COTW: Solving the Stablecoin Trilemma with Algorithmic Stablecoins

A new breed of algorithmic stablecoins are attempting to solve the stablecoin trilemma and offer price stability, capital efficiency and decentralization. We review various algorithmic stablecoin models and offer our thoughts in this week's Chart of the Week.

The Stablecoin Trilemma: Stablecoins are digital currencies whose value is tied to that of another asset, most often US dollars, and are designed to reduce the volatility inherent in cryptocurrencies. Stablecoins are predominantly used to facilitate simple and efficient cryptocurrency trading, though are increasingly used within decentralized applications and for payments, remittances, and settlement, among other use cases. Stablecoins may be fiat-collateralized, where a centralized party mints and burns the stablecoin, backing it one-to-one usually with cash in a bank account. Stablecoins may also be crypto-collateralized, where smart contracts rely on monetary policy, arbitrage, and overcollateralization to maintain their peg. Or they may be algorithmic, where a stability mechanism attempts to maintain the peg despite not having full collateralization. While definitions are not fully set and lines are blurred, the various stablecoin types offer tradeoffs for their users. For example, fiat-collateralized stablecoins have the strongest track record of price stability, are simple, and will be the first to have a robust regulatory regime in many jurisdictions to usher in greater corporate and institutional usage, but they introduce centralization into an otherwise often decentralized environment, and require trust that users won't be blacklisted, reserves are as promised, and governments won't shut them down. Crypto-collateralized stablecoins eliminate many of these centralization drawbacks, but require over-collateralization, making them capital inefficient. And algorithmic stablecoins, by contrast, are decentralized and capital efficient, but have generally had a more checkered past when it comes to price stability. However, a new set of algorithmic stablecoins employing innovative design mechanisms have thus far performed remarkably well, offer additional benefits beyond simple dollars on a blockchain, and represent our best hope yet for achieving one of DeFi's holy grails and solving the stablecoin trilemma.

Algorithmic Stablecoins: While fiat-collateralized stablecoins are by far the most prevalent, algorithmic stablecoins are gaining in prominence. Algorithmic stablecoins use a variety of stabilization

mechanisms intended to absorb the volatility of the stablecoin. According to Fei Protocol founder Joey Santoro, there are three general types of risk-absorbing mechanisms:

- Supply Volatility Model: These stablecoins alter their supply to bring the price back to peg, though have generally been less successful. Supply volatility models include:
  - Rebasing stablecoins, where the protocol uses an oracle to periodically check the stablecoin's price, and if the price is above target, it will increase the number of tokens each holder has proportional to their holdings to bring the price down. Conversely, if the price is below target, it will reduce the number of tokens everyone has to increase the price. Rebasing stablecoins exchange price volatility for supply volatility, and may be more difficult to integrate into other protocols as holders' balances are frequently changing. Examples include Yam Finance and Ampleforth.
  - Seigniorage style stablecoins, which attempt to use one or two additional tokens to absorb the volatility in the stablecoin by changing the stablecoin's supply, printing more stablecoins when demand is high and reducing the supply when demand is low. A three-token system, for example, consists of stablecoin, share, and bond tokens. When the stablecoin price is above target, the protocol will mint more stablecoins and distribute them to the share token holders, who may then sell them, expanding the supply and bringing the price down. Conversely, when the stablecoin's price is below target, the protocol will sell bond tokens at a discount for the stablecoin, reducing the stablecoin's supply and pushing its price back up. Users who purchased the bonds at a discount then make money as the stablecoin rises in value. While effective in theory, seigniorage-based stablecoins suffer from runs on the bank as the bonding incentives typically aren't strong enough to entice users to step in during a price spiral, especially without a collateral backstop. Additionally, some seigniorage style stablecoin designs have been criticized for having pyramid scheme-like elements, as they effectively promise future seigniorage to share token holders, which requires a collective belief in the protocol's future growth. Examples of seigniorage style stablecoins include Empty Set Dollar and Basis Cash.

- Secondary Token Model: Secondary token models use a secondary token to absorb the volatility of the stablecoin via a minting and redemption mechanism. When the demand for the stablecoin goes up and the price rises above peg, users can mint a new stablecoin for $1.00 worth of the secondary token, with the secondary token being burnt. Users can then sell the stablecoin they purchased for $1.00 for the current market price to make a profit, increasing the supply and bringing the price back down. Conversely, when the price is below $1.00, a user can sell their stablecoin for $1.00 worth of a newly created secondary token, with the stablecoin being burnt as part of the process. This allows the holder to profit from the difference between the $1.00 sale price and the current market price and also decreases the stablecoin supply, pushing its price back up. Secondary token models may use a single secondary token such as LUNA with UST or may employ more diverse collateral like Fei and Frax. Secondary token models relying on a single endogenous token allow the secondary token to capture value as the demand for the stablecoin increases (as the secondary token supply is reduced and its price increased). However, such secondary token models can be reflexive, particularly if they are without a sound minting/burning/collateral management

mechanism, as a rapid decline in the price of the secondary token may cause stablecoin holders to redeem them for newly created secondary tokens, which increases the secondary token supply and further pushes down the price in a continued negative loop.

