DeFi エコシステムの担保

Stefan C. Ionescu、Ameen Soleimani

2020 年 5月

概要

ネイティブの担保資産の目標値を変更するために市場の力に自動的に反応する、ガバナンスが最小化された分散型プロトコルを提示します。このプロトコルにより、誰もが自分の暗号資産を活用し、原資産の担保の湿ったバージョンである「反射インデックス」を発行することができます。インデックスが、保有者やその他の分散型金融プロトコルを突然の市場の変化から保護できる、普遍的でボラティリティの低い担保としてどのように役立つかについて概説します。インフラストラクチャを活用して、他のチームが独自のシンセティックスを立ち上げるのを支援する計画を提示します。最後に、多くの DeFi プロトコルによく見られる現在のオラクルおよびガバナンス構造に代わるものを提供します。

コンテンツ

序章

お金は、人類が繁栄するために活用する最も強力な調整メカニズムの 1 つです。マネーサプライを管理する特権は、歴史的に、無意識の一般大衆に課されている間、主権指導者と金融エリートの手に委ねられてきました。ビットコインが草の根の抗議が価値のある商品資産を明示する可能性を示した場合、イーサリアムは、ボラティリティから保護され、担保として使用されるか、参照価格に固定される資産担保合成機器を構築するためのプラットフォームを提供します日常の取引の交換手段として使用され、すべて分散型コンセンサスの同じ原則によって実施されます。

イーサリアムに富と適切に分散化された合成機器を保管するためのビットコインへの許可のないアクセスは、次の金融革命の基盤を築き、現代の金融システムの周辺にいる人々に新しい金融システムの構築を調整する手段を提供します。

このホワイトペーパーでは、他の合成繊維の繁栄を支援し、分散型金融業界全体の主要なビルディングブロックを確立する新しい資産タイプであるリフレックスインデックスを構築するためのフレームワークを紹介します。

反射指数の概要

反射指数の目的は、特定のペグを維持することではなく、担保のボラティリティを弱めることです。インデックスにより、実際の暗号資産を保有するのと同じ規模のリスクなしに、誰でも暗号通貨市場に触れることができます。私たちの最初の反射指数である RAI は、システムに ETH などの不安定な資産は、大幅な市場の変化が発生した場合に、ユーザーがポジションを終了するためのより多くの時間を提供します。

反射指数を理解するために、それらの償還価格の振る舞いをステーブルコインの価格の振る舞いと比較することができます。

償還価格は、システム内の 1 つの債務単位（またはコイン）の価値です。これは内部会計ツールとしてのみ使用されることを意図しており、市場価格（市場がコインを取引している値）とは異なります。法定紙幣の場合

USDC などのステーブルコインの場合、システムオペレーターは、誰でも 1 つのコインを
1米ドルに交換できると宣言しているため、これらのコインの償還価格は常に 1 つです。
MakerDAO の MultiCollat eral DAI（MCD）のように、システムが 1米ドルの固定ペグを
対象としているため、償還価格も 1 に固定されている、暗号通貨で裏付けられたステーブルコインの場合もあります。

ほとんどの場合、ステーブルコインの市場価格とその償還価格には差があります。これらのシナリオは、市場価格が償還よりも高い場合にトレーダーがより多くのコインを作成し、市場価格が償還価格よりも低い場合にステーブルコインを担保（USDC の場合は米ドルなど）に償還する裁定取引の機会を生み出します。

反射指数は、システムが目標とする償還価格もあるため、ステーブルコインに似ています。彼らの場合の主な違いは、彼らの償還は固定されたままではなく、市場の力の影響を受けながら変化するように設計されているということです。セクション 4 では、インデックスの償還価格がどのように変動し、ユーザーに新しい裁定取引の機会を生み出すかについて説明します。

デザイン哲学と市場開拓戦略

私たちの設計哲学は、セキュリティ、安定性、配信速度を優先することです。

マルチコラテラル DAI は、RAI の設計を繰り返すための自然な場所でした。システムは徹底的に監査され、正式に検証されており、外部への依存は最小限であり、専門家の活発なコミュニティが集まっています。開発と通信の労力を最小限に抑えるために、実装を実現するために、元の MCD コードベースに最も単純な変更のみを加えたいと考えています。

最も重要な変更には、自律レートセッター、多くの独立した価格フィードと統合された Oracle Network Medianizer、およびシステムを人間の介入から可能な限り分離することを目的としたガバナンス最小化レイヤーの追加が含まれます。

プロトコルの最初のバージョン（ステージ 1）には、レートセッターとコアアーキテクチャのその他のマイナーな改善のみが含まれます。セッターが期待どおりに機能することを証明したら、オラクルメディアナイザー（ステージ 2）とガバナンス最小化レイヤー（ステージ 3）をより安全に追加できます。

