Rai: Низковолатильное с Минимизированным Доверием Обеспечение экосистемы DeFi

Стефан Ч. Ионеску, Амин Сулеймани

Май 2020 г.

Абстракция. Мы представляем децентрализованный протокол с минимизированным управлением, который автоматически реагирует на состояние рынка, чтобы изменить целевую стоимость своего собственного обеспеченного актива. Протокол позволяет любому использовать свои криптоактивы и выпустить “рефлексный индекс” (“reflex index”), который является ослабленной версией, лежащего в основе его обеспечения. Мы описываем, как индексы могут быть полезны в качестве универсального обеспечения с низкой волатильностью, которое может защитить их держателей, а также другие протоколы децентрализованного финансирования от внезапных рыночных сдвигов. Мы представляем наши планы, чтобы помочь другим командам запустить свои собственные синтетические продукты, используя нашу инфраструктуру. Наконец, мы предлагаем альтернативы существующим структурам оракулов и управления, которые часто встречаются во многих протоколах DeFi.

СОДЕРЖАНИЕ

1. Введение

Деньги - один из самых мощных механизмов координации, которые человечество использует для своего процветания. Привилегия управления денежной массой исторически находилась в руках суверенного руководства и финансовой элиты, но навязывалась невольной широкой публике. Там, где Биткоин продемонстрировал потенциал массового протеста, чтобы продемонстрировать товарный актив, обеспечивающий сбережение, Ethereum дает нам платформу для создания синтетических инструментов, обеспеченных активами, которые можно защитить от волатильности и использовать в качестве обеспечения или привязать к справочной цене и используется в качестве средства обмена для ежедневных транзакций, выполняемых в соответствии с теми же принципами децентрализованного консенсуса.

Беспрепятственный доступ к Биткоину для хранения богатства и должным образом децентрализованным синтетическим инструментам на Ethereum заложит основу для предстоящей финансовой революции, предоставив тем, кто находится на периферии современной финансовой системы, средства для координации создания новой.

В этой статье мы представляем основу для построения рефлексных индексов, нового типа активов, который поможет процветанию других синтетических продуктов и станет ключевым строительным блоком для всей децентрализованной финансовой индустрии.

2. Обзор Рефлексных Индексов

Целью рефлексного индекса является не поддержание определенной привязки, а снижение волатильности его залога. Индексы позволяют любому получить доступ к рынку криптовалюты без того же масштаба риска, что и владение реальными криптоактивами. Мы считаем, что RAI, наш первый рефлексный индекс, будет незамедлительно полезен для других команд, выпускающих синтетические материалы на Ethereum (например, Multi-Collateral DAI [1], UMA [2], Synthetix [3] MakerDAO), потому что это дает их системам меньшую подверженность изменчивым активам, таким как ETH, и дает пользователям больше времени для выхода из своих позиций в случае значительного изменения рынка.

Чтобы понять индексы рефлексов, мы можем сравнить поведение их цены погашения с поведением цены стейблкоина.

Цена выкупа - это стоимость одной единицы долга (или монеты) в системе. Цена выкупа предназначена для использования только в качестве инструмента внутреннего учета и отличается от рыночной цены (стоимости, по которой рынок торгует монетой). В случае стейблкоинов, обеспеченных фиатом, таких как USDC, системные операторы заявляют, что любой может обменять одну монету на один доллар США, и, таким образом, цена выкупа для этих монет всегда равна единице. Есть также случаи стейблкоинов, обеспеченных криптовалютой, таких как Multi Collateral DAI (MCD) MakerDAO, где система нацелена на фиксированную привязку в один доллар США и, таким образом, цена выкупа также фиксируется на уровне единицы.

В большинстве случаев будет разница между рыночной ценой стейблкоина и ценой его выкупа. Эти сценарии создают возможности для арбитража, когда трейдеры будут создавать больше монет, если рыночная цена выше, чем выкуп, и выкупать свои стейблкоины в качестве обеспечения (например, долларов США в случае USDC) в случае, если рыночная цена ниже, чем цена выкупа.

Рефлексные индексы похожи на стейблкоины, потому что у них также есть цена погашения, на которую ориентируется система. Основное отличие в их случае заключается в том, что их погашение не останется фиксированным, а будет изменяться под влиянием рыночных сил. В разделе 4 мы объясняем, как цена погашения индекса колеблется и создает новые возможности арбитража для его пользователей.

3. Философия Дизайна и Стратегия Выхода на Рынок

Наша философия дизайна заключается в том, чтобы уделять приоритетное внимание безопасности, стабильности и скорости доставки.

Мультизалоговый актив DAI (Multi-Collateral DAI) был естественным местом, чтобы начать итерацию дизайна RAI. Система прошла тщательный аудит и формальную проверку, она имеет минимальные внешние зависимости и собрала активное сообщество экспертов. Чтобы свести к минимуму усилия по разработке и взаимодействию, мы хотим внести только самые простые изменения в исходную кодовую базу MCD для достижения нашей реализации.

Наши самые важные модификации включают добавление автономного установщика ставок, Оракул Сетевого Посредничества, который интегрирован со многими независимыми ценовыми потоками, и уровня минимизации управления, предназначенного для максимальной изоляции системы от вмешательства человека.

Самая первая версия протокола (этап 1) будет включать только установщик тарифов и другие незначительные улучшения в архитектуре ядра. Как только мы докажем, что установщик работает должным образом, мы можем более безопасно добавить Посреднический Оракул (этап 2) и уровень минимизации управления (этап 3).

