Rai: Uma Garantia de Baixa Volatilidade e Confiança Minimizada para o Ecossistema DeFi

Stefan C. Ionescu, Ameen Soleimani

May 2020

Resumo. Nós apresentamos uma administração minimizada, um protocolo descentralizado que automaticamente reage às forças do mercado com a intenção de modificar o valor alvo de seu ativo garantido nativo. O protocolo permite que qualquer um aproveite seus criptográficos ativos e emite um "índice de reflexo", que é uma versão amortecida de sua garantia subjacente. Nós delineamos como índices podem ser úteis como universais, baixa volatilidade garantida que pode proteger seus titulares, assim como outros protocolos financeiros descentralizados, de mudanças repentinas de mercado. Nós apresentamos nossos planos para ajudar outras equipes a lançarem seus próprios sintéticos, alavancando nossa infraestrutura. Finalmente, nós oferecemos alternativas para oráculos atuais e estruturas administrativas que são frequentemente encontradas em muitos protocolos DeFi.

Conteúdo

1. Introdução

O dinheiro é um dos mais poderosos mecanismos de coordenação que a humanidade potencializa com a intenção de prosperar. O privilégio de administrar o suprimento de dinheiro foi historicamente mantido nas mãos de lideranças soberanas e da elite financeira, enquanto era imposto a um público geral inconsciente. Onde o Bitcoin tem demonstrado o potencial para um protesto popular para manifestar um ativo de mercadoria de reserva de valor, Ethereum nos fornece uma plataforma para construir instrumentos sintéticos apoiados por ativos que podem ser protegidos de volatilidade e usados como colaterais, ou atrelados a um preço de referência e usado como um meio de troca para transações diárias, todas reforçadas pelos mesmos princípios de consenso descentralizado.

Acesso não permitido ao Bitcoin para armazenar riqueza e instrumentos sintéticos devidamente descentralizados no Ethereum vai lançar a base para a vindoura revolução financeira, provendo aos que estão na periferia do sistema financeiro moderno os meios para coordenar a construção do novo.

Nesse artigo, nós introduzimos uma estrutura para se construir índices de reflexo, um novo tipo de ativo que vai ajudar outros sintéticos a florescer e vai estabelecer um alicerce fundamental para toda a indústria financeira descentralizada.

2. Visão Global de Índices de Reflexo

O propósito do reflexo de índice não é manter um específico alicerce, mas atenuar a volatilidade de suas garantias. Índices permitem que qualquer um ganhe exposição ao mercado de criptomoedas sem a mesma escala de risco que manter os ativos criptográficos reais. Nós acreditamos que RAI, nosso primeiro índice de reflexo, vai ter utilidade imediata para outras equipes que emitem sintéticos no Ethereum (por exemplo: MakerDAO’s Multi-Collateral DAI [1], UMA [2], Synthetix [3]) porque isso garante aos sistemas deles uma menor exposição a ativos voláteis como os ETH e oferece aos usuários mais tempo para sair de suas posições no caso de uma mudança significante no mercado.

Para entender os índices de reflexo, nós podemos comparar o comportamento de seus preços de resgate aos preços de uma moeda estável.

O preço de resgate é o valor de uma unidade de débito (ou moeda) no sistema. É feito para ser usado apenas como uma ferramenta de contabilidade e é diferente do preço de mercado (o valor pelo qual o mercado está negociando a moeda). No caso de estar apoiado por moedas estáveis fiat, como USDC, os operadores do sistema declaram que qualquer um pode resgatar uma moeda por um dólar americano, e, assim, o preço de resgate por essas moedas é sempre o mesmo. Há também casos de moedas estáveis com base em criptografia, como MakerDAO's Multi Collateral DAI (MCD), onde o sistema tem como meta uma atrelagem fixa de um dólar americano, e então o preço de resgate também é fixado em um.

Na maioria dos casos, vai haver uma diferença entre o preço de mercado de uma moeda estável e o preço de resgate. Esses cenários criam oportunidades de arbitragem onde negociantes vão criar mais moedas se o preço de mercado for maior do que o de resgate, e eles resgatarão suas moedas estáveis como garantia (por exemplo, dólares americanos no caso de USDC) caso o preço de mercado for menor do que o preço de resgate.

Índices de resgate são similares a moedas estáveis porque eles também possuem um preço de resgate que o sistema procura. A principal diferença no caso deles é que o seu resgate não permanecerá fixo, mas é projetado para mudar enquanto é influenciado pelas forças do mercado. Na Seção 4, nós explicamos como o preço de resgate de um índice flutua e cria novas oportunidades de arbitragem para seus usuários.

3. Filosofia de Design e Estratégia de Go-To-Market

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

Multi-Collateral DAI foi o caminho 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 com

o desenvolvimento e comunicações, nós queremos fazer apenas as mais simples mudanças para a base de código MCD original, para concretizar nossa implementação.

Nossas modificações mais importantes incluem a adição de um definidor de taxa autônomo, um Oracle Network Medianizer (Medianizador de Rede para Oráculo) que é integrado com muitos feeds de preços independentes e uma camada de minimização de governança planejada para isolar o sistema o quanto for possível de intervenção humana.

