Geminon: un protocolo de criptomonedas supraestables

Herederos de Satoshi

geminon.fi

Primera versión: 8 de abril de 2022

Esta versión: 2 de junio 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.

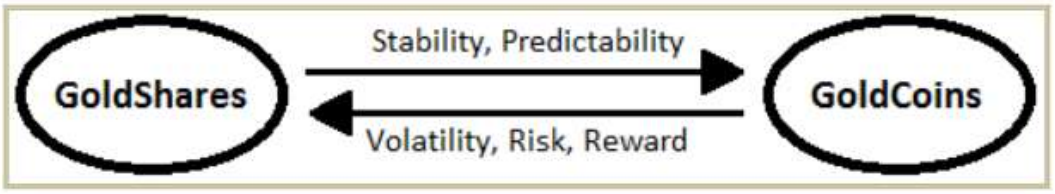

Figura 1: mecanismo de estabilidad algorítmico propuesto por Mastercoin (2012)

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.

Otro de los intentos de crear una moneda estable algorítmica vino de Bitshares (Larimer et al., 2014), que utilizaba también un sistema compuesto por dos monedas (Bitshares / BitUSD) aunque con un principio de funcionamiento basado en un contrato de derivados. El mecanismo de estabilidad consistía en que si BitUSD cotizaba por debajo de su paridad de 1$, los traders lo comprarían a mercado (se pondrían largos), y si cotizaba por encima de 1$ deberían realizar una operación de venta al descubierto (ponerse cortos) depositando BitShares a 30 días en concepto de garantía (colateral) para emitir nuevas unidades de BitUSD que se venderían a mercado, incrementando la oferta monetaria para bajar el precio y restaurar la paridad.

El protocolo Basis (Al Naji et al., 2018) introdujo un innovador sistema algorítmico basado en el uso de tres tokens: acciones, moneda estable y bonos. El sistema propuesto funcionaba así:

- Cuando la moneda estable se encuentra por encima de su precio objetivo y era necesario reducir el suministro, el sistema iniciaba una subasta de bonos que solo podían comprarse pagando con moneda estable.
- Cuando la moneda estable se encuentra por debajo de su par y es necesario aumentar el suministro, el sistema emitía nueva moneda estable que se empleaba para recomprar los bonos emitidos (en caso de existir), pagando la rentabilidad correspondiente a sus tenedores, y en caso de seguir siendo necesario emitir más moneda estable tras liquidar todos los bonos, esta se entregaba como un dividendo prorrateado a los poseedores de las acciones (señoreaje).

Además de su innovador sistema algorítmico, Basis también proponía la idea de que la moneda estable convergiera en el futuro al valor del CPI en lugar de al del dólar, en caso de lograr una adopción masiva. Lamentablemente, el proyecto nunca llegó a ver la luz debido a presiones regulatorias de la SEC en EEUU, que obligaron a cerrarlo y devolver los más de 100 millones $ recaudados entre los mayores fondos de capital riesgo del momento.

El principal obstáculo para la implementación de una moneda referenciada a un índice de precios en todos los proyectos que propusieron esta idea con anterioridad a 2018 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 o al menos pospuesta 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 muy recientemente ningún proyecto se ha propuesto su implementación, 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 colateralizada 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

En los últimos años, las monedas estables han sido objeto de varios estudios académicos, y se han propuesto varias taxonomías atendiendo al tipo de colateral usado, objetivo de paridad y mecanismo tecnológico (Mundt et al, 2020).

