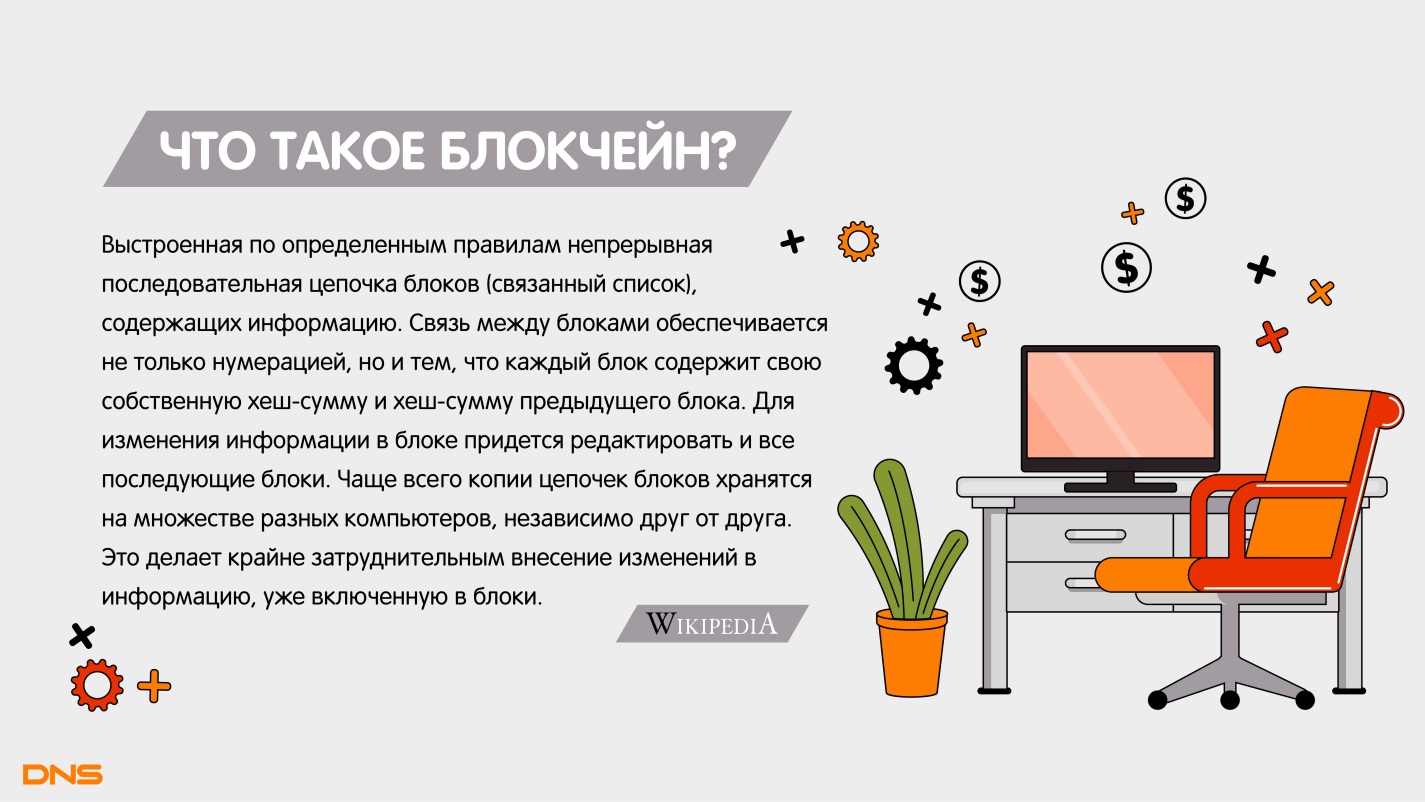
Лекция 6

# Основы блокчейн технологий

***Технологии распределенных вычислений и децентрализованного хранения информации были представлены еще в 90-х годах. Однако, слово «блокчейн» стало известно лишь недавно — когда некий Сатоши Накамото показал, как эти технологии можно использовать для устройства новой финансовой системы. Так, в 2008 году появился биткоин, а вместе с этим началась история развития блокчейна.***

В 2021 году популярность этих технологий оказалась настолько высока, что стоимость того самого биткоина уже превышает 40 000 долларов за штуку.



**Простым языком**

Давным-давно, когда еще не вышел десятый айфон, жили Роман и Антон. У Романа было несколько способов передать денежные средства Антону:

* передать наличные средства самостоятельно (Роман приходит к Антону и лично передает деньги);
* использовать услуги третьей стороны (Роман передает деньги банку, почтовой службе или курьеру, которые передают деньги Антону).



Обычно, третья сторона — это целая совокупность инстанций и сервисов. Поэтому имеем цепочку посредников, схема работы которых находится под грифом секретности. С одной стороны, это полезно в целях безопасности — даже если мы зайдем в банк и попросим рассказать технические детали нашего перевода — никто этого делать не станет. С другой стороны, безопасность легко превращается в незащищенность — не зная технических подробностей, остается лишь слепо доверять банковской системе и надеяться, что «третьи лица» окажутся добросовестными ребятами.