A primeira versão do protocolo (Estágio 1) vai incluir apenas o definidor de taxa e outras melhorias menores na arquitetura central. Uma vez que provarmos que o definidor funciona como esperado, nós podemos adicionar de forma mais segura o oráculo medianizador (Estágio 2) e a cama de minimização de governança (Estágio 3).

4. Mecanismos de Política Monetária

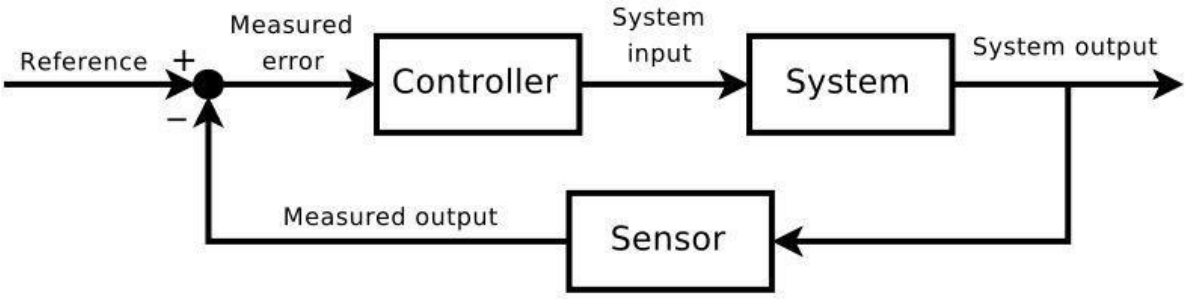
4.1. Introdução à Teoria de Controle

Um sistema de controle comum com o qual muitas pessoas estão familiarizadas é o chuveiro. Quando alguém começa a tomar banho, tem a temperatura ideal em mente, a qual, na teoria de controle, é chamada de ponto de referência. A pessoa, agindo como o controlador, mede continuamente a temperatura de fluxo da água (que é chamada de sistema de saída) e modifica a velocidade com a qual eles giram o botão do chuveiro baseado no desvio (ou erro) entre a desejada e atual temperatura. A velocidade em que o botão é girado é chamada de sistema de entrada. O objetivo é girar o botão rápido o suficiente para alcançar o ponto de referência rapidamente, mas não tão veloz a ponto de ultrapassar a temperatura. Se houverem choques de sistema em que o fluxo de temperatura da água mude de repente, a pessoa deve ser capaz de manter a temperatura atual por saber o quão rápido deve girar o botão em resposta ao distúrbio.

A disciplina científica de manter a estabilidade em sistemas dinâmicos é chamada de teoria de controle, e esta 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 a média de dez minutos

de tempo de bloqueio, apesar da variável de hashrate (poder computacional), é um exemplo de sistema de controle de missão crítica.

Na maioria dos sistemas de controle modernos, um controlador de algoritmo é tipicamente embutido no processo e recebe controle sobre uma entrada do sistema (por exemplo: o pedal do acelerador de um carro a gás) para que o atualize automaticamente, baseado em desvios entre a saída do sistema (por exemplo: a velocidade do carro) e o ponto de ajuste (por exemplo: a velocidade do controle de cruzeiro).



O tipo mais comum de controlador de algoritmo é o controlador PID. Aproximadamente 95% de aplicações industriais e uma ampla variedade de sistemas biológicos empregam elementos de controle PID [4]. Um controlador PID usa uma fórmula matemática com três partes para determinar sua saída:

Controller Output = Proportional Term + Integral Term + Derivative Term
(Controlador de Saída = Termo Proporcional + Termo Integral + Termo Derivado)

O Termo Proporcional é a parte do controlador que é diretamente proporcional ao desvio. Se o desvio é 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 parte do controlador que leva em conta quão longo um desvio persistiu. É determinado tomando o integrante do desvio ao longo do tempo e é primariamente usado para eliminar erro de estado estacionário. Ele se acumula para responder a pequenos, embora persistentes, desvios do ponto de ajuste (por exemplo: o

ponto de ajuste do controle de cruzeiro foi 1mph maior do que a velocidade do carro por alguns minutos).

O Termo Derivado é a parte do controlador que leva em consideração o quão rápido o desvio está crescendo ou encolhendo. 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 é maior do que a velocidade do carro e o carro começar a desacelerar). Também ajuda reduzir a ultrapassagem desacelerando a resposta do controlador quando o desvio está encolhendo (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 independentemente ajustada, dá aos controladores de PID grande flexibilidade manejando uma ampla variedade de aplicações de sistema de controle.

Controladores PID trabalham melhor em sistemas que permitem algum grau de atraso no tempo de resposta, assim como a possibilidade de ultrapassagem e oscilação em volta do ponto de ajuste enquanto o sistema tenta se estabilizar. Sistemas de índice de reflexo como RAI são bem adequadas para esse tipo de cenário onde seus preços de resgate podem ser mudados por controladores PID.

De forma mais geral, foi descoberto recentemente que muitas das regras atuais de política monetária do banco central (exemplo: a Regra Taylor) são na verdade aproximações de controladores PID [5].