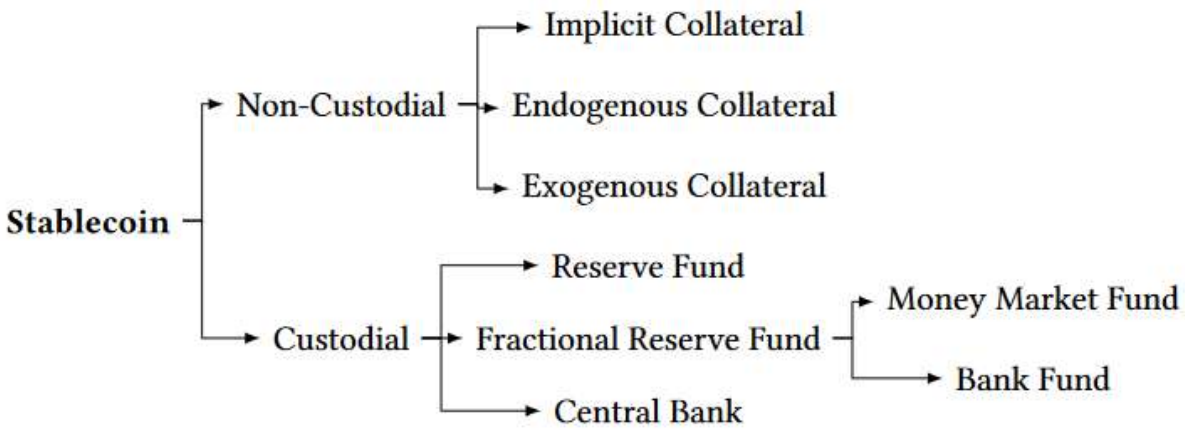

Figura 2: visión general del espacio de diseño de las monedas estables (Mundt et al. 2020)

En este documento, realizaremos la clasificación atendiendo al nivel de descentralización que proporcionan el sistema de custodia y la composición del colateral de forma combinada.

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 3: 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 colateralizadas

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.

FRAX emplea como colateral únicamente otras monedas estables, tanto centralizadas como colateralizadas (que como ya hemos visto resultan ser en su mayoría también dependientes de las centralizadas).

Sperax (2021) es una copia de FRAX que emplea exactamente el mismo modelo de reserva fraccional utilizando como colateral una cesta de monedas estables, compuesta únicamente por USDT y USDC en este momento, lo que lo convierte en una alternativa aún más centralizada al proyecto que copia.

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 que logró adopción masiva fue 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.

3) Acciones combinadas con bonos

La última variante de monedas estables algorítmicas la componen los sistemas de tres tokens que siguen el modelo ideado para el protocolo Basis en 2018.

Neutrino (Ivanov & Pupyshev, 2020) fue el primer protocolo en recuperar la idea de un sistema de estabilización mixto de tres tokens para su USDN utilizando la moneda del protocolo WAVES como colateral y el token NSBT como bono que se emite cuando el valor del colateral está por debajo del valor del USDN emitido, o cuando el USDN se encuentra por debajo de su valor objetivo. En los últimos meses ha tenido grandes problemas para mantener la paridad, cotizando sistemáticamente por debajo de su objetivo.

Empty Set Dollar (2020) intentó replicar el mismo mecanismo propuesto por Basis. El precio del ESD no logró mantenerse estable a 1$, y el protocolo terminó colapsando poco después de su lanzamiento. Idéntica suerte corrió Dynamic Set Dollar (2020), una copia de ESD lanzado casi al mismo tiempo.

Beanstalk (Publius, 2021) ha sido el último proyecto en utilizar un sistema algorítmico complejo basado en la emisión de deuda para mantener estable el precio del BEAN. El sistema propuesto fue capaz de lograr estabilidad de precios tras 4 meses de fuertes oscilaciones iniciales, pero terminó colapsando debido a una vulnerabilidad en los smart contracts que permitió que un ataque de préstamo flash robara todos los fondos del protocolo.

III. PROTOCOLOS EXISTENTES CON MECANISMO DE SEÑOREAJE

Se han hecho varios intentos de poner en práctica la idea de un sistema dual con acciones de señoreaje para estabilizar una moneda. Casi todos los intentos de implementar monedas algorítmicas sin utilizar colateral exógeno han fallado, aunque recientemente algunos protocolos han tenido cierto éxito creando monedas estables de este tipo. En este punto analizamos algunos de estos proyectos recientes.

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.

Debido a la baja adopción y liquidez del protocolo, el precio en los pocos sitios externos en los que cotiza el xUSD experimenta fuertes fluctuaciones. Durante el colapso de Terra, el xUSD se vió afectado llegando a cotizar a 0,90 $, aunque posteriormente fue capaz de volver a recuperar la paridad.

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.

