

Alternative RUBLE Whitepaper

Alternative RUBLE (также ARUB, ArubCoin, неформально: Цифровой Рубль) - стейблкоин Российского Рубля обеспеченный стейблкоином доллара - BUSD (Binance USD), независимыми пулами обеспечения ARUB-RUB, ARUB-USD и алгоритмом стабилизации курса с помощью внутреннего обмена.

Информация о разработчике

Совместное объединение DAO Fund AEON и DAO Alternative RUBLE.

Контакты для связи:

info@alternativeruble.com

Сайт:

<https://alternativeruble.com/>

Фаундер и руководитель проекта:

Mikhail Belyaev

<https://www.linkedin.com/in/mikhail-belyaev-2a17b1243/>

Техническое обеспечение (СТО):

Andrei Nedobylskii

<https://www.linkedin.com/in/%D0%B0%D0%BD%D0%B4%D1%80%D0%B5%D0%B9-%D0%BD%D0%B5%D0%B4%D0%BE%D0%B1%D1%8B%D0%BB%D1%8C%D1%81%D0%BA%D0%B8%D0%B9-920841b4/>

Социальные сети:

<https://twitter.com/arubcoin>

<https://www.linkedin.com/company/alternative-ruble/>

<https://t.me/alternativeruble>

<https://github.com/alternativeruble>

Технические ссылки

PancakeSwap v2 pair:

<https://pancakeswap.finance/swap?inputCurrency=0x05ac02298358bf4ab05b6a566bc6b14bcb4a2798&outputCurrency=0xe9e7cea3dedca5984780bafc599bd69add087d56>

Flatqube.io pair:

<https://app.flatqube.io/pairs/0:87814c61ebd8e5ca40b49455ed9f8ad0333cc38b6ba42d896493fe4923ad626e>

Summary

Alternative RUBLE - стейблкоин, обеспеченный хранимым в контракте BUSD.

Стабилизация курса обеспечивается с помощью использования внутренней системы обмена (Exchange) по по актуальному курсу RUB/BUSD с использованием среднего курса за 15 минут биржи Binance. Подробнее об обеспечении курса обмена смотрите в соответствующем разделе.

Дополнительная стабилизация курса обеспечивается независимыми пулами RUB/ARUB с обменом 1 к 1 (за исключением транзакционных комиссий), а также независимых пулов к другим стейблкоинам RUB/USDT, RUB/EURO и другим.

Алгоритм обмена стремится снижать использование collateral с каждым обменом:

- При обмене BUSD на ARUB, взимается комиссия (текущие комиссии смотрите на сайте), в последующем комиссия в ARUB полностью сжигается. Сжигание будет обеспечено пока collateral utilization превышает 50%
- При обмене ARUB на BUSD взимается дополнительная комиссия (текущие комиссии смотрите на сайте), которая переходит в пул обеспечения, снижая collateral utilization и повышая хранимое обеспечение. Дополнительная комиссия может быть увеличена и снижена в автоматическом режиме, при превышении collateral utilization выше 100%

Выкуп ARUB доступен в любой момент во внутреннем обменнике по курсу и комиссии, указанном на сайте.

Выкуп BUSD доступен в любой момент при условии наличия достаточного обеспечения по курсу и по комиссиям, которые указаны на сайте.

Обеспечение курса

Обеспечение курса ARUB разделено на два этапа:

1. Курс устанавливается централизованным оракулом Alternative RUBLE под управлением команды разработки, с учетом курса обмена на внешних биржах, а также экономической ситуации
2. На втором этапе контроль курса передается под управление DAO, владеющей токеном управления, который будет распределен между первоначальными владельцами токенов ARUB

На этапе централизованного управления курс, сжигание, выпуск токена контролируется оракулом, управляемым командой Alternative RUBLE. Команда ARUB осознаёт, что факт централизованного управления является бутылочным горлышком в доверии к стабильности токена поэтому планирует выполнить переход на управление DAO после завершения следующих этапов:

- Маркетинговая активность и популяризация
- Обеспечения интеграции токена в системы торговли, обменники и биржи

- Получение не менее 60% collateral usage
- Выпуск токенов и контракта управления

Определения завершенности каждого этапа определяется командой проекта. Для обеспечения дополнительного доверия команде, будут выполняться следующие процедуры:

- Опубликование ежедневных и еженедельных отчетов об использовании обеспечения и выпуске токенов
- Публикация информации о состоянии дополнительных пулов обеспечения
- Публикация оценок о завершенности каждого из этапов
- Публикация информации о сжигании токенов и комиссии
- Публикация информации о работе и обеспечении межсетевых мостов
- Техническая поддержка пользователей, AMA сессии, участие в публичных мероприятиях и др.