4.2. Mecanismo de Feedback da Taxa de Resgate

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

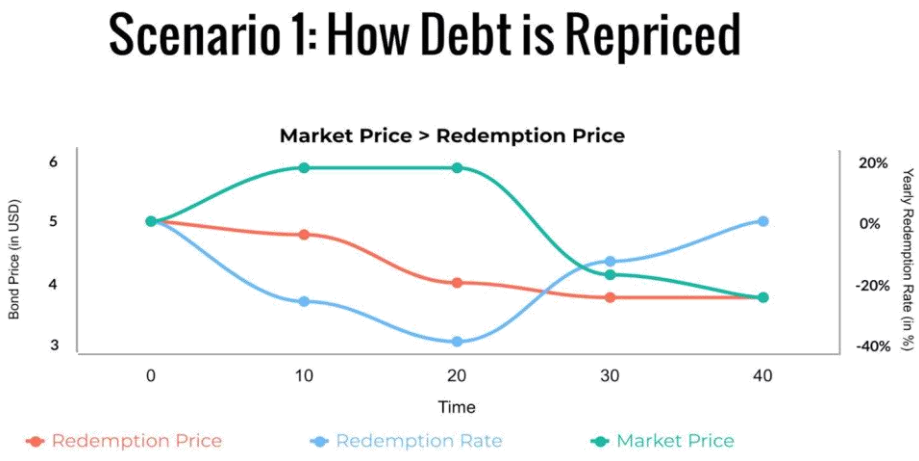
4.2.1. Componentes

Em teoria, seria possível manipular diretamente o índice de reflexo do preço de resgate (descrito na Seção 2) para influenciar usuários de índices e mudar por fim o preço de mercado do índice. Na prática, esse método não teria o efeito desejado nos participantes do sistema. Da perspectiva de um titular da SAFE, se o preço de resgate for aumentado apenas uma vez, eles podem aceitar um preço maior por unidade de débito, absorver a perda de um índice de garantia diminuído e manter sua posição. Se, contudo, eles esperam que o preço de resgate continue a crescer com o tempo, eles provavelmente estariam mais inclinados a evitar perdas futuras já esperadas, e, portanto, escolher pagar suas dívidas e encerrar suas posições.

Nós esperamos que os participantes do sistema de reflexo de índices não respondam diretamente a mudanças no preço de resgate, mas, em vez disso, respondam a taxa de variação do preço de resgate que nós 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 completamente automatizada.

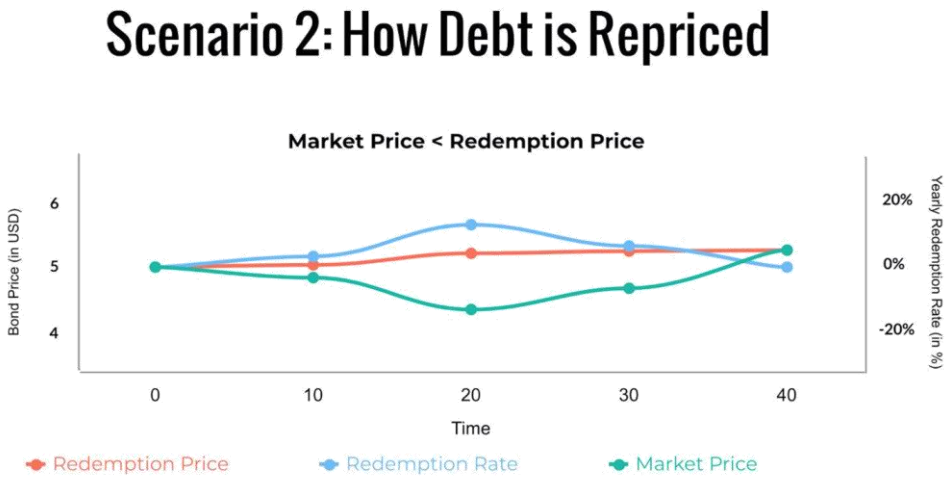
4.2.2. Cenários

Lembre-se 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 mudanças nas forças do mercado. Para conseguir isso, a taxa de resgate é calculada para que ela se oponha aos desvios entre mercado e preços de resgate.
No primeiro cenário abaixo, se o preço de mercado do índice é maior do que o seu preço de resgate, o mecanismo vai calcular uma taxa negativa que vai começar a diminuir o preço de resgate, fazendo, assim, a dívida do sistema se tornar mais barata.



A expectativa de uma diminuição do preço de resgate vai provavelmente desencorajar as pessoas de manter índices e encorajar titulares da SAFE a gerar mais dívida (mesmo se o preço de garantia não mudar) que é então vendida no mercado, equilibrando assim a oferta e a demanda. Note que este é o cenário ideal, onde titulares de índices reagem rapidamente em resposta ao feedback do mecanismo. Na prática (e especialmente em poucos dias após o lançamento), nós esperamos um atraso entre o começo e os resultados reais observados entre o montante de débito emitido e, consequentemente, no preço de mercado.

