RAI: DeFiエコシステムに向けた低ボラティリティで信託が最小限の担保

Stefan C. Ionescu, Ameen Soleimani

2020年5月

概要
市場の動きに自動的に反応してネイティブな担保資産の目標値を修正するガバナンスが最小限で分散化されたプロトコルを提供します。このプロトコルにより誰もが暗号資産を活用し、現担保を減衰させた「reflex index」を発行できるようになります。このインデックスが普遍的でボラティリティの低い担保としていかに有用であり、その保有者や他の分散型金融プロトコルを急激な市場変化から保護できるのかを説明します。また、このインフラを活用して他のチームが独自の統合サービスを立ち上げる支援策も紹介します。最後に、多くのDeFiプロトコルに見られる現状のオラクルとガバナンス構造への代替案を提示します。

目次

導入

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主君である主導者や金融エリートの手に握られたまま、無意識のうちに一般大衆に押し付けられてきました。ビットコインが草の根的な抗議活動によって価値を保有する商品資産を実現する可能性を示したのに対し、イーサリアムはボラティリティから保護できたり、担保として活用できたり、基準価格に固定して日々の取引の交換媒体として利用できる資産担保型の合成金融商品を構築するプラットフォームを提供します。これらの利用方法は全て分散型コンセンサスの同一の原則に基づいて実行されます。

富の保存のためのビットコインの自由参加型アクセスとイーサリアムにより適切に分散化された合成通貨は来るべき金融革命の基礎を築き、現代の金融システム業界に新しい金融システムを構築するための協調手段を提供することになるでしょう。

本紙では、他の合成通貨の発展を促し、分散型金融業界全体の重要な構成要素を確立する新しい資産タイプであるreflex indexesを構築するフレームワークを紹介します。

Reflex Indexesの概要

reflex indexの目的は特定のペグ通貨を維持することではなく、担保のボラティリティを低減させることです。このインデックスにより現物の暗号資産を保有するのと同じ程度のリスクを負うことなく暗号通貨市場へのリスクテイクが可能となります。最初のreflex indexとなるRAIはイーサリアム上で金融商品（MakerDAOのMulti Collateral DAI [1]やUMA[2]、Synthetix[3]など）を発行する他チームにすぐさま役に立つでしょう。その理由にはETHのようなボラティリティの高い資産のリスクを下げ、市場が大きく変動した場合に利用者がポジションを仕舞うための時間を長くできることが挙げられます。

reflex indexesを理解するためには、これらインデックスの償還価格とステーブルコインの価格の挙動を比較できます。

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。これは内部の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（市場でコインが取引されている価値）とは異なります。USDCのようなフィアットに裏付けされたステーブルコインの場合、システム運営者が誰でも1コインを1US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値は常に1です。また、MakerDAOのMulti Collateral DAI（MCD)のような暗号資産が裏付けられたステーブルコインの場合、システムが1USドルの固定ペッグを目標としているため、償還価格も1に固定されています。

ほとんどの場合、ステーブルコインの市場価格と償還価格の間には差が存在します。この状況は例えば、市場価格が償還価格よりも高い場合にはトレーダーは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はステーブルコインを担保（USDCの場合にはUSドル）と交換する裁定機会を創出します。

reflex indexesはシステムが目標とする償還価格を有している点でステーブルコインと似ています。主な違いは、償還価格が固定ではなく、市場の影響を受けながら変化するように設計されて

いる点です。第4章ではindexesの償還価格がどのように変動し、利用者に新たな裁定機会をもたらすのか説明します。

設計理念とマーケット進出戦略

設計理念は安全性と安定性、配信の速度を優先することです。
Multi-Collateral DAIはRAIの設計検討を繰り返し始めるために自然な場所でした。このシステムは厳重な監査と正式な検証が行われており、外部への依存性が最小限で、活発な専門家コミュニティを有しています。開発とコミュニケーションの労力を最小限にするため、実装は元のMCDコードベースに最もシンプルな変更を加えるだけに留めようと考えています。

最も重要な変更点は自律的なレートセッターや多くの独立した価格フィードプロバイダーと統合されたOracle Network Medianizer、人の介入からシステムを可能な限り分離するためのガバナンス最小化レイヤーの追加です。

プロトコルの最初のバージョン（ステージ1）では、レートセッターとコアアーキテクチャへのその他のマイナーな改良のみを実施します。レートセッターが期待通りに動作することが証明されたら、より安全にOracle Network Medianizer（ステージ2）とガバナンス最小化レイヤー（ステージ3）を追加することができます。

