Rai：DeFi生态系统中低波动性及信任最小化的抵押品

Stefan C. Ionescu, Ameen Soleimani

2020年五月

摘要

我们提出了一种治理最小化，去中心化的协议，该协议会自动对市场力量做出反应，以修改其原生抵押资产的目标价值。该协议允许任何人利用其加密资产并发行“反射指数”，这是其基础抵押品的低波动版本。我们概述了指数如何作为通用的低波动性抵押品保护其持有人以及其他去中心化融资协议免受市场突变影响。利用我们的基础架构，这项计划可帮助其他团队来推出自己的合成资产。最后，我们提供了许多DeFi协议中常见的当前预言机（oracle）和治理结构的替代方案。

目录

引言

金钱是人类赖以生存的最强大的协调机制之一。历史上，管理货币供应的特权一直掌握在主权领导人和金融精英手中，而这种特权却被强加给不知情的普通公众。比特币已经证明为基层抗议来证明价值储存商品资产的可能性，而以太坊为我们提供了构建资产抵押合成工具的平台，该工具可以防止波动，用作抵押或与参考价格挂钩，并且用作日常交易的交换媒介。所有交易均遵循去中心化共识的相同原则。

用比特币无需许可存储财富以及在以太坊上恰当地去中心化的合成工具，将为即将到来的金融革命奠定基础，为现代金融系统边缘的人们提供围绕新货币体系进行协调的手段。

本文介绍了建立反射性指数的框架。这是一种新的资产类型，将有助于其他合成金融工具蓬勃发展，并将为整个去中心化金融行业奠定重要的基础。

反射指数概述

反射指数的目的不是维持特定的锚定汇率，而是减少其抵押品的波动性。反射指数使任何人都可以进入加密货币市场，而风险规模比持有实际加密资产要小很多。我们相信，RAI–我们的第一个反射指数，它将对在以太坊上发行合成资产的其他团队（例如MakerDAO的Multi-Collateral DAI [1]，UMA [2]，Synthetix [3]）有直接的实用性，因为它使他们的系统降低了对 ETH等波动资产的唱空，并在市场发生重大变化的情况下为用户提供更多时间退出头寸。

为了了解反射指数，我们可以将其赎回价格与稳定币价格进行比较。

赎回价格是系统中一个债务单位（或一个币）的价值。它只能用作内部会计工具，它不同于市场价格（币的市场交易价格）。对于具有法定后盾的稳定币（例如USDC），系统操作员声明任何人都可以用1美元赎回一枚硬币，因此这些硬币的赎回价格始终为一。但也有其他情况，诸如MakerDAO的Multi Collateral DAI（MCD）等以加密货币为后盾的稳定币，该系统的目标是固定一美元的锚定汇率，因此赎回价格也固定为一美元。

在大多数情况下，稳定币的市场价格与其赎回价格之间会有差异。这些情况带来了套利机会。如果市场价格低于赎回价格，交易者将创建更多硬币，如果市场价格高于赎回价格，他们将赎回其稳定币作为抵押品（例如，USDC中的美元）。

反射指数类似于稳定币，因为它们也有系统的目标赎回价格。它们的主要区别在于反射指数的赎回不会保持固定不变，而是旨在在受到市场力量影响的情况下进行更改。在第4节中，我们将解释指数的赎回价格如何浮动并为其用户创造新的套利机会。

设计理念和进入市场策略

我们的设计理念是优先考虑安全性，稳定性和交付速度。

多抵押DAI是开始迭代RAI设计的最合适的地方。该系统已经过大量审核和正式验证，具有最小的外部依赖性，并且拥有一个活跃的专家社区。为了最大程度地减少开发和通信工作，我们希望仅对原始MCD代码库进行最简单的更改，以便于我们的执行。

我们最重要的修改包括添加了一个自动汇率设置器，一个与许多独立的价格信息集成的Oracle网络中值器和一个治理最小化层，该层旨在将系统与人为干预尽可能地隔离开。

该协议的第一个版本（第1阶段）将仅包括利率设置器和核心体系结构中的其他次要改进。一旦证明设置器可以按预期工作，就可以更安全地添加oracle中值器（阶段2）和治理最小化层（阶段3）。

