Открытые и закрытые блокчейны

Часть 1: эксклюзивные блокчейны

White Paper

(перевод на русский)

BitFury Group

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

22 октября 2015 (Версия 1.0-ru)

Аннотация

Решения на основе блокчейнов — одно из ключевых современных направлений для исследований для финансовых и государственных учреждений. Нет сомнений в том, что костяк технологий, используемых в настоящее время в таких учреждениях, морально устарел и требует реорганизации для соответствия текущим требованиям. Децентрализованные и распределенные реестры в виде блокчейнов на данный момент являются одними из наиболее обсуждаемых решений описанной проблемы. В статье описываются системы на основе блокчейнов с эксклюзивным доступом к обработке транзакций (англ. permissioned), которые могут послужить основой для создания надежных финансовых баз данных или временно упорядоченных реестров документов. Мы обосновываем доступность протокола и данных блокчейн-систем для конечных пользователей; такой доступ позволяет достичь более высокого уровня децентрализации и прозрачности. Мы приводим аргументы в пользу использования доказательства работы (англ. proof of work) в контексте таких блокчейнов для обеспечения и диверсификации безопасности.

История версий

Версия	Дата	Описание изменений
1.0	20 окт. 2015	Начальная версия (англ.)
1.0-ru	22 окт. 2015	Начальная версия (перевод на русский)

Хотя большую часть финализации финансовых сделок между компаниями-трейдерами в принципе можно автоматизировать, соответствующие операции в настоящее время проводятся вручную отчасти из-за юридических требований, а отчасти — по причине инерции и следованию традициям [1]. Аналогично, в государственном секторе существует много реестров документов, и их согласование занимает много времени и усилий. Таким образом, существует запрос на автоматизированные системы реестров, которые могли бы занять место текущих реестров и сформировать единую взаимосвязанную экосистему.

Биткойн [2] — одноранговая система цифровой валюты, в которой блокчейн (англ. blockchain — цепочка блоков) является ключевой инновацией. По сути, блокчейн представляет собой специализированную распределенную базу данных, предназначенную для обработки упорядоченных во времени данных, таких как финансовые транзакции. Основной элемент блокчейнов — встроенная безопасность — отличает их от обыкновенных горизонтально масштабируемых баз данных, таких как MySQL Cluster, MongoDB и Apache HBase. Безопасность блокчейна означает практическую невозможность удалить или изменить записи в базе данных; более того, безопасность обеспечивается не за счет централизованной проверки (что возможно для перечисленных выше баз данных), а за счет самого протокола блокчейна. Распределенность и децентрализация блокчейнов делает их привлекательной заменой для существующих решений, используемых, например, в финансовом секторе. Недостатки блокчейнов, такие как сравнительно медленное подтверждение транзакций и меньший уровень масштабируемости, для многих приложений не настолько важны, как возрастающий уровень безопасности и отсутствие точек отказа (англ. single point of failure). По словам Ника Сабо (Nick Szabo), изобретателя идеи смарт-контрактов, «настоящие финансовые инструменты уже в некоторой степени децентрализованы благодаря “человеческому блокчейну”, состоящему из бухгалтеров, аудиторов и т. п., проверяющих работу друг друга» [3] (перевод наш). Таким образом, автоматизация операций, производимых этой цепочкой при условии сохранения децентрализации, может стать шагом в правильном направлении.

Финансовые учреждения и другие организации, работающие с реестрами данных, не спешат использоваться блокчейном биткойна (самым развитым публичным блокчейном) или другими общественно доступными блокчейнами. Этому существует несколько причин, например, соответствие законам. В разделе 1 описывается текущее состояние внедрения блокчейн-технологии. В разделе 2 исследуется основа блокчейнов и приводятся аргументы в пользу открытости данных и протокола блокчейна для конечных потребителей из соображений безопасности. В разделе 3 мы описываем решения, которые могли бы использоваться в блокчейнах с эксклюзивным доступом к обработке транзакций, такие как объединенный майнинг (англ. merged mining) и привязка к блокчейнам (англ. blockchain anchoring), а также обосновываем целесообразность доказательства работы для таких блокчейнов. Во второй части статьи мы рассмотрим общедоступные блокчейны (англ. permissionless blockchains), которые в перспективе могут стать вездесущим базовым слоем для блокчейн-приложений, и проведем

сравнение закрытых, эксклюзивных и общедоступных моделей блокчейна.

1. Текущая ситуация

С 2014 года тема баз данных на основе блокчейнов стала популярной среди банков и других финансовых учреждений. Было анонсировано несколько прототипов и моделей с использованием технологии блокчейна. В некоторых случаях, блокчейн биткойна используется напрямую:

- Эстонский LHV Bank тестирует Cuber (Cryptographic Universal Blockchain Entered Receivables), систему платежей, основанную на окрашенных монетах (англ. colored coins), организованных поверх биткойновского блокчейна [4].
- Аналогично, биржа NASDAQ планирует использовать один из протоколов покраски биткойнов — Open Assets Protocol — для обеспечения полного цикла управления ценными бумагами [5, 6].
- Крупнейший французский банк BNP Paribas, по некоторым сведениям, исследуют возможные способы интегрировать биткойн в валютные запасы банка [7].
- Британский банк Barclays заключил партнерство с биткойновской биржей Safello для исследования возможных приложений блокчейн-технологии в финансовом секторе [8].
- Goldman Sachs опубликовал отчет «Будущее финансов: революция способов оплаты в грядущем десятилетии», в котором подразумевается, что биткойн и криптовалюты в целом могут изменить платежную экосистему [9]. Goldman Sachs также принял участие в финансировании общим объемом 50 млн. долларов биткойновского стартапа Circle [10].
- Компания UBS, базирующаяся в Швейцарии, считает производные биткойна потенциально привлекательными, при условии принятии соответствующей юридической базы [11].

В некоторых других прототипах задействованы системы Ripple или Ethereum:

- Протокол Ripple был интегрирован с немецким банком Fidor, а также с CBW Bank из Канзаса и банком Cross River из Нью-Джерси [12]. Согласно словам Giles Gade, CEO и президента Cross River, одной из главных мотиваций использовать именно Ripple стало соответствие системы законам США.
- Три австралийских банка — Commonwealth Bank of Australia (CBA), Westpac Banking Corporation, а также Australia and New Zealand Banking Group — экспериментируют с платежами через протокол Ripple [13, 14]. David Whiteing, CIO банка CBA, назвал отсутствие встроенных токенов в Ripple как ключевую причину, по которой система была выбрана вместо биткойна.

- Компания UBS анонсировала эксперименты с блокчейном Ethereum с целью построения полностью автоматизированных бондов [15]. Alex Batlin, директор по инновациям и исследованиям UBS, не исключил возможности использования биткойновского блокчейна для схожих задач.

Однако в большинстве случаев финансовые учреждения готовы строить свои собственные закрытые блокчейны или исследуют блокчейн-технологию без указания конкретной реализации:

- Три крупных нидерландских банка — ABN Amro, ING и Rabobank — исследуют использование блокчейна для платежных систем [16].
- Компания Citigroup построила три закрытых блокчейна и внутреннюю валюту на их основе, фокусируясь на платежах и исключении рисков при сделках с мелкими местными банками [17]. Помимо этого, Citigroup заключила партнерство с Safaricom, мобильным оператором из Кении, для того чтобы обеспечить денежные переводы без необходимости открытия счета в банке.
- Santander, один из крупнейших банков мира согласно рейтингу Форбс [18], выделил от 20 до 25 возможных применений блокчейн-технологии в банковском деле, включая международные денежные переводы, синдицированные займы и управление залоговыми обязательствами [19].
- Аналогично, Deutsche Bank заявил, что у распределенные систем учета и в особенности у блокчейнов есть применения в работе с фиатными валютами и ценными бумагами; они подходят для создания прозрачных систем и упрощения наблюдения согласно системам противодействия отмыванию денег / Know Your Customer [20].
- Финансовое управление Сингапура назвало блокчейны одним из главных трендов технологий, которые могут затронуть финансовые сервисы. Низкая стоимость, более высокая скорость разработки и отказоустойчивость были названы главными преимуществами блокчейн-систем по сравнению с традиционными подходами [21].

Решения на основе блокчейнов используются не только для построения распределенных систем финансового учета. Схожее приложение — Интернет вещей (англ. Internet of Things) — разрабатывается компаниями IBM и Samsung [22]. Проект под названием ADEPT (Autonomous Decentralized Peer-to-Peer Telemetry) использует протокол Ethereum для создания смарт-контрактов. Другой проект IBM также нацелен на создание платформы для смарт-контрактов и рассчитан в первую очередь для людей без доступа к традиционной банковской инфраструктуре [23].

Блокчейн достаточно часто упоминается в финансовой среде как технология, способная преобразить будущее платежей:

- Блокчейн упоминается в двух глобальных сдвигах, которые произойдут в ближайшем будущем, согласно исследованию Всемирного экономического форума [24]. Первый сдвиг —

первый государственный налог, собранный с использованием блокчейнов, предположительно произойдет в 2023 году. Второй сдвиг — хранение более чем 10% мирового ВВП на блокчейнах — состоится до 2027 года.