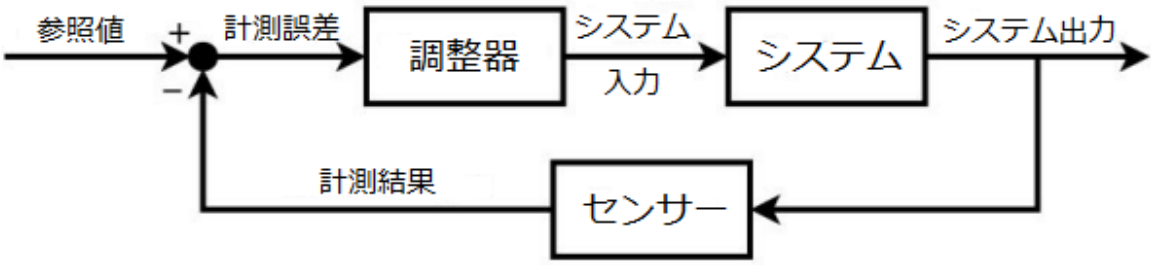
金融政策メカニズム

制御理論の導入

一般的によく知られている制御システムにシャワーが挙げられます。シャワーを浴びるとき、人によって望ましい水温が存在します。この水温のことを制御理論では、基準設定値と呼びます。制御者であるところの人間は、水流の温度（システム出力と呼ぶ）を継続的に測定しながら、望ましい温度と現在の温度との偏差（または誤差）に基づいて、シャワーのノブを回す速度を変更します。このノブを回す速度をシステム入力と呼びます。基準設定値へより短い時間で到達するようにノブを速く回すことが目的になりますが、温度がオーバーシュートするほど速くはありません。水流の温度が突然変化するようなシステムショックが生じた場合、人間は外乱に応じてどれくらい速くノブを回せばいいか知っているので、現在の水温を維持できるはずです。

動的システムにおける安定性の維持に関する科学領域は制御理論と呼ばれ、自動車のクルーズコントロールやフライトナビゲーション、化学反応炉、ロボットアーム、あらゆる種類の工業プロセスなどで幅広く応用されています。ハッシュレートが変動しても平均ブロックタイムを10分で維持しているビットコインの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一例として挙げられます。

現代制御論では、アルゴリズム制御器がプロセスに組み込まれており、システム入力（例：自動車のアクセスペダル）をシステム出力（例：自動車の速度など）と設定値（例：クルーズコントロールの速度など）との偏差に基づいて自動的に更新する制御します。



最も一般的なアルゴリズム制御器はPID制御器です。95%以上の産業用途と幅広い生物学的システムにおいてPID制御が採用されています[4]。PID制御は3項からなる数式に基づき出力を決定します。

制御出力＝比例項＋積分項＋微分項

比例項は偏差に正比例する制御項目です。偏差が大きく正の値であれば（例：クルーズコントロールの速度設定値が現在の速度よりもはるかに高い場合）、比例反応も大きく正の値になります（例：アクセルペダルを踏み込む）。

積分項は偏差がどれくらい継続しているかを考慮する制御項目です。偏差の時間積分により決定され、主に定常状態の誤差を排除するために利用されます。積分項は設定値からの小さいけれど持続的な偏差に対応するために蓄積されます（例：クルーズコントロールの設定値が数分間、自動車の速度よりも1mph高くなっていた場合）

微分項は偏差がどれくらいの速さで大きくなったり小さくなったりしているかを考慮する制御項目です。偏差の微分により決定され、偏差が大きくなったときに制御応答を加速させる役割を果たします（例：クルーズコントロールの設定値が自動車の速度よりも高く、車が減速し始めたときにスピードを上げる）。また、偏差が小さくなってきたときには、制御応答の減速によりオーバーシュートを抑えることができます（例：自動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アクセルを緩める）

それぞれ独立して調整が可能な3項の組み合わせによって、PID制御器は様々な制御システムを柔軟に管理することができるのです。

PID制御器は応答時間にある程度の遅れを許容し、システムが安定しようとする際に設定値付近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も効果を発揮します。RAIのようなreflex indexシステムはPID制御器で償還価値を変更できるこの種のシナリオによく合致しています。

より一般的には、現在の中央銀行の金融政策ルール（テイラー・ルールなど）の多くは、実際にはPID制御器の近似であることが最近判明されています[5]。

償還レートのフィードバック機構

償還レートのフィードバック機構はreflex indexの償還価値を変更するシステム要素です。この機構の仕組みを理解するためには、まずシステムが手動制御ではなくフィードバック機構を必要とする理由と機構の出力は何になるのかに関して説明が必要です。

