

Rai：低ボラティリティ、DeFiエコシステム の信頼が最小化された担保

Stefan C. Ionescu、Ameen Soleimani

2020年5月

要約。

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。

内容

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. 金融政策メカニム
 - 4.1. 制御理論の紹介
 - 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
 - 4.2.4. 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
 - 5.4.1. 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. Oracle
 - 7.1. ガバナンス主導のオラクル
 - 7.2. Oracle Network Medianizer
 - 7.2.1. Oracle Network Backup
8. 金庫
 - 8.1. SAFEライフサイクル
9. SAFE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. 担保オークションのメカニズム
- 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
 - 9.2.3. 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
 - 10.1.1. 余剰オークションパラタ
 - 10.1.2. 余剰オークションメカム
- 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

はじめに

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移されてきました。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。

リフレックスインデックスの概要リフレックスインデックス

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。裏打ちさ

USDCのような法定紙幣でれた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です。MakerDAOのマルチ

カタログ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。

設計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、納期のスピード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

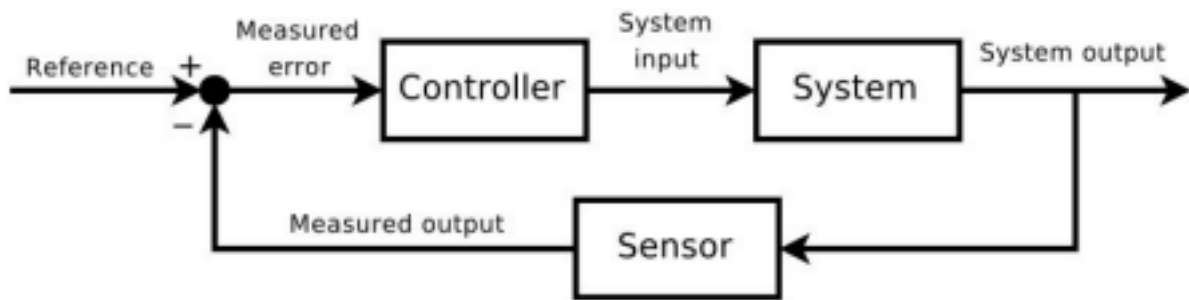
制御理論入門

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ます。彼らは理想的な水温を持っています。制御理論は、と呼ばれ基準設定値になります。

コントローラーとして機能する人 コントローラーは、
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）とに基づいてシャワーのノブを回す速度を変更します 偏差 （または
誤差目的の温度と現在の温度の間の）。での速度
ノブを回すとシステムと呼ばれ 入力され ます。 目的はノブを回すことです。
基準設定値にすばやく到達するのに十分な速さですが、 温度
オーバーシュート。 システム場合 ショック 水が流れるがある
温度が急激に変化した場合、人は現在を維持できるはずで
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って温度。

動的システムの安定性を維持する科学分野は、制御と呼ばれます。理論とそれは車のクルーズコントロール、飛行ナビゲーション、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。ビットコイン 10分の平均ブロック時間を維持する難易度調整アルゴリズム、可変ハッシュレートにもかかわらず、これ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のほとんどで、**アルゴリズムコントローラー** はは通常、プロセスとそれは順番にシステム入力（例えば車のアクセルペダル）の制御を与えられます **システム出力間の偏差に基づいて自動的に更新します**（例：車の速度）と設定値（クルーズコントロールの速度など）。



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*コントローラーです。の95%以上
 産業用アプリケーションおよび幅広い生物学的システムは、*PID*要素を採用して
 います
 制御の[4]。 *PID*コントローラーは、次の3つの部分からなる数式を使用します。
 その出力を決定します。

出力controller=比例項+積分項+微分項

比例項は、直接ているコントローラーの一部であります *比例し* に
 偏差。偏差が大きく正の場合（クルーズコントロール速度など）
 セットポイントは車の現在の速度よりはるかに高い） *比例*応答は
 大きくてポジティブ（例えば、アクセルペダルを床に置く）。

