Проект NISTIR 8202 17
Обзор технологии Blockchain

Dylan Yaga 22
Peter Mell
Отдел компьютерной безопасности
Лаборатория информационных технологий

Nik Roby
G2, Inc. 28
Annapolis Junction, MD

Karen Scarfone
Scarfone Cybersecurity 32
Clifton, VA

Январь 2018 года

Министерство торговли США
Уилбур Л. Росс, мл., Секретарь

Национальный институт стандартов и технологий
Вальтер Копан, директор NIST и заместитель министра торговли стандартами и технологиями

Перевод с английского Наталья Константинова компания Briastorm

Содержание

Список приложений

Список таблиц и рисунков

Резюме

Блокчейны—это неизменяемые цифровые системы реестров*(система регистрации*), реализованные распределенным образом (т. е. без центрального хранилища) и, как правило, без центрального руководства. На самом базовом уровне, они позволяют сообществу пользователей записывать транзакции в реестр, открытый для этого сообщества, таким образом, что ни одна транзакция не может быть изменена после публикации. В 2008 году идея блокчейна инновационным способом была объединена с несколькими другими технологиями и вычислительными концепциями для создания современных криптовалют: электронные деньги защищены через криптографические механизмы, вместо центрального хранилища. Первым, основанным на концепции блокчейн был Биткоин. Эти валютные блокчейн системы новы тем, что они хранят значения(*стоимость*), а не только информацию. Значение прикреплено к цифровому кошельку (электронное устройство (или программа), которое позволяет физическому лицу совершать электронные транзакции). Кошельки используются для засвидетельствования *(подписания*) транзакций, которые проходят с одного кошелька на другой, записывая переданное значение (стоимость) публично, позволяя всем участникам сети независимо подтвердить действительность транзакций. Каждый участник может хранить полную запись всех транзакций, что делает сеть устойчивой к попыткам изменить эту запись (или подделать транзакции) позже.

Из-за того, что существует бесчисленное множество новостных статей и видео, описывающих "магию" блокчейна, эта статья призвана описать метод, лежащий в основе магии (т. е. как работает блокчейн-система). Артур Кларк однажды написал: “любая достаточно развитая технология неотличима от магии” [1]. Заявление Кларка является идеальным представлением новых вариантов использования блокчейн технологии. Существует высокий уровень хайпа вокруг использования блокчейнов, хотя технология еще не совсем понятна. Это не волшебство и она не решит всех проблем. Как и со всеми новыми технологиями, существует тенденция в желании применить ее во всех секторах и всеми способами, которые можно только себе представить. В этом документе мы попытаемся ясно объяснить технологию так, чтобы она могла применяется эффективно.

Как говорилось выше, технология блокчейн является основой современных криптовалют, называемых так из-за интенсивного использования блокчейном криптографических функций. Пользователи используют открытые и закрытые ключи для цифровой подписи и безопасного выполнения транзакций в системе. Пользователи блокчейна могут решить головоломки с использованием криптографического хеширования в надежде быть вознагражденными фиксированной суммой криптовалюты. Однако технология блокчейн применима шире, чем только в криптовалютах. В этой работе мы пытаемся показать эту более широкую применимость, в значительной степени сосредотачиваясь на использовании криптовалюты (так как это основной случай использования сегодня).

Организациям, которые рассматривают внедрение технологии блокчейн нужно понимать важные аспекты технологии. Например, что происходит, когда организация внедряет систему блокчейн, а затем решает, что им нужно внести изменения в хранящиеся данные? Если, используя базу данных, это может быть достигнуто с помощью простого запроса (или основные изменения могут производиться путем обновления схемы базы данных или программного обеспечения), то на блокчейне гораздо труднее изменить данные или обновить программное обеспечение "базы данных". Организации должны понимать, насколько крайне сложно изменить

все, что уже в блокчейне, и что изменения в программном обеспечении блокчейна может вызвать разветвление блокчейна. Еще один критический аспект технологии блокчейн—это то, как участники соглашаются с тем, что транзакция действительна. Это называется " достижение консенсуса", и есть много моделей, по которым это делается, и у каждой есть свои позитивными и негативными моменты, в зависимости от конкретного бизнес-кейса.

Некоторые существующие блокчейн технологии фокусируются на хранении материальных ценностей, в то время как другие являются платформой для смарт-контрактов (программное обеспечение, размещенное на самом блокчейне, и, осуществляющееся компьютерами, которые управляют этим блокчейном). Постоянно разрабатываются новые технологии блокчейн, что позволяет расширять возможности использования и улучшать эффективность существующих систем. Некоторые реализации блокчейна инклюзивные, не требуют разрешения, т.е. любой человек может читать и писать в них. Другие же реализации ограничивают участие конкретными людьми или компаниями, позволяя более детально контролировать и управляться централизованной единицей. Знания этих особенностей позволяет организации понять, что больше отвечает их нуждам.

Несмотря на множество вариаций блокчейн-систем и стремительное развитие новых технологий, большинство блокчейнов используют некоторые общие основные концепции. Каждая транзакция включает в себя один или более адресов, запись того, что произошло и подписано цифровой подписью. Блокчейны состоят из блоков, каждый из которых представляет собой группу транзакций. Все транзакции в блоке сгруппированы друг с другом и связаны вместе криптографическим хэшем предыдущего блока. Наконец, создается новый хэш для заголовка текущего блока, который будет записан как внутри самого блока, так и в следующем блоке. Со временем каждый блок будет прицеплен к предыдущему блоку в цепочке добавлением хэша предыдущего блока в заголовок текущего блока.

Каждая технология, используемая в блокчейн-системе, берет существующие, проверенные концепции и объединяет их вместе таким образом, чтобы можно было решать проблемы, которые были трудными ранее. В этом документе исследуются основы работы блокчейн-технологий, как участники сети приходят к согласию о том, является ли транзакция действительной, что происходит, когда должны быть сделаны изменения для существующего развертывания блокчейна и как работают разрешения. Кроме того, в этом документе исследуются конкретные применения блокчейна и примеры, когда стоит рассмотреть использование блокчейн-системы.

Использование технологии блокчейн не является волшебным средством, и есть проблемы, которые должны быть рассмотрены, например, как работают с вредоносными пользователями, как применяются элементы управления и ограничения по любой реализации блокчейна. Тем не менее, технология blockchain является важной концепцией, которая станет основой для многих новых решений.

1 Введение

Блокчейны—это неизменяемые цифровые системы реестров (система регистрации), реализованные распределенным образом (т. е. без центрального хранилища) и, как правило, без центрального руководства. На самом базовом уровне, они позволяют сообществу пользователей записывать транзакции в реестр, открытый для этого сообщества, таким образом, что ни одна транзакция не может быть изменена после публикации.
Эта технология стала широко известна, начиная с 2008 года, когда она была применена для появления электронной валюты, где цифровые переводы денег происходили в распределенных системах. Это обеспечило успех систем электронной коммерции, таких как Bitcoin, Ethereum, Ripple и Litecoin. Из-за этого блокчейны часто связывают с Биткойном или, возможно,с электронными валютами в общем. Тем не менее, технология является более широко используемой и доступна для различных применений.

Многочисленные компоненты технологии блокчейн, наряду с ее опорой на криптографические примитивы и распределенные системы, могут затруднить понимание. Однако, каждый компонент можно просто описать и использовать как часть для того, чтобы понять более крупную сложную систему. Мы предоставляем неофициальное краткое описание технологии блокчейн:

Блокчейны являются распределенными цифровыми реестрами в которых криптографически подписанные транзакции сгруппированы в блоки. Каждый блок криптографически связан с предыдущим после подтверждения и принятие общего решения. По мере добавления новых блоков, старые блоки становится труднее изменить. Новые блоки воспроизводятся по всем копиям реестра внутри сети, и любые конфликты разрешаются автоматически с помощью установленных правил.

1.1 Предпосылки и история

Основные идеи технологии блокчейн появились в 1991 году, когда подписанная информационная цепочка использовалась в качестве электронного реестра для цифровой подписи документов таким способом, который мог бы легко показать, что ни один из подписанных документов в коллекции не был изменен [2]. Это было в начале применено к цифровым денежным средствам в 2008 году в исходной статье, описывающей решение для электронных денежных средств Bitcoin, *Bitcoin: A Peer to Peer Electronic Cash System* [3], которая была опубликована под псевдонимом Сатоши Накамото. Фактический Автор(ы) и владелец первых Биткоинов остается загадкой. С тех пор блокчейн технология стала тесно связана с Биткоином и часто считается, что она используется для денежных операций (хотя это не ограничивается простыми переводами средств). Документ Накамото содержал концепцию, которой следуют большинство современных схем цифровой наличности, во многих вариациях. Биткойн на самом деле является первым из многих применений или случаев использования блокчейна.

Многие схемы электронных денег существовали до Биткойна, но ни одна из них не достигла широкого распространенного использования. Приняв технологию блокчейн, Биткойн достиг убедительных возможностей, которые способствовали его использованию. Использование

блокчейна позволило распределенным способом реализовать Биткойн так, чтобы не было ни одной точки сбоя, и ни один пользователь не мог контролировать валюту. Самым полезным была возможность проведения прямых электронных финансовых транзакций между пользователями без участия третьего лица. Это также позволило обеспечить выпуск новой валюты справедливым образом для тех пользователей (иногда называют майнеры или minters), которые занимаются поддержанием блокчейн, что в свою очередь, обеспечило низкие транзакционные издержки при использовании системы. Оплата нодам майнинга обеспечила работу распределенного администрирования системы без необходимости организации тех, кто поддерживает систему. Используя распределенный блокчейн и консенсусное обслуживание, был создан механизм самоконтроля, который обеспечивал добавление в блокчейн только действительных транзакций.

Кроме того, блокчейн позволил пользователям быть под псевдонимами, что означает, что пользователи анонимны, но их счета нет—все их сделки открыты для наблюдения. Это позволило Bitcoin эффективно предложить псевдо-анонимность, потому что счета могут быть созданы без какой-либо идентификации или авторизации. Наконец, распределенное обслуживание блокчейна создало систему с полной прозрачностью, которая вызывала доверие к ее использованию. Так как все транзакции прозрачны в системе и должны быть подтверждены перед включением в систему, то это значительно уменьшает возможность двойных расходов своих цифровых активов для пользователей (отправка одного и того же цифрового актива более чем одному пользователю). Одним из самых ценных аспектов приложений, работающих на блокчейне—это то, что они могут позволить вести бизнес с ненадежными и неизвестными пользователями.

1.2 Цель и сфера применения

Этот документ предоставляет глубокий технический обзор технологии блокчейн. В нем глубоко обсуждается его применение для электронной валюты, а также и его более широкое использование. Рассматриваются различные категории подходов, так как существует множество блокчейн-платформ, каждая из которых немного отличается. Этот документ призван помочь читателям понять технологии, которые образуют системы блокчейн и понять, как блокчейны можно правильно и с пользой применить в решении технологических проблем.

1.3 Примечания к терминам

Терминология для технологии блокчейн варьируется от одной реализации к другой, поэтому для того, чтобы говорить о технологии в целом, будут использоваться общие термины. В этом документе термины “пользователь” и “нод”(узел) используются для описания компонентов блокчейна. Для целей этого документа, “пользователь” является общим термином для описания любого лица, организации, реальности, структуры, бизнеса, правительства, и т.д. которые используют систему блокчейн. *Нода*-это индивидуальная система внутри блокчейн-системы, и может быть доработана до *полной ноды* (которая хранит весь блокчейн), *ноды майнинга* (полная нода, которая также поддерживает блокчейн, публикуя новые блоки), и *облегченная нода* (нода, которая не поддерживает историю всего блокчейна).

1.4 Структура Документа

Этот документ состоит из следующих разделов и приложений:

. Раздел 2 определяет высокоуровневые компоненты архитектуры блокчейн-системы, включая хэши, транзакции, реестры (регистры), блоки и блокчейны

· В разделе 3 обсуждается, как блокчейн расширяется за счет добавления новых блоков, в которых представлен набор транзакций.

. Раздел 4 рассматривает потребность в консенсусных моделях для разрешения конфликтов между майнинг нодами блокчейна .

· Раздел 5 вводит понятие форкинга.

· Раздел 6 определяет и рассматривает смарт-контракты.

· Раздел 7 рассматривает модели разрешений в блокчейне, их применение и примеры вариантов использования для каждой модели.

· Раздел 8 содержит несколько примеров блокчейн платформ, используемых сегодня для обозначения различий одной платформы от другой.

· Раздел 9 освещает некоторые ограничения технологии блокчейн.

· В разделе 10 дается краткое заключение по документу.

- Приложение А содержит глоссарий для терминов, определенных в документе.
- Приложение Б содержит список сокращений, используемых в документе.
- Приложение С определяет ссылки, используемые во всем документе.

2 Архитектура Blockchain

Блокчейн системы могут казаться сложными, однако их легко понять, изучив каждый компонент технологии отдельно. На высоком уровне блокчейны используют хорошо известные механизмы компьютерной науки (связанные списки, распределенные сети), а также криптографические примитивы (хеширование, цифровые подписи, общедоступные / закрытые ключи), смешанные с финансовыми концепциями (например, реестры).

2.1 Хеши

Важным компонентом технологии блокчейн является использование криптографических хеш-функций для многих операций, таких как хеширование содержимого блока. Хеширование - это метод вычисления относительно уникального фиксированного выхода (называется *дайджест сообщения* или просто *дайджест)* для входа почти любого размера (например, файл, текст или изображение). Даже небольшое изменение входа (например, одного бита) приведет к совершенно другому выходному дайджесту. В таблице 1 приведены простые примеры этого. Хэш алгоритмы разработаны, чтобы быть в одностороннем порядке (известны, как устойчивые к прообразу): невозможно с вычислительной точки зрения найти какой-либо вход, который сопоставляется с любым заранее заданным выходом. Если требуется конкретный выход, многие входы должны быть проверены путем передачи их через хеш-функцию до тех пор, пока не будет найден входной сигнал, который даст желаемый результат. Хэш-алгоритмы также разработаны для обеспечения устойчивости к коллизиям (как вторая резистентность к прообразу): невозможно с вычислительной точки зрения найти два или более входа, которые

производят тот же результат.

Алгоритм хеширования, используемый во многих технологиях блокчейн —это Secure Hash Algorithm (SHA), с размером выхода*(вывода)* 256 бит (SHA-256). Многие компьютеры поддерживают этот алгоритм в аппаратном обеспечении, это и позволяет быстро вычислять. Этот алгоритм имеет выход из 32 (8-битных) символов (показано ниже, в Таблице 1, в виде 64-символьной шестнадцатеричной строки), что означает, что существует 2256 ≈ 1077 или 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129, 639,936 372 возможных значений дайджеста. Алгоритм для SHA-256, так же как и другие, указан в Federal Information Processing Standard (FIPS) 180-4 [4]. Веб-сайт NIST Secure Hashing [5] содержит спецификации FIPS для всех алгоритмов хеширования, одобренных NIST.

Таблица 1: Примеры входов и значения дайджеста SHA-256

Table 1: Examples of Inputs and SHA-256 Digest Values

Input Text	SHA-256 Digest Value
1	0x6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b
2	0xd4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35
Hello, World!	0xdffd6021bb2bd5b0af676290809ec3a53191dd81c7f70a4b28688a362182986f

Поскольку существует чрезвычайно большое количество возможных входных значений и ограниченое число возможных выходных значений, можно получить коллизию, где hash (x) = hash (y) (т. е. хэш двух разных входов дают один и тот же дайджест). Однако это маловероятно для любого такого входа x и y, что производя один и тот же дайджест для обоих, что они будут действительны в контексте системы блокчейн (в данном случае, оба являются действительными транзакциями цепочки), а также будут вовремя рассчитаны достаточно близко к друг другу. Используемый алгоритм хеширования (SHA-256) считается устойчивым к коллизии, поскольку чтобы найти коллизию в SHA-256, нужно было бы выполнить алгоритм, в среднем, около 2128 раз. Технологии Blockchain берут список транзакций и создают цифровой отпечаток хэш (дайджест - это отпечаток) для списка. Любой, имеющий один и тот же список транзакций, может генерировать точно такой же цифровой отпечаток. Если хоть одно значение в транзакции в списке изменяется, дайджест для этого блокирует изменения, что позволяет легко обнаружить даже незначительные изменения одного бита.