4. Механизмы Денежно-Кредитной Политики

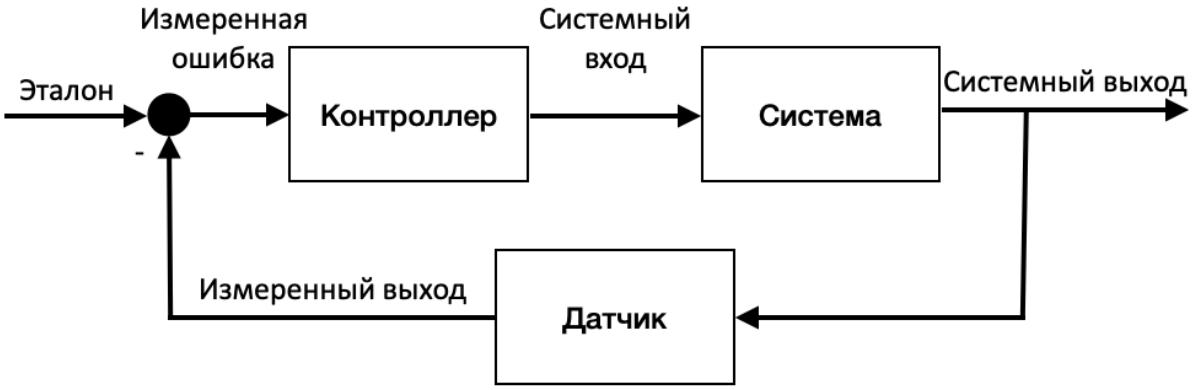
4.1. Введение в Теорию Управления

Одна из распространенных систем управления, с которой знакомо большинство людей, - это душ. Когда кто-то начинает душ, он имеет в виду желаемую температуру воды, которая, согласно теории управления, называется контрольной точкой. Человек, действующий как контроллер, непрерывно измеряет температуру потока воды (которая называется выходом системы) и изменяет скорость, с которой он поворачивает ручку душа, в зависимости от отклонения (или ошибки) между желаемой и текущей температурой. Скорость поворота ручки называется системным входом. Задача состоит в том, чтобы повернуть ручку достаточно быстро, чтобы быстро достичь контрольной установки, но не так быстро, чтобы температура не выскочила за пределы. Если происходят удары системы, при которых температура потока воды внезапно изменяется, человек должен иметь возможность поддерживать текущую температуру, зная, как быстро вращать ручку в ответ на дисбаланс.

Научная дисциплина поддержания устойчивости динамических систем называется теорией управления, и она нашла широкое применение в круиз-контроле для автомобилей, авиационной навигации, химических реакторах, роботизированном оружии и промышленных процессах всех видов. Алгоритм регулировки сложности биткоинов, который поддерживает 10-минутное среднее время блока, несмотря на переменный хешрейт, является примером критически важной системы управления.

В большинстве современных систем управления алгоритмический контроллер обычно встроен в процесс, и ему предоставляется контроль над входом системы (например, педалью газа автомобиля), чтобы автоматически обновлять его на основе

отклонений между выходными данными системы (например, скоростью автомобиля) и заданным значением (например, скорость круиз-контроля).



Наиболее распространенным типом алгоритмического контроллера является *PID контроллер*. Более 95% промышленных приложений и широкий спектр биологических систем используют элементы *PID контроллера* [4]. *PID контроллер* использует математическую формулу, состоящую из трех частей, для определения своего вывода:

Вывод Контроллера = Пропорциональная + Интегральная + Производная

Пропорциональная часть - это часть регулятора, которая прямо пропорциональна отклонению. Если отклонение большое и положительное (например, заданная скорость круиз-контроля намного выше, чем текущая скорость автомобиля), пропорциональный отклик будет большим и положительным (например, нажмите на педаль газа).

Интегральная часть - это часть контроллера, которая учитывает, как долго сохраняется отклонение. Интегральная часть определяется как интеграл отклонения с течением времени и в основном используется для устранения ошибки установившегося состояния. Интегральная часть накапливается, чтобы реагировать на небольшие, хотя и постоянные отклонения от заданного значения (например, заданное значение круиз-контроля было на 1 милю в час выше скорости автомобиля в течение нескольких минут).

Производная часть - это часть контроллера, которая учитывает, насколько быстро отклонение растет или уменьшается. Производная часть определяется путем взятия производной отклонения и служит для ускорения реакции контроллера при

возрастании отклонения (например, ускорение, если заданное значение круиз-контроля выше скорости автомобиля, и автомобиль начинает замедляться). Это также помогает уменьшить перерегулирование за счет замедления реакции контроллера при уменьшении отклонения (например, ослабьте газ, когда скорость автомобиля начинает приближаться к заданному значению круиз-контроля).

Комбинация этих трех частей, каждая из которых может быть настроена независимо, дает *PID контроллерам* большую гибкость при управлении широким спектром приложений систем управления.

PID контроллеры лучше всего работают в системах, которые допускают некоторую задержку во времени отклика, а также возможность перерегулирования и колебаний вокруг заданного значения, когда система пытается стабилизироваться. Системы рефлексного индекса, такие как RAI, хорошо подходят для этого типа сценария, когда цены их выкупа могут быть изменены контроллерами PID.

В более общем плане, недавно было обнаружено, что многие из текущих правил денежно-кредитной политики центрального банка (например, правило Тейлора) на самом деле являются приближенными к *PID контроллерам* [5].

4.2. Механизм обратной связи по процентной ставке погашения

Механизм обратной связи по коэффициенту погашения - это системный компонент, отвечающий за изменение цены погашения рефлексного индекса. Чтобы понять, как это работает, нам сначала нужно описать, почему системе нужен механизм обратной связи, а не использование ручного управления, и каковы результаты этого механизма.

