Geminon: a protocol for super stable cryptocurrencies

Heirs of Satoshi

geminon.fi

First version: April 08, 2022

This version: April 13, 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 maintains 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.

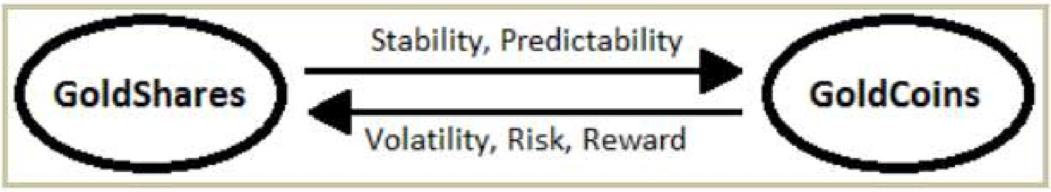

Figure 1: algorithmic stability mechanism proposed by Mastercoin (2012)

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.

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 that 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, to date we haven't found any project that has managed to carry it out, despite being an obvious problem within the crypto ecosystem, being the existing ones constrained to the creation of stable currencies pegged to existing fiat currencies such as the US dollar. For this reason, in this paper we propose a viable solution to put this idea into practice, implementing a protocol composed of a set of currencies: a 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

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.

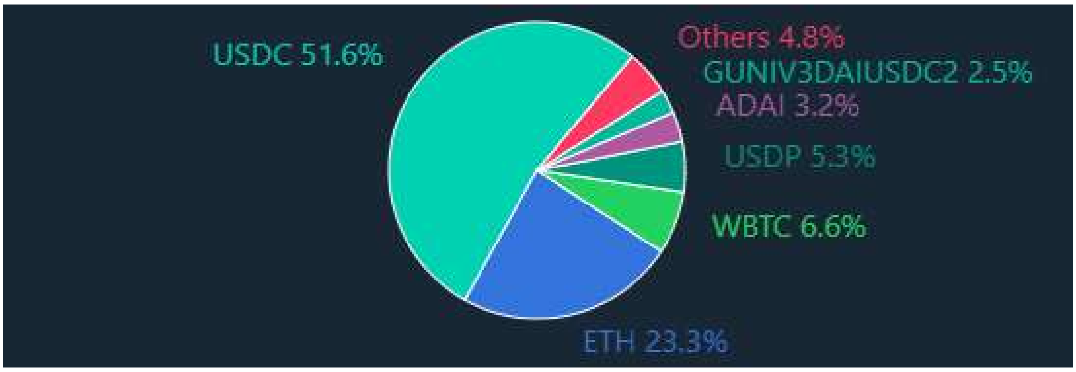

Figure 2: DAI generated by collateral (daistats.com)

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 algorithmic*

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. There are very few protocols of this type, the first to appear was Neutrino (USDN, 2020) and later Frax (2021).

The situation regarding the composition of the collateral of both protocols is opposite: while Neutrino uses only the native token of its network (WAVES) as collateral, FRAX only uses other stable coins, both centralized and collateralized (which, as we have already seen, turn out to be mostly also dependent on the centralized ones).

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 to achieve mass adoption has been 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.

III. Existing algorithmic stablecoin protocols

Various attempts have been made to implement the idea of a dual system with seigniorage shares to stabilize a currency. Although early attempts to implement this idea failed, several protocols have now succeeded in creating purely algorithmic stablecoins.

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.

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 main advantage that Terra has, however, is that it is a blockchain built using the Cosmos IBC protocol, which makes it fully interoperable with all other blockchains built with said protocol and that allows moving Terra assets by any of these chains seamlessly. Additionally, Terra has recently deployed these assets as Ethereum tokens, further expanding that interoperability. The enormous success that the UST has had as a stablecoin has meant that it is even being adopted by centralized exchanges, which places it as the main candidate to replace centralized currencies.

