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  
 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.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 Backup  
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  
 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、次の⾦融⾰命の基礎を築き、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

屈折率の目的は、特定のペグを維持することではなく、それを保護することです。 インデックスにより、誰でも暗号通貨市場にアクセスできます。 実際の暗号資産を保有するのと同じ規模のリスクはありません。 私たちはRAIです。最初の反射率は、イーサリアムで合成繊維を公開している他のチーム（MakerDAOのMulticollateral DAI [1]、UMA [2]、Synthetix [3]など）にすぐに役立ちます。このシステムは、ETHや ユーザーにより多くの時間を与えます。

市場が大きく変化した場合は、ポジションをクローズします。 反射指数を理解するために、彼らの行動を比較することができます償還価格をステーブルコインの価格に変更します。

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。

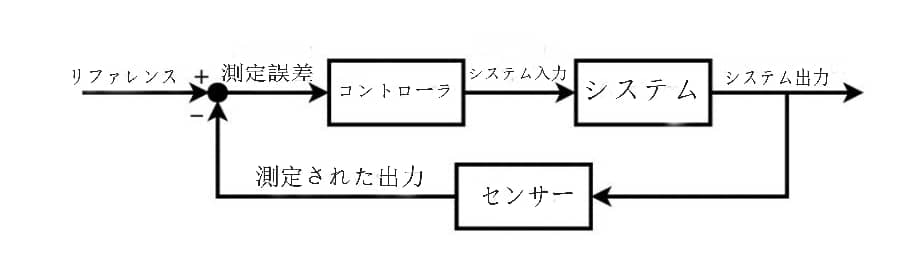
⾦融政策のメカニズム

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。

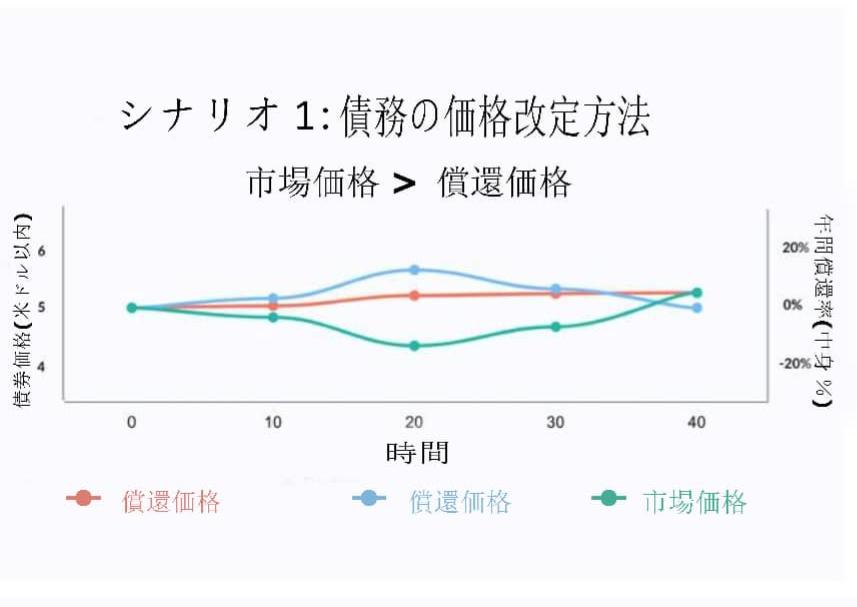
フィードバックメカニズムコンポーネント

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。

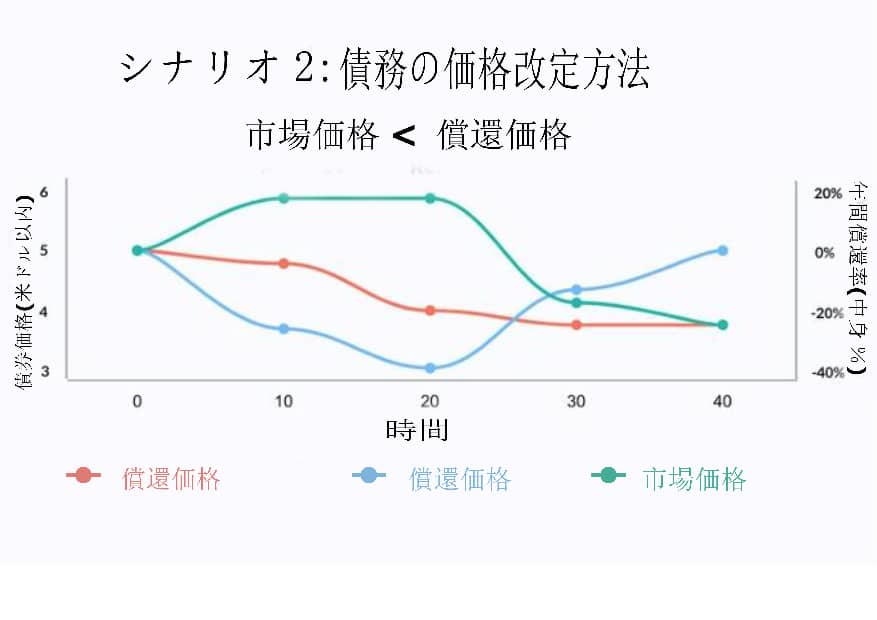
