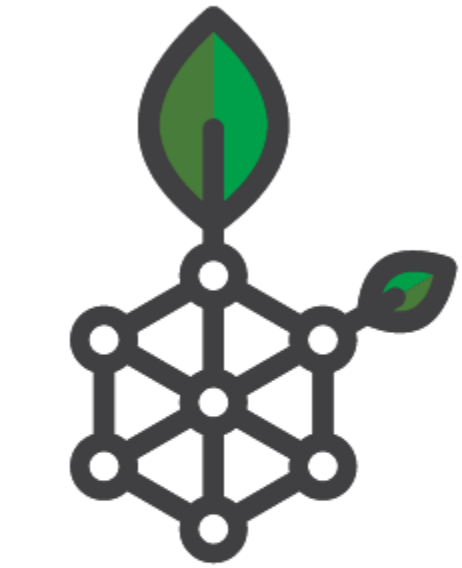

RSK

Обзор официального документа

Редакция: 9
Дата: 19 ноября 2015 года
Автор Серджо Демиан Лернер

Введение

В 2008 году Сатоши Накамото совершил революцию в сфере платежей, создав Биткойн. Биткойн включал очень ограниченное применение так называемых «смарт-контрактов» — концепта, который был введен в 1993 году Ником Сабо (Nick Szabo).

С тех пор множество исследований было посвящено созданию новых криптовалют, которые поддерживают полные по Тьюрингу распределенные программы. Сейчас существует распространенная уверенность в том, что для достижения этой цели могут быть созданы пригодные, надежные и детерминированные виртуальные машины.

Мы верим в то, что необходимо применять новые сценарии использования для того, чтобы Биткойн стал ведущей мировой криптовалютой и что добавление возможностей смарт-контрактов станет ключевым в достижении этого в будущем. С этой мыслью мы создали RSK — платформу для смарт-контрактов, которая позволяет применить к Биткойну машину Тьюринга для вычисления полноты. Это также позволяет улучшить другие параметры сети, например, ускорить операции и увеличить масштабируемость, что, по нашему убеждению, поможет использовать новые сценарии использования.

RSK — это эволюционировавший вариант QixCoin полной по Тьюрингу криптовалюты, созданной в 2013 году той же группой разработчиков. RSK представляет улучшенный вариант платежа с почти мгновенными подтверждениями. В настоящее время она достигает скорости 300 транзакций в секунду и подтверждает большинство платежей менее чем за 20 секунд. И в то же время она основана на тех же гарантиях безопасности, что и Биткойн, что позволяет поддерживать объединенный майнинг SHA-256D.

RSK работает как сайдчейн Биткойнов. Когда Биткойны направляются в RSK blockchain, они становятся Смартбиткойнами (SBTC). Смартбиткойны эквивалентны Биткойнам, которые находятся в RSK blockchain, и они могут быть в любое время переведены обратно в Биткойны без какой-либо дополнительной платы (за исключением обычной операционной комиссии RSK). SBTC является основной валютой, используемой в сайдчейне RSK, которая выплачивается майнерам за транзакции и обработку контрактов. Выпуска валюты не происходит: все SBTC создаются из Биткойнов, которые поступают из Bitcoin blockchain.

RSK усовершенствует Биткойн по следующим параметрам:

- Виртуальная RSK машина Тьюринга для вычисления полноты (RVM) допускает использование смарт-контрактов
- Первое подтверждение транзакций в среднем происходит за 10 секунд
- Безопасный объединенный майнинг, сочетающий доказательство выполнения работы с резервным пороговым федеральным майнингом
- Встроенное скоростное реле с малым временем задержки одноранговой сети.
- Двухстороння привязка с использованием сайдчейнов (в настоящее время федеративная привязка, полностью автоматическая привязка получают усовершенствования Биткойнов)

Аббревиатуры: “RSK” означает Rootstock (платформа), связанные термины «протокол RSK» (спецификация) и «узел отсчета RSK» (применение справки), оригинальная

валюта RSK — «Смартбиткойн», «SBTC» — символ Смартбиткойна, «BTC» означает валюту Биткойн, а «Биткойн» относится к протоколу Биткойн.

Почему RSK важна для экосистемы Биткойн?

Связь держателей Биткойнов и защита ценности

Главная цель управления RSK — связать основных держателей Биткойнов путем создания вознаграждения, которое полностью взаимосвязано с их текущей деятельностью.

Эта философия напрямую отражается в его основополагающей архитектуре, где майнеры Биткойна предоставляют хэшинг, необходимый для оценки доказательства выполнения работы, лидеры индустрии (обменные пункты, кошельки и платежные системы) образуют Федерацию, которая создает пункты оценки и подписывает возвращенные транзакции с двухсторонней привязкой.

Помимо этого, RSK предлагает улучшения своей платформы на основе системы голосования, где майнеры, лидеры индустрии, держатели Биткойнов/RSK и основные разработчики принимают окончательное решение.

В последующих разделах мы опишем, каким образом происходит данное стимулирование.

Модель управления

Каждый участник этого сообщества обладает ноу-хау, позволяющим ему принести наибольшую пользую сообществу: обменные пункты и веб-кошельки знают, как защитить сбережения Биткойнов, майнеры знают, как осуществить крупномасштабные майнинговые операции для защиты пользовательских транзакций, компании блокчейнов совершают обновления сценариев использования и воплощают мечты в жизнь, основные разработчики обладают техническим опытом для решения технически сложных задач, специалисты по обслуживанию узлов обеспечивают связь инфраструктуры и сети, а пользователи являются основой этой системы, обеспечивая доверие и оборотный капитал.

Модель управления RSK нацелена на представление всех действующих лиц сообщества путем создания совета правления, состоящего из 5 мест. Майнеры смогут голосовать путем хеширования (1 голос), пользователи Биткойн и RSK смогут голосовать путем доказательства доли владения (1 голос), пункты обмена и веб-кошельки будут голосовать через федерацию (1 голос), разработчики RSK и Bitcoin Core будут располагать специальной пороговой системой голосования (1 голос), и последний голос будет предложен основанному некоммерческому учреждению Биткойн, такому как Фонд Биткойнов, который может представлять более широкую экосистему. Также институционный голос может быть предложен Фонду Ethereum, если он является представителем сообщества Ethereum.

