УДК 519.7

ОБЗОР ОСНОВНЫХ ПРИНЦИПОВ РАБОТЫ КРИПТОВАЛЮТЫ БИТКОИН И ВОЗМОЖНЫХ НАПРАВЛЕНИЙ НАУЧНЫХ ИССЛЕДОВАНИЙ В ДАННОЙ ОБЛАСТИ

Пестунов А.И.
Новосибирский государственный университет
экономики и управления «НИНХ»
E-mail: pestunov@gmail.com

В статье представлен обзор технологии распределенного реестра «блокчейн», лежащей в основе криптовалюты Биткоин, и рассмотрены некоторые связанные с ней направления исследований, представляющие научный и практический интерес. Рассмотрены альтернативные традиционному proof-of-work варианты подтверждения транзакций. Затронута такая важная проблема функционирования данной криптовалюты, как отсутствие на практике реальной децентрализованности и анонимности, которые заявлены в теории. В качестве аргументов приведены следующие: наличие крупных пулов для майнинга, влиятельное ядро программных разработчиков системы, механизм оповещений и некоторые другие инструменты, которыми в принципе можно злоупотребить.

Ключевые слова: криптовалюта, Биткоин, майнинг, распределенный реестр.

REVIEW OF THE MAIN OPERATING PRINCIPLES OF THE BITCOIN CRYPTOCURRENCY AND POSSIBLE LINES OF RESEARCH IN THIS FIELD

Pestunov A.I.
Novosibirsk State University of Economics and Management
E-mail: pestunov@gmail.com

In this paper, we present a review of the blockchain technology, which underlies the Bitcoin cryptocurrency. We also discuss some related research directions, which are of scientific and practical interest. Alternative algorithms for transactions confirmation are considered. Potentially, they may be more effective and less resource consuming. We also touch such important problem as a lack of actual decentralization and anonymity which are stated as the main Bitcoin benefits comparing with traditional money system. The arguments in favour of this position are as follows: the presence of large mining pools, the influential core developers, the alert mechanism and some other instruments which may be misused.

Keywords: cryptocurrency, Bitcoin, Mining, distributed ledger.

ВВЕДЕНИЕ

Традиционная схема товарно-денежных отношений предполагает, что покупатель передает продавцу деньги, а взамен получает желаемый товар или услуги. При этом должны выполняться условия, делающие эту схему жизнеспособной, а именно:

– покупатель не должен иметь возможности дважды использовать одни и те же денежные средства;

– продавец должен иметь инструменты, чтобы убедиться в получении денег перед передачей товара покупателю;

– должна быть исключена возможность незаконной эмиссии (подделки) денег.

Если какое-либо из этих требований окажется нарушено, то продавец рискует оказать свои услуги или отдать товар бесплатно, не имея позже возможности получить интересующие уже его товары и услуги.

При расчетах посредством наличных денег первые два требования реализуются естественным образом, исходя из физического наличия или отсутствия на руках покупателя купюр и монет, а выполнение третьего требования обеспечивается водяными знаками, законодательством и т.д.

Гарантом выполнения данных требований при безналичных расчетах является банк, через который проходят все платежи. Первое условие обеспечивается списанием средств со счета покупателя, второе – проверкой наличия средств на счете покупателя и выдачей чека банковским терминалом, а третье условие обеспечивается тем, что эмиссия находится под контролем банка – доверенной стороны. Говоря про риски, следует подчеркнуть, что если продавец отдаст товар, не дождавшись подтверждения терминала о переводе средств на его счет, то возникает вероятность того, что он имеет шанс отдать товар бесплатно.

Систему Биткоин можно представлять себе как аналог безналичных денег, где роль банка (третьей доверенной стороны), играет так называемая цепочка блоков или блокчейн (blockchain), которая поддерживается коллективно анонимными узлами, называемыми майнерами (miners). В русскоязычных источниках можно встретить термин «распределенный реестр» [20]. Именно эти особенности позволяют характеризовать биткоин-деньги анонимными и децентрализованными.

