Система tBTC: децентрализованная погашаемая криптовалюта, созданная на основе вычислительной платформы Эфириум и обеспеченная Биткоином

Внимание! Представленный документ должен максимально точно описывать tBTC v1. Замечания о неточностях приветствуются. Их можно направить на канал tBTC Discord или отметить в качестве спорных в системе отслеживания ошибок tBTC.

Аннотация

Система tBTC – это проект децентрализованного, погашаемого по соотношению «1 к 1» токена, привязанного к биткоину. Другими словами, это блокчейн. Представленный проект может быть воплощен на главном сервере хранения данных, в рамках которого разрешены смарт-контракты (электронные алгоритмы для автоматизации процессов исполнения контрактов в блокчейне). Такой сервер поддерживает стандартные токены и подмножество функций, которые необходимы для подтверждения определенных свойств операций, совершаемых с Биткоином.

Представленная работа, в частности, предполагает, что в качестве основной вычислительной платформы выступает Эфириум. Привязка криптовалюты выполняется путем применения метода связанной, соподчиненной связи, в которой случайно выбранное подмножество более широкой сети подписывающих узлов создает основу для индивидуальных депозитов. Последние запрашиваются пользователями для выпуска в обращение TBTC-токенов в рамках основной платформы.

Выбранные стороны умного контракта (подписанты) используют пороговый алгоритм ECDSA для создания Биткоин-кошелька, к соответствующему личному ключу которого не будет иметь доступа ни один подписант. Также они используют облигацию в количестве суммы родных токенов основной платформы (для Эфириума это Эфир – ETH). Это обеспечивает честное поведение подписантов в рамках системы при наличии потери их облигаций в случае недобросовестности или обесценивании залогового обеспечения.

Смарт-контракт, заключенный в рамках основной платформы, является связующим звеном с жизненным циклом депозита, включая его открытие, гарантии обеспечения, обман со стороны подписанта (мошенничество) и погашение.

Погашение позволяет депозиту вернуть удержанные BTC в цепи биткоина и осуществлять выплаты подписантам. Дополнительные механизмы предназначены для того, чтобы должным образом стимулировать установленные сроки депозита, чтобы гарантировать получение подписантами вознаграждения и позволить им выйти из контракта в случае угрозы срыва гарантий обеспечения.

Обзор

Условные обозначения

Ключевые слова этого документа «НЕОБХОДИМО», «НЕДОПУСТИМО», «ОБЯЗАТЕЛЬНЫЙ», «СЛЕДУЕТ», «НЕ СЛЕДУЕТ», «РЕКОМЕНДУЕТСЯ», «ВОЗМОЖНО» И «НА УСМОТРЕНИЕ СТОРОН» должны толковаться так, как это указано в рабочем предложении RFC 2119.

Примечание о наименовании

Описываемая система, будучи цельным образованием, называется «tBTC». В представленном документе, как и во всех связанных с ней проектах, взаимозаменяемый токен, обеспеченный Биткоином, называют «TBTC». Это делают для того, чтобы разграничить понятие с описанным проектом. Такой подход к наименованиям также отображен в контракте Эфириум ERC-20 token.

Дальнейшие обсуждения по этому поводу можно найти в соответствующем разделе сервиса GitHub.

Проделанные работы

Об усилиях, которые ранее были приложены для создания привязки в кросс-чейне Биткоина, хорошо известно. Привязка Биткоина желательна для функциональности сайдчейнов (методов разделения блокчейнов), а также масштабируемости расширений для модернизированного основного блокчейна Биткоина. Ввиду повышенного интереса к сайдчейнам, большое количество подходов привязанного Биткоина предшествуют возникновению основной цепи Эфириум.

Централизованный, доказуемый, погашаемый

На сегодняшний день существует два решения, которые обеспечивают централизованные привязки, полагающиеся на доверенных третьих лиц и основанных на вариациях моделей с федеративной привязкой.

Федеративная привязка предполагает наличие кошелька с мультиподписью, который используется для надежного хранения биткоинов.

Другой блокчейн в таком случае выпускает токены, которые символизирует упомянутые биткоины. Участники такой «множественной подписи» в цепи Биткоин должны совершить действия по утверждению сайдчейна. При этом выпущенные токены могут быть выведены из оборота и сожжены только в том случае, если изъятие биткоинов будет соответствовать установленным правилам сайдчейна.

Liquid – сайдчейн для покупки и продажи большого количества биткоинов, разработанный компанией Blockstream, - выступает в качестве сети расчетов, основанной на сайдчейне с федеративной привязкой. Биткоин хранится в кошельке с множественной подписью, составленной 15 подписантами, включая участников обмена и сайдчейна Liquid, предварительно проверенных компанией Blockstream. Указанные подписанты объявляют сайдчейн действительным в соответствии с подходом, который сама компания называет Strong Federation (Крепкая Федерация). Его особенность состоит в том, что большинство голосует за подписание блоков и соглашается утвердить возможности выхода в основную цепь.

WBTC – это обеспеченный биткоином токен ERC-20, который используют для похожих целей. Токен является частью более грандиозного проекта под названием «Wrapped Tokens».

Цитата из рекламной брошюры «Wrapped Tokens»: *«Wrapped Tokens исходит из централизованной модели, но, вместо полного полагания на только одну организацию, здесь предусмотрена ориентация на консорциум организаций, выполняющих в сети разные функции».*

Консорциум WBTC голосует за добавление или удаление членов из состава попечителей, которые управляют запасами токенов. Каждый попечитель работает с биткоин-кошельком с мультиподписью и контролирует все ключи доступа. Попечители способны перемещать вверенные им биткоины по собственной воле, а также ответственны за выпуск в обращение WBTC на основе платформы Эфириум.

Совместная деятельность попечителей напоминает традиционную федеративную привязку. Тем не менее, вместо необходимости подписания большинством соглашения об изъятии биткоина, один член консорциума может изъять их долю из резервов биткоина в любое время.

Система компромиссов

Такой подход, как взаимные уступки, имеет несколько преимуществ. Это:

1. Эффективность привязки Биткоина к другим блокчейнам.
2. Легкость проверки и контроля над обеспечивающими запасами в любое время.
3. Простота механизмов, что снижает вероятность операционного сбоя, а также общую стоимость эксплуатации.

Тем не менее, все это – отрицательные стороны. Наиболее вероятный исход – введение доверительной модели, несовместимой с биткоином.

Необходимо, чтобы попечители были в полной мере доверенными – и как группа, как модель компании Liquid, и как индивидуальная единица, в соответствии с моделью Wrapped Tokens.

Действуя злонамеренно, попечитель может заблокировать операции по выводу и в некоторых случаях – вступить в заговор и скрыться вместе со средствами. Кроме того, правительства, хакеры и прочие внешние силы могут вынуждать попечителей вмешиваться во вверенные им запасы, преследуя при этом отнюдь не благие цели.

Децентрализованный, искусственный, не подлежащий погашению

Альтернативный подход к централизованной привязке – создание децентрализованного искусственного актива. Один из подходов такого рода, который имел популярность на платформе Эфириум, - система Maker’s Dai stablecoin.

Dai – это токен, искусственно привязанный к курсу доллара США. Другими словами, это криптовалюта, стоимость которой относительно стабильна по отношению к USD. Эфир (одна из цифровых криптовалют) содержится в резервах. Если добавить к этому надежный курс валют и различные механизмы стабилизации, то можно получить спривязку даже в неблагоприятных условиях.

Maker, будучи платформой для «умных контрактов» в криптовалюте Ethereum, пока не запустила искусственный аналог биткоина. Несмотря на это, сам факт достижения привязки криптовалюты Dai свидетельствует о том, что с помощью такого подхода может легко создать продукт, близкий по особенностям к биткоину.

Система компромиссов

Основное преимущество искусственной привязки биткоина – ее гибкость. Благодаря искусственному происхождению нет необходимости в соблюдении правил, которые управляют привязанными активами, к худшему это или к лучшему.

Например, искусственный актив может эффективно «взвинчивать» стоимость основного актива, что, в свою очередь, может быть желательным действием для некоторых финансовых систем. Это позволит прямо достигать цели в стремлении сделать валюту «твердой».

Кроме возможности применять сеть Maker’s повторно, запуск такой искусственной валюты имеет и другие риски. Так, искусственная привязка к таким волатильным активам, как биткоин, обеспеченный таким же волатильным, диверсифицированным активом, состоящим полностью из эфира, является довольно опасной комбинацией.

Цели проекта

Цель системы tBTC – создание протокола ERC-20 token, который поддерживает наиболее важное свойство Биткоина – его статус «крепкой валюты».

Для того, чтобы поддерживать статус «крепкой валюты» относительно активов, которые составляют основу депозитов BTC, система tBTC должна оставаться:

1. Устойчивой к цензуре и захватам путем дружественных и недружественных юрисдикций.
2. Устойчивой к инфляции. Токен, основанный на биткоине, может быть выпущен в обращение только после того, как будет доказано наличие обеспечивающего BTC-депозита.
3. Устойчивой к давлению. Существование системы tBTC не должно допускать в кросс-чейн транзакциях распространения дополнительного искусственно созданного биткоина. Мы не можем запретить кому-либо прекратить запуск искусственной валюты, но искусственным образом расширяющиеся запасы биткоина не являются целью этого проекта.
4. Функционирующей без посредников – в том же смысле, что и Биткоин. Единственным исключением может быть минимальное участие подписантов, которое требуется для обеспечения безопасности сети. Их роль подобна роли майнеров в системе Биткоина.
5. Погашаемой. Способность свободно торговать скриптами по обеспечивающему депозиту – это та черта, которая отличает обеспечиваемую валюту от фидуциарных денег (не обеспеченных чем-либо). Обеспечение системы tBTC всегда основывается на равном количестве внесенных BTC. Это значит, что для того, чтобы выпустить один токен в обращение, нужно изъять из обращения 1 BTC.

В совокупности перечисленные особенности обеспечивают мощную привязку к обеспечению в пределах цепи, а также наиболее близкий к «крепкой валюте» статус, которого только мог бы достичь актив, привязанный к биткоину.

Примечательно, что эти особенности не требуют искусственной привязки к цене, как это наблюдается в среднестатистических стабильных криптовалютных проектах. Вместо этого они требуют привязки к обеспечению в пределах цепей.

Развитие интуиции: простой протокол с участием единственного подписанта

Чтобы понять, каким образом мы можем развить протокол и создать токен, который удовлетворял бы представленным требованиям, стоит рассмотреть простой вариант. При заданных данных он мог бы теоретически выполнить возложенную на него задачу.

Представьте сторону офф-чейн (то есть находящуюся вне цепи), которую мы назовем Подписантом (Signer). Также есть смарт-контракт в сети Эфириум, который выполняет роль интерфейса протокола ERC-20 и который мы будем упоминать как Привязанный Биткоин (PeggedBitcoin), с тикером токена PBTC (привязанным к курсу биткоина токеном). Также есть еще один контракт с разрешением выпускать и сжигать PBTC, который мы назовем запасом привязанного биткоина (PeggedBitcoinReserve).

Другой офф-чейн участник, депозитор (Depositor), желает выпустить в оборот токен на основе контракта PeggedBitcoin. Депозитор делает запрос в PeggedBitcoinReserve о принятии взноса в размере 1 BTC . PeggedBitcoinReserve ожидает, пока подписант не подтвердит и не предоставит новый адрес расположения биткоина, а также пока не произойдет депонирование 150% обеспечения стоимости депозита, выраженного в Эфире, в PeggedBitcoinReserve. Депозитор вносит 1 BTC на новый биткоин-адрес и предоставляет доказательства этого в PeggedBitcoinReserve. PeggedBitcoinReserve в свою очередь выпускает в оборот 1 токен PBTC, отправляя 0,99 Депозитору и 0,01 – Подписанту в качестве вознаграждения.

Изъятие средств происходит в обратном порядке: любой участник транзакции может отправить 1 токен PBTC в PeggedBitcoinReserve, используя биткоин-адрес. Подписант выплачивает этому биткоин-адресу 1 BTC за вычетом каких-либо комиссионных сборов за совершение операции, а также предоставляет доказательства совершенной оплаты в PeggedBitcoinReserve. PeggedBitcoinReserve, в свою очередь, сжигает оставшийся 1 PBTC, соблюдая соотношение «1 к 1» и основываясь на токене PBTC. В данном случае Подписант может свободно изымать соответствующее обеспечение из PeggedBitcoinReserve.

Недостатки

Хотя представленный простой проект на первый взгляд кажется привлекательным, его разработчики все же упустили несколько достаточно сложных вопросов. Во-первых, это достаточное Bitcoin-подтверждение действительности оплаты в виртуальной среде взаимодействий умных контрактов от Эфириума (EVM). Во-вторых, это реализация надежного курса.

Кроме того, описанный проект основан на достаточно небезопасном, уязвимом решении о попечительстве.

Прежде всего, протокол полагается на единственного подписанта. Если стоимость вклада когда-либо превысит стоимость обеспечения, сделанного Подписантом, то в таких условиях ничто не сможет остановить Подписанта, решившего изъять BTC и выйти из депозита. Подписант также может принять решение (как самостоятельно, так и под давлением) о запрете отдельных изъятий, что убивает всякую надежду на сопротивление цензуре или конфискации.

Следующий по важности факт заключается в том, что протокол основывается на единственном виде кошелька – это **hot wallet.** Речь идет о кошельке с активным онлайн-соединением, то есть о непосредственно подключенном к интернету. Поскольку рыночная капитализация токена PBTC с высокой вероятностью возрастет, риск взлома такого кошелька значительно повышается.

И, наконец, в системе протокола не предпринимаются никакие действия, направленные на ограничение возможности сбоев. Если возникают проблемы с единым депозитом или изъятием, то они могут нанести значительный урон целой системе обеспечения PeggedBitcoin, тем самым блокируя все последующие депозиты и возможность изъятия активов.