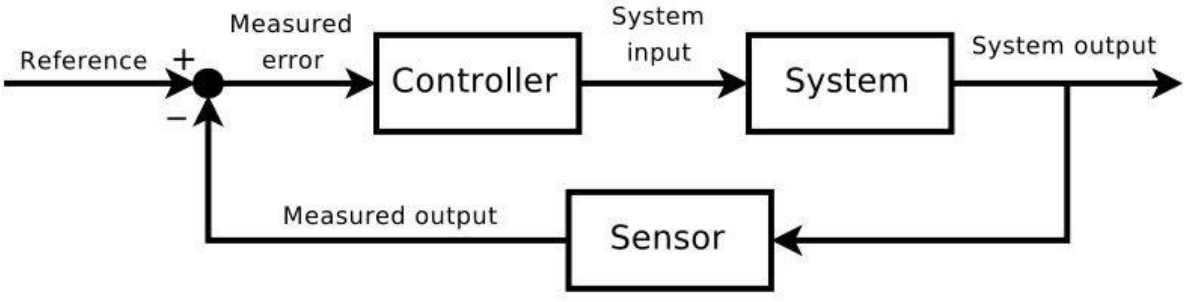
金融政策のメカニズム

制御理論入門

ほとんどの人が精通している一般的な制御システムの 1 つは、シャワーです。誰かがシャワーを浴び始めるとき、彼らは、制御理論では、と呼ばれる望ましい水温を念頭に置いています基準設定値。。 として行動する人コントローラー、水流温度を継続的に測定します（これはシステムと呼ばれます 出力）。。 a。 nd は、シャワーのノブを回す速度を変更します。 偏差（またはエラー）希望の温度と現在の温度の間。ノブを回す速度をシステムと呼びます入力。 T。 目的は、基準設定値にすばやく到達するのに十分な速さでノブを回すことですが、温度ほど速くはありません オーバーシュート。システムがある場合ショック 水流の温度が急激に変化する場合、人は外乱に応じてノブをどれだけ速く回すかを知ることにより、現在の温度を維持できるはずです。

動的システムの安定性を維持する科学分野は制御理論と呼ばれ、自動車、フライトナビゲーション、化学反応器、ロボットアーム、およびあらゆる種類の工業プロセスのクルーズコントロールに幅広く適用されています。可変ハッシュレートにもかかわらず、10 分の平均ブロック時間を維持するビットコイン難易度調整アルゴリズムは、ミッションクリティカルな制御システムの例です。

最新の制御システムでは、アルゴリズム 。コントローラ 通常はプロセスに組み込まれ、システム出力（車の速度など）と設定値（クルーズコントロール速度など）の間の偏差に基づいてシステム入力（車のアクセルペダルなど）を自動的に更新するために、システム入力（車のアクセルペダルなど）を制御します。 ）。



最も一般的なタイプのアルゴリズムコントローラーは PID コントローラー。。 産業用アプリケーションの 95%以上と幅広い生物学的システムが PID の要素を採用しています

コントロール[4]。PID コントローラーは、3 つの部分からなる数式を使用して、その出力を決定します。

コントローラ出力=比例項+積分項+微分項

比例項は、直接であるコントローラーの一部です。比例偏差に。偏差が大きくて正の場合（たとえば、クルーズコントロール速度の設定値が車の現在の速度よりもはるかに高い場合）、比例応答は大きくて正になります（たとえば、アクセルペダルを床に置きます）。

積分項は、偏差が持続した期間を考慮に入れるコントローラーの一部です。それはを取ることによって決定されます積分 時間の経過に伴う偏差の増加とそれは主に排除するために使用されます定常状態エラー。これは、設定値からの永続的な偏差ではありますが、小さな応答のために蓄積されます（たとえば、クルーズコントロールの設定値が数分間車の速度より 1 mph高くなっています）。

微分項は、偏差がどれだけ速く拡大または縮小するかを考慮に入れるコントローラーの一部です。それはを取ることによって決定されますデリバティブ 偏差を測定し、偏差が大きくなっているときにコントローラーの応答を加速するのに役立ちます（たとえば、クルーズコントロールの設定値が車の速度よりも高く、車が減速し始めた場合は速度を上げます）。また、偏差が縮小しているときにコントローラーの応答を減速することにより、オーバーシュートを減らすのに役立ちます（たとえば、車の速度がクルーズコントロールの設定値に近づき始めたら、ガスを緩和します）。

これらの 3 つの部分を組み合わせることで、それぞれを個別に調整できるため、PID コントローラーはさまざまな制御システムアプリケーションを柔軟に管理できます。

PID コントローラーは、応答時間にある程度の遅れがあり、システムが安定しようとするときに設定値の周りでオーバーシュートや振動が発生する可能性があるシステムで最適に機能します。RAI のようなリフレックスインデックスシステムは、PID コントローラーによって償還価格を変更できるこのタイプのシナリオに適しています。

より一般的には、最近、現在の中央銀行の金融政策ルール（テイラールールなど）の多くが実際には PID の近似値であることが発見されました。
コントローラ[5]。

償還率フィードバックメカニズム

償還率フィードバックメカニズムは、反射指数の償還価格の変更を担当するシステムコンポーネントです。それがどのように機能するかを理解するために、最初に、システムが手動制御を使用するのではなくフィードバックメカニズムを必要とする理由とメカニズムの出力が何であるかを説明する必要があります。