ОБЗОР ТЕХНОЛОГИИ РАСПРЕДЕЛЕННОГО РЕЕСТРА «БЛОКЧЕЙН»

Структура цепочки блоков. Цепочка блоков по своей сути представляет журнал транзакций, куда записываются все сделки, осуществляемые в этой валюте, и, таким образом, любой продавец перед передачей товара всегда может проверить наличие денег на счете покупателя, отследив все поступления и расходы, связанные с его счетом (реализуется это посредством специального программного обеспечения). Идеальный журнал транзакций можно представлять себе в виде растиражированных идентичных копий между абсолютно всеми участниками такой платежной системы (покупателями и продавцами).

В случае единственного экземпляра журнала технология перевода денег со счета на счет аналогична работе через банк. В момент запуска системы в журнале делается запись о том, сколько средств находится на счету у каждого участника системы, и эта запись подписывается всеми ими. После этого участники могут переводить друг другу деньги; для этого продавец и покупатель обращаются к журналу, и продавец проверяет по всем записям, есть ли требуемая сумма на счете покупателя, после чего покупатель делает запись в журнале о переводе денег продавцу и скрепляет ее своей подписью. Эмиссионную функциональность также можно реализовать при помощи единовременной подписи всех участников. Поскольку в журнале делаются записи исключительно о тратах (только первая запись о началь-

ном состоянии счетов не является таковой, но она скрепляется подписями всех участников), то говорить о мошенничестве здесь бессмысленно: мошенник может лишь перевести меньше денег, чем требуется, но это контролируется продавцом. Главное здесь – это обеспечить подлинность и сохранность самого журнала.

Аналогичную схему можно реализовать и посредством журнала, растиражированного всем участникам системы. Для этого в момент запуска системы участники получают по экземпляру журнала, где записаны начальные суммы на их счетах (они могут быть нулевыми). После этого журналы необходимо хранить так, чтобы у каждого было доверие к своему экземпляру, или, другими словами, была уверенность в том, что записи в свой журнал делает только его владелец. При такой схеме для перевода денег со счета на счет продавец и покупатель сверяют свои копии журнала, затем продавец проверяет наличие денег у покупателя и обе стороны делают запись о переводе денег в свои журналы. После этого они транслируют информацию о переводе всем остальным участникам системы.

Очевидно, что как минимум в силу технических сложностей описанная система не может быть реализована на практике при большом (и даже умеренно большом) числе участников, поскольку необходима идеальная синхронизация участников для обеспечения идентичности всех копий журнала. Тем не менее концептуально такую систему можно считать неким идеализированным образом системы Биткоин, базирующуюся на распределенном реестре «блокчейн».

Технологии для реализации распределенного реестра. Поскольку реализовать такие идеальные системы не представляется возможным, то необходимо как-то смягчить требования, прежде всего, к синхронизации, «заплатив» чем-то другим. При этом необходимо обеспечить доверие пользователей к этой системе, даже если у них отсутствует копия такого журнала. Для достижения этих свойств система Биткоин опирается на ряд приемлемых на практике механизмов, основными из которых являются следующие: одноранговая (peer-to-peer) сеть, криптографическая цифровая подпись, временной штамп (timestamp), криптографическая хеш-функция SHA-256, дерево Меркля, доказательство выполненной работы (proof-of-work) [3, 9, 13]. Таким образом, в отличие от банка, доверие к которому формируется на основе лицензии, репутации, системы страхования и других инструментов, доверие к криптовалюте базируется на криптографии, алгоритмах и вычислительных мощностях.

Транзакции по переводу денег в системе Биткоин. На пользовательском уровне работа с биткоин-деньгами не отличается от операций с фиатными валютами (рубль, доллар, евро) и электронными деньгами (QIWI, Yandex.Деньги, PayPal). Для пользователя существуют счета, суммы на этих счетах, счета других пользователей, возможность для перевода и т.д. Пользователь может перевести деньги со своего счета на счет другого абонента или, соответственно, получить поступления со счета другого абонента на свой счет.