Структура системы: проектирование надежного протокола со множеством кошельков и подписантов

Оставшаяся часть представленного документа посвящена более подробному ознакомлению с протоколом, который работает с указанными недостатками системы, предоставляя надежные активы, обеспеченные биткоином, на Эфириуме.

Это означает, что указанный протокол должен иметь структуру, допускающую наличие структуры, основанной на концепции мультикошельков со множеством подписантов, находящихся в разных частях мира. Это позволит исключить возможность единой точки отказа, которая может вывести из строя всю систему.

Кроме того, данный протокол должен уравновешивать вторичные эффекты, вызванные представленными требованиями, и детали, которые мы упустили в примере о единственном подписанте. К таким деталям мы отнесем:

- платежи с участием нескольких подписантов;
- более сложную систему облигаций;

- подход к обнаружению подписантов с обесцененными обеспечению, а также принципы работы с ними;
- надежное управление сбоями в системах обоих цепей.

Некоторые компоненты, обязательные для функционирования данного протокола, описаны за рамками представленного документа и будут приниматься во внимание. В частности, мы будем предполагать наличие следующих элементов:

- хорошо распределенного рабочего токена для выбора подписантов;
- случайного узла-«маяка» для выбора подписантов;
- эффективного протокола распределенной генерации ключей на кривой secp256k1, используемой в системе биткоинов;
- эффективного многостороннего порогового протокола ECDSA на кривой secp256k1.

Все перечисленные элементы исполняются протоколом от Keep network. Их важность описана в последующих разделах статьи.

Структура системы состоит из таких элементов:

- создание депозитов и выбор подписантов;
- выпуск облигаций и курс цен;
- выпуск токенов в оборот;
- вознаграждение подписантов;
- подписание;
- сбои в функционировании кошелька;
- погашение;
- управление.

Депозиты

Обзор

Система tBTC обеспечивает механизм для создания токенов (TBTC) на основе главной платформы, которая не имеет отношения к биткоину (для tBTC v1 такой основной платформой являлся Эфириум) и которая обеспечивается биткоином по принципу «1 к 1». Стороны, заинтересованные в выпуске токенов TBTC в оборот, отправляют в систему запрос об их обеспечении адресом биткоин-кошелька.

В ответ система выбирает несколько подписантов, которым поручается создание открытой или закрытой пары асимметричных ключей, а также их внедрение в систему. Заинтересованная сторона становится депозитором путем отправления биткоин на кошелек (количество требуемых биткоинов обсуждается отдельно в разделе о лотах). Депозит невозможно обслуживать бесплатно, так как он требует от подписантов создания облигаций на основе ETH. Это гарантирует правильное поведение в рамках системы (более подробно узнать об этом можно в разделе об экономике вкладов). Чтобы покрыть указанные издержки, депозит оплачивается средствами в виде вознаграждения подписантов, которые распространяются на установленный срок исключительного погашения депозита для его владельца. Этот вопрос обсуждается отдельно в разделе о сроках вклада.

Каждый из описанных шагов отображен в схеме (см. ниже) и обсуждается в последующих разделах документа.

https://docs.keep.network/tbtc/initiate-deposit.svg

Запрос на депозит

Отправной точкой для приобретения токена TBTC является создание *запроса на вклад*. Этот запрос выступает в качестве транзакции по типу умного контракта на основном сервере системы tBTC's и указывает на то, что отправитель требует кошелек, обеспеченный группой подписантов, и названный депозитом. Поскольку группа подписантов в любом случае требует издержек, депозит запрашивает небольшую оплату, выраженную в родных токенах основной платформы, в целях покрыть расходы на создание группы подписантов. Эта оплата может быть возмещена, если группе подписантов не удается создать и выпустить открытый ключ по истечении срока, отведенного на эту процедуру.

Выбор подписанта

После получения запроса на вклад происходит создание группы подписантов путем случайного выбора. Эти подписанты обеспечивают биткоин-кошелька. Это многосторонний процесс, который описан в схеме ниже.

https://docs.keep.network/tbtc/signing-group-creation.svg

Когда поступает запрос на создание группы подписантов, система tBTC запрашивает случайное число (которое в цепи также называют зерном) из надежной децентрализованной системы случайных узлов-маяков. Полученное в результате случайное число используется для случайного выбора членов группы подписантов из числа подходящих на такую роль участников. В конце концов, эти подписанты координируют протокол распределенного создания ключей, в результате чего образуется открытый ECDSA-ключ для группы. Он используется для создания адреса кошелька, который впоследствии выпускается на основной платформе. На этом этап выбора подписантов завершается.

Обязательства подписанта

Перед тем, как выбранные члены группы подписантов начинают выполнять обязанности по распределенной генерации ключа, они обязаны создать залоговое обеспечение, выраженное в родных токенах основной платформы. Подобное обеспечение требуется в нескольких случаях:

1. Для ликвидации депозитов, если они находятся под угрозой обесценивания.
2. Для наказания группы подписантов в случае, если ее члены подписывают неразрешенные части данных.
3. Для наказания группы подписантов в случае, если им не удалось создать подпись для системы в случае такой надобности.
4. Для обеспечения возмещения средств депозитору, если формирование группы подписантов по каким-либо причинам не удалось.

Во всех случаях, кроме последнего, изъятое долговое обязательство торгуется в токенах TBTC для того, чтобы компенсировать владельцу эквивалент его депозита.

Подписанты должны располагать достаточным числом залоговых обеспечений для того, чтобы обеспечить депозит. Только в этом случае они могут быть выбраны членами группы подписантов. Кроме того, залоговое обеспечение должно приобретаться путем вложения средств в ту же транзакцию, с помощью которой выбирают подписантов.

Более подробно вопрос о долговых обязательствах рассмотрен в соответствующем разделе.

Распределенная генерация ключа

Группа подписантов подвергается некоторым незначительным замечаниям, которые касаются распределенной генерации ключа. Протокол распределенной генерации ключа должен создавать следующие условия:

1. Группа подписантов, как единое целое, должна иметь *открытый ключ ECDSA*, который будет разделен на основном сервере и будет относиться к биткоин-кошельку, которым владеет группа подписантов.
2. Каждый член группы подписантов должен иметь долю в пороговом секретном ключе ECDSA, которая может использоваться для создания аналогичной доли для любых других транзакций, включая те, которые проводятся с участием кошелька группы подписантов.
3. Каждый участник группы подписантов должен быть способен скомбинировать пороговое число долей подписи от себя и других членов группы для того, чтобы создать утвержденную транзакцию и предоставить условия для ее выполнения от лица всей группы подписантов.

Создание депозита

Если в системе tBTC есть адрес кошелька, доступный для представленного запроса на внесение депозита, то депозитор может проводить операции с биткоином, отправляя BTC из контролируемого кошелька на адрес кошелька группы подписантов. После того, как транзакция успешно подтвердится в цепи биткоина, депозитор должен произвести транзакцию в рамках основного сервера. Это необходимо для того, чтобы доказать, что депозит был профинансирован.

Единственным связующим звеном между цепью биткоина и основной платформой является система tBTC, которая выступает в качестве комплекса смарт-контрактов на основном сервере. В данном случае проделанные депозитором биткоин-транзакции должны быть одобрены системой tBTC еще до того, как последняя позволит вкладчику поступать таким образом, как если бы он успешно перевел свои BTC на кошелек подписантов.

Если группа подписантов не может обеспечить открытый ключ в течение заданного периода, депозитор может уведомить о том, что это произошло в целях возврата обеспечений платежа, взятого из залоговых обеспечений, которые подписанты установили в качестве части процесса выбора группы подписантов.

Если подтверждение депозита не было получено по истечении указанного периода (период финансирования депозита), группа подписантов может уведомить о том, что это произошло в целях роспуска группы и возврата залоговых обеспечений ее участников.

Простые релейные системы

Чтобы подтвердить депозит, депозитор предоставляет доказательства того, что транзакция была совершена в действующем блоке биткоина с достаточным количеством накопленной работы. Доказательство проверяется смарт-контрактом SPV (упрощенная проверка платежей) на основной платформе. Более подробный обзор кросс-цепных SPV-систем и их характеристики безопасности содержится в соответствующем приложении.

Простые релейные системы передач – это обновленный вариант внутрицепной системы SPV, разработанной специально для tBTC. Их задача – извлечь выгоду из компактных и эффективных SPV-доказательств без сохранения состояния. В то же время они передают достаточно информации для предоставления каждому доказательству без сохранения состояния дополнительных гарантий своевременности.

Мы достигаем этого путем извлечения выгоды из сложности регулировки протокола Биткоина. В системе биткоина проводится проверка на возникающие сложности в каждом 2016 блоке, основываясь на временных метках первого и последнего блока за указанный период (в соответствии с ошибкой неучтенной единицы в программном клиенте Satoshi, один межблочный период исключается из процесса расчета сложности). Изменение предопределено и в допустимых пределах может быть установлено майнером последнего блока.

Релейная система транзакций не сохраняет каждый заголовок, использующийся для идентификации конкретного блока во всем блокчейне. Вместо этого она запоминает только небольшую часть заголовков, связанных с событиями регулировки сложности, а также ведет учет сложности для текущего периода 2016 блока. Упомянутая часть подтверждается ее объективным доказательством работы, так же, как и удостоверением в том, что сложность ее первого заголовка сопоставима со сложностью текущего периода в целом. Учитывается также, что изменения происходят на уровне ожидаемого коэффициента в данной части, а также что новые возникающие сложности соответствуют алгоритму регулировки в системе биткоина. Другими словами, релейные системы в блокчейне отслеживают только текущие сложности в системе Биткоина, однако не передают никакой информации о состоянии.

Обладание информацией о текущих сложностях позволяет предоставить основным SPV-доказательствам без сохранения состояния дополнительные, более мощные гарантии своевременности.

Любые только что созданные SPV без сохранения состояния должны включать описанную сложность в цепь его заголовка. Важно, чтобы эта сложность не стала преждевременно известна какому-либо участнику.

Майнеры, обладающие n-долей хэшрэйта (как правило, показатель n составит >= 2 в соответствии с допущением в 51%), имеют шанс 1/n на разрешение установки сложности. Таким образом, они имеют шанс 1/n на то, чтобы успешно предугадать ее степень за 2 недели (путем создания поддельных доказательств и последующей установки сложности, которая стала бы действительной).

В целом, это составит $1/n^t$ часть шанса на успешное предсказание периодов установки сложности t (2t недели) заранее. Таким образом, использование релейных систем создает более мощные условия безопасности для SPV-доказательств без сохранения состояния в условиях, когда проводится дополнительная проверочная манипуляция. Дело в том, что даже те объекты, которые имеют значительные ресурсы для добычи монет, имеют довольно урезанные шансы на создание поддельных доказательств.

Лоты

При создании депозита обязательно должен быть определен размер его лота. Система tBTC поддерживает управляемый комплекс доступных размеров лота (более подробно можно узнать в разделе об Управлении), гарантируя, что по крайней мере один из размеров лота для 1 BTC будет доступен. В v1 будут запущены 6 доступных размеров лота:

- 0.002 BTC;
- 0.01 BTC;
- 0.1 BTC;
- 0.2 BTC;
- 0.5 BTC;
- 1 BTC.

Стороны, подающие запрос на депозит, могут создавать его исключительно в одном из указанных размеров лота, при этом размеры лота позволяют выпускать только соответствующее им количество токенов TBTC. Если депозитор желает внести сумму в большем размере, чем позволяет максимальный показатель размера лота в системе, ему потребуется создать множество запросов на депозит и профинансировать множество депозитов.

В целях упрощения, все остальное, относящееся к рассматриваемой теме, далее упоминается с предположением о том, что депозиты в размере 1 BTC уже являются открытыми. Тем не менее,

все, что зависит от размера лота (например, размер вознаграждения подписантов), будет определено в виде стоимости, пропорциональной размеру лота.

Ограниченный размер лотов с максимально допустимым порогом позволит каждому вкладу обеспечиваться разными группами подписантов. Это не только упростит процесс внесения залоговых обязательств группами подписантов, но и повысит эластичность системы в отношении провалов со стороны группы подписантов, вне зависимости от того, являются ли они злонамеренными.

Ошибки при создании депозита

Система разработана таким образом, чтобы она могла работать с несколькими предопределенными размерами лотов в отношении всех депозитов, предоставленных в качестве системного параметра. Депозиторы при транзакции финансирования должны отправить точную сумму лота BTC, в противном случае их ожидает потеря средств.

Поскольку система не может заставить пользователей отсылать какую-либо конкретную сумму, идеальным вариантом для системы является аккуратная регулировка переплат и недоплат. В основном переплаты и недоплаты оказывают влияние на коэффициент обеспечения вклада. Система рассматривает переплаты и недоплаты в качестве неправильного поведения депозитора и адресует последнему сопутствующие расходы.

Переплата

Допущение переплат на конкретно взятом вкладе может стать причиной снижения залоговых обеспечений подписантов. При чрезмерном финансировании система принимает подтверждение финансирования, но выпускает в обращение TBTC строго в соответствии с установленным размером лота.

В рамках модели эффективного рынка чрезмерно финансированный депозит должен быть немедленно погашен депозитором в целях возвращения недостающего значения. Если депозитор вместо этого делает выбор в пользу выпуска TBTC из этого депозита, чтобы таким образом разблокировать его (более подробно смотреть в разделе о выпуске), депозит должен быть немедленно погашен другим участником системы, а погашающая сторона должна принять переплаченную сумму в качестве арбитража.

Пользователь, который предоставляет подтверждение финансирования для внесенных на депозит 1.6 BTC с размером лота в 1 BTC, может выпустить только 1.0 TBTC. Любой пользователь, сжигающий 1.0 TBTC, впоследствии получает возможность претендовать на депозит в размере1.6 BTC и погашать содержащийся в нем UTXO (вывод неизрасходованных транзакций). Это позволяет получить выгоду в размере 0.6 BTC.

