Rai: Un colateral de baja Volatilitad y de Confianza Minimizada para el Ecosistema DeFi

Stefan C. Ionescu, Ameen Soleimani

Mayo 2020

Resumen. Presentamos un protocolo descentralizado y de gobernanza minimizada que reacciona automáticamente a las fuerzas del mercado para modificar el valor objetivo de su activo colateral nativo. El protocolo permite a cualquier persona aprovechar sus criptoactivos y emitir un "índice reflejo", que es una versión amortiguada de su colateral subyacente. Describimos cómo los índices pueden ser útiles como colateral universal de baja volatilidad que puede proteger a sus tenedores, así como a otros protocolos financieros descentralizados, de cambios repentinos del mercado. Presentamos nuestros planes para ayudar a otros equipos a lanzar sus propios sintéticos aprovechando nuestra infraestructura. Por último, ofrecemos alternativas a las estructuras de gobierno y oráculos actuales que a menudo se encuentran en muchos protocolos DeFi.

Contenido

Introducción

El dinero es uno de las herramientas colaborativas más poderosas que la humanidad emplea para prosperar. El privilegio de controlar la oferta monetaria ha residido históricamente en las manos del liderazgo de los estados soberanos y la élite financiera, siendo por lo general impuesta a un público inconsciente. Mientras que Bitcoin ha demostrado su potencial reivindicativo de base manifestándose como un activo de reserva de valor, Ethereum nos brinda una plataforma para construir instrumentos sintéticos respaldados por activos que pueden proteger de la volatilidad y usarse como colateral, o anclarse a un precio de referencia y usarse como medio de intercambio para transacciones diarias, cumpliendo todos ellos con los principios del consenso descentralizado.

El acceso sin restricciones a Bitcoin para almacenar riqueza y los instrumentos sintéticos debidamente descentralizados en Ethereum sentarán las bases para la próxima revolución financiera, proporcionando a aquellos que se encuentran en los márgenes del sistema financiero moderno los medios para coordinarse en torno a la construcción del nuevo sistema.

En este documento, presentamos un marco para la construcción de índices reflejos, un nuevo tipo de activo que ayudará a que se desarrollen otros sintéticos y establecerá un pilar clave para toda la industria financiera descentralizada.

Descripción general de los índices reflejos

El propósito de un índice reflejo no es mantener una paridad específica, sino amortiguar la volatilidad de su colateral. Los índices permiten que cualquier persona aumente su exposición al mercado de criptomonedas sin la misma escala de riesgo que tener criptoactivos reales. Creemos que RAI, nuestro primer índice reflejo, tendrá una utilidad inmediata para otros equipos que emiten sintéticos en Ethereum (por ejemplo, MakerDAO's Multi-Collateral DAI [1], UMA [2], Synthetix [3]) porque les da a sus sistemas una menor exposición a activos volátiles como ETH y ofrece a los usuarios más tiempo para salir de sus posiciones en caso de un cambio significativo en el mercado.

Para comprender los índices reflejos, podemos comparar el comportamiento de su precio de canje con el del precio de una moneda estable (stablecoin).

El precio redención es el valor de una unidad de deuda (o moneda) en el sistema. Está destinado a ser utilizado sólo como una herramienta de contabilidad interna y es

diferente del precio de mercado (el valor al que el mercado está negociando la moneda). En el caso de monedas estables respaldadas por dinero fiduciario como el USDC, los operadores del sistema declaran que cualquiera puede canjear una moneda por un dólar estadounidense y, por lo tanto, el precio de canje de estas monedas es siempre uno. También hay casos de monedas estables respaldadas por criptografía, como el DAI Multi-colateral (MCD) de MakerDAO, donde el sistema tiene como objetivo una paridad fija de un dólar estadounidense y, por lo tanto, el precio de canje también se fija en uno.

En la mayoría de los casos, existirá una diferencia entre el precio de mercado de la moneda estable y su precio de canje. Estos escenarios crean oportunidades de arbitraje donde los traders crearán más monedas si el precio de mercado es más alto que el de canje y cambiarán sus monedas estables por colateral (por ejemplo, dólares estadounidenses en el caso del USDC) en caso de que el precio de mercado sea más bajo que el precio de canje.

Los índices reflejos son similares a las monedas estables porque también tienen un precio de redención que apunta el sistema. La principal diferencia en su caso es que su redención no permanecerá fija, sino que está diseñada para cambiar mientras está influenciada por las fuerzas del mercado. En la Sección 4 explicamos cómo el precio de redención de un índice flota y crea nuevas oportunidades de arbitraje para sus usuarios.

Filosofía de Diseño y Estrategia de Comercialización

Nuestra filosofía de diseño es priorizar la seguridad, la estabilidad y la velocidad de suministro.

La moneda Multi-colateral DAI fue el punto de partida natural para comenzar a iterar el diseño de RAI. El sistema ha sido auditado y verificado formalmente, tiene dependencias externas mínimas y ha reunido una comunidad activa de expertos. Con el fin de minimizar el esfuerzo de desarrollo y comunicación, queremos realizar sólo los cambios más simples respecto al código base original MCD para lograr nuestra implementación.

Nuestras modificaciones más importantes incluyen la introducción de un fijador de tarifas autónomo, un medianizador de redes de oráculos que está integrado con muchas fuentes de precios independientes y una capa de minimización de gobernanza destinada a aislar el sistema tanto como sea posible de la intervención humana.

La primera versión del protocolo (Etapa 1) solo incluirá el fijador de tasas y otras mejoras menores en la arquitectura central. Una vez que demostremos que el fijador

funciona como se espera, podemos agregar de manera más segura el medianizador de oráculos (Etapa 2) y la capa de minimización de gobernanza (Etapa 3).