Дело в том, что, превращаясь из бумажных в электронные, деньги не меняют своей формы — актуальные системы просто формируют цифровой код с зашифрованной в нем информацией о типе валюты, ее стоимости и количестве, чтобы передать ее от одного хранилища другому. Физически бумажное подтверждение ценности остается на руках пользователя или в сейфе банкомата.

Другими словами, Роман может найти терминал, предложить ему наличные денежные средства и получить их у себя на карте или отправить Антону. Мы привыкли так работать и считаем это безопасным способом перемещать деньги. Но с появлением блокчейна теория безопасности принимает новый оборот.

**Посредники**



Как работает стандартная банковская система переводов: на специальных компьютерах хранится вся информация о клиентах, операциях, имена, фамилии, отчества, адреса проживания, номера лицевых счетов. Это одна из брешей безопасности, которую блокчейн легко устраняет.

Когда Роман переводит деньги Антону через банкомат или онлайн-банк, он, так или иначе, делает запрос в эту базу данных, в реестр, где программное обеспечение проверяет некоторые условия:

* Достаточно ли у Романа денег, чтобы переслать их Антону?
* Откуда они появились у Романа?
* А не занимался ли Роман нелегальным заработком?
* Заплатил ли он со своей зарплаты налог?

И еще много подобных проверок, производимых программным обеспечением банков.

После того, как системе безопасности все понравилось, у Романа списывают необходимую сумму и зачисляют на счет Антона. Это привычная система и она централизована: здесь есть свой регулятор, органы управления, но, самое главное, — в системе есть обслуживающий персонал, без которого ничего не будет работать.



Программисты, аудиторы, операционисты, бухгалтеры, руководители, и еще два десятка должностных лиц, с помощью которых вся эта система функционирует, косвенно или прямо работают с переводом денег от Романа к Антону. Это следующая брешь в безопасности, которую блокчейн тоже закрывает.

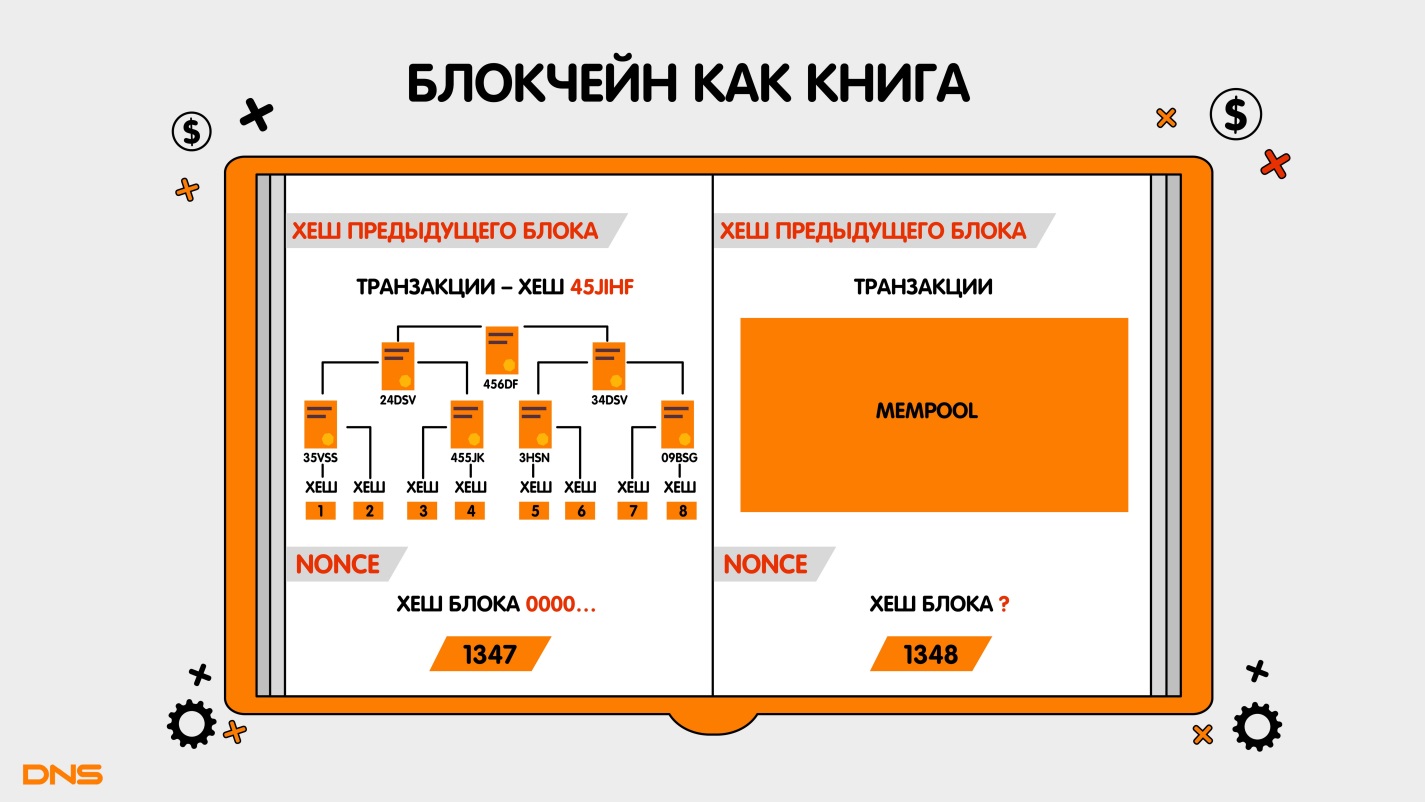
**Что такое блокчейн и как это работает**

Еще совсем недавно все расчеты производились наличными деньгами. С развитием всемирной паутины изменился и способ передачи ценностей. Сегодня, с использованием распределенных вычислений и автономных систем, в сети стало удобнее и безопаснее работать с помощью новых технологий. Например, блокчейн, где информация двигается между различными людьми без участия обслуживающего персонала, а также минуя централизацию, где существует вероятность, что вредная ошибка в коде ПО поможет хакеру забрать деньги или ценную информацию.



