Co-funded by the
Erasmus+ Programme
of the European Union

ТАДЖИКСКИЙ ГОСУДАРСТВЕННЫЙ ФИНАНСОВО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ

БЛОКЧЕЙН: ИННОВАЦИОННЫЙ МЕНЕДЖМЕНТ И ПРОРЫВНЫЕ ТЕХНОЛОГИИ

(Blockchain, Innovation management and Disruptive technology)

(курс лекции)

Душанбе-2021

Автор и составитель к.э.н, доцент кафедры экономики предприятия и предпринимательства Кодиров Фируз Абдулхафизович

The Blockchain, Innovation management and Disruptive technology teaching materials is developed in the framework of ERASMUS+ CBHE project "Digitalization of economic as an element of sustainable development of Ukraine and Tajikistan" / DigEco 618270-EPP-1-2020-1-LT-EPPKA2-CBHE-JP

This project has been funded with support from the European Commission. This document reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

БЛОКЧЕЙН: КРАТКАЯ ИСТОРИЯ

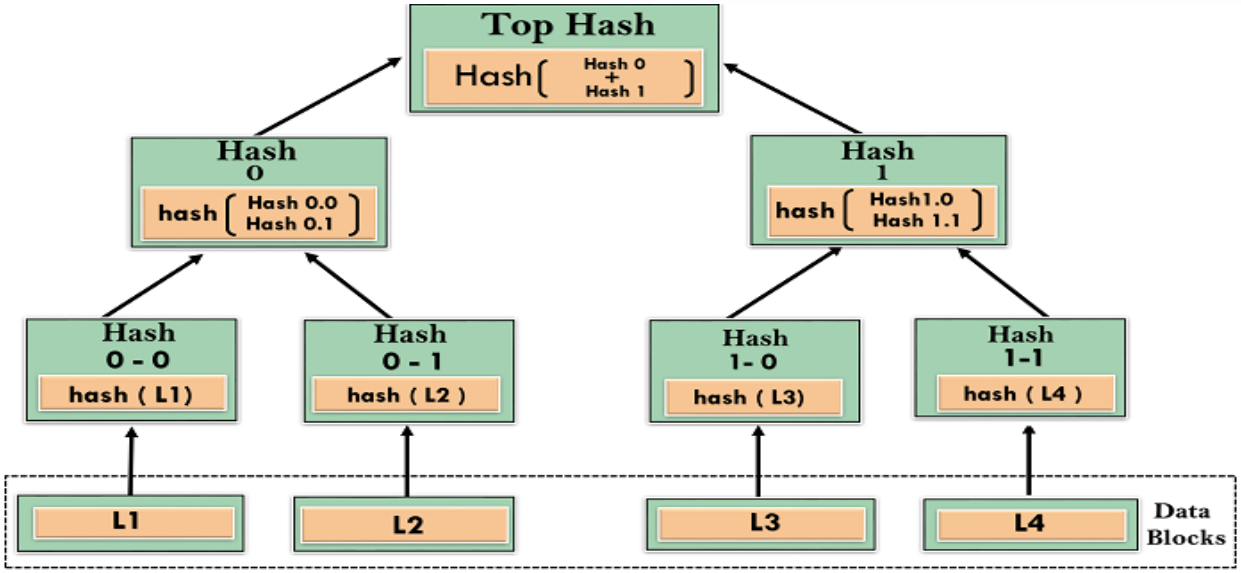
Зарождение и развитие идеи Блокчейна связана с именами Стюарта Хабера и В. Скотта Сторнетты.

Stuart Haber

W. Scott Stornetta

Эти ученые в 1991г. хотели представить вычислительно практичное решение для временных меток цифровых документов, чтобы их нельзя было датировать задним числом или подделывать. Они разрабатывают систему, использующую концепцию криптографически защищенной цепочки блоков для хранения документов с отметками времени.

В 1992 году в дизайн были включены деревья Меркла, что делает блокчейн более эффективным, позволяя собирать несколько документов в один блок. Деревья Меркла используются для создания «защищенной цепочки блоков». В нем хранится серия записей данных, и каждая запись данных связана с предыдущей. Самая новая запись в этой цепочке содержит историю всей цепочки. Однако эта технология не использовалась, и срок действия патента истек в 2004 году.



В 2004 году ученый-компьютерщик и криптографический активист Хэл Финни представил систему под названием Reusable Proof Of Work (RPoW) в качестве прототипа цифровых денег. Это был важный ранний шаг в истории криптовалют. Система RPoW работала, получая взамен не подлежащий обмену или взаимозаменяемому токен подтверждения работы на основе Hashcash, создавая токен, подписанный RSA, который в дальнейшем можно было передавать от человека к человеку.

Hal Finney

RPoW решил проблему двойной траты, сохранив право собственности на токены, зарегистрированное на доверенном сервере. Этот сервер был разработан, чтобы позволить пользователям во всем мире проверять его правильность и целостность в режиме реального времени.

Далее, в 2008 году Сатоши Накамото концептуализировал теорию распределенных блокчейнов . Он уникальным образом улучшает дизайн, добавляя блоки в начальную цепочку, не требуя их подписи доверенными сторонами. Модифи-

цированные деревья будут содержать защищенную историю обмена данными. Он использует одноранговую сеть для отметки времени и проверки каждого обмена. Им можно было управлять автономно, не требуя центрального органа. Эти улучшения оказались настолько полезными, что сделали блокчейны основой криптовалют. Сегодня дизайн служит общедоступной книгой для всех транзакций в криптовалютном пространстве.

Satoshi Nakamoto

Эволюция блокчейнов была стабильной и многообещающей. Слова «блок» и «цепочка» использовались отдельно в оригинальной статье Сатоши Накамото, но в конечном итоге к 2016 году были популяризированы как одно слово «блокчейн» . За последнее время размер файла блокчейна криптовалюты, содержащего записи обо всех транзакциях, произошедших в сети, вырос с 20 ГБ до 100 ГБ .

ЧТО ТАКОЕ БИТКОЙН?

Сатоши Накамото представил биткойн в 2008 году. Биткойн — это криптовалюта (виртуальная валюта) или цифровая валюта , которая использует правила криптографии для регулирования и генерации единиц валюты. Биткойн попал в сферу криптовалюты и стал первым и самым ценным среди них. Ее обычно называют децентрализованной цифровой валютой .

Биткойн — это тип цифровых активов, которые можно покупать, продавать и безопасно передавать между двумя сторонами через Интернет. Биткойн можно использовать для хранения ценностей, таких как чистое золото, серебро и некоторые другие виды инвестиций. Мы также можем использовать биткойн

для покупки продуктов и услуг, а также для совершения платежей и обмена ценностями в электронном виде.

Биткойн отличается от других традиционных валют, таких как доллар , фунт и евро , которые также можно использовать для покупки вещей и обмена ценностями в электронном виде. Нет физических монет для биткойнов или бумажных купюр. Когда вы отправляете биткойны кому-то или используете биткойны для покупки чего-либо, вам не нужно использовать банк, кредитную карту или любую другую третью сторону. Вместо этого вы можете просто безопасно и почти мгновенно отправить биткойны напрямую другому лицу через Интернет.

Как работает биткойн?

Когда вы отправляете электронное письмо другому человеку, вы просто вводите адрес электронной почты и можете напрямую общаться с этим человеком. Это то же самое, когда вы отправляете мгновенное сообщение. Этот тип связи между двумя сторонами обычно известен как одноранговая связь.

Всякий раз, когда вы хотите перевести деньги кому-либо через Интернет, вам необходимо использовать сторонние услуги, такие как банки, кредитную карту, PayPal или какой-либо другой тип услуг по переводу денег. Причина использования третьей стороны заключается в том, чтобы убедиться, что вы переводите эти деньги. Другими словами, вы должны быть в состоянии убедиться, что обе стороны сделали то, что им нужно сделать в реальном обмене.

Например, предположим, вы нажимаете на фотографию, которую хотите отправить другому человеку, поэтому вы можете просто прикрепить эту фотографию к электронному письму, ввести адрес электронной почты получателя и отправить ее. Другой человек получит фотографию, и вы думаете, что это закончится, но это не так. Теперь у нас есть две копии фотографии, одна — простое электронное письмо, а другая — оригинальный файл, который все еще

находится на моем компьютере. Здесь мы отправляем копию файла фотографии, а не исходный файл. Эта проблема широко известна как проблема двойной траты.

Проблема двойной траты ставит задачу определить, является ли транзакция реальной или нет. Как вы можете отправить биткойн кому-то через Интернет, не нуждаясь в банке или другом учреждении для подтверждения факта перевода. Ответ возникает в глобальной сети тысяч компьютеров, называемой сетью Биткойн, и особого типа децентрализованной лазерной технологии, называемой блокчейном .

В Биткойне вся информация, связанная с транзакцией, надежно фиксируется с помощью математики, защищена криптографически, а данные хранятся и проверяются по всей сети компьютеров. Другими словами, вместо того, чтобы иметь централизованную базу данных третьих лиц, таких как банки, для подтверждения транзакции. Биткойн использует технологию блокчейна в децентрализованной сети компьютеров для безопасной проверки, подтверждения и записи каждой транзакции. Поскольку данные хранятся децентрализованно в широкой сети, единой точки отказа не существует. Это делает блокчейн более безопасным и менее подверженным мошенничеству, взлому или общему сбою системы, чем хранение их в одном централизованном месте.

ВЕРСИЯ БЛОКЧЕЙНА

Ниже приводится краткое описание эволюции технологии блокчейн и ее версий с 1.0 до 3.0.

Blockchain version

Блокчейн 1.0: Валюта

Идея создания денег путем решения вычислительных головоломок была впервые представлена в 2005 году Хэлом Финни , который создал первую концепцию криптовалюты (реализация технологии распределенного реестра). Эта книга позволяет выполнять финансовые транзакции, основанные на технологии блокчейн или DLT, с биткойнами . Биткойн является наиболее ярким примером в этом сегменте. Он используется в качестве наличных для Интернета и рассматривается как средство реализации Интернета Денег .

Блокчейн 2.0: смарт-контракты

Основные проблемы, связанные с биткойнами, — это расточительный майнинг и отсутствие масштабируемости сети. Чтобы преодолеть эти проблемы, эта версия расширяет концепцию Биткойна за пределы валюты. Новые ключевые концепции — смарт-контракты. Это небольшие компьютерные программы, которые «живут» в блокчейне . Это бесплатные компьютерные программы, которые выполняются автоматически и проверяют определенные ранее условия, такие как содействие, проверка или обеспечение соблюдения. Большое преимущество этой технологии, которое предлагает блокчейн, делает невозможным подделку или взлом смарт-контрактов. Наиболее ярким примером является блокчейн Ethereum, который предоставляет платформу, на

которой сообщество разработчиков может создавать распределенные приложения для сети Blockchain.

Быстро версия блокчейна 2.0 успешно обрабатывает большое количество ежедневных транзакций в общедоступной сети, где миллионы были собраны через ICO (первичные предложения монет), а рыночная капитализация быстро увеличилась.

Блокчейн 3.0: децентрализованные приложения

DApps также известен как децентрализованное приложение. Он использует децентрализованное хранилище и связь. Его внутренний код работает в децентрализованной одноранговой сети. У DApp может быть внешний код , размещенный в децентрализованных хранилищах, таких как Ethereum Swarm, и пользовательские интерфейсы, написанные на любом языке, который может совершать вызовы на его серверную часть, как традиционные приложения.

РОЛЬ БИТКОЙН-МАЙНЕРОВ

Чтобы понять роль майнеров биткойнов, давайте сначала разберемся с майнингом биткойнов.

Биткойн-майнинг.

Биткойн-майнинг — это процесс добавления записей о транзакциях в общедоступный реестр прошлых транзакций Биткойн. Эта книга прошлых транзакций называется блокчейном, поскольку представляет собой цепочку блоков. Майнинг биткойнов используется для защиты и проверки транзакций в остальной части сети.

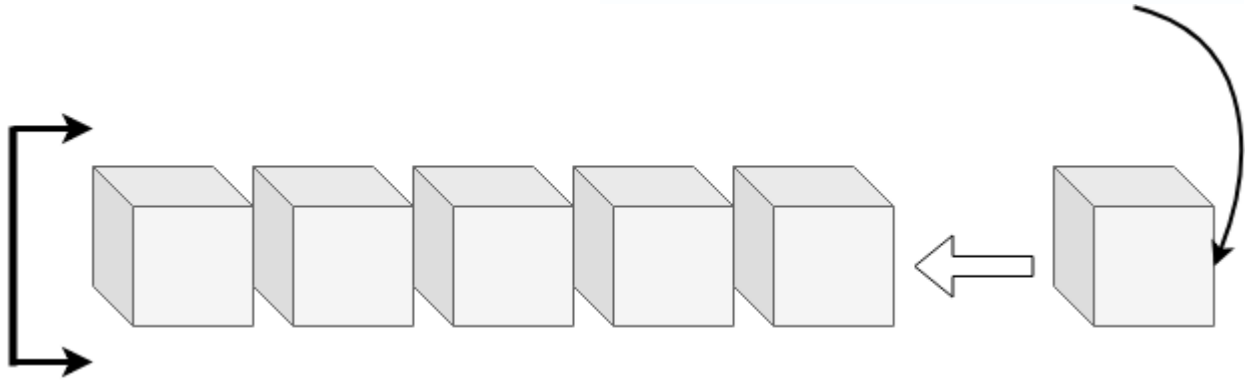
Роль биткойн-майнеров

В биткойн-сетях есть группа людей, известных как майнеры. В майнерах появился процесс и подтверждение транзакций. Подать заявку на несовершеннолетнего может любой желающий, а запустить клиент можно самостоятельно. Однако эти несовершеннолетние используют очень мощные компьютеры, специально предназначенные для майнинга биткойн - транзакций. Они делают это, фактически решая математические задачи и решая криптографические проблемы, потому что каждая транзакция должна быть криптографически закодирована и защищена. Эти математические проблемы гарантируют, что никто не подделает эти данные.

Кроме того, за эту задачу несовершеннолетним платят в биткойнах, что является ключевым компонентом в биткойнах. В Биткойне вы не можете создавать деньги, как обычные фиатные валюты, такие как доллар, евро и юань. Биткойн создается путем вознаграждения этих несовершеннолетних за их работу по решению математических и криптографических задач.