Недоплата

Допущение недоплаты на конкретно взятом вкладе, наоборот, станет причиной повышения залогового обеспечения подписантов. Чтобы предотвратить подобное, система не принимает доказательства финансирования, если размер депозита ниже, чем значение его лота. Это подразумевает, что пользователь, отправляющий депозит в размере ниже определенного размера лота, не получает токены TBTC и теряет право на BTC, заблокированные в финансовых транзакциях группы подписантов.

В свою очередь, группа подписантов может по истечению периода финансирования депозита уведомить, что последний не был профинансирован, и получить свои средства обратно. Также группа подписантов может разблокировать и равномерно распределить средства в транзакциях после того, как будет вынесено решение о том, что этот депозит является транзакцией, произошедшей в блокчейне и записанной с помощью его механизмов.

Множественные UTXO (выводы неизрасходованных транзакций)

Депозитор, допустивший ошибку, также может отправить более одного вывода неизрасходованных транзакций на адрес группы подписантов, при этом не имеет значения характер ошибки, будь этот фактор человеческим или программным. К сожалению, возвращение средств депозитору будет подразумевать значительные сложности в пределах цепи, а также вознаграждения за газ (газ – единица оплаты в сети Эфириум), поскольку каждый UTXO должен быть доказан путем упрощенной проверки платежей (SPV), при этом подпись должна быть полностью правомочной.

Кроме того, нам бы пришлось развивать механизмы, с помощью которых можно экономическими инструментами принуждать подписантов подписывать каждую проводимую транзакцию, несмотря на тот факт, что общая стоимость вывода неизрасходованных транзакций неизвестна. Как таковая, система принимает только первый UTXO с размером, превышающем установленное значение лота. Все остальные BTC, отправленные группе подписантов, утрачиваются. Именно поэтому депозиторы в обязательном порядке должны отправить только один BTC с соответствующей стоимостью.

В качестве частного примера с разрушительными последствиями представьте себе наивного человека, выступающего депозитором. Если он ошибочно отправляет половину значения лота одной транзакцией и вторую половину – еще одной, то лишится обоих UTXO. Это создает опасную ловушку для депозиторов, которые должны, в свою очередь, осторожно руководствоваться пользовательским интерфейсом во избежание потери значительного количества средств.

Запрос на преждевременное прекращение источника финансирования

Система включает незначительную «лазейку» для сценариев с недоплатой или множеством UTXO. Речь идет о следующем: после того, как отмечено истечение срока для финансирования вклада, депозитор может подать запрос на прекращение источника финансирования. Данный запрос включает биткоин-адрес, на который отправляются UTXO, возвращаясь к депозитору. Описанная «лазейка» полностью полагается на честность подписанта: система не может обеспечить экономические гарантии в возвращении биткоина для депозитора.

Экономика депозитов

Подписанты не являются альтруистами – услуги, которые они оказывают, полностью оплачиваются.

Вознаграждение подписантов всегда должно оплачиваться или депонироваться авансом. Чтобы реализовать такую задачу, вознаграждение подписантов гарантируется путем выпуска монет в обращение. В данном случае депозиты должны иметь предсказуемые жизненные циклы.

Узнать более подробно о подходе к вознаграждению подписантов можно из соответствующего раздела.

Сроки

Депозиты с установленными сроками означают, что размер вознаграждения подписантов можно легко рассчитать по каждому из них. Стандартный срок в 6 месяцев предполагает, что депозиторы могут подготовить бюджет для вознаграждения, а подписанты, в свою очередь, будут знать, насколько долго будут недоступны их залоговые обязательства.

В целях стимулирования своевременности погашения структура системы создана таким образом, чтобы депозиты могли быть погашены только их владельцами в течение указанного срока, но при это кто угодно может погашать депозиты в случае, если их срок истек. Дополнительно, выплаты

строго в срок возлагают издержки на вознаграждение для подписантов именно на владельца депозита, если соответствующие средства не будут депонированы торговым автоматом.

Депозиторы, которым в перспективе не потребуется доступ к их депозитам, могут предпочесть передачу издержек системы конечной погашающей стороне и/или пожелать выразить их за пределами стоимости лота BTC либо его взаимозаменяемости. Эти депозиторы могут выбрать получение не взаимозаменяемого токена с возможностью возврата комиссии, который возвращает затраченные на это средства во время досрочного погашения депозита другим пользователем. Механизм возврата комиссии объясняется далее, в разделе о выпуске монет в оборот.

По окончании срока депозит может быть погашен любым участником, включая подписантов как таковых, при этом вознаграждение подписантов взимается с владельца депозита. Этот механизм более подробно обсуждается в разделе о погашении.

Залоговое обеспечение

Поскольку подписанты способны тайно вступить в сговор, чтобы подвергнуть цензуре изъятие средств или скрыться с ними, с каждого депозита и от каждого обеспечивающего его подписанта требуется залоговое обеспечение.

В отличие от установленных рабочих токенов, которые используются для выбора подписантов, залоговые обеспечения подписантов должны выступать в роли ликвидных активов с широкой степенью рыночной капитализации. Данное ограничение повышает расходы на проведение атак, направленных на рынок, где цена залогового обеспечения может быть повышена или, наоборот, понижена в результате рыночных манипуляций.

Подписанты, имеющие залоговые обязательства, предлагают помощь депозиторам в случае тайного сговора подписантов, вмешивающихся в проведение операции. Группа подписантов, которая не предоставляет требуемой для погашения вклада подписи после истечения указанного срока, утрачивает свои залоговые обязательства. Похожим образом группа подписантов, в отношении которой было доказано подписание неправомочных материалов, утрачивает свои залоговые обеспечения, а также рискует долей собственного рабочего токена.

Приемлемые залоговые обеспечения

Два токена выступают в качестве очевидного выбора для подписания залогового обеспечения – это токен TBTC и основной рабочий токен. На протяжении этапа начальной загрузки сети никакой из них не может выступать в качестве подходящего кандидата из-за низкого уровня ликвидности.

Поскольку залоги подписантов должны быть деноминированы в хорошо торгуемые активы в целях исключения манипуляций со стороны рынка, следующим наиболее вероятным выбором для залога станет родной токен основного сервера. Для tBTC v1 таковым является Эфир. Поскольку блокчейн-экосистема продолжает развиваться, прочие опции залогового обеспечения могут стать осуществимыми за счет более сложной реализации.

Измерение уровня безопасности

Очевидно, что вопросы безопасности требуют подписания обязательств, которые пропорциональны значению лота депозита. Чтобы обезопасить ожидаемую отрицательную цену от заговора со стороны подписантов, сумма, утраченная подписантами с «плохим поведением», должна быть строго более высокой, чем сумма, которую они должны получить. Принимая во внимание такие факторы, как размер лота одного 1 BTC, постоянный обменный курс между 1 BTC и залоговым активом, а также M-of-N группы подписантов (где M – минимальное число, а N – общее, суммарное), которые обеспечивают депозит, минимальное залоговое обеспечение для

каждого подписанта будет выражено как (1 BTC)/M, деноминированное в долговом активе (в данном случае речь идет об Эфире – ETH).

Рассмотрим вклад в размере 1 BTC, обеспеченный группой подписантов «3-из-5». В худшем случае трое подписантов могут быть злонамеренными и попытаются украсть депозит, который бы предоставил каждому из них по 1/3 BTC. В результате все 5 подписантов должны внести в качестве залога по 0.33 BTC, обозначенные в ETH.

ПРИМЕЧАНИЕ

Для tBTC v1 ограничения в подписании протокола означают существование группы подписантов, организованной по принципу «3-из-5». В результате требуемое с каждого подписанта залоговое обеспечение составит 50% от размера лота каждого подписанта. В общем размер обязательства составит 150% (читайте в следующей главе о падении цены эфириума относительно биткоина). В соотношении с более поздними версиями, в данном случае залоговые обязательства могут быть снижены путем увеличения группы подписантов или допустимого порога.

Колебания при ценообразовании валюты

Вышеуказанное предполагает наличие постоянного обменного курса между валютами BTC и ETH, но на самом деле каждая из них колеблется относительно друг друга, притом иногда – очень сильно.

Стоимость ETH снижается относительно BTC

Если стоимость ETH стремительно падает относительно BTC, то долларовая стоимость Эфира, который выступает залогом со стороны подписантов, может быть ниже, чем выраженная в долларах стоимость BTC-депозита. Это означает, что, если подписанты попытаются украсть BTC с депозита, то у них сложилась положительная ожидаемая стоимость.

Чтобы исключить такую вероятность, мы требуем, чтобы залог был сверхобеспеченным. Каждому подписанту, который обеспечивает эфир, необходимо внести дополнительные 50% для того, чтобы в целом достичь 150% залогового обеспечения.

***Без сверхобеспечения**: Представим, что стоимость одного биткоина составляет $10 000, а эфира – $200. Подписанты должны предоставить 50 ETH для обеспечения вклада. В соответствии с условиями рынка, ETH теряет 25%, то есть его стоимость теперь составляет $150, в то время как BTC сохраняет свою изначальную стоимость. 50 ETH эквивалентны $7500. Это означает, что подписанты могут получить выгоду в размере $2500 путем кражи депозита.*

***Со сверхобеспечением**: Представим, что стоимость одного биткоина составляет $10 000, а эфира – $200. Подписанты должны предоставить 75 ETH (150% из 50) для обеспечения вклада. В соответствии с условиями, сложившимися на рынке, эфир теряет 25%, таким образом его стоимость снижается до $150, в то время как Биткоин сохраняет первоначальную стоимость. Эквивалент 75 ETH составит $11250, что превышает долларовое выражение указанной суммы биткоина. Это значит, что подписанты, скорее всего, будут вести себя честно, поскольку в данном случае им есть что терять.*

В целом, общее сверхобеспечение в размере 150% (3/2 * 100%) является стимулом для подписантов делать все возможное для благополучия системы вплоть до снижения стоимости залогового актива до 33% ((1 - 2/3) * 100%) в противовес активу депозита. Повышение этого процентного показателя может также повысить прочность всей системы за счет возможности назначить цену для подписантов, которая должна быть компенсирована за счет выплачиваемого вознаграждения.

Если стоимость ETH превышает порог безопасности, открытые депозиты будут подлежать предварительному погашению вплоть до последующего полного погашения.

Снижение стоимости BTC относительно ETH

Поскольку вознаграждение подписантов обозначается строго в BTC (с учетом сверхобеспечения), снижение стоимости биткоина в противовес залоговому активу приводит к более низкому уровню вознаграждения для подписантов. Обратите внимание: это не создает каких-либо проблем для активов TBTC, но делает систему менее привлекательной для подписантов, которые получают вознаграждение, пополняющее их личные активы.

Подписантам следует приобретать TBTC на рынках в ожидании таких сверхобеспеченных депозитов, и им также следует использовать их в целях погашениях подобных позиций, где это только возможно. Таким образом можно восстановить ликвидность эфира, с помощью которого можно обеспечить другие вклады. Альтернативой такому подходу может стать предоставление подписантам возможности безопасно сбалансировать их залоги вплоть до 150%. Тем не менее, это сложно реализовать и, в результате, это не является приемлемым решением для исходного развертывания механизма.

В качестве примера представим, что 1 BTC стоит $10 000, а 1 ETH – $200. Подписантам необходимо внести 75 ETH для обеспечения депозита в 1 BTC. Ожидается, что подписанты вносят плату из 5 базовых точек на депозит в $10 000 для получения обеспечения в размере $15 000 (150% от $10 000), а взамен они уступают возможность сдать 75 ETH на различные нужды.

Предположим, что альтернативное использование вернет пять базовых точек, выраженных в валюте Эфир. В соответствии с текущими рыночными условиями, ETH стремительно повышается на 25% и его стоимость теперь составляет $250, в то время как стоимость BTC остается неизменной.

Подписанты до сих пор располагают пятью базовыми точками в TBTC, хотя те же 5 базовых точек, которые они могли бы получить в ETH, в данный момент представляются более ценными. Если вклад разблокирован и подписант разумно ожидает, что сверхобеспечение сохранится, то ему следует погасить депозит путем выплаты 1.0005 TBTC, используя 1 BTC и изымая 75 ETH, которые были заблокированы всеми подписантами.

Все должным образом сверхобеспеченные подписанты теперь обладают ликвидным Эфиром, который они могут использовать для обеспечения другого вклада при выпуске нового TBTC, теперь с более низкими требованиями по обеспечению в ETH, а также использовать полученную сумму в других целях.

Эластичность ценообразования

В отличие от популярных искусственных схем стейблкоинов, проект системы tBTC не прилагает каких-либо усилий для стабилизации стоимости токена TBTC по отношению к BTC: TBTC, таким образом, оценивается именно рынком. Цель данной системы заключается в том, чтобы обеспечить условия, при которых поставка токенов TBTC должна быть строго меньше, чем активы BTC, обеспечивающие их.

По этой причине единственным вариантом соотношения цены, который системе нужно ясно понимать, является корреляция между залоговыми обеспечениями подписантов и BTC.

Для tBTC v1 это означает, что стоимость ETH соотносится с BTC. Благодаря только требуемым ценам для пары активов система tBTC первоначально будет использовать простое ценообразование.

Обесценивание залогового обеспечения

Предварительная ликвидация: звонок вежливости

При первом пороговом показателе в 125% происходит предварительная ликвидация депозита. Такое состояние также называют «звонком вежливости». Будучи в таком состоянии, депозит может быть погашен любым участником, даже в том случае, если этот депозит заблокирован (более подробно смотрите разделы о погашении и выпуске). Предварительное погашение указывает на то, что подписанты должны закрыть депозит, в противном случае им придется столкнуться с принудительной ликвидацией, которая произойдет после.

Если вклад не закрывают в течение 6 часов, либо если обеспечение вклада падает ниже 110% от залогового обеспечения, следует ликвидация. Это дает стимул каждому подписанту закрыть позицию до того, как ее обеспечение снизится до критического уровня. В качестве альтернативы, если соотношение «ETH-BTC» сможет восстановиться в данных условиях, чтобы обеспечение депозита составляло как минимум 125% в течение 6 часов, то вклад остается в безопасности и выходит из состояния предварительной ликвидации.