One point that raises many questions about the stability of the Terra protocol is that of the maximum supply of LUNA, which is 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 the 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 said coins to be able to redeem them at their peg value, which would mean the collapse of the protocol and the loss of the peg. In fact, the LUNA market value threshold at which this situation would be possible is much higher because not all of the circulating supply is available to the market module. This poses a dichotomy:

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

Currently the market value of LUNA is barely twice the total market value of UST. In a bear market, where there was a greater than 50% market decline at the same time that stablecoin demand increases, it would be easy to find yourself in a technical protocol breakdown situation. However, it is important to emphasize here that as long as users keep confidence in the protocol, a transitory situation of this type would not have to trigger the aforementioned collapse. Let's remember that the traditional banking system operates in a stable way with a reserve ratio of just 2%, which means that only that percentage of deposits could be withdrawn if everyone tried to do it at the same time. Terra currently operates under a reserve ratio close to 200%, a hundred times higher than any traditional bank, which should definitively put away the fears of this so-called "death spiral".

Terra has recently started buying large amounts of quality reserve assets, such as Bitcoin and Avalanche, through the Luna Foundation Guard (LFG). The objective seems to be to dispel fears of the situation described in the previous point through the external collateralization of the protocol. Although the objective pursued is quite desirable -to strengthen the solvency of the protocol-, the approach used, however, is questionable, since it is still fully centralized. As with centralized stablecoins, that collateral is not an asset within the blockchain, and there is currently no cryptographic mechanism that guarantees LUNA and UST holders the possibility of redeeming these against the collateral, nor the conditions under which such access to collateral would be possible.

Although Terra is probably the best stablecoin protocol out there today, it is still not perfect. To begin with, it suffers from the same flaw as all other stablecoin protocols: parity with inherently inflationary fiat money. It also does not have any privacy features, nor are they expected to be introduced. Finally, the recent incorporation of highly centralized components in the management of reserve assets blurs the image of a decentralized protocol that Terra maintained until now.

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. This statement is questionable since Neutrino (Ivanov & Pupyshev, 2020) already used a mixed stabilization system for its USDN a year before the creation of Frax, using the currency of the WAVES protocol as collateral and the base token of the protocol (NSBT) as algorithmic counterparty to stabilize the price, which would effectively make it the first fractional reserve protocol that existed (in the field of cryptocurrencies, as we must also remember that traditional banks have been using this system since its origins in the 17th century). Nor can Frax be considered “unique” since the fractional reserve system is simply a variant of the collateralization system in which a part of the collateral is a protocol token, and there are other algorithmic projects such as Terra, Deus and the aforementioned Neutrino that have collateral reserves.

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.

The main criticism that can be made of this protocol is the same as to all other collateralized currencies, and it is precisely this great dependence on centralized stablecoins, for the reasons that have already been exposed in this document. The proliferation of protocols dependent on these currencies only increases the systemic risk that they pose for decentralized finance.

Frax has recently announced its intention to make a currency that tracks the US inflation index (CPI) in the future, which could make it the first protocol to launch this idea into the market. However, given the basic differences that exist with our protocol, especially in the characteristics of centralization, these are two solutions that are sufficiently differentiated so that they can coexist, and the existence of competition that fosters innovation and development is also desirable within the cryptocurrency ecosystem.

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.

IV. Geminon Protocol

As we have seen when analyzing the existing stablecoin protocols, to date no project has put into practice the proposals of Sams (2014) creating a currency referenced to a price index in a purely algorithmic and decentralized way. In addition, considering the need for protocols that are fully committed to decentralization in which users can take refuge in case of a market event that affects centralized currencies and their collateralized derivatives, we propose the creation of a system that fully meets these objectives. The characteristics of said system are detailed below.

A. The issue of limited supply

One of the first dilemmas that arises when approaching the design of a monetary system is related to the maximum supply of currency. While it might initially seem best to adopt a limited supply for the seigniorage token mimicking Bitcoin and even similar protocols such as Terra, further analysis of the protocol's stability limits would advise against such a move.

As commented when analyzing Terra, it is not very clear if having a limited supply the protocol could maintain the peg of its stablecoins in all circumstances. A simple mathematical analysis shows that under certain conditions, under a maximum supply restriction of the coin that performs the role of seigniorage shares, the protocol would lose the ability to redeem users' stablecoins, which would have the effect of leaving users trapped if there were no other means of swapping them. In case there was exchange pairs in decentralized exchanges, users could exit but the peg would be lost, as the arbitration mechanism would stop working.

