RAI: Um colateral de baixa volatilidade e confiança minimizada para o ecossistema DeFi

Stefan C. Ionescu, Ameen Soleimani

Maio de 2020

Resumo. Nós apresentaremos um protocolo de governança minimizada descentralizado que reage automaticamente as forças do mercado a fim de modificar o valor alvo do seu ativo colateralizado nativo. O protocolo permite que qualquer um alavanque seus criptoativos e emita um "índice de reflexo" que é uma versão suavizada de seus colaterais subjacentes. Nós descrevemos como os índices podem ser úteis como um colateral universal de baixa volatilidade que pode proteger seus proprietários, assim como outros protocolos de finanças descentralizadas de mudanças súbitas no mercado. Nós apresentamos nossos planos para ajudar outras equipes a lançar seus próprios ativos sintéticos alavancando nossa infraestrutura. E finalmente, nós apresentamos uma alternativa para os atuais oracles e estruturas de governança que são frequentemente encontradas em protocolos DeFi.

Conteúdo

1. Introdução
2. Visão geral dos índices de reflexo
3. Filosofia de projeto e estratégia de *Go-to-market*
4. Mecanismos de política monetária
    - 4.1. Introdução a teoria de controle
    - 4.2. Mecanismo de feedback da taxa de resgate
        - 4.2.1. Componentes
        - 4.2.2. Cenários
        - 4.2.3. Algoritmos
        - 4.2.4. Ajuste
    - 4.3. ajustador do mercado monetário
    - 4.4. Liquidação global
5. Governança
    - 5.1. Governança vinculada ao tempo
    - 5.2. Governança vinculada à ação
    - 5.3. Governança da era do gelo
    - 5.4. Áreas centrais onde a governança é necessária
        - 5.4.1. Módulo de migração restrita
6. Desligamento automático do sistema
7. Oracles
    - 7.1. Oracles liderados pela governança
    - 7.2. Moderador da rede Oracle
        - 7.2.1. Rede de Oracles reserva
8. Safes
    - 8.1. Ciclo de vida do SAFE
9. Liquidação de SAFE
    - 9.1. Leilão de colaterais
        - 9.1.1. Seguro de liquidação
        - 9.1.2. Parâmetros do leilão de colaterais
        - 9.1.3. Mecanismo do leilão de colaterais
    - 9.2. Leilão de dívida
        - 9.2.1. Ajuste de parâmetros de leilão de dívida automático
        - 9.2.2. Parâmetros do leilão de dívida
        - 9.2.3. Mecanismo de leilão de dívida
10. Tokens de protocolos
    - 10.1. Leilão de excedentes
        - 10.1.1. Parâmetros do leilão de excedentes
        - 10.1.2. Mecanismo do leilão de excedente
11. Gestão de índices de excedentes

12. Atores externos
13. Mercado endereçável
14. Pesquisas futuras
15. Riscos e mitigação
16. Sumário
17. Referências
18. Glossário

Introdução

O dinheiro é um dos mais poderosos mecanismos de coordenação que a humanidade utiliza para prosperar. O privilégio de administrar a oferta de dinheiro tem sido historicamente mantido nas mãos de lideranças soberanas e da elite financeira, ao mesmo tempo em que é imposto a um público em geral involuntário. O Bitcoin tem demonstrado o potencial como um protesto popular para manifestar uma reserva de valor, a rede Ethereum nos dá uma plataforma para construir instrumentos sintéticos apoiados em ativos que possam ser protegidos da volatilidade e usados como colateral, ou atrelados a um preço de referência e usados como meio de troca para transações diárias, todos reforçados pelos mesmos princípios de consenso descentralizado.

O acesso sem permissão ao Bitcoin para armazenamento de riqueza e instrumentos sintéticos devidamente descentralizados no Ethereum lançará as bases para a próxima revolução financeira, proporcionando àqueles que estão à margem do sistema financeiro moderno os meios que irão conduzir para a construção do novo sistema.

Neste documento, apresentaremos uma estrutura para a construção de índices de reflexo, um novo tipo de ativo que ajudará outros ativos sintéticos a florescer e estabelecerá um bloco de construção chave para toda a indústria financeira descentralizada.

Visão geral dos índices de reflexo

O objetivo de um índice de reflexo não é manter um lastro específico, mas reduzir a volatilidade de seus colaterais. Os índices permitem a qualquer pessoa ganhar exposição ao mercado de criptomoedas sem a mesma escala de risco que a posse de criptoativos reais. Acreditamos que RAI, nosso primeiro índice de reflexo, terá utilidade imediata para outras equipes que emitem ativos sintéticos na rede Ethereum (p. ex., Multi-Collateral DAI da MakerDAO [1], UMA [2], Synthetix [3]) porque dá a seus sistemas uma menor exposição a ativos voláteis como o ETH e oferece aos usuários mais tempo para sair de suas posições no caso de uma mudança significativa no mercado.