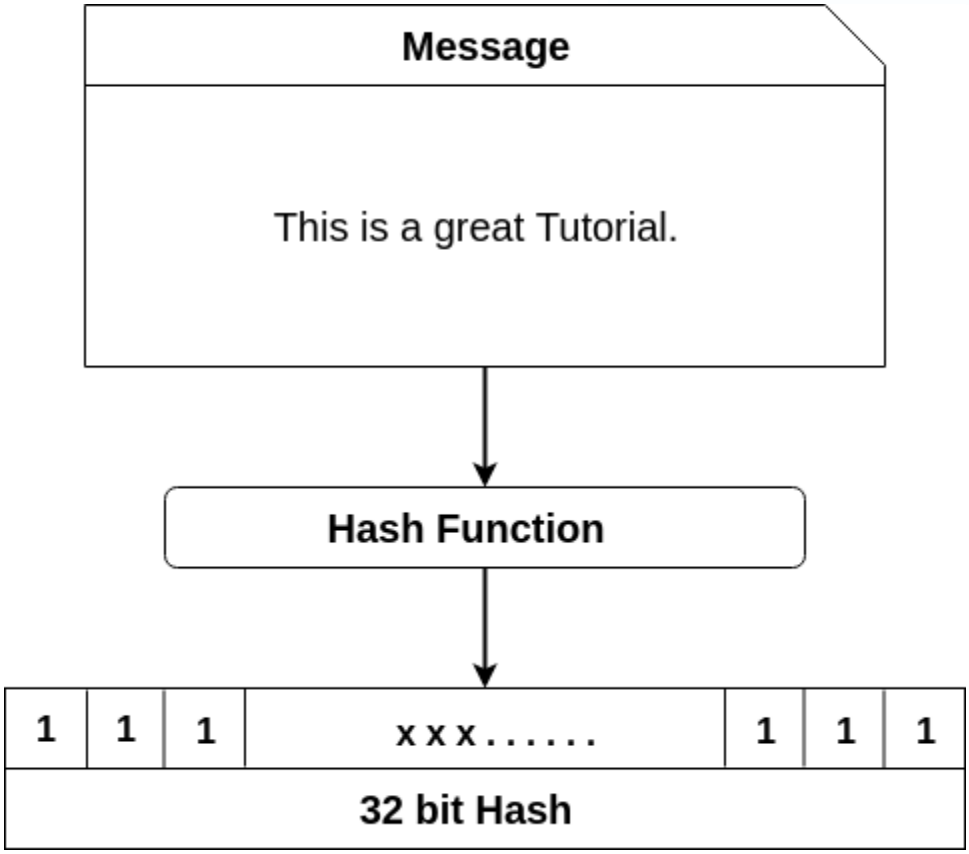
Как строится блокчейн Биткойн?

Роль несовершеннолетнего заключается в создании блокчейна записей, который формирует реестр биткойнов. Эти регистры называются блоками, и каждый блок содержит все различные транзакции, которые произошли. Новый блок добавляется каждые 10 минут, когда происходит новая биткойн-транзакция. Таким образом, когда миноры обрабатывают эти разные транзакции, они создают блок, и когда блок подтверждается, он добавляется в цепочку блоков. Биткойн-блокчейн обеспечивает постоянную запись всех биткойн-транзакций с самого начала.



ХЕШ-ФУНКЦИЯ БЛОКЧЕЙНА

Хэш-функция принимает входную строку (числа, алфавиты, медиафайлы) любой длины и преобразует ее в фиксированную длину. Фиксированная битовая длина может варьироваться (например, 32-битная, 64-битная, 128-битная или 256-битная) в зависимости от используемой хеш-функции. Выход фиксированной длины называется хэшем. Этот хэш также является криптографическим побочным продуктом алгоритма хеширования. Мы можем понять это из следующей диаграммы.



Алгоритм хеширования обладает некоторыми уникальными свойствами:

- Он производит уникальный вывод (или хэш).
- Это односторонняя функция.

В контексте криптовалют, таких как Биткойн , блокчейн использует свойства этой криптографической хэш-функции в своем механизме консенсуса. Криптографический хеш — это дайджест или цифровые отпечатки определенного количества данных. В криптографических хеш-функциях транзакции принимаются в качестве входных данных и обрабатываются алгоритмом хэширования, который дает выходные данные фиксированного размера.

SHA -256

Блокчейн Биткойн использует алгоритм хэширования SHA-256 (Secure Hash Algorithm). В 2001 году Агентство национальной безопасности (АНБ) США разработало алгоритм хеширования SHA-256.

Как работает процесс хеширования?

Для этой хэш-функции мы будем использовать программу, разработанную Андерсом Браунвортом. Эту программу можно найти по ссылке ниже.

Хэш-программа Андерса Браунворта: https://anders.com/blockchain/hash.html

Если мы введем какой-либо символ в разделе данных, мы увидим соответствующий криптографический хеш в разделе хэша.

Например: У нас есть тип в разделе данных: Это отличный учебник.

Он сгенерирует соответствующий хэш:

759831720aa978c890b11f62ae49d2417f600f26aaa51b3291a8d21a4216582a

Теперь если мы изменим текст: « Это отличный учебник ». Чтобы « это отличный учебник ».

Вы найдете соответствующий хэш:

4bc35380792eb7884df411ade1fa5fc3e82ab2da76f76dc83e1baecf48d60018

В приведенном выше примере вы можете видеть, что мы изменили только первое предложение регистра символов с заглавной «T» на маленькую «t», и это изменит все значение хэша.

Примечание. Если мы снова напишем тот же текст в разделе данных, он всегда будет давать один и тот же результат. Это потому, что вы создаете дайджест сообщения определенного объема данных.

Поскольку хэш-функция является односторонней, невозможно получить весь текст из сгенерированного хеша. Это отличается от традиционных криптографических функций, таких как шифрование, когда вы можете зашифровать что-то с помощью ключа, а с помощью расшифровки вы можете расшифровать сообщение в его исходную форму.

ХЕШИРОВАНИЕ БЛОКОВ БЛОКЧЕЙНА

В этом разделе мы узнаем, как SHA-256 применяется для создания блока в блокчейне. Мы обсудим здесь в контексте блокчейна Биткойн и поймем, как это связано с ролью майнеров. Несовершеннолетние на самом деле находятся в процессе построения блоков, и эти блоки добавляются в цепочку блоков, чтобы построить то, чем будет цепочка биткойнов.

На изображении ниже вы можете видеть, что этот блок состоит из номера блока, поля данных, связанного с ним криптографического хэша и одноразового номера.

На изображении выше сгенерированный хэш будет выглядеть как 00001acbm010gfh1010xxx. Я хотел бы отметить, что этот хэш имеет четыре начальных нуля. Четыре начальных нуля описывают, является ли блок действительным или нет. Для практических целей вы увидите, что этот хэш соответствует одноразовому номеру, а номер блока соответствует доступным данным. Поскольку хэш имеет четыре начальных нуля, следовательно, это допустимый блок.

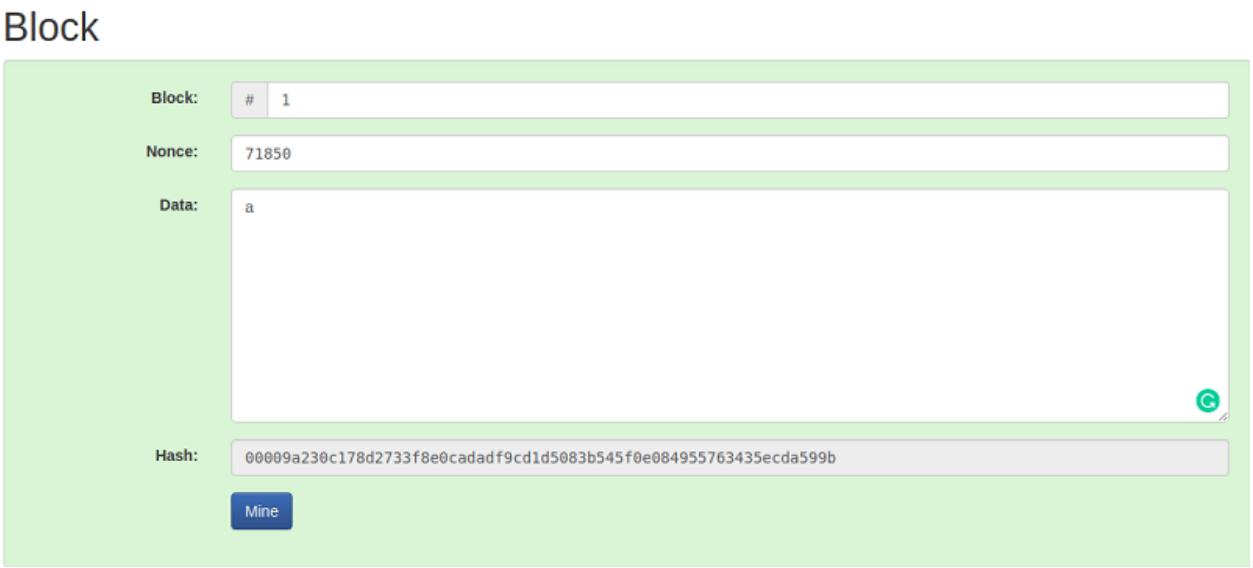
Если мы внесем какие-либо изменения в раздел данных, это даст совершенно другой хеш, который можно показать на изображении ниже.

Если вновь сгенерированный хэш не имеет четырех начальных нулей, то он не будет действительным блоком. Чтобы сделать блок действительным, мы сделаем это, используя поле с именем nonce .

Nonce означает число, используемое один раз в криптографической связи, так что хэш блока соответствует определенному критерию. Этот критерий может быть сгенерирован хэшем, у которого первые четыре цифры должны быть равны нулю. Таким образом, сгенерированный хэш будет выглядеть как 00001acbm010gfh1010xxx .

Nonce — это, по сути, случайное число, которое определяет, как вы можете заставить этот конкретный блок предоставить вам действительный хэш. Это можно сделать, изменив одноразовый номер вручную. Как правило, майнер начинает со значения Nonce, равного 1, и продолжает увеличивать его до тех пор, пока сгенерированный хэш не будет соответствовать указанному критерию. Таким образом, может потребоваться несколько итераций, пока не будет сгенерирован желаемый хэш с четырьмя ведущими нулями. Ожидаемое время генерации блока в системе биткойн составляет 10 минут. Как только майнер успешно добывает блок, он освобождает этот блок в системе и делает его последним блоком в цепочке.

В хеш-программе Андерса Браунворта, когда мы нажимаем кнопку «мой», как показано на изображении, это дает действительный блок. Этот блок имеет уникальный одноразовый номер с четырьмя нулями в начале хеша.

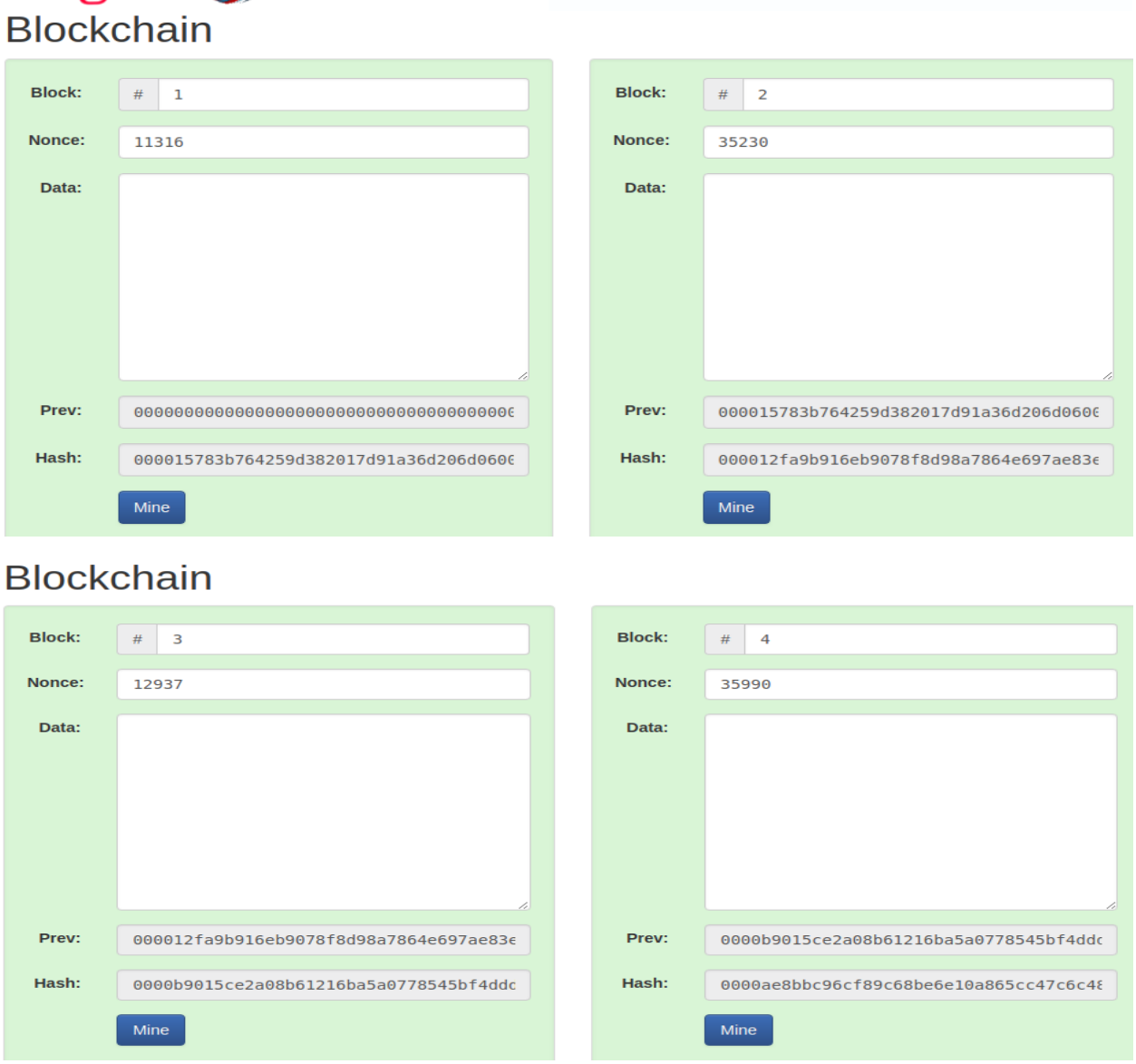


КАК РАБОТАЮТ ХЭШИ БЛОКОВ В БЛОКЧЕЙНЕ

Блокчейн — это концепция хранения данных в цифровом виде. Эти данные поступают блоками. Эти блоки связаны друг с другом и делают данные неизменяемыми . Когда блок данных связан с другими блоками, его данные больше никогда не могут быть изменены. Он будет общедоступен для всех, кто захочет увидеть его снова, и будет доступен в той же последовательности, в которой он был добавлен в блокчейн. Никто не может изменить информацию после ее добавления в блокчейн.

В предыдущем разделе мы узнали, как встроить блок и криптографические связи хеширования в весь процесс. Здесь вы можете увидеть, как блокчейн использует все эти концепции вместе, чтобы сохранить целостность полной цепочки блоков.

Представьте себе набор блоков данных транзакций, как показано на следующем изображении.



На изображениях выше вы можете видеть, что блок собирается в хронологическом порядке . За блоком номер один следует блок номер два, затем блок номер три, затем блок номер четыре, и вы можете продолжать так долго, как хотите. Здесь вы обнаружите, что есть поле номера блока , поле данных , поле одноразового номера, поле хэш -значения и предыдущее поле . Предыдущее поле соответствует полю хэш-значения предыдущего блока.

Мы знаем, что каждый блок в блокчейне криптографически привязан к следующему блоку. В приведенном выше примере предыдущее поле в первом

блоке равно нулю, потому что в первом блоке нет предыдущего хэш-значения, поэтому его значение равно нулю. Во втором блоке вы обнаружите, что в предыдущем поле есть хеш-значение, которое ссылается на хэш-значение предыдущего блока. Этот процесс продолжается до последнего блока.

Теперь представьте, изменились ли данные в каком-либо блоке. Допустим, мы изменили блок номер 2, данные в блоке 2 теперь другие, и майнинг блока также получает новую подпись . Подпись, соответствующая этому новому набору данных, больше не привязана к другим блокам. Он просто разбивает блок номер 2, потому что хеш больше недействителен, а также делает недействительным каждый отдельный блок, который идет после него до конца цепочки. Это указывает другим пользователям этой цепочки блоков, что некоторые данные в блоке 2 были изменены, и, поскольку блок-цепочка должна быть неизменной, они отклоняют это изменение, возвращаясь к предыдущей записи цепочки блоков, где все блоки все еще связаны друг с другом. Это главное преимущество блокчейна.