В последующих версиях системы могут быть введены более сложные механизмы предварительного погашения. Для начальной версии представляется рациональным выбор простого механизма с развитой системой взысканий для происходящего обесценивания залогового обеспечения. Кроме того, путем стимулирования погашения обесцененных или значительно сверхобеспеченных позиций подписанты защищены от привязки к ETH на долгий период времени.

Ликвидация

Вынужденная ликвидация – довольно редкое явление, поскольку расчетливые подписанты погашают депозиты еще до того, как ликвидация становится необходимостью. Тем не менее, перспектива исключительной меры наказания в виде ликвидации необходима для того, чтобы предотвратить нечестное поведение со стороны подписантов. Ликвидация может произойти по таким причинам:

- подписанты не создали действительную подпись в ответ на запрос о погашении;
- ценность залога подписантов опустилась ниже порога ликвидации;
- подписанты не отреагировали должным образом на «звонок вежливости»;
- подписанты создали мошенническую подпись.

Первоочередная цель ликвидационного процесса – удержать позиции депозитора при неправильном поведении со стороны подписантов или при воздействии внешних факторов, которые ставят под угрозу безопасность депозита. Вторая цель – максимально наказать подписантов за неправильное поведение в том случае, если подобное может быть доказано.

Наиболее ценный актив, который имеет система, - это залог подписантов. Таким образом, ликвидационный процесс изымает залог подписантов. Кроме того, предпринимаются попытки использовать залоговую стоимость для того, чтобы продать токены TBTC и таким образом предоставить компенсацию владельцу депозита.

Любой залог подписанта, оставшийся после того, как владельцу депозита предоставили компенсацию, отправляется на счет, ответственный за составление отчетов по неправильному поведению (речь идет о мошенничестве), либо разделяется между подписантами и счетом, который стимулировал ликвидацию (для решения проблем залогового обеспечения).

Чтобы возместить средства владельцу депозита, контракт начинает торги со снижением цены на залоговое обеспечение подписанта. В данном случае предлагается определенная доля залога подписанта – 66, 6667% - взамен на эквивалент непогашенной суммы токена TBTC. Эта сумма

предусматривает, что вклад должным образом обеспечен до уровня 150%. Это, в свою очередь, защищает от нарушений в процессе ценообразования. Последние могут стать причиной создания должным образом обеспеченного депозита для того, чтобы он в противном случае был изъят за слишком завышенную стоимость Эфира. Сумма торгующегося залога со временем повышается, до тех пор, пока кто-либо не приобретет его, либо же торг достигает 100% от стоимости залога. Торги остаются открытыми до тех пор, пока не найдется покупатель на представленный лот.

Токен TBTC, полученный в результате описанного процесса, отправляется владельцу депозита. Если владельцем является игровой автомат, то последний обязан сжечь TBTC в целях сохранения привязки к обеспечению. Если после ликвидации остается какое-либо залоговое обеспечение, то ситуация может развиваться по одному из двух вариантов:

1. При ликвидации, вызванной обесцениванием залогового обеспечения или его преждевременным прекращением, оставшаяся стоимость залога разделяется по принципу «50 на 50» между счетом, который спровоцировал ликвидацию, и подписантами.
2. Если ликвидация была вызвана мошенническими действиями, то оставшаяся стоимость залога отправляется на счет, который спровоцировал ликвидацию путем доказательства факта мошенничества.

В завершении процесса ликвидации подписанты, которые вели себя неподобающе, контролируют внесенные биткоины. Основные варианты того, что эти подписанты могут сделать с биткоином вне системы tBTC, выбирают они сами. Он может быть разделен, украден большинством подписантов или безвозвратно утрачен.

ВНИМАНИЕ! Если токен FRT был выдан для выпуска TBTC, предназначенного для ликвидируемого депозита (более подробно – в разделе о выпуске), владельцу токена FRT не возмещают средства в течение периода ликвидации. Вознаграждение, которое было переведено в депозит в обмен на токен FRT, вместо этого используется для того, чтобы компенсировать затраты подписантов, а токен FRT более непригоден для использования в целях компенсации.

1. Подписанты хранят депозит в размере 1 BTC, обеспеченный 75 ETH при соотношении 0,02 BTC/ETH (1,5 BTC в ETH, соотношение залогового обеспечения в размере 150%).
2. Стоимость ETH снижается до показателя 0.01333 BTC/ETH. Теперь 75 ETH обеспечивают только 100% вклада (1 BTC / 75 ETH).
3. Запускается процесс ликвидации и 75 ETH изымаются для того, чтобы выкупить токен TBTC.
4. Депозит должен использовать 75 ETH для того, чтобы была возможность приобрести 1 токен TBTC. При попытке получить скидку, он торгуется в размере 66.6667% от запасов ETH.
5. Арбитр сжигает 1 TBTC до 90% его торговой стоимости и получает 67,5 ETH. Ликвидация депозита считается завершенной. Арбитр может сделать это по нескольким причинам: поскольку цена восстановилась в процессе торгов; поскольку планируется использование Эфира в целях проведения арбитража против более высокой цены позже или же с другим активом; потому что проводится арбитраж с более ранними, выгодными цен на TBTC, посредством чего приобретается требуемый токен TBTC.
6. Половина от остающейся суммы в размере 7.5 ETH распределяется между подписантами (если они совершали мошеннические действия, то не получают ничего), а остаток предоставляется счету, который начал ликвидационный процесс в рамках смарт-контракта на Ethereum. На этом этапе депозит считается закрытым. Обратите внимание, что владельцу токена FRT не возмещают средства на протяжении периода ликвидации.
7. На усмотрение сторон, определенное количество участников согласовывают и утверждают, каким образом они будут распределять депозит в размере 1 BTC.

Ценообразование

Ценообразование – неотъемлемая часть системы, которая гарантирует достаточное количество залоговых обеспечений для всех подписантов системы tBTC. В рамках tBTC v1 ценообразование стоится на основе специального контракта ETHBTC Medianizer от системы двух токенов MakerDAO, который в настоящее время управляется MakerDAO.

Проект минимального ценообразования в полной мере определяется следующим интерфейсом:

--изображение--

Он главным образом используется для расчета стоимости биткоин-депозитов, установленной в Эфирах. В модели по типу Medianizer стоимость обеспечивается внешней организацией, так что метод updatePrice в данном случае не используется.

Кодирование цены

Биткоин имеет 8 десятичных знаков. Наименьшей единицей является сатоши. То есть, 100 000 000 сатоши равны одному биткоину. В отличие от этой криптовалюты, эфир имеет 18 десятичных знаков, наименьшая частица – вэй. В 1 000 000 000 000 000 000 вэй – 1 эфир.

Чтобы выразить стоимость биткоина относительно эфира, мы должны использовать соотношение количества вэй к сатоши. Несложный расчет предусматривает использование определенного количества вэй (x) – 1 сатоши. Следовательно, при получении значения цены при соотношении 32.32 ETH : 1 BTC (состоянием на июнь 2019 года), возвращается значение в 323 200 000 000 вэй.

Тем не менее, если 1 вэй стоит больше, чем 1 сатоши, цена более не может быть с высокой точностью закодирована. Мы считаем маловероятным, что за очень короткий срок реализуется подобный вариант переворота, когда 1 Эфир приобретает стоимость в 10 000 000 000, как и биткоин. Вместо того, чтобы преждевременно выражать оптимистичные настроения, объединяя соотношение двух целых чисел (где x – вэй, а y – сатоши) и меняя смысл вызова, мы оставим это в качестве предстоящей задачи для системы управления.

Использование контракта Medianizer в системе tBTC v1 можно выразить в словах, которые организация Maker описывает как механизм поддержки для ETHBTC. Речь идет о том, что он возвращает стоимость одного ETH, выраженного в BTC, с точностью до 18 десятков. Названия для восемнадцатого десятка биткоина нет, поскольку наименьший назван обозначением 10^{-8}, то есть это сатоши, поэтому мы будем в дальнейшем называть его «вэйтоши». Чтобы получить соотношение определенного числа вэй (x) к 1 сатоши, система tBTC должна конвертировать стоимость курса ETHBTC (1 Эфир в вэйтоши) в определенное количество вэй, которое содержится в одном сатоши. Это производится путем разделения числа 10^{28} стоимостью контракта Medianizer.

Будущий проект

Ценообразование – неотъемлемая часть системы безопасности tBTC, поэтому в будущем будет управляться преимущественно экосистемой. Первая модернизация будет сконцентрирована на объединении нового механизма ценообразования, основанного на проблемах обратных аукционов, которые были продублированы как "обеспечение без стоимости".

Выпуск токенов

Обзор

Процесс выпуска токенов TBTC в обращение отличается от процесса создания депозита в биткоинах.

Разделяя процесс выпуска токенов на 2 фазы (создание депозита без подтверждения и не взаимозаменяемого токена, а также создание дополнительного доказательства, которое

позволяет совершить сделку по обмену не взаимозаменяемого токена на взаимозаменяемый TBTC), мы можем сохранить равновесие системы полной безопасности при угрозе реорганизаций с лучшим пользовательским опытом и более гибкими вариантами использования.

Упрощенный обзор создания депозита, выпуска токенов и погашения – в представленной схеме:

https://docs.keep.network/tbtc/basic-deposit-lifecycle.svg

Обратите внимание, что представленная выше схема упустила несколько дополнительных возможностей, которые объясняются ниже в данной работе. Речь идет о разном:

- в чем ключевые различия между досрочными и срочными депозитами;
- изменения, связанные с ликвидацией;
- о том, каким образом депозитор может сохранить свой TDT без выпуска TBTC.

Выпуск не взаимозаменяемых токенов системы tBTC для депозита

После того, как поступил запрос на создание депозита и группа подписантов сформировалась, депозитор немедленно получает уникальный не взаимозаменяемый токен. Он имеет название TDT (это токен стандарта ERC-721, являющийся эквивалентом TBTC и предоставляющий собственность на депозит). Собственность такого рода сопряжена с исключительным правом погашать депозит с момента его создания и до тех пор, пока его срок не истечет, за исключением случаев обесценивания залогового обеспечения, которые помещают депозит в состояние «звонка вежливости».

Как только депозит полностью подтверждается путем предоставления достаточных доказательств относительно финансирования биткоин-транзакций, держатель TDT может запросить погашения и, после выплаты каких-либо вознаграждений подписантам, ему предоставляется гарантия того же UTXO, который обеспечивает депозит. Держателю TDT также предоставляются гарантии компенсации в TBTC через залоговое обеспечение группы подписантов в случаях:

- мошенничества или возникновения проблем с залоговым обеспечением (более подробно – в разделе о ликвидации);
- компенсации в TBTC за исключением вознаграждения для подписантов, если депозит погашен другим счетом после наступления срока его исполнения (более подробно – в разделе о срочных погашениях);
- если депозит находится в состоянии «звонка вежливости».

Последствия

Есть несколько неочевидных последствий, которые связаны со специфическим UTXO не взаимозаменяемым токеном.

1. Любые атаки относительно депозита, который обеспечивает TDT, должны оказывать влияние только на держателя токена, а не на всю валюту, привязанную к обеспечению. Атаки, направленные против отдельного депозита, могут проявляться в виде реорганизации или двойного расходования биткоина, DoS-атак (хакерских атак на вычислительную систему в целях доведения ее до отказа), злонамеренных подписантов либо обесценивания депозита.
2. Любому получателю TDT понадобится оценить степень риска токена. Различные токены могут предусматривать различные вероятности реорганизации. Владельцы депозитов могут беспрепятственно перемещать свои TDT, продавая их или используя где-либо в качестве залога.
3. Токены TDTs – идеальная цель для улучшений финансовой конфиденциальности на главном сервере.

4. Подобная конструкция делает возможным делегирование работ по накоплению рабочих доказательств упрощенной системы платежей третьим сторонам. Благодаря таким функциям депозитору необязательно отслеживать события в блокчейне биткоина.

Выпуск в обращение взаимозаменяемого токена TBTC

Когда на депозите накопится достаточное количество рабочих средств, его можно обменять на взаимозаменяемый токен TBTC. Контракт, подтверждающий такую операцию, называется «торговым автоматом».

Торговый автомат TBTC

Торговый автомат TBTC – это контракт на основном сервере, который отвечает за выпуск токена TBTC в обращение.

Любой TDT, представляющий подтвержденный депозит, может подлежать обмену. Квалифицированные депозиты определяются накопленной работой их подтверждений.

В tBTC v1 депозиты квалифицируются установленными рабочими требованиями, доказанными с помощью упрощенного метода проверки SPV, и основываются на 6 блоках с накопленной работой.

TDT, представляющий утвержденный депозит, также имеет право на выпуск в обращение взаимозаменяемого TBTC. Выпуск в обращение TBTC остается мерой на усмотрение сторон; депозиторы могут придерживать свои токены TDT, которые будут оставаться действительными на протяжении всего срока утвержденного депозита. Обратите внимание: если держатель TDT желает совершить транзакцию со стоимостью, которая отличается от размера лота, он должен выпустить в обращение TBTC, поскольку сам по себе tBTC Deposit Token (NFT токен, который создается при запросе пользователя на депозит) не является взаимозаменяемым.

Держатели утвержденного TDT могут обменять его на недавно выпущенный TBTC, как эквивалентный размеру лота депозита (например, 1 TBTC), так и в меньшем размере, чем требуемое вознаграждение за подпись (например, 0.005 TBTC). Чтобы отобразить снижение гарантии заинтересованности владельца TDT в погашении конкретного депозита, вознаграждение за подписание отправляется на депозит, чтобы он был депонирован в момент выпуска TBTC.