Para compreender os índices de reflexo, podemos comparar o comportamento de seu preço de resgate com o preço de uma *stablecoin*.

O preço de resgate é o valor de uma unidade de débito (ou moeda) no sistema. Ele deve ser usado apenas como uma ferramenta de contabilidade interna e é diferente do preço de mercado (o valor em que o mercado está negociando a moeda). No caso de moedas estáveis lastreadas em fiat como USDC, os operadores do sistema declaram que qualquer um pode resgatar uma moeda por um dólar americano e, portanto, o preço de resgate para estas moedas é sempre um só. Há também casos de stablecoins criptografadas, como o Multi-Collateral DAI (MCD) da MakerDAO, em que o sistema tem como alvo um lastro 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 moeda estável e seu preço de resgate. Estes cenários criam oportunidades de arbitragem onde os comerciantes criarão mais moedas se o preço de mercado for maior do que o de resgate e resgatarão suas *stablecoins* como colateral (p. ex., dólares americanos no caso de USDC) caso o preço de mercado seja menor do que o de resgate.

Os índices de reflexo são similares as *stablecoins* porque também têm um preço de resgate que o sistema alveja. A principal diferença em seu caso é que seu resgate não permanecerá fixo, mas é projetado para mudar enquanto é influenciado pelas forças do mercado. Na seção 4 explicamos como flutua o preço de resgate de um índice e criamos novas oportunidades de arbitragem para seus usuários.

Filosofia de projeto e Estratégia de *Go-to-market*

Nossa filosofia de projeto é priorizar a segurança, estabilidade e rapidez de entrega.

O Multi-Collateral DAI foi o lugar natural para começar a renovar o design da RAI. O sistema foi altamente auditado e formalmente verificado, têm dependências externas mínimas e reuniu uma comunidade ativa de especialistas. Para minimizar o esforço de desenvolvimento e comunicação, queremos fazer apenas as mudanças mais simples na base de códigos MCD original para chegar a nossa implementação.

Nossas modificações mais importantes incluem a adição de um ajustador de taxas autônomo, um moderador da rede Oracle que é integrada com muitas fontes 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 ajustador de taxas e outras pequenas melhorias na arquitetura principal. Uma vez que for comprovado que o ajustador funciona como esperado, podemos adicionar com mais segurança o Oracle mediador (Estágio 2) e a camada de minimização da governança (Estágio 3).

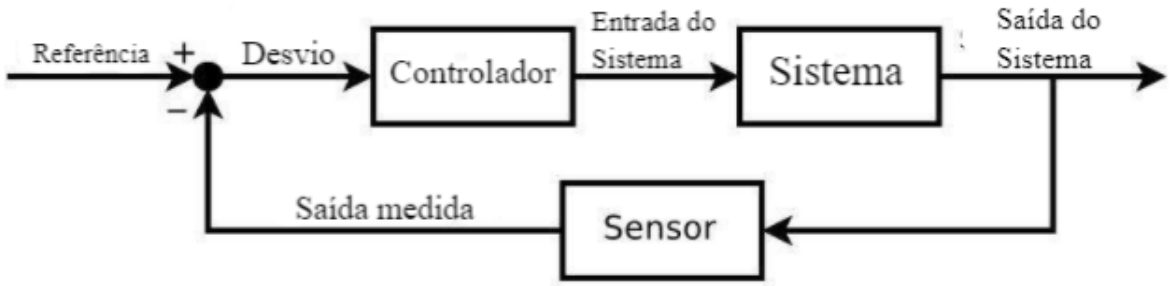
Mecanismos de política monetária

Introdução a teoria de controle

Um sistema de controle comum com o qual a maioria das pessoas está familiarizada é o chuveiro. Quando alguém liga um chuveiro, tem em mente uma temperatura de água desejada que, na teoria de 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 na qual gira o registro do chuveiro com base no desvio (ou erro) entre a temperatura desejada e a temperatura atual. A velocidade na qual o registro é girado é chamada de entrada do sistema. O objetivo é girar o registro suficientemente rápido para atingir o ponto de referência rapidamente, mas não tão rápido que a temperatura ultrapasse o ponto de referência. Se houver choques no sistema onde a temperatura do fluxo de água muda repentinamente, a pessoa deve ser capaz de manter a temperatura atual sabendo o quão rápido deve girar o registro em resposta ao distúrbio.

A disciplina científica de manter a estabilidade em sistemas dinâmicos é chamada teoria de controle e encontrou ampla aplicação no controle de cruzeiro para carros, navegação de vôo, reatores químicos, armas robóticas e processos industriais de todos os tipos. O algoritmo de ajuste de dificuldade do Bitcoin que mantém o tempo médio de mineração de cada bloco de dez minutos, apesar de um hashrate variável, é um exemplo de um sistema de controle de missão crítica.

