Geminon: a protocol for super stable cryptocurrencies

Heirs of Satoshi

geminon.fi

First version: April 08, 2022

This version: June 2, 2022

***Abstract*—Since the inception of Bitcoin in 2008, it has attracted increasing attention and adoption as a store of value asset. However, its huge volatility makes its use as a currency still impractical 12 years later. This has led to the creation of so-called stablecoins, designed to maintain peg with some fiat currency, usually the US Dollar. Although this solves the problem of short-term volatility, it defeats the very basic purpose behind Bitcoin's creation: using a decentralized, trustless, sound money that cannot be devaluated by the government.**

In this paper, we propose a protocol for a fully algorithmic and decentralized super stable cryptocurrency that keeps a constant value relative to the prices of consumer goods in the economy rather than relative to an inflationary fiat currency. To the best of our knowledge it is the first of its kind.

I. Introduction

Bitcoin was created as an electronic payment system based on cryptographic proof to allow people to transact directly with each other without the need for a trusted third party (Nakamoto, 2008). Its economic design, with a total supply limited to 21 million bitcoins, makes it a good store of value asset for the long term. This supply is released in a locally linear manner through rewards paid to miners for each block of transactions generated, every ten minutes on average, and said reward is reduced by half every four years approximately, in the event known as “halving”, giving rise to a long-run supply curve that approximates a logarithmic one.

The fact that the money supply of bitcoin is fixed in advance makes it relatively inelastic to demand, so any variation in said demand means that the adjustment between the two must necessarily be carried out through a variation in price. This in turn causes market expectations of future price, which are the main driver of demand, to change rapidly, amplifying changes in demand and creating a vicious circle that leads to sharp price swings (volatility). It is now commonly accepted that bitcoin has been established more as a digital gold than as good money or currency (Ametrano, 2014).

This volatility due to the rigidity of the money supply is a characteristic that practically all the cryptocurrencies created in the wake of bitcoin have inherited. Although some argue that with mass adoption said volatility would decrease, to date this statement has not been fulfilled and the application of the law of supply and demand in this case indicates that it is very unlikely that cryptocurrencies that follow the same Bitcoin's inelastic monetary policy achieve price stability only close to that of fiat currencies.

Mastercoin (2012, 2013) was the first project to propose the idea of a cryptocurrency that would replicate the price of another asset, specifically gold, using a purely algorithmic mechanism that consisted of using two tokens: one stable with variable supply and another that absorbed the volatility of the former and allowed investors to obtain profits from the minting of stable tokens (seigniorage). In addition to this, they proposed many other ideas such as the use of a second layer on top of Bitcoin, an oracle protocol to bring external price data to the blockchain or the use of a monetary reserve as collateral for the stable currency issued for its use in emergency situations. Although the Mastercoin protocol was not successful, all these ideas have been applied later by other protocols and are a key part of the cryptocurrency ecosystem today.

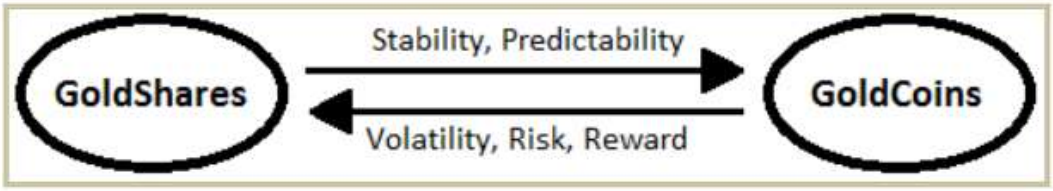

Figure 1: algorithmic stability mechanism proposed by Mastercoin (2012)

The first stablecoin to achieve mass adoption was Tether's USDT (2014). Initially designed to work using a layer 2 solution on top of the Bitcoin blockchain, it was not until the appearance of smart contracts on the Ethereum network and the first decentralized exchanges (Uniswap, 2018) that its widespread adoption began. Despite the great success achieved, becoming at times in 2020 the second largest cryptocurrency only behind Bitcoin, it cannot be accepted as a real solution to the problem at hand, but rather as a patch. The reason is that Tether is a centralized company that claims to support its 1:1 token issuances with dollar reserves, which adds to the already existing problems of fiat money (dependence on centralized entities, need for trust in third parties, constant loss of purchasing power, censorship and confiscation), some of which are typical of cryptocurrencies such as bitcoin (lack of privacy, high transaction costs and difficulty of use).

This lack of solutions that are sufficiently stable in price and at the same time preserve purchasing power over time, forces users of cryptocurrencies to try to achieve that balance themselves through speculation, trying to guess what combination of crypto assets and stablecoins will give them the desired risk/reward ratio. However, it is known that the majority of private investors are unable to align themselves adequately with market cycles, which leads many to even make losses with respect to reference risk-free assets, such as a traditional bank deposit.

One of the first alternatives to fiat-backed centralized stablecoins was proposed by Ametrano (2014) and named by him “Hayek Money” after the Austrian School economist and 1974 Nobel Prize winner Friedrich A. Hayek. Ametrano proposes a coin with a constant value and perfectly elastic supply compared to demand, using a rebase mechanism: to always keep the value of the coin constant against a reference index, the amount of coin in each wallet would be directly modified, effectively affecting the amount of currency in circulation. The price could thus be set arbitrarily to be equal to that of a fiat currency, an index of consumer prices, or a basket of commodities as Hayek originally proposed.

