Открытые и закрытые блокчейны

Часть 2: Общедоступные блокчейны

White Paper

(перевод на русский)

BitFury Group

в сотрудничестве с Jeff Garzik (jeff@bloq.com)

24 октября 2015 (Версия 1.0-ru)

Аннотация

Решения на основе блокчейнов являются одним из ведущих направлений исследований для финансовых учреждений и для других применений. В настоящее время идет обсуждение, подходят ли существующие блокчейны (используемые в биткойне и других криптовалютах) для применения в коммерческом контексте, и является ли их открытость и устойчивость к цензуре подходящими свойствами для подобных приложений. Мы приводим аргументы в пользу использования общедоступных (англ. permissionless) блокчейнов и открытых протоколов блокчейнов для создания финансовых систем учета и реестров; при этом мы уделяем внимание биткойновскому блокчейну как самому коммерчески успешному и безопасному общедоступному блокчейну. Мы изучаем возможности применения общедоступных блокчейнов в частных приложениях за счет использования окраски монет, одноранговых каналов платежей и обработки транзакций известными валидаторами.

История версий

Версия	Дата	Описание изменений
1.0	20 окт. 2015	Начальная версия (англ.)
1.0-ru	24 окт. 2015	Начальная версия (перевод на русский)

Биткойн [1] — одноранговая цифровая система платежей, решающая проблему низкой скорости обработки и возможной цензуры финансовых транзакций в централизованных системах. В отличие от централизованных баз данных, используемых в современных финансовых средах, биткойн полагается на распределенную базу данных, называемую *блокчейном*, в которой транзакции собраны в криптографически защищенные блоки. По сравнению с традиционными финансовыми решениями, биткойн отличается в трех основных аспектах:

- **Децентрализация.** Доверие к биткойновскому блокчейну возникает не вследствие доверия к учреждению, централизованно управляющему обработкой транзакций, а из-за математических свойств системы и высокой экономической стоимости атаки на систему. В соответствии с этим, каждый пользователь биткойна может самостоятельно и независимо проверить текущее состояние системы и прийти к тем же выводам, что и остальные узлы сети.
- **Устойчивость к цензуре.** Сеть биткойна является общедоступной – любой пользователь может передать любую транзакцию, соответствующую протоколу биткойна; такая транзакция будет с высокой вероятностей включена в блокчейн. Аналоггично, любой пользователь может участвовать в процессе добавления транзакций в блокчейн (*майнинг*).
- **Неизменяемость.** Одна из основных целей блокчейна – невозможность или, во всяком случае, высокая цена удаления информации из блокчейна (т. е. обращение транзакций).

Идея блокчейна — определяющая инновация в биткойне; блокчейн было воссоздан с различным успехом во многих цифровых валютах, появившихся после биткойна, таких как Ripple [2], Litecoin [3], Ethereum [4], BitShares [5], Nxt [6], и т. д. Блокчейны в этих валютах отличаются от используемого в биткойне особенностями протокола (например, способом обеспечения неизменяемости заголовков блоков транзакций); в то же время базовые аспекты блокчейна в основном остаются нетронутыми.

Организации, работающие с реестрами и системами финансового учета, не торопятся использовать имеющиеся общедоступные блокчейны. В разделе 1 мы исследуем часто называемые причины прохладного отношения к общедоступным блокчейнам в финансовом секторе: проблему установления личностей обработчиков транзакций, теоретическое отсутствие завершенности транзакций и уязвимость к атакам. В разделе 2 рассматриваются решения, позволяющие в полной мере использовать силу общедоступных блокчейнов для построения реестров и систем учета. В разделе 3 мы обсуждаем преимущества общедоступных блокчейнов и стандартизованных протоколов блокчейнов; мы утверждаем, что общедоступные блокчейны могут создать вездесущую одноранговую основу для инноваций в области финансов. В первой части статьи содержится введение в блокечйны, обзор текущего состояния внедрения блокчейнов и описание эксклюзивных блокчейнов.

1. Воспринимаемые недостатки общедоступных блокчейнов

Блокчейн-технология предоставляет распределенную, устойчивую к отказам и искажениям данных среду для создания реестров, которая может использоваться, например, для создания систем учета в финансовых приложениях. В то же время существуют несколько аргументов, делающих использование существующих общедостпуных блокчейнов проблемным с точки зрения приложений, использующих системы учета и реестры. Мы рассматриваем эти проблемы, фокусируясь на биткойне как на самом коммерчески успешном общедоступном блокчейне; аналогичные проблемы сохраняются и для других блокчейнов, используемых в криптовалютах.

1.1. Процесс майнинга

Проблема. Биткойн — общедоступная (инклюзивная) система; блок в ней может создать любой пользователь сети при условии, что в его распоряжении есть достаточно вычислительных ресурсов для удовлетворения критерию корректности заголовка блока (т. е. доказательству работы) С другой стороны, согласно многим законодательным системам личности обработчиков финансовых транзакций должны быть установлены. Теоретически, анонимность майнеров делает проблемной возможность использования биткойна как среды для обработки финансовых транзакций.

На практике, начиная с 2013 года майнинг осуществляется с использованием специализированного оборудования (ASIC-ов); в каждый момент времени количество майнеров-индивидов сравнительно мало, поскольку майнеры объединены в крупные пулы. Личность майнера определенного блока можно установить исходя из свойств coinbase-транзакции этого блока; восстановленные таким образом личности часто показываются на веб-сайтах биткойн-проводников [7, 8]. Для четкой идентификации личности майнера, он может включить цифровую подпись блока в coinbase-транзакцию; см. приложение A для более детального описания.

Если некоторое учреждение хочет удостовериться в том, что его транзакции обрабатываются сертифицированными майнерами, оно может посылать транзакции по защищенному каналу связи прямо этим майнерам вместо того, чтобы распространять транзакции по сети; прием в блоки нетранслированных транзакций — приемлемое поведение с точки зрения протокола биткойна. Детали этой модели описаны в разделе 2.1.

1.2. Соображения конфиденциальности

В то время как сотрудничество между майнерами и финансовыми учреждениями способно решить проблему нежелательной огласки неподтвержденных транзакций, это сотрудничество оставляет нерешенной проблему сохранения конфиденциальности клиентов.

Проблема. Так как вся история транзакций в биткойне является публичной, клиенты, тран-

закции которых находятся в биткойновском блокчейне, могут быть обеспокоены тем, что знание истории их транзакции может быть использовано с противоправными намерениями.

в биткойне отсутствует идентификация пользователей; система использует схему с открытым ключом для идентификации владения биткойнами. Таким образом, пользователя, использовавшего один и тот же открытый ключ (или, что эквивалентно, один и тот же биткойновский *адрес*) для нескольких платежей, можно идентифицировать с использованием истории транзакций. Эту проблему можно смягчить при использовании иерархических детерминированных (англ. hierarchical deterministic) кошельков [9]. В таких кошельках новый адрес генерируется для каждой последующей транзакции пользователя. Более того, из-за гомоморфного свойства криптографии с эллиптическими кривыми, используемой в биткойне, для создания этих адресов не нужно знания соответствующих секретных ключей; это делает HD-кошельки безопасным решением для больших финансовых фирм. Для внешнего наблюдателя не существует простого способа связать воедино адреса, сгенерированные кошельком. Более сложный пример, использующий гомомрофное свойство эллиптических кривых, — это протокол платежа по контракту (англ. pay-to-contract protocol) [10], согласно которому создается одноразовый адрес для каждого платежа, зависящий от его спецификации (например, количества и типов приобретенных товаров или услуг).