Защита инвестиций майнеров Биткойна

В августе 2016 года маржа прибыли от майнинга упадет до уровня менее чем 50 % ввиду снижения награды за блок с 25 до 12,5 Биткойнов. Сотни миллионов единиц аппаратного оборудования для майнинга сразу станет выведенным из употребления.

Это, вероятно, будет касаться всех машин для майнинга, которые имеются сейчас на рынке, поскольку к 2017 году будет разработано и продано два поколения чипов (более высокоскоростных и с меньшим энергопотреблением). Почти все действующие майнеры, которые не заменили свое аппаратное обеспечение, столкнутся с крахом своего майнинга. RSK, благодаря возможностям объединенного майнинга, позволит этим майнерам продолжать дело в течение еще как минимум четырех лет. Поскольку объединенные майнеры Биткойнов могут осуществлять майнинг монет с нулевыми маржинальными издержками, они будут также в состоянии заниматься майнингом Биткойна до тех пор, пока дополнительный доход, обеспеченный майнингом RSK, не покроет потерю прибыли.

Кроме того, снижение прибыльности майнинга в два раза образует дополнительную концентрацию малобюджетных майнеров, что повысит уязвимость сети Биткойн. Таким образом, RSK может также играть ключевую роль в продвижении широкой базы прибыльных майнеров, повышая надежность и ценность Биткойна.

Также, начав сегодня с минимальной цены и создавая приложения для RSK, майнеры Биткойна могут не только защитить свои инвестиции, но и создать полноценную коммерческую возможность.

Защита Биткойна / Двухсторонняя привязка RSK

Ведущие компании в сфере Биткойн объединятся в федерацию, которая будет играть фундаментальную роль в обеспечении перевода средств между Биткойном и RSK blockchains. Взамен этого, они будут получать выгоду от комиссии, образованной соотношением между входящими и исходящими потоками средств.

Более низкая комиссия на транзакции с Биткойном и выпуск активов со стабильной стоимостью

Настоящие владельцы Биткойнов и перспективные пользователи видели использование финансовой системы, ограниченное определенными сценариями (например, инвестирование, глобальная платежная сеть) преимущественно за счет волатильности цены Биткойна, но это ограничение может усугубиться в дальнейшем по причине потенциального роста комиссии на транзакции во время следующего деления Биткойна пополам.

RSK является решением этой ситуации, предлагая почти мгновенную оценку транзакций (20 секунд) и выпуск активов по ценам, привязанным к цене фиатной валюты или другому стабильному продукту. Снижение потерь от волатильности транзакций при сохранении статуса Биткойна в качестве резервной валюты повышают общую стоимость Биткойна.

Усиление защиты Биткойна

Во время следующего разделения Биткойна устаревшее аппаратное обеспечение на сумму в сотни миллионов долларов будет продано за невысокую цену частным образом или в сети Интернет. Это породит уязвимость, предоставляя агрессивному игроку возможность приобрести огромное количество хэшинга за очень небольшие деньги и предпринять атаку на 51 %. Также снижение защиты может повлиять на выявленную стоимость монеты. Увеличивая прибыльность от майнинга Биткойнов

путем объединенного майнинга, сеть Биткойн может предотвратить обрушение хэшрейта.

RSK как сеть низкозатратных платежей BTC

Если размер блока Биткойнов не увеличен за счет хардфорк при следующем призовом разделении Биткойна, транзакционные комиссии могут стать неприемлемо высокими для определенных приложений. Поскольку блоки RSK могут удерживать гораздо больше транзакций, чем блоки Биткойна, RSK естественным образом предложит более низкую комиссию. Анализ будущих сценариев в отношении комиссии на транзакции см. в следующем разделе.

Будущее Биткойна и комиссий на транзакции с ним представляется неясным: по ходу развития событий спорные предложения в отношении изменения максимального размера блока будут иметь сильное воздействие на будущую транзакционную комиссию. В нижеприведенной таблице мы попытались предсказать будущие сценарии и сравнить RSK и Биткойн, совершив обоснованные предположения в отношении роста и форков.

Параметр	Биткойн	RSK
Время подтверждения с относительной безопасностью в эквивалентах Сатоши	10 минут	10 секунд
Минимальное время подтверждения для обратной прибыльности 0,1 %	20 минут (2 блока)	30 секунд (3 блока)
Максимальное количество транзакций в секунду	3,3 транзакции в секунду (при среднем размере транзакции)	300 транзакций в секунду за один запуск Масштабируется до 1000 транзакций в секунду
Текущая средняя стоимость стандартной транзакции для пользователей	6 центов При: - 1,5 транзакции в секунду	Рыночная цена неприменима
Текущая стоимость для майнеров, включающая стандартную транзакцию	1 цент При: - использовании сети с высокоскоростным реле - UTXO в памяти - 1 мс времени обработки одной транзакции. - среднем вознаграждении за блок 25,2 BTC 5 центов При: - использовании сети со стандартным реле	<1 цент (ориентировочно) При: - отсутствии специальной аппаратной коммутации RSK. - почти полном отсутствии транзакций RSK 1 цент (ориентировочно) - Отвлечение майнера на загрузку нового головного элемента ведет к потере 10 мс от времени процесса
Комиссии на транзакции к концу 2016 года	1,6 доллара США При: - неувеличенном размере блока - неизменном соотношении BTC/доллар США - прежнем уровне безопасности - 3 транзакциях в секунду	1 цент (ориентировочно) При: - 3 транзакциях в секунду

На основе вышеприведенной таблицы важно отметить, что расчет комиссии на транзакции основан на недоказанном факте о том, что цена BTC сохранится на уровне приблизительно 240 BTC/доллар США в течение 2016 года. Если цена поднимется в десять раз в течение этого периода, тогда также поднимется комиссия на транзакции, делая блокчейн Биткойн пригодным в качестве внутрибанковской клиринговой системы, но не в качестве платежной системы. Также важно заметить, что могут появиться платежи в системах вне чейна, обеспечивая более недорогие платежи, но в то же время централизуя сеть и изменяя ее децентрализованный характер.