Na maioria dos sistemas de controle modernos, um algoritmo controlador é normalmente embarcado no processo e é dado controle sobre uma entrada do sistema (p. ex., o acelerador de um carro) a fim de atualizá-lo automaticamente com base nos desvios entre a saída do sistema (p. ex., a velocidade de um carro) e o ponto de ajuste (p. ex., a velocidade de controle de cruzeiro).



O tipo mais comum de algoritmo de controle é o controlador PID. Mais de 95% das aplicações industriais e uma ampla gama de sistemas biológicos empregam elementos de controle PID [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 (p. ex., o ponto de ajuste da velocidade de cruzeiro é muito maior que a velocidade atual do carro), a resposta proporcional será grande e positiva (p. ex., pisar no acelerador).

O Termo Integral é a parte do controlador que leva em conta quanto tempo um desvio persistiu. Ele é determinado tomando a integral do desvio ao longo do tempo e é usado principalmente para eliminar o erro de estado estável. Ele se acumula a fim de responder a pequenos, embora persistentes, desvios do valor-alvo (p. ex., o valor-alvo do controle de cruzeiro foi 1 km/h 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. Ele é determinado tomando a derivada do desvio e serve para acelerar a resposta do controlador quando o desvio está crescendo (p. ex., acelerar se o valor-alvo do controle de cruzeiro for maior do que a velocidade do carro e o carro começar a desacelerar). Também ajuda a reduzir o excesso de velocidade ao desacelerar a resposta do controlador quando o desvio está diminuindo (p. ex., reduzir a gasolina quando a velocidade do carro começa a se aproximar do valor-alvo do controle de cruzeiro).

A combinação destas três partes, cada uma das quais pode ser ajustada independentemente, dá aos controladores PID grande flexibilidade no gerenciamento de uma grande 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 ultrapassar e oscilar em torno do valor-alvo, à medida que o sistema tenta se estabilizar. Sistemas de índice de reflexo como o RAI são bem adequados para este tipo de cenário onde seus preços de resgate podem ser alterados pelos controladores PID.

De modo mais geral, descobriu-se recentemente que muitas das regras atuais de política monetária do banco central (p. ex., a regra Taylor) são na verdade aproximações dos controladores PID [5].

Mecanismo de Feedback da Taxa de Resgate

O Mecanismo de Feedback da Taxa de Resgate é o componente do sistema encarregado de alterar o preço de resgate de um índice de reflexo. A fim de entender como isso funciona, precisamos primeiro descobrir 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) a fim de influenciar os usuários do índice e, em última instância, alterar o preço de mercado do índice. Na prática, este método não teria o efeito desejado sobre os participantes do sistema. Da perspectiva de um investidor SAFE, se o preço de resgate for aumentado apenas uma vez, eles poderiam aceitar um preço mais alto por unidade de dívida, absorver a perda de uma menor taxa de colateralização e manter sua posição. Se, entretanto, eles esperarem que o preço de resgate continue a aumentar ao longo do tempo, 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 índice de reflexo 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 fazer um ajuste fino 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, utilizando a taxa de resgate para contrabalançar as mudanças nas forças de mercado. Para conseguir isso, a taxa de resgate é calculada de forma a se opor ao desvio entre o preço de mercado e o preço de resgate.

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

A expectativa de um preço de resgate decrescente provavelmente desencorajará as pessoas de possuir índices e incentivará os investidores SAFE a gerar mais dívida

(mesmo que o preço do colateral não mude) que é então vendida no mercado, equilibrando assim a oferta e a demanda. Note que este é o cenário ideal onde os possuidores de índices reagem rapidamente em resposta ao mecanismo de Feedback. Na prática (e especialmente nos primeiros dias após o lançamento) esperamos uma defasagem entre o pontapé inicial do mecanismo e os resultados reais observados no montante da dívida emitida e, posteriormente, no preço de mercado.

Por outro lado, no segundo cenário, se o preço de mercado do índice for inferior ao preço de resgate, a taxa se torna positiva e começa a reprecificar toda a dívida para que ela se torne mais cara.

À medida que a dívida se torna mais cara, os índices de colaterais de todos os SAFEs diminuem (assim, os criadores de SAFE são incentivados a pagar sua dívida) e os usuários começam a acumular índices com a expectativa de que eles irão aumentar de valor.

