Rai: Uma garantia de baixa volatilidade e confiança minimizada para o ecossistema DeFi

Stefan C. Ionescu, Ameen Soleimani

Maio de 2020

Resumo. Apresentamos um protocolo de governança minimizado e descentralizado que reage automaticamente às forças do mercado para modificar o valor alvo de seu ativo colateralizado nativo. O protocolo permite que qualquer pessoa aproveite seus ativos criptográficos e emita um "índice de reflexo", que é uma versão atenuada de sua garantia subjacente. Descrevemos como os índices podem ser úteis como garantia universal de baixa volatilidade que pode proteger seus detentores, bem como outros protocolos financeiros descentralizados, de mudanças repentinas no mercado. Apresentamos nossos planos para ajudar outras equipes a lançar seus próprios sintéticos, aproveitando nossa infraestrutura. Por fim, oferecemos alternativas às estruturas oraculares e de governança atuais que são frequentemente encontradas em muitos protocolos DeFi.

Conteúdo

Introdução

O dinheiro é um dos mecanismos de coordenação mais poderosos que a humanidade utiliza para prosperar. O privilégio de administrar a oferta de dinheiro tem sido historicamente mantido nas mãos da liderança soberana e da elite financeira enquanto é imposto a um público em geral inconsciente. Onde o Bitcoin demonstrou o potencial de um protesto popular para manifestar um ativo de commodity de valor, o Ethereum nos dá uma plataforma para construir instrumentos sintéticos lastreados em ativos que podem ser protegidos da volatilidade e usados como garantia, ou atrelados a um preço de referência e usado como meio de troca para transações diárias, todas aplicadas pelos mesmos princípios de consenso descentralizado.

O acesso sem permissão ao Bitcoin para armazenar riqueza e instrumentos sintéticos devidamente descentralizados no Ethereum estabelecerá as bases para a próxima revolução financeira, fornecendo àqueles que estão à margem do sistema financeiro moderno os meios para coordenar a construção do novo.

Neste artigo, apresentamos uma estrutura para a construção de índices reflexos, um novo tipo de ativo que ajudará outros sintéticos a florescer e estabelecerá um alicerce fundamental para todo o setor financeiro descentralizado.

Visão geral dos índices de reflexo

O objetivo de um índice reflexo não é manter uma indexação específica, mas amortecer a volatilidade de suas garantias. Os índices permitem que qualquer pessoa ganhe exposição ao mercado de criptomoedas sem a mesma escala de risco que possui ativos criptográficos reais. Acreditamos que o RAI, nosso primeiro índice de reflexo, terá utilidade imediata para outras equipes que emitem sintéticos no Ethereum (por exemplo, Multi-Collateral DAI da MakerDAO [1], UMA [2], Synthetix [3]) porque dá aos seus sistemas uma menor exposição a ativos voláteis como ETH e oferece aos usuários mais tempo para sair de suas posições em caso de uma mudança significativa no mercado.

Para entender os índices reflexos, podemos comparar o comportamento do preço de resgate com o preço de uma stablecoin.

O preço de resgate é o valor de uma unidade de dívida (ou moeda) no sistema. Ele deve ser usado apenas como uma ferramenta de contabilidade interna e é diferente do preço de mercado (o valor pelo qual o mercado está negociando a moeda). No caso de fiat-backed stablecoins como USDC, os operadores do sistema declaram que qualquer pessoa pode resgatar uma moeda por um dólar americano e, portanto, o preço de resgate dessas moedas é sempre um. Há também casos de stablecoins lastreadas em criptomoedas, como o Multi Collateral DAI (MCD) da MakerDAO, onde o sistema tem como alvo um peg fixo de um dólar americano e, portanto, o preço de resgate também é fixado em um.

Na maioria dos casos, haverá uma diferença entre o preço de mercado de uma stablecoin e seu preço de resgate. Esses cenários criam oportunidades de arbitragem em que os comerciantes criarão mais moedas se o preço de mercado for maior que o resgate e resgatarão suas stablecoins como garantia (por exemplo, dólares americanos no caso do USDC) caso o preço de mercado seja menor que o preço de resgate.

Os índices de reflexo são semelhantes às stablecoins porque também têm um preço de resgate que o sistema visa. A principal diferença no caso deles é que seu resgate não permanecerá fixo, mas é projetado para mudar ao ser influenciado pelas forças do mercado. Na Seção 4, explicamos como o preço de resgate de um índice flutua e cria novas oportunidades de arbitragem para seus usuários.

Filosofia de design e estratégia de entrada no mercado

Nossa filosofia de projeto é priorizar a segurança, estabilidade e velocidade de entrega.
A DAI multicolateral foi o lugar natural para começar a iterar no design da RAI. O sistema foi fortemente auditado e verificado formalmente, tem dependências externas mínimas e reuniu uma comunidade ativa de especialistas. Para minimizar o esforço de desenvolvimento e comunicação, queremos fazer apenas as alterações mais simples na base de código MCD original para alcançar nossa implementação.
Nossas modificações mais importantes incluem a adição de um definidor de taxas autônomo, um Oracle Network Medianizer integrado a muitos feeds de preços independentes e uma camada de minimização de governança destinada a isolar o sistema o máximo possível da intervenção humana.

A primeira versão do protocolo (Estágio 1) incluirá apenas o definidor de taxa e outras pequenas melhorias na arquitetura principal. Assim que provarmos que o setter funciona como esperado, podemos adicionar com mais segurança o medianizador oracle (Estágio 2) e a camada de minimização de governança (Estágio 3).