フィードバック機構の構成要素

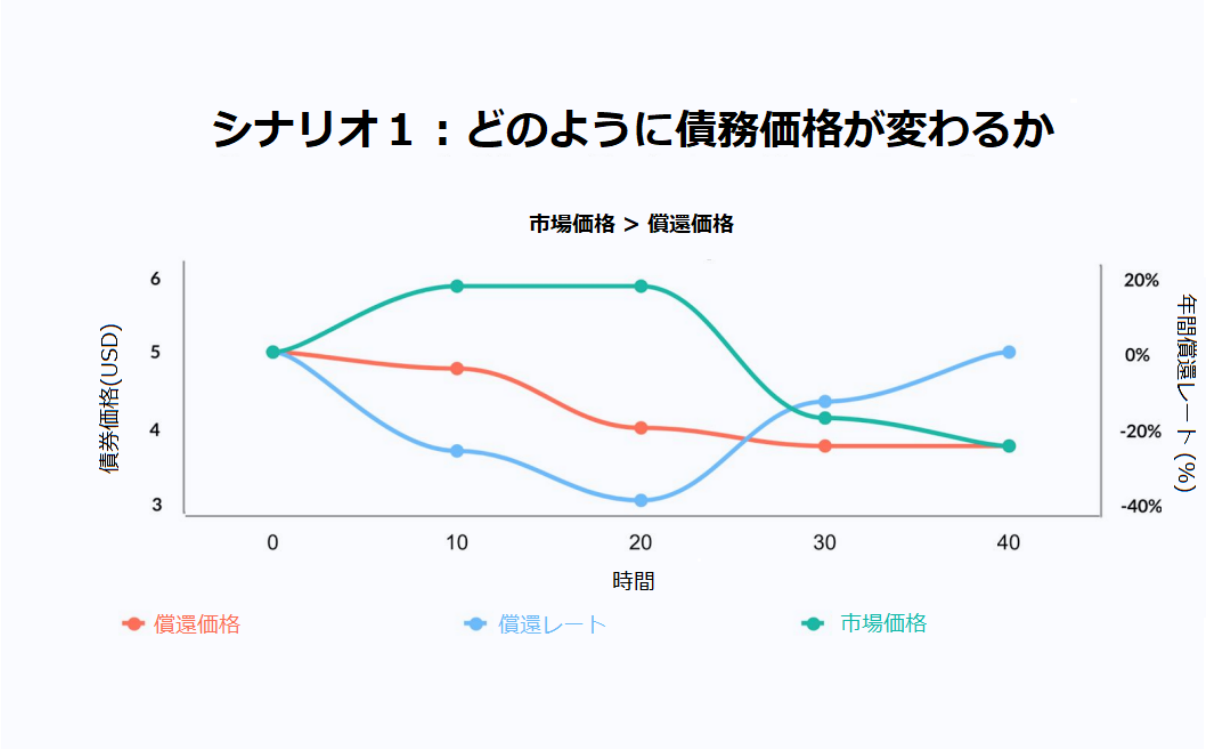
理論的にはreflex indexの償還価値（第2章で説明）の直接操作により、index利用者に影響を与えつつ最終的にindexの市場価格を変更することは可能でしょう。実際にはこの方法ではシステム参加者に望ましい効果を与えられないと思われます。将来株式取得略式契約書（SAFE）の保有者の立場からすると、償還価値が一度だけ引き上げられた場合、債務単位あたりの価値が高くなることを受入れ、担保率の低下による損失を吸収してポジションを維持するかもしれません。しかし償還価値が長期的に上昇すると予想される場合には、将来予想される損失を回避したいと考え、債務を返済してポジションの解消を選択する可能性が高くなります。

reflex indexシステムの参加者は償還価値の変化に直接反応するのではなく、我々が償還レートと呼ぶ償還価値の変化率に反応することを期待しています。償還レートはガバナンスが微調整したり完全に自動化もできるフィードバック機構によって設定されます。

フィードバック機構のシナリオ

フィードバック機構は市場要因における変化に対抗するため償還レートを使って償還価格と市場価格の均衡を保つ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、償還レート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。

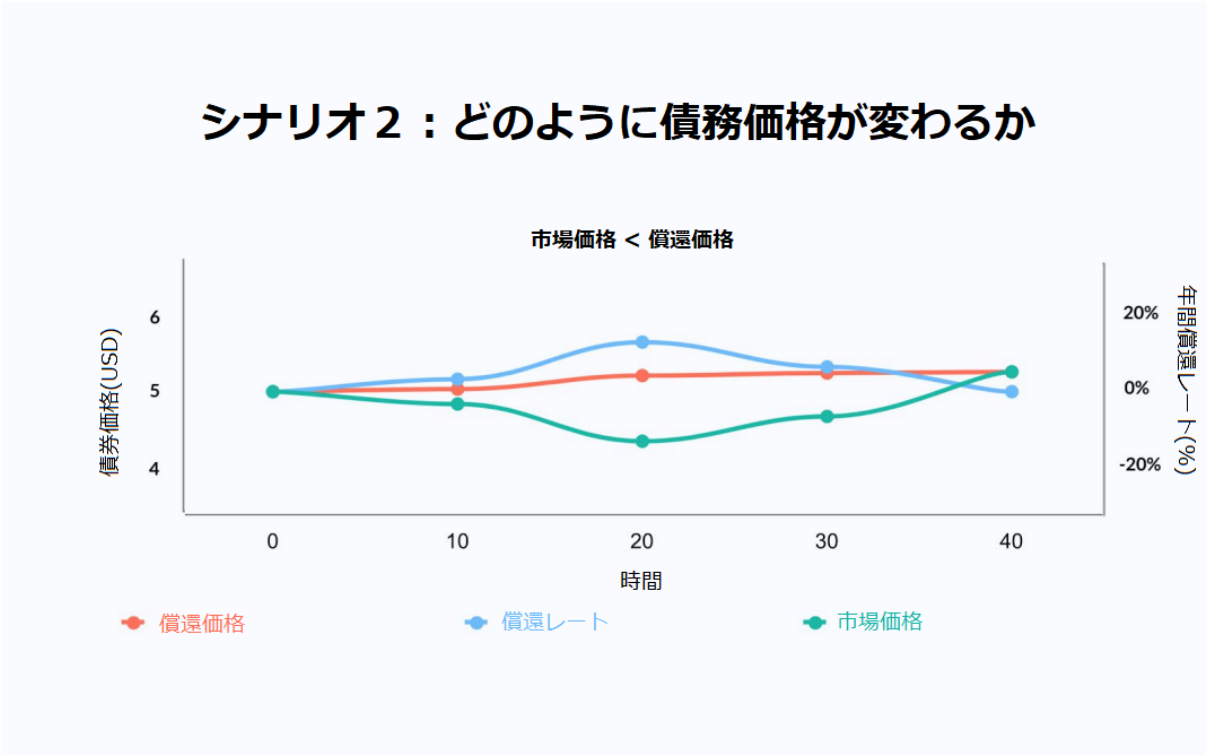
以下の最初のシナリオでは、indexの市場価格が償還価格よりも高い場合、フィードバック機構は負のレートを計算し、償還価格を下げ始めるため、システムの負債が割安になります。