Теперь, если вы попытаетесь исправить это, единственный способ сделать это, выяснив одноразовый номер, который был объяснен в предыдущем уроке. Итак, мы берем один блок и пробуем его. Если он не дает корректного хэша, попробуйте два, три, четыре, и если ни один из них не сработает, то просто майните его. Когда вы майните блок, система определяет, что хэш действителен, так как он имеет четыре начальных нуля. Но, как вы заметили, когда вы пытаетесь хэшировать блок номер два, этот хэш не имеет четырех начальных нулей. Следовательно, это все еще недопустимый блок. Так что вам придется майнить и этот блок. Кроме того, вы должны сделать это с каждым отдельным блоком до начала цепочки, чтобы решить проблему.

Понимание важности четырех начальных нулей в хеше

Теперь поговорим о том, как важно иметь четыре ведущих нуля. Эти четыре начальных нуля связаны с так называемым уровнем сложности. Уровень сложности — это то, что привязано и встроено в сеть блокчейна и определяет, насколько сложно вам получить эквивалентный криптографический хэш для блока. В этом случае этот уровень сложности требует, чтобы у нас был хэш меньше, чем у нас есть в цели.

Для этой конкретной цели нам понадобится цель, имеющая как минимум четыре начальных нуля. Например , если целью хеша является 0000a1b2c3d4e5f6 , любой хеш, меньший или равный этому числу, является допустимым хэшем блока. Многие хэши удовлетворяли бы этому требованию, и любой из них был бы действительным. Однако найти такой хэш — сложная задача. Чем меньше цель хэша, тем сложнее найти действительный хэш.

Эти уровни сложности со временем увеличиваются по мере того, как в сеть биткойн добавляются новые компьютеры для криптографического хеширования. Таким образом, большая вычислительная мощность означает, что уровень сложности должен повышаться. Этот уровень сложности корректируется каждые две недели, чтобы гарантировать, что компьютеру, который фактически конкурирует за решение этих криптографических проблем, потребуется примерно 10 минут, чтобы добыть новый блок.

Примечание. Один блок каждые 10 минут = 6 блоков в час, 6 x 24 в день и 6 x 24 x 14 = 2016 блоков за две недели.

Например: если бы мы нашли хэш меньше или равный 0FFFF, у нас было бы 65 536 вариантов. Однако, если бы мы нашли хэш, меньший или равный 000FF, у нас было бы только 256 вариантов. Меньшее целевое число означает меньше вариантов. Обычно чем больше начальных нулей требуется в нашем хэше, тем сложнее найти правильный хэш.

БЛОКЧЕЙН РАСПРЕДЕЛЕННЫЙ РЕЕСТР

Распределенный реестр — это тип базы данных, которая совместно используется , реплицируется и синхронизируется между участниками децентрализованной сети. Вся информация в этой книге надежно и точно хранится с использованием криптографии . Доступ к этой информации можно получить с помощью ключей и криптографических подписей. Распределенный реестр позволяет транзакциям иметь публичных свидетелей , что затрудняет кибератаку. Он записывает транзакции, такие как обмен активами или данными, между участниками сети.

Все участники сети управляют и согласовывают обновления записей в реестре. Центральный орган отсутствует , или сторонние посредники, такие как финансовые учреждения или государственные учреждения, не участ-

вуют. Каждая запись в распределенном реестре имеет метку времени и уникальную криптографическую подпись. Это делает реестр проверяемой и неизменной историей всех транзакций в сети.

Далее, если в реестр вносятся какие-либо изменения, они отражаются и копируются всем участникам в секундах или минутах. Другими словами, когда в леджере происходят какие-либо изменения или обновления, каждый узел создает новую транзакцию, а затем узлы голосуют по алгоритму консенсуса, какая копия является правильной. Как только алгоритм консенсуса определен, все остальные узлы обновляют себя новой и правильной копией леджера.

Основным преимуществом распределенного реестра является отсутствие центральной власти. Поскольку мы знаем, что централизованные реестры подвержены кибератакам, распределенные реестры по своей природе очень трудно атаковать. Это связано с тем, что все распространяемые копии должны быть атакованы одновременно, чтобы атака была успешной.

ОСНОВНЫЕ КОМПОНЕНТЫ БИТКОЙНА

В этом разделе мы узнаем о четырех основных компонентах биткойна. Эти четыре элемента помогут нам лучше понять блокчейн биткойна. Здесь мы поместим каждый объект, который мы изучили ранее, в одну СЦЕНУ. Как мы знаем, блок состоит из хэша и сложной криптографической среды, но это только одна сторона медали. Биткойн-блокчейн интереснее, чем мы думали.

Мы можем увидеть основные компоненты биткойна на следующем изображении:

Программное обеспечение

Криптография

Аппаратное обеспечение

Шахтеры (теория игр)

Первый компонент: программное обеспечение

Биткойн — это в основном программное обеспечение, которое определяет, что такое биткойн, а также то, как биткойн передается. Он определяет, каковы правила действительного биткойна, кто может находиться внутри биткойна, кто не может быть внутри биткойна, что является действительным, а что нет и т. д. Все основано на программном обеспечении, которое является программным обеспечением биткойна. Программное обеспечение биткойн всегда работает в режиме 24*7.

Второй компонент: Криптография

Программное обеспечение по своей сути использует криптографию и биткойн в качестве криптовалюты. Биткойн использует криптографию для регулирования передачи биткойнов между сторонами, а также для создания но-

вых единиц биткойнов. Без криптографии Биткойн был бы просто невозможен. Итак, мы получили, что это программное обеспечение использует криптографию для управления передачей биткойнов через Интернет.

Криптография — это математический подход, который может решить компьютер, а не человек. Таким образом, все, что защищает ваши данные, обслуживается криптографией.

Третий компонент: оборудование

Для запуска и решения криптографии требуется АППАРАТНОЕ ОБЕСПЕЧЕНИЕ. Это оборудование состоит из тысяч майнеров по всему миру, работающих на своих компьютерах. Таким образом, по всему миру есть тысячи компьютеров, на которых в основном работает программное обеспечение Биткойн или клиент Биткойн. Это оборудование специально разработано для поиска одноразового номера для проверки блока и хэша. Для выполнения простой задачи в блокчейне биткойнов требуется много ресурсов процессора.

Если вы попытаетесь майнить биткойны прямо сейчас со своего смартфона или домашнего компьютера, то в конечном итоге вы потеряете свой компьютер вместе с огромным счетом за электричество.

Четвертый компонент: майнинг (теория игр)

Майнеры — это пользователи, вовлеченные в игровую теорию, потому что биткойн — это действительно игра, которой управляют эти майнеры по всему миру. Выше мы видели, что первый компонент — это программное обеспечение для биткойнов , которое выдает криптографический вызов каждые 10 минут. Задача криптографии заключается в попытке найти одноразовый номер, который сделает хэш для определенного блока действительным. Все хэши и проверки выполняются этими майнерами. После успешного создания блока новый блок добавляется в блокчейн.

Давайте посмотрим, как работает теория игр!

Программное обеспечение Биткойн создает проблему. Теперь начинается игра, и начинается гонка. В гонке участвуют все эти майнеры, соревнующиеся друг с другом за решение задач.

Выполнение этой задачи или задачи займет примерно 10 минут.

Каждый майнер начинает пытаться найти решение для этого одноразового номера, которое удовлетворит хеш для блока.

В какой-то конкретный момент один из тех майнеров в мировом сообществе с более высокой скоростью и отличными характеристиками оборудования решит задачу криптографии и станет победителем этой гонки.

Теперь остальная часть сообщества начнет проверять этот блок, добытый победителем. Это делает Биткойн таким сильным, потому что на одном этапе этого цикла майнеры соревнуются друг с другом, а на следующем этапе цикла остальная часть сообщества объединяется, чтобы обеспечить правильность этого решения.

Если одноразовый номер правильный, он будет содержать новый блок, который будет добавлен в цепочку блоков.

За это задание или испытание победитель получит награду. Эта награда в настоящее время составляет 12,5 биткойнов.

БЛОКЧЕЙН ДОКАЗАТЕЛЬСТВО РАБОТЫ

Proof of Work (PoW) — это оригинальный алгоритм консенсуса в сети блокчейн. Алгоритм используется для подтверждения транзакции и создает

новый блок в цепочке. В этом алгоритме миноры (группа людей) соревнуются друг с другом за совершение транзакции в сети. Процесс конкуренции друг с другом называется майнингом . Как только майнеры успешно создали действительный блок, он получает вознаграждение . Самым известным применением Proof of Work (PoW) является биткойн.

Создание доказательства работы может быть случайным процессом с низкой вероятностью. В этом случае требуется много проб и ошибок , прежде чем будет сгенерировано действительное доказательство работы. Основной рабочий принцип доказательства работы — это математическая головоломка, решение которой можно легко доказать. Доказательство работы может быть реализовано в блокчейне с помощью системы подтверждения работы Hashcash.

На изображении ниже вы можете видеть, что этот блок состоит из номера блока, поля данных, связанного с ним криптографического хэша и одноразового номера. Nonce отвечает за то, чтобы сделать блок действительным.

В игре-головоломке биткойн - программное обеспечение создает вызов, и игра начинается. В этой игре все майнеры соревнуются друг с другом, чтобы решить задачи, и эта задача займет около 10 минут. Каждый майнер начинает пытаться найти решение для этого одноразового номера, которое удовлетво-

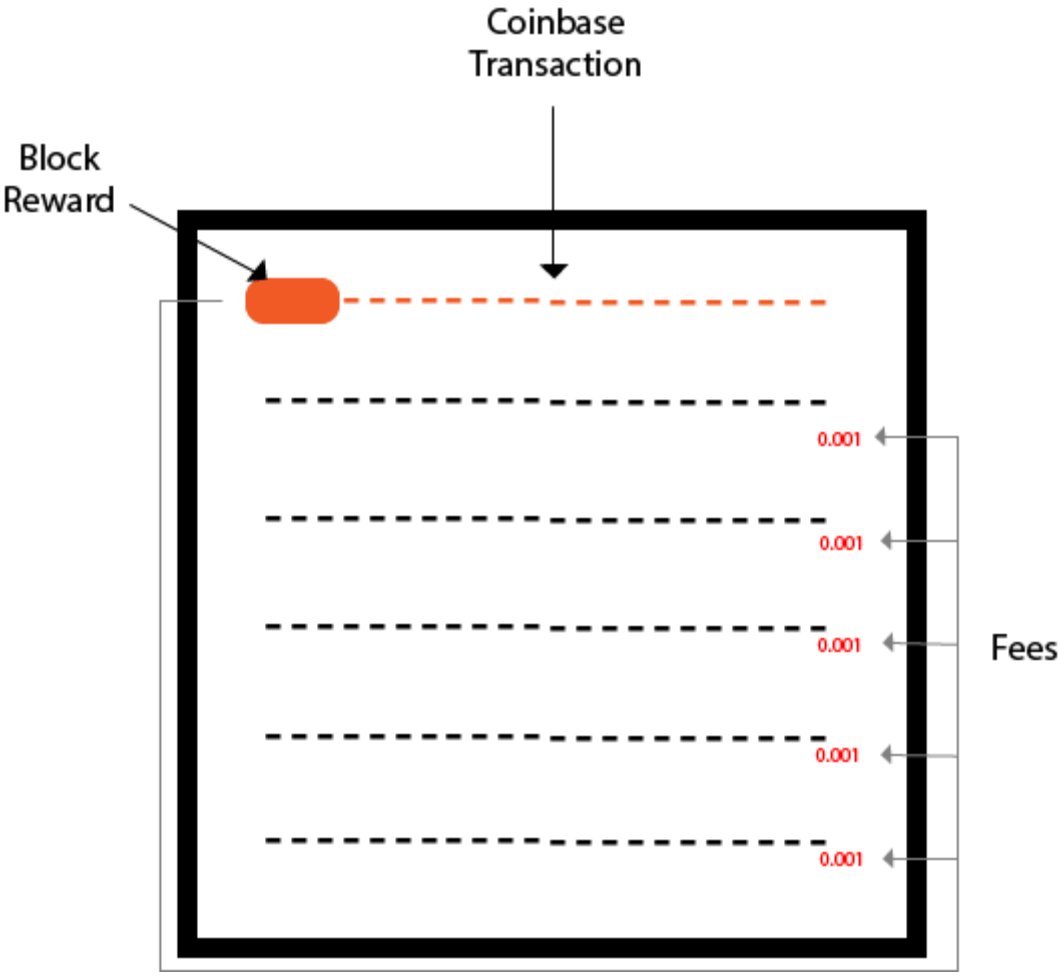
рит хеш для блока. В какой-то конкретный момент один из тех майнеров в мировом сообществе с более высокой скоростью и отличными характеристиками оборудования решит задачу криптографии и станет победителем игры. Теперь остальная часть сообщества начнет проверять этот блок, добытый победителем. Если одноразовый номер правильный, он будет содержать новый блок, который будет добавлен в цепочку блоков. Концепция создания блока дает четкое объяснение доказательства работы (PoW).

КОИНБЕЙС ТРАНЗАКЦИЯ

Coinbase-транзакция — это первая транзакция в блоке. Это уникальный тип биткойн-транзакций, который может быть создан майнером. Майнеры используют его для получения вознаграждения за блок за свою работу, и любые другие сборы за транзакции, взимаемые майнером, также отправляются в этой транзакции.

Объяснение

Каждая транзакция, выполненная в сети биткойн , объединяется вместе, чтобы сформировать блок. Когда блок формируется, он сразу же добавляется в блокчейн. Теперь эти блоки неизменны и защищены от несанкционированного доступа для всех транзакций, совершаемых в сети биткойнов. Каждый блок должен содержать одну или несколько транзакций, и первая транзакция в блоке называется транзакцией coinbase .



Майнеры всегда несут ответственность за создание блока. Когда блок будет успешно создан, он будет вознагражден биткойнами за свою работу. Вознаграждение за биткойн-блок всегда зависит от количества блоков из исходного блока и количества комиссий, включенных в транзакции блока. Общая сумма вознаграждения, которое получит майнер, представляет собой сумму вознаграждения за блок и комиссии за транзакции, взимаемой со всех транзакций, которые были включены в блок.

В начале биткойна вознаграждение за блок составляет 50 биткойнов за блок. Награда за блок уменьшается вдвое после каждых 210 000 блоков, то есть примерно каждые четыре года. Текущая награда за успешное создание блока составляет 12,5 биткойнов. В 2020 году он сократится до 6,25 биткойнов за блок.

Существует одна важная особенность транзакции coinbase: биткойны, участвующие в транзакции, не могут быть потрачены до тех пор, пока они не получат не менее 100 подтверждений блоков в блокчейне.