- Банк Англии опубликовал отчет, в котором утверждается, что технологии распределенных финансовых систем учета представляет собой фундаментальное изменение правил работы платежных систем [25].
- Blythe Masters, CEO компании Digital Asset Holdings, сравнила блокчейн с электронной почтой для денег [26].
- Согласно словам CIO Standard Chartered Anju Patwardhan, инфраструктура на основе блокчейна может сделать финансовые транзакции более надежными и отслеживаемыми, в то же время уменьшив их стоимость для конечных потребителей и упростив противодействие отмыванию денег [27].
- Usama Fayyad, chief data officer банка Barclays, назвал блокчейн революционной технологией для финансового сектора [28].

Общее отношение финансовых учреждений к биткойну и прочим общедоступным блокчейнам остается достаточно скептическим, в то время как мнения насчет закрытых блокчейнах или блокчейнах с регулируемым доступом в целом намного теплее. Основные причины сомнений в целесообразности использования общедоступных блокчейнов в финансовой среде заключаются в следующем:

- Невозможность контролировать обработку транзакций (т. е. майнеров в случае биткойна) [26]. В соответствии со многими юрисдикциями, личности обработчиков транзакций должны быть известными, что прямо противоречит декларируемой биткойном открытости (любой человек может быть майнером, достаточно иметь вычислительные ресурсы). Согласно CEO Metro Bank Craig Donaldson, отсутствие четко определенных правил для сервисов, работающих с биткойном, замедляет их потенциал развития [28].
- Учреждения видят угрозу конфиденциальности клиентов в публичной среде.
- Системы с ограниченным доступом могут быть эффективнее в плане тестирования, для быстрого внесения изменений в протокол блокчейна и т. п. [15].
- Доказательство работы, фундаментальное для биткойна, в случае закрытых блокчейнов является в большой степени избыточным; избавление от него позволяет повысить поток обрабатываемых транзакций и сократить расходы на функционирование [15].

В финансовой среде существуют биткойн-оптимисты, например один из основателей LinkedIn, миллиардер Reid Hoffman [29]: «По крайней мере одна глобальная криптовалюта достигнет массового рынка. Этой валютой будет либо биткойн, либо производная валюта, вдохновленная биткойном» (перевод наш). Аналогично, Richard Gendal Brown, CTO компании R3 CEV, которая занимается блокчейн-инновациями, предупреждает насчет игнорирования биткойна в

пользу распределенных систем с ограниченным доступом: «Основная цель, заложенная в дизайн биткойна — быть цифровыми наличными деньгами с устойчивостью к цензуре — имеет огромный потенциал, хороший и плохой; уже из-за одной этой возможности не стоит сбрасывать биткойн со счетов» [30] (перевод наш).

1.1. Инновации в финансовых системах учета

Недавно сформировавшийся тренд в блокчейн-инновациях — системы, предназначенные специально для обеспечения финансовых сервисов нового поколения. Указанный ниже список компаний не является полным; для более детального анализа существующих решений, мы отсылаем читателя к отчету «Распределенные системы учета с ограниченным доступом» за авторством Tim Swanson [31].

- **Digital Asset Holdings** (digitalasset.com) строит распределенную многослойную систему для обработки трейдинга ценных бумаг. Наличие промежуточного уровеня системы позволит использовать как блокчейн-решения, так и старую инфраструктуру вроде FedWire. Фирма планирует использовать как открытые блокчейны (например, биткойн), так и закрытые, построенные на основе технологии Hyperledger [32].
- Компания **Chain** (chain.com) предлагает коммерческую платформу на основе блокчейна с фокусом на передачу активов. Компания провела успешный раунд финансирования размером 30 млн. долларов при поддержке крупных финансовых организаций, включая Visa, Nasdaq, Citi Ventures и Orange [33].
- **R3 CEV** (r3cev.com) — компания, специализирующаяся на инновациях в области построения глобальных финансовых сервисов нового поколения. R3 возглавляет партнерство между глобальными банками (включая Barclays, Credit Suisse, JP Morgan, UBS, BBVA, и Commonwealth Bank of Australia), целью которого является создание общей распределенной архитектуры финансовых систем учета [34].
- Компания **Clearmatics** (clearmatics.com) строит децентрализованную клиринговую сеть, которая позволит пользователям производить обмен ценных бумаг и автоматизировать финансовые контракты при помощи технологии смарт-контрактов.
- **Eris Industries** (erisindustries.com) предоставляет решения с открытым исходным кодом, позволяющие финансовым учреждениям строить дешевую и качественную инфраструктуру, которая использует блокчейн и смарт-контракты.
- Компания **Tembusu** (tembusu.sg) разработала TRUST (Tembusu Reputation-based Universally Secure Transaction System) — платформу для управления активами на основе блокчейна.
- Проект **Enigma** (enigma.media.mit.edu) создает облачную платформу с гарантированной безопасностью с использованием разделения секретов.

Помимо этого, компании, например, **Factom** (factom.org), разрабатывают инфраструктуру для финансовых сервисов на основе биткойна.

В отличие от блокчейнов, используемых в криптовалютах, компании, перечисленные выше, предлагают решения, которые соответствуют пожеланиям финансовых учреждений:

- Предложенные решения в целом используют группы известных сервисов для создания блоков транзакций. В большинстве случаев, интеграция блоков в цепь не использует доказательство работы, используемое в биткойне и других криптовалютах. По этой причине предложенные дизайны блокчейнов не используют встроенные в протокол монеты для вознаграждения создателей блоков.
- Доступ к блокчейну ограничен кругом финансовых учреждений, создавших его, и регулирующими учреждениями.
- Алгоритм определения корректных транзакций более сложный по сравнению с используемым в биткойне; он в общем случае отображает особенности конкретных типов финансовых услуг. Часто, в блокчейн интегрируется язык сценариев, полный по Тьюрингу [35], с целью реализации комплексных контрактов. Отметим, что язык сценариев в биткойне является *намеренно* неполным по Тьюрингу, так как язык с большим количеством ограничений предотвращает использование уязвимостей в процессе проверки транзакций.

2. Технология блокчейна

Блокчейн — распределенная база данных для обработки транзакций. Хотя в настоящее время большинство блокчейнов обрабатывают финансовые транзакции, в общем случае транзакции можно рассматривать просто как атомарные изменения состояния некоторой системы. Например, блокчейн может использоваться для регистрации документов и защиты их от изменений.

Все транзакции в блокчейне хранятся в едином реестре. Поскольку транзакции полностью упорядочены по времени, текущее состояние системы (набор балансов пользователей в случае финансового блокчейна) определяется исключительно этим реестром транзакций. Хранение полной истории изменений состояния системы имеет свои преимущества, например, возможность определить состояние системы в произвольный момент времени, просто «проиграв» заново соответствующие транзакции.

В идеальном случае, обработка транзакций в рамках блокчейн-технологии должна удовлетворять следующим свойствам:

- Транзакции должны быть **согласованными** с текущим состоянием системы. Например, в случае финансовых транзакций, если баланс Алисы составляет 1 000 рублей, она не может заплатить Бобу 10 000 рублей.

- Транзакции должны быть **авторизованы**, т. е. только у Алисы должен быть к осуществлению транзакций от имени Алисы.
- Транзакции должны быть **неизменяемыми**: после того, как транзакция записана в реестр, ее должно быть невозможно изменить (например, если в реестре записана транзакция, в которой Алиса платит Бобу 100 рублей, у злоумышленника не должно быть возможности изменить сумму платежа, его отправителя или получателя).
- Транзакции должны быть **конечными**: после того, как транзакция записана в реестр, ее будет невозможно удалить оттуда, что по сути привело бы к возврату денег отправителю.
- **Устойчивость к цензуре**: если транзакция удовлетворяет всем правилам блокчейна, она должна быть в конце концов в него добавлена.

Соответствие текущему состоянию системы удовлетворяется за счет проверки транзакции совместно с этим состоянием, хранящимся в защищенной от злоумышленников памяти. Поскольку текущее состояние системы можно восстановить при помощи блокчейна, предположение защищенности не сужает безопасность системы в целом. Это предположение вводит ограничение на блокчейн, которое заключается в организации хранения транзакций таким образом, чтобы надежная верификация транзакций занимала не слишком много времени. Для финансовых блокчейнов один из возможных способов такой организации — использование непотраченных выходов транзакций (англ. unspent transaction outputs, UTXO) вместо явно заданных балансов пользователей. Состояние системы в таком случае фактически представляет собой реестр владения, который содержит информацию об условиях, определяющих владельца каждой единицы активов, циркулирующих в системе.

Проблема авторизации решается за счет использования криптографии с открытым ключом [36]. Каждому пользователю системы выдается пара из секретного и открытого ключа; открытый ключ может быть без проблем опубликован для определения цифровой личности пользователя, так как секретный ключ невозможно вывести из открытого. Например, если Алиса желает перевести 100 рублей Бобу, она (или ее доверенный агент) подписывает соответствующую транзакцию цифровой подписью, использующей ее секретный ключ. Поскольку

- корректная подпись может быть сделана исключительно лицом, знающим секретный ключ Алисы;
- для проверки подписи достаточно знания открытого ключа Алисы;
- подпись становится некорректной при изменении какого-либо из параметров подписываемой транзакции;

использование цифровых подписей решает не только проблему авторизации, но также и проблему изменяемости транзакций. Если цифровые подписи используются для всех транзакций в блокчейне, злоумышленник, получивший внутренний доступ к системе (например, хакер или бывший служащий), не может изменить эти транзакции.