В нижеприведенной таблице указаны возможные будущие сценарии, которые развернутся к концу 2016 года, если предположить, что сложность сетевого хэшинга возрастет в той же мере, что и цена BTC:

Сценарий	Стоимость транзакции Биткойнов для майнеров	Стоимость транзакции RSK для майнеров
Цена Биткойна увеличивается в 10 раз	16 долларов США	2 цента
TPS увеличивается в 10 раз с помощью хардфорк	11 центов	0,2 цента
Цена на BTC и TPS увеличивается в 10 раз	1,1 доллара США	2 цента

Поскольку цена на включение транзакции Биткойна возрастает, пользователи будут переходить на платформы с более низкой стоимостью транзакции, например RSK.

Сценарии использования RSK

Платформа RSK предоставляет полные по Тьюрингу смарт-контракты, как было предложено Ником Сабо в 1993 году. В то же время виртуальная машина RSK обратно совместима с виртуальной машиной Ethereum, таким образом, RSK дает возможность разработчикам, имеющим дело с Ethereum, получать выгоду от устойчивости блокчейна Биткойн. Ниже приведен список потенциальных смарт-контрактов и сценариев использования, которые могут быть разработаны на платформе RSK.

Каналы микроплатежей и веерные сети

Каналы микроплатежей позволяют двум сторонам обеспечить безопасность регулярных низкозатратных платежей без оплаты комиссии за каждый платеж, а только единовременно при закрытии канала.

Веерные сети позволяют пользователям, проявляющим взаимное недоверие, совершать низкозатратные единовременные платежи, косвенно используя платежные каналы в адрес третьего лица, которое пользуется минимальным доверием. RSK позволяет применять веерные сети напрямую, с минимальными усилиями и использованием интерфейса стандартных электронных кошельков.

Одноранговый распределенный обмен

Используя протокол TierNolan, RSK поддерживает контракты, которые действуют как одноранговые обменные пункты. Также можно с легкостью установить автоматическое сопоставление в книге заказов. Это позволяет распределенным рынкам за пределами независимых блокчейнов обменивать криптоактивы без привлечения третьих лиц.

Системы розничных платежей

RSK позволяет адаптировать BTC к каждодневным розничным транзакциям по всему миру. Одним из ограничений использования Биткойна в розничной среде является время подтверждения (от 10 минут до 1 часа для обеспечения невозможности отмены). RSK позволяет пользователям получать выгоду от надежности Биткойна, с подтверждением в пределах нескольких секунд. Торговые предприятия смогут принимать платежи мгновенно, без необходимости привлечения третьих лиц в качестве посредников. Другим ключевым элементом, которым должна обладать любая платформа для достижения успеха на рынке розничной торговли, является возможность поддержки большого количества транзакций в секунду (tps). Сеть RSK, использующая протокол DÉCOR+, позволяет обрабатывать в блокчейне Биткойн до 300 транзакций в секунду (в два раза больше, чем Paypal)

Услуги условного депонирования

RSK позволяет создать услугу условного депонирования, где Oracle подписывает (или нет) транзакцию, определяя, должна ли она выполняться (или нет), без какого-либо контакта со средствами, находящимися в доверительном владении.

Создание криптоактивов

RSK позволяет создавать криптоактивы (или Altcoin), охраняемые сетью Биткойн. Принимая во внимание гибкость RSK в оценке источника контракта, данным

приложением (как и всеми другими) могут пользоваться все, от студентов до банков и корпораций.

Обеспечение безопасности активов

RSK также позволяет создать цифровые токены, обеспеченные реальными активами. Это может использоваться для электронной коммерциализации REIT, акций, выпуска долговых обязательств или любого другого актива (или будущей прибыли). Этот конкретный сценарий использования предоставит уникальное решение для малых предприятий в развивающихся странах, где традиционные финансовые рынки не удовлетворяют потребности в работе или росте капитала.

Децентрализованные переводы средств

Этот конкретный сценарий использования особенно важен в развивающейся экономике, где не обслуживаемое банком или не имеющее документов население вынуждено платить ростовщические проценты для того, чтобы отправить деньги на питание и жилье своим семьям.

Защита IP / Registry

RSK позволяет разрабатывать контракты, которые могут воссоздать то, что называется «доказательством существования», которое позволяет частным лицам и подобным компаниям доказывать существование определенного документа (или права собственности) в любой конкретный момент времени, находясь под защитой блокчейна Биткойн. Этот сценарий использования может быть особенно важен в сообществах Латинской Америки, Африки и Азии, где существуют ненадежные механизмы земельной регистрации.

Система голосования

В качестве конкретного сценария криптоактива RSK позволяет создать цифровые голоса, которые позволят провести крайне безопасные и прозрачные выборы с минимальными затратами.

Микролендинг

Более 50 % мирового населения не имеют доступа к традиционной финансовой системе. Отсутствие доступа к получению кредита является прямой причиной экономического неравенства, с которым мировое сообщество сталкивается в настоящее время. RSK позволяет разработать масштабируемые контракты цифрового микролендинга, что может обеспечить доступ к получению кредита 3 миллиардам беднейших жителей мира.

Отслеживаемость цепочки поставок

RSK также позволяет создать цифровые кошельки для отслеживания и определения (в электронном виде) физического местоположения конкретного продукта или партии. Этот вид контракта может быть особенно полезен в сфере розничной торговли, пищевой индустрии и сфере здравоохранения, помимо остальных областей. Как и во всех других сценариях, при использовании RSK это может быть достигнуто за счет надежности блокчейна Биткойн с минимальными издержками.

Репутация в сети Интернет и электронное удостоверение личности

Одной из главных проблем развивающихся стран является отсутствие документов и удостоверений личности у бедных слоев населения. Это не позволяет беднякам голосовать, получать медицинские услуги, сообщать о преступлениях/правонарушениях и получать финансовую помощь. RSK позволяет создать глобальные цифровые реестры с такой степенью надежности, как блокчейны Биткойн, с чрезвычайно малыми издержками.

Глобальная внутриигровая валюта

Многие многопользовательские игры имеют внутреннюю экономику, включающую собственную валюту. По мере развития этих игр виртуальная валюта становится ценной для пользователей в той же мере, как и фиатные деньги, и она часто продается на вторичных рынках. Инфляция, читерство и воровство в сети Интернет становятся основными проблемами пользователя. Также игровая компания может сталкиваться с правовыми барьерами и препятствиями в обеспечении защиты при пересылке виртуальных денег пользователей. Вместе с глобализацией мирового сообщества это произойдет и с виртуальными играми, и игроки испытают неудобства от того, что деньги, полученные в одной игре, невозможно легко использовать в другой. RSK может решить эти проблемы, позволив принимать BTC в играх (в эквиваленте монет RSK) в качестве внутренней оплаты или создавать частный электронный актив, который защищен RSK. Платежи RSK могут проходить со столь же высокой скоростью, как и замкнутые системы для низкой деноминации, поэтому игровые движки могут использовать RSK в качестве внутриигровой системы покупок для торговли между игроками и виртуальных предложений, совершаемых между компаниями и игроками. С помощью простого клика по URL-адресу или сканирования QR-кода можно стимулировать торговлю с использованием стандартных внешних электронных кошельков игрока, а также с перечислением комиссии в игровую компанию.