КЛЮЧЕВЫЕ ПОНЯТИЯ БИТКОЙН

Есть четыре ключевых понятия, которые вам нужно знать о биткойнах. Эти:

Без посредников

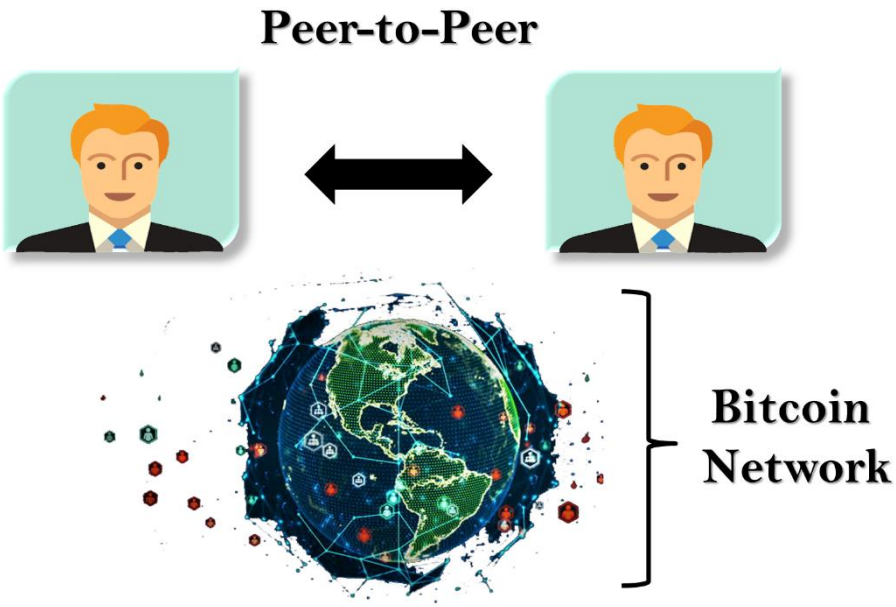
Распределенный

Децентрализованный

ненадежный

Без посредников

Когда вы отправляете деньги кому-то через Интернет, вам нужна третья сторона, такая как банки, которая управляет всеми вашими транзакциями. Но в Биткойне вы совершаете транзакции непосредственно с другой стороной через Интернет. Эта транзакция происходит в сети Биткойн. Эта сеть заботится о подтверждении и проверке того, что между двумя сторонами действительно произошла передача стоимости. Эта концепция называется Disintermediated.



Disintermediated — это действие по устранению посредника. Это один из ключевых компонентов, который делает блокчейн таким ценным, потому что он устраняет ненужную неэффективность, связанную с использованием третьей стороны во время передачи стоимости между сторонами.

Распределенный

Вся биткойн-сеть работает в сети из тысяч распределенных компьютеров, которые совместно работают. Таким образом, вместо того, чтобы иметь один централизованный компьютер, который обрабатывает рабочую нагрузку, вы распределяете ее между несколькими компьютерами. Распределенная сеть более надежна, поскольку в ней нет единой точки отказа. Здесь работа распределяется между тысячами компьютеров, которые все работают и разделяют рабочую нагрузку.

Децентрализованный

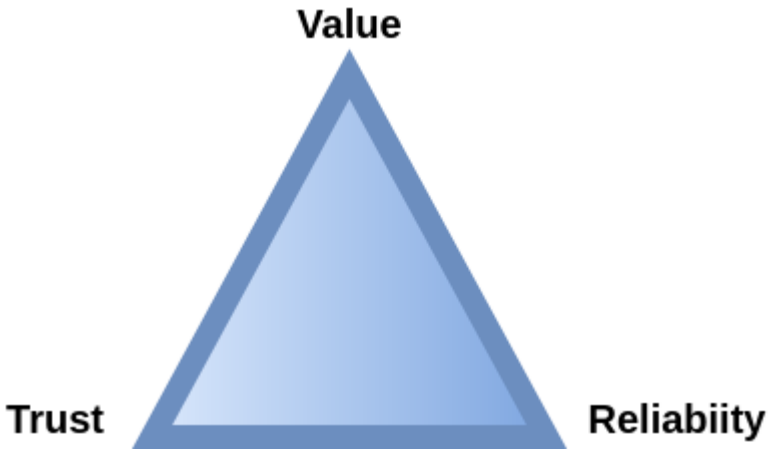
Биткойн децентрализован. Это означает, что нет никакого центрального контроля, никакого центрального хранилища данных и никакого управления посередине, которое наблюдает за тем, что делает Биткойн. В результате нет центральной точки отказа.

Ненадежный

Биткойн не требует доверия, потому что нет необходимости в третьей стороне, такой как банк, для сертификации и обеспечения доверия ко всему процессу транзакций. Вместо этого блокчейн и то, как Биткойн обрабатывает транзакции, позволяют доверять распределенному доверительному консенсусу, в котором все узлы соглашаются с тем, что транзакция имела место.

Ключевые области блокчейна

В технологии блокчейна биткойн является самой известной реализацией блокчейна. Существует много разработок, и направление основано на предпосылке того, что делает блокчейн, чтобы Биткойн мог появиться. Мы можем узнать и расширить, как это может распространиться на множество различных областей.



Технология блокчейн исправляет три вещи, для которых Интернет не был предназначен. Вот эти три вещи:

Стоимость

Доверять

Надежность

Стоимость

С помощью блокчейна вы действительно можете создать ценность цифрового актива. Стоимостью может управлять тот человек, которому она принадлежит. Это позволяет передавать уникальный актив через Интернет без промежуточного централизованного агента.

Доверять

Блокчейн позволяет безопасно назначать право собственности на определенный цифровой актив и иметь возможность отслеживать, кто на самом деле контролирует этот актив в определенный момент времени. Другими словами, блокчейн создает постоянную, безопасную и неизменную запись о том, кому что принадлежит. Он использует передовую хеш-криптографию для сохранения целостности информации.

Надежность

Блокчейн распределяет их рабочую нагрузку между тысячами разных компьютеров по всему миру. Это обеспечивает надежность, потому что если у вас все локализовано в одном месте, это становится единой точкой отказа. Но его децентрализованная сетевая структура гарантирует отсутствие единой точки отказа, которая может вывести из строя всю систему.

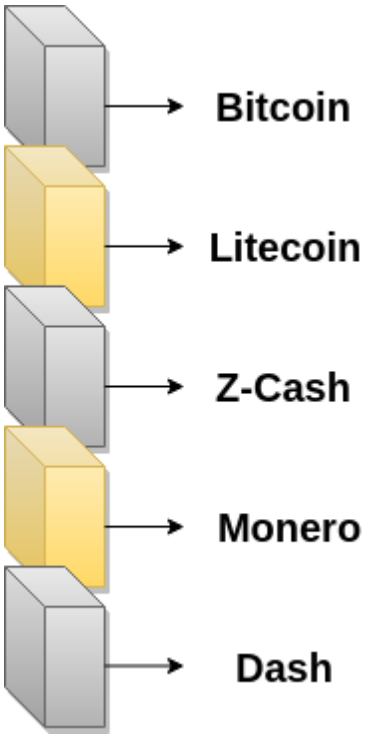
БЛОКЧЕЙН КРИПТОВАЛЮТА

Криптовалюта — это тип цифрового актива , который используется для обмена ценностями между сторонами. Он использует надежную криптографию для защиты финансовых транзакций и контроля создания новых единиц этой валюты и проверки передачи активов. Криптовалюта не существует физически.

Мы знаем, что правительство печатает государственные валюты, такие как фиатные валюты, такие как доллар, иена или юань. Это означает, что существует централизованное учреждение, которое может создавать тысячи, миллионы или миллиарды этой валюты. В отличие от государственных валют, таких как биткойн, валюты этого типа создаются по тем же математическим

формулам, которые заставляют работать криптовалюту. Таким образом, криптовалюты используют децентрализованный контроль, который работает через технологию распределенного реестра, которая служит общедоступной базой данных финансовых транзакций.

Сегодня доступно множество различных типов криптовалют. Некоторые из них приведены ниже.



Биткойн

Биткойн широко известен как первая децентрализованная криптовалюта. Он создается сетью из тысяч конкретных узлов, называемых майнерами . Майнеры могут обрабатывать транзакции биткойнов в сети блокчейн. С момента выпуска биткойна в настоящее время доступно более 4000 альтернативных вариантов биткойна.

Лайткоин

Криптовалюта Litecoin работала очень похоже на биткойн. Мы знаем, что биткойн ожидает обработки блока транзакции десять минут , а лайткойн может сделать это максимум за две с половиной минуты . Litecoin не имеет большой рыночной капитализации. Цена Litecoin ниже, чем биткойн, но это очень эффективный процесс, который также имеет некоторые отличия от биткойнов.

Z-наличные

Z-Cash — это цифровая валюта, защищающая конфиденциальность, которая основана на сильных научных данных в области криптографии. Он обеспечивает повышенную конфиденциальность для своих пользователей по сравнению с другими криптовалютами, такими как биткойн. Здесь данные транзакций остаются конфиденциальными, что стало возможным благодаря доказательствам с нулевым разглашением . Это позволяет проверять транзакции без какой-либо информации об отправителе, получателе и сумме транзакции.

Функции Z-Cash, известные как просмотр ключей и раскрытие платежа , позволяют раскрывать некоторые данные о транзакциях пользователя. Это делает транзакции на Z-Cash проверяемыми и соответствующими нормативным требованиям.

Монеро

Monero — это криптовалюта с открытым исходным кодом, ориентированная на неотслеживаемость , конфиденциальность и децентрализацию . Это быстрые, частные и безопасные цифровые деньги, которыми управляет сеть пользователей. Мы можем использовать его для покупки и продажи вещей и обмена на другие монеты или жетоны.

Он использует особый тип криптографии, который гарантирует, что транзакции остаются неотслеживаемыми на 100%. Он фокусируется на анонимности, которую труднее отследить, в то время как биткойн является псевдонимным, транзакции которого все еще отслеживаются.

Бросаться

Dash — это сокращенная форма Digital Cash . Это криптовалюта с открытым исходным кодом и форма децентрализованной автономной организации, которой управляет группа пользователей, называемая главными узлами. Это одна из самых перспективных альтернатив биткойнам. Он позволяет проводить очень быстрые транзакции, которые невозможно отследить.

БЛОКЧЕЙН DAO

DAO расшифровывается как Децентрализованная автономная организация . Как следует из названия, это организация одновременно автономная и

децентрализованная. Иногда его также называют децентрализованной автономной корпорацией (DAC), но чаще используется термин DAO, поскольку не все организации являются корпорациями.

DAO — это организация, которая представлена правилами, закодированными в виде прозрачной компьютерной программы, контролируемой акционерами и не зависящей от центрального правительства. DAO — это самая сложная форма смарт-контракта . Смарт-контракт — это компьютерная программа, которая автономно существует в Интернете, но в то же время нуждается в людях для выполнения задачи, которую он не может выполнить сам по себе.

Запись финансовых транзакций DAO и правила программы хранятся в блокчейне. Поскольку DAO работает на блокчейне и в распределенной сети, у вас может быть несколько комбинаций разных сторон, обменивающихся ценностями и достигающих соглашений. Это означает, что для децентрализованной автономной организации не имеет значения, человек вы или робот. На самом деле у вас могут быть устройства, взаимодействующие с устройствами, или устройства, взаимодействующие с людьми, или люди, общающиеся с людьми.

Как работает DAO?

Децентрализованная автономная организация работает по правилам, закодированным в виде компьютерной программы, называемой смарт-контрактами. Смарт-контракт — это объект, который живет в Интернете и существует автономно. У него также есть люди для выполнения определенной задачи, которую не может выполнить сама программа автоматизации.

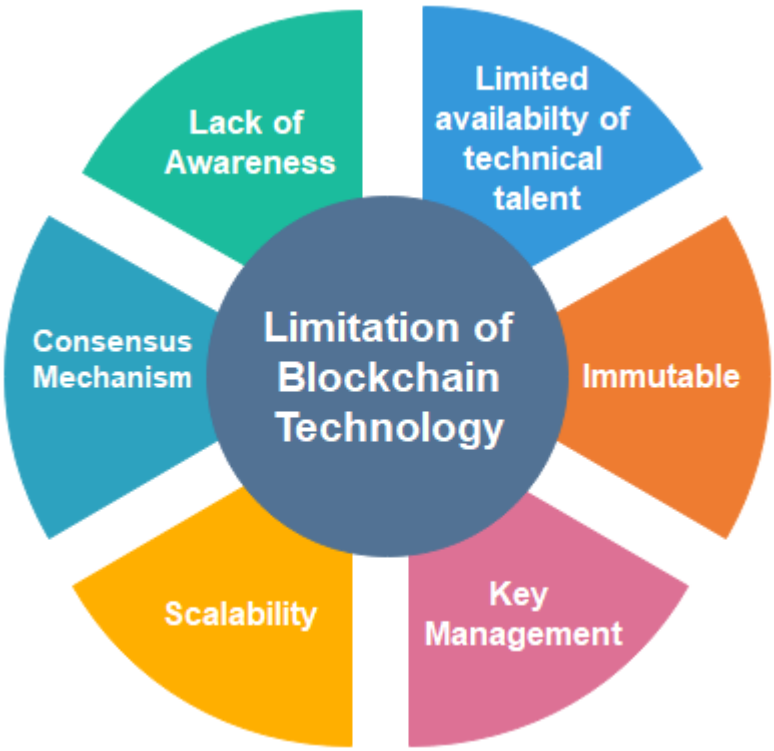
Давайте возьмем пример Uber, чтобы понять работу DAO . Uber — это организация, которая позволяет вам вызывать машину для себя с помощью мобильного приложения. После того, как вы позвоните, водитель подъедет на машине, заберет вас и отвезет к месту назначения. Приложение позаботится об

обработке платежа, а водитель отправится к следующему гонщику. Мобильное приложение управляет всем процессом. Однако есть человеческий компонент, который является водителем, который подъезжает и уезжает.

Теперь, если вы подключаете искусственный интеллект, нет причин, чтобы водитель подходил и взаимодействовал с вами. К вам может приехать беспилотный автомобиль и забрать вас. Все это автоматизировано и выполняется автоматически, поэтому вы можете обрабатывать платежи непосредственно в приложении, и автомобиль будет взаимодействовать с вами напрямую, без участия человека. Этот тип процесса может быть преобразован в децентрализованную автономную организацию. Теперь это не обязательно означает, что вас нужно заменить компьютером. На самом деле у вас может быть несколько человек в распределенной сети, и эти люди будут достигать этих соглашений на основе смарт-контрактов между собой.

ОГРАНИЧЕНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН

Технология блокчейн обладает огромным потенциалом в создании децентрализованных приложений, не требующих доверия. Но это не идеально. Существуют определенные барьеры, которые делают технологию блокчейна неправильным выбором и непригодной для основного применения. Мы можем видеть ограничения технологии блокчейна на следующем изображении.



Недостаточная информированность

Существует много дискуссий о блокчейне, но люди не знают истинной ценности блокчейна и того, как они могут реализовать его в различных ситуациях.

Ограниченная доступность технических талантов

Сегодня доступно множество разработчиков, которые могут делать много разных вещей в каждой области. Но в технологии блокчейн не так много раз-

работчиков, обладающих специальными знаниями в области технологии блокчейн. Следовательно, отсутствие разработчиков является препятствием для разработки чего-либо на блокчейне.

Неизменный

В immutable мы не можем вносить какие -либо изменения ни в одну из записей. Это очень полезно, если вы хотите сохранить целостность записи и убедиться, что никто никогда не вмешивается в нее. Но у неизменности есть и недостаток.

Мы можем понять это в том случае, когда вы хотите внести какие-либо изменения или хотите вернуться и сделать какие-либо изменения. Например , вы обработали платеж и вам нужно вернуться и внести поправку, чтобы изменить этот платеж.

Ключевой менеджмент

Как мы знаем, блокчейн построен на криптографии, что подразумевает наличие разных ключей, таких как открытые ключи и закрытые ключи. Когда вы имеете дело с закрытым ключом, вы также рискуете, что кто-то может потерять доступ к вашему закрытому ключу. Это часто случается в первые дни, когда биткойн не стоил так много. Люди просто собирали много биткойнов, а затем внезапно забывали, какой у них ключ, а сегодня они могут стоить миллионы долларов.

Масштабируемость

Блокчейн, как и биткойн, имеет механизмы консенсуса, которые требуют, чтобы каждый участвующий узел проверял транзакцию. Он ограничивает количество транзакций, которые может обрабатывать сеть блокчейн. Таким образом, биткойн не был разработан для проведения крупномасштабных транзакций, которые делают многие другие учреждения. В настоящее время биткойн может обрабатывать максимум семь транзакций в секунду .

