Rai: uma baixa volatilidade, confiança minimizada

Garantia 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 de mercado para modificar o valor alvo de seu ativo colateralizado nativo. O protocolo permite que qualquer um aproveite seus ativos criptográficos e emita um "índice reflexo", que é uma versão amortecida de sua garantia subjacente. Descrevemos como os índices podem ser úteis como garantia universal de baixa volatilidade que podem proteger seus detentores, bem como outros protocolos financeiros descentralizados, de mudanças repentinas de mercado. Apresentamos nossos planos para ajudar outras equipes a lançar seus próprios sintéticos, aproveitando nossa infraestrutura. Finalmente, oferecemos alternativas para o oráculo atual e estruturas de governança que são freqüentemente 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 o suprimento 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 mercadoria de reserva 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 um meio de troca para transações diárias, tudo reforçado pelos mesmos princípios de consenso descentralizado.

O acesso sem permissão ao Bitcoin para armazenar riqueza e instrumentos sintéticos adequadamente descentralizados no Ethereum estabelecerá as bases para a revolução financeira que se aproxima, fornecendo àqueles que estão à margem do sistema financeiro moderno os meios para se coordenar em torno da 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 atenuar a volatilidade de suas garantias. Os índices permitem que qualquer pessoa ganhe exposição ao mercado de criptomoedas sem a mesma escala de risco que manter os ativos criptográficos reais. Acreditamos que RAI, nosso primeiro índice de reflexo, terá utilidade imediata para outras equipes que emitem sintéticos no Ethereum (por exemplo, MakerDAO Multi-Collateral DAI [1], UMA [2], Synthetix [3]) porque dá a seus sistemas uma menor exposição a ativos voláteis, como ETH, e oferece aos usuários mais tempo para sair de suas posições no caso de uma mudança significativa no mercado.

Para entender os índices reflexos, podemos comparar o comportamento de seu preço de resgate ao do preço de uma moeda estável.

O preço de resgate é o valor de uma unidade de dívida (ou moeda) no sistema. Destina-se a 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 apoiado por fiat stablecoins como o 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. Existem também casos de stablecoins com base em criptografia, como o Multi Collateral DAI (MCD) da MakerDAO, em que o sistema tem como

meta uma atrelagem fixa 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 moeda estável e seu preço de resgate. Esses cenários criam oportunidades de arbitragem em que os comerciantes criarão mais moedas se o preço de mercado for superior ao de resgate e eles resgatarão suas moedas estáveis como garantia (por exemplo, dólares americanos no caso de USDC) caso o preço de mercado seja inferior ao preço de resgate.

Os índices reflexos são semelhantes aos 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 enquanto é 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 Go-To-Market

Nossa filosofia de design é priorizar a segurança, estabilidade e velocidade de entrega.

Multi-Collateral DAI foi o lugar natural para começar a iterar no design da RAI. O sistema foi fortemente auditado e formalmente verificado, 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 taxa autônomo, um Oracle Network Medianizer que é integrado com 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 central. Assim que provarmos que o setter funciona conforme o esperado, podemos adicionar com mais segurança o medianizador oracle (estágio 2) e a camada de minimização de governança (estágio 3).

