Geminon: un protocolo de criptomonedas supraestables

Herederos de Satoshi

geminon.fi

Primera versión: 8 de abril de 2022

Esta versión: 13 de abril de 2022

***Resumen*—Desde el origen de Bitcoin en 2008, este ha atraído una creciente atención y adopción como un activo de reserva de valor. Sin embargo, su enorme volatilidad hace que su uso como moneda siga siendo poco práctico 14 años después. Esto ha llevado a la creación de las denominadas monedas estables, diseñadas para mantener la vinculación con alguna moneda fiduciaria, generalmente el dólar estadounidense. Aunque esto resuelve el problema de la volatilidad a corto plazo, anula el propósito básico detrás de la creación de Bitcoin: usar un dinero sólido, descentralizado y sin confianza en terceros que los gobiernos no puedan devaluar.**

En este documento, proponemos un protocolo para una criptomoneda supraestable completamente algorítmica y descentralizada que mantiene un valor constante en relación con los precios de los bienes de consumo en la economía en lugar de en relación con una moneda fiduciaria inflacionaria. Hasta donde sabemos es el primero de su tipo.

I. INTRODUCCION

Bitcoin se creó como un sistema de pago electrónico basado en pruebas criptográficas para permitir que las personas realicen transacciones directamente entre sí sin la necesidad de un tercero de confianza (Nakamoto, 2008). Su diseño económico, con un suministro total limitado a 21 millones de bitcoins, lo convierte en un buen activo de reserva de valor para el largo plazo. Este suministro se va liberando de forma localmente lineal a través de recompensas pagadas a los mineros por cada bloque de transacciones generado, cada diez minutos en promedio, y dicha recompensa se reduce a la mitad cada cuatro años aproximadamente, en el evento conocido como "halving", dando lugar a una curva de suministro de largo plazo que se aproxima a una logarítmica.

El hecho de que la oferta monetaria de bitcoin esté fijada de antemano hace que esta sea relativamente inelástica a la demanda, por lo que cualquier variación de dicha demanda hace que el ajuste entre ambas deba llevarse a cabo necesariamente mediante una variación del precio. Esto hace a su vez que las expectativas del mercado sobre el precio futuro, que son el principal impulsor de la demanda, cambien rápidamente amplificando los cambios de esta y creando un círculo vicioso que conduce a fuertes oscilaciones del precio

(volatilidad). En la actualidad es comúnmente aceptado que bitcoin se ha establecido más como un oro digital que como un buen dinero o moneda (Ametrano, 2014).

Esta volatilidad debida a la rigidez de la oferta monetaria es una característica que han heredado la práctica totalidad de las criptomonedas creadas siguiendo la estela de bitcoin. Aunque algunos argumentan que con la adopción masiva dicha volatilidad iría en descenso, hasta la fecha dicha afirmación no se ha cumplido y la aplicación de la ley de oferta y demanda en este caso indica que es muy improbable que alguna vez las criptomonedas que siguen la misma política monetaria inelástica de Bitcoin alcancen una estabilidad de precios apenas cercana a la de las monedas fiat.

Mastercoin (2012, 2013) fue el primer proyecto en proponer la idea de una criptomoneda que replicara el precio de otro activo, concretamente el oro, empleando un mecanismo puramente algorítmico que consistía en emplear dos tokens: uno estable con oferta variable y otro que absorbía la volatilidad del primero y permitía a los inversores obtener beneficios por la acuñación de los tokens estables (señoreaje). Además de esto, propusieron otras muchas ideas como el uso de una segunda capa sobre Bitcoin, un protocolo de oráculo para traer a la blockchain los datos de precios del exterior o el uso de una reserva monetaria como colateral de la moneda estable emitida para su uso en situaciones de emergencia. Aunque el protocolo Mastercoin no tuvo éxito, todas estas ideas han sido aplicadas con posterioridad por otros protocolos y son una pieza clave hoy en día en el ecosistema de las criptomonedas.

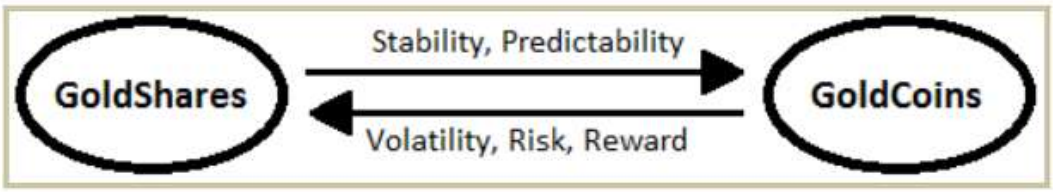

Figura 1: mecanismo de estabilidad algorítmico propuesto por Mastercoin (2012)

La primera moneda estable en lograr adopción masiva fue el USDT de Tether (2014). Inicialmente diseñada para funcionar usando una solución de capa 2 sobre la cadena de bloques de Bitcoin, no fue hasta la aparición de los contratos inteligentes en la red Ethereum y los primeros intercambios descentralizados (Uniswap, 2018) cuando comenzó su adopción generalizada. A pesar del gran éxito alcanzado, llegando a situarse por momentos en 2020 como la segunda mayor criptomoneda solo por detrás de Bitcoin, no se puede aceptar como una solución real al problema que nos ocupa sino más bien como un parche. La razón es que Tether es una empresa centralizada que afirma respaldar sus emisiones de tokens 1:1 con reservas de dólares, lo cual añade a los problemas ya existentes del dinero fiat (dependencia de entes centralizados, necesidad de confianza en terceros, pérdida constante de poder adquisitivo, censura y confiscabilidad), algunos propios de las criptomonedas como bitcoin (falta de privacidad, altos costes de transacción y dificultad de uso).

Esta falta de soluciones que sean lo suficientemente estables en precio y a la vez conserven el poder adquisitivo a lo largo del tiempo, obliga a los usuarios de las criptomonedas a intentar lograr ellos mismos ese equilibrio por la vía de la especulación, intentando acertar qué combinación de criptoactivos y monedas estables les dará la relación riesgo / beneficio deseada. Sin embargo, es conocido que la mayoría de inversores particulares es incapaz de alinearse adecuadamente con los ciclos del mercado, lo cual lleva a muchos incluso a tener pérdidas respecto a los activos libres de riesgo de referencia, como por ejemplo un depósito bancario tradicional.