De outro lado, no cenário dois, se o índice de preço de mercado é menor do que o preço de resgate, a taxa se torna positiva e começa a reavaliar todo o débito para que ele se torne mais caro.
Assim que a dívida se torna mais cara, os índices de garantia de todos os SAFEs caem (assim, os criadores do SAFE são incentivados a pagar suas dívidas) e os usuários começam a acumular índices com a expectativa de que elas irão aumentar de valor.



4.2.3. Algoritmo

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

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

- Em algum momento, o índice do preço de mercado sobe de ‘rand’ para ‘rand’ + x. Depois que o mecanismo de feedback lê o novo preço de mercado, ele calcula um termo p proporcional, que nesse caso é -1 * ((‘rand’ + x) / ‘rand’). O proporcional é negativo para que diminua o preço de resgate e, em vez disso, reavalie os índices para que eles se tornem mais baratos.

- Depois de calcular o proporcional, o mecanismo vai determinar o termo integral *i* adicionando todos os desvios anteriores dos últimos segundos de desvio *Interval*

- O mecanismo soma o proporcional e o integral e calcula uma taxa de redenção por segundo *r*, que lentamente começa a diminuir o preço de resgate. Assim que os criadores SAFE percebem que podem gerar mais débito, eles irão inundar o mercado com mais índices

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

Na prática, o algoritmo será mais robusto e vamos ou tornar algumas variáveis imutáveis (por exemplo: o parâmetro *noise*, desvio *Interval*) ou haverão limites rígidos sobre o que a governança pode mudar.

4.2.4. Otimização

De extrema importância para o funcionamento apropriado do sistema de índice de reflexo é a otimização dos parâmetros do controlador algorítmico. Parametrizações impróprias podem resultar em um sistema muito devagar para conseguir estabilidade, excessivamente ultrapassado ou geralmente instável em face de choques externos.

O processo de otimização para um contralador PID normalmente envolve executar o sistema ao vivo, ajustando os parâmetros de otimização, e observando a resposta do sistema, em geral, introduzindo choques ao longo do caminho, de propósito. Dada a dificuldade e risco financeiro de ajustar os parâmetros de um sistema de índice de reflexo

ao vivo, planejamos alavancar a modelagem de computador e simulação o quanto for possível para definir os parâmetros iniciais, o que irá também permitir que a governança atualize os parâmetros de otimização se dados adicionais da produção se revelarem abaixo do ideal.

4.3. Configurador do Mercado Monetário

No RAI, planejamos manter a taxa de empréstimo (taxa de interesse aplicada quando se está gerando índices) fixa ou limitada e apenas modificar o preço de resgate, e então minimizar a complexidade envolvida em modelar o mecanismo de feedback. A taxa de empréstimo no nosso caso é igual ao *spread* entre a taxa de estabilidade e o DSR em Multi-Collateral DAI.

Apesar de planejarmos manter a taxa de empréstimo fixa, é possível mudá-la juntamente com o preço de resgate, usando um configurador de mercado monetário. O mercado monetário muda a taxa de empréstimo e o preço de resgate de uma forma que incentiva criadores SAFE a gerarem mais ou menos débito. Se o preço de mercado de um índice for maior que o resgate, ambas as taxas começaram a diminuir, enquanto se estiver abaixo do resgate, as taxas aumentarão.

4.4. Liquidação Global

A liquidação global é um método de último recurso para garantir preço de resgate para todos os titulares de índices de reflexo. É feito para permitir que titulares de índices de reflexo e criadores SAFE resgatem as garantias do sistema pelo seu valor líquido (quantidade de índices para cada tipo de garantia, de acordo com o último preço de resgate). Qualquer um pode acionar a liquidação depois de queimar uma certa quantidade de tokens de protocolo.

A liquidação tem três fases principais:

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

● Reivindicar: cada titular de índice de reflexo e criador SAFE pode reivindicar uma quantidade fixa de qualquer garantia do sistema baseada no último preço de resgate registrado no índice

5. Governança

A grande maioria dos parâmetros serão imutáveis e a mecânica interna do contrato inteligente não será atualizável a menos que os titulares de tokens implantem um sistema inteiramente novo. Nós escolhemos essa estratégia porque nós podemos eliminar o meta-jogo onde pessoas tentam influenciar o processo de governança para benefício próprio, danificando assim a confiança no sistema. Nós estabelecemos a operação apropriada do protocolo sem colocar muita fé em humanos (o "efeito bitcoin"), e assim nós maximizamos a escalabilidade e minimizamos os riscos para outros desenvolvedores que vão querer usar RAI como uma infraestrutura núcleo em seus próprios projetos.

Para os poucos parâmetros que podem ser modificados, nós propomos a adição de um Módulo de Governança Restrita, feito para atrasar ou limitar todas as modificações possíveis no sistema. Além disso, nós apresentamos o Governance Ice Age (Era do Gelo de Governança), um registro de permissões que pode bloquear algumas partes do sistema de controle externo, após alguns prazos terem passado.

5.1. Governança Com Limite de Tempo

A Governança Com Limite de Tempo é o primeiro componente do Módulo de Governança Restrita. Ele impõe atrasos no tempo entre mudanças aplicadas ao mesmo parâmetro. Um exemplo é a possibilidade de mudar os endereços dos oráculos usados no Medianizador de Rede para Oráculo (Seção 7.2) após pelo menos T segundos terem passado após a última mudança do oráculo.