- Leverage & Insurance Volatility Hedging Models: Leverage & insurance volatility hedging models utilize derivatives or insurance to hedge collateral volatility. For example, a stablecoin may be collateralized by ETH, which is fully offset by selling a perpetual futures contract, making the ETH collateral delta neutral. The model then relies on arbitraugers minting and redeeming the stablecoin for the underlying collateral to arb the price back to the peg. Such a model introduces additional complexities, such as solving for funding rates, though significant progress here is under way. Examples include UXD Protocol and Angle Finance.

The Contenders: Below we review the largest algorithmic stablecoins, with a focus on their stability mechanisms.

- Dai (DAI): With a four-year track record of stability and integration into over 400 apps and services, DAI is a stablecoin created by MakerDAO soft-pegged to the US dollar and backed by crypto assets. Users lock community-approved Ethereum-based assets into a vault, previously known as a collateralized debt position (CDP) with single-collateral DAI, in order to generate DAI. Importantly, each vault is overcollateralized, and further safety mechanisms include auto-liquidations, a surplus fund created from liquidation fees and cumulative accrued stability fees, and a debt auction mechanism. MakerDAO governance helps maintain the peg by adjusting Maker Vault Stability Fees, which is the interest rate charged on the loan, as well as using the Peg Stability Module. For example, if DAI is below $1.00, the stability fees will increase, incentivizing Vault owners to purchase DAI on the open market to pay down DAI they have generated. Conversely, when DAI is above $1.00, the stability fees will be lowered to lower the cost of generating DAI, enticing users to take out more DAI loans and increasing the DAI supply to bring its price lower. Maker Vaults allow users to increase leverage / exposure to a given asset by using the borrowed DAI to purchase more of the underlying collateral asset, to generate liquidity from collateral assets without selling them, or to use the DAI to earn passive income. While the Maker Protocol is non-custodial, permissionless, and battle-tested, the majority of the collateral backing DAI is comprised of fiat-collateralized stablecoins and WBTC, introducing an element of centralization into the system.

- Magic Internet Money (MIM): Created by cross-chain stablecoin lending protocol Abracadabra Money, MIM is a decentralized stablecoin soft-pegged to the US dollar. Similar to MakerDAO, users deposit assets in return for the stablecoin, however, Abracadabra lets users deposit yield-bearing assets such as yvYFI, yvUSDT, yvUSDC, and xSUSHI to mint MIM. This causes the collateral to accrue in value, reducing the risk of liquidation and improving capital efficiency. Moreover, unlike most protocols where all of a user's collateral is at risk of a liquidation event, Abracadabra isolates each CDP, so only it is at risk of its own liquidation. MIM maintains its peg via arbitrage incentives. For example, if MIM was below $1.00, anyone with an outstanding MIM loan would be incentivized to buy sub-$1.00 MIM to repay their loan, driving up the price of MIM. Conversely, if MIM was over $1.00, users

would be incentivized to borrow MIM from Abracadabra for $1.00 and sell them in the open market, increasing the MIM supply and causing the price to fall.

- TerraUST (UST): With over $11b in circulation, UST is the largest algorithmic stablecoin and is one of the Terra blockchain's many decentralized stablecoins. UST is backed by Terra's LUNA token, and allows anyone to mint UST by burning $1.00 worth of LUNA, or burn one UST in exchange for $1.00 worth of newly-created LUNA. UST has been lauded for its true decentralization, given its exclusive LUNA backing, for its recent protocol upgrades that should only improve on its solid track record, and for its minting mechanism that allows LUNA holders to capture value as UST demand grows. UST, however, has been criticized for its reflexivity and the potential for a rapidly falling LUNA price to cause UST redemption and further LUNA selling (though LUNA has significant intrinsic value as the native token of the Terra blockchain).