以下の最初のシナリオでは、インデックスの市場価格が償還価格よりも⾼い場  
合、メカニズムは負のレートを計算し、償還価格を下げ始め、システムの負債を  
安くします。



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

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。

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 Backup

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



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 BuyCollateral 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。getCollateralBought また getExplicitCollateralBought 。ご了承ください getCollateralBought 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 getExplicitCollateralBought を使⽤しま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。

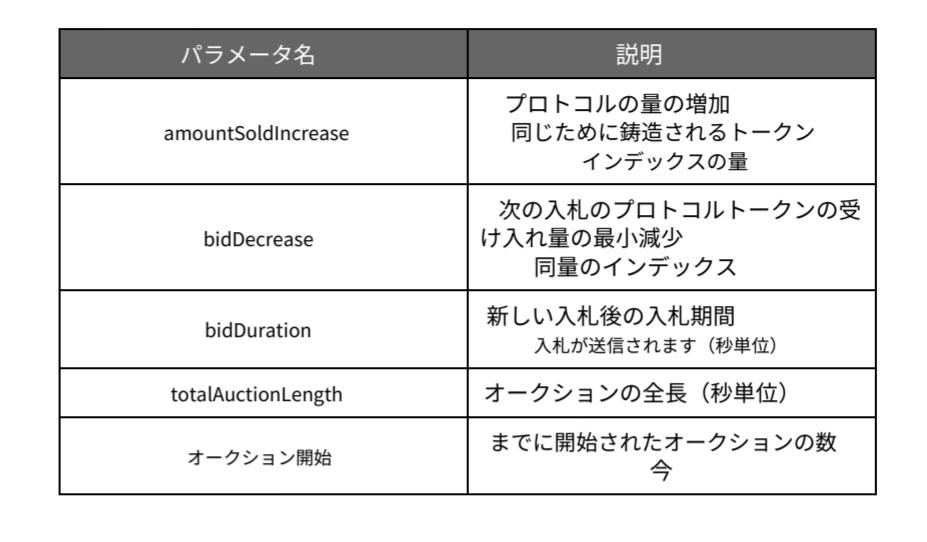
債務オークションを開始するには、システムは2つのパラメーターを使⽤する必要があります。

● 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。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



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。

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負債の合計のパー 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