償還価格が下がるという期待は、人々がindexを保有することを躊躇させ、SAFEの保有者がより多くの債務（担保価値が変わらなくても）を抱え、市場で売却することを促し、その結果、需要と供給の均衡が取られます。なお、これはindex保有者がフィードバック機構に対応して迅速に反応するという理想的なシナリオになります。実際には（特にローンチ後の初期段階では）機構の始動と発行された債権の量やその後の市場価格に見られる実際の結果との間に遅延が生じることが予想されます。

一方のシナリオ2では、indexの市場価値が償還価値よりも低ければレートが正になり、すべての負債が割高になるように再評価され始めます。

負債が高額になると、すべてのSAFEの担保比率が下がり（そのためSAFEの作成者には負債を返済するインセンティブが働く）、人々はindexの価値が上がることを期待してindexをため込み始めます。



フィードバック機構のアルゴリズム

以下のシナリオでは、プロトコルが比例積分制御器を利用して償還レートを計算するとします。

- reflex indexは任意の償還価格「rand」で発売されます
- ある時点でindexの市場価格が「rand」から「rand＋x」に上昇します。フィードバック機構は新しい市場価格を読み取った後、比例項pを計算しますが、この場合は-1*(rand + x) / randとなります。この比例項が負なのは償還価格を下げてindexの価格を再設定し、割安にするためです。
- 比例項の計算後、機構は最後のdeviation interval秒から過去全ての間の偏差を積算して積分項iを決定します。
- 機構は比例項と積分項を合計し、1秒ごとの償還レートrを算出して、償還価格を徐々に下げ始めます。SAFEの作成者はより多くの負債を生み出せることに気が付くと、より多くのindexを市場に投入します。
- n秒後、機構は市場価格と償還価格の乖離が（指定したnoiseパラメータの下で）無視できるレベルになったことを検出します。この時点でアルゴリズムはrを0に設定し、償還価格をそのまま維持します。

実際にはアルゴリズムはよりロバストになり、いくつかの変数（例：noiseパラメータ、deviation interval）を不変にするか、またはガバナンスを変更できるものに厳しい制限を設けることになります。

フィードバック機構の調整

reflex indexシステムを正しく機能させるために最も重要なことは、アルゴリズム制御器のパラメータ調整です。パラメータの設定が不適切だと、システムの安定性を得るのに時間がかかりすぎたり、大幅なオーバーシュートが発生したり、外部からの衝撃に対して全体的に不安定になったりします。

PID制御器のチューニングプロセスでは通常、本番環境においてチューニングパラメータを調整してシステムの応答を観察しますが、その過程で意図的にショックを与えることもあります。本番環境のreflex indexシステムのパラメータを調整することの難しさと経済的なリスクを考慮して、初期パラメータの設定にはできるだけコンピュータモデリングとシミュレーションを活用することを計画していますが、本番環境からの追加データによってチューニングパラメータが最適でないことが判明した場合には、ガバナンスによって更新することも可能にしています。

マネーマーケットセッター

RAIでは借入金利（index生成時に適用される金利）を固定もしくは上限を設け、償還価格のみを変更することでフィードバック機構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。この場合の借入金利はMulti-Collateral DAIにおける安定性手数料とDSRのスプレッドに相当します。

借入金利は固定する予定ですが、マネーマーケットセッターを使って、償還価格とともに借入金利を変更することができます。マネーマーケットはSAFE作成者がより多くの、またはより少ない債務を生み出すインセンティブとなるように、借入金利と償還価格を変化させます。indexの市場価格が償還価格を上回っていれば、両方のレートが下がり始め、逆に償還価格を下回っていればレートが上昇します。

グローバル決済

グローバル決済は、全てのreflex index保有者に償還価格を保証するために用いられる最後の手段です。これはreflex index保有者とSAFE作成者の両方が、システム担保をその正味価値（最新の償還価格に応じた各担保種類ごとのindex量）で償還できるようにするためのものです。誰でも一定量のプロトコル・トークンを焼却した後に決済を開始することができます。

決済には大きく分けて3つのフェーズがあります。

- トリガー：決済が行われ、ユーザーはSAFEの作成ができなくなり、すべての担保価格のフィードと償還価格が凍結され記録されます。
- プロセス：すべての未処理の競売を処理します。
- 請求：すべてのreflex index保有者とSAFE作成者は、index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することができます。

ガバナンス

パラメータの大部分は不変であり、内部のスマートコントラストの仕組みはガバナンストークンの保有者が全く新しいシステムを展開しない限り、更新できません。この戦略を選んだ理由は、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、システムの信頼性を損なわせようとするメタゲームを排除できるからです。また、人間に過度の信頼を置くことなく（「ビットコイン効果」）プロトコルの適切な運用を確立することで、社会的なスケーラビリティを最大化し、他の開発者が自分のプロジェクトのコアインフラとしてRAIを利用する際のリスクを最小限に抑えることができます。