The problem with the rebase system proposed by Ametrano is that it only stabilizes the price of the coin, not the purchasing power of the wallet. Price stability is not only about stabilizing the unit of account of money, but also its store of value (Sams, 2014). In order to stabilize both, Sams (2014) proposes dividing the currency into two types: currency that acts as money and currency that acts as shares in the seigniorage system, which he calls coins and shares, respectively. To stabilize the value of the coins, Sams proposes a supply variation mechanism, according to the following scheme:

- When the supply of currency needs to be increased (to reduce its price when it is above its peg), currency is distributed to shareholders in exchange for a certain percentage of shares, which are destroyed. The supply of currency increases and the supply of shares decreases (increasing the price of these).
- When the coin supply needs to be increased (to increase its price when it is below its peg), shares are distributed to coin holders in exchange for a certain percentage of coins, which are destroyed. The supply of currency decreases and the supply of shares increases (decreasing the price of these).

This two-component system, a stable coin and seigniorage shares that absorb volatility, is similar to the one proposed by MasterCoin (2012, 2013). Another variant of the dual system of shares and currency was proposed by Lee (2014) in the Nu protocol, in which shares (Nushares) were used both to validate the network with a proof-of-stake algorithm and to vote on the network currency issuance (Nubits).

The novelties incorporated by Sams (2014) regarding these protocols were, on the one hand, the use of a periodic auction mechanism to stabilize the currency, in which the protocol calculated the variation in supply necessary to return it to its peg and the holders of shares would bid how many shares they were willing to swap for that amount of currency. The other proposal introduced was to peg the value of the currency to a consumer goods price index instead of another fiat currency.

Another attempt to create an algorithmic stablecoin came from Bitshares (Larimer et al., 2014), which also used a system made up of two currencies (Bitshares / BitUSD), although with an operating principle based on a derivative contract. The stability mechanism was that if BitUSD traded below its $1 peg, traders would buy it at the market, and if it traded above $1 they would go short staking BitShares 30 days as a guarantee (collateral) to issue new units of BitUSD that would be sold on the market, increasing the money supply to lower the price and restore the peg.

Basis protocol (Al Naji et al., 2018) introduced an innovative algorithmic system based on the use of three tokens: shares, stablecoin and bonds. The proposed system worked like this:

- When the stablecoin is above its target price and it was necessary to reduce the supply, the system started an auction of bonds that could only be bought by paying with the stablecoin.
- When the stablecoin is below its peg and it is necessary to increase the supply, the system would issue new stable currency that was used to repurchase the issued bonds (if any), paying the corresponding return to their holders, and in case it was still necessary to issue more stablecoin after liquidating all the bonds, it was delivered as a prorated dividend to the holders of the shares (seigniorage).

In addition to its innovative algorithmic system, Basis also proposed the idea that the stablecoin would converge to the CPI value instead of the dollar in the future, in case of mass adoption. Unfortunately, the project never saw the light of day due to regulatory pressure from the SEC in the US, which forced it to close and return the more than $100 million raised by the largest venture capital funds of the time.

The main obstacle for the implementation of a currency referenced to a price index consisted in the incorporation of said information to the blockchain in a reliable and cryptographically verifiable way. The lack of such a mechanism may have been the reason why this idea was initially abandoned. This problem was solved with the arrival of the first oracles (Chainlink (Ellis et al., 2017), Band Protocol (2020), Berry

Data (2021), API3 (2021)) that allowed the connection from external data sources to the blockchain and decentralized verification of said data.

Despite the fact that the idea of a stable currency tied to the price index was proposed almost a decade ago by Sams (2014) and the technical feasibility of its implementation since the appearance of the first oracles in 2017, until very recently no project has proposed its implementation, even though it is an obvious problem within the crypto ecosystem, being the existing ones constrained to the creation of stablecoins pegged to fiat currencies such as the US dollar. For this reason, in this paper we propose a feasible solution to put this idea into practice, implementing a protocol composed of a set of currencies: a collateralized currency with fixed supply and variable price that absorbs volatility, and super-stable currencies with flexible supply and value linked to an index of prices of goods in an economy.

The rest of the document is organized as follows: First, we look at the different types of stablecoins that exist. Next, we review the main protocols that exist in the market, emphasizing their advantages and disadvantages. Finally, we present our solution, as well as the possible extensions of the protocol.

II. TYPES OF STABLECOIN PROTOCOLS

In recent years, stablecoins have been the subject of various academic studies, and various taxonomies have been proposed based on the type of collateral used, peg target, and technological mechanism (Mundt et al, 2020).

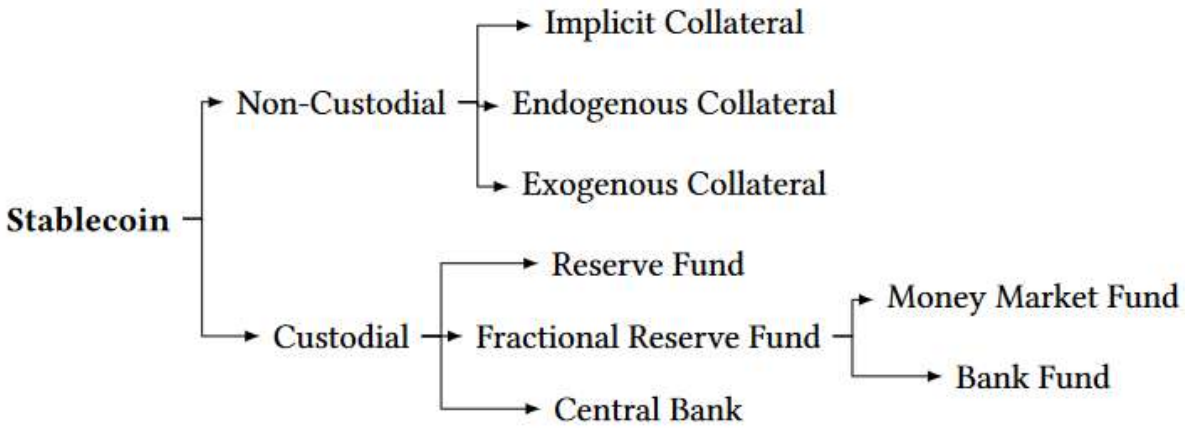

Figure 2: overview of the stablecoin design space. (Mundt et al. 2020)

In this document, we will carry out the classification based on the level of decentralization provided by the custody system and the composition of the collateral in combination.