Неизменяемость и конечность транзакций в системе на основе блокчейна достигается при помощи разделения транзакций в блоки, упорядоченные во времени, и расчете криптографической хэш-функции для каждого из блоков (рис. 1). Хэш-дерево, или дерево Меркла (англ. Merkle tree) — эффективная структура для вычисления такого хэша; для того чтобы избежать разночтений и чтобы соответствовать терминологии, используемой в биткойне, мы будем называть хэш, вычисленный из транзакций, *хэш-корнем* (англ. Merkle root). С целью обеспечения невозможности удаления или замены целых блоков транзакций и чтобы обезопасить вычисленные хэш-корни, блоки организуются в упорядоченную цепь (собственно, цепь блоков — блокчейн). Для упрощения проверки корректности блокчейна, ключевые свойства блоков (такие как хэш-корень и временной интервал, которому соответствует блок) выделяются в заголовок блока. Каждый заголовок блока содержит указатель на предыдущий блок (кроме самого первого блока, который напрямую прописан в протоколе блокчейна). Таким образом, неизменяемость транзакций сводится к обеспечению неизменяемости заголовков блоков. При условии что заголовки блоков должным образом защищены от изменений, для того чтобы заменить один блок, злоумышленнику потребуется заменить и все последующие блоки в блокчейне. Адекватная система защиты заголовков блоков, таким образом, делает невозможным удаление из блокчейна транзакций, записанных в него относительно давно; следовательно, блокчейн удовлетворяет условию конечности транзакций.

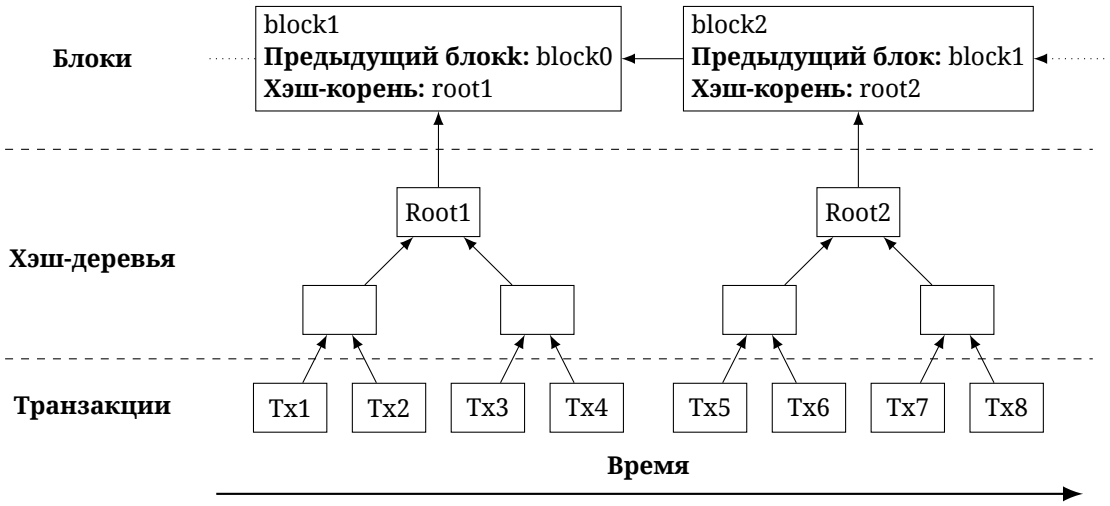

Рис. 1. Общая структура блокчейна, в которой каждый из двух показанных блоков включает в себя 4 транзакции. Поскольку вычисленные хэш-корни деревьев Меркла зависят от порядка включения транзакций в блок, транзакции в блокчейне полностью упорядочены по времени

Неизменяемости заголовков блоков можно достичь многими способами, включая доказательство работы (используемое, например, в биткойне), подтверждение доли (например, как в Nxt) или делегированное подтверждение доли (например, как в BitShares). Согласно протоколу доказательства работы, заголовок блока считается корректным тогда и только тогда, когда его хэш не превышает общего для всей сети значения (*целевой сложности*). Благодаря свойствам

хэш-функций не существует иного способа получить корректные блоки, кроме как перебирать значения полей заголовка блока, которые влияют на его хэш. Примерами таких полей являются *nonce* (специальное целочисленное поле), время создания блока и параметры coinbase-транзакции[1] (изменения в транзакции влекут за собой изменения хэш-корня блока, который является частью его заголовка). Альтернативный протокол обеспечения неизменности заголовков блоков — подтверждение доли. Подтверждение доли не предполагает интенсивных вычислений, в отличие от доказательства работы; с другой стороны, этот протокол может быть менее надежным, поскольку стоимость атак на систему, защищенную при помощи подтверждения доли, ниже [38].

Организация транзакций в блоки делает возможным эффективное доказательство того, что определенная транзакция входит в блокчейн; для этого используется *упрощенное подтверждение платежей* (англ. simplified payment verification, SPV) [2]. Такое доказательство состоит из списка заголовков блоков, начиная от первого блока и закачивая блоком, в который входит транзакция, а также самой транзакции и соответствующей *хэш-ветви* (рис. 2). Хэш-ветвь включает $O(\log N)$ хэшей, где N — количество транзакций в блоке, а ее структура такова, что она позволяет быстро подсчитать и проверить значение хэш-корня блока. Из свойств хэш-деревьев следует, что статистически невозможно подделать хэш-ветвь для транзакции, не входящей в блокчейн (при условии, что заголовки блоков защищены надлежащим образом). Клиенты, использующие упрощенное подтверждение транзакций, не обязаны хранить локально полную копию блокчейна (или даже иметь доступ ко всем данным блокчейна) для того, чтобы иметь возможность проверять корректность своих транзакций. В биткойне клиенты, использующие SPV, более распространены, чем узлы сети, хранящие все данные блокчейна. Существующие схемы упрощенного подтверждения платежей требуют ограниченного доверия к узлам сети, с которыми соединен клиент, и поэтому могут быть уязвимыми к атакам Сибилы. Подтверждение UTXO (включение в заголовок каждого блока хэш-дерева, построенного из текущего множества непотраченных выходов транзакций) предоставило бы возможность по-настоящему независимого упрощенного подтверждения платежей.

2.1. Блокчейн как распределенная система

Согласно CAP-теореме [40], не существует распределенной системы, которая одновременно обладает следующими характеристиками:

- **согласованность** – все узлы располагают одинаковым состоянием системы в каждый момент времени
- **доступность** – на каждый запрос к системе дается ответ
- **устойчивость к разделению** – система продолжает функционировать при отказе некоторых узлов.

[1] Coinbase-транзакция — первая транзакция блока, которая вознаграждает майнера блока созданными «из ниоткуда» монетами блокчейна

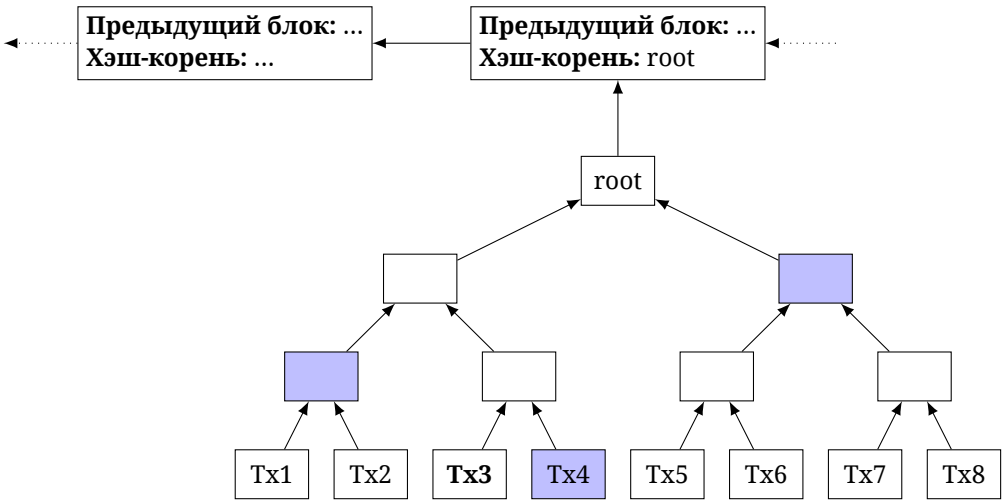

Рис. 2. Схема упрощенного подтверждения для транзакции **Tx3**. Хэши, включаемые в хэш-ветвь, обозначены заливкой

Блокчейн-системы являются доступными и устойчивыми к разделению, но не согласованными. В самом деле, доступность означает, что узлы системы могут принять две противоречащих друг другу транзакции. Например, Узел А может принять транзакцию о пересылке 1 000 рублей от Алисы Бобу, а Узел Б в то же время может принять транзакцию о пересылке 1 500 рублей от Алисы Стивену, в то время как баланс Алисы равен 2 000 рублей.

При использовании блокчейна, состояние системы, которое является общим для всех узлов – это сам блокчейн; новые транзакции изначально не принадлежат ни одному из блоков, т. е. являются *неподтвержденными*. Протокол блокчейна определяет правила по созданию новых блоков; когда новый блок создан, он распространяется по сети, и множество неподтвержденных транзакций на всех узлах системы меняется в соответствии с новым состоянием (в частности, противоречащие новому состоянию транзакции удаляются). Это правило гарантирует, что, в то время как неподтвержденные транзакции могут противоречить друг другу, транзакции в блокчейне всегда соответствуют протоколу его построения. Адекватный протокол минимизирует вероятность того, что несколько узлов одновременно добавят «свои» блоки в блокчейн. Например, если в системе существует ограниченное количество известных узлов, они могут создавать блоки по очереди с интервалом, который в несколько раз превышает интервал распространения блока по системе. Общедоступные блокчейны, т. е. блокчейны с открытым участием, которые позволяют всем узлам сети производить блоки, применяют более сложные алгоритмы из необходимости.