Una de las primeras alternativas a las monedas estables centralizadas respaldadas por fiat fue propuesta por Ametrano (2014) y bautizada por este como “Dinero Hayek” en honor al economista de la Escuela Austriaca y ganador del Premio Nobel en 1974 Friedrich A. Hayek. Ametrano propone una moneda de valor

constante y suministro perfectamente elástico frente a la demanda, empleando un mecanismo de rebase: para mantener siempre constante el valor de la moneda frente a un índice de referencia, se modificaría directamente la cantidad de moneda existente en cada monedero, afectando de forma efectiva la cantidad de moneda en circulación. El precio podría fijarse así arbitrariamente para ser igual al de una moneda fiat, a un índice de precios al consumo o a una cesta de materias primas como propuso originalmente Hayek.

El problema del sistema de rebase propuesto por Ametrano es que solo estabiliza el precio de la moneda, no el poder de compra del monedero. La estabilidad de precios no consiste únicamente en estabilizar la unidad de cuenta del dinero, sino también su almacén de valor (Sams, 2014). Para lograr estabilizar ambas, Sams (2014) propone dividir la moneda en dos tipos: moneda que actúa como dinero y moneda que actúa como acciones en el sistema de señoreaje, a las que denomina moneda y acciones respectivamente. Para estabilizar el valor de la moneda, Sams propone un mecanismo de variación del suministro, según el siguiente esquema:

- Cuando el suministro de moneda necesita incrementarse (para reducir su precio cuando este está por encima de su objetivo), se distribuye moneda a los accionistas a cambio de un cierto porcentaje de acciones, que son destruidas. El suministro de moneda aumenta y el de acciones disminuye (aumentando el precio de estas).
- Cuando el suministro de moneda necesita aumentarse (para aumentar su precio cuando este está por debajo de su objetivo), se distribuyen acciones a los tenedores de moneda a cambio de un cierto porcentaje de monedas, que son destruidas. El suministro de moneda disminuye y el de acciones aumenta (disminuyendo el precio de estas).

Este sistema de dos componentes, una moneda estable y unas acciones de señoreaje que permiten absorben la volatilidad, es similar al propuesto por MasterCoin (2012, 2013). Otra variante del sistema dual de acciones y moneda fue propuesta por Lee (2014) en el protocolo *Nu*, en el que las acciones (*Nushares*) eran utilizadas a la vez para validar la red con un algoritmo de prueba de participación y para votar sobre la emisión de moneda (*Nubits*).

Las novedades incorporadas por Sams (2014) respecto a estos protocolos fueron por un lado el uso de un mecanismo de subasta periódica para estabilizar la moneda, en la cual el protocolo calculaba la variación de suministro necesaria para devolverla a su paridad y los tenedores de acciones pujaban qué cantidad de acciones estaban dispuestos a permutar por esa cantidad de moneda. La otra propuesta introducida fue referenciar el valor de la moneda a un índice de precios de bienes de consumo en lugar de a otra moneda fiat.

El principal obstáculo para la implementación de una moneda referenciada a un índice de precios consistía en la incorporación de dicha información a la cadena de bloques de una forma fiable y verificable criptográficamente. La falta de dicho mecanismo pudo ser la causa de que esta idea fuera abandonada en un principio. Este problema fue resuelto con la llegada de los primeros oráculos (Chainlink (Ellis et al., 2017), Band Protocol (2020), Berry Data (2021), API3 (2021)) que permitían la conexión con fuentes de datos externas a la cadena de bloques y la verificación descentralizada de dichos datos.

A pesar de que la idea de una moneda estable atada al índice de precios fue propuesta hace casi una década por Sams (2014) y de la viabilidad técnica de su implementación desde la aparición de los primeros oráculos en 2017, hasta la fecha no consta que ningún proyecto haya logrado llevarla a cabo, a pesar de ser un problema evidente dentro del ecosistema cripto, limitándose a la creación de monedas estables pareadas con las monedas fiat existentes como el dólar americano. Por esta razón, en este documento proponemos una solución viable para llevar a la práctica dicha idea, implementando un protocolo compuesto por un conjunto de monedas: una moneda de suministro fijo y precio variable que absorbe la volatilidad, y monedas supraestables con suministro flexible y valor unido a un índice de precios de los bienes de una economía.

El resto del documento está organizado de la siguiente manera: primero, analizamos los diferentes tipos de monedas estables que existen. A continuación, repasamos los principales protocolos algorítmicos que hay

actualmente en el mercado, destacando sus ventajas y desventajas. Finalmente, presentamos nuestra solución, así como las posibles extensiones de la misma.

II. TIPOS DE MONEDAS ESTABLES

A. Monedas estables respaldadas por fiat

La forma más fácil de implementar una moneda estable es hacer que tenga paridad con una moneda fiat existente, y emitir una unidad del criptoactivo por cada unidad de la moneda fiat recibida. Esto asegura que la moneda mantendrá su paridad siempre que sus usuarios mantengan la confianza en que el emisor realmente posee el efectivo que la respalda en un ratio 1:1. El problema con esta aproximación es que requiere confianza en un emisor centralizado, lo que va contra el mismo principio fundacional de las criptomonedas: construir un sistema para transferencias de dinero descentralizado, sin confianza ni permisos de terceros.

Las monedas estables más utilizadas actualmente pertenecen a esta categoría : Tether (USDT), USD Coin (USDC) de Circle y Binance USD (BUSD) emitido por Paxos (no por Binance, como mucha gente cree). Otros protocolos de este tipo son TrueUSD (TUSD), Pax Dollar (USDP), Gemini Dollar (GUSD), Euro Tether (EURT), Hot USD (HUSD) emitido por *Stable Universal Limited*, una compañía con sede en la Islas Vírgenes, STASIS EURO (EURS) emitido pos STASIS con sede en la Isla de Man y USDK emitido por el exchange OKEx.

Todas las monedas de esta categoría sin excepción implementan en el contrato inteligente de su token una función de 'lista negra' que permite bloquear los fondos de cualquier dirección, ya sea un monedero o un contrato inteligente, evitando que los tokens que contienen puedan ser transferidos. Como estos tokens representan una cantidad de moneda fiat depositada en entidades centralizadas, el saldo que representan los tokens puede ser además confiscado.

