

Bitcoin



**Биткоин – цифровое золото
и финансовая революция**

Артем Демиденко / ИИ

Артем Демиденко
Артем Демиденко
Искусственный Интеллект
Bitcoin: Биткоин –
цифровое золото и
финансовая революция

http://www.litres.ru/pages/biblio_book/?art=69938650

SelfPub; 2023

Аннотация

Это захватывающее исследование величайшей финансовой инновации XXI века. Автор погружается в мир криптовалюты, начиная с загадочного создателя Bitcoin'a, Сатоши Накамото, и раскрывает удивительную историю её возникновения и развития. Через страницы книги читатели узнают о технологии блокчейн и её революционных возможностях, которые лежат в основе Биткоина. Автор детально исследует роль Биткоина в мировой экономике и финансовой системе, объясняя, как криптовалюта изменила парадигмы доверия и децентрализации. Книга также затрагивает этические и правовые аспекты Биткоина и обсуждает вопросы безопасности, инвестирования и рисков, связанных с криптовалютой. Автор анализирует влияние Биткоина на

мировой финансовый ландшафт и дает прогнозы относительно будущего криптовалюты.

Содержание

Глава 1: Загадка Сатоши Накамото	5
Глава 2: Революция Блокчейн	22
Конец ознакомительного фрагмента.	28

Артем Демиденко Bitcoin: Биткоин – цифровое золото и финансовая революция

Глава 1: Загадка Сатоши Накамото

1.1. Предыстория:

Перед тем как мы углубимся в историю создания Биткоина, давайте взглянем на обстановку, которая стала плодородной почвой для зарождения криптовалюты. Кризис 2008 года был ключевым событием, которое подтолкнуло Сатоши Накамото к идее создания альтернативной финансовой системы.

В конце 2000-х годов многие страны столкнулись с экономическими трудностями. Американский рынок недвижимости обрушился, что привело к каскаду финансовых бедствий. Банки и финансовые институты были в упадке, а множество людей потеряли свои дома, сбережения и рабочие места.

Как реакция на финансовый кризис, правительства многих стран начали масштабные финансовые стимулы и сни-

жение процентных ставок. Это привело к увеличению денежной массы и вызвало опасения относительно инфляции. Большинство людей начали задаваться вопросами о том, насколько надежными являются традиционные финансовые институты и государственные валюты.

В этой обстановке появилась идея о создании цифровой валюты, которая была бы независимой от центральных банков и правительств. Именно в этот момент на сцену выходит Сатоши Накамото и его белая книга о Биткоине.

Белая книга Сатоши, опубликованная в октябре 2008 года под заголовком "Bitcoin: A Peer-to-Peer Electronic Cash System," предложила альтернативу традиционной финансовой системе. В ней описывался концептуальный фреймворк для децентрализованной цифровой валюты, которая могла бы функционировать без посредников и контроля со стороны государства.

Сатоши Накамото представил первую криптовалюту – Биткоин, в январе 2009 года, когда был запущен первый блок в блокчейн-цепи. Это событие стало отправной точкой для революции в финансовом мире, историю которой мы будем рассматривать в данной книге.

1.2. Мистическая личность:

Сатоши Накамото – это псевдоним или имя настоящей личности? Этот вопрос стал одним из наиболее интригующих в истории криптовалют. С момента выпуска Биткоина в 2009 году Сатоши оставался анонимным, и его настоящая

личность так и не была установлена. Вместо этого он взаимодействовал с миром через электронные сообщения и форумы, где он общался с другими участниками сообщества.

- **Имя и псевдоним:** Сатоши Накамото – это псевдоним, используемый для обозначения создателя Биткойна. На самом деле, многие считают, что это имя является вымышленным, и Сатоши – это псевдоним для одной или группы людей.

- **Оригинальная белая книга:** В октябре 2008 года Сатоши Накамото опубликовал белую книгу, которая стала основой для создания Биткойна. Эта белая книга содержит техническое описание принципов функционирования Биткойна и технологии блокчейн.