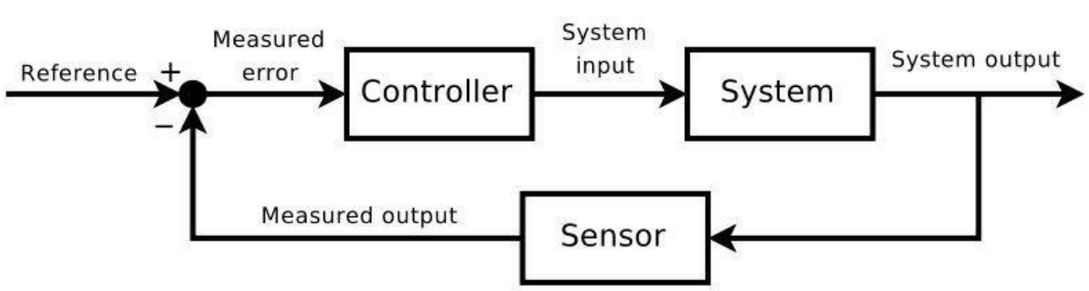
Mecanismos de Política Monetária

Introdução à Teoria de Controle

Um sistema de controle comum com o qual a maioria das pessoas está familiarizada é o chuveiro. Quando alguém liga o banho, tem em mente a temperatura desejada da água que, na teoria de controle, é chamada de*ponto de referência*. A pessoa, agindo como o *controlador*, mede continuamente a temperatura do fluxo de água (que é chamada de sistema *saída*) uma nd modifica a velocidade com que eles giram o botão do chuveiro com base no *desvio*(ou*erro*) entre a temperatura desejada e a atual. A velocidade com que o botão é girado é chamada de sistema*entrada.* T O objetivo é girar o botão rápido o suficiente para atingir o ponto de ajuste de referência rapidamente, mas não tão rápido que a temperatura *ultrapassagens*. Se houver sistema*choques* quando a temperatura do fluxo de água muda repentinamente, a pessoa deve ser capaz de manter a temperatura atual sabendo com que rapidez girar o botão em resposta ao distúrbio.

A disciplina científica de manutenção da estabilidade em sistemas dinâmicos é chamada de teoria do controle e encontrou ampla aplicação no 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*algorítmico controlador* é tipicamente incorporado no processo e recebe controle sobre uma entrada do sistema (por exemplo, o pedal do acelerador de um carro), a fim de atualizá-lo automaticamente com base nos desvios entre a saída do sistema (por exemplo, a velocidade de um carro) e o ponto de ajuste (por exemplo, a velocidade do controle de cruzeiro)



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:

C*ontroller Output = Proportional Term + Integral Term + Derivative Term*

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

O Termo Integral é a parte do controlador que leva em consideração por quanto tempo um desvio persistiu. É determinado tomando o*integrante* do desvio ao longo do tempo e é usado principalmente para eliminar*erro de estado estacionário*. Ele se acumula para responder a pequenos desvios, 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 consideração a rapidez com que o desvio está crescendo ou diminuindo. É determinado tomando o*derivado* do desvio e serve para acelerar a resposta do controlador quando o desvio está crescendo (por exemplo, acelere se o ponto de ajuste do controle de cruzeiro for maior do 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, acelere quando a velocidade do carro começa a se aproximar do ponto de ajuste do controle de cruzeiro).

A combinação dessas três partes, cada uma das quais pode ser ajustada independentemente, dá aos controladores PID grande flexibilidade no gerenciamento de uma ampla variedade de aplicações de sistema 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 ponto de ajuste conforme o sistema tenta se estabilizar. Os sistemas de índice reflex, como o RAI, são adequados para esse tipo de cenário, em que seus preços de resgate podem ser alterados por controladores PID.

De forma mais geral, foi descoberto recentemente que muitas das regras atuais 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 ele 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

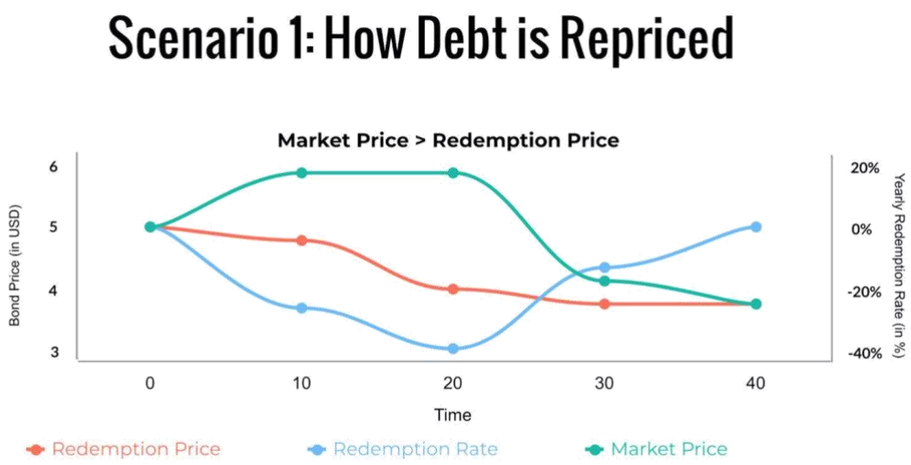
Em teoria, seria possível manipular diretamente o preço de resgate do índice de reflexo (descrito na Seção 2) para influenciar os usuários do índice e, em última instância, alterar o preço de mercado do índice. Na prática, esse método não teria o efeito desejado nos participantes do sistema. Do ponto de vista de um detentor de SAFE, se o preço de resgate for aumentado apenas uma vez, ele pode aceitar um preço mais alto por unidade de dívida, absorver a perda de um índice de garantia reduzido e manter sua posição. Se, no entanto, eles esperam que o preço de resgate continue a aumentar ao longo do tempo, eles provavelmente estarão mais inclinados a evitar perdas futuras esperadas e, assim, escolher pagar suas dívidas e encerrar suas posições.

