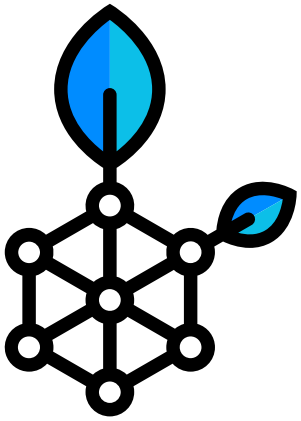


rif

RSK Infrastructure
Framework

RIF Identity Protocol

Создание инфраструктуры для распределенных
приложений следующего поколе

V 1.21

Краткое описание

Мы считаем, что в следующем десятилетии рынок криптовалют ожидает экспоненциальный рост. Однако, чтобы криптовалютами пользовалось большинство людей, а не только технически продвинутое сообщество, каждый пользователь должен иметь возможность управлять своими цифровыми кошельками и активами. То есть одним из основных препятствий для развития технологии блокчейн является присущая ей сложность.

Именно простота в использования позволит привлечь к операциям с криптовалютами пользователей вне банковской и технической сфер. Не стоит надеяться, что технология, в которой для передачи или получения цифровых активов пользователи должны копировать и вставлять длинные шестнадцатеричные адреса, станет популярной. Кроме того, при ручном вводе адреса можно ошибиться, при этом простая опечатка может привести к потере средств. Если добавить систему преобразования имен, так называемых «псевдонимов» или «доменов», вероятность ошибок при вводе значительно снизится и работать с системой станет проще, а значит технология блокчейн получит большее распространение.

Протокол RIF Directory (RDP) разработан для поиска различных типов ресурсов по их именам. Примерами ресурсов являются: RSK-адреса, открытые ключи шифрования, заголовки социальных сетей и т. д.

Кроме того, централизация доступа к определенным ресурсам, которые позволяют удобно считывать имена, улучшает работу пользователей платформы. Поскольку имена ресурсов могут периодически меняться, система должна быть достаточно гибкой, чтобы поддерживать частые изменения. Наконец, система позволяет пользователям легко покупать, продавать и проводить аукционы с помощью токена RIF.

Введение

Одной из основных опор Интернета является система доменных имен (DNS). Она отвечает за сопоставление имен, удобных для чтения людьми, с IP-адресами. Корпорация по управлению доменными именами и IP-адресами (ICANN) отвечает за координацию обслуживания и правила работы нескольких баз данных, связанных с пространствами имен и цифровыми пространствами в Интернете, которые обеспечивают работу сети. ICANN проводит фактическое техническое обслуживание реестров корневой зоны DNS.

Эти службы являются центральной точкой доверия и возможных сбоев[1][2]; их можно отключить с помощью DDoS-атак, а сопоставление имен доменов можно изменить с помощью принудительного изменения DNS-серверов или подмены ответов от них. Кроме того, в этой системе есть определенные проблемы с безопасностью. Например, интернет-провайдеры могут подвергать имена цензуре, что достаточно сложно заметить.

Создатели RIF Directory стремятся сделать его децентрализованной и безопасной системой, аналогичной DNS. Учитывая расширение индивидуальной свободы и доступа к финансовым услугам, существует множество вариантов использования имен. В первую очередь службы имен позволят упростить передачу активов, определяя конечную точку операции. Это позволит людям использовать псевдонимы для безопасного общения или оплаты сделок. Компании также могут использовать псевдонимы, чтобы безопасно определять адреса поступления пожертвований или перенаправлять свои внутренние потоки. Служба имен могла бы использоваться для того, чтобы предоставить указатели ресурсов для децентрализованных интернет-сайтов, страницы которых хранятся в децентрализованной сети. Имена также могут использоваться для определения любого объекта, который собирает репутационные токены, являющиеся публичными.