フィードバックメカニズムコンポーネント

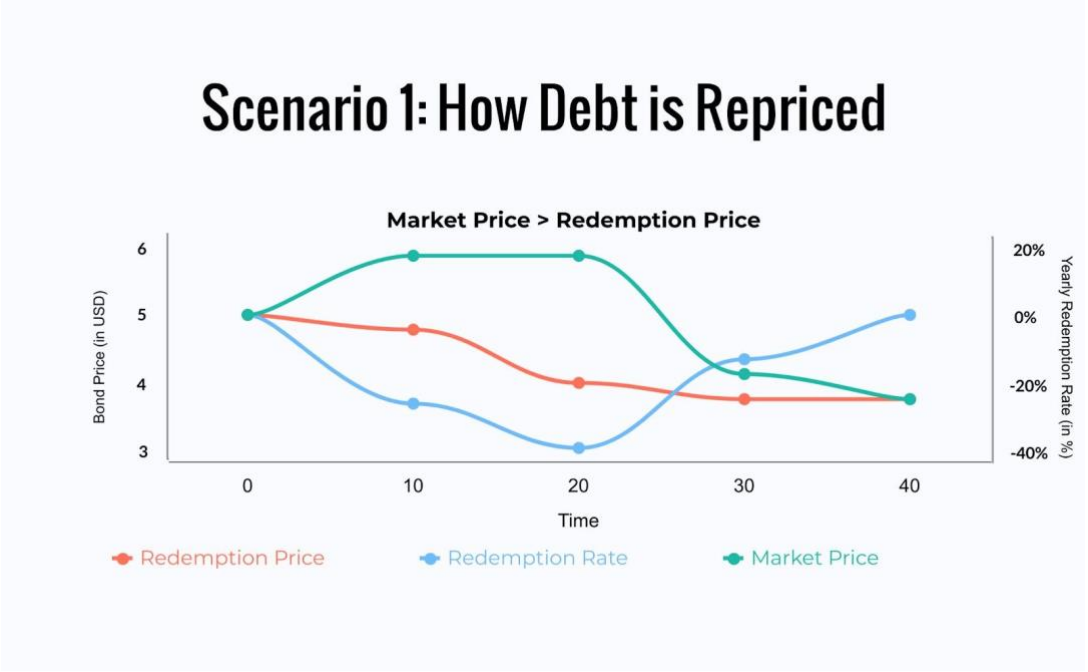
理論的には、インデックスのユーザーに影響を与え、最終的にインデックスの市場価格を変更するために、リフレックスインデックスの償還価格（セクション 2 で説明）を直接操作することが可能です。実際には、この方法はシステム参加者に望ましい効果をもたらしません。SAFE 保有者の観点からすると、償還価格が 1 回だけ引き上げられた場合、債務単位あたりのより高い価格を受け入れ、担保比率の低下による損失を吸収し、ポジションを維持する可能性があります。ただし、償還価格が時間の経過とともに上昇し続けると予想する場合は、予想される将来の損失を回避する傾向が強くなり、債務を返済してポジションを閉じることを選択する可能性があります。

リフレックスインデックスシステムの参加者は、償還価格の変更に直接応答するのではなく、代わりに応答することを期待しています償還価格の変動率 これを償還率。償還率はによって設定されますフィードバックメカニズム そのガバナンスは、微調整するか、完全に自動化することができます。

フィードバックメカニズムのシナリオ

フィードバックメカニズムは、償還率を使用して市場の力の変化に対抗することにより、償還価格と市場価格の間の均衡を維持することを目的としていることを思い出してください。これを達成するために、償還率は、市場価格と償還価格の間の偏差に対抗するように計算されます。

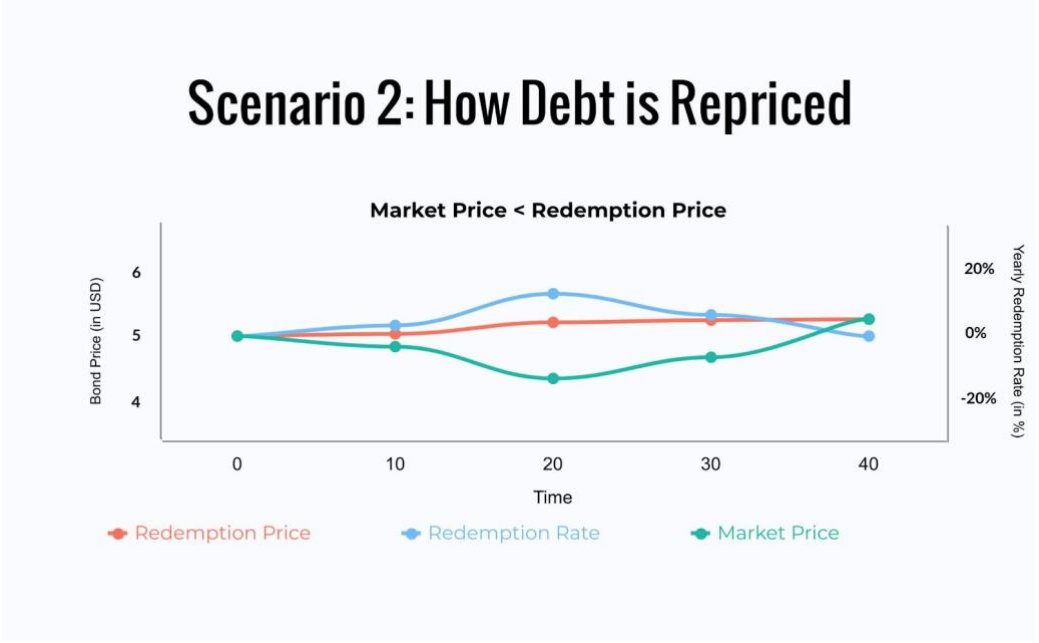
以下の最初のシナリオでは、インデックスの市場価格が償還価格よりも高い場合、メカニズムは負のレートを計算し、償還価格を下げ始め、システムの負債を安くします。



償還価格の低下が予想されるため、人々はインデックスを保有することを思いとどまり、SAFE 保有者は（担保価格が変わらない場合でも）より多くの債務を生成し、それを市場で販売することで、需要と供給のバランスをとることができます。これは、インデックスホルダーがフィードバックメカニズムに応答して迅速に反応する理想的なシナリオであることに注意してください。実際には（そして特にローンチ後の初期には）、メカニズムのキックオフと実際の結果との間で、発行された債務の額とその後の市場価格に遅れが生じると予想されます。

一方、シナリオ 2 では、インデックスの市場価格が償還価格よりも低い場合、レートは正になり、すべての債務の価格を再設定し始めて、より高価になります。

債務が高額になると、すべての SAFE の担保比率が低下し（したがって、SAFE の作成者は債務を返済するように促されます）、ユーザーは、価値が上がることを期待してインデックスを蓄え始めます。