2.2 Транзакции

Транзакция— это запись передачи активов (цифровая валюта, единицы инвентаря и т. д.) между сторонами. Аналогом этого будет являться запись на расчетном счете каждый раз, когда деньги внесены или сняты. В таблице 2 показан условный пример транзакции. Каждый блок в блокчейне содержит несколько транзакций. Для одной транзакции обычно требуется по крайней мере следующие информационные поля (но их может быть и больше):

- **Сумма** - общая сумма цифрового актива для передачи.

· **Входы** - список цифровых активов, подлежащих передаче (их общая стоимость равна сумме).

Обратите внимание, что каждый цифровой актив уникально идентифицирован и может иметь отличные значения от других активов. Однако активы не могут быть добавлены или удалены из существующих цифровых активов. Вместо этого цифровые активы могут быть разделены на несколько новых цифровых активов (каждый с меньшим значением) или объединены, чтобы сформировать меньшее количество новых цифровых активов (каждый с соответственно большим значением).

· **Выходы** - учетные записи, которые будут получателями цифровых активов. Каждый выход

указывает значение, которое должно быть передано новому владельцу (владельцам), личность нового владельца(ов), и набор условий, которыми должны отвечать новые владельцы, чтобы получить значение. Если цифровые активы предоставлены больше, чем нужно, лишние средства вернуться отправителю (это механизм “make change”(*размен, получение сдачи)).*

· **ID транзакции / Хэш** - уникальный идентификатор для каждой транзакции. Некоторые блокчейны используют ID, а другие принимают хеш конкретной транзакции как уникальный идентификатор.

Таблица 2: Пример транзакции

	Вход	Выход	Количество	Всего
Transaction ID: 0xa1b2c3 *ID транзакции*	Account A	Account B	0.0321	
		Account C	2.5000	
				2.5321

Определение валидности транзакции важно. Просто потому, что кто-то утверждает, что сделка состоялась, не означает, что это действительно произошло. Транзакции подписаны и могут быть проверены с помощью пар public / private key (открытый/закрытый ключ) в любое время.

2.3 Криптография с асимметричным ключом

Основополагающей технологией, используемой технологиями блокчейн, является криптография с асимметричным ключом1 (также называемой криптографией открытого/ закрытого ключа). Криптография с асимметричным ключом использует пару ключей: открытый ключ и закрытый ключ, которые математически связаны друг с другом. Открытый ключ может быть открытым без снижения безопасности процесса, но закрытый ключ должен оставаться секретными, если данные удерживают за собой криптографическую защиту. Даже несмотря на то, что оба ключа соотносятся друг с другом, закрытый ключ не может эффективно быть определен, основываясь на знании открытого ключа.

Криптография с асимметричным ключом использует различные ключи из пары ключей для определенных функций, в зависимости от того, какая услуга должна быть предоставлена. Например, при цифровой подписи данных криптографический алгоритм использует приватный ключ для подписи. Затем подпись может быть проверена с использованием соответствующего открытого ключа.

Использование криптографии с асимметричным ключом в системах блокчейн:

• Закрытые ключи используются для цифровой подписи транзакций.
• Открытые ключи используются для получения адресов, что позволяет использовать подход «один-ко-многим» для псевдонимности (одна пара открытых ключей может давать несколько адресов, в некоторых случаях – несколько пар открытых ключей используются для создания нескольких адресов).
• Открытые ключи используются для проверки подписей, сгенерированных с помощью закрытых ключей.
• Криптография с асимметричным ключом обеспечивает возможность проверки того, что у пользователя, передающего значение для другого пользователя есть закрытый ключ, способный подписать значение.

1 FIPS Publication 186-4, Digital Signature Standard [6] определяет общий алгоритм цифровой подписи, используемый в технологиях blockchain: Elliptic Curve Digital Signature Algorithm (ECDSA).

2.4 Адреса и наследование адреса

Адрес пользователя представляет собой короткую буквенно-цифровую строку, полученную из открытого ключа пользователя с использованием хеша а также некоторые дополнительные данные (используемые для обнаружения ошибок). Адреса используются для отправки и получения цифровых активов. Большинство блокчейн систем используют адреса как «to» и «from» конечных точек в транзакции.

Адреса короче открытых ключей и не являются секретными. Сгенерировать адрес, это обычно означает использовать открытый ключ, хэшировать его и преобразовать хэш в текст:

открытый ключ -> хэш-функция -> адрес

Пользователи могут генерировать столько пар открытых/закрытых ключей и, следовательно, адресов сколько пожелают, что дает возможность существованию различной степени псевдо-анонимности. Адреса выступают в качестве общедоступной «идентичности» для пользователя на блокчейне, и часто адрес преобразуется в QR-код для удобства использования.

Когда блокчейн распределяет цифровые активы, он делает это, назначая им адрес. Чтобы потратить этот цифровой актив, пользователь должен доказать, что он владеет закрытым ключом соответствующим адресу. Подписывая транзакции закрытым ключом в цифровом виде, транзакция может быть подтверждена открытым ключом.

2.4.1 Хранение закрытого ключа

Большинство пользователей блокчейн системы не записывают свои личные ключи вручную, скорее, программное обеспечение, обычно называемое кошельком, надежно хранит их. Кошелек может хранить закрытые ключи, открытые ключи и привязанные адреса. Программное

обеспечение кошелька также может рассчитать общее количество активов, которые может иметь пользователь.

Закрытый ключ обычно генерируется с использованием безопасной случайной функции, что означает, что восстановление его сложно, если совсем невозможно. Если пользователь теряет закрытый ключ, то любой актив, связанный с этим ключом потерян. Если закрытый ключ украден, злоумышленник получит полный доступ ко всем активам, контролируемым этим закрытым ключ. Безопасность закрытых ключей настолько важна, что многие пользователи используют специальные устройства, чтобы сохранить его.

Приватное хранилище ключей является чрезвычайно важным аспектом технологии блокчейн. Когда сообщают в новостях, что «биткойн был украден из ...», это почти наверняка означает, что были найдены закрытые ключи и использованы для подписи транзакции (перевод денег на новую учетную запись) а не то, что система была скомпрометирована. Обратите внимание, что поскольку данные блокчейна обычно не могут быть изменены, когда преступник крадет закрытый ключ и публично перемещает связанные средства на другой счет, это не может быть отменено.

2.5 Регистры/Реестры

Реестры представляют собой набор транзакций. На протяжении всей истории использовались бумажные реестры, в которые делались записи для отслеживания обмена товаров и услуг. Совсем недавно реестры стали храниться в цифровом виде, часто в больших базах данных, принадлежащих и управляемых исключительно централизованным «доверенными» третьими лицами от имени сообщества пользователей (т. е. третье лицо является владельцем реестра).

У централизованных реестров могут быть недостатки, например:
• Они могут быть потеряны или уничтожены. Пользователь должен быть уверен, что владелец правильно делает бэкап системы.
• Транзакции могут быть недействительными. Пользователь должен быть уверен, что владелец проверяет каждую полученную транзакцию.
• Список транзакций может быть неполным. Пользователь должен быть уверен, что владелец включает все действительные транзакции, которые были получены.
• Данные транзакции могут быть изменены. Пользователь должен верить, что владелец не изменит прошлые транзакции.

Разумеется, в лучших интересах централизованного реестра делать резервное копирование (бэкап) данных, проверять транзакции, включать все действительные транзакции, а не изменять историю.

Реестр, реализованный с использованием блокчейна, может уменьшить эти проблемы с помощью распределенного механизма консенсуса. Одним из аспектов этого является то, что реестр блокчейна будет скопирован и распределен между каждой нодой в системе. На рисунке 1 показана простая сеть с четырьмя нодами, каждая из которых имеет копию реестра транзакций.

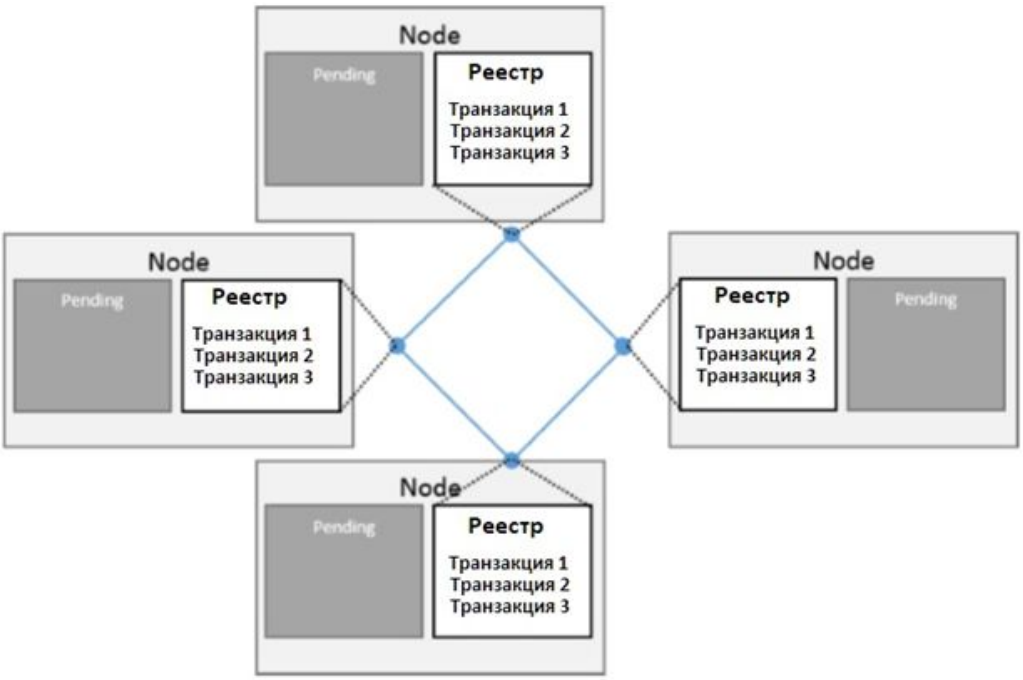


Рис. 1 – Простая сеть, поддерживающая реестр среди нод

Новые транзакции отправляются на ноду (как показано на рисунке 2), которая затем предупреждает остальную часть сети, в которую поступила новая транзакция (как видно на рисунке 3).

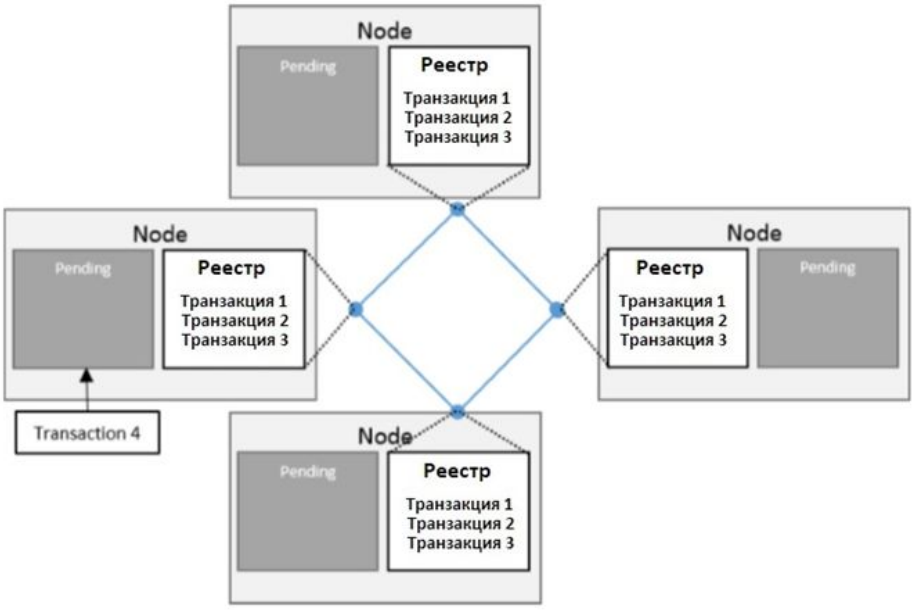


Рисунок 2 - Передача транзакции ноде, ожидающей в списке пендинг(ожидающих обработки) транзакций.

На данный момент эта транзакция ожидающая обработки(пендинг транзакция), которая не входит в блок внутри реестра.

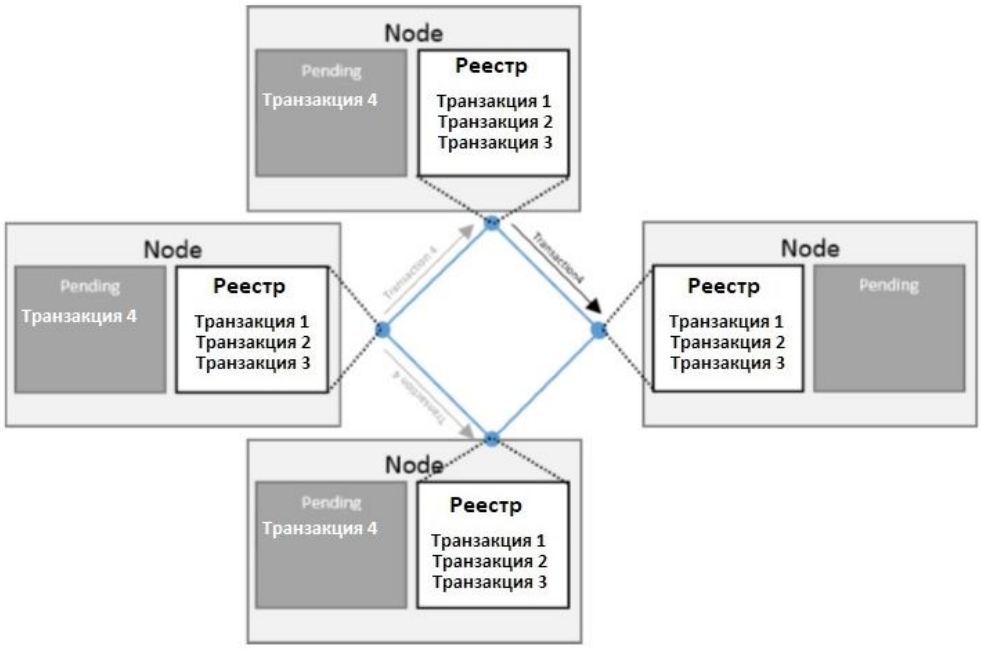


Рис. 3 – Информация о транзакции 4, передаваемая от ноде к ноде

В итоге, нода включит эту новую транзакцию внутрь блока и выполнит консенсус метод, требуемый системой (поясняется ниже). Этот новый блок будет распределен по системе и все реестры будут обновлены, чтобы включить новую транзакцию (как показано на рисунке 4).

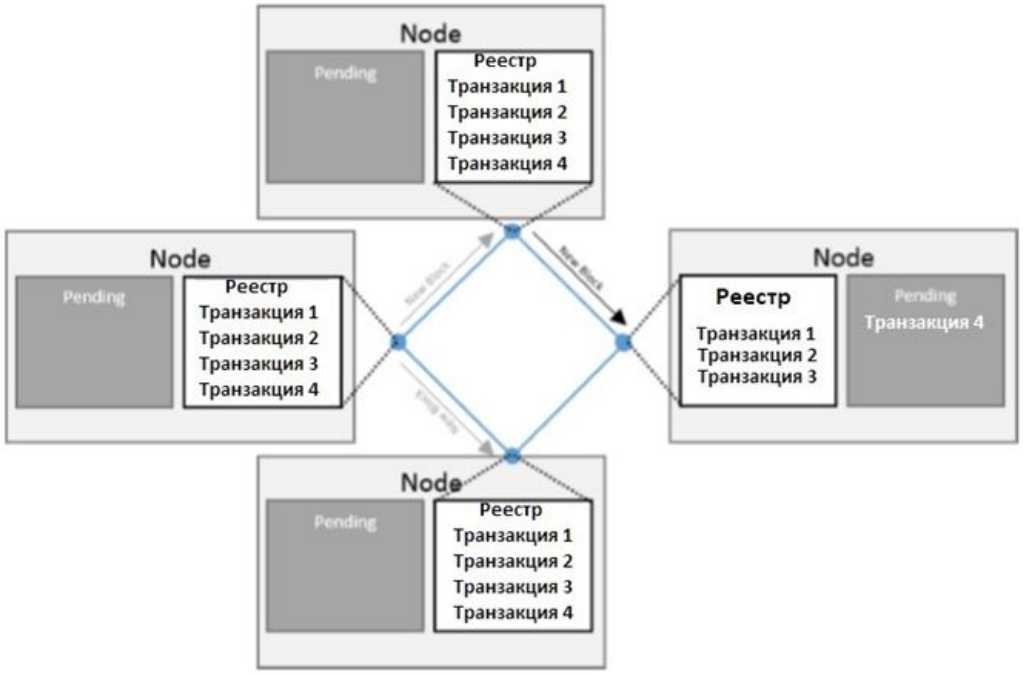


Рис.4 – Транзакция 4 была включена в блок, ноды передают информацию. Конечная нода еще не получила последнюю информацию.

