Rai: Eine geringe Volatilität, minimiertes Vertrauen

Sicherheiten für das DeFi-Ökosystem

Stefan C. Ionescu, Ameen Soleimani

Mai 2020

Abstrakt. Wir stellen ein Governance-minimiertes, dezentralisiertes Protokoll vor, das automatisch auf Marktkräfte reagiert, um den Zielwert seines nativen besicherten Vermögenswerts zu ändern. Das Protokoll ermöglicht es jedem, seine Krypto-Assets zu nutzen und einen „Reflexindex“ auszugeben, der eine gedämpfte Version seiner zugrunde liegenden Sicherheiten ist. Wir skizzieren, wie Indizes als universelle Sicherheiten mit geringer Volatilität nützlich sein können, die ihre Inhaber sowie andere dezentrale Finanzprotokolle vor plötzlichen Marktbewegungen schützen können. Wir stellen unsere Pläne vor, um anderen Teams dabei zu helfen, ihre eigenen Kunststoffe auf den Markt zu bringen, indem wir unsere Infrastruktur nutzen. Schließlich bieten wir Alternativen zu aktuellen Orakel- und Governance-Strukturen, die häufig in vielen DeFiProtokollen zu finden sind.

Inhalt

1. Einleitung
2. Überblick über Reflexindizes
3. Designphilosophie und Go-to-Market-Strategie
4. Geldpolitische Mechanismen
    4.1. Einführung in die Kontrolltheorie
    4.2. Feedback-Mechanismus für die Rückzahlungsrate
        4.2.1. Komponenten
        4.2.2. Szenarien
        4.2.3. Algorithmus
        4.2.4. Abstimmung
    4.3. Geldmarktsetzer
    4.4. Globale Abwicklung

5. Verwaltung
5.1. Zeitlich begrenzte Governance
5.2. Aktionsgebundene Governance
5.3. Governance-Eiszeit
5.4. Kernbereiche, in denen Governance erforderlich ist
5.4.1. Eingeschränktes Migrationsmodul
6. Automatische Systemabschaltung
7. Orakel 7.1. Governance-geführte Orakel
7.2. Oracle Network Medianizer
7.2.1. Oracle-Netzwerksicherung
8. Tresore
8.1. SICHERER Lebenszyklus
9. SICHERE Liquidation
9.1. Sicherheiten-Auktion
9.1.1. Liquidationsversicherung 9.1.2. Auktionsparameter für Sicherheiten
9.1.3. Sicherheitenauktionsmechanismus
9.2. Schuldenauktion
9.2.1. Autonome Schuldenauktion Parametereinstellung
9.2.2. Parameter der Schuldenauktion
9.2.3. Schuldenauktionsmechanismus
10. Protokoll-Token
10.1. Überschuss-Auktionen
10.1.1. Überschussauktionsparameter
10.1.2. Überschussauktionsmechanismus
11. Verwaltung von Überschussindizes
12. Externe Akteure
13. Adressierbarer Markt
14. Zukunftsforschung
15. Risiken und Minderung
16. Zusammenfassung
17. Referenzen 18. Glossar

Einführung

Geld ist einer der mächtigsten Koordinationsmechanismen, die die Menschheit nutzt, um zu gedeihen. Das Privileg, die Geldmenge zu verwalten, wurde historisch in den Händen der souveränen Führung und der Finanzelite gehalten, während es einer unwissenden Öffentlichkeit auferlegt wurde. Wo Bitcoin das Potenzial für einen Basisprotest gezeigt hat, um einen Wertaufbewahrungswert für Rohstoffe zu manifestieren, bietet uns Ethereum eine Plattform, um durch Vermögenswerte gesicherte synthetische Instrumente zu bauen, die vor Volatilität geschützt und als Sicherheit verwendet oder an einen Referenzpreis gekoppelt werden können und als Tauschmittel für tägliche Transaktionen verwendet werden, die alle durch die gleichen Prinzipien des dezentralisierten Konsenses durchgesetzt werden.

Der erlaubnisfreie Zugang zu Bitcoin zur Speicherung von Vermögen und ordnungsgemäß dezentralisierte synthetische Instrumente auf Ethereum werden die Grundlage für die bevorstehende Finanzrevolution legen und denjenigen an den Rändern des modernen Finanzsystems die Mittel zur Koordinierung beim Aufbau des neuen bereitstellen.

In diesem Dokument stellen wir einen Rahmen für den Aufbau von Reflex-Indizes vor, einem neuen Anlagetyp, der anderen synthetischen Werten zum Erfolg verhelfen und einen wichtigen Baustein für die gesamte dezentralisierte Finanzbranche bilden wird.

Überblick über Reflexindizes

Der Zweck eines Reflexindex besteht nicht darin, eine bestimmte Bindung aufrechtzuerhalten, sondern die Volatilität seiner Sicherheiten zu dämpfen. Indizes ermöglichen es jedem, Zugang zum Kryptowährungsmarkt zu erhalten, ohne das gleiche Risiko wie beim Halten tatsächlicher Krypto-Assets. Wir glauben, dass RAI, unser erster Reflexindex, für andere Teams, die synthetische Wertpapiere auf Ethereum ausgeben (z. B. MakerDAOs MultiCollateral DAI [1], UMA [2], Synthetix [3]), unmittelbar nützlich sein wird, da ihre Systeme dadurch weniger stark gefährdet sind volatile Vermögenswerte wie ETH und bietet Benutzern mehr Zeit, ihre Positionen im Falle einer signifikanten Marktverschiebung zu schließen.

Um Reflexindizes zu verstehen, können wir das Verhalten ihres Rückzahlungspreises mit dem Preis einer Stablecoin vergleichen.

Der Rückzahlungspreis ist der Wert einer Schuldeinheit (oder Münze) im System. Es soll nur als internes Buchhaltungsinstrument verwendet werden und unterscheidet sich vom Marktpreis (dem Wert, zu dem der Markt die Münze handelt). Im Fall von Fiat-Backed Bei Stablecoins wie USDC erklären die Systembetreiber, dass jeder einen Coin für einen US-Dollar einlösen kann und somit der Einlösungspreis für diese Coins immer eins ist. Es gibt auch Fälle von kryptogestützten Stablecoins wie dem Multi Collateral DAI (MCD) von MakerDAO, bei denen das System auf eine feste Bindung von einem US-Dollar abzielt und somit auch der Rücknahmepreis auf eins festgelegt ist.

In den meisten Fällen wird es einen Unterschied zwischen dem Marktpreis einer Stablecoin und ihrem Rückzahlungspreis geben. Diese Szenarien schaffen Arbitragemöglichkeiten, bei denen Händler mehr Münzen erstellen, wenn der Marktpreis höher als die Rückzahlung ist, und sie werden ihre Stablecoins gegen Sicherheiten (z. B. US-Dollar im Fall von USDC) einlösen, falls der Marktpreis niedriger als der Rückzahlungspreis ist.

Reflex-Indizes ähneln Stablecoins, da sie auch einen Rücknahmepreis haben, auf den das System abzielt. Der Hauptunterschied in ihrem Fall besteht darin, dass ihre Rückzahlung nicht fest bleibt, sondern sich ändern soll, während sie von den Marktkräften beeinflusst wird. In Abschnitt 4 erklären wir, wie der Rücknahmepreis eines Index schwankt und neue Arbitrage-Möglichkeiten für seine Benutzer schafft.

Designphilosophie und Go-to-Market-Strategie

Unsere Designphilosophie besteht darin, Sicherheit, Stabilität und Liefergeschwindigkeit zu priorisieren.