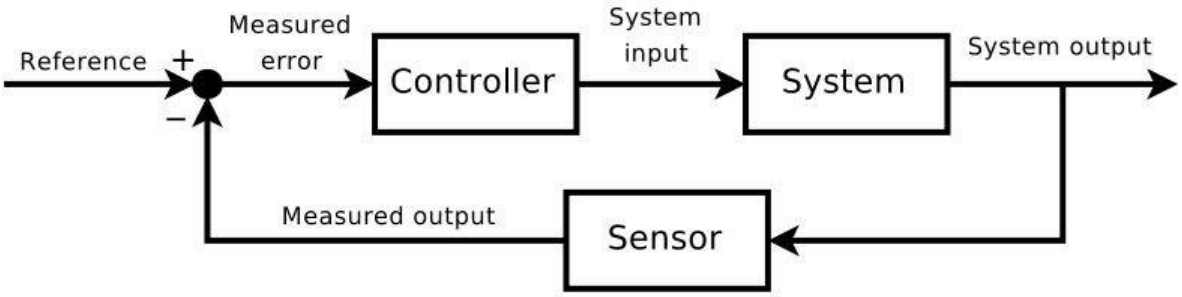
Mecanismos de política monetária

Introdução à teoria de controle

Um sistema de controle comum com o qual a maioria das pessoas está familiarizada é o chuveiro. Quando alguém inicia um banho, tem em mente uma temperatura desejada da água que, na teoria do controle, é chamada de ponto de referência. A pessoa, atuando como controlador, mede continuamente a temperatura do fluxo de água (que é chamada de saída do sistema) e modifica a velocidade com que gira o botão do chuveiro com base no desvio (ou erro) entre a temperatura desejada e a atual. A velocidade na qual o botão é girado é chamada de entrada do sistema. O objetivo é girar o botão rápido o suficiente para atingir o ponto de referência rapidamente, mas não tão rápido que a temperatura ultrapasse. Se houver choques no sistema em que a temperatura do fluxo de água mude repentinamente, a pessoa deve ser capaz de manter a temperatura atual sabendo com que rapidez deve girar o botão em resposta à perturbação.

A disciplina científica de manter a estabilidade em sistemas dinâmicos é chamada de teoria de controle e encontrou ampla aplicação em controle de cruzeiro para carros, navegação aérea, reatores químicos, braços robóticos e processos industriais de todos os tipos. O algoritmo de ajuste de dificuldade do Bitcoin, que mantém o tempo médio de bloqueio de dez minutos, apesar de um hashrate variável, é um exemplo de sistema de controle de missão crítica.

Na maioria dos sistemas de controle modernos, um controlador algorítmico é normalmente incorporado ao processo e recebe controle sobre uma entrada do sistema (por exemplo, o pedal do acelerador de um carro) para atualizá-lo automaticamente com base em desvios entre a saída do sistema (por exemplo, a velocidade de um carro) e o ponto de ajuste (por exemplo, a velocidade do piloto automático).



O tipo mais comum de controlador algorítmico é o controlador PID. Mais de 95% das aplicações industriais e uma ampla gama de sistemas biológicos empregam elementos de PID.

controle [4]. Um controlador PID usa uma fórmula matemática com três partes para determinar sua saída:

Saída do Controlador = Termo Proporcional + Termo Integral + Termo Derivativo

O Termo Proporcional é a parte do controlador que é diretamente proporcional ao desvio. Se o desvio for grande e positivo (por exemplo, o ponto de ajuste da velocidade do controle de cruzeiro é muito maior que a velocidade atual do carro), a resposta proporcional será grande e positiva (por exemplo, pise no pedal do acelerador).

O Termo Integral é a parte do controlador que leva em consideração quanto tempo um desvio persistiu. É determinado tomando a integral do desvio ao longo do tempo e é usado principalmente para eliminar o erro de estado estacionário. Ele se acumula para responder a desvios pequenos, embora persistentes, do ponto de ajuste (por exemplo, o ponto de ajuste do controle de cruzeiro foi 1 mph mais alto que a velocidade do carro por alguns minutos).

O Termo Derivativo é a parte do controlador que leva em conta a rapidez com que o desvio está crescendo ou diminuindo. É determinado pela derivada do desvio e serve para acelerar a resposta do controlador quando o desvio está aumentando (por exemplo, acelerar se o ponto de ajuste do controle de cruzeiro for maior que a velocidade do carro e o carro começar a desacelerar). Também ajuda a reduzir o overshoot desacelerando a resposta do controlador quando o desvio está diminuindo (por exemplo, alivie o acelerador quando a velocidade do carro começar a se aproximar do ponto de ajuste do controle de cruzeiro).

A combinação dessas três partes, cada uma das quais pode ser ajustada independentemente, oferece aos controladores PID grande flexibilidade no gerenciamento de uma ampla variedade de aplicações de sistemas de controle.

Os controladores PID funcionam melhor em sistemas que permitem algum grau de atraso no tempo de resposta, bem como a possibilidade de overshoot e oscilação em torno do setpoint enquanto o sistema tenta se estabilizar. Sistemas de índices Reflex como o RAI são adequados para este tipo de cenário onde seus preços de resgate podem ser alterados pelos controladores PID.

De maneira mais geral, descobriu-se recentemente que muitas das atuais regras de política monetária do banco central (por exemplo, a Regra de Taylor) são na verdade aproximações do PID controladores [5].