Начнем с того, что **блокчейн**(Block — блок, chain — цепь) — это децентрализованная база данных, которая предназначена для хранения последовательных блоков с набором характеристик (версия, дата создания, информация о предыдущих действиях в сети). Аналоговым примером его структуры представляется бесконечно длинная металлическая цепь, в которой нельзя разорвать или поменять местами звенья.

А еще цепочку блокчейна можно представить как книгу с возможностью добавлять страницы. Каждая новая страница пишется в режиме «онлайн», а остальные нельзя отредактировать или удалить.



Основное движение в такой системе происходит с помощью транзакций. Во время транзакции может выполняться какой-то скрипт, либо прописываться некая заметка с данными. То есть слово «транзакция» не равно денежному переводу и скорее обозначает способ обработки информации внутри сети.

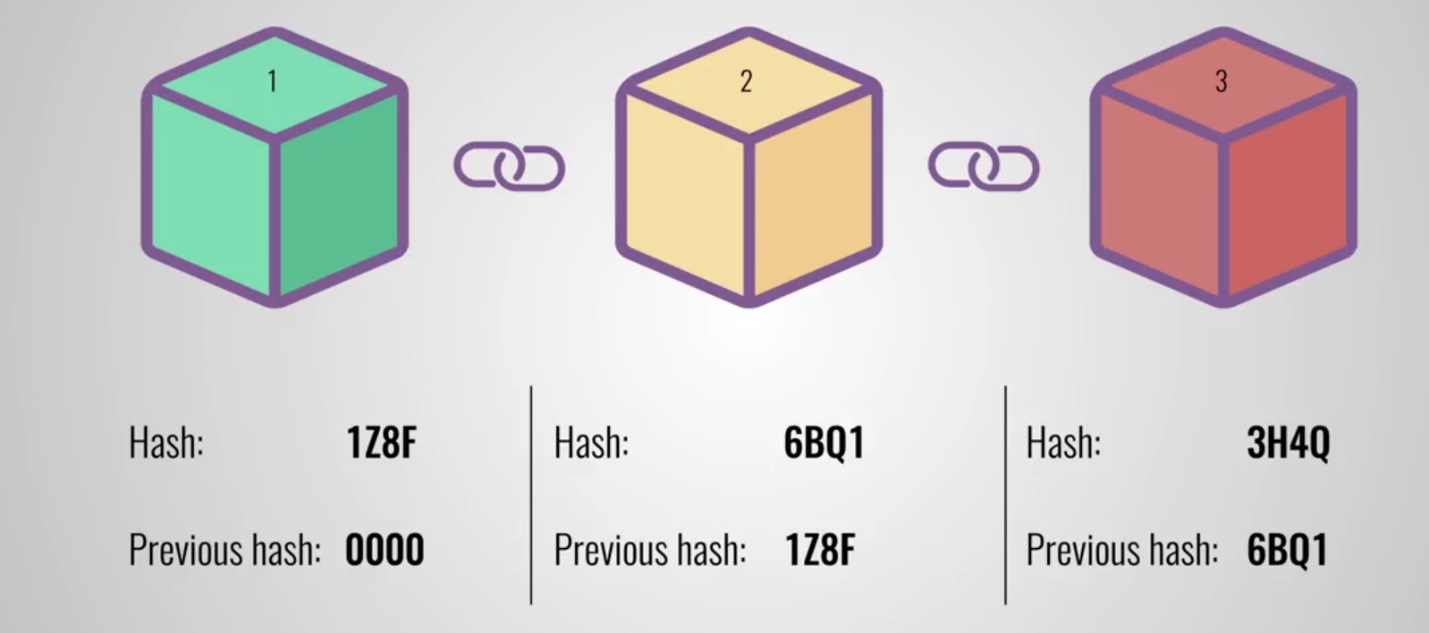
Помимо основных данных, каждый блок имеет уникальный набор параметров: nonce, хеш предыдущего блока, хеш текущего блока и список транзакций.

Чтобы лучше понять, как устроены переводы внутри сети, снова представим страницу книги, где есть такая информация:

* Олег перевел Никите 100 долларов.
* Вася перевел Хуану 300 песо.
* Никита подтвердил пополнение счета на 100 долларов.

В пределах одного блока может храниться несколько тысяч таких записей. Когда память в блоке заканчивается — он закрывается, подписывается и переходит на новый блок в виде хеша или «отпечатка».

Хеш — это некий набор символов, несущий в себе уникальный отпечаток. Он формируется исходя из того, какие транзакции и в каком количестве хранит в себе каждый блок.