フィードバックメカニズムアルゴリズム

次のシナリオでは、プロトコルが比例積分コントローラーを使用して償還率を計算すると仮定します。

●● リフレックスインデックスは、任意の償還価格「ランド」で開始されます

●● ある時点で、インデックスの市場価格は「ランド」から「ランド」+ x に上昇します。フィードバックメカニズムが新しい市場価格を読み取った後、比例項を計算します p、。 この場合、これは-1 *（（ 'rand' + x）/ 'rand'）です。償還価格を下げ、次にインデックスの価格を変更してインデックスを安くするために、比例は負になります

●● 比例を計算した後、メカニズムは積分項を決定します私は 最後からの過去のすべての偏差を追加することによって偏差間隔 秒

●● このメカニズムは、比例と積分を合計し、1 秒あたりの償還率を計算します r それはゆっくりと償還価格を下げ始めます。SAFE クリエイターは、より多くの債務を生み出すことができることに気付くと、より多くのインデックスで市場を氾濫させます。

- 後 n 秒、メカニズムは、市場価格と償還価格の間の偏差が無視できることを検出します（指定されたパラメーターの下で ノイズ）。この時点で、アルゴリズムは r をゼロに設定し、償還価格を現在の場所に維持します

実際には、アルゴリズムはより堅牢になり、いくつかの変数を不変にします（例：ノイズ パラメータ、偏差間隔）または、ガバナンスが変更できるものには厳しい制限があります。

フィードバックメカニズムの調整

反射指数システムが適切に機能するために最も重要なのは、アルゴリズムのコントローラーパラメーターの調整です。不適切なパラメータ設定は、システムが遅すぎて安定性を達成できない、大幅にオーバーシュートする、または外部からの衝撃に直面して一般的に不安定になる可能性があります。

PID コントローラーの調整プロセスには、通常、ライブシステムの実行、調整パラメーターの調整、およびシステムの応答の観察が含まれ、多くの場合、途中で意図的にショックが発生します。ライブリフレックスインデックスシステムのパラメーターを微調整することの難しさと経済的リスクを考慮して、初期パラメーターを設定するために可能な限りコンピューターモデリングとシミュレーションを活用する予定ですが、本番環境からの追加データがある場合は、ガバナンスがチューニングパラメーターを更新できるようにします。それらが最適ではないことを示しています。

マネーマーケットセッター

RAI では、借入金利（インデックス生成時に適用される金利）を固定または上限を設定し、償還価格のみを変更することで、フィードバックメカニズムのモデル化に伴う複雑さを最小限に抑えることを計画しています。この場合の借入率は、マルチ担保 DAI の安定手数料と DSR のスプレッドに等しくなります。

借入金利は固定する予定ですが、短期金融市場セッターを利用して、償還価格と合わせて変更することが可能です。短期金融市場は、SAFE クリエーターが多かれ少なかれ債務を生み出すように動機付ける方法で、借入レートと償還価格を変更します。インデックスの市場価格が償還を上回っている場合、両方のレートが低下し始めますが、償還を下回っている場合、
料金が上がります。

グローバル決済

グローバル決済は、すべてのリフレックスインデックス保有者に償還価格を保証するために使用される最後の手段です。これは、リフレックスインデックス保有者と SAFE 作成者の両方が、システム担保をその正味額（最新の償還価格に応じた各担保タイプごとのインデックスの量）で償還できるようにすることを目的としています。一定量のプロトコルトークンを書き込んだ後、誰でも決済をトリガーできます。

決済には 3 つの主要なフェーズがあります。

●● **引き金**：決済がトリガーされ、ユーザーは SAFE を作成できなくなり、すべての担保価格フィードと償還価格が凍結されて記録されます

●● **プロセス**：すべての未処理のオークションを処理します

●● **請求**：すべてのリフレックスインデックス保有者と SAFE 作成者は、インデックスの最後に記録された償還価格に基づいて、任意のシステム担保の固定額を請求できます

ガバナンス

パラメータの大部分は不変であり、ガバナントークンの所有者がまったく新しいシステムを展開しない限り、内部のスマートコントラクトの仕組みはアップグレードできません。この戦略を選択したのは、人々が自分の利益のためにガバナンスプロセスに影響を与えようとするメタゲームを排除し、システムへの信頼を損なう可能性があるためです。私たちは、人間をあまり信頼せずにプロトコルの適切な動作を確立し（「ビットコイン効果」）、社会的スケーラビリティを最大化し、RAI を自分のプロジェクトのコアインフラストラクチャとして使用したい他の開発者のリスクを最小化します。

変更できるいくつかのパラメーターについては、考えられるすべてのシステム変更を遅延または制限することを目的とした制限付きガバナンスモジュールの追加を提案します。さらに、Governance Ice Age を紹介します。これは、特定の期限が過ぎた後、システムの一部を外部の制御からロックできる権限レジストリです。

時間制限のあるガバナンス

Time Bounded Governance は、Restricted GovernanceModule の最初のコンポーネントです。同じパラメータに適用される変更の間に時間遅延を課します。例としては、少なくとも Oracle Network Medianizer（セクション 6.2）で使用されるオラクルのアドレスを変更する可能性があります。T s。 前回のオラクルの変更以降、econds は経過しています。

制限付きガバナンスモジュールの 2 番目のコンポーネントは、アクション制限付きガバナンスです。すべての管理可能なパラメーターには、設定できる値と、特定の期間に変更できる値に制限があります。注目すべき例は、ガバナントークン保有者が微調整できる償還率フィードバックメカニズム（セクション 4.2）の初期バージョンです。