Multi-Collateral DAI war der natürliche Ort, um mit der Iteration des RAI-Designs zu beginnen. Das System wurde streng geprüft und formal verifiziert, es hat minimale externe Abhängigkeiten und es hat eine aktive Expertengemeinschaft versammelt. Um den Entwicklungs- und Kommunikationsaufwand zu minimieren, wollen wir nur die einfachsten Änderungen an der ursprünglichen MCD-Codebasis vornehmen, um unsere Implementierung zu erreichen.

Zu unseren wichtigsten Modifikationen gehören die Hinzufügung eines autonomen Rate Setters, eines Oracle Network Medianizer, der mit vielen unabhängigen Preis-Feeds integriert ist, und einer Governance-Minimierungsschicht, die das System so weit wie möglich von menschlichen Eingriffen isolieren soll.

Die allererste Version des Protokolls (Stufe 1) wird nur den Rate Setter und andere geringfügige Verbesserungen in der Kernarchitektur enthalten. Sobald wir beweisen, dass der Setter wie erwartet funktioniert, können wir den Orakel-Medianizer (Stufe 2) und die GovernanceMinimierungsschicht (Stufe 3) sicherer hinzufügen.

Geldpolitische Mechanismen

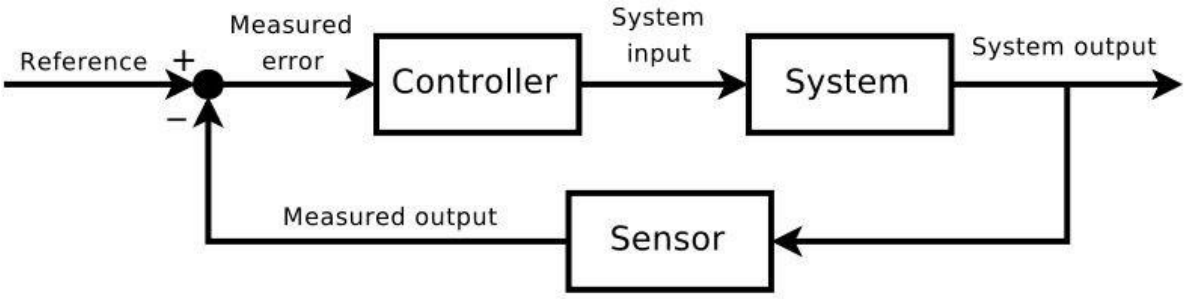
Einführung in die Kontrolltheorie

Ein gängiges Steuerungssystem, mit dem die meisten Menschen vertraut sind, ist die Dusche. Wenn jemand mit dem Duschen beginnt, hat er eine gewünschte Wassertemperatur im Sinn, die in der Regelungstheorie als bezeichnet wirdReferenzsollwert. Die Person, die alsController, misst kontinuierlich die Wasservorlauftemperatur (die als System bezeichnet wird Ausgang) ein nd ändert die Geschwindigkeit, mit der sie den Knopf der Dusche drehen, basierend auf der Abweichung(oder Fehler) zwischen der gewünschten und der aktuellen Temperatur. Die Geschwindigkeit, mit der der

Knopf gedreht wird, wird als System bezeichnetEingang. T Ziel ist es, den Knopf schnell genug zu drehen, um den Referenzsollwert schnell zu erreichen, aber nicht so schnell, dass die Temperatur überschwingt. Wenn es System gibtSchocks Wenn sich die Wasserdurchflusstemperatur plötzlich ändert, sollte die Person in der Lage sein, die aktuelle Temperatur aufrechtzuerhalten, indem sie weiß, wie schnell der Knopf als Reaktion auf die Störung gedreht werden muss.

Die wissenschaftliche Disziplin der Aufrechterhaltung der Stabilität in dynamischen Systemen wird Steuerungstheorie genannt und hat breite Anwendung in der Geschwindigkeitsregelung für Autos, der Flugnavigation, chemischen Reaktoren, Roboterarmen und industriellen Prozessen aller Art gefunden. Der Bitcoin-Schwierigkeitsanpassungsalgorithmus, der trotz einer variablen Hashrate die durchschnittliche Blockzeit von zehn Minuten beibehält, ist ein Beispiel für ein unternehmenskritisches Kontrollsystem.

In den meisten modernen Steuerungssystemen ist ein algorithmisch Regler ist typischerweise in den Prozess eingebettet und erhält die Kontrolle über einen Systemeingang (z. B. das Gaspedal eines Autos), um ihn automatisch zu aktualisieren, basierend auf Abweichungen zwischen dem Systemausgang (z. B. der Geschwindigkeit eines Autos) und dem Sollwert (z. B. der Tempomatgeschwindigkeit).).



Die gebräuchlichste Art von algorithmischen Controllern ist die PID-Regler. Über 95 % der industriellen Anwendungen und ein breites Spektrum biologischer Systeme verwenden Elemente der PID Kontrolle [4]. Ein PID-Regler verwendet eine mathematische Formel mit drei Teilen, um seine Ausgabe zu bestimmen:

Reglerausgang = Proportionalanteil + Integralanteil + Differentialanteil

Der anteilige Begriff ist der Teil des Controllers, der direkt istproportionalzur Abweichung. Wenn die Abweichung groß und positiv ist (z. B. der Tempomat-Geschwindigkeitssollwert ist viel höher als die aktuelle Geschwindigkeit des Fahrzeugs), ist die proportionale Reaktion groß und positiv (z. B. das Gaspedal durchtreten).

Der Integralanteil ist der Teil des Reglers, der berücksichtigt, wie lange eine Abweichung andauert. Es wird durch die Einnahme bestimmtIntegral- der Abweichung über die Zeit und dient in erster Linie zur Beseitigung von Steady-State-Fehler. Sie summiert sich auf, um auf kleine, aber anhaltende Abweichungen vom Sollwert zu reagieren (z. B. wenn der TempomatSollwert einige Minuten lang 1 km/h über der Fahrzeuggeschwindigkeit liegt).

Der Derivative Term ist der Teil des Controllers, der berücksichtigt, wie schnell die Abweichung wächst oder schrumpft. Es wird durch die Einnahme bestimmtDerivat der Abweichung und dient zur Beschleunigung der Reglerreaktion bei zunehmender Abweichung (z. B. beschleunigen, wenn der Tempomat-Sollwert höher als die Fahrzeuggeschwindigkeit ist und das Fahrzeug langsamer wird). Es trägt auch dazu bei, das Überschwingen zu reduzieren, indem es die Reaktion des Reglers verlangsamt, wenn die Abweichung schrumpft (z. B. Gas loslassen, wenn sich die Geschwindigkeit des Fahrzeugs dem Tempomat-Sollwert nähert).

Die Kombination dieser drei Teile, von denen jeder unabhängig abgestimmt werden kann, verleiht PID-Reglern eine große Flexibilität bei der Verwaltung einer Vielzahl von Steuersystemanwendungen.

PID-Regler funktionieren am besten in Systemen, die eine gewisse Verzögerung in der Reaktionszeit sowie die Möglichkeit eines Überschwingens und Oszillierens um den Sollwert herum zulassen, wenn das System versucht, sich selbst zu stabilisieren. Reflexindexsysteme wie RAI eignen sich gut für diese Art von Szenario, in dem ihre Rücknahmepreise durch PID-Controller geändert werden können.

Ganz allgemein wurde kürzlich entdeckt, dass viele der aktuellen geldpolitischen Regeln der Zentralbank (z. B. die Taylor-Regel) eigentlich Annäherungen an die PID sind Controller [5].

