Rai：ボラティリティが低く、信頼が最⼩化されています

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

1.はじめに

2.反射指数の概要

3.設計哲学と市場開拓戦略

4.⾦融政策のメカニズム

4.1。制御理論⼊⾨

4.2。償還率フィードバックメカニズム

4.2.1。コンポーネント

4.2.2。シナリオ

4.2.3。アルゴリズム

1. 2.4。チューニング

4.3。マネーマーケットセッター

4.4。グローバル決済

5.ガバナンス

5.1。時間制限のあるガバナンス

5.2。アクションバウンドガバナンス

5.3。ガバナンス氷河期

5.4。ガバナンスが必要なコアエリア

1. 4.1。制限付き移⾏モジュール

6.⾃動システムシャットダウン

7.オラクル

7.1。ガバナンス主導のオラクル

7.2。Oracle Network Medianizer

7.2.1。Oracle Network Ba ckup

# 8.⾦庫

8.1。安全なライフサイクル

9.安全な清算

9.1。担保オークション

9.1.1。清算保険

9.1.2。担保オークションパラメータ

9.1.3。担保オークションメカニズム

9.2。債務オークション

9.2.1。⾃律債務オークションパラメータ設定

9.2.2。債務オークションパラメータ

1. 2.3。債務オークションメカニズム

10.プロトコルトークン

10.1。余剰オークション

1. 1.1。 余剰オークションパラメータ余

10.1.2。 剰オークションメカニズム

11.余剰インデックス管理

12.外部アクター

13.アドレス可能な市場

14.将来の研究

15.リスクと軽減

16.まとめ

17.参考⽂献

18.⽤語集

# 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

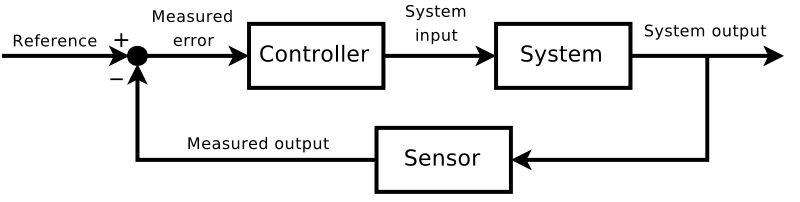
### 制御理論⼊⾨

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。

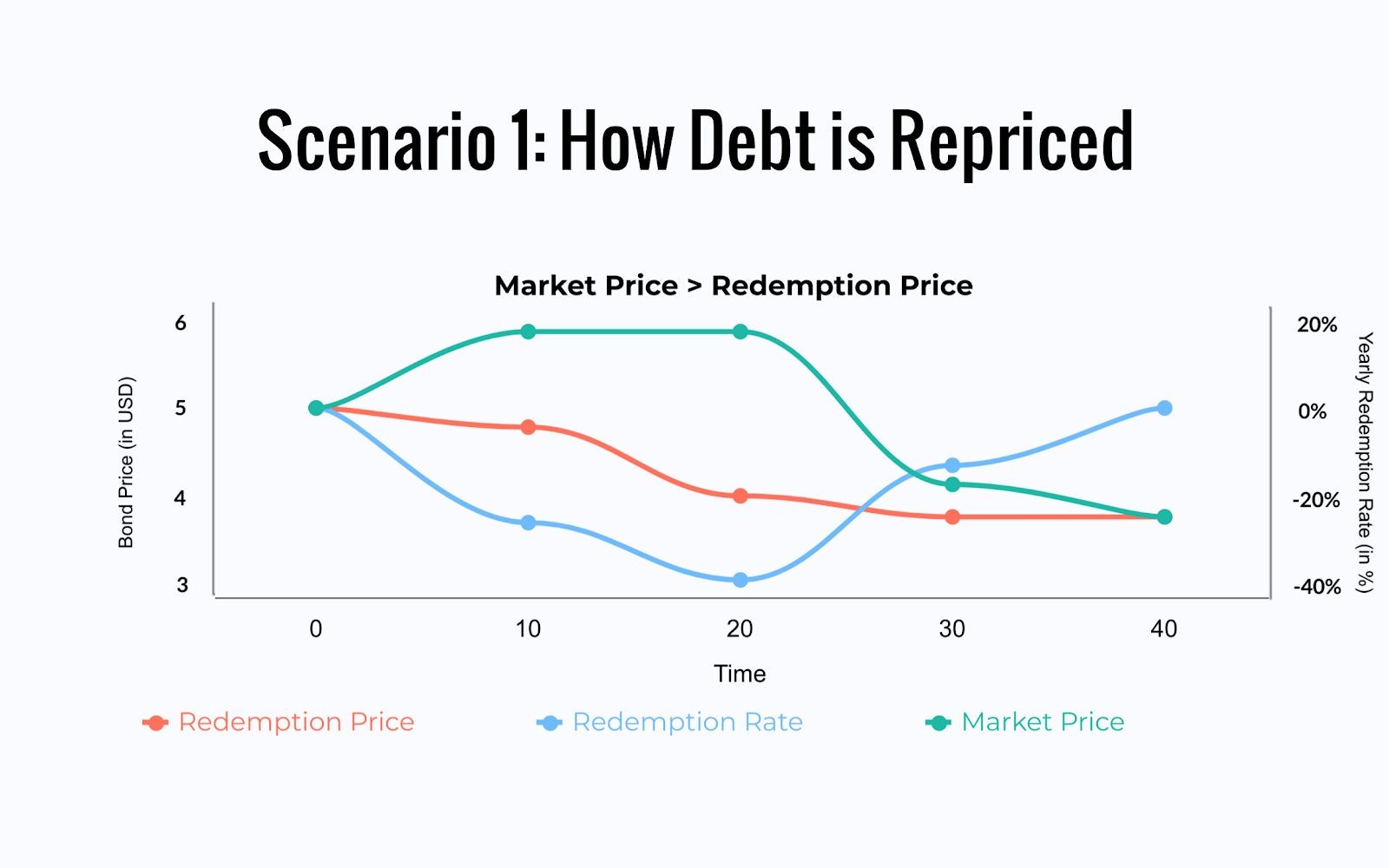
リフレックスインデックスシステムの参加者は、償還価格の変更に直接応答する

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。