Закрытые блокчейны, в особенности работающие со смарт-контрактами, могут использовать технологию разделения секретов [11]. Это является целью проекта Enigma [12]. В случае, если блокчейн использует непотраченные входы транзакций (UTXO) подобно биткойну, секретами будут значения, связанные с выходами (т. е. посторонний наблюдатель не должен иметь возможность определить сумму активов, которыми оперируют транзакции). У узлов сети не будет доступа к этим значениям, а только к их зашифрованным представлениям. Целью схемы шифрования будет проверка корректности транзакции без расшифровки значений выходов, т. е. проверка следующих условий:

- значение каждого выхода является неотрицательным;
- сумма значений выходов не превышает или, если в системе отсутствуют комиссии за транзакции, в точности равна сумме выходов, тратящихся транзакцией.

Системы, предоставляющие возможность проверки таких условий уже реализованы на основе разделения секретов (например, [13]). В контексте блокчейнов зашифрованные значения UTXO, соответствующие приведенным выше условиям реализованы в проекте Sidechain Elements компании Blockstream [14].

1.3. Криптовалюты как активы с правом собственности на предъявителя

С легальной точки зрения, биткойн и другие криптовалюты можно классифицировать как активы, собственность на которые принадлежит предъявителю (англ. bearer assets). Это означает, что собственность активов не отмечается в специализированном реестре; право соб-

ственности определяется простым знанием соответствующего секретного ключа по аналогии с тем, как владельцем наличных денег является лицо, имеющее наличность. Из аннотации исследовательской статьи по биткойну немедленно следует, что этот вид владения активами был заложен в дизайн системы: «Полностью одноранговая версия электронных денег позволила бы совершать онлайн-платежи между участниками сети, минуя финансовые учреждения» (перевод наш). Поскольку большинство ценных бумаг представляет собой регистрируемые активы (т. е. активы, собственность над которыми определяется не только фактическим владением), существует мнение, что блокчейн биткойна не подходит для хранения подобных активов [15]. Однако есть несколько соображений, делающих это мнение не совсем очевидным.

Во-первых, передача цифровых активов не происходит при помощи встроенных средств протокола биткойна; протокол не замечает цифровых активов и способен определять и верифицировать передвижение средств исключительно в биткойнах. Системы, интегрирующие цифровые активы с биткойновским блокчейном, используют различные протоколы покраски монет (англ. colored coins protocols) для кодирования выпуска и перемещения активов (см. раздел 2.2). Ничто не мешает адаптировать такой протокол для работы с регистрируемыми активами. Транзакции активов могут использовать биткойн как универсальную согласованную валюту аналогично тому, как «настоящие» ценные бумаги теоретически можно приобрести или продать с помощью наличных денег. Даже если транзакция активов не использует биткойн напрямую, биткойновский блокчейн применяется как защищенное, публичное, неизменяемое хранилище данных, которое позволяет надежно фиксировать время проводки транзакций. Существуют разумные опасения насчет повышенного риска атак, связанные с хранением на блокчейне ценных активов; мы рассматриваем их в разделе 1.6.

Во-вторых, схемы с использованием мультисигнатур [16] (т. е. требующие нескольких цифровых подписей) позволяют создавать среду с ограниченным доверием в пределах биткойна; эта среда может быть полезна для работы с регистрируемыми активами и в других подобных вариантах использования. В то время как обыкновенные биткойны подобны наличным деньгам, мультисигнатуры действуют похоже на дебетовые карты и дебетовые банковские счета; пользователь по-прежнему контролирует свои средства, а сервис мультисигнатур предоставляет репутацию и услуги оценки риска транзакций. Например, сервисы мультисигнатур могут позволить продавцам принимать транзакции оплаты без задержки, поскольку цифровая подпись сервиса предусматривает меньший риск мошеннических действий чем в случае обыкновенной биткойновской транзакции. Другой пример использования мультисигнатур — это определение пользовательской активности, часто возникающей при взломе профиля (например, попытка перевести все средства на другой адрес); сервис может обнаружить такие действия и отказать в подписи соответствующих транзакций или потребовать определенного подтверждения (например, по телефону).

Один из вариантов использования схемы с 2 из 3 необходимых подписей — это условное

депонирование (англ. escrow) с участием доверенного посредника. Покупатель определенных товаров или услуг запирает свой платеж при помощи «замка», который может требует двух из трех подписей: от продавца, покупателя и от доверенного посредника. Таким образом, средства могут быть потрачены

- продавцом, если он достигнет соглашения с покупателем (т. е. успешная сделка);
- покупателем, если он предоставит посреднику доказательства в пользу возврата денег;
- продавцом, если он предоставит посреднику доказательство успешной сделки в отсутствие соглашения с покупателем.

В третьих, общий тренд децентрализации играет в пользу систем, подобных биткойну, в которых регулирование выражено через предельно четкие правила протокола, а не произвольно диктуется единым источником. С легальной точки зрения, криптография с открытым ключом, используемая в биткойне, не является менее надежной, чем системы авторизации веб-сайтов, которые в определенных случаях могут служить доказательством.

1.4. Внутренние монеты в общедоступных блокчейнах

Проблема. Учреждения могут остерегаться использования блокчейнов с внутренней валютой (например, биткойна). Вместо этого организации могут предпочесть дизайн блокчейна, в котором выделенная внутренняя валюта отсутствует (например, транзакции представляют собой перевод фиатных валют или активов).

Внутренние валюты в общедоступных блокчейнах необходимы для предоставления экономических и математических инициатив для пользователей поддерживать и развивать систему. Например, создаваемые «из ниоткуда» биткойны в каждом блоке, а также комиссии за транзакции предоставляют инициативу для майнеров поддерживать безопасность биткойновского блокчейна в форме высокого хэшрейта. Фактически, объем награды за создание блоков может служить хорошей мерой защищенности общедоступного блокчейна.

Аналогичный протокол вознаграждения органично вписался бы в эксклюзивный блокчейн, если обработка транзакций и обеспечение защиты системы разделены между различными организациями, например, при помощи объединенного майнинга. В таком случае в каждый блок можно включать транзакцию, аналогичную по своей семантике coinbase-транзакциям, которая будет вознаграждать организацию, обеспечившую защиту заголовка блока. Отметим, что награды в случае эксклюзивного блокчейна не обязательно требует введения внутренней валюты в блокчейне; транзакции с вознаграждением майнеров могут соответствовать формату обычных транзакций. Протокол вознаграждения, описанный выше, был бы предпочтительнее обыкновенного контракта с поставщиками безопасности на блокчейнах, поскольку этот способ вознаграждения можно независимо проверить и он реализован алгоритмически (т. е. отвечает духу блокчейн-технологии).

1.5. Завершенность транзакций

Проблема. Транзакции, хранимые на биткойновском блокчейне, не являются по-настоящему завершенными. Любую транзакцию можно теоретически удалить из блокчейна, реорганизовав его, начиная с блока, который содержит эту транзакцию.

На первый взгляд, проблема усугубляется сравнительно часто происходящими реорганизациями биткойновского блокчейна, проистекающими из неоптимальной организации сети. Эти реорганизации возникают, поскольку для распространения блока по всей сети требуется достаточно ощутимое время. Если два узла сети находят новый блок практически одновременно, согласно протоколу биткойна сеть будет разделена на две части, каждая из которых выберет соответствующий блок. Такие разделения быстро улаживаются и редко длятся более двух блоков. Таким образом, разделения блокчейна, возникающие без злого умысла, не удаляют транзакции из блокчейна навсегда, а просто замедляют их подтверждение. Предложено несколько механизмов уменьшить вероятность разделения сети, например, обратимые таблицы Блума [17], позволяющие блокам распространяться в сети значительно быстрее.