Протокол RIF Directory и расширение доступа к финансовым услугам

Основная проблема, которая замедляет широкое распространение криптовалют — это сложности при использовании адресов пользователей. Не стоит надеяться, что технология, в которой для передачи или получения цифровых активов пользователи должны копировать и вставлять длинные шестнадцатеричные адреса, станет популярной. Посмотрите на пример RSK-адреса: “06f1b66ffe49df7fce684df16c62f59dc9adbd3f”. При попытке пользователя

расшифровать такое имя часто возникают ошибки, а простая опечатка может привести к потере средств. И самое главное — его очень трудно запомнить.
Также имена могут использоваться в качестве псевдонима банковского счета. В банковской финансовой системе каждый счет имеет свой уникальный номер. Например, в банках Аргентины номер счета начинается с сочетания CBU и включает 22 цифры. Поскольку эти номера достаточно сложные, банки разрешают создавать псевдонимы в виде уникального имени из букв и цифр длиной от 6 до 20 символов. Такой псевдоним должен состоять из букв английского алфавита, кроме этого он может включать точки (.) и тире (-). Такая услуга пользуется популярностью для операций между пользователями банка. Например, Боб отправляет Алисе свой краткий псевдоним, а Алиса вводит этот псевдоним в адрес получателя и выполняет перевод. Из-за удобства в банковских операциях псевдонимы в качестве учетных записей используются всеми сообществами.
Таким образом, RDP представляет собой протокол, который позволяет пользователям приобретать коммерческие домены и псевдонимы. Домены связаны с децентрализованными или централизованными ресурсами, например, веб-страницами, а псевдонимы имеют однозначную связь с персональными ресурсами (например, кошельком, хранилищем или контактными адресами). Преимуществом использования удобных для чтения человеком адресов является уменьшение видимой сложности технологии блокчейн для конечного пользователя.

Первоначальные принципы такой процедуры могут со временем меняться по мере того, как в будущем идеи и архитектура будут постепенно обсуждаться и улучшаться экосистемой.

Реализация протокола RIF Directory

Компания RIF Labs стала первым поставщиком услуги RDP под названием служба имен RIF (RIF Name Services, RNS). RNS использует блокчейн RSK для поддержки и контроля доступа к информации об имени. Таким образом, RNS обеспечивает децентрализацию и безопасность блокчейна RSK. Хотя в будущем могут появиться другие поставщики услуг RDP, мы считаем, что служба имен по своей сути в значительной степени выигрывает от сетевых эффектов, и поэтому предполагаем, что сообщество RIF и RSK в конечном итоге остановится на одном провайдере.

Разработка протокола RIF Directory

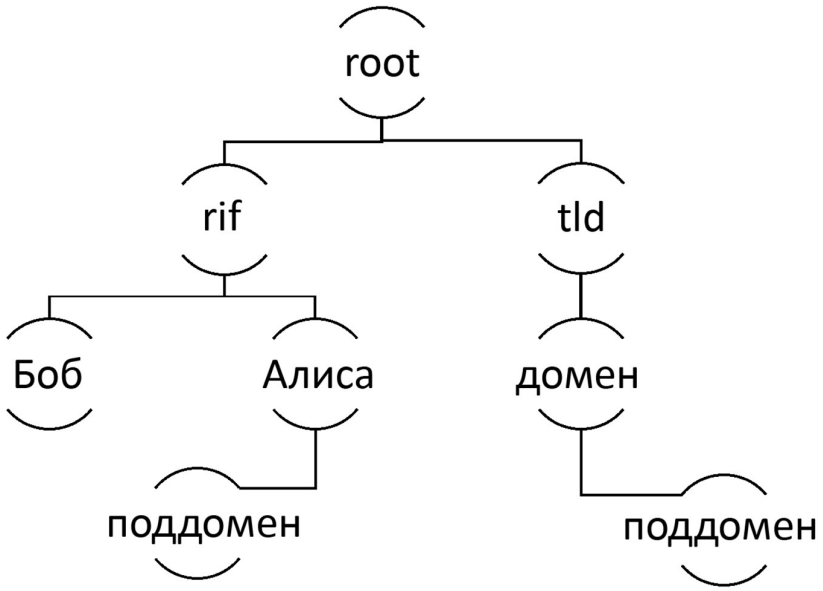
Протокол RIF Directory определяет интерфейс, который используется для упрощения работы с адресами.
Интерфейс поддерживает механизм, который позволяет отображать имя доменов в удобном для чтения виде (например, в виде RSK-адреса). Система должна быть