Азартные игры в сети Интернет и рынок предсказаний

Быстрые платежи также означают быстрые выплаты. Сайты азартных игр с использованием Биткойна, такие как SatoshiDice, сумели предоставить услуги по приему быстрых ставок без регистрации, подтверждения и цепочных транзакций, но с риском безопасности для игорного сайта. RSK позволяет совершать ставки с немедленными выплатами посредством блочного подтверждения.

Честная игра

Внедряя смарт-контракты и вместе с хорошо изученными криптографическими протоколами, такими как Mental Poker, RSK может предоставлять открытую и честную платформу для карточной игры без необходимости привлечения проверенных третьих лиц в качестве крупье.

Мы привели всего несколько вариантов из множества примеров того, что можно создать и спрограммировать на платформе RSK, используя технологию Биткойна в основе. Важно упомянуть о том, что майнеры Биткойна (путем объединенного майнинга) планируют управлять этими контрактами и получать выгоду от огромного количества ресурсов, потребляемых для обеспечения этих контрактов.

Обзор технологии

Платформа RSK в своей основе представляет собой сочетание:

- детерминированной виртуальной машины Тьюринга для вычисления полноты учетных записей ресурсов (для смарт-контрактов)
- сайдчейна Биткойн с двухсторонней привязкой (для торговли BTC с выраженной номинальной стоимостью)
- динамического гибридного объединенного майнинга/федеративного согласованного протокола (для защиты согласованности) и сети с низким значением задержки (для быстрых платежей).

Виртуальная машина Тьюринга для вычисления полноты

Виртуальная машина RSK (RVM) представляет собой основу платформы смарт-контрактов. Смарт-контракты выполняются параллельно высоким процентом сетевых узлов. Результатом выполнения смарт-контрактов может быть обработка сообщений, содержащихся внутри контракта, создание денежных операций и изменение состояния постоянной памяти контрактов. Операционный код RVM совместим с EVM, чтобы позволить безупречную обработку контрактов Ethereum на платформе RSK. Во время первого запуска виртуальная машина выполняет интерпретацию. Во время последующих запусков планируется эмулировать EVM операционными кодами динамического ретаргетинга EVM, чтобы набор байт-кодов типа Java и виртуальная машина типа Java с повышенной надежностью и ограничением памяти стала новой виртуальной машиной (RVM2). Это поставит RSK по производительности выполнения кода близко к уровню собственного кода.

Основные характеристики:

- Независимая виртуальная машина, при этом совместимая с EVM на уровне операционного кода.
- RSK предоставляет пользователям Ethereum возможность вести проекты под защитой сети Биткойн.
- Новые операционные коды для быстрых арифметических действий типа int32 и лучшей своевременной компиляции (планируемой), для повышения производительности.

Сайдчейн

Сайдчейн — это независимый блокчейн, курс оригинальной валюты которого автоматически привязан к курсу валюты другого блокчейна с помощью использования защиты платежа. Существует двухсторонняя привязка, когда две валюты можно обменивать между собой свободно, автоматически и без обсуждения цены. На платформе RSK Смартбиткойн (SBTC) имеет двухстороннюю привязку к BTC (точнее, Рутоши, минимальная единица исчисления в RSK, привязана к Сатоши, минимальной единице исчисления в Биткойн).

На практике, когда BTC обменивается на RTS, перечисление валюты между блокчейнами в рамках одной транзакции не происходит, поскольку Биткойн не может подтвердить подлинность балансов на другом блокчейне. Когда происходит перевод, некоторые BTC оказываются заблокированными в Биткойн, а то же самое количество SBTC разблокируется в RSK. Когда необходимо конвертировать SBTC обратно в BTC, SBTC снова блокируется в RSK, а то же самое количество BTC разблокируется в Биткойн.

Сайдчейны с неполным доверием

Возможно установление привязок с полным доверием и без участия третьих лиц, с использованием смарт-контрактов на обеих платформах. Однако поскольку Биткойн в настоящее время не поддерживает ни смарт-контракты, ни операционные коды для оценки внешней защиты SPV, часть двухсторонней системы привязок в RSK требует полагаться на определенных сторонних участников с неполным доверием (STTP). Ни один STTP не может контролировать заблокированные BTC, и только у их большинства имеется возможность разблокировать активы BTC. STTP временно хранят BTC, которые являются заблокированными, и разблокируют BTC для оплаты пользователям Биткойн, SBTC заблокированы в RSK для дальнейшей отправки обратно в Биткойн.

В RSK те STTP, которые защищают заблокированные фонды, всегда становятся участниками Федерации. Это происходит потому, что стимулы Федерации тесно связаны с STTP: они должны быть уважаемыми участниками сообщества, такими как университеты, а также должны иметь техническую возможность для обслуживания надежного сетевого узла. Блокирование и разблокирование средств происходит с помощью этих надежных сетевых узлов без вмешательства человека. Поэтому требование быть частью Федерации обусловлено возможностью контролировать надлежащее поведение программного обеспечения, которым оборудован узел, особенно в отношении правильности работы компонента, ответственного за принятие решения о разблокировке активов BTC. Мы планируем создать измененное защищенное аппаратное оборудование, которое усилит федеративный алгоритм поверки для дальнейшего усовершенствования системы безопасности.

Как только Биткойн внедрит специальные операционные коды или расширяемость для оценки защиты SPV в качестве хардфорк и новая система подтвердит свою надежность и заслужит доверие, роль Федерации в качестве STTP утратит свою необходимость и команда RSK применит изменения для адаптации RSK к системе с неполным доверием.