Злоумышленник может использовать намеренную реорганизацию блокчейна, чтобы обратить определенную транзакцию. Чтобы противостоять атакам, связанным с реорганизациями, а также спонтанным реорганизациям блокчейна, транзакцию можно считать *практически завершенной*, когда у нее есть достаточно подтверждений. (Количество подтверждений транзакции — это число блоков в блокчейне, начиная с блока с этой транзакцией. Для транзакций, еще не включенных в блок, число подтверждений равно нулю.) Самая длинная реорганизация биткойновского блокчейна произошла в 2013 году и включала 24 блока; эта реорганизация была связана с ошибкой в протоколе, а не злым умыслом [18]. Аналогично, две длинных реорганизации (6 и 3 блока), произошедших в июле 2015 года, были вызваны нарушением процедуры майнинга [19]. Таким образом транзакции с более чем 36 подтверждениями (что соответствует возрасту транзакции в 6 часов при нормальном функционировании системы) могут считаться практически завершенными.

Рассмотрим случай, когда транзакция считается практически завершенной, если у нее есть по крайней мере H подтверждений. Цель атакующего — сделать транзакцию практически завершенной и затем обратить ее. Гипотетический сценарий атаки выглядит следующим образом:

1. Злоумышленник посылает транзакцию **Tx**, которую он хочет позже обратить, в сеть или замечает эту транзакцию в блоке.
2. Атакующий начинает строить альтернативный блокчейн, базирующийся на блоке перед блоком, содержащем транзакцию **Tx**. Атакующему необходимо действовать тайно: если цепь, которую строит атакующий, будет опубликована до того, как **Tx** наберет H подтверждений, атака станет очевидной для второй стороны, и сделка сорвется.

3. После того, как **Tx** набирает H подтверждений и цепь атакующего длиннее, чем публично доступный блокчейн, атакующий публикует свою цепь блоков.

Если **Tx** не тратит средства злоумышленника, эта транзакция после окончания атаки возвратится в набор неподтвержденных транзакций и может быть по-прежнему подтверждена в будущем.

Для того чтобы совершить атаку со 100% вероятностью, злоумышленнику надо контролировать более 50% хэшрейта сети на время атаки [20]. Атакующий может либо купить соответствующее количество оборудования, либо подкупить существующих майнеров для участия в атаке. В первом случае приготовления к атаке будут, скорее всего, замечены. Во втором случае, если для проведения атаки требуется большое количество подтверждений (например, 36), атака будет замечена еще до ее окончания из-за существенно возросшего интервала между блоками в наблюдаемом блокчейне. Поскольку на настоящее время майнинг производится сравнительно небольшим количеством майнинг-пулов, пулы, участвующие в атаке, также можно будет обнаружить до ее окончания. В любом случае, атака станет очевидной после ее завершения, поскольку длинные реорганизации блокчейна являются статистически невероятными событиями.

В текущей версии протокола биткойна после публикации цепи атакующего она в действительности заменит предыдущую цепь, даже если все пользователи сети знают, что это результат атаки. Для предотвращения этого протокол можно модифицировать, чтобы он отвергал реорганизации, длящиеся больше определенного количества блоков (как это сделано, например, в Nxt). Однако это сделает протокол биткойна *слабо субъективным* [21], т. е. введет в экосистему биткойна социально управляемую безопасность. С другой стороны, после внесения такого изменения транзакции биткойна обретут «настоящую» завершенность. Например, если протокол не допускает реорганизации глубиной более 35 блоков, то транзакции с 36 или более подтверждениями являются завершенными и не могут быть удалены из блокчейна.

1.6. Атака с цензурой транзакций

Проблема. Рассмотрим злоумышленника, контролирующего более 50% хэширующей мощности сети биткойна. Такой злоумышленник может проводить цензуру произвольных транзакций, не включая их в свои блоки и отвергая все блоки, содержащие транзакции, попавшие под цензуру. Хотя долговременная атак подобного рода не будет прибыльной для атакующего, атака может производиться из других соображений (например, с целью требования выкупа).

Устойчивость к цензуре является определяющей характеристикой биткойна; ликвидация этого свойства за счет описанной атаки будет иметь отрицательные последствия для цены и репутации криптовалюты. Для противодействия атаке протоколу биткойна нужно выявлять и предотвращать проведение, связанное с цензурой, которое проявляется двумя способами:

- злоумышленник игнорирует блоки, созданные честной частью сети;

- злоумышленник не включает определенные транзакции в свои блоки.

Один из возможных методов борьбы с проблемой — обязательная синхронизация пула неподтвержденных транзакций (с приблизительной логикой: если транзакция в пуле неподтвержденных транзакций достаточно стара и ее приоритет, определяемый комиссией, достаточно большой, то такая транзакция должна присутствовать в пуле для всех узлов, производящих блоки). Поскольку синхронизация неподтвержденных транзакций поможет более быстрому распространению созданных блоков, логика синхронизации включена в предложение по использованию обратимых таблиц Блума [17].

Безопасность биткойновской сети в случае экономического равновесия определяется наградами, получаемыми майнерами и поэтому связана с обменным курсом биткойна. Следовательно, создание большого потока транзакций для дорогих цифровых активов на основе биткойновского блокчейна несет в себе потенциальные риски: транзакции увеличивают потенциальный выигрыш от успешно проведенной атаки, в то время как защищенность сети остается на приблизительно одинаковом уровне (поскольку не существует специальной комиссии на транзакции с цифровыми активами; комиссии за такие транзакции по-прежнему платятся в биткойнах). Этот риск можно сократить, если комиссии за транзакции с активами будут высокими согласно сознательному решению создателей таких транзакций либо вследствие спецификации протокола окраски монет; это позволит майнерам биткойнов увеличить защищенность в соответствии со средствами, циркулирующими в сети как в виде биткойнов, так и в виде цифровых активов.

2. Приложения для общедоступных блокчейнов

Как и в разделе 1, мы концентрируем внимание на биткойне. Биткойновский блокчейн в настоящее время является наиболее безопасным общедоступным блокчейном с точки зрения стоимости атак на систему; в общедоступной среде стоимость атаки пропорциональна вознаграждению создателей блоков, которые в случае биткойна составляют около 900 000 долларов в день. В то же время стоимость поддержки безопасности сравнительно невелика для пользователей биткойна; эта стоимость образуется за счет двух факторов:

- комиссии за транзакции (около $2 \cdot 10^{-4}$ биткойнов в среднем за транзакцию на время написания статьи, т. е. приблизительно 5 центов).
- контролируемая инфляция денежной массы (около 9% в год в 2015 году).

Таким образом, биткойновский блокчейн — естественный выбор среди имеющихся общедоступных блокчейнов для рациональных экономических игроков.

2.1. Известные обработчики транзакций

Поскольку в биткойне активно достаточно малое количество майнинг-пулов, майнеры могут выступать в роли известных обработчиков для биткойновских транзакций, происходящих от учреждений (например, с целью соответствия законам). Взаимодействие с организациями может иметь форму защищенных каналов для биткойновских транзакций, установленных между учреждениями и майнерами. Например, транзакции, посылаемые учреждениями, могут быть зашифрованы с помощью публичного ключа майнера и асимметричной схемы шифрования (например, ECIES [22]); транзакции, зашифрованные таким образом, могут быть расшифрованы исключительно майнером. Важно отметить, что предложенное сотрудничество не подразумевает цензуры биткойновских транзакций, поступающих от «обыкновенных» пользователей.