Всегда, когда новые пользователи присоединяются к системе, они получают полную копию блокчейна, что делает практически невозможным потерю или разрушение реестра. Все транзакции хранятся в блоках в блокчейне (транзакции обсуждаются в секции 2.2)

2.6 Блоки

Пользователи могут добавлять желаемые транзакции в реестр, отправляя эти транзакции в некоторые ноды, участвующие в блокчейне. Переданные транзакции распространяются на другие ноды в сети (но это само по себе не включает транзакцию в блокчейн).

Распределенные транзакции затем ожидают в очереди или *пуле транзакций*, пока они не будут добавлены в блокчейн майнинг нодой.

Майнинг ноды – это разновидность узлов, которые поддерживают блокчейн, публикуя новые блоки. Транзакция добавляется в блокчейн, когда майнинг нода публикует блок. *Блок* содержит набор валидных транзакций. «Валидность» обеспечивается путем проверки того, что поставщики средств в каждой транзакции (перечисленные в значениях «вход»(input) транзакции) криптографически подписали каждую транзакцию. Это подтверждает, что поставщики средств для транзакции имели доступ к закрытому ключу, который может подписать имеющиеся средства. Остальные майнинг ноды будут проверять валидность всех транзакций в опубликованном блоке и не будут принимать блок, если он содержит недействительные транзакции.

После создания, каждый блок хэшируется, тем самым создавая дайджест, представляющий блок. Изменение даже одного бита в блоке полностью изменило бы хэш-значение. Хэш-дайджест блока используется для защиты блока от изменения, поскольку все ноды будут иметь копию хэша блока и смогут проверить, чтобы убедиться, что блок не был изменен.

Фактическая конструкция блока несколько сложнее. Поля данных, составляющие блок обычно состоят из следующего:

- Номер блока, также известный как высота блока
- Текущее значение хеша блока
- Предыдущее значение хеша блока
- Корень(root) хэш дерева Меркла(определен ниже)(Merkle root hash)
- Метка времени (Timestamp)
- Размер блока
- Значение *nonce*(случайный код), которое представляет собой число, управляемое майнинг нодой для решения хеш-головоломки, которая дает им право опубликовать блок (подробнее см. Раздел 4.1)
- Список транзакций, включенных в блок

Вместо того, чтобы хранить хэш каждой транзакции в заголовке блока, используется структура данных, известная как дерево Меркла. Дерево Меркла объединяет хэш-значения данных вместе до единого Root (root хэш дерева Меркла). Root(корень) - это эффективный механизм, который используется для того, чтобы суммировать транзакции в блоке и проверить наличие транзакции внутри блока. Эта структура гарантирует, что данные, отправленные в распределенную сеть, валидны, т.к. любые изменения до основных данных будут обнаружены и могут быть отклонены. На рисунке 5 показан пример дерева Меркла:

• Нижняя строка представляет данные, которые должны быть суммированы, в случае с блокчейнами это данные транзакции.
• Вторая в нижней строке показывает, что данные хэшируются.
• Хешированные данные из второй строки затем объединяются, а затем хэшируются на третьем нижнем ряду.
• Наконец, верхний ряд показывает Root хеш, который объединяет и хеширует H4 и H5.
Root хэш—хэш всех предыдущих сделанных комбинаций и хэшей.

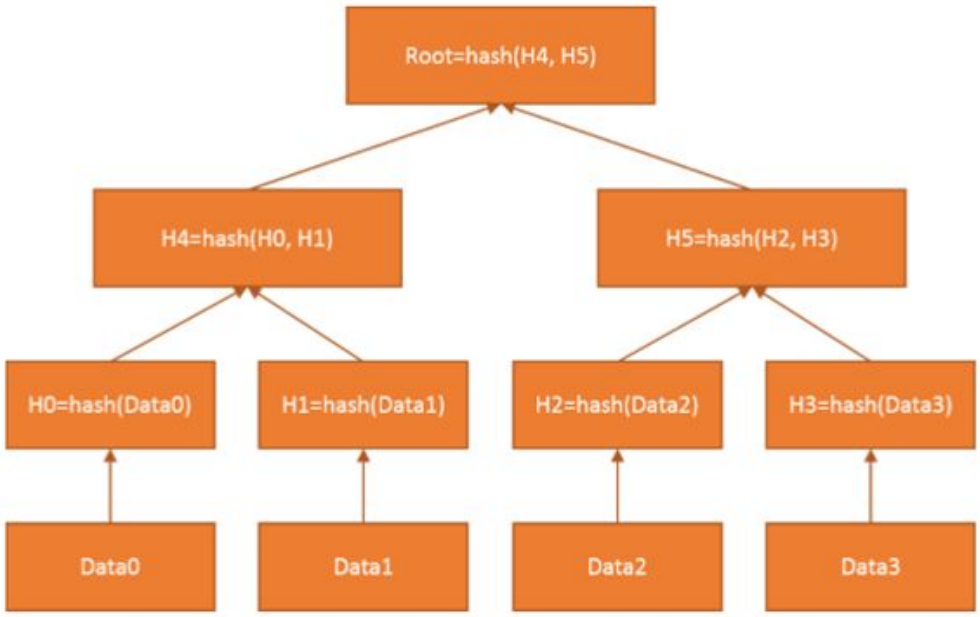


Рис.5: Пример дерева Меркла

На рисунке 6 показана взаимосвязь между деревом Меркла и блоком. Нижняя строка дерева содержит блокчейн транзакции Tx0 - Tx3. Root Меркла хранится в заголовке блока.

Весь заголовок блока хешируется. Значение хеш-заголовка блока хранится как внутри самого блока, так и внутри следующего блока, что позволяет обеспечить неизменность транзакций, поскольку root хэш Меркла не будет соответствовать, если в транзакции будут внесены какие-либо изменения.

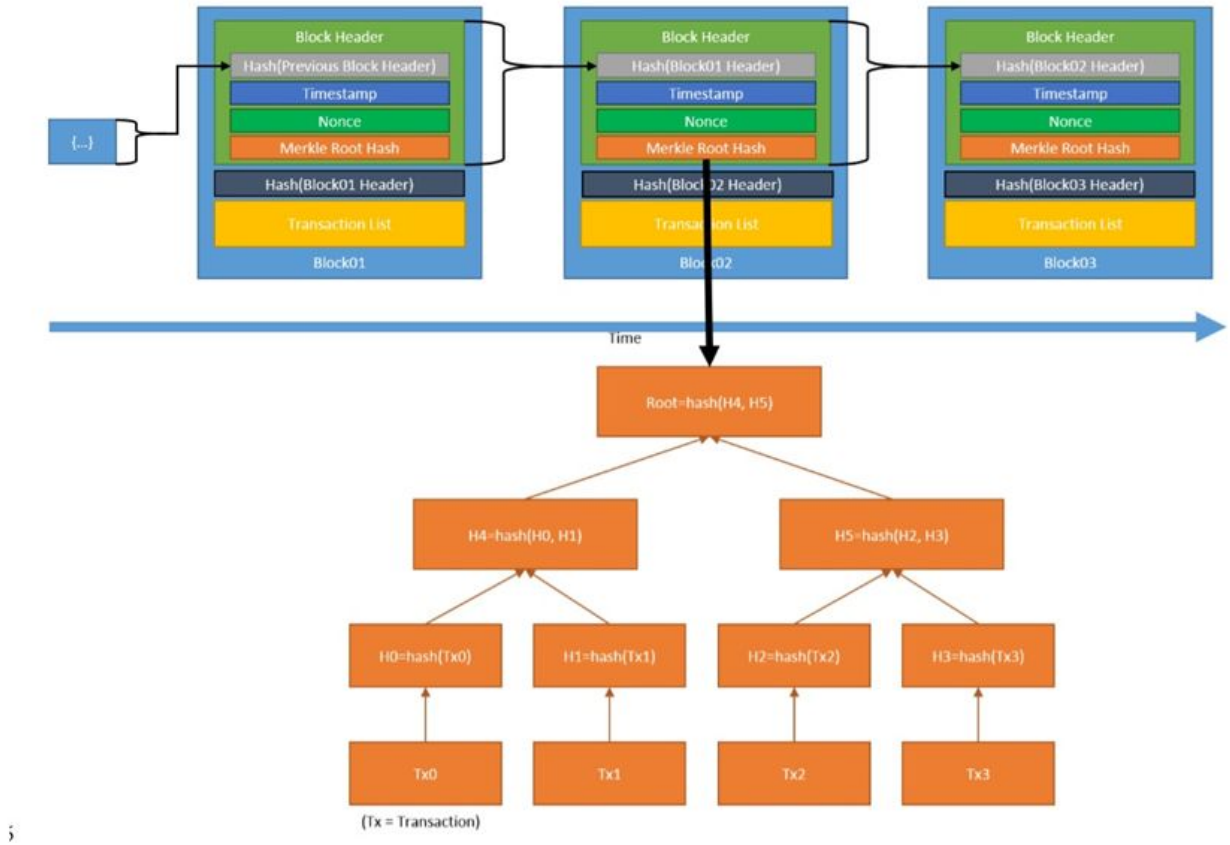


Рис.6 Блокчейн с деревом Меркла

2.7 Сцепление блоков

Блоки соединены друг с другом через каждый блок, содержащий хэш заголовка предыдущего блока, тем самым формируя цепочку. Если ранее опубликованный блок был изменен, у него был бы другой хеш. Это, в свою очередь, приведет к тому, что все последующие блоки также будут иметь другие хэши, поскольку они включают хеш предыдущего блока. Это позволяет легко обнаруживать и отклонять любые изменения ранее опубликованных блоков. На рисунке 7 показана общая цепочка блоков.

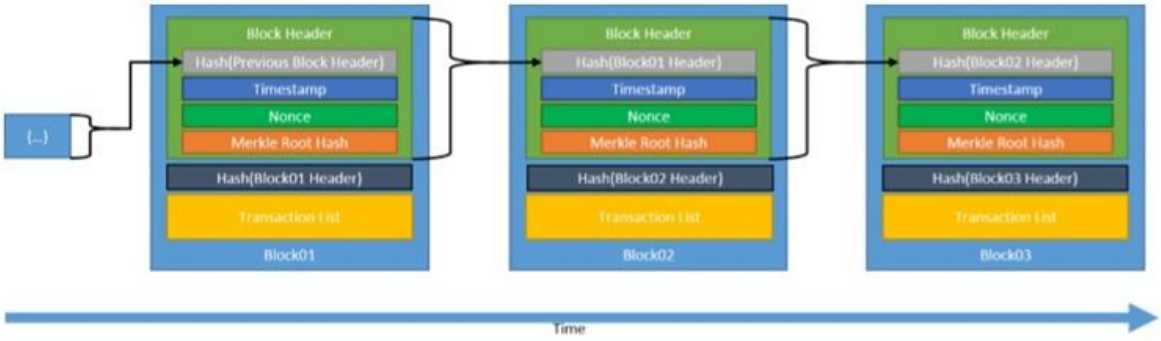


Рис.7: Общая цепочка блоков

3 Функционирование Blockchain

В предыдущем разделе мы предоставили статический вид компонентов общего блокчейна. В этом разделе мы обсудим, как блокчейн расширяется за счет добавления новых блоков, представляющих совокупности транзакций. Здесь мы обсудим инклюзивный блокчейн, который использует Proof-of-Work консенсус метод (тот, который используется Bitcoin и его деривативами и самый популярный метод на сегодняшний день). Информация о других консенсусных методах обсуждается ниже, в разделе 4.

Блокчейны поддерживаются на основе консенсуса множества компьютеров, на которых запущено программное обеспечение блокчейна, известное как майнинговые ноды. Нет центрального органа управления, определяющего, какая нода публикует следующий блок на блокчейне. Каждая нода поддерживает копию цепочки блоков и может предлагать новый блок другим майнинг нодам. Недействительные блоки будут обнаружены и отклонены, потому что сложно вычислить валидный блок, но вычислительно его легко проверить. Майнинг – задача намеренно ресурсоемкая, требующая больших вычислительных мощностей, памяти или и того и другого, в зависимости от конкретного применения блокчейна. Консенсусный протокол, определяющий какой новый блок будет добавлен в блокчейн, обсуждается в разделе 4.

Как упоминалось ранее, любой компьютер, на котором запущено программное обеспечение блокчейна, считается *нодой* этого блокчейна. Обычно существуют два типа узлов: полные узлы и облегченные узлы. Работой *полных нод* является хранение данных блокчейна, передача данных другим нодам и обеспечивать уверенность в том, что новые добавленные блоки валидны. Валидация предполагает проверку, что формат блока правильный, все хэши в новом блоке были вычислены правильно, новый блок содержит хэш предыдущего блока, и каждая транзакция в блоке действительна и подписана соответствующими сторонами. *Полные ноды* могут также выступать в качестве майнинг нод(т.е. генерировать новые блоки). *Облегченным нодам* нет необходимости хранить полные копии блокчейна и часто передавать свои данные на полные ноды для обработки. Облегченные ноды, как правило, обнаруживаются на смартфонах и устройствах Интернета вещей(IoT)—устройствах с ограниченными вычислительными возможностями и / или возможностями хранения. Любая нода может предложить новые транзакции, и эти предложенные транзакции будут распространятся между нодами до тех пор, пока они в конечном итоге не добавятся в блок.

Предлагаемые транзакции в блокчейне хранятся на майнинг нодах в пуле неизрасходованных транзакций, ожидая быть включенным в блок, как показано на рисунке 8.

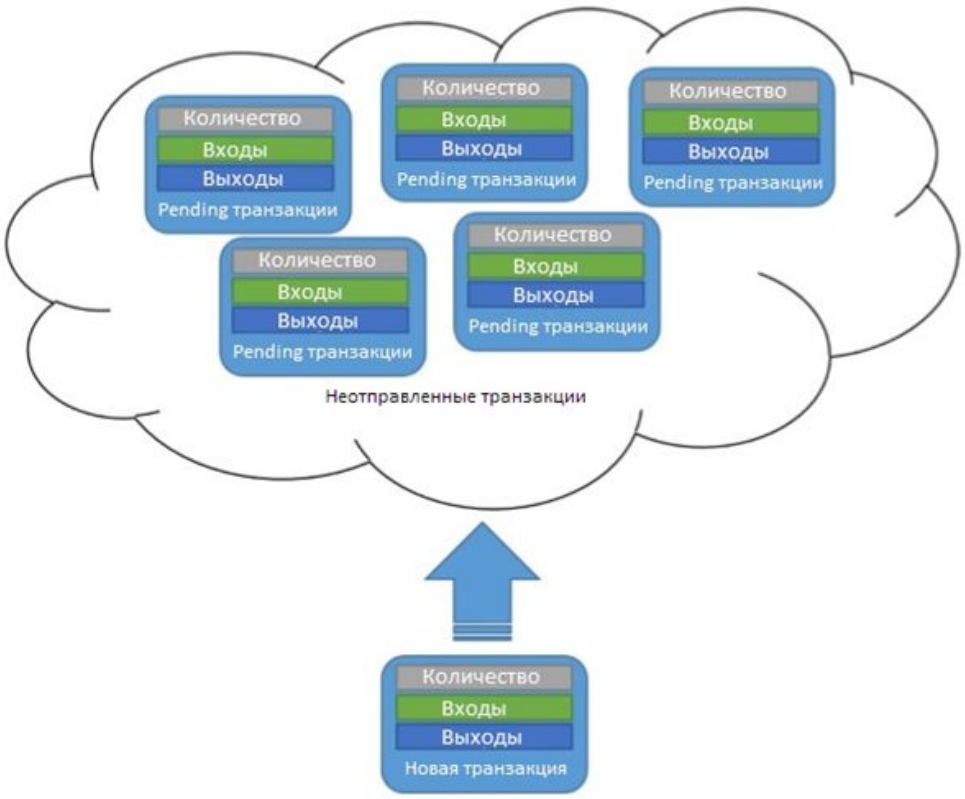


Рис. 8: Транзакция была добавлена в пул неизрасходованных транзакций

Когда майнинг ноды объединяют новый потенциальный блок, они включают в себя набор неотправленных транзакций. Они могут принять комбинацию более старых транзакций, которые находились в ожидании некоторое время и новых, которые предлагают более высокую оплату (в виде платы за транзакцию, уплаченной пользователем, отправившим транзакцию). Майнинг нода проверяет, что каждая транзакция сама по себе валидна, т.к. другие ноды отклонят блок, если он включает в себя недействительные транзакции. В этот момент майнинг нода заполняет всю информацию, необходимую блочной структуре, рассмотренную в Разделе 2.6, кроме nonce.