Feedback-Mechanismus für die Rückzahlungsrate

Der Rückzahlungsmechanismus ist die Systemkomponente, die für die Änderung des Rückzahlungspreises eines Reflex-Index zuständig ist. Um zu verstehen, wie es funktioniert, müssen wir zunächst beschreiben, warum das System einen Rückkopplungsmechanismus benötigt, im Gegensatz zur Verwendung einer manuellen Steuerung, und was die Ausgabe des Mechanismus ist.

Komponenten des Rückkopplungsmechanismus

Theoretisch wäre es möglich, den Rücknahmepreis des Reflex-Index (beschrieben in Abschnitt 2) direkt zu manipulieren, um Indexbenutzer zu beeinflussen und letztendlich den Marktpreis des Index zu verändern. In der Praxis würde diese Methode bei den Systemteilnehmern nicht die gewünschte Wirkung erzielen. Aus der Sicht eines SAFE-Inhabers könnte er bei einer einmaligen Erhöhung des Rücknahmepreises einen höheren Preis pro Schuldeinheit akzeptieren, den Verlust aus einer niedrigeren Besicherungsquote auffangen und seine Position halten. Wenn sie jedoch davon ausgehen, dass der Rückzahlungspreis im Laufe der Zeit weiter steigen wird, sind sie wahrscheinlich eher geneigt, erwartete zukünftige Verluste zu vermeiden und sich daher dafür zu entscheiden, ihre Schulden zurückzuzahlen und ihre Positionen zu schließen.

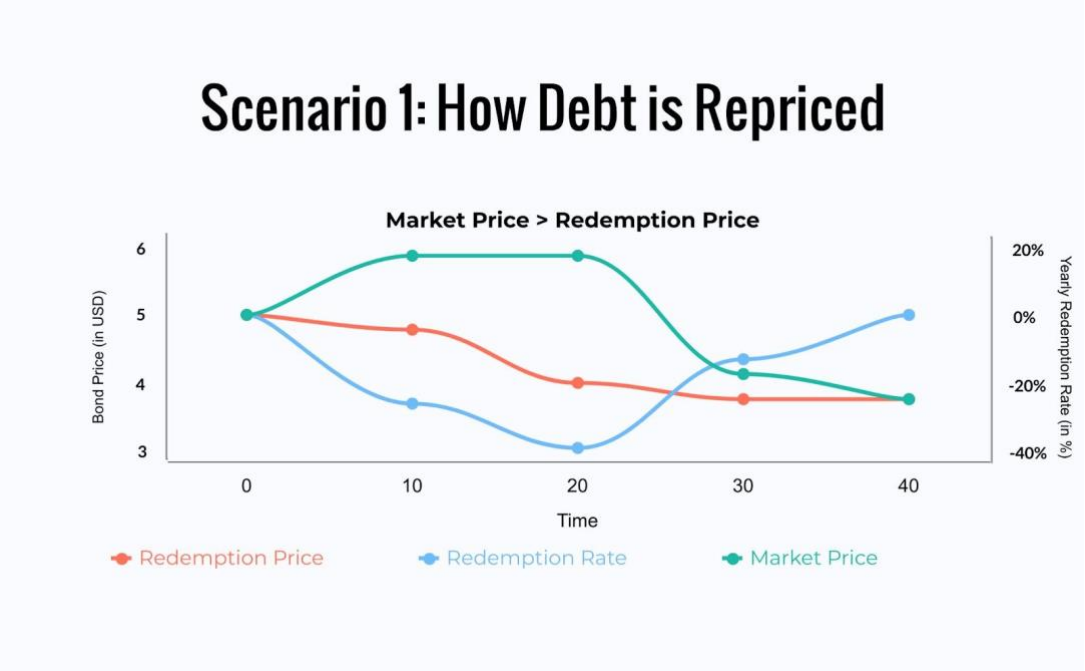
Wir erwarten, dass die Teilnehmer des Reflex-Indexsystems nicht direkt auf Änderungen des

Rücknahmepreises reagieren, sondern stattdessen auf die Änderungsrate des Rücknahmepreises die wir die nennenRückzahlungsquote. Der Rückzahlungskurs wird durch eine festgelegtFeedback-Mechanismus Diese Governance kann feinabgestimmt oder vollständig automatisiert werden.

Feedback-Mechanismus-Szenarien

Denken Sie daran, dass der Rückkopplungsmechanismus darauf abzielt, das Gleichgewicht zwischen dem Rücknahmepreis und dem Marktpreis aufrechtzuerhalten, indem der Rücknahmesatz verwendet wird, um Veränderungen der Marktkräfte entgegenzuwirken. Um dies zu erreichen, wird der Rücknahmesatz so berechnet, dass er der Abweichung zwischen Markt- und Rücknahmepreis entgegenwirkt.

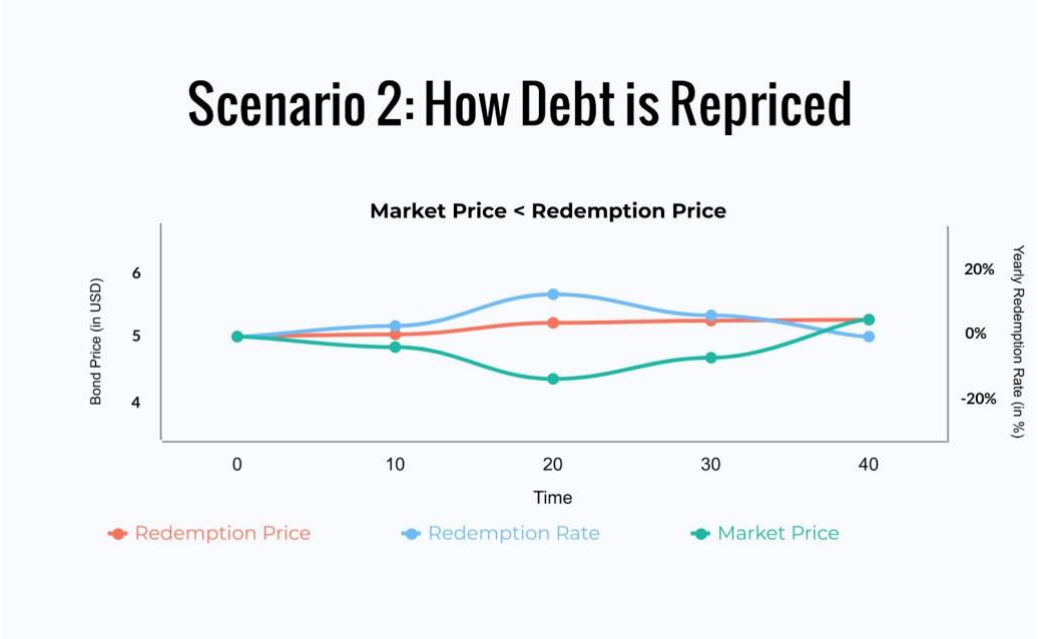
Wenn im ersten Szenario unten der Marktpreis des Index höher ist als sein Rückzahlungspreis, berechnet der Mechanismus einen negativen Zinssatz, der den Rückzahlungspreis zu senken beginnt, wodurch die Schulden des Systems billiger werden.



Die Erwartung eines sinkenden Rücknahmepreises wird Menschen wahrscheinlich davon abhalten, Indizes zu halten, und SAFE-Inhaber dazu ermutigen, mehr Schulden zu generieren (selbst wenn sich der Preis der Sicherheit nicht ändert), die dann auf dem Markt verkauft werden, wodurch Angebot und Nachfrage ausgeglichen werden. Beachten Sie, dass dies das ideale Szenario ist, in dem Indexinhaber schnell auf den Feedback-Mechanismus reagieren. In der Praxis (und insbesondere in den frühen Tagen nach der Einführung) erwarten wir eine Verzögerung zwischen dem Start des Mechanismus und den tatsächlichen Ergebnissen in der Höhe der ausgegebenen Schuldtitel und anschließend im Marktpreis.