- **Сообщества и форумы:** Сатоши Накамото активно общался с другими участниками сообщества криптовалют, в том числе через форум bitcointalk.org. Он отвечал на вопросы, обсуждал технические детали и совершал изменения в коде Биткойна.

- **Исчезновение:** В апреле 2011 года Сатоши Накамото прекратил свою активность и перестал взаимодействовать с сообществом. Он передал доступ к проекту другим разработчикам и исчез из публичного внимания.

Множество теорий было предложено относительно личности Сатоши Накамото, но до сих пор нет окончательного ответа на вопрос, кто он или они на самом деле. Эта загадка придает Биткойну и его созданию особую ауру таинственно-

сти и интриги, что делает его историю ещё более удивительной и увлекательной.

1.3. Энергия и ресурсы:

Создание Биткоина – это задача, которая потребовала огромного количества вычислительных ресурсов и энергии. В этом разделе мы более подробно рассмотрим, какой объём работы ушел на первоначальную добычу и поддержание Биткоин-сети.

- **Подсчеты и вычисления:** В самом начале, когда Биткоин только запускался, Сатоши Накамото майнил монеты на своем собственном компьютере. Он использовал вычислительные мощности своей CPU (центрального процессора) для решения математических задач, необходимых для создания новых блоков. Но это было короткоживущим методом, так как сеть быстро росла в сложности, требуя более мощных ресурсов.

- **Появление GPU:** Скоро майнеры начали использовать графические процессоры (GPU), которые оказались гораздо более эффективными в решении задач блокчейна. Это привело к буму майнинга и к тому, что майнеры объединились в так называемые "пулы майнинга" для совместного использования ресурсов.

- **ASIC-майнеры:** Дальнейший рост сети привел к появлению специализированных майнинг-устройств, известных как ASIC (Application-Specific Integrated Circuit). Эти машины спроектированы исключительно для майнин-

га и способны выполнять вычисления с невероятной скоростью. Они стали стандартом в индустрии майнинга и существенно повысили уровень сложности.

- **Энергопотребление:** Однако рост вычислительной мощности и использование ASIC-майнеров привели к росту энергопотребления. Майнинг Биткоина стал известным своим высоким энергопотреблением, что вызывало беспокойство среди экологических активистов и обсуждение его устойчивости.

- **Обсуждение устойчивости:** В этом разделе мы также касаемся вопроса устойчивости сети Биткоина в контексте энергопотребления и экологических вопросов. Разные точки зрения на это обсуждаются, включая аргументы о том, что Биткоин может стать стимулом для развития возобновляемой энергетики.

Все эти аспекты энергопотребления и ресурсов важны для понимания, как создание и поддержание Биткоина затрагивают сферу энергетики и технологического развития, и какие вызовы они представляют для будущего криптовалют.

1.4. Загадочное исчезновение:

После создания Биткоина и активной работы над его развитием в течение первых двух лет, Сатоши Накамото внезапно исчез из общественности в апреле 2011 года. Это событие остается загадкой до сих пор, и множество теорий и догадок окружают его исчезновение. В данной части мы рассмотрим несколько ключевых моментов, связанных с загадочным ис-

чезновением Сатоши:

Последние контакты:

Перед своим исчезновением Сатоши Накамото поддерживал активные коммуникации с другими разработчиками и участниками сообщества Биткойна. Эти контакты представляют собой важное звено в истории его исчезновения:

- **Электронная почта:** Сатоши использовал электронную почту для коммуникации с другими разработчиками и участниками сообщества. Одним из его последних известных электронных писем было сообщение, отправленное Майку Херну, разработчику Биткойна, в котором он выразил свою обеспокоенность будущим развитием проекта.

- **Форумы:** Сатоши активно участвовал в форумах, таких как `BitcoinTalk`, где обсуждались вопросы развития Биткойна. Его последние сообщения на форумах также стали предметом внимания, поскольку они стали реже и менее информативными.

- **Сообщения в коде:** Сатоши также оставался в контакте с сообществом через изменения в коде Биткойна. Его последние изменения кода были внесены в репозиторий проекта на `GitHub`.