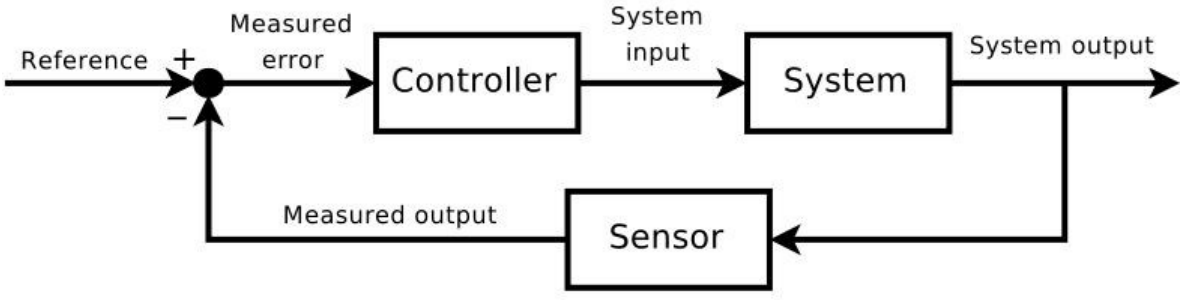
Mecanismos de Política Monetaria

Introducción a la Teoría de Control

Un sistema de control común con el que la mayoría de la gente está familiarizada es la ducha. Cuando alguien se va a duchar, tiene en mente una temperatura de agua deseada que, en la teoría de control, se denomina *punto fijo de referencia*. La persona, que actúa como *controlador*, mide continuamente la temperatura del flujo de agua (que se denomina *salida del sistema*) y modifica la velocidad a la que gira la manilla de la ducha en función de la *desviación* (o *error*) entre la temperatura deseada y la actual. La velocidad a la que se gira la manilla se denomina *entrada* del sistema. El objetivo es girar la manilla lo suficientemente rápido como para alcanzar el punto fijo de referencia rápidamente, pero no tan rápido como para que la temperatura se *dispare*. Si se producen shocks en el sistema donde la temperatura del flujo de agua cambia repentinamente, la persona debería ser capaz de mantener la temperatura actual sabiendo cómo de rápido debe girar la manilla en respuesta a la perturbación.

La disciplina científica encargada de mantener la estabilidad en sistemas dinámicos se denomina Teoría de Control y ha encontrado una amplia aplicación en el control de crucero para automóviles, navegación aérea, reactores químicos, brazos robóticos y procesos industriales de todo tipo. El algoritmo de ajuste de dificultad de Bitcoin que mantiene el tiempo promedio de bloque en diez minutos, a pesar de una tasa de hash variable, es un ejemplo de un sistema de control de misión crítica.

En la mayoría de los sistemas de control modernos, generalmente un *controlador algorítmico* está integrado en el proceso y tiene el control sobre una entrada del sistema (por ejemplo, el pedal del acelerador de un automóvil) para actualizarlo automáticamente en función de las desviaciones entre la salida del sistema (por ejemplo, la velocidad de un automóvil) y el punto de ajuste (por ejemplo, la velocidad del control de crucero).



El tipo más habitual de controlador algorítmico es el controlador PID. Más del 95% de

las aplicaciones industriales y una amplia gama de sistemas biológicos emplean elementos de control PID [4]. Un controlador PID usa una fórmula matemática con tres partes para determinar su salida:

Salida Controlador = Término Proporcional + Término Integral + Término Derivado

El Término Proporcional es la parte del controlador que es directamente proporcional a la desviación. Si la desviación es grande y positiva (por ejemplo, el punto de ajuste de la velocidad de control de crucero es mucho más alto que la velocidad actual del automóvil), la respuesta proporcional será grande y positiva (p.ej. pisar el pedal del acelerador).

El Término Integral es la parte del controlador que tiene en cuenta cuánto tiempo ha persistido una desviación. Se determina realizando la integral de la desviación a lo largo del tiempo y se usa principalmente para eliminar el *error de estado estable*. Se acumula para responder a desviaciones pequeñas, aunque persistentes, del punto de ajuste (por ejemplo, el punto de ajuste del control de crucero ha sido 1 mph más alto que la velocidad del automóvil durante unos minutos).

El Término Derivado es la parte del controlador que tiene en cuenta cuánto de rápido crece o se contrae la desviación. Se determina tomando la derivada de la desviación y sirve para acelerar la respuesta del controlador cuando la desviación está creciendo (p.ej. acelerar si el punto de ajuste del control de crucero es mayor que la velocidad del automóvil y el automóvil comienza a reducir la velocidad). También ayuda a reducir el sobreimpulso al desacelerar la respuesta del controlador cuando la desviación se está reduciendo (p.ej. desacelerando el acelerador cuando la velocidad del automóvil comience a acercarse al punto de ajuste del control de crucero).

La combinación de estas tres partes, cada una de las cuales se puede ajustar de forma independiente, brinda a los controladores PID una gran flexibilidad para administrar una amplia variedad de aplicaciones de sistemas de control.

Los controladores PID funcionan mejor en sistemas que permiten cierto grado de retraso en el tiempo de respuesta, así como la posibilidad de sobreimpulso y oscilación alrededor del punto de ajuste cuando el sistema intenta estabilizarse. Los sistemas de índices reflejos como RAI son adecuados para este tipo de escenario en el que los controladores PID pueden cambiar sus precios de canje.

De manera general, se ha descubierto recientemente que muchas de las reglas

actuales de la política monetaria del banco central (p.ej. la regla de Taylor) son en realidad aproximaciones de los controladores PID [5].

Mecanismo de retroinformación de la tasa de redención

El mecanismo de retroinformación de la tasa de redención es la parte del sistema a cargo del cambio del precio de redención del índice reflejo. Para entender cómo funciona, en primer lugar necesitamos describir por qué el sistema necesita un mecanismo de retroinformación en vez de utilizar un control manual y en segundo lugar cuál es la salida del sistema.

Componentes del mecanismo de retroinformación

En teoría, sería posible manipular directamente el precio de redención del índice reflejo (descrito en el capítulo 2) para influenciar a los usuarios del índice y en último lugar alterar el precio de mercado del índice. En la práctica, este método no tendría el efecto deseado sobre los participantes del sistema. Desde la perspectiva de un inversor en SAFE (Acuerdo Simplificado sobre Acciones Futuras), si el precio de redención se incremente sólo una vez, podrían aceptar un precio más alto por unidad de deuda, absorber la pérdida por una reducción del ratio de colateralización y mantener su posición. Si por el contrario, ellos esperan que el precio de redención continúe creciendo a lo largo del tiempo, probablemente estarán más inclinados a evitar esperables pérdidas futuras y por tanto elegir cancelar su deuda y cerrar sus posiciones.