Algoritmo do Mecanismo de Feedback

No cenário seguinte, assumimos que o protocolo utiliza 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 aumenta de '*rand*' para '*rand*' + x. Depois o mecanismo de Feedback lê o novo preço de mercado, calcula um termo proporcional p, que neste caso é -1 * (('*rand*' + x) / '*rand*'). O proporcional é negativo a fim de diminuir o preço de resgate e, por sua vez, reprecificar os índices para que se tornem mais baratos

- Após o cálculo da proporcionalidade, o mecanismo determinará o termo integral *i* adicionando todos os desvios passados dos últimos segundos do *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. Conforme os criadores de SAFE percebem que podem gerar mais dívidas, eles inundarão o mercado com mais índices

- Após *n* segundos, o mecanismo detecta que o desvio entre o mercado e os preços de resgate é insignificante (sob um ruído de parâmetro especificado). Neste ponto, o algoritmo estabelece *r* para zero e mantém o preço de resgate onde ele está

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

Ajuste do Mecanismo de Feedback

O mais importante para o bom funcionamento do sistema de índice de reflexo é o ajuste dos parâmetros do algoritmo controlador. A parametrização inadequada

poderia resultar em um sistema muito lento para alcançar a estabilidade, em um superfaturamento maciço, ou ser geralmente instável em face de choques externos.

O processo de ajuste para um controlador PID normalmente envolve a execução do sistema em atividade, ajustando os parâmetros 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 em atividade, planejamos aproveitar ao máximo a modelagem e simulação computadorizada para definir os parâmetros iniciais, mas também permitiremos que a governança atualize os parâmetros de ajuste se dados adicionais da produção mostrarem que eles estão abaixo do ideal.

Ajustador do Mercado Monetário

Em 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 em nosso caso é igual a extensão entre a taxa de estabilidade e o DSR (relação do serviço da dívida) no *DAI Multi-Collateral*.

Embora planejamos manter a taxa de empréstimo fixa, é possível alterá-la juntamente com o preço de resgate usando um ajustador do mercado monetário. O mercado monetário muda a taxa de empréstimo e o preço de resgate de forma a incentivar os criadores de 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 que se estiver abaixo do resgate, as taxas aumentarão.

Liquidação Global

A liquidação global é um método de último recurso utilizado para garantir o preço de resgate a todos os titulares de índices reflexos. Ele visa permitir tanto aos possuidores de índices de reflexo quanto aos criadores de SAFE resgatar a garantia 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 após queimar uma certa quantidade de tokens de protocolo.

A liquidação tem três fases principais:

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

- **Processo:** processar todos os leilões pendentes

- **Reivindicação:** todo possuidor de índices de reflexo e criador de SAFE pode reivindicar uma quantia fixa 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 possuidores de tokens de governança implantem um sistema totalmente novo. Escolhemos esta estratégia porque podemos eliminar o meta-jogo em que as pessoas tentam influenciar o processo de governança em seu próprio benefício, prejudicando assim a confiança no sistema. Estabelecemos a operação adequada do protocolo sem depositar demasiada fé nos humanos (o "efeito Bitcoin") para maximizar a escalabilidade social e minimizar os riscos para outros desenvolvedores que queiram usar a 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 *Governança da era do gelo*, um registro de permissões que pode bloquear algumas partes do sistema de fora do controle, após determinados prazos terem passado.

Governança vinculada tempo

A governança vinculada ao tempo é o primeiro componente do módulo de governança restrita. Ele impõe atrasos de tempo entre as mudanças aplicadas ao mesmo parâmetro. Um exemplo é a possibilidade de alterar os endereços dos *Oracles* usados no Moderador da Rede *Oracle* (Seção 6.2) depois de pelo menos *T* segundos desde a última modificação do *Oracle*.

Governança vinculada à ação

O segundo componente do Módulo de Governança Restrita é a governança vinculada à ação. Cada parâmetro governável tem limites sobre quais valores ele pode ser definido e quanto ele pode mudar durante um determinado período de tempo. Exemplos notáveis são as versões iniciais do Mecanismo de Feedback da taxa de resgate (Seção 4.2) que os possuidores dos tokens de governança serão capazes de fazer um ajuste fino.

Governança da era do gelo

A Era do Gelo é um contrato inteligente imutável que impõe prazos para a mudança de parâmetros específicos do sistema e para a atualização do protocolo. Ele pode ser usado no caso em que a governança quer ter certeza de que eles podem corrigir bugs antes que o protocolo se bloqueie e negue a intervenção externa. A Era do Gelo verificará se uma mudança é permitida, verificando o nome do parâmetro e o endereço do contrato afetado em relação a um registro de prazos. Se o prazo tiver passado, a chamada será revertida.

A governança pode ser capaz de atrasar a Era do Gelo um número fixo de vezes se forem encontrados bugs próximos à data em que o protocolo deve começar a se bloquear. Por exemplo, a idade do gelo só pode ser atrasada três vezes, cada vez por um mês, para que as novas correções de bugs implementadas sejam testadas adequadamente.

