Rai: Eine Sicherheit mit geringer Volatilität und minimiertem Vertrauen für das DeFi Ökosystem

Stefan C. Ionescu, Ameen Soleimani

Mai 2020

Kurzbeschreibung. Wir präsentieren ein Verwaltung-minimiertes, dezentralisiertes Protokoll, das automatisch auf die Marktkräfte reagiert, um den Zielwert seines nativen gesicherten Vermögenswertes zu verändern. Das Protokoll erlaubt es jedem, seine Krypto-Vermögenswerte zu nutzen und einen "Reflex Index" auszugeben, der eine gedämpfte Version seiner zugrundeliegenden Sicherheit ist. Wir stellen dar, wie Indizes als universelle Sicherheiten mit geringer Volatilität, die ihre Inhaber sowie andere dezentrale Finanzprotokolle vor plötzlichen Marktveränderungen schützen können, nützlich sein können. Wir präsentieren unsere Pläne, um den anderen Teams bei der Einführung ihrer eigenen synthetischen Anlageprodukte zu helfen, indem unsere Infrastruktur gehebelt wird. Schließlich bieten wir Alternativen zu den derzeitigen Orakel- und Verwaltung-Strukturen, die in vielen DeFi-Protokollen gefunden werden.

Inhaltsangabe

Einführung

Geld ist einer der mächtigsten Koordinationsmechanismen, die die Menschheit hebelt, um zu gedeihen. Das Privileg, die Geldmenge zu verwalten, war in der Vergangenheit in den Händen der souveränen Regierung und der Finanzelite gehalten, zugleich war es der ahnungslosen Öffentlichkeit aufgezwungen. Wo Bitcoin das Potenzial gezeigt hat, das Basisprotest eines wertbeständigen Wertaufbewahrungsmittels bekannt zu machen, Ethereum gibt uns eine Plattform, mit Vermögenswerten unterlegte synthetische Instrumente zu schaffen, die vor Volatilität geschützt werden und als Sicherheit verwendet werden, oder an einen Referenzpreis angebunden und als Tauschmittel für alltägliche Transaktionen genutzt werden können, die alle durch die gleichen Prinzipien dezentralen Konsens durchgesetzt werden.

Der erlaubnisfreie Zugang zu Bitcoin für die Aufbewahrung von Vermögen und ordnungsgemäßen dezentralisierten synthetischen Instrumenten auf Ethereum werden den Grundstein für die kommende Finanzrevolution legen und denjenigen, die am Rande des modernen Finanzsystems stehen, die Mittel geben, den Aufbau des neuen Systems zu koordinieren.

In diesem Beitrag stellen wir einen Rahmen für die Erstellung von Reflex-Indizes vor, einer neuen Anlageform, die anderen synthetischen Vermögenswerten zum Erfolg verhelfen werden und einen wichtigen Baustein für die gesamte dezentralisierte Finanzindustrie etablieren werden.

Überblick der Reflex Indizes

Der Zweck eines Reflex-Indexes ist nicht einen bestimmten Pflock aufrechtzuerhalten, sondern die Volatilität seiner Sicherheit zu dämpfen. Indizes ermöglichen es jedem, sich auf dem Kryptowährungsmarkt zu engagieren, ohne das gleiche Risiko einzugehen wie der Besitz tatsächlicher Krypto-Vermögenswerte. Wir glauben, dass RAI, unser erster Reflex-Index, einen unmittelbaren Nutzen für andere Teams haben wird, die synthetische Anlageprodukte auf Ethereum ausgeben (z.B. MakerDAO's Multi-Collateral DAI [1], UMA [2], Synthetix [3]), weil es ihren Systemen eine geringere Exposition gegenüber volatilen Vermögenswerten wie ETH gibt und den Nutzern mehr Zeit anbietet, um ihre Positionen im Falle einer signifikanten Marktverschiebung zu schließen.

Um Reflex-Indizes zu verstehen, können wir das Verhalten ihres Rückzahlungspreises mit dem Preis eines Stablecoins vergleichen.

Der Rückzahlungspreis ist der Wert einer Schuldeneinheit (oder Coin) im System. Er ist gedacht nur als internes Buchhaltungsinstrument verwendet zu werden und unterscheidet sich vom Marktpreis (von dem Wert, zu dem der Coin auf dem Markt gehandelt wird). Im Falle von Fiat-gestützten Stablecoins wie USDC erklären die Systembetreiber, dass jeder einen Coin gegen einen US-Dollar einlösen kann und somit der Rückzahlungspreis für diese Coins ist immer eins. Es gibt auch Fälle von kryptogestützten Stablecoins wie MakerDAOs Multi Collateral DAI (MCD), bei dem das System auf einen festen Wert von einem US-Dollar abzielt und somit der Rückzahlungspreis ebenfalls auf einen Dollar festgelegt ist.

In den meisten Fällen gibt es eine Differenz zwischen dem Marktpreis eines Stablecoins und seinem Rückzahlungspreis. Diese Szenarien schaffen Arbitragemöglichkeiten, bei denen Händler mehr Münzen erzeugen, wenn der Marktpreis höher als der Rückkaufpreis ist, und sie ihre Stablecoins gegen Sicherheiten (z. B. US-Dollar im Falle von USDC) einlösen, wenn der Marktpreis niedriger als der Rückzahlungspreis ist.

Reflex-Indizes sind den Stablecoins ähnlich, da sie ebenfalls einen Rückzahlungspreis haben den das System zum Ziel setzt. Der Hauptunterschied besteht darin, dass der Rückzahlungspreis nicht feststeht, sondern entworfen ist, um sich unter dem Einfluss der Marktkräfte zu ändern. In Abschnitt 4 erklären wir, wie der Rückzahlungspreis eines Index schwankt und neue Arbitragemöglichkeiten für seine Nutzer schafft.

Design-Philosophie und Markteinführungsstrategie

Unsere Design-Philosophie besteht darin, Sicherheit, Stabilität und Schnelligkeit der Bereitstellung in den Vordergrund zu stellen.

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

Zu unseren wichtigsten Änderungen gehört das Hinzufügen eines autonomen Kursfestsetzers, eines Oracle Network Medianizers, der mit vielen unabhängigen Preisdaten integriert ist und einer Verwaltung-Minimierungsschicht, um das System so viel wie möglich von menschlichen Interventionen zu isolieren.

Die allererste Version des Protokolls (Stufe 1) wird nur den Kursfestsetzer und andere kleinere Verbesserungen in der Kernarchitektur beinhalten. Sobald wir bewiesen haben, dass der Setzer wie erwartet funktioniert, können wir mit größerer Sicherheit den Orakel-Medianizer (Stufe 2) und die Verwaltung-Minimierungsschicht (Stufe 3) hinzufügen.