A. Fiat backed stablecoins

The easiest way to implement a stablecoin is to make it pegged to an existing fiat currency, and issue one unit of the crypto asset for every unit of fiat currency received. This ensures that the currency will keep its peg as long as its users maintain confidence that the issuer actually holds the cash backing it in a 1:1 ratio. The problem with this approach is that it requires trust in a centralized issuer, which goes against the very founding principle of cryptocurrencies: build a system for decentralized money transfers, trustless and permissionless.

The most widely used stablecoins currently fall into this category: Tether (USDT), Circle USD Coin (USDC) and Binance USD (BUSD) issued by Paxos (not Binance as many people believe). Other such protocols are TrueUSD (TUSD), Pax Dollar (USDP), Gemini Dollar (GUSD), Euro Tether (EURT), Hot USD (HUSD) issued by Stable Universal Limited, a company based in the Virgin Islands, STASIS EURO (EURS) issued by STASIS based in the Isle of Man and USDK issued by the OKEx exchange.

All coins in this category without exception implement a 'blacklist' function in the smart contract of their token that allows blocking funds from any address, be it a wallet or a smart contract, preventing the tokens they contain from being transferred. As these tokens represent an amount of fiat currency deposited in centralized entities, the balance represented by the tokens can also be confiscated.

Precisely due to their wide adoption, this type of stablecoin represents serious risks in the medium term for the survival of decentralized finance as we know it today for several reasons:

- Arbitrary censorship. As already explained, all the centralized stablecoin protocols out there have built in the code of their tokens methods that allow them to block any address at their discretion. This means that in practice there is no difference between keeping that money in a traditional bank, in a centralized exchange or in a cold wallet, since in no case is there full custody of the coins.
- Regulations. Cryptocurrencies get their amazing resilience from their decentralization. This property, however, does not hold for centralized coins. Any authority that wanted to attack cryptocurrencies as a whole, any protocol or set of individuals using these currencies could easily do so. In addition, the victims of these attacks would have difficulty defending themselves, due to the large legal loopholes that exist in relation to cryptoassets in much of the world.
- Lack of solvency of the issuer. Despite the fact that in theory the entity that issues the coins keeps a 1:1 reserve in cash to back them, in practice it is not clear that this statement is 100% true. Assuming that we trust that the issuer is not committing fraud and that it actually holds those reserves, the question of the quality and liquidity of those reserves would still have to be resolved. The case of Tether is paradigmatic, which has been receiving public accusations for years of having used USDT reserves for high-risk investments such as low-rated bonds and even that the liquid reserves did not cover 100% of the issues, to the point that Since 2018, the company has been facing an investigation by the US Department of Justice for alleged fraud.
- Systemic risk. Currently, more than 80% of the stablecoins in circulation, which in turn have accounted for between 5% and 10% of the total cryptocurrency market capitalization in 2021, are centralized directly or indirectly (via collateral). Stablecoins are also a key part of all decentralized finance protocols that operate on smart contract blockchains and even all associated centralized exchanges and futures markets, where USDT is the most widely used currency for the settlement. This, together with the risks listed above, currently makes these centralized currencies a time bomb that threatens the entire cryptocurrency market. Whether due to fraud, legal action or crack down by governments, the effect of the fall of a large issuer like Tether could trigger a real Armageddon in the cryptocurrency market as a whole.

The risks exposed make it a priority to develop fully decentralized, trustworthy, self-custodial and censorship resistant stablecoin solutions that can replace centralized solutions.

B. Currencies based on collateralized debt

1) Fully collateralized

In an attempt to solve the main drawbacks of centralized fiat-backed stablecoins, another ancient invention of the traditional banking system was turned to: debt-money. The first protocol to successfully implement this system was DAI (Maker Dao, 2017). In this type of protocol, the user takes a stablecoin loan by depositing a guarantee in the form of cryptocurrencies (the collateral). Given the great volatility of

cryptocurrencies, the initial value of this guarantee far exceeds that of the loan granted (overcollateralization), with the usual collateral/debt ratio being between 1.6:1 and 2:1. Given the inefficiency in the use of capital that this entails, the collateral has ended up consisting mostly of other stablecoins, and since the most used are the centralized ones, they have ended up taking over the asset balances of these protocols that were initially intended to be decentralized.

Figure 2: DAI generated by collateral (daistats.com)

DAI has long been the largest decentralized stablecoin protocol (only recently surpassed by Terra's UST, although the latter belongs to the category of purely algorithmic coins). Given its relative success, a large number of protocols with the same operating principle have recently appeared. In order of market capitalization at the time of writing this paper, we find: Magic Internet Money (MIM, 2021), Liquity USD (LUSD, 2021), Fei USD (FEI, 2021), MAI (MIMATIC, 2021), Alchemix USD (ALUSD, 2021), synthetix USD (SUSD, 2019), Origin Dollar (OUSD, 2020), Flex USD (FLEXUSD, 2021), USDX (2020), Celo Dollar (CUSD, 2021), mStable USD (mUSD, 2020) and VAI (2021), the latter with major problems keeping its peg with the dollar.

All of these protocols have very similar operating principles in terms of the mechanism for issuing currency from collateral. The differences are found in the types of collateral accepted, the settlement mechanism, the interest charged for the loan and the incorporation of profit generation strategies using synergies with other decentralized finance protocols (yield farming). In this aspect, protocols such as Origin Dollar (OUSD, 2020) and mStable USD (mUSD, 2020) can be highlighted, which only accept other stable currencies as collateral in a 1:1 ratio and invest this collateral in other protocols, which allows only not to charge interest on the issued loan, but to pay interest to the holders.