Áreas centrais onde a governança é necessária

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

- **Adicionando novos tipos de colaterais:** A RAI será suportado apenas pela ETH, mas outros índices serão suportados por múltiplos tipos de colaterais e a governança será capaz de diversificar o risco ao longo do tempo

- **Mudança de dependências externas:** Oracles e DEXs dos quais o sistema depende podem ser atualizados. A governança pode apontar o sistema para dependências mais novas para que ele continue a funcionar corretamente

- **Ajustadores finos de taxas:** os primeiros controladores de política monetária terão parâmetros que podem ser mudados dentro de limites razoáveis (como descrito por Governança vinculada a ação e tempo)

- **Migração entre versões do sistema:** em alguns casos, a governança pode implantar um novo sistema, dar-lhe permissão para emitir 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 de migração entre as versões do sistema:

- Há um registro de migração que mantém registro de quantos sistemas diferentes o mesmo token de protocolo cobre e quais sistemas podem ser negados a permissão para emitir tokens de protocolo em um leilão de dívida

- Toda vez que a governança implementa uma nova versão do sistema, eles apresentam o endereço do contrato de leilão da dívida do sistema no registro de migração. A governança também precisa especificar se eles serão capazes de impedir que o sistema emita 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

- Há um período de reflexão entre propor um novo sistema e retirar as permissões de um sistema antigo

- Um contrato opcional pode ser estabelecido para que ele desligue automaticamente um sistema antigo após ser negada a permissão para emitir

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

Desligamento automático do sistema

Há casos que o sistema pode detectar automaticamente e como resultado, acionar a liquidação por si só, sem a necessidade de usar tokens do protocolo:

- **Atrasos severos na entrada de preços:** o sistema detecta que uma ou mais das fontes de preços colaterais ou índices não foram atualizados em um longo tempo

- **Migração do sistema:** este é um contrato opcional que pode fechar o protocolo após um período de arrefecimento passar do momento em que a governança retira a capacidade do mecanismo de leilão de dívida para emitir 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 tem sido x% desviado por um longo tempo em comparação com o preço de resgate

A governança será capaz de atualizar estes módulos de desligamento autônomo enquanto ainda estiver limitada ou até que a Era do Gelo comece a bloquear algumas partes do sistema.

Oracles

Há três tipos principais de ativos para os quais o sistema precisa ler os preços de entrada: o índice, o símbolo do protocolo e cada tipo de colateral permitido. As fontes de preços podem ser fornecidas por Oracles liderados pela governança ou por redes Oracles já estabelecidas.

Oracles liderados pela governança

Os possuidores de tokens de governança ou a equipe central que lançou o protocolo podem formar parcerias com outras entidades que reúnem várias fontes de preços off-chain e depois submeter uma única transação a um contrato inteligente que verifica todos os pontos de dados.

Esta abordagem permite maior flexibilidade na atualização e mudança da infraestrutura do Oracle, embora seja feita às custas da falta de confiança.

Moderador da rede Oracle

Um Moderador da rede Oracle é um contrato inteligente que lê preços de múltiplas fontes que não são diretamente controladas pela governança (p. ex., estoque da UniswapV2 entre um tipo de índice colateral e outras moedas estáveis) e depois modera todos os resultados. Funciona da seguinte forma:

- Nosso contrato mantém o controle das redes de Oracles aprovadas que pode chamar a fim de solicitar preços colaterais. O contrato é financiado por parte do excedente que o sistema acumula (usando o Excedente do Tesouro, Seção 11). Cada rede de Oracles aceita tokens específicos como pagamento, de modo que nosso contrato também mantém registro do montante mínimo e do tipo de tokens necessários para cada solicitação

- A fim de impulsionar uma nova alimentação de preço no sistema, todos os Oracles precisam ser chamados de antemão. Ao chamar um Oracle, o contrato primeiro troca algumas taxas de estabilidade com um dos tokens aceitos do Oracle. Após a chamada de um Oracle, o contrato marca a chamada como "válida" ou "inválida". Se uma chamada for inválida, o Oracle defeituoso específico não poderá ser chamado novamente até que todos os outros sejam chamados e o contrato verifique se há uma maioria válida. Uma chamada de Oracle válida não deve reverter e deve recuperar um preço que tenha sido postado na cadeia nos últimos *m* segundos. "Recuperar" significa coisas diferentes, dependendo de cada tipo de Oracle:

    - Para Oracles baseados em puxar, dos quais podemos obter um resultado imediatamente, nosso contrato precisa pagar uma taxa e buscar diretamente o preço

    - Para Oracles baseados em empurrar, nosso contrato paga a taxa, chama o Oracle e precisa esperar um período de tempo *n* específico antes de chamar o Oracle novamente, a fim de obter o preço solicitado

- Cada resultado do Oracle é salvo em um vetor. Depois que cada Oracle aprovado é chamado e se o vetor tiver dados válidos suficientes para formar uma maioria (p. ex., o contrato recebeu dados válidos de 3/5 Oracles), os resultados são ordenados e o contrato escolhe a mediana

- Quer o contrato encontre a maioria ou não, a vetor com os resultados do Oracle é limpo e o contrato terá de esperar *p* segundos antes de iniciar todo o processo de novo

Rede de Oracles reserva

A governança pode adicionar uma opção de reserva de Oracles que começa a empurrar os preços no sistema se o verificador não conseguir encontrar a maioria das redes de oráculos válidos várias vezes seguidas.

