

Блокчейн первого поколения

Блокчейн



Оглавление

Введение	2
Словарь терминов	3
Предпосылки возникновения блокчейна	4
Дерево Меркла	4
Родоначальники блокчейна	7
Первый в мире блокчейн	8
Вайтпейпер Биткоина	8
Аннотация	9
Стимулы	11
Экономия дискового пространства	12
Как читать вайтпейперы	13
Три основы блокчейна	16
Что такое децентрализация	19
Кто разрабатывает Биткоин	22
Как выглядит блокчейн Биткоина	24
Публичные и приватные блокчейны	24
Блокчейн-обозреватели	25
Недостатки Биткоина	30
Атака 51%	30
Квантовая устойчивость	31
Ограниченная функциональность	32
Заключение	32
Дополнительные материалы	32
Использованная литература	33

Введение

Всем привет! Мы начинаем курс о блокчейне, на котором изучим технические основы этой технологии и познакомимся с решением прикладных задач, как в сфере финансов, так и в разработке приложений.

Чтобы структурировано во всём разобраться, мы воспользуемся классификацией блокчейнов по поколениям. Первая лекция будет посвящена блокчейнам первого поколения — мы изучим технические основы на примере Биткоина, самого известного блокчейна в мире. На второй лекции мы детально рассмотрим блокчейны второго поколения — центральным примером для нас станет Эфириум. В последней лекции будем говорить о блокчейнах третьего поколения, которые пока только зарождаются.

Сразу стоит отметить, что это достаточно условная классификация. Некоторые эксперты могут рассматривать и четыре, и пять поколений блокчейнов, либо даже предполагать, что второго поколения еще нет. Кроме того, вы можете встретить и другие классификации блокчейнов, например, по уровням или алгоритмам консенсуса. Но концепция с тремя поколениями является самой распространённой и будет удобна для обучения.

На этой лекции вы узнаете:

- как возник блокчейн;
- что революционного было в блокчейне Биткоина;
- какие теории легли в основу блокчейна;
- что такое децентрализация на самом деле;
- где получать данные из публичных блокчейнов;
- какие есть недостатки у Биткоина.

Словарь терминов

Вайтпейпер — документ, излагающий суть, цели, и принципы работы блокчейн-проекта.

Хеш — уникальный набор символов, которым зашифровано сообщение с помощью хеш-функции (математической функции).

Дерево Меркла — это алгоритм, позволяющий получить один хеш для множества фрагментов данных. Метод используют для определения целостности файлов и верификации информации ([Forklog](#)).

Двойная трата (двойное расходование) — использование одного и того же баланса для двух или более операций.

Криптография — совокупность алгоритмов шифрования информации для обеспечения аутентификации, конфиденциальности и целостности данных без постороннего вмешательства.

Теория игр — математический метод изучения оптимальных стратегий в играх. Под игрой понимается процесс, в котором участвуют две и более стороны, ведущие борьбу за реализацию своих интересов.

Архитектура сети — принцип, по которому происходит обмен информацией в интернете.

Одноранговая сеть — сеть, в которой нет центрального элемента. Узлы взаимодействуют между собой без посредника, и передача информации происходит напрямую.

Майнеры — участники блокчейна, которые занимаются созданием новых блоков и проверкой транзакций.

Транзакция — запись об изменении состояния активов.

Алгоритм консенсуса — метод, который описывает, как выбирается майнер в блокчейне и по каким правилам он создаёт блоки.

Закон Мура — эмпирическое наблюдение, согласно которому количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 24 месяца.

Блокчейн-обозреватель — онлайн-сервис, содержащий историю транзакций одного или нескольких публичных блокчейнов.

Предпосылки возникновения блокчейна

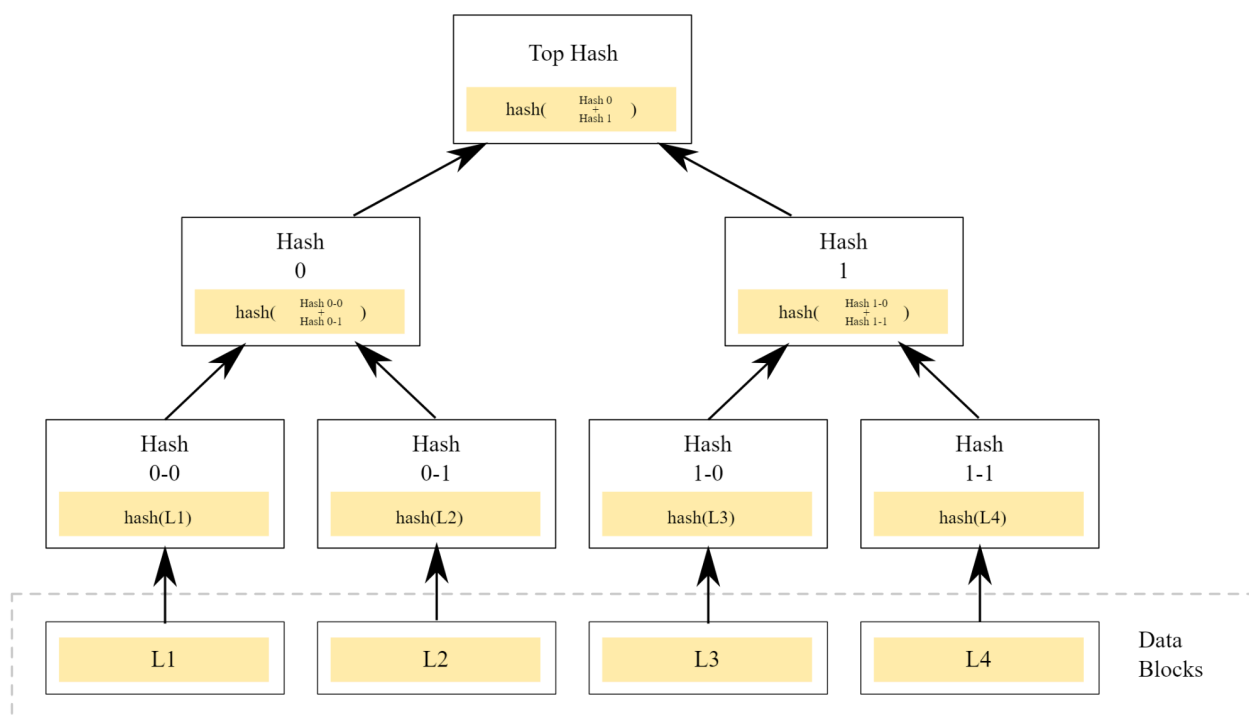
Прежде чем мы начнём рассматривать блокчейн, давайте поговорим о том, что ему предшествовало. Это поможет сразу развеять некоторые распространённые заблуждения и понять, что именно в нём инновационного. Любые технологии и научные открытия не появляются на пустом месте. Прогресс — это последовательный процесс и у блокчейна есть свои технологические основы.

Дерево Меркла

Первой важной вехой в истории блокчейна можно назвать статью 1987 года «Цифровая подпись, основанная на обычной функции шифрования». Её автор — американский ученый-информатик Ральф Меркл. В статье описывается концепция хеш-дерева или, как его теперь называют, дерева Меркла. Эти деревья представляют собой структуру данных, хранящуюся, в связанных с помощью криптографии, блоках.

Дерево Меркла — это алгоритм, позволяющий получить один хеш для множества фрагментов данных. Метод используют для определения целостности файлов и верификации информации.

Строго говоря, дерево Меркла — это двоичное дерево криптографических хэш-указателей, конечные узлы которого — это хэши транзакций, а внутренние вершины представляют собой результаты сложения значений связанных вершин. Оно создаётся путем хэширования парных данных (обычно транзакций на уровне «листьев»), а затем повторного хэширования парных хэшей следующего уровня и так вплоть до корневого узла, называемого *корнем Меркла*.

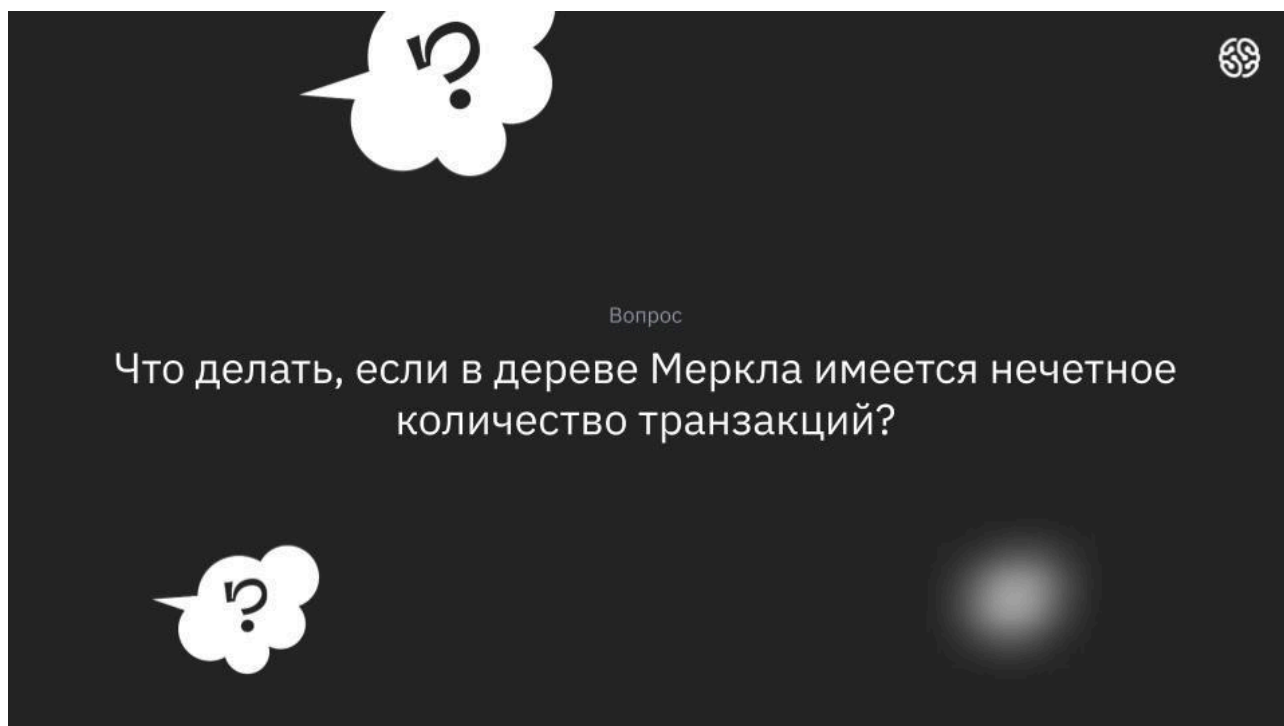


Структура дерева Меркла. Источник: [wikipedia.org](https://ru.wikipedia.org/wiki/Меркловское_дерево)

У дерева Меркла есть две важные особенности, которые важно указать для последующего обсуждения блокчейна:

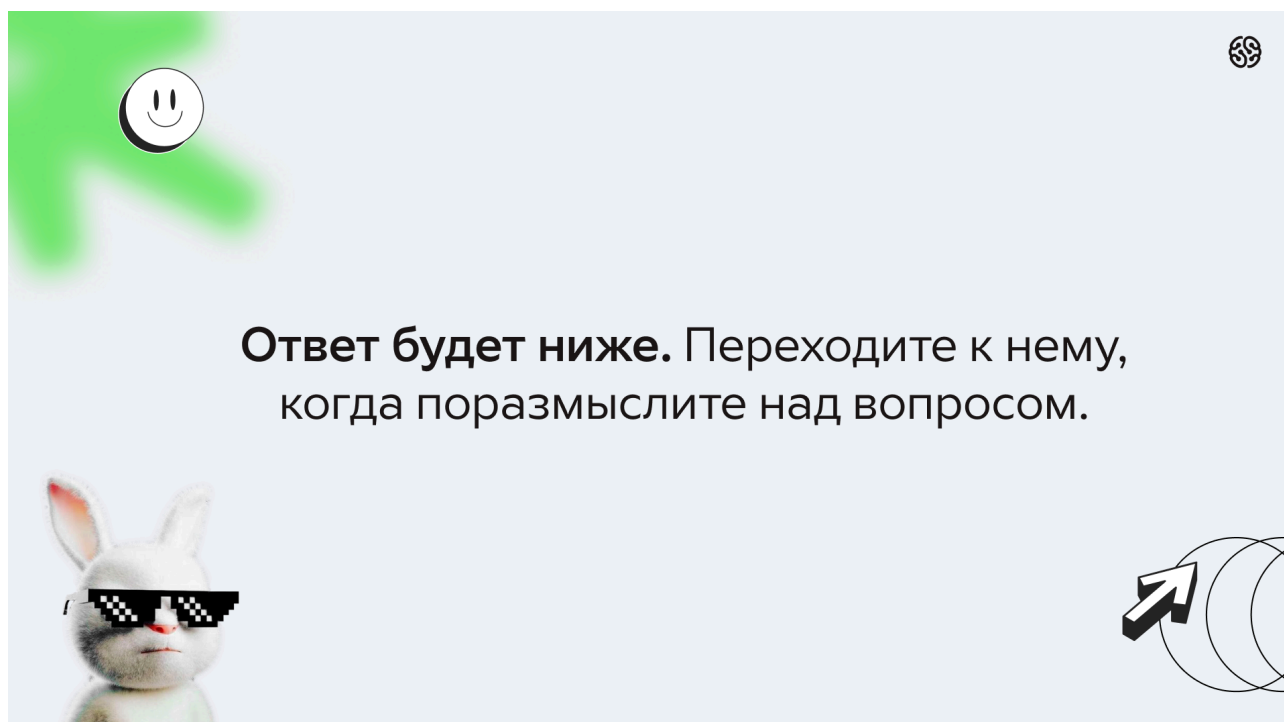
1. **Защита от взлома.** При наличии поддельной транзакции, хэш на любом уровне дерева не будет совпадать с хэшем, хранящимся на одном уровне вверх по иерархии, а также вплоть до корневого узла. Злоумышленнику трудно изменить все хэши во всем дереве.
2. **Целостность порядка транзакций.** Если вы измените только порядок транзакций (даже не меняя сами транзакции), то также изменятся и хэши в дереве до самого корня Меркла.

Есть интересная тонкость, дерево Меркла — это бинарное дерево, то есть, на уровне листьев должно быть четное количество элементов. Как вы думаете, что делать, если имеется нечетное количество транзакций?



Вопрос

Что делать, если в дереве Меркла имеется нечетное количество транзакций?



Ответ будет ниже. Переходите к нему, когда поразмыслите над вопросом.

Ответ: хорошим решением является дублирование хэша последней транзакции. Это не создаст проблем, таких как двойные расходы или повторные транзакции, поскольку мы дублируем именно хэш, а не саму транзакцию. Таким образом, мы можем сбалансировать дерево.

Родоначалники блокчейна

С развитием интернета криптография развивалась всё быстрее. Описание протоколов, схожих с современными блокчейными, можно было встретить во многих научных статьях. Вот лишь некоторые, самые важные из них:

1. В 1982 года американский криптограф Дэвид Чаум написал диссертации на тему «Компьютерные системы, созданные, поддерживаемые и пользующиеся доверием взаимно подозрительных групп».
2. В 1991 году математики С. Хабер и У. Скотт Сторнетта описали криптографически защищённую цепочку блоков. Они преследовали цель внедрить систему, в которой временные метки документов нельзя было бы подделать.
3. В 1992 году Хабер, Сторнетта и ещё Дейв Бейер включили в свою технологию дерево Меркла, что повысило её эффективность, позволив собирать несколько сертификатов документов в один блок.

Мы не будем подробно рассматривать эти статьи. Если вам интересно, вы сможете самостоятельно их изучить. Ссылки на них есть в конце методички. Далее мы рассмотрим статью Сатоши Накамото 2008 года, в которой впервые был описан Биткоин.

Первый в мире блокчейн

Вероятно, вы так или иначе, уже знакомы с блокчейном: изучали концепцию этой технологии на предыдущих курсах GeekBrains, самостоятельно читали статьи в интернете или хотя бы слышали новости о падении или росте Биткоина. Поэтому мы не будем долго останавливаться на деталях. Давайте сформулируем несколько важных для понимания темы определений, вспомним суть блокчейна на верхнем уровне, а затем уже заглянем глубже, с более технической стороны.

- **Централизованная система** — это такая система, в которой есть главный узел, ответственный за дробление задач или данных, а также распределение нагрузки между узлами.
- **Децентрализованная система** — это такая система, где нет главного узла как такового. Блокчейн — один из таких примеров. По-другому его называют одноранговой сетью, «peer-to-peer» сетью или пиринговой сетью. Сеть для передачи данных без участия доверенной третьей стороны.

- **Блокчейн** — это децентрализованный и открытый реестр транзакций. База данных этого реестра реплицируется (копируется) на множество узлов. Она работает только в режиме добавления записей и не может быть изменена или исправлена. Это означает, что каждая запись является постоянной и неизменной. Любая новая запись появляется во всех копиях базы данных, размещенных на разных узлах.

Если вы всё же чувствуете, что не можете в двух словах сформулировать описание блокчейна, то можете прочитать [серию статей «Блокчейн-новичок»](#). Там простыми словами объясняется как устроен блокчейн и где он используется.

Вайтпейпер Биткоина

Документ, в котором впервые описан блокчейн в современном его представлении — вайтпейпер Биткоина. Вайтпейпер — это документ, излагающий суть, цели, и принципы работы блокчейн-проекта. Также его называют «технический документ», «информационный документ», «белая книга», «white paper» или «whitepaper».

Термин вайтпейпер корнями уходит в политику. Первым в истории вайтпейпером была «Белая Книга» Черчилля в 1922 году, в которой была представлена политическая идея до того, как она стала законом. Поначалу их использовали лишь политики, но в 90-х годах вайтпейперы получили широкое распространение в маркетинге и продажах. Сегодня вайтпейперы есть практически у каждого блокчейна.

В зависимости от целевой аудитории, вайтпейперы могут нести в себе разные цели. Вайтпейпер Биткоина написан для информирования людей о технологическом прорыве: возможности пересылки наличных денег от одной стороны к другой без посредника.

Первое, на что стоит обратить внимание — название «Биткоин: система цифровой пиринговой наличности». В нём, как и далее в статье, вы не встретите термина «блокчейн». Это довольно интересный факт. Термин «блокчейн» вошел в оборот позднее.

Аннотация

Вайтпейпер был опубликован 31 октября, 2008 года. В аннотации описывается существующая проблема электронных денег:

«Полностью одноранговое устройство системы электронных денег позволяет совершать электронные транзакции между участниками напрямую, минуя любые финансовые институты. Частично эту задачу решает использование цифровых подписей, но необходимость доверенного лица для контроля за двойной тратой лишает этот подход основных преимуществ».

Здесь следует обратить внимание на то, что Биткоин — это прикладное применение последних достижений криптографии в узкой сфере — в сфере финансов. Прежде алгоритмы шифрования рассматривались чаще всего в контексте развития интернет-технологий и средств коммуникации. При этом Сатоши Накамото не рассматривает коммерческий потенциал применения Биткоина. Вы не найдёте в вайтпейпере ничего о возможностях заработка, устранении неравенства и прочем. Хотя многие последующие криптовалютные проекты будут злоупотреблять этим.

“Несмотря на то что существуют подходы к реализации децентрализованной финансовой системы, в современных системах онлайн-платежей всё равно есть узлы с иными правами, чем у остальных. Речь идёт о банках, которые решают проблему двойной траты.”, — пишет Сатоши Накамото.

Давайте рассмотрим, что такое двойная трата и почему «доверенные лица» для контроля за ней, лишают современный подход основных преимуществ.

Простыми словами, двойное расходование средств означает использование одного и того же баланса для двух или более операций. Существование в традиционных платежных системах посредников между отправителем и получателем, таких как банки и компании, выпускающие кредитные карты, облегчает проверку достоверности транзакций. Этим третьим лицам доверяют, чтобы убедиться, что у отправителя достаточно баланса для проведения транзакции, и он не отправляет две или более транзакции, которые засчитываются как одна.

Рассмотрим пример, чтобы проиллюстрировать двойную трату. Если покупатель заплатит пять тысяч рублей физическими деньгами за пару обуви, он не сможет потратить те же деньги снова, потому что у него их больше нет. Он отдал их продавцу в магазине. Дважды потратить, в этом случае, означает использовать те же пять тысяч наличными, которые уже отдала продавцу, для покупки другого товара. Это крайне маловероятно при использовании физических наличных денег.

Проблема, использования цифровых валют, заключается в том, как защититься от такой ситуации, когда покупатель потенциально может скопировать пять тысяч рублей и тратить их снова и снова.

Далее в аннотации предлагается решение этой проблемы:

«Мы предлагаем децентрализованное решение проблемы “двойной траты” с использованием одноранговой (пиринговой) сети. Сеть ставит метки времени на транзакции, соединяя их в цепочку доказательств проделанной работы на основе хэширования. Сформированные таким образом записи, невозможно изменить, не выполнив заново всего объема вычислений. Самая длинная версия цепочки служит не только подтверждением очередности событий, но и доказывает, что над ней произвел работу самый большой вычислительный сегмент сети. До тех пор, пока большая часть вычислительных мощностей контролируется узлами, не объединенными с целью атаковать сеть, они будут генерировать самую длинную цепочку, опережая любых злоумышленников. Устройство самой сети очень простое: сообщения рассылаются на основе принципа “наименьших затрат”, а узлы могут покидать сеть и снова подключаться к ней в любой момент, принимая самую длинную версию цепочки для восстановления пропущенной истории транзакций».

Реализацией этого решения и является блокчейн Биткойна, который был запущен 1 января 2009 года.

Стимулы

Далее в вайтпейпере Биткойна описывается суть работы описанной системы. Рассматриваются транзакции, хеши и алгоритм консенсуса Proof of Work. Вероятно, вы уже знакомы с этими понятиями, а краткие их определения есть в начале методички. Поэтому останавливаться на этих пунктах мы не будем. Однако, самостоятельно всё же стоит прочитать вайтпейпер, чтобы ознакомиться со строгими и каноничными определениями.

Мы остановимся на главе вайтпейпера Биткойна, посвященной стимулам. Ввиду отсутствия центрального органа, который определяет судьбу денег, мотивация для узлов (майнеров) устроена своеобразным образом:

«По умолчанию, первая транзакция в блоке является специальной, создающей новую монету, которая принадлежит создателю блока. Такая схема поощряет честных участников сети, стимулируя их поддерживать работу сети, а также решает вопрос о начальном распределении денежной массы в отсутствие центрального эмитента».

Простыми словами, майнеры получают монеты за обеспечение функционирования и безопасности сети. Одновременно с этим, мотивацию представляет механизм, посредством которого новые монеты попадают в обращение. Другими словами, именно майнеры добывают новые монеты.

Далее Сатоши Накамото говорит, что подобные процессы создают добавленную стоимость благодаря времени и ресурсам, потраченным на создание монет, подобно добыче золота:

«Равномерное увеличение числа монет в обращении можно сравнить с добычей золота, в которую золотоискатели тоже вкладывают свои ресурсы. В роли последних в нашем случае выступают процессорное время и электричество».

Когда в обращение войдёт предварительно заданное число монет, мотивация сможет полностью перейти к транзакционным комиссиям, и инфляция окончательно прекратится.

Сегодня мы знаем, что Биткоин не бесплатен, и его создание обходится дорого. Это делает его полезным средством сбережения и средством обмена в пиринговой сети, которая не требует доверия. В отличие от фиатных валют, которые выпускают правительства и центральные банки, Биткоин не подвержен инфляции. Ведь его нельзя создать по собственному желанию — биткоинов будет ровно 21 миллион.

Накамото также утверждает, что система вознаграждений сети побуждает узлы оставаться честными и злоумышленникам будет сложно атаковать Биткоин:

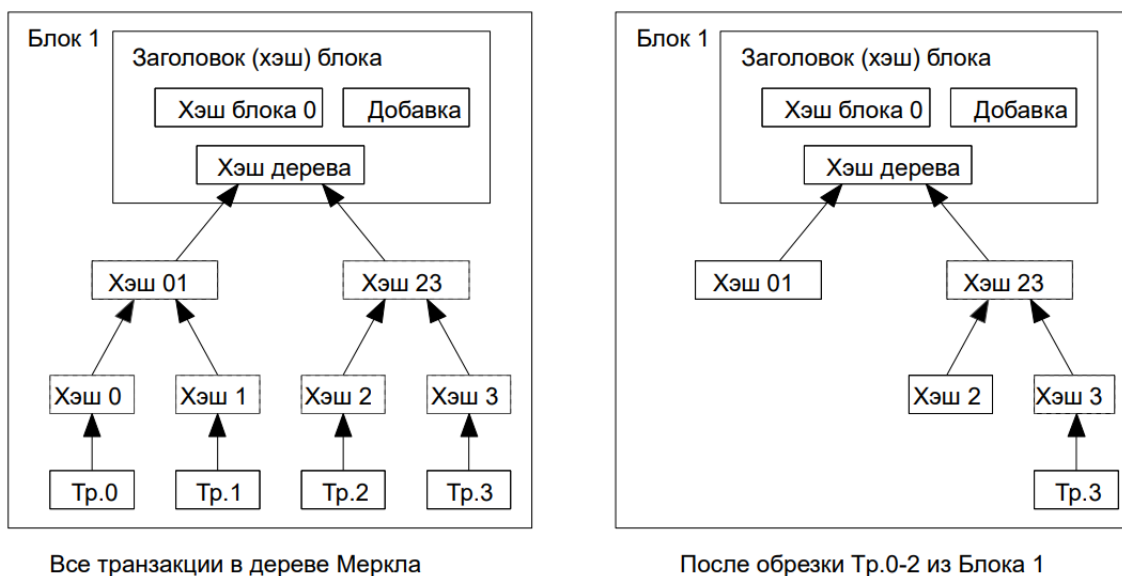
«Такая форма стимулирования может также способствовать уменьшению случаев мошенничества. Если жадный злоумышленник способен выделить больше вычислительных мощностей, чем все честные участники, он может обманывать продавцов, аннулируя свои транзакции и возвращая средства, или же направить свои ресурсы на генерацию новых блоков и монет. Более выгодным для него является вариант «игры по правилам», который обеспечивает получение более половины всех новых денег, чем вариант “саботажа системы” и поддержания своего капитала на постоянном уровне».

Экономия дискового пространства

Ранее в лекции мы рассмотрели дерево Меркла, как отправную точку в развитии блокчейнов. Давайте рассмотрим, как именно этот алгоритм нашел своё применение в Биткоине. Седьмой раздел вайтпейпера посвящен экономии дискового пространства:

«Как только последняя транзакция в монете-цепочке окажется внутри достаточно старого блока, все предшествующие ей транзакции в цепочке могут быть удалены в целях очистки дискового пространства. Чтобы хэш блока остался неизменным, все транзакции в блоке хранятся в виде хэш-дерева Меркла и, лишь его корень

включается в хэш блока. Размер старых блоков может быть уменьшен за счет удаления ненужных ветвей этого дерева, хранить промежуточные хэши необязательно».



Применение дерева Меркла в блок Биткоина. Источник: bitcoin.org

«Заголовок пустого блока будет составлять около 80 байт. Из расчета скорости генерации блока раз в десять минут получаем $80 \cdot 6 \cdot 24 \cdot 365 = 4.2$ Мб в год. Для среднестатистического на 2008 год компьютера с 2 Гб оперативной памяти с учетом закона Мура, предсказывающего рост на 1.2 Гб в год, хранение данных не будет проблемой, даже если все заголовки блоков будут находиться в памяти».

Закон Мура — эмпирическое наблюдение, согласно которому количество транзисторов, размещаемых на кристалле интегральной схемы, удваивается каждые 24 месяца.

Одним словом, функционирование системы, даже спустя много лет, не будет представлять сложности. Дерево Меркла помогает экономить дисковое пространство.

Как читать вайтпейперы

В первые годы существования Биткоина появились много аналогичных блокчейнов. Все они, так или иначе, были связаны со сферой финансов и предлагают пользователям разные виды криптовалют в качестве альтернативы традиционным

деньгам. Например, сегодня остаются достаточно популярными Bitcoin Cash и Litecoin. Их принято относить к первому поколению блокчейнов.

Вы сможете сами достаточно глубоко разобраться с любым другим блокчейном, лишь отыскав его вайтпейпер. Умение читать и анализировать вайтпейпер — важный навык, который понадобится любому блокчейн-разработчику. Давайте рассмотрим аспекты, которые вам будет важно помнить при самостоятельном изучении.

Задание: Какую разницу вы видите между вайтпейпером Биткоина и вайтпейпером Enjin?

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshi@gmx.com
www.bitcoin.org


Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

Introduction



Enjin® is the largest gaming community creation platform online:

- 250,000 gaming communities¹ across thousands of games.
- 18.7 million registered gamers
- Launched in 2009, based in Singapore
- 60M global views per month²
- Gaming focused Content Management System and Forum creator
- Millions of USD per month in virtual goods sales across Enjin community stores

Enjin® is introducing Enjin Coin ("ENJ"), a new cryptocurrency (ERC-20 Token) and smart contract platform that gives game developers, content creators and gaming communities the required crypto-backed value and tools for implementing and managing virtual goods.

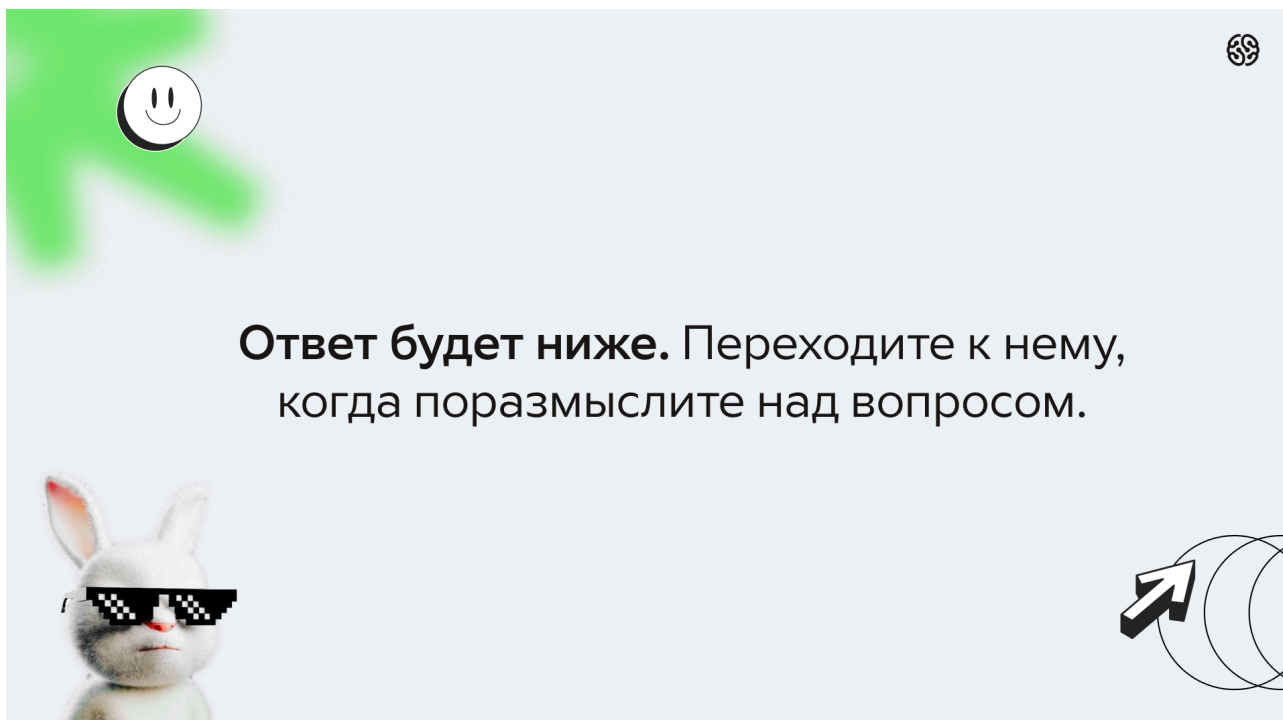
The Enjin platform will have full support for these tokens in the next 6 months.

Enjin will develop a powerful framework of open-source software development kits (SDKs), wallets, game plugins, virtual item management apps and a payment gateway platform.

Join us in launching the **most usable** cryptocurrency for gaming!

¹ Enjin Internal Data as of June 2017: <https://www.enjin.com/communities>
² Quantcast data for Enjin Network: <https://www.quantcast.com/ip-e29QTu7yneec>
Whitepaper v1.10 <https://enjincoin.io> for latest version. ©2017, Enjin® PTE LTD

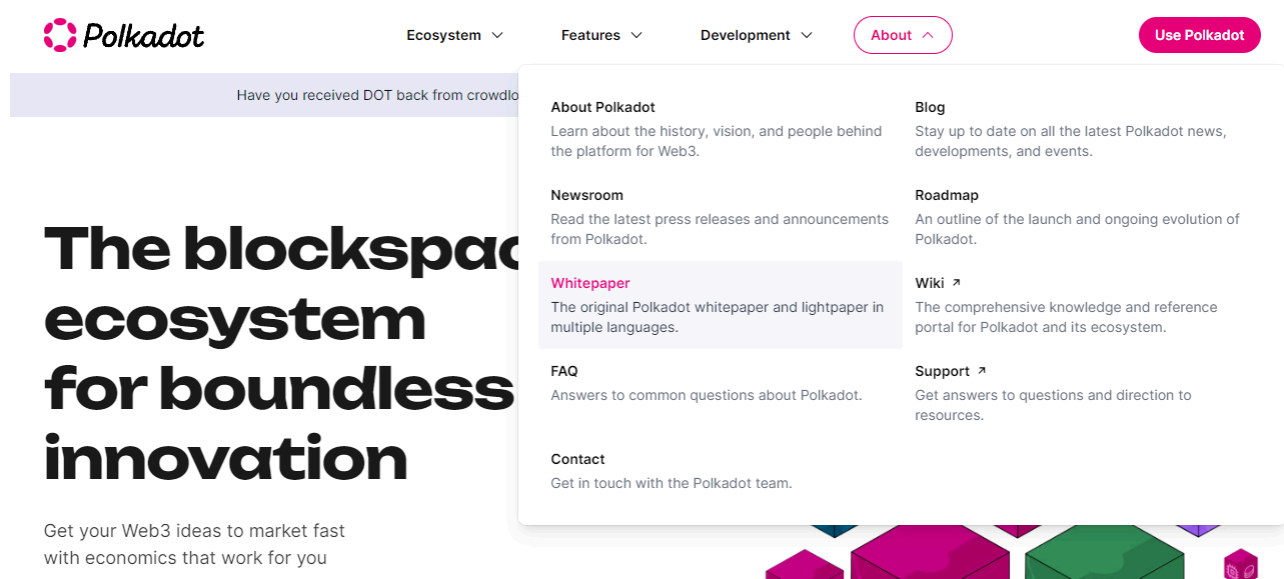
Сравнение первых страниц вайтпейперов Биткоина и Enjin. Источник: coinmarketcap.com



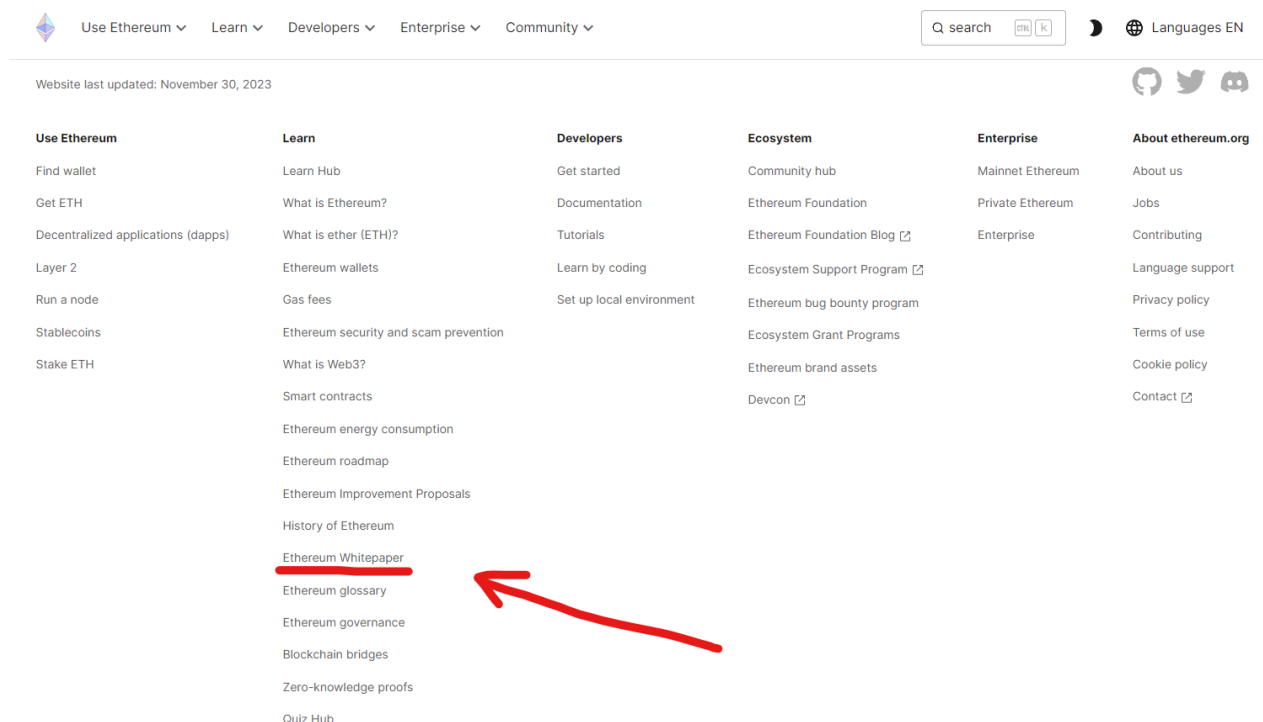
Ответ: У Биткоина академический тон и стиль, это более информативный и технический документ. У Enjin проще содержание и красочнее дизайн, он больше ориентирован на маркетинг.

Большинство современных вайтпейперов пишутся для маркетинга проекта или для привлечения средств на его реализацию. Иногда можно встретить упрощенную версию вайтпейпера — лайтпейпер.

Где найти вайтпейпер? Большинство проектов публикуют свои документы на основном сайте.



Некоторые проекты, например, *Polkadot*, выставляют свои документы на передний план главной страницы. Источник: polkadot.network



В случае с *Ethereum*, вайтпейпер стоит поискать в футере, или «подвале» сайта. Источник: ethereum.org

Если не удастся найти документ на сайте проекта, то, вероятно, его можно найти на сайте whitpaper.io. Также вы можете найти интересующий вас проект на сайте coinmarketcap.com и на странице с информацией о нём будет ссылка вайтпейпера.

В заключение отметим наиболее очевидные признаки плохого вайтпейпера. Если вы заметили хотя бы один из этих них, стоит задуматься, стоит ли работать с ним.

- **Опечатки и плохой язык.** Некоторые вайтпейперы написаны не носителями английского языка и не для них. Тем не менее компетентная команда должна, по крайней мере, иметь возможность нанять носителя языка в качестве редактора.
- **Неясность.** Многие плохие вайтпейперы делают расплывчатые заявления вроде «революционизировать платежи» или «стать частью движения web3». Если проект не может точно объяснить, что он делает, то он просто пускает пыль в глаза.
- **Слишком грандиозные обещания.** Бывает и наоборот: если проект обещает перевернуть всю индустрию и стать «следующим Биткоином», – стоит быть

начеку. Криптовалютные компании — мастера в том, чтобы обещать слишком много и выполнять слишком мало.

- **Разделы пропущены или не содержат полезной информации.** Правило простое: чем больше информации — тем лучше. Если проект не предоставляет достаточно информации о себе, он является весьма сомнительным и должен рассматриваться как таковой.
- **Вайтпейпер где-то спрятан.** В настоящее время большинство проектов имеют раздел или ссылку на документацию на официальном сайте. Если вам приходится поднапрячься, чтобы найти необходимую информацию о проекте, это признак того, что команда не очень хочет, чтобы вы её нашли.

Три основы блокчейна

Как следует из вайтпейпера Биткоина, с технической точки зрения блокчейн представляет собой объединение концепций криптографии, теории игр и информатики. Давайте в общих словах рассмотрим, какую роль эти компоненты играют в устройстве блокчейна.



Схема технологических основ блокчейна

Все транзакции блокчейна криптографически защищены, независимо от их назначения. Используя криптографию, можно гарантировать, что лишь подлинный пользователь инициирует транзакцию, и никто не может выступать от его имени.

Но что, если узел или пользователь пытается запустить атаку с двойным расходом? Обратите внимание — двойные траты являются криптографически допустимыми. Алгоритму шифрования безразлично, сколько у вас денег. Единственный способ предотвратить двойные расходы — сделать так, чтобы каждый узел знал обо всех транзакциях.

Однако это приводит к другим интересным проблемам:

- Поскольку каждый узел должен поддерживать базу данных транзакций, как они могут согласовать общее состояние базы данных?
- Как система может оставаться невосприимчивой к ситуациям, когда один или несколько вычислительных узлов намеренно пытаются подорвать систему и внедрить фальшивое состояние базы данных?

На самом деле и подобные проблемы, и их решения пришли из теории игр. **Теория игр** — это математический метод изучения оптимальных стратегий в играх. Под игрой понимается процесс, в котором участвуют две и более стороны, ведущие борьбу за реализацию своих интересов.

Например, при описании алгоритмов консенсуса в блокчейне, часто приводится проблема византийских генералов. Это задача из теории игр, которая была описана ещё в 1982 году. Вероятно, именно она подтолкнула Сатоши Накамото на идею блокчейна.

Действительно, теория игр привнесла принципиально иной подход к определению поведения системы. Её методы, пожалуй, самые жесткие и циничные. Обычно они никогда не учитывают, является ли узел честным, злонамеренным, этичным или имеет какие-либо другие подобные характеристики. Считают, что участники действуют исключительно в соответствии с выгодами, которые они получают, и не подвержены предрассудкам морали. Цель теории игр в блокчейне — обеспечить стабильность системы (т. е. равновесие по Нэшу) с консенсусом среди участников.

Равновесие по Нэшу гласит, что в любых некооперативных играх, в которых игроки знают стратегии друг друга, существует, по крайней мере, одно равновесие, при котором все игроки используют свои лучшие стратегии для получения максимальной выгоды, и ни одна из сторон не выиграет от изменения своей стратегии.

Базовые протоколы криптографии и консенсуса теории игр могут быть разными в зависимости от прикладного применения, но общий принцип ведения согласованного реестра или базы данных проверенных транзакций всегда один и тот же. Хотя понятия криптографии и теории игр существуют уже весьма давно, именно в области информатики эти фрагменты соединяются между собой посредством организованных структур данных и технологий одноранговой сети.

Устройство блокчейна показывает, что для реализации любых логических или математических концепций в разработке, необходимо охватывать смежные области знаний. Именно благодаря такому подходу, разработчики Биткойна смогли внедрить в систему онлайн-платежей понятия криптографии и теории игр, позволяя децентрализовать и распределить вычисления между узлами.

Что такое децентрализация

Мы увидели, что блокчейн создан для децентрализации и отвергает централизованный подход. Тем не менее термины «децентрализованный» и «централизованный» не всегда понятны. Зачастую они очень плохо определены и вводят в заблуждение. Дело в том, что почти не существует систем, которые являются чисто централизованными или децентрализованными.

Централизация или децентрализация системы определяется не только технической архитектурой. Система может быть централизованной или децентрализованной с технической точки зрения, но логически или политически может быть устроена совершенно иначе. Давайте рассмотрим эти аспекты архитектур, чтобы в будущем мы могли правильно проектировать системы исходя из потребностей пользователей.

Технический аспект. Здесь мы анализируем, сколько физических компьютеров (или узлов) используется для создания системы, а также количество отказов узлов, которые она может выдержать до того, как вся система рухнет и т. д.

Политический аспект. Здесь мы анализируем контроль, который человек, группа людей или организация имеют над системой в целом. Если все компьютеры системы контролируются узким кругом лиц, то система совершенно очевидно централизована. Однако если ни один конкретный субъект или группа не контролирует систему, и у всех пользователей есть равные на нее права, то в политическом смысле это децентрализованная система.

Логический аспект. Система может быть логически централизована или децентрализована исходя из ее устройства, — вне зависимости от того, централизована она или децентрализована технически и политически. Это можно пояснить таким примером: представьте, что вы вертикально разрезаете систему пополам, причем каждая половина имеет своих поставщиков услуг и потребителей. Если обе половины могут работать как независимые единицы, значит, они логически децентрализованы. В противном случае — это логически централизованная система.

Все вышеупомянутые подходы имеют решающее значение при разработке реальной системы и определении ее как централизованной или децентрализованной. Давайте обсудим некоторые из примеров смешанного подхода, чтобы стало понятнее:

- Если вы рассматриваете корпорации, то они централизованы архитектурно (один головной офис), централизованы политически (управляются генеральным директором или советом директоров) и они также централизованы логически (вы не можете разрезать их пополам);
- Наш язык общения децентрализован со всех точек зрения — как в архитектурном, так и в политическом плане, а также логически. Когда общаются два человека, их язык не обусловлен политически, а также логически не связан с языком общения других людей;
- Системы торрентов — такие как BitTorrent — также децентрализованы со всех точек зрения. Любой узел может быть поставщиком или потребителем. Даже если вы разрезаете систему на половинки, она по-прежнему функционирует;
- Сеть доставки контента является децентрализованной по архитектуре, а также децентрализованной логически, но политически она централизована, поскольку принадлежит корпорациям. Примером может служить Amazon CloudFront;

- Теперь рассмотрим блокчейн. Назначение блокчейна заключается в том, чтобы обеспечить децентрализацию. Действительно, он децентрализован технически. Кроме того, он децентрализован с политической точки зрения, поскольку его никто не контролирует. Однако блокчейн централизован логически, так как существует единственное общее согласованное состояние, и вся система ведет себя как один глобальный компьютер. Забегая немного вперед, это исправляется наличием шардинга, о котором мы поговорим на второй лекции.

Следующий вопрос: почему децентрализация вообще полезна? Обычно выдвигается несколько аргументов:

- **Отказоустойчивость.** Децентрализованные системы с меньшей вероятностью случайно выйдут из строя, поскольку они полагаются на множество отдельных компонентов.
- **Устойчивость к атакам.** Децентрализованные системы дороже атаковать, уничтожать или манипулировать ими, поскольку в них отсутствуют центральные точки.
- **Соппротивление сговору.** Участникам децентрализованных систем трудно вступать в сговор, чтобы получить выгоду для себя, за счет других участников. В то же время руководство корпораций и правительств вступают в сговор, способами, которые приносят пользу им самим, но наносят вред пользователям.

Блокчейн, представляющий собой децентрализованную одноранговую систему, имеет свои преимущества и недостатки. Имейте в виду, что блокчейн — это не волшебная палочка, которая может решить все проблемы в мире, но есть конкретные случаи, когда он помогает прямо сейчас. Бывают также ситуации, когда добавление блокчейна в существующее решение делает его более надежным, прозрачным и защищенным. Внедрение блокчейна может привести к катастрофе, если не будет реализовано правильно.

Если вы обратите внимание на положение дел в области программного обеспечения, то увидите, что многие программные решения имеют централизованный характер. Причина не в том, что их легко разрабатывать и поддерживать, а в том, что мы привыкли к такому устройству, чтобы иметь возможность доверять системе. Нам всегда нужна надежная третья сторона, которая может подтвердить, что нас не обманывают, и мы не станем жертвами мошенничества. Мало кто захочет иметь дело с теми, кого не знал раньше.

Давайте приведем пример из повседневной жизни, который покажет, что и у централизованных систем есть свои преимущества. Сегодня, когда мы заказываем что-то из маркетплейса, мы чувствуем себя в безопасности и уверены в доставке товара. Производитель товара — это одна сторона сделки, а покупатель — другая сторона. Тогда какую роль здесь играет маркетплейс? Он действует в качестве доверенного посредника, а также упрощает транзакции. Покупатель доверяет продавцу, хотя доверительные отношения фактически навязаны посредником.

Изобретение блокчейна показало, что в современную цифровую эпоху, не нужна третья сторона, которая навязывает доверие, и технология уже достаточно развита, чтобы обойтись без посредника. В блокчейне доверие является неотъемлемой частью системы, по умолчанию.

Кто разрабатывает Биткоин

Как уже говорили, Сатоши Накамото — тот, кто впервые описал Биткоин и блокчейн, в современном его представлении. Есть много конспирологических версий о том, кто этот человек, или даже группа людей. Не будем их рассматривать, вы сами можете узнать об этом в интернете. Нам важно разобраться, кто разрабатывает Биткоин и как ведётся работа над ним. Во-первых, чтобы убедиться в том, что Биткоин децентрализован не только технически, но и политически. Во-вторых, чтобы рассмотреть пример того, как устроена разработка блокчейн-проекта.

Людей и организаций, работающих над Биткоином, очень много. Главная задача команды, которая трудится над кодом и тестами, — обеспечить стабильность системы, поэтому изменения принимаются медленно. Программное обеспечение разрабатывается [на GitHub](#) с использованием системы управления версиями Git. Посмотреть публичный репозиторий может любой, как и предложить правку. Поэтому в списке участников на официальном сайте много людей, внесших минимальный вклад.

Bitcoin Core — это проект с открытым исходным кодом, который поддерживает и выпускает клиентское программное обеспечение под названием «Bitcoin Core». Оно является прямым потомком оригинального программного клиента Биткоин, запущенного Сатоши Накамото после того, как он опубликовал знаменитый вайтпейпер.

Обсуждение нововведений ведётся на GitHub. Также используется почтовая рассылка и сервер `irc.freenode.net #bitcoin-dev` для отдельных обсуждений.

Значительные корректировки в протоколе почти не допускаются. Тем, кто хочет нововведений, предлагается делать форки (альтернативные версии). Существенные изменения должны быть приняты большинством владельцев майнинговых пулов, по всем вопросам ведется голосование. Давать разрешение на добавление любой новой правки в основной код могут только ключевые пользователи — мейнтейнеры или технические администраторы.

В репозитории проекта по созданию Биткоина находится 8 доверенных ключей. Принадлежат следующим людям:

1. Владимир ван дер Лаан (Wladimir van der Laan, laanwj). Занимается проектом с 2011-го. Ведет блог на английском. В начале 2021-го решил отойти от активной разработки и выполняет функции зрителя.
2. Питер Вьюлле (Pieter Wuille, sipa). Согласно его профилю на LinkedIn (LinkedIn заблокирован на территории РФ за нарушение правил хранения персональных данных российских пользователей) работает в Chaincode Labs. В 2014-м стал соучредителем Blockstream. Известен по работе над Segregated Witness (BIP 141 и 144) и Taproot / Schnorr (BIP 340, 341 и 342).
3. Йонас Шнелли (Jonas Schnelli, jonasschnelli). Участвует с 2013-го года. В начале 2021-го получил грант от Marathon Patent Group. В октябре 2021 заявил, что уходит из группы главных разработчиков, но на текущее время все еще остается среди технических администраторов.
4. Марко Фальк (Marco Falke, MarcoFalke). Наиболее активный участник проекта (порядка 2 тысяч коммитов). Работает с 2016-го года. Предпочитает заниматься тестированием. Номинант и получатель грантовой выплаты от биржи OKCoin.
5. Сэмюэль Добсон (Samuel Dobson, meshcollider). Имел прямой доступ к коду криптовалюты, занимался безопасностью протокола. 9-го декабря 2021-го официально заявил, что уходит, чтобы заниматься наукой.
6. Майкл Форд (Michael Ford, fanquake). В проекте с 2012-го года. Стал мейнтейнером в 2019-м году после собрания CoreDev. Получил грантовое поощрение от Gemini.
7. Геннадий Степанов (Hennadii Stepanov, hebasto). Опытный программист, получил грант на участие в поддержке и улучшении Биткоина в 2020-м году, заслужил продление этого гранта — 2021. Занимается сетевой обработкой, интерфейсом, сборкой и проверкой, контролем тестирования.

8. Эндрю Чая (Andrew Chow, achow101). Работает инженером в Blockstream, основное направление деятельности — интерфейс аппаратного кошелька. Проводит тематические трансляции по программированию в Twitch.

Людей, которые обладают доверенными ключами, называют также техническими администраторами. Как поступать с доступом ушедших из группы людей, решает команда разработчиков программы. В Bitcoin-репозитории пока прописаны все доверенные ключи, в том числе и тех людей, которые заявили о своем уходе.

Предложить изменения в коде Bitcoin Core может любой. Поэтому на сайте криптовалюты перечислено 350 человек — все у кого было хотя бы 2 коммита.

Похожим образом в опенсорсе развивается большинство других блокчейнов, о которых мы поговорим на следующих лекциях.

Как выглядит блокчейн Биткоина

Теперь, когда мы рассмотрели теоретическую основу блокчейна, давайте взглянем на него с практической стороны. Для этого продолжим рассматривать пример Биткоина, потому что это первый в истории блокчейн, это главный представитель блокчейнов первого поколения и он до сих пор остаётся самым популярным блокчейном в мире.

Публичные и приватные блокчейны

Первое, что необходимо отметить, Биткоин — это публичный блокчейн. Простыми словами, это означает, что мы можем узнать любую информацию, которая в нём хранится, пусть даже и в зашифрованном виде. Но для дальнейшего повествования будет важно рассмотреть разницу между публичными и приватными блокчейнами.

Виталик Бутерин, сооснователь блокчейна Ethereum, в статье 2015 года «О публичных и частных блокчейнах» выделил три типа блокчейнов:

1. **Публичные блокчейны.** Они общедоступны — любой пользователь может создавать блоки, совершать транзакции и смотреть их историю. При этом пользователи могут оставаться анонимными. Такие блокчейны обычно полностью децентрализованы, то есть не имеют администраторов. Большинство криптовалют используют публичные блокчейны.
2. **Приватные блокчейны.** В таких блокчейнах, правом записи информации обладает только один участник или узлы, уполномоченные этим

единственным администратором. Это централизованные персонифицированные системы, поскольку существует иерархия полномочий. Но, сохраняется распределённый характер хранения данных, при котором узлы содержат полные копии в формате взаимосвязанных цепочек блоков. Доступ к информации может быть общим или иметь произвольные ограничения. Чаще всего такие блокчейны используют внутри одной компании.

3. **Консорциумные блокчейны.** В таких блокчейнах процесс согласования обеспечивается несколькими, заранее оговорёнными, равноправными узлами. Например, консорциум из 15 банков договаривается считать действительным блок с подписью не менее 10 участников консорциума. Данные блокчейны наиболее полезны для нескольких организаций, которым требуется единая платформа проведения транзакций или обмена информацией.

Так как Биткоин — это публичный блокчейн, все данные, которые хранятся в нём, можно посмотреть в блокчейн-обозревателе.

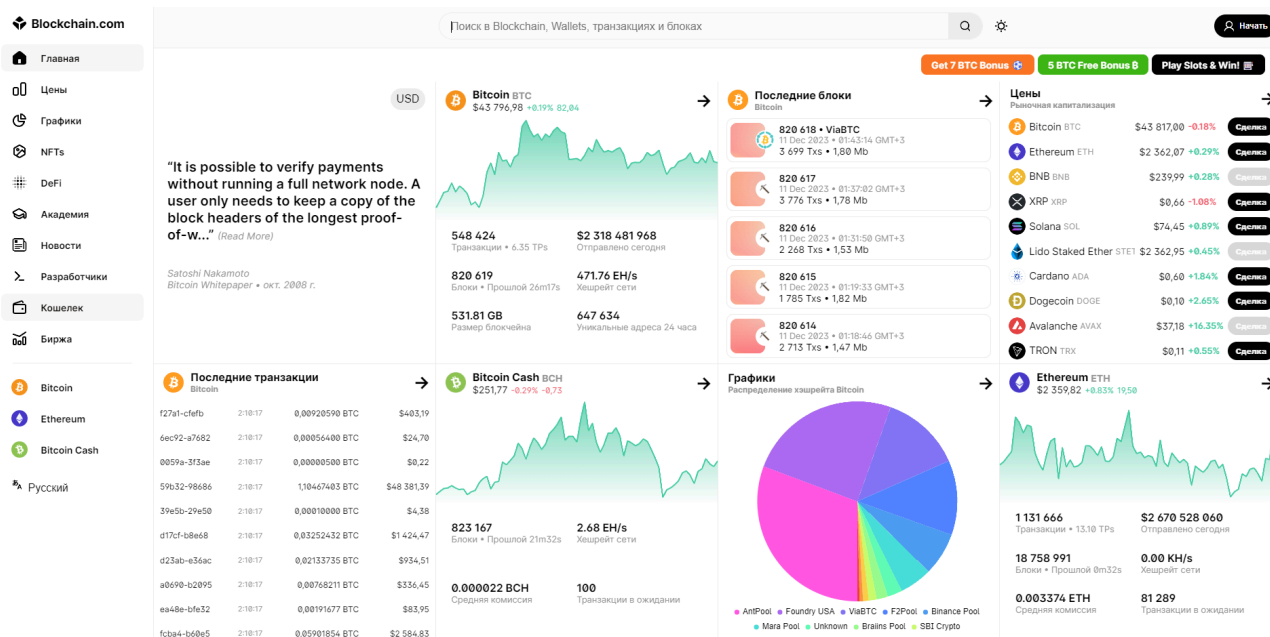
Блокчейн-обозреватель — это онлайн-сервис, содержащий историю транзакций одного или нескольких публичных блокчейнов.

Блокчейн-обозреватели

Как вы уже знаете, структура блокчейна представляет собой цепочку блоков транзакций. Другими словами, блоки связаны друг с другом посредством криптографического хеша. Именно эта структура делает блокчейн-обозреватель не только возможным, но и мощным инструментом для обеспечения прозрачности и доверия в экосистеме.

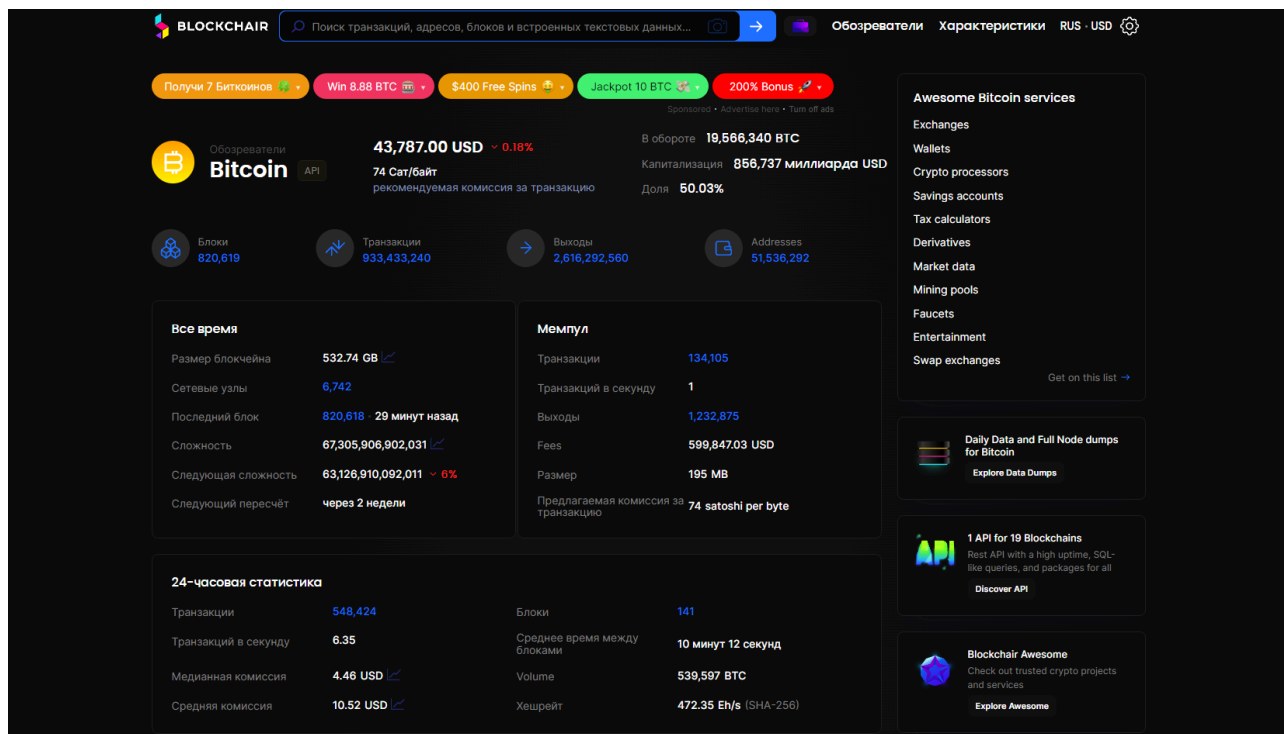
Несколько самых популярных блокчейн-обозревателей:

1. **Blockchain.com Explorer.** Сервис стал одним из первых в своем роде и сохраняет популярность и на сегодняшний день. Поддерживает сети Bitcoin, Ethereum и Bitcoin Cash. Представленная информация: сведения о транзакциях, адресах и блоках, размер и статус. Можно отслеживать отдельные криптовалюты, их бэкграунд, динамику цен, а также блоки и транзакции.



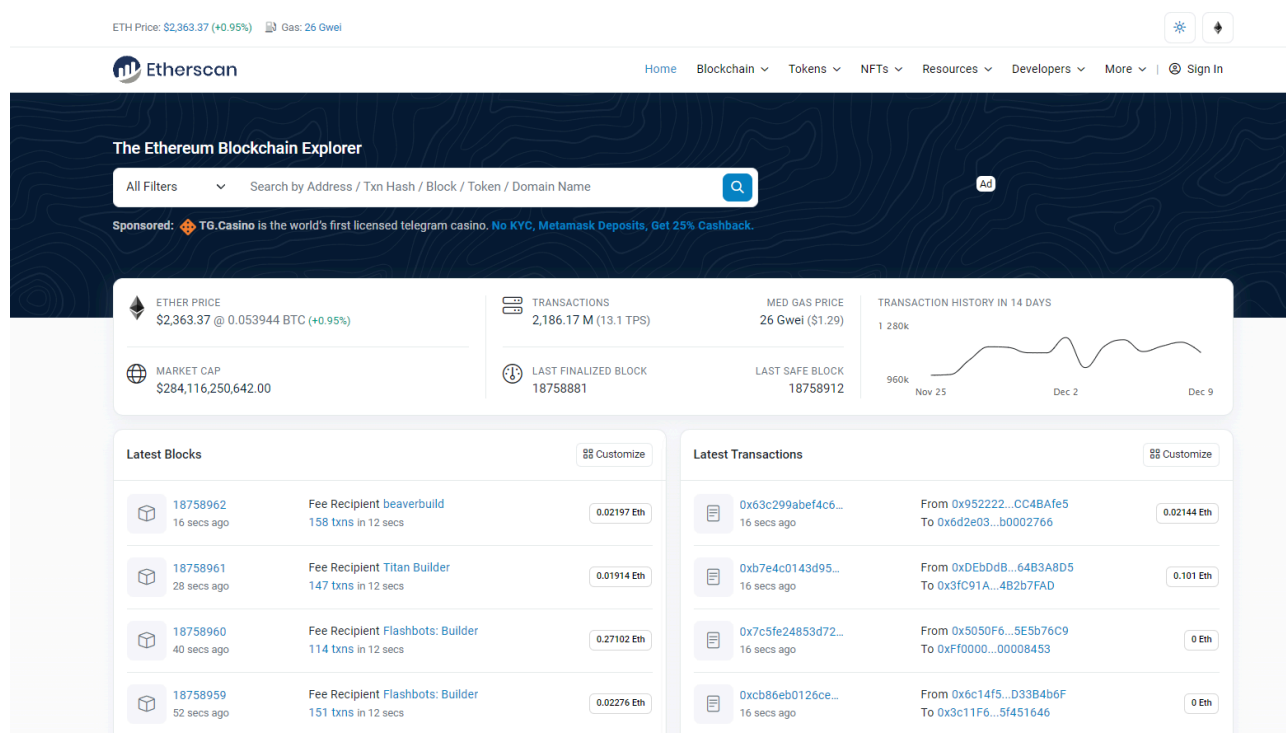
Blockchain.com Explorer удобен тем, кто следит за динамикой цен криптовалют

2. **Blockchair.** Этот блокчейн-обозреватель предлагает больше данных, чем Blockchain.com. Помимо Биткоина, он поддерживает ещё 16 блокчейнов. Blockchair позволяет искать транзакции, адреса, блоки и даже встроенные текстовые данные. Помимо информации о конкретных транзакциях, система также собирает данные о статусе блокчейнов, включая объемы криптовалют, количество транзакций на блок и т. д.



Blockchain удобен тем, кому важно получить максимум технической информации

3. **Etherscan.** Это обозреватель блокчейна Ethereum. Позволяет отслеживать любые элементы события в сети: транзакции, блоки (в том числе до и после форка), токены стандартов ERC-20, ERC721 и ERC-1155 и их перемещения, а также многое другое.



На Etherscan представлена самая полная информация о блокчейне Ethereum

Большинство блокчейн-обозревателей обладают следующими базовыми возможностями:

- **История транзакций.** Просмотр истории транзакций для любого адреса кошелька.
- **Анализ блоков.** Просмотр подробной информации о каждом блоке, включая время, размер, информацию о майнере и содержащихся в нем транзакций.
- **Отслеживание в реальном времени.** Данные о блоках и транзакциях в реальном времени по мере их передачи и подтверждения.

Рассмотрим пример того, какую пользу могут принести блокчейн-обозреватели. Представьте, что вы отправляете биткоины своему другу. Когда вы вводите адрес его кошелька и жмете «отправить», создается транзакция. В ней записывается следующая информация:

1. кто отправил биткоины;
2. кому отправили биткоины;
3. когда отправили биткоины;
4. сколько биткоинов отправили.

Однако, что происходит дальше с транзакцией непонятно. Ваш друг может долго ждать, когда ему придут биткоины и не понимать, действительно ли вы их отправили или ошиблись адресом.

Эту и другую информацию о своей транзакции можно узнать в блокчейн-обозревателе. При этом не обязательно вручную искать конкретный блок. Самый простой способ найти и отследить транзакцию в блокчейне — это выполнить ее поиск по идентификатору транзакции (TXID). Когда происходит транзакция, блокчейн генерирует эту уникальную строку букв и цифр. Если вы являетесь отправителем или получателем транзакции, ваш кошелек отобразит связанный с ней TXID.

Введя TXID в блокчейн-обозревателей, любой может просмотреть детали транзакции, включая адреса кошельков отправителя и получателя, переведенную сумму, дату и время транзакции, а также ее текущий статус (ожидает ли она подтверждения, подтверждена или не удалась). Например, в блокчейн-обозревателей Blockchair информация о транзакции будет выглядеть следующим образом.

Transaction hash

f6bb9c7057f79e9bf8e3e162e129c73119b30832518386e6951abc4ffa5a7614

Сумма сделки

0.00006329 BTC · 2.77 USD

Комиссия

0.0000201 BTC · 0.88 USD

Комиссия за байт

16 satoshi

3 минуты назад ·

10 дек 2023 г., 23:24 UTC

Статус транзакции

Ожидание подтверждений · 0 of 6

Очередь: 54688 of 131608

Расчетное время до подтверждения: через 1 день

Размер	267
Уничтоженные монетодни	0
Вес	513
Комиссия за Кбайт	7,528 satoshi · 3.29 USD
Комиссия за весовую единицу	3,918 satoshi · 1.71 USD
Coinbase?	No
Есть данные свидетеля?	Yes
RBF включен	Yes
Время блокировки	0
Версия	2 ₁₀

Additional info

Получение транзакции

Notify me

Отправители 1

bc1p2mhhz749t8jx669phugynnesc9ak6wmch5chss5yxz1xzchxhgns726tcp

← 0.00008339 BTC · 3.64 USD

Получатели 1

bc1q3jznjp8nywcm94x8g9c96kn5zmq0s5px5qnga0

0.00006329 BTC · 2.77 USD

BC.GAME - the best crypto casino. Up to 5 BTC daily bonus, 760% deposit bonus. Play now.

Sponsored · Advertise here · Turn off ads

Конфиденциальность

60 Moderate

Вопросы: 1

Privacy-o-meter shows the level of traceability of a transaction via various tracking tools

Данные о случайной транзакции в блокчейн-обозревателе Blockchair

Данная транзакция ожидает подтверждения. Это означает, что другие участники блокчейна — майнеры — ещё не проверили её и не добавили в новый блок. В каждом блоке Биткоина помещается около 2,5 тыс. транзакций. В первую очередь майнеры добавляют в блоки те транзакции, за которые пользователи предложили наибольшую комиссию. Так как в среднем новые блоки создаются раз в 10 минут, 54688 место в очереди означает, что транзакция подтвердится не раньше, чем через день.

Можно заметить, что в созданной транзакции был включен RBF. Эта аббревиатура расшифровывается как «Replace-By-Fee» и означает функцию, с помощью которой существующая транзакция может быть заменена новой транзакцией с повышенной комиссией. Такую функцию поддерживают не все кошельки, поэтому не всегда ускорить транзакцию в блокчейне Биткоина оказывается легко.

В примере, блокчейн-обозреватель помог узнать, что для транзакции была выбрана слишком низкая комиссия, и мы можем ее повысить. Случаев, когда может вам

пригодиться блокчейн-обозреватель гораздо больше. Например, в Blockchair также можно оценить уровень конфиденциальности своего адреса или сформировать чек.

Недостатки Биткоина

В заключении отметим, что блокчейн Биткоина не является идеальной технологией. У него есть свои уязвимости и недостатки. Большинство из них стали предпосылкой для дальнейшего развития децентрализованных технологий и появления следующих поколений блокчейнов.

Атака 51%

Напомним, что алгоритмом консенсуса в блокчейне, называется метод, который описывает, как выбирается майнер в блокчейне и по каким правилам он создаёт блоки. В Биткоине и других блокчейнах первого поколения используется алгоритм доказательства работы — Proof of Work (PoW). Его суть заключается в том, что для создания новых блоков майнер должен будет использовать свой компьютер для решения сложных криптографических задач.

Алгоритм будет считать верной версией блокчейна ту, в которой больше всего блоков. А больше всего блоков будет в той версии, на создание которой майнеры потратили больше всего компьютерных мощностей. Получается очень демократичный метод: если 51% майнеров считают, что транзакции в блоки правильные, так и будет. Поэтому такой блокчейн почти невозможно взломать. Но в слове «почти» и кроется уязвимость.

Атака 51% – это захват системы, при котором майнинговая мощность злоумышленника превышает остальную мощность системы как минимум на 1%.

Наиболее актуальна эта проблема для небольших блокчейнов. Для успешной атаки на биткоин хакеры должны владеть мощностью, превышающей остальную часть сети. Так как в блокчейне Биткоина работают сотни тысяч майнеров, мошенникам потребуется потратить огромные суммы денег на технику, чтобы конкурировать с остальной частью сети. Даже самое совершенное майнинговое оборудование не может напрямую конкурировать с общей вычислительной мощностью в этой сети.

Помимо этого, есть ряд других аргументов против выполнения атаки 51% на Биткоин. Например, риск быть привлеченным к ответственности, высокие расходы на электроэнергию, хранение оборудования для майнинга и аренду помещения.

Потенциальная уязвимость Биткоина стала основой для дальнейшего развития блокчейнов и алгоритмов консенсуса. Для более современных блокчейнов, второго и третьего поколений, атака 51% уже не является актуальной.

Квантовая устойчивость

Блокчейн, как и большинство распространённых на сегодняшний день методов шифрования информации, оказывается уязвимым для квантовых компьютеров. С помощью асимметричного шифрования, которое используется в блокчейне, легко проверить, что хэш блока соответствует его содержимому и очень сложно подобрать содержимое блока, которое соответствовало бы конкретному хэшу. Квантовые алгоритмы способны обогнать обычные компьютеры при переборе хэшей.

Если одним из узлов сети блокчейна станет квантовый компьютер, то он сможет подделать электронные подписи пользователей, проводящих транзакции, и подписи авторов блоков. Более того, квантовый компьютер может гораздо быстрее создавать новые блоки. Это может обеспечить квантовому узлу преимущество и в теории позволить генерировать больше половины всех новых блоков в сети. В теории это позволит владельцу узла записать новую ветвь блокчейна с желаемой информацией и сделать ее основной.

Проблему квантовых компьютеров можно назвать потенциальной, но пока не реальной. В ближайшие годы криптомиру ничего не угрожает: квантовые компьютеры пока остаются в лабораториях, и вряд ли будут доступны частным лицам.

Алгоритмы шифрования и методы обеспечения безопасности в блокчейне тоже не стоят на месте — на потенциальную угрозу всегда найдется способ предотвращения. При известном прогрессе в квантовых вычислениях есть время для разработки методов противодействия.

Что может обезопасить блокчейн от квантовых компьютеров:

- более сложный алгоритм хэширования (например, SHA-512),
- больший размер приватного ключа,

- переход на постквантовую криптографию.

Ограниченная функциональность

Блокчейн окончательно сформировался как технология в 2009 году, вместе с появлением криптовалюты Биткоин. Но оказалось, что это лишь частное применение блокчейна в сфере финансов. Вскоре после запуска Биткоина люди смогли оценить истинный потенциал блокчейна, далеко выходящий за рамки криптовалют.

В следующей лекции мы рассмотрим потенциал блокчейна в других отраслях. Мы будем говорить о блокчейнах второго поколения, которые значительно расширили практическое применение этой технологии.

Заключение

- Запуск Биткоина в 2009 году стал первым примером блокчейна в современном его понимании.
- Биткоин и другие похожие системы денежных переводов принято называть блокчейнами первого поколения.
- Основой блокчейна стали последние достижения науки в областях криптографии, теории игр и информатики.
- Система может быть централизованной или децентрализованной с технической точки зрения, но логически или политически может быть устроена совершенно иначе.
- Биткоин и прочие публичные блокчейны чаще всего развиваются как опенсорс-проекты.
- Блокчейны первого поколения уязвимы для атаки 51% и ограничены лишь использованием в сфере финансов.

Дополнительные материалы

1. Вайтпейпер «[Биткойн: система цифровой пиринговой наличности](#)», Сатоши Накамото, 2008.
2. Серия статей «[Блокчейн-новичок](#)».

3. Статья [с описанием задачи византийских генералов](#).
4. Видео «[Основные теоремы в теории игр — Алексей Савватеев на ПостНауке](#)».
5. Статья «[A Digital Signature Based on a Conventional Encryption Function](#)», Ralph C. Merkle, 1987.
6. Статья «[How to time-stamp a digital document](#)», Stuart Haber, W. Scott Stornetta, 1991.
7. Статья «[On the Origins and Variations of Blockchain Technologies](#)», Alan T. Sherman, Farid Javani, Haibin Zhang, Enis Golaszewski, 2019.
8. База данных вайтпейперов [whitepaper.io](#).

Использованная литература

1. [«Блокчейн. Руководство для начинающих разработчиков», Сингхал Бикрамадитья, Панда Приянсу Сехар, Дамеджа Гаутам, 2020 год.](#)
2. [A Digital Signature Based on a Conventional Encryption Function | SpringerLink](#)
3. [Биткойн: система цифровой пиринговой наличности](#)
4. [Как читать и анализировать вайтпейперы? | CoinMarketCap](#)
5. [Что такое Вайтпейпер \(White Paper\) и как его читать](#)
6. [Что такое дерево Меркла? | Все, что нужно знать](#)
7. [Что такое двойная трата?](#)
8. [Вайтпейпер Биткоина понятными словами - 2Bitcoins.ru](#)
9. [The Meaning of Decentralization](#)
10. [Кто разрабатывает и финансирует Bitcoin \(BTC\)? | CoinsPaid Media](#)
11. [Vitalik Buterin: On Public and Private Blockchains](#)