変更可能ないくつかのパラメータについては、制限付きガバナンス・モジュールの追加を提案し、起こり得るすべてのシステム変更を遅らせたり制限したりします。さらに、一定の期限が過ぎた後にシステムの一部を外部による制御からロックすることができるパーミッション・レジストリである「ガバナンス・アイスエイジ」を提案します。

時間制限付きガバナンス

時間制限付き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。これは同じパラメータに適用される変更の間に時間的な遅延を課すものです。例えばOracle Network Medianizer（6.2章）で使用されるオラクルのアドレスを、最後にオラクルが更新されてから少なくとも T 秒が経過した後に変更することができます。

行動制限付きガバナンス

制限付きガバナンスモジュールの2つ目のコンポーネントは、行動制限付きガバナンスです。ガバナンス可能なパラメータには、設定可能な値や一定期間に変更可能な値幅に制限があります。代表的な例としては、償還率フィードバック機構（4.2章）の初期バージョンが挙げられ、ガバナンストークン保有者がこれを微調整できます。

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やプロトコルの更新に期限を課す不変のスマートコントラストです。これはプロトコル自身をロックして外部からの介入を拒否する前に、ガバナンスがバグを修正できるかどうかを確認したい場合に使用することができます。アイスエイジはパラメータ名と影響を受けるコントラクトのアドレスを期限のレジストリと照合することで、変更が許可されているかどうかを確認します。期限が過ぎていれば、呼び出しは元に戻ります。

ガバナンスはプロトコル自身のロック開始日に近い時期にバグが発見された場合、アイスエイジを一定の回数だけ遅らせることができます。例えば、新たに実装されたバグ修正が適切にテストされるように、アイスエイジを3回、毎回1か月間だけ遅らせることができます。

ガバナンスが必要とされるコア領域

このフレームワークの初期段階では、特に4つの分野でガバナンスが必要になると考えています。

- 新しい担保の種類の追加：RAIはETHのみが担保となりますが、他のindexは複数の担保タイプが担保となり、ガバナンスは長期的にリスクを分散させることができます。

- 外部依存関係の変更：システムが依存しているオラクルやDEXを更新することができます。ガバナンスはシステムが正常に機能し続けるために、より新しい依存関係をシステムに示すことができます。

- 微調整可能なレートセッター：初期の金融政策制御器は、合理的な範囲内で変更可能なパラメータを持つ（「行動と時間に縛られたガバナンス」で説明されているように）

- システムバージョン間の移行：場合によっては、ガバナンスが新しいシステムを展開し、そのシステムにプロトコルトークンを発行する権限を与え、古いシステムからこの権限を取り消すことができます。この移行は、以下に概要を示す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

システムのバージョン間を移行するための簡単な仕組みを紹介します。

- 同じプロトコルトークンがいくつの異なるシステムをカバーしているのか、どのシステムがデット競売でプロトコルトークンを発行する許可を拒否されるかを記録する移行レジストリがあります。

- ガバナンスは新しいシステムバージョンを展開するたびに、システムのデット競売契約のアドレスを移行レジストリに提出します。またガバナンスはシステムがプロトコルトークンを発行するのを止めることができるかどうかを指定する必要があります。さらにガバナンスはいつでも、あるシステムが常にトークンを発行できるようにしておき、他への移行を発生させなくします。

- 新しいシステムを提案する時と、古いシステムから許可を取り消すときの間にはクールダウン期間があります。

- 発行権限を拒否された古いシステムを自動的にシャットダウンさせるオプショナルコントラストを設定することができます。

移行モジュールは特定のシステムに常にトークンを発行できる権限を自動的に与えるアイスエイジと組み合わせることができます。

システムの自動シャットダウン

システムが自動的に検知した結果、プロトコルトークンを焼却しなくてもシステムが勝手に決済をするケースもあります。

- 価格フィードの深刻な遅延：担保やindexの価格フィードのうち1つ以上が長期間にわたって更新されていないことをシステムが検知した場合

- システムの移行：これはオプショナルコントラクトで、ガバナンスがデット競売メカニズムでプロトコルトークンを発行する権限を撤回した時点（5.4.1章、制限付き移行モジュール）からクールダウン期間が経過した後、プロトコルを停止することができます

- 市場価格の一貫した乖離：indexの市場価格が償還価格に比べて長期間にわたって x % 乖離していることをシステムが検知すること。

ガバナンスは制限されたままでも、あるいはアイスエイジでシステムの一部がロックされ始めるまで、これらの自律的なシャットダウンモジュールを更新することができる。

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index、プロトコルトークン、ホワイトリストされたすべての担保タイプの3つです。価格フィードはガバナンス主導オラクルや、既に確立されたオラクルネットワークによって提供されます。

ガバナンス主導オラクル

ガバナントークンの保有者やプロトコルを立ち上げたコアチームは、オフチェーンで複数の価格フィードを収集する他のエンティティと提携し、全てのデータポイントを中央化するスマートコントラクトに単一トランザクションを提出することができます。

