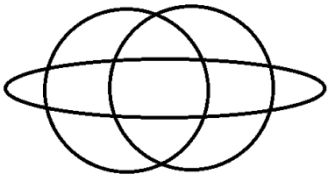


T Y R

Регулируемый токен стабильной рублевой стоимости

Аннотация. TYR - это криптографический токен, который (i) распространяется компанией Flymining SARL, (ii) строго привязан к рублю РФ 1: 1000 и (iii) построен на сети Ethereum [1] в соответствии со стандартом ERC20. TYR - это токен со стабильной стоимостью, который сочетает в себе цену рубля РФ с технологическими преимуществами криптовалюты. В качестве токена, совместимого с ERC20, TYR можно передавать в сети Ethereum. Токены TYR создаются во время вывода с платформы TYRCOIN и выкупаются или «уничтожаются» во время депонирования на платформе TYRCOIN.

1. Введение.

В последнее время значительно выросли популярность криптовалют и интерес к ним у российских инвесторов. Хотя инвестиции в криптовалюты несут в себе обещание, возможно, столь же глубокое, как и сам Интернет, они страдают от сложности перехода из фиатной валюты в криптовалюту и обратно, что затрудняет их использование в качестве средства обмена и расчетной единицы. Одним из предлагаемых решений является создание токена со стабильной рублевой стоимостью, посредством которой, эмитент предоставляет криптографический токен клиентам в обмен на указанную валюту, рубль РФ, по фиксированному обменному курсу 1000 рублей РФ за 1 токен. Поскольку рубль является весьма желательным средством обмена в России, а также признанной расчетной единицей, он является желательной привязкой для стабильного токена.

Нужен стабильный токен, которому люди могут доверять. В этой статье мы предлагаем TYR, регулируемый стабильный токен, который сочетает в себе ценовую и обменную способность рубля РФ с технологическими преимуществами криптовалюты и надзором со стороны аудиторов за наполненностью токена TYR.

2. Доверие.

Создание жизнеспособного стабильного токена – очень серьезная проблема доверия. В то время как биткойн создал систему, основанную на криптографическом доказательстве вместо доверия, стабильный токен с фиксированной привязкой требует как криптографического доказательства, так и человеческого доверия, из-за его зависимости от централизованного эмитента.

Система, которая полагается (хотя бы частично) на доверие, требует надзора. В контексте стабильного токена мы заявляем, что эмитент должен подлежать аудиторскому надзору. Исходя из этого, прозрачность и экспертиза становятся требованиями системы, обеспечивая ее целостность и доверие рынка. Мы предлагаем швейцарскую компанию Flymining SARL, как эмитента токена TYR.

Flymining SARL подчиняется применимым законам и правилам Швейцарии. Flymining SARL поддерживает необходимые лицензии и регистрации, чтобы законно выпустить токен TYR.

3. Подтверждение платежеспособности.

Основным качеством стабильной монеты является поддержание соотношения между выпущенными токенами и рублями РФ, обмененными на созданные токены. Количество выпущенных и находящихся в обращении токенов можно наблюдать на блокчейне, кроме того необходимо демонстрировать базовый баланс в рублях РФ, проверенный доверенной стороной, чтобы продемонстрировать доказательство платежеспособности.

Flymining SARL привлекает независимую аудиторскую фирму для регулярного изучения и засвидетельствования баланса компании в рублях РФ в соответствии со стандартами бухгалтерского аудита.

4. Создание, выкуп и передача

Необходим простой и элегантный механизм для создания и выкупа токенов, для повышения удобства использования и поощрения его принятия в обращение. Мы достигаем этого, позволяя клиентам платформы TYRCOIN выкупать и погашать токены TYR на платформе TYRCOIN.

Токены TYR создаются в момент выхода с платформы TYRCOIN в результате выкупа клиентом суммы токенов TYR по курсу 1000 руб. РФ за 1 TYR, инициировав снятие TYR с платформы TYRCOIN на любой указанный им адрес Ethereum.

Токены TYR погашаются компанией Flymining SARL по запросу клиента на платформе TYRCOIN. При погашении токены TYR уничтожаются, а клиент получает эквивалентную сумму по курсу 1000 руб. РФ за 1 TYR.

Клиент также может хранить токены на своем аккаунте TYRCOIN, снять TYR со своего аккаунта на платформе TYRCOIN на любой указанный им адрес Ethereum, либо депонировать токены TYR на платформу TYRCOIN.