прозрачной: пользователи должны иметь возможность подтвердить, что у них есть собственный домен и что они за него заплатили требуемую сумму. Кроме того, должна быть четко видна дата окончания действия, чтобы пользователи могли заранее оплатить арендую плату, уменьшая риск случайной потери прав на доменное имя. Также необходимо учесть ситуацию, когда разные пользователи хотят получить одно и то же доменное имя и хотят решить этот вопрос до его покупки, чтобы избежать затрат при разрешении споров. Наконец, система должна свести к минимуму риск цензуры и сквоттинга имен. Важным элементом RDP является токен RIF, который используется в качестве предпочтительного токена при первом получении имени. Токен RIF используется как средство обеспечения на аукционах имен, а также для оплаты обслуживания.

Приобретение доменов

Базу данных доменных имен можно представить в виде дерева. Корень дерева (так называемый корневой узел) контролирует все имена доменов верхнего уровня, или TLD (Top Level Domain). Элементы, которые являются дочерними для доменов верхнего уровня, называются просто доменами. Кроме того, дочерние элементы доменов иногда называют поддоменами.

Все имена RNS создаются по следующему принципу: «поддомен(n)....поддомен(1).домен.tld». Имена состоят из набора меток, разделенных точками. Последняя метка соответствует домену верхнего уровня. Дочерние домены всегда располагаются перед родительским доменом. Кроме того, каждая метка должна быть допустимой меткой, как это описано в UTS46 [3] с определенными ограничениями: переход должен быть ложным, а использование STD3AsciiRules должно быть истинным.



Покупка доменов через слепые аукционы

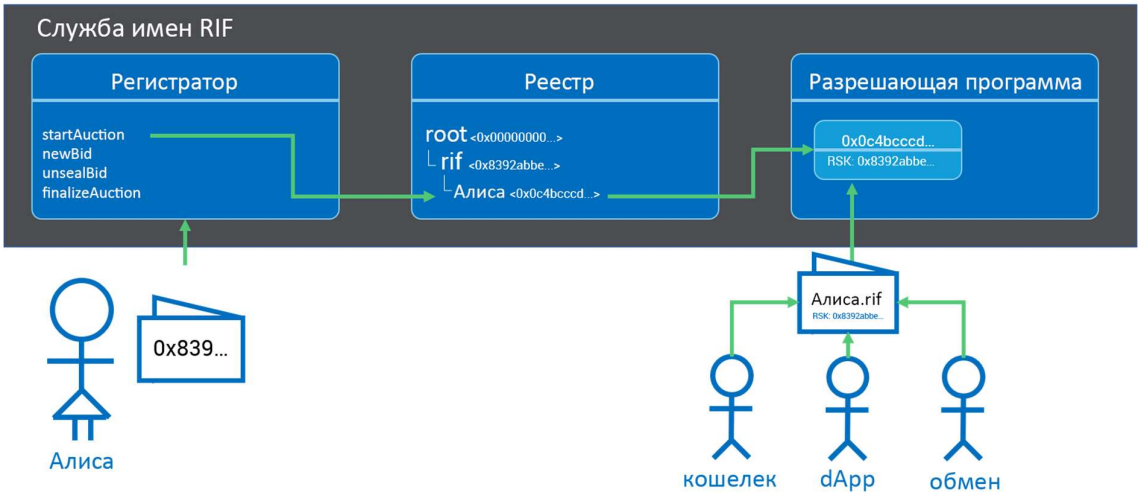
В первый раз домен всегда продается с помощью слепого аукциона Викри [4]. «Аукцион Викри — это тип аукциона с закрытыми предложениями. Участник подает письменную заявку, не зная о том, что предложили другие участники торгов. Побеждает самая высокая ставка, но цена определяется на основе ставки, следующей за самой высокой» [4]. Практика показала, что результаты аукционов определяют не только спрос и предложение, но и причуды людей. Механизм аукциона Викри снижает вероятность того, что претендент переплатит за какой-либо товар, и повышает вероятность того, что продавец получит от него хорошую цену.
Например, если «.rif» — это TLD, а пользователь Алиса хочет получить домен «alice.rif» (как показано на предыдущем рисунке), она может открыть аукцион на этот домен, сделать ставку, и если ставка окажется самой высокой, она станет новым владельцем домена «alice.rif».