Debido precisamente a su gran adopción, este tipo de monedas estables representan graves riesgos a medio plazo para la supervivencia de las finanzas descentralizadas tal y como las conocemos hoy en día por varios motivos:

- Censura arbitraria. Como ya se ha explicado, todos los protocolos de moneda estable centralizados que existen han incorporado en el código de sus tokens funciones que les permiten bloquear a discreción cualquier dirección. Esto supone que en la práctica no exista ninguna diferencia entre guardar ese dinero en un banco tradicional, en un intercambio centralizado o en un monedero frío, puesto que en ningún caso se dispone de la custodia plena de las monedas.
- Regulaciones. Las criptomonedas obtienen su asombrosa resiliencia de su descentralización. Esta propiedad sin embargo no se cumple para las monedas centralizadas. Cualquier autoridad que deseara atacar al conjunto de las criptomonedas, a cualquier protocolo o conjunto de individuos que utilicen estas monedas podría hacerlo fácilmente. Además, las víctimas de estos ataques tendrían dificultades para defenderse, debido a los grandes vacíos legales que existen en lo relativo a los criptoactivos en buena parte del Mundo.
- Falta de solvencia del emisor. A pesar de que en teoría la entidad que emite las monedas guarda una reserva 1:1 en dinero efectivo para respaldarlas, en la práctica no está claro que esta afirmación se cumpla al 100%. Suponiendo que confiamos en que el emisor no está cometiendo un fraude y que realmente guarda esas reservas, todavía quedaría por dirimir la cuestión de la calidad y liquidez de esas reservas. Es paradigmático el caso de Tether, que lleva años recibiendo acusaciones públicas de haber utilizado las reservas de USDT para inversiones de alto riesgo como bonos de baja calificación e incluso que las reservas liquidas no cubrían el 100% de las emisiones, hasta el punto de que la empresa afronta desde 2018 una investigación del Departamento de Justicia de EEUU por presunto fraude.

- Riesgo sistémico. En la actualidad más del 80% de las monedas estables criptográficas en circulación, que a su vez han supuesto durante 2021 entre un 5% y un 10% de la capitalización total del mercado de criptomonedas, son centralizadas directa o indirectamente (vía colateral). Las monedas estables son además una pieza clave de todos los protocolos de finanzas descentralizadas que operan en las cadenas de bloque de contratos inteligentes e incluso de todos los intercambios centralizados y los mercados de futuros asociados, donde USDT es la moneda más utilizada para la liquidación de los contratos. Esto unido a los riesgos enunciados anteriormente, hace que en la actualidad estas monedas centralizadas sean una bomba de relojería que amenaza a todo el mercado de criptomonedas. Bien sea por un fraude, una acción judicial o por ataques estatales, el efecto de la caída de un gran emisor como Tether podría desencadenar un auténtico Armagedón en el conjunto del mercado de criptomonedas.

Los riesgos expuestos hacen prioritario el desarrollo de soluciones de moneda estable plenamente descentralizadas, fiables, autocustodiadas y no censurables que puedan reemplazar a las soluciones centralizadas.

B. Monedas basadas en deuda colateralizada

1) Totalmente colateralizadas

En un intento de resolver los principales inconvenientes de las monedas estables centralizadas respaldadas por fiat, se recurrió a otro antiguo invento del sistema bancario tradicional: el dinero-deuda. El primer protocolo en implementar con éxito este sistema fue DAI (Maker Dao, 2017). En este tipo de protocolos, el usuario toma un préstamo de moneda estable depositando a cambio una garantía en forma de criptomonedas (el colateral). Dada la gran volatilidad de las criptomonedas, el valor inicial de esta garantía supera ampliamente el del préstamo concedido (sobrecolateralización), siendo lo habitual que el ratio colateral/deuda esté entre 1,6:1 y 2:1. Dada la ineficiencia en el uso del capital que esto supone, el colateral ha terminado compuesto en su mayoría por otras monedas estables, y dado que las más utilizadas son las centralizadas, estas han terminado copando los balances de activos de estos protocolos que inicialmente pretendían ser descentralizados.

Figura 2: DAI generado por cada colateral (daistats.com)

DAI ha sido durante mucho tiempo el mayor protocolo de moneda estable no centralizado (solo superado recientemente por el UST de Terra, aunque este último pertenece a la categoría de monedas puramente algorítmicas). Dado su relativo éxito, han aparecido recientemente una gran cantidad de protocolos con el mismo principio de funcionamiento. Por orden de capitalización de mercado en la fecha de redacción de este documento, encontramos : 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), Rai Reflex Index (RAI, 2020) y VAI (2021), este último con grandes problemas para mantener la paridad con el dólar.

Todos estos protocolos tienen principios de funcionamiento muy similares en lo relativo al mecanismo de emisión de moneda a partir de un colateral. Las diferencias se encuentran en los tipos de colateral aceptado, el mecanismo de liquidación, el interés cobrado por el préstamo y la incorporación de estrategias de generación de beneficio usando sinergias con otros protocolos de finanzas descentralizadas (*yield farming*). En este aspecto se pueden destacar protocolos como Origin Dollar (OUSD, 2020) y mStable USD (mUSD, 2020), que aceptan como colateral únicamente otras monedas estables en un ratio 1:1 e invierten este colateral en otros protocolos, lo que permite no solo no cobrar interés por el préstamo emitido, sino pagar intereses a los poseedores.

En general todos los protocolos de esta categoría han terminado recurriendo, en mayor o menor medida, al empleo de otras monedas estables como colateral, y como las más utilizadas son centralizadas, el resultado final ha sido paradójicamente que los protocolos inicialmente creados para aportar una alternativa puramente descentralizada de monedas estables han terminado dependiendo de estas.

El hecho de que todas las monedas de esta categoría estén colateralizadas, parcial o totalmente en algunos casos, con monedas centralizadas no hace sino aumentar los riesgos sistémicos de los entes centralizados que comentamos en el punto anterior. En el caso de estos protocolos, la existencia de contratos inteligentes que concentran grandes cantidades de moneda confiscable les convierte en presa fácil de cualquier gobierno que desee apropiarse de dichos activos, con la consiguiente cascada de liquidaciones y pérdidas masivas producidas para los usuarios.

2) Parcialmente algorítmicas

La principal crítica que reciben los protocolos sobrecolateralizados es que son ineficientes desde el punto de vista del aprovechamiento del capital. Esto ha propiciado la aparición de protocolos híbridos, que combinan el uso de un porcentaje de colateral inferior al valor de la moneda emitida con un sistema de dos tokens como el propuesto por Mastercoin (2012, 2013) para complementar el déficit de colateral. Existen muy pocos protocolos de este tipo, el primero en aparecer fue Neutrino (USDN, 2020) y posteriormente Frax (2021).