この方法ではオラクルインフラの更新や変更をより柔軟に行うことができますが、その分、信頼性が損なわれます。

Oracle Network Medianizer

Oracle Network Medianizer（ONM）とはガバナンスが直接制御しない複数ソース（例：index担保型と他のステーブルコイン間のUniswap V2プール）から価格を読み取り、全ての結果を中央可するスマートコントラクトです。ONMは以下のように動作します。

- コントラクトは、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されたオラクルネットワークの記録を保持しています。このコントラクトはシステムで発生した余剰金の一部で賄われています（11章の余剰金庫を使用）。各オラクルネットワークは支払いに特定のトークンを受け付けるため、コントラクトは各要求に必要な最小量とトークンの種類も記録しています。

- 新しい価格フィードをシステムにプッシュするためには、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際、コントラクトはまず安定性手数料の一部をオラクルの受け入れ可能なトークンの1つと交換します。オラクルが呼び出された後、コントラクトはその呼び出しを「有効」または「無効」としてタグ付けします。呼び出しが無効な場合、他のすべてのオラクルが呼び出され、コントラクトが有効な多数派が存在することが確認されるまで、特定の欠陥のあるオラクルは再び呼び出されません。有効なオラクルの呼び出しは元に戻してはならず、過去m 秒の間にチェーン上に提示された価格を取得しなければなりません。「取得」の意味は各オラクルの種類によって異なります。

    - すぐに結果が得られるプル型のオラクルの場合、コントラクトは料金を支払い、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、コントラクトは料金を支払い、オラクルを呼び出し、要求された価格を得るためにオラクルを再び呼び出す前に、特定の期間 n だけ待つ必要があります。

- すべてのオラクルの結果は配列に保存されます。ホワイトリストされたすべてのオラクルが呼び出された後、配列に過半数を形成するのに十分な有効データポイントがある場合（例えば、コントラクトが3/5のオラクルから有効データを受け取った場合）、結果はソートされ、コントラクトは中央値を選択します。

- コントラクトが過半数を見つけても見つけなくても、オラクルの結果が入った配列はクリアされ、コントラクトはプロセス全体を再度開始する前にp 秒間待つ必要があります。

オラクルネットワークバックアップ

ガバナンスはバックアップオラクルオプションを追加できます。このオプションはMedianizerが有効なオラクルネットワークの過半数を何度も連続して見つけることができなかった場合に、システムの価格をプッシュし始めます。

バックアップオプションは後から変更することができないため、Medianizerをデプロイする際に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中央値化メカニズムにとって代わっている時間が長すぎ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。

SAFE

indexを生成するために、誰もが自身の暗号担保をSAFEに預けてレバレッジをかけることができます。SAFEが有効な間は預かった担保の借り入れ率に応じて負債が発生し続けます。SAFE作成者が負債を返済するにつれ、ロックされた担保をより引き出せるようになります。

SAFEのライフサイクル

reflex indexを作成し、その後SAFEの負債を返済するためには、主に4つのステップが必要です。

- SAFEに担保を預ける

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

- SAFEの担保に裏付けられたindexの生成

  ユーザーは生成したいindexの数を指定します。システムは担保の借り入れ率に応じて発生し始める同額の債務を作成します。

- SAFEの負債を返す

  SAFE作成者が担保を引き出す際には、当初の債務に加えて経過利息を支払わなければなりません。

- 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の精算

システムの支払い能力を維持し、債務残高全体をカバーするために各SAFEは担保率が一定の閾値を下回った場合に精算されます。誰でも精算のトリガーを引くことができ、その場合システムはSAFEの担保を没収し、担保競売で売却します。

精算保険

このシステムのあるバージョンでは、SAFE作成者は自分のSAFEが精算されるときのトリガーを選択できるようになっています。トリガーとはSAFEに自動的に担保を追加し、精算から救う余地を生むスマートコントラクトを指します。トリガーの例としては、ショートポジションを売却するコントラクトや、Nexus Mutual [6]などの保険プロトコルと通信するコントラクトが挙げられます。

SAFEを保護するもう一つの方法は、安全とリスクという2つの異なる担保設定の閾値を追加することです。SAFEユーザーは（リスクよりも高い）SAFE閾値に達するまで負債を発生させることができ、SAFEの担保がリスク閾値を下回った場合にのみ精算されます。

担保競売

担保競売を開始するためにはシステムは *liquidationQuantity* という変数を使用して、各競売で考慮されるべき債務の額と、それに対応する売却されるべき担保の額を決定する必要があります。競売されたSAFEには精算ペナルティが適用されます。

担保競売のパラメータ

パラメータ名	説明
minimumBid	1回の入札で提示する必要のあるコインの最小量
discount	担保を売却する際の割引額
lowerCollateralMedianDeviation	オラクル価格と比較して担保中央値が取り得る下限偏差の最大値
upperCollateralMedianDeviation	オラクル価格と比較して担保中央値が取り得る上限偏差の最大値
lowerSystemCoinMedianDeviation	システムコインのオラクル価格と比較してシステムコインのオラクル価格フィードが取り得る下限偏差の最大値
upperSystemCoinMedianDeviation	システムコイン・オラクル価格と比較して、担保中央値が取り得る上限偏差の最大値
minSystemCoinMedianDeviation	中央値を考慮するため、償還価格と比較したシステムコインの中央値の偏差の最小値