Wenn andererseits in Szenario zwei der Marktpreis des Index niedriger als der Rückzahlungspreis ist, wird der Zinssatz positiv und beginnt, alle Schulden neu zu bewerten, sodass sie teurer werden.

Wenn Schulden teurer werden, sinken die Besicherungsquoten aller SAFEs (somit erhalten SAFE-Ersteller einen Anreiz, ihre Schulden zurückzuzahlen) und Benutzer beginnen, Indizes zu horten, in der Erwartung, dass sie an Wert gewinnen.



Feedback-Mechanismus-Algorithmus

Im folgenden Szenario gehen wir davon aus, dass das Protokoll einen Proportional-Integral-Controller verwendet, um die Rückzahlungsrate zu berechnen:

- Der Reflex-Index wird mit einem willkürlichen Rücknahmepreis „Rand“ eingeführt
- Irgendwann steigt der Marktpreis des Index von „Rand“ auf „Rand“ + x. Nachdem der Feedback-Mechanismus den neuen Marktpreis gelesen hat, berechnet er eine proportionale LaufzeitP, was in diesem Fall -1 * (('rand' + x) / 'rand') ist. Der Anteil ist negativ, um den Rücknahmepreis zu senken und die Indizes im Gegenzug günstiger zu bewerten
- Nach der Berechnung des Anteils bestimmt der Mechanismus den integralen Termich indem alle vergangenen Abweichungen von der letzten addiert werdenAbweichungIntervall Sekunden
- Der Mechanismus summiert das Proportionale und das Integral und berechnet eine RückzahlungsrateR pro Sekundedas beginnt langsam den Rücknahmepreis zu senken. Wenn die Schöpfer von SAFE erkennen, dass sie mehr Schulden generieren können, werden sie den Markt mit mehr Indizes überschwemmen

- Nachn Sekunden erkennt der Mechanismus, dass die Abweichung zwischen dem Markt- und dem Rücknahmepreis vernachlässigbar ist (unter einem bestimmten Parameter Lärm). An diesem Punkt setzt der Algorithmus r auf Null und behält den Rückzahlungspreis bei, wo er ist

In der Praxis wird der Algorithmus robuster sein und wir werden entweder einige Variablen unveränderlich machen (z. B. die Lärm Parameter,AbweichungIntervall) oder es wird strenge Grenzen dafür geben, was die Governance ändern kann.

Abstimmung des Rückkopplungsmechanismus

Von größter Bedeutung für das ordnungsgemäße Funktionieren des Reflexindexsystems ist die Abstimmung der algorithmischen Steuerungsparameter. Eine unsachgemäße Parametrierung könnte dazu führen, dass das System zu langsam ist, um Stabilität zu erreichen, massiv überschießt oder angesichts externer Schocks allgemein instabil ist.

Der Tuning-Prozess für einen PID-Regler umfasst typischerweise das Ausführen des Live-Systems, das Optimieren der Tuning-Parameter und das Beobachten der Reaktion des Systems, wobei häufig absichtlich Schocks auf dem Weg eingebracht werden. Angesichts der Schwierigkeit und des finanziellen Risikos, die Parameter eines Live-Reflexindexsystems zu optimieren, planen wir, Computermodellierung und -simulation so weit wie möglich zu nutzen, um die Anfangsparameter festzulegen, werden aber auch der Governance erlauben, die Abstimmungsparameter zu aktualisieren, wenn zusätzliche Daten aus der Produktion stammen zeigt, dass sie suboptimal sind.

Geldmarktsetzer

In RAI planen wir, den Fremdkapitalzinssatz (Zinssatz, der bei der Erstellung von Indizes angewendet wird) fest oder begrenzt zu halten und nur den Rückzahlungspreis zu ändern, wodurch die Komplexität bei der Modellierung des Rückkopplungsmechanismus minimiert wird. Der Sollzins entspricht in unserem Fall dem Spread zwischen der Stabilitätsgebühr und dem DSR im Multi-Collateral DAI.

Auch wenn wir planen, den Sollzins festzuhalten, ist es möglich, ihn parallel zum Rücknahmepreis über einen Geldmarktsetzer zu ändern. Der Geldmarkt verändert den Sollzins und den Rückzahlungspreis in einer Weise, die SAFE-Ersteller dazu anregt, mehr oder weniger Schulden zu machen. Wenn der Marktpreis eines Index über der Rückzahlung liegt, beginnen beide Kurse zu sinken, während, wenn er unter der Rückzahlung liegt, der Die Raten werden steigen.

Globale Abrechnung

Global Settlement ist eine Methode der letzten Instanz, die verwendet wird, um den Rücknahmepreis für alle Inhaber von Reflex-Indizes zu garantieren. Es soll sowohl Inhabern von Reflex-Indizes als auch Erstellern von SAFEs ermöglichen, Systemsicherheiten zu ihrem Nettowert (Menge an Indizes pro Sicherheitentyp gemäß dem letzten Rücknahmepreis) einzulösen. Jeder kann die Abwicklung auslösen, nachdem er eine bestimmte Menge an Protokolltoken gebrannt hat.

Die Abwicklung besteht aus drei Hauptphasen:

- **Abzug** : Die Abwicklung wird ausgelöst, Benutzer können keine SAFEs mehr erstellen, alle Sicherheitenpreis-Feeds und der Rücknahmepreis werden eingefroren und aufgezeichnet
- **Verfahren** : Alle ausstehenden Auktionen bearbeiten
- **Beanspruchen** : Jeder Reflex-Index-Inhaber und SAFE-Ersteller kann einen festen Betrag einer beliebigen Systemsicherheit basierend auf dem letzten aufgezeichneten Rücknahmepreis des Index beanspruchen

Führung

Die überwiegende Mehrheit der Parameter wird unveränderlich sein und die inneren intelligenten Vertragsmechanismen werden nicht aktualisierbar sein, es sei denn, Inhaber von Governance-Token setzen ein völlig neues System ein. Wir haben uns für diese Strategie entschieden, weil wir das Meta-Spiel eliminieren können, bei dem Menschen versuchen, den Governance-Prozess zu ihrem eigenen Vorteil zu beeinflussen und so das Vertrauen in das System zu beschädigen. Wir stellen den ordnungsgemäßen Betrieb des Protokolls her, ohne zu viel Vertrauen in Menschen zu setzen (der „Bitcoin-Effekt“), damit wir die soziale Skalierbarkeit maximieren und die Risiken für andere Entwickler minimieren, die RAI als Kerninfrastruktur in ihren eigenen Projekten verwenden möchten.

Für die wenigen Parameter, die geändert werden können, schlagen wir die Hinzufügung eines Restricted Governance Module vor, das alle möglichen Systemänderungen verzögern oder einschränken soll. Darüber hinaus präsentieren wir Governance Ice Age, eine Berechtigungsregistrierung, die einige Teile des Systems nach Ablauf bestimmter Fristen vor der Kontrolle von außen sperren kann.

Zeitlich begrenzte Governance

Time Bounded Governance ist die erste Komponente des Restricted Governance Module. Es führt zu Zeitverzögerungen zwischen Änderungen, die auf denselben Parameter angewendet werden. Ein Beispiel ist die Möglichkeit, die Adressen der verwendeten Orakel im Oracle Network Medianizer (Abschnitt 6.2) nach mindestens zu ändernT_S Sekunden sind seit der letzten Oracle-Modifikation vergangen.

