Frax: Fractional-Algorithmic Stablecoin Protocol

Sam Kazemian
sam@frax.finance

Kedar Iyer
kedar@frax.finance

Jason Huan
sino@ucla.edu

July 2020

Abstract

We propose a 2-token, fully-autonomous protocol which transitions a fully collateralized stablecoin (FRAX) to a fully algorithmic one, moving through a fractional-collateral phase. As the monetary premium of FRAX increases through usage, the backing collateral is lowered in small increments to create a fiat-like stablecoin. FRAX is backed 100% by collateral at genesis. As usage of FRAX as a medium of exchange grows, so does its monetary premium and demand. This allows the backing to be incrementally lowered as long as the price target of $1/FRAX holds.

1 Introduction

Stablecoins have been a mainstay of the crypto industry since they first emerged in 2014 with Tether being the first major token to gain widespread use and attention. As of 2020, the Ethereum network transfers more Tether value than any other token, including the chain's native ETH token. Tether has a global daily volume of over $50B on average, significantly higher than that of Bitcoin itself. The total combined market capitalization of ERC20 stablecoins in comparison to ETH has been slowly narrowing, with some predicting a 'stablecoin flipping' in the coming months. Such an occurrence would be the first time in blockchain history where a subtoken of a major network is more valuable than the endogenous unit of account of the protocol.

Stablecoins have gone from under 10% of active Ethereum addresses to almost 40% of active Ethereum addresses as of July 2020. As more new Ethereum addresses transition to stablecoin-holding addresses, it becomes clear that most of the growth in Ethereum today is led and fuelled by stablecoin demand.

Although there are many ways to categorise stablecoins, two distinct design concepts have stood out over time: collateralized stablecoins and algorithmic stablecoins. Variations of each type have been tested with degrees of success (or lack thereof). Collateralized stablecoins are usually subcategorized into either crypto-collateralized (MakerDAO's Dai) or fiat-collateralized tokens (Tether, BUSD, USDC), with both subgroups having had significant adoption. Algorithmic stablecoins have had almost no meaningful traction although various high profile attempts have been made. Algorithmic stablecoins attempt to change the circulating supply of the token so that changes in demand for the stablecoin minimally affect its price. Additionally, algorithmic stablecoins are not collateralized or redeemable for an underlying asset. We contend that a prevailing reason for the lack of traction of algorithmic stablecoins was not their economic infeasibility, but their flawed designs and execution.

FRAX is the first decentralized, fractional-reserve stablecoin–one which begins as a fully collateralized stablecoin, but then transitions to a fully algorithmic design as it matures. This unique design allows FRAX to move through a fractional phase where it is only partially backed with collateral and price-stabilized through supply changes. We believe this design will prove to be the most resilient, transparent, scalable stablecoin yet developed.

Figure 1: Three FRAX tokens minted through 3 different collateral pools (USDT, DAI, and USDC respectively) at a collateral ratio of 72%. Each FRAX is composed of two pieces of value denoted by their icons: the fiat value/monetary premium (Frax icon) and the collateral-backed value (collateral icon). As FRAX is used as a medium of exchange and money, its fiat value increases as priced by the market. The Frax Protocol's minting process is designed to determine what that fiat value is at any given time.[1]

2 A Unique, Hybrid Approach to Algorithmic Stability

The Frax protocol is designed to begin completely collateralized at genesis and move through three stages: 100% phase, fractional phase, and algorithmic phase.

FRAX stablecoins can be minted by placing the appropriate amount of its constituent parts into a smart contract. At genesis, FRAX is 100% collateralized, meaning that minting FRAX only requires placing collateral into the minting contract. During the fractional phase, minting FRAX requires placing the appropriate ratio of collateral and Frax Shares (FXS) into the system. While the protocol is designed to accept any type of cryptocurrency as collateral, this implementation of the Frax Protocol will mainly accept on-chain stablecoins as collateral to smoothen out volatility in the underlying asset so that FRAX can transition to its algorithmic phase smoothly and slowly.

FRAX can always be minted and redeemed from the system for $1 of value. This allows arbitrageurs to balance the demand and supply of FRAX in the open market. If the market price of FRAX is above the price target of $1, then there is an arbitrage opportunity to mint FRAX tokens by placing $1 of value into the system per FRAX and sell the minted FRAX for over $1 in the open market.