Динамический гибридный объединенный майнинг/Федерация

Мы считаем, что PoW — это единственная недорогостоящая согласованная система, которая предотвращает переписывание истории блокчейна. Все другие согласованные системы, которые не требуют привлечения ценных ресурсов для майнинга, обладают этим недостатком и полагаются на репутацию, и не допускают анонимное участие в майнинге. Все другие согласованные системы требуют от новых пользователей полагаться на определенных лиц при поиске проверенного пункта реестра.

Высокоскоростные согласованные PoW на основе периодических блоков с низкой потерей объектов требуют от майнеров остановки аппаратного обеспечения и его перезапуска на новом головном элементе каждый раз, когда новый блок заполняется сетью. Результатом служат временные промежутки или увеличенные интервалы ожидания сети в процессе майнинга при переключении в серединное положение, в среднем. Эти промежутки снижают эффективность майнинга Биткойнов, даже если процесс занимает несколько миллисекунд. Таким образом, RSK использует схему призового разделения блока DECOR+ для того, чтобы снизить конкуренцию и

позволить майнерам переключиться на лучший блок RSK на позднем этапе. Если майнеры коммутируют свое аппаратное оборудование каждый раз при обнаружении блока RSK, они соревнуются за получение вознаграждения за полный блок RSK. При позднем коммутировании и майнинге после получения советов, они создают ростовщиков и получают часть вознаграждения за блок. В противном случае они теряют все объекты, потому что система DECOR+ выплачивает вознаграждение ростовщикам и правило GHOST пересчитывает ростовщиков в виде обычных блоков и обеспечивает наилучший чейн. Эффективность майнинга BTC, таким образом, повышается до максимума.

Согласно нашим ожиданиям, период хэшинга RSK будет ниже 50 % от суммарного хэшинга BTC. Это могло бы сделать систему уязвимой к 51 % атак, где остальной хэшинг превосходит существующий хэшинг RSK при атаке двойной траты.

Для предотвращения подобной ситуации RSK включает федеративные пункты для майнинга блоков PoW. Федеративные пункты подписаны членами Федерации, и клиенты могут использовать большинство подписей для принятия наиболее верного решения о том, какой чейн лучший. Также RSK располагает протоколом действий в исключительных обстоятельствах, при котором если майнинг опускается ниже 5% от хэшинга, Федерация получает возможность создать подписанные блоки. По умолчанию клиенты прекращают использовать федеративные пункты, если при хэшинге Roostock, превышающем 66% от максимального хэшинга BTC, наблюдается сложность в лучшем чейне и комиссии, выплачиваемые в блоке, выше или равны среднему вознаграждению за блок Биткойн.

Платформа RSK будет запущена в рамках федерации широко известных и уважаемых в сообществе участников. Каждый участник определяется по публичному ключу к схеме контроля подписей. Федерация в состоянии добавлять или исключать участников, используя встроенную систему голосования, хотя эти действия могли бы потребовать большего процента голосов участников.

Цель основателей RSK состоит в том, чтобы сеть RSK побуждала к объединенному майнингу. Однако RSK устойчива к дефициту объединенного майнинга, поскольку Федерация автоматически ориентируется на защиту сети в случае дефицита.

Основные характеристики:

- 1-дневный срок вознаграждения за майнинг.
- Пункты проверки федеративных участников
- Пункты проверки с встроенным кодом в период начальной загрузки.
- Отсутствие потерь эффективности майнинга Биткойнов, ожидаемых в случае объединенного майнинга (менее 0,1 % при немедленном коммутировании и 0 % при позднем коммутировании)

Быстрые платежи и сеть с низким значением задержки

Мы стремимся сделать RSK лучшей платежной сетью. Существует несколько решений для быстрой обработки платежей:

- Использование безконкурентного выбора блоков (например, Hyperledger, Ripple, системы с замкнутым контуром)

- Использование веерных сетей (например, протокол Lightning Network для биткойна)
- Использование высоких показателей для блоков PoW

Звездообразные сети добавляют новые центральные узлы и требуют полной адаптации клиентских кошельков к совершенно новой модели оплаты. Хотя такое решение можно легко реализовать в RSK, его нельзя назвать системой, которая изначально предназначена для быстрых платежей. RSK использует протоколы DECOR+ и FastBlock5, которые позволяют создавать блок через 10 секунд, что не создает стимулов для централизации майнинга, то есть не поддерживает эгоистичный майнинг и одновременно стимулирует работу.

Основные характеристики:

- интервал между блоками составляет 10 секунд;
- протокол двухступенчатого распространения блоков (2SBP);
- протокол подталкивания пропущенных транзакций (PMT);
- Полное распространение по сети последних конкурирующих блоков позволяет предотвратить эгоистичный майнинг и снизить скорость устаревания блоков.
- Эвристическая процедура отложенного включения транзакций (DTI). Транзакции задерживаются на 5 секунд в очереди блочных транзакций каждого майнера, чтобы обеспечить максимально быструю проверку блоков, поскольку эти транзакции уже присутствуют в пулах каждого узла сети.
- Новая сетевая команда для распространения заголовков блоков с приоритетом немедленной обработки.
- Новая сетевая команда для распространения списка хэшей блока транзакций сразу после распространения заголовка блока.
- Эвристическая процедура майнинга на непроверенных блоках (MUB). Майнинг на основе заголовков блоков с непроверенными транзакциями с 5-секундным возвратом.
- Заголовки блоков помечаются, если у них нет транзакций (за исключением базы монет)
- Протокол двух приоритетных потоков для каждого соединения (2PSC). Новый транспортный уровень с разделением сообщений, который позволяет проводить два параллельных сеанса с различными приоритетами. Это позволяет отправлять заголовки блоков в ходе сеанса с высоким приоритетом и прерывать любое сообщение, передаваемое в ходе сеанса с низким приоритетом.
- Протокол оптимизации локального маршрута (LRO). Локальная оптимальная маршрутизация блоков на основе приоритетов равноправных систем. Локальная оптимальная маршрутизация транзакций на основе приоритетов равноправных систем
- Протокол DECOR+ для распределения награды между конкурирующими блоками.
- Протокол GHOST для цепного взвешивания.

Сравнение характеристик RSK

Мы сравниваем RSK с другими блокчейнами, и стараемся показать, что по сути RSK дает лучший технический выбор, не разрушая децентрализацию систем. Для оценки децентрализации используется инверсия стоимости запуска экземпляра с полным узлом.