Некоторые блокчейны требуют жертв для создания следующего блока - например, времени и усилий, или делают ставку на привилегии. Для систем, требующих времени и усилий, майнинг нода вычисляет множество случайных значений nonce, чтобы попытаться вычислительно решить трудную головоломку. Победившая майнинг нода получает право опубликовать следующий блок (см. Раздел 4,1). Обычно майнинг ноды используют множество значений nonce перед решением головоломки. Когда головоломка решена с помощью конкретного nonce, нода создает хэш данных блока и хранит его в самом блоке. На рисунке 9 изображена структура построенного блока высокого уровня. Затем блок отправляется на другие ноды для верификации. Если все верифицировано, ноды принимают его, как последний блок и продолжают передавать его. В разделе 4.4 обсуждается, что произойдет, если несколько нод решат задачу в тот же таймфрейм, создав несколько конкурирующих «следующих» блоков.

Рис.9: Конечный блок(обобщенный)

Timestamp: отметка времени(дата и время создания блока)

4 Консенсус

В нашем общем представлении о блокчейне из предыдущего раздела многие майнинг ноды конкурируют в одно и то же время, чтобы решить загадку, чтобы получить право опубликовать следующий блок (и если применимо—финансовую награду). Они, как правило, все не доверяют пользователям, которые могут знать друг друга только по их публичным адресам. Каждый пользователь может быть замотивирован желанием получить финансовую выгоду, а не благосостоянием других майнинг нодов или даже сети в целом. В такой ситуации, почему пользователь должен распространять блок, разрешенный другим пользователем? Кроме того, кто разрешает конфликты, когда несколько майнинг нод решают блок примерно в одно и то же время? Чтобы сделать эту работу, блокчейны используют множество консенсусных моделей, которые позволяют группе взаимно недоверчивых пользователей работать вместе.

Обратите внимание, что когда пользователь присоединяется к блокчейн системе, он соглашается с исходным состоянием системы. Это записывается только в предварительно сконфигурированном блоке, *блоке генезиса*. Каждый блокчейн имеет опубликованный блок генезиса, и каждый блок должен быть добавлен к блокчейну после него на основе согласованного метода консенсуса. Независимо от метода, каждый блок должен быть валидным и, следовательно, может быть независимо проверен каждым пользователем в сети блокчейн. Затем объединив начальное состояние и возможность верификации каждого блока, пользователи могут договориться о текущем состоянии блокчейна. Обратите внимание, что если для пользователя были представлены две допустимые цепочки, то, по умолчанию, механизм в большинстве систем блокчейна состоит в том, что более длинная цепочка—«более» валидна и должна быть принята (это случается периодически и будет обсуждаться позже).

Затем действуют следующие свойства:

• Согласовано начальное состояние системы.

• Пользователи соглашаются о методе консенсуса, по которому блоки добавляются в систему.
• Каждый блок связан с предыдущим блоком хешем (кроме первого «генезис» блока, который не имеет предыдущего блока и обычно имеет хэш-значение всех нулей для предыдущего блока).
• Пользователи могут проверять каждый блок.

На практике программное обеспечение ноды обрабатывает все детали. Ключом к концепции блокчейн является то, что нет необходимости иметь доверенную третью сторону для предоставления состояния системы - каждый пользователь в системе может проверить целостность системы. Чтобы добавить новый блок в блокчейн, все участвующие ноды должны прийти к общему согласию в течение долгого времени, однако некоторое временное несогласие допустимо. Метод согласия (или консенсуса) должен работать даже в присутствии, возможно, вредоносных пользователей, пытающихся разрушить или взять под контроль блокчейн. В этом разделе обсуждается несколько основных моделей консенсуса, а также разрешение конфликтов.

4.1 Proof of Work консенсус модель

В модели proof of work пользователь получает право публиковать следующий блок решая сложный вычислительный пазл(головоломку). Решение этой головоломки и является “proof”(доказательством) работы которой они проделали. Головоломка спроектирована так, что решать ее сложно, но проверять валидна ли она просто. Это позволяет всем другим майнинг нодам валидировать любые предоставленные следующие блоки, и если блок не подошел головоломке, он будет отброшен. Часто используемый метод головоломки требует, чтобы хэш блока был меньше определенного значения. Затем майнинг ноды делают небольшие изменения в блок(nonce) пытаясь найти хэш блока, который отвечает требованиям. Для каждой попытки, майнинг нода должна вычислить хэш для заголовка текущего блока, что является сложным вычислительным процессом. Требуемое значение может быть изменено со временем, чтобы настроить уровень сложности, влияющий на то, как часто публикуются блоки. Например, Биткойн, который использует POW, настраивает сложность головоломки каждые две недели, чтобы влиять на скорость публикации блока примерно один раз в десять минут.

Важным аспектом этой модели является то, что проведенная работа с головоломкой, не влияет на ее вероятность решения будущих головоломок. Хеширование потенциального блока тысячу или один миллион раз (с разными значениями nonce) увеличивает вероятность решения только текущей головоломки (так как пространство ввода nonce уменьшается при каждом вычислении хэша),но не увеличивает вероятность решения пользователем любых будущих головоломок, и поэтому каждая головоломка для решения блока независима и требует такой же работы. Это означает, что когда пользователь получает завершенный блок от другого пользователя, они заинтересованы на включение нового блока, потому что они знают, что другие майнинг ноды будут включать его и начнут выстраивать его. Если они откажутся принять новый блок, они будут выстраивать более короткую цепочку блоков и (как упоминалось ранее), по умолчанию, будет использоваться самая длинная действующая цепочка.

В качестве примера рассмотрим головоломку, где, используя алгоритм SHA-256, компьютер должен найти хэш-значение, удовлетворяющее следующим целевым критериям:

SHA256(“blockchain” + Nonce) = Hash Value starting with “**000000**”

В этом примере, текстовая строка: “blockchain” добавляется с nonce значением и затем вычисляется хэш-значение. Используемые значения nonce будут только числовыми значениями. Это довольно простая головоломка для решения, и некоторые результаты выборки следующие:

SHA256("blockchain0") = 678
0xbd4824d8ee63fc82392a6441444166d22ed84eaa6dab11d4923075975acab938 679
(not solved)

SHA256("blockchain1") = 681
0xdb0b9c1cb5e9c680dfff7482f1a8efad0e786f41b6b89a758fb26d9e223e0a10 682
(not solved)
…
SHA256("blockchain10730895") =
0x000000ca1415e0bec568f6f605fcc83d18cac7a4e6c219a957c10c6879d67587 686
(solved)

Чтобы решить эту загадку, потребовалось 10 730 896 попыток (завершено за 54 секунды на относительно старом оборудовании, начиная с 0 и тестируя одно значение за раз). Однако каждое дополнительное значение-«ведущий ноль» увеличивает сложность. Увеличивая цель на один дополнительный начальный нуль («**0000000**»), то же оборудование сделало 934,224,175 попыток для решения головоломки (завершено за 1 691 час, 18 минут, 12 секунд):

SHA256("blockchain934224174") =
0x**0000000**e2ae7e4240df80692b7e586ea7a977eacbd031819d0e603257edb3a81

Для этого процесса нет легких путей, майнинг ноды должны затрачивать вычислительные усилия, время и ресурсы, чтобы найти правильное значение nonce для цели.

После того, как пользователь выполнил эту работу, они отправляют свой блок с валидным nonce в другие ноды сети. Ноды-получатели подтверждают, что эта работа была выполнена правильно, добавляют блок в свою копию блокчейн и повторно отправляют блок на их peer ноды. Таким образом, новый блок быстро распространяется по всей сети участвующих нод. Верификация nonce проста, потому что нужно чтобы был сделан только один хеш, чтобы проверить, решает ли он головоломку.

POW модель консенсуса разработана для случая, когда доверие пользователей к системе практически отсутствует. Она гарантирует, что майнинг ноды не могут играть с системой[3], всегда имея возможность решать головоломки и тем самым управлять блокчейном и транзакциями, добавленными к ней. Тем не менее, основным недостатком POW модели консенсуса является чрезмерное использование энергии в решении головоломок. Это не тривиально, например, в настоящее время Биткойн-блокчейн использует больше электричества, чем вся Ирландия, и было высказано предположение, что он будет потреблять там много электроэнергии как вся Дания к 2020 году [7] [8] [9]. Программное обеспечение и оборудование постоянно совершенствуются, в результате чего головоломки могут быть решены более эффективно, но блокчейн сети растут, а задачи головоломок усложняются по мере того, как увеличивается число участвующих майнинг нод.

Из-за растущей трудности головоломок POW , становится все труднее для любого компьютера решить головоломку в одиночку. Таким образом, майнинг ноды организовали себя в «пулы» или «коллективы», посредством которых они вместе решают головоломки. Это связано с тем, что можно распределять работу между двумя или несколькими нодами в коллективе для совместного распределения рабочей нагрузки и вознаграждений. Разбивая примерную программу на четверти, каждая нода может принимать равное количество диапазонов значений nonce для проверки:

- Node 1: check nonce 0000000000 to 0536870911 717
- Node 2: check nonce 0536870912 to 1073741823 718
- Node 3: check nonce 1073741824 to 1610612735 719
- Node 4: check nonce 1610612736 to 2147483647

Следующий результат, был первым найденным для решения головоломки:

SHA256("blockchain1700876653") = 722
0x**0000000**3ba55d20c9cbd1b6fb34dd81c3553360ed918d07acf16dc9e75d7c7f

Это совершенно новый nonce, тот, который решил загадку. На это потребовалось 90 263 918 попыток(догадок)(завершено за 10 минут, 14 секунд). Распределение работы среди многих других машин дает гораздо лучшие результаты, а также более последовательные награды в POW модели.

3 Используйте правила и процедуры, предназначенные для защиты системы, чтобы фактически управлять системой для получения желаемого результата.

4.2 Proof of stake модель консенсуса

Proof of stake модель консенсуса основана на идее о том, что чем больше ставка[4] у пользователя в системе,
тем скорее, она захочет, чтобы система преуспела, и тем менее вероятно, что она захочет подорвать ее. Блокчейн системы Proof of stake используют количество ставок (долей), которые пользователь имеет в качестве определяющего фактора для создания новых блоков. Методы, по которым система блокчейн использует ставки, могут различаться: от случайных выборов статичных пользователей до голосования с участием многочисленных заинтересованных сторон и до устаревающих систем монет. Вне зависимости от конкретного подхода, пользователи с большей ставкой с большей вероятностью будут создавать новые блоки.

С помощью этой модели консенсуса нет необходимости выполнять ресурсоемкие вычисления (время, электричество, мощность обработки), как это в POW. Поскольку этот консенсусный метод использует меньше ресурсов, некоторые блокчейны решили отказаться от награды за создание нового блока. Эти
системы разработаны таким образом, что все криптовалюты уже распределены среди пользователей, нежели новые монеты генерируются с постоянными темпами.

В рамках POS системы, где выбор создателя блока является случайным выбором (иногда называемое *Chain-based proof of stake*), система блокчейн будет смотреть на всех пользователей со ставками и выбирать среди них на основе их доли в общем соотношении котировок. Итак, если

у пользователя было 42% доли, они будут выбраны в 42% случаев; те, у кого 1%, будут выбраны в 1% случаев.

Когда выбор создателя блока представляет собой систему с несколькими раундами (иногда называемая *Byzantine Fault Tolerance proof of stake*[10]), появляется сложность. Система блокчейн выберет несколько stake пользователей для создания предлагаемых блоков. Затем система спросит всех staked пользователей голосовать за следующий блок. После нескольких раундов этого голосования будет определен новый блок. Этот метод позволяет всем staked пользователям иметь голос для каждого нового блока в процессе выбора блока.

Наконец, существует PoS метод, который позволяет пользователям создавать блоки «тратами» старой криптовалюты (иногда называемый «возрастом монеты» coin age PoS). Пользовательская staked криптовалюта имеет дополнительное «возрастное» свойство и через определенное количество времени (например, 30 дней) фиксированная криптовалюта может быть «потрачена» и позволяет пользователю создать новый блок на блокчейне. Затем «возраст» «потраченной» криптовалюты сбрасывается до 0, и его нельзя использовать снова, пока не пройдет необходимое время. Этот метод позволяет пользователям с большей ставкой(stake) создавать больше блоков, но не доминировать над системой - так как у них есть таймер восстановления, прикрепленный к каждой криптовалюте потраченный на создание блоков.

По системам PoS, «богатые» могут легче получить больше средств от цифровых активов, заработав
больше активов; однако, это дорого получить большинство активов в рамках системы, чтобы «контролировать».

4.3 Round-robin консенсус Модель

В некоторых блокчейн системах существует определенный уровень доверия между майнинг нодами. В этом случае нет необходимости в сложных консенсусных механизмах для определения того, кто из участников добавляет следующий блок в цепочку. Эта модель консенсуса часто используется для приватных цепочек и называется round robin, где ноды поочередно создают блоки. Для обработки ситуаций, когда
Майнинг нод недоступен, эти системы, когда наступает их очередь, могут включать элемент случайности, позволяющий доступным узлам публиковать блоки, так, что недоступные узлы не будут вызывать остановки в производстве блоков. Эта модель гарантирует, что не только один единственный нод создает большинство блоков. Эта модель выигрывает от простого подхода, в ней мало криптографических головоломок и требует меньше мощностей.

К сожалению, из-за необходимости некоторого уровня доверия между нодами, round robin не работает хорошо в permissionless(инклюзивных) открытых сетях, используемых большинством блокчейн криптовалют, потому что вредоносные ноды могут непрерывно добавлять дополнительные ноды для увеличения коэффициентов подрыва сети.

4.4. Конфликты и решения реестра

Как обсуждалось ранее, есть возможность, что несколько блоков будут опубликованы примерно в одно и то же время. Это может привести к тому, что различные версии блокчейна могут

существовать в любой момент. Это должно быть быстро решено, чтобы была последовательность в блокчейне. В этом параграфе мы обсудим, как справляются с этими ситуациями.

В любой распределенной сети некоторые системы внутри сети будут отставать от информации или иметь альтернативную информацию. Это зависит от задержки сети между нодами и близостью групп нодов. Блокчейн системы, которые позволяют любому ноду генерировать блоки, более предрасположены к
конфликтам из-за своей открытости. Большая часть согласия по состоянию блокчейн системы (достижение консенсуса) - это разрешение противоречивых данных.

Например, если node_A создает block_n (A) и распределяет его по нескольким пирам, а node_B создает block_n (B) и распространяет его на некоторых пиров, будет конфликт. block_n не будет одинаковым по всей сети. Этот конфликт показан на рисунке 11, реестр node_a находится в
красном, а node_b - в синем. Каждый из них сделал block_n, но каждый имеет разные транзакции внутри них (block_n (A) содержит транзакцию 3, но не транзакцию 4, а block_n (B) содержит транзакцию 4, но не транзакцию 3).