Рис. 1. Защищенные каналы связи между финансовыми учреждениями и биткойновскими майнерами для размещения транзакций на биткойновском блокчейне. Майнеры биткойна подтверждают свою личность, подписывая блоки цифровыми подписями в соответствии с протоколом, описанном в приложении A

В настоящее время в биткойне не существует общепринятых инструментов для принятия транзакции в пул неподтвержденных транзакций без передачи ее по сети. Этой функциональности можно легко достичь при помощи рефакторинга RPC-метода **sendrawtransaction** клиента Bitcoin Core, используемого для майнинга [23]. Данный метод сначала проверяет корректность транзакции и принимает ее в пул неподтвержденных транзакций (что полностью соответствует требуемой функциональности), а затем передает транзакцию в сеть. Если это необходимо, приоритет транзакций, полученных от учреждений, можно регулировать при помощи RPC-метода **prioritisetransaction** [24] для того, чтобы ускорить процесс включения таких

транзакций в блоки. В идеальном случае, однако, приоритет транзакций определяется по их комиссии (т. е. так же, как и приоритет всех остальных транзакций), которая одновременно является платой за обработку транзакции известным субъектом. Такая форма обработки транзакций соответствует общему предположению майнинга биткойнов, согласно которому майнеры — рациональные экономические игроки, пытающиеся максимизировать свою прибыль. Отметим, что включение в блоки транзакций, не распространяемых по сети, может уменьшить эффективность некоторых средств повышения масштабируемости биткойна, таких как обратимые таблицы Блума.

Партнерство между учреждениями и майнерами могут минимизировать риск в случае, когда содержимое транзакций не должно быть доступно до их подтверждения. Подобно тому как предварительное раскрытие деталей сделок с высоким объемом может отрицательно сказаться на участниках сделки, информация о неподтвержденных транзакциях, связанных с финансами, может стать отрицательным фактором при трейдинге. Партнерство с майнерами биткойна эффективны даже в случае, если мощности, используемые в майнинге, географически распределены (например, для майнинг-пулов с открытым участием); протоколы, используемые в распределенном майнинге, такие как Stratum [25], уже не распространяют транзакции среди участников пула. Таким образом, доступ к транзакциям имеет только администратор пула; обычные участники пула не имеют к ним доступа и не могут восстановить транзакции исходя из высылаемых для майнинга данных.

2.2. Окраска монет

Протоколы окраски монет (англ. colored coins protocols) — основной способ встраивания определенных пользователями цифровых активов в биткойновский блокчейн. Эти протоколы используют данные малого размера (чаще всего, до 40 байт) для кодирования выпуска и / или перемещения цифровых активов в рамках обыкновенных биткойновских транзакций. Протоколы (табл. 1) отличаются в том, как именно кодируются данные, и в том, требуется или нет дополнительный уровень инфраструктуры для обработки транзакций с цифровыми активами.

- Такие протоколы как Open Assets Protocol, Colored Coins Protocol и ChromaWay предоставляют готовый каркас для работы с транзакциями активов; эти протоколы не зависят от дополнительного программного обеспечения.
- Более сложные протоколы (Counterparty, OmniLayer, CoinSpark) требуют специализированной или дополненной версии биткойновского клиента, которая предоставляет более широкие возможности по работе с активами (например, автоматический подбор заказов на куплю / продажу активов, выплата дивидендов и так далее). Промежуточный уровень чаще всего выкладывается в свободный доступ и представляет собой распределенную сеть (аналогично с самим биткойном), так что этот уровень не представляет собой точку отказа.

Таблица 1. Протоколы окраски монет

Название	Веб-сайт	Год основания	Потребность в доп. ПО
ChromaWay	chromaway.com	2012	нет
Open Assets Protocol	github.com/OpenAssets	2013	нет
Colored Coins Protocol	coloredcoins.org	2015	нет
OmniLayer / Mastercoin	omnilayer.org	2013	да
CoinSpark	coinspark.org	2014	да
Counterparty	counterparty.io	2014	да

Сервисы, построенные на основе протоколов окраски монет, включают проводники для исследования определенных пользователями активов, кошельки и облачные платформы (Storj и MaidSafe). Одно из интересных финансовых применений окрашенных монет — стартап Tether (tether.to), в котором цветные монеты представляют доллары США, используемые для быстрых денежных переводов. Некоторые криптовалюты, например, Nxt и BitShares, имеют встроенные средства работы с определенными пользователями активами.

По сравнению с эксклюзивными блокчейнами, у технологии окраски монет есть некоторые преимущества при использовании в финансовых приложениях (рис. 2):

- Окрашенные монеты полагаются на существующую инфраструктуру; решения на основе этой технологии требуют меньше усилий по разработке и сопровождению.
- Окрашенные монеты более прозрачны для конечных потребителей и аудиторов по сравнению с эксклюзивными блокчейнами.
- Поскольку окрашенные монеты организованы поверх общедоступного блокчейна, системы с использованием окрашенных монет устойчивы к цензуре – ограничения на транзакции могут полностью задаваться протоколом окраски монет вместо централизованного управления определенной организацией.
- Существующие протоколы окраски являются открытыми; это позволяет пользователям провести независимый аудит кода и удостовериться в наличии декларируемых свойств.

С другой стороны, эксклюзивные блокчейны более гибки:

- Эксклюзивные блокчейны предоставляют баланс между прозрачностью и конфиденциальностью пользователей (например, в таких блокчейнах могут быть введены различные уровни доступа к данным блокчейна для различных категорий пользователей).
- Меньшая нагрузка по сравнению с протоколами окраски. Проверка транзакций на эксклюзивных блокчейнах может быть подстроена под конкретные категории активов. В эксклюзивный блокчейн могут быть включены средства для реализации смарт-контрактов, в то время как окрашенные монеты подходят в основном для перемещения средств.

- Эксклюзивные блокчейны могут в большей мере соответствовать законам (например, из-за известных обработчиков транзакций).

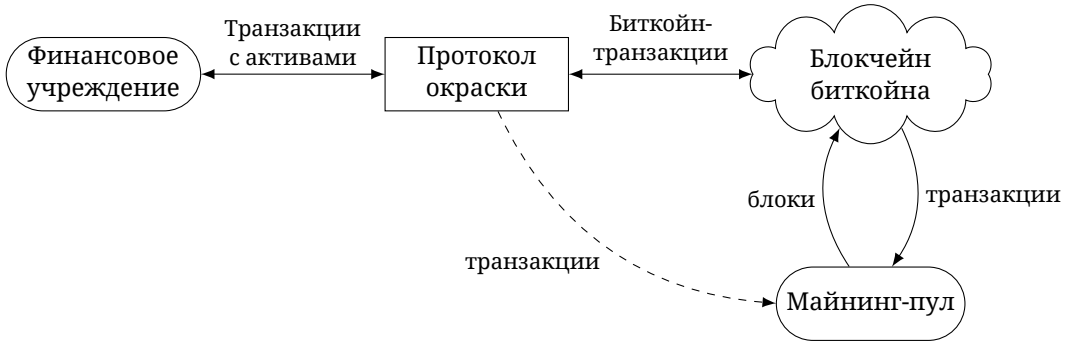

Рис. 2. Использование окрашенных монет на биткойновском блокчейне для реализации транзакций с активами. В целях соответствия законам финансовые учреждения могут использовать безопасные каналы связи с майнерами, описанные в разделе 2.1, для помещения транзакций на блокчейн

Финансовые учреждения могут реализовать проприетарные протоколы окраски монет, которые в большей степени отвечали бы их нуждам:

- более ограничивающий набор правил относительно владения и перевода активов, например, для соответствия законодательству;
- более качетсвенное отображение семантики конкретных категорий активов, например, ограниченное время существования;
- шифрование данных с целью соблюдения конфиденциальности клиентов.

