Rai: baja volatilidad, garantía de confianza minimizada para el ecosistema DeFi

Stefan C. Ionescu, Ameen Soleimani

mayo de 2020

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

Contenido

Introducción El

dinero es uno de los mecanismos de coordinación más poderosos que la humanidad aprovecha para prosperar. Históricamente, el privilegio de administrar la oferta monetaria se ha mantenido en manos del liderazgo soberano y la élite financiera, mientras se impone a un público en general inconsciente. Donde Bitcoin demostró el potencial de una protesta popular para manifestar un valioso activo de materias primas de reserva, Ethereum nos ofrece una plataforma para construir instrumentos sintéticos respaldados por activos que pueden protegerse de la volatilidad y usarse como garantía, o vincularse a un precio de referencia y usarse como medio de intercambio para las transacciones diarias, todo ello reforzado por los mismos principios de consenso descentralizado.

El acceso no autorizado a Bitcoin para almacenar riqueza e instrumentos sintéticos correctamente descentralizados en Ethereum sentará las bases para la revolución financiera que se avecina, proporcionando a los que están al margen del sistema financiero moderno los medios para coordinar la construcción del nuevo.

En este artículo, presentamos una estructura para la construcción de índices reflejos, un nuevo tipo de activo que ayudará a que otros sintéticos florezcan y establezcan una base fundamental para todo el sector financiero descentralizado.

Descripción general deíndices de

losreflejos El propósito de un índice de reflejos no es mantener una fijación específica, sino amortiguar la volatilidad de su garantía. Los índices permiten que cualquier persona se exponga al mercado de las criptomonedas sin la misma escala de riesgo que los activos criptográficos reales. Creemos que RAI, nuestro primer índice reflejo, será de uso inmediato para otros equipos que emiten sintéticos en Ethereum (por ejemplo, MakerDAO Multi-Collateral DAI [1], UMA [2], Synthetix [3]) porque da su sistemas menos exposición a activos volátiles, como ETH, y les da 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 rescate con el de una moneda estable.

El precio de rescate es el valor de una unidad de deuda (o moneda) en el sistema. Está destinado a ser utilizado solo como una herramienta de contabilidad interna y es diferente del precio de mercado (la cantidad por la cual el mercado está negociando la moneda). En el caso de las
monedas estables fiduciarias, 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 basadas en criptomonedas, como el DAI Multi Colateral (MCD) de MakerDAO, en el que el sistema apunta a 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, habrá una diferencia entre el precio de mercado de una moneda estable y su precio de reembolso. Estos escenarios crean oportunidades de arbitraje en las que los operadores crearán más divisas si el precio de mercado es más alto que el precio de rescate y redimirán sus divisas estables como garantía (por ejemplo, dólares estadounidenses en el caso del USDC) si el precio de mercado es inferior a el precio de redención.

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

Filosofía de diseño y estrategia de entrada al mercado

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

El DAI de múltiples garantías fue el lugar natural para comenzar a iterar a través del diseño de RAI. El sistema ha sido auditado y verificado formalmente, tiene dependencias externas mínimas y ha reunido a una comunidad activa de expertos. Para minimizar el esfuerzo de desarrollo y comunicación, queremos hacer solo los cambios más simples en la base del código MCD original para lograr nuestra

implementación.

Nuestras modificaciones más importantes incluyen la adición de un definidor de tarifas independiente, un Oracle Network Medianizer que está integrado con muchas fuentes de precios independientes y una capa de minimización de gobierno diseñada para aislar el sistema tanto como sea posible de la intervención humana.

La primera versión del protocolo (Etapa 1) incluirá solo el definidor de velocidad y otras mejoras menores a la arquitectura central. Una vez que demostremos que el establecedor funciona como se esperaba, podemos agregar con seguridad el mediador de Oracle (Etapa 2) y la capa de minimización de gobierno (Etapa 3).