Aktionsgebundene Governance

Die zweite Komponente im Restricted Governance Module ist Action Bounded Governance. Jeder regelbare Parameter hat Grenzen, auf welche Werte er eingestellt werden kann und wie stark er sich über einen bestimmten Zeitraum ändern kann. Bemerkenswerte Beispiele sind die ersten Versionen des Redemption Rate Feedback Mechanism (Abschnitt 4.2), die Governance-TokenInhaber verfeinern können.

Governance-Eiszeit

The Ice Age ist ein unveränderlicher Smart Contract, der Fristen für die Änderung bestimmter Systemparameter und die Aktualisierung des Protokolls vorschreibt. Es kann verwendet werden, wenn die Verwaltung sicherstellen möchte, dass sie Fehler beheben kann, bevor sich das Protokoll selbst sperrt und Eingriffe von außen verweigert. Ice Age überprüft, ob eine Änderung zulässig ist, indem es den Namen des Parameters und die Adresse des betroffenen Vertrags mit einem Fristenregister vergleicht. Wenn die Frist verstrichen ist, wird der Anruf zurückgestellt.

Die Governance kann Ice Age möglicherweise eine festgelegte Anzahl von Malen verzögern, wenn Fehler in der Nähe des Datums gefunden werden, an dem das Protokoll beginnen sollte, sich selbst zu sperren. Ice Age kann beispielsweise nur dreimal um jeweils einen Monat verschoben werden, damit die neu implementierten Bugfixes ordentlich getestet werden.

Kernbereiche, in denen Governance erforderlich ist

Wir stellen uns vier Bereiche vor, in denen Governance erforderlich sein könnte, insbesondere in den frühen Versionen dieses Frameworks:

- **Hinzufügen neuer Sicherheitentypen** : RAI wird nur von der ETH unterstützt, aber andere Indizes werden von mehreren Arten von Sicherheiten unterstützt und Governance wird möglich sein

  um das Risiko im Laufe der Zeit zu streuen

- **Ändere externe Abhängigkeiten** : Oracles und DEXs, von denen das System abhängt, können aktualisiert werden. Governance kann das System auf neuere Abhängigkeiten hinweisen, damit es weiterhin ordnungsgemäß funktioniert

- **Feinabstimmung der Rateneinsteller** : Frühzeitige geldpolitische Controller werden Parameter haben, die innerhalb vernünftiger Grenzen geändert werden können (wie in Action and Time Bounded Governance beschrieben)

- **Migration zwischen Systemversionen**: In einigen Fällen kann die Governance ein neues

System bereitstellen, ihm die Erlaubnis erteilen, Protokolltoken zu drucken, und diese Erlaubnis einem alten System entziehen. Diese Migration wird mit Hilfe des unten beschriebenen eingeschränkten Migrationsmoduls durchgeführt

Eingeschränktes Migrationsmodul

Das Folgende ist ein einfacher Mechanismus zum Migrieren zwischen Systemversionen:

- Es gibt ein Migrationsregister, das nachverfolgt, wie viele verschiedene Systeme das gleiche Protokoll-Token abdeckt und welchen Systemen die Erlaubnis zum Drucken von ProtokollToken in einer Schuldenauktion verweigert werden kann

- Jedes Mal, wenn die Governance eine neue Systemversion einsetzt, übermittelt sie die Adresse des Schuldenauktionsvertrags des Systems im Migrationsregister. Governance muss auch spezifizieren, ob sie jemals in der Lage sein wird, das System daran zu hindern, Protokoll-Tokens zu drucken. Außerdem kann die Governance jederzeit sagen, dass ein System immer in der Lage sein wird, Tokens zu drucken, und daher niemals migriert wird

- Zwischen dem Vorschlagen eines neuen Systems und dem Entzug der Berechtigungen für ein altes System gibt es eine Ruhephase

- Ein optionaler Vertrag kann so eingerichtet werden, dass ein altes System automatisch heruntergefahren wird, nachdem ihm die Druckberechtigung verweigert wurde

Das Migrationsmodul kann mit einem Ice Age kombiniert werden, das bestimmten Systemen automatisch die Erlaubnis gibt, Token immer drucken zu können.

Automatische Systemabschaltung

Es gibt Fälle, die das System automatisch erkennen und dadurch die Abwicklung selbst auslösen kann, ohne dass Protokoll-Tokens verbrannt werden müssen:

- **Schwere Preis-Feed-Verzögerungen** : Das System erkennt, dass eine oder mehrere der Sicherheiten- oder Indexpreis-Feeds seit langem nicht mehr aktualisiert wurden

- **Systemmigration** : Dies ist ein optionaler Vertrag, der das Protokoll abschalten kann, nachdem eine Ruhezeit verstrichen ist, nachdem die Governance die Fähigkeit des

Schuldenauktionsmechanismus zum Drucken von Protokoll-Token entzogen hat (Restricted Migration Module, Abschnitt 5.4.1).

- **Konsequente Marktpreisabweichung** : Das System erkennt, dass der Marktpreis des Index gewesen ist x% lange Zeit gegenüber dem Rücknahmepreis abgewichen

Governance wird in der Lage sein, diese autonomen Shutdown-Module zu aktualisieren, während sie noch begrenzt sind oder bis die Eiszeit beginnt, einige Teile des Systems zu sperren.

Orakel

Es gibt drei Haupt-Asset-Typen, für die das System Preis-Feeds lesen muss: den Index, das ProtokollToken und alle Arten von Sicherheiten auf der Whitelist. Die Preis-Feeds können von Governancegeführten Orakeln oder von bereits etablierten Orakel-Netzwerken bereitgestellt werden.

Governance-geführte Orakel

Governance-Token-Inhaber oder das Kernteam, das das Protokoll eingeführt hat, können mit anderen Unternehmen zusammenarbeiten, die mehrere Preis-Feeds außerhalb der Kette sammeln und dann eine einzelne Transaktion an einen intelligenten Vertrag senden, der alle Datenpunkte medianisiert.

Dieser Ansatz ermöglicht mehr Flexibilität beim Aktualisieren und Ändern der OracleInfrastruktur, obwohl dies auf Kosten der Vertrauenslosigkeit geht.

Oracle Network Medianizer

Ein Oracle Network Medianizer ist ein intelligenter Vertrag, der Preise aus mehreren Quellen liest, die nicht direkt von der Governance kontrolliert werden (z. B. Uniswap V2-Pool zwischen einem Indexsicherheitentyp und anderen Stablecoins) und dann alle medianisiert Ergebnisse. ONM funktioniert wie folgt:

- Unser Vertrag verfolgt Oracle-Netzwerke auf der Whitelist, die er anrufen kann, um Preise für Sicherheiten anzufordern. Der Vertrag wird durch einen Teil des Überschusses finanziert, den das System erwirtschaftet (unter Verwendung der Überschusskasse, Abschnitt 11). Jedes Orakelnetzwerk akzeptiert bestimmte Token als Zahlungsmittel, sodass unser Vertrag auch den Mindestbetrag und die Art der für jede Anfrage erforderlichen Token verfolgt

- Um einen neuen Preis-Feed in das System zu pushen, müssen vorher alle Orakel angerufen werden. Beim Anrufen eines Orakels tauscht der Vertrag zunächst einige Stabilitätsgebühren

gegen einen der vom Orakel akzeptierten Token. Nachdem ein Orakel aufgerufen wurde, kennzeichnet der Vertrag den Aufruf als „gültig“ oder „ungültig“. Wenn ein Aufruf ungültig ist, kann das bestimmte fehlerhafte Orakel nicht erneut aufgerufen werden, bis alle anderen aufgerufen wurden und der Vertrag prüft, ob eine gültige Mehrheit vorliegt. Ein gültiger Orakelaufruf darf nicht rückgängig gemacht werden und muss einen Preis abrufen, der irgendwann im letzten Jahr in der Kette veröffentlicht wurdem Sekunden. „Abrufen“ bedeutet je nach Orakeltyp unterschiedliche Dinge:

- ○ Für Pull-basierte Orakel, von denen wir sofort ein Ergebnis erhalten können, muss unser Vertrag eine Gebühr zahlen und den Preis direkt abrufen
- ○ Für Push-basierte Orakel zahlt unser Vertrag die Gebühr, ruft das Orakel auf und muss eine bestimmte Zeit wartenn bevor Sie das Orakel erneut anrufen, um den angeforderten Preis zu erhalten

- ● Jedes Oracle-Ergebnis wird in einem Array gespeichert. Nachdem jedes Orakel auf der weißen Liste aufgerufen wurde und wenn das Array genügend gültige Datenpunkte hat, um eine Mehrheit zu bilden (z. B. der Vertrag hat gültige Daten von 3/5 Orakeln erhalten), werden die Ergebnisse sortiert und der Vertrag wählt den Median

- ● Unabhängig davon, ob der Vertrag eine Mehrheit findet oder nicht, wird das Array mit Oracle-Ergebnissen gelöscht und der Vertrag muss wartenP Sekunden, bevor der gesamte Vorgang von vorne beginnt

Oracle-Netzwerksicherung

Governance kann eine Backup-Oracle-Option hinzufügen, die beginnt, die Preise im System zu drücken, wenn der Medianizer mehrmals hintereinander keine Mehrheit gültiger Oracle-Netzwerke finden kann.

Die Sicherungsoption muss beim Einsatz des Medianizers eingestellt werden, da sie nachträglich nicht mehr geändert werden kann. Darüber hinaus kann ein separater Vertrag überwachen, ob das Backup den Medianisierungsmechanismus zu lange ersetzt hat, und das Protokoll automatisch abschalten.

Tresore

Um Indizes zu generieren, kann jeder seine Krypto-Sicherheiten in Safes hinterlegen und nutzen. Während ein SAFE geöffnet ist, werden entsprechend dem Sollzinssatz der hinterlegten Sicherheiten weiterhin Schulden anfallen. Wenn der SAFE-Ersteller seine Schulden zurückzahlt, kann er immer mehr seiner gesperrten Sicherheiten abheben.

Es sind vier Hauptschritte erforderlich, um Reflex-Indizes zu erstellen und anschließend die Schulden eines SAFEs zurückzuzahlen:

- Hinterlegen Sie Sicherheiten im SAFE

  Der Benutzer muss zunächst einen neuen SAFE erstellen und Sicherheiten darin hinterlegen.

- Generieren Sie Indizes, die durch die Sicherheiten des SAFE gedeckt sind

  Der Benutzer gibt an, wie viele Indizes er generieren möchte. Das System erstellt einen gleichen Schuldenbetrag, der entsprechend dem Sollzinssatz der Sicherheit anwächst.

- Zahlen Sie die SAFE-Schulden zurück

  Wenn der SAFE-Ersteller seine Sicherheiten zurückziehen möchte, muss er seine ursprüngliche Schuld zuzüglich der aufgelaufenen Zinsen zurückzahlen.

- Sicherheiten zurückziehen

  Nachdem der Benutzer einen Teil oder alle seine Schulden zurückgezahlt hat, kann er seine Sicherheiten zurückziehen.

SICHERE Liquidation

Um das System solvent zu halten und den Wert der gesamten ausstehenden Schuld zu decken, kann jeder SAFE liquidiert werden, falls seine Besicherungsquote unter einen bestimmten Schwellenwert fällt. Jeder kann eine Liquidation auslösen, in diesem Fall konfisziert das System die Sicherheiten des SAFE und verkauft sie in einem Sicherheiten Auktion.

Liquidationsversicherung

In einer Version des Systems haben SAFE-Ersteller die Möglichkeit, eine Abzug wenn ihre SAFEs liquidiert werden. Auslöser sind intelligente Verträge, die automatisch mehr Sicherheiten in einem SAFE hinzufügen und ihn möglicherweise vor der Liquidation bewahren. Beispiele für Auslöser sind Verträge, die Short-Positionen verkaufen, oder Verträge, die mit Versicherungsprotokollen wie Nexus Mutual kommunizieren [6].

Eine weitere Methode zum Schutz von SAFEs ist das Hinzufügen von zwei verschiedenen Besicherungsschwellen: sicher undRisiko. SAFE-Benutzer können Schulden generieren, bis sie die sichere Schwelle erreichen (die höher ist als das Risiko), und sie werden nur dann liquidiert, wenn die Besicherung des SAFE unter die Risikoschwelle fällt.

Sicherheiten-Auktionen

Um eine Auktion für Sicherheiten zu starten, muss das System eine Variable namens verwenden LiquidationMenge um bei jeder Auktion die zu deckende Forderungssumme und die entsprechende zu verkaufende Sicherheitenhöhe zu ermitteln. EinLiquidationsstrafe wird auf jeden ersteigerten SAFE angewendet.

Auktionsparameter für Sicherheiten

Parametername	Beschreibung
Mindestgebot	Mindestmenge an Münzen, die benötigt werden in einem Angebot angeboten werden
Rabatt	Diskont, zu dem Sicherheiten verkauft werden
LowerCollateralMedianDeviation	Maximale Abweichung der unteren Grenze, mit der der Median der Sicherheiten verglichen werden kann der Orakelpreis
obereSicherheitenMedianAbweichung	Maximale Obergrenzenabweichung, mit der der Median der Sicherheiten verglichen werden kann der Orakelpreis
LowerSystemCoinMedianDeviation	Maximale untere Grenzabweichung, die der System-Coin-Orakel-Preis-Feed haben kann im Vergleich zum System Münzorakel Preis
UpperSystemCoinMedianDeviation	Maximale Obergrenzenabweichung, mit der der Median der Sicherheiten verglichen werden kann Der Orakelpreis der Systemmünze
minSystemCoinMedianAbweichung	Min. Abweichung für die Systemmünze Medianergebnis im Vergleich zum Rücknahmepreis, um die Median berücksichtigt

Sicherheitenauktionsmechanismus

Die Fixed-Discount-Auktion ist eine unkomplizierte Möglichkeit (im Vergleich zu englischen Auktionen), Sicherheiten im Austausch gegen Systemmünzen, die zur Begleichung uneinbringlicher Schulden verwendet werden, zum Verkauf anzubieten. Bieter sind lediglich verpflichtet, dem Auktionshaus die Übertragung ihrer `safeEngine.coinBalance` und kann dann anrufen `Sicherheiten kaufen` um ihre auszutauschen Systemmünzen für Sicherheiten, die mit einem Abschlag im Vergleich zu ihrem zuletzt aufgezeichneten Marktpreis verkauft werden.

Bieter können auch die Höhe der Sicherheiten überprüfen, die sie von einer bestimmten Auktion erhalten können, indem sie

anrufen getCollateralBought odeGetApproximateCollateralBoughtr . Beachten Sie, dass getCollateralBought wird nicht als Ansicht markiert, da es die liest (und auch aktualisiert). Einlösungspreis vom Orakel-Relayer, während GetApproximateCollateralBought nutzt die lastReadRedemptionPrice .

Schuldenauktionen

In dem Szenario, in dem eine Collateral Auction nicht alle uneinbringlichen Forderungen in einem SAFE abdecken kann und das System keine Überschussreserven hat, kann jeder eine Debt Auction auslösen.