Esperamos que os participantes do sistema de índice reflexo não respondam diretamente às mudanças no preço de resgate, mas sim ao*taxa de variação 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 ser totalmente automatizada.

Cenários de 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 combater as mudanças nas forças de mercado. Para tanto, a taxa de resgate é calculada de forma a se opor ao desvio entre os preços de mercado e de resgate.

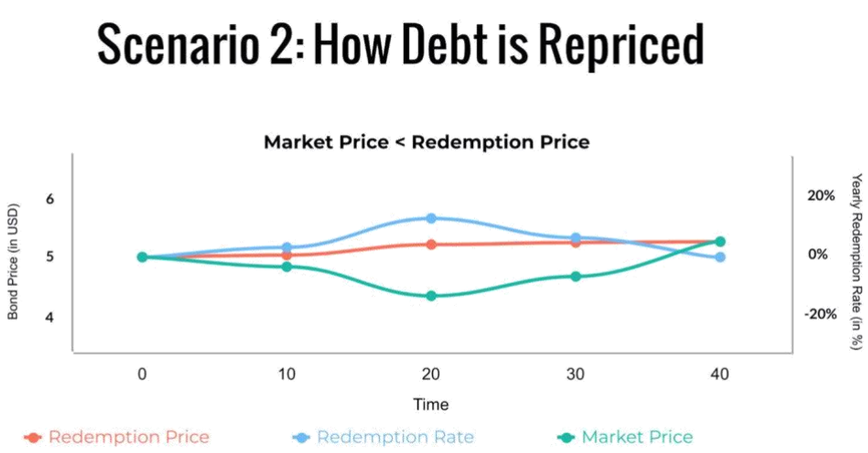
No primeiro cenário abaixo, se o preço de mercado do índice for superior ao seu preço de resgate, o mecanismo calculará uma taxa negativa que passará a diminuir o preço de resgate, tornando a dívida do sistema mais barata.



A expectativa de um preço de resgate decrescente provavelmente desencorajará as pessoas de manter índices e encorajará os detentores do SAFE a gerar mais dívida (mesmo que o preço da garantia não mude) que é então vendida no mercado, equilibrando assim a oferta e a demanda. Observe que este é o cenário ideal onde os detentores do índice reagem rapidamente em resposta ao mecanismo de feedback. Na prática (e especialmente nos primeiros dias após o lançamento), esperamos uma defasagem entre o kickoff 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 torna-se positiva e passa a repactuar toda a dívida para que fique mais cara.

A medida que a dívida se torna mais cara, os índices de garantia de todos os SAFEs diminuem (assim, os criadores do SAFE são incentivados a pagar suas dívidas) e os usuários começam a acumular índices com a expectativa de que aumentem de valor.



Algoritmo de Mecanismo de Feedback

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

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

- Em algum ponto, 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 reprice os índices para que fiquem mais baratos

- Após o cálculo do proporcional, o mecanismo determinará o termo integral *i* adicionando todos os desvios anteriores dos últimos segundos de *deviationInterval*

- 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 percebem que podem gerar mais dívidas, eles inundarão o mercado com mais índices.

- Depois *n* segundos, o mecanismo detecta que o desvio entre o mercado e os preços de resgate é insignificante (sob um parâmetro especificado *noise*) Neste ponto, o algoritmo define r como zero e mantém o preço de resgate onde está.

Na prática, o algoritmo será mais robusto e faremos algumas variáveis imutáveis (por exemplo, o *noise* parâmetro ,*deviationInterval*) ou haverá limites rígidos sobre o que a governança pode mudar.

Ajuste do Mecanismo de Feedback

De extrema importância para o funcionamento adequado do sistema de índice de reflexo é o ajuste dos parâmetros do controlador algorítmico. A parametrização inadequada pode resultar em um sistema muito lento para atingir a estabilidade, excessivamente ultrapassado ou geralmente instável em face de choques externos.