Mecanismo de Feedback da Taxa de Resgate

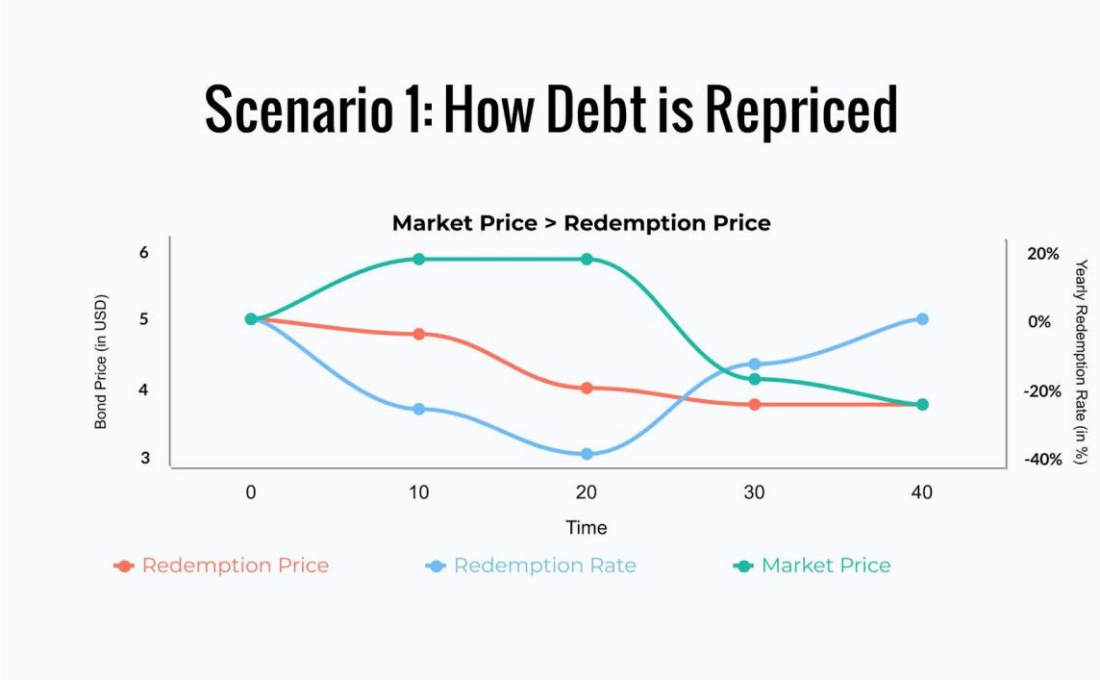
O Mecanismo de Feedback da Taxa de Resgate é o componente do sistema responsável por alterar o preço de resgate de um índice reflexo. Para entender como funciona, primeiro precisamos descrever por que o sistema precisa de um mecanismo de feedback em vez de usar o controle manual e qual é a saída do mecanismo.

Componentes do Mecanismo de Feedback

Em teoria, seria possível manipular diretamente o preço de resgate do índice reflexo (descrito na Seção 2) para influenciar os usuários do índice e, finalmente, alterar o preço de mercado do índice. Na prática, esse método não teria o efeito desejado nos participantes do sistema. Do ponto de vista de um detentor de SAFE, se o preço de resgate for aumentado apenas uma vez, ele poderá aceitar um preço mais alto por unidade de dívida, absorver a perda de uma redução do índice de garantia e manter sua posição. Se, no entanto, eles esperam que o preço de resgate continue a aumentar ao longo do tempo, eles provavelmente estariam mais inclinados a evitar perdas futuras esperadas e, assim, optariam por pagar sua dívida e fechar suas posições.
Esperamos que os participantes do sistema de índices reflexos não respondam diretamente às mudanças no preço de resgate, mas respondam à taxa de mudança do preço de resgate que chamamos de taxa de resgate. A taxa de resgate é definida por um mecanismo de feedback que a governança pode ajustar ou permitir que seja totalmente automatizada.

Cenários do Mecanismo de Feedback

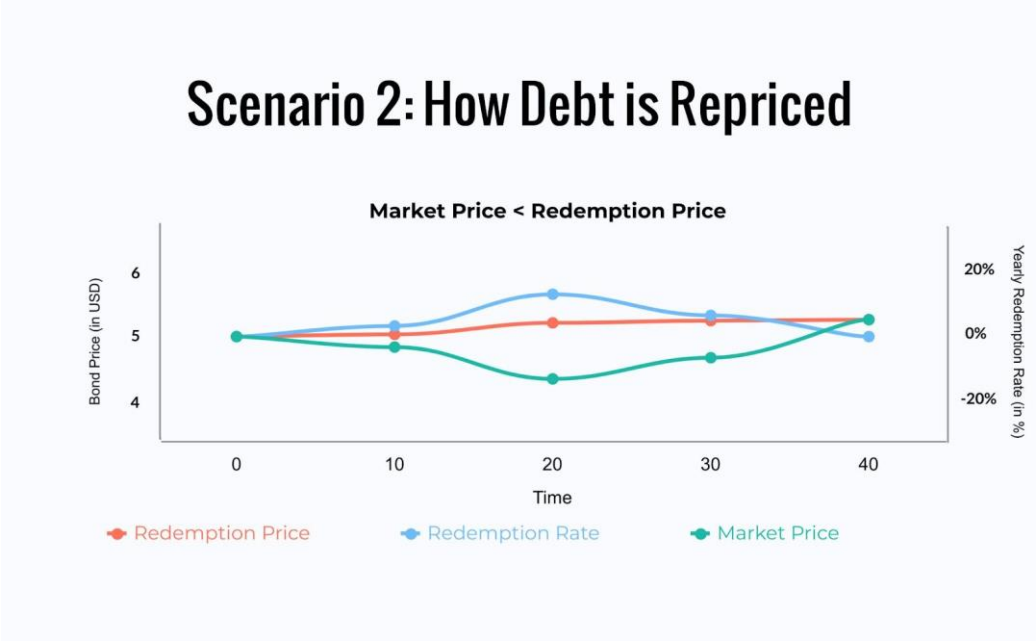
Lembre-se de que o mecanismo de feedback visa manter o equilíbrio entre o preço de resgate e o preço de mercado usando a taxa de resgate para contrabalançar as mudanças nas forças de mercado. Para tal, a taxa de resgate é calculada de forma a contrariar o desvio entre os preços de mercado e os preços de resgate. No primeiro cenário abaixo, se o preço de mercado do índice for superior ao seu preço de resgate, o mecanismo calculará uma taxa negativa que passará a diminuir o preço de resgate, barateando a dívida do sistema.