- **Другие контакты:** Существуют также отчеты о личных встречах и обмене сообщениями между Сатоши и другими ключевыми участниками. Некоторые из этих контактов документированы, но большинство остались конфиденциальными.

Эти последние контакты предоставляют некоторое представление о состоянии ума и мотивации Сатоши перед его исчезновением. Несмотря на исчезновение Сатоши, сообщество Биткоина продолжило развивать криптовалюту и блокчейн-технологию, но загадка его личности остается актуальной и до сих пор вызывает интерес исследователей и участников криптографического сообщества.

Страх перед идентификацией:

Один из ключевых аспектов загадки исчезновения Сатоши Накамото – это страх перед идентификацией

Сатоши как создатель Биткоина: Сатоши Накамото был явно идентифицирован как создатель Биткоина благодаря сообщениям и публикациям, которые он сделал в начальные годы развития криптовалюты. Его роль в создании первого блока (блока генезиса) и первой транзакции на Биткоин сети делают его основоположником этой цифровой валюты.

Законодательство и риски: В момент создания Биткоина в 2009 году и в первые годы его существования законодательство в отношении криптовалют было мало разработано, и регулирование было неясным. Это могло создавать значительные юридические и налоговые риски для Сатоши. Он, возможно, опасался преследования и юридических последствий, связанных с созданием и продвижением Биткоина.

Финансовая независимость: Считается, что Сатоши контролировал большое количество первых майнинговых наград (монет Биткоина, выплачиваемых майнерам за созда-

ние новых блоков). Эти награды могли придать ему значительное финансовое состояние. Его анонимность позволила ему сохранить финансовую независимость и избежать интереса со стороны правительств и финансовых организаций.

Преследование или угрозы: С увеличением популярности Биткоина и ростом его цены, Сатоши мог стать объектом внимания различных групп и лиц, которые видели в нем угрозу для собственных интересов. Это могло привести к реальным угрозам его безопасности и могло быть одной из причин его решения оставаться анонимным.

Давние попытки выявления:

Сразу после исчезновения Сатоши в 2011 году, сообщество и множество независимых исследователей начали активные попытки выявить его личность. Эти попытки были направлены на разгадывание загадок, связанных с его активностью и коммуникациями в сети Биткоина. В этом разделе мы рассмотрим несколько известных попыток выявления Сатоши:

Поиск в истории сообщений: Исследователи, а также любознательные члены сообщества, начали анализировать все доступные сообщения и комментарии, написанные Сатоши Накамото на различных форумах и платформах. Эти попытки включали в себя следующие аспекты:

1. Анализ языка и стиля письма: Исследователи стремились найти уникальные черты в структуре фраз и языковых особенностях, которые могли бы указать на происхож-

дение Сатоши. Они искали особые слова, фразы или грамматические конструкции, которые могли бы быть ключами к его личности.

2. Ошибки и опечатки: Другой подход включал в себя анализ ошибок и опечаток в сообщениях Сатоши. Некоторые исследователи считали, что определенные ошибки могут быть характерными для носителей определенных языков или даже указывать на уровень образования. Это подразумевало анализ текста на наличие погрешностей.

3. Часовые пояса и активность: Исследователи также пытались анализировать, когда Сатоши был наиболее активен в сети. Они сравнивали его активность с часовыми поясами и пытались определить его привычки сна и активности. Это могло бы дать подсказку о его географическом положении.

4. Публичные источники: Информация о Сатоши и его коммуникациях была доступна в публичных источниках, таких как форумы Bitcointalk, электронные письма, публичные блоги и другие. Исследователи и любопытные участники сообщества активно сканировали и анализировали эти данные. Несмотря на множество усилий исследователей, ни одна из попыток выявить Сатоши Накамото на основе анализа его коммуникаций не привела к определенным результатам. Множество людей высказывали разные мнения и предположения, но идентификация Сатоши оставалась сложной задачей.