В целом, взвешенный поход, использующий и окрашенные монеты, и эксклюзивные блокчейны, мог бы объединить преимущества обеих технологий.

2.3. Сайдчейны

Сайдчейны (англ. sidechains) [26] позволяют интегрировать финансовые блокчейны в единую взаимосвязанную среду, а также объединить их с общедоступными блокчейнами. Цель сайдчейнов — позволить переводы средств с одного блокчейна на другой по фиксированному или детерминированному курсу. Реализация сайдчейнов без доверия потребовала бы от протоколов обоих блокчейнов внедрения информации о других блокчейнах; насколько известно, на данный момент не существует блокчейнов, удовлетворяющих такому требованию. Другие способы проводить платежи между блокчейнами заключается в использовании независимых сервисов-оракулов, которые проверяют корректность платежей (*разделенная привязка*, англ. federated peg) либо при помощи прямого обмена между пользователями блокчейнов (*атомарные свопы*, англ. atomic swaps [27]). Эти виды переводов могут быть реализованы в биткойне.

Общая идея сайдчейнов заключается в следующем:

1. Пользователь, желающий перевести средства с блокчейна А на блокчейн Б, перемещает средства на первом блокчейне в специальным образом заблокированный выход.
2. Затем пользователь создает транзакцию на блокчейне Б, которая ссылается на заблокированный выход. Протокол на блокчейне Б должен обладать возможностью проверить, что средства, на которые ссылается транзакция, присутствуют и должным образом заперты на другом блокчейне, при помощи упрощенной верификации платежей.
3. Пользователь продолжает работать со средствами, которые теперь де-факто находятся на блокчейне Б; например, эти средства можно продать другому пользователю. Если владелец желает перевести средства обратно на первый блокчейн, он посылает их на специальным образом сформированный выход на блокчейне Б; указание этого выхода позволяет разблокировать средства на блокчейне А.

В случае разделенной привязки в биткойне запирания и разблокирования средств можно достичь при помощи адресов для платежей по контрактам [10], которые используют гомоморфное свойство криптографии на основе эллиптических кривых. Такие адреса создаются заново для каждого перевода из одного блокчейна на другой на основе шаблона мультисигнатуры, который требует цифровых подписей нескольких сервисов-оракулов (например, 4 из 5). Открытые ключи оракулов известны, однако подписи для того, чтобы потратить соответствующий выход, надо производить при помощи *модифицированных* секретных ключей сервисов, причем модификация зависит от деталей перевода. Гомоморфное свойство криптографии с эллиптическими кривыми позволяет создавать адреса для платежей по контрактам, модифицируя открытые ключи оракулов тем же способом, каким модифицируются скрытые ключи; таким образом, пользователь не обязан сотрудничать с оракулами для производства адреса. Поскольку адрес создается заново для каждого платежа между блокчейнами, эти адреса невозможно выделить постороннему наблюдателю или подвергнуть цензуре.

Сайдчейны может использоваться финансовыми учреждениями как удобный инструмент для кросс-трейдинга между специализированными блокчейнами, принадлежащими одной финансовой группе (например, если различные блокчейны соответствуют различным видам активов) или между блокчейнами, принадлежащими различным группам. Сравнительно простые блокчейны, напоминающие по совей структуре биткойн, могут использоваться как базис для финансовой среды, в от время как более сложные блокчейны можно использовать для смарт-контрактов, перемещающих средства на базовых блокчейнах (рис. 3). Этот подход сможет объединить безопасность биткойно-образных блокчейнов со скоростью и многофункциональностью блокчейнов со смарт-контрактами. Открытый и стандартизованный дизайн протоколов блокчейнов поможет в их интеграции. Среда, в которой на базисе биткойна объединены смарт-контракты и переводы активов, в настоящее время разрабатывается Counterparty [28]; похожую цель — построение сайдчейна, обрабатывающего смарт-контракты для биткойна, — реализует проект Rootstock [29].

Биткойн и другие открытые общедоступные блокчейны могут стать частью взаимосвязан-

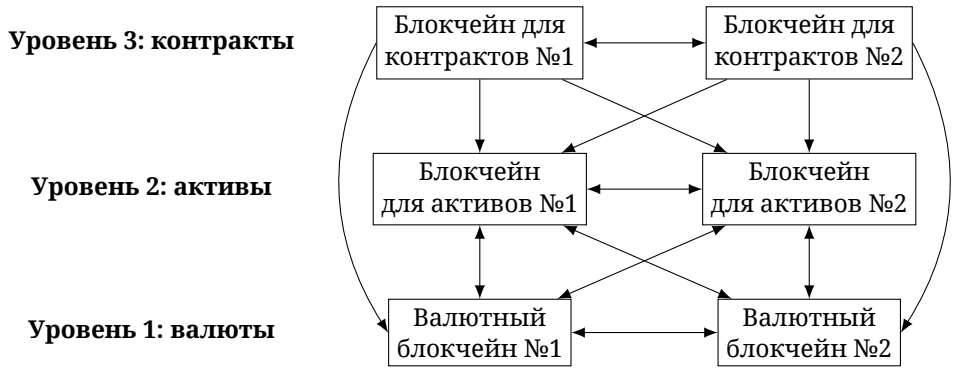

Рис. 3. Многоуровневая финансовая среда на основе блокчейнов, компоненты которой связаны с помощью технологии сайдчейнов

ной финансовой экосистемы подобно тому, как наличные деньги образуют основу банковской системы. Более конкретно, криптовалюты могут использоваться в качестве:

- одного из способов покупки / продажи активов на эксклюзивных блокчейнах;
- инструмент, позволяющий быстро проводить транзакции между эксклюзивными блокчейнами;
- нейтральная среда, в которой по общей договоренности проводится клиринг между блокчейнами, принадлежащими различным учреждениям (рис. 4).

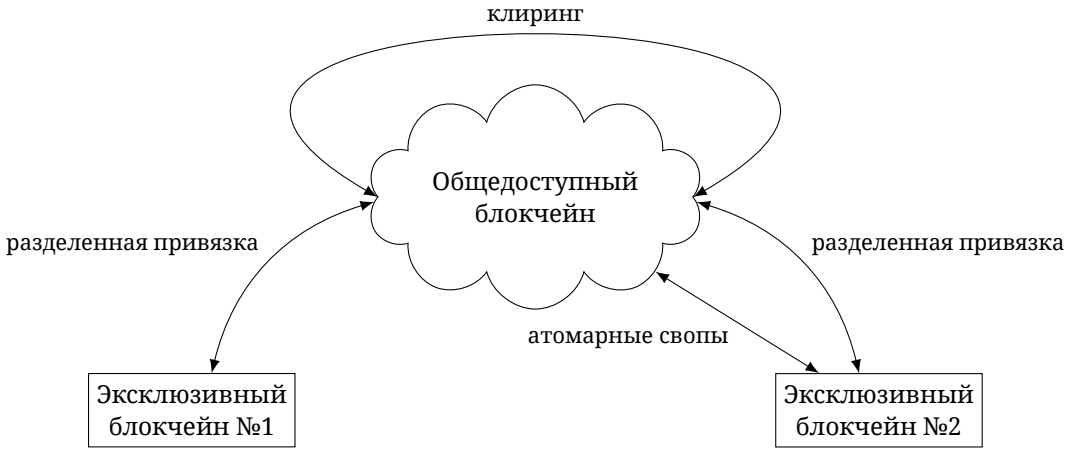

Рис. 4. Использование общедоступных сайдчейнов для клиринга между коммерческими блокчейнами, поддерживаемыми финансовыми учреждениями