A expectativa de um preço de resgate decrescente provavelmente desencorajará as pessoas a manter os índices e incentivará os detentores do SAFE a gerar mais dívida (mesmo que o preço do colateral não

mude), que é então vendido no mercado, equilibrando oferta e demanda. Observe que este é o cenário ideal em que os detentores de índices reagem rapidamente em resposta ao mecanismo de feedback. Na prática (e especialmente nos primeiros dias pós-lançamento) esperamos uma defasagem entre o início do mecanismo e os resultados reais observados na quantidade de dívida emitida e posteriormente no preço de mercado.

Por outro lado, no cenário dois, se o preço de mercado do índice for inferior ao preço de resgate, a taxa se torna positiva e passa a reprecificar toda a dívida para que fique mais cara.
À medida que a dívida se torna mais cara, os índices de garantia de todos os SAFEs diminuem (assim, os criadores de SAFEs são incentivados a pagar suas dívidas) e os usuários começam a acumular índices com a expectativa de que eles aumentem de valor.



Algoritmo do Mecanismo de Feedback

No cenário a seguir, assumimos que o protocolo usa um controlador proporcional-integral para calcular a taxa de resgate:

• O índice de reflexo é lançado com um preço de resgate arbitrário 'rand'

• Em algum momento, o preço de mercado do índice sobe de 'rand' para 'rand' + x. Depois que o mecanismo de feedback lê o novo preço de mercado, ele calcula um termo proporcional p, que neste caso é -1 * (('rand' + x) / 'rand'). O proporcional é negativo para diminuir o preço de resgate e, por sua vez, reprecificar os índices para que fiquem mais baratos

• Depois de calcular o proporcional, o mecanismo determinará o termo integral i adicionando todos os desvios passados do último desvioInterval segundos

• O mecanismo soma o proporcional e o integral e calcula uma taxa de resgate por segundo r que lentamente começa a diminuir o preço de resgate. À medida que os criadores do SAFE perceberem que podem gerar mais dívidas, eles inundarão o mercado com mais índices
• Após n segundos, o mecanismo detecta que o desvio entre os preços de mercado e de resgate é insignificante (sob um parâmetro de ruído especificado). Neste ponto, o algoritmo define r para zero e mantém o preço de resgate onde é

Na prática, o algoritmo será mais robusto e tornaremos algumas variáveis imutáveis (por exemplo, o parâmetro de ruído, desvioInterval) ou haverá limites estritos sobre o que a governança pode mudar.

Ajuste do mecanismo de feedback

De extrema importância para o bom funcionamento do sistema de índice de reflexo é o ajuste dos parâmetros do controlador algorítmico. A parametrização inadequada pode fazer com que o sistema seja muito lento para alcançar a estabilidade, superando massivamente ou geralmente instável diante de choques externos.

O processo de ajuste para um controlador PID normalmente envolve a execução do sistema ativo, ajustando os parâmetros de ajuste e observando a resposta do sistema, muitas vezes introduzindo choques propositalmente ao longo do caminho. Dada a dificuldade e o risco financeiro de ajustar os parâmetros de um sistema de índice de reflexo ao vivo, planejamos aproveitar ao máximo a modelagem e a simulação por computador para definir os parâmetros iniciais, mas também permitiremos que a governança atualize os parâmetros de ajuste se dados adicionais da produção mostra que eles são sub-ótimos.

Definidor do mercado monetário

No RAI, planejamos manter a taxa de empréstimo (taxa de juros aplicada na geração de índices) fixa ou limitada e apenas modificar o preço de resgate, minimizando assim a complexidade envolvida na modelagem do mecanismo de feedback. A taxa de empréstimo no nosso caso é igual ao spread entre a taxa de estabilidade e o DSR na DAI Multi-Colateral.

Embora planejemos manter a taxa de empréstimo fixa, é possível alterá-la juntamente com o preço de resgate usando um setter do mercado monetário. O mercado monetário altera a taxa de empréstimo e o preço de resgate de uma forma que incentiva os criadores do SAFE a gerar mais ou menos dívida. Se o preço de mercado de um índice estiver acima do resgate, ambas as taxas começarão a diminuir, enquanto se estiver abaixo do resgate, o
as taxas aumentarão.

Acordo Global

A liquidação global é um método de último recurso utilizado para garantir o preço de resgate a todos os detentores do índice reflexo. Destina-se a permitir que tanto os detentores de índices reflexivos quanto os criadores de SAFE resgatem as garantias do sistema pelo seu valor líquido (quantidade de índices por cada tipo de garantia, de acordo com o último preço de resgate). Qualquer pessoa pode acionar a liquidação depois de queimar uma certa quantidade de tokens de protocolo.
A liquidação tem três fases principais:

- Acionador: a liquidação é acionada, os usuários não podem mais criar SAFEs, todos os feeds de preços colaterais e o preço de resgate são congelados e registrados

- Processar: processar todos os leilões pendentes

- Reivindicação: cada detentor de índice de reflexo e criador de SAFE pode reivindicar um valor fixo de qualquer garantia do sistema com base no último preço de resgate registrado do índice

Governança

A grande maioria dos parâmetros será imutável e a mecânica interna do contrato inteligente não será atualizável, a menos que os detentores de tokens de governança implantem um sistema totalmente novo. Escolhemos essa estratégia porque podemos eliminar o meta-jogo em que as pessoas tentam influenciar o processo de governança em benefício próprio, prejudicando assim a confiança no sistema. Estabelecemos a

operação adequada do protocolo sem colocar muita fé em humanos (o “efeito bitcoin”) para maximizar a escalabilidade social e minimizar os riscos para outros desenvolvedores que desejam usar o RAI como infraestrutura central em seus próprios projetos.
Para os poucos parâmetros que podem ser alterados, propomos a adição de um Módulo de Governança Restrita para retardar ou limitar todas as modificações possíveis do sistema. Além disso, apresentamos o Governance Ice Age, um registro de permissões que pode bloquear algumas partes do sistema do controle externo após determinados prazos.