O processo de ajuste para um controlador PID normalmente envolve executar o sistema ao vivo, ajustar os parâmetros de ajuste e observar 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 alavancar a modelagem de computador e simulação tanto quanto possível para definir os parâmetros iniciais, mas também permitirá que a governança atualize os parâmetros de ajuste se dados adicionais de produção mostra que estão abaixo do ideal.

Configurador do Mercado Monetário

No RAI, planejamos manter a taxa de empréstimo (taxa de juros aplicada na geração dos 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 em nosso caso é igual ao spread entre a taxa de estabilidade e o DSR em Multi-Collateral DAI.

Embora planejemos manter a taxa de empréstimo fixa, é possível alterá-la juntamente com o preço de resgate usando um definidor do mercado monetário. O mercado monetário altera a taxa de empréstimo e o preço de resgate de uma forma que incentiva os criadores do SEGURO 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 usado para garantir o preço de resgate a todos os detentores do índice reflexo. Destina-se a permitir que tanto os detentores do índice reflexo como os criadores do 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 um pode acionar a liquidação após gravar uma certa quantidade de tokens de protocolo.

A liquidação tem três fases principais:

- Acionar: A liquidação é acionada, os usuários não podem mais criar SAFEs, todos os feeds de preço de garantia e o preço de resgate são congelados e registrados

- Processo: Processar todos os leilões pendentes

- Alegar: Cada detentor do índice reflexo e criador do 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 inteiramente novo. Escolhemos essa estratégia porque podemos eliminar o meta-jogo em que as pessoas tentam influenciar o processo de governança em seu próprio benefício, prejudicando 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 queiram usar 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 destinado a atrasar 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 o término de certos prazos.

Governança Com Limite de Tempo

A governança limitada pelo tempo é o primeiro componente do Módulo de governança restrita. Ele 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* s econds se passaram desde a última modificação do oráculo.

Governança de Ação Limitada

O segundo componente no Módulo de Governança Restrita é a Governança de Ações Limitadas. Cada parâmetro governável tem limites para quais valores ele pode ser definido e quanto ele pode mudar em 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.

Idade do Gelo de Governança

A Idade do Gelo é um contrato inteligente imutável que impõe prazos para a alteração de parâmetros específicos do sistema e para a atualização do protocolo. Ele pode ser usado no caso em que a governança deseja ter certeza de que pode corrigir os bugs antes que o protocolo se bloqueie e negue a intervenção externa. A Idade do Gelo verificará se uma alteração é permitida comparando o nome do parâmetro e o endereço do contrato afetado em um registro de prazos. Se o prazo tiver expirado, a chamada será revertida.

A governança pode atrasar a Idade do Gelo um número fixo de vezes se os bugs forem encontrados perto da data em que o protocolo deve começar a se bloquear. Por exemplo, a Era do Gelo só pode ser adiada três vezes, cada vez por um mês, para que as correções de bug recém-implementadas sejam testadas corretamente.

Áreas Principais Onde a Governança é Necessária

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

- Adicionando novos tipos de garantia: RAI será lastreado apenas pela ETH, mas outros índices serão lastreados por vários tipos de garantias e a governança será capaz para diversificar o risco ao longo do tempo

- Alterar dependências externas: Oráculos e DEXs dos quais o sistema depende podem ser atualizados. A governança pode apontar o sistema

para dependências mais recentes para que continue funcionando corretamente

- Ajustadores de taxa de ajuste fino: Os primeiros controladores de política monetária terão parâmetros que podem ser alterados dentro de limites razoáveis (conforme descrito por Action and Time Bounded Governance)

- Migrando entre versões do sistema: em alguns casos, a governança pode implantar um novo sistema, dar-lhe 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

O seguinte é um mecanismo simples para migrar entre as versões do sistema:

- Há um registro de migração que rastreia quantos sistemas diferentes o mesmo token de protocolo cobre e quais sistemas podem ter negada a permissão para imprimir tokens de protocolo em um leilão de dívida

- Cada vez que a governança implanta uma nova versão do sistema, ela envia o endereço do contrato de leilão da dívida do sistema no registro de migração. A governança também precisa especificar se algum dia será capaz de impedir o sistema de imprimir tokens de protocolo. Além disso, a governança pode, a qualquer momento, dizer que um sistema sempre será capaz de imprimir tokens e, portanto, nunca será migrado de;