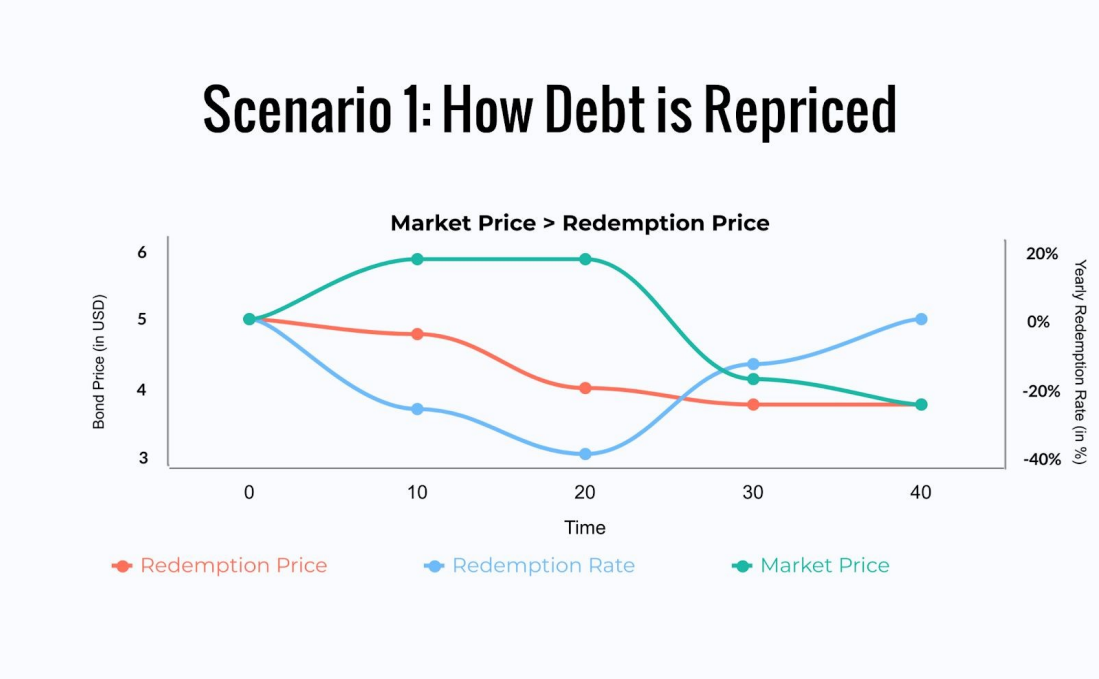
Esperamos que los participantes en el sistema de índice reflejo no respondan directamente a los cambios en el precio de redención, sino que en su lugar respondan la *tasa de cambio del precio de redención* que nosotros llamamos la *tasa de redención*. La tasa de redención se establece por medio de un *mecanismo de retroinformación* que la gobernanza puede ajustar o permitir que se completamente automatizada.

Escenarios de mecanismos de retroinformación

Recordar que el mecanismo de retroinformación tiene como objeto mantener el equilibrio entre el precio de redención y el precio de mercado utilizando la tasa de redención para contrarrestar los cambios en las fuerzas del mercado. Para lograr esto, la tasa de redención se calcula de manera que se oponga a la desviación entre los precios de mercado y de redención.

En el primer siguiente escenario, si el precio de mercado del índice es más alto que

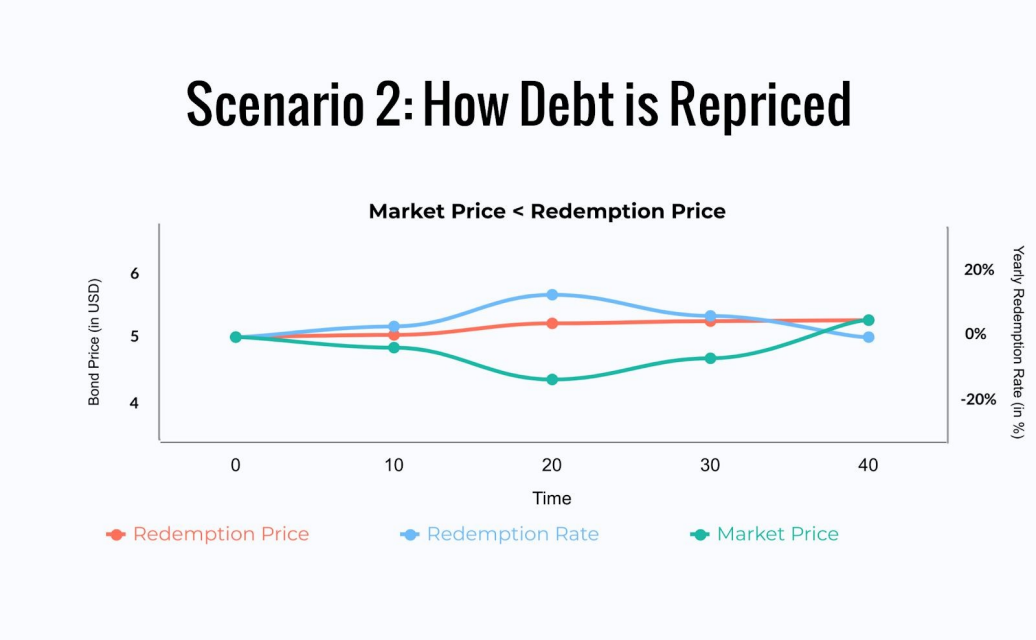
su precio de redención, el mecanismo calculará una tasa negativa que empezará a disminuir el precio de redención, abaratando de esta forma la deuda del sistema.



Probablemente la expectativa de un precio de redención decreciente disuadirá a las personas de mantener índices y alentará a los tenedores de SAFE a generar más deuda (incluso si el precio del colateral no cambia) que luego se vende en el mercado, equilibrando así la oferta y la demanda. Téngase en cuenta que éste es el escenario ideal donde los tenedores de índices reaccionan rápidamente en respuesta al mecanismo de retroinformación. En la práctica (y especialmente en los primeros días posteriores al lanzamiento), esperamos un desfase entre el inicio del mecanismo y los resultados reales observados en la cantidad de deuda emitida y posteriormente, en el precio de mercado.

Por otro lado, en el segundo escenario, si el precio de mercado del índice es más bajo que el precio de redención, la tasa se vuelve positiva y comienza a recalcularse el precio de toda la deuda de tal forma que se vuelva más cara.