4.2.1.Компоненты механизма обратной связи

Теоретически можно было бы напрямую манипулировать ценой погашения рефлексного индекса (описанной в разделе 2), чтобы повлиять на пользователей индекса и, в конечном итоге, изменить рыночную цену индекса. На практике этот метод не окажет желаемого эффекта на участников системы. С точки зрения держателя SAFE, если цена погашения повышается только один раз, он может согласиться на более высокую цену за единицу долга, поглотить убыток от снижения коэффициента обеспечения и сохранить свою позицию. Однако, если держатели ожидают, что цена выкупа будет продолжать расти с течением времени, то, вероятно,

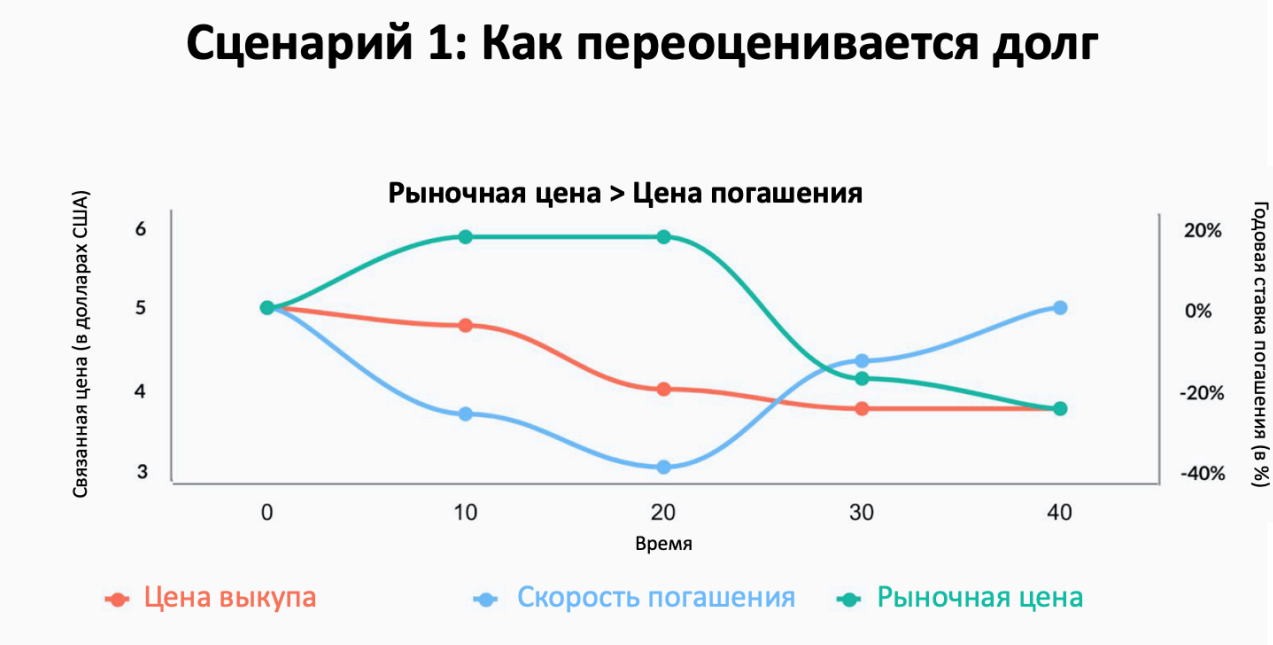
держатели будут более склонны избегать ожидаемых будущих убытков и, таким образом, предпочтут выплатить свой долг и закрыть свои позиции.

Мы ожидаем, что участники системы рефлексного индекса не будут напрямую реагировать на изменения цены выкупа, а вместо этого будут реагировать на скорость изменения цены выкупа, которую мы называем ставкой погашения. Ставка погашения устанавливается механизмом обратной связи, который руководство может настроить или полностью автоматизировать.

4.2.2.Сценарии механизма обратной связи

Напомним, что механизм обратной связи направлен на поддержание равновесия между ценой погашения и рыночной ценой путем использования ставки погашения для противодействия сдвигам в рыночных силах. Для этого коэффициент погашения рассчитывается таким образом, чтобы компенсировать отклонение между рыночной ценой и ценой погашения.

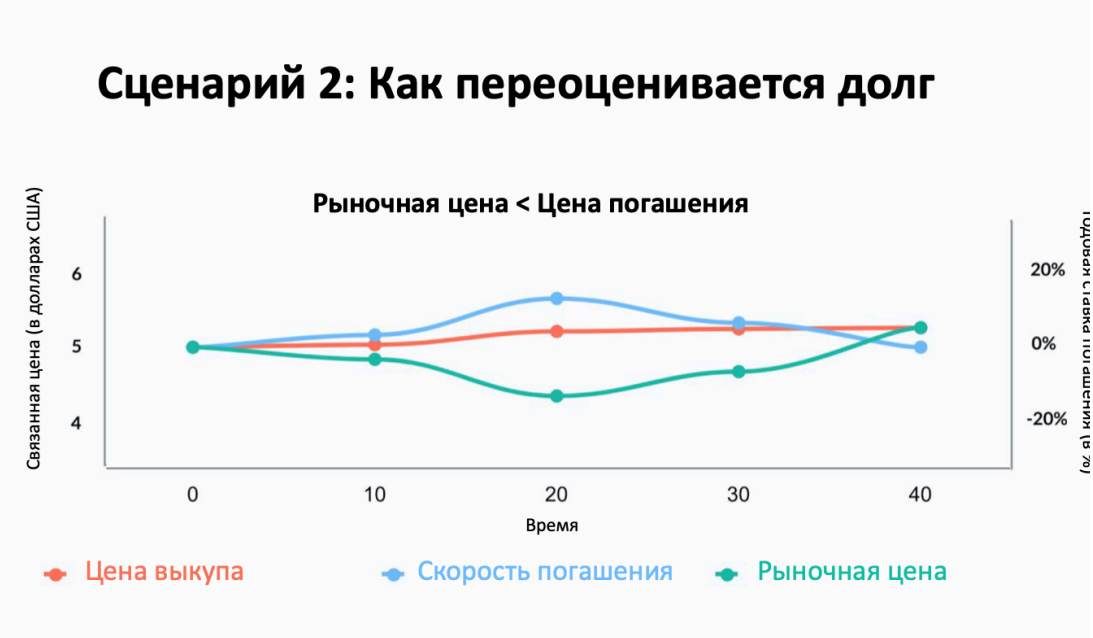
В первом сценарии ниже, если рыночная цена индекса выше, чем цена его погашения, механизм рассчитает отрицательную ставку, которая начнет снижать цену погашения, тем самым удешевляя долг системы.