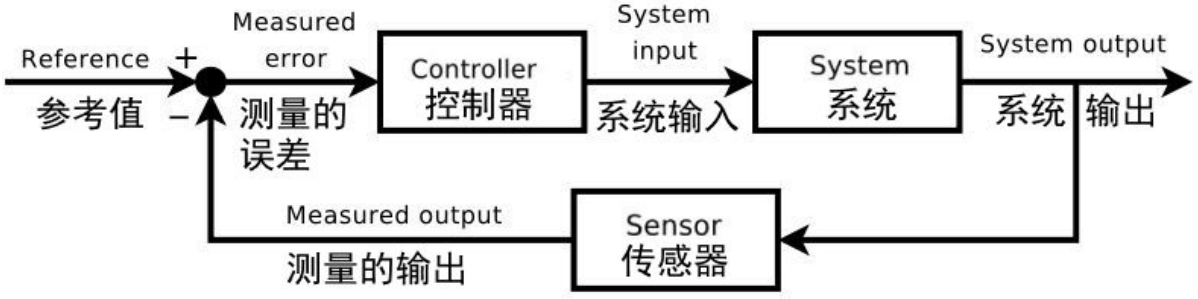
货币政策机制

控制理论导论

大多数人都熟悉的一种常见控制系统是淋浴。当有人开始淋浴时，他们会设定一个理想的水温，根据控制理论，该温度称为参考设定点。该人员充当控制器，持续测量水温（称为系统输出），并根据所需温度与当前温度之间的偏差（或误差）来修改他们旋转淋浴器旋钮的速度。旋钮旋转的速度称为系统输入。目的是足够快地旋转旋钮，以快速达到参考设定点，但又不能太快以至于温度过冲。如果有水流温度突然变化的系统冲击，该人员因为了解旋转旋钮的速度，可以保持当前温度而响应干扰。

在动态系统中保持稳定性的科学学科称为控制理论，它已广泛应用于汽车巡航控制，飞行导航，化学反应堆，机械臂和各种工业过程。关键任务控制系统的一个示例是比特币难度调整算法，虽然具有可变的哈希率，但算法可保持十分钟的平均阻塞时间。

在大多数现代控制系统中，算法控制器通常被嵌入在过程中。算法可以控制控制系统输入（例如汽车的油门踏板），以便根据系统输出（例如汽车的速度）和 设定值（例如巡航控制速度）的偏差更新输入值。



最常见的算法控制器类型是PID控制器。超过95%的工业应用及广泛的生物系统都采用PID控制的元素[4]。PID控制器使用具有三个部分的数学公式来确定其输出：

控制器输出=比例单元+积分单元+导数单元

比例单元是控制器中与偏差成比例的部分。如果偏差较大且为正数（例如，巡航控制速度设定点远高于汽车的当前速度），则比例响应将较大且为正数（例如将油门踏板放下）。

积分单元是控制器中考虑偏差持续时间的部分。它是通过取随时间推移的偏差的积分确定的，并且主要用于消除稳态误差。它会逐渐累积以响应微小的，与设定点的持续偏差（例如，巡航控制设定点在几分钟内比汽车速度高出1 mph）。

导数单元是控制器中考虑偏差增长或缩小的速度的部分。它是根据偏差的导数确定的，并在偏差增大时加快控制器响应速度（例如，如果巡航控制设定点高于汽车速度且汽车开始减速。当

偏差减小时，它还可以通过降低控制器响应速度来减少过冲现象（例如，当汽车的速度开始接近巡航控制设定点时减轻油耗）。

三部分都可以独立调整，组合起来使PID控制器在管理各种控制系统应用程序时具有极大的灵活性。

PID控制器在允许响应时间有一定程度的滞后以及系统试图使其自身稳定时可能在设定点附近出现过冲和振荡的系统中效果最佳。像RAI这样的反射指数系统非常适合此类情况，因为PID控制器可以更改其赎回价格。