Распределенные блокчейн-системы предоставляют встроенный механизм восстановления от ошибок в базе данных. Рассмотрим следующий пример: есть 5 узлов системы, в двух из которых есть информация об определенной транзакции, а в трех остальных — нет. В общем случае транзакция либо было добавлена (например, в результате атаки) в базы данных двух узлов, либо была удалена из баз дынных оставшихся трех узлов; не существует причин, по которым один из этих вариантов был бы предпочтителен другому. Более того, узел не может сразу же

определить, что его база данных отличается от базы данных других узлов. В случае базы данных на основе блокчейна, испорченные версии базы данных можно определить немедленно; их можно исправить, пока в сети остается хотя бы один узел с корректной версией блокчейна.

В случае биткойна блокчейн решает проблему византийских генералов [41] с вероятностью близкой к единице, т. е. узлы системы достигают консенсусного состояния системы даже при наличии в сети злонамеренных узлов или произвольных отказов узлов системы [42]. Технология блокчейна не является единственным способом создать отказоустойчивую децентрализованную сеть; существуют и другие алгоритмы консенсуса в таких сетях, например, Paxos [43] и Raft [44]. В то же время блокчейны лучше подходят конкретно для обработки транзакций, так как они предоставляют встроенный протокол проверки корректности транзакций. По аналогии, блокчейны можно рассматривать как решение проблемы репликации с несколькими ведущими узлами (англ. multi-master replication), которая не решена удовлетворительно для других распределенных архитектур баз данных [45].

2.2. Доступ к данным блокчейна

Блокчейны можно разделить на группы в соответствии с доступом к данным.

Определение 1. *Открытый блокчейн* (англ. public blockchain) — это блокчейн, в котором не существует ограничений на чтение данных блоков (при этом данные могут быть зашифрованы) и ограничений на отсылку транзакций для включения в блокчейн.

Определение 2. *Закрытый блокчейн* (англ. private blockchain) — это блокчейн, в котором прямой доступ к данным и к отправке транзакций ограничен определенным узким кругом организаций.

Определение 3. *Общедоступный (инклюзивный) блокчейн* (англ. permissionless blockchain) — это блокчейн, в котором не существует ограничений на личность обработчиков транзакций (т. е., пользователей, которые могут создавать блоки транзакций).

Определение 4. *Эксклюзивный блокчейн* (англ. permissioned blockchain) — это блокчейн, в котором обработка транзакций осуществляется определенным списком субъектов с установленными личностями.

Отметим, что эксклюзивный блокчейн не обязан быть закрытым (табл. 1). В самом деле, существует несколько уровней доступа к данным блокчейна, например:

1. чтение транзакций из блокчейна, возможно, с определенными ограничениями (например, у клиента может быть доступ только к транзакциям, которые затрагивают его);
2. предложение транзакций для включения в блокчейн;
3. создание новых блоков транзакций и добавление блоков в блокчейн.

Таблица 1. Категории блокчейнов по доступу к обработке транзакций (общедоступные / эксклюзивные) и по доступу к данным (открытые / закрытые)

По доступу к транзакциям	По доступу к обработке транзакций	
	Эксклюзивные	Общедоступные
Открытые	Коммерческие протоколы покраски монет	Существующие криптовалюты (напр., биткойн)
Регулируемые	Прямой доступ к чтению / созданию транзакций для клиентов (ограничен; с использованием дружественных интерфейсов и приложений) и для регуляторов	Некоторые протоколы покраски (напр., Colored Coins Protocol), в которых возможность создания транзакций может быть ограничена
Закрытые	Доступ к данным ограничен обработчиками транзакций (т. е., непрозрачен для клиентов); преимущества блокчейнов частично теряются	Не применим

В то время как третий уровень доступа в эксклюзивных блокчейнах предоставляется ограниченному кругу учреждений (например, банкам, которые совместно управляют блокчейном, или лицензированным обработчикам транзакций), доступ к блокчейну не обязан ограничиваться этими учреждениями. Напротив, финансовые учреждения, управляющие эксклюзивным блокчейном, теоретически могут

- предоставить доступ на чтение транзакций и заголовков блоков (возможно, ограниченный) для клиентов с целью обеспечения технологичного, прозрачного и надежного способа проверки сохранности средств клиентов;
- предоставить полный доступ на чтение данных блокчейна для регулирующих учреждений для соответствия законам;
- предоставить всем лицам и учреждениям к доступом к данным четкое и исчерпывающее описание протокола блокчейна, который включает в себя объяснение возможных взаимодействий с данными блокчейна.

Эти шаги могут облегчить независимый аудит и проверку целостности данных блокчейна, например, регулирующими учреждениями. В идеальном случае, протоколы блокчейнов и способ доступа к данным должны быть стандартизированы, что облегчит взаимодействие с клиентами и интеграцию блокчейнов в единую экосистему.

Если база данных блокчейна полностью непрозрачна для клиентов (т. е. клиенты не имеют доступ к данным блокчейна), то безопасность блокчейна уменьшается. В то время как система остается защищенной против атак на саму базу данных, взаимодействие с клиентами становится уязвимым, например, для MitM-атак. Поскольку встроенный протокол авторизa-

ции транзакций является одним из ключевых моментов блокчейн-технологии, его игнорирование в пользу централизованных решений может отрицательно сказаться на защищенности системы. Кроме того, так как транзакции в этом случае доступны ограниченному числу компьютеров, возникают риски вмешательства человеческого фактора в функционирование этих компьютеров, причем клиенты не смогут выявить это вмешательство. Таким образом, непрозрачный дизайн блокчейнов по своей сути подрывает два ключевых аспекта блокчейн-технологии:

- децентрализацию — отсутствие единых точек отказа;
- недоверчивость (англ. trustlessness) — опора на алгоритмически заложенные правила обработки транзакций без вмешательства человека.

В целом, любое взаимодействие с данными блокчейна в обход его протокола вводит в систему уязвимости. Согласно словам Nick Szabo [3]: «Чтобы устранить уязвимости, банкам нужно устранить контроль со стороны конкретных людей и людей с правами администрирования. У банков [...] нет выбора, если они хотят получить в свое распоряжение армию независимых компьютеров, которые постоянно четко и безопасно проверяют работу друг друга» (перевод наш). Мы проведем более полное сравнение закрытых, эксклюзивных и общедоступных блокчейнов во второй части работы.

Эксклюзивная природа блокчейнов для коммерческих приложений может быть необходимым компромиссом в среднесрочной перспективе из-за законов и других факторов. В то же время, доступ на чтение данных блокчейна совместно с открытым протоколом позволяют устранить большинство уязвимостей, связанных с архитектурой закрытых блокчейнов, а также могут быть более привлекательны для клиентов учреждений, обрабатывающих транзакции. Как свидетельствует биткойн, программное обеспечение, работающее на основе упрощенного подтверждения платежей, может предоставить прямой доступ к данным блокчейна, который в одно и то же время безопасен и не требует много ресурсов.

3. Эксклюзивные блокчейны

Эксклюзивные блокчейны привлекательны для учреждений, работающих с реестрами и финансовыми системами учета, поскольку большинство систем законодательства предусматривает необходимость регистрации обработчиков транзакций. Эти блокчейны могут сформировать более контролируемую и прогнозируемую среду, чем общедоступные блокчейны. В отличие от криптовалют, в эксклюзивных блокчейнах обычно не используются встроенные монеты. Встроенные монеты необходимы в криптовалютах для предоставления награды за обработку транзакций; в эксклюзивных блокчейнах обработчики транзакций могут вознаграждаться другими способами.

Создание блоков в эксклюзивном блокчейне в простейшем случае не требует вычислений, связанных с алгоритмами доказательства работы. В самом деле, рассмотрим следующий

протокол создания блоков, похожий на делегированное подтверждение доли, используемое в BitShares [46]:

Ротация майнеров

- Существует фиксированное количество обработчиков транзакций N. Каждый обработчик владеет пару из секретного и открытого ключа; открытые ключи всех операторов блокчейна, а также их личности известны. Создатель каждого блока определяется по обязательной цифровой подписи блока, являющейся частью заголовка блока.
- Операторы создают блоки по очереди через фиксированные интервалы времени (например, 10 секунд). Интервал достаточно большой, чтобы обеспечить распространение блока по сети и его верификацию всеми узлами до создания нового блока. Порядок создания блоков может быть фиксирован (например, в соответствии с упорядочением открытых ключей операторов), или случайным образом перемешиваться после каждого полного цикла из N блоков.
- Если оператор по какой-либо причине не может создать блок в отведенный ему интервал времени, он пропускает этот раунд. Если такое поведение или другой вид злонамеренного поведения (например, создание некорректных блоков) повторяется, оно подвергается расследованию.

Чтобы обратить транзакцию с более чем N подтверждениями, атакующий должен получить доступ ко всем секретным ключам майнеров (ср. с атакой 51% в биткойне). Таким образом, если обработчики транзакций являются единственными потребителями данных блокчейна, приведенный выше протокол теоретически более надежен, чем доказательство работы.