積分項は、コントローラーの一部であり、
 偏差が続いています。これはのとることによって決定され、積分
 、偏差をあらわします。 *時間とそれは主にを排除するために使用される*
定常状態のエラーです。 *順番にたまります*
 設定値からの永続的な逸脱ではあるが、小さなものに対応するため（例：クルー
 ズ 制御設定値は、数分間、車の速度より1 mph高くなっています）。

微分項は、どのくらいの速さかを考慮に入れるコントローラーの一部です
 偏差は拡大または縮小しています。それはの取ることによって決定されます
導関数 *を* *偏差があり、偏差が*
 成長している（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い
 場合は速度を上げる

そして車は減速し始めます）。また、減速することでオーバーシュートを減らすのに役立ちます。

偏差が縮小しているときのコントローラーの応答（たとえば、ガスを緩和する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ます）。

これらの3つの部分の組み合わせは、それぞれ独立して調整できます。

PIDコントローラーにさまざまな制御システムを管理する際の優れた柔軟性を提供します。

PIDコントローラーは、応答にある程度の遅れが生じるシステムで最適に機能します。時間だけでなく、設定値の周りのオーバーシュートと振動の可能性としてシステムはそれ自体を安定させようとします。RAIのような反射指数システムは償還価格をPIDで変更できるこのタイプのシナリオコントローラー。

より一般的には、現在の中央の多くが銀行の金融政策ルール（テイラールールなど）は、実際にはPID近似値ですコントローラーの[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、担当するシステムコンポーネントで反射指数の償還価格を変更します。それがどのように機能するかを理解するために、

最初に、システムがではなくフィードバックメカニズムを必要とする理由を説明する必要があります。手動制御とメカニズムの出力を使用します。

フィードバックメカニズムコンポーネント

理論的には、反射指数の償還を直接操作することは可能です。

インデックスユーザーに影響を与え、最終的に変更するための価格（セクション2で説明）

インデックスの市場価格。実際には、この方法では望ましい効果は得られません。
システム参加者について。SAFE保有者の観点から、償還の場合
価格は一度だけ上げられます。

彼らは債務単位あたりのより高い価格を受け入れるかもしれませんが、吸収します
担保比率の低下による損失とその地位の維持。もしも、彼らは償還価格が時間
とともに上昇し続けることを期待しています。彼らは
予想される将来の損失を回避する傾向があり、したがって支払うことを選択す
る可能性があります。彼らの借金を返済し、彼らの立場を閉じます。

リフレックスインデックスシステムの参加者は、変化に直接反応しないことを期
待しています。償還価格ですが、代わりに償還価格に対応し の変化率を
これと呼び 償還率ます。償還率はによって設定され フィードバックされます
メカニズム ガバナンスが微調整したり、完全に自動化できるようにする。

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、
償還率を使用して対抗することによる償還価格と市場価格
市場の力の変化。これを達成するために、償還率は次のように計算されます
市場価格と償還価格の間の偏差に反対します。

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よりも高い場合
価格、メカニズムは負のレートを計算し、それは減少し始めます
償還価格、したがってシステムの負債をより安くします。

Scenario 1: How Debt is Repriced



償還価格の低下への期待は、人々を落胆させる可能性があります

インデックスを保持し、SAFE保有者がより多くの債務を生成することを奨励します（担保価格は変更されません）これは市場で販売されるため、バランスが取れます

需要と供給を出します。これは、インデックス所有者がいる理想的なシナリオであることに注意してください

フィードバックメカニズムに応じて迅速に反応します。実際に（そして特に発売後の初期）メカニズムのキックオフと

発行された債務の額とその後の市場で見られる実際の結果 価格。

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、レートは正になり、すべての債務の価格を再設定し始めます。

それはより高価になります。

債務がより高額になると、すべてのSAFEの担保比率が低下します

（したがって、SAFEクリエイターは彼らの借金を返済するように動機付けられます）そしてユーザーは買いだめし始めます

値が増加することを期待してインデックスを作成します。

Scenario 2: How Debt is Repriced



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を使用すると仮定します
償還率を計算するコントローラー：