5. Почему Ethereum

Технические характеристики токена TYR требуют использования сети, которая учитывает развитие децентрализованных приложений (включая смарт-контракты), которые могут быть использованы для хранения и передачи стоимости в соответствии с определенными условия, установленные разработчиком. Сеть Ethereum отвечает этим критериям и имеет технический

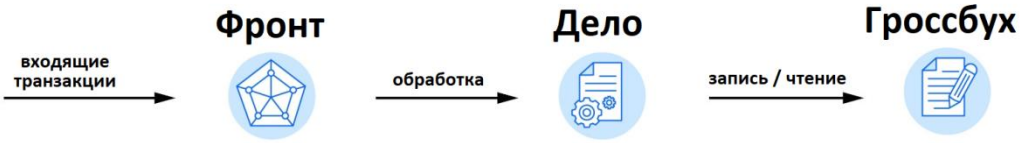
стандарт для токенов - стандарт «ERC20» [4], который получил широкое распространение во всем мире. Уже существует множество программного обеспечения и услуг, которые поддерживают токены, совместимые с ERC20, и предоставляют доступ и удобство использования для конечных пользователей. В качестве альтернативы, если бы токен TYR был построен на базе собственного блокчейна, для создания такой же динамичной экосистемы сторонних разработчиков и программного обеспечения, потребовалось бы большое время.

В результате мы построили TYR как токен, соответствующий требованиям ERC20, в сети Ethereum. Следовательно, токен TYR может быть переведен в сеть Ethereum и сохранен в любом ее адресе.

6. Разделение смарт-контракта

Как эмитенту, нам нужны такие технические решения, которые бы дали нам возможность:
1) Устранять уязвимости;
2) Расширять систему новыми функциями;
3) Оптимизировать операционную эффективность;
4)Приостановить, заблокировать или отменить передачу токена в ответ на инцидент безопасности (т.е. катастрофическое событие), или если возникнут юридические обязательства, или если Flymining SARL будет вынуждена выполнять решение суда или другого государственного органа.

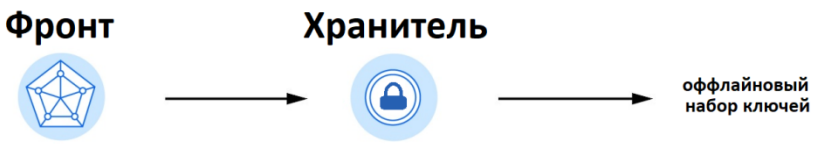
Мы будем производить транзакции в сети TYRCOIN, создав Систему смарт-контрактов, которые взаимодействуют друг с другом. Основные компоненты TYRCOIN представляет собой три смарт-контракта, которые мы называем «Фронт»(Front), «Дело»(Delo) и «Гроссбух»(Grossbuch). Смарт-контракт «Фронт» является публичным лицом токена TYR - это постоянный адрес TYRCOIN на Ethereum блокчейн. Существует и будет существовать только один экземпляр «Фронта». Он обеспечивает интерфейс, с которым держатели токенов могут взаимодействовать и выполнять такие операции, как передача токенов и просмотр остатков токенов; однако «Фронт» не содержит ни кода, ни данных, которые включают в себя поведение и состояние токенов TYR. Вместо этого «Фронт» делегирует право выполнять логику, управляющую токеном, такие как передача, выдача и другие основные функции смарт-контракту «Дело». В свою очередь, «Дело» не будет непосредственно контролировать данные, которые составляют бухгалтерскую книгу TYRCOIN (то есть, отображение держателей токенов и их балансы); вместо этого он делегирует право на бухгалтерскую книгу смарт-контракту, известному как «Гроссбух» - внешняя и вечная книга учета TYRCOIN.



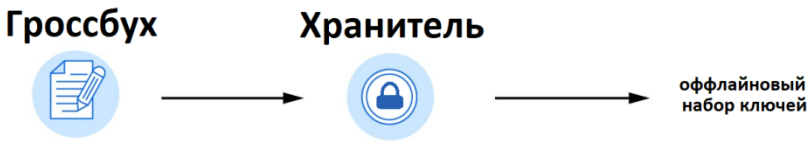
7. Хранение контракта

Для определенных действий с высокой степенью риска, в системе TYRCOIN нам необходим оффлайновый механизм подтверждения. Поэтому мы требуем, чтобы каждый смарт-контракт в системе TYRCOIN обращался к Хранителю за подтверждением. Хранителем может быть другой смарт-контракт или набор ключей (онлайн или оффлайн). Хранитель может обратиться к другому Хранителю, который может обратиться к другому Хранителю и т. д. Тем самым создав цепочку хранения. Например, смарт-контракт может обратиться к другому смарт-контракту, который в конечном итоге обращается к набору ключей для подтверждения. Если Хранитель смарт-контракта достигает оффлайнового набора ключей, значит оффлайновая процедура подтверждения его действий завершена.