Однако если доступ к данным блокчейна есть у третьих сторон, ситуация меняется. Поскольку предложенная схема создания блоков напоминает консенсус на основе подтверждения доли, она страдает от недостатка, аналогичного главной проблеме подтверждения доли — «ничего на кону» (англ. nothing at stake). Наблюдатель, имеющий доступ на чтение данных блокчейна, не может быть уверен, что блокчейн, который он имеет возможность наблюдать, в действительности используется между операторами. Поскольку создание блоков в предложенной схеме (т. е. их цифровые подписи) является тривиальной операцией с точки зрения вычислительной сложности, сговорившиеся майнеры могут создать произвольное количество копий блокчейна для разных целей: внутреннего ведения учета, показа регуляторам, и так далее. Проблема смягчается при условии, что доступ к заголовкам блоков не ограничен; однако, разбирающихся в технике клиентов и регуляторов все равно будет сложно убедить, что блокчейн неуязвим к атакам, так как операторы имеют возможность поменять произвольную часть блокчейна в любой момент времени. Таким образом, приведенный выше протокол консенсуса безопасен только в случае, если не существует вероятности сговора между опера-

торами блокчейна (например, если операторы представляют собой идеальные стороны с противоречащими интересами). Доказательство работы позволяет удостовериться в отсутствии сговора *алгоритмически*, т. е. в соответствии с общим духом блокчейн-технологии.

Второе рассуждение, делающее доказательство работы возможным алгоритмом консенсуса в эксклюзивных блокчейнах, заключается в следующем. В приведенном выше протоколе, усилия, которые надо затратить на обращение транзакции, не зависят от количества подтверждений; транзакции возрастом 1 час и 1 год требуют от атакующего знания тех же N секретных ключей. При использовании подтверждения работы, чем старее транзакция, тем больше вычислений требуется для ее обращения; транзакция возрастом в 1 год потребует от атакующего около 1 года непрерывных вычислений при условии, что хэшрейт атакующего в два раза превышает хэшрейт честных майнеров. В самом деле, атакующему надо догнать цепь, создаваемую честными майнерами с начальным отставанием в 1 год вычислений. Интуитивно, атакующий в среднем создает блоки в два раза быстрее честных майнеров; следовательно, если обозначить время, необходимое, чтобы перегнать честный блокчейн, как t,

$$t + 1 \text{ год} = 2t \;\Rightarrow\; t = 1 \text{ год}.$$

Более точную оценку можно произвести при помощи распределения Скеллама [47]. Пусть t_0 — ожидаемый интервал между блоками в честной сети; атакующий может поддерживать генерацию блоков с ожидаемым интервалом $t_0/2$. Количество блоков, созданное честными майнерами за период времени $t - n_h(t)$, дискретная случайная величина, имеющая распределение Пуассона со средним t/t_0. Аналогично, число блоков, созданных атакующим $n_a(t)$ — случайная величина, имеющая распределение Пуассона со средним $2t/t_0$. Разность $n_a(t) - n_h(t)$ имеет распределение Скеллама; таким образом, вероятность того, что успешная атака состоится за время t, равна

$$P\{\text{Skellam}(2t/t_0, t/t_0) > N\},$$

где N — начальное отставание злоумышленника, выраженное в количестве блоков. Например, если $t_0 = 10$ минут, $N = 1 \text{ год}/t_0 = 52\,560$ блоков, то вероятность успешной атаки за один год составляет приблизительно 49,9%. Для атаки с вероятностью успеха 99%, она должна длиться немного дольше — приблизительно 372 дня.

Протокол с ротацией майнеров, описанный выше, может быть адаптирован для доказательства работы:

Ротация майнеров с доказательством работы

- По-прежнему существует фиксированное количество майнеров с известными личностями, которые показываются при помощи цифровых подписей в заголовках блоков. Майнинг и обработка транзакций могут осуществляться различными учреждениями; в случае если майнинг делегирован доверенным компаниям, заголовки блоков следует подписывать как майнерам, так и обработчикам транзакций.

- Майнеры создают блоки, удовлетворяющие доказательству работы, похожему на использующееся в биткойне.
- Выполняется условие принудительного чередования майнеров [48]: майнер не может создать более rW блоков из произвольных W подряд идущих блоков, где W — целочисленное окно (например, $W = 10$), а r — параметр разнообразия (например, $r = 0.4$, что означает, что ни один майнер не может создать более 40% блоковв долгосрочной перспективе).

Условие чередования майнеров несколько снижает хэшрейт, обеспечивающий защиту системы. Однако при адекватном выборе параметров W и r эту потерю можно минимизировать. Например, если $W = 10, r = 0.4$, и существует пять майнеров, каждый с доле хэшрейта $p = 20\%$, то потеря хэшрейта из-за принудительного чередования майнеров равна

$$\sum_{i=\lfloor rW \rfloor+1}^{W} \binom{W}{i} p^i (1-p)^{W-i} = \sum_{i=5}^{10} \binom{10}{i} 0.2^i \cdot 0.8^{10-i} \approx 3.3\%.$$

Предложенный протокол делает невозможным возможность создания операторами блокчейна неограниченного количества альтернативных версий блокчейна. Поддержка нескольких версий блокчейна при помощи доказательства работы стоит ресурсов: электричества и хэширующего оборудования. Хэшрейт, затраченный на создание блокчейна и хэшрейт каждого майнера по отдельности можно с удовлетворительной точностью оценить исходя из целевой сложности сети и периодов между созданными блоками; аудитор может сравнить эти числа с объемом хэширующего оборудования, находящимся в распоряжении операторов блокчейна, и сделать соответствующие выводы.

Главный недостаток ротации майнеров с доказательством работы — экспоненциальное распределение периодов между соседними блоками транзакций. Ожидаемый период времени между блоками можно сократить до минуты или меньше. Проблему с возможным ненамеренным расщеплением цепочки блоков из-за того, что два майнера создали блок почти одновременно, можно решить при помощи обратимых таблиц Блума (англ. invertible Bloom lookup tables) [49].

Для сокращения времени обработки транзакций в эксклюзивном блокчейне можно ввести дополнительный механизм синхронизации неподтвержденных транзакций (например, при помощи двухэтапного протокола внесения изменений [50]). Использование подобного механизма практически неизбежно в случае, если система должна принимать решение о включении / исключении транзакции в блокчейн быстрее, чем минимальный возможный интервал между блоками; пример — блокчейн для трейдинга. Блокчейн по-прежнему затребован в таких случаях как неизменяемое хранилище полной истории транзакций. Использование дополнительного протокола консенсуса для неподтвержденных транзакций также решает большинство проблем, связанных с встречающимися длинными интервалами между блоками при использовании доказательства работы.

Поскольку учреждениям, управляющим эксклюзивным блокчейном с доказательством работы, не надо постоянно повышать хэшрейт для максимизации прибыли (ср. с биткойном и

другими криптовалютами), хэшрейт эксклюзивного блокчейна вряд ли должен досигать уровня биткойна (порядка 10^{17} хэшей в секунду во время написания статьи). С другой стороны, хэшрейт должен быть достаточно высоким для того, чтобы сделать атаки на систему извне маловероятными; этой цели можно достичь, если уровень хэшрейта делает необходимым использование специализированного оборудования — ASIC-ов (англ. application-specific integrated circuits), дизайн которых отличается от дизайнов, использующихся в майнинге существующих криптовалют. Поскольку количество производителей такого оборудования ограничено, вероятность скрытной атаки в этом случае будет достаточно низкой (отметим, что кроме производства оборудования, злоумышленнику также придется достать все секретные ключи майнеров на эксклюзивном блокчейне).

Рассмотрим оценку хэшрейта, основанную на балансе между расходами на его поддержание и доходами от внедрения блокчейн-технологии, безопасность которой обеспечивается доказательством работы. Предположим, что расходы на функционирование оборудования связаны с потреблением электричества. Поскольку

- энергоэффективность современного хэширующего оборудования составляет порядка 0,1 кВт / (ТХэш / с)[2] [51],
- цена электричества составляет порядка 0,1 $ за кВт · час [52],

расходы на работу оборудования приблизительно равны $0{,}01H$ $ в час, где H — хэшрейт, измеренный в ТХэш / с. Стоимость оборудования сейчас составляет около $400 на ТХэш / с [53]; таким образом, если принять период амортизации равным 3 годам, то затраты на амортизацию равны

$$\$400H/(3 \cdot 365 \cdot 24) \approx \$0.015H \text{ в час.}$$

Таким образом, общие затраты составляют порядка 0,03 $ на 1 ТХэш / с в час, или

$$\$0.03H \cdot 24 \cdot 365 = \$262.8H \text{ в год.}$$

Итак, затраты на уровне 10 млн. долларов в год на обеспечение безопасности при помощи доказательства работы (что достаточно мало про сравнению с потенциальной прибылью от внедрения блокчейнов, которая оценивается в несколько миллиардов долларов в год [54]) соответствуют хэшрейту около 38 петахэшей в секунду, или немного меньше 10% от общего хэшрейта сети биткойна.

Отметим, что при использовании объединенного майнинга все эксклюзивные блокчейны, обслуживаемые одним учреждением, могут защищаться одним и тем же оборудованием, существенно сокращая затраты на безопасность. Более того, доказательство работы может частично или полностью обеспечиваться существующими открытыми блокчейнами как описано в последующих разделах; атаки путем сговора операторов остаются нереализуемыми независимо от того, каким образом доказательство работы задействовано в безопасности блокчейна.