- Há um período de espera entre a proposta de um novo sistema e a retirada de permissões de um antigo

- Um contrato opcional pode ser configurado de forma que ele desligue automaticamente um sistema antigo após ter negado as permissões de impressão

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

Desligamento Automático do Sistema

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

- Atrasos severos no feed de preços: O sistema detecta que uma ou mais das garantias ou feeds de preços de índice não foram atualizados há muito tempo

- Migração de sistema: Este é um contrato opcional que pode encerrar o protocolo após um período de resfriamento 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 consistente do preço de mercado: O sistema detecta que o preço de mercado do índice foi *x%* desviou por um longo tempo em comparação com o preço de resgate

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

Oráculos

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

Oráculos liderados pela 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, enviar 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 oracle, embora acarrete a falta de confiança.

Oracle Network Medianizer

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

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

- Para empurrar um novo feed de preço no sistema, todos os oráculos precisam ser chamados de antemão. 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 defeituoso específico não pode ser chamado novamente até que todos os outros sejam chamados e o contrato verifique se há maioria válida. Uma chamada de oracle válida não deve ser revertida e deve recuperar um preço que foi postado na rede em algum momento no último*m* segundos. “Recuperar” significa coisas diferentes dependendo de cada tipo de oráculo:

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

    - Para oráculos baseados em push, nosso contrato paga a taxa, liga para o oráculo e precisa esperar um período específico de tempo*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 na lista de permissões é chamado e se a matriz tem 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 oracle liberada e o contrato terá que esperar*p* segundos antes de iniciar todo o processo novamente.

Oracle Network Backup

A governança pode adicionar uma opção de oráculo 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 o protocolo automaticamente.

Cofres

A fim de gerar índices, qualquer pessoa pode depositar e alavancar sua garantia criptográfica dentro de cofres. Enquanto um SAFE é 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 será capaz de retirar cada vez mais de sua garantia bloqueada.

Ciclo de Vida SAFE

Existem quatro etapas principais necessárias para criar índices de reflexo e, posteriormente, pagar uma dívida do SAFE:

- Depositar garantia no SAFE

- O usuário primeiro precisa criar um novo SEGURO e depositar a garantia nele.

- Gerar índices apoiados pela garantia 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 a totalidade de sua dívida, ele pode retirar sua garantia.

Liquidação SAFE

A fim de manter o solvente do sistema e cobrir o valor de toda a dívida em aberto, cada SAFE pode ser liquidada no caso de seu índice de garantia cair abaixo de um determinado limite. Qualquer um pode iniciar 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*acionar* para quando seus SAFEs forem liquidados. Os gatilhos são contratos inteligentes que adicionam automaticamente mais garantias em um SEGURO e, potencialmente, salvam-no da liquidação. Exemplos de gatilhos são contratos que vendem posições curtas ou contratos que se comunicam com protocolos de seguro como o Nexus Mutual [6].

Outro método para proteger SAFEs é a adição de dois limites de colateralização diferentes:*seguro* e*risco*. 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 colateralização do SAFE ficar abaixo do limite de risco.

Leilões Colaterais

Para iniciar um leilão de garantia, o sistema precisa usar uma variável chamada *liquidationQuantity* a fim de determinar o montante da dívida a ser coberto em cada leilão e o montante correspondente de garantias a serem vendidas. A*pena de liquidação* será aplicado a todos os SEGUROS leiloados.

Parâmetros de Leilão Colateral

Nome do parâmetro	Descrição
minimumBid	Quantidade mínima de moedas que precisam ser oferecido 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 moeda do sistema pode ter em comparação com o oráculo de moedas do sistema preço
upperSystemCoinMedianDeviation	Desvio máximo do limite superior que a mediana colateral pode ter em comparação com o preço do oráculo da moeda do sistema
minSystemCoinMedianDeviation	Desvio mínimo para a moeda do sistema resultado mediano em comparação com o preço de resgate, a fim de levar o mediana em consideração

Mecanismo de Leilão Colateral

O leilão de desconto fixo é uma maneira simples (em comparação com os leilões ingleses) de colocar garantias à venda em troca de moedas do sistema usadas para liquidar dívidas inadimplentes. Os licitantes são obrigados apenas a permitir que a casa de leilões transfira seus safeEngine.coinBalance e pode

então ligar buyCollateral a fim de trocar suass moedas do sistema para garantia vendidas com desconto em relação ao último preço de mercado registado.