Governança Limitada no Tempo

A Governança Limitada no Tempo é o primeiro componente do Módulo de Governança Restrita. Impõe atrasos de tempo entre as alterações aplicadas ao mesmo parâmetro. Um exemplo é a possibilidade de alterar os endereços dos oráculos usados no Oracle Network Medianizer (Seção 6.2) após pelo menos T segundos desde a última modificação do oráculo.

Governança Limitada à Ação

O segundo componente do Módulo de Governança Restrita é a Governança Limitada à Ação. Cada parâmetro governável tem limites sobre quais valores podem ser definidos e quanto pode mudar ao longo de um determinado período de tempo. Exemplos notáveis são as versões iniciais do Mecanismo de Feedback da Taxa de Resgate (Seção 4.2) que os detentores de tokens de governança poderão ajustar.

Governança Era do Gelo

A Era do Gelo é um contrato inteligente imutável que impõe prazos na alteração de parâmetros específicos do sistema e na atualização do protocolo. Ele pode ser usado no caso em que a governança deseja garantir que eles possam corrigir bugs antes que o protocolo se bloqueie e negue a intervenção externa. A Ice Age verificará se uma alteração é permitida verificando o nome do parâmetro e o endereço do contrato afetado em relação a um registro de prazos. Caso o prazo tenha expirado, a chamada será revertida.
A governança pode atrasar a Era do Gelo um número fixo de vezes se os bugs forem encontrados perto da data em que o protocolo deve começar a se travar. Por exemplo, a Era do Gelo só pode ser adiada três vezes, cada vez por um mês, para que as correções de bugs recém-implementadas sejam testadas adequadamente.

Áreas principais onde a governança é necessária

Prevemos quatro áreas em que a governança pode ser necessária, especialmente nas primeiras versões desta estrutura:

- Adição de novos tipos de garantias: o RAI será apoiado apenas por ETH, mas outros índices serão apoiados por vários tipos de garantias e a governança poderá
diversificar o risco ao longo do tempo

- Alterando dependências externas: oráculos e DEXs dos quais o sistema depende podem ser atualizados. A governança pode apontar o sistema para novas dependências para que ele continue funcionando corretamente

- Ajustar as taxas de ajuste: os controladores iniciais da política monetária terão parâmetros que podem ser alterados dentro de limites razoáveis (conforme descrito por Action and Time Bounded Governance)

- Migração entre versões do sistema: em alguns casos, a governança pode implantar um novo sistema, dar permissão para imprimir tokens de protocolo e retirar essa permissão de um sistema antigo. Esta migração é realizada com a ajuda do Módulo de Migração Restrita descrito abaixo

Módulo de migração restrita

Veja a seguir um mecanismo simples para migrar entre as versões do sistema:

• Existe um registro de migração que acompanha quantos sistemas diferentes o mesmo token de protocolo abrange e quais sistemas podem ter a permissão negada para imprimir tokens de protocolo em um leilão de dívida

• Toda vez que a governança implanta uma nova versão do sistema, eles enviam o endereço do contrato de leilão de dívida do sistema no registro de migração. A governança também precisa especificar se eles poderão impedir que o sistema imprima tokens de protocolo. Além disso, a governança pode, a qualquer momento, dizer que um sistema sempre poderá imprimir tokens e, portanto, nunca será migrado de

• Há um período de espera entre propor um novo sistema e retirar as permissões de um antigo

• Um contrato opcional pode ser configurado para que ele desligue automaticamente um sistema antigo depois que as permissões de impressão forem negadas

O módulo de migração pode ser combinado com uma Era do Gelo que dá automaticamente a sistemas específicos a permissão para sempre poder imprimir tokens.

Desligamento automático do sistema

Há casos em que o sistema pode detectar automaticamente e, como resultado, acionar a liquidação sozinho, sem a necessidade de queimar tokens de protocolo:

• Atrasos graves no feed de preço: o sistema detecta que um ou mais feeds de preço de garantia ou índice não foram atualizados por um longo tempo

• Migração do sistema: este é um contrato opcional que pode encerrar o protocolo após um período de desaquecimento a partir do momento em que a governança retira a capacidade do mecanismo de leilão de dívida de imprimir tokens de protocolo (Módulo de migração restrita, seção 5.4.1)

• Desvio de preço de mercado consistente: o sistema detecta que o preço de mercado do índice está desviado há muito tempo x% em relação ao preço de resgate

A governança poderá atualizar esses módulos de desligamento autônomo enquanto ainda estão limitados ou até que a Era do Gelo comece a bloquear algumas partes do sistema.

Oráculos

Existem três tipos principais de ativos para os quais o sistema precisa ler os feeds de preços: o índice, o token de protocolo e cada tipo de garantia na lista de permissões. Os feeds de preços podem ser fornecidos por oráculos liderados por governança ou por redes oraculares já estabelecidas.

Oráculos de Governança

Os detentores de tokens de governança ou a equipe principal que lançou o protocolo podem fazer parceria com outras entidades que reúnem vários feeds de preços fora da cadeia e, em seguida, enviam uma única transação para um contrato inteligente que medianiza todos os pontos de dados.

Essa abordagem permite mais flexibilidade na atualização e alteração da infraestrutura da Oracle, embora isso venha à custa da falta de confiança.