В процессе обработки транзакций постоянно проверяются хеши, после чего, словно по пирамиде, система поднимается к последнему хешу, где подтверждается целостность и верность всех предыдущих кодов, чтобы блок закрылся.

Если вдруг кому-то захочется добавить себе в кошелек пару сотен долларов без подтверждения со стороны остальных участников сети, то такая транзакция будет считаться неверной и перезапишется теми хешами, что хранятся у большинства узлов. То есть, если изменить хоть один байт, хоть одну точку, запятую или ноль, то итоговый хеш изменится, и блокчейну придется проверять все эти суммы заново для того, чтобы понять, правда это или ложь.

Из всего этого можно сделать вывод: сеть состоит из блоков, которые можно менять здесь и сейчас, пока они не закрылись. Все записывается в виде транзакций с информацией, которая шифруется как хеши и постоянно хранится в сети в каждом последующем блоке. Если изменить что-то и не найти этому подтверждение у большинства участников, то такие изменения просто не применятся, а блок будет считаться невалидным.

Простыми словами — в системе больше не получится подделать документы задним числом, как бы этого не хотели даже сотни человек, если общая сеть контролируется миллионами участников.

Отсюда и название Blockchain — все работает по цепочке, последовательно и непрерывно.

**Кто такие майнеры и зачем они нужны**

основной фактор безопасности заключается в добросовестности третьих лиц, тех, кто занимается обработкой информации. Как и у банковской системы — у блокчейна есть свой обслуживающий персонал. Но это не люди, а программный код, установленный на системах с нодой (сетью) блокчейна, то есть, на компьютерах, которые поддерживают сеть блокчейн. Другими словами — с помощью майнеров.

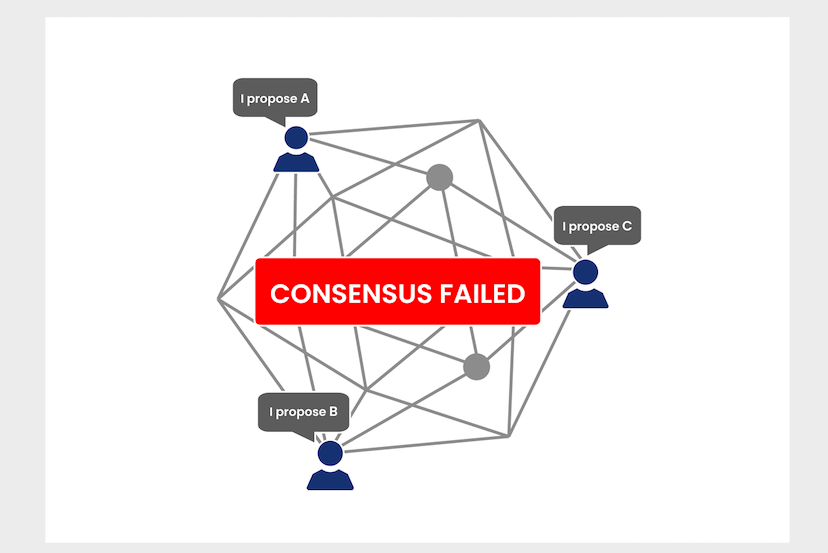
Для того чтобы провести операцию в блокчейне, необходимо ее создать и поместить в mempool — некую область, где хранятся все транзакции, которые в данный момент хотят совершить люди в блокчейне.



Что делают майнеры: они подключаются к mempool и начинают обрабатывать всю очередь. В глобальном смысле это работает так: система узнает о всех транзакциях в мемпуле, обрабатывает их, записывает в блок, высчитывает хеши и переходит к обработке новых заявок. Чтобы подтвердить валидность (правильность) блока, майнеру необходимо предоставить решение в сеть, которое проверяют другие майнеры и, если все хорошо, и большинство участников принимают результат вычисления хешей, блок считается правильным. Или nonce.

**Разберемся на жизненном примере:**

За круглым столом сидят десять человек. У них есть пять слов, из которых нужно составить предложение, которое может быть единственно верным из всех вариантов, которые можно придумать. Так, один из участников составил предложение первым и записал его на бумагу. После того, как все закончили задание, полученные предложения сравниваются. Так получилось, что первому участнику удалось составить верное предложение, и остальные семеро подтвердили, что у них получилось то же самое. И только один участник представил другое решение — но, так как он является меньшинством, а его предложение отличается от остальных, этот вариант из пяти слов считают недействительным и выкидывают из системы.



Выходит, для подтверждения настоящей информации в сети нужно договориться, чье решение подходит всем участникам в сети. Этим и занимаются криптовалютные майнеры.

Именно поэтому, в момент появления блокчейна, началась гонка за производительностью распределенных вычислений. Ведь чем больше у майнера вычислительной мощности, тем быстрее и больше информации он обработает в сети. Соответственно, как и банковский персонал, майнеры получают вознаграждение за свою работу. Это и есть основная причина, по которой все стремятся принять участие в добыче криптовалюты.

**Децентрализация и распределенность**

Для поддержки сети требуется постоянная и непрерывная работа нескольких мощных компьютеров. На сегодняшний день блокчейн обладает самой большой вовлеченностью вычислительных систем на планете. Даже такие гиганты как Google, Amazon и Apple не могут соревноваться с этой сетью по мощности.