Путем обмена и депонирования, владелец TDT отказывается от своего исключительного права погашения. По сути, он также получает не взаимозаменяемый токен FRT, который предоставляет право на возврат комиссии, если/когда срочный депозит погашается другим участником. В редких случаях, когда TDT используется в целях выпуска TBTC, извлеченного из торгового автомата и перенаправленного в торговый автомат до срока его истечения, вознаграждение за подписание депонируется только в первый раз, когда TDT торгуется на торговом автомате. Поскольку вознаграждение за подписание не депонируется во второй раз, когда TDT торгуется на торговом автомате, FRT также не выпускается в этот период. Взамен FRT, выпущенный первоначально в момент торгов TDT на торговом автомате, остается действительным.

Торговля TBTC для получения токенов tBTC Deposit

Любой TDT, принадлежащий торговому автомату, может быть получен по стоимости его лота, выраженной в TBTC (в приведенном выше примере депозит может быть получен за 1 TBTC). Торговый автомат должен сжечь любой полученный им TBTC в любом случае, когда он может получить TBTC.

Этот автоматический процесс позволяет «заблокированным» депозитам быть «открытыми» заранее, в счет более позднего погашения. Фактически, выпуск в обращение TBTC – это просто особый случай разблокировки: TDT, используемый для выпуска TBTC, блокируется в торговом

автомате, который обеспечивает прямой путь к передаче данного токена другому счету по стоимости размера его лота, выраженного в TBTC.

Сжигание всех полученных TBTC позволяет поддерживать обеспечивающую привязку не только в случаях, когда собственность на депозит передается от торгового автомата, но и когда депозиты, владельцами которых до последнего момента является торговый автомат, ликвидируются или погашаются в срок. Поэтому в данных случаях компенсация для владельца депозита направляется торговому автомату, который немедленно сжигает полученную сумму.

Вознаграждение подписантам

Подписанты подвергают риску собственные средства для того, чтобы предоставить депозиторам гарантии исключения риска «грязных игр». Залоговые обеспечения, которые они вносят, являются капиталом. Подписантам необходимо заработать средства, сопоставимые с риском, чтобы оставаться конкурентоспособными при других возможностях.

Плата за безопасность

Есть ряд моделей ценообразования, которые могли бы покрыть альтернативные издержки подписантов.

Минимальный уровень ценообразования может происходить от соответствующих моделей ценообразования в сфере криптовалюты: сегодняшние централизованные попечители криптовалюты расходуют 50 из 75 ключевых точек (между 0,5-0,75%) на активы, находящиеся под попечительством (AUC) ежегодно. Таким образом, каждый год централизованные попечители защищают биткоин-депозит, то есть такую сумму, которую составляет потеря 0,75% средств относительно средств попечителя.

Децентрализованная модель должна в конце концов разрешать вознаграждения в более низком размере путем внесения более конкурентных условий в эту сферу. Тем не менее, есть и предостережение: децентрализованный подход к попечительству усложняет средства правовой защиты, так как требует дополнительного залогового обеспечения в целях гарантии возмещения при сбоях.

При применении описанной модели ценообразования к залоговому обеспечению tBTC становится ясно, что подписанту понадобится совершить аналогичный возврат на минимальном уровне общего капитала, который он защищает.

Оценка параметров вознаграждения

Терминология

Депозит

Не взаимозаменяемый смарт-контракт, для которого назначена группа подписантов. Депозит координирует создание и погашение размера лота в TBTC.

Размер лота

Общая стоимость депозита, выраженного в биткоинах.

Фактор сверхобеспечения

Добавочная сумма, которая должна быть внесена подписантами в качестве залогового обеспечения и выражена в качестве процентного отношения размера лота.

Стоимость залога

Сумма, которую подписант должен заблокировать в смарт-контракте в качестве залога для выпуска в обращение TBTC. Первоначально стоимость залога будет выражена в Эфире (ETH). Требуемый размер залога депозита, внесенного всеми подписантами, может быть выражен в виде схемы: Фактор сверхобеспечения*размер лота* (уровень соотношения ETHBTC).

N

Количество подписантов, уполномоченных на подписание запроса об отзыве депозита.

M

Минимальное количество участников, которое требуется для подписания разрешения по запросу на отзыв депозита.

Описание

Предполагается, что каждый подписант делает свой вклад, равный залоговому обеспечению депозита.

Основные затраты каждого подписанта высчитываются по формуле *Стоимость залога*/N, где размер лота равен 1 BTC и Фактор сверхобеспечения равен 150%, что создает формулу 1,5 BTC / N.

Начальная оценка параметров системы может задействовать трех подписантов на каждый лот. Кроме того, ввиду недостатка в механизме совокупной подписи, мы выбираем соотношение M = N. Это требует 50% от стоимости BTC в основных затратах каждого подписанта на каждый выпущенный в обращение TBTC.

Подписание

Все вышеупомянутые механизмы требуют наличия кошелька с мультиподписью по принципу «M-of-N», который содержит каждый биткоин-депозит.

Алгоритм консенсуса в биткоине ограничивает размер скрипта 520 байтами (10 000 байтов для выходов Сегвит – протокола для улучшения и исправления в криптовалюте), тем самым ограничивая и максимальный размер скриптов мультиподписи до 80 участников (OP_CHECKMULTISIG ограничен 20 открытыми ключами, но это можно обойти, используя OP_CHECKSIG ADD или <threshold> OP_GREATERTHAN, как показано здесь (Nomic Labs).

Дальнейшие предложения, такие, как MAST (концепция использования деревьев Меркла и абстрактных синтаксических деревьев), могли бы допустить осуществление большего количества мультиподписей, однако исторически сложилось так, что включение в систему биткоина новых особенностей стало процедурой с неопределенными временными рамками.

Наконец, крупные кошельки с мультиподписью в Эфириуме и Биткоине увеличивают расходы на верификацию, что связано с увеличением числа участников. Создание кошельков с мультиподписью в Эфириуме особо сложное. Путем использования совокупных подписей с накоплением открытых ключей мы можем устранить все перечисленные выше трудности и заменить их простой верификацией, требующей единственной подписи.

Совокупный открытый ключ генерируется всеми участниками мультиподписи, которые взаимодействуют через внегрупповой протокол. Этот процесс также известен как распределенная генерация ключа (DKG). Каждый участник подписывает соответствующее сообщение своим закрытым ключом и вносит долю в окончательную совокупную подпись. С учетмо ECDSA (алгоритм с открытым ключом для создания цифровой подписи), совокупная подпись в таком случае может быть сверена с совокупным открытым ключом с помощью OP_CHECKSIGVERIFY на Биткоине или операции на Эфириуме. Это простой и недорогой процесс, который к тому же исключает сложный алгоритм проверки мультиподписи. Последний может быть модернизирован

для разных M-of-N-конфигураций. Если требуется какая-либо иная конфигурация, нужно только настроить скрипт или смарт-контракт таким образом, чтобы использовать новый совокупный открытый ключ после повторного проведения манипуляции DKG.

Порог ECDSA (алгоритма с открытым ключом для создания цифровой подписи)

Для закрытого ключа, обозначенного как x, сообщения (M), хэш-функции (H) и однозначно выбранного числа (k), подпись ECDSA является парой (r, s), в которой s = k (m + xr), r = R_x, R = $g^{(k}$-1) и m = H(m). Эта подпись может быть переведена в пороговую при условии, что значения k и x рассчитываются путем секретного обмена между участниками протокола t of n. Документ Розарио Дженнаро и Стивена Голдфедера описывает эффективный механизм для выполнения данной процедуры. Обратите внимание, что похожий механизм был предложен Йегудой Линделлом в этом же году (2018).

Неофициально участники выполняют следующие действия для того, чтобы подписать послание:

1. Создать добавочную долю, выражающуюся формулой k * x, где каждый участник i проводит k_i и x_i.
2. Рационально рассчитать R = g^(1/k), используя Bar-Ilan and Beaver's inversion trick, без каких-либо участников i, обнаруживающих k_i, а также установить r = R_x.
3. Каждый участник высчитывает свою долю в подписи с помощью следующего выражения: s_i = m * k_i + r * k_i * x_i.
4. Пороговая подпись – сумма всех подписей s_i.

Более подробное описание протокола можно найти в разделах 4.1. и 4.2. данного документа.

Улучшенное распределение ошибок

В настоящее время, когда подписанты неправильно себя ведут в рамках системы, все принадлежащие им залоги для обеспечения безопасности изымаются и сжигаются. Если системе задают параметры вплоть до использования мультиподписей по принципу M-of-N в целях обеспечения депозита, это означает, что, в случае неправильного поведения M-сторон, залоговые обязательства всех N-сторон будут резко сокращены. Это ситуация, которой при идеальных условиях мы стараемся избежать.

Множественные подписи ответственной подгруппы (более подробно описано в разделе 4 связанного с представленной работой документа) позволяют различать подпись, сделанную подгруппой S в множественной подписи M-of-N от аналогичной подписи, сделанной подгруппой S'. В данном случае есть возможность установить наказание только для неправильно ведущих себя подписантов M, что устраняет риск наказания честных подписантов.

Протокол порога ECDSA, описанный в предыдущих главах, не поддерживает распределения ошибок между подгруппами подписантов. Мы будем применять tBTC без такого свойства и включим его в последующих обновлениях протокола.

Схемы подписания, которые будут использоваться в дальнейшем

В этом разделе мы исследуем другие схемы совокупной подписи, которые мы сможем использовать в дальнейшем. Описанные методы безопасны при использовании в простых моделях открытого ключа. Это значит, что пользователям не нужно доказывать право собственности на их секретный ключ. Именно поэтому данные методы являются привлекательными для использования в блокчейнах. Мы кратко опишем подписи MuSig и BLS.

MuSig

Обратите внимание: эта часть работы взята из последнего раздела официального блога MuSig от технологической компании Blockstream.

1. Пусть H будет обозначать криптографическую хэш-функцию.
2. Назовем L = H(X_1,X_2,…).
3. Назовем X суммой всего H(L,X_i) * X_i.
4. Каждый подписант выбирает случайным образом одноразовый код r_i и делит R_i = r_i * G с другими подписантами.
5. Обозначим символом R сумму точек R_i.
6. Каждый подписант высчитывает значение s_i = r_i + H(X,R,m) * H(L,X_i) * x_i.
7. Окончательная подпись – это (R,s), где s – сумма всех значений s_i.
8. Подтверждение должно удовлетворять значению: sG = R + H(X,R,m) * X.

Вопреки более ранним схемам, данный алгоритм подтверждения подписи является безопасным даже при угрозе нападения мошенников в целях кражи ключа, поскольку X определяется как взвешенная сумма открытых ключей подписантов. Здесь взвешивающий коэффициент зависит от хэша всех участвующих открытых ключей.

Парные мультиподписи

Основываясь на работе в подписях MuSig и BLS, Дэн Бонэх, Ману Дрижверс и Грегори Нэвэн представили действенный вариант предшествующей конструкции подписи BLS, который требует только двух парных операций для подтверждения. Такой вариант также является устойчивым к атакам мошенников на ключи доступа.

Представленная мультиподпись короче, чем MuSig, поэтому в данном случае требуется только одна группа, а не две. MuSig также требует дополнительного цикла взаимодействия для создания случайно выбранного одноразового кода R, который не представлен в подписи BLS. Все подписанты могут направить свои подписи третьей стороне, которая сгруппирует их, устраняя необходимость в дальнейшем взаимодействии, как и необходимость для всех сторон постоянно быть в сети.

Обратите внимание: этот отрывок взят из Раздела 1 официальной публикации Дэна Бонэха.

1. Назовем выражение e: G_0 x G_1 → G_T билинейным невырожденным отображением, которое позволяет эффективно произвести вычисление; g_0 и g_1 – источники G_0 и G_1 соответственно.
2. Назовем sk секретным ключом пользователя, а g_1^{sk} – его открытым ключом.
3. Назовем H_0 криптографической хэш-функцией от области сообщения до значения G_0.
4. Назовем H_1 криптографической хэш-функцией в пределах от G_1^n до R^n.
5. Подпись в m выражается как s_i = H_0(m)^sk_i.
6. Чтобы сгруппировать N-количество подписей для того же сообщения из общественных ключей (pk_1, …, pk_n), нужно:
    1. Высчитать соотношение (t_1, …, t_n) = H_1(pk_1, …, pk_n).
    2. Получить совокупную подпись: s = s_1^t_1 * … * s_n^t_n.
7. Чтобы подтвердить совокупную подпись к тем же открытым ключам:

- Высчитайте (t_1, …, t_n) = H_1(pk_1, …, pk_n).
- Высчитайте значение совокупного открытого ключа: pk = pk_1 ^ t_1 * … * pk_n ^ t_n (вне зависимости от того, было ли подписано сообщение).
- Подтвердите подпись: e(g_1, s) = e(pk, H_0(m)) (это потребует двух отображений, поскольку идет подписание одного и того же сообщения).

Работа над проблемами в системе

Преждевременные прерывания/жизнеспособность

Одно из требований системы – возникновение переломных действий (финансирование, погашение) в четко определенное время после поступившего запроса. Если совершить указанные

действия в строго ограниченные сроки удалось, то сложившуюся ситуацию называют преждевременным прерыванием. В то время как мошенничество демонстрирует принудительно положительное или запрещенное поведение, преждевременное прерывание указывает на неспособность некоторых участников поддерживать жизнеспособность. По сути, в то время как преждевременное прерывание остается наказуемым и может стать причиной ликвидации, оно все же наказывается не столь строго, как мошенничество.

Например, если у подписантов не получается создать подпись для погашения в указанные сроки, их залоговые обязательства ликвидируются в целях защиты обеспечивающей привязки, но любые оставшиеся после этого средства возвращаются им сразу после того, как инициатор ликвидационного процесса будет вознагражден.

Мошенничество

Система признает один вид доказательств факта мошенничества – это доказательства, полученные с помощью алгоритма ECDSA. В этом случае группа подписантов создает подпись на сообщение, которое было неявно запрошено. После обнаружения факта мошенничества система наказывает подписантов путем изъятия их залогового обеспечения и начинает процесс ликвидации.