Ожидание снижения цены погашения, вероятно, оттолкнет людей от держания индексов и побудит держателей SAFE генерировать больше долгов (даже если цена

залога не меняется), которые затем продаются на рынке, таким образом уравновешивая спрос и предложение. Обратите внимание, что это идеальный сценарий, когда держатели индекса быстро реагируют на механизм обратной связи. На практике (и особенно в первые дни после запуска) мы ожидаем отставания между запуском механизма и фактическими результатами, видимыми в размере выпущенного долга и, следовательно, в рыночной цене.

С другой стороны, во втором сценарии, если рыночная цена индекса ниже, чем цена погашения, ставка становится положительной и начинает переоценку всего долга, так что он становится дороже.



По мере удорожания долга коэффициенты обеспечения всех SAFE снижаются (таким образом, создатели SAFE получают стимул выплатить свои долги), и пользователи начинают накапливать индексы, ожидая, что их стоимость возрастет.

4.2.3.Алгоритм механизма обратной связи

В следующем сценарии мы предполагаем, что протокол использует пропорционально-интегральный контроллер для расчета коэффициента погашения:

- Рефлексный индекс запускается с произвольной ценой погашения «rand».

- В какой-то момент рыночная цена индекса повышается с «rand» до «rand» + x. После того, как механизм обратной связи считывает новую рыночную цену, он вычисляет пропорциональный член p, который равен:

  -1 * ((«rand» + x) / «rand»)

  Пропорциональная величина отрицательна, чтобы уменьшить цену выкупа и, в свою очередь, переоценить индексы, чтобы они стали дешевле.

- После вычисления пропорционального механизма механизм определит интегральный член i, добавив все прошлые отклонения от последнего отклонения Интервал секунд

- Механизм суммирует пропорциональную величину и интеграл и вычисляет посекундную ставку погашения r, которая постепенно начинает уменьшать цену погашения. Поскольку создатели SAFE понимают, что они могут генерировать больше долгов, они наводнят рынок большим количеством индексов.

- Через n секунд механизм обнаруживает, что отклонение между рыночной ценой и ценой погашения незначительно (при заданном параметре шума). На этом этапе алгоритм устанавливает r равным нулю и сохраняет цену выкупа на прежнем уровне.

На практике алгоритм будет более надежным, и мы либо сделаем некоторые переменные неизменяемыми (например, параметр шума, deviationInterval), либо введем строгие ограничения на то, что будет состояние может измениться.

4.2.4.Настройка механизма обратной связи

Чрезвычайно важным для правильного функционирования системы Рефлексного индекса является настройка параметров алгоритмического контроллера. Неправильная параметризация может привести к тому, что система будет работать слишком медленно, чтобы достичь стабильности, резко отклониться от нормы или вообще стать нестабильной перед лицом внешних потрясений.

Процесс настройки PID контроллера обычно включает в себя запуск системы в реальном времени, настройку параметров и наблюдение за реакцией системы, часто

целенаправленно создавая удары по пути. Учитывая сложность и финансовый риск настройки параметров системы Рефлексного индекса в реальном времени, мы планируем максимально использовать компьютерное моделирование и симуляцию для установки начальных параметров, что также позволит руководству обновлять параметры настройки, если дополнительные данные из производственной версии показывают, что они не оптимальны.

4.3. Сеттер Денежного Рынка

В RAI мы планируем сохранить фиксированную или ограниченную ставку заимствования (процентную ставку, применяемую при создании индексов) и изменять только цену погашения, тем самым минимизируя сложность моделирования механизма обратной связи. Ставка заимствования в нашем случае равна распределению между комиссией за стабильность и DSR в мультизалоговом DAI.

Несмотря на то, что мы планируем сохранить фиксированную ставку по займам, ее можно изменить вместе с ценой погашения с помощью установщика денежного рынка. Денежный рынок изменяет ставку заимствования и цену погашения таким образом, чтобы побудить создателей SAFE генерировать больший или меньший долг. Если рыночная цена индекса выше погашения, обе ставки начнут снижаться, тогда как если она ниже погашения, ставки увеличатся.

4.4. Глобальное Урегулирование

Глобальный расчет - это метод последней инстанции, используемый для гарантии цены выкупа всем держателям Рефлексных индексов. Он предназначен для того, чтобы как держатели Рефлексных индексов, так и создатели SAFE могли выкупить системное обеспечение по его чистой стоимости (количество индексов для каждого типа залога в соответствии с последней ценой погашения). Любой может инициировать расчет после сжигания определенного количества токенов протокола.

Расчет состоит из трех основных этапов:

- **Триггер:** инициируется расчет, пользователи больше не могут создавать SAFE, все потоки цены обеспечения и цены погашения замораживаются и регистрируются.

- **Процесс:** обработка всех невыполненных аукционов.

- **Заявление:** каждый держатель Рефлексного индекса и создатель SAFE может потребовать фиксированную сумму любого системного обеспечения на основе последней зарегистрированной цены погашения индекса.

5. Управление

Подавляющее большинство параметров будут неизменными, а внутренняя механика смарт-контрактов не будет обновляться, если держатели токенов управления не развернут совершенно новую систему. Мы выбрали эту стратегию, потому что мы можем исключить мета-игру, в которой люди пытаются влиять на процесс управления для собственной выгоды, тем самым подрывая доверие к системе. Мы устанавливаем надлежащую работу протокола, не слишком доверяя людям («эффект биткоина»), чтобы максимально повысить социальную масштабируемость и минимизировать риски для других разработчиков, которые захотят использовать RAI в качестве базовой инфраструктуры в своих собственных проектах.

Для нескольких параметров, которые можно изменить, мы предлагаем добавить модуль ограниченного управления, предназначенный для задержки или ограничения всех возможных модификаций системы. Кроме того, мы представляем Заморозку Управления, реестр разрешений, который может заблокировать некоторые части системы от внешнего контроля по прошествии определенных сроков.