Mecanismos de política monetaria

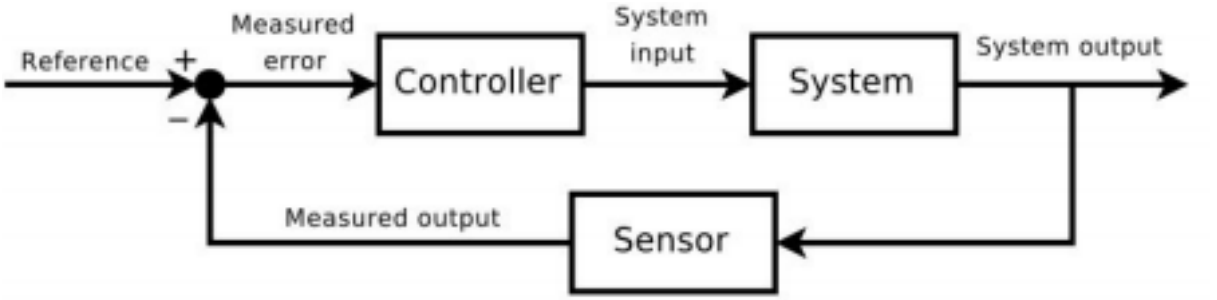
Introducción a la teoría del control

Un sistema de control común con el que la mayoría de la gente está familiarizada es la ducha. Cuándo alguien comienza a bañarse, tiene una temperatura de agua deseada en mente que en teoría de control, se denomina *punto de referencia de referencia*. La persona, que actúa comodel *responsabletratamiento*, mide continuamente la temperatura del flujo de agua (que se llama *salida*) y modifica la velocidad a la que giran el pomo de la ducha en función de la *desviación* (o *error*) entre la temperatura deseada y la actual. La velocidad a que se gira la perilla se llama el sistema dededo *entrada de.* El objetivo es girar la perilla lo suficientemente rápido para alcanzar el punto de ajuste rápidamente, pero no tan rápido como para temperatura *excesiva*. Si hubiera *choques en* el flujo de agua la temperatura cambia repentinamente, la persona debe poder mantener la corriente temperatura sabiendo qué tan rápido girar la perilla en respuesta a la perturbación.

La disciplina científica de mantener la estabilidad en sistemas dinámicos se llama control teoría y encontró una amplia aplicación en el control de crucero para automóviles, navegación aérea, reactores químicos, brazos robóticos y procesos industriales de todo tipo. Bitcoin algoritmo de ajuste de dificultad que mantiene el tiempo medio de bloqueo de diez minutos, a pesar de un hashrate variable, es un ejemplo de un sistema de control de misión crítica.

En la mayoría de los sistemas de control modernos, un *controlador algorítmico* suele estar integrado en el proceso y recibe control sobre una entrada del sistema (por ejemplo, el pedal del acelerador de un automóvil) para para actualizarlo automáticamente en función de las desviaciones entre la salida del sistema (por

ejemplo, un velocidad del automóvil) y punto de ajuste (por ejemplo, velocidad de control de crucero).



El tipo más común de controlador algorítmico es el *controlador PID*. Más del 95% de Las aplicaciones industriales y una amplia gama de sistemas biológicos emplean elementos dePID
control[4]. Un controlador PID utiliza una fórmula matemática de tres partes para determina tu salida:

C= salida proporcional en el término del controlador + término integral + término derivado

El Término Proporcional es la parte del controlador que es directamente *proporcional* al la desviación. Si la desviación es grande y positiva (por ejemplo, la velocidad del control de crucero punto de ajuste es mucho más alto que la velocidad actual del automóvil), la respuesta proporcional será grande y positivo (por ejemplo, acelerar).

El Término Integral es la parte del controlador que toma en cuenta cuánto tiempo la desviación persistió. Se determina tomando la *integral* de la desviación a lo largo de tiempo y se utiliza principalmente para eliminar el *error de estado estable*. Se acumula en orden para responder a desviaciones pequeñas pero persistentes del punto de ajuste (por ejemplo, el crucero el punto de ajuste de control fue 1 mph más alto que la velocidad del automóvil durante unos minutos).

El término derivado es la parte del controlador que tiene en cuenta la velocidad la desviación aumenta o disminuye. Se determina tomando la *derivada* de desviación y sirve para acelerar la respuesta del controlador cuando la desviación es creciendo (por ejemplo, acelerando si el punto de ajuste del control de crucero es mayor que la velocidad del automóvil y el coche empieza a reducir la velocidad). También ayuda a reducir el sobreimpulso al ralentizar el respuesta del controlador cuando la desviación

está disminuyendo (por ejemplo, aliviando el gas la velocidad del automóvil comienza 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 sistemas de control formas.

Los controladores PID funcionan mejor en sistemas que permiten cierto grado de retraso en la respuesta tiempo, así como la posibilidad de adelantar y oscilar alrededor del set point El sistema intenta estabilizarse. Los sistemas de índice de reflejo como RAI son adecuados para este tipo de escenario en el que el PID puede modificar los precios de reembolso controladores.

De manera más general, se ha descubierto recientemente que muchos de los Las reglas de política monetaria de los bancos (por ejemplo, la regla de Taylor) son en realidad aproximaciones de los PID de
control [5].

Mecanismo de retroalimentación de la tasa de canje

El mecanismo de retroalimentación de la tasa de reembolso es el componente del sistema responsable de cambiar el precio de rescate de un índice reflejo. Para entender cómo funciona, Primero necesita describir por qué el sistema necesita un mecanismo de retroalimentación en lugar de utilizando el control manual y cuál es la salida del mecanismo.

Componentes del mecanismo de retroalimentación

En teoría, sería posible manipular directamente el índice de amortización de la reflexión. precio (descrito en la Sección 2) para influir en los usuarios del índice y, en última instancia, cambiar el precio de mercado del índice. En la práctica, este método no tendría el efecto deseado. en los participantes del sistema. Desde la perspectiva de un tenedor ASEGURADO, si la redención el precio se eleva solo una vez, pueden aceptar un precio más alto por unidad de deuda, absorber la pérdida por un índice de garantía reducido y mantener su posición. Si, sin embargo, esperan que el precio de reembolso continúe aumentando con el tiempo, probablemente estaría más inclinado a evitar pérdidas futuras esperadas y, por lo tanto, optaría por pagar paga