A opção de reserva deve ser definida quando o verificador for implementado, pois não pode ser alterada posteriormente. Além disso, um contrato separado pode monitorar se o reserva está substituindo o mecanismo de verificação há muito tempo e desliga automaticamente o protocolo.

Safes

A fim de gerar índices, qualquer pessoa pode depositar e alavancar seus criptocolaterais dentro dos Safes. Enquanto um SAFE esta aberto, ele continuará acumulando dívidas de acordo com a taxa de empréstimo dos colaterais depositados. Assim que o criador do SAFE paga sua dívida, eles poderão retirar mais e mais de suas garantias bloqueadas.

Ciclo de vida do SAFE

Há quatro etapas principais necessárias para criar índices de reflexo e posteriormente pagar a dívida de um SAFE:

- Depósito de colateral no SAFE

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

- Gerar índices suportados pelos colaterais da SAFE

  O usuário especifica quantos índices eles querem gerar. O sistema cria uma quantidade igual de dívida que começa a acumular de acordo com a taxa de empréstimo do colateral.

- Pagar a dívida da SAFE

  Quando o criador do SAFE quer sacar seus colaterais, ele tem que pagar sua dívida inicial mais os juros acumulados.

- Sacar colateral

  Após o usuário pagar parte ou a totalidade de sua dívida, é permitido ao usuário retirar seus colaterais.

Liquidação de SAFE

A fim de manter a liquidez do sistema e cobrir o valor de toda a dívida pendente, cada SAFE pode ser liquidado no caso de sua taxa de colateralização cair abaixo de um determinado limite. Qualquer um pode desencadear uma liquidação, caso em que o sistema confisca o colateral da SAFE e o venderá em um leilão de colaterais.

Seguro de Liquidação

Em uma versão do sistema, os criadores de SAFE podem ter a opção de escolher um gatilho para quando seus SAFE forem liquidados. Os gatilhos são contratos inteligentes que automaticamente adicionam mais colaterais em um SAFE e potencialmente o salvam 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 os SAFEs é a adição de dois diferentes limiares de colateralização: seguro e de risco. Os usuários de SAFE podem gerar dívidas até atingir o limiar de segurança (que é maior que o risco) e só são liquidados quando a colateralização do SAFE fica abaixo do limiar de risco.

Leilão de colaterais

Para iniciar um leilão de colaterais, o sistema precisa utilizar uma variável chamada *liquidationQuantity* para determinar o montante da dívida a ser coberta por cada leilão e o montante correspondente do colateral a ser vendido. Uma penalidade de liquidação será aplicada a cada SAFE leiloado.

Parâmetros do leilão de colaterais

Nome do parâmetro	Descrição
minimumBid	Quantidade mínima de moedas que precisam ser oferecidas em uma oferta
discount	Desconto em que o colateral está sendo vendido

lowerCollateralMedianDeviation	Desvio máximo do limite inferior que a mediana do colateral pode ter se comparado com o preço no Oracle
upperCollateralMedianDeviation	Desvio máximo do limite superior que a mediana do colateral pode ter se comparado com o preço no Oracle
lowerSystemCoinMedianDeviation	Desvio máximo do limite inferior que o preço da moeda do sistema de alimentação dos Oracles pode ter em comparação com o preço da moeda do sistema de Oracles
upperSystemCoinMedianDeviation	Desvio máximo do limite superior que a mediana do colateral pode ter se comparado com o preço da moeda do sistema de Oracle
minSystemCoinMedianDeviation	Mediana do resultado do desvio mínimo da moeda do sistema em comparação com o preço de resgate a fim de tomar o mediana em conta

Mecanismo do leilão de colaterais

O leilão com desconto fixo é uma forma simples (em comparação com os leilões ingleses) de colocar à venda colaterais em troca de moedas do sistema utilizadas para liquidar dívidas incobráveis. Os licitantes só são obrigados a permitir que a casa de leilão transfira seu *safeEngine.coinBalance* e possam então chamar a *buyCollateral* para trocar suas moedas do sistema por colaterais que são vendidas com desconto em comparação com seu último preço de mercado registrado.

Os licitantes também podem rever a quantidade de garantias que podem obter de um leilão específico chamando *getCollateralBought* ou *getApproximateCollateralBought*. Note que *getCollateralBought* não é marcado como vista porque lê (e também atualiza) o Preço de Resgate do retransmissor do Oracle enquanto *getApproximateCollateralBought* usa o *lastReadRedemptionPrice*.

Leilão de dívida

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

Os leilões de dívidas destinam-se a cunhar mais tokens de protocolo (Seção 10) e vendê-los para índices que possam anular o endividamento ruim restante do sistema.