5.1. Ограниченное по Времени Управление

Ограниченное по времени управление - это первый компонент модуля ограниченного управления. Это накладывает временные задержки между изменениями, применяемыми к одному и тому же параметру. Примером является возможность изменить адреса оракулов, используемых в Оракуле Сетевого Посредничества (раздел 7.2), по прошествии не менее T секунд с момента последней модификации оракула.

5.2. Ограниченное по Действию Управление

Второй компонент модуля ограниченного управления - это управление, ограниченное действиями. Каждый регулируемый параметр имеет ограничения на то, какие значения он может быть установлен и насколько они могут изменяться за

определенный период времени. Яркими примерами являются начальные версии Механизма обратной связи по коэффициенту погашения (раздел 4.2), которые держатели управляющих токенов смогут настраивать.

5.3. Заморозка Управления

Заморозка - это неизменный смарт-контракт, который устанавливает сроки для изменения определенных параметров системы и обновления протокола. Его можно использовать в том случае, если руководство хочет убедиться, что оно может исправить ошибки, прежде чем протокол заблокируется и откажется от вмешательства извне. Заморозка проверит, разрешено ли изменение, проверив имя параметра и адрес затронутого контракта в реестре сроков. Если срок истек, вызов вернется.

Руководство может отсрочить Заморозку фиксированное количество раз, если ошибки будут обнаружены ближе к дате, когда протокол должен начать блокировать себя. Например, «Заморозку» можно отложить только три раза, каждый раз на один месяц, чтобы новые исправления ошибок были протестированы должным образом.

5.4. Основные Области, в Которых Необходимо Управление

Мы предполагаем четыре области, в которых может потребоваться управление, особенно в ранних версиях этой структуры:

- **Добавление новых типов обеспечения:** RAI будет поддерживаться только ETH, но другие индексы будут поддерживаться несколькими типами обеспечения, и управление будет иметь возможность диверсифицировать риск с течением времени

- **Изменение внешних зависимостей:** оракулы и DEX, от которых зависит система, могут быть обновлены. Управление может указать системе на новые зависимости, чтобы она продолжала нормально функционировать.

- **Установщики ставок тонкой настройки:** ранние контроллеры денежно-кредитной политики будут иметь параметры, которые можно изменять в разумных пределах (как описано в Ограниченное по Времени Управление и в Ограниченное по Действию Управление).

- **Миграция между версиями системы:** в некоторых случаях руководство может развернуть новую систему, дать ей разрешение на печать токенов протокола и отозвать это разрешение у старой системы. Эта миграция выполняется с помощью модуля Ограниченный Модуль Миграции, описанного ниже

5.4.1.Ограниченный Модуль Миграции

Ниже приводится простой механизм миграции между версиями системы:

- Существует миграционный реестр, который отслеживает, сколько разных систем покрывает один и тот же токен протокола, и каким системам может быть отказано в разрешении на печать токенов протокола на долговом аукционе.

- Каждый раз, когда руководство развертывает новую версию системы, оно вносит адрес договора о долговом аукционе системы в миграционный регистр. Руководству также необходимо указать, смогут ли они когда-либо остановить печать токенов протокола в системе. Кроме того, руководство может в любое время сказать, что одна система всегда сможет печатать токены и, следовательно, она никогда не будет перенесена из

- Между предложением новой системы и снятием разрешений у старой проходит период восстановления.

- Дополнительный контракт может быть настроен таким образом, чтобы он автоматически отключал старую систему после отказа в разрешении на печать.

Модуль миграции может быть объединен с Заморозкой, которая автоматически дает определенным системам разрешение всегда иметь возможность печатать токены.

6. Автоматическое отключение системы

Есть случаи, когда система может автоматически обнаруживать и, как результат, инициировать расчет самостоятельно, без необходимости сжигать токены протокола:

- **Серьезные задержки подачи цен:** система обнаруживает, что один или несколько источников обеспечения или индексных цен не обновлялись в течение длительного времени.

- **Миграция системы:** это дополнительный контракт, который может закрыть протокол после того, как пройдет период восстановления с момента, когда руководство отменяет возможность механизма долгового аукциона печатать токены протокола (Ограниченный Модуль Миграции, раздел 5.4.1)

- **Постоянное отклонение рыночной цены:** система обнаруживает, что рыночная цена индекса в течение длительного времени отклонялась на x% по сравнению с ценой погашения.

Руководство сможет модернизировать эти автономные модули отключения, пока они все еще ограничены или пока Ледниковый период не начнет блокировать некоторые части системы.

7. Оракулы

Система должна считывать данные о ценах на три основных типа активов: индекс, токен протокола и все типы обеспечения из белого списка. Ценовые каналы могут быть предоставлены оракулами под управлением руководства или уже созданными сетями оракулов.

7.1. Управление под Руководством Оракулов

Держатели токенов управления или основная группа, запустившая протокол, могут сотрудничать с другими организациями, которые собирают несколько ценовых потоков вне сети, а затем отправляют одну транзакцию в смарт-контракт, который объединяет все точки данных.

Такой подход обеспечивает большую гибкость при обновлении и изменении инфраструктуры Оракулов, хотя это происходит за счет отсутствия доверия.

7.2. Оракул Сетевого Посредничества

Оракул Сетевого Посредничества (ONM) - это смарт-контракт, который считывает цены из нескольких источников, которые напрямую не контролируются органами

управления (например, пул Uniswap V2 между типом обеспечения индекса и другими стейблкоинами), а затем усредняет все результаты. ONM работает следующим образом:

- В нашем контракте отслеживаются сети оракулов из белого списка, по которым он может позвонить, чтобы запросить дополнительные цены. Контракт финансируется за счет части излишков, накопленных системой (с использованием излишков казначейства, раздел 11). Каждая сеть Оракулов принимает в качестве оплаты определенные токены, поэтому наш контракт также отслеживает минимальную сумму и тип токенов, необходимых для каждого запроса.