El protocolo Terra colapsó por completo durante los días del 9 al 13 de mayo de 2022, en un efecto dominó característico del fallo de las monedas estables algorítmicas denominado “espiral de la muerte”, y que había sido advertido por algunos analistas en los meses anteriores, produciéndose la pérdida definitiva de la paridad del UST con el dólar y la caída del precio de Luna a prácticamente 0 $, teniendo incluso que detenerse la blockchain debido al riesgo de ataques sobre esta al emplear un algoritmo de Proof of Stake para la validación.

Un punto que en su momento generaba muchas dudas sobre la estabilidad del protocolo Terra era la cuestión del suministro máximo de LUNA, que teóricamente era 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 era mucho más cercano porque no todo el suministro circulante se encontraba a disposición del módulo de mercado. Esto planteaba una dicotomía:

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

Durante el colapso del protocolo, se pudo comprobar que la respuesta correcta era esta última, pues cuando se desencadenó el pánico entre los inversores y el valor total de mercado de Luna cayó por debajo del de UST, el protocolo comenzó a acuñar billones de tokens Luna, creando una espiral hiperinflacionaria que llevó el precio del token prácticamente a cero.

La causa de colapso de Luna fue una implementación deficiente del *módulo de mercado*, que era el corazón del protocolo puesto que era el punto donde debía hacerse efectiva la promesa de que “siempre se podía redimir 1$ de UST por 1$ de Luna”, y por tanto era el punto del que nacía el arbitraje que permitía preservar la paridad en el resto de exchanges. Este módulo tenía varios defectos importantes de diseño:

- Estaba diseñado como un pool de liquidez de producto constante, derivado de los que se emplean en Uniswap, que totalmente inadecuado para mantener un mecanismo de estabilidad de precios ya que cualquier desequilibrio en la liquidez del pool (como el que se produciría durante un pánico de

mercado) podía hacer que dejara de funcionar correctamente, introduciendo un gran deslizamiento en el valor de referencia del UST como finalmente sucedió.

- Los desarrolladores introdujeron limitaciones al volumen diario de moneda estable que se podía redimir en el módulo de mercado, introduciendo una comisión variable con el objetivo de disuadir grandes salidas de UST. Esto sin embargo tuvo un efecto no previsto al afectar al precio efectivo de redención, y es que el valor objetivo de arbitraje que determinaba el precio de UST en el mercado quedaba fijado sistemáticamente por debajo del valor teórico de 1$ en caso de superarse ese límite diario, como pasó cuando se inició el colapso, haciendo imposible que la moneda estable pudiera recuperar la paridad de forma rápida, lo que generó alarma y finalmente pánico en el mercado.

La combinación de estos dos defectos de diseño propició un círculo vicioso, en el que a medida que el UST permanecía más tiempo por debajo de su valor objetivo más inversores entraban en pánico vendiendo, y estas ventas acrecentaban tanto el deslizamiento como las comisiones del módulo de mercado, fijando un precio efectivo de arbitraje del sistema aún más alejado de la paridad. Este diseño inherentemente inestable del sistema fue la causa última de que se produjera una "espiral de la muerte" que terminó por colapsar completamente el protocolo.

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.

El principio de funcionamiento del protocolo 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.

Frax anunció a principios de este año su intención de elaborar en el futuro una moneda que siga al índice de inflación de EEUU (CPI), casi al mismo tiempo que el proyecto Geminon fue creado, y recientemente han lanzado el token FPI para este fin.

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.

Recientemente, tras el colapso de Terra, DEI ha perdido la paridad con el dólar y está teniendo bastantes problemas para recuperarla.

IV. EL PROTOCOLO GEMINON

Geminon fue concebido inicialmente como un protocolo principalmente algorítmico, con un diseño a medio camino entre Frax y Terra. Sin embargo, el reciente colapso de este último hizo aconsejable replantear el diseño del protocolo, situándolo ahora plenamente en la misma categoría que Frax. Sin embargo, el protocolo Geminon no es similar a Frax, sino más bien un antagonista:

	FRAX	GEMINON
Tipo de colateral	Monedas estables	Activos variables
Fuente del colateral	Mayoritariamente centralizado	Mayoritariamente descentralizado
Nivel de colateral	Predeterminado	Variable
Aplicación del colateral	Moneda estable	Token del protocolo
Emisión de tokens del protocolo	Discrecional	Minería de colateral
Foco del protocolo	Moneda fiat USD	Índices de inflación USD y EUR

Además de estas diferencias, el protocolo Geminon incorpora importantes novedades, como el uso de oro tokenizado como activo de reserva, la disposición del colateral como liquidez del protocolo, la minería de colateral y el uso de nuevos pools con algoritmos de creación automática de mercado (AMM) avanzados.