[2] 1 ТХэш / с $= 10^{12}$ хэшей в секунду

3.1. Объединенный майнинг

Объединенный майнинг (англ. merged mining) — технология, позволяющая использовать одно и то же оборудование для доказательства работы для обеспечения безопасности более чем одного блокчейна [55]. Например, объединенный майнинг поддерживается неймкойном (Namecoin) [56]; майнеры могут биткойновское доказательство работы вместо внутреннего для неймкойна для создания блоков. Однако, поскольку протокол биткойна сам не поддерживает концепцию объединенного майнинга, предоставить доказательство работы другого блокчейна для биткойновских блоков невозможно.

Объединенный майнинг и привязка блокчейна, которая рассматривается в следующем разделе, оба используют понятия транзакций-свидетельств.

Определение 5. *Транзакция-свидетельство* на цепи А (поддерживающий блокчейн), которая свидетельствует блок на цепи Б (главный блокчейн) — это транзакция, корректная с точки зрения протокола цепи А, которая содержит уникальный идентификатор этого блока (например, 32-байтный хэш заголовка блока) как часть данных транзакции.

В случае когда в качестве поддерживающего блокчейна используется биткойн, хэш заголовка блока может быть включен в транзакцию при помощи инструкции языка сценариев **RETURN** или при помощи других технологий, используемых в протоколах покраски монет.

Рассмотрим принципы объединенного майнинга на примере пары биткойн / неймкойн:

1. Майнер, желающий создавать блоки одновременно для биткойна и неймкойна обрабатывает транзакции для обеих этих систем. Собрав достаточно транзакций в неймкойне, майнер создает шаблон блока, заполняет его заголовок и вычисляет хэш блока. Полученный блок не является корректным с точки зрения протокола неймкойна, поскольку он не удовлетворяет условию доказательства работы.
2. Майнер добавляет транзакцию-свидетельство, т. е. транзакцию, которая включает вычисленный хэш неймкойновского блока, во множество неподтвержденных биткойновских транзакций. С точки зрения протокола биткойна, это обыкновенная транзакция.
3. Майнер собирает биткойновский блок, содержащий транзакцию, созданную на предыдущем шаге, и пытается решить блок, чтобы он соответствовал целевой сложности для биткойна или неймкойна.
4. Если майнер находит корректный биткойновский блок, он публикуется в сеть биткойна.
5. Если же майнер находит заголовок биткойновского блока, удовлетворяющий целевой сложности для неймкойна, майнер создает и публикует новый блок в неймкойне, основанный на ранее созданном шаблоне. Новый блок дополнительно включает в себя заголовок биткойновского блока, транзакцию-свидетельство и хэш-ветвь, которая соответствует этой транзакции.

Объединенный майнинг может использоваться для принятия биткойновского доказательства работы в эксклюзивных или частных блокчейнах (рис. 3). Отметим, что майнер не обязан обрабатывать транзакции на блокчейне, который поддерживает объединенный майнинг; ему досататочно просто знать шаблон заголовка блока для этой цепи, с которым надо работать. Например, эксклюзивный блокчейн может принимать протокол доказательства работы на основе хэш-функции SHA-256 [57], используемой в биткойне. В этом случае безопасность блокчейна может достигаться путем сотрудничества с майнинг-пулами в биткойне: операторы эксклюзивных блокчейнов предоставляют шаблоны заголовков блоков по защищенным соединениям и получают в ответ готовые заголовки блоков, защищенные доказательством работы.

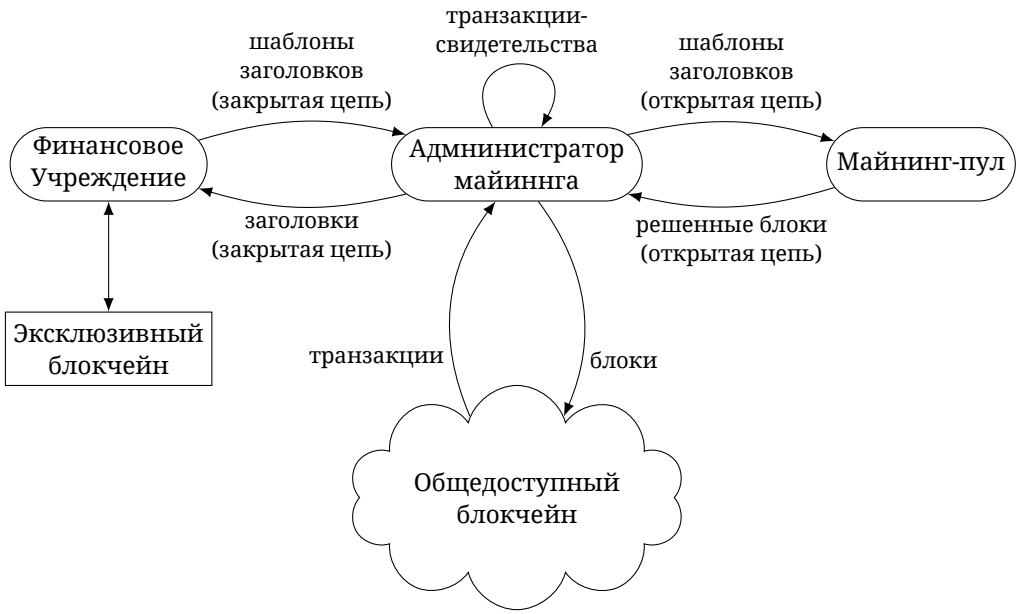

Рис. 3. Объединенный майнинг для эксклюзивного блокчейна и общедоступного блокчейна (например, биткойна)

Объединенный майнинг также можно использовать для агрегации большого количества эксклюзивных блокчейнов (рис. 4). В этом случае локальные узлы сети, работающие с блокчейнами одного учреждения, предоставляют шаблоны заголовков блоков в специализированный центр обработки. Центр строит специальную *метацепь*, состоящую из из присланных шаблонов заголовков блоков, которые полностью заменяют транзакции (т. е., единственная цель метацепи состоит в обеспечении защиты других блокчейнов; в метацепи отсутствуют встроенные монеты и она не предназначена для обмена активами). Когда обнаруживается новый блок метацепи, он рассылается всем привязанным эксклюзивным блокчейнам. Таким образом, все связанные блокчейны имеют безопасность, определяемую хэшрейтом метачейна, который может быть установлен на достаточно высоком уровне, отвечающем размеру транзакций на всех блокчейнах. Более того,

- предлагаемый подход является масштабируемым, так как он разделяет безопасность и

обработку транзакций и может быть адаптирован для обработки сотен эксклюзивных блокчейнов;

- поддержка метацепи может быть предоставлена доверенному поставщику безопасности без риска разглашения конфиденциальных деталей транзакций.

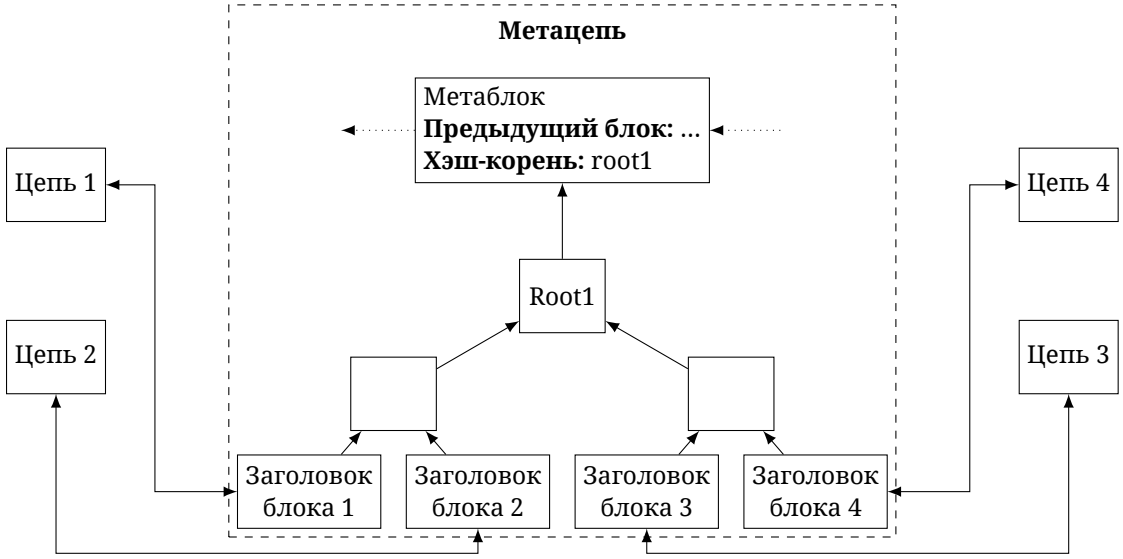

Рис. 4. Объединенный майнинг, обеспечивающий защиту четырех эксклюзивных блокчейнов при помощи единой метацепи

3.2. Привязка блокчейнов

Привязка блокчейна (англ. blockchain anchoring) — технология, напоминающая объединенный майнинг (термин используется, например, в исследовательской статье Factom [58]). В соответствии с технологией, операторы эксклюзивного блокчейна время от времени отправляют хэши заголовков блоков для включения в поддерживающий общедоступный блокчейн в виде транзакций-свидетельств; включенная в поддерживающий блокчейн информация может быть проверена пользователями эксклюзивного блокчейна за счет упрощенных доказательств платежа, аналогичных используемым в объединенном майнинге (рис. 5). Привязка предоставляет дополнительные гарантии неизменности блокчейна, но основной источник безопасности заголовков блоков по-прежнему находится внутри эксклюзивного блокчейна (например, используется ротация операторов блокчейна, описанная выше). Напротив, при объединенном майнинге использование поддерживающего блокчейна — основной источник неизменяемости; большинство блоков в цепи, поддерживающей объединенный майнинг, может быть защищено с помощью внешнего доказательства работы, как это происходит в неймкойне. По сравнению с объединенным майнингом, у привязки блокчейна есть преимущества:

- Привязка может использоваться для блокчейнов, не использующих доказательство работы как внутренний механизм достижения консенсуса; например, привязка может ис-

пользоваться совместно с протоколом ротации операторов блокчейна.