2.4. Одноранговые каналы платежей

Одноранговые сети каналов платежей без доверия, например Lightning Network [30], могли бы стать ответом проблемы масшабируемости для биткойна и других открытых блокчейнов. Идея, стоящая за каналами платежей, заключается в следующем: если между двумя сторонами существует стабильный канал платежей (например, стороны — это провайдер цифрового

потокового контента и его потребитель), то промежуточные транзакции не требуется записывать в блокчейне; достаточно сохранить транзакцию, создавшую канал, и транзакцию, его закрывшую. При использовании такой системы блокчейн может адаптироваться к потоку в тысячи транзакций в секунду, при этом оставаясь в разумных пределах по размеру; блокчейн в этом случае используется для открытия и финализации финансовых контрактов.

Предложенная архитектура Lightning Network является

- **децентрализованной** — нет необходимости в медиаторе, создающем и поддерживающем канал связи;
- **работающей без доверия** — структура канала делает его устойчивым к злонамеренной активности одной из сторон или третьей стороны.

Эти свойства делают необходимой комплексную структуру промежуточных транзакций (каждый новый платеж от одной стороны другой производит по меньшей мере 8 транзакций). Каналы с доверенным посредником могут быть организованы более просто, но у них есть проблемы с маштабируемостью, поскольку посредник должен уметь обслуживать все активные каналы.

Lightning Network предоставляет высокую степень масштабируемости в форме временных контрактов на основе хэшей (англ. hashed timelock contracts, HTLCs). Эти контракты предоставляют возможность пользователям проводить платежи при отсутствии открытого канала связи, используя один или несколько промежуточных узлов (рис. 1). Таким образом, организация платежей напоминает сеть Ripple, с существенным отличием в том, что сеть Ripple основана на доверии, в то время как Lightning Network работает без доверия.

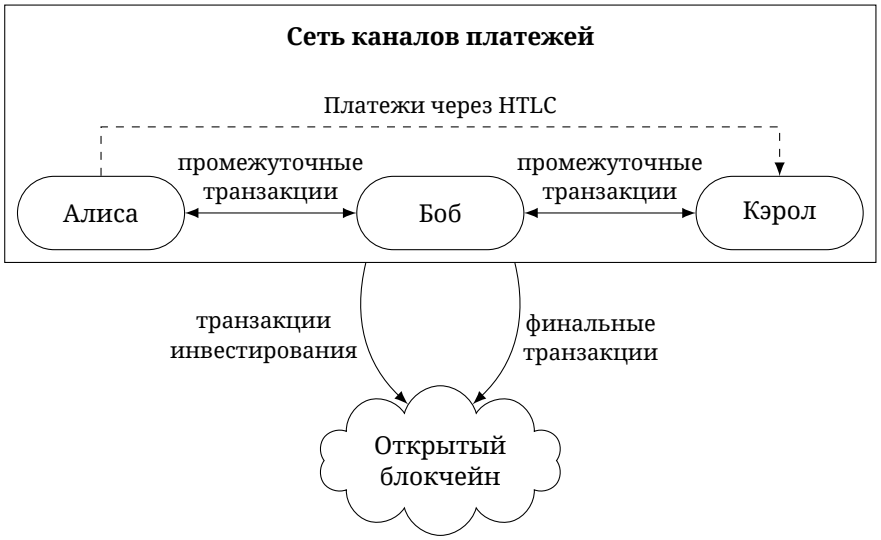

Рис. 5. Организация сети платежных каналов поверх открытого блокчейна

Платежные каналы, основанные на принципах Lightning Network могут быть теоретически построены поверх любого открытого блокчейна, который поддерживает функциональ-

ность биткойна (включая эксклюзивные блокчейны, описанные в первой части статьи). Каналы платежей могут использоваться совместно с протоколом окраски монет для кодирования перевода произвольных цифровых активов вместо встроенных в блокчейн монет.

3. Необходимость общедоступных блокчейнов

Эксклюзивные блокчейны лучше соответствуют существующему законодательству и по этой причине могут быть более привлекательными в плане внедрения блокчейнов в существующие приложения в среднесрочной перспективе. Однако такие блокчейны ограничивают один из ключевых аспектов блокчейн-технологии – *функционирование без доверия* (англ. trustlessness). Блокчейны спроектированы с прицелом на решение проблемы византийских генералов [31], т. е. они предусматривают возможность отказов или злонамеренного поведения узлов сети, обслуживающей блокчейн. Одна из основных целей блокчейнов — устранение человеческого фактора из процесса обработки транзакций и замена его на четко определенный и публично доступный протокол, соблюдение которого обеспечивается сетью независимых компьютеров.

Если блокчейн непрозрачен для его конечных пользователей (например, это банковская система, которая по-прежнему использует старые интерфейсы коммуникации вроде кредитных карт), аспект отсутствия доверия в системе существенно снижен. Конечные пользователи не могут удостовериться в том, что блокчейн действительно используется и тем более не могут проверить корректность данных блокчейна (так как к этим данным нет доступа, и не существует доступных правил, которые используются в построении блокчейна). Фактор человеческого вмешательства остается главной уязвимостью в закрытых моделях блокчейна до тех пор, пока состояние блокчейна в каждый момент времени не определяется исходя из протокола системы, который выполняется автоматически с минимальным вмешательством со стороны человека. Взаимодействие с системой, основанное на устаревших интерфейсах аутентификации пользователей могут стать источником уязвимостей при закрытом дизайне блокчейна; интерфейсы, основанные на криптографии с открытым ключом, способны сократить риск связанных атак.

Поддержка закрытых блокчейнов малым количеством компаний делает их менее доступными для разработчиков и инноваций; стандартизированные реализации блокчейнов с открытым исходным кодом могут создать более привлекательную среду. В этом смысле блокчейны с открытым протоколом напоминают открытые Интернет-стандарты вроде IP, TCP и HTTP, а проприетарные модели блокчейнов могут походить на закрытые Интернет-протоколы, которые в конечном итоге не получили существенного распространения. Закрытый протокол блокчейна может содержать в себе уязвимости, которые остаются необнаруженными и используются в течении длительного промежутка времени, в то время как стандартизированный и открытый протокол можно независимо изучить и подвергнуть аудиту на предмет уяз-

вимостей. Это замечание в особенности справедливо для общедоступных блокчейнов, потому что у их пользователей есть экономическая инициатива обнаруживать и использовать в свою пользу дыры в протоколе. Поскольку протокол биткойна интенсивно изучался криптографами и учеными *in vivo*, он мог бы стать основой для унифицированного дизайна блокчейна.

Эксклюзивные блокчейны с регулируемым или открытым доступом к данным могут стать более безопасной альтернативой закрытых блокчейнов. Такие блокчейны предоставляют доступ к данным блокчейна и его протоколу, что позволяет проводить независимый аудит данных и проверку транзакций (эти возможности могут быть ограничены регулирующими учреждениями и конечными пользователями системы). Клиенты могут желать конфиденциальности данных; в то же время, ограничения доступа к данным блокчейна усложняет его аудит, в особенности, при наличии взаимосвязанной блокчейн-среды.