In the presence of liquidity pools of the currency in external exchanges, if Alice decides to sell her stablecoin in said pools, it will cause the price of the stablecoin to decrease against its theoretical peg, which would open an arbitrage opportunity consisting of buying the coin in the pool and redeem it in the protocol for its peg price. But since the capacity of the protocol to redeem stable currency is exhausted because the maximum supply has been reached, said operation would not be possible, so the price of the currency in external pools would continue to fall uncontrollably, causing a chain reaction that would collapse the protocol.

For this reason, a system based on seigniorage shares should not have a limit on the issuance of said shares. The largest protocols that currently exist that use this mechanism, Terra and Frax, however, have a maximum supply limit on their shares, which places them at risk of suffering an event of this type. This risk is lower in the case of Frax due to its high percentage (>85%) of collateralization. However, the fact that this collateral is mainly made up of centralized coins puts the protocol at risk that a market event associated with said coins could cause a chain reaction that would endanger the peg of its stablecoins, even temporarily.

To solve this risk, the protocol must have, in addition to the ability to issue currency within the limits of the maximum initial supply, a reserve of shares and assets of recognized value, and once both channels have been exhausted, there must also be the possibility to issue currency beyond the maximum initial supply. These three measures ensure that the protocol delivers on its promise to allow stablecoins to be redeemed at peg value under any circumstances.

B. Protocol owned liquidity

One of the latest ideas to be successfully incorporated into decentralized finance has been bonus programs for the protocol to take ownership of liquidity (Olympus, 2021). The objective of this idea, highly praised by analysts, is for the protocol to retain the commissions generated by the swaps of its tokens, contributing to its sustainability and increasing the revenue for token holders.

The bonding mechanism broadly consists of establishing rewards in protocol tokens to liquidity providers who deliver their LP tokens (which represent ownership of a pair of coins deposited in a liquidity pool) in exchange. The reward is that these protocol tokens are received at a discount to the current trading price after a short vesting period, which is equivalent to receiving a bond denominated in tokens, hence the name of the system.

This bond system makes sense for those protocols that have a large number of third-party liquidity providers and want to take ownership of that liquidity. For a newly created protocol, however, once the benefits of owning the liquidity have been seen, it makes more sense to set a proprietary liquidity deployment strategy from the outset than paying interest on these bonds. For this reason, the protocol will instead deploy a smart liquidity strategy aimed at managing the level of liquidity to maximize the protocol's liquidity revenue and protect investors from price declines as the market capitalization increases.

C. Automatic collateralization of the reserve treasury

The good accounting practices of any organization dictate that it has a sufficient cash reserve to face any unforeseen event that may arise during the exercise of its activity. Geminon is not a collateralized stablecoin protocol, in the sense that collateralized stablecoins are not issued as debt backed by external assets deposited by users nor can stablecoins be redeemed against collateral (under normal conditions). However, at a global level it is interesting that the protocol has reserves of decentralized assets considered safe values in relation to the set of all existing crypto assets.

Although the discussion about what can be considered a safe asset in the cryptocurrency environment can be tough, here we will limit ourselves to a conservative view of the issue, and we will define safe assets as those that meet these four criteria:

- Consolidated position in the market with a clear position of dominance over its competitors
- Committed community, both in future development and in the use and expansion
- Strong use case, with assured continuous demand for the currency
- Non-inflationary economic design.

Following these criteria, the selected reserve assets would be:

- The native currencies of the blockchains in which our protocol will be implemented: Ethereum, BNB and Avalanche initially.
- Bitcoin
- The oracle token: Chainlink.

Once the assets to be incorporated into the treasury have been selected, it is necessary to design a decentralized and trustless mechanism that allows users to be sure that said assets are punctually incorporated into the treasury, and that if necessary, they will be able to access them. To this end, it will be established that one third of the shares used for the issuance of currency will be used for the market purchase of said assets. To guarantee that this procedure is fulfilled, it must be automated in a smart contract. Similarly, the contract will implement the conditions under which users will be able to redeem stablecoin against reserve assets rather than against protocol shares. The following points will delve into this mechanism.

D. Treasury loans

Until now, the most used approach by cryptocurrency lending protocols has been to leave the creation of the offer of said loans in the hands of the users. Geminon uses a different approach, with a triple objective: to simplify the generation of revenue for users, who will not have to choose between different alternatives to generate returns, improve the liquidity available for loans and optimize interest rates.