In general, all the protocols in this category have ended up resorting, to a greater or lesser extent, to the use of other stable currencies as collateral, and since the most used are centralized, the end result has paradoxically been that the protocols initially created to provide an alternative purely decentralized stablecoins have ended up relying on these.

The fact that all the currencies in this category are collateralized, partially or totally in some cases, with centralized currencies only increases the systemic risks of the centralized entities that we discussed in the previous point. In the case of these protocols, the existence of smart contracts that concentrate large amounts of confiscable currency makes them easy prey for any government that wishes to appropriate said assets, with the consequent cascade of liquidations and massive losses produced for users.

2) Partially collateralized

The main criticism received by overcollateralized protocols is that they are inefficient from the point of view of leveraging capital. This has led to the appearance of hybrid protocols, which combine the use of a high percentage of collateral with a two-token system such as the one proposed by Mastercoin (2012, 2013) to complement the collateral deficit.

FRAX only uses other stablecoins as collateral, both centralized and collateralized (which, as we have already seen, turn out to be also mostly dependent on the centralized ones).

Sperax (2021) is a copy of FRAX that employs the exact same fractional reserve model using a basket of stablecoins as collateral, consisting solely of USDT and USDC at this time, making it an even more centralized alternative to the project that it copies.

These coins could also be considered as a particular case of collateralized coins, in which the composition of the collateral also includes the protocol token itself.

C. Algorithmic stablecoins

1) Rebase tokens

The coins in this category follow the approach proposed by Ametrano (2014), of keeping the price constant and varying the number of coins held by holders (rebase). Few protocols have dared to implement this type of solution, without a doubt the best known is Ampleforth (Kuo and Iles, 2018).

More recently, Olympus DAO (OHM, 2021) created a highly successful project based on the rebase idea, but adding collateralization (via DAI and Frax) and game theory elements in the economic incentive design of the protocol. This design rewarded high incentives for staking the OHM token, so that they received both the interest for depositing the tokens and all the new supply of tokens created to try and return the coin to its parity of $1. However, given the large interest they received for the deposit, this new supply was not released on the market, which created a vicious circle of demand -> price increase -> reward increase that placed the annual interest for depositing OHM above 1000%. This project has generated enormous controversy, being accused by many of being a Ponzi scheme, although this point is still the subject of debate.

2) Seigniorage shares

In this category are the protocols that use the dual system of shares / currency proposed by Mastercoin (2012, 2013). It is interesting to note that this system is basically equivalent to collateralization, with the only difference that in this case a self-created token is used as collateral instead of different ones. In fact, all the stablecoin categories described, with the exception of rebase tokens, could be grouped under a single category of collateralized coins in which only the composition, centralization and redemption mechanism of said collateral varies.

The first protocol in this category that achieved mass adoption was Terra (Kereiakes et al., 2019) with the UST. Haven Protocol (2018) and Terra were the first two projects to successfully implement a purely algorithmic stablecoin system. In the next point we analyze in detail the characteristics of these protocols.

3) Shares combined with bonds

The latest variant of algorithmic stablecoins is made up of three-token systems that follow the model devised for the Basis protocol in 2018.

Neutrino (Ivanov & Pupyshev, 2020) was the first protocol to bring back the idea of a three-token mixed stabilization system for its USDN using the WAVES protocol currency as collateral and the NSBT token as a bond that is issued when the collateral value is below the value of the issued USDN, or when the USDN is

below its peg. In recent months it has had major problems maintaining the peg, systematically trading below its target.

Empty Set Dollar (2020) tried to replicate the same mechanism proposed by Basis. The ESD price failed to hold steady at $1, and the protocol ended up crashing shortly after its launch. The same fate befell Dynamic Set Dollar (2020), a copy of ESD released almost at the same time.

Beanstalk (Publius, 2021) has been the latest project to use a complex algorithmic system based on debt issuance to keep the price of the BEAN stable. The proposed system was able to achieve price stability after 4 months of strong initial swings, but ended up collapsing due to a vulnerability in the smart contracts that allowed a flash loan attack to steal all the funds from the protocol.

III. EXISTING PROTOCOLS WITH SEIGNIORAGE MECHANISM

Various attempts have been made to implement the idea of a dual system with seigniorage shares to stabilize a currency. Almost all attempts to implement algorithmic currencies without using exogenous collateral have failed, although recently some protocols have had some success creating such stablecoins. At this point we analyze some of these recent projects.

A. Haven protocol

Haven (XHV) is a Monero fork that inherits all the privacy features of the latter. It extends that functionality by providing private, anonymous, synthetic currencies and commodities (xAssets) which can only exist through the "burning" of the Haven base currency (Haven Protocol, 2018).

The first synthetic asset added to the protocol was the xUSD (Haven Dollar), a private stablecoin pegged to the US Dollar whose transactions cannot be traced. The premise of the protocol is that 1 xUSD will always be redeemable for 1$ worth of XHV.

Being Monero the safest cryptocurrency that exists, Haven is an excellent project on a technical level as it derives directly from the first. However, the lack of interoperability with other blockchains and centralized exchanges in which to operate with the asset has been a significant brake on its adoption, relegating it to a marginal role in the market. Another disadvantage of the project is the exclusive use of stable currencies paired with fiat money, with the drawbacks for the long-term store of value that this entails due to their constant devaluation.

Due to the low adoption and liquidity of the protocol, the price on the few external sites where xUSD is listed fluctuates wildly. During the Terra crash, xUSD took a hit trading as low as $0.90, though it was later able to regain peg.