Ограниченное множество обработчиков транзакций в эксклюзивных блокчейнах вызывает определенные опасения:

- Аутентификация обработчиков вводит в систему уязвимости. (Отметим, что один взломанный обработчик не может нанести много вреда системе в случае адекватного протокола блокчейна и настоящей децентрализации обработки транзакций.) В общедоступных блокчейнах обработка транзакций нейтральна и равноудалена от участников системы, в эксклюзивных блокчейнах обработка доверяется малому количеству операторов. Это оставляет более широкие возможности для коррупции, ручного вмешательства в систему и скрытого наблюдения за пользователями.
- Ключевой элемент дизайна блокчейнов — встроенная экономика, надмножество встроенной защищенности и обработки транзакций. Каждый блокчейн образует собственную экономическую экосистему; централизованно контролируемый блокчейн поэтому является центрально управляемой экономикой, со всеми вытекающими последствиями.
- Существует риск сговора операторов с целью создания нескольких копий блокчейна или изменения произвольных кусков блокчейна. Этот риск можно уменьшить, введя доказательство работы в алгоритм консенсуса блокчейна.
- Не ясно, как блокчейн будет функционировать в случае, если операторы будут незаинтересованы в его поддержке или после успешной атаки на блокчейн (ср. с общедоступными блокчейнами, в которых есть сильный компонент самоорганизации).

Открытые общедоступные блокчейны используют отсутствие доверия в полной мере. Закрытые и эксклюзивные блокчейны соответствуют различным уровням доверия при взаимодействии конечных пользователей с обработчиками транзакций; в то же время, общедоступные блокчейны построены с целью устранить это доверие вкупе с связанными уязвимостями. Среды с ограниченным доверием можно создать в пределах общедоступных блокчейнов с помощью различных технологий, описанных ранее в этой статье, например, мультисигнатур и протоколов окраски монет. В этом случае общедоступный блокчейн предоставляет децентра-

лизованную среду для функционирования доверенного приложения по аналогии с протоколами HTTP / TCP, предоставляющими инфраструктуру без доверия для веб-сервисов.

Поскольку общедоступные системы спроектированы с устойчивостью к злонамеренному поведению и отказов узлов, они хорошо подходят для создания одноранговых сетей между конечными пользователями. Одно из возможных применений таких сетей — масштабируемые каналы платежей (раздел 2.4). Многослойные сети, в которых промежуточные транзакции, составляющие большую часть операций, осуществляются напрямую между конечными пользователями, в то время как финализация сделок зарезервирована за ограниченным перечнем организаций, могут стать полезными во многих случаях, например, для организации микроплатежей и вездесущих платежей.

4. Выводы

Если эксклюзивные блокчейны могут создать базис инноваций в краткосрочной перспективе, общедоступные блокчейны естественно менее уязвимы к атакам, поскольку они спроектированы на основе предположения, что стороны могут не доверять друг другу. Общедоступные блокчейны минимизируют влияние человеческого фактора и делают акцент на алгоритмическом подходе к защите и целостности данных, — свойствам, являющимся ключевыми в блокчейн-технологии. Следовательно, общедоступные блокчейны могут стать основой инфраструктуры блокчейнов, а эксклюзивные приложения могут строиться на их основе. Кроме того, общедоступная среда предоставляет необходимые условия для построения масштабируемых и надежных глобальных одноранговых сетей, например, для платежных каналов.

Существующие открытые общедоступные блокчейны, используемые в биткойне и других криптовалютах, могут реализовать определенные изменения, чтобы повысить свою привлекательность для использования в финансовых приложениях; потенциальные модификации включают решение проблемы завершенности транзакций и введение цифровых подписей для блоков транзакций. При условии внесения соответствующих изменений криптовалюты могут играть роль быстрого средства для платежей с малой комиссией либо среды для операций внутри и между финансовыми учреждениями.

Много приложений, использующих блокчейн в эксклюзивном контексте (т. е. с ограниченным кругом обработчиков транзакций), можно построить на основе общедоступных блокчейнов с использованием существующих технологий:

- Протоколы окраски монет могут предоставить средства для кодирования переводов произвольных активов в пределах обыкновенных транзакций, таким образом увеличивая возможности использования открытых блокчейнов в финансовом контексте.
- Схожие протоколы можно использовать для фиксирования времени появления / изменения документов, что может помочь при создании децентрализованных реестров.

- Сети каналов платежей могут масштабировать платежи, создав одноранговую сеть между конечными пользователями поверх общедоступных блокчейнов.
- Технология сайдчейнов может использоваться для интеграции общедоступных и эксклюзивных блокчейнов в единую взаимосвязанную среду. Сайдчейны могут использоваться в случаях когда протокол основного блокчейна чересчур ограничивает возможности построения конкретного приложения (например, в скорости обработки транзакций или в ограничении на время подтверждения транзакций).

Преимущества использования существующих открытых блокчейнов в создании систем финансового учета и реестров — это их прозрачность, а также открытость базовых технологий и протоколов. Среда биткойна в частности может быть перспективной в блокчейн-инновациях из-за следующих факторов:

- развитая инфраструктура в виде сервисов и протоколов, использующих биткойновский блокчейн;
- широкое сообщество разработчиков;
- сравнительно малое количество майнинг-пулов с известными личностями, что позволяет пулам выступать в роли обработчиков транзакций в сотрудничестве с организациями, поставляющими такие транзакции.
- высокий уровень защиты, предоставляемый хэшрейтом биткойновской сети.

Приложение A. Необязательные цифровые подписи в coinbase-сценариях

Майнер, желающий формально установить свою личность в создании блока, может включить цифровую подпись содержимого блока в coinbase-сценарий (отпирающий сценарий первого выхода первой транзакции в блоке). Эта подпись, которую мы в дальнейшем называем *подписью блока,* может использовать ту же криптографию на основе эллиптических кривых, что и в протоколе авторизации биткойновских транзакций. Поскольку у большей части майнеров биткойна есть публичная репутация, им необязательно включать соответствующий открытый ключ в coinbase-сценарий (в отличие от авторизации обыкновенных транзакций); достаточно опубликовать открытый ключ на веб-сайте или в другом защищенном месте. Более того, в текущей версии протокола биткойна одновременное включение цифровой подписи (70 байтов) и открытого ключа (около 34 байтов) в coinbase-сценарий невозможно, так как его размер не должен превышать 100 байтов. Вместо полного ключа, майнер может включить в сценарий его сокращенную и / или хэшированную версию.

Поскольку подпись блока непрямым образом влияет на заголовок блока через хэш-корень транзакций, протокол не может требовать подписи непосредственно заголовка блока. Вместо это майнер может подсчитать *измененный корень хэш-дерева,* полученный путем замены

coinbase-сценария на пустую последовательность байт и подписать измененный заголовок блока, полученный из заголовка блока путем замены хэш-корня на вычисленное значение. Этот прием позволяет сделать подпись независимой от главного источника энтропии при майнинге. Идея состоит в том, чтобы подпись изменялась медленно в процессе майнинга и не приводила к дополнительным вычислениям, но при этот покрывала всю важную информацию в блоке. По этой причине в модифицированном заголовке значения специального поля перебора nonce и времени создания блока могут быть заменены на фиксированные значения. По аналогии с подписями транзакций подпись блока может включать дополнительные сведения, которые указывают, какие именно данные блока подписаны.