ガバナンス氷河期

Ice Age は、特定のシステムパラメータの変更とプロトコルのアップグレードに期限を課す不変のスマートコントラクトです。これは、プロトコルがそれ自体をロックして外部の介入を拒否する前に、ガバナンスがバグを修正できることを確認したい場合に使用できます。Ice Age は、パラメータの名前と影響を受ける契約のアドレスを期限のレジストリと照合することにより、変更が許可されているかどうかを確認します。期限が過ぎると、通話は元に戻ります。

プロトコルがそれ自体をロックし始める日付の近くにバグが見つかった場合、ガバナンスは IceAge を一定の回数遅らせることができる場合があります。たとえば、Ice Age は 1 か月ごとに 3 回しか遅延できないため、新しく実装されたバグ修正は適切にテストされます。

ガバナンスが必要なコアエリア

特にこのフレームワークの初期バージョンでは、ガバナンスが必要になる可能性のある 4 つの領域を想定しています。

- **新しい担保タイプの追加**：RAI は ETH によってのみサポートされますが、他のインデックスは複数の担保タイプによってサポートされ、ガバナンスが可能になります
  時間の経過とともにリスクを分散させる

- **外部依存関係の変更**：システムが依存するオラクルと DEX はアップグレードできます。ガバナンスは、システムが適切に機能し続けるために、システムを新しい依存関係に向けることができます

- **レートセッターの微調整**：初期の金融政策管理者は、合理的な範囲内で変更できるパラメーターを持ちます（アクションと時間制限のあるガバナンスで説明されています）

●● **システムバージョン間の移行**： 場合によっては、ガバナンスは新しいシステムを展開し、プロトコルトークンを印刷する許可を与え、古いシステムからこの許可を取り消すことができます。この移行は、以下に概説する制限付き移行モジュールの助けを借りて実行されます制限付き移行モジュール

以下は、システムバージョン間で移行するための簡単なメカニズムです。

●● 同じプロトコルトークンがカバーする異なるシステムの数と、債務オークションでプロトコルトークンを印刷する許可を拒否できるシステムを追跡する移行レジストリがあります

●● ガバナンスが新しいシステムバージョンを展開するたびに、システムの債務オークション契約のアドレスを移行レジストリに送信します。ガバナンスは、システムによるプロトコルトークンの印刷を停止できるかどうかも指定する必要があります。また、ガバナンスはいつでも、1 つのシステムが常にトークンを印刷できるため、トークンがから移行されることはないと言うことができます。

●● 新しいシステムを提案してから古いシステムから許可を取り消すまでには、クールダウン期間があります。

●● オプションの契約は、印刷許可が拒否された後に古いシステムを自動的にシャットダウンするように設定できます。

移行モジュールは、特定のシステムに常にトークンを印刷できるようにする許可を自動的に与える IceAge と組み合わせることができます。

自動システムシャットダウン

プロトコルトークンを書き込む必要なしに、システムが自動的に検出し、その結果、それ自体で決済をトリガーできる場合があります。

●● **深刻な価格フィードの遅延**：システムは、1 つ以上の担保またはインデックス価格フィードが長期間更新されていないことを検出します

●● **システムの移行**：これはオプションの契約であり、ガバナンスが債務オークションメカニズムのプロトコルトークンを印刷する機能を撤回した瞬間からクールダ

ウン期間が経過した後にプロトコルをシャットダウンできます（制限付き移行モジュール、セクション 5.4.1）

- **一貫した市場価格の偏差**：システムは、インデックスの市場価格が バツ% 償還価格と比較して長い間逸脱している

ガバナンスは、制限されたまま、または Ice Age がシステムの一部をロックし始めるまで、これらの自律シャットダウンモジュールをアップグレードできます。

オラクル

システムが価格フィードを読み取る必要がある 3 つの主要な資産タイプがあります。インデックス、プロトコルトークン、およびすべてのホワイトリストに登録された担保タイプです。価格フィードは、ガバナンス主導のオラクルまたはすでに確立されているオラクルネットワークによって提供できます。

ガバナンス主導のオラクル

ガバナントークンの所有者またはプロトコルを開始したコアチームは、複数の価格フィードをオフチェーンで収集し、すべてのデータポイントを仲介するスマートコントラクトに単一のトランザクションを送信する他のエンティティと提携できます。

このアプローチにより、信頼性が犠牲になりますが、Oracle インフラストラクチャのアップグレードと変更の柔軟性が高まります。

Oracle Network Medianizer

オラクルネットワークメディアナイザーは、ガバナンスによって直接制御されていない複数のソースから価格を読み取り（たとえば、インデックス担保タイプと他のステーブルコインの間のユニスワップ V2 プール）、すべての結果。ONM は次のように機能します：

- 私たちの契約は、担保価格を要求するために呼び出すことができるホワイトリストに登録されたオラクルネットワークを追跡します。契約は、システムが発生する余剰の一部によって資金が供給されます（余剰財務、セクション 11 を使用）。各オラクルネットワークは特定のトークンを支払いとして受け入れるため、契約では各リクエストに必要なトークンの最小量とタイプも追跡されます

●● システムに新しい価格フィードをプッシュするには、すべてのオラクルを事前に呼び出す必要があります。オラクルを呼び出すとき、コントラクトは最初にいくつかの安定料金をオラクルが受け入れたトークンの 1 つと交換します。オラクルが呼び出された後、コントラクトは呼び出しに「有効」または「無効」のタグを付けます。呼び出しが無効な場合、他のすべての Oracle が呼び出され、コントラクトが有効な過半数があるかどうかを確認するまで、特定の障害のある Or acle を再度呼び出すことはできません。有効なオラクル呼び出しは元に戻してはならず、最後にチェーンに投稿された価格を取得する必要があります m 秒。「取得」とは、各 Oracle タイプに応じて異なる意味を持ちます。