Механизм консенсуса

В блокчейне мы знаем, что блок может создаваться каждые 10 минут. Это потому, что каждая совершенная транзакция должна гарантировать, что каждый блок в сети блокчейна должен достичь общего консенсуса. В зависимости от размера сети и количества блоков или узлов, задействованных в цепочке блоков, обратная связь, необходимая для достижения консенсуса, может потребовать значительного количества времени и ресурсов.

ДВОЙНЫЕ ТРАТЫ НА БЛОКЧЕЙНЕ

Двойная трата означает двойную трату одних и тех же денег. Как известно, любая транзакция может быть обработана только двумя способами. Один офлайн, другой онлайн.

Оффлайн: транзакция, в которой используется физическая валюта или наличные деньги, называется офлайн-транзакцией.

Онлайн: транзакция, в которой используются цифровые деньги, называется онлайн-транзакцией.

Рассмотрим этот пример:

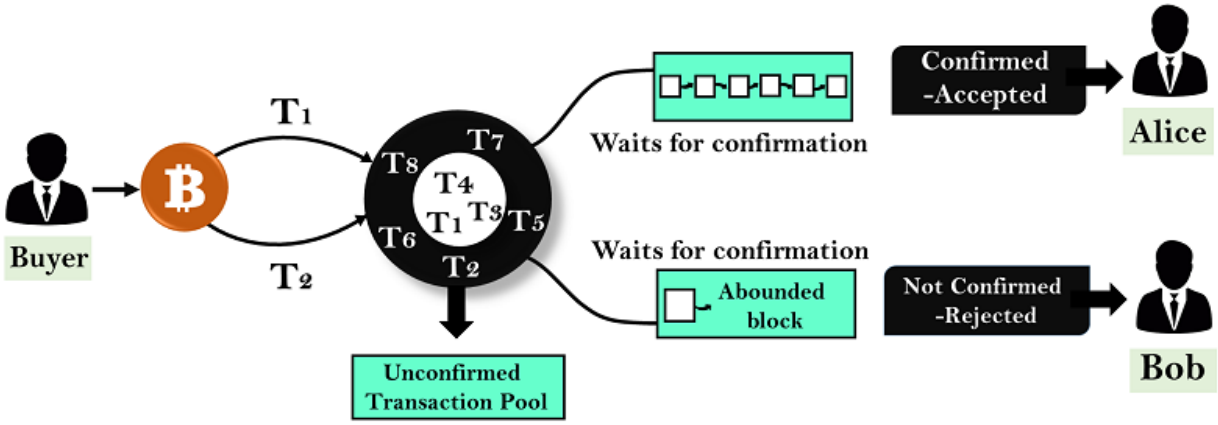
Вы идете в рестораны и заказываете капучино стоимостью 5 долларов. Вы платите наличными. Поставщик услуг в ресторане мгновенно подтвердил, что вы заплатили, и вы получили свой кофе в обмен на деньги. Теперь можно потратить те же 5 долларов где-то еще, чтобы сделать еще одну покупку? Ответ НЕТ . Но что, если ответ ДА ? Это означает, что один и тот же человек может использовать одни и те же деньги более одного раза. Этот тип проблемы известен как проблема двойной траты.

В физической валюте никогда не может возникнуть проблема двойной траты. Но в цифровых деньгах, подобных биткойнам, может возникнуть проблема двойного расходования средств. Следовательно, биткойн-транзакции могут быть скопированы и ретранслированы. Это открывает возможность того, что один и тот же BTC может быть потрачен его владельцем дважды.

Как Биткойн решает проблему двойных расходов?

Биткойн решает проблему двойной траты, реализуя механизм подтверждения и поддерживая универсальную бухгалтерскую книгу, называемую блокчейном.

Предположим, у вас есть 1 BTC и вы пытаетесь потратить его дважды. Вы совершили транзакцию в размере 1 BTC для Алисы. Вы снова подписываете и отправляете Бобу ту же транзакцию в 1 BTC. Обе транзакции попадают в пул неподтвержденных транзакций, где уже хранится много неподтвержденных транзакций. Неподтвержденные транзакции — это транзакции, которые никто не выбирает. Теперь любая транзакция, которая первой получила подтверждение и была проверена майнерами, будет считаться действительной. Другая транзакция, которая не смогла получить достаточное количество подтверждений, будет вытащена из сети. В этом примере транзакция T1 действительна, и Алиса получит биткойн.



Что произойдет, если обе транзакции будут совершены майнерами одновременно?

Предположим, что два разных майнера одновременно выбирают обе транзакции и начинают создавать блок. Теперь, когда блок будет подтвержден, и Алиса, и Боб будут ждать подтверждения своей транзакции. Та транзакция, которая первой получила подтверждение, будет проверена первой, а другая транзакция будет извлечена из сети.

Теперь предположим, что если и Алиса, и Боб получили первое подтверждение одновременно, то между Алисой и Бобом начнется гонка. Таким образом, какая бы транзакция не получила максимальное количество подтверждений из сети, она будет включена в блокчейн, а другая будет отброшена.

БЛОКЧЕЙН БИТКОЙН КЭШ

Bitcoin Cash — это одноранговые электронные деньги для Интернета. Он полностью децентрализован, без центрального банка и не требует для работы доверенных третьих сторон.

Bitcoin Cash — это криптовалюта, разработанная в результате хардфорка сети биткойн. Он появился в середине 2017 года. Bitcoin Cash отличается от Bitcoin. Это обновленная версия основного программного обеспечения биткойн. Это быстрее , дешевле и надежнее в использовании. Это увеличивает размер блока биткойнов с 1 МБ до 8 МБ и позволяет обрабатывать около двух миллионов транзакций в день.

Как появился Bitcoin Cash?

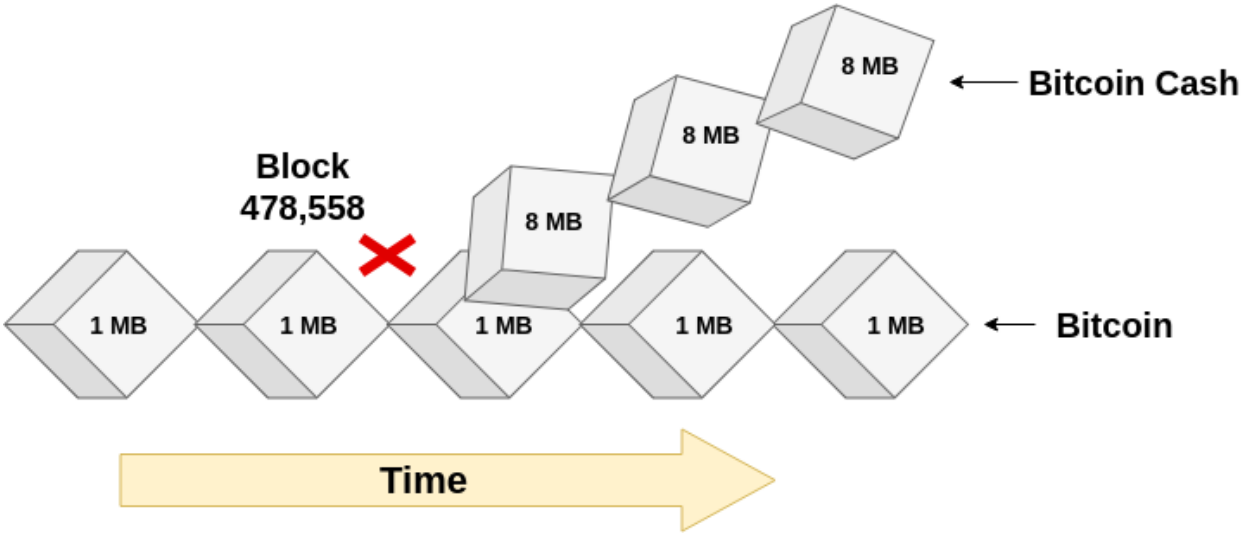
Блокчейн Биткойн — это постоянно обновляемая книга, в которой перечислены все транзакции, происходящие в сети Биткойн. В сети Биткойн первый блок транзакций произошел в январе 2009 года, и каждый новый блок добавляется в эту цепочку блоков Биткойн примерно каждые 10 минут. Биткойн-протокол гарантирует, что каждый отдельный блок, добавляемый в цепочку блоков, действителен и соответствует правилам биткойна. Кроме того, каждый блок, добавляемый в цепочку блоков, содержит криптографический хэш предыдущего блока.

1 августа 2017 года в блоке номер 478 558 произошел раскол . Пул ViaBTC создал блок размером 1,9 МБ, который недействителен в устаревшей сети Биткойн, поскольку биткойн имеет ограничение в 1 МБ. Этот новый блок не имел ограничения в 1 МБ, а вместо этого включал 1,9 МБ. Это вызывает раскол, который привел к созданию Bitcoin Cash. Компьютеры, которые добывают Bitcoin Cash, имеют протокол, который ограничивает размер блока 8 МБ, а не 1 МБ.

Что такое хардфорк биткойна?

Форк происходит, когда блокчейн разделяется на два разных пути вперед. В случае хардфорка биткойнов, чтобы увеличить скорость транзакций в сети, одна группа (майнеры) в сообществе биткойнов хотела увеличить размер блоков в цепочке биткойнов. В результате блокчейн биткойна может разделиться на две разные версии , что приведет к возникновению двух разных цепочек с отдельной монетой в каждой, что порождает Bitcoin Cash.

Как вы можете видеть на этой диаграмме, в сети происходит разделение, которое, по сути, создает новую цепочку блоков с измененными правилами. Оригинальная и разветвленная версия криптовалюты имели идентичные блокчейны вплоть до блока, когда произошло разделение. После разделения все, у кого были биткойны до хардфорка, получили одинаковое количество токенов Bitcoin Cash.



Чем отличается Bitcoin Cash от других криптовалют?

Биткойн Кэш основан на оригинальном исходном коде Биткойн с разницей в большем размере блоков (8 МБ).

В отличие от биткойнов, биткойн-кэш не нацелен на то, чтобы стать средством сбережения. Вместо этого его основные цели — использовать только для цифровых платежей.

БЛОКЧЕЙН-ИНТЕРВЬЮ: ВОПРОСЫ

Список наиболее часто задаваемых вопросов и ответов на интервью с Blockchain приведен ниже.

1) Что такое блокчейн?

Блокчейн — это постоянно растущий реестр (файл), в котором хранится постоянная запись обо всех совершенных транзакциях безопасным, хронологическим и неизменным способом. Его можно использовать для безопасной

передачи денег, имущества, контрактов и т. д. без необходимости стороннего посредника, такого как банк или правительство.

Блокчейн является основой самой известной криптовалюты под названием Биткойн. Это одноранговая система электронных денег и децентрализованная сеть, которая позволяет пользователям совершать транзакции напрямую без участия третьих лиц для управления обменом средств.

Чтобы узнать больше, нажмите здесь...

---

2) В чем разница между блокчейном Биткойн и блокчейном Эфириума?

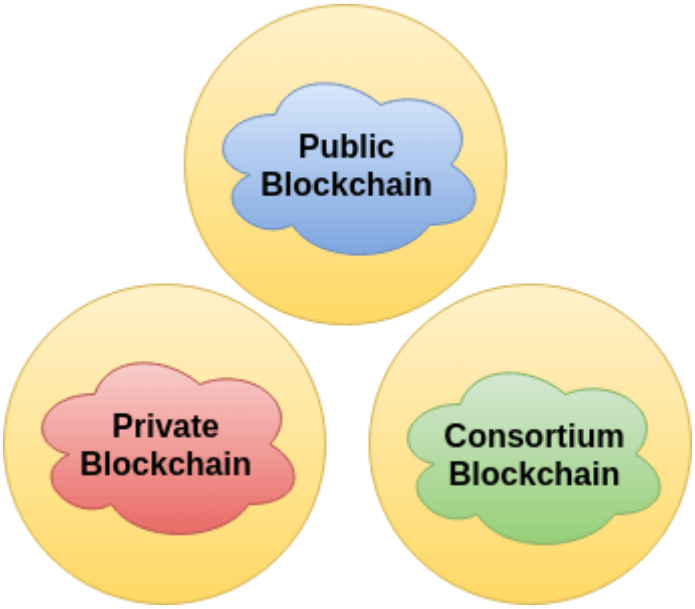
Мы можем увидеть основные различия между блокчейном Биткойн и блокчейном Эфириума в таблице ниже.

Точки	Биткойн Блокчейн	Блокчейн Эфириума
Основатель	Сатоши Накамото	Виталик Бутерин
Дата выпуска	9 января 2008 г.	30 июля 2015 г.
Метод выпуска	Блок Бытия добыт	Предпродажа
Применение	Цифровая валюта	Смарт-контракты
Криптовалюта	Использовал	Биткойн Эфир
Алгоритм	ША-256	Эташ
Блокирует время	10 минут	12-14 секунд
Масштабируемость	Еще нет	да

---

3) Какие существуют типы блокчейнов?

Различные типы блокчейнов, которые представляют миру:



В мире представлены в основном три типа блокчейнов.

1. Публичный блокчейн

Публичный блокчейн — это своего рода блокчейн, который предназначен « для людей, людьми и людьми ». Нет ответственности, это означает, что любой может читать, писать и проверять блокчейн. Это распределенная и децентрализованная публичная книга с открытым исходным кодом, поэтому любой может просматривать что угодно в общедоступной цепочке блоков. Они считаются блокчейном без разрешения .

2. Частный блокчейн

Частный блокчейн — это частная собственность человека или организации. Он контролируется единой организацией, которая определяет, кто может его читать, отправлять ей транзакцию и кто может участвовать в процессе консенсуса. Они считаются разрешенным блокчейном .

3. Блокчейн консорциума или федеративный блокчейн

В этом блокчейне процесс достижения консенсуса контролируется предварительно выбранной группой, т. е. группой компаний или представителями отдельных лиц. Эта предварительно отобранная группа собирается вместе и

принимает решения на благо всей сети. Такие группы также называются консорциумами или федерациями, поэтому название консорциум или федеративный блокчейн.

---

4) Где хранится блокчейн?

Блокчейн может храниться либо в виде плоского файла, либо в виде базы данных.

---

5) Какие типы записей присутствуют в базе данных блокчейна?

В базе данных блокчейна есть два типа записей.

Транзакционные записи

Блокировать записи

К обеим записям можно легко получить доступ, и они могут интегрироваться друг с другом без следования какому-либо сложному алгоритму.

---

6) Перечислите ключевые особенности блокчейна?

Важнейшими свойствами блокчейна являются:

Децентрализованные системы

Распределенный реестр

Более безопасная и надежная экосистема

Быстро

Низкие комиссии за транзакции

Отказоустойчивой

Чеканка

---

7) Чем Блокчейн отличается от реляционных баз данных?

Блокчейн отличается от реляционной базы данных следующими способами.

Точки	Блокчейн	Реляционная база данных
Единица данных	Блокировать	Стол
Отказ	Никто	Может случиться
Централизованное управление	Нет	да
Модификация данных	Невозможно	Возможно
Единая точка отказа	Не существует	Существует

8) Назовите несколько популярных платформ для разработки блокчейн-приложений.