La situación respecto a la composición del colateral de ambos protocolos es opuesta: mientras que Neutrino utiliza como colateral únicamente el token nativo de su red (WAVES), FRAX emplea únicamente otras monedas estables, tanto centralizadas como colateralizadas (que como ya hemos visto resultan ser en su mayoría también dependientes de las centralizadas).

Estas monedas podrían ser consideradas también como un caso particular de monedas colateralizadas, en las que la composición del colateral incluye también al propio token del protocolo.

C. Monedas estables algorítmicas

1) Monedas de rebase

Las monedas de esta categoría siguen la aproximación propuesta por Ametrano (2014), de mantener constante el precio y variar la cantidad de monedas que poseen los tenedores (rebase). Pocos protocolos se han atrevido a implementar este tipo de solución, sin duda el más conocido es Ampleforth (Kuo and Iles, 2018).

Más recientemente, Olympus DAO (OHM, 2021) creó un proyecto de gran éxito basado en la idea del rebase, pero añadiendo colateralización (mediante DAI y Frax) y elementos de teoría de juegos en el diseño

de incentivos económicos del protocolo. Este diseño recompensaba con grandes incentivos el *staking* del token OHM, de modo que recibieran tanto los intereses por depositar los tokens como todo el suministro nuevo de tokens creado para intentar devolver la moneda a su paridad de 1$. Sin embargo, dados los grandes intereses que recibían por el depósito este nuevo suministro no se liberaba en el mercado, lo cual creaba un círculo vicioso de demanda -> subida de precio -> incremento de recompensas que llegó a situar el interés anual por depositar OHM por encima del 1000%. Este proyecto ha generado una enorme controversia, siendo acusado por muchos de ser un esquema Ponzi, aunque este punto sigue siendo objeto de debate.

2) Acciones de señoreaje

En esta categoría se encuentran los protocolos que emplean el sistema dual de acciones / moneda propuesto por Mastercoin (2012, 2013). Es interesante notar que este sistema en el fondo es también equivalente al de colateralización, con la única diferencia de que en este caso se emplea como colateral un token de propia creación en lugar de otros diferentes. De hecho, todas las categorías de moneda estable descritas a excepción de los tokens de rebase, se podrían agrupar bajo una única categoría de monedas colateralizadas en las que únicamente varía la composición, centralización y mecanismo de redención de dicho colateral.

El primer protocolo de esta categoría en lograr adopción masiva ha sido Terra (Kereiakes et al., 2019) con el UST. Haven Protocol (2018) y Terra fueron los dos primeros proyectos en implementar de forma exitosa un sistema puramente algorítmico de moneda estable. En el siguiente punto analizamos en detalle las características de estos protocolos.

III. PROTOCOLOS EXISTENTES DE MONEDA ESTABLE ALGORÍTMICA

Se han hecho varios intentos de poner en práctica la idea de un sistema dual con acciones de señoreaje para estabilizar una moneda. A pesar de que los primeros intentos de implementar esta idea fallaron, en la actualidad varios protocolos han tenido éxito creando monedas estables puramente algorítmicas.

A. Haven protocol

Haven (XHV) es una bifurcación de Monero que hereda todas las características de privacidad de esta última. Extiende esa funcionalidad al proporcionar monedas y productos básicos privados, anónimos y sintéticos (xAssets) que solo pueden existir a través de la "quema" de la moneda base de Haven (Haven Protocol, 2018).

El primer activo sintético agregado al protocolo fue xUSD (Haven Dollar), una moneda estable privada vinculada al dólar estadounidense cuyas transacciones no se pueden rastrear. La premisa del protocolo es que 1 xUSD siempre se podrá canjear por 1$ de XHV.

Siendo Monero la criptomoneda más segura que existe, Haven es un proyecto excelente a nivel técnico al derivar directamente del primero. Sin embargo, la falta de interoperabilidad con otras cadenas de bloques y de intercambios centralizados en los que operar con el activo ha supuesto un importante freno a su adopción, quedando relegado a un papel marginal en el mercado. Otra desventaja del proyecto es el uso únicamente de monedas estables pareadas con dinero fiat, con los inconvenientes para el depósito de valor a largo plazo que ello supone debido a la constante devaluación de las mismas.

B. Terra money

El protocolo Terra (Kereiakes et al., 2019) apareció casi al mismo tiempo que Haven (2018). El principio de funcionamiento de ambos es el mismo. En el caso de Terra, el token LUNA realiza las funciones de acciones que pueden ser siempre cambiadas por la cantidad equivalente de moneda estable UST al precio de 1$. La principal diferencia entre ambos es que Terra no cuenta con ninguna característica de privacidad, al contrario que Haven que está derivado de Monero.

La principal ventaja con la que cuenta Terra sin embargo es que se trata de una cadena de bloques construida utilizando el protocolo IBC de Cosmos, lo cual hace que sea plenamente interoperable con todas las demás cadenas de bloques construidas con dicho protocolo, lo que permite mover los activos de Terra por cualquiera de estas cadenas perfectamente. Además, recientemente Terra ha desplegado estos activos como tokens de Ethereum, ampliando aún más esa interoperabilidad. El enorme éxito que ha tenido el UST como moneda estable, ha hecho que incluso esté siendo adoptado por los intercambios centralizados, lo que lo coloca como el principal candidato a sustituir a las monedas centralizadas.

Un punto que genera muchas dudas sobre la estabilidad del protocolo Terra es la cuestión del suministro máximo de LUNA, que teóricamente es de 1000 millones de tokens. Imaginemos una situación en la cual se ha alcanzado dicho límite de suministro, y por tanto el protocolo impide la creación de más tokens LUNA. En dicha situación, si el valor de mercado total de los tokens LUNA cayera por debajo del valor de mercado total de la cesta de monedas estables que respalda, no sería matemáticamente posible que todos los tenedores de dichas monedas las pudieran redimir por su valor de paridad, lo que supondría el colapso del protocolo y la pérdida de paridad de las monedas. De hecho, el umbral de valor de mercado de LUNA en el que esta situación sería posible es mucho más alto porque no todo el suministro circulante se encuentra a disposición del módulo de mercado. Esto plantea una dicotomía:

- O bien existen unas condiciones de mercado en las cuales el protocolo no puede mantener su promesa de permitir la redención de 1$ de UST por 1$ de LUNA, con lo que dicha promesa es falsa,
- O realmente LUNA no tiene un suministro máximo, en cuyo caso los inversores operan bajo una premisa falsa (suministro limitado).