Форс мажорные ситуации

1. При резком изменении курса валюты привязки может возникнуть ситуация переиспользования collateral. При достижении утилизации обеспечения более 102% система обмена автоматически повышает комиссии обмена, для повышения количества обеспечения в контракте. При невозможности повышения обеспечения а также превышения использования обеспечения на 150%, торговля во внутреннем обменнике останавливается до стабилизации пула до 102% ИЛИ на 30 дней.
Если по истечении 30 дней стабилизации достичь не удалось, каждый владелец токена в праве потребовать возврата из обеспечения соответствующей владению токена доли пула.
2. Несмотря на тщательную проверку и контроль безопасности, в случае обнаружения критичных или фатальных ошибок в работе смарт контракта, системы контроля курса, а также обнаружения взлома, команда выполняет остановку работы смарт-контракта и выводит обеспечение на escrow контракт, который заморозит все BUSD на срок 30 дней для расследования инцидента. По истечении этого срока, escrow контракт переведет все обеспечение на указанный во время расследования адрес контракта.
3. Несмотря на то, что утечка ключей управления маловероятна, ключи будут обновляться каждые 6 месяцев, владение контрактом также передается на обновленный ключ (только на этапе контроля командой)

Обеспечение безопасности

Самыми уязвимыми элементами системы являются:

- Оракул курса обмена
- Оракулы кроссчейн мостов
- Люди :)

Для обеспечения безопасности оракулов используется трехточечная схема контроля доступа:

- Подписывающий оракул находится на зашифрованном VDS
- Для VDS выделена отдельная VPN сеть не связанная с сетью хост-машины
- Точная локация хоста известна только обслуживающему хост администратору, однако доступ на vds у администратора отсутствует
- Местоположение хоста недоступно администратору с правами обновления
- Администратор обновления не имеет доступа к исходному коду и ключам на VDS
- Разработчики не имеют доступа ни к хост серверу, ни к VDS, ни к ключам, хранящимся на сервере
- Ротация ключей выполняется полностью автоматически на VDS, без участия человека
- Резервирование VDS выполняется каждый час, а также каждую ротацию ключей в зашифрованном виде (снэпшот) на ресурсы организации (минимум 4 географически разнесенных хранилища)

Независимые пулы

Токен ARUB можно стабилизировать с помощью независимых пулов обмена. Обычно такими пулами являются участники, выполняющие обмен валюты привязки 1 к 1 к стейблкоину, независимые биржи и обменники.

Alternative RUBLE также реализует свой независимый пул прямого обмена, но местонахождение пула остаётся анонимным во избежания атак.

Мотивация команды Alternative RUBLE

Команда получает комиссию (на текущий момент 1%) с каждого обмена. Комиссия также будет сохранена при переходе на управление DAO. До достижения уровня обеспечения 50% команда намерена сжигать всю комиссию полученную в ARUB а также выполнять обмен полученных BUSD на ARUB с последующим сжиганием за исключением понесенных на обеспечение работы Alternative RUBLE расходов.

Политика использования

Риски

Alternative RUBLE делает всё возможное, для снижения рисков использования токена ARUB, но всегда следует помнить о внешних рисках изменения рынков, технических сбоях, внешних факторов, включающих нестабильность валюты, целенаправленных атаках на целостность обеспечения. Команда проекта не может нести ответственность за потери вызванные форс мажорными обстоятельствами, техническими сбоями, внешними атаками и другим. ARUB не является инвестиционным инструментом, пирамидой или казино. Используя ARUB вы признаете что полностью осознаете все

риски связанные с криптовалютой торговлей и возможными потерями при её использовании.

Техническая политика

Почему мы не используем обновляемые контракты?

Механизм обновляемых контактов обычно использует контракты-прокси. Наша политика подразумевает максимально простую и прямую реализацию функционала, что бы любой человек даже с базовыми знаниями программирования мог понять как работает контракт. При необходимости обновлений, мы будем создавать отдельный контракт, и настраивать возможности миграции между новым и старым.