担保競売の仕組み

固定割引競売は担保を売却してシステムコインと交換し、不良債権を処理するという（イングリッシュオークションに比べて）分かりやすい方法です。入札者は競売会社が自分のsafeEngine.coinBalanceを転送することに許可するだけで、buyCollateralを呼び出して、自分のシステムコインを直近の記録された市場価格よりも割引された価格で担保と交換することができます。

入札者はgetCollateralBoughtまたはgetApproximateCollateralBoughtを呼び出すことで、特定の競売で得られる担保の量を確認することもできます。getApproximateCollateralBoughtは

lastReadRedemptionPriceを使用しているのに対し、getCollateralBoughtはオラクルリレーからredemptionPriceの読み込み（および更新）をしているため、view修飾子が付いていないことに注意してください。

債務競売

担保競売ではSAFEの不良債権をすべてカバーできず、システムに余剰準備金がない場合、誰でも債務競売を行うことができます。

債務競売はより多くのプロトコルトークン（10章）を発行し、販売することでシステムに残っている不良債権を無効化することを目的としています。

債務競売を開始するためには、システムは2つのパラメータを使用する必要があります。

- initialDebtAuctionAmount：競売後に発行するプロトコルトークンの初期量
- debtAuctionBidSize：初期入札サイズ（*InitialDebtAuctionAmount*プロトコルトークンと引き換えに、いくつのindexを提供しなければならないか）

自律的債務競売のパラメータ設定

債務競売で発行されるプロトコルトークンの初期量はガバナンスの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ではシステムがプロトコルトークンとreflex indexの市場価格を読み取るオラクル（6章）と統合する必要があります。システムは次に*debtAuctionBidSize* indexのために発行されるプロトコルトークンの初期量（*initialDebtAuctionAmount*）を設定します。*initialDebtAuctionAmount*は、入札のインセンティブを高めるために、実際のプロトコル/index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。

債務競売のパラメータ

パラメータ名	説明
amountSoldIncrease	同量のindexに対して発行されるプロトコルトークンの量の増加
bidDecrease	次回入札における同量のindexに対するプロトコルトークンの受け入れ可能量の最小減少量
bidDuration	新しい入札が行われてから競売が継続する時間（秒）

totalAuctionLength	競売の合計時間（秒）
auctionsStarted	今までに何回競売が行われたか

債務競売の仕組み

担保競売とは異なり、債務競売には1つのステージしかありません。

decreaseSoldAmount(uint id, uint amountToBuy, uint bid)：一定量のindexと引き換えに受け入れるプロトコルトークンの量を減らします。

競売は入札がないと再スタートされ、そのたびに同じ量のindex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の量は*lastTokenAmount * amountSoldIncrease* / 100 として計算されます。競売が終了すると、システムは最高入札者のためにトークンを発行します。

プロトコルトークン

前章で説明したように、各プロトコルは債務競売で発行されたトークンによって保護される必要があります。トークンは保護以外にも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量は余剰金競売を利用して徐々に減少します。余剰資金が競売にかけられる前にシステムに発生する必要のある余剰資金の量は*surplusBuffer*と呼ばれ、発行された負債総額に対する割合として自動的に調整されます。

保険基金

ガバナンスはプロトコルトークンとは別に、無相関の資産を幅広く保有する保険基金を作り、それを債務競売の裏付けとして使用することができます。

余剰金競売

余剰金競売では、システムで発生した安定性手数料をプロトコルトークンで販売し、そのトークンは焼却されます。

余剰金競売のパラメータ

パラメータ名	説明

bidIncrease	次の入札での最小増加量
bidDuration	新しい入札が行われてから競売が継続する時間（秒）
totalAuctionLength	競売の合計時間（秒）
auctionsStarted	今までに何回競売が行われたか

余剰金競売の仕組み

余剰金競売はステージが1つです。

increaseBidSize(uint id, uint amountToBuy, uint bid)：誰でも同じ量のindex（余剰）に対して、より大きい量のプロトコルトークンを入札できます。全ての新しい入札は*lastBid* * *bidIncrease* / 100よりも高いか、または等しい必要があります。競売は最大*totalAuctionLength*秒が経過するか、最新の入札から*bidDuration*秒が経過し、その間に新しい入札が行われなかった場合に終了します。

競売は入札者がいない場合には再スタートします。一方、競売に少なくとも1件の入札があった場合、システムは最高額の入札者に余剰分を提供し、集まったプロトコルトークンを全て焼却します。

余剰index管理

ユーザーがindexを生成して暗黙的に負債を作るたびに、システムはユーザーのSAFEに借入金利の適用を開始します。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。

- 負債（9.2章）と余剰金（10.1章）の競売を行うために使用される*accounting engine*
- インフラの中核部分を賄い、外部のアクターにシステム維持のインセンティブを与える*surplus tresury*

余剰資金はシステムの3つのコアコンポーネントの資金調達を担当しています。

- オラクルモジュール（6章）。オラクルがどのように構成されているかに応じてトレジャリーは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ガバナンスを支払うか、またはオラクルネットワークに向けた呼び出しに支払いを行う。トレジャリーはオラクルを呼び出しや更新のためにガスを払ったアドレスに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保守する独立したチームも存在します。例えば、新しい担保の種類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です（4.2章）