Actualmente el valor de mercado de LUNA es apenas el doble del valor de mercado total de UST. En un mercado bajista, en el que se produjera una caída del mercado mayor del 50% a la vez que la demanda de moneda estable aumenta, sería fácil encontrarse en una situación de quiebra técnica del protocolo. Sin embargo, es importante recalcar aquí que mientras los usuarios mantengan la confianza en el protocolo, una situación transitoria de este tipo no tendría por qué desencadenar el citado colapso. Recordemos que el sistema bancario tradicional opera de forma estable con un coeficiente de reservas de apenas el 2%, lo cuál quiere decir que solo ese porcentaje de los depósitos podría llegar a ser retirado en caso de que todo el mundo intentara hacerlo a la vez. Terra opera actualmente bajo un coeficiente de reservas cercano al 200%, 100 veces mayor que cualquier banco tradicional, lo que debería alejar definitivamente los temores a esa llamada *"espiral de la muerte"*.

Recientemente Terra ha comenzado a comprar grandes cantidades de activos de reserva de calidad, como Bitcoin y Avalanche, a través de la Luna Foundation Guard (LFG). El objetivo parece ser alejar los temores a la situación descrita en el punto anterior mediante la colateralización externa del protocolo. Aunque el objetivo perseguido es bastante deseable -reforzar la solvencia del protocolo-, la aproximación empleada sin embargo resulta cuestionable, pues no deja de ser plenamente centralizada. Al igual que sucede con las monedas estables centralizadas, ese colateral no es un activo dentro de la cadena de bloques, y no existe actualmente ningún mecanismo criptográfico que garantice a los tenedores de LUNA y UST la posibilidad de redimir estos frente al colateral, ni las condiciones en que dicho acceso al colateral sería posible.

Aunque Terra es probablemente el mejor protocolo de moneda estable que existe en la actualidad, sigue sin ser perfecto. Para empezar, tiene el mismo defecto que el resto de protocolos de moneda estable: la paridad con dinero fiat inherentemente inflacionario. Tampoco posee ninguna característica de privacidad, ni se espera que vayan a introducir ninguna. Por último, la reciente incorporación de componentes fuertemente centralizados en la gestión de los activos de reserva desdibuja la imagen de protocolo descentralizado que Terra mantenía hasta ahora.

C. Frax

Frax (2021) ha sido definido por sus creadores como el primer y único protocolo de moneda estable que combina un sistema de reserva fraccional (colateral) con un sistema algorítmico. Esta afirmación resulta cuestionable ya que Neutrino (Ivanov & Pupyshev, 2020) ya utilizaba un año antes de la creación de Frax un sistema de estabilización mixto para su USDN utilizando la moneda del protocolo WAVES como colateral y el token base del protocolo (NSBT) como contrapartida algorítmica para estabilizar el precio, lo que lo convertiría efectivamente en el primer protocolo de reserva fraccional que existió (en el ámbito de las criptomonedas, pues recordemos además que los bancos tradicionales llevan usando este sistema desde sus orígenes en el S. XVII). Tampoco puede considerarse a Frax como "único" ya que el sistema de reserva fraccional es simplemente una variante del sistema de colateralización en el que una parte del colateral es un token del protocolo, y existen otros proyectos algorítmicos como Terra, Deus y el ya mencionado Neutrino que tienen reservas de colateral.

El principio de funcionamiento del protocol Frax es idéntico al empleado por Haven y Terra, que fue propuesto por Mastercoin (2012, 2013) y Sams (2014), con la única diferencia de que a la hora de emitir o redimir la moneda estable no se emplean exclusivamente las acciones del protocolo (Frax Shares, FXS) sino una combinación en proporción variable de estas y un colateral compuesto por otras monedas estables.

Las monedas estables que componen el colateral de Frax son USDC, USDP, sUSD, DAI, FEI y LUSD, que como se ha visto son centralizadas o están compuestas por un colateral mayoritariamente centralizado. Según las propias estimaciones de Frax, el grado de centralización de su colateral estaría cerca del 70% actualmente.

La principal crítica que se puede hacer a este protocolo es la misma que a todas las demás monedas colateralizadas, y es precisamente esa gran dependencia de las monedas estables centralizadas, por los motivos que ya se han expuesto en este documento. La proliferación de protocolos dependientes de estas monedas no hace sino incrementar cada vez más el riesgo sistémico que estas suponen para las finanzas descentralizadas.

Frax ha anunciado recientemente su intención de elaborar en el futuro una moneda que siga al índice de inflación de EEUU (CPI), lo que podría convertirlo en el primer protocolo en lanzar esta idea al mercado. Sin embargo, dadas las diferencias de base que existen con nuestro protocolo, especialmente en las características de centralización, se trata de dos soluciones lo suficientemente diferenciadas para que puedan coexistir, siendo además deseable la existencia de competencia que fomente la innovación y el desarrollo dentro del ecosistema de las criptomonedas.

D. Deus Finance

Deus es una arquitectura de derivados digitales que proporciona la infraestructura para que otros puedan construir cualquier tipo de instrumento financiero: acciones sintéticas, CFDs, opciones, mercados de predicción, derivados OTC y futuros. Dentro de esta arquitectura, el token DEI ejerce la función de moneda estable empleada como medio de liquidación de los derivados. Además, gracias a un mecanismo de puenteo entre cadenas muy eficiente, DEI es una buena alternativa como moneda estable de uso general por sí misma.

El mecanismo de estabilidad del DEI es idéntico al utilizado por Frax, consistente en un sistema de reserva fraccional en el que un porcentaje del valor de la moneda estable está soportado por un colateral compuesto por otras monedas estables, y el resto por el propio token DEUS, por lo que todas las críticas que hemos hecho para Frax se mantienen para Deus: dependencia indirecta de entes centralizados, riesgo sistémico y riesgo de censura.