A continuación detallamos las principales características del protocolo.

A. Pool de Liquidez Génesis (GLP)

Tomando como base el concepto de *Liquidity Bootstrapping Pool* (LBP) de Balancer (Martinelli & Mushegian, 2019), hemos creado un diseño propio de pool inteligente que permite estrategias de AMM paramétricas. Gracias a este diseño obtenemos la flexibilidad requerida en los pools de colateral del protocolo para hacer posibles ciertas características del protocolo que no serían posibles empleando un pool de liquidez normal:

- Posibilidad de crear un pool desde cero, con únicamente uno de los dos tokens. Esto permite el lanzamiento de proyectos sin liquidez inicial, algo que no era posible hasta ahora.
- Adicionalmente, es posible también definir un tramo de suministro inicial de un token a precio constante, lo que permite realizar una IDO (Initial DEX Offering) de forma autónoma.
- Emisión / quema de tokens desde el pool, habilitando características como la minería de liquidez y el control del invariante del pool y con ello de la curva de respuesta del precio.
- Provisión de liquidez para la redención de moneda estable, asegurando que estas tienen siempre un 100% de liquidez de salida y nunca se producen situaciones de bloqueo o pérdida de paridad por falta de liquidez en el pool de estables.
- Préstamos desde el pool, habilitando la opción de préstamos de los activos del colateral que se comenta más detalladamente en los puntos siguientes.
- Rebalanceos automáticos de colateral, permitiendo modificar el peso deseado de cada activo que compone el colateral con una transición suave entre estados.
- Gestión personalizada de las comisiones generadas por el pool.

De entre todas las características que permite implementar el GLP la más importante para Geminon es probablemente la capacidad de alterar de forma dinámica la curva de respuesta de precio del token GEX mediante la variación del suministro de tokens en el pool.

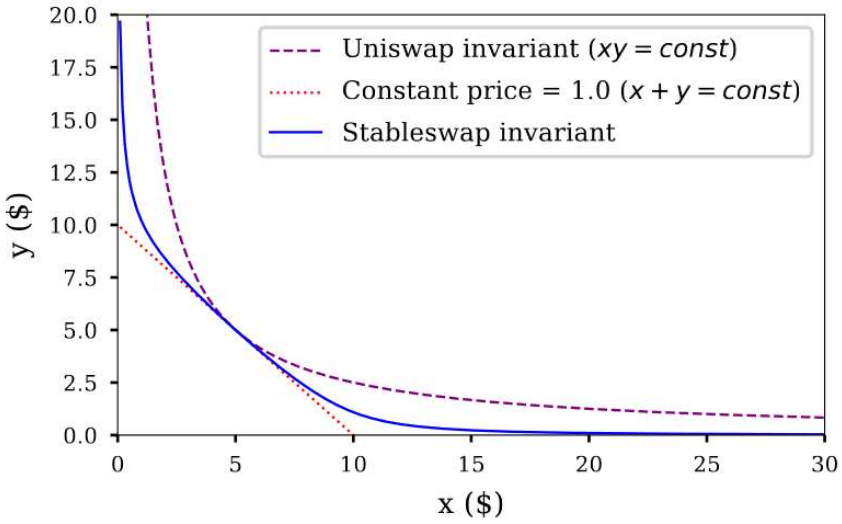

Figura 4: Comparación de los invariantes de Curve y Uniswap (Egorov, 2019)

En un pool de producto constante, como los empleados por Uniswap y la práctica totalidad de los DEX existentes, el precio de un token es una función cuadrática de la cantidad del segundo token con el que forma el pool:

$$Q_x Q_y = K$$

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

Esto hace que el precio se comporte de forma exponencial ante variaciones lineales del colateral depositado en el pool, siendo este comportamiento especialmente acusado cuando el balance del token en el pool se reduce excesivamente.