Позиция	Биткойн	Ethereum	Factom	Counterparty	RSK
Среднее время подтверждения	10 минут	12 сек (GHOST)	1 минута (Федеративные сервера)	10 минут	10 сек (DECOR+GHOST)
Порог безопасности (из-за эгоистичного майнинга)	~30%	от 30 до 50%	~30%	~30%	50% (DECOR+GHOST)
Принцип Тьюринга для завершения смарт-контрактов	Нет	Да	Да	Плановый	Да
Добавляет ценность для Биткойн	-	Нет	Нет	Нет	Да (слитый майнинг)
Интеграция с биткойнами	-	Нет	Протокол наложения	Протокол наложения	Сайдчейн
Масштабируемость на основе вероятностной верификации и подтверждения мошенничества	Нет	Нет	Нет	Нет	Да
Клиенты SPV	Да	Да	Нет	Нет	Да
Блок реле основной цепи	Да	Нет	Да	Да	Да
Встроенная поддержка пользовательских структур доступа	Да	Нет	Да	Нет	Да
Встроенная поддержка пользовательских схем подписи	Нет	Нет	Нет	Нет	Да
Простая интеграция с аппаратным кошельком	Нет	Да	Нет	Нет	Да
Гарантия безопасности	Майнеры SHA256D	Майнеры Ethash	Майнеры SHA256D + Federation	Майнеры SHA256D	Слитные майнеры SHA256D + Federation
Конфиденциальные транзакции	Нет	Через контракт	Через внешнюю программу	Нет	Планируется встроенная поддержка с использованием протокола AppeCoin
Уникальный идентификатор транзакции	Нет (пластич.)	Да	Нет	Нет	Да
Масштабируемость [tps]	от 3 из 24	несвязанный	несвязанный	от 3 из 24	300 при запуске
Родной токен	BTC	ETH	FACTOID	XCP	BTC через двустороннюю привязку

Предварительный просмотр технологии мгновенных платежей

С момента появления биткойна наблюдается тенденция к уменьшению интервалов подтверждения транзакций с криптовалютами на основе цепочки PoW. Сначала появился Bitcoin с 10-минутным интервалом, затем LiteCoin с интервалом 2,5 минуты, DogeCoin — 1 минута, QuarkCoin — 30 секунд и Ethereum — 12 секунд. Каждая новая криптовалюта немного сокращает этот интервал, но очень немногие программисты на самом деле понимают, что это значит. Для понимания того, как интервал между блоками влияет на стабильность и возможности криптовалютной сети, необходимо учитывать несколько факторов. Прежде всего, наиболее важным фактором, влияющим на жизнеспособность коротких интервалов подтверждения транзакций, является количество сгенерированных устаревших блоков. Два других фактора в основном влияют на скорость устаревания блоков: протокол распространения блоков и время распространения блоков между главными майнерами. В RSK мы тщательно проанализировали эти факторы и создали модель для проверки производительности, удобства использования и безопасности сети. В этом разделе мы рассмотрим новые протоколы, которые используются в RSK для снижения скорости устаревания блоков.

Протокол DECOR+

В биткойне, когда два или более майнера разрешают блоки на одном уровне, возникает явный конфликт интересов. Каждый конкурирующий майнер хочет, чтобы его блок был выбран остальными майнерами в качестве конечного блока лучшей цепи, в то время как остальным майнерам, как правило, не важно, какой блок будет для этого выбран. Однако все оставшиеся честные майнеры и пользователи предпочли бы, чтобы все выбирали один и тот же конечный блок, потому что это уменьшает вероятность естественного разворота. Идеальное решение в этом случае — стимулировать конкурирующих майнеров также выбирать один и тот же родительский блок, поэтому в протоколе DECOR+ используются экономические стимулы для конвергентного выбора, который не требует дальнейшей конкуренции между майнерами. В протоколе DECOR+ также используется стратегия распределения вознаграждений, которая стимулирует экономическое решение конфликтов, чтобы:

1. Решение конфликта было детерминированным, когда все стороны имеют доступ к одной и той же информации о состоянии цепочки блоков.
2. Было выбрано решение, которое позволяет как конфликтующим, так и всем остальным майнерам получить максимальный доход.
3. На решение конфликта тратится совсем немного времени.

Протокол распространения блоков

Биткойн и Эфириум пересылают каждый блок, упаковывая в заголовок блока все транзакции, содержащиеся в блоке. Известно, что такая стратегия значительно упрощает анализ, однако негативно влияет как на задержку распространения блока, так и использование полосы пропускания, которую приходится удваивать. Майнеры биткойна частично решили эту проблему с помощью технологии Fast Relay Network: это централизованная магистраль, которая ретранслирует блоки в сжатой форме и обслуживается одним пользователем. Платформа RSK появилась уже после того, как эта технология была встроена в сетевой протокол, то есть параметры низкой задержкой вытекают из топологии сети и не требуют централизации.

Двухступенчатое распространение блоков (2SBP)

Блоки RSK отправляются в два этапа: на первом этапе отправляется только заголовок блока. На втором этапе отправляется список хэшей транзакций, входящих в блок. При использовании 2SBP пропускная способность канала удваивается, что позволяет хранить больше транзакций в каждом блоке. После получения каждым узлом заголовка блока и списка хэшей транзакций, связанный с этим заголовком, узел пытается реконструировать блок, чтобы полностью его проверить.

Протокол подталкивания пропущенных транзакций (PMT)

Поскольку каждый узел хранит хэши транзакций, объявленных его одноранговыми узлами, майнер тоже немедленно отправляет транзакции, включенные в блок, который, как он знает, отсутствует в пуле каждого одноранговового узла. Это полностью исключает необходимость повторного взаимодействия для запроса дополнительных транзакций. Отправка пропущенных транзакций до того, как их запросит одноранговый узел, является третьей фазой протокола 2SBP.

Эвристическая процедура отложенного включения транзакций (DTI)

Майнеры вносят только те транзакции, которые были получены более, чем несколько секунд назад. Это с высокой вероятностью гарантирует, что эти транзакции будут получены одноранговыми узлами до того, как блок будет добыт. Обратите внимание, что задержка транзакций отвечает интересам майнера, так как она уменьшает время проверки блока и, соответственно, уменьшает шансы конкурирующих блоков. Эта оптимизация не требуется, если в сети выполняется Эвристическая процедура майнинга на непроверенных блоках (MUB).