A medida que la deuda se vuelve más cara, los ratios de colateralización de todos los SAFEs disminuyen (por tanto, los creadores de SAFE están incentivados a pagar su deuda) y los usuarios comienzan a acumular índices con la expectativa de que aumentarán su valor.



Algoritmo del mecanismo de retroinformación

En el siguiente escenario, asumimos que el protocolo utiliza un controlador proporcional-integral para calcular la tasa de redención:

- El índice reflejo es lanzado con precio de redención arbitrario y ‘aleatorio’

- En algún momento, el precio del mercado del índice se eleva de 'aleatorio' a 'aleatorio' + x. Después de que el mecanismo de retroinformación haya leído el nuevo precio de mercado, calcula un término proporcional *p*, que en este caso es -1 * (('aleatorio' + x) / 'aleatorio'). La parte proporcional es negativa para disminuir el precio de redención y a la vez recalcular los índices para que se vuelvan más baratos.

- Después de calcular el término proporcional, el mecanismo determinará el término integral sumando todas las desviaciones pasadas de los últimos *deviationInterval* segundos.

- El mecanismo suma las partes proporcional y la integral y calcula una tasa de redención por segundo *r* que lentamente empieza a disminuir el precio de redención. Al darse cuenta los creadores de SAFE de que pueden generar más deuda, inundarán el mercado con más índices.

- Después de n segundos, el mecanismo detecta que la desviación entre los precios del mercado y de redención es despreciable (bajo unos parámetro específico de ruido). Llegados a este punto, el algoritmo establece r a cero y mantiene el precio de redención donde está

En la práctica, el algoritmo será más robusto y o bien haremos que algunas variables sean inmutables (p.ej. el parámetro de *ruido*, *deviationInterval*) o bien habrá límites estrictos sobre lo que la gobernanza pueda cambiar.

Ajuste del mecanismo de retroinformación

De una importancia crucial para el correcto funcionamiento del sistema de índice reflejo es el ajuste de los parámetros del controlador algorítmico. La parametrización inadecuada podría resultar en que el sistema sea demasiado lento para lograr la estabilidad, masivamente sobreexcitado, o ser por regla general inestable frente a cambios bruscos externos.

El proceso de ajuste para un controlador PID generalmente implica ejecutar el sistema en vivo, retocando los parámetros de ajuste y observando la respuesta del sistema, a menudo introduciendo cambios bruscos a propósito durante el proceso. Dada la dificultad y el riesgo financiero que supone retocar los parámetros de un sistema de índice de reflejos en vivo, planeamos aprovechar el modelado de computadoras y la simulación tanto como sea posible para establecer los parámetros iniciales, pero también permitirá que la gobernabilidad actualice los parámetros de ajuste de la producción. Muestra que sean subóptimos.

Fijador del mercado monetario

En RAI, nuestro plan es mantener la tasa de interés (la tasa de interés aplicada al generar índices) fija o limitada y sólo modificar el precio de redención, minimizando de esta forma la complejidad involucrada en modelar el mecanismo de retroinformación. En nuestro caso la tasa de interés es igual al diferencial entre la tarifa de estabilidad y el DSR en el DAI Multi-Colateral.

Aunque nuestro plan es mantener fija la tasa de interés, es posible modificarla junto con el precio de redención utilizando un fijador del mercado monetario. El mercado monetario cambia la tasa de interés y el precio de redención de una manera que incentiva a los creadores de SAFE a generar más o menos deuda. Si el precio de mercado de un índice está por encima del de rendención, ambas tasas comenzarán a disminuir, mientras que si está por debajo de la redención, las tarifas aumentarán.

Liquidación Global

La liquidación global es un método de último recurso utilizado para garantizar un precio de redención para todos los tenedores de índices reflejos. Está destinado a permitir que tanto los titulares de índices reflejos como los creadores SAFE canjeen los colaterales del sistema a su valor neto (cantidad de índices por cada tipo de colateral, de acuerdo con el último precio de redención). Cualquiera puede activar la liquidación después de quemar una cierta cantidad de tokens de protocolo.

La liquidación tiene tres fases principales:

- **Disparador**: se activa la liquidación, los usuarios ya no pueden crear SAFE, todos los precios de los colarerales y el precio de redención se congelan y registran

- **Proceso**: realización de todas las subastas pendientes

- **Claim**: todos los titulares de índices reflejos y creadores de SAFE pueden reclamar una cantidad fija de cualquier colateral del sistema en función del último precio de redención registrado del índice.

Gobernanza

La gran mayoría de los parámetros serán inmutables y la mecánica interna del contrato inteligente no se podrá actualizar a menos que los titulares de tokens de gobernanza implementen un sistema completamente nuevo. Elegimos esta estrategia porque así podemos eliminar el metajuego en el que ciertas personas intentan influir en el proceso de gobernanza para su propio beneficio, dañando así la confianza en el sistema. Establecemos el correcto funcionamiento del protocolo sin poner demasiada fe en los humanos (el “efecto bitcoin”) para maximizar la escalabilidad social y minimizar los riesgos para otros desarrolladores que querrán utilizar RAI como infraestructura central en sus propios proyectos.

Para los pocos parámetros que se pueden cambiar, proponemos la adición de un módulo de gobernanza restringido destinado a retrasar o limitar todas las posibles modificaciones del sistema. Además, presentamos una Edad de Hielo de Gobernanza, un registro de permisos que puede bloquear del control externo algunas partes del sistema después de que hayan pasado ciertos plazos.

Gobernanza limitada en el tiempo

La gobernanza limitada en el tiempo es el primer componente del módulo de gobernanza restringida. Establece retrasos temporales entre los cambios aplicados a un mismo parámetro. Un ejemplo es la posibilidad de cambiar las direcciones de los oráculos utilizados en el Medianizador de Redes de Oráculos (Sección 6.2) después de que hayan pasado al menos T segundos desde la última modificación del oráculo.

Gobernanza limitada de acción

El segundo componente del Módulo de Gobernanza Restringida es la gobernanza limitada de acción. Cada parámetro gobernable tiene límites sobre los valores que pueden ser establecidos y cuánto pueden cambiar durante un cierto período de tiempo. Ejemplos destacables son las versiones iniciales del Mecanismo de Retroinformación de la Tasa de Redención (Sección 4.2) que los titulares de tokens de gobierno podrán ajustar

Edad de Hielo de Gobernanza

La Edad de Hielo es un contrato inteligente inmutable que impone plazos para cambiar parámetros específicos del sistema y actualizar el protocolo. Se puede usar en el caso de que el gobierno quiera asegurarse de que pueden corregir errores antes de que el protocolo se bloquee y bloquee la intervención externa. La Edad de Hielo verificará si se permite un cambio, verificando el nombre del parámetro y la dirección del contrato afectado con un registro de fechas límite. Si la fecha límite se ha sobrepasado, la petición se revertirá.

La gobernanza puede retrasar la Edad de Hielo un número fijo de veces si se encuentran errores cerca de la fecha en que el protocolo debería comenzar a bloquearse. Por ejemplo, la Edad de Hielo sólo se puede retrasar tres veces, cada vez durante un mes, para que las nuevas correcciones de errores implementadas puedan ser probadas correctamente.

Áreas Núcleo donde se necesita Gobernanza

Visualizamos cuatro áreas donde la gobernanza podría ser necesaria, especialmente en las primeras versiones de este marco de trabajo:

- **Añadir nuevos tipos de colateral**: RAI estará respaldado sólo por ETH, pero otros índices estarán respaldados por diferentes tipos de colateral y la gobernanza podrá diversificar el riesgo a lo largo del tiempo.

- **Cambiar dependencias externas**: los oráculos y DEX de los que depende el sistema pueden ser actualizados. La gobernanza puede enfocar el sistema a dependencias más nuevas para que continúe funcionando correctamente

- **Ajuste fino del configurador de tasas**: los primeros controladores de la política monetaria tendrán parámetros que se pueden cambiar dentro de unos límites razonables (como se describe en la Gobernanza limitada de Acción y Tiempo)

- **Migrar entre versiones del sistema**: en algunos casos, la gobernanza puede implementar un nuevo sistema, darle permiso para imprimir tokens de protocolo y retirar este permiso del sistema antiguo. Esta migración se realiza con la ayuda del módulo de Migración Restringida que se describe a continuación

Modulo de Migración Restringida

Lo siguiente es un mecanismo simple para migrar entre versiones del sistema:

- Existe un registro de migración que realiza un seguimiento de cuántos sistemas diferentes cubre el mismo token de protocolo y a qué sistemas se le puede negar el permiso para imprimir tokens de protocolo en una subasta de deuda.

- Cada vez que la gobernanza implementa una nueva versión del sistema, envía la dirección del contrato de subasta de deuda del sistema al registro de migración. La gobernanza también debe especificar si alguna vez podrá evitar que el sistema imprima tokens de protocolo. Además, la gobernanza puede, en cualquier momento, decir que un sistema siempre podrá imprimir tokens y, por lo tanto, nunca se migrará desde ahí

- Hay un período transitorio entre la propuesta de un nuevo sistema y la retirada de los permisos de uno anterior.

- Se puede configurar un contrato opcional para que apague automáticamente

un sistema antiguo después de que se le nieguen los permisos de impresión.

El módulo de migración se puede combinar con una Edad de Hielo que automáticamente otorga a sistemas específicos el permiso para poder imprimir tokens en todo momento.

Apagado Automático del Sistema

Hay casos en los que el sistema automáticamente puede detectar y, como resultado, desencadenar la liquidación por sí mismo, sin la necesidad de quemar tokens de protocolo.:

- **Graves retrasos en el feed de precios**: el sistema detecta que uno o más de los feeds de precios de colaterales o índices no se han actualizado en mucho tiempo

- **Migración del sistema**: este es un contrato opcional que puede cerrar el protocolo después de que pase un período transitorio desde el momento en que la gobernanza retire la capacidad del mecanismo de subasta de deuda, para imprimir tokens de protocolo (Módulo de Migración Restringida, Sección 5.4.1)

- **Desviación constante del precio de mercado**: el sistema detecta que el precio de mercado del índice se ha desviado un x% durante mucho tiempo comparado con el precio de redención

La Gobernanza podrá actualizar estos módulos de apagado autónomo mientras aún estén limitados o hasta que la Edad de Hielo comience a bloquear algunas partes del sistema.

Oráculos

Hay tres tipos principales de activos para los que el sistema necesita leer los feeds de precios: el índice, el token de protocolo y todos los tipos de colaterales incluidos en la lista blanca. Las fuentes de precios pueden ser proporcionadas por Oráculos dirigidos por la Gobernanza o por redes de oráculos ya establecidas.

Oráculos dirigidos por Gobernanza

Los titulares de tokens de Gobernanza o el equipo central que lanzó el protocolo pueden asociarse con otras entidades que recopilan múltiples fuentes de precios off-chain y luego envían una sola transacción a un contrato inteligente que calcula la mediana de todos los puntos de datos.

Este enfoque permite una mayor flexibilidad para actualizar y cambiar la

infraestructura de Oráculos, aunque se produzca a expensas de la falta de confianza.

Medianizador de Redes de Oráculos

Un Medianizador de Red de Oráculo es un contrato inteligente que lee precios de múltiples fuentes que no están controladas directamente por la gobernanza (p.ej. un pool de Uniswap V2 entre un tipo de colateral de índice y otras monedas estables) y luego hacen la media de todos los resultados. MRO funciona de la siguiente manera:

- Nuestro contrato realiza un seguimiento de las redes de Oráculos incluidas en la lista blanca a las que puede llamar para solicitar precios de colaterales. El contrato se financia con parte del superávit que acumula el sistema (utilizando la Tesorería Excedente, Sección 11). Cada red de un Oráculo acepta tokens específicos como pago, por lo que nuestro contrato también realiza un seguimiento de la cantidad mínima y el tipo de tokens necesarios para cada solicitud.

- Para introducir un nuevo feed de precios en el sistema, es necesario solicitarlo a todos los oráculos de antemano. Al llamar a un oráculo, el contrato primeramente intercambia algunas tarifas de estabilidad con alguno de los tokens aceptados por el oráculo. Después de llamar al oráculo, el contrato etiqueta la petición como "válida" o "inválida". Si una petición no es válida, no se puede volver a solicitar al oráculo defectuoso específico hasta que se soliciten a todos los demás y el contrato verifique si hay una mayoría válida. Una petición de oráculo válida no debe revertirse y debe recuperar un precio que se haya publicado en la cadena en algún momento de los últimos *m* segundos. "Recuperar" significa cosas diferentes según cada tipo de oráculo:

    - Para los oráculos basados en *pull*, de los cuales podemos obtener un resultado de inmediato, nuestro contrato debe pagar una tarifa y obtener el precio directamente.

    - Para los oráculos basados en *push*, nuestro contrato paga la tarifa, llama al oráculo y necesita esperar un período de tiempo específico *n* antes de volver a llamar al oráculo para obtener el precio solicitado

- Cada resultado de un Oráculo se guarda en una matriz. Después de llamar a cada oráculo de la lista blanca y si la matriz tiene suficientes puntos de datos válidos para formar una mayoría (p.ej. el contrato recibió datos válidos de 3/5 oráculos), los resultados se ordenan y el contrato selecciona el valor medio.

- Tanto si el contrato encuentra una mayoría como si no, la matriz con los

resultados del Oráculo se borra y el contrato deberá esperar *p* segundos antes de comenzar todo el proceso de nuevo.

Backup de la Red de Oráculos

La Gobernanza puede agregar una opción backup de Oráculos que comienza a impulsar los precios en el sistema si el medianizador no puede encontrar la mayoría de las redes de Oráculos válidas varias veces seguidas.

La opción de backup debe configurarse cuando se implementa el medianizador, ya que posteriormente no se puede cambiar. Además, un contrato separado puede monitorizar si el backup ha estado reemplazando el mecanismo de medianización durante demasiado tiempo y apagar automáticamente el protocolo.

Safes

Para generar índices, cualquier persona puede depositar y aprovechar su cripto colateral dentro de Safes. Mientras se abre un SAFE, se seguirá acumulando deuda de acuerdo con la tasa de interés del colateral depositado. A medida que el creador del SAFE pague su deuda, podrá retirar más y más de su colateral bloqueado.

Ciclo de vida del SAFE

Son necesarios cuatro pasos principales para crear índices reflejos y, posteriormente, pagar la deuda del SAFE.:

- Depositar colateral en el SAFE

  El usuario primero tiene que crear un nuevo SAFE y depositar colateral en él.

- Generar índices respaldados por el colateral del SAFE

  El usuario especifica cuántos índices quiere generar. El sistema crea una cantidad igual de deuda que comienza a acumularse de acuerdo con la tasa de endeudamiento del colateral.

- Pagar de vuelta la deuda del SAFE

  Cuando los creadores del SAFE quieran retirar el colateral, tienen que pagar el interés inicial más los intereses devengados,

- Retirar el colateral

Después de que el usuario pague una parte o toda su deuda, entonces puede retirar su colateral.

Liquidación del SAFE

Para mantener la solvencia del sistema y cubrir el valor de la totalidad de la deuda pendiente, cada SAFE puede liquidarse en caso de el ratio de colateralización caiga por debajo de cierto umbral. Cualquier persona puede desencadenar una liquidación, en cuyo caso el sistema confiscará el colateral del SAFE y lo venderá en una *subasta de colateral*.

Seguro de Liquidación

En una de las versiones del sistema, los creadores de SAFE tienen la opción de elegir un disparador para cuándo sus SAFE son liquidados. Los desencadenantes son contratos inteligentes que agregan automáticamente más garantías en un SAFE y potencialmente lo salvan de la liquidación. Ejemplos de desencadenantes son contratos que venden posiciones cortas o contratos que se comunican con protocolos de seguros como Nexus Mutual [6].

Otro método para proteger los SAFE es la adición de dos umbrales de colateral diferentes: *seguro* y *riesgo*. Los usuarios de SAFE pueden generar deuda hasta que alcanzan el umbral seguro (que es mayor que el riesgo) y sólo se liquidan cuando la colateralización del SAFE desciende por debajo del umbral de riesgo.

Subastas de Colateral

Para iniciar una subasta de colateral, el sistema necesita usar una variable llamada *liquidationQuantity* para determinar la cantidad de deuda que se cubrirá en cada subasta y la cantidad correspondiente de colateral que será vendida. Se aplicará una *multa de liquidación* a cada SAFE subastado.

Parámetros de la Subasta de Colateral

Nombre del parámetro	Descripción
minimumBid	Cantidad mínima de monedas que deben ofrecerse en una oferta
discount	Descuento al que el colateral es vendido

lowerCollateralMedianDeviation	Desviación máxima del límite inferior que puede tener la mediana del colateral en comparación con el precio del oráculo
upperCollateralMedianDeviation	Desviación máxima del límite inferior que puede tener la mediana del colateral en comparación con el precio de oráculo
lowerSystemCoinMedianDeviation	Desviación máxima del límite inferior que puede el feed de precio del oráculo de la moneda del sistema en comparación con el precio del oráculo de la moneda del sistema
upperSystemCoinMedianDeviation	Desviación máxima del límite superior que puede tener la mediana del colateral en comparación con el precio del oráculo de la moneda del sistema
minSystemCoinMedianDeviation	Desviación mínima para el resultado de la mediana de la moneda del sistema en comparación con el precio de redención para tener en cuenta la mediana

Mecanismo de la Subasta de Colateral

La subasta de descuento fijo es una forma sencilla (en comparación con las subastas en inglesas) de poner un colateral a la venta a cambio de las monedas del sistema que se utilizan para liquidar deudas malas. Los postores sólo deben permitir que la casa de subastas transfiera su *safeEngine.coinBalance* y luego pueden llamar a *buyCollateral* para intercambiar las monedas de su sistema por un colateral que se vende con un descuento en comparación con su último precio de mercado registrado.

Los postores también pueden revisar la cantidad de colateral que pueden obtener de una subasta específica llamando a *getCollateralBought* o *getApproximateCollateralBought*. Téngase en cuenta que *getCollateralBought* no está marcado como visible porque lee (y también actualiza) el *redemptionPrice* del remitente del oráculo, mientras que *getApproximateCollateralBought* usa *lastReadRedemptionPrice*.

Subastas de deuda

En el escenario en el que una subasta de colateral no puede cubrir todas las deudas malas en un SAFE y si el sistema no tiene reservas excedentes, cualquiera puede desencadenar una subasta de deuda.
Las subastas de deuda están destinadas a acuñar más tokens de protocolo (Sección 10) y venderlos por índices que pueden anular la deuda incobrable restante del sistema.

Para iniciar una subasta de deuda, el sistema tiene que utilizar dos parámetros:

- initialDebtAuctionAmount: la cantidad inicial de tokens de protocolo para acuñar después de la subasta

- debtAuctionBidSize: el tamaño de la oferta inicial (cuántos índices deben ofrecerse a cambio de tokens de protocolo *initialDebtAuctionAmount*)

Configuración autónoma de los parámetros de la subasta de deuda

La cantidad inicial de tokens de protocolo acuñados en una subasta de deuda puede establecerse mediante una votación de la gobernanza o puede ser ajustada automáticamente por el sistema. Se necesitaría integrar una versión automatizada con oráculos (Sección 6) desde los cuales el sistema leería el token de protocolo y los precios del mercado de índices reflejos. Luego, el sistema establecería la cantidad inicial de tokens de protocolo (*initialDebtAuctionAmount*) que se acuñarían para los índices de *deudaAuctionBidSize*. *initialDebtAuctionAmount* se puede establecer con un descuento en comparación con el precio de mercado real de PROTOCOLO / ÍNDICE para incentivar la puja.

Parámetros de la Subasta de Deuda

Nombre de Parámetro	Descripción
amountSoldIncrease	Aumento de la cantidad de tokens de protocolo que se acuñarán para la misma cantidad de índices.
bidDecrease	Disminución mínima para la próxima oferta en la cantidad aceptada de tokens de protocolo para la misma cantidad de índices

bidDuration	Cuánto tiempo dura la puja después de que se envía una nueva puja (en segundos)
totalAuctionLength	Duración total de la subasta (en segundos)
auctionsStarted	Cuántas subastas han comenzado hasta ahora

Mecanismo de la Subasta de Deuda

A diferencia de las subastas de colateral, las subastas de deuda solo tienen una etapa:

`decreaseSoldAmount(uint id, uint amountToBuy, uint bid)`: disminuir la cantidad de tokens de protocolo aceptados a cambio de una cantidad fija de índices.

La subasta se reiniciará si no se han realizado ofertas. Cada vez que se reinicia, el sistema ofrecerá más tokens de protocolo para la misma cantidad de índices. La cantidad del token del nuevo protocolo se calcula como *lastTokenAmount * amountSoldIncrease* /
100. Después de que se liquide la subasta, el sistema emitirá tokens para el mejor postor.

Tokens del Protocolo

Como se describió en secciones anteriores, cada protocolo deberá estar protegido por un token que se acuña a través de subastas de deuda. Además de protección, el token se utilizará para controlar algunos componentes del sistema. También, el suministro de tokens de protocolo se reducirá gradualmente con el uso de subastas de excedentes. La cantidad de excedentes que deben acumularse en el sistema antes de que se subasten los fondos adicionales se denomina *surplusBuffer* y se ajusta automáticamente como un porcentaje de la deuda total emitida.

Fondo de seguro

Además del token de protocolo, la gobernanza puede crear un fondo de seguros que contenga una amplia gama de activos no correlacionados y que se puedan utilizar como respaldo para las subastas de deuda.

Subastas de Excedentes

Las subastas de excedentes venden tarifas de estabilidad acumuladas en el sistema por tokens de protocolo que luego se queman.

Parámetros de Subata de Excedentes

Parameter Name	Description
bidIncrease	Incremento mínimo en la próxima puja
bidDuration	Cuánto tiempo dura la subasta después de que se envía una nueva oferta (en segundos)
totalAuctionLength	Duración total de la subasta (en segundos)
auctionsStarted	Cuántas subastas han comenzado hasta ahora

Mecanismo de las Subastas de Excedentes

Las subastas de excedentes tienen una sola etapa:

`increaseBidSize(uint id, uint amountToBuy, uint bid)`: cualquiera puede ofertar una mayor cantidad de tokens de protocolo por la misma cantidad de índices (excedente). Cada nueva oferta debe ser mayor o igual a *lastBid * bidIncrease /* 100. La subasta finalizará después de que hayan transcurrido los segundos máximos de *totalAuctionLength* o después de que hayan pasado los segundos de *bidDuration* desde la última oferta y no se hayan presentado nuevas ofertas durante este tiempo.

Una subasta se reiniciará si no tiene ofertas. Por otro lado, si la subasta tiene al menos una oferta, el sistema ofrecerá el excedente al mejor postor y luego quemará todos los tokens de protocolo reunidos.

Gestión de Índices de Excedentes

Cada vez que un usuario genera índices y a la vez implícitamente crea deuda, el sistema comienza a aplicar una tasa de endeudamiento al SAFE del usuario. El interés acumulado se agrupa en dos contratos inteligentes diferentes:

- El *accounting engine* utilizado para activar las subastas de deuda (Sección 9.2) y excedentes (Sección 10.1).
- El *surplus treasury* utilizado para financiar los componentes básicos de la

infraestructura e incentivar a los actores externos a mantener el sistema

El excedente de tesorería se encarga de financiar tres componentes básicos del sistema:

- Módulo de oráculos (Sección 6). Dependiendo de cómo esté estructurado un oráculo, la tesorería paga los oráculos off-chain de la lista blanca de gobernanza o paga las peticiones a las redes de oráculos. La tesorería también se puede configurar para pagar a las direcciones que gastaron gas para llamar a un oráculo y actualizarlo.

- En algunos casos, equipos independientes que mantienen el sistema. Algunos ejemplos son los equipos que incluyen en la lista blanca nuevos tipos de colateral o ajustan el fijador de tarifas del sistema (Sección 4.2).

La tesorería puede configurarse para que automáticamente a algunos beneficiarios de excedentes se les niegue la financiación en el futuro y otros puedan ocupar su lugar.

Actores Externos

El sistema depende de actores externos para funcionar correctamente. Estos actores están económicamente incentivados para participar en áreas como subastas, proceso de liquidación global, creación de mercado y actualización de precios para mantener la salud del sistema.

Proporcionaremos interfaces de usuario iniciales y scripts automatizados para permitir que tantas personas como sea posible mantengan el protocolo seguro.

Mercado objetivo

Vemos que RAI es útil en dos áreas principales:

- **Diversificación de portfolio**: los inversores usan RAI para amortiguar la exposición a un activo como ETH sin todo el riesgo de tener realmente ether

- **Colateral para activos sintéticos**: RAI puede ofrecer a protocolos como UMA, MakerDAO y Synthetix una menor exposición al mercado cripto y dar a los usuarios más tiempo para salir de sus posiciones en el caso de escenarios como el Jueves Negro de marzo de 2020 cuando se liquidaron millones de dólares en criptoactivos.

Investigación Futura

Para expander los límites del dinero descentralizado y traer más innovación a las finanzas descentralizadas, continuaremos buscando alternativas en áreas núcleo como la minimización de la gobernanza y los mecanismos de liquidación.

En primer lugar, queremos sentar las bases para estándares futuros en torno a protocolos que se bloquean a sí mismos del control externo y para verdaderos "robots de dinero" que se adaptan en respuesta a las fuerzas del mercado. Posteriormente, invitamos a la comunidad de Ethereum a debatir y diseñar mejoras en torno a nuestras propuestas con un enfoque específico en las subastas de colateral y deudas.

Riesgos y Mitigación

Existen varios riesgos involucrados en el desarrollo y lanzamiento de un índice reflejo, así como en los sistemas posteriores que se construyen sobre una capa superior:

- **Errores en el contrato inteligente**: el mayor riesgo que presenta el sistema es la posibilidad de un error que permita a cualquiera extraer todo el colateral o bloquee el protocolo en un estado del que no se puede recuperar. Planeamos que varios investigadores de seguridad revisen nuestro código y lanzar el sistema en una testnet antes de comprometernos a implementarlo en producción.

- **Fallo de oráculo**: agregaremos feeds de múltiples redes de oráculos y habrá reglas estrictas para actualizar solo un oráculo a la vez, de modo que una gobernanza maliciosa no pueda introducir fácilmente precios falsos.

- **Eventos de Cisne Negro del colateral**: existe el riesgo de un evento de cisne negro en el colateral que puede resultar en una gran cantidad de SAFE liquidadas. Es posible que las liquidaciones no puedan cubrir la totalidad de la deuda mala pendiente y, por lo tanto, el sistema cambiará continuamente su colchón de superávit para cubrir una cantidad decente de deuda emitida y resistir los shocks del mercado.

- **Parámetros de establecimiento de tasa inadecuados**: los mecanismos de retroinformación autónomos son muy experimentales y pueden no comportarse exactamente como predecimos durante las simulaciones. Planeamos permitir que la gobernanza ajuste este componente (sin dejar de

estar limitado) para evitar escenarios inesperados

- **No se pudo iniciar un mercado saludable de liquidadores**: los liquidadores son actores vitales que se aseguran de que toda la deuda emitida esté cubierta por colateral. Planeamos crear interfaces y scripts automatizados para que tantas personas como sea posible puedan participar en mantener el sistema seguro.

Resumen

Hemos propuesto un protocolo que se aísla progresivamente del control humano y emite un activo garantizado de baja volatilidad llamado índice reflejo. Primero presentamos el mecanismo autónomo destinado a influir en el precio de mercado del índice y luego describimos cómo varios contratos inteligentes pueden limitar el poder que los poseedores de tokens tienen sobre el sistema. Describimos un esquema autosostenible para medianizar de los feeds de precios de múltiples redes de oráculos independientes y finalmente terminamos presentando el procedimiento general para acuñar índices y liquidar SAFE.

Referencias

[1] "The Maker Protocol: MakerDAO's Multi Collateral Dai (MCD) System", https://bit.ly/2YL5S6j

[2] "UMA: A Decentralized Financial Contract Platform", https://bit.ly/2Wgx7E1

[3] Synthetix Litepaper, https://bit.ly/2SNHxZO

[4] K.J. Åström, R.M. Murray, "Feedback Systems: An Introduction for Scientists and Engineers", https://bit.ly/3bHwnMC

[5] R.J. Hawkins, J.K. Speakes, D.E. Hamilton, "Monetary Policy and PID Control", https://bit.ly/2TeQZFO

[6] H. Karp, R. Melbardis, "A peer-to-peer discretionary mutual on the Ethereum blockchain", https://bit.ly/3du8TMy

[7] H. Adams, N. Zinsmeister, D. Robinson, "Uniswap V2 Core", https://bit.ly/3dqzNEU

Glosario

Índice Reflejo: un activo colateralizado que amortigua la volatilidad de su subyacente

RAI: nuestro primer índice reflejo

Precio de Redención: el precio que el sistema quiere que tenga el índice. Cambia, influenciado por la tasa de redención (calculada por RRFM), en caso de que el precio de mercado no se acerque a ella. Tiene la intención de influir en los creadores de SAFE para que generen más o paguen parte de su deuda.

Tasa de endeudamiento tasa de interés anual aplicada a todas las SAFE que tienen deuda pendiente

Mecanismo de Retroinformación de la Tasa de Redención (RRFM): un mecanismo autónomo que compara los precios de mercado y de redención de un índice reflejo y luego calcula una tasa de redención que influye lentamente en los creadores de SAFE para generar más o menos deuda (e implícitamente trata de minimizar la desviación del precio de mercado / redención)

Fijador Monetario de Mercado (MMS): un mecanismo similar al RRFM que acciona múltiples palancas monetarias a la vez. En el caso de los índices reflejos, modifica tanto el tipo de interés pasivo como el precio de redención.

Medianizador de la Red de Oráculos (ONM): un contrato inteligente que extrae precios de múltiples redes de oráculos(que no están controladas por la gobernanza) y los medianiza si una mayoría (por ejemplo, 3 de 5) devolvió un resultado sin lanzar

Módulo de Gobernanza Restringida (RGM): un conjunto de contratos inteligentes que vinculan el poder que tienen los titulares de tokens de gobernanza sobre el sistema. Implica retrasos en el tiempo o limita las posibilidades que tiene la gobernanza para establecer ciertos parámetros.

Edad de Hielo de la Gobernanza: contrato inmutable que bloquea la mayoría de los componentes de un protocolo de la intervención externa después de que haya pasado un plazo determinado.

Motor de Contabilidad: componente del sistema que desencadena las subastas de deuda y excedentes. También realiza un seguimiento del monto de la deuda actualmente subastada, la deuda mala no procesada y el colchón de excedentes

Amortiguador de excedentes: cantidad de interés a devengar y mantener en el sistema. Cualquier interés acumulado por encima de este umbral se vende en subastas excedentes que queman tokens de protocolo

Excedentes de Tesorería: contrato que da permiso a diferentes módulos del sistema para retirar el interés acumulado (p.ej. ONM para peticiones de oráculo)