B. Terra money

The Terra protocol (Kereiakes et al., 2019) appeared around the same time as Haven (2018). The principle of operation of both is the same. In the case of Terra, the LUNA token performs the functions of shares that can always be exchanged for the equivalent amount of UST stablecoin at the price of $1. The main difference between the two is that Terra does not have any privacy features, unlike Haven which is derived from Monero.

The Terra protocol completely collapsed during the days of May 9-13, 2022, in a domino effect characteristic of the failure of algorithmic stablecoins called "death spiral", and that had been warned by some analysts in the previous months, producing the definitive loss of the peg of the UST and the fall of the Luna price to practically $0, even having to stop the blockchain due to the risk of attacks as it used a Proof of Stake algorithm for validation.

One point that at the time raised many questions about the stability of the Terra protocol was the question of the maximum supply of LUNA, which was theoretically 1 billion tokens. Let us imagine a situation in which said supply limit has been reached, and therefore the protocol prevents the creation of more LUNA tokens. In such a situation, if the total market value of LUNA tokens fell below the total market value of the basket of stablecoins it backs, it would not be mathematically possible for all holders of such coins to redeem them at peg value, which would mean the collapse of the protocol and the loss of currency peg. In fact, the LUNA market value threshold at which this situation would be possible was much closer because not all of the circulating supply was available to the market module. This posed a dichotomy:

- Either there were market conditions in which the protocol could not keep its promise to allow the redemption of $1 of UST for $1 of LUNA, so said promise was false,
- Or really LUNA did not have a maximum supply, in which case the investors were operating under a false premise (limited supply).

During the collapse of the protocol, it was found that the correct answer was the latter, because when the panic among investors was triggered and the total market value of Luna fell below that of UST, the protocol began to mint trillions of Luna tokens, creating a hyperinflationary spiral that brought the price of the token to practically zero.

The cause of Luna's collapse was a poor implementation of the market module, which was the heart of the protocol since it was the point where the promise that "you could always redeem $1 of UST for $1 of Luna" had to become effective, and therefore it was the point from which the arbitrage was born that allowed parity to be preserved in the rest of the exchanges. This module had several major design flaws:

- It was designed as a constant product liquidity pool, derived from those used in Uniswap, which was totally inadequate to maintain a price stability mechanism since any imbalance in the liquidity of the pool (such as that which would occur during a panic market) could cause it to stop working properly, introducing a large slippage in the UST reference value as it eventually did.
- The developers introduced limitations on the daily volume of stablecoin that could be redeemed in the market module, introducing a variable fee with the aim of deterring large UST outflows. This, however, had an unforeseen effect by affecting the effective redemption price, and it is that the arbitrage target value that determined the price of UST in the market was systematically set below the theoretical value of $1 if that daily limit was exceeded, as it did when the crash started, making it impossible for the stablecoin to recover the peg quickly, causing alarm and ultimately panic in the market.

The combination of these two design flaws created a vicious cycle, whereby as the UST stayed below its target value longer, more investors panicked selling, and these sales increased both the slippage and the fees of the market module, setting an effective arbitrage price of the system even further away from the peg. This inherently unstable design of the system was the ultimate cause of a "death spiral" that eventually collapsed the protocol completely.

C. Frax

Frax (2021) has been defined by its creators as the first and only stablecoin protocol that combines a fractional (collateral) reserve system with an algorithmic system.

The operating principle of the Frax protocol is identical to that used by Haven and Terra, which was proposed by Mastercoin (2012, 2013) and Sams (2014), with the only difference that when issuing or redeeming the stable currency, they don’t exclusively use the shares of the protocol (Frax Shares, FXS) but rather a combination in variable proportion of these and a collateral made up of other stable currencies.

The stablecoins that make up the Frax collateral are USDC, USDP, sUSD, DAI, FEI and LUSD, which, as has been seen, are centralized or are made up of a mostly centralized collateral. According to Frax's own estimates, the degree of centralization of its collateral would be close to 70% today.

Frax announced earlier this year their intention to craft a currency that tracks the US inflation index (CPI) in the future, around the same time the Geminon project was created, and they have recently launched the FPI token for this purpose.

D. Deus Finance

Deus is a digital derivatives architecture that provides the infrastructure for others to build any type of financial instrument: synthetic shares, CFDs, options, prediction markets, OTC derivatives, and futures. Within this architecture, the DEI token performs the function of a stablecoin used as a means of settlement of derivatives. Also, thanks to a very efficient cross-chain bridging mechanism, DEI is a good alternative as a general-purpose stablecoin on its own.

The DEI stability mechanism is identical to the one used by Frax, consisting of a fractional reserve system in which a percentage of the stablecoin's value is supported by collateral made up of other stablecoins, and the rest by the DEUS token itself, for what all the criticisms we have made for Frax remain for Deus: indirect dependence on centralized entities, systemic risk and risk of censorship.

Recently, after the collapse of Terra, DEI has lost peg to the dollar and is having quite a bit of trouble getting it back.

IV. GEMINON PROTOCOL

Geminon was initially conceived as a primarily algorithmic protocol, with a design midway between Frax and Terra. However, the recent collapse of the latter made it advisable to rethink the design of the protocol, placing it now squarely in the same category as Frax. However, the Geminon protocol is not similar to Frax, but rather an antagonist:

	FRAX	GEMINON
Collateral type	Stablecoins	Variable assets
Colateral source	Mostly centralized	Mostly decentralized
Collateral level	Predetermined	Variable
Collateral applied to	Stablecoin	Protocol token
Protocol token issuing	Discretionary	Collateral mining
Protocol focus	USD fiat currency	USD and EUR Inflation indexes

In addition to these differences, the Geminon protocol incorporates important novelties, such as the use of tokenized gold as a reserve asset, the provision of collateral as protocol liquidity, collateral mining and the use of new pools with advanced automatic market maker (AMM) algorithms.

Below we detail the main characteristics of the protocol.