Medianizador de Rede Oracle

Um medianizador de rede oracle é um contrato inteligente que lê preços de várias fontes que não são diretamente controladas pela governança (por exemplo, pool Uniswap V2 entre um tipo de garantia de índice e outras stablecoins) e medianiza todos os resultados. O ONM funciona da seguinte forma:

• Nosso contrato rastreia as redes oracle na lista de permissões para as quais ele pode ligar para solicitar preços de garantia. O contrato é financiado por parte do excedente que o sistema acumula (usando o Tesouro Excedente, Seção 11). Cada rede oracle aceita tokens específicos como pagamento, então nosso contrato também acompanha o valor mínimo e o tipo de tokens necessários para cada solicitação

• Para empurrar um novo feed de preços no sistema, todos os oráculos precisam ser chamados previamente. Ao chamar um oráculo, o contrato primeiro troca algumas taxas de estabilidade por um dos tokens aceitos pelo oráculo. Depois que um oráculo é chamado, o contrato marca a chamada como “válida” ou “inválida”. Se uma chamada for inválida, o oráculo específico defeituoso não poderá ser chamado novamente até que todos os outros sejam chamados e o contrato verifique se há uma maioria válida. Uma chamada oracle válida não deve ser revertida e deve recuperar um preço que foi postado na cadeia em algum momento nos últimos m segundos. “Recuperar” significa coisas diferentes dependendo de cada tipo de oráculo:

◦ Para oráculos baseados em pull, dos quais podemos obter um resultado imediatamente, nosso contrato precisa pagar uma taxa e buscar diretamente o preço

◦ Para oráculos baseados em push, nosso contrato paga a taxa, chama o oráculo e precisa esperar um período de tempo específico n antes de chamar o oráculo novamente para obter o preço solicitado

• Cada resultado do oráculo é salvo em um array. Depois que cada oráculo da lista de permissões é chamado e se a matriz tiver pontos de dados válidos suficientes para formar uma maioria (por exemplo, o contrato recebeu dados válidos de 3/5 oráculos), os resultados são classificados e o contrato escolhe a mediana

• Quer o contrato encontre a maioria ou não, a matriz com os resultados do oráculo é limpa e o contrato precisará aguardar p segundos antes de iniciar todo o processo novamente

Backup de Rede Oracle

A governança pode adicionar uma opção oracle de backup que começa a empurrar os preços no sistema se o medianizador não conseguir encontrar a maioria das redes oracle válidas várias vezes seguidas.

A opção de backup deve ser definida quando o medianizador é implantado, pois não pode ser alterado posteriormente. Além disso, um contrato separado pode monitorar se o backup está substituindo o mecanismo de medianização por muito tempo e desligar automaticamente o protocolo.

Cofres

Para gerar índices, qualquer pessoa pode depositar e alavancar suas garantias criptográficas dentro de Cofres. Enquanto um SAFE estiver aberto, ele continuará acumulando dívidas de acordo com a taxa de empréstimo da garantia depositada. À medida que o criador do SAFE paga sua dívida, ele poderá retirar cada vez mais de suas garantias bloqueadas.

Ciclo de Vida de um SAFE (Cofre)

Existem quatro etapas principais necessárias para criar índices reflexos e, posteriormente, pagar a dívida de um SAFE:

- Depositar garantias no SAFE

O usuário primeiro precisa criar um novo SAFE e depositar garantias nele.

- Gerar índices lastreados em garantias do SAFE

O usuário especifica quantos índices deseja gerar. O sistema cria um montante igual de dívida que começa a acumular de acordo com a taxa de empréstimo da garantia.

- Pague a dívida SAFE

Quando o criador do SAFE deseja retirar sua garantia, ele deve pagar sua dívida inicial mais os juros acumulados.

- Retirar garantia

Depois que o usuário paga parte ou toda a sua dívida, ele pode retirar sua garantia.

Liquidação do SAFE

Para manter o sistema solvente e cobrir o valor de toda a dívida em aberto, cada SAFE pode ser liquidado caso seu índice de garantia caia abaixo de um determinado limite. Qualquer pessoa pode desencadear uma liquidação, caso em que o sistema confiscará a garantia do SAFE e a venderá em um leilão de garantia.

Seguro de Liquidação

Em uma versão do sistema, os criadores do SAFE podem ter a opção de escolher um gatilho para quando seus SAFEs forem liquidados. Os gatilhos são contratos inteligentes que adicionam automaticamente mais garantias em um SAFE e potencialmente o salvam da liquidação. Exemplos de gatilhos são contratos que vendem posições vendidas ou contratos que se comunicam com protocolos de seguro como o Nexus Mutual [6].

Outro método para proteger os SAFEs é a adição de dois diferentes limites de colateralização: seguro e risco. Os usuários do SAFE podem gerar dívida até atingirem o limite seguro (que é maior que o risco) e só são liquidados quando a garantia do SAFE ficar abaixo do limite de risco.

Leilões de garantia

Para iniciar um leilão de garantias, o sistema precisa utilizar uma variável chamada LiquidationQuantity para determinar o valor da dívida a ser coberta por cada leilão e o valor correspondente da garantia a ser vendida. Uma penalidade de liquidação será aplicada a cada SAFE leiloado.

Parâmetros do Leilão de Garantias

Parameter Name	Description
minimumBid	Quantidade mínima de moedas que precisam ser oferecidas em um lance
discount	Desconto pelo qual a garantia está sendo vendida
lowerCollateralMedianDeviation	Desvio máximo do limite inferior que a mediana colateral pode ter em comparação com o preço do oráculo

upperCollateralMedianDeviation	Desvio máximo do limite superior que a mediana colateral pode ter em comparação com o preço do oráculo
lowerSystemCoinMedianDeviation	Desvio máximo do limite inferior que o feed de preço do oráculo de moedas do sistema pode ter em comparação com o preço do oráculo de moedas do sistema
upperSystemCoinMedianDeviation	Desvio máximo do limite superior que a mediana da garantia pode ter em comparação com o preço do oráculo da moeda do sistema
minSystemCoinMedianDeviation	Desvio mínimo para o resultado da mediana da moeda do sistema em relação ao preço de resgate para levar em consideração a mediana

Mecanismo de Leilão de Garantias

O leilão de desconto fixo é uma maneira direta (em comparação com os leilões ingleses) de colocar garantias à venda em troca de moedas do sistema usadas para liquidar dívidas incobráveis. Os licitantes só são obrigados a 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 desconto em comparação com o último preço de mercado registrado.