- Frax (FRAX): Realizing that collateral backing doesn't have to be all or nothing, Frax is the world's first fractional-algorithmic stablecoin, partially backed by collateral and partially stabilized algorithmically. Moreover, this ratio of collateralized and algorithmic is determined by the market. Frax relies on arbitrageurs to mint and redeem FRAX using a two-token system, with the other token being Frax Shares (FXS), its governance token that accrues fees, seigniorage revenue, and excess collateral value. If FRAX is trading above $1.00, the protocol decreases the collateral ratio, expanding the supply of FRAX and using excess collateral to burn FXS. For example, if FRAX is trading at $1.01 and has a current collateralization ratio of 85.25%, the protocol will decrease the collateralization ratio by 25 bps to 85.00%, and a user can put in $0.85 of USDC and $0.15 of FXS tokens, the latter of which is then burned, in exchange for a newly minted FRAX token. The user now has a FRAX with a market price of $1.01 that they minted for $1.00 of value, and when they sell it, this expands the supply of FRAX and brings down its price, while also allowing FXS holders to benefit from the increased demand and capture the seigniorage. By contrast if FRAX is trading at $0.99, the protocol will increase the collateral ratio back to 85.25%, and a user can redeem one FRAX for $0.8525 of USDC and $0.1475 of FXS. The user can sell the FXS and USDC immediately for $1.00, profiting off of the spread, and the entire transaction removed FRAX from circulation to increase its price back towards $1.00, all while generating additional confidence in the system given the higher collateralization ratio. Frax v2 introduces algorithmic market operations (AMOs) built on top of the above mechanism that allow the protocol itself to stabilize the FRAX price, for example, by minting or burning FRAX from the Curve Frax3CRV pool when the pool is off balance. Lastly, FRAX is currently pegged to the USD, but is working on creating a crypto native CPI called the Frax Price Index to ultimately become the first decentralized, permissionless native unit of account to hold the standard of living stable.

- Fei USD (FEI): With the goal of becoming the decentralized USDC and servicing DAOs, Fei pioneered the concept of Protocol Controlled Value, assets that fully collateralize its FEI stablecoin, are owned by the protocol, and include decentralized stablecoins, ether, and interest-bearing assets. Fei originally used a direct incentives mechanism to reward or penalize users trading towards or away from the peg, but now uses redeemability of FEI for PCV reserves as its primary stabilization mechanism. Moreover, Fei's PCV is used to generate additional income for the protocol and perhaps more importantly, to provide

liquidity services for DAOs such as with its liquidity-as-a-service product offering with Ondo Finance and its forthcoming Turbo product. Fei uses Balancer v2 Investment Pools to manage its PCV composition, algorithmically adjusting it towards safer assets as the collateral ratio falls towards 100% and to riskier assets as it rises much higher. Lastly, Fei's TRIBE governance token benefits from TRIBE buybacks and also acts as a backstop for the protocol. Fei recently merged with permissionless lending market protocol Rari Capital with the goal of becoming a full-stack DeFi infrastructure.

- Others: In addition to the above, there are many other models. Ampleforth, for example, is a tokenized unit of account targeting the 2019 US dollar, which it does so by changing the number of AMPL tokens in each holders' wallet, achieving both elasticity and non-dilution. While not pegged to a specific fiat currency, Olympus DAO employs unique bonding and staking mechanisms in its quest to be cryptocurrency's decentralized reserve currency (Olympus is a PCV-backed asset similar to Fei, but lets the market determine its price rather than use its PCV and redeemability to target $1.00). And Djed, an algorithmic stablecoin developed by IOG, acts like an autonomous bank and uses formal verification to remove price volatility.

Risks: Achieving the stablecoin trilemma is not without risk. There is the risk of a run on a stablecoin - see Empty Set Dollar, Basis Cash, and Iron Finance to name a few - particularly for those without redeemability, and to a lesser extent for those without full collateralization or that are self-referential. There is also oracle risk, where oracle prices used in some stability mechanisms may be stale in the face of extreme volatility or could be manipulated by flashloan attacks. There is also contagion risk, as stablecoins are often used as collateral for each other and are also connected by Curve pools, as we saw a few weeks ago when MIM selling caused many to question UST. All this said, these risks, in our opinion, are worth the end reward.