A. Genesis Liquidity Pool (GLP)

Based on Balancer's Liquidity Bootstrapping Pool (LBP) concept (Martinelli & Mushegian, 2019), we have created our own smart pool design that enables parametric AMM strategies. Thanks to this design we obtain the required flexibility in the protocol's collateral pools to make possible certain features of the protocol that would not be possible using a normal liquidity pool:

- Possibility of creating a pool from scratch, with only one of the two tokens. This allows the launch of projects without initial liquidity, something that was not possible until now.
- Additionally, it is also possible to define an initial supply tranche of a token at a constant price, which allows an IDO (Initial DEX Offering) to be carried out autonomously.
- Issuance / burning of tokens from the pool, enabling features such as liquidity mining and control of the pool invariant and thus the price response curve.
- Provision of liquidity for the redemption of stablecoin, ensuring that these always have 100% outgoing liquidity and there are never situations of blockage or loss of parity due to lack of liquidity in the stablecoin pool.
- Loans from the pool, enabling the collateral asset loan option, which is discussed in more detail in the following points.
- Automatic collateral rebalancing, allowing you to modify the desired weight of each asset that makes up the collateral with a smooth transition between states.
- Personalized management of commissions generated by the pool.

Among all the features that the GLP allows to implement, the most important for Geminon is probably the ability to dynamically alter the price response curve of the GEX token by varying the supply of tokens in the pool.

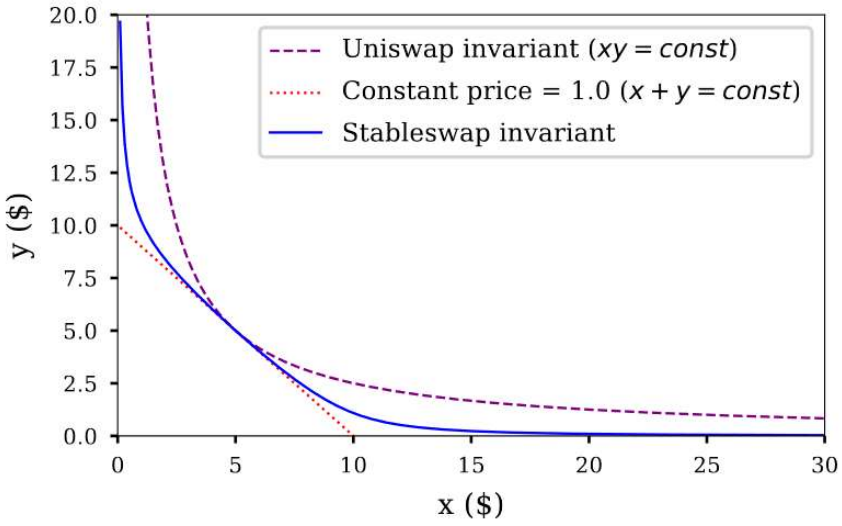

Figure 4: Comparison of Curve and Uniswap invariants (Egorov, 2019)

In a constant product pool, such as those used by Uniswap and practically all existing DEXs, the price of a token is a quadratic function of the amount of the second token with which it forms the pool:

$$Q_x Q_y = K$$

$$P_x = \frac{Q_y}{Q_x} = \frac{Q_y^2}{K}$$

This causes the price to behave exponentially in the face of linear variations of the collateral deposited in the pool, this behavior being especially pronounced when the balance of the token in the pool is excessively reduced.

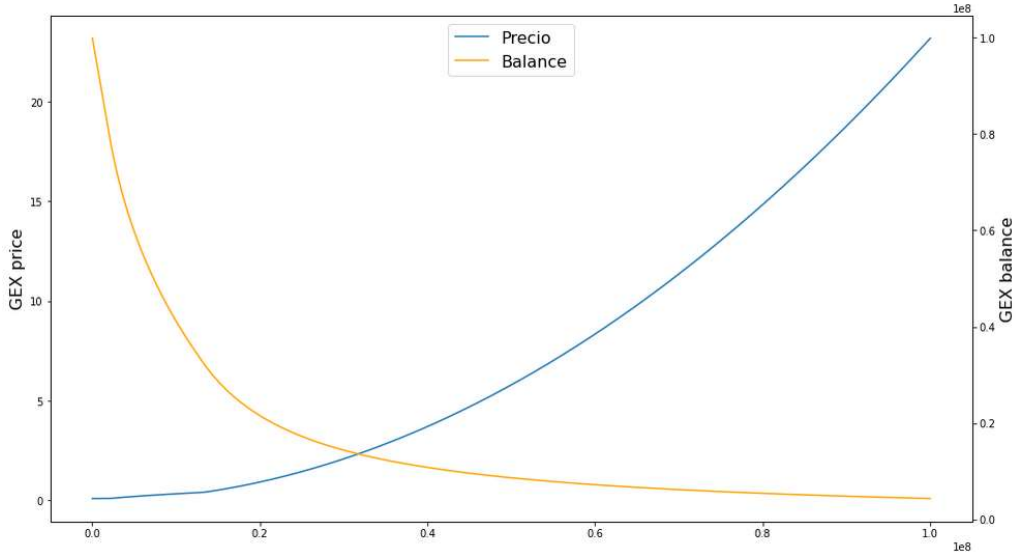

Figure 5: Simulation of GEX token price based on pool balance

The simulations carried out with the smart contract show that during the growth stage in the adoption of the protocol, when the amount of stablecoin issued is multiplied by 10, and with it the collateral deposited in the pool, the price of the GEX token is multiplied by 100. Although this behavior may seem desirable at first, since it generates significant profits for the holders of the protocol token, it should be noted that it also works in reverse: falls in the amount of collateral deposited imply greater falls in the price of the token. This "leverage" that occurs in a constant product pool is a consequence of having a supply that is totally inelastic to demand, that is, a fixed balance.