○○すぐに結果を得ることができるプルベースのオラクルの場合、契約は料金を支払い、直接価格を取得する必要があります

○○プッシュベースのオラクルの場合、契約は料金を支払い、オラクルを呼び出し、特定の期間待機する必要があります n 要求された価格を取得するためにオラクルを再度呼び出す前に

●● すべての Oracle の結果は配列に保存されます。ホワイトリストに登録されたすべてのオラクルが呼び出され、アレイに過半数を形成するのに十分な有効なデータポイントがある場合（たとえば、契約が 3/5 のオラクルから有効なデータを受け取った場合）、結果が並べ替えられ、契約が中央値を選択します

●● コントラクトが過半数を検出したかどうかに関係なく、オラクルの結果を含む配列はクリアされ、コントラクトは待機する必要があります p プロセス全体を最初からやり直す数秒前

Oracle Network Ba ckup

ガバナンスは、メディアナイザーが有効な Oracle ネットワークの過半数を連続して数回見つけることができない場合に、システムの価格を押し上げ始めるバックアップ Oracle オプションを追加できます。

メディアナイザーを展開するときは、後で変更できないため、バックアップオプションを設定する必要があります。さらに、別のコントラクトは、バックアップがメディア化メカニズムを長期間置き換えているかどうかを監視し、プロトコルを自動的にシャットダウンすることができます。

金庫

インデックスを生成するために、誰でも金庫内に暗号担保を預けて活用することができます。SAFE が開かれている間、SAFE は、預け入れられた担保の借入金利に応じて債務

を発生させ続けます。SAFE の作成者が債務を返済するにつれて、ロックされた担保をますます引き出すことができるようになります。

安全なライフサイクル

反射インデックスを作成し、その後 SAFE の債務を返済するために必要な 4 つの主要なステップがあります。

●● SAFE に担保を預ける

ユーザーはまず、新しい SAFE を作成し、その中に担保を預ける必要があります。

●● SAFE の担保に裏打ちされたインデックスを生成する

ユーザーは、生成するインデックスの数を指定します。システムは、担保の借入率に応じて発生し始める同額の債務を作成します。

●● 安全な債務を返済する

SAFE の作成者が担保を引き出したい場合は、初期債務と未収利息を返済する必要があります。

●● 担保を撤回する

ユーザーが債務の一部または全部を返済した後、担保を引き出すことができます。

安全な清算

システムの支払能力を維持し、未払いの債務全体の価値をカバーするために、各 SAFE は、担保比率が特定のしきい値を下回った場合に清算することができます。誰でも清算をトリガーできます。その場合、システムは SAFE の担保を没収し、売却します。担保オークション。

清算保険

システムの 1 つのバージョンでは、SAFE 作成者はを選択するオプションを持つことができます引き金 彼らの SAFE が清算されたときのために。トリガーは、SAFE に担保を自動的に追加し、清算から保護する可能性のあるスマートコントラクトです。トリガーの例としては、ショートポジションを販売する契約や、Nexus Mutual [6]などの保険プロトコルと通信する契約があります。

SAFE を保護する別の方法は、2 つの異なる担保しきい値を追加することです。安全な および危険。。 SAFE ユーザーは、安全なしきい値（リスクよりも高い）に達するまで債務を生成でき、SAFE の担保がリスクしきい値を下回った場合にのみ清算されます。

担保オークション

担保オークションを開始するには、システムは次の変数を使用する必要があります。清算量 すべてのオークションでカバーされる債務の金額と、それに対応する販売される担保の金額を決定するため。A 清算ペナルティ オークションにかけられたすべての SAFE に適用されます。

担保オークションパラメータ

パラメータ名	説明
minimumBid	する必要があるコインの最小量 1 回の入札で提供される
割引	担保が販売されている割引
lowerCollat eralMedianDeviation	担保の中央値が比較できる最大下限偏差オラクル価格
upperCollat eralMedianDeviation	担保の中央値が比較できる最大上限偏差オラクル価格
lowerSystemCoinMedianDeviation	システムコインオラクル価格フィードが持つことができる最大下限偏差システムコインオラクルと比較して価格
upperSystemCoinMedianDeviation	担保の中央値が比較できる最大上限偏差システムコインオラクル価格
minSystemCoinMedianDeviation	システムコインの最小偏差 取得するための償還価格と比較した結果の中央値 中央値を考慮に入れる

担保オークションメカニズム

固定割引オークションは、不良債権の決済に使用されるシステムコインと引き換えに担保を売りに出すための簡単な方法です（英語のオークションと比較して）。入札者は、オークションハウスが彼らの safeEngine.coinBalance その後、呼び出すことができます BuyCollat eral 彼らを交換するために最新の記録された市場価格と比較して割引価格で販売される担保用のシステムコイン。

入札者は、電話をかけることで、特定のオークションから取得できる担保の金額を確認することもできます。 getCollat eralBought また getExplicitCollat eralBought 。ご了承ください getCollat eralBought は、読み取り（および更新）するため、ビューとしてマークされません。 オラクルリレーから getExplicitCollat eralBought を使用します lastReadRedemptionPrice 。

債務オークション

担保オークションが SAFE のすべての不良債権をカバーできず、システムに余剰準備金がない場合、誰でも債務オークションをトリガーできます。
債務オークションは、より多くのプロトコルトークン（セクション 10）を作成し、システムの残りの不良債権を無効にする可能性のあるインデックスにそれらを販売することを目的としています。

債務オークションを開始するには、システムは 2 つのパラメーターを使用する必要があります。

- ●initialDebtAuctionAmount ：ミントするプロトコルトークンの初期量オークション後
- ●債務オークション BidSize ：初期入札サイズ（提供する必要のあるインデックスの数交換 initialDebtAuctionAmount プロトコルトークン）