Например, «Фронт» обращается к смарт-контракту под названием «Хранитель», который в конечном итоге обращается к оффлайновому набору ключей для подтверждения.

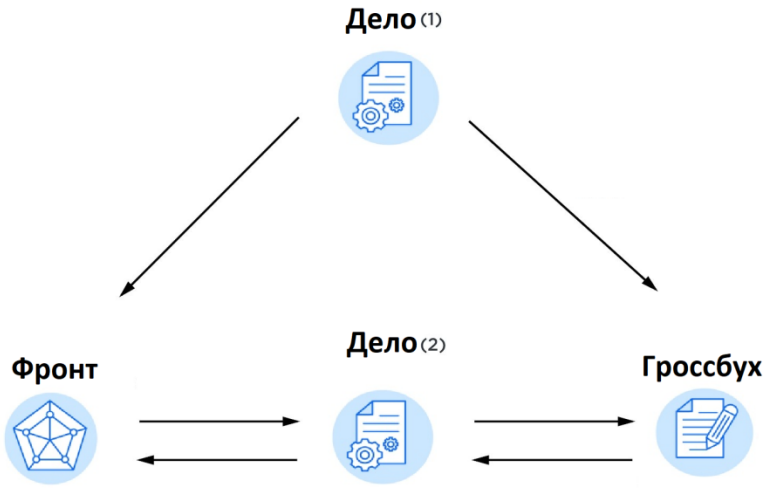


Также Гроссбух обращается к Хранителю, который в итоге обращается к оффлайновому набору ключей для подтверждения.



8. Обновления контракта

Обновление смарт-контракта TYRCOIN - это рискованное действие, в котором используется оффлайновая процедура подтверждения системы TYRCOIN. При совершении замены текущего экземпляра «Дела»(1), поручаем «Фронту» (через Хранитель) перенаправить текущую реализацию токена на новый экземпляр «Дела»(2) и дать команду «Гроссбуху» (через Хранитель) для обработки этого нового экземпляра «Дела»(2) как единственного надежного источника при принятии изменений для бухгалтерской книги TYRCOIN.

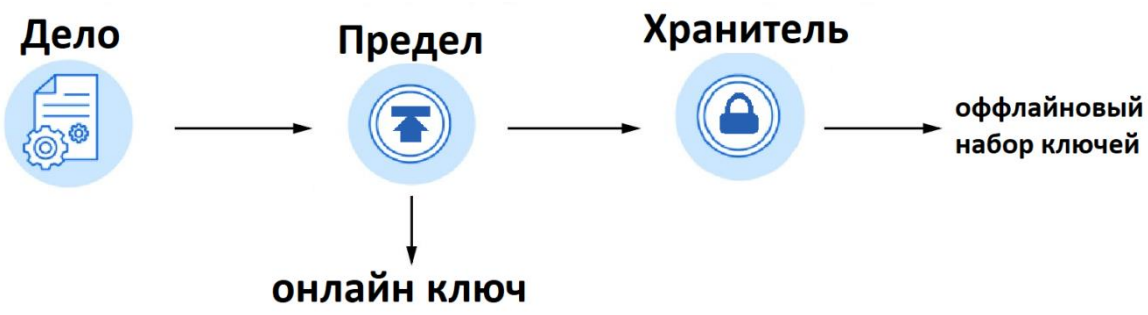


Приведенная выше диаграмма отражает состояние Системы после обновления, согласно которому предыдущий экземпляр «Дело» (1) был заменен новым экземпляром «Дело» (2). Экземпляр «Фронт» теперь обращается к «Дело» (2). Аналогичным образом, экземпляр «Гроссбух» теперь принимает вызовы только от «Дело» (2). Предыдущий экземпляр «Дело»(1) остается, но становится инертным, потому что теперь он не связан с системой.