Покупка доменов с помощью делегирования

Владелец домена может делегировать право собственности на поддомен покупателю без проведения аукциона. Например, если пользователь Боб является владельцем домена «bob.rif», а Алиса хочет получить поддомен «alice.bob.rif», Боб может передать Алисе право собственности на этот поддомен без аукциона.
С точки зрения уровня доменов, делегирование проводится в виде передачи права собственности. Получив домен, Алиса должна установить разрешающую программу, которая даст разрешение для нового домена и желаемого ресурса. Этот процесс мы подробно рассмотрим в следующем разделе.

Получение разрешения для адреса домена

Получение разрешения для домена — это процесс, при котором система проверяет наличие имени в базе данных и, при положительном ответе, возвращает информацию, связанную с этим доменом. Такое разрешение может использоваться в кошельках, в процессе торговли или в dApps для обработки удобных имен, вместо сложных адресов. Например, Алиса хочет отправить деньги Бобу. Для этого Боб отправляет свой зарегистрированный псевдоним Алисе, по нему Алиса может найти адрес Боба в приложении кошелька, а сама программа кошелька будет искать это имя в базе данных RDP и получит оттуда информацию об адресе этого псевдонима.



Вторичные рынки

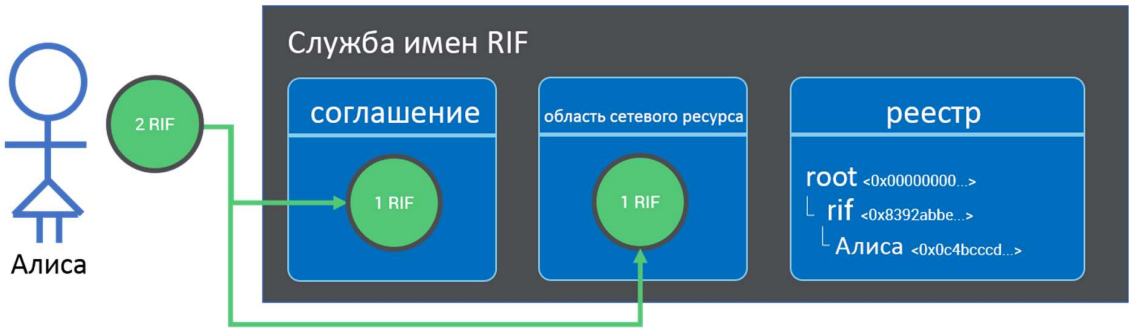
Несмотря на то, что протокол RIF Directory не связан с определенным вторичным рынком, который будет использоваться для продажи доменов после их приобретения, существуют децентрализованные вторичные рыночные решения, где люди могут покупать и продавать домены. При наличии спроса мы ожидаем, что сообщество RIF создаст новые вторичные рынки, нацеленные на продажу доменов. Вторичные рынки могут принимать платежи за домены разными криптовалютами, поддерживать другие виды аукционов, а также простую первичную передачу услуг. Вторичные рынки для доменных имен могут также использовать токен RIF и другие средства платежа.

Доходы поставщика услуг

Поставщики услуг могут получать комиссионные от аукционов по продаже имен и арендную плату. Они могут по своему выбору либо просто потратить эти средства, либо сделать пожертвование, либо использовать их для получения дохода. Плата за токен RIF также препятствует сквоттингу имен, поскольку владелец имени должен вносить годовую плату за обслуживание каждого приобретенного домена.

Заблокированные токены

Когда пользователь участвует в аукционе, предлагаемые токены RIF блокируются по Соглашению, как показано на следующей схеме.