The ability of GLP to issue and burn tokens makes it possible to make supply elastic, which implies smoother variations in price in response to changes in demand. In the mature stage of the protocol, the coefficient of mint and burning of tokens in the collateral pools can be dynamically varied, being able to achieve a linear and even damped response of the price to changes in the collateral level, thus achieving compliance the protocol's promise of lower volatility than the underlying assets. This is an approximation that produces results equivalent to Curve's liquidity concentration proposal (Egorov, 2021), although using a different method.

B. Stablecoin mint

The main purpose of the Geminon protocol is the issuance of superstable currencies, which are those that present stability against the prices of goods in an economy instead of against an inflationary fiat currency.

The issuance mechanism is algorithmic, being necessary to deposit the same value in GEX tokens that is intended to be issued in stable currency, and vice versa. The price of the stablecoin is determined from the data obtained by the inflation index (CPI) oracle associated with the coin in question. The target value is obtained predictively, so that the currency discounts the current period's inflation expectations in real time instead of lagging one period as is the case with the Frax FPI.

The Geminon stablecoin mint module is designed in such a way that an event like the one on Terra is not possible:

- The fees charged by the protocol for the issuance/redemption of stable coins are fixed, so that they do not affect the effective arbitration price and do not contribute to deviating the currency from its parity value.
- The module is not a liquidity pool, but a token mint and burning mechanism with infinite liquidity, and therefore operates without slippage, which guarantees efficient arbitrage in all market circumstances. In the event that the GEX token balance of the contract is depleted, it can take it from the GLP balance in small increments, causing the price of the token to rise in response to the relative scarcity of this one. Although counterintuitive, a massive redemption of stablecoin in the protocol could, under certain conditions, lead to an instant rise in the price of the GEX token instead of a fall. In this case, the characteristic of the constant product curve of the liquidity pools would be used, which makes it impossible to deplete the balance, in order to attend to any volume of redemptions without collapsing the protocol by printing tokens out of the air, as happened with Terra.

At the launch of the protocol, only one superstable currency referenced to the inflation of the US dollar will be available, and shortly afterwards another one indexed to the euro will be added, making it possible to carry out direct exchanges (swaps) between the two. In the future, the addition of other currencies will be studied, including also stablecoins directly referenced to fiat.

C. Treasury loans

The incorporation of a token lending system is already common in all DeFi protocols. The novelty introduced by Geminon, taking advantage of the unique collateralization characteristics already explained, is to introduce the possibility of lending the collateral deposited in the pools.

This practice, on which the business of the traditional banking system is based, allows the protocol to obtain additional income. The system would not compete with loans made by users, since the latter would be limited to the protocol token and stablecoins, while the treasury would be in charge of lending reserve assets, thus greatly expanding the supply of available assets for loan.

The interest rate on Treasury loans is calculated based on a reserve ratio that measures what percentage of the total collateral pools has been lent. This means that if there is a high supply of capital or little demand for loans, the interest rate tends to zero, while if there is low supply (high percentage of borrowed collateral) or high demand, interest rates rise, increasing the income of the protocol and avoiding an excessive decline in the reserve ratio.

D. Multichain bridge

Analyzing existing protocols, the strategic importance of blockchain interoperability has become clear. In a currency protocol like Geminon, that ability to use the currency on different blockchains depending on the needs of each user becomes even more important. For this reason, we consider it important that the protocol has its own capabilities from the beginning to migrate its assets between blockchains, while guaranteeing the security of transactions and adequate control of the total supply of tokens across all blockchains.

Today it is not uncommon to find a large number of variants of the same stablecoin when trading a DEX on chains like Solana or Avalanche, due to duplications introduced by bridges. By employing third-party bridges, many protocols not initially developed with a multi-chain mindset have to rely on third-party liquidity providers to facilitate the transfer of assets across the bridge, resulting in token doubling for each bridge used. In addition, this adds extra costs to users, who not only have to pay the cost of the bridging transaction, but also swaps in the origin and destination blockchain between the asset they wish to transfer and the ancillary asset used by the bridge.

To avoid this, Geminon will have a native bridge with the ability to mint and burn currency in the chain of destination and origin, achieving unlimited liquidity transfers and therefore with zero slippage, without the need for intermediate swaps or duplicate tokens, and at a much lower cost than external solutions. And all this in addition to retaining the commissions of the bridge as revenue for the shareholders of the protocol.

E. Protocol revenue

As with any organization, the long-term sustainability of any cryptocurrency protocol depends on its ability to generate revenue to reward shareholders. To achieve this, it is necessary for the protocol to store as many revenue paths as possible derived from the use of its tokens. In our case, these routes would be:

- Seigniorage: commissions for the issuance and redemption of stable currency.
- Internal swaps: commissions for trading between the different stablecoins of the protocol and collateral pools.
- External swaps: commissions for trading on external decentralized exchanges, in which the protocol owns the liquidity of the liquidity pools.
- Multichain bridge: commissions for the transfer of protocol assets between different blockchains.
- Lending. Interest rates and commissions derived from leverage and short selling instruments.
- Arbitrage. Income obtained from arbitrage operations to ensure price parity in external DEX.

Additionally, the amount of these commissions will be variable, depending on parameters such as the size and direction of the order and volatility.

V. The arbitrage attack

One possible reason why no project has yet managed to implement Sams's (2014) idea of linking the price of an algorithmic currency to a price index is the arbitrage attack problem. Given that at present it is still an unresolved issue how to measure the price of consumer goods in the outside world in real time, weight them and bring this data in a decentralized and verifiable way to a blockchain, it is necessary to use the approach originally proposed by Sams (2014) to use a consumer price index, such as the CPI published by the Federal Reserve.