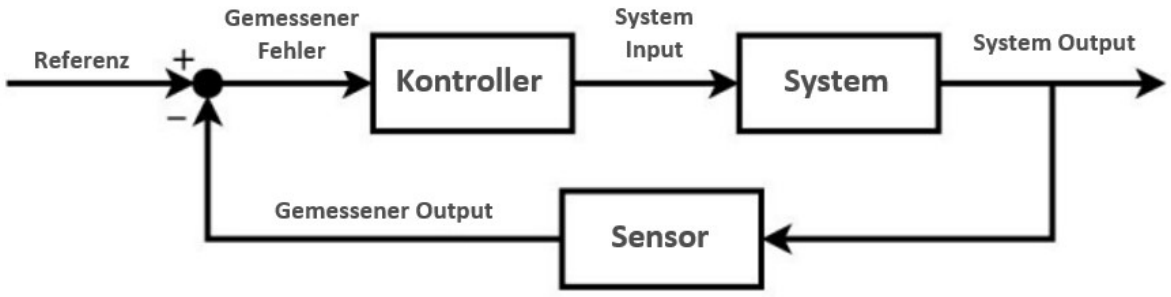
Geldpolitische Mechanismen

Einführung in die Kontrolltheorie

Ein gängiges Kontrollsystem, mit dem die meisten Menschen vertraut sind, ist die Dusche. Wenn jemand anfängt zu duschen, hat er eine gewünschte Wassertemperatur im Kopf, die in der Regelungstheorie als Referenzsollwert bezeichnet wird. Die Person, die als Regler fungiert, misst kontinuierlich die Temperatur des Wasserdurchflusses (die als Output bezeichnet wird) und modifiziert die Geschwindigkeit, mit der sie den Drehknopf der Dusche dreht, aufgrund der Abweichung (oder Fehler) zwischen der gewünschten und der aktuellen Temperatur. Die Geschwindigkeit, mit der der Knopf gedreht wird, wird als Input bezeichnet. Das Ziel ist es, den Drehknopf genug schnell zu drehen, um den Referenzsollwert schnell zu erreichen, aber nicht so schnell, dass die Temperatur überschießt. Wenn es zu Systemstößen kommt, bei denen sich die Wasser Temperatur plötzlich ändert, sollte die Person in der Lage sein, die aktuelle Temperatur aufrechtzuerhalten, indem sie weiß, wie schnell sie den Drehknopf als Reaktion auf die Störung drehen muss.

Die wissenschaftliche Disziplin, die sich mit der Aufrechterhaltung der Stabilität in dynamischen Systemen befasst, heißt Kontrolltheorie. Sie findet breite Anwendung bei den Temporeglern von Autos, der Flugnavigation, chemischen Reaktoren, Roboterarmen und industriellen Prozessen aller Art. Der Bitcoin Schwierigkeitsanpassungsalgorithmus, der die durchschnittliche Blockzeit von zehn Minuten aufrechterhält, trotz variabler Hashrate, ist ein Beispiel für ein missionskritisches Kontrollsystem.

In den meisten modernen Steuerungssystemen ist in der Regel eine algorithmische Steuerung in den Prozess eingebettet und ihm wird die Kontrolle über einen Input (z. B. das Gaspedal eines Autos) gegeben, um es automatisch zu aktualisieren, basierend auf den Abweichungen zwischen dem Output (z. B. die Fahrzeuggeschwindigkeit) und dem Sollwert (z. B. der Geschwindigkeit des Tempomats).



Der gebräuchlichste Typ eines algorithmischen Reglers ist der PID-Regler. Über 95% der industriellen Anwendungen und einer Vielzahl von biologischen Systemen setzen die Elemente des PID Regelung ein [4].

Ein PID-Regler verwendet eine mathematische Formel mit drei Teilen, um seinen Ausgang zu bestimmen:

Reglerausgang = Proportionalitätsfaktor + Integralfaktor + Derivativfaktor

Der Proportionalitätsfaktor ist der Teil des Reglers, der direkt proportional zur Abweichung ist. Wenn die Abweichung groß und positiv ist (z. B. wenn die Geschwindigkeit des Tempomats Geschwindigkeits-Sollwert weit höher als die aktuelle Geschwindigkeit des Fahrzeugs ist), wird die proportionale Reaktion groß und positiv sein (z. B. das Gaspedal durchtreten).

Der Integralfaktor ist der Teil des Reglers, der berücksichtigt, wie lange eine Abweichung angedauert hat. Er wird bestimmt, indem man das Integral der Abweichung über die Zeit ermittelt und dient in erster Linie dazu, die Fehler im stationären Zustand zu beheben. Er akkumuliert, um auf kleine, aber anhaltende Abweichungen vom Sollwert zu reagieren (z. B. wenn der Tempomat-Sollwert des Geschwindigkeitsreglers einige Minuten lang um 1 mph höher war als die Geschwindigkeit des Fahrzeugs).

Der Derivativfaktor ist der Teil des Reglers, der berücksichtigt, wie schnell die Abweichung wächst oder schrumpft. Er wird bestimmt, durch das Nehmen der Ableitung der Abweichung und dient dazu, die Reaktion des Reglers zu beschleunigen, wenn die Abweichung (z. B. Beschleunigung, wenn der Sollwert des Geschwindigkeitsreglers höher ist als die Geschwindigkeit des Fahrzeugs und das Auto beginnt zu verlangsamen). Es hilft auch das Überschwingen durch Verlangsamung der Reaktion des Reglers zu reduzieren, wenn die Abweichung kleiner wird, (z. B. Gas wegnehmen, wenn sich die Geschwindigkeit dem Sollwert des Geschwindigkeitsreglers nähert).

Die Kombination dieser drei Teile, von denen jeder unabhängig eingestellt werden kann verleiht PID-Reglern große Flexibilität bei der Steuerung einer Vielzahl von Regelsystemanwendungen.

PID-Regler funktionieren am besten in Systemen, die eine gewisse Verzögerung in der Reaktionszeit, sowie die Möglichkeit des Überschwingens und der Oszillation um den Sollwert zulassen, wenn das System versucht, sich selbst zu stabilisieren. Reflex-Index-Systeme wie RAI sind gut geeignet für diese Art von Szenario, da ihre Rückzahlungspreise durch PID Regler geändert werden können.

Generell wurde kürzlich festgestellt, dass viele der derzeitigen geldpolitischen Regeln der Zentralbanken (z. B. die Taylor-Regel) eigentlich Annäherungen von PID Kontroller sind [5].

Rückmeldungsmechanismus der Rückzahlungsrate

Der Rückmeldungsmechanismus der Rückzahlungsrate ist die Systemkomponente, die für die Änderung des Rückzahlungspreises eines Reflex-Indexes zuständig ist. Um zu verstehen, wie er funktioniert, müssen wir zuerst beschreiben, warum das System einen Rückmeldungs-Mechanismus benötigt, im Gegensatz zur manuellen Steuerung und was der Output dieses Mechanismus ist.

Komponenten des Rückmeldungsmechanismus

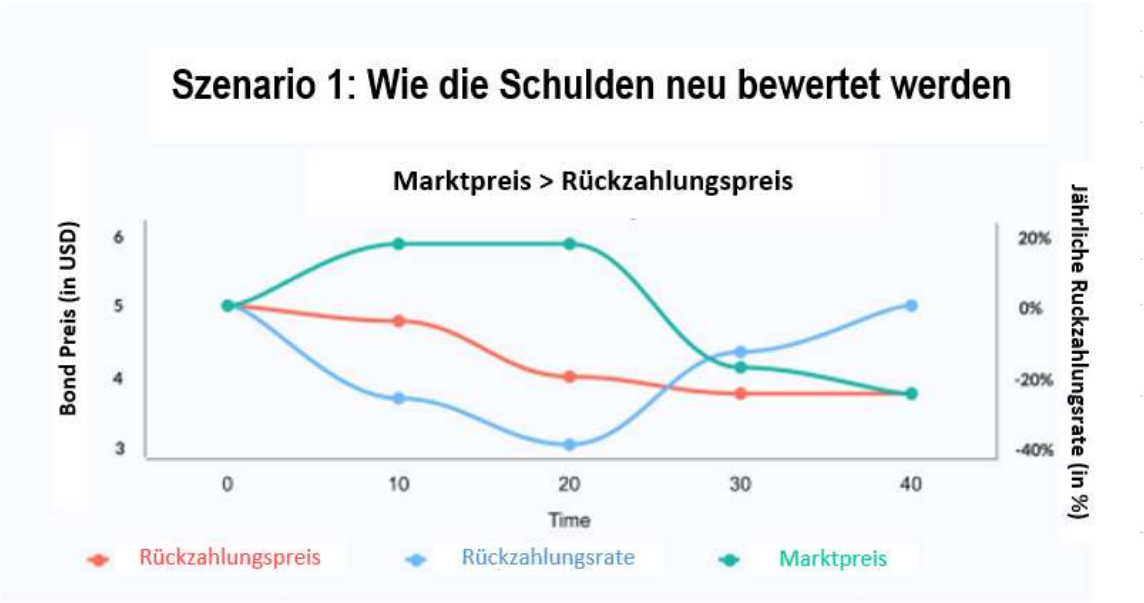
Theoretisch wäre es möglich, den Rückzahlungspreis des Reflex-Index (wie in Abschnitt 2 beschrieben) direkt zu manipulieren, um die Indexnutzer zu beeinflussen und schließlich den Marktpreis des Index zu verändern. In der Praxis hätte diese Methode nicht die gewünschte Auswirkung auf die Systemteilnehmer. Aus der Sicht eines Tresor-Inhabers, wenn der Rückzahlungspreis nur einmal erhöht wird, könnte er einen höheren Preis pro Schuldtitel akzeptieren und den Verlust durch eine geringere Besicherungsquote absorbieren und seine Position beibehalten. Wenn sie jedoch erwarten, dass der Rückzahlungspreis im Laufe der Zeit weiter steigen wird, würden sie wahrscheinlich eher dazu neigen, den erwarteten künftigen Verlust zu vermeiden und sich daher für die Rückzahlung ihrer Schulden und die Schließung ihrer Positionen entscheiden.

Wir gehen davon aus, dass die Teilnehmer des Reflex-Indexsystems nicht direkt auf Änderungen des Rückzahlungspreises reagieren, sondern stattdessen auf die Änderungsrate des Rückzahlungspreises, die wir als Rückzahlungsrate bezeichnen antworten. Die Rückzahlungsrate wird durch einen Rückmeldungsmechanismus festgelegt, der von der Verwaltung fein abgestimmt oder vollständig automatisiert werden kann.

Szenarien für den Rückmeldungsmechanismus

Der Rückmeldungsmechanismus zielt darauf ab, ein Gleichgewicht zwischen dem Rückzahlungspreis und dem Marktpreis aufrechtzuerhalten, indem der Rückzahlungspreis verwendet wird, um den Verschiebungen der Marktkräfte entgegenzutreten. Um dies zu erreichen, wird die Rückzahlungsrate so berechnet, dass er der Abweichung zwischen Markt- und Rückzahlungspreis entgegenwirkt.

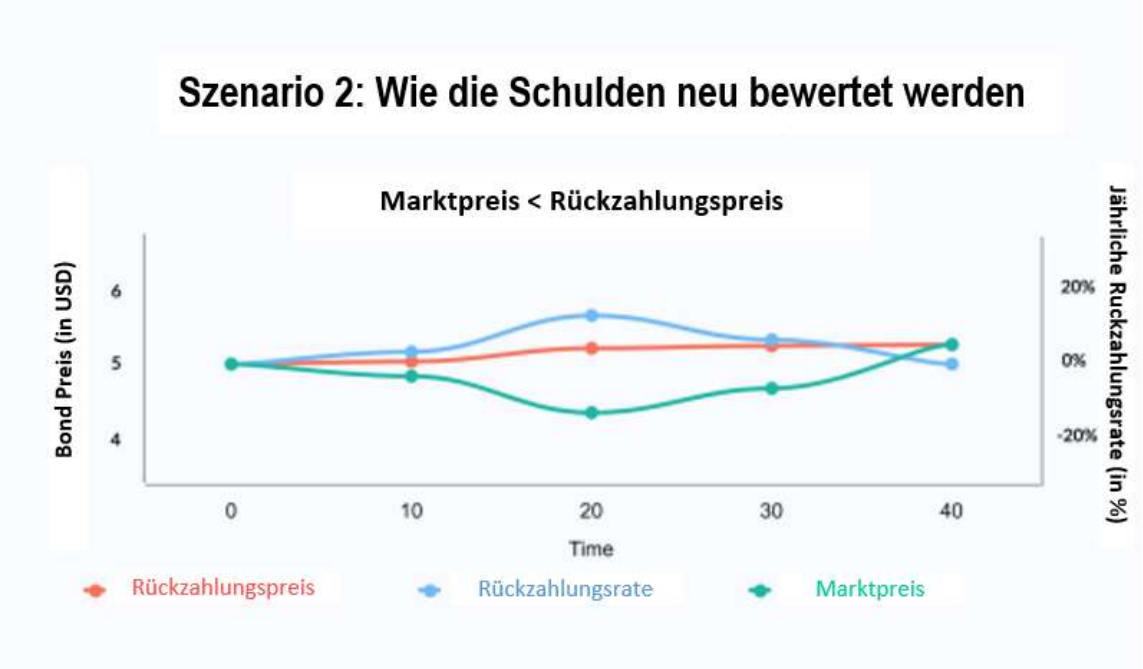
Im ersten Szenario unten, wenn der Marktpreis des Index höher ist als der Rückzahlungspreis, berechnet der Mechanismus einen negativen Kurs (eine negative Rate), der (die) anfängt den Rückzahlungspreis zu senken, wodurch die Schulden des Systems günstiger werden.



Die Erwartung eines sinkenden Rückzahlungspreises wird die Menschen wahrscheinlich davon abhalten Indizes zu halten und die Tresor-Inhaber zu ermutigen, mehr Schulden zu generieren (selbst wenn sich der Preis der Sicherheiten nicht ändert), die dann auf dem Markt verkauft werden, dementsprechend wird das Angebot und Nachfrage ausgeglichen. Beachten Sie, dass dies das ideale Szenario ist, in dem die Index-Inhaber schnell auf den Rückmeldungsmechanismus reagieren. In der Praxis (und insbesondere in den ersten Tagen nach der Einführung) erwarten wir eine Verzögerung zwischen dem Start des Mechanismus und den tatsächlichen Ergebnissen, die in der Menge der ausgegebenen Schuldtitel und nachfolgend im Marktpreis gesehen werden.

Andererseits, in Szenario zwei, wenn der Marktpreis des Index niedriger ist als der Rückzahlungspreis, wird die Rate positiv und beginnt, allen Schuldtiteln einen neuen Preis anzupassen, so dass sie teurer werden.

Da die Schulden teurer werden, sinken die Besicherungsquoten aller Tresore (so dass Tresor-Ersteller die Motivation haben, ihre Schulden zurückzuzahlen), und die Nutzer beginnen, Indizes zu horten, in der Erwartung, dass sie an Wert gewinnen werden.



Algorithmus für den Rückmeldungsmechanismus

Im folgenden Szenario gehen wir davon aus, dass das Protokoll einen proportional-integralen Kontroller verwendet, um die Rückzahlungsrate zu berechnen:

- Der Reflex-Index wird mit einem beliebigen Rückzahlungspreis 'Rand' eingeführt
- Zu einem bestimmten Zeitpunkt steigt der Marktpreis des Index von 'Rand' auf 'Rand' + x. Nachdem der Rückmeldungsmechanismus den neuen Marktpreis abliest, berechnet er einen proportionalen Faktor *p*, der in diesem Fall -1 * (('Rand' + x) / 'Rand') beträgt. Der Proportionalwert ist negativ, um den Rückzahlungspreis zu senken und im Gegenzug die Indizes neu zu bewerten, so dass sie günstiger werden
- Nach der Berechnung des Proportionalwertes bestimmt der Mechanismus den integralen Faktor *i*, indem er alle vergangenen Abweichungen von der letzten *AbweichungIntervall* Sekunden addiert
- Der Mechanismus summiert den proportionalen und den integralen Faktor und berechnet eine Rückzahlungsrate *r* pro Sekunde, die beginnt den Rückzahlungspreis langsam zu senken. Wenn die Tresor-Ersteller erkennen, dass sie mehr Schulden generieren können, werden sie den Markt mit weiteren Indizes überschwemmen

- Nach *n* Sekunden entdeckt der Mechanismus, dass die Abweichung zwischen dem Markt- und Rückzahlungspreisen unwesentlich ist (unter einem bestimmten Parameter *Noise*). Zu diesem Zeitpunkt setzt der Algorithmus r auf Null und hält den Rückzahlungspreis dort, wo er ist

In der Praxis wird der Algorithmus robuster sein und wir werden entweder einige Variablen unveränderlich machen (z. B. der Noise Parameter, *AbweichungInterval*) oder es werden strenge Grenzen geben, was das Management ändern kann.

Abstimmung des Rückmeldungsmechanismus

Von größter Bedeutung für das reibungslose Funktionieren des Reflex-Index-Systems ist die Abstimmung der Parameter der algorithmischen Steuerung. Eine unsachgemäße Parametrisierung könnte dazu führen, dass das System zu langsam ist, die Stabilität zu erreichen, es massiv überschießt oder generell instabil gegenüber externen Schocks ist.

Der Abstimmungsprozess für einen PID-Regler umfasst in der Regel das Ausführen des Live-Systems, die Optimierung der Abstimmungsparameter und das Beobachten der Reaktion des Systems, dabei auch oft gezielt die Schocks auf dem Weg eingeführt werden. Angesichts der Schwierigkeit und des finanziellen Risikos, die Parameter eines laufenden Reflex-Index-Systems zu verändern, planen wir, die Computermodellierung und Simulation so weit wie möglich zu nutzen, um die Anfangsparameter festzulegen, aber auch die Möglichkeit, die Abstimmungsparameter zu aktualisieren, wenn zusätzliche Daten aus der Produktion zeigen, dass sie nicht optimal sind.

Geldmarktsetzer

In RAI planen wir, die Sollzinsrate (Zinssatz, der bei der Erstellung von Indizes angewendet wird) fest oder abgedeckt zu halten und nur den Rückzahlungspreis zu ändern, somit die Komplexität bei der Modellierung des Rückmeldungsmechanismus zu minimieren. Der Sollzins entspricht in unserem Fall der Spanne zwischen der Stabilitätsgebühr und dem DSR in Multi-Sicherheit DAI.

Obwohl wir planen, den Sollzinssatz fest zu halten, ist es möglich, ihn zusammen mit dem Rückzahlungspreis mithilfe eines Geldmarktsetzers zu ändern. Der Geldmarkt ändert die Sollzinsrate und den Rückzahlungspreis in gewisser Weise, die den Tresor-Ersteller anregt, mehr oder weniger Schulden zu generieren. Liegt der Marktpreis eines Index über dem Rückzahlungsbetrag, sinken beide Zinssätze, wogegen wenn es unter dem Rückzahlungsbetrag ist, die Raten werden steigen.

Globales Settlement

Das Globale Settlement ist eine Methode der letzten Instanz, den Rückzahlungspreis für alle Reflex-Index-Inhaber zu garantieren. Sie soll es erlauben, sowohl den Inhabern von Reflex-Indizes als auch den Tresor-Erstellern die Rücknahme von Systemsicherheiten zu ihrem Nettowert einzulösen (Anzahl der Indizes für jede Sicherheitsart, entsprechend dem letzten Rückzahlungspreis). Jeder kann das Settlement auslösen, nachdem er eine bestimmte Menge an Protokoll-Token verbrannt hat.

Das Settlement erfolgt in drei Hauptphasen:

- Auslöser: Das Settlement wird ausgelöst, Nutzer können keine Tresore mehr erstellen, alle Preisdaten der Sicherheiten und der Rückzahlungspreis werden eingefroren und aufgezeichnet

- Prozess: Verarbeitung aller ausstehenden Auktionen

- Anspruch: Jeder Reflex-Index-Inhaber und Tresor-Ersteller kann einen festen Betrag von einer beliebigen Systemsicherheit auf der Grundlage des letzten aufgezeichneten Rückzahlungspreises des Index beanspruchen

Verwaltung

Die überwiegende Mehrheit der Parameter wird unveränderlich sein und die inneren intelligente Vertragsmechanismen werden nicht aktualisierbar sein, es sei denn, die Inhaber von Verwaltung-Token ein völlig neues System bereitstellen. Wir haben uns für diese Strategie entschieden, weil wir das Meta-Spiel ausschließen können, bei dem die Menschen versuchen, den Verwaltungsprozess zu ihrem eigenen Nutzen zu beeinflussen und damit das Vertrauen in das System zu beeinträchtigen. Wir etablieren die ordnungsgemäße Funktionsweise des Protokolls, ohne zu viel Vertrauen in Menschen zu setzen (der "Bitcoin-Effekt"), so dass wir die soziale Skalierbarkeit maximieren und die Risiken für andere Entwickler minimieren, die RAI als Kerninfrastruktur in ihren eigenen Projekten nutzen wollen.

Für die wenigen Parameter, die geändert werden können, schlagen wir die Hinzufügung eines eingeschränkten Verwaltungsmoduls vor, um alle möglichen Systemänderungen zu verzögern oder zu begrenzen. Darüber hinaus stellen wir die Verwaltung-Eiszeit vor, ein Berechtigungsregister, das einige Teile des Systems nach Ablauf bestimmter Fristen für die Kontrolle von außen sperren kann.

Zeitlich begrenzte Verwaltung

Zeitbasierte Verwaltung ist die erste Komponente des Eingeschränkten Steuerung Moduls. Sie führt zu zeitlichen Verzögerungen zwischen den Änderungen, die auf denselben Parameter angewendet werden. Ein Beispiel ist die Möglichkeit, die Adressen der Orakel zu ändern, die im Oracle Netzwerk Medianizer (Abschnitt 6.2) verwendet wurden, nachdem mindestens *T* Sekunden seit der letzten Orakel-Änderung vergangen sind.

Handlungsgebundene Verwaltung

Die zweite Komponente des Eingeschränkten Steuerung Moduls ist die Handlungsgebundene Verwaltung. Jeder regelbare Parameter hat Grenzen für die Werte, auf die er gesetzt werden kann und wie stark er sich in einem bestimmten Zeitraum ändern kann. Bemerkenswerte Beispiele sind die ersten Versionen des Rückmeldungsmechanismus einer Rückzahlungsrate (Abschnitt 4.2), wo die Verwaltung-Token-Inhaber in der Lage sein werden, eine Feinabstimmung vorzunehmen.

Verwaltung-Eiszeit

Die Eiszeit ist ein unveränderlicher intelligenter Vertrag, der Fristen für die Änderung bestimmten Systemparametern und für die Aktualisierung des Protokolls auferlegt. Er kann für den Fall verwendet werden, wenn die Verwaltung sicherstellen will, dass sie Fehler beheben kann, bevor sich das Protokoll selbst sperrt und Eingriffe von außen ablehnt. Die Eiszeit wird verifizieren, ob eine Änderung zulässig ist, indem sie den Namen des Parameters und die Adresse des betroffenen Vertrags dem Fristenverzeichnis gegenüberstellt. Ist die Frist verstrichen, wird der Aufruf rückgängig gemacht.

Die Verwaltung kann in der Lage sein die Eiszeit eine feste Anzahl von Malen zu verzögern, wenn Fehler kurz vor dem Datum gefunden werden, an dem das Protokoll beginnen sollte, sich selbst zu sperren. Eiszeit kann zum Beispiel nur dreimal um jeweils einen Monat verzögert werden, damit die neu eingeführten Fehlerbehebungen ordnungsgemäß getestet werden.

Kernbereiche, in denen die Verwaltung erforderlich ist

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

- **Hinzufügen neuer Typen von Sicherheiten**: RAI wird nur mit ETH gesichert sein, aber andere Indizes werden durch mehrere Typen von Sicherheiten gesichert sein und die Verwaltung wird in der Lage sein das Risiko im Laufe der Zeit zu diversifizieren

- **Änderung externer Abhängigkeiten**: Orakel und DEXs, von denen das System abhängt, können aktualisiert werden. Die Verwaltung kann das System auf neuere Abhängigkeiten verweisen damit es weiterhin ordnungsgemäß funktioniert

- **Feinabstimmung der Zinssetzung**: Frühe geldpolitische Kontrolleure werden die Parameter haben, die innerhalb vernünftiger Grenzen geändert werden können (wie in Handlungs- und Zeitbasierter Verwaltung beschrieben)

- **Migration zwischen Systemversionen**: In einigen Fällen kann die Verwaltung ein neues System einrichten, ihm die Erlaubnis erteilen die Protokoll-Tokens 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 für die Migration zwischen Systemversionen:

- Es gibt eine Migrationsregister, das den Überblick hat, wie viele verschiedene Systeme dasselbe Protokoll-Token abdeckt und welchen Systemen die Erlaubnis verweigert werden kann, die Protokoll-Tokens in einer Schuldauktion zu drucken

- Jedes Mal, wenn die Verwaltung eine neue Systemversion einführt, reicht sie dem Migrationsregister die Adresse des Schuldauktionsvertrags des Systems ein. Die Verwaltung muss auch angeben, ob sie jemals in der Lage sein wird, das System vom Drucken von Protokoll-Tokens zu stoppen. Außerdem, kann die Leitung jederzeit feststellen, dass ein System immer in der Lage sein wird, die Tokens zu drucken, und daher nie von einem anderen System migriert werden wird

- Es gibt eine Abkühlphase zwischen einem neuen Systemvorschlag und dem Entzug von Berechtigungen für ein altes System

- Ein optionaler Vertrag kann so eingerichtet werden, dass er ein altes System automatisch abschaltet, nachdem ihm die Druckrechte entzogen wurden

Das Migrationsmodul kann mit einer Eiszeit kombiniert werden, die automatisch bestimmten Systemen die Erlaubnis erteilt, immer in der Lage zu sein die Tokens zu drucken.

Automatische Systemabschaltung

Es gibt Fälle, die das System automatisch erkennen kann und infolgedessen das Settlement selbständig auslösen kann, ohne die Protokoll-Tokens verbrennen zu müssen:

- **Schwerwiegende Preisdaten-Verzögerungen**: Das System stellt fest, dass eine oder mehrere der Sicherheiten- oder Indexpreis-Daten über einen längeren Zeitraum nicht aktualisiert wurden

- **Systemmigration**: Dies ist ein optionaler Vertrag, den das Protokoll abschalten kann nach Ablauf einer Abkühlungsphase ab dem Zeitpunkt, an dem die Verwaltung die Fähigkeit des Schuldauktionsmechanismus zum Drucken von Protokoll-Tokens entzieht (Eingeschränktes Migrationsmodul, Abschnitt 5.4.1).

- **Konsistente Marktpreisabweichung**: Das System stellt fest, dass der Marktpreis des Index über einen längeren Zeitraum um *x%* im Vergleich zu dem Rückzahlungspreis abgewichen ist

Verwaltung wird in der Lage sein, diese autonomen Abschaltmodule zu aktualisieren, während sie noch gebunden sind oder bis die Eiszeit beginnt, einige Teile des Systems zu sperren.

Orakel

Es gibt drei Haupttypen von Vermögenswerten, für die das System Preisdaten lesen muss: der Index, das Protokoll-Token und jeder auf der Whitelist stehende Sicherheitstyp. Die Preisdaten können von Verwaltung geführten Orakeln oder von bereits etablierten Orakelnetzwerken bereitgestellt werden.

Verwaltung-geführte Orakel

Inhaber der Verwaltung-Token oder das Kernteam, das das Protokoll eingeführt hat, können mit anderen Einheiten zusammenarbeiten, die mehrere Preisdaten außerhalb der Kette sammeln und dann eine einzige Transaktion an einen intelligenten Vertrag senden, der alle Datenpunkte vermittelt.

Dieser Ansatz ermöglicht mehr Flexibilität bei der Aufrüstung und Änderung der Orakel Infrastruktur, was allerdings auf Kosten der Vertrauenswürdigkeit geht.

Oracle Netzwerk-Medianizer

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

- Unser Vertrag hat einen Überblick der auf der Whitelist stehenden Orakelnetzwerken, die er aufrufen kann, um Preise für Sicherheiten anzufordern. Der Vertrag wird durch einen Teil des Überschusses finanziert, den das System erwirtschaftet (mit Hilfe der Überschuss-Schatzkammer, Abschnitt 11). Jedes Orakelnetzwerk akzeptiert bestimmte Tokens als Zahlungsmittel, also unser Vertrag hat auch einen Überblick der Mindestmenge und der Art der Tokens, die für jede Anfrage benötigt werden

- Um einen neuen Preis in das System einzuspeisen, müssen alle Orakel vorher aufgerufen werden. Wenn ein Orakel aufgerufen wird, tauscht der Vertrag zunächst einige Stabilitätsgebühren mit einem der vom Orakel akzeptierten Tokens. Nach dem ein Orakel aufgerufen wird, kennzeichnet der Vertrag den Aufruf als "gültig" oder "ungültig". Wenn ein Aufruf ungültig ist, kann das fehlerhafte Orakel erst wieder aufgerufen werden, bis alle anderen aufgerufen wurden und der Vertrag prüft, ob es eine gültige Mehrheit gibt. Ein gültiger Orakelaufruf darf nicht zurückkehren und muss einen Preis wiederfinden, der irgendwann in den letzten *m* Sekunden on-chain gepostet wurde. "Wiederfinden" bedeutet je nach Orakeltyp unterschiedliche Dinge:

    - Bei Pull-basierten Orakeln, bei denen wir sofort ein Ergebnis erhalten können, muss unser Vertrag eine Gebühr zahlen und den Preis direkt abrufen

    - Bei Push-basierten Orakeln zahlt unser Vertrag die Gebühr, ruft das Orakel ab und muss eine bestimmte Zeitspanne *n* warten, bevor er das Orakel erneut abruft, um den angeforderten Preis zu erhalten

- Jedes Orakelergebnis wird in einem Array gespeichert. Nachdem jedes der sich auf der Whitelist befindenden Orakel aufgerufen wurde und wenn das Array genügend gültige Datenpunkte enthält, 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 den Orakelergebnissen gelöscht und der Vertrag muss *p* Sekunden warten, bevor er den gesamten Prozess wieder von vorne beginnt

Oracle Netzwerk-Backup

Verwaltung kann eine Backup-Orakel-Option hinzufügen, die beginnt, Preise im System zu pushen, wenn der Medianizer mehrmals hintereinander keine Mehrheit gültiger Orakelnetzwerke finden kann.

Die Backup-Option muss bei der Bereitstellung des Medianizers festgelegt werden, da sie nachträglich nicht geändert werden kann. Außerdem kann ein separater Vertrag überwachen, ob das Backup den Medianisierung-Mechanismus zu lange ersetzt hat und das Protokoll automatisch abschalten.

Tresore

Um Indizes zu generieren, kann jeder seine Krypto-Sicherheiten in Tresoren deponieren und hebeln. Solange ein Tresor geöffnet ist, wird er weiterhin Schulden entsprechend dem Sollzinssatz der hinterlegten Sicherheiten erwirtschaften. Wenn der Tresor-Ersteller seine Schulden zurückzahlt, kann er mehr und mehr von ihren gesperrten Sicherheiten abheben.

Tresor-Lebenszyklus

Es gibt vier Hauptschritte, die für die Erstellung von Reflex Indizes notwendig sind und die anschließende Rückzahlung der Schulden eines Tresors:

- Deponieren von Sicherheiten im Tresor

  Der Benutzer muss zunächst einen neuen Tresor erstellen und Sicherheiten darin deponieren.

- Erzeugen von Indizes, die durch die Sicherheiten des Tresors gedeckt sind

  Der Benutzer gibt an, wie viele Indizes er erstellen möchte. Das System erzeugt eine gleiche Schuldmenge, die entsprechend dem Sollzinssatz der hinterlegten Sicherheiten zu erwirtschaften beginnt.

- Rückzahlung der Tresor-Schulden

  Wenn der Tresor-Ersteller seine Sicherheiten zurückziehen möchte, muss er seine ursprüngliche Schuld plus die aufgelaufenen Zinsen zurückzahlen.

- Sicherheiten zurückziehen

  Nachdem der Benutzer seine Schulden ganz oder teilweise zurückgezahlt hat, kann er seine Sicherheiten zurückziehen.

Tresor-Liquidierung

Um das System solvent zu halten und den Wert der gesamten ausstehenden Schulden zu decken, kann jeder Tresor aufgelöst werden, wenn seine Besicherungsquote unter einen bestimmten Grenzwert fällt. Jeder kann eine Liquidation auslösen, in diesem Fall wird das System die Sicherheiten des Tresors beschlagnahmen und diese in einer Sicherheit-Auktion verkaufen.

Liquidationsversicherung

In einer Version des Systems können Tresor-Ersteller die Option haben, einen *Auslöser* zu wählen, für den Fall, wenn ihre Tresore aufgelöst werden. Auslöser sind intelligente Verträge, die automatisch mehr Sicherheiten zu einem Tresor hinzufügen und es möglicherweise vor der Auflösung retten. 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 Tresoren ist die Hinzufügung von zwei verschiedenen Grenzwerten: *sicher* und *Risiko*. Tresor-Benutzer können so lange Schulden machen, bis sie die sichere Grenze erreichen (die höher als die Risikogrenze ist), und sie werden nur dann aufgelöst, wenn die Besicherung des Tresors unter die Risikogrenze fällt.

Sicherheit-Auktionen

Um eine Sicherheit-Auktion zu starten, muss das System eine Variable bezeichnet als *Liquidationsmenge* verwendet werden, um die Höhe der Schulden zu bestimmen, die bei jeder Auktion zu decken ist, und den entsprechenden Betrag der dazugehörenden Sicherheiten. *Eine Liquidationsstrafe* wird auf jeden versteigerten Tresor angewandt.

Parameter einer Sicherheit-Auktion

Name des Parameters	Beschreibung
minimalesGebot	Mindestmenge an Coins, die in einem Gebot angeboten werden müssen
Rabatt	Rabatt, zu dem die Sicherheiten verkauft werden

untereSicherheitMedianAbweichung	Maximale untere Grenze der Abweichung, die der Median der Sicherheiten im Vergleich zu dem Orakelpreis haben kann
obereSicherheitMedianAbweichung	Maximale obere Abweichung, die der Median der Sicherheiten im Vergleich zu dem Orakelpreis haben kann
untereSystemCoinMedianAbweichung	Maximale untere Grenze der Abweichung, die die System-Coin-Orakel-Preisangabe haben kann im Vergleich zum System-Coin-Orakelpreis
obereSystemCoinMedianAbweichung	Maximale obere Abweichung, die der Sicherheitsmedian haben kann im Vergleich zu dem System-Coin-Orakelpreis
minSystemCoinMedianAbweichung	Mindestabweichung für das System-Coin-Medianergebnis im Vergleich zum Rückzahlungspreis, um den Median zu berücksichtigen

Mechanismus einer Sicherheit-Auktion

Die Auktion mit festem Abschlag ist ein unkomplizierter Weg (im Vergleich zu englischen Auktionen), um Sicherheiten im Austausch gegen System-Coins zur Begleichung uneinbringlicher Schulden zum Verkauf anzubieten. Die Bieter müssen nur dem Auktionshaus erlauben, ihre sicherEngine.CoinBalance zu transferieren und können dann kaufenSicherheit aufrufen, um ihre System-Coins gegen Sicherheit einzutauschen, die mit einem Abschlag gegenüber dem zuletzt verzeichneten Marktpreis verkauft wird.

Bieter können auch die Menge der Sicherheiten überprüfen, die sie bei einer bestimmten Auktion erhalten können indem sie erhaltenSicherheitGekauft oder erhaltenApproximativSicherheitGekauft aufrufen. Beachten Sie, dass erhaltenKollateralGekauft nicht als Ansicht gekennzeichnet ist, da es den Rückzahlungspreis aus dem Orakel-Relayer (und auch aktualisiert) während erhaltenApproximativKollateralGekauft den letzteLiesRückzahlungspreis verwendet.

Schuldauktionen

Für den Fall, dass eine Sicherheit-Auktion nicht alle uneinbringlichen Schulden in einem Tresor abdecken kann und wenn das System keine Überschussreserven hat, kann jeder eine Schuldauktion auslösen.

Schuldauktionen dienen dazu, mehr Protokoll-Tokens zu erstellen (Abschnitt 10) und sie für Indizes, die die verbleibenden uneinbringlichen Schulden des Systems annullieren können.

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

- anfänglicheSchuldauktionsmenge: die anfängliche Menge der Protokoll-Tokens, die Post-Auktion erstellt werden sollten

- Schuldauktionsgebotshöhe: die anfängliche Gebotshöhe (wie viele Indizes müssen im für anfänglicheSchuldAuktionsmenge Protokoll-Token angeboten werden)

Autonome Parametereinstellung einer Schuldauktion

Die anfängliche Menge der in einer Schuldauktion erstellten Protokoll-Tokens kann entweder durch die Abstimmung der Verwaltung festgelegt werden, oder sie kann durch das System automatisch angepasst werden. Eine automatische Version müsste mit Orakeln integriert werden (Abschnitt 6), aus denen das System die Marktpreise der Protokoll-Tokens und des Reflex-Indexes ablesen würde. Das System würde dann die anfängliche Menge an Protokoll-Tokens (anfänglicheSchuldauktionsmenge) festlegen, die für Schuldauktionsgebotshöhe Indizes erstellt werden. anfänglicheSchuldauktionsmenge kann mit einem Abschlag im Vergleich zu dem aktuellen PROTOKOLL/INDEX-Marktpreis festgelegt werden, um Anreize zum Bieten zu schaffen.

Parameter einer Schuldauktion

Name des Parameters	Beschreibung
MengeVerkauftErhöhung	Erhöhung der Menge an Protokoll-Tokens, die für die gleiche Anzahl der Indizes erstellt werden
Gebotsminderung	Mindestminderung des nächsten Gebots für die akzeptierte Menge von Protokoll-Tokens für die gleiche Anzahl der Indizes
Gebotsdauer	Wie lange das Bieten dauert, nachdem ein neues Gebot abgegeben wurde (in Sekunden)
Gesamtauktionslänge	Gesamtlänge der Auktion (in Sekunden)
AuktionenGestartet	Wie viele Auktionen haben bis jetzt begonnen

Mechanismus einer Schuldauktion

Im Gegensatz zu Sicherheit-Auktionen gibt es bei Schuldauktionen nur eine Stufe:

reduzierenVerkaufteMenge(uint id, uint Verkaufmenge, uint Gebot): Verringerung der Menge an Protokoll-Tokens, die im Austausch für eine feste Anzahl von Indizes akzeptiert werden.

Die Auktion wird neu gestartet, wenn sie keine abgegebenen Gebote hat. Jedes Mal, wenn sie neu gestartet wird, bietet das System mehr Protokoll-Tokens für die gleiche Anzahl von Indizes. Der neue Protokoll-Token-Betrag wird berechnet als *letzteTokenmenge* MengeVerkauftErhöhung* / 100. Nachdem die Auktion begleicht wird erstellt das System Tokens für den Höchstbietenden.

Protokoll-Token

Wie in früheren Abschnitten beschrieben, muss jedes Protokoll durch einen Token geschützt werden, der durch Schuldauktionen erstellt wird. Neben dem Schutz wird der Token auch dazu verwendet um einige Systemkomponenten zu steuern. Außerdem wird das Angebot an Protokoll-Token durch Überschussauktionen schrittweise reduziert werden. Die Höhe des Überschusses, der im System anfallen muss, bevor zusätzliche Mittel versteigert werden, wird als *Überschusspuffer* bezeichnet und er wird automatisch als Prozentsatz der ausgegebenen Gesamtschuld angepasst.

Versicherungsfonds

Neben dem Protokoll-Token kann die Verwaltung einen Versicherungsfonds einrichten, der eine breite Reihe von unkorrelierten Vermögenswerten hält und als Absicherung für Schuldauktionen genutzt werden kann.

Überschussauktionen

Bei Überschussauktionen werden die im System angefallenen Stabilitätsgebühren für Protokoll-Token verkauft, die dann verbrannt werden.

Parameter einer Überschussauktion

Name des Parameters	Beschreibung
Gebotserhöhung	Mindesterhöhung des nächsten Gebots
Gebotsdauer	Wie lange die Auktion nach Abgabe eines neuen Gebots dauern wird (in Sekunden)
Gesamtauktionslänge	Gesamtlänge der Auktion (in Sekunden)
GestarteteAuktionen	Wie viele Auktionen bisher gestartet wurden

Mechanismus einer Überschussauktion

Überschuss-Auktionen haben eine einzige Stufe:

erhöhenGebotsgröße(uint id, uint Kaufmenge, uint Gebot): jeder kann einen höheren Betrag von Protokoll-Tokens für die gleiche Menge an Indizes (Überschuss) bieten. Jedes neue Gebot muss höher oder gleich sein als *letztesGebot * Gebotserhöhung* / 100. Die Auktion wird beendet nach maximalen *Gesamtauktionslänge* Sekunden oder nachdem *Gebotsdauer* Sekunden seit dem letzten Gebot und in der Zwischenzeit keine neuen Gebote abgegeben wurden.

Eine Auktion wird neu gestartet, wenn sie keine Gebote enthält. Liegt hingegen mindestens ein Gebot für die Auktion, bietet das System den Überschuss dem Höchstbietenden an und verbrennt dann alle gesammelten Protokoll-Tokens.

Verwaltung überschüssiger Indizes

Jedes Mal, wenn ein Nutzer Indizes generiert und damit implizit Schulden macht, beginnt das System einen Sollzinssatz auf den Tresor des Nutzers anzuwenden. Die aufgelaufenen Zinsen werden in zwei verschiedenen intelligenten Verträgen zusammengelegt:

- *Die Buchhaltung-Engine*, die zum Auslösen von Schulden- (Abschnitt 9.2) und Überschuss- (Abschnitt 10.1) Auktionen
- *Die Überschusskasse*, die zur Finanzierung von Kerninfrastrukturkomponenten und zur Schaffung der Anreize für die externen Akteure zur Aufrechterhaltung des Systems verwendet wird

Die Überschusskasse ist für die Finanzierung von drei Kernkomponenten des Systems zuständig:

- Orakel-Modul (Abschnitt 6). Je nachdem, wie ein Orakel strukturiert ist, zahlt die Schatzkammer entweder den sich auf der Verwaltung-Whitelist, außerhalb der Kette befindenden Orakeln oder zahlt sie für Aufrufe bei Orakelnetzwerken. Die Schatzkammer kann auch so eingerichtet werden, dass sie den Adressen zahlt, die Gas ausgegeben haben, um ein Orakel aufzurufen und es zu aktualisieren

- In einigen Fällen unabhängige Teams, die das System warten. Beispiele hierfür sind Teams, die neue Arten von Sicherheiten auf die Whitelist setzen oder den Preisfestsetzer des Systems feinabstimmen (Abschnitt 4.2)

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

Externe Akteure

Das System ist von externen Akteuren abhängig, um ordnungsgemäß zu funktionieren. Diese Akteure haben wirtschaftliche Anreize, sich an Bereichen wie Auktionen, globales Settlement, Market-Making und Preisaktualisierung zu beteiligen, um die Gesundheit des Systems aufrechtzuerhalten.

Wir werden erste Benutzerschnittstellen und automatisierte Skripte bereitstellen, um so viele Menschen wie möglich zu befähigen, das Protokoll sicher zu halten.

Adressierbarer Markt

Wir sehen RAI in zwei Hauptbereichen als nützlich an:

- **Portfoliodiversifizierung**: Investoren nutzen RAI, um eine gedämpfte Exposition in einem Vermögenswert wie ETH zu erhalten, ohne das gesamte Risiko des Besitzes von Ether einzugehen

- **Sicherheiten für synthetische Anlagenprodukte**: RAI kann den Protokollen wie UMA, MakerDAO und Synthetix eine geringere Exposition auf dem Kryptomarkt anbieten und den Nutzern mehr Zeit geben, um ihre Positionen zu verlassen im Falle von Szenarien wie der Schwarze Donnerstag vom März 2020, als Krypto-Vermögenswerte im Wert von Millionen von Dollar liquidiert wurden

Zukünftige Forschung

Um die Grenzen des dezentralen Geldes zu erweitern und weitere Innovationen im dezentralen Finanzwesen zu bringen, werden wir weiterhin nach Alternativen in Kernbereichen wie Verwaltung-Minimierung und Liquidationsmechanismen suchen.

Wir wollen zunächst die Grundlage für künftige Standards rund um Protokolle schaffen, die sich selber von der Kontrolle von außen sperren und für echte "Geldroboter", die sich an die Marktkräfte anpassen. Anschließend laden wir die Ethereum-Gemeinschaft zur Diskussion und Entwicklung der Verbesserungen rund um unsere Vorschläge ein, mit besonderem Fokus auf Sicherheiten und Schuldauktionen.

Risiken und Schadensminderung

Es gibt einige Risiken die mit der Entwicklung und Einführung eines Reflex-Index verbunden sind, sowie mit den darauf aufgebauten Systemen:

- **Fehler in intelligenten Verträgen**: Das größte Risiko für das System ist die Möglichkeit, dass ein Fehler jedem erlaubt, alle Sicherheiten zu entnehmen oder das Protokoll in einem Zustand festzuhalten, von dem es sich nicht wiederherstellen kann. Wir planen, unseren Kode von mehreren Sicherheitsforschern überprüfen zu lassen und das System in einem Testnetz zu testen, bevor wir es in die Produktion einführen

- **Oracle-Ausfall**: Wir werden Eingaben aus mehreren Oracle-Netzwerken zusammenfassen und es wird strenge Regeln an einem Ort geben, um jeweils nur ein Orakel zu aktualisieren, damit eine böswillige Steuerung nicht einfach falsche Preise einführen kann

- **Schwarze-Schwan-Ereignisse bei Sicherheiten**: Es besteht das Risiko eines schwarzen Schwan-Ereignisses bei den zugrundeliegenden Sicherheiten, was zu einer hohen Anzahl der liquidierten Tresore führen kann. Die Liquidationen sind möglicherweise nicht in der Lage, die gesamten ausstehenden uneinbringlichen Schulden zu decken, also das System wird kontinuierlich seinen Überschusspuffer verändern, um einen angemessenen Betrag an ausgegebenen Schuldtiteln zu decken und Marktschocks zu widerstehen

- **Ungeeignete Zinssetzungsparameter**: Autonome Rückmeldungsmechanismen sind sehr experimentell und verhalten sich möglicherweise nicht genau so, wie wir es in Simulationen voraussehen. Wir planen, der Verwaltung zu erlauben, diese Komponente fein abzustimmen (während sie begrenzt ist), um unerwartete Szenarien zu vermeiden.

- **Fehler einen gesunden Markt für Insolvenzverwalter zu laden**: Insolvenzverwalter sind wichtige Akteure die sicherstellen, dass alle ausgegebenen Schulen durch Sicherheiten gedeckt sind. Wir planen Schnittstellen und automatisierte Skripte zu schaffen, damit so viele Menschen wie möglich sich an der Sicherheit des Systems beteiligen können.

Zusammenfassung

Wir haben ein Protokoll vorgeschlagen, das Schritt für Schritt der menschlichen Kontrolle entkommt und einen besicherten Vermögenswert mit geringer Volatilität, einen so genannten Reflex-Index, ausgibt. Wir haben zuerst den autonomen Mechanismus zur Beeinflussung des Marktpreises des Index vorgestellt und dann beschrieben, wie mehrere intelligente Verträge die Macht der Token-Inhaber über das System begrenzen können. Wir haben ein selbstversorgendes Schema zur Medianisierung von Preisdaten von mehreren unabhängigen Orakelnetzwerken dargestellt und dann haben wir mit der Präsentation des allgemeinen Mechanismus für die Erstellung von Indizes und die Liquidierung von Tresoren beendet.

Referenzen

[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

Glossar

Reflex-Index: ein besicherter Vermögenswert, der die Volatilität seines Basiswerts dämpft

RAI: unser erster Reflex-Index

Rückzahlungspreis: der Preis, den das System für den Index haben möchte. Er ändert sich, beeinflusst durch eine (vom RRFM berechneten) Tilgungsrate, falls der Marktpreis nicht nahe daran liegt. Er soll die Tresor-Ersteller dazu bewegen, mehr zu erwirtschaften oder einen Teil ihrer Schulden zurückzuzahlen

Sollzinssatz: jährlicher Zinssatz, der auf alle Tresore mit ausstehenden Schulden angewandt wird

Rückmeldungsmechanismus der Rückzahlungsrate (Englische Abkürzung: RRFM): ein autonomer Mechanismus, der die Markt- und Rückzahlungspreise eines Reflex-Indexes vergleicht und dann eine Rückzahlungsrate berechnet, die die Tresor-Ersteller langsam dazu bringt, mehr oder weniger Schulden zu machen (und versucht implizit, die Abweichung zwischen Markt- und Rückzahlungspreis zu minimieren)

Geldmarktsetzer (Englische Abkürzung: MMS): ein dem RRFM ähnlicher Mechanismus, der mehrere monetäre Hebel gleichzeitig betätigt. Im Fall von Reflex-Indizes verändert er sowohl den Anleihezins und den Rückzahlungspreis

Oracle Netzwerk Medianizer (Englische Abkürzung: ONM): ein intelligenter Vertrag, der die Preise aus mehreren Orakelnetzwerken abruft (die nicht von der Verwaltung kontrolliert werden) und sie medianisiert, wenn eine Mehrheit (z.B. 3 von 5) ein Ergebnis zurückgibt, ohne zu werfen

Eingeschränktes Verwaltungsmodul (Englische Abkürzung: RGM): eine Reihe von intelligenten Verträgen, die die Macht der Inhaber von Verwaltung-Token über das System einschränken. Es setzt entweder Zeit Verzögerungen durch oder begrenzt die Möglichkeiten der Verwaltung, bestimmte Parameter festlegen zu müssen

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

Buchhaltung-Engine: Systemkomponente, die Schuld- und Überschussauktionen auslöst. Sie behält auch den Überblick über die Höhe der aktuell versteigerten Schulden, der nicht verarbeiteten uneinbringlichen Schulden und den Überschusspuffer

Überschusspuffer: Betrag der anfallenden und im System verbleibenden Zinsen. Alle Zinsen die über diesen Grenzwert hinaus anfallen, werden in Überschussauktionen verkauft, bei denen Protokoll-Tokens gebrannt werden

Überschuss-Schatzkammer: Vertrag, der den verschiedenen Systemmodulen die Erlaubnis gibt aufgelaufene Zinsen zu entnehmen (z.B. ONM für Orakelaufrufe)