*Чем больше людей используют блокчейн, тем мощнее и безопаснее он становится.*

Участником сети может стать каждый: достаточно установить официальный кошелек и загрузить полную ноду к себе на диск. С этого момента компьютер станет полноправным узлом в сети.

Например, у одного человека на компьютере стоит копия блокчейна. Есть еще один компьютер, на котором есть еще одна копия блокчейна, и таких десятки тысяч по всему миру. Если какой-либо злоумышленник захочет взломать систему и «нарисовать» себе миллион, мало того, что ему придется пересчитывать все эти блоки самостоятельно, ему еще придется сделать это в каждом компьютере, на каждом узле. А это, конечно же, невозможно — система полностью децентрализована и не имеет управляющих узлов. И с каждым днем таких узлов становится все больше, а шансов на взлом все меньше.



В централизованной системе вся информация хранится на сервере, и, если с ним что-то произойдет — можно попрощаться с ценными данными. В случае с централизованной системой злоумышленникам также проще найти уязвимость, чтобы атаковать главные компьютеры. Это может быть простая брешь в программной безопасности или безответственная работа сотрудника безопасности банка.

Такой большой вопрос безопасности можно решить только с помощью такой же большой сети. А под эти критерии как раз подходит система блокчейн, где каждый блок с информацией копируется одновременно на тысячи устройств без главенствующих в структуре систем.

**Транзакции в блокчейн**

В отличие от банков и электронных счетов, где для работы требуется слишком много конфиденциальной информации, блокчейн не требует от пользователей ничего: для работы понадобятся лишь два ключа, которые система выдаст при регистрации.

У каждого человека, желающего принять участие в блокчейне, есть свой публичный ключ, которым он подписывает транзакцию (как бы замыкает на ключ и пишет «отправить Васе»), а также приватный ключ, которым он может открыть посылку, которую ему прислал Вася обратно.

Публичный ключ — это некая фраза из цифр и символов, доступная к просмотру всем желающим. Если провести аналогию с биткоином, то публичный ключ — это номер кошелька, который можно отправить кому угодно для перевода средств.

Приватный ключ — это самое ценное. С помощью него подписываются все транзакции в пределах личного кошелька, а поэтому его нужно хранить в конфиденциальном месте. Например, как пароли от онлайн-банков.



**Как это работает.**

Например, у Романа и Антона есть кошельки и приватные ключи.

* Роман пишет Антону сообщение: Привет, Антон!
* Шифрует его публичным ключом Антона. И отправляет в сеть.
* Теперь Антону, чтобы прочесть сообщение Романа, нужно подключиться к сети, найти адресованную ему транзакцию, дешифровать все это своим приватным ключом и прочитать послание: Привет, Антон! (Лучше бы 100 долларов отправил).

Все, что зашифровано приватным ключом пользователя, любой человек может расшифровать при помощи своего публичного ключа. Но не открыть! Так можно узнать информацию по каждому переводу, по каждой транзакции счета — система полностью прозрачна. И в то же время анонимна — ведь никакой личной информации о человеке ключи, кошельки и блоки не хранят.

**Биткоин — это не деньги**

Мы привыкли считать, что биткоин это какая-то разновидность валюты, денег. На самом деле, понятия баланса в блокчейне нет. Все потому, что блокчейн — это просто записная книга. Обратимся к примеру на картинке:

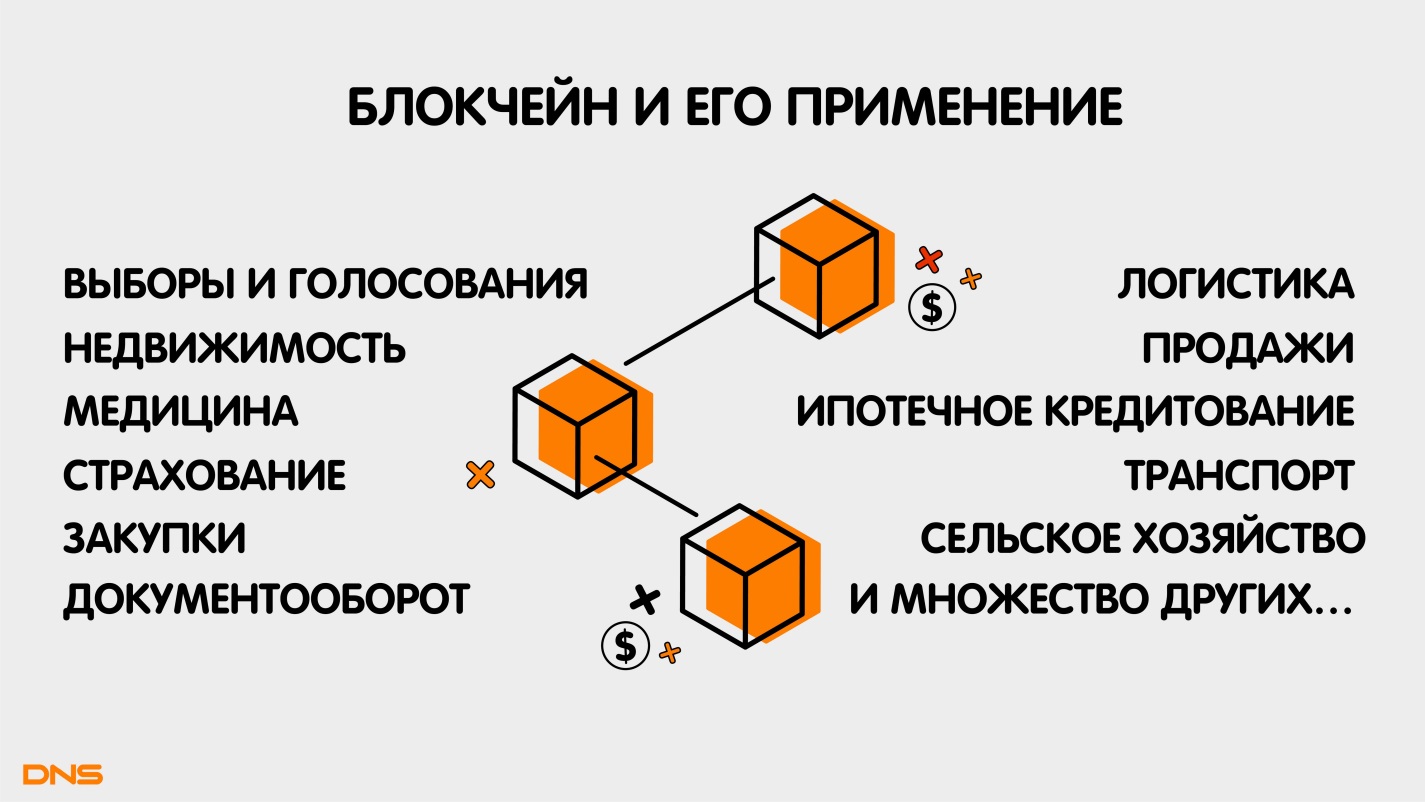


Понятно, что блокчейн собирает всю информацию о движениях Романа, Антона и Марины, а затем передает это в виде транзакций в мемпул блокчейна. А там все как по инструкции — майнеры подхватывают информацию, считают хеши и подписывают блоки, чтобы поддержать сеть и получить вознаграждение в виде комиссии, которую ребята заплатили во время своих переводов.

**Блокчейн и его применение**

Биткоин — это не золото и не деньги, а обобщенный и удачный пример работы децентрализованных сетей, где каждый может стать участником и следить за честным исполнением всех событий.

Стоимость таких технологий нельзя считать оправданной или наоборот, недостаточной — здесь все, как на настоящем фондовом рынке. Если продукт хороший и правда что-то из себя представляет, то и цифровой актив прибавит в капитализации и стоимости. Если наоборот — проект считается провалом.



Конечно, все, что связано с блокчейн и монетами, пока еще является сильно волатильными инструментами, которые порой неподвластны даже очень крутым игрокам на рынке. И все потому, что основной объем инвестиций в этой сфере делают обычные люди.

И все же, несмотря на сложность и непонятность некоторых вопросов в этой индустрии, многие уже понимают ценность, удобство и безопасность децентрализованных технологий. Каждый день появляются новости о том, как государства внедряют инновации в привычные для людей сферы. Например, учатся отслеживать подлинность паспортов здоровья с помощью блокчейна, а также разрешают проводить регистрацию ценных бумаг с помощью децентрализованных сетей.