Однако с технологической точки зрения транзакции и счета в системе Биткоин имеют иную природу, нежели их традиционные двойники. Первое отличие заключается в том, что биткоин-счет не просто указывает на то, у

какого клиента сколько денег на счету, но и отличает суммы, поступившие из разных источников. Другими словами, при традиционных расчетах единственной релевантной информацией является объем денежных средств на счете. Важна лишь сумма. Равно как и в случае наличных денег, где нет разницы, откуда поступила та или иная купюра: продавец перед тем, как отпустить товар, проверяет лишь получаемую сумму. В системе Биткоин счет содержит информацию о суммах поступления и об источниках поступления; причем каждая сумма привязана к источнику и для осуществления платежа на требуемую сумму необходимо взять поступления на сумму, превышающую (или равную) сумму покупки, а затем вернуть остаток на свой счет. Естественно, эти операции осуществляются программно, но алгоритм именно таков. В частности, невозможно перегруппировать свои финансы по-другому, не прибегая к формированию транзакции, на вход которой подать поступления, а на выходе указать, как их перераспределить и вернуть на свой счет.

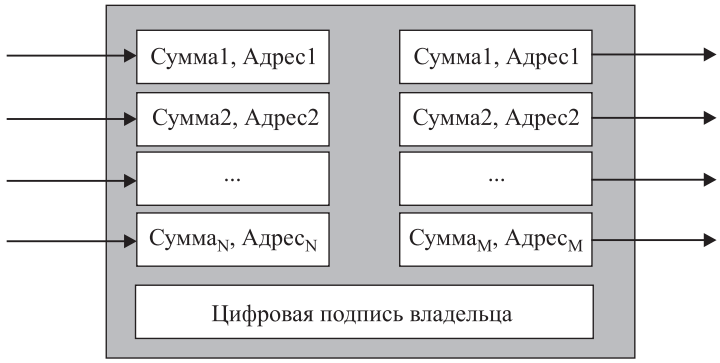

Рис. 1. Схема транзакции в системе Биткоин

Схематично структура транзакции изображена на рис. 1. Входы указывают на то, какие поступления необходимо поместить в транзакцию, а выходы – на какие счета и в каком объеме отправить. Важно отметить, что суммы входов плательщик не может указывать сам; все, что он может сделать, – это выбрать поступления, суммарный объем которых не меньше, чем размер желаемого платежа. В то же время суммы в выходах плательщик выбирает самостоятельно. Например, для оплаты покупки стоимостью 100 BTC плательщик может выбрать поступления на сумму 120 BTC, перевести 90 BTC продавцу, а 30 вернуть на свой счет. Подлинность транзакции подкрепляется цифровой подписью ECDSA.

Технология подтверждения транзакций. Рассмотрим теперь технологию подтверждения транзакций, согласно которой вырабатывается цепочка блоков. Если бы система Биткоин была идеальной в том смысле, что все пользователи существовали бы в системе постоянно, без добавления новых, то доверие к журналу транзакций формировалось бы инкрементно, транзакция за транзакцией. Однако на практике, естественно, к системе будут подключаться новые пользователи, которым необходимы инструменты, которые бы позволили им убедиться в правильности всех транзакций и сформировать доверие к системе.

С целью технологической целесообразности транзакции подтверждаются блоками, а не по одной. В настоящее время каждый блок, вырабатываемый приблизительно один раз в 10 мин, состоит приблизительно из 1000–2000 транзакций [21]. Подтверждением блоков занимаются так называемые майнеры (miners), за которыми могут стоять как отдельные люди, так и группы людей. Система Биткоин спроектирована таким образом, что подтверждение очередного блока является вычислительно сложной проблемой и имеет форму своеобразного соревнования, победитель которого присоединяет блок к существующей цепочке и получает награду в виде эмитированных биткоинов. Здесь следует особо подчеркнуть, что такая схема подтверждения транзакций подчинена достижению одновременно двух (в общем случае не связанных между собой) целей: обеспечению работоспособности системы и поддержанию технологии эмиссии.

Упомянутая вычислительно-сложная проблема заключается в частичном обращении двойного применения криптографической хеш-функции SHA-256 методом перебора. Необходимо найти часть прообраза этой функции, обеспечивающей определенное число нулей в качестве старших разрядов ее значения. В момент запуска системы Биткоин требовалось найти 32 нуля, однако в настоящее время это число составляет 69–70 нулей из-за подключения к данному соревнованию большого числа майнеров и созданию специализированных аппаратных архитектур, спроектированных и оптимизированных для решения именно этой задачи.