- Для того, чтобы отправить новый ценовой поток в систему, все оракулы должны быть вызваны заранее. При вызове оракула контракт сначала обменивает некоторую плату за стабильность с одним из принятых токенов оракула. После вызова оракула контракт помечает вызов как «действительный» или «недействительный». Если вызов недействителен, конкретный неисправный оракул не может быть вызван снова, пока не будут вызваны все остальные и контракт не проверит, есть ли действительное большинство. Действительный вызов оракула не должен возвращаться, и он должен получить цену, которая была размещена в цепочке где-то за последние m секунд. «Получить» означает разные вещи в зависимости от каждого типа оракула:

    - Для оракулов на основе pull, из которых мы можем получить результат сразу, наш контракт должен платить комиссию и напрямую получать цену

    - Для оракулов на основе push наш контракт оплачивает комиссию, вызывает оракул и должен подождать определенный период времени n, прежде чем снова вызвать оракула, чтобы получить запрошенную цену.

- Каждый результат оракула сохраняется в массиве. После вызова каждого оракула из белого списка и если в массиве достаточно действительных точек данных для формирования большинства (например, контракт получил действительные данные от 3/5 оракулов), результаты сортируются, и контракт выбирает среднее значение.

- Независимо от того, набирает ли контракт большинство или нет, массив с результатами оракула очищается, и контракту нужно будет подождать p секунд, прежде чем заново запустить весь процесс.

7.2.1.Резервирвирование Сетевого Оракула

Управление может добавить резервную опцию оракула, которая начинает подталкивать цены в системе, если посредник не может найти большинство действительных сетей оракула несколько раз подряд.

Параметр резервного копирования должен быть установлен при развертывании посредника, поскольку его нельзя будет изменить впоследствии. Кроме того, отдельный контракт может отслеживать, если резервная копия слишком долго заменяет механизм подсчета среднего значения, и автоматически отключать протокол.

8. SAFE

Для создания индексов любой может внести свой криптовалютный залог и использовать его внутри SAFE. Пока SAFE открыт, он будет продолжать накапливать задолженность в соответствии со ставкой заимствования депонированного обеспечения. По мере того как создатель SAFE выплатит свой долг, он сможет снимать все больше и больше своего заблокированного обеспечения.

8.1. Жизненный Цикл SAFE

Для создания индексов рефлексов и последующего погашения долга SAFE необходимо выполнить четыре основных шага:

- Внесите обеспечение в SAFE. Сначала пользователю необходимо создать новый SAFE и внести в него обеспечение.

- Создание индексов, подкрепленных залогом SAFE. Пользователь указывает, сколько индексов он хочет генерировать. Система создает равную сумму долга, которая начинает накапливаться в соответствии со ставкой заимствования залога.

- Выплатить SAFE долг. Когда создатель SAFE хочет отозвать свое обеспечение, он должен выплатить свой первоначальный долг плюс начисленные проценты.

- Снять залог.

После того, как пользователь выплатит часть или весь свой долг, ему разрешено снять свое обеспечение.

9. Ликвидация SAFE

Чтобы сохранить платежеспособность системы и покрыть стоимость всей непогашенной задолженности, каждый SAFE может быть ликвидирован в случае, если его коэффициент обеспечения упадет ниже определенного порога. Любой может инициировать ликвидацию, и в этом случае система конфискует залог SAFE и продаст его на аукционе залога.

9.1. Залоговый Аукцион

9.1.1. Ликвидационное страхование

В одной из версий системы создатели SAFE могут иметь возможность выбрать триггер, когда их SAFE будут ликвидированы. Триггеры - это смарт-контракты, которые автоматически добавляют дополнительное обеспечение в SAFE и потенциально спасают его от ликвидации. Примерами триггеров являются контракты на продажу коротких позиций или контракты, которые взаимодействуют с протоколами страхования, такими как Nexus Mutual [6].

Еще один метод защиты SAFE - это добавление двух разных пороговых значений обеспечения: безопасного и рискованного. Пользователи SAFE могут генерировать долги до тех пор, пока не достигнут безопасного порога (который выше, чем риск), и они будут ликвидированы только тогда, когда обеспечение SAFE опустится ниже порога риска.

Чтобы запустить аукцион обеспечения, система должна использовать переменную, называемую ликвидацией, чтобы определить сумму долга, которая должна быть покрыта на каждом аукционе, и соответствующую сумму обеспечения, которое будет

продано. Ликвидационный штраф будет применяться ко всем выставленным на аукционе SAFE.

9.1.2.Параметры залогового аукциона

Наименование Параметра	Описание
minimumBid	Минимальное количество монет, которое должно быть предложено за одну ставку
discount	Скидка при продаже обеспечения
lowerCollateralMedianDeviation	Максимальное отклонение нижней границы, которое может иметь медиана обеспечения по сравнению с ценой оракула
upperCollateralMedianDeviation	Максимальное отклонение верхней границы, которое может иметь медиана обеспечения по сравнению с ценой оракула
lowerSystemCoinMedianDeviation	Максимальное отклонение нижней границы, которое может иметь подача цены системной монеты оракула по сравнению с ценой оракула системной монеты
upperSystemCoinMedianDeviation	Максимальное отклонение верхней границы, которое может иметь медиана обеспечения по сравнению с ценой оракула системной монеты
minSystemCoinMedianDeviation	Минимальное отклонение для медианного результата системной монеты по сравнению с ценой погашения для учета медианы

9.1.3.Механизм залогового аукциона

Аукцион с фиксированной скидкой - это простой способ (по сравнению с английскими аукционами) выставить обеспечение на продажу в обмен на системные монеты, используемые для погашения безнадежных долгов. От участников торгов требуется только разрешить аукционному дому передать свой safeEngine.coinBalance, а затем вызвать buyCollateral, чтобы обменять свои системные монеты на обеспечение, которое продается со скидкой по сравнению с его последней зарегистрированной рыночной ценой.