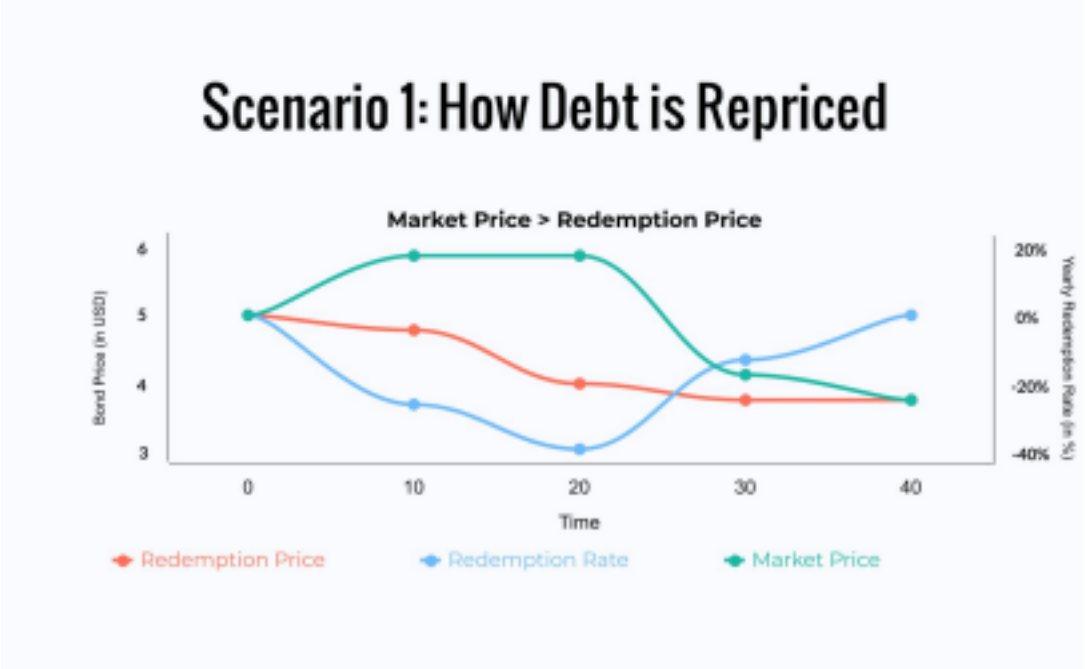
tus deudas y cierra tus posiciones.

Esperamos que los participantes en el sistema de índice de reflejos no respondan directamente a los cambios en el precio de redención, sino que responden a la *tasa de cambio del precio de redención* lo que llamamos *tarifa de redención*. La tasa de reembolso se define por *retroalimentación mecanismo* que la gobernanza puede ajustar o permitir que sea completamente automatizado.

Escenarios del motor de retroalimentación

Recuerde que el mecanismo de retroalimentación tiene como objetivo mantener un equilibrio entre precio de rescate y precio de mercado utilizando la tasa de rescate para compensar cambios en las fuerzas del mercado. Para lograr esto, la tarifa de reembolso se calcula de manera que se opone a la desviación entre los precios de mercado y de reembolso.

En el primer escenario a continuación, si el precio de mercado del índice es más alto que su redención precio, el motor calculará una tasa negativa que comenzará a disminuir el precio de rescate, abaratando la deuda del sistema.

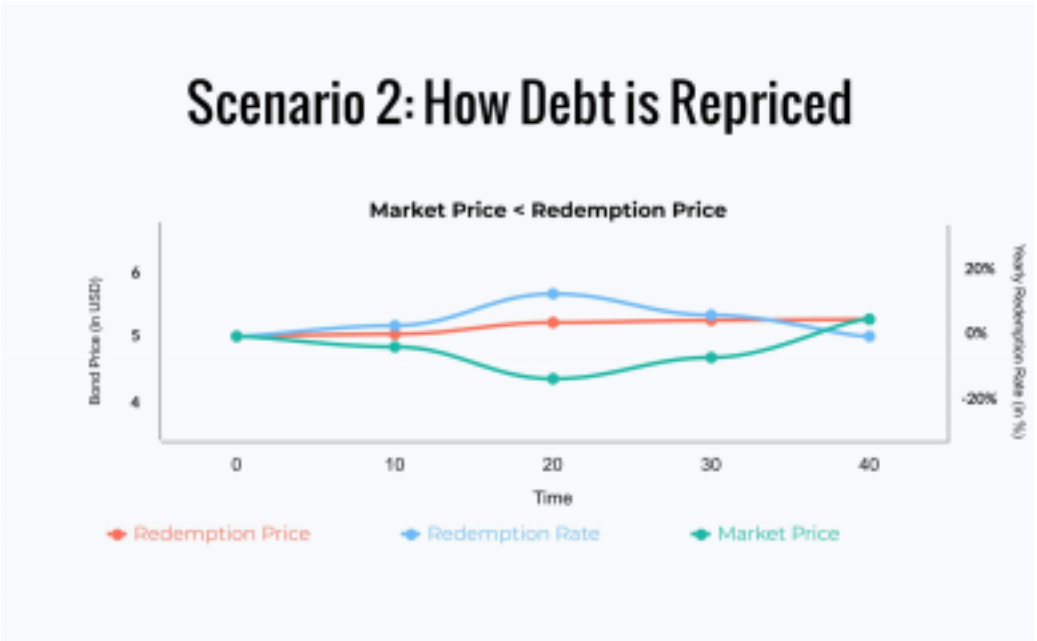


Es probable que la expectativa de una reducción en el precio del rescate desaliente a las personas de mantener índices y alentar a los tenedores de SAFE a generar más deuda (incluso si el el precio de garantía no cambia) que luego se vende en el mercado, equilibrando así oferta y demanda. Tenga en cuenta que este es el escenario ideal donde los titulares de índices reaccionar rápidamente en respuesta al mecanismo de retroalimentación. En la práctica (y especialmente en en los primeros