Анализ времени активности: Исследователи и участники сообщества Биткойна долго анализировали время, когда Сатоши Накамото был наиболее активен в сети и вел свою коммуникацию. Этот анализ проводился с целью выявить его географическое расположение или хотя бы определить, в какой часовой пояс он мог находиться. Несмотря на сложность этой задачи, были предприняты несколько попыток анализа:

1. Графики активности: Исследователи создавали графики, отображающие активность Сатоши на форумах и в социальных сетях, а также временные метки его сообщений. Путем анализа этой активности они пытались определить, когда и в какие часы дня Сатоши был наиболее активен. Это могло бы дать подсказку о его часовом поясе.

2. Вычисление времени сообщений: Иногда исследователи пытались анализировать время, указанное в сообщениях Сатоши. Однако это представляло собой сложную задачу, так как время, указанное в сообщениях, могло быть легко изменено, и многие сообщения были написаны в формате UTC (координированное всемирное время), что не предоставляло ясной информации о местоположении.

3. Гипотезы о времени активности: Разные гипотезы были предложены, основанные на предположениях об активности Сатоши. Например, некоторые исследователи считали, что Сатоши мог быть активен в определенное время дня или недели, и пытались использовать это, чтобы сузить диапазон

часовых поясов.

4. Ограниченные результаты: Не смотря на усилия исследователей, анализ времени активности Сатоши Накамото не привел к определению его часового пояса или местоположения. Многие сообщения были отправлены с использованием анонимных прокси-серверов, что усложнило задачу выявления местоположения.

Исследование биткоин-кошельков: Одной из методик, используемых для попытки выявления личности Сатоши Накамото, было анализирование биткоин-кошельков, которые были связаны с ним или могли быть связаны с его активностью. Эта попытка включала в себя несколько ключевых аспектов:

1. Идентификация биткоин-кошельков Сатоши: Исследователи попытались идентифицировать биткоин-кошельки, которые были известны как принадлежащие Сатоши Накамото. Один из таких кошельков был первым в сети Биткоин и часто назывался "Genesis Block". Он был использован для майнинга первого блока в блокчейне Биткоина и имел символическое значение.

2. Анализ средств на биткоин-кошельках: После идентификации биткоин-кошельков, исследователи анализировали средства, находящиеся на них. Вопрос заключался в том, были ли эти средства двигаемыми или оставались нетронутыми. Если бы средства начали двигаться, это могло бы быть интерпретировано как признак активности Сатоши.

3. Попытки связать биткоин-кошельки с активностью: Исследователи также пытались выяснить, связаны ли биткоин-кошельки Сатоши с какими-либо транзакциями или событиями, которые могли бы указать на его личность. Это могли быть транзакции между кошельками или другие показатели активности.

4. Препятствия и загадки: Сатоши Накамото оставил после себя множество загадок и защитных механизмов, чтобы сохранить свою анонимность. Например, он использовал псевдоним для общения, что делало невозможным установить его личность на основе языковых анализов. Кроме того, он мог использовать технические методы для сокрытия своей активности и реального IP-адреса.

5. Результаты и выводы: Несмотря на все усилия исследователей, их попытки выявления личности Сатоши Накамото через анализ биткоин-кошельков оказались неудачными. Он оставался анонимным, и его личность оставалась загадкой. Это стало частью легенды и мистики, окружающей создание Биткоина, и укрепило понимание важности анонимности и децентрализации в мире криптовалют.

Журналистские расследования: Журналисты из разных стран предприняли собственные расследования, в надежде найти Сатоши Накамото и разгадать загадку его личности. Эти журналистские расследования включали в себя разнообразные методы и подходы:

1. Отслеживание доменных имен: Журналисты иска-

ли доменные имена, связанные с Сатоши Накамото и первыми версиями программного обеспечения для Биткойна. Они пытались выяснить, кто зарегистрировал эти домены и какие могли бы быть связи с личностью Сатоши.

2. Разговоры с близкими криптографами: Журналисты контактировали с известными криптографами и экспертами в области криптовалют с целью получения их мнения и гипотез относительно Сатоши. Эти эксперты могли предоставить информацию о том, кто мог быть Сатоши или какие технические знания ему были доступны.