What May Lie Ahead: We believe we are closer than ever before to algorithmic stablecoins achieving price stability, capital efficiency, and decentralization. Going forward, we see algorithmic stablecoins coexisting and in some ways benefitting from CBDCs and fiat-backed stablecoins. The larger algorithmic stablecoins grow and the longer they demonstrate price stability, the stronger the collective social belief in their $1.00 value will become, the greater their liquidity, and the better their stability mechanisms work. We see algorithmic stablecoins pushing forth new innovative stability mechanisms that add new use cases and value propositions, such as Fei's liquidity-as-a-service, as well as new design elements, such as moving more towards decentralized cryptocurrency assets as collateral. We may see more non-USD fiat-denominated stablecoins given the global nature of cryptocurrencies. And stablecoin projects will likely introduce innovative, non-fiat-based peg targets, freeing themselves from central bank fiat debasement that attracted so many to crypto in the first place. This will include new price indexes, such as Frax's Frax Price Index, and non-sovereign or non-pegged stablecoins like Olympus DAO's OHM, Reflexer's RAI, and Float Protocol's FLOAT. Lastly, we're likely to see improved stablecoin infrastructure, allowing users to hold whichever stablecoin they choose, with seamless conversion occurring behind the scenes and abstracted away from the user. Though there will surely be failure along the way, ultimately, we see algorithmic stablecoins continuing to grow in prominence as they make their way to solving the stablecoin trilemma.

Exhibit 1: Algorithmic Stablecoin Performance, Last 12 Months
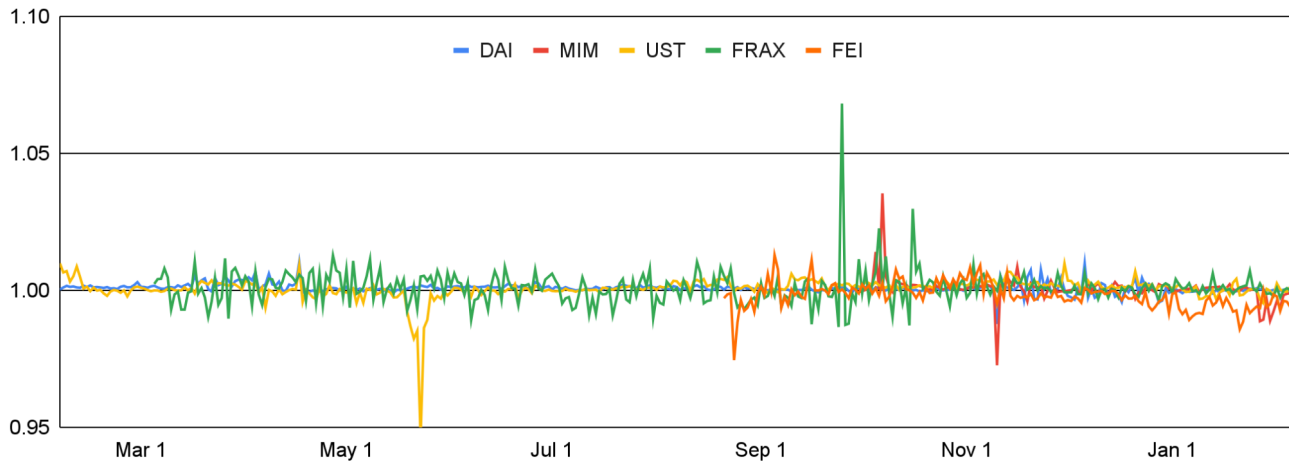
Source: Santiment, GSR

Author: Brian Rudick, Senior Strategist

<u>Sources</u>
- [Joey Santoro : An Overview of Algorithmic Stablecoins](#)
- [Chainlink: Stablecoin Founders: The Future of Stablecoins](#)
- [Epicenter Podcast: Joey Santoro: Fei Protocol – Introducing Fei V2 #422](#)
- [Multicoin Capital: Solving the Stablecoin Trilemma](#)
- [Valentin Kalinoff: Algorithmic Stablecoins](#)
- [CoinDesk: The Quest for a Truly Decentralized Stablecoin](#)
- [Messari: The Art of Central Banking on Blockchains: Algorithmic Stablecoins](#)
- [Coin Bureau: Algorithmic Stablecoins - Everything You Need to Know!](#)
- [Built to Fail: The Inherent Fragility of Algorithmic Stablecoins](#)
- [The Block Stablecoins: Bridging the Network Gap Between Traditional Money and Digital Value](#)

About GSR

GSR is a global leader in digital asset trading, market making, OTC derivatives, and investments. We operate in a culture of excellence and leverage our first-rate reputation, deep relationships and proprietary trading technology to move swiftly and capitalize on market opportunities.

GSR's experienced team brings together decades of institutional trading expertise, while our industry-leading proprietary technology stack anchors everything we do.

Our main service areas are: market making; proprietary and algorithmic trading; client execution; structured products; risk management solutions; and portfolio investments.

For more information or if we can help with anything, please see gsr.io or contact us at gsr@gsr.io.

Required Disclosures