自律債務オークションパラメータ設定

デットオークションで作成されたプロトコルトークンの初期量は、ガバナンス投票によって設定することも、システムによって自動的に調整することもできます。自動化されたバージョンは、システムがプロトコルトークンとリフレックスインデックスの市場価格を読み取るオラクル（セクション 6）と統合する必要があります。次に、システムはプロトコルトークンの初期量を設定します（initialDebtAuctionAmount）それは債務オークション BidSize

インデックス。。initialDebtAuctionAmount入札を奨励するために、実際のプロトコル/インデックスの市場価格と比較して割引価格で設定することができます。

債務オークションパラメータ

パラメータ名	説明
amountSoldIncrease	プロトコルの量の増加 同じために鋳造されるトークンインデックスの量
bidDecrease	次の入札のプロトコルトークンの受け入れ量の最小減少同量のインデックス
bidDuration	新規入札後の入札期間 入札が送信されます（秒単位）
totalAuctionLength	オークションの全長（秒単位）
オークション開始	までに開始されたオークションの数今

債務オークションメカニズム

担保オークションとは対照的に、債務オークションには 1 つの段階しかありません。

：量を減decreaseSoldAmount（uint id、uint amountToBuy、uint bid）らす

一定量のインデックスと引き換えに受け入れられるプロトコルトークン。

入札がない場合、オークションは再開されます。再起動するたびに、システムは同じ量のインデックスに対してより多くのプロトコルトークンを提供します。新しいプロトコルトークンの量は次のように計算されます最後の TokenAmount *amountSoldIncrease / 100.オークションが決済された後、システムは最高入札者のトークンを作成します。

プロトコルトークン

前のセクションで説明したように、各プロトコルは、債務オークションを通じて作成されたトークンによって保護される必要があります。保護とは別に、トークンはいくつかのシステムコンポーネントを管理するために使用されます。また、プロトコルトークンの供給は、余剰オークションの使用により徐々に減少します。追加の資金が競売にかけられる前にシステ

ムに蓄積する必要がある余剰の量は、と呼ばれます surplusBuffer そしてそれは発行された総債務のパーセンテージとして自動的に調整されます。

保険基金

プロトコルトークンとは別に、ガバナンスは、さまざまな無相関資産を保持し、債務オークションのバックストップとして使用できる保険基金を作成できます。

余剰オークション

余剰オークションは、システムで発生したプロトコルトークンの安定料金を販売します。

余剰オークションパラメータ

パラメータ名	説明
bidIncrease	次の入札の最小増加
bidDuration	新しいオークション後のオークション期間 入札が送信されます（秒単位）
totalAuctionLength	オークションの全長（秒単位）
オークション開始	までに開始されたオークションの数今

余剰オークションメカニズム

余剰オークションには単一の段階があります。

増加 BidSize（uint id、uint amountToBuy、uint bid）：誰でもより高い金額で入札できます同量のインデックス（余剰）のプロトコルトークンの数。すべての新しい入札は、以上である必要があります lastBid *bidIncrease / 100.オークションは最大後に終了します totalAuctionLength 秒以降 bidDuration 最後の入札から数秒が経過し、その間に新しい入札は送信されていません。

入札がない場合、オークションは再開されます。一方、オークションに少なくとも 1 つの入札がある場合、システムは余剰分を最高入札者に提供し、収集されたすべてのプロトコルトークンを焼きます。

余剰インデックス管理

ユーザーがインデックスを生成し、暗黙的に債務を作成するたびに、システムはユーザーの SAFE に借入レートを適用し始めます。未収利息は、2 つの異なるスマートコントラクトにプールされます。

- ●● 。会計エンジン債務（セクション 9.2）と余剰（セクション 10.1）オークション
- ●● The 余剰財務 コアインフラストラクチャコンポーネントに資金を提供し、システムを維持するために外部の関係者にインセンティブを与えるために使用されます

余剰財務は、3 つのコアシステムコンポーネントへの資金提供を担当しています。

- ●● Oracle モジュール（セクション 6）。オラクルがどのように構成されているかに応じて、財務省はガバナンスのホワイトリストに登録されたオフチェーンオラクルを支払うか、オラクルネットワークへの呼び出しに対して支払います。オラクルを呼び出して更新するためにガスを使用したアドレスを支払うように財務を設定することもできます

- ●● 場合によっては、システムを維持する独立したチーム。例としては、新しい担保タイプをホワイトリストに登録したり、システムのレートセッターを微調整したりするチームがあります（セクション 4.2）。

一部の余剰受取人が将来自動的に資金提供を拒否され、他の受取人が代わりになるように、財務を設定することができます。

外部アクター

システムは、適切に機能するために外部のアクターに依存しています。これらの関係者は、システムの健全性を維持するために、オークション、グローバル決済処理、マーケットメイク、価格フィードの更新などの分野に参加するように経済的に動機付けられています。

できるだけ多くの人がプロトコルを安全に保つことができるように、初期ユーザーインターフェイスと自動スクリプトを提供します。

アドレス可能な市場

RAI は、次の 2 つの主要な領域で役立つと考えています。

- **ポートフォリオの多様化**：投資家は RAI を使用して、実際にイーサリアムを保有するリスクを冒すことなく、ETH などの資産へのエクスポージャーを抑制します

- **合成資産の担保**：RAI は、UMA、MakerDAO、Synthetix などのプロトコルを提供して、暗号市場への露出を減らし、数百万ドル相当の暗号資産があった 2020 年 3月のブラックサーズデイなどのシナリオの場合に、ユーザーがポジションを終了する時間を増やすことができます清算今後の研究分散型マネーの限界を押し広げ、分散型ファイナンスにさらなるイノベーションをもたらすために、ガバナンスの最小化や清算メカニズムなどのコア領域で代替案を探し続けます。