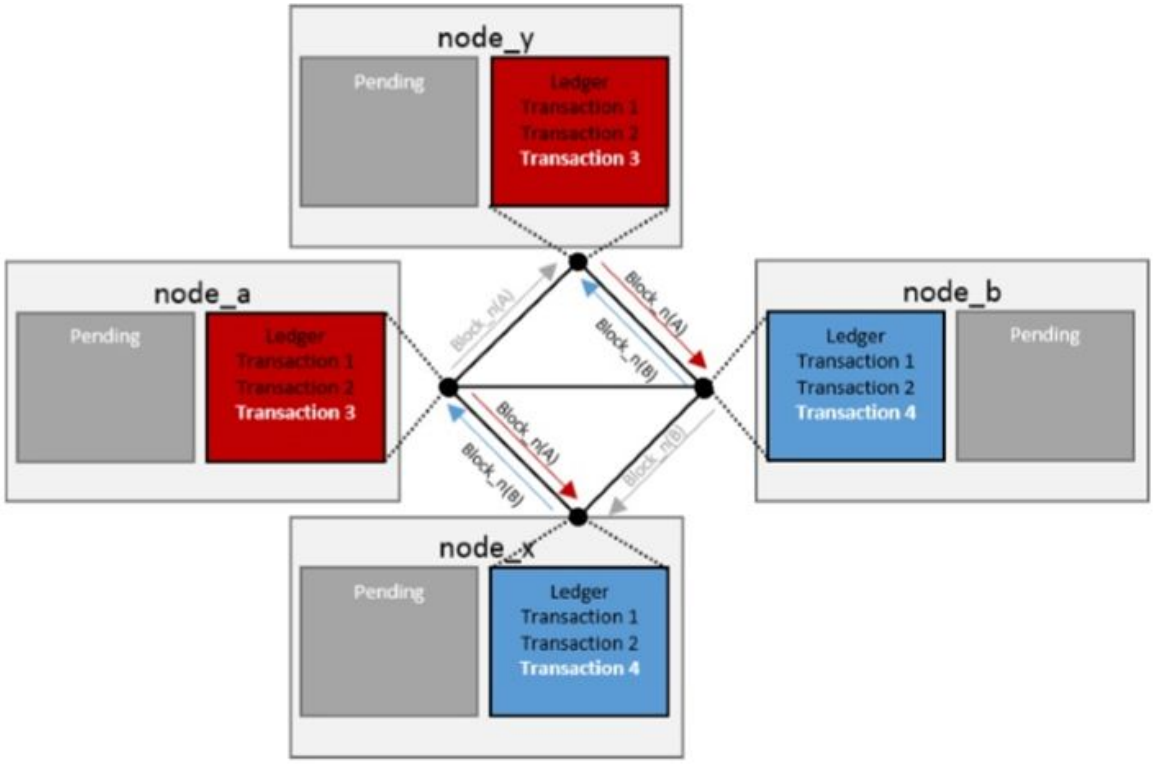


Рисунок 10: Распределенная сеть в конфликте

Конфликты временно генерируют разные версии блокчейна, которые изображены на рисунке 11. Эти разные версии не являются «неправильными»; скорее, они были созданы с информацией, которая была доступна ноду. Конкурирующие блоки, вероятно, будут иметь разные транзакции в пределах списка транзакций, поэтому те, у которых есть block_n (A), могут видеть перенос цифровых активов, отсутствующими в block_n (B). Если блокчейн имеет дело с цифровой

валютой, деньги могут быть потрачены и нет, в зависимости от того, какая версия блочной цепи просматривается.

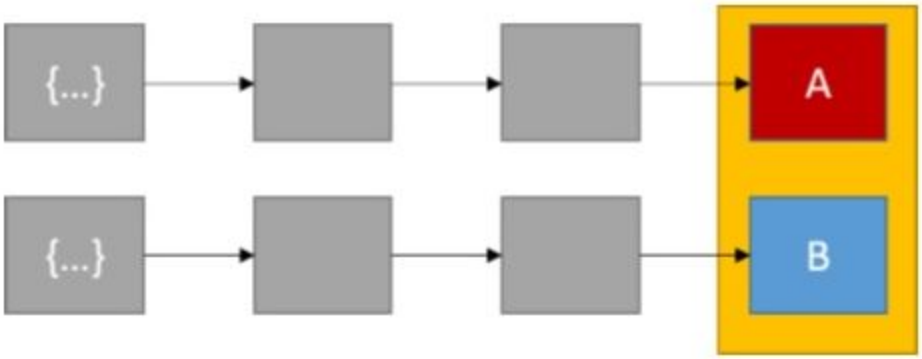


Рисунок 11: Блокчейн в конфликте

Конфликты обычно быстро устраняются. Большинство блочных систем будут ждать, пока следующий блок не будет сгенерирован и будет использовать эту цепочку как «официальный» блокчейн, тем самым приняв «более длинный блокчейн». Как и на рисунке 12, синий блокчейн становится «официальной» цепью, так как он получил следующий валидный блок. Любая транзакция, которая присутствовала в цепочке, не была выбрана и не присутствует в новом «официальном» блокчейне, возвращается в неиспользованный пул транзакций. Обратите внимание, что этот набор ожидающих транзакции поддерживается локально на каждом ноде (в архитектуре нет центрального сервера).

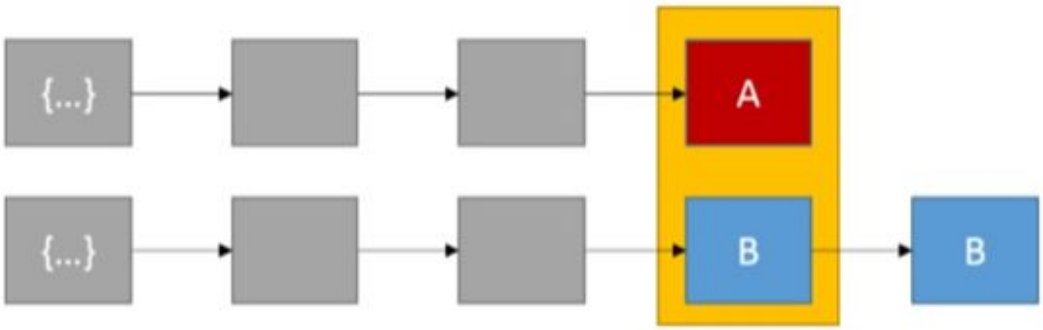


Рисунок 12: Цепочка B добавляет следующий блок

5 Форкинг

Технология обновления может быть сложной даже в самые лучшие времена, например, когда системы централизованы. Когда система состоит из множества пользователей, распределенных по всему миру и управляемых консенсусом пользователей, она становится чрезвычайно сложной. Изменения в программном обеспечении блокчейн и реализация называется форками.

5.1 Софт форки

Софт форк - это изменение технологии, которая **не** избавит пользователей, которые не принимают изменение (например, обновление до последней версии) от использования измененной системы блокчейна. Поскольку не обновленные ноды будут распознавать новые блоки как валидные, софт форк может быть обратно совместим, только требуя, чтобы *большинство* нодов обновлялось для обеспечения соблюдения новых правил софт форк.

Пример софт форк произошел в биткойне, когда было добавлено новое правило консенсуса для поддержки escrow[5] и time-locked refunds. В 2014 году было предложено переделать код операции который не выполнял операции (OP_NOP2) по CHECKLOCKTIMEVERIFY, который позволяет output(выход) транзакций сделать непотрачиваемым в будущем[11]. Для будущих клиентов, которые реализовают это изменение, переводчик(interpreter) блокчейн выполнит эту новую операцию, но для клиентов, которые не поддерживают изменение, скрипт по-прежнему действителен, и выполнение будет продолжаться, как если бы NOP[6] был выполнен.

5.2 Жесткие форки

Жесткий форк -- это изменение технологии, которая полностью избавит пользователей, которые не принимают ее от использования измененной системы блокчейн.
Под жестким форком, блокчейн протокол изменится таким образом, что заставит пользователей либо обновляться, либо оставаться с «основной форк» разработчика или продолжить исходный путь без обновлений. Пользователи на разных жестких форках не могут взаимодействуют друг с другом. Любое изменение структуры блока, такое как алгоритм выборочного хеширования, потребует жесткого форка.

Известный пример жесткого форка- это Эфириум. В 2016 году смарт-контракт построенный на Эфириуме под названием Децентрализованная автономная организация (DAO). Из-за недостатков в том, как был построен смарт-контракт, злоумышленник извлек Эфир, криптовалюту, используемую Ethereum, по сути, позволяя кражу $ 50 миллионов [12]. За предложение жесткого форка было проголосовано держателями Ether, и 89 процентов согласились с жесткой вилкой и создали новую версию блокчейн, который вернул украденные средства.

5 Средства, размещенные в третьей стороне для распространения на основе условий (посредством транзакций с несколькими подписями)

6 NOP означает отсутствие операции

С криптовалютами, если есть жесткий форк и разделения блокчейнов, монеты которые имеет каждый человек во время разделения, будут отображаться на каждом форке. Если вся деятельность переходит к новой цепочке, старая в конечном итоге не будет использоваться. В случае жесткого форка Ethereum, подавляющее большинство поддержки переместилась на новую вилку, а старая вилка была переименована в Ethereum Classic, у которой есть всего лишь часть исходной базы пользователей.

5.3 Криптографические изменения и форки

Если в криптографических технологиях обнаружены недостатки для использования блокчейна, единственым решением может быть создание жесткого форка, в зависимости от значительности недостатка. Например, если недостаток был обнаружен в основных алгоритмах, тогда форк будет требовать от всех будущих клиентов использовать более сильный алгоритм. До тех пор, пока более 50 процентов сети на новом программном обеспечении версии, уязвимость все еще может существовать. Переход на новый алгоритм хеширования может представлять собой значительную практическую проблему, поскольку она может аннулировать все существующее специализированные майнинг оборудование.

Гипотетически, если в SHA-256 был обнаружен недостаток, нужен был бы жесткий форк для перехода к новому алгоритму хеширования. Блок, который переключается на новый алгоритм хеширования
будет «закреплять» все предыдущие блоки в SHA-256 (для верификации), и всем новым блокам придется утилизировать новый алгоритм хэширования. Например, Bitcoin использует хеши SHA-256, что можно легко и быстро реализовать на железе ASIC. Другие криптовалюты, такие как Ethereum, используют Keccak-256 (на основе SHA-3) [13], в то время как Litecoin использует алгоритм хэширования scrypt.

Одной возможностью по изменению криптографических функций, присутствующих в блокчейне могла бы быть разработка практической квантовой компьютерной системы, которая была бы способна
значительно ослаблять (а в некоторых случаях и выводить из строя) существующие криптографические алгоритмы.
Внутренний отчет NIST (NISTIR) 8105, Отчет о пост-квантовой криптографии [14] таблица, описывающая влияние квантовых вычислений на общие криптографические алгоритмы. Таблица 3 воспроизводит эту таблицу.

Таблица 3: Влияние квантового компьютера на общие криптографические алгоритмы

Криптографический алгоритм	**Тип**	**Цель**	**Влияние широкомасштабного Квантового компьютера**
AES	Симметричный ключ	Шифрование	Нужен ключ большего размера
SHA-2, SHA-3	Нет данных	Хэш-функции	Нужен больший выход
RSA	Открытый ключ	Подписи, создание ключа	Больше не безопасно
ECDSA, ECDH (Elliptic Curve Cryptography)	Открытый ключ	Подписи, обмен ключа	Больше не безопасно

DSA (Finite Field Cryptography)	Открытый ключ	Подписи, обмен ключа	Больше не безопасно

Криптографические алгоритмы, используемые в большинстве блокчейн технологий для пар открытых / закрытых ключей, должны будут быть заменены, если мощный квантовый компьютер станет реальностью. Это связано с тем, что алгоритмы, которые полагаются на вычислительную сложность целочисленной факторизации (например, RSA) или работают над решением дискретных логарифмов (таких как DSA и Diffie-Hellman), очень восприимчивы к квантовым вычислениям. Алгоритмы хеширования и дерево Меркла, которые являются другим основанием для блокчейнов, намного менее восприимчивы к атакам квантовых компьютеров, но все еще ослаблены, когда квантовые компьютеры станут реальностью.

6 Смарт контракты

Смарт контракт - это набор кода и данных (иногда называемых функциями и состоянием) который размещается в блокчейне (например, Ethereum). Будущие транзакции, отправленные в блокчейн, могут затем отправлять данные общедоступным методам, предлагаемыми смарт контрактом. Контракт выполняет соответствующий метод с предоставленными пользователем данными для выполнения обслуживания. Код, находящийся на блокчейне, является неизменным и поэтому может использоваться (среди прочих целей) в качестве доверенной третьей стороны для финансовых транзакций, которые являются более сложными, чем просто отправка средств между счетами. Смарт контракт может выполнять расчеты, хранить информацию и автоматически отправлять средства на другие счета. Ему необязательно даже выполнять финансовую функцию. Например, авторы этого документа создали смарт контракты, которые публично генерируют достоверные случайные числа [15].

На практике все майнинг ноды одновременно выполняют код смарт контракта при майнинге новых блоков. Таким образом, выполнение смарт контракта может быть более дорогостоящим, чем простые переводы средств в других криптовалютах, основанных на блокчейне. Часто пользователю, совершившему сделку по смарт контракту, придется заплатить за стоимость исполнения кода в дополнение к обычной комиссии за транзакцию.
Существует ограничение на то, сколько времени исполнения может быть использовано при вызове смарт контракта. Если этот предел превышен, выполнение прекращается и транзакция отбрасывается. Этот механизм не только вознаграждает майнеров за выполнение кода смарт-контракта, но также защищает от злоумышленников, которые хотят внедриться и получить доступ к интеллектуальным контрактам, чтобы произошел отказ в обслуживании на майнинг нодах, потому что они будут потреблять все ресурсы (например, используя бесконечные циклы).

7 Категоризация блокчейн

Блокчейны обычно категорированы по permission модели, которая определяет, кто может получить доступ к ней. Если кто угодно может читать и писать в блокчейн, то он является permissionless(инклюзивный, общедоступный). Если только определенные пользователи может читать и писать в нем, то это permissioned(эксклюзивный) блокчейн. Простыми словами, эксклюзивный блокчейн это как корпоративный интранет, который контролируется, а permissionless (инклюзивный) это как общедоступный интернет, в котором могут участвовать кто угодно.

7.1 Эксклюзивный (permissioned)

Эксклюзивные блокчейны бросают вызов первоначальной концепции блокчейн биткойна, где каждый может читать и писать в блокчейн, а реестр является прозрачным / общедоступным. Организации, которые хотят работать вместе, но не доверяют полностью друг другу, могут создать эксклюзивный блокчейн и пригласить деловых партнеров для записи своих транзакций в общий распределенный реестр. Этот эксклюзивный блокчейн может иметь одинаковую прослеживаемость активов, поскольку они проходят через блокчейн, а также одну и ту же распределенную, устойчивую и резервную систему хранения данных в виде блокчейна. Эти организации могут определять используемый консенсусный механизм в зависимости от того, насколько они доверяют друг другу.

Permissioned блокчейны могут быть настроены так, чтобы каждый мог их прочитать, но только выбранные участники могут записывать на них транзакции. Этот тип блокчейна обеспечит полное понимание внутренних взаимодействий организации любым, у кого есть интерес, но общественность в целом не сможет вмешиваться в данные. Эксклюзивные блокчейны также могут быть настроены так, чтобы каждый мог записывать транзакции на блокчейн, но только выбранные члены могут читать данные.

7.1.1 Рассмотрение аспектов эксклюзивных блокчейнов

Хотя эксклюзивные блокчейны часто рассматриваются как улучшение по сравнению с текущими системами, некоторые конструктивные характеристики должны быть тщательно рассмотрены для обеспечения безопасности. Например, когда используя базу данных, можно иметь детальную грануляцию разрешений, например, позволяя определенным пользователям выполнять определенные запросы или разрешать отдельным пользователям писать только в определенные таблицы.

Приложениям, использующим блокчейн, может потребоваться определить достаточно ли разрешения, поддерживающиеся блокчейном гранулярны для создания достаточного количества ролей в системе (разрешения позволяют использовать более традиционные роли, такие как администратор, пользователь, валидатор, аудитор и т. д.).

Это также относится к тому, как разрешения управляются. Как только пользователь получает доступ на запись в блокчейн можно ли отменить это разрешение? Большинство реализаций блокчейн являются неизменными, что может сделать разрешения более сложными.

Доверие - еще один критический фактор при принятии решения о создании приложения на блокчейне.

В рамках эксклюзивного блокчейна метод консенсуса, как правило, менее вычислительно интенсивен, поэтому есть возможность, что пользователи могут действовать злонамеренно. Однако доверие не должно распространяться на всех пользователей. Управляющий блокчейном может обозначить ограниченный набор майнинг нодов. Если они заслуживают доверия, тогда нет

необходимости в том, чтобы в целом все пользователи были заслуживающими доверия, поскольку майнеры будут применять правила блокчейна.

Еще один важный фактор состоит в том, что он имеет очевидный дизайн. Если злонамеренный майнинг нод попытался изменить блок, он может, например, подделать транзакцию, чтобы дать себе деньги.
Будет ли обнаружено такое изменение? Существуют ли системы для определения того, что произошло?

Неизменность важна и является одним из основополагающих принципов блокчейна. В целом, вредоносные транзакции, входящие в цепочку, не могут быть отменены, даже если они идентифицированы. Для этого требуется переписать опубликованные блоки, которые по существу разрывают блокчейн и требуют одобрения большинства майнинг нодов. В эксклюзивной системе это может быть проще, поскольку майнинг ноды обычно представляют собой доверенный набор, который имеет особые отношения. Это гораздо сложнее, но технически возможно, для инклюзивных систем, таких как биткойн.