更一般而言，最近发现，当前许多中央银行货币政策规则（例如泰勒规则）实际上类似PID控制器 [5]。

赎回率反馈机制

赎回率反馈机制是负责更改反射指数赎回价格的系统组件。为了了解其工作原理，我们首先需要描述为什么系统需要反馈机制而不是使用手动控制，以及该机制的输出是什么。

反馈机制组成部分

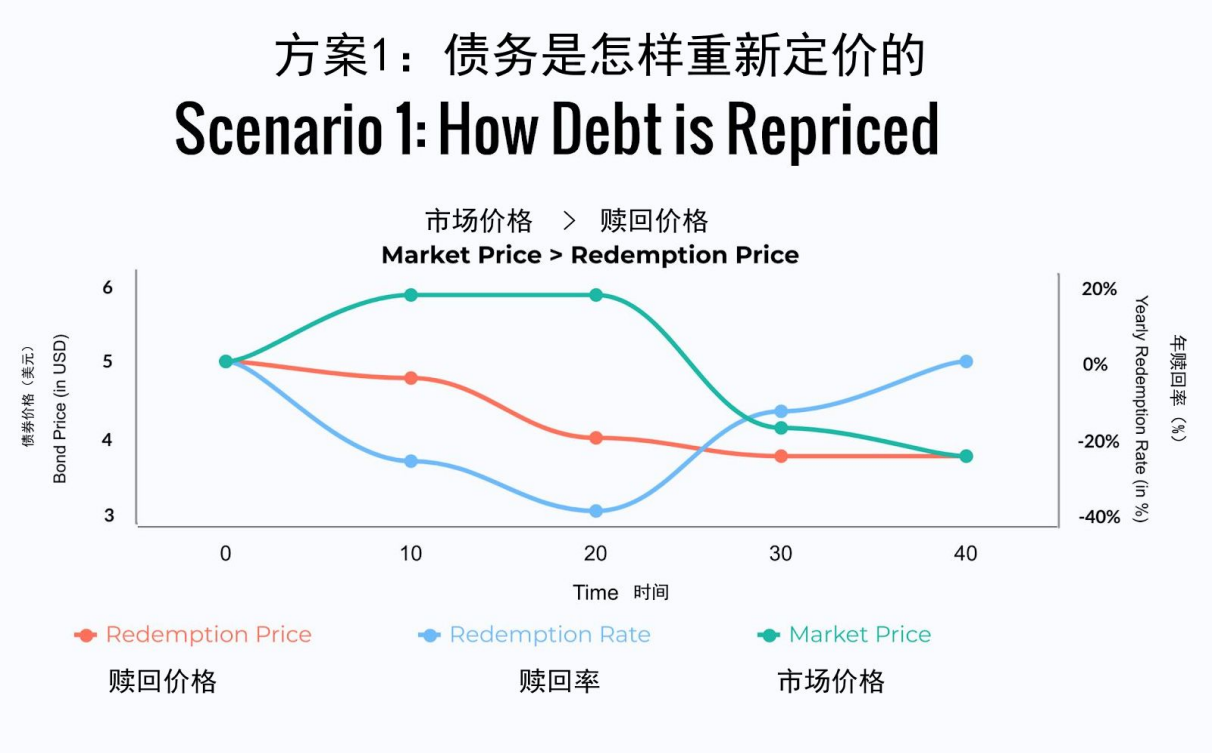
从理论上讲，是有可能直接操纵反射指数的赎回价格的（如第2节所述），以影响指数使用者并最终改变指数的市场价格。但实际上，这种方法不会对系统参与者产生期望的效果。从SAFE持有人的角度来看，如果赎回价格仅提高一次，则他们可能会接受更高的每债务单位价格，通过降低抵押率吸收损失并维持其头寸。但是，如果他们预计赎回价格会随着时间的推移继续增加，则他们可能会更倾向于避免预期的未来损失，从而选择偿还债务并关闭头寸。

我们期望反射指数系统参与者不直接对赎回价格的变化做出响应，而是对赎回价格的变化率做出响应，我们将其称为*赎回率*。赎回率由*反馈机制*设置，治理可以微整或允许其完全自动化。

反馈机制方案

回想一下，反馈机制旨在通过使用赎回率来抵消市场力量的变化，从而在赎回价格和市场价格之间保持均衡。为达到这一目的，赎回率与市场价格和赎回价格之间的偏差相反。

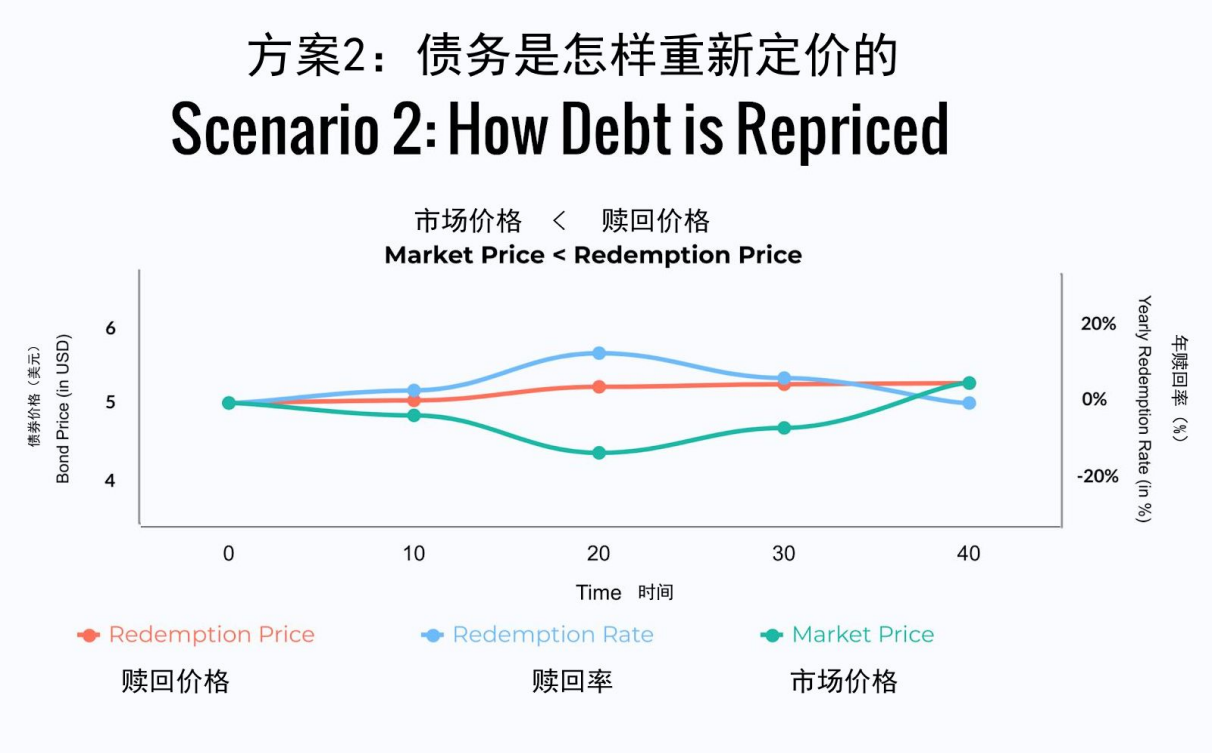
在下面的第一种情况下，如果指数的市场价格高于其赎回价格，则该机制将计算负利率，这将开始降低赎回价格，从而使该系统的债务更便宜。