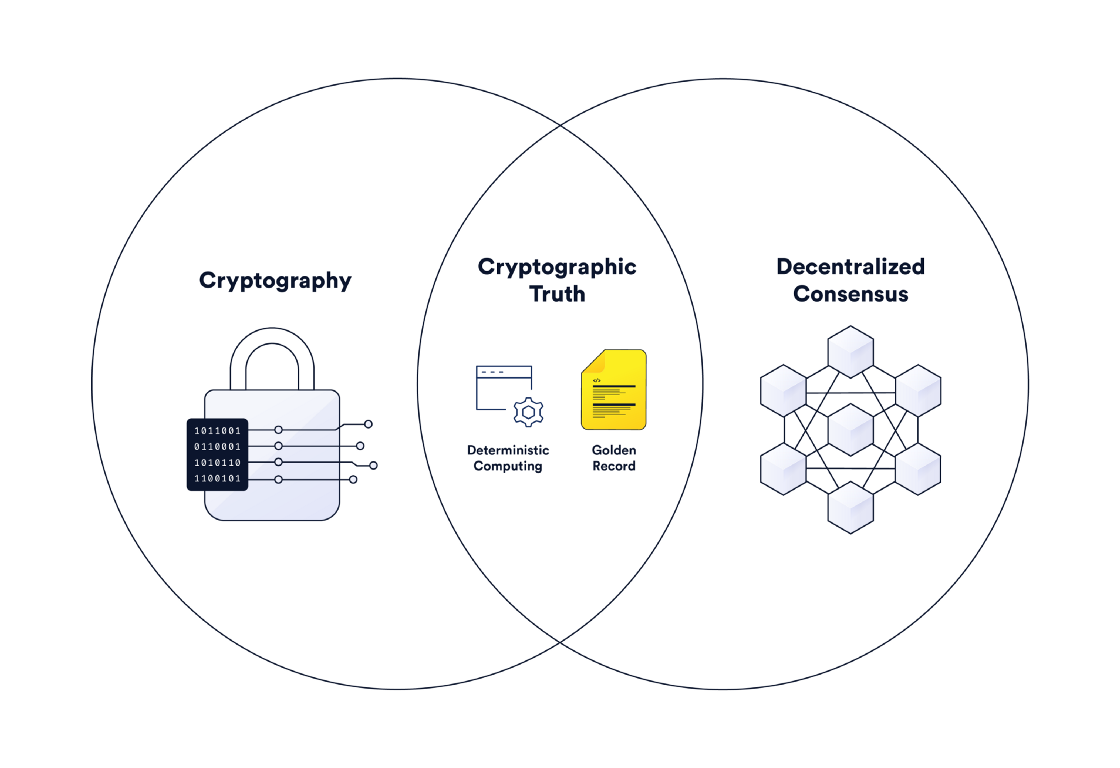


С биткоином или любым другим проектом, децентрализованные технологии станут неотъемлемой частью жизни современных структур. Ведь люди хотят обезопасить себя от мошенников, коррупционеров, хотят научиться контролировать свою жизнь больше, чем когда-либо. А блокчейн — это первый и самый большой шаг к новой системе.

# Криптография за блокчейном

Хотя технологии на основе блокчейн обладают многими качествами, которые отличают их от других вычислительных парадигм, их основным ценностным предложением является генерация криптографической истины. В самом простом смысле, криптографическая истина — это форма вычислений и ведения учета, которая является более точной, доступной, проверяемой и защищенной от взлома, чем существующие альтернативы.

Криптографическая истина происходит от инфраструктуры с минимизацией доверия — кода, который работает именно так, как задумано, потому что его выполнение и проверка не зависят от доверия к незнакомцам или неконтролируемым переменным. Блокчейн генерирует минимизацию доверия, используя криптографию для аутентификации данных и обеспечения хронологического порядка записей, а также децентрализованный консенсус для подтверждения новых записей и сохранения их неизменности. Благодаря этому механизму многосторонние процессы могут отслеживаться и выполняться на общем, достоверно нейтральном бэкенде, который стимулируется к честному управлению.

Криптографическая истина сочетает в себе криптографию и децентрализованный консенсус для создания золотой записи среди распределенного набора сущностей и детерминированного вычисления приложений.

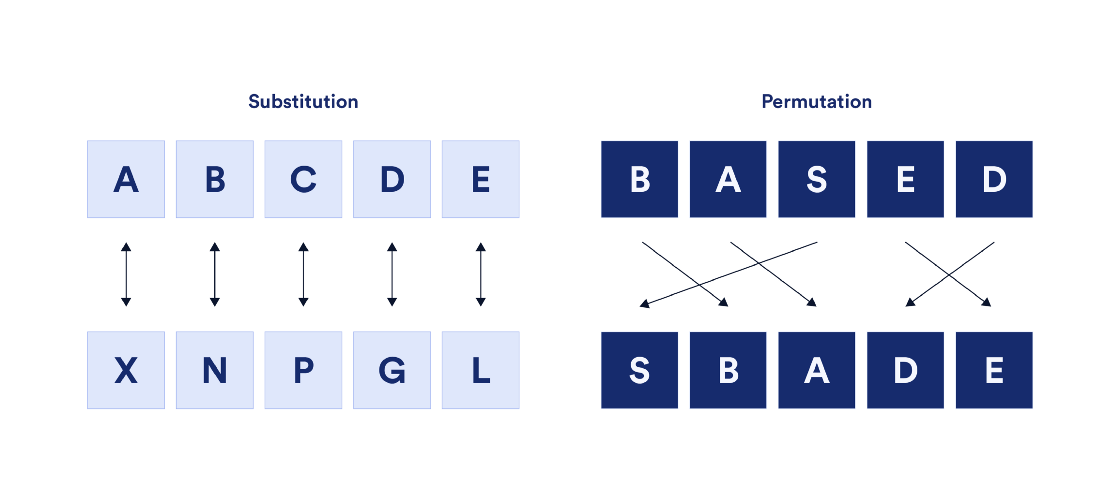
**Понимание криптографии и ее использования в блокчейн**

**Введение в криптографию**

Криптография — это наука о безопасном общении в присутствии враждебного поведения. Роль криптографии в сохранении конфиденциальности коммуникации (например, приложения для обмена сообщениями с шифрованием), она также используется для аутентификации происхождения, проверки целостности и установления безответности коммуникации; т.е. для определения того, что сообщение пришло от конкретного человека и не было подделано, и что эти свойства не могут быть опровергнуты отправителем.

Криптография используется для преобразования оригинального сообщения в неразборчивое сообщение, которое может интерпретировать только тот, кто в курсе. Шифрование — это двусторонняя функция, которая шифрует исходное сообщение (т.е. открытый текст) в неразборчивое сообщение (т.е. шифротекст), которое может расшифровать только получатель, чтобы извлечь открытый текст. Другие криптографические функции являются односторонними и направлены только на доказательство какого-либо знания или свойства данных, а не на то, чтобы сделать исходные данные известными.

Алгоритм шифрования называется шифром, а ключ — это секрет, обычно строка символов, которая позволяет кому-то понять шифр. В шифрах используются два основных типа техник: подстановка и перестановка (также называемая транспортировкой). Шифры подстановки заменяют буквы, цифры и символы открытого текста другими буквами, цифрами или символами. Шифры перестановки используют буквы открытого текста, но меняют их порядок. Для создания сложности эти методы часто комбинируются, наслаиваются друг на друга, подвергаются влиянию внешних данных и изменяются с течением времени.