7.1.2 Примеры использования

В следующих разделах представлены примеры использования (неисчерпывающий список). Включение или исключение из этого раздела не значит подтверждение или признание недействительным какого-либо потенциального случая.

Банковское дело

Предположим, что несколько банков хотят иметь доступный частный, распределенный реестр только для участвующих банков. Это обеспечило бы возможность записи транзакций из каждого банка способом, который видим для участников, но не для общественности. Однако, чтобы сделать это как закрытый блокчейн (чтобы избежать необходимости использовать дорогостоящий Proof of work алгоритм), каждый банк по очереди подписывает блоки по распределенному консенсус-алгоритму, как Byzantine Paxos [16].
Есть несколько интересных замечаний, которые надо учесть при использовании закрытого блокчейна с несколькими участниками, такие как возможность преодолевать его неизменность. Если бы была какая-то серьезная ситуация с бедствиями или исключительными случаями, банки могли бы скоординироваться, чтобы откатить блокчейн и записать другую транзакцию. Кроме того, транзакции не будут анонимными, потому что для присоединения потребуется банковский идентификатор.

Цепочка поставок

Запись трансфера физических товаров от производителя, в терминал доставки, на судно, в грузовой поезд, на грузовик и в магазин является привлекательным применением технологии блокчейнов. Блокчейн может сыграть решающую роль в доверии и прозрачности с конечными клиентами.
Блокчейн также может использоваться для контроля действий поставщиков. Поставщики могут записывать произведенный продукт (например, X количество виджетов на определенную дату) таким образом, чтобы другие наблюдатели блокчейна могли проверить. Благодаря блокчейну можно эффективно управлять логистикой, избегая затоваривания.

Страхование и здравоохранение

Всякий раз, когда кто-то посещает поставщика медицинских услуг, за кулисами происходит множество транзакций.
Административные операции со стороны медсестер, врачей, персонала, медицинских работников, страховых компаний и аптек могли быть записаны в блок-цепь. Транзакции (такие как проверка льгот, права на получение, покрытие и доступное лекарственное обеспечение) могут быть прочитаны из блокчейна.

В настоящее время записи этих транзакций находятся в разрозненных системах, получая результаты в конце (часто ручного) процесса.

7.2 Инклюзивный (permissionless)
Инклюзивные блокчейны - это децентрализованные платформы без централизованного управления, которые открыты для участия без запроса на доступ к пользователям. Инклюзивные блокчейны часто используют метод консенсуса, который требует приложить больше нетривиальных усилий, чтобы предотвратить возможность системе быть разрушенной плохими юзерами. Такие консенсусные методы включают proof of work и proof of stake. Причина, по которой инклюзивный блокчейн может работать, заключается в том, что за участие в этом процессе есть вознаграждения.

7.2.1 Замечания по применению для инклюзивных блокчейнов
При принятии решения о том, следует ли использовать инклюзивный блокчейн, нужно учитывать, нужны ли приложения следующие качества:

• **Данные, связанные с общественностью** – Поскольку инклюзивные реестры, как правило, позволяют кому угодно проверять и вносить свой вклад в блокчейн, данные, как правило, являются общедоступными. Должны ли данные для приложения быть доступными для всех? Есть ли вред в том, чтобы данные были публичны?
• **Полная история транзакций** – Благодаря открытому характеру данных для этих систем каждый может отслеживать передачу активов между счетами, от создания активов до каждой совершенной транзакции.
• **Попытки ввода ложных данных** – Поскольку любой может внести вклад в блокчейн, некоторые могут отправлять ложные данные в блокчейн, имитируя данные из достоверных источников. Есть ли для приложения способ обеспечения того, чтобы оно собирало только данные из авторитетных источников?
• **Неизменяемость данных** – Многие приложения следуют «CRUD» (создавать, читать, обновлять, удалять) функции для данных. В ситуации с блокчейном существует только «CR» (создание, чтение). Существуют
методы, которые можно использовать для «обесценивания» старых данных, если найдена более новая версия, но процесс удаления для исходных данных отсутствует. Может ли приложение обрабатывать (возможно устаревшие) неизменяемые данные? Предоставляют ли данные данные о неизменности?
• **Транзакционная пропускная способность** – В настоящее время транзакции по блокчейну не проводятся в том же темпе, что и другие решения (например, блоки не добавляются достаточно быстро), поэтому может произойти некоторое замедление при ожидании публикации данных. Может ли приложение обработать это?

7.2.2 Примеры вариантов использования

В следующих разделах представлены примеры использования (не исчерпывающий список). Включение или исключение из этого раздела не подтверждают или подтверждают какой-либо потенциальный прецедент.

Доверие электронной отметке времени

Доверие электронной отметке времени - это способ доказать, что определенная информация существовала в данной точке [17].

Использование блокчейна позволяет стороне доказать, что они имели доступ к части данных таким образом, который не может быть отменен. Например, если человек хотел доказать, что у него был файл, они могли бы хэшировать файл и записать хэш-значение в качестве аннотации к транзакции. Затем, если ему или ей когда-либо понадобится доказать владение файлом, он записан публично.

Другие варианты использования timestamping (отметка времени) на блокчейне включают в себя подтверждение того, что задание было завершено в определенную дату, подтверждение владения фотографией, подтверждение того, что контракт был подписан, или подтверждение произошедших событий.

Энергетическая промышленность

Еще одним применением блокчейна является запись автономных, межкомпьютерных транзакций, связанных с использованием электроэнергии [18]. Это позволит использовать возможности цифровых платформ и изменять бизнес-модели для отслеживания транзакций на "умной" электросети. Одним из примечательных вариантов использования блокчейна в энергетической отрасли является регистрация сертификатов. Существуют различные электростанции, вырабатывающие энергию и создающие сертификаты, свидетельствующие о количестве энергии, производимой для последующего обмена. В настоящее время существуют проблемы, такие как сертификаты выбросов, которые проводятся дважды, а также необходимость решения проблем регулирования и обеспечения более равномерного доступа для всех на рынке. Блокчейн может эффективно отслеживать выпуск и расходование этих энергетических сертификатов.

Другим примером того, как блокчейны применимы в энергетической отрасли, является торговля избыточной возобновляемой энергией. Здания могут быть подключены к устройствам, использующим энергию, и записывающие их на блокчейн, что позволяет продавать и покупать избыточную энергию на рынке.

8 Блокчейн Платформы

Многие блокчейны используются сегодня, прежде всего для решений в сфере цифровой валюты. В этом разделе обсуждается выбор блокчейн платформ, чтобы выделить технические различия и используемые подходы. Это не поддержка ни одной из этих платформ, и это не должно толковаться как список наиболее популярных или важных платформ.

8.1. Криптовалюты

Многочисленные применения технологий блокчейн в первую очередь ориентированы на перемещение валюты с одной учетной записи на другую. В этом разделе описывается несколько примеров таких блокчейн приложений.

8.1.1 Биткойн (BTC)

Биткойн - это система цифровой валюты, которая ранее обсуждалась как пионер в использовании блокчейна. Новые блоки создаются примерно раз в 10 минут, используя хеширование SHA-256, чтобы связать их вместе. Это PoW система, в которой майнинг ноды должны найти nonce для включения в свой блок, чтобы хэш блока был меньше некоторого предопределенного значения сложности. Трудность корректируется вверх или вниз, чтобы попытаться достичь 10-минутной цели для создания блока. Раньше в истории Биткойна отдельные компьютеры могли создавать и публиковать блоки, в настоящее время Bitcoin требует специализированного оборудования, крупных центров обработки данных или многих людей, работающих вместе в майнинг пуле, чтобы выиграть конкуренцию на публикацию блоков.

С Bitcoin оплата транзакционных сборов технически опциональна, поскольку майнинг ноды получают большую часть своих средств за счет публикации блоков. Эта комиссия рассчитана на небольшую плату за каждую транзакцию, но она может стать, и стала значительной из-за существенного отставания от ожидающих транзакций. Оплата более высокой комиссии за транзакцию может дать транзакции более высокий приоритет для добавления в блокчейн. Первоначально майнинг ноды получали 50 биткоинов за каждый блок, и только половина из них после определенного количества блоков. Например, вознаграждение за разработку блока составляло 12,5 биткоинов в июле 2016 года. По протоколу Биткоин эта награда будет сокращаться вдвое за каждые 210 000 блоков (около четырех лет) и будет уменьшаться до нуля, когда будет произведен 21 миллион биткойнов [19]. Биткойн майнинг будет продолжаться в этот момент, но вознаграждение будет полностью вытекать из транзакционных сборов.

Одним из последних технических замечаний,которое стоит принять во внимание это то, что каждая транзакция Bitcoin содержит код, написанный на языке Script. Этот код представляет собой простую программу, которая определяет транзакцию. Он не содержит циклов и сильно ограничен в отношении функциональности (т. е. это Turing complete system[8]). Биткойн-транзакции сегодня используют лишь небольшую часть доступных функций Script.
На практике большинство транзакций биткойнов используют один из нескольких шаблонов кода для перемещения средств между сторонами.

7 Веб-сайт Map of Coins (http://mapofcoins.com/) представляет собой хороший пример целого ряда блокчейнов, но пока далеко не полный список
8 A Turing complete system (компьютерная система, язык программирования и т. д.) Может быть использована для любого алгоритма, независимо от сложности, для поиска решения.

8.1.2 Bitcoin Cash (BCC)

В июле 2017 года примерно 80-90 процентов вычислительной мощности Bitcoin проголосовали за то, чтобы
включить Segregated Witness (SegWit, где транзакции разделены на два сегмента: транзакционные данные и данные подписи), что позволило уменьшить количество данных, проверяемых в каждом блоке. Данные подписи могут составлять до 65 процентов транзакционного блока, поэтому может быть полезно изменение в способах реализации подписей. Когда SegWit был активирован, это

вызвало жесткий форк, и все майнинг ноды и пользователи, которые не хотели менять, начали называть исходную биткойн блокчейн Bitcoin Cash (BCC). Технически, биткойн - это форк, а Bitcoin Cash - это исходный блокчейн. Когда произошел жесткий форк, у людей был доступ к тому же количеству монет на Bitcoin и Bitcoin Cash.

8.1.3 Litecoin (LTC)

Litecoin вдохновлен биткоином и очень похож на него, но стремится обеспечить более быстрое время подтверждения. Litecoin реализовал SegWit, разделив транзакции на два сегмента и скрыв увеличенный размер блока [20]. Подпись «свидетеля» отделена от дерева Меркла. Еще одна разница между Bitcoin и Litecoin заключается в том, что Litecoin использует алгоритм Scrypt для хэширования вместо SHA-256. Алгоритм Scrypt сложнее решить, чем SHA-256, поскольку он использует больше памяти, что затрудняет разработку обычных интегральных схем специального назначения (ASIC). Существует большее количество монет, которые можно майнить (84 миллиона Litecoins). Litecoin является дополнением к биткойну с более высокими объемами транзакций и не предназначен для его замены [21].

8.1.4. Ethereum (ETH)

Ethereum - блокчейн платформа, ориентированная на предоставление смарт контрактов. Смарт контракты - это программы, которые существуют на блокчейне, к которым могут получать доступ пользователи Ethereum. Они могут получать и отправлять средства во время вычислений любой сложности. Правильно разработанный контракт может выступать в качестве доверенной третьей стороны в финансовых транзакциях, поскольку его код является открытым и неизменным. Язык программирования транзакций Ethereum полный по Тьюрингу. Майнинг ноды получают средства за счет майнинг и транзакционных платежей.

Ethereum также имеет понятие «газ», используемое для управления транзакционными вычислениями (и обычно составляет около 1/100 000 эфира). Каждая транзакция поглощает газ по мере его выполнения, а отправитель конкретной транзакции должен платить необходимый газ или транзакция будет прекращена. Максимальный газовый предел для каждого смарт контракта (в настоящее время - три миллиона газа), существует для того, чтобы не допустить, чтобы дорогостоящие программы были отправлены на майнинг ноды Ethereum. Это связано с тем, что все майнинг ноды должны выполнять транзакции параллельно [22].
Добавление транзакции к контракту Ethereum заставляет программу запускаться параллельно на компьютерах майнинг нодов. Полученное состояние контракта хранится на блокчейне пользователем, который публикует следующий блок.

8.1.5 Ethereum Classic (ETC)

Ethereum Classic был создан, когда произошел хардфорк Ethereum после взлома DAO [12]. Злоумышленник вывел около 50 миллионов долларов, и Ethereum Foundation создал хардфорк, чтобы вернуть украденные средства обратно до состояния, которое было до атаки. Пользователи, которые владели Ethereum перед хардфорком DAO, имели такое же количество Ethereum Classic (ETC) после форка. Причина, по которой она существует, состоит в том, что ряд пользователей блокчейна Ethereum отклонил форк по философским соображениям [23], включая принцип, что блокчейн не может быть изменен, и решили продолжать использовать оригинальную блокчейн Ethereum. Майнинг и программное обеспечение во многом одинаковы между Ethereum и Ethereum Classic, с той разницей, что Ethereum является форком и более популярной цепью.

8.1.6 Dash (DASH)

Dash - это криптовалюта, созданная с целью обеспечения более быстрых транзакций. Он использует сеть «masternode» и может совершать транзакции в течение четырех секунд [24]. Dash использует детерминированное упорядочение для мастернодов, используя хэш и PoW для каждого блока.

Интересно, что для того, чтобы стать мастернодом требуется залог в 1000 Dash, что делает это очень дорогостоящим (почти невозможным) для управления более чем 50 процентами сети [25]. Требование обеспечения залога для мастернодов стремится снизить проблемы ненадежных нодов в peer-to-peer сети.

Dash использует другой алгоритм хеширования, чем большинство, x11. Это состоит из использования всех 11 учавствующих алгоритмов SHA-3 (включая BLAKE, JH, Keccak и Skein), причем каждый хэш передается следующему алгоритму в цепочке [25]. Причиной тому является то, что использование нескольких алгоритмов усложняет создание ASIC, который нацелен на решение этих хэшей на аппаратном обеспечении.

8.1.7 Ripple (XRP)

Ripple - это название как криптовалюты, так и платежной сети, по которой она передается. Цель Ripple – строится на подходе Bitcoin и объединяет различные платежные системы. Он имеет фиксированный запас в 100 миллиардов XRP, причем половина из них предназначена для обращения [26]. Клиентам Ripple не нужно загружать целый блокчейн, что упрощает подключение клиентов за считанные секунды. Кроме того, для запуска сервера не существует вознаграждения за майнинг, поскольку каждая транзакция стоит небольшое количество Ripple, это похоже на газ Ethereum. Поэтому нет майнинг нодов или майнинг пулов, вместо этого уничтожается примерно одна тысячная процента от каждой транзакции [27]. Ripple не разрабатывается с явными целями анонимности, но у него есть функции обеспечивания конфиденциальности, например, платежные шлюзы, использующие прокси.

8.2 Hyperledger

Hyperledger - это группа проектов, направленных на создание распределенных регистров корпоративного класса с открытым исходным кодом [28]. Проект Hyperledger организован и поддерживается Linux Foundation.

Несмотря на то, что он был организован Фондом Linux, каждый проект был разработан и дополнен различными источниками. В рамках проекта Hyperledger есть несколько проектов, каждый из которых предоставляет блокчейн для решения конкретных проблем.

8.2.1 Hyperledger Fabric

Это модульный эксклюзивный блокчейн, который может запускать смарт контракты (называемые chaincode) [29].

Блокчейн Fabric был первоначально внесен в проект Hyperledger от Digital Asset и IBM.

8.2.2 Hyperledger Sawtooth

Это модульный распределенный реестр с использованием proof of elapsed time (доказательство истёкшего времени) в качестве консенсусного протокола. В системе proof of elapsed time каждый участник запрашивает «время ожидания» из hardware enclave (надежной и защищенной функции, доступной на каком-либо аппаратном обеспечении), которая распределяет время ожидания случайным образом.

Тот участник, который был награжден за самое короткое время создает следующий блок в цепочке. Использование Hyperledger Sawtooth тесно связано с оборудованием, которое поддерживает hardware enclave функцию. Hyperledger Sawtooth был первоначально предоставлен Intel'ом.