At all times in order to mint new FRAX a user must place $1 worth of value into the system. The difference is simply what proportion of collateral and FXS makes up that $1 of value. When FRAX is in the 100% collateral phase, 100% of the value that is put into the system to mint FRAX is collateral. As the protocol moves into the fractional phase, part of the value that enters into the system during minting becomes FXS (which is then burned from circulation). For example, in a 98% collateral ratio, every FRAX minted requires $0.98 of collateral and $0.02 of FXS. In a 97% collateral ratio, every FRAX minted requires $0.97 of collateral and $0.03 of FXS, and so on.

If the market price of FRAX is below the price range of $1, then there is an arbitrage opportunity to mint FRAX tokens by purchasing cheaply on the open market and redeeming FRAX for $1 of value from the system. At all times, a user is able to redeem FRAX for $1 worth of value from the system. The difference is simply what proportion of the collateral and FXS is returned to the redeemer. When FRAX is in the 100% collateral phase, 100% of the value returned from redeeming FRAX is collateral. As the protocol moves into the fractional phase, part of the value that leaves the system during redemption becomes FXS (which is minted to give to the redeeming user). For example, in a 98% collateral ratio, every FRAX can be redeemed for $0.98 of collateral and $0.02 of FXS. In a 97% collateral ratio, every FRAX can be redeemed for $0.97 of collateral and $0.03 of FXS.

The protocol adjusts the collateralization ratio during times of expansion and retraction. During times of expansion, the protocol decollateralizes (lowers the ratio) the

[1] Each FRAX is redeemable for $1 of total value with a proportion of value coming from collateral and the remaining from FXS.

system so that less collateral and more FXS must be deposited to mint FRAX. This lowers the amount of collateral backing all FRAX. During times of retraction, the protocol recollateralizes (increases the ratio) the system so that redeemers of FRAX receive more FXS and less collateral from the system. This increases the ratio of collateral in the system as a proportion of FRAX supply, increasing market confidence in FRAX as its backing increases. At genesis, the protocol will adjust the collateral ratio using a designated oracle in the same way that prices are reported. The oracle will adjust the collateral ratio up or down periodically given the reported price of FRAX in the open market. In a future protocol update, the price feeds for collateral can be deprecated and the minting process can be moved to an auction based system to limit reliance on price data and further decentralize the protocol. In such an update, the protocol would run with only price data of FRAX and FXS. Minting and redemptions would happen through open auction blocks where bidders post the highest/lowest amount of collateral plus FXS they are willing to mint/redeem FRAX for. This auction arrangement would lead to collateral price discovery from within the system itself and not require any additional price information. Additionally, in a further update, the collateral ratio controller can be automated as well. A predefined, deterministic rule set can be designed for decolalteralization and recollateralization [2]

FRAX can always be minted and redeemed from the system for $1 of value. This allows arbitrageurs to balance the demand and supply of FRAX in the open market. If the market price of FRAX is above the price target of $1, then there is an arbitrage opportunity to mint FRAX tokens by placing $1 of value into the system per FRAX and sell the minted FRAX for over $1 in the open market.

At all times in order to mint new FRAX, a user must place $1 worth of value into the system. The difference is simply what proportion of collateral and FXS makes up that $1 of value. When FRAX is in the 100% collateral phase, 100% of the value that is put into the system to mint FRAX is collateral. As the protocol moves into the fractional phase, part of the value that enters into the system during minting becomes FXS (which is then burned from circulation). For example, in a 98% collateral ratio, every FRAX minted requires $.98 of collateral and $.02 of FXS. In a 97% collateral ratio, every FRAX minted requires $.98 of collateral and $.03 of FXS. And so on..

If the market price of FRAX is below the price range of $1, then there is an arbitrage opportunity to mint FRAX tokens by purchasing cheaply on the open market and redeeming FRAX for $1 of value from the system. At all times, a user is able to redeem FRAX for $1 worth of value from the system. The difference is simply what proportion of the collateral and FXS is returned to the redeemer. When FRAX is in the 100% collateral phase, 100% of the value returned from redeeming FRAX is collateral. As the protocol moves into the fractional phase, part of the value that leaves the system during redemption becomes FXS (which is minted to give to the redeeming user). For example, in a 98% collateral ratio, every FRAX can be redeemed for $.98 of collateral and $.02 of FXS. In a 97% collateral ratio, every FRAX can be redeemed for $.97 of collateral and $.03 of FXS.

The protocol adjusts the collateralization ratio during times of expansion and retraction. During times of expansion, the protocol decollateralizes (lowers the ratio) the system so that less collateral and more FXS must be deposited to mint FRAX. This lowers the amount of collateral backing all FRAX. During times of retraction, the protocol recollateralizes (increases the ratio) the system so that redeemers of FRAX receive more FXS from the system than collateral. This increases the ratio of collateral in the system as a proportion of FRAX supply.