5.2. Governança de Ação Limitada

O segundo componente no Módulo de Governança Restrita é a Governança de Ação Limitada. Todo parâmetro governável tem limites em quais valores podem ser definidos

e o quanto isso pode mudar durante um certo período de tempo. Exemplos notáveis são as versões iniciais do Mecanismo de Feedback da Taxa de Resgate (Seção 4.2) que os titulares de tokens de governança serão capazes de otimizar.

5.3. Era do Gelo de Governança

A Era do Gelo é um contrato inteligente imutável que impõe prazos para mudanças em parâmetros específicos do sistema e em atualizações do protocolo. Pode ser usado em casos em que a governança queira ter certeza de que pode consertar bugs antes que o protocolo bloqueie a si mesmo e impeça intervenções externas. A Era do Gelo vai verificar se uma mudança é permitida checando o nome do parâmetro e o endereço do contrato afetado em relação a um registro de prazos. Se o prazo tiver esgotado, a chamada será revertida.

A governança pode atrasar a Era do Gelo por um número fixo de vezes se bugs forem encontrados perto da data em que o protocolo deve começar a se bloquear. Por exemplo, a Era do Gelo pode ser atrasada apenas três vezes, cada vez por um mês, para que os novos consertos de bugs implementados sejam testados apropriadamente.

5.4. Principais Áreas Onde a Governança é Necessária

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

- Adicionando novos tipos de garantia: RAI será apoiado apenas pelo ETH, mas outros índices serão apoiados por múltiplos tipos de garantia e governança serão capaz de diversificar o risco ao longo do tempo
- Mudando dependências externas: oráculos e DEXs dos quais o sistema depende podem ser atualizados. A governança pode apontar o sistema para novas dependências para que continue funcionando apropriadamente.
- Ajustando as taxas de ajuste: os primeiros controladores de política monetária terão parâmetros que podem ser mudados dentro de limites razoáveis (como descritos em Ação e Governança Com Limite de Tempo)

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

5.4.1. Módulo de Migração Restrita

A seguir, um mecanismo simples para migrar entre versões do sistema:
● Há um registro de migração que rastreia quantos sistemas diferentes o mesmo protocolo de tokens cobre e quais sistemas podem ter permissões negadas para imprimir tokens de protocolo em um leilão de débitos

● Cada vez que a governança implanta uma nova versão do sistema, eles submetem o endereço do contrato de leilão de débito do sistema no registro de migração. A governança também precisa especificar se eles irão em algum momento ser capazes de impedir o sistema de imprimir tokens de protocolo. Além disso, a governança pode, em qualquer momento, dizer que um sistema irá sempre ser capaz de imprimir tokens e assim nunca será migrado

● Existe um período de espera entre propor um novo sistema e retirar permissões de um antigo

● Um contrato opcional pode ser definido para que ele automaticamente desligue um sistema antigo após ter permissão para imprimir negada

O módulo de migração pode ser combinado com uma Era do Gelo que automaticamente concede a itens específicos a permissão para sempre ter a capacidade de imprimir tokens.

6. Desligamento Automático do Sistema

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

● Graves Atrasos no Feed de Preço: o sistema detecta que uma ou mais das garantias ou feeds de índice de preço não tem sido atualizados há muito tempo

● Migração de Sistema: esse é um contrato opcional que pode desligar o protocolo após um período de espera, a partir do momento em que a governança retira a capacidade do mecanismo de leilão de débito de imprimir tokens de protocolo (Módulo de Migração Restrita, Seção 5.4.1.)

● Desvio Consistente no Preço de Mercado: o sistema detecta que o mercado de preço do índice tem estado x% desviado por um longo tempo, comparado ao preço de resgate

A governança terá a capacidade de atualizar esses módulos de desligamento autônomos enquanto ainda estiverem limitados ou até que a Era do Gelo comece a bloquear algumas partes do sistema.

7. Oráculos

Existem três principais tipos de ativos para os quais o sistema precisa ler feeds de preço: o índice, o token de protocolo e todos os tipos de garantias na lista de permissões. Os preços de feed podem ser providenciados por oráculos governados pela liderança ou por redes de oráculos já estabelecidas.

7.1. Oráculos Liderados pela Governança

Os titulares de tokens de governança ou a equipe núcleo que lançou o protocolo podem trabalhar juntos com outras entidades que reúnem múltiplos preços de feed fora da cadeia, e então submetem uma única transação para um contrato inteligente que medianiza todos os pontos de dados.
Essa abordagem permite mais flexibilidade para atualizar e mudar a infraestrutura do oráculo, embora acarrete falta de confiança.

7.2. Medianizador de Rede para Oráculo

Um medianizador de rede de oráculo é um contrato inteligente que lê preços de múltiplas fontes que não são diretamente controladas pela governança (exemplo: pool Uniswap V2 entre um tipo de índice de garantia e outras moedas estáveis) e assim medianiza todos os resultados. A ONM funciona da seguinte forma:

● Nosso contrato rastreia as redes de oráculo permitidas, as quais ele pode chamar para solicitar preços de garantia. O contrato é fundado por parte do excedente que o sistema acumula (usando a Tesouraria Excedente, Seção 11). Cada rede de oráculo aceita tokens específicos como pagamento, e então o nosso contrato rastreia o valor mínimo e o tipo de tokens necessário para cada solicitação.