Las simulaciones realizadas con el smart contract muestran que durante la etapa de crecimiento en la adopción del protocolo, cuando la cantidad de moneda estable emitida se multiplica por 10, y con ello el colateral depositado en el pool, el precio del token GEX se multiplica por 100. Aunque este comportamiento puede parecer deseable en un principio ya que genera importantes ganancias a los poseedores del token del protocolo, debe tenerse en cuenta que también funciona a la inversa: las caídas en la cantidad de colateral depositado implican caídas superiores en el precio del token. Este "apalancamiento" que se produce en un pool de producto constante es una consecuencia de tener una oferta totalmente inelástica a la demanda, es decir, un balance fijo.

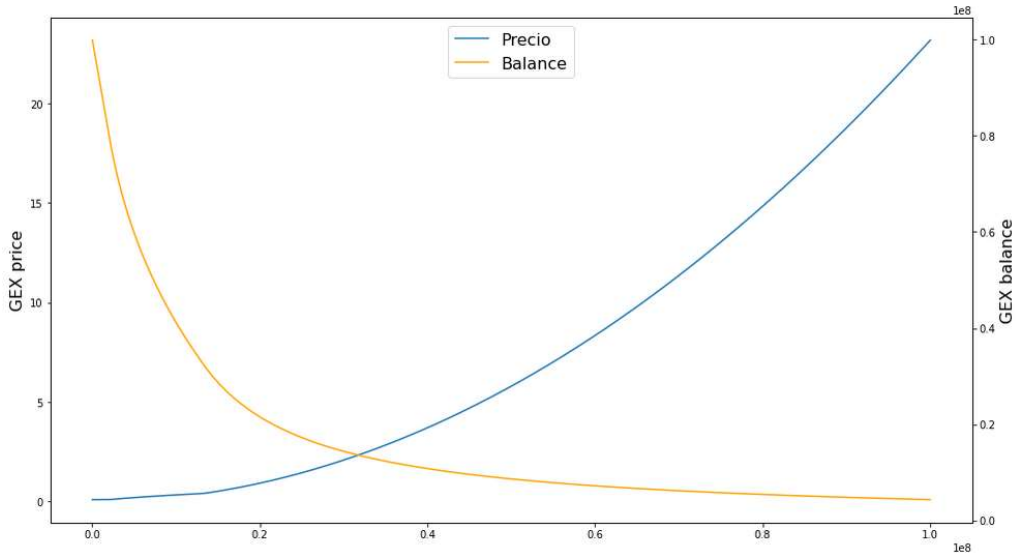

Figura 5: Simulación de precio del token GEX en función del balance del pool

La capacidad del GLP de emitir y quemar tokens permite hacer que la oferta sea elástica, lo que implica variaciones más suaves del precio ante cambios en la demanda. En la etapa madura del protocolo, se puede variar dinámicamente el coeficiente de emisión y quema de tokens en los pools de colateral, pudiendo lograrse una respuesta lineal e incluso amortiguada del precio frente a los cambios en el nivel de colateral, logrando de esta forma cumplir la promesa del protocolo de una volatilidad inferior a la de los activos subyacentes. Se trata de una aproximación que produce resultados equivalentes a la propuesta de concentración de liquidez de Curve (Egorov, 2021), aunque empleando un método diferente.

B. Emisión de moneda estable

El objeto principal del protocolo Geminon es la emisión de monedas supraestables, que son aquellas que presentan estabilidad frente a los precios de los bienes de una economía en lugar de frente a una moneda fiat inflacionaria.

El mecanismo de emisión es algorítmico, siendo necesario depositar el mismo valor en tokens GEX que se pretende emitir en moneda estable, y viceversa. El precio de la moneda estable se determina a partir de los datos obtenidos por el oráculo del índice de inflación (CPI) asociado a la moneda en cuestión. El valor objetivo se obtiene de forma predictiva, de forma que la moneda descuenta en tiempo real las expectativas de inflación del periodo actual en lugar de ir retrasada un periodo como sucede en el caso del FPI de Frax.