días después del lanzamiento), esperamos un retraso entre el arranque del motor y resultados reales observados en el monto de la deuda emitida y posteriormente en el mercado precio.

Por otro lado, en el escenario dos, si el precio de mercado del índice es menor que el precio de rescate, la tasa se vuelve positiva y renegocia la totalidad de la deuda para que se vuelve más caro.

A medida que la deuda se encarece, los coeficientes de garantía de todos los SAFE disminuyen (por lo que se anima a los creadores SAFE a pagar sus deudas) y los usuarios comienzan a acumular índices con la expectativa de que aumenten de valor.



Algoritmo del mecanismo de retroalimentación

En el siguiente escenario, asumimos que el protocolo utiliza una integral proporcional controlador para calcular la tasa de reembolso:

- El índice reflejo se lanza con un precio de canje arbitrario "rand".
- En algún momento, el precio de mercado del índice aumenta de 'rand' a 'rand' + x. Después de el mecanismo de retroalimentación lee el nuevo precio de mercado, calcula un término proporcional *p*, que en este caso es -1 * (('rand' + x) / 'rand'). O proporcional es negativo para disminuir el precio de reembolso y, a su vez, reparar los índices para abaratarlos

- Después de calcular el proporcional, el motor determinará el integral término *i* sumando todas las desviaciones anteriores de la última *desviación Intervalo* segundos de

- El mecanismo suma el proporcional y el integral y calcula un tasa de rescate por segundo *r* que lentamente comienza a disminuir el rescate precio. A medida que los creadores de SAFE se den cuenta de que pueden generar más deuda, inundarán el mercado con más índices
- Después de *n* segundos, el mecanismo detecta que la desviación entre los Los precios de mercado y de reembolso son insignificantes (bajo un parámetro específico *ruido*). En este punto, el algoritmo establece r en cero y mantiene el rescate precio donde esta

En la práctica, el algoritmo será más robusto y haremos algunas variables inmutable (por ejemplo, *ruido de* parámetros, *deviationInterval*) o habrá límites estrictos sobre qué puede cambiar la gobernanza.

Ajuste del mecanismo de retroalimentación

De extrema importancia para el correcto funcionamiento del sistema de índice de reflejos es el Ajuste de los parámetros del controlador algorítmico. Una parametrización inadecuada puede resultar en que el sistema sea demasiado lento para lograr estabilidad, adelantamientos masivos o siendo generalmente inestable ante choques externos.

El proceso de ajuste de un controlador PID generalmente implica ejecutar el sistema en vivo, ajustar los parámetros de ajuste y observar la respuesta del sistema, a menudo introduciendo choques a propósito en el camino. Dada la dificultad y el riesgo financiero para ajustar los parámetros de un sistema de índice de reflejos en vivo, planeamos aprovechar modelado y simulación por computadora tanto como sea posible para definir los parámetros iniciales, pero también permitirá a la gobernanza actualizar los parámetros de ajuste si hay datos adicionales de producción muestra que están por debajo de lo ideal.

Configurador de mercado monetario

En RAI, pretendemos mantener la tasa de préstamo (tasa de interés aplicada al generar fijo o limitado y solo modificar el precio de redención, minimizando así la complejidad involucrada en el modelado del mecanismo de retroalimentación. La tasa de préstamo de nuestro caso es igual al diferencial entre la tasa de estabilidad y el DSR en el DAI de múltiples garantías.

Aunque planeamos mantener fija la tasa del préstamo, es posible cambiarla junto al precio de reembolso mediante un configurador de mercado monetario. El mercado de dinero cambia la tasa de préstamo y el precio de reembolso de una manera que fomenta el SEGURO creadores para generar más o menos deuda. Si el precio de mercado de un índice está por encima redención, ambas tasas comenzarán a disminuir, mientras que si está por debajo de la redención, las
tasas aumentarán.

Acuerdo global

La liquidación global es un método de último recurso utilizado para garantizar el precio de reembolso. a todos los titulares de índices reflejos. Está destinado a permitir a los titulares del índice reflejo y SEGURO creadores para canjear la garantía del sistema a su valor neto (número de índices para cada tipo de garantía, según el último precio de reembolso). Cualquiera puede desencadenar liquidación después de quemar una cierta cantidad de tokens de protocolo.