● Para empurrar um novo preço de feed no sistema, todos os oráculos precisam ser chamados antecipadamente. Ao chamar um oráculo, o contrato primeiramente troca algumas taxas de estabilidade com um dos tokens aceitos pelo oráculo. Depois que um oráculo é chamado, o contrato marca a chamada como "válida" ou "inválida". Se uma chamada é inválida, o oráculo defeituoso específico não pode ser chamado outra vez até que todos os outros sejam chamados e o contrato cheque se há uma maioria válida. Uma chamada de oráculo válida não deve ser revertida e deve retornar um preço que tenha sido postado na cadeia em algum momento nos últimos *m* segundos. "Retornar" tem diferentes significados dependendo de cada tipo de oráculo:

○ Para oráculos baseados em pull, dos quais nós podemos ter um resultado rápido, 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 específico período de tempo *n* antes de chamar o oráculo novamente para conseguir o preço requerido

● Todo resultado de oráculo é salvo em uma matriz. Depois que cada oráculo na 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

● O contrato tendo encontrado uma maioria ou não, a matriz com resultados do oráculo é limpa e o contrato precisará esperar *p* segundos antes de começar o processo inteiro novamente

7.2.1. Backup de Rede para Oráculo

A governança pode adicionar uma opção de backup para oráculo que começa a empurrar preços no sistema se o medianizador não puder encontrar uma maioria de redes de oráculo válidas várias vezes seguidas.

A opção de backup deve ser definida quando o medianizador estiver implantado, já que ele não pode ser mudado mais tarde. Além do mais, um contrato separado pode monitorar se o backup tem substituído o mecanismo de medianização por muito tempo e automaticamente desligar o protocolo.

8. Cofres

Para gerar índices, qualquer um pode depositar e alavancar suas garantidas criptográficas dentro de Cofres. Quando um SAFE é aberto, ele continuará acumulando débito de acordo com a taxa de empréstimo de depósitos de garantia. Quando o criador de SAFE paga seu débito, ele será capaz de retirar mais e mais de suas garantias bloqueadas.

8.1. Ciclo de Vida SAFE

Existem quatro passos principais necessários para criar índices de reflexo e consequentemente pagar uma dívida de SAFE:

● Depositar garantias no SAFE
O usuário primeiro precisa criar um novo SAFE e depositar garantias nele.

● Gerar índices apoiados pelas garantias do SAFE

Os usuários especificam quantos índices eles querem gerar. O sistema cria uma quantidade igual de débito que começa a acumular de acordo com a taxa de empréstimo das garantias.

● Pagar a dívida SAFE

Quando o criador SAFE quer retirar suas garantias, ele precisa pagar o débito inicial e mais o interesse acumulado.

● Retirar garantia

Depois que o usuário paga alguma ou todas as suas dívidas, ele tem permissão para retirar sua garantia.

9. Liquidação SAFE

Para manter o sistema solvente e cobrir o valor de todo seu débito em aberto, cada SAFE pode ser liquidado caso seu índice de garantia caia abaixo de um limite específico. Qualquer um pode acionar uma liquidação, e, nesse caso, o sistema irá confiscar a garantia do SAFE e vendê-la em um *leilão de garantia*.

9.1. Leilão de Garantia

9.1.1. Seguro de Liquidação

Em uma versão do sistema, criadores SAFE podem ter a opção de escolher um acionamento para quando seus SAFEs estiverem liquidados. Acionamentos são contratos inteligentes que automaticamente adicionam mais garantia em um SAFE e potencialmente os salvam de uma liquidação. Exemplos de acionamentos são contratos que vendem posições curtas ou contratos que se comunicam com seus protocolos de segurança, como o Nexus Mutual [6].

Outro método para proteger SAFEs é a adição de dois limites de garantia diferentes: segurança e risco. Usuários SAFE podem gerar débito até alcançarem o limite do cofre (que é maior do que o risco) e só são liquidados quando a garantia do SAFE desce abaixo do risco limite.

Leilões de Garantia

Para começar um leilão de garantia, o sistema precisa usar uma variável chamada *liquidationQuantity* para determinar a quantidade de débito que precisa ser coberto por cada leilão e a quantidade correspondente de garantias que precisam ser vendidas. Uma penalidade de liquidação será aplicada a cada SAFE leiloado.