- リフレックスインデックスは、任意の償還価額「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は新しい市場価格を読み取り、計算します 比例項 p 。この場合は $-1 * ((\text{'rand'} + x) / \text{'rand'})$ です。
The 償還価格を下げるために、比例は負になります。
インデックスの価格を変更して、安くなるようにします
- 比例を計算した後、メカニズムは積分を決定します 項 i
最後のからの過去のすべての偏差を加算することによる $deviationInterval$ 秒
- メカニズムは、比例と積分を合計し、1秒あたりの償還率 r ゆっくりと償還を減らし始める 価格。
SAFEの作成者は、より多くの借金を生み出すことができることに気付く

と、氾濫します 複数のインデックスと市場

- 後 n 秒、機構の検出そのときの偏差
市場価格と償還価格はごくわずかです（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、償還を維持し
ます それがあるところの価格

実際には、アルゴリズムはより堅牢になり、いくつかの変数を作成します。

不変（たとえば、ノイズ パラメータ、
deviationInterval）または厳密な境界があります
ガバナンスがどのように変化するかについて。

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、
アルゴリズムコントローラーパラメーターの調整。不適切なパラメータ化は
その結果、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も一般的に不安定です。

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が含まれます。

チューニングパラメータを微調整し、システムの応答を観察することがよくあります。途中で意図的にショックを導入します。困難と経済的リスクを考えると
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を微調整することで、
初期パラメータを設定するために可能な限りコンピュータモデリングとシミュレーション、

ただし、追加のデータがあれば、ガバナンスがチューニングパラメータを更新できるようにになります 生産からは、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（生成時に適用される金利）を維持する予定です。

インデックス) 固定または上限があり、償還価格のみを変更するため、フィードバックメカニズムのモデリングに伴う複雑さ。私たちの借入率ケースは、マルチ担保DAIの安定性手数料とDSRの間のスプレッドに等しくなります。

借入金利は一定に保つ予定ですが、変更することは可能です。マネーマーケットセッターを使用した償還価格と一緒に。マネーマーケットSAFEにインセンティブを与える方法で借入レートと償還価格を変更します。多かれ少なかれ借金を生み出すクリエイター。インデックスの市場価格が上回っている場合。償還の場合、両方のレートが下がり始めますが、償還を下回ると、レートが上がります。

グローバル決済

グローバル決済は、償還価格を保証するために使用される最後の手段の方法です。

すべての反射指数所有者に。これは、リフレックスインデックスホルダーとSAFEの両方を許可することを目的としています。

クリエイターは、システム担保をその正味額（各インデックスの量）で償還します（最新の償還価格に応じた担保タイプ）。誰でもトリガーできます。一定量のプロトコルトークンを書き込んだ後の決済。

決済には3つの主要なフェーズがあります。

- トリガー：決済がトリガーされ、ユーザーはSAFEを作成できなくなります。担保価格フィードと償還価格は凍結され、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。
- 主張：すべてのリフレックスインデックスホルダーとSAFEクリエイターは、一定額を請求できます。

インデックスの最後に記録された償還価格に基づくシステム担保

ガバナンス

パラメーター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。

時間ガバナンス

制限のある時間制限のあるガバナンスは、制限付きガバナンスモジュール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、Oracle Network Medianizer（セクション6.2）で使用されるOracleのアドレスを少なくとも後に変更する可能性があります T 、最後のOracleの変更から秒が経過した。

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、アクションバウンドガバナンスです。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

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。

ガバナンスアイスエイジ

アイスエイジは、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領域

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のみによって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ます。ガバナンスはできるようになります、時間の経過とともにリスクを多様化に
- 外部依存関係の変更：システムが依存するオラクルとDEXをアップグレードできます。ガバナンスは、それが適切に機能し続けるようにするために、新しい依存関係にシステムを指すことができます