La liquidación tiene tres etapas principales:

- **Activador**: se activa la liquidación, los usuarios ya no pueden crear SAFE, todos los precios de garantía y el precio de reembolso se congelan y registran

- **Proceso**: procesar todas las subastas pendientes

- **Reclamo**: cada titular de índice reflejo y creador SAFE puede reclamar una cantidad fija de cualquier garantía del sistema basada en el último precio de reembolso 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 los tokens de gobernanza implementen un sistema completamente nuevo. Elegimos esta estrategia porque podemos eliminar el metajuego en el que las personas intentan influir en el proceso de gobernanza para su propio beneficio, socavando la confianza en el sistema. Establecimos 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 quieran 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 diseñado para retrasar o limitar todas las posibles modificaciones al sistema. Además, presentamos Governance Ice Age, un registro de permisos que puede bloquear algunas partes del sistema de control externo después de que hayan expirado ciertos plazos.

Gobernanza por tiempo limitado La gobernanza por tiempo limitado

es el primer componente del Módulo de gobernanza restringida. Impone retrasos de tiempo entre los cambios aplicados al mismo parámetro. Un ejemplo es la posibilidad de cambiar las direcciones de Oracle utilizadas en Oracle Network Medianizer (Sección 6.2) después de queal menosOracle *T* hayan pasadosegundos desde la última modificación del.

Gobernanza limitada por acciones

El segundo componente del Módulo de gobernanza restringida es la gobernanza limitada por acciones. Cada parámetro gobernable tiene límites sobre los valores que se pueden establecer y cuánto puede cambiar en un período de tiempo determinado. Ejemplos notables son las primeras versiones del mecanismo de retroalimentación de la tasa de canje (Sección 4.2), que los titulares de tokens de gobernanza podrán ajustar.

Ice Age Governance

AGelo es un contrato inteligente inmutable que impone plazos para cambiar parámetros específicos del sistema y actualizar el protocolo. Se puede utilizar en caso

de que el gobierno quiera asegurarse de que puede corregir errores antes de que el protocolo se bloquee y niegue la intervención externa. Ice Age comprobará si se permite un cambio comparando el nombre del parámetro y la dirección del contrato afectado en un registro de términos. Si el período ha expirado, la llamada 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 solo se puede posponer tres veces, cada vez durante un mes, para que las correcciones de errores recién implementadas se prueben correctamente.

Áreas centrales donde se necesita gobernanza

Anticipamos cuatro áreas donde la gobernanza puede ser necesaria, especialmente en las primeras versiones de esta estructura:

- **Agregar nuevos tipos de garantías**: RAI estará respaldado solo por ETH, pero otros índices estarán respaldados por varios tipos de las garantías y la gobernanza podrán
  diversificar el riesgo a lo largo del tiempo.

- **Cambio de dependencias externas**: se pueden actualizar oráculos y DEX de los que depende el sistema. La gobernanza puede orientar el sistema hacia dependencias más nuevas para que continúe funcionando correctamente

- **Definidores de tasas de ajuste fino**: los primeros controladores de política monetaria tendrán parámetros que se pueden cambiar dentro de límites razonables (como se describe en Acción y gobernanza con límite de tiempo)

- **migración entre versiones del**sistema:en algunos casos, el gobierno puede implementar un nuevo sistema, otorgarle permiso para imprimir tokens de protocolo y eliminar este permiso de un sistema antiguo. Esta migración se logra con la ayuda del Módulo de migración restringida que se describe a continuación.migración restringida

Módulo de

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

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

- Cada vez que el gobierno implementa una nueva versión del sistema, envían 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.

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

- Un contrato opcional puede configurarse para apagar 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 otorga automáticamente permisos a sistemas específicos para poder imprimir tokens en todo momento.

Apagado automático del sistema

Hay casos en los que el sistema puede detectar automáticamente y, como resultado, activar asentamiento 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 garantía o índice no se han actualizado durante mucho tiempo.

- **Migración del sistema**: este es un contrato opcional que puede rescindir el protocolo después de un período de enfriamiento pasado el Momento en que la gobernanza elimina 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 *x%* desvió undurante mucho tiempo en comparación

con el precio de rescate, la

gobernanza podrá actualizar estos módulos de apagado autónomo mientras aún siendo limitado o hasta que la Edad de Hielo comience a bloquear algunas partes del sistema.

Oráculos

Hay tres tipos de activos principales para los que el sistema necesita leer los feeds de precios: índice, token de protocolo y cada tipo de garantía en la lista blanca. Los feeds de precios pueden ser proporcionado por oráculos dirigidos por el gobierno o por redes de oráculos establecidas.

Oráculos dirigidos por la 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 de la red y luego envían una transacción para un contrato inteligente que media todos los puntos de datos.

Este enfoque permite una mayor flexibilidad para actualizar y cambiar el oráculo. infraestructura, aunque a costa de una falta de confianza.