Требуемое число нулей адаптируется системой автоматически с целью поддержания приблизительно постоянной скорости майнинга – время между подтверждениями двух соседних блоков должно составлять около 10 мин. При подтверждении блока берется служебная информация (далее – Value) и перебираемое значение (Nonce). Целью является подбор такого Nonce, чтобы результат вычисления хеш-функции имел заданное системой число нулей вначале:

$$\begin{aligned}
&SHA256(\, SHA256(\, Value \,||\, Nonce_1 \,)\,) = 1001011101010011..11\\
&SHA256(\, SHA256(\, Value \,||\, Nonce_2 \,)\,) = 1001011101011001..10\\
&SHA256(\, SHA256(\, Value \,||\, Nonce_3 \,)\,) = 1001011101011001..11\\
&SHA256(\, SHA256(\, Value \,||\, Nonce_4 \,)\,) = 1001011101010101..00\\
&SHA256(\, SHA256(\, Value \,||\, Nonce_5 \,)\,) = 1001011101010101..01\\
&\qquad\qquad\qquad\qquad\qquad\qquad \ldots\\
&SHA256(\, SHA256(\, Value \,||\, Nonce_N \,)\,) = 0000000000000001..01
\end{aligned}$$

Эмиссия в Биткоин. Эмиссия в системе Биткоин реализуется в виде награды майнерам за закрытие очередного блока и является основным фактором, мотивирующим майнеров выполнять свою работу, обеспечивая тем самым работу всей системы. Такая схема эмиссии призвана децентрализовать криптовалюту, поскольку кроме подбора подходящего значения Nonce другой способ эмиссии отсутствует. Можно сказать, что «печатный станок» не контролируется какой-то одной организацией наподобие Центрального Банка или ФРС. Напротив, система предоставляет возможность любому желающему «напечатать» новые купюры, но при этом подобный доход может быть лишь усредненным, поскольку над выработкой блока одновременно работает большое число узлов, и награда достается тому, кто закрыл

блок первым. Причем, строго говоря, увеличение компьютерных мощностей не гарантирует повышение дохода, а только повышает вероятность закрыть блок первым. Однако, согласно законам теории вероятностей, при работе в течение длительного времени, действительно, усредненный доход майнеров пропорционален вычислительным мощностям, имеющимся в их распоряжении.

Доход одного конкретно взятого узла зависит от двух факторов: мощности этого узла и общего количества узлов, занятых в майнинге. Для более наглядной демонстрации связи транзакций, эмиссии и майнинга в системе Биткоин проведем аналогию с традиционными безналичными транзакциями и эмиссией фиатных денег. Фактически Биткоин эмитирует деньги за осуществление транзакции или за перевод денег. Очевидно, что для существующей банковской системы такая ситуация неприемлема в силу простоты перевода денег со счета на счет. Тогда для заработка банк мог бы просто фиктивно переводить деньги со счета на счет и получать новые купюры от Центробанка. Принципиальное отличие Биткоин от фиатных денег в том, что перевести и напечатать бумажные деньги технологически легко, а «напечатать» и перевести биткоины технологически сложно. Таким образом, proof-of-work представляет собой ограничение в скорости «печатания» биткоинов.

ОБЗОР РИСКОВ И АКТУАЛЬНЫХ НАПРАВЛЕНИЙ ИССЛЕДОВАНИЙ БИТКОИН

Проблемы децентрализованности Биткоин. Хотя в статье С. Накамото [13], в которой Биткоин был представлен, система заявлена как децентрализованная (в теории) не подконтрольная никаким конкретным организациям, существуют признаки того, что с практической точки зрения в полной мере ее нельзя считать таковой. В работе [10] указывается на ряд свойств, которые позволяют сделать вывод о том, что в настоящее время ряд жизненно важных решений относительно функционирования системы Биткоин принимаются ограниченным кругом лиц. Кроме того, существуют участники системы, имеющие возможность в одностороннем порядке обесценить денежные средства, находящиеся в определенных Биткоин-кошельках.