Доказательства факта мошенничества, полученные с помощью ECDSA

Подписанты совместно контролируют пару ключей алгоритма ECDSA. Взаимодействуя, они могут создавать подписи по открытому ключу. Обязанность подписантов – создание надежных подписей (такие, например, могут понадобится при выполнении операции погашения). Любая действительная подпись, выполненная по открытому ключу подписантов и не запрашиваемая специально системой, рассматривается как факт мошенничества.

Доказательство мошенничества по алгоритму ECDSA – это подпись по открытому ключу подписантов, дайджест (цифровой отпечаток) подписанного обращения и оригинал этого дайджеста. Исходя из перечисленного, мы создаем постоянное подтверждение по алгоритму ECDSA. Если оригинал соответствует краткому изложению и подпись под ним является действительной, но при этом выясняется, что дайджест открыто не запрашивался системой, то можно быть уверенным, что подписант, который создал эту подпись, больше не может считаться надежным.

Здесь стоит отметить, что процесс верификации соотношения между оригиналом и его дайджестом нельзя упускать. При предоставлении любого открытого ключа возникает возможность создать подпись по нему и подобрать дайджест, который соответствует этой подписи. Это значит, что любой участник может создать действительную подпись под каким-либо неизвестным сообщением. Только прямая верификация существования первоначального обращения, которая достигается путем измерения ее соотношения с подписанным дайджестом, может предотвратить мошенническую атаку. Дело в том, что при таких условиях нападающему в придется менять порядок в хэш-функции, чтобы подделать данное соотношение.

Формально система может верифицировать любую подпись, созданную подписантами. Тем не менее, возможности основного сервера на практике ограничены. Например, на платформе Эфириум доступны только определенные функции дайджеста, поэтому мы не можем подтвердить подписи с цифровым отпечатком, которые были созданы неподдерживаемыми хэш-функциями. На практике это препятствует верификации транзакций с криптовалютой Decred (DCR), основанной на платформе биткоина, которая использует монеты blake256. Подписанты в системе платформы Эфириум могут создавать подписи по транзакциям с Decred без вероятности последующего наказания.

Все основные платформы налагают издержки на размер аргумента, поэтому стоимость верификации соотносится с длиной оригинала обращения. Таким образом, есть вероятность того, что будет экономически неосуществимо подтверждать подписи на очень длинных оригинальных сообщениях, а также, что попытки сделать это превысят ограничения по использованию ресурса (например, ограничение блоков Газа, единицы исчисления для расчета и оплаты комиссии, в Эфириуме).

К счастью, хэш-алгоритм подписи в системе Биткоин использует алгоритм double-sha256, который делает оригинал подписи результатом первого sha256. Это значит, что оригинал подписанного дайджеста всегда будет составлять 32 байта. Таким образом, это не позволит издержкам на верификацию соотноситься с размером транзакции, при этом даже очень крупные транзакции не смогут избежать проверки на мошенничество по алгоритму ECDSA.

Погашение

Обзор

Депозиты представляют собой реальные UTXO-транзакции с биткоином (выводы неизрасходованных транзакций) и погашаются за счет BTC, содержащихся в них. Система погашения в tBTC стремится к обеспечению доступа к этим BTC путем процесса публичной проверки.

До тех пор, пока депозит сохраняет хорошую репутацию, владелец депозита с не взаимозаменяемым токеном tBTC может создать запрос на погашение, отказываясь от этого токена и выплачивая любые неуплаченные ранее вознаграждения подписантам, связанные с этим депозитом.

С этой точки зрения процесс погашения не может быть отменен.

Поскольку было запрошено погашение, подписанты должны создать действительную биткоин-подпись, отправляя основной BTC на запрошенный адрес. После выпуска подписи любой участник системы, используя ее, может создать и отправить транзакцию погашения в блокчейн Биткоина.

Сроки и погашение депозита

Как указано в разделе о сроках депозита, депозит имеет установленный срок. После того, как этот срок истекает, депозит открывается для его держателя. Именно поэтому он может быть погашен любым счетом (включая и счет владельца депозита). С этой точки зрения издержки на погашение депозита в точности соответствуют установленному размеру его лота без учета той суммы, которая причитается подписантам в качестве вознаграждения.

Если депозит депонировал сумму вознаграждения подписантов в процессе выпуска в обращение токена TBTC, то она выплачивается из целевого депозитного счета, а владельцу депозита отправляют полный размер лота, выраженный в TBTC. Если депозит не содержит депонированного вознаграждения, его владельцу отправляют TBTC, использованные для погашения, а также вознаграждение подписантам в меньшем размере, которое распределяется между ними.

Обратите внимание! Владелец срочного депозита может бесплатно погасить его, если в нем присутствуют депонированные вознаграждения, или же внести плату в размере вознаграждения подписантов, если они отсутствуют. В этом состоит тонкое отличие от преждевременного погашения, где владелец депозита должен оплатить вознаграждение подписантам даже при наличии депонированных вознаграждений. Добавочная разница отправляется владельцу токена FRT, которому делают скидку на выплату вознаграждений подписантам при преждевременном погашении, но не в случае срочного погашения.

Запросы на погашение

Запрос на погашение подается в нескольких случаях:

1. Если депозит имеет хорошую репутацию (не был ранее погашен и уличен в мошенничестве или не вступал в процесс ликвидации подписи), является досрочным, а запрашивающая сторона владеет соответствующим NFT-токеном.
2. Если депозит имеет хорошую репутацию и является срочным либо просроченным, вне зависимости от того, имеет ли запрашивающая сторона соответствующий NFT-токен.
3. Если депозит перешел в состояние «звонок вежливости», которое было создано для того, чтобы сделать возможным закрытие депозита до того, как он окажется под угрозой обесценивания, вне зависимости от того, имеет ли подающий запрос на погашение участник соответствующий NFT-токен.

Чтобы запросить погашение, участник создает соответствующую транзакцию для смарт-контракта на основной платформе. Запрос на погашение включает:

1. Сумму вознаграждения за биткоин-транзакцию, которая должна превышать или быть равной 2000 сатоши (около 20 сатоши на каждый байт).
2. Стандартный скрипт выхода для передачи BTC (одна из форм совершения транзакций в сети Биткоин – p2pkh, p2sh, p2wpkh, или p2wsh), которому предшествует длина скрипта. Для обеспечения безопасности и приватности это должно контролироваться новой парой ключей.
3. Сумма погашения депозита, выраженная в TBTC.

После получения запроса на погашение смарт-контракт депонирует сумму погашения (которая, если это требуется, включает в себя вознаграждение подписантам), регистрирует получение запроса и уведомляет подписантов о необходимости создания подписи.

Будучи уведомленными о запросе на погашение, подписанты должны ожидать подтверждения на основной платформе. Если они не ожидают подтверждения, запрос на погашение может быть «выброшен» из цепи путем реорганизации. В данном случае любая подпись, которую они создали, может быть использована как для погашения BTC, так и для предоставления свидетельства о мошенничестве подписантов. Подтверждение факта мошенничества, созданное таким путем, будет являться действительным для смарт-контракта главной платформы, потому что у него больше нет записи о запросе на погашение.

Сумма погашения

Теоретически, сумма погашения – это сумма размера лота депозита и вознаграждение подписанта в размере 0.005 TBTC с каждого TBTC (50 основных точек). Это предоставляет гарантию, что подписантам выплатят средства после завершения процесса погашения, а также, что владельцу компенсируют затраты за погашенный депозит (в случае погашений третьими сторонами, а не владельцем). Еще одна гарантия состоит в том, что держатель FRT сможет получить свое вознаграждение (для случаев досрочного погашения).

Если отойти от математических расчетов, то сумма погашения может изменяться в зависимости от таких факторов, как погашающая сторона, держатель TDT, держатель FRT, а также текущий срок депозита.

В Таблице потока депозитных платежей перечислены различные возможные комбинации, а также соответствующие суммы погашения, которые должна внести погашающая сторона. В данной таблице представлены 3 возможные стороны системы – A, B и C. Также в ней перечислены соответствующие расходы по подтверждению погашения.

Формат транзакции по погашению

Операция погашения имеет совершенно канонический формат, прикрепленный к смарт-контрактам, которые выполняются на основной платформе. Это предотвращает вероятность множества сложных атак на систему tBTC, как и упрощение логики контракта. Тот, кто подает запрос, может определить только 2 аспекта транзакции: размер вознаграждения за ее выполнение и ее предназначение. Остальная информация, касающаяся депозита (например, стоимость UTXO), известна контракту на депозит заранее.

Транзакция погашения имеет один вход (UTXO депозита) и один выход (выход погашения). Она не имеет выходов для изменений или дополнительных входов, так как они не требуются. Путем такой транзакции стороне, подающей запрос, просто передается основной BTC в единоличное попечительство. Временные рамки транзакции и последовательные числа начинаются с 0, а ее версия – с 1. Полную документацию формата и структуру sighash-флагов можно найти в соответствующем приложении.

Поскольку формат прост и каноничен, любой наблюдатель может использовать публично доступную информацию для того, чтобы создать его. После выпуска подписи достаточно просто добавить в транзакцию доказательство и распространить его. Итак, в то время как подписанты имеют мощный стимул для распространения транзакции в кратчайшие сроки, любой участник имеет возможность совершить такое действие, если этого не сделали сами подписанты.

Доказательство погашения

Доказательство погашения – это доказательство, полученное методом SPV и подтверждающее, что транзакция погашения была одобрена блокчейном биткоина. Когда запрос на погашение утвержден, смарт-контракт депозита ожидает подтверждения о погашении в течение 6 часов. Чтобы сделать это подтверждение действительным, смарт-контракт выполняет стандартную верификацию методом SPV и дополнительно подтверждает, что получатель соответствует определенному запрашивающей стороной скрипту выхода, а также что стоимость больше или равна установленной стоимости, которая является максимально допустимым вознаграждением (чтобы получить больше информации, смотрите раздел Разрешение на регулирование биткоин-платежей).

После подтверждения доказательства погашения происходит выплата вознаграждения подписантам. Владелец FRT получает свои депонированные резервы (в случае, если депозит был погашен раньше срока), а владелец TDT получает оставшуюся от суммы погашения часть. Как и с суммой погашения, сумма, которую получает каждая сторона в случае успешного погашения, может меняться в зависимости от следующих влияющих факторов:

- владелец TDT;
- владелец FRT;
- собственно погашающая сторона;
- состояние депозита.

В Таблице потока депозитных платежей перечислены различные возможные комбинации и соответствующие суммы погашения, которые должна внести погашающая сторона, включая 3 возможные стороны системы – A, B и C.

Утверждение подписи

После утверждения запроса на погашение на основной платформе, подписанты должны создать подпись с помощью запрашиваемой хэш-функции для создания подписи по транзакции погашения. В распоряжении подписантов – 3 часа, в течение которых они должны создать либо подпись, либо подтверждение погашения. В противном случае они подвергаются наказанию.

После подачи действующей подписи доказательство погашения все равно требуется, но срок выполнения задачи в целом увеличивается до 6 часов.

Как обсуждалось ранее, смарт-контракт на главной платформе, управляющий депозитом, имеет полную информацию, необходимую для расчета хэш-суммы подписи для транзакции погашения. Сюда входит пороговой открытый ключ подписантов. Используя этот открытый ключ, а также хэш подписи и запрос на погашение, смарт-контракт получает информацию о действенности подписи, а также о том, что подпись на дайджесте запрашивалась в качестве части процесса погашения.

Разрешение на регулирование биткоин-платежей

Поскольку Биткоин-платежи определяются степенью нагрузки сети и другими крайне непредсказуемыми факторами, запрашивающая сторона не может выбрать соответствующий платеж. Подписантов наказывают, если не предоставляется доказательство погашения, или если они сделали подпись без четко обозначенных полномочий. Это может стать причиной создания безвыигрышного сценария для подписантов, в котором они не смогли бы добиться подтверждения запрашиваемой транзакции при текущих платежных условиях, и в конце концов могли бы быть наказаны даже несмотря на честное поведение в рамках системы.

К сожалению, мы не можем полностью положиться на то, что запрашивающая сторона постоянно будет оставаться онлайн или честно обновлять коэффициенты платежей. Следовательно, система требует определенного механизма, который мог бы справедливо регулировать коэффициент платежей без разрешения запрашивающей стороны.

Простейшая схема – позволить подписантам увеличивать платеж без разрешения запрашивающей стороны после истечения указанного срока. По сути, мы позволяем подписантам увеличивать платежи линейно каждые 4 часа. Другими словами, если платеж обозначен как f, спустя 4 часа подписанты могут уведомить контракт об увеличении суммы до 3f. Это гарантирует, что транзакция погашения в конечном счете будет подтверждена в блокчейне биткоина в размере минимального коэффициента платежа при условии текущей перегруженности сети.

Чтобы защитить подписантов от неоднократно запрашиваемых повышений платежа, нужно, чтобы они действительно предоставляли подпись на каждом этапе платежа. Это гарантирует, что каждый коэффициент платежа был действительно испробован перед запрашиванием повышения.

Управление

Идея

Идея управления проста: управляй как можно меньшим количеством параметров системы. Такое ограниченное видение управления означает полагание скорее на общественные обновления – включая новый экземпляр системы, – нежели на обновления управляемого контракта.

Общественные обновления подобны хардфоркам (изменениям, которые несовместимы с предыдущими версиями). Они требуют подавляющего экономического консенсуса, поскольку новый токен-контракт и другие новые контракты будут нуждаться в координации и утверждении через рынок. Препятствие для общественного обновления намного выше, чем для других общих парадигм управления.

Ограниченное управление, включенное в проект системы, следует нескольким принципам, которые заключаются в следующем:

1. Управление должно оказывать влияние только на новые депозиты всякий раз, когда представляется такая возможность. Каждый депозит должен иметь предсказуемое поведение в долгосрочной перспективе, несмотря на выбор управления.

2. Управление должно соблюдать задержку времени, если это возможно, в целях предоставления пользователям времени для того, чтобы приспособиться к изменениям в системе.
3. Роль управления должна быть передана надежной нейтральной третьей стороне или конечной децентрализации.