IV. EL PROTOCOLO GEMINON

Como se ha visto al analizar los protocolos de moneda estable existentes, hasta la fecha ningún proyecto ha llevado a la práctica las propuestas de Sams (2014) creando una moneda referenciada a un índice de precios de forma puramente algorítmica y descentralizada. Vista además la necesidad de protocolos que apuesten plenamente por la descentralización en los que los usuarios puedan refugiarse en caso de un evento de mercado que afecte a las monedas centralizadas y sus derivados colateralizados, proponemos la creación de un sistema que cumpla plenamente con estos objetivos. A continuación se detallan las características de dicho sistema.

A. La cuestión del suministro limitado

Uno de los primeros dilemas que surge al abordar el diseño de un sistema monetario es el relativo al suministro máximo de moneda. Aunque inicialmente podría parecer que lo mejor es adoptar un suministro limitado para el token que ejerce las funciones de acciones de señoreaje imitando a Bitcoin e incluso a protocolos similares como Terra, un análisis más detallado de los límites de estabilidad del protocolo desaconsejaría esta medida.

Tal y como se ha comentado al analizar Terra, no está muy claro si teniendo un suministro limitado el protocolo podría mantener la paridad de sus monedas estables en todas las circunstancias. Un sencillo análisis matemático muestra que en determinadas condiciones, bajo una restricción de suministro máximo de la moneda que realiza el papel de acciones de señoreaje el protocolo perdería la capacidad para redimir las monedas estables de los usuarios, lo que tendría el efecto de dejar a estos atrapados si no existiera otro medio para cambiarlas por otra. En caso de existir pares de cambio de la moneda en intercambios descentralizados, se produciría los usuarios podrían salir pero se produciría la pérdida de paridad de la moneda, al dejar de funcionar el mecanismo de arbitraje.

En presencia de *pools* de liquidez de la moneda en intercambios externos, si Alice decide vender su moneda estable en dichos *pools*, provocará una disminución del precio de esta frente a su paridad teórica, lo que abriría una oportunidad de arbiraje consistente en comprar la moneda en el *pool* y redimirla en el protocolo por su precio de paridad. Pero al estar agotada la capacidad del protocolo de redimir moneda estable por haberse alcanzado el suministro máximo, dicha operación no sería posible, por lo que el precio de la moneda en los *pools* externos seguiría bajando sin control, provocando una reacción en cadena que colapsaría el protocolo.

Por este motivo un sistema basado en acciones de señoreaje no debería tener límite de emisión de dichas acciones. Los mayores protocolos que existen actualmente que utilizan este mecanismo, Terra y Frax, tienen sin embargo un límite máximo de suministro en sus acciones, lo cual los coloca en riesgo de sufrir un evento de este tipo. Dicho riesgo es menor en el caso de Frax debido a su alto porcentaje (>85%) de colateralización. Sin embargo, el hecho de que ese colateral esté compuesto principalmente por monedas centralizadas, pone al protocolo en riesgo de que un evento de mercado asociado a dichas monedas provoque una reacción en cadena que ponga en peligro la paridad de sus monedas estables, aunque sea temporalmente.

Para solventar este riesgo, el protocolo debe contar, además de con la capacidad de emitir moneda dentro de los límites del suministro máximo inicial, con una reserva de acciones y activos de valor reconocido, y una vez agotadas ambas vías, debe existir además la posibilidad de emitir moneda más allá del suministro inicial máximo. Estas tres medidas aseguran que el protocolo cumple con su promesa de permitir la redención en cualquier circunstancia de las monedas estables por su valor de paridad.

B. Liquidez propiedad del protocolo

Una de las últimas ideas en incorporarse con éxito a las finanzas decentralizadas ha sido los programas de bonificación para que el protocolo se haga con la propiedad de la liquidez (Olympus, 2021). El objetivo de

esta idea, muy alabada por los analistas, es que el protocolo retenga las comisiones generadas por el intercambio de sus tokens, contribuyendo a su sostenibilidad y a aumentar los ingresos de los tenedores de tokens.

El mecanismo de bonding consiste a grandes rasgos en el establecimiento de recompensas en tokens de protocolo a los proveedores de liquidez que entreguen sus tokens LP (que representan la propiedad de un par de monedas depositado en un *pool* de liquidez) a cambio. La recompensa consiste en que se reciben dichos tokens del protocolo con un descuento respecto al precio de cotización actual tras un breve periodo de *vesting*, lo que equivale a recibir un bono denominado en tokens, de ahí el nombre del sistema.

Este sistema de bonos tiene sentido para aquellos protocolos que cuentan con un gran número de proveedores de liquidez externos y desean hacerse con la propiedad de dicha liquidez. Para un protocolo de nueva creación sin embargo, una vez vistos los beneficios de tener la liquidez en propiedad, tiene más sentido emplear una estrategia de despliegue de liquidez propia desde el principio que el pago de intereses de estos bonos. Por este motivo, el protocolo desplegará en su lugar una estrategia de *liquidez inteligente* destinados a gestionar el nivel de liquidez para maximizar los ingresos del protocolo por esta vía y la protección de los inversores frente a caídas del precio a medida que la capitalización de mercado aumenta.

C. Colateralización automática de la reserva del tesoro

Las buenas prácticas contables de cualquier organización dictan que esta disponga de una reserva de tesorería suficiente para afrontar cualquier imprevisto que pueda aparecer durante el ejercicio de su actividad. Geminon no es un protocolo de moneda estable colateralizada, en el sentido de que no se emiten dichas monedas como deuda respaldada por activos externos depositados por los usuarios ni tampoco se pueden redimir monedas estables frente al colateral (en condiciones normales). Sin embargo, a nivel global resulta interesante que el protocolo cuente con reservas de activos descentralizados considerados valores seguros en relación al conjunto de todos los criptoactivos existentes.

Aunque la discusión sobre qué puede considerarse un activo seguro en el entorno de las criptomonedas puede ser dura, aquí nos limitaremos a una visión conservadora de la cuestión, y definiremos activo seguro a los que cumplan estos cuatro criterios :

- Posición consolidada en el mercado con una clara posición de dominio sobre sus competidores
- Comunidad comprometida, tanto en el desarrollo futuro como en el uso y expansión
- Caso de uso sólido, con una demanda continua de la moneda asegurada
- Diseño económico no inflacionario.

Siguiendo estos criterios, los activos de reserva seleccionados serían :

- Las monedas nativas de las cadenas de bloques en las que se implementará nuestro protocolo: Ethereum, BNB y Avalanche inicialmente.
- Bitcoin
- El token del oráculo : Chainlink.