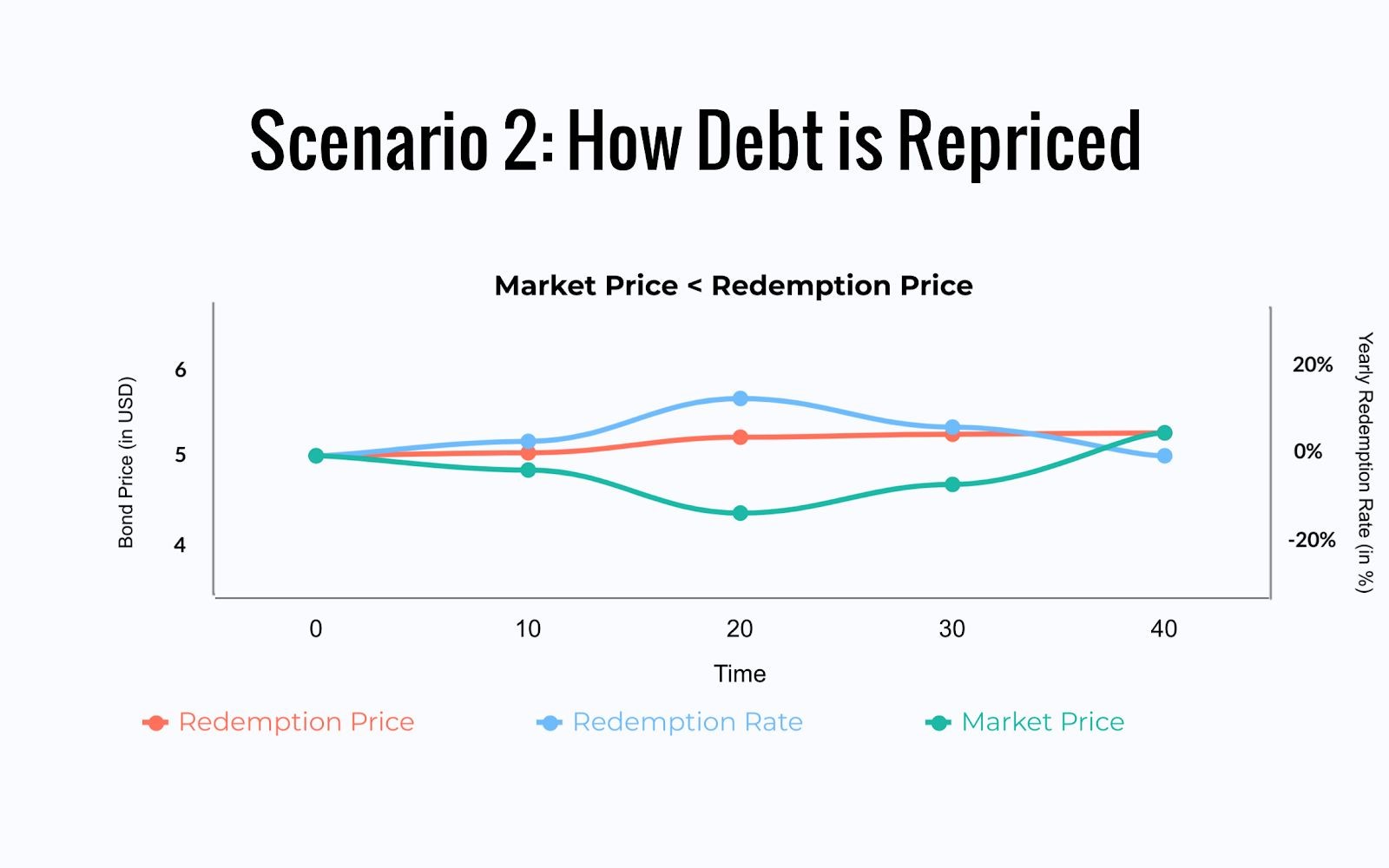
以下の最初のシナリオでは、インデックスの市場価格が償還価格よりも⾼い場合、メカニズムは負のレートを計算し、償還価格を下げ始め、システムの負債を安くします。



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、ガバナンス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。

アクションバウンドガバナンス

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、ガバナンス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⻑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⻑い間逸脱している

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

ガバナンス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⻑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 |
|  | 担保の中央値が⽐較できる最⼤下限 |
| lowerCollat eralMedianDeviation | 偏差オラクル価格 |
|  | 担保の中央値が⽐較できる最⼤上限 |
| upperCollat eralMedianDeviation | 偏差オラクル価格 |
|  | システムコインオラクル価格フィード |
| lowerSystemCoinMedianDeviation | 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 |
|  | 担保の中央値が⽐較できる最⼤上限 |
| upperSystemCoinMedianDeviation | 偏差システムコインオラクル価格 |
|  | システムコインの最⼩偏差 |
| minSystemCoinMedianDeviation | 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。

償還価格 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 |
|  | プロトコルの量の増加 |
| amountSoldIncrease | 同じために鋳造されるトークンインデックスの量 |
|  | 次の⼊札のプロトコルトークンの受 |
| bidDecrease | 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 | オークションの全⻑（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。

|  |
| --- |
| decreaseSoldAmount（uint id、uint amountToBuy、uint bid） |

：量を減らす

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 | オークションの全⻑（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/2YL5S6](https://bit.ly/2YL5S6j)j

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

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

[4]KJÅs[tröm、R](https://www.cds.caltech.edu/~murray/amwiki/index.php?title=Karl_J._%C3%85str%C3%B6m)M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」、 。ht[tps://bit.ly/3bHwnMC](https://bit.ly/3bHwnMC)

1. RJ Hawkins、JK Speakes、DE Hamilton、「⾦融政策とPID制御」、

[https://bit.ly/2TeQZF](https://bit.ly/2TeQZFO)O

1. 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](https://bit.ly/3du8TMy)

1. H. Adams、N。Zinsmeister、D。Robinson、「Uniswap V2 Core」、 [https://bit.ly/3dqzNE](https://bit.ly/3dqzNEU)U

# 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）