Наличие крупных майнинговых пулов. Работоспособность всей системы Биткоин зиждется на процедуре закрытия блоков, или майнинге. При этом вероятность одного конкретно взятого узла закрыть блок, подобрав подходящий Nonce, зависит от вычислительных мощностей в его распоряжении. Поэтому с целью более частого получения награды узлы заинтересованы в увеличении своих ресурсов, и это можно сделать посредством объединения нескольких или многих узлов в один, а затем распределять награду между участниками пропорционально их мощностям. В таком случае они получают награду в меньшем размере, но более регулярно. Особенно это может быть выгодно тем, кто в одиночку, согласно законам теории вероятностей, не имеет возможности получить награду за приемлемый срок.

В настоящее время за закрытие блока майнеры получают награду в виде эмитированных биткоинов и в виде суммарной комиссии, оставленной

инициаторами транзакций, что в целом является достаточно прибыльным делом и мотивирует пользователей становиться «профессиональными» майнерами, которые создают майнинговые «фермы» и пулы, настолько превосходящие по мощности отдельных майнеров, что подавляющую часть блоков закрывают именно они. Так, по данным на 2017 г. [18], 10 крупнейших в мире пула (среди них F2Pool, AntPool, BitFury) контролировали порядка 80 % мощности всей Биткоин-сети. Такие факты говорят об угрозе сговора администраторов перечисленных пулов, что может позволить им не только получать значительную долю эмиссионных денег, но и вырабатывать более одной цепочки блоков одновременно, имея возможность расплачиваться по несколько раз одними и теми же деньгами (правда лишь в краткосрочной перспективе, поскольку как только это станет известно, курс биткоина резко упадет). Кроме того, они смогут блокировать или замедлять исполнение невыгодных для них транзакций. Фактически владельцы или менеджеры таких крупных пулов могут сформировать нечто подобное совету директоров и принимать выгодные им стратегически важные решения, касающиеся функционирования системы. В работе [14] показано, что нарушение стабильности может наблюдаться даже при контроле злоумышленником всего лишь 38,2 % мощности Биткоин-сети.

Web-сервисы и упрощенная верификация. Размер цепочки блоков целиком достаточно велик (на ноябрь 2017 г. он составлял уже более 140 Gb [21]), что неприемлемо для многих клиентов, обладающих ограниченными ресурсами. Уже только для ее скачивания необходимо затратить несколько часов. Некоторым клиентам, например, пользующимся мобильными устройствами, это может оказаться не просто неудобным, но и неприемлемым. Для решения такой проблемы, во-первых, создаются web-сервисы, предоставляющие различную функциональность по работе с Биткоин, а, во-вторых, существует механизм упрощенной верификации, позволяющий проверять корректность транзакций без скачивания всей цепочки блоков. В обоих случаях клиенты должны полагаться на другие узлы, которых, очевидно, меньше, чем всех клиентов. В итоге такие клиенты ставят себя в зависимость от тех узлов, которые имеют в своем распоряжении полную цепочку блоков. Таким образом, реально функциональные возможности контролируются неким меньшинством, реальная структура и подчинение которого может быть скрыта.

Обновление системы ядром разработчиков и механизм оповещений. Поскольку система Биткоин существенным образом базируется на программном обеспечении, то возникает необходимость его периодически обновлять. Полномочиями для этого обладает ядро разработчиков, которое, например, может изменять комиссионную политику, разрешать конфликтные «жесткие вилки» (hard forks), уведомлять клиентов об обновлениях и т.д. Все эти механизмы дают этим разработчикам целый ряд инструментов влияния на всю экосистему Биткоин.