Часть выигрышного предложения, равная по сумме второму по величине предложению, блокируется в обмен на право пользования доменом. Заблокированные суммы проигравших заявок возвращаются их законным владельцам по запросу.
Заблокированные токены RIF будут возвращаются владельцу при его отказе от домена за вычетом комиссии, которую определяет поставщик услуг.

Годовые выплаты

Чтобы оставить за собой право пользования доменом, владелец должен выплачивать ежегодную арендную плату. Через девять месяцев с момента последней выплаты ежегодной арендной платы владелец может оплатить ее на следующий год, чтобы продолжить пользоваться доменом, или отказаться от него.
Если владелец не оплатил арендную плату, это означает, что он отказывается от права собственности на домен. В этом случае ему возвращаются первоначально заблокированные токены, за вычетом комиссии, установленной поставщиком услуг.

Взгляд в будущее

Мы создали полезный и справедливый в использовании протокол, который стимулирует пользователей заниматься торговлей именами без злоупотреблений. Тем не менее, мы считаем, что он должен развиваться и в будущем его могут заменить другие, более совершенные протоколы RIF. Давайте обсудим, в каких направлениях может развиваться этот протокол.

Обновления

Поставщик услуг RDP может вносить обновления, чтобы добавить новые функции или исправить ошибки. Управлять такими обновлениям будет поставщик услуг. Необходимо учесть, что такие обновления должны быть полностью совместимыми с предыдущими версиями протокола. Другими словами, не следует менять принципы владения доменами (за исключением изменения доменов DNS, описанного в следующем разделе). А изменения в платежных структурах, моделях аукционов и другие функциях вполне допустимы.

Домены DNS и оракулы

RDP открывает возможности для миграции обычных DNS-адресов в RDP, путем сопоставления доменов DNS и TLD с доменами RDP и TLD. Чтобы этот процесс был справедливым, владелец домена DNS должен иметь возможность получить домен RDP, если он докажет, что является законным владельцем, который использует либо оракулы, либо цифровые цепочки сертификации. Для разрешения конфликтов, возникших из-за совпадений доменных имен RDP и ICANN, может быть использована система арбитража. Она может быть реализована с помощью оракулов или децентрализованными методами. Хотя текущая версия RIF Directory не использует специальный интерфейс, мы предвидим, что в будущих версиях протокола такая возможность будет реализована.

Анонимность

Пользователям может потребоваться скрыть платежные адреса своих псевдонимов. Это можно сделать с помощью шифрования ресурсов. Владелец должен передать ключ дешифрования пользователю через внешний канал связи, возможно, предлагаемый поставщиком услуг связи RIF. Кроме того, можно использовать зашифрованные адреса. Шифрование адреса позволит плательщику получать новый уникальный адрес для каждого платежа, снижая вероятность его отслеживания.

Создание нового домена верхнего уровня

Компания RIF Labs выступает в качестве поставщика услуг RDP. Она развернула первоначальный регистратор TLD. В рамках этого процесса компания RIF Labs в будущем поможет пользователям создавать, покупать и продавать свои собственные TLD.

Краткий обзор

Протокол RIF Directory был разработан на основе знаний, собранных различными организациями, которые работали над созданием служб имен. Он использует единый унифицированный интерфейс, совместимым с интерфейсами существующих поставщиков услуг, связанных с именами доменов. Интерфейс системы позволяет пользователям приобретать домены, делать ставки на аукционах, управлять субдоменами и с помощью токенов RIF легко оплачивать необходимые сборы за услуги, которые предоставляются в централизованной и децентрализованной сети.

Ссылки

[1] М. Али, Р. Ши, Дж. Нельсон, М. Дж. Фридман, «Blockstack: новый интернет для децентрализованных приложений» (2017) https://blockstack.org/whitepaper.pdf
[2] «Часто задаваемые вопросы о неймкоине»https://namecoin.org/docs/faq/
[3] Библиотека NPMhttps://www.npmjs.com/package/idna-uts46
[4] «Аукцион Викри» https://en.wikipedia.org/wiki/Vickrey_auction