---

[2] i.e. If the price of FRAX is greater than $1 for more than X blocks, decollateralize by Y%".

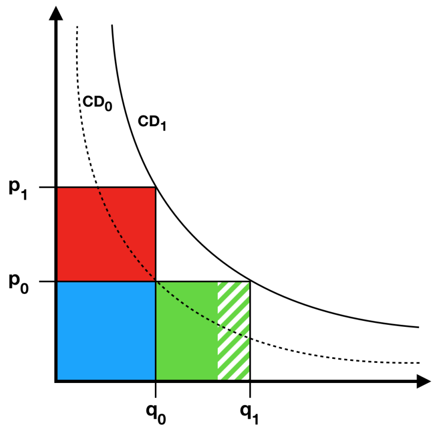

Figure 2: The demand curve illustrates how minting and redeeming FRAX keeps the price stabilized (q = quantity, p = price). At CD_0 the price of FRAX is $p_0 = \$1$ at q_0. If there is more demand for FRAX, the curve shifts right to CD_1 and a new price, p_1, corresponds to the same quantity q_0. In order to recover the price to $1, new FRAX must be minted until q_1 is reached and the p_0 price is recovered. Since market capitalization is calculated as price times quantity, the market cap of FRAX at q_0 is the blue square. The market cap of FRAX at (q_1, p_0) is the sum of the areas of the blue square and green square. Notice that in this example the new market cap of FRAX would have been the same if the quantity did not increase because the increase in demand is simply reflected in the price, p_1. Given an increase in demand, market cap increases either through an increase in price or increase in quantity (at a stable price). This is clear because the red square and green square have the same area and thus would have added the same amount of value in market cap.[3]

3 Redeemability

Redeeming FRAX seamlessly for collateral and FXS is crucial. Otherwise, the price of FRAX tokens could trade at a discount to the actual collateral in the reserve if redemption is tedious or costly. Redemption simply requires sending FRAX tokens to a smart contract and paying a negligible redemption fee (currently set to 0.04% of the transaction), which then immediately sends collateral and FXS back to the user. The redemption fee accumulates in the system and a future FXS governance vote can allocate the funds for usage.

During the 100% phase, each FRAX is redeemable for $1 worth of collateral (and zero FXS) at all times. During the fractional phase, each FRAX is backed by only a partial amount of collateral. However, since FRAX will likely trade at $1, it must be redeemable from the system's smart contract for $1 of value. Thus, during the fractional phase, FRAX is redeemable for the ratio of collateral backing it and the remaining value in FXS minted from the system. For example, at a 90% collateral ratio, each FRAX token is only backed by $0.90 of collateral. However, users can still redeem each FRAX for $1 worth of value by receiving $0.90 of collateral and $0.10 worth of minted FXS. This allows for redemptions to not affect the collateral ratio of the system. It is important to note that FRAX is always redeemable for $1 of value from the system and not simply 1 'unit' of collateral or FXS. For example, if the collateral ratio is 90% then each FRAX is redeemable for $0.90 of collateral value and not 0.9 units of collateral. This is important because while the Frax Protocol uses stablecoins as collateral to prevent large swings in collateral ratio, it is still possible for each unit of collateral to slightly deviate in value

[3]The semi-shaded portion in the green square denotes the total value of FXS shares that would be burned if the new quantity of FRAX was generated at a hypothetical collateral ratio of 66%. This is important to visualize because FXS market cap is intrinsically linked to demand for FRAX.

(e.g. \$1.01 or \$0.99 per USDT). If FRAX was redeemable for 1 unit of collateral rather than \$1 of value, then there would be arbitrage opportunities to empty the collateral pools when the price of FRAX is at or above \$1 and the price of collateral is below \$1/unit. This type of arbitrage is not desired by the protocol and is more akin to swap services like Curve.fi and Uniswap.

If or when the protocol reaches the fully algorithmic phase, each FRAX is backed by 0% collateral and thus always redeemable for \$1 worth of FXS minted from the system. Conversely, during the fully algorithmic phase, each FRAX can only be minted by placing \$1 worth of FXS into the system.

This redemption process is seamless, easy to understand, and economically sound. During the 100% phase, it is trivially simple. During the latter two phases, as FRAX is minted, FXS is burned. As FRAX is redeemed, FXS is minted. As long as there is demand for FRAX, redeeming it for collateral plus FXS simply initiates minting of a similar amount of FRAX into circulation on the other end (which burns a similar amount of FXS). Thus, the FXS token's value is determined by the demand for FRAX. The value that accrues to the FXS market cap is the summation of the non-collateralized value of FRAX's market cap.