Os licitantes também podem revisar o valor da garantia que podem obter de um leilão específico ligando para getCollateralBought ou getApproximateCollateralBought . Observe que getCollateralBought não é marcado como visualização porque lê (e também atualiza) o redemptionPrice do oracle relayer enquanto getApproximateCollateralBought usa o 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 dívida inadimplente remanescente do sistema.

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

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

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

Definição de Parâmetro de Leilão de Dívida Autônoma

A quantidade inicial de tokens de protocolo cunhados em um leilão de dívida pode ser definida por meio de um voto 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. O sistema então definiria a quantidade inicial de tokens de protocolo (*initialDebtAuctionAmount*) que será cunhado para*dívidaAuctionBidSize* índices. *initialDebtAuctionAmount*pode ser definido com um desconto em comparação com o preço de mercado real do PROTOCOLO / ÍNDICE para incentivar a licitação.

Parâmetros de Leilão de Dívida

Nome do parâmetro	Descrição
amountSoldIncrease	Aumento na quantidade de protocolo tokens a serem cunhados para o mesmo 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 um novo o lance é enviado (em segundos)
totalAuctionLength	Duração total do leilão (em segundos)
auctionsStarted	Quantos leilões começaram até agora

Mecanismo de Leilão de Dívida

Ao contrário dos leilões de garantia, os leilões de dívida têm apenas um estágio:

decreaseSoldAmount(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 caso não haja lances colocados. Cada vez que for reiniciado, o sistema oferecerá mais tokens de protocolo para a mesma quantidade de índices. A nova quantidade de token de protocolo é calculada como *lastTokenAmount * amountSoldIncrease /100.* Depois que o leilão for encerrado, o sistema cunhará tokens para o licitante com lance mais alto.

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 gradualmente

reduzido com o uso de leilões excedentes. A quantidade de excedente que precisa ser acumulada no sistema antes que os fundos extras sejam leiloados é chamada de *surplusBuffer* e é ajustado automaticamente como uma porcentagem da dívida total 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 barreira para leilões de dívida.

Leilões de Excedente

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

Parâmetros de Leilão Excedente

Nome do parâmetro	Descrição
bidIncrease	Aumento mínimo no próximo lance
bidDuration	Quanto tempo dura o leilão após um novo o lance é enviado (em segundos)
totalAuctionLength	Duração total do leilão (em segundos)
auctionsStarted	Quantos leilões começaram até agora

Mecanismo de Leilão Excedente

Os leilões de excedentes têm um único estágio:

increaseBidSize(uint id, uint amountToBuy, uint bid): qualquer um pode dar um lance maior de tokens de protocolo para a mesma quantidade de índices (excedente). Cada novo lance deve ser maior ou igual a *lastBid* **bidIncrease* / 100. O leilão terminará após no máximo *totalAuctionLength* segundos ou depois*bidDuration* segundos se passaram desde o último lance e nenhum novo lance foi submetido entretanto.

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 com maior lance e, em seguida, queimará todos os tokens de protocolo recolhidos.

Gestão de Índices Excedentes

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

O *Accounting Engine* usado para acionar dívida (Seção 9.2) e excedente (Seção 10.1) leilões

O *surplus treasury* usado para financiar os principais componentes da infraestrutura e incentivar os atores externos a manter o sistema.

A tesouraria excedente é responsável por financiar três componentes principais do sistema:

- Módulo Oracle (Seção 6). Dependendo de como um oráculo está estruturado, o tesouro paga oráculos de governança incluídos na lista de permissões, fora da rede, ou paga por chamadas para redes oráculos. A tesouraria também pode ser configurada para pagar os endereços que gastaram gás para chamar um oráculo e atualizá-lo

- Em alguns casos, equipes independentes que mantêm o sistema. Os exemplos são as 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 forma que alguns recebedores de excedentes tenham automaticamente negado financiamento no futuro e outros possam tomar seu lugar.

Atores Externos

O sistema depende de atores externos para funcionar corretamente. Esses atores são economicamente incentivados a participar de áreas como leilões, processamento de liquidação global, criação de mercado e atualização de preços para manter a saúde 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 reduzir a exposição a um ativo como a ETH, sem todo o risco de realmente deter o éter.