- 微調整率セッターを：**（アクションと時間有界ガバナンスによって記載されているように）初期の金融政策のコントローラは、合理的な範囲内で変更可能なパラメータを持っています
- 間の移行システムバージョン：**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権限を付与し、古いシステムからこの権限を撤回することができます。この移行は、以下に概説する移行モジュールを使用して実行されます。

制限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、システムは、デット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される可能性があります**
- 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、システムは移行レジストリでシステムのデットオークション契約のアドレスを送信します。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、移行されないことを意味します。**
- 新しいシステムの提案と古いシステムからのアクセス許可の撤回の間にはクールダウン期間があり**
- まずオプションの契約印刷権限が拒否された後、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権限を自動的に与える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

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

- 重大な価格フィードの遅延**：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システムが検出します
- システム移行**：これは、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るオプションの契約です。ガバナンスがプロトコルトークンを印刷する債務オークションメカニズムの機能を撤回する瞬間（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逸脱**：システムは、インデックスの市場価格がていることを検出します。 $x\%$ 長期間にわたって逸脱し償還価格

ガバナンスは、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るようになります。

制限されているか、氷河期がシステムの一部をロックし始めるまで。

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主なアセットタイプは3つあります。

インデックス、プロトコルトークン、およびホワイトリストに登録されたすべての担保タイプ。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されます。

ガバナンス主導のオラクル

ガバナンストークン保有者またはプロトコルを開始したコアチームはパートナーになることができます

複数の価格フィードをオフチェーンで収集し、単一の価格フィードを送信する他のエンティティと

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へのトランザクション。

このアプローチにより、オラクルのアップグレードと変更の柔軟性が高まります。インフラストラクチャは信頼性を犠牲にしてもたらされますが。

Oracle Network Medianizer

は、複数の価格から価格を読み取るスマートコントラクトです。

ガバナンスによって直接制御されていないソース（例：Uniswap V2プール）インデックス担保タイプと他のステーブルコインの間）そしてすべての結果。ONMは次のように機能します。

- 私たちの契約では、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。

担保価格を要求します。契約は余剰金の一部によって賄われていますシステムが発生します（余剰財務、セクション11を使用）。各オラクルネットワーク

支払いとして特定のトークンを受け入れるので、私たちの契約はまた、各リクエストに必要な最小量とトークンのタイプ

- システムに新しい価格フィードをプッシュするには、すべてのオラクルが事前に呼ばれます。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を交換します。

オラクルが受け入れたトークンの1つを使用した安定性料金。オラクルの後

呼び出されると、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。通話が無効な場合、

他のすべてのオラクルが呼び出されるまで、特定の障害のあるオラクルを

再度呼び出すことはできません。

契約は、有効な過半数があるかどうかをチェックします。有効なOracle呼び出しはしてはいけません。

元に戻すと、チェーンに投稿された価格を取得する必要があります

最後の m 秒。「取得」とは、それぞれに応じて異なる意味を持ちます
オラクルタイプ：

○ オラクルのオラクルの場合、すぐに結果を得ることができます。

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、当社の契約は料金を支払い、オ

ラクルに電話し、 n 、特定の時間待機する必要があります

オラクルを再度呼び出す前に 要求された価格を取得するために

● 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た後

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（例：

契約は3/5オラクルから有効なデータを受け取りました）、結果は並べ替えられ、契約は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、Oracleの結果を含む配列は次のようになります。クリアされ、契約は待つ必要があります p