Некоторые из популярных платформ для разработки блокчейна:

Эфириум

Гиперледжер Пилообразный

Кворум

пульсация

R3 Корда

Кутум

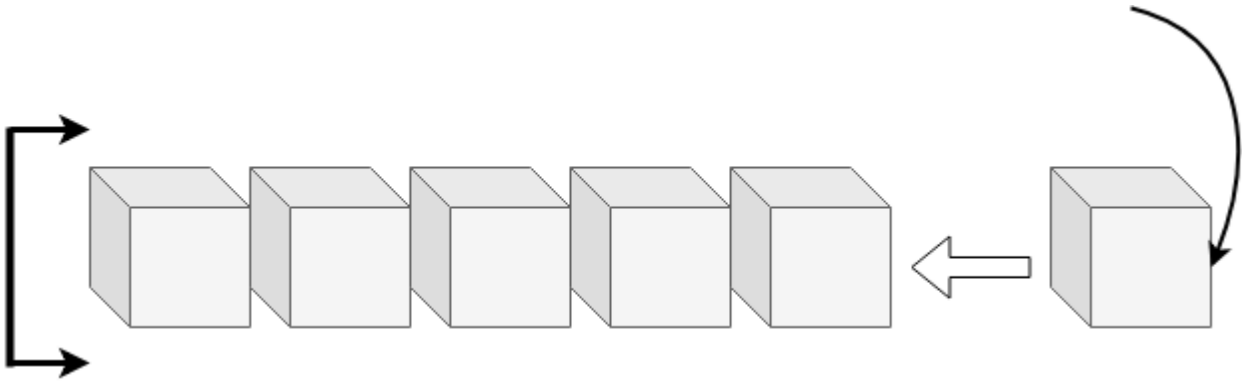
ЙОТА

ЭОС

9) Что вы подразумеваете под блоками в технологии блокчейн?

Блокчейн состоит из списка записей (некоторые или все последние транзакции). Такие записи хранятся в блоках. Каждый раз, когда блок завершается, создается новый блок. Блок, связанный с другими блоками, образует цепочку блоков, называемую Blockchain. Каждый блок после добавления в блокчейн

будет храниться как постоянная база данных. Мы не можем удалить или отменить какой-либо блок из блокчейна.



Чтобы узнать больше, нажмите здесь...

---

10) Из каких элементов состоит каждый блок блокчейна?

Каждый блок должен включать в себя эти три вещи:

Хэш-указатель на предыдущий блок

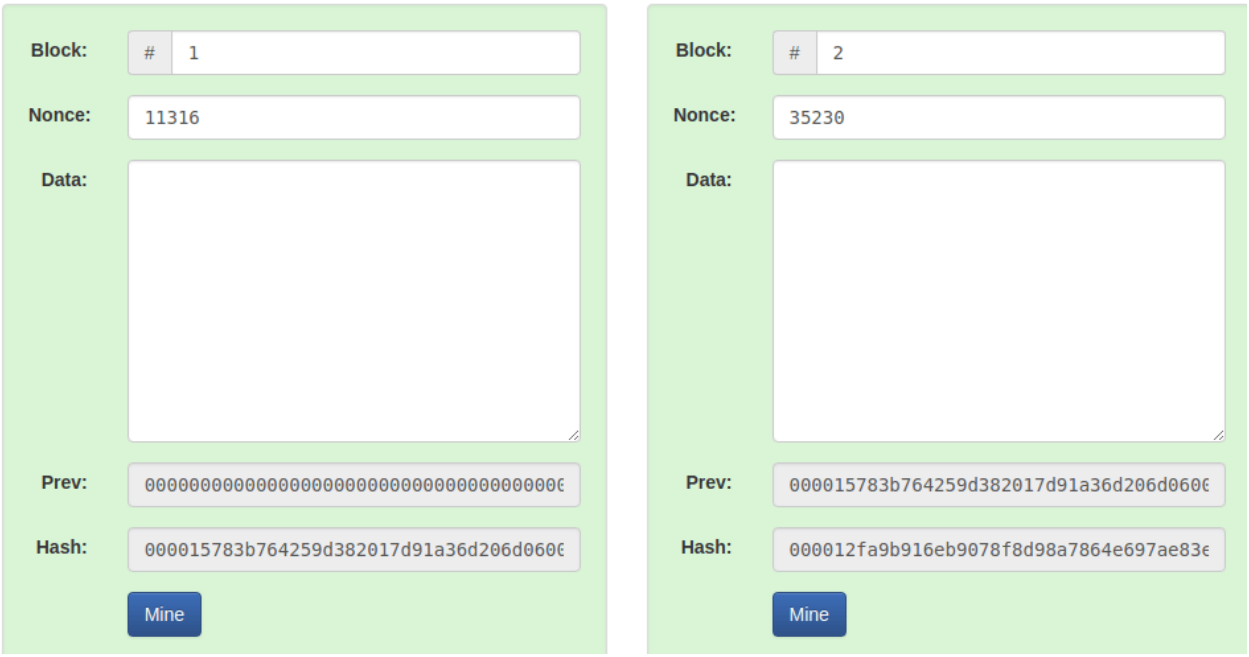
Отметка времени

Список транзакций

---

11) Как распознается блок в подходе Blockchain?

Каждый блок в блокчейне состоит из хеш-значения. Хэш-значение действует как ссылка на блок, который находится перед ним, данные транзакции и фактически отметка времени.



---

12) Как можно идентифицировать блоки?

Блоки можно идентифицировать по их высоте блока и хешу заголовка блока.

---

13) Можно ли изменить данные в блоке?

Нет, изменить данные в блоке невозможно. В случае, если потребуется какая-либо модификация, вам также придется стереть информацию из всех других связанных блоков.

---

14) Можно ли удалить полную блокировку из сети?

Да, можно снять полную блокировку из сети. Бывают случаи, когда необходимо учитывать только определенную часть этой онлайн-бухгалтерии. Существуют параметры и фильтры по умолчанию, которые могут помочь нам сделать это, не прилагая особых усилий.

---

15) Какие типы записей можно хранить в блокчейне? Есть ли ограничения на то же самое?

Нет, невозможно дать ограничение на ведение записей в блокчейн-подходе. Мы можем разместить в блокчейне любые типы данных, такие как банковские записи, медицинские записи, изображения, сообщения Facebook и т. д.

Вот некоторые из распространенных типов записей, которые можно хранить в блокчейне:

Записи о медицинских операциях

Обработка транзакции

Управление идентификацией

События, связанные с организациями,

Управленческая деятельность

Документация

---

16) Какой криптографический алгоритм используется в блокчейне?

Блокчейн использует алгоритм хеширования SHA-256. Агентство национальной безопасности (АНБ) США разработало алгоритм хеширования SHA-256. Чтобы узнать больше, нажмите здесь...

---

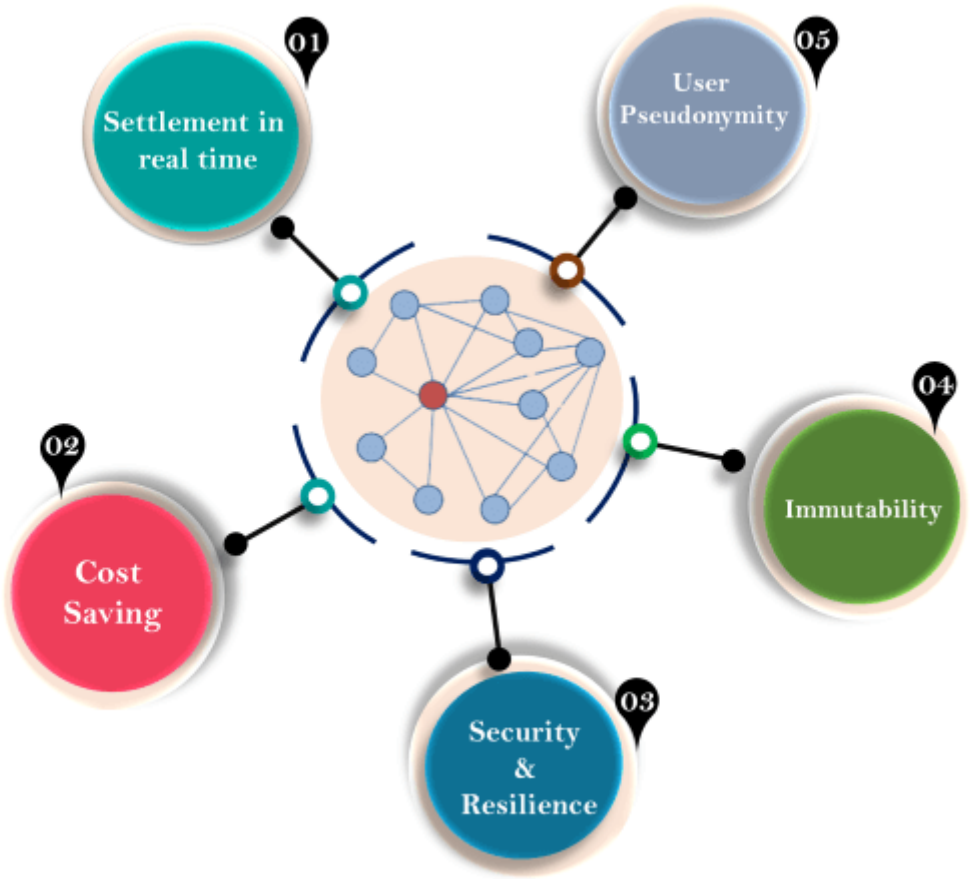
17) В каком порядке блоки связаны в блокчейне?

Блокчейн всегда связывает каждый блок в обратном порядке. Другими словами, блокчейн связывает каждый блок с предыдущим блоком.

---

18) Каковы преимущества блокчейна?

Некоторые из важных преимуществ блокчейна:



Расчеты в режиме реального времени: в финансовой индустрии блокчейн позволяет быстрее проводить расчеты по сделкам. Для проверки, расчетов и очистки не требуется длительного процесса, поскольку между всеми держателями стеков доступна единая версия согласованных данных.

Экономия затрат: блокчейн позволяет выполнять одноранговые транзакции без необходимости в третьей стороне, такой как банк, что снижает накладные расходы на обмен активами.

Безопасность и отказоустойчивость: Блокчейн использует очень продвинутую криптографию, чтобы гарантировать, что информация, которая будет заблокирована внутри блокчейна, защищена от хакерских атак и мошенничества. Он использует технологию распределенного реестра, в которой каждая сторона имеет копию исходной цепочки, поэтому система остается работоспособной даже при выходе из строя большого количества других узлов.

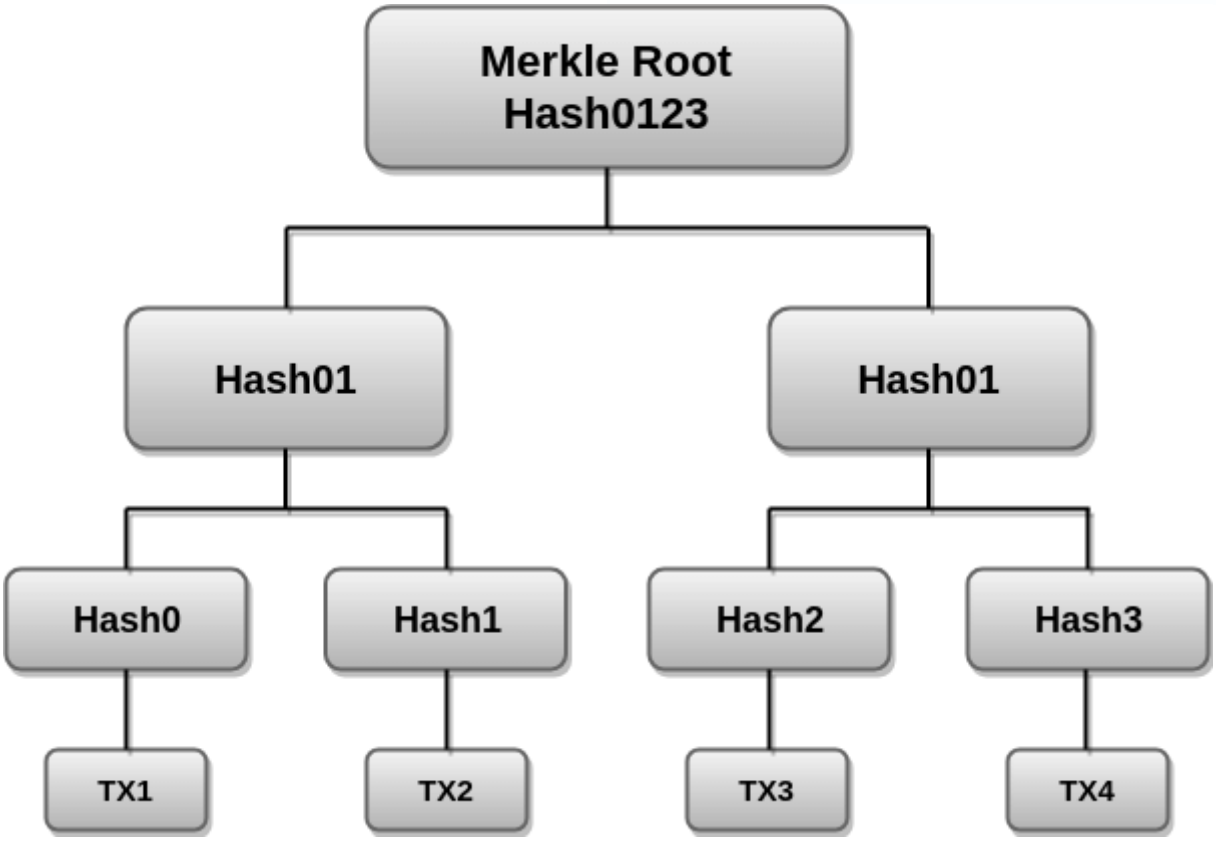
Неизменяемость: блокчейн регистрирует транзакции в хронологическом порядке, что означает, что каждая транзакция происходит после предыдущей. Хронологический порядок удостоверяет неизменность всех операций в блокчейне. Это означает, что когда новый блок добавляется в цепочку реестров, его нельзя удалить или изменить.

Псевдоним пользователя: это состояние, при котором пользователь имеет постоянный идентификатор, который не является настоящим именем пользователя. Настоящие личности доступны только администраторам. Это позволяет пользователям общаться с другими людьми в целом анонимно. Это помогает поддерживать конфиденциальность пользователей и позволяет проводить бесплатные транзакции без каких-либо проблем с безопасностью. В блокчейне ваш псевдоним — это адрес, на который вы получаете биткойны. Каждая транзакция, связанная с этим адресом, постоянно хранится в блокчейне. Если ваш адрес связан с вашей личностью, каждая транзакция будет связана с вами. Всегда хорошо каждый раз использовать новый адрес для каждой транзакции, чтобы избежать привязки транзакций к общему владельцу.

---

19) Что такое деревья Меркла? Каково его значение в блокчейне?

Дерево Меркла является фундаментальной частью технологии блокчейн. Это математическая структура данных, состоящая из хэшей различных блоков данных и служащая сводкой всех транзакций в блоке. Это также позволяет эффективно и безопасно проверять содержимое большого массива данных. Это также помогает проверить согласованность и содержание данных. И Биткойн, и Эфириум используют структуру Merkle Trees. Дерево Меркла также известно как Хэш-дерево .



Дерево Меркла играет жизненно важную роль в технологии блокчейн. Если кому-то нужно проверить наличие конкретной транзакции в блоке, то нет необходимости загружать весь блок, чтобы проверить транзакцию в блоке. Он может только загрузить цепочку заголовков блоков. Это позволяет загрузить коллекцию ветвей дерева, содержащих эту транзакцию. Мы проверяем хэши, которые имеют отношение к вашим транзакциям. Если проверка этих хэшей верна, то мы знаем, что эта конкретная транзакция существует в этом блоке.

Чтобы узнать больше, нажмите здесь...

---

20) Что такое двойная трата? Можно ли удвоить расходы в системе Blockchain?

Двойная трата означает трату одних и тех же денег несколько раз. В физической валюте никогда не может возникнуть проблема двойной траты. Но в цифровых деньгах, подобных биткойнам, может возникнуть проблема двойного

расходования средств. Следовательно, в биткойн-транзакциях существует вероятность копирования и ретрансляции. Это делает возможным, что один и тот же биткойн может быть потрачен его владельцем дважды. Одной из основных целей технологии Blockchain является максимальное устранение этого подхода.

Блокчейн предотвращает проблему двойной траты, реализуя механизм подтверждения от нескольких сторон до того, как фактическая транзакция будет добавлена в реестр.

Чтобы узнать больше, нажмите здесь...

---

21) Что такое бухгалтерская книга? Назовите распространенный тип регистров, которые пользователи могут рассматривать в блокчейне?

Леджер — это файл, который постоянно растет. Он ведет постоянную запись всех транзакций, которые произошли между двумя сторонами в сети блокчейн.

Существует три распространенных типа реестра, которые пользователи могут рассматривать в блокчейне:

Централизованная сеть

Децентрализованная сеть

Распределенная сеть

---

22) Почему блокчейн является надежным подходом?

Блокчейн является надежным подходом по следующим причинам:

Он легко совместим с другими бизнес-приложениями благодаря своей природе с открытым исходным кодом.

Это безопасно, защищено от взлома и зашифровано.

Нет центрального органа, который бы это контролировал.

Все участники согласились с тем, как транзакция вставляется в блокчейн.

Транзакция является неизменной, то есть после того, как транзакция вставлена в блокчейн, мы не можем ее изменить.

---

23) Что подразумевается под ДАО?

DAO расшифровывается как Децентрализованная автономная организация. Это организация, которая является одновременно автономной и децентрализованной. Он представлен правилами, закодированными в виде прозрачной компьютерной программы, контролируемой акционерами и не зависящей от центрального правительства.

DAO можно рассматривать как наиболее сложную форму смарт-контракта. Смарт-контракт — это компьютерная программа, которая автономно существует в Интернете, но в то же время ей нужны люди для выполнения задачи, которую она не может выполнить сама.

Запись финансовых транзакций DAO и правила программы хранятся в блокчейне. Поскольку DAO работает на блокчейне и в распределенной сети, у вас может быть несколько комбинаций разных сторон, обменивающихся ценностями и достигающих соглашений. Это означает, что для децентрализованной автономной организации не имеет значения, человек вы или робот. На самом деле у вас могут быть устройства, взаимодействующие с устройствами, или устройства, взаимодействующие с людьми, или люди, общающиеся с людьми. Для DAO это не имеет значения, потому что, пока он запрограммирован на набор смарт-контрактов, все это может работать автоматически и неизменно.

Чтобы узнать больше, нажмите здесь...

---

24) Что вы подразумеваете под транзакцией Coinbase?

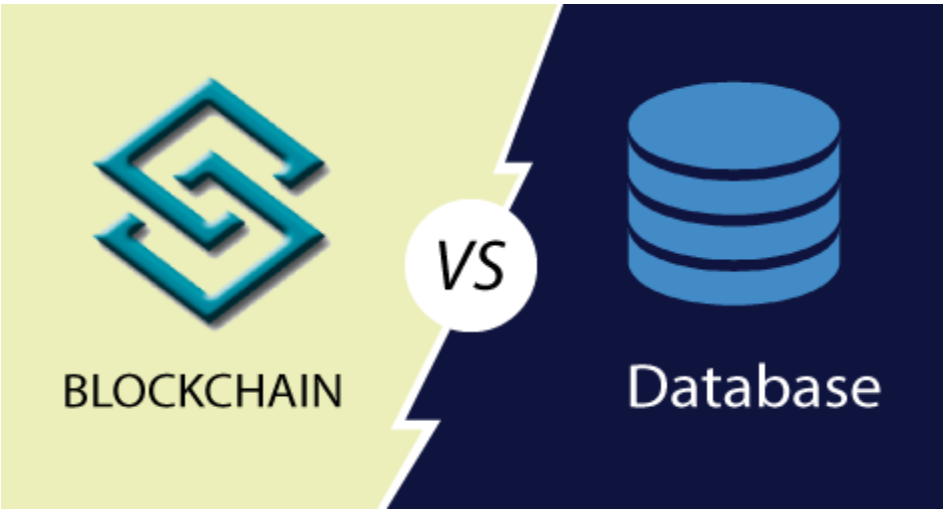
Транзакция Coinbase — это первая транзакция в блоке. Это уникальный тип биткойн-транзакций, который может быть создан майнером. Майнеры используют его для получения вознаграждения за блок за свою работу, и любые другие сборы за транзакции, взимаемые майнером, также отправляются в этой транзакции.

Чтобы узнать больше, нажмите здесь...

---

25) В чем разница между блокчейном и базой данных?

Важными различиями между блокчейном и базой данных являются:



серийный номер	Блокчейн	База данных
1.	Блокчейн децентрализован. Здесь никто не является администратором, значит, все ответственны.	База данных централизована. У него есть администраторы, которые контролируют все данные.

2.	Каждый имеет право читать и писать.	Только авторизованные люди могут читать и писать.
3.	Одноранговая архитектура.	Клиент-серверная архитектура.
4.	Здесь разрешена только операция добавления.	Возможен механизм CRUD (создание, чтение, обновление, удаление).
5.	Исторические данные цифровых записей.	Нет записей о собственности.
6.	Блокчейны полностью конфиденциальны.	Базы данных не являются полностью конфиденциальными.
7.	Блокчейн работает медленно, потому что зависит от скорости хеширования.	База данных работает быстро, потому что ее администрирует меньше людей.
8.	Блокчейн не имеет разрешений.	База данных разрешена.

Чтобы узнать больше, нажмите здесь...

---

26) Что такое криптовалюта?

Криптовалюта — это цифровой актив (валюты), который можно использовать для обмена ценностями между сторонами. Он использует надежную криптографию для защиты и проверки финансовых транзакций, а также для контроля создания новых единиц этой валюты. Как мы знаем, это цифровая валюта, поэтому физически ее не существует. Некоторые популярные криптовалюты — биткойн, лайткойн, Z-Cash, Monero, Dash и т. д.

Мы знаем, что правительство печатает государственные валюты, такие как фиатные валюты, такие как доллары, рупии, иены или юани. Это означает, что

существует централизованное учреждение, которое может создавать тысячи, миллионы или миллиарды этой валюты. В отличие от государственных валют, таких как биткойн, валюты этого типа создаются по тем же математическим формулам, которые заставляют работать криптовалюту. Таким образом, криптовалюты используют децентрализованный контроль, который работает через технологию распределенного реестра, которая служит общедоступной базой данных финансовых транзакций.

Чтобы узнать больше, нажмите здесь...

---

27) Каковы ограничения блокчейна?

Основные ограничения блокчейна:

Отсутствие технического таланта

Сегодня доступно множество разработчиков, которые могут делать много разных вещей в каждой области. Но в технологии блокчейн не так много разработчиков, обладающих специальными знаниями в области технологии блокчейн. Следовательно, отсутствие разработчиков является препятствием для разработки чего-либо на блокчейне.

Размер сети

Блокчейн требует обширной сети пользователей. Поэтому он мало сопротивляется неправильному действию, а также реагирует на атаки и становится сильнее. Блокчейн — это надежная сеть с широко распределенной сеткой узлов, что затрудняет получение всех преимуществ.

Недостаток безопасности

Биткойн и другие блокчейны связаны с одним существенным недостатком безопасности, известным как «атака 51%». Этот недостаток безопасности относится к ситуации, когда группа «майнеров» берет под свой контроль более половины вычислительной мощности сети блокчейна. Если майнеры каким-то

образом приобретут достаточную вычислительную мощность, то не будет централизованной власти, которая помешала бы им влиять на всю сеть Биткойн. Это означает, что злоумышленник может заблокировать выполнение или подтверждение новых транзакций. Они также могут отменить транзакции, которые уже были подтверждены в течение того же периода. За счет этого они могли тратить монеты дважды.

По этой причине пулы майнинга биткойнов находятся под пристальным наблюдением сообщества, которое следит за тем, чтобы никто не получил такого сетевого влияния.

Скорость и стоимость транзакций

Первые несколько лет существования блокчейна стоимость транзакций была «почти бесплатной». Но по мере роста сети это НЕ будет самым экономичным вариантом перевода денег из-за роста транзакционных издержек в сети. С конца 2016 года он обрабатывает только семь транзакций в секунду, и каждая транзакция стоит около 0,20 доллара США.

Механизм консенсуса

В блокчейне мы знаем, что блок может создаваться каждые 10 минут. Это потому, что каждая совершенная транзакция должна гарантировать, что каждый блок в сети блокчейна должен достичь общего консенсуса. В зависимости от размера сети и количества блоков или узлов, задействованных в цепочке блоков, обратная связь, необходимая для достижения консенсуса, может потребовать значительного количества времени и ресурсов.

Чтобы узнать больше, нажмите здесь...

---

28) Что такое атака 51%?

Атака 51% на сеть блокчейна относится к майнеру или группе майнеров, которые пытаются контролировать более 50% мощности майнинга сети, вычис-

лительной мощности или скорости хеширования. В этой атаке злоумышленник может заблокировать выполнение или подтверждение новых транзакций. Они также могут отменять транзакции, которые уже были подтверждены, когда они контролировали сеть, что приводит к проблеме двойного расходования средств.

Чтобы узнать больше, нажмите здесь...

---

29) Что такое шифрование? Какова его роль в блокчейне?

Мы знаем, что безопасность данных всегда имеет значение. Шифрование — это процесс преобразования информации или данных в код для предотвращения несанкционированного доступа. Это помогает организациям обеспечивать безопасность своих данных (т. е. предотвращать несанкционированный доступ). В этом методе данные кодируются или преобразуются в нечитаемый формат до некоторой степени, прежде чем отправитель отправит их из сети. Только получатель может понять, как декодировать то же самое.

В технологии блокчейн этот подход очень полезен, потому что он обеспечивает общую безопасность и подлинность блоков и помогает поддерживать их безопасность.

---

30) В чем разница между Proof-of-work и Proof-of-stake?

Основные различия между Proof of Work и Proof of Stake:

Доказательство работы

Алгоритм Proof of Work (PoW) используется для подтверждения транзакции и создает новый блок в цепочке. В этом алгоритме майнеры соревнуются друг с другом, чтобы завершить транзакцию в сети. Процесс конкуренции друг с другом называется майнингом. Это определяет дорогостоящий компьютерный расчет. При этом вознаграждение дается первому майнеру, решившему задачу каждого блока.

Доказательство доли

В случае алгоритма PoS набор узлов решает поставить свои собственные криптовалюты для проверки транзакции. Их называют «стейкерами». При доказательстве доли создатель нового блока выбирается детерминированным образом в зависимости от его богатства, также определяемого как доля. Он не дает никакого вознаграждения за блок, поэтому майнеры берут только комиссию за транзакцию. Proof-of-Stake может быть в несколько тысяч раз более рентабельным по сравнению с Proof-of-Work.

---

31) Как работает безопасность блока?

Блокчейн — это цепочка блоков, содержащих записи транзакций. Блок — самая безопасная часть блокчейна. Запись блокчейна защищена с помощью криптографического алгоритма хеширования. Каждый блок связан со всеми другими блоками до и после него с помощью характерного хеш-указатора, который повышает безопасность блока. Если значение внутри блока изменено, хеш-значение также изменится. Этот хеш является идентификатором безопасности, который обеспечивает разумный уровень безопасности всей цепочки блоков.

Амбициозным хакерам также необходимо знать хэш-ключ предыдущего блока, чтобы внести изменения в информацию о блоке. Для этих амбициозных хакеров блокчейны децентрализованы и распределены по одноранговым сетям, которые постоянно обновляются и синхронизируются. Поскольку эти записи не хранятся в одном месте, блокчейны не имеют единой точки отказа и не могут быть изменены с одного компьютера.

---

32) В чем разница между открытым и закрытым ключом?

Закрытый ключ используется для шифрования или блокировки сообщения или транзакции, которые отправляются в сети блокчейн. Отправитель может отправить сообщение, используя открытый ключ получателя. С другой стороны, получатель может расшифровать сообщение или транзакцию, используя свой закрытый ключ. Используя закрытый и открытый ключ, связь или транзакция защищены от несанкционированного доступа.

---

33) Назовите платформы, которые активно разрабатывают приложения Blockchain?

Технология блокчейн впервые использовалась для финансовых транзакций. Но в настоящее время его масштабы расширяются и применяются в различных отраслях, таких как электронная коммерция, управление данными, энергетика, игры, электронное управление и многие другие. Существует несколько коммерческих платформ с открытым исходным кодом, которые обеспечивают основу для создания приложений, поддерживающих блокчейн. Hyperledger и Ethereum активно улучшают экосистему блокчейна, создавая передовые межотраслевые блокчейн-технологии.

Hyperledger — это совместная работа с открытым исходным кодом, которая предоставляет инструменты и методы для разработки блокчейн-решения корпоративного уровня. В то время как Ethereum является ведущей платформой с открытым исходным кодом, предназначенной для разработчиков, организаций и бизнеса для создания и развертывания приложений блокчейна.

---

34) Как биткойн использует блокчейн?

Транзакция — это передача стоимости между биткойн-кошельками, которая включается в блокчейн. Биткойн-кошельки хранят секретную часть дан-

ных, называемую закрытым ключом. Закрытый ключ используется для подписи транзакций и предоставления математического доказательства того, что они исходят от владельца кошелька.

---

35) Что такое алгоритм консенсуса?

Алгоритм консенсуса — это метод достижения консенсуса при изменении данных в системе или распределенной сети. Алгоритмы консенсуса широко используются в блокчейнах, поскольку они позволяют сети неизвестных узлов достигать консенсуса в отношении данных, которые хранятся или передаются через блокчейн.

---

36) Какие существуют типы алгоритмов консенсуса?

Существует много типов консенсусных алгоритмов или методов. Самый популярный алгоритм консенсуса:

Доказательство работы (PoW)

Доказательство доли (PoS)

Делегированное доказательство доли (DPoS)

Подтверждение полномочий (PoA)

Подтверждение прошедшего времени (PoET)

Византийская отказоустойчивость

БИТКОЙН-ИНТЕРВЬЮ: ВОПРОСЫ

Ниже приведен список наиболее часто задаваемых вопросов и ответов на интервью о биткойнах.

1) Что такое биткойн?

Биткойн — это тип цифровой валюты, которую можно покупать, продавать и безопасно передавать между двумя сторонами через Интернет. Его нельзя потрогать и увидеть, но им можно торговать в электронном виде. Мы можем хранить их на наших мобильных телефонах, компьютерах или любых других носителях в качестве виртуальной валюты . Биткойн может хранить ценности так же, как чистое золото, серебро и некоторые другие виды инвестиций. Его можно использовать для покупки товаров и услуг, а также для совершения платежей и обмена ценностями в электронном виде. Это самая популярная криптовалюта в мире.

Чтобы прочитать больше информации, нажмите здесь...

---

2) Что вы подразумеваете под майнингом биткойнов?

Добыча биткойнов осуществляется майнерами биткойнов (группой людей). Процедура майнинга биткойнов выполняется на специализированных компьютерах, оборудованных для решения алгоритмических уравнений. Майнеры достигают добычи биткойнов, решая вычислительную задачу, которая создает цепочку блоков транзакций. Эти специализированные компьютеры

помогают майнерам аутентифицировать блок транзакций, хранящийся в каждой сети биткойнов. Всякий раз, когда в блокчейн добавляется новый блок, майнеры сразу же получают вознаграждение за этот новый блок. Майнеры получают вознаграждение в биткойнах вместе с комиссией за транзакции.

---

3) Кто разработал Биткойн?

Биткойн был изобретен неизвестным человеком Сатоши Накамото в 2008 году. Но для этого нет веских доказательств, потому что человек, стоящий за биткойнами, никогда не давал интервью. Он был выпущен как программное обеспечение с открытым исходным кодом в 2009 году. Это была первая успешная виртуальная валюта, разработанная с верой и эквивалентная официальной валюте централизованного правительства. Это цифровая валюта, которая использует правила криптографии для регулирования и генерации единиц валюты. Ее обычно называют децентрализованной цифровой валютой.

Чтобы прочитать больше информации, нажмите здесь...

---

4) Кто управляет биткойнами?

Биткойн — это не компания, поэтому никто не может управлять биткойном. Биткойн — это децентрализованные цифровые деньги, которые выпускаются и управляются без какой-либо централизованной власти. Он создан в качестве награды за соревнование, в котором майнеры, владеющие специализированным компьютером, предлагают свои вычислительные мощности для проверки и создания новых биткойнов. Они также несут ответственность за обеспечение безопасности сети в блокчейне. Деятельность по созданию биткойнов известна как майнинг, и каждый успешный майнер получает вознаграждение в виде вновь созданных биткойнов и комиссии за транзакции.

---

5) Что такое биткойн-кошелек?

Биткойн-кошелек (цифровой кошелек) — это программа, в которой хранятся биткойны. Технически биткойн-кошелек хранит закрытый ключ (секретный номер) для каждого биткойн-адреса. Владелец кошелька может отправлять, получать и обменивать биткойны. Биткойн-кошелек имеет множество форм, и некоторые из них представляют собой настольный кошелек, мобильный кошелек, веб-кошелек и аппаратный кошелек.

Чтобы прочитать больше информации, нажмите здесь...

---

6) Как выбрать биткойн-кошелек?

Выбор лучшего биткойн-кошелька — самый важный шаг на пути к тому, чтобы стать пользователем биткойнов. Ниже приведены два начальных шага для поиска биткойн-кошелька:

Решите, какой криптокошелек вам нужен

Рассмотрите конкретные кошельки, чтобы найти лучший для вас. Биткойн-кошельки различаются по многим параметрам, таким как безопасность, удобство, уровень конфиденциальности, поддержка монет и анонимность, поддержка клиентов, пользовательский интерфейс, сборы, встроенные службы и другие переменные.

Наиболее распространенное различие при выборе биткойн-кошельков заключается в том, являются ли они холодным или горячим кошельком.

Холодный: холодные кошельки относятся к автономному хранению биткойнов. Такие кошельки менее удобны для частого использования, но они более безопасны.

Горячие: Горячие кошельки большую часть времени подключены к Интернету. Этот тип кошельков подходит для повседневного использования, но не является безопасным.

Здесь я возьму пример страницы под названием bitcoin.org для выбора кошелька. Bitcoin.org — очень хорошая отправная точка для объяснения того, как выбрать кошелек, потому что доступно множество вариантов. На этой странице мы перейдем к опции «Выберите свой кошелек» и выберем тип кошелька, который вам нужен. Эти кошельки представляют собой настольный кошелек, мобильный кошелек, веб-кошелек и аппаратный кошелек.

Чтобы прочитать больше информации, нажмите здесь...

---

7) Что такое биткойн-адрес?

Биткойн-адрес — это уникальный идентификатор , состоящий из 26-35 буквенно-цифровых символов . Идентификатор начинается с цифры 1 или 3, которая представляет место, куда можно отправить криптовалюту. Пользователь биткойнов может сгенерировать биткойн-адрес без каких-либо затрат. Однако биткойн-адрес не является постоянным, то есть он может меняться для каждой новой транзакции.

В настоящее время используются три стандартных формата адресов:

P2PKH: всегда начинается с цифры 1, например, 1BvBMSEYvtWesqTFn5Au4n4GFg7xJaNVN2.

P2SH: всегда начинается с цифры 3, например, 3J78t1WpEZ72CMnQviedrnyiWrnqRhWMLy.

Bech32: всегда начинается с bc1, например, bc1qat0srrr7xdkvy5l643lxcnw9re59gtzxwf5ndq.

---

8) Является ли биткойн анонимным?

Нет, биткойн не является полностью анонимным; вместо этого оно псевдонимное, т.е. каждая личность связана с поддельным именем. Это потому, что у каждого пользователя есть публичный адрес, и всякий раз, когда происходят финансовые транзакции, мошенники выживут, чтобы отследить эти адреса.

9) Кто устанавливает цену биткойна?

Цена биткойна определяется рынком, на котором он торгуется. Это определяется тем, сколько кто-то готов заплатить за этот биткойн. Рынок устанавливает цену биткойна так же, как определяется золото, нефть, сахар, зерно и т. д. Биткойн, как и любой другой рынок, подчиняется правилам спроса и предложения. т.е.,

Больше спроса, меньше предложения = цена растет

Больше предложения, меньше спроса = цена падает

В частности, никто не устанавливает цену биткойна, и мы не можем торговать им в одном месте. Каждый рынок/биржа определяет свою цену на основе спроса и предложения.

Чтобы прочитать больше информации, нажмите здесь...

---

10) Почему цены на биткойны колеблются?

Цена биткойна колеблется, потому что она очень нестабильна по своей природе. Поскольку количество биткойнов в обращении ограничено, новые биткойны создаются с уменьшающейся скоростью. Это означает, что спрос должен следовать за этим уровнем инфляции, чтобы цена оставалась стабильной. Рынок биткойнов все еще относительно мал по сравнению с другими отраслями. Поэтому для движения рыночной цены вверх или вниз не требуются значительные суммы денег.

Чтобы прочитать больше информации, нажмите здесь...

---

11) Как покупается биткойн?

Мы можем купить биткойн из многих источников. Некоторые из них приведены ниже.

Его можно приобрести в Интернете с помощью кредитных карт или других электронных кошельков, таких как PayPal и т. д.

Его также можно приобрести с помощью LocalBitcoins и в биткойн-кассирах, что эквивалентно банкоматам по продаже наличных.

Bitcoin.com предоставляет список аутентифицированных центров онлайн-обмена, где вы можете продавать и покупать биткойны.

---

12) Как вы можете продавать биткойны?

Мы можем продавать биткойны разными способами. Мы можем продать его онлайн на биржу или другим людям, которые живут поблизости. Его можно продать так же, как и купить. Цена биткойна регулярно колеблется в зависимости от спроса и предложения. Его также можно продать через биткойн-банкоматы, которые позволяют продавать и покупать биткойны. Комиссия за транзакцию биткойнов является самой низкой среди всех банковских комиссий, применяемых во всем мире.

---

13) Могут ли магазины принимать биткойны?

Как мы знаем, любой может принять биткойн. Для удобства владельцев магазинов доступны многие услуги B2B и установка оборудования. Все эти бизнес-организации предоставляют услуги по выставлению счетов и бухгалтерскому учету. Все сторонние услуги не являются обязательными. Физические лица также могут совершать сделки и выставлять счета самостоятельно.

---

14) Как вы можете конвертировать биткойны в фиатные валюты?

Очень важно знать, как обналичить биткойн или вывести из биткойнов в фиатную валюту (доллары США, евро, индийские рупии), которая будет принята в их родных странах. Ниже перечислены несколько простых способов

конвертации BTC в доллары США, индийские рупии, евро или фунты стерлингов. Прежде чем выбрать любой из перечисленных способов, вам необходимо выяснить, как вы хотите получить фиатную валюту. Вы можете продать биткойны лично за наличные или продать их на биржах и получить деньги прямо на свой банковский счет.

Обмен криптовалюты

Биткойн дебетовая карта

Продажа биткойнов

Биткойн-банкоматы

Чтобы прочитать больше информации, нажмите здесь...

---

15) Могу ли я добывать биткойны?

Майнинг биткойнов — не простой процесс. Для этого требуются специализированные компьютеры, которые могут выполнять расчет большого математического алгоритма. Эти специализированные компьютеры очень дороги, а энергопотребление стало чрезвычайно высоким. Для установки одного такого компьютера или машины вы должны найти экономически эффективную среду, что в наши дни непросто. Сегодня машины для майнинга биткойнов постоянно модернизируются, и момент устаревает. Поэтому добывать биткойны будет очень сложно.

---

16) Могу ли я торговать биткойнами, не продавая их на бирже?

Да, можно торговать биткойнами напрямую, без продажи на бирже. Многие люди предпочитают это из-за их безопасности и доверия. В последнее время многие биржи были взломаны, и в результате их биткойны исчезли без каких-либо объяснений.

Другая причина — его конфиденциальность. В наши дни биржи имеют такие же требования KYC, как и банки. Информация KYC подвержена риску кражи, если безопасность биржи актуальна.

---

17) Что я могу купить за биткойны?

Мы можем купить за биткойны все, что продается в мире на законных основаниях, от одежды, электроники, продуктов питания и предметов искусства до ремесел ручной работы. Биткойн также можно использовать для покупки крупных предметов, таких как автомобили, недвижимость и инвестиционные инструменты, такие как драгоценные металлы. Если вы покупаете что-либо на Amazon через биткойны, вы можете получить скидку до 20%. Некоторые другие также предоставляют скидку людям, которые платят цифровой валютой. Биткойн имеет собственные магазины, в которых можно купить футболки, сумки, худи, аксессуары и т. д.

---

18) Законен ли биткойн?

Биткойн является законным во многих странах мира, но некоторые страны заявляют, что они запретили его использование, например, Индия, Китай и Эквадор. Правила обращения с криптовалютами могут различаться в разных странах, поэтому вам следует провести тщательный поиск, прежде чем инициировать транзакцию с биткойнами в любой организации. В Википедии и многих других онлайн-сервисах есть отличное руководство о том, как к биткойнам относятся во всех странах мира с их регулятивной политикой.

---

19) Как работает биткойн?

Каждый биткойн представляет собой компьютерный файл, который хранится в виде цифрового кошелька на смартфоне или компьютере и функ-

ционирует аналогично любому приложению электронного кошелька. Биткойны используют его валюту в цифровой форме, которая имеет свои пределы производства и ограничена только 21 миллионом биткойнов. Вы можете отправить биткойны на свой цифровой кошелек, а затем отправить биткойны другим людям. Каждая биткойн-транзакция записывается в общедоступный реестр, называемый блокчейном. Блокчейн позволяет отслеживать историю биткойнов, чтобы люди не тратили биткойны, которыми они не владеют. Это также ограничивает копирование или отмену транзакций.

---

20) Каковы преимущества биткойна?

Ниже приведены преимущества биткойнов:

Он принимается во всем мире по одинаковым ставкам, и нет риска обесценивания или повышения курса.

У него самые низкие транзакционные сборы в мире.

Он имеет меньше рисков и необратимую транзакцию, приносящую пользу продавцам.

Он полностью защищен и контролируется криптографическим алгоритмом шифрования.

Это прозрачный и нейтральный режим администрирования, так как любой может проверить данные в режиме реального времени.

---

21) Каковы недостатки Биткойна?

Ниже приведены недостатки: биткойнов.

Степень принятия: в Биткойне степень принятия очень низкая, потому что многие люди до сих пор не знают о его преимуществах.

Волатильный: общее количество биткойнов в обращении очень мало, поэтому даже небольшое изменение может сделать цену биткойна неустойчивой.

Текущая разработка: программное обеспечение Биткойн все еще находится в бета-версии, и многие незавершенные функции находятся в активной разработке .

---

22) Что подразумевается под неподтвержденной транзакцией?

Неподтвержденная транзакция — это та транзакция, которая не была включена в блок, а также не завершена. Каждая транзакция требует хотя бы одного подтверждения для завершения транзакции.

Распространенными причинами неподтвержденных транзакций являются:

Вы сделали перевод. Сети Биткойн требуется не менее 10 минут, чтобы включить транзакцию в блок.

Плата за блокчейн очень низкая. Таким образом, чем ниже комиссия за транзакцию, тем ниже приоритет вашей транзакции в сети Биткойн. Следовательно, требуется более длительное подтверждение, чтобы быть действительной транзакцией.

---

23) Кто контролирует сеть Биткойн?

Биткойн-сеть — это термин, используемый для описания всех серверов, которые обрабатывают различные транзакции, совершаемые с биткойнами. Никто особенно не может контролировать сеть Биткойн. Все пользователи биткойнов по всему миру контролируют его. Чтобы быть совместимыми друг с другом, все пользователи биткойнов должны использовать программное обеспечение, которое соответствует одним и тем же правилам. Майнинг биткойнов может работать правильно только при полном согласии между всеми пользователями. Поэтому у всех пользователей и разработчиков есть сильный стимул защищать этот консенсус.

---

24) Какова цена одного биткойна? Могу ли я купить часть одного биткойна?

Курс покупки одного биткойна по состоянию на апрель 2019 года составляет примерно 3 67 569,51 индийской рупии. Цена биткойна будет меняться каждую секунду. Если вы не хотите покупать один биткойн целиком, вы также можете купить часть биткойна. Это потому, что каждый биткойн можно разделить до 8 знаков после запятой (0,00000001). Например, вы можете купить биткойн за 1000 или 5000 рупий.

---

25) Законно ли покупать и продавать биткойны в Индии?

Покупка и продажа биткойнов в Индии не является незаконной. В Индии нет закона, объявляющего это незаконным. В Индии на пороге цифровой революции криптовалюта еще не признана официально. Резервный банк Индии (RBI), который регулирует индийскую рупию, ранее предупредил пользователей, держателей и трейдеров виртуальных валют, включая биткойны.

Ни один центральный банк или финансовый орган не разрешают создание, торговлю или использование биткойнов в качестве платежного средства. Отсутствуют разрешения регулирующих органов, указывается, что заинтересованные лица получили регистрацию или разрешение на осуществление такой деятельности. Однако центральный банк однозначно не запретил биткойны в стране.

---

26) Как работают биткойн-транзакции?

Транзакция — это передача стоимости между биткойн-кошельками отправителя и получателя в сети блокчейн. Каждая биткойн-транзакция состоит из суммы.

Сумма — это вход (адрес отправителя), выход (адрес получателя) и закрытые ключи, которые позволяют тратить биткойны со счета человека.

Блокчейн — это база данных, в которой хранится история транзакций с момента создания биткойна.

---

27) Какие шаги вы должны предпринять, чтобы обезопасить себя от мошенничества с биткойнами?

Основной совет заключается в том, что вы не должны инвестировать в то, что вы не понимаете. Существует множество схем и мошеннических схем, связанных с добычей биткойнов.

Блокчейн — это технология высокого риска, у нее есть потенциал, но мы никогда ничего не гарантируем. В мире биткойнов нет гарантированного возврата. На домашней странице Zebpay есть раздел, в котором перечислены случаи мошенничества и махинаций, а также даны советы пользователям, как защитить себя.

---

28) В чем разница между Биткойном и Блокчейном?

серийный номер	Блокчейн	Биткойн
1.	Блокчейн — это реестр с криптографической целостностью.	Биткойн — это криптовалюта.
2.	Блокчейн может легко передавать что угодно, от валюты до прав собственности на акции.	Биткойн ограничен торговлей в качестве валюты.
3.	Он имеет широкий охват из-за открытого исходного кода.	Он имеет ограниченную область применения и менее гибкий.

4.	Он обеспечивает недорогую безопасную и защищенную среду для одноранговых транзакций.	Чтобы упростить и увеличить скорость транзакций без особых государственных ограничений.
5.	Он прозрачен, поскольку должен соответствовать KYC для каждого бизнеса.	Его можно назвать анонимным, потому что нет нормативной базы и стандартов, которым следовал биткойн.