Цифровые подписи могут эффективно использоваться с существующими протоколами распределенного майнинга (например, Stratum). В случае использования таких протоколов секретный ключ, соответствующий подписи майнера, должен храниться исключительно у администратора пула; участникам пула необязательно знать этот ключ, так как они могут использовать готовые цифровые подписи, предоставляемые через протокол. Предлагаемое изменение не требует изменений в оборудовании для майнинга; в самом деле, оборудование может не знать, что часть coinbase-сценария отведена под подпись блока.

Для проверки корректности подписи блока достаточно выполнить следующие шаги, напоминающие упрощенную верификацию платежа:

1. проверить, что цепь заголовков блока является корректной;
2. запросить coinbase-транзакцию для проверяемого блока и соответствующую хэш-ветвь;
3. подсчитать модифицированный хэш-корень дерева транзакций на основе coinbase-транзакции и ее хэш-ветви;
4. определить измененный заголовок блока на основе модифицированного хэш-корня дерева транзакций и, возможно, типа подписи;
5. определить открытый ключ майнера блока на основе coinbase-сценария;
6. проверить цифровую подпись блока, основываясь на открытом ключе майнера и измененном заголовке блока.

Приведенное выше описание можно обобщить на случай, когда майнер желает подписать определенную часть транзакций блока вместо всех транзакций. Например, майнер может подписывать только транзакции, полученные от финансовых учреждений, как описано в разделе 2.1. В этом случае модифицированный хэш-корень будет строиться на основе только этих транзакций и coinbase-транзакции; для того чтобы предоставить возможность независимой проверки подписи блока, подписываемые транзакции можно размещать в начале блока, а количество таких транзакций может быть включено в coinbase-сценарий.

Список литературы

[1] *Satoshi Nakamoto*. Bitcoin: A peer-to-peer electronic cash system. — 2008.
URL: https://bitcoin.org/bitcoin.pdf

[2] *David Schwartz, Noah Youngs, Arthur Britto*. The Ripple protocol consensus algorithm. — 2014.
URL: https://ripple.com/files/ripple_consensus_whitepaper.pdf

[3] Litecoin // Litecoin Wiki.
URL: https://litecoin.info/Litecoin

[4] Ethereum: A next-generation smart contract and decentralized application platform // Ethereum project wiki
URL: https://github.com/ethereum/wiki/wiki/White-Paper

[5] *Daniel Larimer, Charles Hoskinson, Stan Larimer*. BitShares: a peer-to-peer polymorphic digital asset exchange. — 2014.
URL: http://scribd.com/doc/173481633/BitShares-White-Paper

[6] Whitepaper: Nxt // Nxt Wiki.
URL: https://wiki.nxtcrypto.org/wiki/Whitepaper:Nxt

[7] Blockchain.info
URL: https://blockchain.info/

[8] Blocktrail
URL: https://www.blocktrail.com/BTC

[9] *Pieter Wuille*. Hierarchical deterministic wallets (BIP 32). — 2012.
URL: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[10] *Ilja Gerhardt, Timo Hanke*. Homomorphic payment addresses and the pay-to-contract protocol. — 2012.
URL: http://arxiv.org/pdf/1212.3257v1.pdf

[11] Secret sharing // English Wikipedia
URL: https://en.wikipedia.org/wiki/Secret_sharing

[12] *Guy Zyskind, Oz Nathan, Alex Pentland*. Enigma: decentralized computation platform with guaranteed privacy. — 2015.
URL: http://enigma.media.mit.edu/enigma_full.pdf

[13] *Dan Bogdanov, Sven Laur, Jan Willemson*. Sharemind: a framework for fast privacy-preserving computations. // Proc. of 13th European Symposium on Research in Computer Security, ESORICS 2008, LNCS. — 2008. — № 5283. — pp. 192–206.
URL: http://kodu.ut.ee/~swen/publications/articles/bogdanov-laur-willemson-2008.pdf

[14] *Greg Maxwell*. Confidential transactions. — 2015.
URL: https://github.com/ElementsProject/elementsproject.github.io/blob/master/confidential_values.md

[15] *Robert Sams*. No, Bitcoin is not the future of securities settlement // Clearmatics blog. — 2015.
URL: http://www.clearmatics.com/2015/05/no-bitcoin-is-not-the-future-of-securities-settlement/

[16] *Gavin Andresen*. M-of-N standard transactions (BIP 11). — 2011.
URL: https://github.com/bitcoin/bips/blob/master/bip-0011.mediawiki

[17] *Gavin Andresen*. O(1) block propagation. — 2014.
URL: https://gist.github.com/gavinandresen/e20c3b5a1d4b97f79ac2

[18] *Gavin Andresen*. March 2013 chain fork post-mortem (BIP 50). — 2013.
URL: https://github.com/bitcoin/bips/blob/master/bip-0050.mediawiki

[19] Some miners generating invalid blocks. — 2015.
URL: https://bitcoin.org/en/alert/2015-07-04-spv-mining

[20] *Meni Rosenfeld*. Analysis of hashrate-based double-spending. — 2012.
URL: https://bitcoil.co.il/Doublespend.pdf

[21] *Vitalik Buterin*. Proof of stake: How I learned to love weak subjectivity // Ethereum Blog. — 2014.
URL: https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/

[22] *V. Gayoso Martínez, L. Hernández Encinas, C. Sánchez Ávila*. A survey of the elliptic curve integrated encryption scheme // Journal of Computer Science and Engineering. — 2011. — № 2 (2). — pp. 7–13.
URL: http://www.researchgate.net/profile/Carmen_Sanchez_Avila/publication/255970113_A_Survey_of_the_Elliptic_Curve_Integrated_Encryption_Scheme/links/02e7e5212654222f0a000000.pdf

[23] src/rpcrawtransaction.cpp // Bitcoin Core Github repository (получено 30 сен. 2015)
URL: https://github.com/bitcoin/bitcoin/blob/master/src/rpcrawtransaction.cpp

[24] src/rpcmining.cpp // Bitcoin Core Github repository (получено 30 сен. 2015)
URL: https://github.com/bitcoin/bitcoin/blob/master/src/rpcmining.cpp

[25] Stratum protocol
URL: https://mining.bitcoin.cz/help/#!/manual/stratum-protocol

[26] Enabling blockchain innovations with pegged sidechains / *Adam Back, Matt Corallo, Luke Dashjr и др.* — 2014.
URL: https://www.blockstream.com/sidechains.pdf

[27] Atomic cross-chain trading // Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Atomic_cross-chain_trading

[28] Counterparty recreates Ethereum's smart contract platform on Bitcoin // Counterparty News. — 2014.
URL: http://counterparty.io/news/counterparty-recreates-ethereums-smart-contract-platform-on-bitcoin/

[29] *Luke Parker*. Rootstock is coming, are Ethereum's days numbered, or will the $18 million dollar idea survive // Brave New Coin. — 2015.
URL: http://bravenewcoin.com/news/rootstock-is-coming-are-ethereums-days-numbered-or-will-the-18-million-dollar-idea-survive/

[30] *Joseph Poon, Thaddeus Dryja*. The Bitcoin Lighting Network: scalable off-chain instant payments. — 2015.
URL: http://lightning.network/lightning-network-paper.pdf

[31] *Leslie Lamport, Robert Shostak, Marshall Pease*. The Byzantine generals problem // ACM Transactions on Programming Languages and Systems. — 1982. — № 4 (3). — pp. 382–401.
URL: http://research.microsoft.com/en-us/um/people/lamport/pubs/byz.pdf