Для примера рассмотрим яркую ситуацию, имевшую место 11.03.2013 г. и связанную с так называемой «жесткой вилкой». Суть проблемы заключалась в том, что после очередного обновления системы произошло раздвоение цепочки блоков так, что часть узлов по техническим причинам стала присоединять новые блоки к одной ветке, а часть – к другой. И вследствие

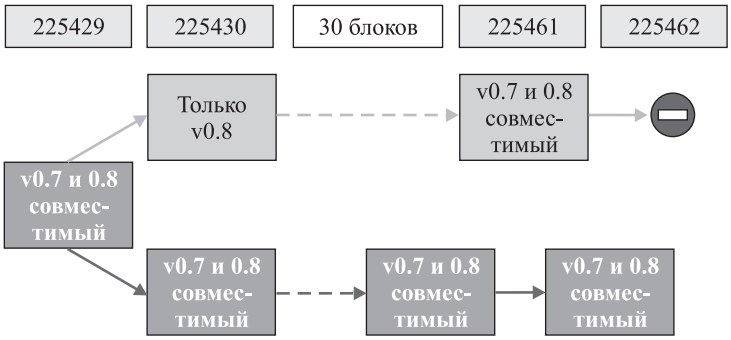

Рис. 2. Аннулирование транзакций вследствие возникновения «жесткой вилки», имевшей место 11.03.2013 г.

этого технического сбоя ветки стали расти параллельно вопреки законам Биткоин. Схематично эта ситуация изображена на рис. 2.

Такая ситуация продолжалась порядка 90 мин, после чего ядро разработчиков, заручившись поддержкой одного из крупнейших майнинговых пулов, внесло изменение в программное обеспечение и в одностороннем порядке признало недействительной более длинную из этих веток, обесценив тем самым порядка 1700 транзакций. Этот инцидент стал примером, когда группа из нескольких человек оказала большее влияние, чем более половины мощности всей Биткоин-сети [10].

Возможность использования «меченых денег». Поскольку транзакции по своему существу образуют цепочку цифровых подписей, любые траты можно отследить с момента эмиссии. И хотя без использования дополнительных инструментов выявить реальных стоящих за ними людей может быть невозможно, но привязать платежи к конкретным адресам довольно просто. В связи с этим если адрес ведет себя неправильно (в каком-либо смысле), любой заинтересованный участник системы Биткоин может ограничивать взаимодействие с подобными адресами или же полностью блокировать поступающие от них платежи. Так, известен случай, когда после кражи большой суммы с торговой площадки Bitcoinica [16], крупная биржа цифровых денег сервис MtGox [19] отследил, куда ушли эти деньги и внес соответствующий адрес в свой черный список [17]. Принимая во внимание такие возможности использования «меченых денег», можно понять, что подобные блокировки могут быть осуществлены специально, но не только с целью обеспечить честное функционирование системы, но и с целью контроля части оборота [10]. Существуют и научно обоснованные алгоритмы, позволяющие нарушать анонимность в некоторых случаях [5, 7].

Альтернативы для proof-of-work. Технология доказательства выполненной работы (proof-of-work), лежащая в основе функционирования всей системы Биткоин имеет ряд свойств, допускающих как нерациональное использование ресурсов, так и вовсе злоупотребления, приводящие даже к нарушению исходно заявленных характеристик. В связи с этим некоторые научные исследования направлены на то, чтобы предложить альтернативные «загадки», которые можно разгадывать с пользой для чего-либо, а также пресечь злоупотребления и нарушения заявленных свойств.

Рассмотрим вначале так называемые «полезные» задачи. Существующая система майнинга подталкивает людей к нерациональному использованию ресурсов, в частности, энергии, затрачиваемой на подбор аргумента для требуемого хеш-значения, и затрат на производство специализированного оборудования для реализации этого процесса. В масштабах всей Биткоин-сети это может выливаться в колоссальные объемы, сопоставимые с затратами на электроэнергию целых европейских стран. Таким образом, если удастся сохранить заявленный уровень безопасности и стабильности при трансформации затраченных ресурсов в какие-либо полезные ценности, то «отходы» уменьшатся. Одна из идей для реализации такого подхода может состоять в использовании функции, направленной на решение какой-либо актуальной научной проблемы [11]. По этому пути пошли создатели системы Primecoin (prime – простое), побочным эффектом которой оказываются сгенерированные простые числа, необходимые для многих криптографических протоколов. Другая система вместо майнинга использует доказательство доступности, основанное на том, что майнеры не вырабатывают какой-то Nonce, а предоставляют ресурсы памяти в коллективное полезное использование. Разработка других эффективных средств поддержки работы Биткоин – это актуальное направление исследований.