3. Попытки интервью: Некоторые журналисты пытались установить контакт с людьми, которые могли бы знать Сатоши лично или иметь информацию о нем. Они предпринимали попытки организовать интервью с такими людьми, включая близких друзей и коллег Сатоши.

4. Изучение технических характеристик: Журналисты анализировали технические характеристики и методы программирования, использованные в оригинальном коде Биткойна и других проектах, связанных с Сатоши. Они пытались выявить подписи кода или технические детали, которые могли бы указывать на личность Сатоши.

5. Публикация результатов: Журналисты, проводящие такие расследования, публиковали свои результаты и гипотезы в различных медиа. Некоторые статьи и исследования становились весьма популярными и вызывали большой интерес со стороны сообщества криптовалют.

Несмотря на множество усилий, подходов и публикаций, журналистские расследования не привели к конкретным результатам в определении личности Сатоши Накамото. Мистика и тайна, окружающие его личность, остаются несводимыми счетами в истории криптовалют и блокчейна.

Мнения о его судьбе:

С годами после исчезновения Сатоши Накамото, появилось множество мнений и теорий относительно его судьбы. Эти мнения разнообразны и отражают разные точки зрения на то, что могло произойти с создателем Биткоина после его исчезновения. В данном разделе мы рассмотрим некоторые из наиболее распространенных мнений:

1. Сатоши остался анонимным: Эта теория предполагает, что Сатоши Накамото остался верен своему идеалу анонимности. По мнению сторонников этой теории, он мог просто решить уйти в тень и больше не возвращаться к разработке Биткоина. Это может быть связано с его опасениями относительно правовых последствий или просто желанием сохранить анонимность.

2. Сатоши ушел по личным причинам: Некоторые считают, что личные обстоятельства, такие как здоровье, семейные обязанности или другие личные проблемы, могли стать причиной исчезновения Сатоши. Это мнение предполагает, что он больше не мог уделять достаточно времени и энергии развитию Биткоина.

3. Сатоши умер: Следуя этой теории, Сатоши Накамо-

то мог умереть после исчезновения. Это объяснило бы, почему он больше не активен в сообществе. Однако нет никаких достоверных доказательств или официальных объявлений, подтверждающих эту теорию.

4. Сатоши вернется в будущем: Некоторые верят, что Сатоши мог вернуться в будущем, когда наступит подходящее время, чтобы продвигать развитие Биткоина или объявить о своей личности. Эта теория предполагает, что Сатоши может ждать момента, когда его появление будет иметь наибольший эффект на криптовалютное сообщество.

5. Другие мнения и теории: Существует множество других теорий и мнений о судьбе Сатоши Накамото, включая теории заговора и даже предположения о том, что он может быть частью группы людей, а не одиночкой.

1.5. Наследие и влияние:

Сатоши Накамото, несмотря на свою таинственность и исчезновение, оставил глубокий след в мире финансов и технологий. Его наследие и влияние можно разделить на несколько ключевых аспектов:

Блокчейн-технология: Сатоши Накамото создал Биткоин, используя технологию блокчейн, которая стала фундаментом для многих других криптовалют и проектов. Блокчейн – это децентрализованный, надежный и прозрачный способ записи и передачи данных, который нашел применение в различных отраслях, от финансов до логистики и медицины.

Децентрализация и контроль над собственными средствами: Биткоин и другие криптовалюты поднимают вопрос о децентрализации и управлении собственными финансами. Они позволяют людям контролировать свои деньги независимо от государственных или банковских органов. Это стимулировало обсуждение вопросов личной финансовой свободы и прозрачности.

Революция в финансовых услугах: Криптовалюты и блокчейн технология также привнесли новшества в финансовые услуги. Криптовалютные биржи, смарт-контракты и децентрализованные финансовые платформы изменили способ, которым мы инвестируем, отправляем деньги и заключаем сделки.