Участники торгов могут также проверить сумму обеспечения, которую они могут получить вызвав getCollateralBought или getApproximateCollateralBought на конкретном аукционе. Обратите внимание, что getCollateralBought не помечен как представление, потому что этот параметр читает (а также обновляет) redemptionPrice

из ретранслятора оракула, тогда как getApproximateCollateralBought использует расширение.

9.2. Долговые аукционы

В сценарии, когда аукцион обеспечения не может покрыть всю безнадежную задолженность в SAFE и если в системе нет избыточных резервов, любой может инициировать аукцион по долговым обязательствам.

Долговые аукционы предназначены для создания большего количества токенов протокола (раздел 10) и продажи их для получения индексов, которые могут аннулировать оставшуюся безнадежную задолженность системы.

Для запуска долгового аукциона системе необходимо использовать два параметра:

- initialDebtAuctionAmount: начальное количество токенов протокола для источника после аукциона
- dutyAuctionBidSize: начальный размер ставки (сколько индексов должно быть предложено в обмен на токены протокола initialDebtAuctionAmount)

9.2.1. Настройка параметров автономного долгового аукциона

Первоначальное количество токенов протокола, отчеканенных на долговом аукционе, может быть либо установлено путем голосования руководства, либо оно может быть автоматически скорректировано системой. Автоматизированная версия должна быть интегрирована с оракулами (раздел 6), из которых система будет считывать токены протокола и рыночные цены рефлексных индексов. Затем система установит начальное количество токенов протокола (initialDebtAuctionAmount), которые будут отчеканены для индексов dutyAuctionBidSize. initialDebtAuctionAmount может быть установлен со скидкой по сравнению с фактической рыночной ценой PROTOCOL / INDEX, чтобы стимулировать торги.

9.2.2.Параметры долгового аукциона

Наименование Параметра	Описание
amountSoldIncrease	Увеличение количества токенов протокола, которые будут отчеканены для того же количества индексов
bidDecrease	Минимальное уменьшение следующей ставки допустимого количества токенов протокола для того же количества индексов
bidDuration	Как долго длится торги после подачи новой ставки (в секундах)
totalAuctionLength	Общая продолжительность аукциона (в секундах)
auctionsStarted	Сколько аукционов началось до сих пор

9.2.3.Механизм долгового аукциона

В отличие от залогового аукциона, долговые аукционы имеют только один этап:

reduceSoldAmount(uint id, uint amountToBuy, uint bid): уменьшить количество токенов протокола, принимаемых в обмен на фиксированное количество индексов.

Аукцион будет возобновлен, если на него не поступят заявки. При каждом перезапуске система будет предлагать больше токенов протокола для того же количества индексов. Сумма нового токена протокола рассчитывается как lastTokenAmount * amountSoldIncrease / 100. После завершения аукциона система отчеканит токены для участника, предложившего самую высокую цену.

10. Токены Протокола

Как описано в предыдущих разделах, каждый протокол должен быть защищен токеном, который создается на долговых аукционах. Помимо защиты, токен будет использоваться для управления несколькими компонентами системы. Кроме того, предложение токенов протокола будет постепенно сокращаться с использованием избыточных аукционов. Сумма излишка, которая должна накопиться в системе до того, как дополнительные средства будут выставлены на аукцион, называется излишним буфером и автоматически корректируется как процент от общей суммы выпущенного долга.

Страховой Фонд

Помимо токена протокола, руководство может создать страховой фонд, который содержит широкий спектр некоррелированных активов и может использоваться в качестве поддержки для долговых аукционов.

10.1.Аукционы Излишков

Аукционы излишков продают комиссию за стабильность, накопленную в системе, за токены протокола, которые затем сжигаются.

10.2.Параметры Аукциона Излишков

Наименование Параметра	Описание
bidIncrease	Минимальное увеличение следующей ставки
bidDuration	Как долго длится аукцион после подачи новой ставки (в секундах)
totalAuctionLength	Общая продолжительность аукциона (в секундах)
auctionsStarted	Сколько аукционов началось до сих пор

10.3.Механизм Аукциона Излишков

Аукционы излишков проходят в один этап:

IncreaseBidSize (uint id, uint amountToBuy, uint bid): любой может предложить большее количество токенов протокола за такое же количество индексов (излишек). Каждая новая ставка должна быть выше или равна lastBid * bidIncrease / 100. Аукцион завершится по истечении максимального totalAuctionLength секунд или после того, как с момента последней ставки пройдут секунды bidDuration, а новые ставки пока не поступали.

Аукцион возобновится, если на нем не будет ставок. С другой стороны, если на аукционе есть хотя бы одна ставка, система предложит излишек тому, кто сделал самую высокую ставку, а затем сожжет все собранные токены протокола.

11. Управление избыточными индексами

Каждый раз, когда пользователь генерирует индексы и неявно создает задолженность, система начинает применять ставку заимствования к SAFE пользователя. Начисленные проценты объединяются в два разных смарт-контракта:

- Механизм учета используемый для проведения аукционов по продаже долга (раздел 9.2) и излишков (раздел 10.1).

- Излишки казначейства, используемые для финансирования основных компонентов инфраструктуры и стимулирования внешних субъектов к поддержанию системы.

Избыточное казначейство отвечает за финансирование трех основных компонентов системы:

- Модуль Оракула (раздел 6). В зависимости от того, как устроен оракул, казначейство либо оплачивает управление оракулам из белого списка вне сети, либо оплачивает вызови в сети оракулов. Казначейство также может быть настроено для оплаты адресов, которые потратили бензин, на вызов оракула и его обновление.

- В некоторых случаях независимые команды, обслуживающие систему. Примерами являются команды, которые вносят новые типы залога в белый список или настраивают установщик ставок системы (раздел 4.2).

Казначейство может быть настроено таким образом, что некоторым получателям излишков будет автоматически отказано в финансировании в будущем, а другие могут занять их место.

12. Внешние субъекты

Для правильного функционирования система зависит от внешних субъектов. Эти субъекты экономически заинтересованы в участии в таких областях, как аукционы, обработка глобальных расчетов, создание рынков и обновление ценовых данных, чтобы поддерживать работоспособность системы.