全体を開始する前に秒ます もう一度処理する

Oracle Network Backup

Governanceは、次の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。

メディアナイザーは、有効なOracleネットワークの大部分を連続して数回見つけることができません。

メディアナイザーを展開する場合は、バックアップオプションを設定する必要があります。その後変更されました。さらに、別の契約でバックアップに

メディア化メカニズムを長期間交換し、自動的にシャットダウンしている
プロトコルをダウンします。

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。

SAFEのライフサイクル

：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

● 預金担保をSAFEに

ユーザーが最初にニーズを満たすために新しいSAFEと預金担保
を作成するには。

●SAFEの担保に裏打ちされたインデックスを生成するは、生 成するインデックスの数を

ユーザーを指定します。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。

● SAFE債務の返済

SAFE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。

● 担保の引き出し

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。

SAFEの清算

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、担保オークションで売却します。

清算保険

システムの1つのバージョンでは、SAFE作成者は、SAFEを選択するオプションを使用できます トリガー
が清算されたときの。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 安全 と
リスクということです。

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、システムはと呼ばれる変数を使用する必要があります

liquidationQuantity

、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に、 清算ペナルティは
、すべての競売SAFEに適用されます。

担保オークションのパラメーター

Parameter Name	Description
minimumBid1	回の入札提供する必要があるコインの最小量
discount	担保が販売される割引

lowerCollateralMedianDeviation	担保の中央値がオラクル価格と比較して持つことができる
upperCollateralMedianDeviation	最大下限偏差最大上限偏差担保の中央値はオラクル価格と比較して行うことができます
lowerSystemCoinMedianDeviation	、システムコインオラクルの価格フィードをシステムコインオラクル価格と比較していることができる最大下限偏差
upperSystemCoinMedianDeviation	担保中央値は、システムコインオラクル価格と比較していることができる最大上限偏差
minSystemCoinMedianDeviation	ミンのと比較したシステムコイン中央値の結果の偏差中央値を考慮に入れるため償還価格

担保オークションメカニズム

固定割引オークションは、担保をeで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)。不良債権の決済に使用されるシステムコインのexchange。入札者は、オークションハウスがを転送することを許可するだけでsafeEngine.coinBalance 呼び出すことができ よくbuyCollateral、システムコインを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と交換するためにをます。

入札者は、呼び出すことにより、特定のオークションから取得できる担保の量を確認することもできます getCollateralBought または getExplicitCollateralBoughtを。ことに注意してください getCollateralBought。getIncludemateCollateralBought 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ないは redemptionPrice 、オラクルからを リレーlastReadRedemptionPriceを 使用します。

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。

デットオークションを開始するには、システムは次の2つのパラメータを使用する必要があります。

- initialDebtAuctionAmount：オークション後に作成するプロトコルトークンの初期量
- debtAuctionBidSize：初期入札サイズ（と引き換えに提供する必要のあるインデックスの数） initialDebtAuctionAmount プロトコルトークン）

自律型デット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

される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反射指数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。

その後、債務に対してミントされるプロトコルトークンの初期量（initialDebtAuctionAmount）が設定されます。AuctionBidSizeインデックス。

initialDebtAuctionAmountは、入札を奨励するために、実際のPROTOCOL/INDEX市場価格と比較して割引価格に設定できます。

債務オークションのパラメータ

Parameter Name	Description
amountSoldIncrease	同じ量のインデックスに対してミントされるプロトコルトークンの量の増加
bidDecrease	次回の入札では、同じインデックス量のプロトコルトークンの許容量が最小限に減少します。
bidDuration	新規入札の送信後の入札継続時間（秒単位）
totalAuctionLength	オークションの合計時間（秒単位）
auctionsStarted	今までオークションが何回始まったか

債務競売メカニズム

担保競売とは対照的に、債務競売は一段階だけだ。

recreaseSoldAmount(uintid, uintamountToBuy, uintbid):

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の量を減らします。

入札がなければ競売は再開されるだろう。

システムが再起動するたびに、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が提供されます。

新しいプロトコルトークン量が最後に計算されます。 $\text{TokenAmount} * \text{amount SoldIncrease} / 100$ 。

競売が確定した後、このシステムは最高入札者のためにトークンを鋳造する。

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、債務オークションで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、余剰オークションの利用により、プロトコルトークンの供給も徐々に減少する。