Экономика и инвестиции: Биткоин стал активом, который привлек внимание инвесторов и спекулянтов. Его волатильность и потенциал для прироста стоимости привели к формированию криптовалютных инвестиционных стратегий и созданию новых инвестиционных продуктов, таких как ETF на основе криптовалюты.

Эксперименты с цифровыми валютами: Сатоши Накамото создал прецедент для экспериментов с цифровыми валютами в разных странах. Несколько государств начали исследовать создание собственных цифровых валют (центральных банковских цифровых валют, CBDC), вдохновленных успехом Биткоина.

Сообщество и активизм: Сатоши Накамото вдохновил

множество людей по всему миру на активное участие в сообществе криптовалют. Команда разработчиков, майнеры, трейдеры и энтузиасты собрались вокруг Биткоина и других криптовалют, создавая сообщество, готовое защищать и продвигать идеи децентрализации и инноваций.

Глава 2: Революция Блокчейн

Во второй главе нашей книги мы погрузимся в удивительный мир технологии блокчейн, которая лежит в основе Биткойна и оказала непередаваемое влияние на множество отраслей и аспектов нашей жизни. Начнем с объяснения, что такое блокчейн, как он работает и почему он стал ключевым элементом Биткойна.

1. Что такое блокчейн?

Блокчейн (или blockchain) – это основная технология, лежащая в основе большинства криптовалют, включая Биткойн, и множества других инновационных приложений. Эта технология представляет собой распределенную базу данных, которая хранит информацию в виде непрерывной цепи блоков. Давайте разберемся более подробно в том, что это означает:

Распределенная база данных: В отличие от традиционных централизованных баз данных, которые управляются центральными учреждениями или организациями, блокчейн представляет собой базу данных, которая хранится и управляется децентрализованным сообществом. Это означает, что информация хранится на множестве компьютеров, или узлов, распределенных по всему миру, и каждый узел имеет копию всей базы данных.

Непрерывная цепь блоков: Блокчейн состоит из бло-

ков, которые связаны между собой в хронологическом порядке, образуя непрерывную цепь. Каждый блок содержит набор данных, таких как транзакции, и информацию о предыдущем блоке (хеш предыдущего блока). Эта связь между блоками делает блокчейн надежным и устойчивым к манипуляциям, так как изменение данных в одном блоке требует изменения данных во всех последующих блоках, что практически невозможно.

Криптография и безопасность: Для обеспечения безопасности и целостности данных блокчейн использует криптографию. Каждый блок содержит хеш предыдущего блока, который делает его и все последующие блоки зависимыми друг от друга. Любое изменение в одном блоке изменит хеш, и это будет заметно всем участникам сети. Кроме того, блокчейн использует асимметричное шифрование для обеспечения безопасности транзакций и доступа к данным.

Децентрализация и доверие: Одной из ключевых особенностей блокчейна является его децентрализация. Нет центрального учреждения или власти, которая контролирует блокчейн. Вместо этого, участники сети совместно поддерживают и обновляют базу данных, и каждый участник имеет копию данных. Это создает высокий уровень доверия, так как изменение данных требует согласия большинства участников.

Прозрачность и доступность: Все транзакции и данные в блокчейне обычно являются общедоступными и про-

зрачными. Любой может проверить данные в блокчейне, и это способствует устранению недоверия и мошенничества.

2. Работа блокчейна

В этом разделе мы подробно рассмотрим, как именно работает технология блокчейн, начиная с инициации транзакции и заканчивая добавлением новых блоков в цепь.

2.1. Инициация транзакции

Инициация транзакции – это первый шаг в работе блокчейна, где пользователь или участник сети желает отправить средства или информацию другому пользователю. Давайте рассмотрим этот процесс более подробно:

1. *Создание транзакции:* Все начинается с того, что пользователь, имея доступ к своему криптовалютному кошельку, решает отправить криптовалюту или выполнить другую операцию, которая будет записана в блокчейне. Это может быть перевод биткоинов, создание смарт-контракта в сети Ethereum или даже запись данных в блокчейне, если платформа поддерживает такую функциональность.