Следующий тип задач – задачи, не допускающие аутсорсинг, – возник вследствие того, что, как уже отмечалось выше, крупнейшие майнинговые пулы контролируют настолько большие ресурсы, что возникает угроза их сговора и монополизации эмиссии и подтверждения транзакций [8]. Такие задачи призваны исключить возможность объединения усилий множества узлов для концентрации мощности под флагом одного. Тем самым сохраняется изначальное правило Биткоин «один процессор – один голос». Преследуют задачу сохранения «честной игры» и загадки, устойчивые против интегральных схем специального назначения (ASIC), которые на сегодняшний день дают максимально возможные ресурсы для майнинга, оставляя далеко позади традиционные, в том числе и майнинг на видеокартах [6,8]. Создаются также альтернативы, которые должны быть устойчивыми против квантового компьютера, создание которого прогнозируется в ближайшие десятилетия [1].

ЗАКЛЮЧЕНИЕ

В настоящем обзоре затронуто функционирование криптовалюты Биткоин, основанное на распределенном реестре «блокчейн». Но распределенный реестр может быть использован гораздо шире, чем только для замены банка. Блокчейн может выступать в качестве третьей доверенной стороны для реализации целого ряда других протоколов [4], среди которых, например, защищенное распределение секретных ключей [12] и электронное голосование [15]. Весь этот спектр возможностей открывает обширное поле для научных исследований и для инженерных разработок.

Литература

1. *Aggarwal D., Brennen G. etc*. Quantum attacks on Bitcoin, and how to protect against them // arXiv: 1710.10377v1. 2017. 21 p.

2. *Andrychowicz M., Dziembowski S., Malinowski D. etc*. Fair two-party computations via Bitcoin deposits // Proc. 18-th International Conference on Financial Cryptography and Data Security (FC 2014). Lecture Notes in Computer Science. Vol. 8438. P. 105–121.
3. *Back A*. Hashcash – a denial of service counter-measure // Technical Report. 2002.
4. *Bentov I., Kumaresan R*. How to use Bitcoin to design fair protocols // Proc. CRYPTO-2014. Lecture Notes in Computer Science. 2014. Vol. 8617. P. 421–439.
5. *Biryunov A., Khovratovich D., Pustogarov I*. Deanonymisation of clients in Bitcoin P2P network // Proc. ACM SIGSAC Conference on Computer and Communications Security. 2014. P. 15–29.
6. *Biryunov A., Khovratovich D*. Equihash: asymmetric proof-of-work based on the generalized birthday problem // Ledger. 2017. Vol. 2. P. 1–30.
7. *Biryukov A., Pustogarov I*. Bitcoin over Tor isn't a good idea // Proc. 36-th IEEE Symposium on Security and Privacy. 2015. P. 122–134.
8. *Bonneau J., Miller A., Clark J. etc*. SoK: research perspectives and challenges for Bitcoin and cryptocurrencies // Proc. 36-th IEEE Symposium on Security and Privacy. 2015. P. 104–121.
9. *Dwork C., Naor M*. Pricing via processing or combatting junk mail // Proc. CRYPTO-92. Lecture Notes in Computer Science. 1993. P. 139–147.
10. *Gervais A., Karame G., Capkun V. etc*. Is Bitcoin a decentralized currency? // IEEE Security & Privacy. 2014. Vol. 12. P. 54–60.
11. *Kroll J., Davey I., Felten E*. The economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries // Proc. 12-th Workshop on the Economics of Information Security (WEIS 2013). P. 1–21.
12. *McCorry P., Shahandashti S., Clarke D. etc*. Authenticated key exchange over Bitcoin // Proc. 2-nd International Conference on Research in Security Standardisation. Lecture Notes in Computer Science. 2015. Vol. 9497. P. 3–20.
13. *Nakamoto S*. Bitcoin: A Peer-to-Peer Electronic Cash System // Whitepaper. 2008.
14. *Teutsch J., Jain S., Saxena P*. When cryptocurrencies mine their own business // Proc. 20-th International Conference on Financial Cryptography and Data Security (FC 2016). Lecture Notes in Computer Science. 2017. Vol. 9603. P. 499–514.
15. *Zhao Z., Hubert-Chan T.-H*. How to vote privately using Bitcoin // Proc. 17-th International Conference on Information and Communications Security (ICICS 2015). Lecture Notes in Computer Science. 2016. Vol. 9543. P. 82–96.
16. Bitcoinica // https://en.bitcoin.it/wiki/Bitcoinica
17. Bitcointalks forum // https://bitcointalk.org/
18. Top-10 Bitcoin mining pools // fomag.ru/news/top-10-mayning-pulov-bitkoina/
19. MtGox // https://ru.wikipedia.org/wiki/Mt.Gox
20. Программа «Цифровая экономика Российской Федерации». URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
21. Blockchain observer // www.blockchain.info