Una vez seleccionados los activos que se desea incorporar al tesoro, es necesario diseñar un mecanismo descentralizado y sin confianza que permita que los usuarios estén seguros de que dichos activos se incorporan puntualmente al tesoro, y que en caso de ser necesarios, podrán acceder a ellos. A este fin, se establecerá que un tercio de las acciones empleadas para la emisión de moneda serán empleadas para la compra a mercado de dichos activos. Para garantizar que se cumpla este procedimiento, este deberá quedar automatizado en un contrato inteligente. Del mismo modo, el contrato implementará las condiciones bajo las cuales los usuarios podrán redimir moneda estable frente a los activos de reserva en lugar de frente a las acciones del protocolo. En los siguientes puntos se profundizará sobre este mecanismo.

D. Préstamos del tesoro

Hasta ahora, la aproximación más utilizada por los protocolos de préstamo de criptomonedas ha sido dejar en manos de los usuarios la creación de la oferta de dichos préstamos. Geminon emplea una aproximación diferente, con un triple objetivo: simplificar la generación de beneficio a los usuarios, que no tendrán necesidad de elegir entre distintas alternativas para generar retornos, mejorar la liquidez disponible para préstamo y optimizar las tasas de interés.

Para lograr estos objetivos, el capital para los préstamos es proporcionado directamente por el tesoro del protocolo. Como la oferta de capital es conocida y estable, el protocolo puede optimizar la tasa de interés, variando esta en función del ratio entre préstamos de moneda estable y acciones (largos / cortos) y el porcentaje total del capital prestado.

E. Puente multicadena

Al analizar los protocolos existentes ha quedado clara la importancia estratégica de la interoperabilidad entre cadenas. En un protocolo de moneda como Geminon, esa capacidad de usar la moneda en diferentes cadenas en función de las necesidades de cada usuario cobra más importancia si cabe. Por este motivo, consideramos importante que el protocolo disponga desde su inicio de capacidades propias para migrar sus activos entre cadenas, garantizando a la vez la seguridad de las transacciones y un control adecuado del circulante total de tokens a lo largo de todas las cadenas.

Hoy en día no es raro encontrarse una gran cantidad de variantes de la misma moneda estable al operar en un DEX en cadenas como Solana o Avalanche, debido a las variantes introducidas por los puentes. Al emplear puentes de terceros, muchos protocolos no desarrollados inicialmente con mentalidad multicadena tienen que recurrir a proveedores de liquidez externos que faciliten la transferencia de activos a través del puente, lo cual da lugar a la duplicación de tokens por cada puente utilizado. Además, esto añade costes extra a los usuarios, que no solo tienen que pagar el coste de la transacción de puente, sino además swaps en la cadena inicial y de destino entre el activo que desean transferir y el activo auxiliar que emplea el puente.

Para evitar esto, Geminon contará con un puente nativo con capacidad de emitir y quemar moneda en la cadena de destino y origen, logrando de esta transferencias de liquidez ilimtada y por tanto con deslizamiento cero, sin necesidad de swaps intermedios ni tokens duplicados, y a un coste muy inferior al de soluciones externas. Y todo ello además reteniendo las comisiones del puente como beneficio paralos accionistas del protocolo.

F. Staking de moneda estable

Una parte fundamental de cualquier protocolo de finanzas descentralizadas es el diseño de un sistema adecuado de recompensas para atraer y fidelizar a los usuarios. El nivel de competencia en este mercado es probablemente uno de los más extremos que existen debido a la total ausencia de regulaciones que frenen la innovación y a la propia cultura de código abierto que impera en la comunidad. Por este motivo es necesario buscar un equilibrio entre un nivel elevado de recompensas y la sostenibilidad del protocolo a largo plazo.

Las recompensas del protocolo Geminon han sido diseñadas teniendo en cuenta estos principios. En lugar de distribuir estas recompensas usando el token del protocolo como suele ser habitual en otros proyectos, lo cual da lugar a movimientos del precio de tipo *pump & dump* o como mínimo a presiones inflacionistas extremas que terminan por deprimir el precio, Geminon encamina esta emisión de tokens de forma indirecta a través del staking de monedas estables. Esto logra un doble efecto:

- Mantener estable el circulante inicial de tokens, reduciendo al mínimo la presión inflacionaria debida a las emisiones iniciales y creando escasez de oferta en el mercado, lo que hace que todo incremento de la demanda se traduzca en crecimiento del precio del token.

- Crear un incentivo fuerte a la posesión de la moneda estable y atraer a los inversores gracias a una relación riesgo / beneficio inmejorable en la inversión.

Estos dos efectos se combinan formando un círculo virtuoso que genera crecimiento constante y sostenible. Al generar las recompensas en moneda estable, no es necesario compensar a los inversores por la volatilidad del token del proyecto con rentabilidades de 3 dígitos, lo que permite mantener unas emisiones sostenidas en el tiempo hasta que el número de usuarios crezca lo suficiente para generar ingresos de forma autosuficiente a través de las comisiones del protocolo.

G. Ingresos del protocolo

Al igual que sucede con cualquier organización, la sostenibilidad a largo plazo de todo protocolo de criptomoneda depende de la capacidad de este para generar ingresos con los que recompensar a los accionistas. Para lograr esto, es necesario que el protocolo guarde la mayor cantidad posible de vías de ingreso derivadas del uso de sus tokens. En nuestro caso, dichas vías serían:

- Señoreaje: comisiones por la emisión y redención de moneda estable.
- Permutas internas: comisiones por comercio entre las diferentes monedas estables del protocolo.
- Permutas externas: comisiones por comercio en intercambios descentralizados externos, en los que el protocolo es propietario de la liquidez de los *pools* de liquidez.
- Puente entre cadenas: comisiones por el traslado de activos del protocolo entre diferentes cadenas de bloques.
- Préstamos. Tasas de interés y comisiones derivadas de los instrumentos de apalancamiento y venta en corto.
- Arbitraje. Ingresos obtenidos por operaciones de arbitraje para asegurar la paridad de precios en los intercambios externos.

Adicionalmente, el importe de estas comisiones podría tener un carácter variable, actuando como una suerte de política fiscal del protocolo que tenga un efecto anticíclico para reducir la volatilidad de los tokens como veremos en el punto siguiente.