9.1.2. Parâmetros de Leilão de Garantia

Nome do Parâmetro	Descrição
Lance Mínimo	Quantidade mínima de moedas que precisam ser oferecidas em um lance
Desconto	Desconto pelo qual a garantia está sendo vendida
lowerCollateralMedianDeviation	Desvio máximo do limite inferior que a mediana de garantia pode ter em comparação com o preço do oráculo
upperCollateralMedianDeviation	Desvio máximo do limite superior que a mediana de garantia 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 de garantia pode ter em comparação com o preço do oráculo da moeda do sistema
minSystemCoinMedianDeviation	Desvio mínimo para o resultado mediano da moeda do sistema em comparação com o preço de resgate para ter em conta a mediana

9.1.3. Mecanismo de Leilão de Garantia

O leilão de desconto fixo é uma forma direta (comparada com leilões ingleses) para colocar garantias à venda em troca de moedas do sistema usadas para liquidar dívidas inadimplentes. Os licitantes só são obrigados a permitir que a casa de leilão transfira seu safeEngine.coinBalance e podem chamar buyCollateral para trocar suas moedas do sistema por garantias que são vendidas com desconto comparado com o seu último preço de mercado registrado.
Os licitantes também podem revisar a quantidade de garantia que eles podem conseguir de um leilão específico, chamando getCollateralBought ou getCollateralBought. Observe que getCollateralBought não é marcado como exibição porque lê (e também atualiza) o redemptionPrice do oráculo retransmissor, enquanto getApproximateCollateralBought utiliza o lastReadRedemptionPrice.

9.2. Leilão de Dívida

No cenário onde um leilão de garantia não pode cobrir todo o débito inadimplente em um SAFE, e se o sistema não tem nenhuma reserva excedente, qualquer um pode acionar um leilão de dívida.
Leilões de dívida são planejados para cunhar mais tokens de protocolo (Seção 10) e vendê-los por índices que podem anular o restante do débito inadimplente do sistema.

Para começar um leilão de dívida, o sistema precisa usar dois parâmetros:
● initialDebtAuctionAmount: a quantidade inicial de tokens de protocolo para cunhar após o leilão
● debtAuctionBidSize: o tamanho inicial do lance (quantos índices devem ser oferecidos em troca de tokens de initialDebtAuctionAmountprotocol)

9.2.1. Definição de Parâmetro de Leilão de Dívida

A quantidade inicial de tokens de protocolo cunhados em um leilão de dívida pode ou ser definido em uma votação de governança ou pode ser ajustado automaticamente pelo sistema.

Uma versão automatizada precisaria ser integrada com oráculos (Seção 6) dos quais o sistema leria o token de protocolo e refletiria o índice de preços de mercado. O sistema iria então definir a quantidade inicial de tokens de protocolo (initialDebtAuctionAmount) que será cunhado por índices debtAuctionBidSize. initialDebtAuctionAmount pode ser definido em um desconto comparado com o atual PROTOCOLO/ÍNDICE de preço de mercado, para incentivar a licitação.

9.2.2. Parâmetros de Leilão de Dívida

Nome do Parâmetro	Descrição
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

9.2.3. Mecanismos de Leilão de Dívida

Em oposição aos leilões de garantia, leilões de dívida tem 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 se não houverem lances colocados. Cada vez que ele reinicia, o sistema irá oferecer mais tokens de protocolo para a mesma quantidade de índices. O novo token de protocolo é calculado como o último *TokenAmount * amountSoldIncrease* / 100. Assim que o leilão tiver fim, o sistema irá cunhar tokens para o lance mais alto.

10. Tokens de Protocolo

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

Fundo de Seguro

Além do protocolo de token, a governança pode criar um fundo de seguro que detém uma ampla variedade de ativos não relacionados que pode ser usada como uma barreira para leilões de dívidas.

10.1. Leilões de Excedente

Leilões de excedente vendem taxas de estabilidade acumuladas no sistema por tokens de protocolo que são então queimadas.

10.1.1. Parâmetros de Leilão de Excedente

Nome do Parâmetro	Descrição
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

10.1.2. Mecanismo de Leilão de Excedente

Leilões de excedentes tem um único estágio:

increaseBidSize(uint id, uint amountToBuy, uint bid): qualquer um pode oferecer uma quantidade maior de tokens de protocolo pela mesma quantidade de índices (excedente). Cada lance precisa ser maior ou igual ao *lastBid* * *bidIncrease* / 100. O leilão vai terminar após o máximo de *totalAuctionLength* segundos ou depois que *bidDuration* segundos tenham passado desde o último lance e nenhum novo lance tenha sido submetido durante este tempo.

Um leilão irá recomeçar se não houverem lances. De outra forma, se o leilão tiver pelo menos um lance, o sistema irá oferecer o excedente para o maior lance e então irá queimar todos os tokens de protocolo recolhidos.

11. Gestão de Índices de Excedente

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

- O mecanismo de contabilidade, usado para acionar os leilões de dívida (Seção 9.2) e excedente (Seção 10.1)
- A tesouraria excedente, usada para financiar os principais componentes da infraestrutura e incentivar atores externos a manterem o sistema

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

- Módulo oráculo (Seção 6). Dependendo de como um oráculo é estruturado, a tesouraria paga oráculos de governança incluídos na lista de permissões, fora da rede, ou paga por chamadas para redes oraculares. A tesouraria também pode ser definida 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 equipes que colocam na lista de permissões novos tipos de garantia ou ajustam o definidor de taxas do sistema (Seção 4.2)

A tesouraria pode ser definida para que alguns recebedores de excedentes automaticamente tenham financiamento negado no futuro, e outros poderão pegar seus lugares.