私たちはまず、外部の制御から身を守るプロトコルに関する将来の標準と、市場の力に応じて適応する真の「マネーロボット」の基礎を築きたいと考えています。その後、イーサリアムコミュニティに、担保と債務のオークションに特に焦点を当てて、提案に関する改善について議論し、設計するよう呼びかけます。

リスクと軽減

反射インデックスの開発と起動、およびその上に構築された後続のシステムには、いくつかのリスクが伴います。

- **スマートコントラクトのバグ**：システムにもたらされる最大のリスクは、誰もがすべての販促素材を抽出したり、プロトコルを回復できない状態でロックしたりする可能性があるバグの可能性です。コードを複数のセキュリティ研究者にレビューしてもらい、テストネットでシステムを起動してから、本番環境に導入する予定です。

- **Oracle の失敗**：複数のオラクルネットワークからのフィードを集約し、悪意のあるガバナンスが誤った価格を簡単に導入できないように、一度に 1 つのオラクルのみをアップグレードするための厳格なルールがあります

●● **付随的なブラックスワンイベント**：下にある担保にブラックスワンイベントが発生するリスクがあり、その結果、大量の清算された SAFE が発生する可能性があります。清算は未払いの不良債権全体をカバーできない可能性があるため、システムは、発行された債務のまともな金額をカバーし、市場のショックに耐えるために、余剰バッファーを継続的に変更します

●● **不適切なレートセッターパラメータ**：自律フィードバックメカニズムは非常に実験的であり、シミュレーション中に予測したとおりに動作しない場合があります。予期しないシナリオを回避するために、ガバナンスがこのコンポーネントを（制限されたままで）微調整できるようにする予定です。

●● **健全な清算人市場のブートストラップの失敗**：清算人は、発行されたすべての債務が担保でカバーされていることを確認する重要なアクターです。できるだけ多くの人がシステムの安全を維持するために参加できるように、インターフェースと自動スクリプトを作成する予定です。

概要

私たちは、人間のコントロールから徐々に自分自身をロックし、反射指数と呼ばれる低ボラティリティの担保資産を発行するプロトコルを提案しました。最初に、インデックスの市場価格に影響を与えることを目的とした自律メカニズムを紹介し、次に、いくつかのスマートコントラクトがトークン所有者がシステムに対して持つ力を制限する方法について説明しました。複数の独立したオラクルネットワークからの価格フィードを中央化するための自立したスキームの概要を説明し、インデックスの作成と SAFE の清算の
一般的なメカニズムを示して終了しました。

参考文献

[1]「メーカープロトコル：MakerDAO のマルチ担保ダイ（MCD）システム」、https://bit.ly/2YL5S6j

[2]「UMA：分散型金融契約プラットフォーム」、https://bit.ly/2Wgx7E1

[3] Synthetix Litepaper、https://bit.ly/2SNHxZO

[4]KJÅström、RM マレー、「フィードバックシステム：科学者とエンジニアのための紹介」、。 https://bit.ly/3bHwnMC

[5] RJ Hawkins、JK Speakes、DE Hamilton、「金融政策と PID 制御」、https://bit.ly/2TeQZFO

[6] H. Karp、R。Melbardis、「イーサリアムブロックチェーン上のピアツーピアの任意の相互」、https://bit.ly/3du8TMy

[7] H. Adams、N。Zinsmeister、D。Robinson、「Uniswap V2 Core」、https://bit.ly/3dqzNEU

用語集

反射指数：原資産のボラティリティを弱める担保資産

RAI：私たちの最初の反射指数

償還価格：システムがインデックスに持たせたい価格。市場価格がそれに近くない場合、償還率（RRFM によって計算される）の影響を受けて変化します。SAFE クリエイターに影響を与えて、より多くの収入を生み出したり、債務の一部を返済したりすることを目的としています

借入率：未払いの債務があるすべての SAFE に適用される年利

償還率フィードバックメカニズム（RRFM）：反射指数の市場価格と償還価格を比較し、SAFE 作成者にゆっくりと影響を与えて多かれ少なかれ債務を生成する償還率を計算する（そして暗黙的に市場/償還価格の偏差を最小化しようとする）自律メカニズム

マネーマーケットセッター（MMS）：複数の金銭的レバーを一度に引く RRFM と同様のメカニズム。リフレックスインデックスの場合、借入レートと償還価格の両方を変更します

Oracle Network Medianizer（ONM）：複数のオラクルネットワーク（ガバナンスによって制御されていない）から価格を引き出し、過半数（たとえば 5 つのうち 3 つ）がスローせずに結果を返した場合にそれらを中央化するスマートコントラクト

制限付きガバナンスモジュール（RGM）： ガバナンストークンの所有者がシステムに対して持つ力を制限する一連のスマートコントラクト。時間遅延を強制するか、ガバナンスが特定のパラメーターを設定しなければならない可能性を制限します

ガバナンス氷河期：特定の期限が過ぎた後、プロトコルのほとんどのコンポーネントを外部の介入からロックする不変の契約

会計エンジン：債務および余剰オークションをトリガーするシステムコンポーネント。また、現在オークションにかけられている債務、未処理の不良債権、および余剰バッファーの金額を追跡します。

余剰バッファー：システムに蓄積して保持する利息の額。興味がある
このしきい値を超えて発生したものは、プロトコルトークンを燃やす余剰オークションで販売されます

余剰財務：さまざまなシステムモジュールに未収利息を引き出す許可を与える契約（例：オラクルコールの ONM）