H. Estabilizadores automáticos

Se ha argumentado que los protocolos de emisión de moneda puramente algorítmicos presentan ciertos riesgos de cola que pueden manifestarse en momentos de extrema volatilidad si se produce una pérdida masiva de confianza de los inversores y estos deciden abandonar de forma desordenada el protocolo. Si bien en nuestra opinión estos riesgos no son mayores de los que pueden existir en el sistema bancario tradicional, donde recordemos se mantiene menos de un 2% de los depósitos de los clientes en reserva, lo que significa que en caso de una corrida bancaria se produciría el colapso del sistema, el principio de diligencia debida en el diseño económico del protocolo invita a tomar en cuenta estos riesgos y lidiar con ellos adecuadamente.

Se han mencionado ya los mecanismos de capitalización del tesoro mediante reservas en criptoactivos de primera calidad y la posibilidad de deslimitar el suministro máximo de acciones como último recurso para asegurar que se mantiene siempre el tipo de cambio de la moneda estable. Estos mecanismos deberían brindar protección suficiente al protocolo en todas las condiciones de mercado, pero aquí debe tenerse en cuenta también la posibilidad de un ataque económico, donde un actor malintencionado con grandes recursos financieros intentara desestabilizar el protocolo mediante ventas masivas instantáneas para tratar de inducir al pánico al resto de inversores.

Para atajar un escenario de pánico o ataque por venta masiva o simplemente para amortiguar la volatilidad propia de los ciclos del mercado sin recurrir a soluciones centralizadas y poco elegantes como pausar los contratos inteligentes, es necesario introducir mecanismos de estabilización económica mediante incentivos y penalizaciones. En el caso de la redención de moneda estable para vender las acciones, el mecanismo

consistiría en introducir una comisión de venta dinámica proporcional al porcentaje del suministro total de moneda destruido en las últimas 24 horas, desincentivando de este modo las ventas masivas a partir de un cierto umbral y asegurando la estabilidad del protocolo al aumentar el valor de este.

V. El ataque de arbitraje

Una posible causa de que ningún proyecto haya logrado implementar todavía la idea de Sams (2014) de vincular el precio de una moneda algorítmica a un índice de precios, es el problema del ataque de arbitraje. Dado que en la actualidad todavía es una cuestión por resolver el cómo medir en tiempo real el precio de los bienes de consumo en el mundo exterior, ponderarlos y llevar estos datos de forma descentralizada y verificable a una cadena de bloques, es necesario emplear la aproximación propuesta originalmente por Sams (2014) de emplear un índice precios al consumo, como por ejemplo el CPI que publica la Reserva Federal.

El problema que surge de la aplicación de esta idea es que dicho índice de referencia se publica con una determinada periodicidad que es conocida de antemano. Supongamos que se conoce el momento de la publicación del dato, y se utiliza un oráculo Ω para obtener un consenso verificable sobre dicho dato dentro de la cadena de bloques. Si el protocolo del oráculo tarda un tiempo T_Ω en llegar a un consenso sobre el dato y propagarlo a la cadena de bloques, y dicho dato implica una alteración instantánea del precio del activo X de valor Δ, entonces cualquiera que pueda realizar una operación sobre X en un tiempo inferior a T_Ω puede obtener un beneficio libre de riesgo proporcional a Δ, puesto que conoce de antemano el valor futuro del activo antes de que este refleje el cambio, lo que permite realizar una operación de arbitraje temporal. El beneficio de esta operación se obtendría en perjuicio de los tenedores de las acciones de señoreaje, por lo que un atacante podría utilizar este explotable para drenar sistemáticamente el valor del protocolo.

La solución de este problema resulta clave para una implementación viable de una moneda que siga a un índice de precios público y discreto. El protocolo Geminon soluciona este problema de una forma robusta y elegante que asegura la imposibilidad de llevar a cabo ataques de arbitraje, sin la necesidad de imponer altas comisiones de transacción a sus usuarios.

VI. Extensiones del protocolo

Este punto será objeto de un análisis en mayor profundidad en futuras versiones de este documento. A día de hoy, podemos enumerar como posibles extensiones las siguientes:

A. Capa de privacidad

La privacidad es un derecho básico, y por extensión la privacidad de las transacciones financieras forma parte de ese derecho. Aunque las cadenas de bloques compatibles con Ethereum (EVM) no cuentan actualmente con funciones nativas que permitan la privacidad de las transacciones, existen protocolos que utilizan la funcionalidad de los contratos inteligentes para proporcionar dicha privacidad (Tornado Cash, 2019).

B. Índice de precios descentralizado

Los índices de precios al consumo que elaboran los organismos oficiales han sido ampliamente criticados en los últimos tiempos por mostrar datos de inflación sistemáticamente inferiores a los que la gente observa en el día a día. Además, si lo que buscamos es la máxima descentralización, la dependencia de un emisor centralizado para los datos de importancia estratégica del protocolo parece desaconsejable. La búsqueda por tanto de mecanismos que permitan la obtención de estos datos de una forma puramente descentralizada es un objetivo deseable para una futura extensión del protocolo.

VII. CONCLUSIÓN

Las monedas estables son una pieza clave del ecosistema de las criptomonedas, sin cuya existencia no hubiera sido posible alcanzar el nivel de desarrollo logrado en los últimos años en las finanzas descentralizadas (DeFi). A pesar de la variedad de soluciones algorítmicas desarrolladas para brindar precios estables, más del 95% de la capitalización de mercado actual de las monedas estables proviene directa o indirectamente de emisores centralizados que han implementado mecanismos de censura en sus contratos inteligentes. Esto plantea un grave riesgo sistémico para todo el mercado que hace necesario promover la adopción de soluciones puramente algorítmicas o garantizadas por activos totalmente descentralizados.

Además del riesgo que representa el uso extensivo de criptomonedas centralizadas, el mismo hecho de utilizar como referencia el precio de las monedas fiduciarias expone a sus tenedores a la devaluación progresiva de sus activos cuando estos deciden no exponerse a la volatilidad de los criptoactivos no estables durante un mercado bajista.

Para tratar de paliar estos problemas, proponemos un nuevo tipo de moneda súper estable no referenciada fijamente a una moneda fiduciaria, sino a un índice de precios asociado a ella, con respaldo puramente algorítmico y una tesorería compuesta por criptoactivos descentralizados de primera calidad. Además, proponemos la implementación de mecanismos que permitan mejorar la privacidad de las transacciones utilizando contratos inteligentes como proxy.

REFERENCIAS

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. 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.

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.

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.

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

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