Garantia para ativos sintéticos: A RAI pode oferecer protocolos como UMA, MakerDAO e Synthetix uma exposição menor ao mercado de criptografia e dar aos usuários mais tempo para sair de suas posições no caso de cenários como a quinta-feira negra de março de 2020, quando milhões de dólares em ativos criptográficos eram liquidado.

Future Research

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

Em primeiro lugar, queremos estabelecer as bases para padrões futuros em torno de protocolos que se fecham ao controle externo e para verdadeiros "robôs de dinheiro" que se adaptam em resposta às forças do mercado. Posteriormente, convidamos a comunidade Ethereum para debater e projetar melhorias em torno de nossas propostas com um foco específico em leilões de garantias e dívidas.

Riscos e Mitigação

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

- Bugs de contrato inteligente: O maior risco para o sistema é a possibilidade de um bug que permite a qualquer pessoa extrair todas as garantias ou bloqueia 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 um testnet antes de nos comprometermos a implantá-lo em produção

- Falha Oracle: Vamos agregar feeds de várias redes oracle e haverá regras

- estritas em vigor para atualizar apenas um oracle por vez, de modo que a governança maliciosa não possa facilmente introduzir preços falsos

- Eventos colaterais cisne negro: Existe o risco de um evento cisne negro na garantia subjacente que pode resultar numa elevada quantidade de SAFEs liquidados. As liquidações podem não ser capazes de cobrir toda a inadimplência pendente e, portanto, o sistema mudará continuamente sua reserva excedente a fim de cobrir uma quantidade razoável de dívida emitida e resistir aos choques do mercado

- Parâmetros de definição de taxa inadequados: Os mecanismos de feedback autônomo são altamente experimentais e podem não se comportar exatamente como previmos durante as simulações. Planejamos permitir que a governança ajuste esse componente (embora ainda esteja sendo limitado) a fim de evitar cenários inesperados

- Falha em iniciar um mercado liquidante saudável: Os liquidatários são atores vitais que garantem que toda a dívida emitida seja coberta por garantias. Planejamos criar interfaces e scripts automatizados para que o maior número possível de pessoas possa participar da manutenção da segurança do sistema.

Resumo

Propusemos um protocolo que progressivamente se bloqueia do controle humano e emite um ativo colateralizado de baixa volatilidade denominado índice de 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 medianizar os feeds de preços de várias redes oráculos independentes e, em seguida, concluímos apresentando o mecanismo geral para cunhar índices e liquidar SAFEs.

Referências

“The Maker Protocol: MakerDAO's Multi Collateral Dai (MCD) System”, https://bit.ly/2YL5S6j

“UMA: Uma plataforma de contrato financeiro descentralizada”,https://bit.ly/2Wgx7E1

Synthetix Litepaper,https://bit.ly/2SNHxZO

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

RJ Hawkins, JK Speakes, DE Hamilton, “Monetary Policy and PID Control”, https://bit.ly/2TeQZFO

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

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

Glossário

Índice de Reflexo: Um ativo colateralizado que amortece a volatilidade de seu subjacente

RAI: Nosso primeiro índice de reflexo

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

Taxa de Empréstimo: Taxa de juros anual aplicada a todos os SAFEs que têm dívida pendente

Mecanismo de Feedback da Taxa de Resgate (RRFM): Um mecanismo autônomo que compara o mercado e os preços de resgate de um índice de 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 mercado / desvio do preço de resgate)

Configurador do Mercado Monetário (MMS): Um mecanismo semelhante ao RRFM que puxa várias alavancas monetárias de uma vez. No caso de índices reflexos, ele modifica tanto a taxa de empréstimo quanto o preço de resgate

Oracle Network Medianizer (ONM): Um contrato inteligente que puxa preços de várias redes oracle (que não são controladas pela governança) e os medianiza se uma maioria (por exemplo, 3 de 5) retornou um resultado sem lançar

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

Idade do Gelo de Governança: Contrato imutável que bloqueia a maioria dos componentes de um protocolo de intervenção externa após um determinado prazo ter passado

Mecanismo de Contabilidade: Componente do sistema que desencadeia leilões de dívida e excedentes. Ele também mantém o controle do valor da dívida leiloada atualmente, dívidas inadimplentes não operadas e o buffer de excedente

Buffer Excedente: Montante de juros a acumular e manter no sistema. Algum interesse acumulado acima desse limite é vendido em leilões excedentes que queimam tokens de protocolo

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