Мы предоставим начальные пользовательские интерфейсы и автоматизированные сценарии, чтобы как можно больше людей могли обеспечить безопасность протокола.

13. Адресный рынок

Мы считаем, что RAI полезен в двух основных областях:

- **Диверсификация портфеля:** инвесторы используют RAI, чтобы снизить риск использования такого актива, как ETH, без полного риска фактического владения эфиром

- **Обеспечение для синтетических активов:** RAI может предложить такием протоколам, как UMA, MakerDAO и Synthetix, меньшую подверженность криптовалютному рынку и дать пользователям больше времени для выхода из своих позиций в случае таких сценариев, как Черный четверг с марта 2020 года, когда были ликвидированы криптоактивы на миллионы долларов.

14. Будущие исследования

Чтобы раздвинуть границы децентрализованных денег и внедрить дальнейшие инновации в децентрализованные финансы, мы продолжим искать альтернативы в основных областях, таких как минимизация управления и механизмы ликвидации.

Сначала мы хотим заложить основу для будущих стандартов для протоколов, которые блокируются от внешнего контроля, и для настоящих «денежных роботов», которые адаптируются в ответ на рыночные силы. После этого мы приглашаем сообщество Ethereum для обсуждения и разработки улучшений, касающихся наших предложений, с особым акцентом на аукционах по залоговому обеспечению и долговым обязательствам.

15. Риски и смягчение

Есть несколько рисков, связанных с разработкой и запуском Рефлексного индекса, а также последующих систем, построенных на его основе:

- **Ошибки смарт-контрактов:** наибольший риск для системы - это возможность ошибки, которая позволяет кому-либо извлечь все залоги или блокирует протокол в состоянии, из которого он не может восстановиться. Мы

планируем провести проверку нашего кода несколькими исследователями безопасности и запустить систему в тестовой сети, прежде чем мы приступим к ее развертыванию в производственной среде.

- **Ошибка Оракула:** мы будем агрегировать потоки из нескольких сетей Оракулов, кроме того, будут действовать строгие правила для обновления только одного Оракула за один раз, чтобы злонамеренное управление не могло легко ввести ложные цены.

- **Сопутствующие события «Черный Лебедь»:** существует риск события «черный лебедь» в базовом обеспечении, что может привести к большому количеству ликвидированных SAFE. Ликвидация может оказаться не в состоянии покрыть всю непогашенную безнадежную задолженность, и поэтому система будет постоянно менять буфер излишков, чтобы покрыть приличную сумму выпущенного долга и противостоять рыночным шокам.

- **Неправильные параметры установки скорости:** автономные механизмы обратной связи в значительной степени экспериментальные и могут вести себя не так, как мы прогнозируем во время моделирования. Мы планируем позволить руководству доработать этот компонент (пока он еще ограничен), чтобы избежать неожиданных сценариев.

- **Неспособность создать здоровый рынок ликвидаторов:** ликвидаторы являются жизненно важными участниками, которые обеспечивают покрытие всех выпущенных долговых обязательств. Мы планируем создать интерфейсы и автоматизированные сценарии, чтобы как можно больше людей могли участвовать в обеспечении безопасности системы.

16. Резюме

Мы предложили протокол, который постепенно блокирует себя от человеческого контроля и выдает низковолатильный обеспеченный актив, называемый Рефлексным индексом. Сначала мы представили автономный механизм, предназначенный для влияния на рыночную цену индекса, а затем описали, как несколько смарт-контрактов могут ограничивать власть держателей токенов над системой. Мы обрисовали самоподдерживающуюся схему для медиализации ценовых потоков от нескольких независимых сетей оракулов, а затем закончили, представив общий механизм создания индексов и ликвидации SAFE.

17. Ссылки

[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

18. Глоссарий

Рефлексный индекс: обеспеченный актив, который снижает волатильность его базового актива.

RAI: наш первый Рефлексный индекс

Цена погашения: цена, которую система хочет, чтобы индекс имел. Он изменяется под влиянием коэффициента погашения (рассчитанного RRFM) в случае, если рыночная цена не близка к нему. Предназначен для оказания влияния на создателей SAFE, чтобы они заработали больше или выплатили часть своего долга.

Ставка заимствования: годовая процентная ставка применяется ко всем SAFE, имеющим непогашенный долг.

Механизм обратной связи по коэффициенту погашения (RRFM): автономный механизм, который сравнивает рыночную цену и цену погашения индекса рефлекса, а затем вычисляет коэффициент погашения, который медленно влияет на создателей SAFE для создания большего или меньшего долга (и неявно пытается минимизировать рыночную цену / цену погашения. отклонение)

Установщик денежного рынка (MMS): механизм, похожий на RRFM, который задействует сразу несколько денежных рычагов. В случае индексов рефлекса он изменяет как ставку заимствования, так и цену погашения.

Оракул Сетевого Посредничества (ONM): смарт-контракт, который извлекает цены из нескольких сетей оракулов (которые не контролируются системой управления) и усредняет их, если большинство (например, 3 из 5) вернули результат, не выбрасывая

Модуль ограниченного управления (RGM): набор смарт-контрактов, которые ограничивают власть держателей токенов управления над системой. Он либо вводит временные задержки, либо ограничивает возможности управления по установке определенных параметров.

Заморозка Управления: неизменный контракт, который блокирует большинство компонентов протокола от внешнего вмешательства после истечения определенного срока.

Система учета: компонент системы, запускающий аукционы по продаже долга и излишка. Он также отслеживает сумму долга, выставленного на аукцион, безрезультатного безнадежного долга и избыточного буфера

Буфер излишков: сумма процентов, которые нужно накапливать и хранить в системе. Любые проценты, начисленные выше этого порога, продаются на аукционах излишков, на которых сжигаются токены протокола.

Избыточное казначейство: контракт, который дает разрешение различным модулям системы снимать накопленные проценты (например, ONM для вызовов оракула)