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つある場合

入札すると、システムは余剰分を最高入札者に提供し、その後すべてを燃やします

収集されたプロトコルトークン。

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、システムが起動します

ユーザーのSAFEに借入レートを適用します。 未収利息は2つにプールされます

さまざまなスマートコントラクト：

●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

●コアインフラストラクチャコンポーネントと

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

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）。オラクルの構造に応じて、

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のオラクルに支払うか、

オラクルネットワークへの呼び出し。財務省はまた、支払うために設定することができます

オラクルを呼び出して更新するためにガスを消費したアドレス

●場合によっては、システムを維持する独立したチーム。例はチームです

新しい担保タイプをホワイトリストに登録するか、システムのレートセッターを微調整する人（セクション

4.2）

一部の余剰受取人が自動的に拒否されるように財務を設定することができます

将来の資金調達や他の人が彼らの代わりになることができます。

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。これらの俳優

オークション、グローバル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る

決済処理、マーケットメイク、および維持するための価格フィードの更新

システムの状態。

初期のユーザーインターフェイスと自動化されたスクリプトを提供して、できるだけ多くのユーザーを有効にします

プロトコルを安全に保つために可能な限り人々。

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。

●ポートフォリオの分散：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のないETHのような資産

●合成資産の担保：RAIは、UMAなどのプロトコルを提供できます。

MakerDAOとSynthetixは暗号市場への露出を減らし、

黒などのシナリオの場合、ユーザーは自分のポジションを終了するためのより多くの時間を

数百万ドル相当の暗号資産が

清算された

今後の研究

分散型マネーの限界を押し広げ、さらなるイノベーションをもたらすために

分散型ファイナンスでは、次のようなコア分野で代替案を探し続けます

ガバナンスの最小化と清算のメカニズム。

まず、ロックするプロトコルに関する将来の標準の基礎を築きたい

外部からの制御と、それに応じて適応する真の「マネーロボット」のために

市場の力に。 その後、Ethereumコミュニティを招待して討論と設計を行います

担保と債務に特に焦点を当てた提案に関する改善

オークション。

リスクと軽減

反射指数の開発と立ち上げにはいくつかのリスクがあります。

上に構築された後続のシステム：

●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、

誰でもすべての担保を抽出したり、プロトコルを状態にロックしたりできるバグ

から回復することはできません。コードを複数のセキュリティでレビューする予定です

研究者は、システムを展開する前に、テストネットでシステムを起動します

生産中

●Oracleの失敗：複数のOracleネットワークからのフィードを集約します

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適用されます。

悪意のあるガバナンスは簡単に誤った価格を導入することはできません

●付随的なブラックスワンイベント：ブラックスワンイベントのリスクがあります

大量の清算されたSAFEをもたらす可能性のある基礎となる担保。

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、まともなものをカバーするために、その余剰バッファを継続的に変更します

発行された債務の額と市場のショックに耐える

●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。 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予定です（

予期しないシナリオを回避するために）

●健全な清算人市場のブートストラップの失敗：清算人は重要なアクターです

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します。 作成する予定ですできるだけ多くの人ができるようにインターフェースと自動スクリプト

システムの安全性の維持に参加します。

概要

私たちは、人間の制御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します。 私たちは最初に

インデックスの市場価格に影響を与え、その後

いくつかのスマートコントラクトがトークン所有者が持つ力をどのように制限できるかを説明しました

システム。 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ました

複数の独立したオラクルネットワーク、そして一般的なものを提示することによって終了しました

インデックスの作成とSAFEの清算のメカニズム

参考文献

[1]「Makerプロトコル：MakerDAOのマルチコラテラルダイ（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] K.J. Åström、R.M。 マレー、「フィードバックシステム：科学者と

エンジニア」、https：//bit.ly/3bHwnMC

[5] R.J. ホーキンス、J.K。 話す、D.E。 ハミルトン、「金融政策とPID制御」、

https://bit.ly/2TeQZFO

[6] H. Karp、R。Melbardis、「イーサリアムでのピアツーピアの裁量的相互関係

ブロックチェーン」、https：//bit.ly/3du8TMy

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

3dqzNEU

用語集

リフレックスインデックス：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。それは変わる、

市場価格がそうでない場合、償還率（RRFMによって計算される）の影響を受けますそれに近い。 SAFEクリエイターに影響を与えて、より多くを生み出したり、一部を返済したりすることを目的としています

借金

借入金利：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）：自律メカニズム

反射指数の市場価格と償還価格を比較してから、

SAFEクリエーターにゆっくりと影響を与えて多かれ少なかれ債務を生み出す償還率（および

暗黙的に市場/償還価格の偏差を最小化しようとします）

マネーマーケットセッター（MMS）：複数をプルするRRFMに似たメカニズム

一度に金銭的なレバー。リフレックスインデックスの場合、両方の借用を変更します

レートと償還価格

Oracle Network Medianizer（ONM）：複数から価格を引き出すスマートコントラクト

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）および

大多数（例：5つのうち3つ）はスローせずに結果を返しました

制限付きガバナンスモジュール（RGM）：権力を制限する一連のスマートコントラクト

ガバナンストークンの所有者がシステムに対して持っていること。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

Governance Ice Age：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

特定の期限が過ぎた後の外部介入から

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。これ

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

余剰バッファー：システムに蓄積して保持する利息の量。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許可を与える契約

未収利息を撤回する（例：オラクルコールのONM）