预期赎回价格下降将可能使人们不愿持有指数，并鼓励SAFE持有人产生更多债务（即使抵押价格不变），然后再在市场上出售，从而平衡供求关系。请注意，这是指数持有人对反馈机制做出快速反应的理想方案。在实践中（尤其是在发行后的初期），从发行债务的数量和随后的市场价格来看，我们预计该机制的启动与实际结果之间存在一定的滞后性。

另一方面，在方案二中，如果指数的市场价格低于赎回价格，则利率变为正数并开始对所有债务重新定价，从而使其价格更高。

随着债务变得更加昂贵，所有SAFE的抵押率都会下降（因此SAFE创建者有动力偿还债务），并且用户开囤积指数，期望它们会增值。



反馈机制算法

在以下情况下，我们假设该协议使用比例积分控制器来计算赎回率：

- 反射指数以任意赎回价格“rand”发行。
- 在某个时刻，指数的市场价格从“ rand”升至“ rand” + x。在反馈机制读取新的市场价格后，它将计算一个比例单元p，在这种情况下为-1 *（（“rand”+ x）/“rand”）。该比例为负，为了降低赎回价格，然后对指数重新定价，从而使它们变得更便宜。
- 计算比例后，该机制将通过将最后偏差积分秒中所有过去的误差相加来确定积分单元i（deviationInterval ）。
- 该机制将比例和积分相加，然后计算每秒的赎回率r，此比率逐渐开始降低赎回价格。随着SAFE创建者意识到他们可以产生更多的债务，他们将发行更多的指数充斥市场。
- 在n秒后，该机制检测到市场价格和赎回价格之间的偏差可以忽略不计（在指定的参数噪声下）。此时，算法将r设置为零，并保持赎回价格。

在实践中，该算法将更加稳健。我们要么使某些变量不可变（例如，噪声参数、deviationInterval），要么对治理可调整的项目进行严格限制。

反馈机制调整

对于反射指数系统的正常运行而言，最重要的是算法控制器参数的调整。不正确的参数设置可能会导致系统太慢而无法实现稳定性，严重超调或在面对外部冲击时不稳定。

PID控制器的调整过程通常包括运行实时系统，微调调整参数并观察系统的响应，通常会在此过程中故意引入冲击。考虑到调整实时反射指数系统参数的困难和财务风险，我们计划尽可能利用计算机建模和仿真来设置初始参数，但是如果生产中有其他数据显示它们为次优，则还可以允许治理更新调整参数。

货币市场设置工具

在RAI中，我们计划将借贷利率（生成指数时使用的利率）保持固定（或设定上限），并且仅修改赎回价格，从而最大程度地减少建模反馈机制的复杂性。在我们的案例中，借款利率等于稳定费与多抵押DAI中DSR之间的价差。

即使我们计划保持固定的借入利率，也仍可以使用货币市场设置工具将其与赎回价格一起更改。货币市场改变借入利率和赎回价格，从而激励SAFE创建者产生或多或少的债务。如果指数的市场价格高于赎回价格，则两种利率都将开始下降，而如果低于赎回价格，则利率将升高。

全球结算

全球结算是用于保证所有反射指数持有人赎回价格的最后手段。这意味着允许反射指数持有人和SAFE创建者均以其净值（根据最新赎回价格，每种抵押品的指数数量）赎回系统抵押品。刻录一定数量的协议代币后，任何人都可以触发结算。

结算有三个主要阶段：

- 触发：触发结算后，用户无法再创建SAFE。所有抵押品喂价和赎回价格都会被冻结及记录下来。
- 处理：处理所有未完成的拍卖。
- 债权：每个反射指数持有人和SAFE创建者都可以根据指数最后记录的赎回价格对任何系统抵押品索取固定金额的款项。