Os licitantes também podem revisar a quantidade de garantias que podem obter de um leilão específico chamando getCollateralBought ou getApproximateCollateralBought. Observe que getCollateralBought não é marcado como exibição porque lê (e também atualiza) o resgatePrice do retransmissor oracle, enquanto getApproximateCollateralBought usa o lastReadRedemptionPrice.

Leilões de dívida

No cenário em que um leilão de garantias não pode cobrir todas as dívidas incobráveis em um SAFE e se o sistema não tiver reservas excedentes, qualquer pessoa pode acionar um leilão de dívidas.

Os leilões de dívida destinam-se a cunhar mais tokens de protocolo (Seção 10) e vendê-los por índices que podem anular a dívida incobrável restante do sistema.

Para iniciar um leilão de dívida, o sistema precisa utilizar dois parâmetros:

- initialDebtAuctionAmount: a quantidade inicial de tokens de protocolo para cunhar após o leilão

- dívidaAuctionBidSize: o tamanho do lance inicial (quantos índices devem ser oferecidos em troca de tokens de protocolo initialDebtAuctionAmount)

Configuração de Parâmetros do 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 com oráculos (Seção 6) a partir dos quais o sistema leria o token de

protocolo e os preços de mercado do índice reflexo. O sistema então definiria a quantidade inicial de tokens de protocolo (initialDebtAuctionAmount) que serão cunhados para índices de dívidaAuctionBidSize. initialDebtAuctionAmount pode ser definido com um desconto em comparação com o preço de mercado real do PROTOCOLO/ÍNDICE para incentivar a licitação.

Parâmetros do Leilão de Dívidas

Parameter Name	Description
amountSoldIncrease	Aumento na quantidade de tokens de protocolo a serem cunhados para a mesma quantidade de índices
bidDecrease	Diminuição mínima do próximo lance na quantidade aceita de tokens de protocolo para a mesma quantidade de índices
bidDuration	Quanto tempo dura o lance após o envio de um novo lance (em segundos)
totalAuctionLength	Duração total do leilão (em segundos)
auctionsStarted	Quantos leilões começaram até agora

Mecanismo de Leilão de Dívidas

Ao contrário dos leilões de garantias, os leilões de dívida têm apenas uma etapa:

diminuiSoldAmount(uint id, uint amountToBuy, uint bid): diminui a quantidade de tokens de protocolo aceitos em troca de uma quantidade fixa de índices.

O leilão será reiniciado se não houver lances colocados. Toda vez que for reiniciado, o sistema oferecerá mais tokens de protocolo para a mesma quantidade de índices. O novo valor do token de protocolo é calculado como lastTokenAmount * amountSoldIncrease /
100. Após a conclusão do leilão, o sistema cunhará fichas para o maior lance.

Tokens de protocolo

Conforme descrito nas seções anteriores, cada protocolo precisará ser protegido por um token que é cunhado por meio de leilões de dívida. Além da proteção, o token será usado para controlar alguns componentes do sistema. Além disso, o fornecimento de tokens de protocolo será reduzido gradualmente com o uso de leilões excedentes. O valor do excedente que precisa acumular no sistema antes que os fundos extras sejam leiloados é chamado de buffer de excedente e é ajustado automaticamente como uma porcentagem do total da dívida emitida.

Fundo de Seguro

Além do token de protocolo, a governança pode criar um fundo de seguro que detém uma ampla gama de ativos não correlacionados e que pode ser usado como backstop para leilões de dívida.

Leilões de Excedentes

Os leilões excedentes vendem taxas de estabilidade acumuladas no sistema para tokens de protocolo que são então queimados.

Parâmetros do Leilão Excedente

Parameter Name	Description
bidIncrease	Aumento mínimo no próximo lance
bidDuration	Quanto tempo dura o leilão após o envio de um novo lance (em segundos)
totalAuctionLength	Duração total do leilão (em segundos)
auctionsStarted	Quantos leilões começaram até agora

Mecanismo de Leilão de Excedentes

Os leilões de excedentes têm uma única etapa:

aumentoBidSize(uint id, uint amountToBuy, uint bid): qualquer pessoa pode oferecer uma quantidade maior de tokens de protocolo para a mesma quantidade de índices (excedente). Cada novo lance precisa ser maior ou igual a lastBid * bidIncrease / 100. O leilão terminará após o máximo de totalAuctionLength segundos ou após bidDuration segundos desde o último lance e nenhum novo lance foi enviado nesse meio tempo.

Um leilão será reiniciado se não houver lances. Por outro lado, se o leilão tiver pelo menos um lance, o sistema oferecerá o excedente ao licitante mais alto e, em seguida, queimará todos os tokens de protocolo coletados.

Gestão de Índices Excedentes

Toda vez que um usuário gera índices e cria dívidas implicitamente, o sistema começa a aplicar uma taxa de empréstimo ao SAFE do usuário. Os juros acumulados são agrupados em dois contratos inteligentes diferentes:

- O mecanismo de contabilidade usado para acionar leilões de dívida (Seção 9.2) e excedente (Seção 10.1)
- O tesouro excedente usado para financiar os principais componentes de infraestrutura e incentivar atores externos a manter o sistema

O tesouro excedente é responsável por financiar três componentes principais do sistema:

- Módulo Oracle (Seção 6). Dependendo de como um oráculo é estruturado, a tesouraria paga oráculos fora da cadeia de governança na lista de permissões ou paga por chamadas para redes oraculares. A tesouraria também pode ser configurada para pagar os endereços que gastaram gasolina para chamar um oráculo e atualizá-lo

- Em alguns casos, equipes independentes que mantêm o sistema. Exemplos são equipes que colocam na lista de permissões novos tipos de garantias ou ajustam o definidor de taxas do sistema (Seção 4.2)

A tesouraria pode ser configurada de modo que alguns beneficiários excedentes sejam automaticamente negados no futuro e outros possam substituí-los.

Atores Externos

O sistema depende de atores externos para funcionar adequadamente. Esses atores são incentivados economicamente a participar de áreas como leilões, processamento de liquidação global, criação de mercado e atualização de feeds de preços para manter a integridade do sistema.