- В отличие от объединенного майнинга, привязка не требует взаимодействия с майнерами на общедоступном блокчейне. В то время как объединенный майнинг теоретически не затратен для майнеров, его широкое внедрение может тормозиться различными факторами. В случае привязки, сотрудничество между операторами эксклюзивного блокчейна и майнерами на поддерживающем блокчейне носит необязательный характер.
- Привязка использует полный хэшрейт поддерживающей цепи, в то время как объединенный майнинг чаще всего использует сравнительно малую долю этого хэшрейта, равную доле майнеров, которые поддерживают объединенный майнинг.

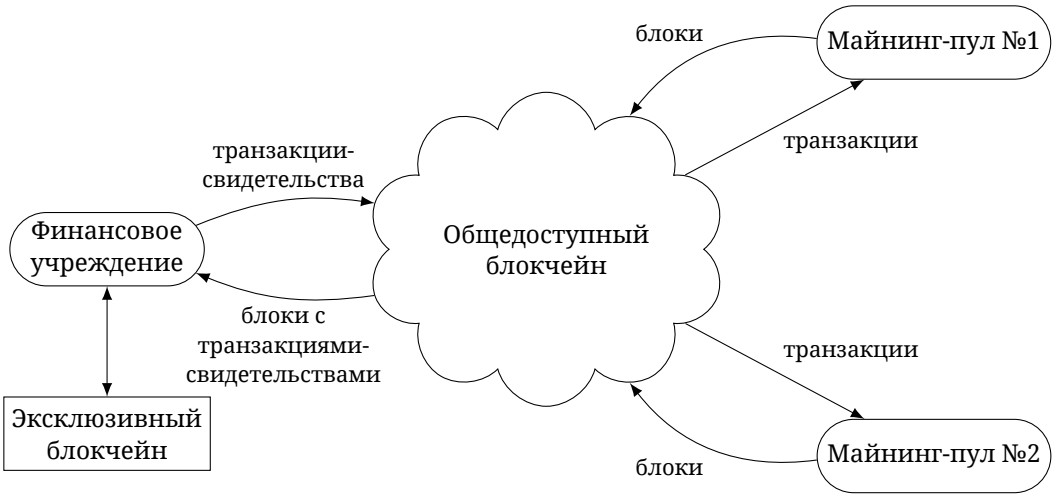

Рис. 5. Привязка эксклюзивного блокчейна при помощи поддерживающего общедоступного блокчейна (например, биткойна). В отличие от объединенного майнинга, привязка не требует сотрудничества с майнинг-пулами

В случае автоматизации, протокол привязки должен учитывать то, что блоки на поддерживающей цепи чаще всего создаются с нерегулярными интервалами, значительно превышающими интервалы между блоками на эксклюзивном блокчейне. По этой причине, протокол привязки может указывать, что заголовок блока в эксклюзивной цепи может (но не обязан) включать SPV-доказательство транзакции-свидетельства одного из предыдущих блоков эксклюзивного блокчейна. Например, если блоки в эксклюзивной цепи создаются с интервалом в 10 секунд:

1. Транзакцию-свидетельство можно отсылать для одного из 180 блоков (т. е. каждые полчаса).
2. Транзакция-свидетельство должна приобрести необходимое количество подтверждений (например, 4 или 6), чтобы реорганизация блокчейна, которая исключила бы свидетельство из вспомогательного блокчейна стала статистически маловероятным событием.

3. После этого SPV-доказательство, соответствующее свидетельству, можно включить в заголовок блока эксклюзивной цепи.

В случае биткойна, весь процесс может занять пару часов. Вероятность того, что транзакция-свидетельство обретет необходимое количество подтверждений, может быть подсчитано при помощи распределения Пуассона:

$$P_c(C) \stackrel{\text{def}}{=} P\{\langle\text{подтвержений за 2 часа}\rangle \geqslant C\} = 1 - \sum_{k=0}^{C-1} \frac{\lambda^k e^{-\lambda}}{k!}, \tag{1}$$

где $\lambda = 12$ — ожидаемое число подтверждений за 2 часа. Из уравнения (1) получается $P_c(4) \approx 99.8\%$ и $P_c(6) \approx 98.0\%$.

Для атаки на цепь, защищенной привязкой к открытому блокчейну, злоумышленнику требуется преодолеть механизмы консенсуса как для эксклюзивного блокчейна, так и для поддерживающей цепи. Например, если эксклюзивный блокчейн защищен ротацией операторов и привязан к биткойновскому блокчейну, злоумышленнику необходимо заполучить все секретные ключи на первом блокчейне и взять под контроль 50% хэшрейта биткойновской сети. Таким образом, привязка представляет собой эффективный способ диверсификации безопасности блокчейна.

4. Выводы

Решения на основе блокчейнов образуют безопасный и естественно децентрализованный каркас для обработки транзакций. Одно из главных преимуществ блокчейнов по сравнению с другими моделями распределенных баз данных — интеграция обработки данных, обеспечения корректности и безопасности в единый протокол, реализуемый алгоритмически и минимизирующий человеческий фактор. Из-за юридических и технических причин, учреждения, в которых задействованы финансовые системы учета или реестры, могут быть заинтересованы в использовании блокчейнов с ограниченным доступом к обработке транзакций (эксклюзивных), по крайней мере, в краткосрочной перспективе. Однако, эксклюзивность блокчейна не обязательно означает его закрытость; два ключевых элемента блокчейн-технологии – децентрализация и недоверчивость – раскрываются в полной мере, только когда протокол блокчейна и его содержимое предоставлены конечным пользователям.

Эксклюзивные блокчейны могут стать базой для блокчейн-инноваций в сервисах, использующих реестры или финансовые системы учета. Хотя эксклюзивные блокчейны могут не использовать доказательство работы, этот протокол консенсуса может по-прежнему использоваться как дополнительный уровень защиты, для упрощения аудита и увеличения привлекательности системы для конечных потребителей, в особенности если данные блокчейна частично или полностью открыты. В блокчейнах, использующих доказательство работы, объединенный майнинг может использоваться как эффективный инструмент для сокращения

затрат на оборудование или для передачи майнинга третьим сторонам без уменьшения защищенности системы. Привязка к блокчейнам решает схожую проблему диверсификации безопасности блокчейна и может использоваться в блокчейнах, которые не используют внутреннее доказательство работы. Оба подхода не являются взаимно исключающими и могут использоваться вместе для обеспечения подходящего уровня защищенности в среде с известными обработчиками транзакций.

Биткойн может использоваться вместе с эксклюзивными блокчейнами как поддерживающая цепь в объединенном майнинге или для привязки благодаря следующим факторам:

- сравнительно малое количество майнинг-пулов с известными личностями, что позволяет использовать их в качестве известных обработчиков транзакций, генерируемых учреждениями;
- высокий уровень безопасности, обеспечиваемый хэшрейтом сети.

Список литературы

[1] *Matt Levine*. Blockchain for banks probably can't hurt // Bloomberg View. — 2015.
URL: http://www.bloombergview.com/articles/2015-09-01/blockchain-for-banks-probably-can-t-hurt

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

[3] *Ian Allison* Nick Szabo: If banks want benefits of blockchains they must go permissionless // International Business Times. — 2015.
URL: http://www.ibtimes.co.uk/nick-szabo-if-banks-want-benefits-blockchains-they-must-go-permissionless-1518874

[4] *Leon Pick*. Estonia's LHV Bank Testing Colored Coins-Based 'Cuber' // Finance Magnates. — 2015.
URL: http://www.financemagnates.com/cryptocurrency/news/estonias-lhv-bank-testing-colored-coins-based-cuber/

[5] Nasdaq launches enterprise-wide blockchain technology initiative. — 2015.
URL: http://www.nasdaqomx.com/newsroom/pressreleases/pressrelease?messageId=1361706&displayLanguage=en

[6] Nasdaq and Chain to partner on blockchain technology initiative. — 2015.
URL: http://www.nasdaqomx.com/newsroom/pressreleases/pressrelease?messageId=1373282&displayLanguage=en

[7] *Ian Allison*. The French bitcoin revolution: BNP Paribas testing crypto on its currency funds // International Business Times. — 2015.
URL: http://www.ibtimes.co.uk/french-bitcoin-revolution-bnp-paribas-plans-add-crypto-its-currency-funds-1512360

[8] *Grace Caffyn*. Barclays trials Bitcoin tech with pilot program // CoinDesk. — 2015.
URL: http://www.coindesk.com/barclays-trials-bitcoin-tech-with-pilot-program/