12. Atores Externos

O sistema depende de atores externos para funcionar apropriadamente. Esses atores são economicamente incentivados a participar em áreas como leilões, processamento de liquidação global, criação de mercado e atualizar feeds de preço para manter a saúde do sistema.

Nós providenciaremos interfaces de usuários iniciais e scripts automatizados para permitir que o maior número de pessoas possíveis mantenha o protocolo seguro.

13. Mercado Endereçável

Nós vemos RAI sendo útil em duas principais áreas:

- Diversificação de portfólio: investidores usam RAI para diminuir a exposição a um ativo como ETH sem todo o risco de realmente manter o Ether
- Garantia para ativos sintéticos: RAI pode oferecer a protocolos como UMA, MakerDAO e Synthetix uma exposição menor ao mercado criptográfico e oferecer aos usuários mais tempo para sair de suas posições no caso de cenários como a Black Thursday de março de 2020, quando ativos criptográficos de milhões de dólares foram liquidados

14. Pesquisas Futuras

Para aumentar os limites do dinheiro descentralizado e trazer mais inovação nas finanças descentralizadas, nós iremos continuar a procurar alternativas em áreas principais como minimização de governança e mecanismos de liquidação.

Primeiro, queremos estabelecer as bases para futuros padrões acerca de protocolos que bloqueiam a si mesmos dos controles externos e para verdadeiros “robôs de dinheiro” que

se adaptam em resposta às forças do mercado. Em seguida, nós convidamos a comunidade Ethereum para debater e projetar melhorias acerca de nossas propostas com um foco específico em garantias e leilões de dívidas.

15. Riscos e Mitigação

Existem muitos riscos envolvidos em desenvolver e lançar um índice de reflexo, assim como sistemas subsequentes que são construídos no topo:

● Bugs de contratos inteligentes: o maior risco para o sistema é a possibilidade de um bug que permite que qualquer um extraia toda a garantia ou bloqueie o protocolo em um estado do qual não seja possível haver recuperação. Nós planejamos ter nosso código revisado por múltiplos pesquisadores de segurança e lançar o sistema em uma rede de teste antes de nos comprometermos a implantá-lo em produção

● Falha de oráculo: nós agregaremos feeds de múltiplas redes de oráculo e haverá regras rígidas para atualizar apenas um oráculo por vez, assim, governanças maliciosas não poderão introduzir preços falsos com facilidade

● Eventos de garantia de cisne negro: existe o risco de um evento de cisne negro na garantia subjacente, que pode resultar em uma grande quantidade de SAFEs liquidados. Liquidações podem não ser capazes de cobrir inteiramente a dívida inadimplente pendente, então o sistema irá mudar de forma contínua seu armazenamento excedente para cobrir uma quantidade decente de débito emitido e resistir a choques de mercado

● Parâmetros impróprios de definidor de taxas: mecanismos de feedback autônomos são altamente experimentais e podem não se comportar exatamente como nós previmos durante as simulações. Nós planejamos permitir que a governança ajuste esse componente (enquanto ainda estiver limitado) para evitar cenários inesperados

● Falha em iniciar um mercado liquidante saudável: liquidatários são atores vitais que garantem que todos os débitos emitidos sejam cobertos pela garantia. Nós planejamos

criar interfaces e scripts automatizados para que a maior quantidade de pessoas possíveis possa participar na segurança do sistema.

16. Sumário

Nós propomos um protocolo que progressivamente bloqueia a si mesmo do controle humano e emite um ativo de garantia chamado índice de reflexo. Primeiramente, apresentamos o mecanismo autônomo feito para influenciar o preço de mercado do índice e então descrevemos como inúmeros contratos inteligentes podem limitar o poder que titulares de tokens possuem sobre o sistema. Delineamos um esquema autossustentável para medianizar feeds de preço de múltiplas redes de oráculo independentes, e então, encerramos apresentando o mecanismo geral para cunhar índices e liquidar SAFEs.

17. 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

18. Glossário

Índice de Reflexo: um ativo de garantia que amortece a 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 (calculada por RRFM), no caso de o preço de mercado não estiver próximo a ela. Pensado para influenciar criadores SAFE a gerar mais ou pagar algumas de suas dívidas

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

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

Configurador do Mercado Monetário (MMS): um mecanismo similar ao RRFM que puxa múltiplas alavancas monetárias de uma vez. No caso dos índices de reflexo, ele modifica a taxa de empréstimo e o preço de resgate

Medianizador de Rede para Oráculo (ONM): um contrato inteligente que extrai preços de múltiplas redes de oráculo (que não são controladas pela governança) e as medianiza se uma maioria (exemplo: 3 de 5) retornou com um resultado sem lançar

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

Era do Gelo de Governança: contrato imutável que bloqueia a maioria dos componentes de um protocolo de intervenção exterior depois que uma certa data limite tenha passado

Mecanismo de Contabilidade: componente do sistema que aciona débito e leilões de excedente. Ele também rastreia a quantidade de dívida leiloada atual, dívida inadimplente não leiloada e o armazenamento excedente

Armazenamento Excedente: quantidade de juros a acumular e manter no sistema. Quaisquer juros acumulados acima desse limite são vendidos em leilões de excedente que queimam tokens de protocolo

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