Аффилированность с Российской Федерацией

Alternative RUBLE не аффилирован с Российской Федерацией и с каким-либо государством. Цель проекта в создании актива имеющего основное обеспечение в альтернативной валюте и возможность создания прямого обмена с помощью независимых пулов, которые обеспечивают сторонние участники проекта.

Санкции

Несмотря на отсутствие аффилированности проекта с РФ, токен также может попадать под санкции США и Европейских стран. Токен реализован таким образом, что у нас нет технической возможности блокировки средств на кошельках пользователей, однако у различных бирж (PancakeSwap, Binance) есть возможность влиять на обмен токена для конкретных адресов. Будьте осторожны в вопросе выбора способа хранения и обмена токена.

Техническая реализация

Внутренний обмен

Внутренний обмен через биржу работает на основе информации о курсе выпускаемой оракулом (O). Порядок выполнения обмена:

- Пользователь переходит на страницу обмена на сайте Alternative RUBLE
- Пользователь вводит необходимую сумму и направление обмена
- Сайт выполняет запрос через web 3 в смарт контракт а также запрос на север оракула (O) о текущем курсе обмена
- Информация о результатах обмена выводится пользователю
- Пользователь нажимает кнопку обмен

- При отсутствии у контракта доступа к токенам для обмена, направляется approval запрос в контракт BUSD/ARUB и пользователю предлагается подписать транзакцию
- При успешном выполнении транзакции или если подтверждение не требуется сайт отправляет запрос на север оракула (O) с информацией об обмене
- Оракул отправляет сайту подписанное сообщение с информацией об обмене и временем истечения - 60 секунд
- В течении 60 секунд пользователь подписывает и отправляет транзакцию обмена в смарт контракт ARUB
- Пользователь получает токены по результату обмена, за исключением комиссии
- Комиссия платформы отправляется на кошелек команды Alternative RUBLE
- Комиссия на обеспечение пула остаётся в смарт контракте

Обновление курсов

В качестве источника курса используется api Binance в паре RUB/BUSD. Курс агрегируется для периода 15 минут, и вычисляется среднее.

Перед обновлением курса выполняются проверки на ошибки:

- Среднее изменение курса за 15 минут не должно превышать 10%. Если изменение сохраняется в течении 40 минут, устанавливается новый курс
- Колебания курса за период 5 минут не превышают 30%. Это условие выполняется до стабилизации.
- Если колебания курса не превышают 5% за 5 минут, используется текущее полученное значение курса

Защита от влияния

Разовые большие операции блокируются оракулом на 10 минут в случае превышения объема операции более чем на 10% от обеспечения. Оракул уведомляет команду Alternative RUBLE о появлении большого обмена. Если команда не блокирует операцию обмена в течении 10 минут, её можно выполнить. **Условие временно отключено на период запуска стейблока.**

Операции обмена блокируются при расхождении внутреннего курса и курса обмена в паре ARUB/BUSD на PancakeSwap более чем на 10%. **Условие временно отключено на период запуска стейблока.**

Стабилизация

Основной механизм стабилизации валюты на внешних рынках - внутренний обменник, работающий по внешнему курсу RUB/BUSD. При расхождении курса более чем на размер комиссии обмена, пользователям становится выгодно продавать или покупать ARUB на внутреннем обменнике, тем самым не только уравнивая курс между внешними рынками ARUB и RUB, но и, благодаря комиссии на обеспечение, увеличивая количество BUSD в смарт контракте

Базовая комиссия на стабилизацию BUSD-ARUB: 0%

ARUB-BUSD: 1%

Комиссия стабилизации увеличивается при превышении утилизации обеспечения более чем на 99%.

При превышении от 99% до 110% комиссия вычисляется по формуле

$$\text{Fee} = (110 - \text{PoolUtilization}) / \text{AvgSwaps}$$

Где PoolUtilization - текущий процент утилизации пула

AvgSwaps - общее количество обменов за последний час.

При превышении утилизации пула более 110%:

$$\text{Fee} = (\text{PoolUtilization} - 100) / \text{AvgSwaps}$$

Изменение комиссии происходит в автоматическом режиме.

Версия документа 1.0 от 02.07.2022