治理

除非治理代币持有者部署一个全新的系统，否则绝大多数参数将是不可变的，并且内部智能合约机制将无法升级。我们之所以选择这种策略，是因为我们可以消除人们为了自己的利益而试图影响治理流程的元博弈，从而破坏对系统的信任。我们建立协议的正确运行时无需过分相信人类（“比特币效应”），因此我们可以最大程度地提高社会延展性，并将其他希望将RAI用作自己项目核心基础结构的开发人员的风险降至最低。

对于可以更改的几个参数，我们建议添加“受限治理模块”，以延迟或限制所有可能的系统修改。此外，我们介绍了“治理冰河时代”。它是一个权限注册表，可以在某些截止日期过去之后将系统的某些部分锁定以不受外部控制。

限时治理

限时治理是“受限治理模块”的第一部分。它在应用于同一参数的更改之间强加了时间延迟。一个例子是，自上次oracle修改以来至少经过T秒之后，便可以更改在Oracle网络中值器（Oracle Network Medianizer）（第6.2节）中使用的oracle的地址。

行动约束治理

“受限治理模块”中的第二个组件是“行动约束治理”。每个可管理的参数都限制了它可以设置为什么值以及在一段时间内可以更改的值。值得注意的例子是“赎回率反馈机制”（第4.2节）的初始版本，治理代币持有者将可以对其进行微调。

治理冰期

“冰期”是一成不变的智能合约，规定了更改特定系统参数和升级协议的截止日期。在治理想要确保在协议锁定并拒绝外部干预之前可以修复错误的情况下，可以使用它。“冰期”将通过在截止日期注册表中检查参数名称和受影响合同的地址来验证是否允许更改。如果截止日期已过，则请求将恢复。

如果在协议应该开始锁定的日期附近发现错误，则治理能够将“冰期”延迟固定的次数。例如，“冰期”只能延迟3次，每次延迟一个月，以便恰当地测试新实施的错误修复。

需要治理的核心领域

我们设想了可能需要治理的四个领域，尤其是在此框架的早期版本中：

- 添加新的抵押品类型：RAI仅由ETH支持，而其他指数将由多种抵押品支持，并且治理能够随着时间分散风险。
- 更改外部依赖项：可以升级系统所依赖的oracle和DEX。治理可以使系统指向较新的依赖项，以便其继续正常运行。
- 调整利率设定器：早期的货币政策控制者将具有可以在合理范围内更改的参数（如“行动与限时治理”所述）
- 在系统版本之间迁移：在某些情况下，治理可以部署新系统，授予其打印协议代币的权限并从旧系统撤回该权限。此迁移是在下面概述的“受限迁移模块”的帮助下执行的。

受限迁移模块

以下是一个在系统版本之间迁移的简单机制：

- 有一个迁移注册表，用于跟踪同一协议代币涵盖多少个不同的系统，以及哪些系统可以在债务拍卖中被拒绝打印协议代币的权限。
- 每次治理部署新的系统版本时，他们都会在迁移注册表中提交系统债务拍卖合同的地址。治理还需要指定他们是否能够阻止系统打印协议代币。同样，治理可以随时指定一个系统将始终能够打印令牌，因此将永远不会从此迁移出去。
- 在提出新系统和从旧系统撤消权限之间有一段冷却期。
- 可以设置可选合同，以便在拒绝打印权限后自动关闭旧系统。

迁移模块可以与“冰期”结合使用。“冰期”自动为特定系统提供始终能够打印代币的权限。

自动系统关闭

在某些情况下，系统可以自动检测并自动触发结算，而无需销毁协议代币：

- 严重的喂价延迟：系统检测到很长一段时间一项或多项抵押品或指数喂价并未更新。
- 系统迁移：这是一个可选合同，可以在冷却期后关闭协议，在从治理撤回债务拍卖机制打印协议代币的能力之时起（受限迁移模块，第5.4.1节）。
- 一致的市场价格偏差：系统检测到指数的市场价格与赎回价格相比已经长时间偏离了x%。

治理在仍然受限的同时能够升级这些自主关闭模块，或者直到冰期开始锁定系统的某些部分。

预言机（oracles）

系统需要给三种主要资产类型读取喂价：指数，协议代币和每个列入白名单的抵押品类型。价格信息可以由治理主导的预言机或已经建立的预言网提供。

治理领导的预言机

治理代币持有者或发起该协议的核心团队可以与其他实体合作，这些实体在链下收集多个喂价信息，然后将单个交易提交给对所有数据点进行中值处理的智能合约。

尽管此方法以不信任度为代价，但该方法在升级和更改oracle基础结构方面具有更大的灵活性。

Oracle网络中值器

一个oracle网络中值器是一种智能合约，可从不受治理直接控制的多个来源读取价格（例如，一种指数抵押品类型与其他稳定币之间的Uniswap V2池），然后将所有结果取中值。ONM的工作方式如下：