The problem that arises from the application of this idea is that said reference index is published with a certain periodicity that is known in advance. Suppose that the time of publication of the data is known, and an oracle Ω is used to obtain a verifiable consensus on said data within the blockchain. If the oracle protocol takes a time T_Ω to reach a consensus on the data and propagate it to the blockchain, and said data implies an instantaneous alteration of the price of asset X of value Δ, then anyone who can carry out an operation on X in less than T_Ω, he can obtain a risk-free profit proportional to Δ, since he knows in advance the future value of the asset before it reflects the change, which allows a temporary arbitrage operation to be carried out. The benefit of this operation would be obtained to the detriment of the holders of the seigniorage shares, so an attacker could use this exploit to systematically drain the value of the protocol.

Solving this problem is key to a viable implementation of a currency that follows a public and discrete price index. The Geminon protocol solves this problem in a robust and elegant way that ensures the impossibility of carrying out arbitrage attacks, without the need to impose high transaction fees on its users.

VI. Protocol extensions

This point will be the subject of a more in-depth analysis in future versions of this document. Today, we can list the following as possible extensions:

A. Privacy layer

Privacy is a basic right, and by extension the privacy of financial transactions is part of that right. Although Ethereum-compatible blockchains (EVM) do not currently have native features that enable transaction privacy, there are protocols that use the functionality of smart contracts to provide such privacy (Tornado Cash, 2019). A possible future extension of the protocol could include some variant of this technology, which without being a copy of Tornado or without trying to achieve the same level of privacy, would at least allow users to anonymize small daily transactions, which is a necessary requirement for secure mainstream adoption of cryptocurrencies.

B. Governance

Another important point with a view to the future development of the platform is the implementation of mechanisms that allow, once the main development and growth objectives of the project have been achieved, to delegate its management to the community, thus banishing any future risk derived from centralized management.

VII. CONCLUSION

Stablecoins are a key part of the cryptocurrency ecosystem, without whose existence it would not have been possible to reach the level of development achieved in recent years in decentralized finance (DeFi). Despite the variety of algorithmic solutions developed to provide stable prices, more than 95% of the current stablecoin market capitalization comes directly or indirectly from centralized issuers that have implemented censorship mechanisms in their smart contracts. This poses a serious systemic risk for the entire crypto space that makes it necessary to promote the adoption of solutions that are purely algorithmic or collateralized by fully decentralized assets.

In addition to the risk posed by the extensive use of centralized cryptocurrencies, the very fact of using the price of fiat currencies as a reference exposes their holders to the progressive devaluation of their assets when they decide not to expose themselves to the volatility of non-stable crypto assets during a bear market.

To try to alleviate these problems, we propose a new type of super stable currency not fixedly referenced to a fiat currency, but to a price index associated with it, with a new algorithmic mixed backing model with full collateralization of the protocol token and a reserve made up of top-quality crypto assets, including tokenized gold as a novelty. We are also introducing a new type of liquidity pool with an advanced AMM system that enables complex collateral management and token supply strategies. In addition, we propose the implementation of mechanisms that allow improving the privacy of transactions using smart contracts as a proxy.

REFERENCES

Adams, H., Zinsmeister, N. & Robinson, D. (2020). Uniswap v2 Core

Al-Naji, N., Chen, J. & Diao, L. (2018). Basis: A Price-Stable Cryptocurrency with an Algorithmic Central Bank

Ametrano, Ferdinando M. (2016). Hayek Money: The Cryptocurrency Price Stability Solution.

Egorov, M. (2019). StableSwap - efficient mechanism for Stablecoin liquidity.

Egorov, M. (2021). Automatic market-making with dynamic peg.

Ellis, S., Juels, A. & Nazarov, S. (2017). Chainlink: A Decentralized Oracle Network.

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

Haven Protocol (2018). Private Decentralized Finance v3.

Ionescu S. C. & Soleimani A. (2020). Rai: A Low Volatility, Trust Minimized Collateral for the DeFi Ecosystem.

Kereiakes, E., Do Kwon, M. D. M., & Platias, N. (2019). Terra money. Stability and adoption.

Larimer, D., Hoskinson, C. & Larimer, S. (2014). BitShares A Peer-to-Peer Polymorphic Digital Asset Exchange

Lee, J. (2014). Nu Whitepaper.

MakerDao (2017). The Dai Stablecoin System.

Martinelli, F. & Mushegian, N. (2019). A non-custodial portfolio manager, liquidity provider, and price sensor.

Mastercoin (2012). The second Bitcoin Whitepaper.

Mastercoin (2013). Mastercoin Complete Specification.

Mundt, K. et al. (2020). Stablecoins 2.0. Economic Foundations and Risk-based Models

Nakamoto, S. (2008). Bitcoin. a P2P e-cash system. The Cryptography Mailing List.

Ivanov, S. & Pupyshev, A. (2020). Neutrino: an algorithmic price-stable cryptocurrency protocol backed by a platform's native token. https://wp.neutrino.at/

Olympus (2021). https://docs.olympusdao.finance/

Piau, M. & Tabor, L. (2022). DEUS Finance. A Peer-to-Peer Bilateral Agreement System.

Platias, N., Lee, E.J. & Di Maggio, M. (2020). Anchor: Gold Standard for Passive Income on the Blockchain.

Publius (2021) Beanstalk. A Decentralized Credit Based Stablecoin Protocol.

Sams, R. (2014). A Note on Cryptocurrency Stabilisation. Seigniorage Shares.

Santoro, J. (2021) Fei Protocol. A Decentralized, Fair, Liquid, and Scalable Stablecoin Platform.

Sperax Research (2021) - USDs Whitepaper.

Tether (2014). Fiat currencies on the Bitcoin blockchain.

Tornado Cash (2019). https://docs.tornado.cash/general/readme

USDD (2022). Decentralized Stablecoin Protocol v1.1