Forneceremos interfaces de usuário iniciais e scripts automatizados para permitir que o maior número possível de pessoas mantenha o protocolo seguro.

Mercado endereçável

Vemos o RAI como útil em duas áreas principais:

• Diversificação de portfólio: os investidores usam o RAI para obter exposição atenuada a um ativo como o ETH sem todo o risco de realmente manter o Ether

• Colateral para ativos sintéticos: RAI pode oferecer protocolos como UMA, MakerDAO e Synthetix uma exposição menor ao mercado de criptomoedas e dar aos usuários mais tempo para sair de suas posições no caso de cenários como Black Thursday a partir de março de 2020, quando milhões de dólares valem dos ativos criptográficos foram liquidados

Pesquisa futura

Para ampliar os limites do dinheiro descentralizado e trazer mais inovação nas finanças descentralizadas, continuaremos a procurar alternativas em áreas centrais, como minimização de governança e mecanismos de liquidação.

Primeiro, queremos estabelecer as bases para futuros padrões em torno de protocolos que se isolam do controle externo e para verdadeiros “robôs de dinheiro” que se adaptam em resposta às forças do mercado. Em seguida, convidamos a comunidade Ethereum para debater e projetar melhorias em torno de nossas propostas com foco específico em leilões de garantias e dívidas.

Riscos e Mitigação

Existem vários riscos envolvidos no desenvolvimento e lançamento de um índice reflexivo, bem como sistemas subsequentes que são construídos em cima:

• Bugs de contratos inteligentes: o maior risco para o sistema é a possibilidade de um bug que permita a qualquer pessoa extrair todas as garantias ou bloquear o protocolo em um estado do qual não pode se recuperar. Planejamos ter nosso código revisado por vários pesquisadores de segurança e lançar o sistema em uma rede de teste antes de nos comprometermos a implantá-lo em produção

• Falha do Oracle: agregaremos feeds de várias redes oracle e haverá regras rígidas para atualizar apenas um oracle por vez, para que a governança maliciosa não possa introduzir facilmente preços falsos

• Eventos colateral cisne negro: existe o risco de um evento cisne negro no colateral subjacente que pode resultar em uma quantidade elevada de SAFEs liquidados. As liquidações podem não ser capazes de cobrir toda a dívida incobrável e, portanto, o sistema mudará continuamente seu buffer excedente para cobrir uma quantidade decente de dívida emitida e resistir a choques de mercado

• Parâmetros de definição de taxa inadequados: mecanismos de feedback autônomos são altamente experimentais e podem não se comportar exatamente como prevemos durante as simulações. Planejamos permitir que a governança ajuste esse componente (enquanto ainda está limitado) para evitar cenários inesperados

• Falha em iniciar um mercado de liquidantes saudável: os liquidatários são atores vitais que garantem que todas as dívidas emitidas sejam cobertas por garantias. Planejamos criar interfaces e

scripts automatizados para que o maior número possível de pessoas possa participar da manutenção do sistema seguro.

Resumo

Propusemos um protocolo que progressivamente se isola do controle humano e emite um ativo colateralizado de baixa volatilidade chamado índice reflexo. Apresentamos primeiro o mecanismo autônomo destinado a influenciar o preço de mercado do índice e, em seguida, descrevemos como vários contratos inteligentes podem limitar o poder que os detentores de tokens têm sobre o sistema. Delineamos um esquema autossustentável para mediar feeds de preços de várias redes oraculares independentes e, em seguida, terminamos apresentando o mecanismo geral para cunhar índices e liquidar SAFEs.

Referências

[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 andEngineers", 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 Ethereumblockchain", https://bit.ly/3du8TMy

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

Glossário

Índice reflexo: um ativo garantido que amortece a volatilidade de seu subjacente

RAI: nosso primeiro índice reflexo

Preço de resgate: o preço que o sistema deseja que o índice tenha. Varia, influenciada por uma taxa de resgate (computada pelo RRFM), caso o preço de mercado não esteja próximo a ela. Destinado a influenciar os criadores do SAFE a gerar mais ou pagar parte de suas dívidas

Taxa de Empréstimo: taxa de juros anual aplicada a todos os SAFEs que possuem dívidas pendentes

Mecanismo de feedback da taxa de resgate (RRFM): um mecanismo autônomo que compara os preços de mercado e de resgate de um índice reflexo e, em seguida, calcula uma taxa de resgate que influencia lentamente os criadores do SAFE para gerar mais ou menos dívida (e implicitamente tenta minimizar o preço de mercado/resgate desvio)

Money Market Setter (MMS): um mecanismo semelhante ao RRFM que puxa várias alavancas monetárias de uma só vez. No caso de índices reflexos, modifica tanto a taxa de captação quanto o preço de resgate

Oracle Network Medianizer (ONM): um contrato inteligente que extrai preços de várias redes oracle (que não são controladas pela governança) e os medianiza se a maioria (por exemplo, 3 de 5) retornar um resultado sem jogar

Módulo de Governança Restrita (RGM): um conjunto de contratos inteligentes que limitam o poder que os detentores de tokens de governança têm sobre o sistema. Ele impõe atrasos de tempo ou limita as possibilidades que a governança tem de definir certos parâmetros

Governança Ice Age: contrato imutável que bloqueia a maioria dos componentes de um protocolo de intervenção externa após um determinado prazo ter passado

Motor de Contabilidade: componente do sistema que aciona os leilões de dívidas e excedentes. Ele também acompanha o valor da dívida atualmente leiloada, dívidas incobráveis não acionadas e o buffer excedente

Tampão de Excedente: montante de juros a acumular e manter no sistema. Algum interesse acumulados acima desse limite são vendidos em leilões excedentes que queimam tokens de protocolo

Tesouraria Excedente: contrato que dá permissão a diferentes módulos do sistema para retirar juros acumulados (por exemplo, ONM para chamadas de oráculo)