El módulo de emisión de moneda estable de Geminon está diseñado de forma que un evento como el de Terra no sea posible:

- Las comisiones que cobra el protocolo por emisión / redención de monedas estables son fijas, de forma que no afecten al precio efectivo de arbitraje y no contribuyan a desviar la moneda de su valor de paridad.
- El módulo no es un pool de liquidez, sino un mecanismo de emisión y quema de tokens con liquidez infinita, y por tanto opera sin deslizamiento, lo que garantiza un arbitraje eficiente en todas las circunstancias de mercado. En caso de que se agote el balance de tokens GEX del contrato, este puede tomarlo del balance de los GLP en pequeños incrementos, provocando que el precio del token suba como respuesta a la escasez relativa que existe del mismo. Aunque resulte contraintuitivo, una redención masiva de moneda estable en el protocolo podría provocar en determinadas condiciones una subida instantánea de precio del token GEX en lugar de una caída. En este caso se aprovecharía la

característica de la curva de producto constante de los pools de liquidez, que hace imposible el agotamiento del balance, para poder atender cualquier volumen de redenciones sin colapsar el protocolo imprimiendo tokens del aire como sucedió con Terra.

En el lanzamiento del protocolo estará disponible únicamente una moneda supraestable referenciada a la inflación del US dólar, y brevemente después se añadirá otra indexada al euro, siendo posible realizar intercambios directos (swaps) entre ambas. En el futuro se estudiará la adición de otras monedas, incluyendo también monedas estables referenciadas directamente a fiat.

C. Préstamos del tesoro

La incorporación de un sistema de préstamo de tokens es ya habitual en todos los protocolos DeFi, La novedad introducida por Geminon, aprovechando las características únicas de colateralización ya explicadas, es introducir la posibilidad de préstamos del colateral depositado en los pools.

Esta práctica, sobre la que se sustenta el negocio del sistema bancario tradicional, permite al protocolo obtener ingresos adicionales. El sistema no competiría con los préstamos realizados por los usuarios, ya que estos últimos se limitarían al token del protocolo y las monedas estables, mientras que el tesoro se encargaría de realizar préstamos de los activos de reserva, ampliando así enormemente la oferta de activos disponibles para préstamo.

El tipo de interés de los préstamos del tesoro se calcula en función de un coeficiente de reserva que mide qué porcentaje total de los pools de colateral se ha prestado. Esto hace que si existe una oferta de capital elevada o poca demanda de préstamo el tipo de interés tienda a cero, mientras que si existe baja oferta (porcentaje de colateral prestado elevado) o alta demanda, los tipos de interés suban aumentando los ingresos del protocolo y evitando un excesivo descenso del coeficiente de reservas.

D. 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 forma transferencias de liquidez ilimitada 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 para los accionistas del protocolo.

E. 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 y pools de colateral.
- 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 será variable, en función de parámetros como el tamaño y dirección de la orden y la volatilidad.

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). Una posible extensión futura del protocolo podría incluir alguna variante de esta tecnología, que sin tratarse de una copia de Tornado o sin pretender alcanzar el mismo nivel de privacidad, permitiera al menos a los usuarios anonimizar las pequeñas transacciones diarias, lo cual es un requisito necesario para una adopción generalizada segura de las criptomonedas.

B. Gobernanza

Otro punto importante de cara al desarrollo futuro de la plataforma es la implementación de mecanismos que permitan, una vez alcanzados los objetivos principales desarrollo y crecimiento del proyecto, delegar la gestión de este a la comunidad, desterrando así cualquier riesgo futuro derivado de una gestión centralizada.

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 un nuevo modelo de respaldo mixto algorítmico con colateralización completa del token del protocolo y una reserva compuesta por criptoactivos de primera calidad, incluyendo como novedad el oro tokenizado. También presentamos un nuevo tipo de pool de liquidez con un sistema AMM avanzado que permite estrategias complejas de gestión del colateral y el suministro de tokens. Además, proponemos la implementación de mecanismos que permitan mejorar la privacidad de las transacciones utilizando contratos inteligentes como proxy.

REFERENCIAS

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

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

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

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

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

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

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

Haven Protocol (2018). Private Decentralized Finance v3.

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

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

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

Lee, J. (2014). Nu Whitepaper.

MakerDao (2017). The Dai Stablecoin System.

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

Mastercoin (2012). The second Bitcoin Whitepaper.

Mastercoin (2013). Mastercoin Complete Specification.

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

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

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

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

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

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

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

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

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

Sperax Research (2021) - USDs Whitepaper.

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

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

USDD (2022). Decentralized Stablecoin Protocol v1.1