- 我们的合同跟踪白名单中可调用的Oracle网络以获取抵押价格。合同由系统产生的部分盈余资助（使用“盈余金库”，第11节）。每个Oracle网络都接受特定的代币作为付款方式，因此我们的合同还跟踪每个请求所需的最小金额和代币类型。
- 为了在系统中推送新的喂价，需要预先调用所有oracle。调用预言时，合同首先与oracle接受的代币之一交换一些稳定费。在调用了oracle之后，合同将调用标记为“有效”或“无效”。如果调用无效，则只有在调用了所有其他oracle并且合同检查是否存在有效多数时，才能再次调用特定的故障预兆。一个有效的oracle调用不得还原，并且必须检索最近m秒内某个时间发布在链上的价格。“检索”的含义取决于每种oracle类型：
    - 对于基于拉取的oracle，我们可以从中立即获得结果，我们的合同需要支付费用并直接获取价格。
    - 对于基于推送的oracle，我们的合同需要支付费用，调用oracle并需要等待一定的时间n后才能再次调用oracle，以获取所需价格。
- 每个Oracle结果保存在一个数组中。在调用每个列入白名单的oracle之后，如果数组具有足够的有效数据点以形成多数（例如，合同从3/5的预言机中接收到有效数据），则对结果进行排序，然后合同选择中位数。
- 不管合同是否找到多数，都将清除带有oracle结果的数组。合同将需要等待p秒，然后重新开始整个过程。

Oracle网络备份

如果中值器连续几次无法找到大多数有效的oracle网络，则治理可以添加一个备份oracle选项，该选项开始推高系统中的价格。

部署中值器时，必须设置备份选项，因为此后无法更改。此外，一个单独的合同可以监视备份是否已经替代中位机制太长时间并自动关闭协议。

保险箱（Safes)

为了创建指数，任何人都可以在保险箱（Safes)中存放和利用其加密抵押品。SAFE打开时，它将继续根据存入的抵押品的借贷利率计提债务。随着SAFE创建者偿还债务，他们将能够提取越来越多的锁定抵押品。

SAFE生命周期

建立反射指数并随后偿还SAFE的债务需要四个主要步骤：

- 将抵押品存入SAFE

  用户首先需要创建一个新的SAFE并将抵押品存入其中。

- 创建由SAFE抵押担保的指数

  用户指定他们要生成多少指数。系统会创建等额的债务，并根据抵押品的借入利率开始累计。

- 偿还SAFE债务

  当SAFE创建者想要提取其抵押品时，他们必须偿还其初始债务和应计利息。

- 提取抵押品

  在用户偿还部分或全部债务后可以提取抵押品。

SAFE清算

为了保持系统的偿债能力并覆盖全部未偿债务的价值，可以在其抵押比率低于一定阈值的情况下清算每个SAFE。任何人都可以触发清算，在这种情况下，系统将没收SAFE的抵押品，并在抵押品拍卖中出售。

清算保险

在系统的一个版本中，SAFE创建者可以选择为SAFE到期时选择触发器。触发器是智能合约，可自动在SAFE中添加更多抵押品，并有使其免受清算。触发的例子有卖空仓合约或与保险协议通信的合约（例如Nexus Mutual [6]）。

保护SAFE的另一种方法是增加两个不同的抵押阈值：安全和风险。SAFE用户会产生债务，直到他们达到安全阈值（高于风险）为止，并且只有在SAFE抵押物品于风险阈值时他们才会清算。

抵押拍卖

要开始抵押品拍卖，系统需要使用一个名为清算数量（liquidationQuantity）的变量，以确定每次拍卖所涵盖的债务数量以及相应的要出售的抵押品数量。所有拍卖的SAFE将被处以*清算罚款*。

抵押拍卖参数

参数名称	描述
最低出价（minimumBid）	一次竞标需要提供的最低币的数量
折扣（discount）	出售抵押品的折扣
下限抵押品中值偏差（lowerCollateralMedianDeviation）	与oracle价格相比，抵押品中值可拥有的最大下限偏差
上限抵押品中值偏差（upperCollateralMedianDeviation）	与oracle价格相比，抵押品中值可拥有的最大上限偏差
下限系统币中值偏差（lowerSystemCoinMedianDeviation）	与系统币oracle价格相比，抵押品中值可拥有的最大下限偏差
上限系统币中值偏差（upperSystemCoinMedianDeviation）	与系统币oracle价格相比，抵押品中值可拥有的最大上限偏差
最低系统币中值偏差（minSystemCoinMedianDeviation）	与赎回价格相比，最小的系统币中值结果以考虑中值

抵押拍卖机制

固定折扣拍卖是一种直接出售抵押品的方式（与英国拍卖相比），以换取用于清算坏账的系统币。竞价人仅需允许拍卖行转让他们的safeEngine.coinBalance，然后可以调用buyCollateral，以便将其系统币兑换为抵押品。该抵押品与其最新记录的市场价格相比以折扣价出售。