Функции управления

Все функции и отсрочки управления перечислены ниже. Каждая из них должна быть востребована владельцем контракта. Для функций, которые предусматривают отсрочки, есть эквивалент finalize<Function> для begin<Function>, который может завершить внесенное изменение после определенной отсрочки (например, beginLotSizesUpdate/finalizeLotSizesUpdate).

Таблица 1. Функции управления

Функция	Отсрочка	Влияние на существующий депозит
emergencyPauseNewDeposits()	нет	отсутствует
beginSignerFeeDivisorUpdate(uint16 divisor)	2 дня	отсутствует
beginLotSizesUpdate(uint64[] _lotSizes)	2 дня	отсутствует
beginCollateralizationThresholdsUpdate(uint16 initial, …)	2 дня	отсутствует
beginEthBtcPriceFeedAddition(address ethBtcPriceFeed)	90 дней	Только при снижении ценообразования

emergencyPauseNewDeposits()

Неизменный код и безопасность пользователя в случае обнаружения новых уязвимых мест часто рассматриваются как противоречия. На самом деле, многие системы смарт-контрактов в большей степени полагаются на доверенный ключ администратора, делая возможными обновления произвольного контракта. Конечно, если такая возможность существует, зачем вообще использовать блокчейн?

Вместо обновления контракта, tBTC v1 включает возможность приостановить новый депозит на 10 дней. Такая возможность может быть использована только один раз, и она не оказывает влияния на существующие депозиты или функциональность другой системы. После истечения десятидневного срока новые депозиты снова получают возможность приостановки.

Такая возможность дает возможность команде разработчиков приостановить новые депозиты в случае угрозы нулевого дня (вредоносной программы, использующей уязвимости программного обеспечения для атаки на вычислительную систему) и тем самым выиграть драгоценное время, чтобы уберечь пользователей от возможного риска для их обеспечений (средств). Так как существует намерение использовать эту возможность при сложных обстоятельствах, механизм был структурирован таким образом, чтобы команда разработчиков не могла использовать ее каждый раз в качестве «универсальной аварийной кнопки».

По истечении 365 дней депозиты более не могут быть приостановлены, и любой призыв к специальной процедуре emergencyPauseNewDeposits() должен быть возвращен к первоначальным параметрам.

beginLotSizesUpdate(uint64[] _lotSizes)

Владелец контракта может обновить размеры лотов, разрешенные для новых депозитов, после двухдневной отсрочки.

Всегда должен быть в наличии размер лота одного биткоина, способного предохранять его от действий по типу непреднамеренного использования аварийной кнопки. Любое обновление, которое не включает размер лота одного BTC, должно вернуться к первоначальным показателям.

beginSignerFeeDivisorUpdate(uint16 divisor)

К сожалению, проект tBTC v1 не оставляет возможности для исследуемых рынком вознаграждений для подписантов. Вместо этого функция установления размера вознаграждения для подписантов делегируется управлению.

Владелец контракта может обновить делитель для значения вознаграждения подписантов после двухдневной отсрочки, влияя при этом на новые депозиты. Вознаграждение ограничивается 0.03% - 10.0%. Это необходимо для того, чтобы предотвратить слишком малое или слишком большое изменение вознаграждения подписантов.

Любое изменение, находящееся вне этого диапазона, должно вернуться к первоначальным показателям.

beginCollateralizationThresholdsUpdate(uint16 initial, …)

Владелец контракта может изменить пороги залогового обеспечения для новых депозитов после двухдневной отсрочки.

В то время как изменения воздействуют прямо только на новые депозиты, если владелец контракта был в сговоре с тем, кто совершил атаку, они (эти изменения) могут навредить привязке. По этой причине любой начальный порог ниже 100% или свыше 300% должен вернуться к первоначальным параметрам.

beginEthBtcPriceFeedAddition(address ethBtcPriceFeed)

Владелец контракта может добавить новое, подкрепляющее соотношение ETHBTC-ценообразования для всех депозитов после отсрочки в 90 дней. Обратите внимание, что эта отсрочка значительно дольше, чем другие отсрочки, контролируемые правлением.

Ценообразование должно отслеживаться в списке, и ценообразование в данном списке должно использоваться только в том случае, если все ранее добавленные факторы ценообразования являются неактивными.

Ценообразование обеспечивает функцию скрипта Peek, которая возвращает значение цены из начала очереди наряду с логической индикацией, отображающей активность подачи. Если вторая цена в данном ответе является неправильной, строка считается неактивной, и потому должна использоваться следующая по списку строка.

Данное обновление делает возможным прямое планирование преднамеренного списания начального курса медианайзера (смарт-контракт с курсами цен, которые помещают непосредственно в него и из которых берется усредненное значение). Продолжительное время выполнения оставляет всем существующим депозиторам, которых может так или иначе коснуться новая цена, достаточно времени для закрытия открытых депозитов и извлечения средств из них.

Данное обновление также может быть использовано при работе с неожиданными прекращениями активности курса, хотя в данном случае система восстанавливается в течение 90-дневного срока.

Приложение

Выплаты в счет погашения и сценарии оплаты

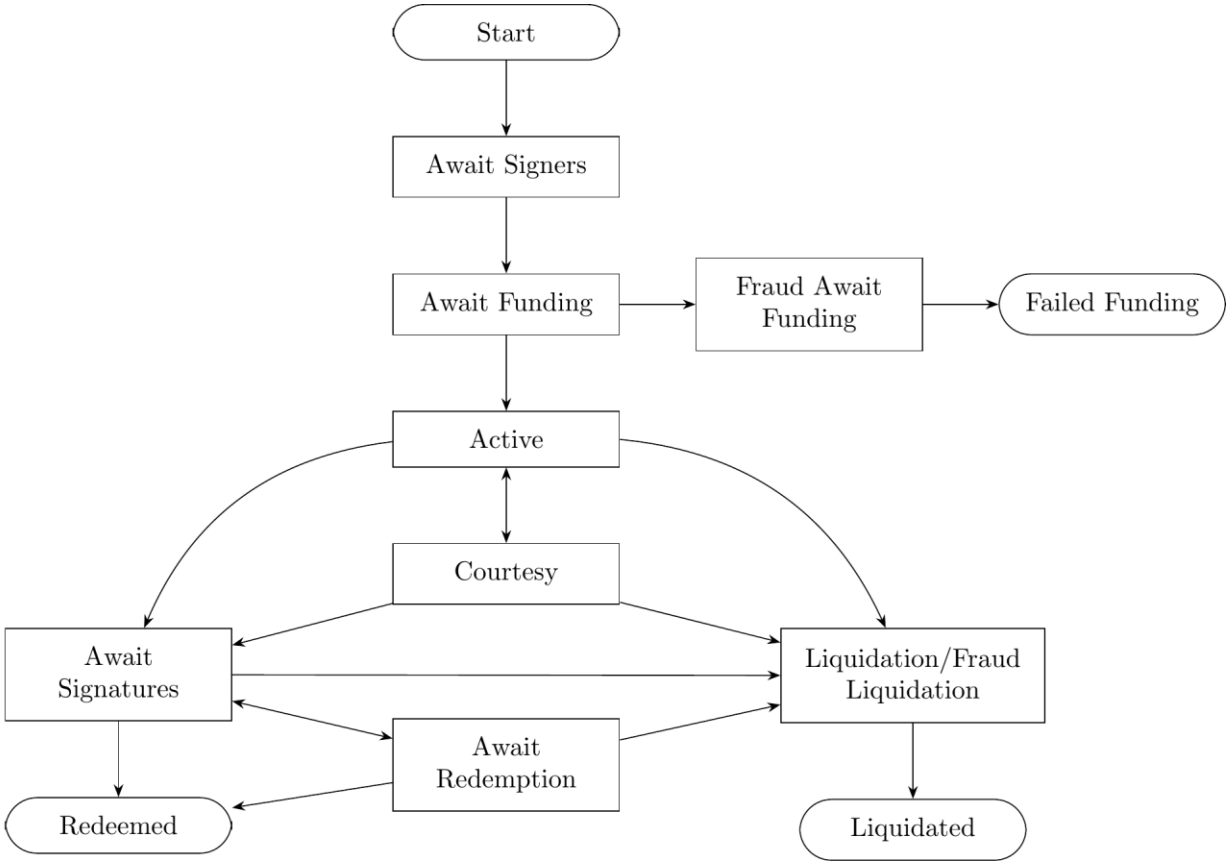
Для BTC размера лота, в котором 1 BTC соответствует 1 TBTC, а вознаграждение подписантам составляет 0,005 TBTC (50 основных точек), представленная таблица описывает суммы,

выделенные каждой стороне в момент погашения досрочного или срочного депозита, в зависимости от того, кто владеет TDT и FRT. Также это зависит от того, кто стал инициатором процесса погашения. В таблице представлены 3 возможные стороны – A, B и C. В перечисленных ниже сценариях раскрыты ситуации, в которых одни и те же стороны являются владельцами сразу двух токенов и инициируют процесс погашения. Разные стороны имеют свои роли и возможности.

Обратите внимание, что все эти сценарии могут быть концептуализированы, так как владелец токена TDT, всегда получающий 1 TBTC, привык к погашению депозита; когда владелец токена TDT погашает свой собственный депозит, то TBTC, который он получает, будет изыматься у него, поэтому в данном случае он просто в меньшей мере остается в долгу. Похожим образом владелец FRT всегда получает обратно депонированные средства, когда погашает депозит досрочно, поэтому в случаях, когда погашающая сторона является держателем FRT, она просто не должна выплачивать вознаграждение подписантам во время погашения.

Приложение

Автомат состояний депозита и погашения



Мы формируем каждый депозит по принципу автомата состояний.

Поток финансирования

Обзор

Поток финансирования – процесс, устанавливающий депозит. Он финансируется в BTC. После успешного финансирования источник финансирования (спонсор) становится собственником нового депозита и получает возможность создать новый TBTC. Чтобы начать процесс финансирования, спонсор размещает небольшое залоговое обеспечение и создает запрос на создание нового хранилища для попечительства над BTC. Если такое хранилище успешно создано, то контракты хранения передают депозиту открытый ключ группы подписантов. Если создания

такого хранилища по какой-либо причине не происходит, процесс финансирования прерывается, а система хранения выбирает меру наказания для сторон, которые послужили причиной срыва.

После завершения формирования хранилища спонсор отправляет BTC на содержание хранилища в целях засвидетельствования хэш-адреса открытого ключа (p2wpkh). Упомянутый BTC становится основополагающим обеспечением для нового депозита. Спонсор доказывает валидность депозита через SPV -доказательство без сохранения состояния, свидетельствующее о присоединении к блокчейну Биткоина. Если спонсору не удается выполнить эту передачу своевременно, то процесс финансирования прерывается, а обеспечение спонсора утрачивается им.

После того, как залоговое обеспечение BTC становится доказанным, депозит переходит в активное состояние. Теперь спонсор имеет право изъять TBTC вплоть до суммы обеспечения BTC (сумма меньше, чем отложенные TBTC). Результатом процесса финансирования может стать только активное состояние депозита либо прерванное состояние.

Упрощенная верификация платежей (SPV)

Несмотря на то, что полное обсуждение доказательств по алгоритму SPV находится за пределами представленного документа, важно дать понимание их особенностей, поскольку множество важнейших процессов системы полагаются именно на предположения безопасности алгоритма SPV. Доказательства SPV используются при финансировании и погашении, а также в процессах, связанных с мошенничеством, для предоставления главной платформе информации о состоянии удаленной цепи. С практической точки зрения, нет никакого другого способа для получения основной платформой информации о состоянии или истории удаленной цепи.

Объективность в доказательстве работы

Доказательства SPV, которые используются в этой системе, полагаются на свойство PoW (доказательства работы). Такое свойство называется объективностью. Проще говоря, доказательство работы не может быть поддельным, и никакая информация извне не требуется для того, чтобы проверить его подлинность.

Не зная истории цепи, мы можем исследовать заголовок блока биткоина и определить с высокой долей вероятности, какое количество хэшей было задействовано для его создания. Количество хэшей, которое потребовалось для создания заголовка, представляет собой не поддающуюся подделке стоимость, свойственную данному заголовку, вне зависимости от его контекста или истории.

Сравните это с Proof of Stake (подтверждение доли) – алгоритмом, в котором стоимость создания заголовка зависит от всей его истории вплоть до сегодняшнего дня. Мы не можем достоверно знать, представляют ли подписи дольщика набор текущих сервисов без полной истории. Другими словами, Proof of Work даже обособленно до сих пор имеет значение, в то время как Proof of Stake – нет.

Пока возможна проверка систем Proof of Stake по алгоритму SPV, модель безопасности в корне отличается. Кроме того, подходы к ее реализации гораздо более дорогостоящие, чем проверка объективных систем по алгоритму SPV. По сути, этот раздел касается только вопросов верификации Proof of Work, а будущие версии системы, использующие метод SPV для проверки систем Proof of Stake, мы оставим на потом.

Модель безопасности

В Консенсусе Накамото каждый узел следует за наиболее сильной действительной цепью. Определение «наиболее сильная» относится к метрической системе объективного доказательства

работы. Цепь с наибольшим скоплением работы считается самой сильной. Действительность в рамках консенсуса участвует в немного большей степени.

В теории, узлы утверждают оценку новой информации в соответствии с комплексом правил, а также отклонение всего, что противоречит указанным правилам. На практике эти правила определяют блоки, состоящие из заголовков и транзакций, описывают формат транзакций, а также предоставляют некоторые правила, программируемые пользователями – такие, как Script и EVM.

Узлы, следующие протоколу, всегда будут принимать одинаковые решения о сроке действия и выбирать наиболее сильную цепь с заголовком, включающую только действительные транзакции и блоки. Следовательно, честные узлы всегда будут достигать одного и того же состояния, что, нужно сказать, позволит всегда достигать консенсуса.