トレジャリーは余剰金を受け取った人が将来自動的に資金援助を受けられなくなった際に、代わりに別の人が資金援助を受けられるように設定することができます。

外部アクター

システムは正常に機能するため、外部のアクターに依存しています。これらのアクターは、システムの健全性を維持するために競売やグローバルな決済処理、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よう経済的なインセンティブを与えられています。

できるだけ多くの人がプロトコルの安全性を保てるように、初期のユーザーインターフェースや自動化スクリプトを提供していきます。

参照可能な市場

RAIは主に2つの分野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を利用することで、現物保有のリスクを負わずにETHのような資産へのエクスポージャーを弱めることができます。

- 合成資産の担保：RAIはUMAやMakerDAO、Synthetixなどのプロトコルに暗号市場へのエクスポージャーを少なくし、2020年3月の暗黒の木曜日のような数百万ドル相当の暗号資産が清算されたシナリオの場合、ユーザーがポジションを解消する時間を稼ぐことができます。

今後の研究

分散型マネーの限界を押し広げ、分散型金融に更なる革新をもたらすために、ガバナンスの最小化や精算の仕組みといった中核的な分野での代替案を模索し続けます。

まず外部からのコントロールから自らをロックするプロトコルや市場の力に応じて適用する真の「マネーロボット」に関する将来の標準化のための基礎を築きたいと考えています。その後Ethereumコミュニティと担保や債務の競売に特に焦点を当てた我々の提案について議論し、改善策を画策します。

リスクと緩和策

reflex indexの開発と販売、そしてその上に構築される後続のシステムにはいくつかのリスクがあります。

- スマートコントラクトのバグ：このシステムの最大のリスクは誰もがすべての担保を引き出すことができるバグやプロトコルを復帰できない状態にロックしてしまうバグの可能性です。今後は複数のセキュリティ研究者によるコードのレビューを受け、テストネット上でシステムを稼働させてから、本番環境への導入を決定する予定です。

- オラクルの障害：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容易に偽の価格をフィードできないように一度に1つのオラクルのみを更新する厳格なルールを設けます。

- 担保のブラックスワン・イベント：裏付けとなる担保にブラックスワン・イベントが発生し、その結果、清算されるSAFEが大量に発生するリスクがあります。精算されても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、システムは適切な量の発行済み債務をカバーし、市場のショックに耐えられるように、余剰バッファを継続的に変更します。

- レートセッターのパラメータが不適切：自律的なフィードバックメカニズムは非常に実験的なものであり、シミュレーション時に予測したとおりの動作をしない可能性があります。予期せぬシナリオを避けるために、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ことを計画しています（ただし、制限はあります）。

- 健全なリクイデータ市場の立ち上げに失敗：リクイデーター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性を保つために参加できるよう、インターフェースや自動化されたスクリプトを作成する予定です。

まとめ

人間のコントロールから徐々にロックしていくプロトコルを提案し、reflex indexと呼ばれる低ボラティリティの担保付資産を発行しました。まずindexの市場価格に影響を与えるための自律的な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によって、トークン保有者がシステムに対して持つ力を制限する方法を説明しました。そして、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律的なスキームを説明し、最後にindexの発行とSAFEの精算のための一般的な仕組みを紹介しました。

引用

[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

用語集

reflex index：原資産のボラティリティを減衰させる担保付資産

RAI：最初のreflex index

償還価格：システムがindexに要求する価格。償還価格は市場価格が償還価格から乖離している場合に、（RRFMによって計算される）償還レートの影響を受けて変化する。SAFE作成者により多くの資金を生み出したり、負債の一部を返済させるよう影響を与えることを目的とする。

借入金利：借入残高のあるすべてのSAFEに適用される年間金利

償還レートフィードバックメカニズム（**RRFM)**：reflex indexの市場価格と償還価格を比較し、償還レートを算出する自律的なメカニズムでSAFE作成者がより多くのまたはより少ない債務を生み出すようにゆっくりと影響を与える（また暗黙のうちに市場価格と償還価格の乖離を最小化しようとする）

マネーマーケットセッター（**MMS)**：RRFMに似たメカニズムで、一度に複数の金融レバーを引くことができる。reflex indexの場合は、借入金利と償還価格の両方を変更する。

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コントロールされていない）から価格を引き出し、スローイングせずに過半数（例えば3/5）が結果を返した場合に中央値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保有者がシステムに対して持つ力を制限するスマートコントラクトのセット。時間の遅延を強制したり、ガバナンスが特定のパラメータを設定する可能性を制限したりする。

ガバナンスアイスエイジ：一定の期限が過ぎると、プロトコルのほとんどのコンポーネントを外部からの介入からロックする不変的なコントラクト

Accounting Engine：債務や余剰金の競売のトリガーとなるシステムコンポーネント。また現在競売にかけられている債務、未処理の不良債権、余剰バッファの量を記録する。

余剰金バッファ：発生した利息をシステム内に留めておく量。任意の金利。この閾値を超えて発生した分は、プロトコルトークンを焼却する余剰競売で販売されます。

余剰資金：別のシステムモジュールに未収利息の引き出しを許可するコントラクト（例：オラクルコールのONM)