Oracle Networkde

MedianizermedianizerUmrede oracle es un contrato inteligente que lee precios de varios fuentes que no están directamente controladas por la gobernanza (por ejemplo, grupo Uniswap V2 entre un tipo de garantía de índice y otras monedas estables) y luego media todas resultados. ONM funciona de la siguiente manera:

- Nuestro contrato rastrea las redes de Oracle permitidas a las que puede llamar. pregunte por precios de garantía. El contrato se financia con el excedente de la acumula el sistema (utilizando el excedente de tesorería, sección 11). Cada red de Oracle acepta tokens específicos como pago por nuestro contrato para rastrear también el cantidad mínima y tipo de tokens necesarios para cada solicitud

- Para impulsar un nuevo feed de precios en el sistema, todos los oráculos deben

ser llamado de antemano. Al llamar a un oráculo, el contrato primero intercambia algunos tasas de estabilidad con uno de los tokens aceptados por el oráculo. Después de que un oráculo es llamado, el contrato marca la llamada como "válida" o "inválida". Si una llamada no es válida, el oráculo defectuoso específico no se puede volver a llamar hasta que todos los demás sean llamados y el contrato verifica que existe una mayoría válida. Una llamada de Oracle válida no debería revertir y debería recuperar un precio que se publicó en la red en algún momento los últimos *m* segundos. "Recuperar" significa cosas diferentes dependiendo de cada tipo de oráculo:

    - Para oráculos basados en pull, de los cuales podemos obtener un resultado de inmediato, nuestro el contrato debe pagar una tarifa y buscar 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 del oráculo se guarda en una matriz. Después de que se llame a cada oráculo de la lista blanca y si la matriz tiene suficientes puntos de datos válidos para formar una mayoría (por ejemplo, el contrato recibió datos válidos de 3/5 oráculos), los resultados se clasifican y el contrato elige la mediana

- Ya sea que el contrato encuentre la mayoría o no, la matriz con los resultados de Oracle es cancelado y el contrato tendrá que esperar *p* segundos antes de comenzar todo proceso todo de nuevo

Oracle Network BackupOracle

Governance puede agregar una opción de copia de seguridad deque comienza a impulsar los precios del sistema si el mediador no puede encontrar la mayoría de las redes de Oracle válidas varias veces seguidas.

La opción de respaldo debe configurarse cuando se implementa el medianizador, ya que no se puede cambiado más tarde. Además, un contrato separado puede monitorear si la copia de seguridad fue ha estado reemplazando el mecanismo de medianización durante mucho tiempo y se cierra automáticamente el protocolo.

Cajas fuertes

Para generar índices, cualquiera puede depositar y aprovechar su seguridad criptográfica dentro de cajas fuertes. Mientras se abra un SAFE, seguirá acumulando deuda de acuerdo con la tasa de préstamo de la garantía depositada. A medida que el creador de SAFE pague su deuda, podrá retirar cada vez más su garantía bloqueada.

Ciclo de vida de SAFE

Hay cuatro pasos principales necesarios para crear índices reflexivos y, posteriormente, para pagar una deuda SAFE:

- Garantía de depósito con SAFE

  El usuario primero debe crear un nuevo SAFE y depositar la garantía allí. ● Generar índices respaldados por la garantía SAFE

  El usuario especifica cuántos índices quiere generar. El sistema crea una cantidad igual de deuda que comienza a acumularse a la tasa del préstamo de garantía.

- Pagar la deuda de SAFE

  Cuando el creador de SAFE quiere retirar su garantía, debe pagar su deuda inicial más los intereses devengados.

- Retirada de la garantía

  Una vez que el usuario haya pagado parte o la totalidad de su deuda, se le permitirá retirar la garantía.

Liquidación SEGURA

Para mantener el sistema solvente y cubrir el valor de toda la deuda pendiente, cada SAFE puede liquidarse en caso de que su índice de garantía caiga por debajo de un determinado umbral. Cualquiera puede iniciar un acuerdo, en cuyo caso el sistema confiscará garantías SAFE y las venderá en una *subasta de garantías*.

Seguro de liquidación

En una versión del sistema, los creadores de SAFE pueden tener la opción de elegir un

desencadenante para cuando se liquiden sus SAFE. Los desencadenantes son contratos inteligentes que agregan automáticamente más garantías a un SEGURO 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 las SAFE es la adición de dos límites de garantía diferentes: *seguro* y *riesgo*. Os usuários do SAFE podem gerar dívidas até atingirem o limite seguro (que é mais alto do que o risco) e só serão liquidados quando a garantia do SAFE ficar abaixo do limite do risco.

Leilões de garantias

Para iniciar um leilão de garantias, o sistema precisa usar uma variável chamada *liquidationQuantity* para determinar o valor da dívida a ser coberto em cada leilão e o valor correspondente de garantias a serem vendidas. Uma *penalidade de liquidação* será aplicada a cada SAFE leiloado.

Collateral leilão Parâmetros

MINIMUMBID	montantemínima de moedas que precisam ser oferecido emum lance
desconto de	Discountem que a garantia está sendo vendido

lowerCollateralMedianDeviation	Max diminuir desvio limite que a mediana garantia pode ter em relação ao preço oráculo
upperCollateralMedianDeviation	Max desvio limite superior que o mediano garantia pode ter em relação ao preço do oracle
lowerSystemCoinMedianDeviation	Max desvio do limite inferior que a alimentação de moeda sistema preço oracle pode ter em relação ao preço do oracle moeda sistema

upperSystemCoinMedianDeviation	Max desvio limite superior que a mediana garantia pode ter em relação ao preço do oracle moeda sistema
minSystemCoinMedianDeviation	Min desvio para o resultado mediano da moeda do sistema em relação ao preço de resgate, a fim de levar em consideração a mediana.