余分な資金が競売にかけられる前にシステムに蓄積される必要がある余剰額を余剰バッファと呼び、発行された総負債に占める割合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、関連のない幅広い資産を保持し、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、プロトコルトークンに対してシステムで蓄積された安定性料金を販売し、その後燃やされます。

余剰オークションパラメータ

Parameter Name	Description
bidIncrease	次の入札で最低限の値上げ
bidDuration	新しい入札が送信されてからオークションが継続する時間（秒）
totalAuctionLength	オークションの合計時間（秒単位）
auctionsStarted	今までオークションが何回始まったか

余剰競売メカニズム

余剰オークションには、次のような単一ステージがあります。

`increaseBidSize(uint id, uint amountToBuy, uint bid):`

誰でも同じ量のインデックス（余剰）に対してより多くのプロトコルトークンを入札できます。

すべての新規入札は、 $\text{lastBid} * \text{bidIncrease} / 100$ 以上である必要があります。

オークションは、最長合計オークション長さ秒後、または入札期間秒が経過し、その間に新しい入札が提出されなかった場合に終了します。

入札がなければ競売が再開されます。

一方、オークションに少なくとも1件の入札がある場合、システムは余剰分を最高入札者に提供し、収集されたプロトコルトークンをすべて燃やす。

余剰インデックス管理

ユーザ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、システムはユーザのSAFEに借入金利を適用し始めます。

発生した利息は、次の2つの異なるスマート契約にプールされます。

- 債務（第9.2節）と余剰（第10.1節）のオークションを誘発する会計エンジン
- 余剰資金は、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、外部の関係者にシステムを維持するよう奨励するために使用されます。余剰財務省は、次の3つのコアシステムコンポーネントの資金調達を担当しています。
- Oracleモジュール（セクション6）。財務省は、オラクルの構造に応じて、ガバナンスホワイトリスト、オフチェーンオラクル、またはオラクルネットワークへのコールに対して支払いを行います。
財務省は、オラクルを呼び出して更新するためにガスを使った住所を支払うように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もあります。新しい担保タイプのホワイトリストを作成したり、システムのレート設定を微調整したりするチーム（セクション4.2）

財務省は、将来、一部の余剰受給者が自動的に資金提供を拒否され、他の受給者がその代わりを務めることができるように設定できます。

外部アクター

このシステムは、適切に機能するために外部アクターに依存します。

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、マーケットメイキング、価格フィードの更新などの分野に参加することを経済的に奨励されています。

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、できるだけ多くのユーザーがプロトコルを安全に保つことができるようにします。

アドレス指定可能な市場

RAIは、主に次の2つの分野で役立ちます。

●ポートフォリオの多様化:

投資家はRAIを利用して、実際にイーテルを保有するリスクを全く伴わずにETHのような資産にさらされることになる

●合成資産の担保:

RAIは、UMA、MakerDAO、Synthetixなどのプロトコルを暗号化市場への露出を減らし、数百万ドル相当の暗号化資産が清算された2020年3月のブラック・サザデーのようなシナリオの場合、ユーザーにより多くの退社時間を与えることができる。

今後の調査

分散資金の境界を押し広げ、分散金融にさらなる革新をもたらすため、ガバナンスの最小化や清算メカニズムなど、中核分野で代替案を模索し続ける。

我々はまず、外部統制から自らをロックするプロトコルを中心とした将来の標準と、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。その後、私たちはイーサリアムコミュニティを招待して、担保と債務競売に特定の焦点を当てた提案に関する討論と改善案を設計する。

リスクと軽減

リフレックスインデックスの開発と起動には、いくつかのリスクがあります。また、その上に構築された後続のシステムもあります。

●スマートコントラクトバグ:

システムに発生する最大のリスクは、誰でもすべての担保物を抽出したり、プロトコルを復旧できない状態でロックするバグの可能性です。複数のセキュリティ研究者にコードを確認してもらい、テストネットでシステムを起動してから、本番環境への導入を約束する予定です。

●オラクルの失敗:

複数のオラクルネットワークからのフィードを集約し、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しいルールを設けることで、悪意のあるガバナンスが簡単に偽価格を導入しないようにします。