Schuldenauktionen sollen mehr Protokoll-Token (Abschnitt 10) prägen und sie für Indizes verkaufen, die die verbleibenden uneinbringlichen Schulden des Systems zunichte machen können.

Um eine Schuldenauktion zu starten, muss das System zwei Parameter verwenden:

- initialDebtAuctionAmount : die anfängliche Menge an zu prägenden Protokolltoken nach der Auktion
- DebtAuctionBidSize : die anfängliche Gebotsgröße (wie viele Indizes müssen angeboten werden Austausch gegeninitialDebtAuctionAmount Protokoll-Token)

Autonome Schuldenauktion Parametereinstellung

Die anfängliche Menge der in einer Schuldenauktion geprägten Protokoll-Token kann entweder durch eine Governance-Abstimmung festgelegt oder automatisch vom System angepasst werden. Eine automatisierte Version müsste in Orakel (Abschnitt 6) integriert werden, aus denen das System die Marktpreise des Protokolltokens und des Reflexindex lesen würde. Das System würde dann die anfängliche Menge an Protokolltoken (initialDebtAuctionAmount), die geprägt werden für DebtAuctionBidSize Indizes. initialDebtAuctionAmountkann im Vergleich zum tatsächlichen PROTOKOLL/INDEX-Marktpreis mit einem Abschlag festgelegt werden, um Anreize für Gebote zu schaffen.

Parameter der Schuldenauktion

Parametername	Beschreibung
verkaufter BetragErhöhung	Erhöhung der Protokollmenge Tokens, die dafür geprägt werden Menge an Indizes
bidDecrease	Die Mindestabnahme des nächsten Gebots in der akzeptierten Menge an Protokolltoken für die gleiche Anzahl von Indizes

Gebotsdauer	Wie lange dauert das Bieten nach einem neuen Gebot wird abgegeben (in Sekunden)
totalAuctionLength	Gesamtdauer der Auktion (in Sekunden)
Auktionen gestartet	Wie viele Auktionen haben begonnen bis jetzt

Schuldenauktionsmechanismus

Im Gegensatz zu Sicherheitenauktionen haben Schuldenauktionen nur eine Stufe:

:VerringernSoldAmount(uint id, uint betragToBuy, uint bid) Verringerung der Menge an Protokoll-Token, die im Austausch gegen eine feste Anzahl von Indizes akzeptiert werden.

Die Auktion wird neu gestartet, wenn keine Gebote abgegeben wurden. Bei jedem Neustart bietet das System mehr Protokolltoken für die gleiche Anzahl von Indizes an. Die neue ProtokollToken-Menge wird wie folgt berechnet:letzte TokenAmount *verkaufter BetragErhöhung / 100. Nachdem die Auktion abgeschlossen ist, prägt das System Token für den Höchstbietenden.

Protokoll-Token

Wie in früheren Abschnitten beschrieben, muss jedes Protokoll durch einen Token geschützt werden, der durch Schuldenauktionen geprägt wird. Abgesehen vom Schutz wird das Token verwendet, um einige Systemkomponenten zu steuern. Außerdem wird das Protokoll-Token-Angebot durch den Einsatz von Überschussauktionen schrittweise reduziert. Der Überschussbetrag, der im System anfallen muss, bevor zusätzliche Gelder versteigert werden, wird als bezeichnetÜberschusspuffer und es wird automatisch als Prozentsatz der ausgegebenen Gesamtschuld angepasst.

Versicherungsfonds

Abgesehen vom Protokoll-Token kann die Governance einen Versicherungsfonds schaffen, der eine breite Palette von nicht korrelierten Vermögenswerten hält und der als Backstop für Schuldenauktionen verwendet werden kann.

Überschuss-Auktionen

Überschussauktionen verkaufen im System anfallende Stabilitätsgebühren für Protokolltoken, die dann verbrannt werden.

Überschüssige Auktionsparameter

Parametername	Beschreibung
GebotErhöhung	Mindesterhöhung im nächsten Gebot
Gebotsdauer	Wie lange dauert die Auktion nach einem neuen Gebot wird abgegeben (in Sekunden)
totalAuctionLength	Gesamtdauer der Auktion (in Sekunden)
Auktionen gestartet	Wie viele Auktionen haben begonnen bis jetzt

Überschuss-Auktionsmechanismus

Überschussauktionen sind einstufig:

`ErhöhenBidSize(Uint-ID, Uint-BetragZuKaufen, Uint-Gebot)`

: Jeder kann einen höheren Betrag bieten Protokolltoken für die gleiche Menge an Indizes (Überschuss). Jedes neue Gebot muss größer oder gleich seinletztesGebot *GebotErhöhung / 100. Die Auktion endet nach maximal totalAuctionLength Sekunden oder danachGebotsdauer seit dem letzten Gebot sind Sekunden vergangen und es wurden in der Zwischenzeit keine neuen Gebote abgegeben.

Eine Auktion wird neu gestartet, wenn sie keine Gebote hat. Wenn die Auktion andererseits mindestens ein Gebot hat, bietet das System den Überschuss dem Höchstbietenden an und verbrennt dann alle gesammelten Protokolltoken.

Verwaltung von Überschussindizes

Jedes Mal, wenn ein Benutzer Indizes generiert und implizit Schulden erstellt, beginnt das System, einen Sollzinssatz auf den SAFE des Benutzers anzuwenden. Die aufgelaufenen Zinsen werden in zwei verschiedenen Smart Contracts gepoolt:

- DieAbrechnungsmaschineverwendet, um Schulden (Abschnitt 9.2) und Überschuss (Abschnitt 10.1) Auktionen
- Der überschüssige Schatzkammer verwendet, um Kerninfrastrukturkomponenten zu finanzieren und externe Akteure zur Wartung des Systems anzuregen

Die Überschusskasse ist für die Finanzierung von drei Kernsystemkomponenten zuständig:

- Oracle-Modul (Abschnitt 6). Je nachdem, wie ein Orakel strukturiert ist, bezahlt das Finanzministerium entweder Governance-Whitelists, Off-Chain-Orakel oder es zahlt für Aufrufe an Orakelnetzwerke. Die Schatzkammer kann auch so eingerichtet werden, dass sie die Adressen, die Benzin ausgegeben haben, bezahlt, um ein Orakel anzurufen und es zu aktualisieren

- In einigen Fällen unabhängige Teams, die das System warten. Beispiele sind Teams, die neue Sicherheitentypen auf die Whitelist setzen oder den Kurssetzer des Systems optimieren (Abschnitt 4.2).

Die Schatzkammer kann so eingerichtet werden, dass einigen Überschussempfängern zukünftig automatisch die Förderung verweigert wird und andere an ihre Stelle treten können.

Externe Akteure

Das System ist auf externe Akteure angewiesen, um ordnungsgemäß zu funktionieren. Diese Akteure haben einen wirtschaftlichen Anreiz, sich an Bereichen wie Auktionen, globaler Abwicklung, Market Making und Aktualisierung von Preis-Feeds zu beteiligen, um die Gesundheit des Systems aufrechtzuerhalten.

Wir werden erste Benutzeroberflächen und automatisierte Skripte bereitstellen, damit so viele Menschen wie möglich das Protokoll sicher halten können.