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

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

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

Ajuste de parâmetros de leilão de dívida automático

A quantidade inicial de tokens de protocolo cunhadas em um leilão de dívida pode ser definida através de um voto de governança ou pode ser automaticamente ajustada pelo sistema. Uma versão automatizada precisaria ser integrada com Oracles (seção 6) a partir da qual 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 serão cunhados para os índices de *debtAuctionBidSize*. *initialDebtAuctionAmount* pode ser definido com desconto em relação ao preço de mercado real do PROTOCOLO/ÍNDICE, a fim de incentivar a licitação.

Parâmetros do leilão de dívida

Nome do parâmetro	Descrição
amountSoldIncrease	Aumento da quantidade de tokens de protocolo a serem cunhados para a mesma quantidade de índices
bidDecrease	O próximo lance mínimo de redução da quantidade aceita de Tokens de protocolo para a mesma quantidade de índices
bidDuration	Quanto tempo dura a licitação depois que uma nova licitação é submetida (em segundos)

totalAuctionLength	Duração total do leilão (em segundos)
auctionsStarted	Quantos leilões já começaram até agora

Mecanismo de leilão de dívida

Ao contrário dos leilões de colaterais, os leilões de dívidas têm apenas uma etapa:

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 se não houver nenhuma licitação. Toda vez que for reiniciado, o sistema oferecerá mais tokens de protocolo para a mesma quantidade de índices. A nova quantidade de tokens de protocolo é calculada com *lastTokenAmount* * *amountSoldIncrease* / 100. Depois que um leilão é combinado, o sistema irá cunhar os tokens para o licitante com a maior oferta.

Tokens de protocolos

Como descrito nas seções anteriores, cada protocolo precisará ser protegido por um Token que é cunhado através de leilões de dívidas. Além da proteção, o Token será usado para governar alguns componentes do sistema. Além disso, o fornecimento do Token do protocolo será gradualmente reduzido com o uso de leilões de excedentes. A quantidade de excedente que precisa ser acumulada no sistema antes dos fundos extras serem leiloados é chamada de *surplusBuffer* e é automaticamente ajustada como uma porcentagem do total da dívida emitida.

Fundo de Seguros

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

Leilão de excedentes

Os leilões de excedentes vendem taxas de estabilidade acumuladas no sistema por tokens de protocolo que depois são queimadas.

Parâmetros do leilão de excedentes

Nome do parâmetro	Descrição
bidIncrease	Aumento mínimo na próxima licitação
bidDuration	Quanto tempo dura o leilão depois que uma nova proposta é apresentada (em segundos)
totalAuctionLength	Duração total do leilão (em segundos)
auctionsStarted	Quantos leilões já começaram até agora

Mecanismo do leilão de excedentes

O leilão de excedentes têm uma única etapa:

increaseBidSize(uint id, uint amountToBuy, uint bid): qualquer pessoa pode licitar uma quantidade maior de tokens de protocolo para a mesma quantidade de índices (excedente). Cada nova licitação precisa ser maior ou igual à *lastBid * bidIncrease* / 100. O leilão terminará após o total máximo de segundos do *totalAuctionLength* de duração do leilão ou após os segundos de *bidDuration* terem passado desde a última licitação e nenhuma nova licitação tiver sido apresentada 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 maior licitante e então queimará todos os tokens de protocolo reunidos.

Gestão de índices de excedentes

Toda vez que um usuário gera índices e implicitamente cria dívidas, 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 contábil utilizado para acionar leilões de dívida (Seção 9.2) e excedente (Seção 10.1)
- A *tesouraria de excedentes* utilizado para financiar os componentes centrais da infraestrutura e incentivar os atores externos a manter o sistema

A tesouraria de excedentes está encarregada de financiar três componentes centrais do sistema:

- Módulo do Oracle (Seção 6). Dependendo de como um Oracle é estruturado, a tesouraria ou paga os oráculos de governança off-chain liberados ou paga por chamadas para redes de Oracles. A tesouraria também pode ser configurada para pagar os endereços que gastaram *gas* para chamar um Oracle e atualizá-lo.

- Em alguns casos, equipes independentes fazem a manutenção do sistema. Exemplos são as equipes que fazem uma lista de novos tipos de colaterais liberados ou fazem ajuste fino no definidor de taxa do sistema (Seção 4.2).

A tesouraria pode ser ajustada para que alguns beneficiários excedentes tenham o financiamento automaticamente negado no futuro e outros possam tomar seu lugar.

Atores externos

O sistema depende de atores externos para poder funcionar corretamente. Estes atores são economicamente incentivados a participar em áreas como leilões, processamento de liquidações globais, criação de mercado e atualização de preços de alimentação para manter o funcionamento correto do sistema.