To achieve these goals, the capital for the loans is provided directly by the protocol treasury. As the supply of capital is known and stable, the protocol can optimize the interest rate, varying it based on the ratio between stable currency loans and shares (longs / shorts) and the total percentage of the capital borrowed

E. 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.

F. Stablecoin staking

A fundamental part of any decentralized finance protocol is the design of a suitable reward system to attract and retain users. The level of competition in this market is probably one of the most extreme that exists due to the total absence of regulations that stop innovation and the open source culture that prevails in the community. For this reason, it is necessary to find a balance between a high level of rewards and the long-term sustainability of the protocol.

The Geminon protocol rewards have been designed with these principles in mind. Instead of distributing these rewards using the protocol token as is common in other projects, leading to pump & dump price movements or at the very least extreme inflationary pressures that ultimately depress the price, Geminon is routing this issue of tokens indirectly through stablecoin staking. This achieves a double effect:

- Keep the initial circulation of tokens stable, minimizing the inflationary pressure due to initial emissions and creating a shortage of supply in the market, which means that any increase in demand translates into growth in the price of the token.

- Create a strong incentive to own the stablecoin and attract investors thanks to an unbeatable risk/benefit ratio on investment.

These two effects combine to form a virtuous circle that generates constant and sustainable growth. By generating the rewards in stablecoin, it is not necessary to compensate investors for the volatility of the project token with triple digit returns, which makes it possible to keep steady emissions over time until the number of users grows enough to generate self-sustained income through the protocol fees.

G. 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.
- 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 could have a variable character, acting as a kind of fiscal policy of the protocol that has a countercyclical effect to reduce the volatility of the tokens as we will see in the next point.

H. Automatic stabilizers

It has been argued that purely algorithmic currency issuance protocols present certain tail risks that can manifest themselves in times of extreme volatility if there is a massive loss of investor confidence and those decide to abandon the protocol in a disorderly manner. Although in our opinion these risks are not greater than those that may exist in the traditional banking system, where, let us remember, less than 2% of customer deposits are kept in reserve, which means that in the event of a bank run the collapse of the system would happen, the principle of due diligence in the economic design of the protocol invites us to take these risks into account and deal with them appropriately.

The mechanisms of capitalization of the treasury through reserves in top quality crypto assets and the possibility of limiting the maximum supply of shares as a last resort to ensure that the exchange rate of the stable currency is always maintained have already been mentioned. These mechanisms should provide enough protection to the protocol in all market conditions, but here the possibility of an economic attack must also be taken into account, where a malicious actor with large financial resources would try to destabilize the protocol through instant massive sales to try to induce the panic to other investors.

To head off a panic or sell-off scenario or simply to cushion the volatility of market cycles without resorting to centralized and inelegant solutions such as pausing smart contracts, it is necessary to introduce economic stabilization mechanisms through incentives and penalties. In the case of the redemption of stablecoin to sell the shares, the mechanism would consist of introducing a dynamic sale commission proportional to the percentage of the total coin supply burned in the last 24 hours, thus discouraging massive sales from a certain threshold and ensuring the stability of the protocol by increasing the value of this.

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).

B. Decentralized Price index

The consumer price index produced by official agencies have been widely criticized in recent times for showing systematically lower inflation data than what people observe on a day-to-day basis. Furthermore, if maximum decentralization is what we are seeking, reliance on a centralized issuer for the strategically important data of the protocol seems inadvisable. Therefore, the search for mechanisms that allow obtaining this data in a purely decentralized way is a desirable objective for a future extension of the protocol.

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 purely algorithmic backing and a treasury made up of top quality decentralized crypto assets. In addition, we propose the implementation of mechanisms that allow improving the privacy of transactions using smart contracts as a proxy.

REFERENCES

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

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

Frax Finance (2021). Fractional-Algorithmic Stablecoin Protocol.

Haven Protocol (2018). Private Decentralized Finance v3.

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

Lee, J. (2014). Nu Whitepaper.

MakerDao (2017). The Dai Stablecoin System.

Mastercoin (2012). The second Bitcoin Whitepaper.

Mastercoin (2013). Mastercoin Complete Specification.

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

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.

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