Adressierbarer Markt

Wir sehen RAI in zwei Hauptbereichen als nützlich an:

- **Diversifikation des Portfolios** : Anleger nutzen RAI, um ein gedämpftes Engagement in einem Vermögenswert wie ETH zu erhalten, ohne das ganze Risiko eingehen zu müssen, Ether tatsächlich zu halten

- **Sicherheiten für synthetische Vermögenswerte** : RAI kann Protokollen wie UMA, MakerDAO und Synthetix ein geringeres Engagement im Kryptomarkt bieten und den Benutzern mehr Zeit geben, ihre Positionen im Falle von Szenarien wie dem Schwarzen Donnerstag ab März 2020 zu verlassen, als Krypto-Assets im Wert von Millionen von Dollar waren liquidiert

Zukunftsforschung

Um die Grenzen des dezentralisierten Geldes zu erweitern und weitere Innovationen in die dezentralisierte Finanzierung einzubringen, werden wir weiterhin nach Alternativen in Kernbereichen wie GovernanceMinimierung und Liquidationsmechanismen suchen.

Wir wollen zunächst den Grundstein für zukünftige Standards rund um Protokolle legen, die sich der Kontrolle von außen entziehen, und für echte „Geldroboter“, die sich an die Marktkräfte anpassen. Anschließend laden wir die Ethereum-Community ein, Verbesserungen rund um unsere Vorschläge mit besonderem Fokus auf Sicherheiten- und Schuldenauktionen zu diskutieren und zu entwerfen.

Risiken und Minderung

Die Entwicklung und Einführung eines Reflexindex sowie darauf aufbauender Folgesysteme birgt mehrere Risiken:

- **Intelligente Vertragsfehler** : Das größte Risiko für das System ist die Möglichkeit eines Fehlers, der es jedem ermöglicht, alle Sicherheiten zu extrahieren, oder das Protokoll in einem Zustand sperrt, aus dem es sich nicht mehr erholen kann. Wir planen, unseren Code von mehreren Sicherheitsforschern überprüfen zu lassen und das System in einem Testnetz zu starten, bevor wir uns verpflichten, es in der Produktion einzusetzen

- **Oracle-Fehler** : Wir werden Feeds aus mehreren Orakelnetzwerken aggregieren und es wird strenge Regeln geben, um jeweils nur ein Orakel zu aktualisieren, damit böswillige Regierungsführung nicht so einfach falsche Preise einführen kann

- **Begleitende Black Swan-Ereignisse** : Es besteht das Risiko eines Black-Swan-Ereignisses in der zugrunde liegenden Sicherheit, was zu einer hohen Anzahl liquidierter SAFEs führen kann. Liquidationen sind möglicherweise nicht in der Lage, die gesamten ausstehenden Forderungsausfälle abzudecken, und daher wird das System seinen Überschusspuffer kontinuierlich ändern, um einen angemessenen Betrag der ausgegebenen Schuldtitel abzudecken und Marktschocks standzuhalten

- **Falsche Rate-Setter-Parameter** : Autonome Rückkopplungsmechanismen sind sehr experimentell und verhalten sich möglicherweise nicht genau so, wie wir es in Simulationen vorhersagen. Wir planen, der Governance die Feinabstimmung dieser Komponente zu ermöglichen (während sie noch begrenzt ist), um unerwartete Szenarien zu vermeiden

- **Versäumnis, einen gesunden Liquidatorenmarkt aufzubauen** : Liquidatoren sind wichtige Akteure, die sicherstellen, dass alle ausgegebenen Schulden durch Sicherheiten gedeckt sind. Wir planen, Schnittstellen und automatisierte Skripte zu erstellen, damit so viele Menschen wie möglich daran teilnehmen können, das System sicher zu halten.

Zusammenfassung

Wir haben ein Protokoll vorgeschlagen, das sich schrittweise der menschlichen Kontrolle entzieht und einen besicherten Vermögenswert mit geringer Volatilität namens Reflexindex ausgibt. Wir haben zuerst den autonomen Mechanismus vorgestellt, der den Marktpreis des Index beeinflussen soll, und dann beschrieben, wie mehrere Smart Contracts die Macht der Token-Inhaber über das System einschränken können. Wir skizzierten ein sich selbst tragendes Schema zur Medianisierung von Preis-Feeds aus

mehreren unabhängigen Orakel-Netzwerken und endeten mit der Vorstellung des allgemeinen Mechanismus zum Prägen von Indizes und Liquidieren von SAFEs.

Verweise

[1] „Das Maker-Protokoll: Das Multi Collateral Dai (MCD) System von MakerDAO“, https://bit.ly/2YL5S6j

[2] „UMA: Eine dezentralisierte Finanzvertragsplattform“, https://bit.ly/2Wgx7E1

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

[4] KJ Åström , RM Murray, „Feedback Systems: An Introduction for Scientists and Engineers“, https://bit.ly/3bHwnMC

[5] RJ Hawkins, JK Speakes, DE Hamilton, „Geldpolitik und PID-Steuerung“, https://bit.ly/2TeQZFO

[6] H. Karp, R. Melbardis, „Ein diskretionärer Peer-to-Peer-Gegenseitigkeitsfonds auf der EthereumBlockchain“, https://bit.ly/3du8TMy

[7] H. Adams, N. Zinsmeister, D. Robinson, „Uniswap V2 Core“, https://bit.ly/3dqzNEU

Glossar

Reflexindex : ein besicherter Vermögenswert, der die Volatilität seines Basiswerts dämpft

RAI : unser erster Reflexindex

Rücknahmepreis : Der Preis, den das System für den Index haben möchte. Er ändert sich, beeinflusst durch einen Rückzahlungssatz (berechnet von RRFM), falls der Marktpreis nicht nahe daran liegt. Soll SAFE-Ersteller beeinflussen, mehr zu generieren oder einen Teil ihrer Schulden zurückzuzahlen

Sollzinssatz : Jährlicher Zinssatz, der auf alle SAFEs angewendet wird, die ausstehende Schulden haben

Tilgungsraten-Feedback-Mechanismus (RRFM) : ein autonomer Mechanismus, der die Markt- und Rücknahmepreise eines Reflexindex vergleicht und dann eine Rückzahlungsrate berechnet, die die SAFE-Ersteller langsam beeinflusst, um mehr oder weniger Schulden zu generieren (und implizit versucht, die Markt-/Rücknahmepreisabweichung zu minimieren)

Money Market Setter (MMS) : ein Mechanismus ähnlich wie RRFM, der mehrere monetäre Hebel gleichzeitig zieht. Bei Reflexindizes modifiziert es sowohl den Sollzins als auch den Rücknahmepreis

Oracle Network Medianizer (ONM) : Ein intelligenter Vertrag, der Preise aus mehreren OracleNetzwerken (die nicht von der Governance kontrolliert werden) zieht und sie medianisiert, wenn eine
Mehrheit (z. B. 3 von 5) ein Ergebnis ohne Werfen zurückgibt

Eingeschränktes Governance-Modul (RGM): eine Reihe intelligenter Verträge, die die Macht der Inhaber von Governance-Token über das System binden. Sie erzwingt entweder zeitliche Verzögerungen oder schränkt die Möglichkeiten der Governance ein, bestimmte Parameter festzulegen

Governance-Eiszeit : unveränderlicher Vertrag, der die meisten Komponenten eines Protokolls nach Ablauf einer bestimmten Frist vor Eingriffen von außen sperrt

Buchhaltungs-Engine : Systemkomponente, die Schulden- und Überschussauktionen auslöst. Es verfolgt auch die Höhe der derzeit versteigerten Schulden, der nicht eingelösten uneinbringlichen Forderungen und des Überschusspuffers

Überschusspuffer : Zinsbetrag, der aufgelaufen und im System gehalten werden soll. Irgendein Interesse
Über diesem Schwellenwert angesammelte Werte werden in Überschussauktionen verkauft, bei denen Protokoll-Token verbrannt werden

Überschüssige Schatzkammer : Vertrag, der verschiedenen Systemmodulen die Erlaubnis gibt, aufgelaufene Zinsen abzuheben (z. B. ONM für Orakelaufrufe)