4 Frax Share Tokens (FXS)

The Frax share token (FXS) is the non-stable, value-accrual token in the protocol. It is meant to be volatile and an investment asset, unlike the FRAX stablecoin, which remains at \$1. FXS has the potential of upside and downside of the system, where the delta changes in value are always stabilized away from the FRAX token itself. FXS supply is initially set to 100 million tokens at genesis, but the amount in circulation will likely vary as FRAX is minted and redeemed. Regardless, the design of the protocol is such that FXS would be largely deflationary as FRAX demand grows.

The FXS token's market capitalization should be calculated as the future expected net value creation from seigniorage of FRAX tokens in perpetuity. Additionally, as the market cap of FXS increases, so does the system's ability to keep FRAX stable. Thus, the priority in the economic design is to accrue maximal value to the FXS token while maintaining FRAX as a stable currency. As Robert Sam's described in the original Seigniorage Shares whitepaper: "Share tokens are like the asset side of a central bank's balance sheet. The market capitalisation of shares at any point in time fixes the upper limit on how much the coin supply can be reduced." Likewise, the Frax protocol takes inspiration from Sams' proposal as Frax is a hybrid (fractional) seigniorage shares model system.

4.1 FXS Distribution and Incentivization

FXS must be dispersed widely so that there is a diverse initial distribution as future governance actions are decided by FXS holders. Additionally, at genesis, there is low utility and reason to use FRAX as money compared to its underlying collateral (stablecoins with more traction). For these two reasons, an initial supply of FXS tokens are paid out to FRAX minters who stake their FRAX in a separate staking contract that is available for a period of time until distribution of FXS tokens end. This system acts as a sort of interest payment to early adopters. This can be thought of as the FRAX stablecoin acting as 'interest-bearing' currency to incentivize its own adoption for a period of time until it reaches sufficient critical mass of volume, usage, and velocity. Because there is no initial coin offering or fundraising event, this staking program (modeled after 'liquidity mining' and 'yield farming' DeFi programs) is the main way to attain FXS tokens.

Additionally, the staking rewards program will incentivize FRAX liquidity providers on the Uniswap protocol. Users can provide liquidity to the FRAX:ETH Uniswap pool and stake their LP tokens in the staking contract to obtain FXS rewards allotted for

FRAX Uniswap LPs. As adoption increases, FXS rewards can be channeled to other decentralized finance services that FRAX users demand such as Aave or Compound.

4.2 Governance

FXS holders also take part in governance including (but not limited to): system upgrades, forks, setting global system parameters such as voting on price feed oracles, and how to utilize the collateral assets within the reserve. Governance actions are temporary proposals that require a quorum (minimum amount of approvals) to be reached in a given timeframe.

The protocol requires the price of FRAX, FXS, and collateral to run essential processes. In the initial version of the protocol, FXS holders vote for price oracles similar to other stablecoin designs. In future system upgrades, the price of FRAX and FXS can be obtained through on-chain transactions such as Uniswap pools and decentralized exchanges. Additionally, a future protocol upgrade would remove the requirement for the collateral price feed entirely by making the FRAX minting process an auction. In such a system, only the USD price of FRAX and FXS would be necessary which could be easily retrieved from the averaging of stablecoin pairs on-chain.

Lastly, should the protocol gain sufficient worldwide adoption and critical mass, FXS holders can create a "Frax Standard" and de-peg from USD. FXS holders would have the sole discretion of when and what reference price to follow when transitioning away from USD.

5 Frax Pools

A Frax Pool is the smart contract that mints FRAX tokens to users for placing collateral or returns collateral by redeeming FRAX sent into the contract. Each Frax Pool has a different type of accepted collateral. Frax Pools can be in any kind of cryptocurrency, but stablecoins are easiest to implement due to their small fluctuations in price. Frax is designed to accept any type of cryptocurrency as collateral, but low volatility pools are preferred at inception since they do not change the collateral ratio erratically. There are promising new projects, such as Reflex Bonds, which dampen the volatility of their underlying crypto assets. Reflex Bonds could make for ideal FRAX collateral in the future. New Frax Pools can be added through FXS governance votes.

Each pool contract has a pool ceiling (the maximum allowable collateral that can be stored to mint FRAX) and a price feed for the asset. The initial Frax Pool at genesis will be USDT (Tether) due to its large market capitalization, stability, and availability on Ethereum. The protocol plans to support BUSD, sUSD, USDC, and Dai in the future.