Модель безопасности алгоритма SPV значительно слабее, чем модель Консенсуса Накамото, однако остается достаточной для достижения поставленных нами целей. Модель SPV проверяет работу заголовков, однако применяет только небольшое подмножество правил обоснованности. По сути, верификаторы SPV делают предположение о том, что майнеры не потратят ресурсы, создавая доказательства работы на пике недействительных блоков или транзакций. Они проверяют действительность некоторых заголовков, в том числе – действительность работы, включенной в данные заголовки, но не верифицируют каждую транзакцию. Вместо этого, верификаторы SPV проверяют только те транзакции, в которых они заинтересованы. В контексте tBTC мы заинтересованы только в конкретных UTXO в сети биткоина, поэтому мы отдаем предпочтение только тем транзакциям и заголовкам, которые относятся к упомянутым UTXO.

Если предположение оказывается неверным, модель безопасности также может выйти из строя. Мы называем это «поддельными» доказательствами и поддельными заголовками, потому что они не являются семантически действительными транзакциями или заголовками биткоина.

Мы доказываем, что поддельные доказательства будут крайне редким явлением. Наше убеждение происходит из объективной экономики алгоритма Proof of Work. Если майнер решает предоставить ресурсы для производительной работы на пике недействительной транзакции, он должен отказаться от вознаграждения за майнинг, в то время как он продолжает принимать на себя расходы на электричество и аппаратуру, которые задействуются в процессе майнинга. Майнер отказывается от вознаграждения за майнинг, поскольку недействительные транзакции никогда не включаются в основную цепь Биткоина. Такая транзакция будет отклонена всеми в полной мере действительными узлами. Следовательно, создание поддельного доказательства имеет далеко идущие последствия. Мы доказываем, что система экономически безопасна до тех пор, пока стоимость создания поддельного доказательства высока. Также мы утверждаем, что сумма, которую можно получить путем создания фальшивой подписи, на порядок меньше стоимости, затраченной на майнинг.

Безопасность SPV-систем также выигрывает от неотъемлемого предположения модели Консунсуса Накамото. Оно состоит в том, что ни одна сторона, совершающая атаку, не может получить более, чем 50% хэшрейта. Если предположить, что это действительно так, то можно сделать вывод: ни один нападающий не может сгенерировать доказательство работы биткоина быстрее, чем основной блокчейн биткоина.

Это подразумевает, что честные заголовки генерируются (в допустимых пределах Пуассоновского распределения) быстрее, чем мошеннические. Если расширить данную модель, то можно увидеть, что, если ни у одного нападающего нет больше, чем n-число текущего хэшрейта биткоина (где n >= 2), то честные заголовки могут быть сгенерированы в (n^{-1} – 1) количество раз быстрее. Например, нападающий, который контролирует 25% (1/4) хэшрейта биткоина, мог бы

генерировать заголовок в среднем каждые 40 минут. Основная цепь, замедленная потерей указанных 25%, могла бы генерировать заголовки каждые 13 1/3 минут, то есть в 3 раза быстрее. Чтобы извлечь преимущество из данной ситуации, доказательство должно передавать некую свежую информацию, которая ранее была неизвестна нападающему. Например, это может быть предыдущий заголовок блока или новый хэш открытого ключа. Это обеспечивает более низкую привязку ко времени, в течение которого нападающий начинает создавать поддельное доказательство.

Релейные сети

Наиболее простой принципиально новой системой SPV является реле. В таких системах каждый заголовок доказательства работы предоставляется и верифицируется основной платформой. Смарт-контракты основной платформы следят за наиболее известными заголовками, а также всеми увиденными ранее заголовками. SPV-доказательство в системе реле демонстрирует, что транзакция подтверждается лучше всего видимым заголовком и является достаточно глубоко вложенной, поэтому отсутствие ее подтверждения невозможно.

Каждый дополнительный заголовок в релейной системе подтверждения обеспечивает безопасность всех предыдущих заголовков. Таким образом мы становимся более уверенными в событиях «старшей» цепи по прошествии времени.

SPV без сохранения состояния

В случаях, когда системы реле отказываются от проверки действительности, системы SPV без сохранения состояния отказываются не только от проверки действительности, но и от следования наиболее сильной цепи. По сути, системы SPV без сохранения состояния ничего не отслеживают. Вместо этого SPV-доказательства без сохранения состояния полностью полагаются на объективную работу, которая присутствует в отдельной части заголовков.

SPV-доказательство без сохранения состояния состоит из:

- одной и более транзакций;
- доказательств Меркла по включению указанных транзакций;
- ряда последовательных заголовков на пиковой точке транзакций.

Верификатор может исследовать заголовки и предоставлять доказательства объективного количества показателя качества. Это доказательство основывается на объеме работ в указанных заголовках. Любая сторона, заинтересованная в использовании текущего состояния и исторических данных в информации SPV-доказательств без сохранения состояния, может определить, что стоит сделать: принять или отказаться от него, исходя из качества доказательства.

SPV без сохранения состояния являются относительно недавней работой, инициатором которой стал стартап Summa. Их описание дано в технической работе по кросс-чейн аукционной системе Summa. Непреодолимыми преимуществами этих SPV являются размер и эффективность затрат.

SPV-доказательство без сохранения состояния занимает менее одного килобайта, при этом каждое такое доказательство после утверждения «сбрасывается». С другой стороны, релейная система сохраняет каждый он-чейн заголовок. Это значит, что реле со временем будет линейно расходовать увеличивающееся пространство состояния. Эксплуатационные расходы и так уже непомерно высоки, о чем свидетельствует сбой в функционировании моста BTCRelay в декабре 2017 года. При уже завышенных расходах на хранение он-чейн и высокой вероятности введения аренды в наиболее крупных основных платформах, полагание на стабильное реле выглядит недальновидным. Высшая система, которая жизнеспособна сегодня, в будущем может такой не быть.

Мы утверждаем, что для более ранних транзакций безопасность SPV без сохранения состояния эквивалента такому же уровню, который предоставляет и реле. Нападающей стороне придется затратить то же количество хэшей для предоставления фальшивых заголовков в систему реле, которое она бы затратила на предоставление верификатору SPV без сохранения состояния доказательства о достаточной работе.

Тем не менее, если сравнивать с доказательствами в рамках релейной системы, SPV-доказательства без сохранения состояния не получают со временем достаточного уровня безопасности без расширения каждого из них для включения новых заголовков. В данном случае важно то, что известен срок давности транзакции. Если такая информация неизвестна, то совершающая нападение сторона может начать создание доказательства задолго до наступления срока его предоставления. Таким путем злонамеренная сторона получает преимущество в основной цепи.

Система релейной передачи данных получает своевременные гарантии на каждом блоке, поскольку каждый новый заголовок должен ссылаться на основной заголовок, непосредственно предшествуя ему. Но SPV-доказательство без сохранения состояния должно получить свою своевременную гарантию от каждого внешнего источника.

Стандартизированная конструкция SIGHASH-флагов

Обзор

В целях выполнения подписания Биткоин преображает транзакции, используя процесс, который известен как алгоритм SignatureHash (sighash). Первоначально данный алгоритм имел множество недостатков и острых краев. В SegWit-скриптах алгоритм был изменен для того, чтобы следовать коду BIP143, определяющему новый алгоритм верификации подписей при совершении транзакций. При этом legacy-адреса (Биткоин-адреса стандартного формата) до сих пор используются в оригинальном алгоритме.

Цель sighash-алгоритма – взять на себя обязательства по выбранным аспектам транзакции в подписанном дайджесте. Это демонстрирует намерение подписанта относительно данного вопроса. Конкретно код BIP143 берет на себя следующие вопросы (их расположение ниже произвольно):

- один или все входы;
- ни один из, один или все выходы;
- конкретная превосходящая функция, которая удостоверяется данной подписью;
- скрипт открытого ключа или код скрипта погашения, блокирующего эту превосходящую функцию;
- порядок входа, который расходует данную превосходящую функцию;
- версия транзакции;
- время блокировки транзакции.

Перечисленные функции совершаются через алгоритм double-sha256 упорядоченной строки. Данный дайджест подписан и может быть воспроизведен любой стороной, проводящей проверку транзакции (при условии, что у них есть доступ к историческим данным цепочки для подтверждения превосходящей стоимости).

Использование алгоритма Sighash для вычислений – ключевой этап процесса заключения консенсуса в рамках биткоина.

Поскольку группа подписантов имеет право воздержаться от создания подписей, движение процесса погашения заставляет их обеспечить действительную подпись в течение определенного

периода. Это подразумевает, что поток погашения должен быть способным оценить средства подтверждения действительности в данном контексте.

Поскольку конечной целью является именно погашение, «валидная» подпись является тем фактором, который засвидетельствует транзакцию, отправляющую средства на хэш открытого ключа, который запрашивался в начале процесса погашения. Для того, чтобы проверить, что предоставленная подпись свидетельствует о такой транзакции, нам необходимо позволить нашим контрактам подтверждать подписанный sighash-дайджест.

Безусловно, наиболее простым путем сделать это является создание канонической транзакции. Таким образом мы можем воплотить в жизнь значительно уменьшенный набор функций кода BIP143, в то же время оставаясь способными оценить действительность подписи в процессе погашения. Это позволит нам, вместо расчета сайхэша транзакции входа, определить этот сайхэш и усилить конструкцию транзакций, которая ему соответствует. Таким образом, контракт может запрашивать максимально точные транзакции погашения с минимальными расходами.

Sighash канонического погашения

BIP143 следует данному общему формату:

Для более подробной информации о различных типах меток Sighash смотрите описание от стартапа Summa.

Поскольку нам не нужно использовать временные метки в наших транзакциях погашения, мы запрещаем их использование, позволяя себе непосредственно стандартизировать многие элементы. Также мы запрещаем использование любых sighash-флагов кроме SIGHASH_ALL. Таким образом мы можем стандартизировать их. Здесь мы расположили элементы со стандартизированными шестнадцатеричными строками.

--изображение--

Запрет для транзакции иметь более одного входа или выхода дает нам одно дополнительное преимущество. Указанный в пункте 3 (схема выше) код hashSequence определяется как «double SHA256 сериализации n-чередования всех входов». Имея один вход и устраняя его временные метки, мы можем стандартизировать это таким образом:

--изображение--

Далее, мы заполняем строки информацией о том, что контракт имеет открытый доступ, начиная с деталей UTXO, находящегося под попечительством. Контракт по депозиту подтвердил SPV-доказательство о финансировании и сохранил его стоимость, как и его преимущество. Код BIP143 определяет hashPrevouts как «double SHA256 сериализации всех превосходящих значений входа». Поэтому мы можем заполнить столбцы 2,4 и 6 (см. ниже), используя известную информацию:

--изображение--

Значение scriptCode также доступно в контракте, поскольку оно происходит из хэша порогового открытого ключа подписантов. В соответствии с BIP143, «для программы доказательства доступен scriptCode 0x1976a914{20-byte-pubkey-hash}88ac».

--изображение--

Неизвестным для нас фактором в контракте на момент погашения остается только hashOutputs. Это имеет смысл, поскольку контракт располагает сведениями о месте хранения средств, но не имеет данных о том, куда они могут быть отправлены в момент погашения. Как обычно, мы обратимся к коду BIP143, который гласит: «hashOutputs – это double SHA256 сериализации всех

значений выходов (восьмибайтный обратный порядок) с scriptPubKey». В случае со множественными выходами он может быть довольно объемным, но, как упоминалось ранее, мы можем стандартизировать транзакции с единственным выходом. Это означает, что происходит погашение суммы double-sha256 из 8-byte LE (размер меньше, чем вознаграждение за майнинг), а скрипт открытого ключа включает хэш скрипта погашающей стороны. В нашем процессе погашения оба эти фактора установлены пользователем в момент запроса. Это значит, что контракт имеет доступ к ним как к аргументам функции, когда требуется, чтобы группа подписантов создала подпись. Следовательно, контракт может определить точный дайджест для этой подписи:

--изображение--

Достаточно просто выразить это в виде чистой функции на языке программирования контрактов Solidity:

--изображение--

Словарь терминов

Host chain – цепочка, в которой происходит выпуск TBTC

Keep – безопасные вычислительные установки, активирующие процесс подписания tBTC

PKH – хэш открытого ключа

Random beacon – безопасный, проходящий верификацию источник допустимой случайности на основной платформе

tBTC

Deposit. Депозит – это ключевой компонент в структуре системы. Каждый депозит представляет определенный комплекс подписантов, создающий открытый ключ в системе Bitcoin и принимающий единственный UTXO биткоина, из которого может быть выведен токен TBTC.

Deposit beneficiary. Депозит имеет единственный бенефициарный счет на Эфириуме. Бенефициарий имеет право на некоторые средства в виде вознаграждения, получаемые при погашении депозита.

Deposit request. Запрос на выбор подписантов и создание новой пары ключей ECDSA. Успешный запрос позволяет подготовить новый биткоин-адрес к принятию финансирования. То же касается и подписантов с залоговым обеспечением.

Lot size. Наиболее подходящий размер BTC UTXO профинансированного депозита. Стандартизация размеров лота в депозитах упрощает процесс погашения BTC-депозитов, а также оценку депозита рынком.

Signing bond. Обязательство, которое принимают подписанты перед финансированием депозита. Это залоговое обеспечение, которое гарантирует, что подписанты будут наказаны за бездействие или мошенничество.

Reserved TBTC. Сумма TBTC, которая не может быть изъята из нового депозита. Удержанные в процессе финансирования депозита токены создают резервы, которые используются для выплаты вознаграждения подписантам в течение срока депозита.

Cross-chain communication

Consensus relay. Упрощенная система верификации, осуществляющая отслеживание цепи на основе какой-либо другой цепи (например, BTCRelay). Это кросс-чейн механизмы, которые отслеживают состояния консенсуса в другой цепи.

SPV. Упрощенная верификация оплаты.

Stateless SPV. Не отслеживаемое в пределах цепи SPV