Прямое распространение заголовка блока (IBHP)

После получения заголовка обновленного блока узлы пересылают заголовок блока перед проверкой транзакций или достоверности блока, проверяя во время пересылки только PoW и высоту блока. Это позволяет распространить заголовок по сети менее чем за секунду.

Протокол двух приоритетных потоков для каждого соединения (2PSC)

Каждое сетевое соединение включает два логических двунаправленных потока с двумя различными приоритетами. Поток с высоким приоритетом используется для немедленной отправки заголовка блока, даже если в потоке с низким приоритетом отправляется сообщение с более низким приоритетом.

Эвристическая процедура майнинга на непроверенных блоках (MUB)

Узлы могут начать майнинг пустого блока поверх заголовка, даже если транзакции отсутствуют в течение фиксированного срока. По истечении этого срока они возобновляют майнинг на любом блоке, который был добыт раньше. Такие пустые блоки уменьшают эффективную пропускную способность канала и хранение данных в цепочках блоков, однако моделирование показывает, что если используется DBI,

количество создаваемых пустых блоков и пространство, необходимое для хранения пустых блоков и сокращения TPS, невелики.

Протокол оптимизации локального маршрута (LRO)

Для уменьшения количества устаревших блоков важно уменьшить задержку в передаче между майнерами. Сеть RSK динамически оптимизируется, чтобы уменьшить задержку в передаче и определить приоритеты трафика между майнерами. Другими словами, RSK встраивает быструю ретрансляцию в одноранговую сеть, расширяя протокол с помощью геолокации и оптимизации локальных маршрутов. Пересылка блоков между майнерами является критически важным каналом для распространения блоков, поэтому играет важную роль в организации одноранговой сети. Существование не майнерских сетевых узлов в одноранговой сети на критически важном канале, как правило, увеличивает скорость устаревания блоков. Узлы майнеров (например, конечные пользователи или узлы мониторинга) в критически важном канале могут выступать в роли майнеров только в качестве слабых переходов при обезличивании. Чтобы создать критически важные каналы только для решений локальных узлов, расстановка приоритетов для таких узлов выполняется с помощью протокола LRO. Этот протокол использует динамическое встраивание ориентированного ациклического графа (DAC) в случайную топологию сети RSK, где этот граф позволяет оптимально соединить майнеров.

Повторное использование сети майнинга биткойна

Централизованная сеть майнинга, которая использует большие пулы, имеет тенденцию генерировать гораздо меньше устаревших блоков, чем полностью распределенная топология майнинга. Поэтому в отношении быстрых платежей криптовалюты на основе SHA-256D PoW имеют преимущество перед не криптовалютами на основе PoW, которые не поддерживают ASIC.

Реальная топология сети

Структура биткойна предполагает, что сеть похожа на случайный граф, имеющий среднюю исходящую и входящую ступени. Хотя фактически это далеко от истины, сетевые узлы принимают локальные решения, чтобы избежать формирования географических кластеров (по крайней мере, для внешних соединений). Это не лучшая топология для распространения блоков. Лучшая топология для распространения блоков должна в первую очередь обслуживать майнеров, поощряя прямые соединения между ними или ускоряя маршрутизацию блоков. Кроме того, основная цепь между майнерами помогает заметно уменьшить количество устаревших блоков. Такое решение было предложено сети биткойна для повышения устойчивости к атакам. RSK использует эвристическая процедура LRO для создания основной динамической цепи майнера без затрат на его аутентификацию, обеспечение конфиденциальности, раскрытие IP-адресов и, возможно, связанные DoS-атаки.

Функция PoW верификации времени

Оценка в SHA-256 проводится очень быстро, поэтому время проверки PoW биткойна ничтожно мало. Напротив, оценка скрипта PoW может занимать от 3 до 30 миллисекунд, в зависимости от выбранных параметров («сопротивления» GPU или ASIC). Чтобы защитить сеть от спама и DoS-атак, каждый узел должен проверить PoW блока перед повторной пересылкой его заголовка, таким образом задержка при проверке умножается на количество переходов в критически важном канале между майнерами.

Сетевой стек клиента

Как только узел получает заголовок блока, лучшее, что он может сделать, чтобы сократить появление устаревших блоков — это как можно быстрее переслать полученный заголовок. Это означает, что все остальные действия узла необходимо приостановить или отложить. Структура RSK позволяет немедленно отменять операции с низким приоритетом и делать повторные попытки. Чтобы разрешить немедленную пересылку заголовков, сетевой стек не блокирует клиента в процедурах проверки транзакций или других служебных действиях, например, реорганизации цепочки. Для этого используется клиент RSK, который позволяет динамически назначать приоритеты потоков, чтобы повысить значимость потока, который получил заголовок блока.

Потери для блоков

Заголовки блоков в большинстве криптовалют имеют небольшой размер (~100 байт), поэтому отправка заголовка (по сравнению с размером всего блока) не создает значительных потерь. Заголовок RSK больше, но потери из-за заголовка блока оказывают заметное негативное влияние на время его распространения, поскольку сетевой MTU низкого уровня обычно составляет 1500 байт, что превышает размер заголовка блока.

Моделирование

Мы провели моделирование распространения блоков на основе дискретной модели событий, специально созданной для этой цели. Эта модель имитирует взаимодействие между небольшим набором топ-майнеров, каждый из которых представляет собой случайный график, где расстояние между ними близко к среднему расстоянию между узлами в сети. Мы использовали не наихудший вариант, поскольку топ-майнеры заинтересованы в поддержании хороших связей, поэтому мы предполагаем, что майнеры будут работать не хуже, чем со средними показателями. Мы смоделировали создание блока в одной из точек и его распространение во все остальные точки майнинга. Результаты моделирования показывают работу платформы RSK с интервалом между блоками 5 секунд и 300 транзакций в секунду (в настоящее время интервал между блоками составляет 10 секунд). Главный результат моделирования заключается в том, что транзакция принимается с вероятностью 99,98% (вероятность разворота 0,02%) до истечения 20,35 секунд. Обратите внимание, что в указанной вероятности разворота не учитывается, что замещающая параллельная ветвь также может содержать удаленную транзакцию, поэтому на практике вероятность может быть ниже.