5.1 Utilizing Frax Pool Assets for Protocol Revenue

Since Frax Pools hold crypto assets that can be put to work earning interest, liquidity fees, and yield farming rewards, future updates of the Frax Pool contract can auto-deposit collateral in whitelisted DeFi protocols to earn revenue for the Frax Protocol. Due to the unique risk profile each kind of activity brings, the original Frax Pool design does not utilize any revenue generating service. Upgraded Frax Pools can be deployed at a future date that deposit their underlying collateral into these services and accrue revenue for the system. It is up to FXS holders to vote for new Frax Pools that make use of DeFi protocols such as Curve.fi, Uniswap, Aave, Compound etc. These modified pool contracts must also guarantee that their associated cTokens, LP tokens, etc are redeemable for FRAX at the same collateral ratio of the Frax Protocol.

6 Conclusion

The Frax Protocol is a blockchain-agnostic stablecoin protocol which starts off fully collateralized, but then transitions to a fully algorithmic design as it matures. This unique design allows FRAX to move through a fractional phase where it is only partially backed with collateral and price-stabilized through supply changes. The Frax Protocol can be deployed to multiple networks as long as both FRAX and FXS remain fungible. Since multiple types of collateral can be accepted, it is not required that the collateral be available on all networks that the protocol operates on. While the Frax Protocol is only slated for release on Ethereum, we are working to bring the technology to other leading networks with sufficient decentralized finance demand. Furthermore, a simpler cross-chain implementation would be to have Frax Pools and minting contracts only deployed to one or two main chains where collateral is located (and FXS is issued) and make FRAX stablecoins swappable between many more diverse networks. This would allow FRAX to be the unified stablecoin across many ecosystems without needing any of the actual monetary policy to reside on every chain. This approach is much simpler and the initial starting point for cross-chain FRAX.

The Frax Protocol is intended to be a fully autonomous system that has minimal need for human intervention and governance outside of protocol upgrades. It takes a minimalist-governance approach to decentralization similar to Bitcoin rather than a governance-heavy approach such as MakerDAO's frequent monetary policy changes. The protocol is designed to be completely self-sustaining and autonomous with a concerted timeline to phase out trusted-oracle feeds entirely. This would allow the protocol to exist in a self-contained manner in all aspects. Such a design is tantamount for the aim of becoming a global, decentralized currency. For the Frax Protocol to be truly successful, it must become the most censorship resistant and permissionless stablecoin to ever exist, otherwise it would not deliver its unique value proposition that its unique design allows for.

Lastly, further algorithmic stability mechanisms can be built on Frax's "base layer" such as bond issuance, debt based monetary policy, and bi-directional interest rates. The Frax Protocol can also "wrap" other stablecoins to compliment other stability mechanisms. In this way, the protocol is highly utilitarian and flexible. For example, Dai is a likely candidate for an early Frax Pool and thus can be 'wrapped' over with Frax's algorithmic stability mechanism on top of its crypto-collateralized base design. Frax is intended to provide a completely decentralized, zero-trust base (or second) layer for building additional stability on top of the underlying collateral.

7 Glossary

Algorithmic Ratio (AR): The algorithmic ratio is always the inverse of the collateral ratio (1 - CR). The AR denotes the percent of each FRAX token that is redeemable for FXS. For example, an algorithmic ratio of 3% means that each FRAX is redeemable for $.03 of FXS and $.97 of collateral (the same as the above example).

Collateral Ratio (CR): A global percent value denoting what percent of each FRAX token is backed (redeemable) by collateral. For example, a 97% collateral ratio means that each FRAX is redeemable for $.97 of collateral and $.03 of FXS.

Decollateralization: The process of moving FRAX to become more fractional by shifting the collateralization rate of the network as long as FRAX is above $1.

Frax: The fractional-algorithmic stablecoin protocol.

FRAX: The stablecoin in the Frax protocol.

FXS: The share token within the Frax protocol.

Market Price: The market price is the actual aggregate open price of assets (ie: FRAX, FXS, and collateral etc) on global markets.

Monetary Premium: The portion of FRAX's value attributed to its utility as money. This is a specific type of demand that is separate and different from speculative.

Pool ceiling: The limit of a particular type of collateral that can be held in the protocol denominated in USD value. For example, a pool ceiling of $10m in the USDT pool denotes that a maximum of $10m worth of USDT can be used to mint FRAX. Pool ceilings can be changed by FXS governance votes.

Quorum: The amount of votes necessary for FXS holders to pass a decision on governance.

Recollateralization: The process of moving FRAX to become less fractional (inverse of hop) by shifting the collateralization rate of the network by the unit of one step.

Redemption fee: A small fee paid to the system during the redemption process. The fee is set to .04% of the amount of FRAX sent to be redeemed. The fee can be adjusted by an FXS governance vote.