●付随的なブラックスワンイベント:

基礎となる資料にブラックスワンイベントが発生し、大量の清算SAFEが発生する危険性があります。

清算は不良債権全体をカバーできない可能性があるため、発行債務を適切にカバーし、市場の衝撃に耐えるために、システムは余剰バッファを継続的に変更します。

●不適切な速度設定媒介変数:

自律フィードバックメカニズムは実験的であり、シミュレーション中に予測したように正確に動作しないことがある。

予期せぬ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微調整できるようにする計画です（制限されたまま）。

●健全な清算人市場を開拓できない●清算人は、発行されたすべての債務が担保になるように保障する重要な主体だ。

できるだけ多くの人々がシステムの安全性を保つために参加できるように、インターフェイスと自動スクリプトを作成する予定です。

概要

私たちは徐々に人間の制御から担保資産が反射指数という、揮発性の低い発行自体をロックするプロトコルを提案しています。私たちは、まずは幾つかスマート契約トークンホルダ、システムを持っている権力を制限ことができる自律機構は、インデックスの市場価格に影響を意味した。私たちは、SAFEs配当指標の鋳造を一般的な機構を提示して終了複数の独立した神託をネッ

トワークからmedianizing価格飼料の自律的なスキームについて概括した。

参考資料

[1] 「メーカープロトコル:

MakerDAOのマルチカタログダイ(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] シンセティックス・リトペーパー <https://bit.ly/2SNHxZO>

[4] Kjåström,RMMurray,"フィードバックシステム:

科学者とエンジニアのための入門書」、<https://bit.ly/3bHwnMC>

[5]RJHawkins、JKSpeaks、DEHamilton、「通貨政策と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におけるピアツーピアの裁量的相互作用"<https://bit.ly/3du8TMy>

[7] H. Adams, N. Zinsmeister, D. Robinson, “UniswapV2コア”,
<https://bit.ly/3dqzNEU>

用語集

反射指数: 基礎となるRAIの変動性を減衰させる担保資産:

我々の最初の反射指数

償還価格: システムが指数を持つことを望む価格。

市場価格がそれに近づかない場合に備えて、償還率（RRFMで計算）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、より多くの借金を生み出したり、借金

の一部を返済したりすることを目的としています。

借入金利: 未払い債務を抱えるすべてのSAFEに適用される年間金利

償還率フィードバックメカニズム（RRFM）:

反射指数の市場と償還価格を比較し、SAFEクリエイターに徐々に影響を

与え、負債を多かれ少なかれ発生させる償還率を計算する自律メカニズム

（暗黙的に市場/償還価格偏差を最小限に抑えようとする）

マネーマーケットセッター（MMS）:

一度に複数の通貨レバーを引くRRFMに似たメカニズム。

反射指数の場合、借入金利と償還価格の両方を修正する。

OracleNetworkMedianizer（ONM）:

（ガバナンスによって制御されない）複数のOracleネットワークから価格を取得し、多数派（5人に3人など）が結果を返した場合に価格を中央値化するスマート契約

制限付きガバナンスモジュール（RGM）：

ガバナンストークン所有者がシステムに対して持つ権限を拘束する一連のスマート契約。

時間遅延を強制するか、ガバナンスが特定のパラメータを設定する必要がある可能性を制限します。

ガバナンスの氷河期：

一定の期限が過ぎた後、外部の介入によってプロトコルのほとんどのコンポーネントをロックする不変の契約

会計エンジン：負債と余剰競売を誘発するシステム構成要素。

また、現在競売にかけられている債務、未実施の不良債権、余剰バッファの量も追跡しています。

余剰バッファ：システムに蓄積され、維持される利子の量。 任意の利子

このしきい値を超えると、プロトコルトークンを焼き付ける余剰オークションで売却されます。

剰余金：

異なるシステムモジュールに未払利息の回収を許可する契約（オラクルコールのONMなど）