Безопасный слитный майнинг

Слитный майнинг — это метод, который позволяет майнерам биткойнов одновременно добывать другие криптовалюты с почти нулевыми предельными издержками. Та же инфраструктура майнинга и настройки, которые они используют для майнинга биткойнов, одновременно используются для майнинга RSK. Это означает, что, поскольку RSK платит дополнительные комиссионные за транзакции, это стимулирует слитный майнинг. Однако это также означает, что стоимость атаки на сеть с использованием накачки или параллельных цепочек здесь ниже, чем стоимость атаки для неслитных криптовалют. В RSK используются определенные средства защиты от атак на начальном этапе загрузки:

- Федеративные контрольные точки: Клиенты RSK ожидают создания контрольных точек, которые будут подписаны участниками Федерации. В состав Федерации войдут биржи и другие участники с высокой степенью защиты, заинтересованные в успехе платформы. Узлы будут использовать федеративные контрольные точки для обнаружения атак Сибил и информирования об этом пользователей.

- Срок погашения добытых монет: срок погашения монет составляет 24 часа, что немного выше, чем в биткойне. Увеличение времени созревания монет снижает стимулы для атак по схеме накачки и сброса.

- Контрольные точки, встроенные в исходный код

Конфиденциальность транзакций

Сама по себе платформа RSK не обеспечивает более высокий уровень защиты конфиденциальности транзакций, чем биткойн, полагаясь на использование псевдонимов. Тем не менее, виртуальная машина RSK является полной машиной по Тьюрингу, поэтому позволяет безопасно внедрить технологии обезличивания, такие как CoinJoin или AppeCoin, без участия третьих сторон.

Безопасность

Слитный майнинг не получил широкое распространение для альткойна, потому что в течение начального периода начальной загрузки криптовалюты он позволяет крупным пулам майнинга биткойнов разрушать новые криптовалюты с помощью атак 51%. Для снижения этого риска в платформе RSK внедряются федеративные контрольные точки, как безопасный способ начальной загрузки платформы. Также для RSK с минимальной мощностью хэширования, эквивалентной 30% мощности хэширования биткойна. Фонд RSK будет следить за состоянием сети и использовать свою систему оповещения для информирования пользователей и защиты сети от атак методом возврата к старой версии.

Масштабируемость

В своем нынешнем состоянии сеть RSK может выйти далеко за пределы Биткойна.

Для оплаты RSK требуется пятая часть размера стандартного платежа в биткойнах, а полезная нагрузка блока за интервал времени в 8 раз выше, чем у биткойна. Также RSK предоставит пользователям несколько схем подписи на выбор: ECDSA, Schnorr и Ed25519. Последняя схема, в целом, является в несколько раз более производительной, чем кривая биткойна ECDSA.

При прочих равных условиях, RSK использует в среднем на 50% меньше пропускной способности, чем биткойн, поскольку блоки не содержат данных транзакций, а только ссылаются на ранее известные транзакции. Использование хранилища данных и загрузку пропускной способности можно дополнительно уменьшить с помощью вероятностной верификации и подтверждения мошенничества.

Вероятностная верификация и подтверждение мошенничества

Стоимость владения полным узлом является основным фактором, который влияет на степень централизации криптовалюты. Чем выше стоимость, тем выше централизация. Однако мы считаем, что максималистский подход к децентрализации приводит к тому, что криптовалюта не сможет стать глобальной платежной сетью. Таким образом эти две цели противоречат друг другу. Биткойн уже предоставляет собой высоко децентрализованную сеть, поскольку ограничения размера цепочки блоков недостаточно, чтобы обеспечить участие большинства отдельных пользователей. Это позволяет слайдчейну RSK повысить масштабируемость за пределами биткойна, при этом используя сеть биткойн в качестве защиты от централизации контроля над валютой.

Мы считаем, что можно сбалансировать участие третьих сторон, сетевых узлов и самопроверку, поэтому приглашаем пользователей найти собственный, наиболее удобный вариант. Платформа RSK позволяет узлам хранить и проверять подмножество полной цепочки блоков, чтобы снизить стоимость узла. Это делается с помощью вероятностной верификации и подтверждения мошенничества. Вероятностная верификация — это метод, при котором (частичный) узел случайным образом выбирает, какие блоки он будет проверять, и считает оставшиеся блоки правильными, при условии соблюдения некоторых условий: после создания прошло определенное время, были добавлены некоторые подтверждающие блоки, было установлено сетевое подключение, отсутствуют подтверждения мошенничества и, возможно, были переданы сообщения с определенных авторитетных контрольных точек. Подтверждением мошенничества являются блоки, помеченные как «мошеннические». Когда узел получает подтверждение мошенничества, он проверяет, был ли блок с той же высотой локально принят (но не проверен), и если это так, он проводит проверку блока. Если блок оказывается недействительным, соответствующим образом реорганизуется лучшая локальная цепочка. Стоимость трансляции подтверждения мошенничества высока, поскольку они включат доказательства работы. Узел, который получает подтверждение мошенничества от одноранговой узла, банит мошеннический одноранговый узел. При необходимости узлы запрашивают первоначальное подтверждение работы от одноранговых узлов, чтобы предотвратить дешевые DoS-атаки, которые используют скомпрометированные IP-адреса. Майнеры (как PoW, так и Федеративные) должны быть полными узлами, поэтому злоумышленник, который удерживает данные блока (но передает его заголовок), не влияет на лучшую цепочку, поскольку майнеры быстро отбросят такой мошеннический блок.

Выводы

Платформа RSK представляет собой результат четырехлетних усилий по усовершенствованию технологии блокчейна. Она позволит экосистеме криптовалют пользоваться лучшими возможностаями программируемых денег и платежей при одновременном увеличении стоимости биткоина (валюты).

Это позволит разработчикам по всему миру создавать личные и корпоративные децентрализованные решения для самой защищенной сети во всем мире с низкой стоимостью транзакций, которые соответствует широкому спектру человеческих потребностей.

Кроме того, платформа позволит майнерам биткойна принимать участие в работе рынка смарт-контрактов, что значительно повышает ценность сферы майнинга и обеспечит ее долгосрочную устойчивость.

Это будет способствовать расширению базы майнеров, укрепляющих безопасность сети Биткойн.

В целом, платформа позволит развить децентрализованную, мгновенную и недорогую финансовую систему, которой смогут пользоваться три миллиарда человек по всему миру, которые оказались за бортом действующей системы банковских услуг и испытывают финансовые затруднения.

Основная команда RSK