Bibliography

1. *Aggarwal D., Brennen G. etc*. Quantum attacks on Bitcoin, and how to protect against them // arXiv: 1710.10377v1. 2017. 21 p.
2. *Andrychowicz M., Dziembowski S., Malinowski D. etc*. Fair two-party computations via Bitcoin deposits // Proc. 18-th International Conference on Financial Cryptography and Data Security (FC 2014). Lecture Notes in Computer Science. Vol. 8438. P. 105–121.
3. *Back A*. Hashcash – a denial of service counter-measure // Technical Report. 2002.
4. *Bentov I., Kumaresan R*. How to use Bitcoin to design fair protocols // Proc. CRYPTO-2014. Lecture Notes in Computer Science. 2014. Vol. 8617. P. 421–439.

5. *Biryunov A., Khovratovich D., Pustogarov I*. Deanonymisation of clients in Bitcoin P2P network // Proc. ACM SIGSAC Conference on Computer and Communications Security. 2014. P. 15–29.
6. *Biryunov A., Khovratovich D*. Equihash: asymmetric proof-of-work based on the generalized birthday problem // Ledger. 2017. Vol. 2. P. 1–30.
7. *Biryukov A., Pustogarov I*. Bitcoin over Tor isn't a good idea // Proc. 36-th IEEE Symposium on Security and Privacy. 2015. P. 122–134.
8. *Bonneau J., Miller A., Clark J. etc*. SoK: research perspectives and challenges for Bitcoin and cryptocurrencies // Proc. 36-th IEEE Symposium on Security and Privacy. 2015. P. 104–121.
9. *Dwork C., Naor M*. Pricing via processing or combatting junk mail // Proc. CRYPTO-92. Lecture Notes in Computer Science. 1993. P. 139–147.
10. *Gervais A., Karame G., Capkun V. etc*. Is Bitcoin a decentralized currency? // IEEE Security & Privacy. 2014. Vol. 12. P. 54–60.
11. *Kroll J., Davey I., Felten E*. The economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries // Proc. 12-th Workshop on the Economics of Information Security (WEIS 2013). P. 1–21.
12. *McCorry P., Shahandashti S., Clarke D. etc*. Authenticated key exchange over Bitcoin // Proc. 2-nd International Conference on Research in Security Standardisation. Lecture Notes in Computer Science. 2015. Vol. 9497. P. 3–20.
13. *Nakamoto S*. Bitcoin: A Peer-to-Peer Electronic Cash System // Whitepaper. 2008.
14. *Teutsch J., Jain S., Saxena P*. When cryptocurrencies mine their own business // Proc. 20-th International Conference on Financial Cryptography and Data Security (FC 2016). Lecture Notes in Computer Science. 2017. Vol. 9603. P. 499–514.
15. *Zhao Z., Hubert-Chan T.-H*. How to vote privately using Bitcoin // Proc. 17-th International Conference on Information and Communications Security (ICICS 2015). Lecture Notes in Computer Science. 2016. Vol. 9543. P. 82–96.
16. Bitcoinica // https://en.bitcoin.it/wiki/Bitcoinica
17. Bitcointalks forum // https://bitcointalk.org/
18. Top-10 Bitcoin mining pools // fomag.ru/news/top-10-mayning-pulov-bitkoina/
19. MtGox // https://ru.wikipedia.org/wiki/Mt.Gox
20. Программа «Цифровая экономика Российской Федерации». URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf
21. Blockchain observer // www.blockchain.info