[9] *Joon Ian Wong*. Goldman Sachs report says Bitcoin could shape 'future of finance' // CoinDesk. — 2015.
URL: http://www.coindesk.com/goldman-sachs-report-says-bitcoin-could-shape-future-of-finance/

[10] *Emily Spaven*. Circle raises $50 million with Goldman Sachs support // CoinDesk. — 2015.
URL: http://www.coindesk.com/circle-raises-50-million-with-goldman-sachs-support/

[11] *Pete Rizzo*. UBS: Banks could 'absorb the benefits' of Bitcoin // CoinDesk. — 2014.
URL: http://www.coindesk.com/swiss-bank-ubs-banks-absorb-benefits-bitcoin/

[12] *Stan Higgins*. US banks announce Ripple protocol integration // CoinDesk. — 2014.
URL: http://www.coindesk.com/us-banks-announce-ripple-protocol-integration/

[13] *Jon Southurst*. Australia's Commonwealth Bank latest to experiment with Ripple // CoinDesk. — 2015.
URL: http://www.coindesk.com/australia-commonwealth-bank-ripple-experiment/

[14] *Grace Caffyn*. Australian banks Westpac and ANZ experiment with Ripple // CoinDesk. — 2015.
URL: http://www.coindesk.com/australian-banks-westpac-and-anz-experiment-with-ripple/

[15] *Ian Allison*. UBS reveals its interest in Sidechains as well as Ethereum // International Business Times. — 2015.
URL: http://www.ibtimes.co.uk/ubs-reveals-its-interest-sidechains-well-ethereum-1519706

[16] *Diana Ngo*. ING, other major Dutch banks take interest in blockchain tech // CoinTelegraph. — 2014.
URL: http://cointelegraph.com/news/113033/ing-other-major-dutch-banks-take-interest-in-blockchain-tech

[17] *Ian Allison*. Codename Citicoin: Banking giant built three internal blockchains to test Bitcoin technology // International Business Times. — 2015.
URL: http://www.ibtimes.co.uk/codename-citicoin-banking-giant-built-three-internal-blockchains-test-bitcoin-technology-1508759

[18] *Liyan Chen*. 2015 Global 2000: The world's largest banks // Forbes. — 2015.
URL: http://www.forbes.com/sites/liyanchen/2015/05/06/2015-global-2000-the-worlds-largest-banks/

[19] *Oscar Williams-Grut*. Santander is experimenting with bitcoin and close to investing in a blockchain startup // Business Insider. — 2015.
URL: http://www.businessinsider.com/santander-has-20-25-use-cases-for-bitcoins-blockchain-technology-everyday-banking-2015-6

[20] *Deutsche Bank Group*. Re: Deutsche Bank's response to ESMA's call for evidence on virtual currencies and distributed ledgers. — 2015.
URL: http://scribd.com/doc/273151640/Deutsche-Bank-Letter

[21] *Ravi Menon*. A smart financial centre (keynote address at Global Technology Law Conference 2015). — 2015.
URL: http://www.mas.gov.sg/news-and-publications/speeches-and-monetary-policy-statements/speeches/2015/a-smart-financial-centre.aspx

[22] *Stan Higgins*. IBM reveals proof of concept for blockchain-powered Internet of Things // CoinDesk. — 2015.
URL: http://www.coindesk.com/ibm-reveals-proof-concept-blockchain-powered-internet-things/

[23] *Stan Higgins*. IBM developing new blockchain smart contract system // CoinDesk. — 2015.
URL: http://www.coindesk.com/ibm-developing-new-blockchain-smart-contract-system/

[24] *Global Agenda Council on the Future of Software & Society*. Deep shift: technology tipping points and societal impact. — 2015.
URL: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

[25] *Robleh Ali, John Barrdear, Roger Clews, James Southgate*. Innovations in payment technologies and the emergence of digital currencies. — 2014.
URL: http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin1.pdf

[26] *Edward Robinson, Matthew Leising*. Blythe Masters tells banks the blockchain changes everything // Bloomberg Business. — 2015.
URL: http://www.bloomberg.com/news/features/2015-09-01/blythe-masters-tells-banks-the-blockchain-changes-everything

[27] *Anju Patwardhan*. Blockchain – a disruptive force for good? // LinkedIn Pulse. — 2015.
URL: https://www.linkedin.com/pulse/blockchain-disruptive-force-good-anju-patwardhan

[28] *Emily Spaven*. Barclays data officer praises blockchain tech at SWIFT forum // CoinDesk. — 2015.
URL: http://www.coindesk.com/barclays-data-officer-praises-blockchain-tech-at-swift-forum/

[29] *Reid Hoffman*. Why the block chain matters // Wired. — 2015.
URL: http://www.wired.co.uk/magazine/archive/2015/06/features/bitcoin-reid-hoffman

[30] *Richard Gendal Brown*. Blockchain is where banks have the most obvious opportunity. But you ignore Bitcoin at your peril. — 2015.
URL: http://gendal.me/2015/05/12/blockchain-is-where-banks-have-the-most-obvious-opportunity-but-you-ignore-bitcoin-at-your-peril/

[31] *Tim Swanson*. Permissioned distributed ledgers. — 2015.
URL: http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf

[32] Hyperledger summary. — 2015.
URL: http://d1iohkh6wgqugq.cloudfront.net/static/resources/hyperledger-summary.pdf

[33] Chain raises $30 million from financial industry leaders. — 2015.
URL: http://www.prnewswire.com/news-releases/chain-raises-30-million-from-financial-industry-leaders-300140260.html

[34] *Justin OConnell*. Nine major banks partner on block chain initiative // CCN: Financial Bitcoin & Cryptocurrency News. — 2015.
URL: https://www.cryptocoinsnews.com/nine-major-banks-partner-block-chain-initiative/

[35] Turing completeness // English Wikipedia.
URL: https://en.wikipedia.org/wiki/Turing_completeness

[36] Public-key cryptography // English Wikipedia.
URL: https://en.wikipedia.org/wiki/Public-key_cryptography

[37] *Ralph Merkle*. A digital signature based on a conventional encryption function // Advances in Cryptology – CRYPTO '87. — 1988. — № 293. — pp. 369–378.
URL: http://link.springer.com/chapter/10.1007%2F3-540-48184-2_32

[38] *BitFury Group*. Proof of stake versus proof of work. — 2015.
URL: http://bitfury.com/content/4-white-papers-research/2-proof-of-stake-vs-proof-of-work/pos-vs-pow-1.0.2.pdf

[39] *Andrew Miller*. Storing UTXOs in a balanced Merkle tree (zero-trust nodes with $O(1)$-storage) // BitcoinTalk Forums. — 2012.
URL: https://bitcointalk.org/index.php?topic=101734.0

[40] *Seth Gilbert, Nancy Lynch*. Brewer's conjecture and the feasibility of consistent, available, partition-tolerant web services // ACM SIGACT News. — 2002. — № 33 (2). — pp. 51–59.

[41] *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

[42] *Andrew Miller, Joseph J. LaViola, Jr.* Anonymous Byzantine consensus from moderately-hard puzzles: a model for Bitcoin.
URL: https://socrates1024.s3.amazonaws.com/consensus.pdf

[43] *Leslie Lamport*. The part-time parliament // ACM Transactions on Computer Systems. — 1998. — № 16 (2). — pp. 133–169.
URL: http://research.microsoft.com/en-us/um/people/lamport/pubs/lamport-paxos.pdf

[44] *Diego Ongaro, John Ousterhout* (2013). In search of understandable consensus algorithm
URL: https://ramcloud.stanford.edu/wiki/download/attachments/11370504/raft.pdf

[45] *Gideon Greenspan*. Ending the bitcoin vs blockchain debate // MultiChain blog. — 2015.
URL: http://www.multichain.com/blog/2015/07/bitcoin-vs-blockchain-debate/

[46] *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

[47] Skellam distribution // English Wikipedia
URL: https://en.wikipedia.org/wiki/Skellam_distribution

[48] *Gideon Greenspan*. MultiChain private blockchain. — 2014.
URL: http://www.multichain.com/download/MultiChain-White-Paper.pdf

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

[50] Two-phase commit protocol // English Wikipedia
URL: https://en.wikipedia.org/wiki/Two-phase_commit_protocol

[51] *Pete Rizzo*. BitFury raises $20 million to power new ASIC chip development // CoinDesk. — 2014.
URL: http://www.coindesk.com/bitfury-raises-20-million-asic-development-mining-output/

[52] Average price of electricity to ultimate customers by end-use sector, July 2015 and 2014 // U.S. Energy Information Administration
URL: http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_06_a

[53] Antminer S7 batch 1 // Bitmain
URL: https://bitmaintech.com/productDetail.htm?pid=000201508270840214710HYdwd9D06A0

[54] *Yessi Bello Perez*. Santander: blockchain tech can save banks $20 billion a year // CoinDesk. — 2015.
URL: http://www.coindesk.com/santander-blockchain-tech-can-save-banks-20-billion-a-year/

[55] Merged mining specification // Bitcoin Wiki
URL: https://en.bitcoin.it/wiki/Merged_mining_specification

[56] Namecoin
URL: http://namecoin.info/

[57] SHA-2 // English Wikipedia
URL: https://en.wikipedia.org/wiki/SHA-2

[58] *Paul Snow, Brian Deery, Jack Lu, David Johnston, Peter Kirby*. Factom: business processes secured by immutable audit trails on the blockchain. — 2014.
URL: https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf