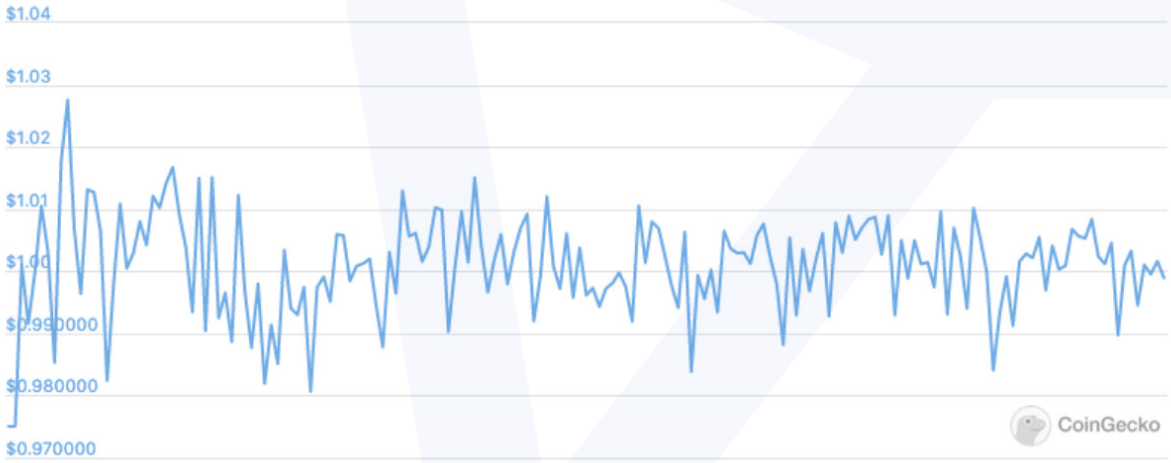
During the minting process, users must also buy Frax Shares (FXS) on the open market and burn it with USDC. In addition to serving as a governance token, this volatile asset also plays a crucial role in the system, as it ensures that value accrues to the protocol.

FRAX founder Sam Kazemian describes the process in a recent podcast:

Let's say Frax is 90% collateralized, and I want to mint 1,000 Frax...That means that basically $900 worth of collateral, 900 USDC, I have to put up. What happens to the $100 of free Seigniorage? Those are basically unbacked Frax, right? Well, that value has to be captured by the Frax share distribution. And the way that we do that is that the person actually coming to mint on the open market, because the price is above it, that person, before they're able to get their Frax, has to go and buy $100 worth of Frax shares and actually burn it in the same minting transaction.

So the end user does have to pony up a full 100% of the "loan's" value (the USDC plus the necessary FXS), albeit in a way that doesn't require over-collateralization.

The system appears to be working as intended. In sharp contrast to early algorithmic stablecoin experiments such as Dynamic Set Dollar (DSD), FRAX has done an admirable job of maintaining its peg:



Source: Coingecko.com.

Governance

In another departure from DAI, FRAX opts for a governance-minimized approach, where there are relatively few algorithmic dials for the community to tweak. As the white paper describes:

Parameters that are up for governance through FXS include adding/adjusting collateral pools, adjusting various fees (like minting or redeeming), and refreshing the rate of the collateral ratio. No other actions such as active management of collateral or addition of human-modifiable parameters are possible other than a hard fork that would require voluntarily moving to a new implementation entirely.

Risks

The most notable point of failure of FRAX is its underlying collateral. USDC falls squarely in the "centralized stablecoin" category, and as such, a portion or all of those assets could hypothetically be frozen by the entity that mints the token. Over time, the addition of non-centralized forms of collateral (such as ETH or DAI) could mitigate this threat.

In addition to smart contact risk, the system might be prone to flash loan exploits; with only a few months of history, it's safe to say there may still be game-theoretical potholes lurking over the horizon. Nonetheless, FRAX's stability thus far is impressive, which bodes well for future adoption.

04 FEI

NEW FRONTIERS

FEI

FEI Protocol is another project that aims to address the capital inefficiencies inherent in stablecoins like DAI. Its high-profile backing from VCs such as a16z, along with $1.3 billion in pre-launch funding, garnered a lot of attention—as did its post-launch turbulence. Most notable, however, is the unique approach FEI takes in its effort to maintain stability.

How It Works

In contrast to the other projects discussed here, FEI does not provide a mechanism where users can swap collateral for the stablecoin. Instead, digital wealth enters the system through the use of a bonding curve that sells FEI for ETH, and is locked in something called "Protocol Controlled Value," (PCV).

As you might glean from the name, PCV is the pool of collateral that the platform holds. Crucially, though, users can't access this value by locking or burning FEI. The purpose of PCV is to maintain the peg through management of liquidity on exchanges such as Uniswap (although the project points out additional potential uses such as insurance funds and governance treasuries). So there's an important shift here: rather than go to the protocol itself to sell FEI, traders can simply do so on the secondary market, with the protocol providing much of that liquidity.

That's an interesting approach, but how is the system supposed to maintain a stable peg with the dollar and avoid the fate of some early algorithmic stablecoins, which entered a death spiral after dropping below $1.00? Enter direct incentives: an attempt to incentivize—and disincentivize—certain economic behaviors. When FEI falls under its peg, sellers of FEI incur a penalty that effectively lowers their sale price. This penalty increases as the price declines.

On paper, this mechanism should prevent the death-spiral scenario, since it limits sell-side liquidity. The reality, as we'll explore shortly, is that these price control mechanisms have initially failed to hold up to the rigours of a live market.

Governance

Separate governance tokens are a common attribute of these for algorithmic stablecoins, and FEI is no exception. The protocol's TRIBE token allows holders to determine how PCV value is allocated, add new bonding curves to sell additional FEI, and tweak other parameters. While the protocol described itself as "governance-minimized," these are pretty powerful abilities in the hands of token-holders!

TRIBE played an important role in FEI's genesis funding round, as these early investors received a proportional amount of the governance token in exchange for funding FEI's bonding curve.

Risks

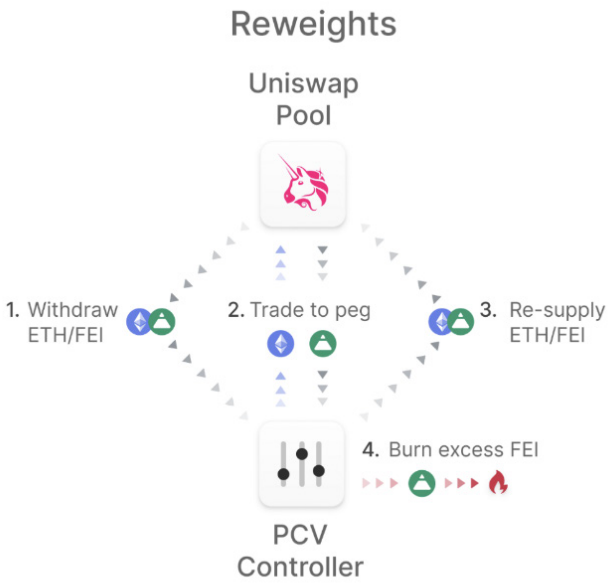
Some risks fall squarely into the "hypothetical scenario" column. Others, like FEI's early trading, are real-life events manifesting before our eyes.

An in-depth post-mortem of FEI's difficulties could cover an entire report of its own. The TL;DR is that FEI's combination of penalties designed to correct a misaligned peg failed to work as intended. As FEI slipped lower and lower from its peg, confidence in the system was reduced. Sellers were discouraged from liquidating their holdings due to the inherent penalties.

While this was an intentional system design, it also appears to have led to lower demand for the token. Perhaps buyers, frightened by the prospect of further weakness, weren't keen to face penalties of their own should they eventually want to sell below the peg. And on a more simple level, it appears that the built-in incentives were not sufficient to overcome the perceived risk of purchasing a stablecoin that immediately went awry after it started trading.

FEI is yet another experiment in the vast DeFi labs. This one happens to have locked well over $1 billion in user funds prior to trading. Yet as we've seen, its success is not guaranteed. While the protocol's attempt to predict and guide behavior seemed strong enough on paper, the vagaries of traders' emotions (and the impact it had on FEI's supply/demand curve) led to an entirely different outcome. As was vividly exemplified by Nixon-era efforts to rein in inflation, price controls have invariably failed to accomplish their goals when enacted by centralized authorities. Should we expect things to play out any differently in a permissionless environment with voluntary actors? Time will tell.

Despite its early challenges, all is not lost for FEI. The system's vast collateral reserves have already been used to "reweight" the token on two separate occasions—and there's a lot more where that came from. Reweighting is a way for the protocol to bring FEI's price closer to the peg, as shown here:



PCV reweights of FEI/ETH Uniswap pool to peg price

Source: https://medium.com/fei-protocol/introducing-fei-protocol-2db79bd7a82b

TRIBE could also be used to re-collateralize the protocol, providing a second backstop. And DeFi is replete with projects that overcame early challenges (SushiSwap is one such example) to find a lasting product/market fit.

Don't expect FEI to go quietly into the night; the protocol will likely regear with modified parameters and resume its efforts to provide an under-collateralized stablecoin to DeFi users.

05 Key Takeaways

Key Takeaways

Algorithmic stablecoins are in their infancy, and not all of these ambitious experiments will succeed. After all, building new types of money is no easy feat! However, the multi-month track record of both RAI and FRAX in reducing volatility via in-protocol parameterization has provided much-needed validation to the concept. Meanwhile, the jury's still out on FEI, and it could still succeed despite its birthing pains.

As an overall asset sub-class, algorithmic stablecoins present some unique considerations:

They offer differing regulatory profiles

As seen by the proposed STABLE Act, some regulators and legislators are eager to assert control over assets that strive to maintain a dollar peg. Centralized stablecoins may be the most vulnerable to this; whether it's Facebook with its proposed Diem (formerly Libre) token, Tether (USDT), or Circle (USDC), the existence of a centralized issuer provides a clear regulatory target. Decentralized stablecoins such as DAI could be more difficult to target, and it's interesting to note that all three of the assets covered in this report lack a single issuing off-chain authority.

RAI also stands out due to its lack of a dollar peg. Perhaps regulators would find this less of a threat, or at least less of a tempting target, since RAI floats freely and has opted for volatility-minimization over remaining in lockstep with the greenback.

They're good for DeFi

When it comes to stablecoins powering DeFi, more options are a good thing. Whereas in the early days DeFi DApps mainly used DAI, they were also exposed to all of DAI's risks. These days, with the likes of USDC and Terra USD (UST) providing liquidity across the ecosystem, those risks have been spread out. This dynamic will only accelerate with the rise of algorithmic volatility-reducing assets, thus making the overall DeFi world more resilient.

Algorithmic stablecoins could be a good fit for niche use cases

Even if DeFi remains the bastion of DAI, USDC, and other incumbents, there's plenty of room for alternatives. For instance, RAI and its "volatility-reduced ETH" value proposition might appeal to decentralization maximalists who prefer to be further removed from any semblance of fiat. Similarly, many DeFi users might gladly trade off some perceived added execution risk for the ability to mint FRAX without needing to over-collateralize.

They all rely on the same type of oracle

One interesting commonality between RAI, FRAX, and FEI is that they all employ exchange-based, time-weighted price oracles (in the case of RAI, data is provided by Chainlink). This approach is effective, but it's not without downsides. Even though time-weighting makes it more difficult for an attacker to manipulate the price of an asset on an ongoing basis, the risk hasn't been completely eliminated. Additionally, this type of oracle inherently adds latency, which can lead to algorithms lagging the market and failing to modify supply and demand in a timely fashion.

More than ever, there is a clear need for other oracle types with less latency. Microtick, with its ability to provide pricing data on a block-by-block basis, while simultaneously making it possible for DApps to hedge said data, could be an especially good fit for algorithmic stablecoins.