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

Mercado endereçável

Vemos a RAI como sendo útil principalmente em duas áreas:

- **Diversificação da carteira:** os investidores usam a RAI para se exporem a um ativo como ETH sem todo o risco de realmente ter Ether

- **Garantias para ativos sintéticos:** A RAI pode oferecer protocolos como UMA, MakerDAO e Synthetix uma menor exposição ao mercado cripto e dar aos usuários mais tempo para sair de suas posições no caso de cenários como a Black Thursday em março de 2020, quando milhões de dólares em criptoativos foram liquidados

Pesquisas futuras

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

Primeiro queremos lançar as bases para padrões futuros em torno de protocolos que se auto-bloqueiam do controle externo e para verdadeiros "robôs do dinheiro" que se adaptam em resposta às forças do mercado. Em seguida, convidamos a comunidade Ethereum a debater e projetar melhorias em torno de nossas propostas com um foco específico em colaterais e leilões de dívidas.

Riscos e mitigação

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

- **Bugs no contrato inteligente:** o maior risco apresentado ao sistema é a possibilidade de um bug que permite a qualquer pessoa extrair todas as garantias ou bloquear o protocolo em um estado do qual ele não possa se recuperar. Planejamos ter nosso código revisado por vários pesquisadores de segurança e lançar o sistema em uma testnet antes de nos comprometermos a implementá-lo na produção.

- **Falha no Oracle:** agregaremos as alimentações de múltiplas redes de Oracles e haverá regras rigorosas para atualizar apenas um Oracle de cada vez, de modo que a governança maliciosa não possa facilmente introduzir preços falsos
- **Eventos de cisne negro em colaterais:** há o risco de um evento de cisne negro em um colateral subjacente que pode resultar em uma alta quantidade de SAFEs liquidados. As liquidações podem não ser capazes de cobrir toda a dívida pendente e, portanto, o sistema mudará continuamente seu buffer

excedente a fim de cobrir uma quantidade decente da dívida emitida e resistir aos choques do mercado.

- **Parâmetros de ajuste de taxa impróprios:** mecanismos autônomos de feedback são altamente experimentais e podem não se comportar exatamente como previámos durante as simulações. Planejamos permitir que a governança faça ajustes finos neste componente (enquanto ainda está limitado) a fim de evitar cenários inesperados.

- **Falha em iniciar um mercado de liquidantes corretamente:** os liquidantes são atores vitais que asseguram 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 para manter o sistema seguro.

Sumário

Propusemos um protocolo que se bloqueia progressivamente do controle humano e emite um ativo de baixa volatilidade, colateralizado, chamado de índice de reflexo. Primeiro apresentamos o mecanismo autônomo destinado a influenciar o preço de mercado do índice e depois descrevemos como vários contratos inteligentes podem limitar o poder que os donos dos tokens têm sobre o sistema. Delineamos um esquema auto-sustentável para a moderação dos preços de alimentação de múltiplas redes de Oracles independentes e depois 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 and Engineers”,https://bit.ly/3bHwnMC

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

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

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

Glossário

Índice de reflexo: um ativo colateralizado que suaviza volatilidade de seu subjacente

RAI: nosso primeiro índice de reflexo

Preço de resgate: o preço que o sistema quer que o índice tenha. Ele muda, influenciado por uma taxa de resgate (computada pelo MFTR), caso o preço de mercado não esteja próximo a ele. Significa influenciar os criadores do SAFE a gerar mais ou pagar parte de sua dívida

Taxa de empréstimo: taxa de juros anual aplicada a todos os SAFEs que têm dívidas pendentes

Mecanismo de Feedback da Taxa de Resgate (MFTR): um mecanismo autônomo que compara os preços de mercado e de resgate de um índice de reflexo e depois calcula uma taxa de resgate que lentamente influencia os criadores do SAFE para gerar mais ou menos dívida (e implicitamente tenta minimizar o desvio do preço de mercado/resgate)

ajustador do mercado monetário (AMM): um mecanismo similar ao MFTR que puxa múltiplas alavancas monetárias de uma só vez. No caso de índices de reflexos, ele modifica tanto a taxa de empréstimo quanto o preço de resgate

Moderador da Rede Oracle (MRO): um contrato inteligente que puxa os preços de múltiplas redes de Oracles (que não são controladas pela governança) e os modera se uma maioria (p. ex., 3 em 5) retornasse um resultado ilegal

Módulo de Governança Restrita (MGR): um conjunto de contratos inteligentes que limitam o poder que os donos de tokens de governança têm sobre o sistema. Impõe atrasos de tempo ou limita as possibilidades que a governança tem de estabelecer certos parâmetros

Era do Gelo: 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 leilões de dívidas e excedentes. Também acompanha o montante da dívida atualmente leiloada, a dívida incobrável não acionada e o buffer do excedente.

Buffer Excedente: quantidade de juros a acumular e manter no sistema. Qualquer juro acumulado acima deste limite é vendido em leilões de excedentes que queimam tokens de protocolo.

Tesouraria de Excedentes: contrato que dá permissão a diferentes módulos do sistema para retirar os juros acumulados (p. ex., MRO para chamadas de oráculo)