8.2.3 Hyperledger Iroha

Это действует как услуга Identity / Know Your Customer (KYC), использующая технологии блокчейн, которая позволяет организациям обмениваться данными и управлять ими. Hyperledger Iroha изначально был предоставлен Soramitsu, Hitachi, NTT Data и Colu.

8.2.4 Hyperledger Burrow

Hyperledger Burrow - это эксклюзивная блокчейн платформа с поддержкой смарт-контрактов. Он принимает код смарт контракта на основе Ethereum. Hyperledger Burrow первоначально был представлен Monax'ом и коспонсором от Intel.

8.2.5 Hyperledger Indy

Это независимая платформа идентификации, которая устанавливает происхождение доверительных транзакций и подотчетности. Он поддерживает контролируемые пользователями обмены проверяемых запросов об идентификационной информации, а также модели аннулирования. Он поддерживает три важные функции конфиденциальности: децентрализованные идентификаторы (DID), указатели на источники вне реестра, чтобы никакие личные данные не записывались в реестр, и доказательство с нулевым разглашением. Код Indy представлен Hyperledger Проектом Sovrin Foundation.

8.3 MultiChain

MultiChain - это платформа с открытым исходным кодом, которая позволяет любому пользователю устанавливать, настраивать и развертывать частный, полу-частный или публичный блокчейн. MultiChain - это форк Bitcoin, но со многими изменениями. Пользователи могут определить, должна ли быть привязанная криптовалюта, а также метод консенсуса (round robin или proof of work). В конфигурации по умолчанию MultiChain является частным, основанным на эксклюзивности блокчейном, использующий round-robin консенсус. Это означает, что первый человек, создавший блокчейн, действует как администратор и начальная нода. Все дополнительные пользователи должны направлять своих клиентов блокчейна MultiChain на этот первый узел, и администратор должен предоставить им разрешения.

MultiChain Streams [30] - уникальная функция; они описываются как «общие неизменяемые key-value базы данных временного ряда», которые хранятся на блокчейне.

9 Ограничения блокчейна и мисконцепции

Существует тенденция оверхайпу и чрезмерному использованию самой зарождающейся технологии. Многие проекты будут пытаться внедрить эту технологию, даже если она не нужна. Это связано с тем, что технология является относительно новой и не совсем понятной, или технологией, окруженной неправильными представлениями. Технология Blockchain не была защищена. В этом разделе

ограничения и заблуждения о технологии blockchain.

9.1 Управление блокчейном

Распространенное заблуждение состоит в том, что инклюзивный(общедоступный) блокчейн - это системы без контроля и владельцев. Часто восклицают фразу: «никто не контролирует блокчейн!», однако, хотя ни один пользователь, правительство или страна не контролируют блокчейн, все еще существует группа основных разработчиков, которые отвечают за разработку системы. Эти разработчики могут действовать в интересах сообщества в целом, но они по-прежнему поддерживают некоторый уровень контроля. Например, в 2013 году разработчики Bitcoin выпустили новую версию самого популярного клиента Bitcoin, который внес недостаток и начал две конкурирующие цепочки блоков. Разработчикам пришлось решить либо сохранить новую версию (которая еще не была принята всеми), либо вернуться к старой версии [31]. Любой выбор приведет к тому, что одна цепь будет отброшена, а некоторые денежные операции некоторых людей станут недействительными.

Разработчики сделали выбор, вернулись к старой версии и успешно контролировали прогресс блокчейна Биткоина. Этот пример был непреднамеренным форком, однако разработчики могут намеренно создавать новых клиентов, и с достаточным переходом из базы пользователей может быть создан успешный форк. Эти форки часто обсуждаются подробно и дается длительный период перехода, прежде чем стать обязательными для продолжения записи транзакций на новом «основном» форке.

Фраза «никто не контролирует блокчейн!» будет правильнее звучать, как «никто не контролирует, с кем и когда вы можете выполнять транзакции, в рамках правил системы блокчейн».

9.2 Вредоносные пользователи

В то время как система блокчейн может обеспечивать соблюдение правил и спецификаций транзакций, она не может обеспечить соблюдение кодекса поведения. Это проблематично в инклюзивных блокчейнах, поскольку пользователи под псевдонимами, и между нодами блокчейна и пользователями системы нет каких-либо однозначных сопоставлений. Инклюзивные блокчейны обеспечивают поощрение (например, криптовалюта), чтобы мотивировать пользователей действовать справедливо, однако некоторые могут выбирать злонамеренно, если это дает больше поощрения.

Самая большая проблема для злонамеренных пользователей - получить достаточную мощность (будь то стейк в системе, вычислительная мощность и т. д.), чтобы нанести ущерб. Когда создается достаточно большой вредоносный сговор, злоумышленные действия могут включать:

- Игнорирование транзакций у конкретных пользователей, нодов или даже целых стран.
- Создавать измененную, альтернативную цепочку в секрете, а затем добавлять ее целиком, как только альтернативная цепочка станет длиннее реальной. Честные ноды будут переключаться на цепочку, которая имеет наибольшую «работу» (по протоколу блокчейна). Это наносит удар по концепции «неизменности» в блокчейн системе [32].
- Отказ от передачи блоков другим нодам, по существу нарушающий распространение информации.

9.3 Отсутствие доверия

Другая распространенная неверная интерпретация исходит от людей, которые слышат, что нет «доверенной третьей стороны» в блокчейне, и предполагают, что системы блокчейнов являются «ненадежными» средами. Хотя и нет доверительной третьей стороны, которая сертифицирует транзакции в инклюзивных блокчейн системах (в эксклюзивных системах это менее понятно, так как администраторы этих систем действуют как администраторы доверия, предоставляя пользователям доступ и разрешения), все равно требуется большое доверие для работы в блокчейне:

• Существует доверие к используемым криптографическим технологиям. К примеру, криптографические
алгоритмы или реализации могут иметь недостатки, а смарт контракты могут иметь непреднамеренные лазейки и недостатки.
• Существует доверие к разработчикам программного обеспечения для производства программного обеспечения, которое, насколько это только возможно, не содержит багов.
• Существует уверенность в том, что большинство пользователей блокчейна не вступили в сговор в тайне. Если отдельная группа или физическое лицо может контролировать более 50 процентов всей мощности создания блоков, это может подорвать инклюзивную блокчейн систему. Однако, как правило, получение необходимой вычислительной мощности является чрезмерно дорогостоящим.
• Существует доверие к тому, что ноды принимают и обрабатывают транзакции справедливо.

9.4. Использование ресурсов

Технология Blockchain позволила использовать всемирную сеть, где каждая транзакция проверяется, а блокчейн хранится в синхронизации между множеством пользователей. Для блокчейн систем, использующих PoW, это означает, что большое количество пользователей тратят в пустую время обработки и потребляют много электроэнергии. PoW метод является отличным решением для «трудно создавать, легко проверять» доказательств, но, как обсуждалось в разделе 4.1, это требует значительного использования ресурсов.

Дополнительная нагрузка на ресурсы возникает всякий раз, когда создается новая полная нода. Нода должна получить (обычно путем загрузки) большую часть или все данные блокчейна (данные блокчейна Биткойна имеют размер более 100 гигабайт на момент написания) [33]. Этот процесс использует большую пропускную способность сети.

Блокчейны часто сравниваются с базами данных, и хотя они все хранят информацию, блокчейны имеют ограничения на объем данных, которые могут быть сохранены и не предназначены быть носителем общего хранения данных. Чтобы быстро вычислить хэши транзакций и распределить транзакции по сети, транзакции должны быть относительно небольшими. Большие объемы данных обычно хранятся в «off chain» с «pointers/references» или хешами данных, хранящихся в самом блокчейне.
Блокчейны также извлекают выгоду от того, что данные являются неизменными, что обычно не является особенностью данных общего назначения.

9.5 Передача бремени хранения учетных данных пользователям

Поскольку блокчейны не централизованы, не существует неотъемленного центрального места для управления ключами пользователя. Пользователи должны управлять своими личными ключами, то есть если он потерян, все, что связано с этим личным ключом, теряется (цифровые

активы и т. д.). Нет функции «забыл мой пароль» или «восстановить мою учетную запись» для цепочки блоков. В то время как централизованные управленческие решения могут быть внедрены, они создают те же проблемы, что и в существующих системах: центральные точки отказа.

9.6. Инфраструктура и идентификация частного / открытого ключа

Некоторые люди, услышав, что технология blockchain включает инфраструктуру открытого / закрытого ключа, немедленно верят, что она по своей сути поддерживает личность. Это не так, поскольку нет один-к-одному(OneToOne) отношения закрытых(приватных) пар ключей с пользователями (пользователь может иметь несколько закрытых ключей), а также не существует один-к-одному(OneToOne) отношения между блокчкейн адресами и открытыми ключами (несколько адресов могут быть получены из одного открытого ключа). Ноды на Биткойн блокчейне проверяют транзакции до того, как они будут добавлены в блок и впоследствии включены в блокчейн. Для одного этапа этой проверки требуется, чтобы пользователь, инициировавший транзакцию, подписал транзакцию с помощью закрытого ключа. Ноды блокчейна проверяют подпись, чтобы доказать, что пользователь действительно имеет переданное значение биткойна.

Цифровые подписи часто используются для подтверждения идентичности в мире кибербезопасности, и это может привести к путанице в отношении потенциального применения блочной цепи для управления идентификацией. Процесс проверки подписи транзакции блокчейна связывает транзакции с владельцами закрытых ключей, но не предоставляет возможности для связывания реальных личностей с этими владельцами. В некоторых случаях можно связывать личности реального мира с закрытыми ключами, но эти соединения выполняются через внешние процессы, а не явно поддерживаемые блокчейном. Например, правоохранительные органы могут требовать от биржи записей, которые связывают транзакции с конкретными лицами. Другим примером является индивидуальное размещение адреса онлайн для пожертвований.

Хотя можно использовать блокчейны в рамках управления идентификационными данными, для которых требуется компонент распределенных регистров, важно понимать, что типичные реализации блокчейн не предназначены для автономеных систем управления идентификацией. Существует больше возможностей иметь надежные цифровые идентификаторы, чем просто реализовать блокчейн.

10 Выводы

Блокчейны являются важным новым направлением в технологических достижениях, которое обеспечивает безопасные транзакции без необходимости в центральном органе. Начиная с 2009 года, с использованием Биткоином блокчейн технологии, стало возникать все большее число криптовалют на основе блокчейн. Возможно, что более важны новые приложения, выходящие за рамки валют, которые основываются на фундаментальных принципах технологии блокчейн.

Первыми приложениями были цифровые валюты с распределением глобального реестра, содержащего все транзакции. Эти транзакции обеспечены криптографическими хэшами, а транзакции подписываются и проверяются, используя пары открытых / закрытых ключей. История транзакций суммируется с деревьями Меркла, чтобы эффективно и безопасно записывать цепочку событий таким образом, чтобы любая попытка отредактировать или изменить прошлую транзакцию требовала пересчета всех последующих блоков транзакций.

Использование блокчейнов все еще находится на ранних стадиях, но оно построено на широко понятных и обоснованных криптографических принципах. Забегая вперед, вполне вероятно, что блокчейны станут еще одним инструментом, который можно использовать для решения новых задач. Финансовые организации, скорее всего, будут тем видом бизнеса, на который больше всего повлияют блокчейны . Им, возможно, придется адаптироваться или даже полностью изменить свою практику, чтобы сосредоточиться на том, чтобы быть платформами обмена ценностями, а не просто местами для хранения ценностей.

Блокчейны также оцифровывают активы, отличные от денег. Компании, которые должны хранить публичные документы, например, право собственности на землю, брак или записи о рождении, должны рассмотреть вопрос о том, как их проблемы могут быть решены с помощью технологии блокчейн. Блокчейны также имеют сильный потенциал для хранения и записи данных цепочки поставок. Блокчейн может записывать каждый шаг в жизни продукта, начиная с момента его создания на заводе, до того, как он был отправлен, а затем доставлен в магазин и, наконец, когда потребитель приобрел его. Могут появиться даже новые отрасли, такие как цифровые нотариусы, которые могут доказать, что человек имел доступ к определенной части информации, записав ее хэш в блокчейн. Существует много потенциальных сфер использования и возможностей для блокчейн технологий.

Как описано в этой публикации, блокчейн использует существующие сетевые, криптографические и учетные технологии, но использует их по-новому. Важно, чтобы организации могли смотреть на технологии, и видеть преимущества и недостатки их использования. Как только блокчейн внедряется и широко применяется, становится очень трудно изменить его без форкинга. Когда-то что-то записывается в блокчейн, это обычно происходит навсегда, даже когда есть ошибка. Для некоторых организаций это желаемые функции. Для других это могут быть срыв сделок, которые препятствуют использование блокчейна.

Технологии Blockchain способны нарушать работу многих отраслей. Чтобы избежать упущенных возможностей и нежелательных сюрпризов, организациям следует изучить, может ли блокчейн помочь им или нет.

Приложение A—Сокращения

Выбранные аббревиатуры и сокращения, используемые в этом документе, определены ниже:
ASIC Application-Specific Integrated Circuit
BCC Bitcoin Cash
BFT Byzantine Fault Tolerant
BTC Bitcoin
CPU Central Processing
Unit CR Create, Read
CRUD Create, Read, Update, Delete
DAO Decentralized Autonomous Organization
DID Decentralized Identifier
DSA Digital Signature Algorithm
ECDSA Elliptic Curve Digital Signature Algorithm
ETC Ethereum Classic
ETH Ethereum
EVM Ethereum Virtual Machine

FIPS Federal Information Processing Standard
FOIA Freedom of Information Act
GPU Graphics Processing Unit
I2P Invisible Internet Project IoT
Internet of Things
IR Internal Report
ITL Information Technology Laboratory
KYC Know Your Customer
NIST National Institute of Standards and Technology
NISTIR National Institute of Standards and Technology Internal Report
RSA Rivest-Shamir-Adleman
SegWit Segregated Witness
SHA Secure Hash Algorithm
XMR Monero
XRP Ripple

Приложение B—Глоссарий

Выбранные термины, используемые в этом документе, определены ниже.

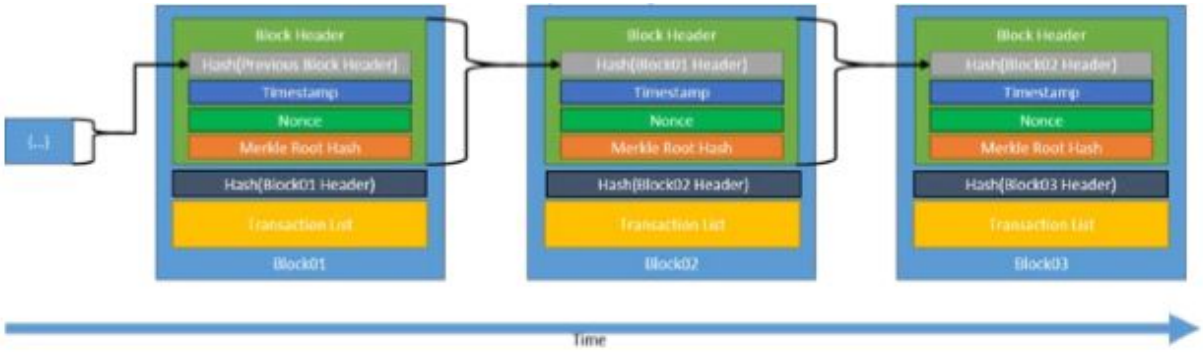
Адрес Короткая буквенно-цифровая строка, полученная из открытого ключа пользователя с использованием хэш-функции, с дополнительными данными для обнаружения ошибок. Адреса используются для отправки и получения цифровых активов.

Активы Все, что может быть передано.

Блок Набор проверенных транзакций.

Заголовок блока. Часть блока, которая содержит информацию о самом блоке (метаданные блока), обычно включающая метку времени(timestamp) для публикации блока, root хэш дерева Меркла, хэш предыдущего блока и криптографический nonce (при необходимости).

Blockchain Распределенный цифровой реестр криптографически подписанных транзакций, которые сгруппированы в блоки. Каждый блок криптографически связан с предыдущим после проверки и прошедший консенсусное решение. По мере добавления новых блоков более старые блоки становится сложнее модифицировать. Новые блоки воспроизводятся по всем копиям реестра в сети, и любые конфликты разрешаются автоматически с использованием установленных правил.