Mecanismo de leilão de garantia

O leilão de desconto fixo é uma forma direta (em comparação com os leilões ingleses) de colocar garantias à venda em e xchange para moedas do sistema usadas para liquidar dívidas incobráveis. Os licitantes só precisam permitir que a casa de leilões transfira seu safeEngine.coinBalance e podem então chamar buyCollateral para trocar suas moedas do sistema por garantias que são vendidas com um desconto em relação ao último preço de mercado registrado.

Os licitantes também podem revisar o valor da garantia que podem obter de um leilão específico chamando getCollateralBought ou getApproximateCollateralBought. Observe que getCollateralBought não está marcado como view porque lê (e também atualiza) o redemptionPrice do relayer oracle, enquanto getApproximateCollateralBought usa lastReadRedemptionPrice.

Leilões de dívida

No cenário em que um leilão de garantia não pode cobrir todas as dívidas inadimplentes em um SEGURO e se o sistema não tiver reservas excedentes, qualquer pessoa pode acionar um leilão de dívida.
Os leilões de dívida têm como objetivo cunhar mais tokens de protocolo (Seção 10) e vendê-los por índices que podem anular a inadimplência remanescente do sistema.

A fim de iniciar um leilão de dívida, as necessidades do sistema de usar dois parâmetros:

- initialDebtAuctionAmount:a quantidade inicial de fichas de protocolo para hortelã pós-leilão

- debtAuctionBidSize:o tamanho inicial de oferta (quantos índices devem ser oferecidas em troca de *initialDebtAuctionAmount* fichas de protocolo)

Definição de Parâmetros de Leilão de Dívida Autônoma

A quantidade inicial de tokens de protocolo cunhados em um leilão de dívida pode ser definida por meio de uma votação de governança ou pode ser ajustada automaticamente pelo sistema. Uma versão automatizada precisaria ser integrada aos oráculos (Seção 6) a partir dos quais o sistema leria o token de protocolo e os preços de mercado do índice de reflexo. The system would then set the initial amount of protocol tokens (*initialDebtAuctionAmount*) that will be minted for *debtAuctionBidSize* indexes. *initialDebtAuctionAmount* can be set at a discount compared to the actual PROTOCOL/INDEX market price in order to incentivize bidding.

Debt Auction Parameters

amountSoldIncrease	Increase in the amount of protocol tokens to be minted for the same amount of indexes
bidDecrease	Next bid's minimum decrease in the accepted amount of protocol tokens for the same amount of indexes
bidDuration	How long the bidding lasts after a new bid is submitted (in seconds)
totalAuctionLength	Total length of the auction (in seconds)
auctionsStarted	How many auctions have started until now

Debt Auction Mechanism

As opposed to collateral auctions, debt auctions only have one stage:

decreaseSoldAmount(uint id, uint amountToBuy, uint bid): decrease the amount of

protocol tokens accepted in exchange for a fixed amount of indexes.

The auction will be restarted if it has no bids placed. Every time it restarts, the system will offer more protocol tokens for the same amount of indexes. The new protocol token amount is calculated as *lastTokenAmount* * *amountSoldIncrease* / 100. After the auction settles, the system will mint tokens for the highest bidder.

Protocol Tokens

As described in earlier sections, each protocol will need to be protected by a token that is minted through debt auctions. Apart from protection, the token will be used to govern a few system components. Also, the protocol token supply will gradually be reduced with the use of surplus auctions. The amount of surplus that needs to accrue in the system before extra funds are auctioned is called the *surplusBuffer* and it is automatically adjusted as a percentage of the total debt issued.

Insurance Fund

Apart from the protocol token, governance can create an insurance fund that holds a wide array of uncorrelated assets and which can be used as a backstop for debt auctions.

Surplus Auctions

Surplus auctions sell stability fees accrued in the system for protocol tokens that are then burned.

Surplus Auction Parameters

bidIncrease	Minimum increase in the next bid
bidDuration	How long the auction lasts after a new bid is submitted (in seconds)
totalAuctionLength	Total length of the auction (in seconds)

auctionsStarted	How many auctions have started until now

Surplus Auction Mechanism

Surplus auctions have a single stage:

`increaseBidSize(uint id, uint amountToBuy, uint bid)`: anyone can bid a higher amount of protocol tokens for the same amount of indexes (surplus). Every new bid needs to be higher than or equal to *lastBid* * *bidIncrease* / 100. The auction will end after maximum *totalAuctionLength* seconds or after *bidDuration* seconds have passed since the latest bid and no new bids have been submitted in the meantime.

An auction will restart if it has no bids. On the other hand, if the auction has at least one bid, the system will offer the surplus to the highest bidder and will then burn all the gathered protocol tokens.