2. *Подписание транзакции:* После того как пользователь решает совершить транзакцию, его кошелек автоматически создает саму транзакцию. Эта транзакция включает в себя информацию о том, кому и сколько средств отправляется, а также другие необходимые данные. Затем пользователь подписывает эту транзакцию с помощью своего закрытого ключа.

3. *Защита секретного ключа:* Закрытый ключ (private

key) – это критически важная часть процесса. Этот ключ должен оставаться строго секретным и доступным только владельцу. Он используется для подписи транзакции и подтверждения, что она отправлена именно владельцем кошелька.

4. *Формирование хеша*: После подписания, транзакция суммируется в хеш (криптографический хеш), который представляет собой уникальную строку, созданную на основе данных в транзакции и закрытом ключе отправителя. Этот хеш будет позже использоваться для верификации транзакции.

5. *Отправка транзакции в сеть*: Подписанная транзакция отправляется в сеть блокчейна. В сети существует множество узлов, которые служат как посредники для транзакций. Транзакция будет распределена между этими узлами и станет доступной для последующей обработки.

6. *Ожидание подтверждения*: Транзакция не сразу включается в блокчейн. В зависимости от сети, это может занять некоторое время. Пока транзакция не получит необходимое количество подтверждений (обычно требуется несколько подтверждений в сети Биткойна), она считается неподтвержденной.

2.2. Подтверждение транзакции

Подтверждение транзакции – это ключевой этап работы блокчейна, обеспечивающий доверие и безопасность в системе. Давайте рассмотрим этот процесс подробнее:

Сбор транзакций: После того как пользователь А ини-

цировал транзакцию и отправил ее в сеть, она попадает в пул транзакций (transaction pool) или мемпул (mempool). Это временное хранилище для транзакций, ожидающих подтверждения. Транзакции в мемпуле ожидают, пока майнеры не выберут их для включения в новый блок.

Создание блока: Майнеры – это специальные участники сети, ответственные за создание новых блоков. Они выбирают транзакции из мемпула и объединяют их в новом блоке. Выбор транзакций может зависеть от различных факторов, таких как комиссии, прикрепленные к транзакциям, приоритет и другие.

Решение криптографической задачи (Proof of Work): После того как майнеры выбрали транзакции для нового блока, они начинают работу над решением сложной криптографической задачи, которая называется "Proof of Work" (PoW). Эта задача требует вычислительной мощности и времени. Майнеры решают ее, перебирая множество вариантов, путем хеширования данных в блоке и добавления специфической "цели" (target), которая должна быть достигнута.

Добавление блока: Первый майнер, который успешно решит криптографическую задачу (находя так называемый "золотой" хеш), объявляет о создании нового блока. Этот блок содержит выбранные транзакции, служебную информацию и хеш предыдущего блока. Остальные участники сети проверяют блок на корректность и соглашаются с добавле-

нием его в цепь.

Обновление распределенной копии: Каждый участник сети, получивший уведомление о новом блоке, обновляет свою локальную копию блокчейна, добавляя новый блок в цепь. Это происходит одновременно во всей сети, обеспечивая единое состояние блокчейна для всех участников.

Этот процесс подтверждения транзакции гарантирует, что каждая транзакция в блокчейне прошла через процесс проверки и была добавлена к общей истории транзакций. Это также делает блокчейн безопасным и надежным, так как изменение данных в одном блоке потребовало бы пересоздания всех последующих блоков, что крайне сложно и требует огромных ресурсов.

2.3. Добавление блока

После того как майнер решает сложную криптографическую задачу (Proof of Work) и создает новый блок, происходит несколько важных шагов, связанных с добавлением этого блока в блокчейн:

Хеш предыдущего блока

Каждый блок в цепи содержит информацию о хеше (хеш – это уникальная строка символов) предыдущего блока. Это связывает блоки вместе и обеспечивает непрерывность цепи. Если даже один символ в предыдущем блоке был бы изменен, это изменение отразилось бы на хеше, и блокчейн был бы бит. Таким образом, хеш предыдущего блока служит неким "отпечатком" предыдущего состояния блокчейна.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.