Byzantine Fault Толерантное доказательство консенсусной модели

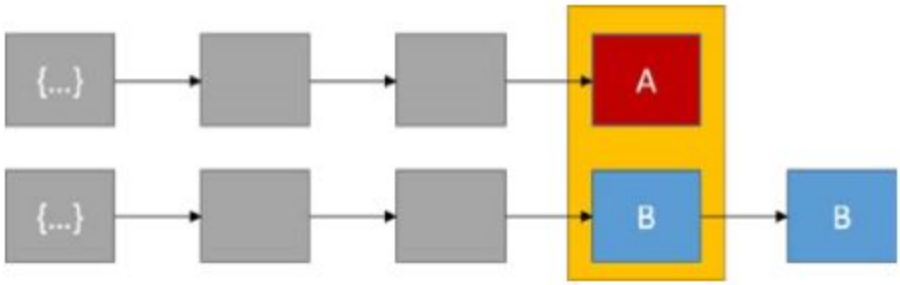
PoS модель консенсуса , в которой блокчейн решает следующий блок, позволяя всем staked участникам «голосовать», какой блок будет включен следующим.

Централизованная сеть Конфигурация сети, в которой участники должны взаимодействовать с центральным органом для связи друг с другом. Поскольку все участники должны пройти через один централизованный источник, потеря этого источника помешает всем участникам взаимодействовать.

Chain-based консенсус модель PoS PoS модель консенсуса, где система блокчейна решает следующий блок, через псевдо-рандомный выбор, на основе личной доли(stake) в общем соотношении активов системы

Конфликт Один или несколько участников не согласны с состоянием системы.

Решение конфликта Предопределенный метод достижения консенсуса в отношении состояния системы (например, когда часть участников системы заявляют, что существует состояние_A, а остальные участники заявляют, что существует состояние_B, появляется конфликт - система автоматически разрешит этот конфликт выбрав «Действительное» состояние одной из групп,добавляя следующий блок данных, любые транзакции «потерянные» по состоянию, добавляются обратно в неиспользованный пул транзакций).

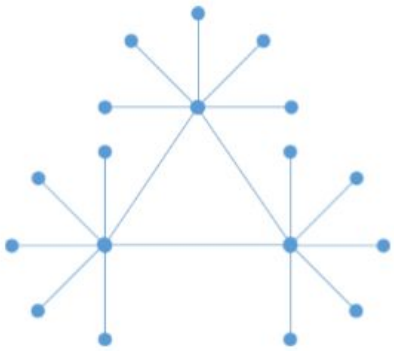


Алгоритм консенсуса Предопределенный метод для определения того, можно ли зафиксировать некоторые данные в хранилище данных. Также известна как *модель консенсуса*.

Криптовалюта Цифровой актив / кредит / блок в системе, который криптографически отправляется от одного пользователя другому пользователю. В случае создания криптовалюты (например, вознаграждение за добычу) сама система генерирует и распределяет валюту с помощью тех же криптографических механизмов. Эти активы переносятся из одного кошелька в другой, используя цифровые подписи с парами открытых / закрытых ключей.,

Криптографическая хэш-функция Функция, которая отображает битовую строку произвольной длины в битовую строку фиксированной длины. Утвержденные хеш-функции удовлетворяют следующим свойствам:

1. (Однонаправленно). Невозможно вычислить любой вход, который сопоставляется любому предварительно заданному выводу, и
2. (Устойчивость к конфликтам). В вычислительном отношении невозможно найти любые два разных входа ведущих на тот же вывод.



От NIST SP 800-175B. Руководство по использованию криптографических стандартов в федеральном правительстве: криптографические механизмы, http://dx.doi.org/10.6028/NIST.SP.800-175B

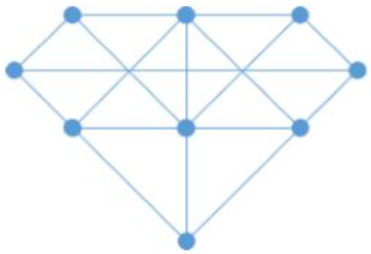
Криптографический nonce Произвольное число (обычно случайно выбранное), которое используется один раз

Децентрализованная сеть Конфигурация сети, где есть несколько органов, которые служат в качестве централизованного хаба для части участников. Поскольку некоторые участники находятся за централизованным хабом,, потеря этого хаба помешает этим участникам общаться.

Цифровая подпись Криптографическая техника, которая использует открытый /закрытый ключи для определения подлинности (т. е. Пользователи могут проверить, что сообщение было подписано закрытым ключом, соответствующим указанному открытому ключу), неотказуемость (пользователь не может отрицать, что отправил сообщение) и целостность (что сообщение не было изменено во время передачи).

Распределенная сеть

Конфигурация сети, в которой каждый участник может общаться друг с другом без прохождения централизованной точки. Поскольку существует несколько путей для общения, потеря любого участника не будет препятствовать коммуникации. Также известен как peer-to-peer.



Форк Изменение программного обеспечения и реализации блокчейна.

Полная нода нода(узел) блокчейна, который хранит данные блокчейна, передает данные другим нодам и гарантирует, что вновь добавленные блоки действительны.

Блок генезиса Первый блок блокчейна. Он записывает начальное состояние системы.

Жесткий форк Форк, который полностью предотвратит пользователей, которые не принимают ее, от использования измененной блокчейн системы. Пользователи должны либо обновиться, чтобы остаться с основной вилкой разработчика, либо продолжить исходный путь без обновлений. Пользователи на разных жестких форках не могут взаимодействовать друг с другом

Цепочка хэшей. Append-only структура данных, где данные объединяются в блоки, содержащие хэш данных предыдущего блока в новом блоке. Эта структура данных свидетельствует о вмешательстве, поскольку любая модификация данных блока изменит хэш-дайджест, записанный следующим блоком.

Хэш-дайджест Выход хеш-функции (например, hash(data) = digest). Также известен как *дайджест*.

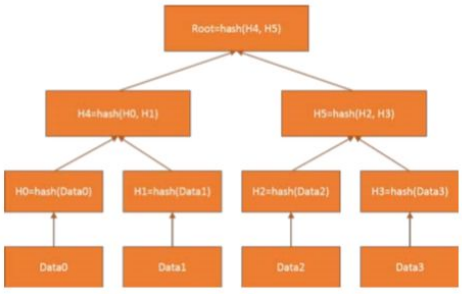
Хеширование Метод вычисления относительно уникального результата (называемый *хэш-дайджестом*) для входа почти любого размера (файл, текст, изображение и т. д.). Алгоритмы хеширования предназначены для односторонней обработки; вычислить дайджест входа это просто, но восстановление входа из дайджеста является значительно сложным и должно быть устойчивым к коллизии, так что вычислительно невозможно найти два входа, которые приводят к одному и тому же дайджесту. Кроме того, небольшое изменение ввода, даже одного бита, приведет к совершенно другому выходному дайджесту.

Неизменность Данные, которые могут быть записаны, но не изменены.

Реестр Коллекция транзакций, записанных в хронологическом порядке.

Облегченная нода блокчейн нода, которой не нужно хранить полную копию блокчейна, и, которая часто передает свои данные на полные ноды для обработки.

Дерево Меркла Структура данных, где данные хэшируются и комбинируются, до тех пор, пока не появится единственный хэш root, который представляет всю структуру.



Майнинг Акт выполнения требуемой работы (в соответствии с консенсусным алгоритмом системы) для добавления следующего

блока в систему и обычно вознаграждения с помощью криптовалюты. Также известен как *minting*.
Нода Индивидуальная система в цепочке
Permissioned (эксклюзивный) система, в которой каждому пользователю администратором назначаются определенные права.
Permissionless (инклюзивный) система, в которой все права пользователей равны и не установлены никаким администратором.
Permissions (разрешения, права) допустимые действия пользователя (например, чтение, запись, выполнение)
Proof of Stake (Доказательство доли владения) консенсус модель Консенсусная модель, в которой блокчейн сеть защищена пользователями, фиксирующими(блокирующими) количество криптовалют в системе блокчейна, процесс, называемый *staking*. Участники с большей долей в системе, скорее всего, захотят, чтобы она преуспела и не разрушилась, что придает им больший вес при консенсусе.
Proof of work (Доказательство выполнения работы) консенсус модель Консенсусная модель, в которой майнинг нода получает право опубликовать следующий блок, затрачивая время, энергию и вычислительные циклы, чтобы решить труднорешаемую, но легко проверяемую проблему (например, найти nonce, который при объединении с данными, которые будут добавлены в блок, приведет к определенной модели выхода).
Public/private key cryptography (Криптосистема с открытым/закрытым ключом) Криптографическая система, в которой пользователи имеют закрытый ключ, который хранится в секрете и используется для создания открытого ключа (который свободно предоставляется другим). Пользователи могут подписывать цифровой подписью данные с помощью своего закрытого ключа, а подпись,полученная в результате, может быть проверена любым, кто использует соответствующий открытый ключ. Также известна как асимметричная криптография.
Round robin consensus model (Round robin консенсус модель) Консенсусная модель для частных блокчейнов, где ноды псевдослучайно выбираются для создания блоков, но нода должна подождать несколько циклов создания блоков, прежде чем быть выбранной снова, чтобы создать еще один новый блок. Эта модель гарантирует, что ни один из участников не создает большинство блоков, и эта модель выигрывает на фоне простого подхода, ввиду отсутствия криптографических головоломок и низкого потребления энергии.
Soft fork(Мягкий форк) Форк, который не будет полностью препятствовать пользователям, которые не принимают его, использовать измененный блокчейн. Мягкий форк может быть обратно совместим, только требуется, чтобы большинство майнинг нодов обновлялись, обеспечивая соблюдение новых правил мягкого форка.
Транзакция Запись о передаче активов (цифровая валюта, единицы инвентаря и т. д.) между сторонами.
Пул транзакций. Распределенная очередь, в которой кандидатные транзакции ждут, пока они не будут добавлены в цепочку. Также известен как Unspent transaction pool(пул непотраченных транзакций).
Turing complete(Полнота по Тьюрингу) Система (компьютерная система, язык программирования и т. д.), которая может быть использована для любого алгоритма, независимо от сложности, для поиска решения.
Пользователь Любой человек, группа, бизнес или организация, которая использует или управляет нодой блокчейна
Wallet(Кошелек) Программное обеспечение, используемое для управления открытыми / закрытыми ключами и адресами, используемыми для транзакций.

Приложения C—Ссылки

[1] Clarke, A.C., “Hazards of Prophecy: The Failure of Imagination,” from Profiles of the Future: An Inquiry into the Limits of the Possible, 1962.
[2] Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfede, S., Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, 2016.
[3] Nakamoto, S., “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. https://bitcoin.org/bitcoin.pdf
[4] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 180-4, Secure Hash Standard (SHS), August 2015. https://doi.org/10.6028/NIST.FIPS.180-4
[5] National Institute of Standards and Technology (NIST), Secure Hashing website, https://csrc.nist.gov/projects/hash-functions
[6] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 186-4, Digital Signature Standard, July 2013. https://doi.org/10.6028/NIST.FIPS.186-4
[7] Deetman, S., “Bitcoin Could Consume as Much Electricity as Denmark by 2020,” Motherboard, March 29, 2016. https://motherboard.vice.com/en_us/article/bitcoin-could-consume-as-muchelectricity-as-denmark-by-2020
[8] Hern, A., “Bitcoin mining consumes more electricity a year than Ireland,” The Guardian, November 27, 2017. https://www.theguardian.com/technology/2017/nov/27/bitcoin-mining-consumeselectricity-ireland
[9] Power Compare, https://powercompare.co.uk/bitcoin/
[10] Bahsoun, J.P., Guerraoui, R., and Shoker, A., “Making BFT Protocols Really Adaptive,” 2015 IEEE International Parallel and Distributed Processing Symposium, Hyderabad, India, pp. 904-913, 2015. https://doi.org/10.1109/IPDPS.2015.21
[11] Todd, P., Bitcoin Improvement Proposal (BIP) 65, “OP_CHECKLOCKTIMEVERIFY,” October 1, 2014. https://github.com/bitcoin/bips/blob/master/bip-0065.mediawiki
[12] Wong, J. and Kar, I., “Everything you need to know about the Ethereum ‘hard fork,’” Quartz Media, July 18, 2016. https://qz.com/730004/everything-you-needto-know-about-the-ethereum-hard-fork/
[13] National Institute of Standards and Technology (NIST), Federal Information Processing Standards (FIPS) Publication 202, SHA-3 Standard: PermutationBased Hash and Extendable-Output Functions, August 2015. https://doi.org/10.6028/NIST.FIPS.202
NISTIR 8202 (DRAFT) BLOCKCHAIN TECHNOLOGY OVERVIEW
56
[14] Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and SmithTone, D., National Institute of Standards and Technology (NIST), NIST Internal Report (NISTIR) 8105, Report on Post-Quantum Cryptography, April 2016. https://doi.org/10.6028/NIST.IR.8105
[15] Mell, P., Kelsey, J., and Shook, J., “Cryptocurrency Smart Contracts for Distributed Consensus of Public Randomness.” October 7, 2017. https://doi.org/10.1007/978-3-319-69084-1_31
[16] Lamport, L., “Leaderless Byzantine Paxos,” Distributed Computing: 25th International Symposium: DISC 2011, p. 141-142, December 27, 2011. https://www.microsoft.com/en-us/research/publication/leaderless-byzantine-paxos
[17] Gipp, B., Meuschke, N., and Gernandt, A., “Decentralized Trusted Timestamping using the Crypto Currency Bitcoin,” in Proceedings of the iConference 2015, Newport Beach, California, 2015.
[18] Mattila, J., Seppälä, T., Naucler, C., Stahl, R., Tikkanen, M., Bådenlid, A., and Seppälä, J., The Research Institute of the Finnish Economy (ETLA) Working Papers No. 43, “Industrial Blockchain

Platforms: An Exercise in Use Case Development in the Energy Industry," The Research Institute of the Finnish Economy, October 11, 2016. https://www.etla.fi/wp-content/uploads/ETLAWorking-Papers-43.pdf
[19] Donnelly, J., "What is the 'Halving'? A Primer to Bitcoin's Big Mining Change," CoinDesk, June 12, 2016. https://www.coindesk.com/making-sense-bitcoinshalving/
[20] Hertig, A., "Litecoin's SegWit Activation: Why it Matters and What's Next," CoinDesk, April 26, 2017. https://www.coindesk.com/litecoins-segwit-activationwhy-it-matters-and-whats-next/
[21] Litecoin Project. https://litecoin.org/
[22] Wood, G., "Ethereum: A Secure Decentralised Generalised Transaction Ledger." https://bravenewcoin.com/assets/Whitepapers/Ethereum-A-Secure-DecentralisedGeneralised-Transaction-Ledger-Yellow-Paper.pdf
[23] Pearson, J., "The Ethereum Hard Fork Spawned a Shaky Rebellion," Motherboard, July 27, 2016. https://motherboard.vice.com/en_us/article/theethereum-hard-fork-spawned-a-shaky-rebellion-ethereum-classic-etc-eth
[24] "What Is Dash?", WeUseCoins. https://www.weusecoins.com/what-is-dash/
[25] Duffield, E. and Diaz, D., "Dash: A Privacy-Centric Crypto-Currency." https://github.com/dashpay/dash/wiki/Whitepaper
[26] "Introduction to Ripple for Bitcoiners," last modified December 10, 2013. https://wiki.ripple.com/Introduction_to_Ripple_for_Bitcoiners
[27] Brown, A., "10 things you need to know about Ripple," CoinDesk, May 17, 2013. https://www.coindesk.com/10-things-you-need-to-know-about-ripple/

[28] "Hyperledger Business Blockchain Technologies," The Linux Foundation. https://www.hyperledger.org/projects
[29] Cachin, C., "Architecture of the Hyperledger blockchain fabric," in Workshop on Distributed Cryptocurrencies and Consensus Ledgers, July 2016.
[30] Greenspan, G., "Introducing MultiChain Streams," MultiChain, September 15, 2016. http://www.multichain.com/blog/2016/09/introducing-multichain-streams/
[31] Narayanan, A., "Analyzing the 2013 Bitcoin fork: centralized decision-making saved the day," MultiChain, July 28, 2015. https://freedom-totinker.com/2015/07/28/analyzing-the-2013-bitcoin-fork-centralized-decisionmaking-saved-the-day
[32] Greenspan, G., "The Blockchain Immutability Myth," MultiChain, May 4, 2017. https://www.multichain.com/blog/2017/05/blockchain-immutability-myth/ [33] "Bitcoin blockchain size reaches 100 GB," Coinfox, December 19, 2016. http://www.coinfox.info/news/6700-bitcoin-blockchain-size-reaches-100-gb