投标者还可以通过调用getCollateralBought或getroxCollateralBought来查看从特定拍卖中可获得的抵押品数量。注意getCollateralBought未标记为view，因为它从oracle中继器读取（并更新）redemptionPrice，而getroxCollateralBought使用lastReadRedemptionPrice。

债务拍卖

在抵押拍卖无法覆盖SAFE中的所有坏帐的情况下，如果系统没有任何盈余准备金，则任何人都可以触发债务拍卖。债务拍卖意在铸造更多的协议代币（第10节），并出售代币以换取指数，从而使该系统注销剩余坏账。

为了启动债务拍卖，系统需要使用两个参数：

- 初始债务拍卖数量（initialDebtAuctionAmount）：拍卖后需要铸造的协议代币的初始数量
- 债务拍卖出价大小（debtAuctionBidSize）：初始出价大小（必须提供多少指数以换取*初始拍卖数量*（initialDebtAuctionAmount）协议代币）

自动债务拍卖参数设置

债务拍卖中铸造的协议代币的初始数量可以通过治理投票来设置，也可以由系统自动调整。自动化版本将需要与oracle集成（第6节），系统将从中读取协议代币和反射指数市场价格。然后，系统将设置为债务拍卖出价大小（debtAuctionBidSize）指数铸造的协议代币的初始数量（初始债务拍卖数量（initialDebtAuctionAmount））。可以为初始债务拍卖数量（initialDebtAuctionAmount）设置一个与 协议/指数 实际市场价格相比的折扣率，以激励出价。

债务拍卖参数

参数名称	描述

出售数量增长（amountSoldIncrease）	对于相同数量的指数，要增铸的协议代币的数量
出价跌幅（bidDecrease）	对于相同数量的指数，下一个出价接受的协议代币的最小减少量
出价持续时间（bidDuration）	提交新出价后拍卖持续多长时间（秒）
拍卖总时长（totalAuctionLength）	拍卖的总时长（秒）
开始的拍卖（auctionsStarted）	截至目前已经开始的拍卖数量

债务拍卖机制

与抵押拍卖不同，债务拍卖只有一个阶段：

decreaseSoldAmount(uint id, uint amountToBuy, uint bid)；减少出售量（编号，购买数量，出价）：减少为了交换固定数量指数而接受的协议代币的数量。

如果没有出价，拍卖将重新开始。每次重新启动时，系统将为相同数量的指数提供更多协议代币。新协议代币的数量将计算为 最后的代币数量（TokenAmount）* 出售数量增长（amountSoldIncrease）/100。拍卖结束后，系统将为最高出价者铸造代币。

协议代币

如前面各节所述，每个协议都需要通过债务拍卖产生的代币来保护。除保护外，代币还将用于管理一些系统组件。此外，随着剩余拍卖的使用，协议代币的供应将逐渐减少。拍卖盈余资金之前需要在系统中产生的盈余金额称为“盈余缓冲”（surplusBuffer）。它会自动调整为已发行债务总额的百分比。

保险基金

除了协议代币之外，治理还可以创建一个保险基金。该基金拥有大量不相关的资产，并且可以支持债务拍卖。

盈余拍卖

盈余拍卖会出售系统中应计的协议代币产生的稳定费，协议代币之后会被销毁。

盈余拍卖参数

参数名称	描述
出价涨幅（bidIncrease）	下一个出价的最小增加量
出价持续时间（bidDuration）	提交新出价后拍卖持续多长时间（秒）
拍卖总时长（totalAuctionLength）	拍卖的总时长（秒）
开始的拍卖（auctionsStarted）	截至目前已经开始的拍卖数量

盈余拍卖机制

剩余拍卖有一个阶段：

增加出价（increaseBidSize）（uint 编号（id），uint 购买数量（amountToBuy），uint 出价（bid））：任何人都可以为相同数量的指数（盈余）出价更高数量的协议代币。每个新的出

价都必须大于或等于 上次出价（lastBid） * 出价涨幅（bidIncrease）/100。拍卖将在最高拍卖总时长（totalAuctionLength）或自最近出价以来的出价持续时间（bidDuration）过去之后结束，并且在此期间没有新的出价。

如果没有出价，拍卖将重新开始。但是，如果拍卖有至少一个出价，则系统将把盈余提供给最高出价者，然后将销毁收集的所有协议代币。

盈余指数管理

每次用户创建指数并隐含地产生债务时，系统都会开始将借入利率应用于用户的SAFE。应计利息汇总在两个不同的智能合约中：

- 用于触发债务拍卖（第9.2节）和盈余拍卖（第10.1节）的会计引擎
- 用于为核心基础设施组件提供资金并激励外部参与者维护系统的盈余金库

盈余金库负责资助三个核心系统组成部分：

- Oracle模块（第6节）。根据oracle的结构，金库要么支付治理白名单中的链下oracle，要么支付对oracle的调用。金库还可以同来支付花费大量时间调用oracle并对其进行更新的地址
- 在某些情况下，需要独立的团队来维护系统。例如，将新抵押品类型列入白名单或对系统的汇率设定进行微调的团队（第4.2节）

可以设置金库，以便将来一些盈余接收者将被自动拒绝资助，而其他接收者可以代替他们。

外部参与者

该系统依赖外部参与者才能正常运行。这些参与者得到经济激励，可以在如拍卖、全球结算处理、做市和更新喂价等领域参与，以维护系统的健康。

我们将提供初始用户界面和自动化脚本，以使尽可能多的人能够确保协议安全。

潜在市场

我们认为RAI在两个主要方面用处很大：

- **投资组合多元化**：投资者使用RAI可以减低对ETH等资产的敞口，而没有实际持有以太坊的全部风险
- **合成资产抵押品**：RAI可以为UMA，MakerDAO和Synthetix等协议提供更低的加密货币市场敞口，并为用户提供更多时间退出其头寸，例如2020年3月黑色星期四的情况，当时价值数百万美元的加密资产已被清算

未来研究

为了突破去中心化货币的界限并进一步推动去中心化金融的创新，我们将继续在核心领域寻求替代方案，例如最小化治理和清算机制。

我们首先要为协议未来的标准奠定基础，以使协议自我锁定不受外部控制，并为能适应市场力量的真正“货币机器人”奠定基础。之后，我们邀请以太坊社区围绕我们的提案进行辩论和设计改进，尤其侧重于抵押品和债务拍卖。

风险与风险缓解

开发及发行反射指数以及在此之上构建的后续系统涉及多重风险：

- **智能合约错误**：给系统带来的最大风险是可能使任何人都可以提取所有抵押品或将协议锁定在无法恢复的状态的错误。我们计划让我们的代码由多位安全研究人员审查，并在我们将其部署到生产中之前在测试网上启动该系统。
- **Oracle失败**：我们将汇总来自多个oracle网络的喂价，并且将制定严格的规则，一次只能升级一个oracle，以便恶意治理无法轻易引入虚假价格。
- **抵押品黑天鹅事件**：基础抵押品中有发生黑色天鹅事件的风险，这可能导致大量SAFE被清算。清算可能无法覆盖全部未偿还的坏帐，因此系统将不断更改其盈余缓冲以覆盖相当数量的已发行债务并承受市场冲击。
- **不正确的利率设置器参数**：自主反馈机制是高度实验性的，其行为可能与我们在模拟过程中所预测的完全不同。我们计划允许治理微调此组件（同时仍受限制），以避免出现意外情况。
- **无法引导健康的清算人市场**：清算人是确保所有已发行债务均由抵押物覆盖的重要参与者。我们计划创建界面和自动化脚本，以使尽可能多的人可以参与以确保系统安全。

总结

我们提出了一种协议，该协议逐渐将自身锁定并不受人为控制，并发行低波动性的抵押资产——反射指数。我们首先介绍了旨在影响指数市场价格的自治机制，然后介绍了几种智能合约如何限制代币持有者对该系统的控制权。我们概述了一种自我维持计划，用于对来自多个独立的Oracle网络的喂价进行中值处理，最后介绍了铸指数和清算SAFE的一般机制。

参考文献

[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

词汇表

反射指数：一种抵押资产，可减轻其基础资产的波动性

RAI：我们的第一个反射指数

赎回价格：系统希望指数拥有的价格。如果市场价格与赎回价格不接近，则它会在赎回率（由RRFM计算）影响下发生变化。赎回结果的意图是影响SAFE创建者产生更多或偿还部分债务。

借款利率：适用于所有有未偿债务的SAFE的年利率

赎回率反馈机制（RRFM）：一种自治机制，用于比较反射指数的市场价格和赎回价格，然后计算赎回率，该赎回率会缓慢影响SAFE创建者产生更多或更少的债务（并间接尝试最小化市场/赎回价格偏差）

货币市场设定工具（MMS）：一种类似于RRFM的机制，可以同时拉动多个货币杠杆。就反射指数而言，它同时修改了借入利率和赎回价格

Oracle网络中值器（ONM）：一种智能合约，可从多个oracle网络（不受治理控制）中提取价格，并在大多数（例如5个中的3个）返回结果而不出现错误时，对它们取中值

受限治理模块（RGM）：一组智能合约，这些合约约束了治理代币持有者对系统的控制权。它要么强制实施时间延迟，要么限制治理设置某些参数的可能性

治理冰期：一份在经过一定期限后，将协议的大多数组件锁定，不受外部干预的合同

会计引擎：触发债务和盈余拍卖的系统组件。它还跟踪当前拍卖的债务，未采取行动的坏账和盈余缓冲的数量

盈余缓冲：应计并保留在系统中的利息。超过此阈值的任何应计利息将在销毁协议代币的盈余拍卖中出售

盈余金库：允许不同系统模块提取应计利息的合同（例如，ONM用于调用oracle）