Совместное опекунство со стороны "Фронт" и "Гроссбух" делает безопасным обновления системы TYRCOIN. Кроме того, само опекунство может быть улучшено. Например, если нам нужно изменить наш оффлайн набор ключей, мы можем поручить Хранителю поручить «Фронту» обратиться к новому экземпляру Хранителя, который обратится к новому оффлайновому набору ключей.

9. Выпуск токенов TYR

Выпуск токенов - это рискованное действие. Количество выпущенных и находящихся в обращении токенов TYR никогда не должно превышать суммарные ликвидные активы компании Flymining SARL. Нам нужно решение, которое бы обеспечило уровень безопасности оффлайновой процедуры подтверждения, в сочетании с гибкостью онлайн-процедуры. Мы предлагаем гибридное решение, в результате которого хранение смарт-контракта «Дело», который контролирует увеличение объема выпущенных токенов TYR, включает как онлайн, так и оффлайн процедуры подтверждения. Для реализации этого уникального подхода мы добавили в цепочку выпуска токенов «Делом» смарт-контракт с именем «Предел»(Predel).



Получив подтверждение онлайн-ключа, «Дело» может выпускать токены TYR до суммы или «лимита», которые указаны в «Пределе». Этот лимит может быть увеличен с подтверждением оффлайнового набора ключей (или уменьшен с подтверждением онлайн ключа). Это решение обеспечивает системе TYRCOIN требуемый уровень безопасности и гибкости в отношении выпуска токенов.

10. Безопасность Контракта

Система TYRCOIN реализует следующие элементы системы безопасности:

1) Оффлайновые ключи: ключи, которые одобряют действия с высокой степенью риска, хранятся в оффлайне в системе хранения TYRCOIN.

2) Генерация ключей: ключи генерируются, хранятся и управляются аппаратными модулями безопасности. Мы используем только модули, каждый из которых является «подписантом», рейтинга FIPS PUB 140-2. Уровень 3 или выше [7].

3) Двойной контроль (мультиподпись). Действия высокого риска требуют подтверждения (т.е. Цифровых подписей) от минимум двух подписантов. Мы используем схему M подписей от N подписантов, при этом M = 2. Это обеспечивает безопасность и отказоустойчивость.

4) Блокировка времени: даже после подтверждения, действия с высокой степенью риска блокируются на минимальный период времени перед тем, как будут исполнены. Это обеспечивает льготный период для обнаружения и превентивного ответа на потенциально опасные события.

5) Откат: ожидающие действия могут быть отменены, что позволяет аннулировать ошибочные или вредоносные действия перед выполнением.

11. Заключение

Мы предложили решение для стабильной монеты, которое устанавливает доверие с помощью криптографического доказательства и регулирующего надзора. Наш проект реализован в сети Ethereum. Включает в себя функцию обновления, процедуру оффлайн подтверждения действий с высокой степенью риска и гибридную онлайн-оффлайновую процедуру подтверждения выпуска токенов, обеспечивающую желаемый уровень безопасности и гибкости.

Наше проект связывает лицензированные финансовые учреждения и экспертов в сеть доверия.

Вместе эти решения формируют токен TYR, регулируемый стабильный токен, который может служить жизнеспособным средством обмена и единицей учета для централизованных и децентрализованных приложений.

Ссылки

[1] V. Buterin et al., “A next-generation smart contract and decentralized application platform,” https://github.com/ethereum/wiki/wiki/White-Paper , 2014.

[2] M. Hochstein, “Tether Confirms Its Relationship With Auditor Has 'Dissolved',” In CoinDesk , www.coindesk.com/tether-confirms-relationship-auditor-dissolved/ , January 2018.

[3] N. Popper, “Warning signs about another giant bitcoin exchange,” In New York Times , https://www.nytimes.com/2017/11/21/technology/bitcoin-bitfinex-tether.html , November 2017.

[4] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” https://bitcoin.org/bitcoin.pdf , 2008.

[5] Ethereum Wiki, “ERC20 Token Standard,” https://theethereum.wiki/w/index.php/ERC20_Token_Standard .

[6] Tether. Tether: Fiat currencies on the Bitcoin blockchain. https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf .

[7] National Institute for Standards and Technology, “Digital Signature Standard (DSS),” In Federal Information Processing Standards Publication 186-4 , https://csrc.nist.gov/publications/detail/fips/186/4/final , July 2013.