Surplus Indexes Management

Every time a user generates indexes and implicitly creates debt, the system starts applying a borrowing rate to the user's SAFE. The accrued interest is pooled in two different smart contracts:

- The *accounting engine* used to trigger debt (Section 9.2) and surplus (Section 10.1) auctions
- The *surplus treasury* used to fund core infrastructure components and incentivize external actors to maintain the system

The surplus treasury is in charge of funding three core system components:

- Oracle module (Section 6). Depending on how an oracle is structured, the treasury either pays governance whitelisted, off-chain oracles or it pays for calls toward oracle networks. The treasury can also be set up to pay the addresses that spent gas to call an oracle and update it

- In some cases, independent teams that maintain the system. Exemplos são teams who whitelist new collateral types or fine tune the system's rate setter (Seção 4.2)

The treasury can be set up so that some surplus recipients will automatically be denied funding in the future and others can take their place.

External Actors

The system depends on external actors in order to function properly. These actors are economically incentivized to participate in areas such as auctions, global settlement processing, market making and updating price feeds in order to maintain the system's health.

We will provide initial user interfaces and automated scripts to enable as many people as possible to keep the protocol secure.

Addressable Market

We see RAI as being useful in two main areas:

- **Portfolio diversification**: investors use RAI to get dampened exposure to an asset like ETH without the whole risk of actually holding ether

- **Collateral for synthetic assets**: RAI can offer protocols such as UMA, MakerDAO and Synthetix a lower exposure to the crypto market and give users more time to exit their positions in the case of scenarios such as Black Thursday from March 2020 when millions of dollars worth of crypto assets were liquidated

Future Research

To push the boundaries of decentralized money and bring further innovation in decentralized finance, we will continue to look for alternatives in core areas such as governance minimization and liquidation mechanisms.

We first want to lay the groundwork for future standards around protocols that lock themselves from outside control and for true “money robots” which adapt in response to market forces. Afterwards, we invite the Ethereum community to debate and design improvements around our proposals with a specific focus on collateral and debt auctions.

Risks and Mitigation

There are several risks involved in developing and launching a reflex index, as well as subsequent systems that are built on top:

- **Smart contract bugs**: the greatest risk posed to the system is the possibility of a bug that allows anyone to extract all the collateral or locks the protocol in a state it cannot recover from. We plan to have our code reviewed by multiple security researchers and launch the system on a testnet before we commit to deploying it in production

- **Oracle failure**: we will aggregate feeds from multiple oracle networks and there will be strict rules in place for upgrading only one oracle at a time so that malicious governance cannot easily introduce false prices

- **Collateral black swan events**: there is the risk of a black swan event in the underlying collateral which can result in a high amount of liquidated SAFEs. Liquidations may not be able to cover the entire outstanding bad debt and so the system will continuously change its surplus buffer in order to cover a decent amount of issued debt and withstand market shocks

- **Improper rate setter parameters**: autonomous feedback mechanisms are highly experimental and may not behave exactly like we predict during simulations. We plan to allow governance to fine-tune this component (while still being bounded) in order to avoid unexpected scenarios
- **Failure to bootstrap a healthy liquidator market**: liquidators are vital actors that make sure all issued debt is covered by collateral. We plan to create interfaces and automated scripts so that as many people as possible can participate in keeping the system secure.

Summary

We have proposed a protocol that progressively locks itself from human control and issues a low volatility, collateralized asset called a reflex index. We first presented the autonomous mechanism meant to influence the index's market price and then described how several smart contracts can limit the power that token holders have

over the system. We outlined a self-sustaining scheme for medianizing price feeds from multiple independent oracle networks and then finished by presenting the general mechanism for minting indexes and liquidating SAFEs.

References

[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] KJ Åström, RM Murray, “Feedback Systems: An Introduction for Scientists and Engineers”, https://bit.ly/3bHwnMC

[5] RJ Hawkins, JK Speakes, DE 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

Glossary

Reflex index: a collateralized asset that dampens the volatility of its underlying

RAI: our first reflex index

Redemption Price: the price that the system wants the index to have. It changes, influenced by a redemption rate (computed by RRFM), in case the market price is not close to it. Meant to influence SAFE creators to generate more or pay back some of their debt

Borrowing Rate: annual interest rate applied to all SAFEs that have outstanding debt

Redemption Rate Feedback Mechanism (RRFM): an autonomous mechanism which

compares the market and redemption prices of a reflex index and then computes a redemption rate that slowly influences SAFE creators to generate more or less debt (and implicitly tries to minimize the market/redemption price deviation)

Money Market Setter (MMS): a mechanism similar to RRFM which pulls multiple monetary levers at once. In the case of reflex indexes, it modifies both the borrowing rate and the redemption price

Oracle Network Medianizer (ONM): a smart contract that pulls prices from multiple oracle networks (which are not controlled by governance) and medianizes them if a majority (eg 3 out of 5) returned a result without throwing

Restricted Governance Module (RGM): a set of smart contracts that bound the power that governance tokens holders have over the system. It either enforces time delays or limits the possibilities that governance has to set certain parameters

Governance Ice Age: immutable contract that locks most components of a protocol from outside intervention after a certain deadline has passed

Accounting Engine: system component which triggers debt and surplus auctions. It also keeps track of the amount of currently auctioned debt, unactioned bad debt and the surplus buffer

Surplus Buffer: amount of interest to accrue and keep in the system. Any interest accrued above this threshold gets sold in surplus auctions that burn protocol tokens

Surplus Treasury: contract that gives permission to different system modules to withdraw accrued interest (eg ONM for oracle calls)