Две основные техники шифрования, используемые в шифрах, — это подстановка и перестановка (также называемая транспортировкой).

Первые шифры были аппаратными, то есть они запоминались, писались от руки или создавались с помощью нецифровых машин. Однако с появлением компьютеров алгоритмы шифрования на основе программного обеспечения стали доминирующей формой шифрования.

**Современная криптография**

Современная криптография в значительной степени основана на предположениях о вычислительной трудности — представлении о том, что конкретная проблема не может быть решена эффективно. Таким образом, хотя большинство криптографических функций теоретически возможно взломать, на практике их невозможно взломать, учитывая современные ограничения вычислительной техники. Таким образом, современные криптографические алгоритмы стремятся найти правильный баланс между вычислительной эффективностью и вычислительной безопасностью, опираясь на математику и информатику для принятия решений относительно таких факторов, как длина ключа. Именно поэтому многие криптографические функции основаны на времени и бюджете, которые требуются современным вычислительным системам для поиска решений трудноразрешимых математических проблем, таких как проблема дискретного логарифма, проблема факторизации целых чисел и теоретические проблемы эллиптических кривых.

Существует три общих класса современной криптографии на основе программного обеспечения: хэш-функции, симметричное шифрование и асимметричное шифрование.

# Хеш-функции

Хэш-функции преобразуют данные любой длины в фиксированную битовую длину, называемую хэшем. Хэш — это уникальный идентификатор данных, сродни отпечатку пальца, по сути, проверяющий исходный набор данных. Хеширование данных широко используется для индексации данных и эффективного извлечения их из базы данных. Оно также используется для безопасного хранения данных, например, в случае веб-сайтов, которые хранят только соленый хэш паролей пользователей, чтобы предотвратить утечку паролей в случае взлома базы данных.

Хеш-функции не используют ключи и основаны на односторонних функциях, что обеспечивает их устойчивость к предварительным образам — практически невозможно, чтобы кто-то, кто не знает исходного сообщения, смог вычислить его по одному лишь хешу. Единственным реальным методом получения оригинального сообщения является перебор, т.е. угадывание всех возможных входных данных, что в случае хэшей представляет собой неограниченный набор возможных комбинаций символов. Алгоритмы хэширования также обычно разрабатываются таким образом, чтобы быть устойчивыми к сговору — практически невозможно, чтобы два разных входа генерировали один и тот же хэш. Эти свойства делают так, что изменение чего-либо во входных данных, например, написание буквы заглавными буквами или добавление знака препинания, приведет к совершенно другому и, казалось бы, случайному хэшу.

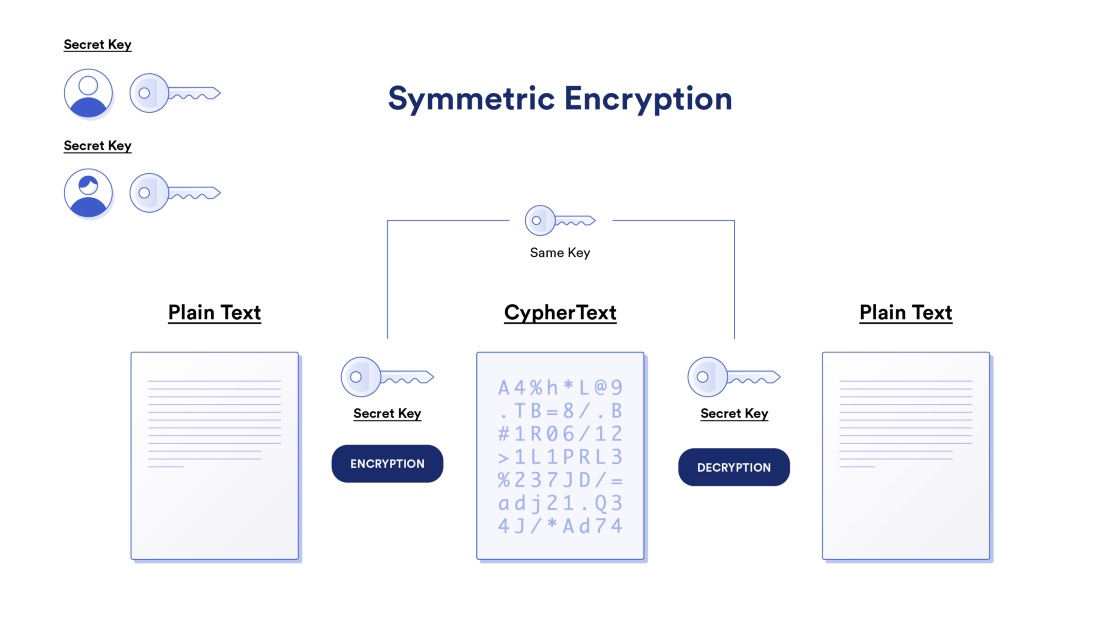
Самым популярным безопасным алгоритмом хэширования на сегодняшний день является SHA-256, который создает строки длиной 256 бит (т.е. 256 последовательных 1 и 0). 256-битные хэши часто представляются в шестнадцатеричном формате строк, поэтому их длина может составлять 32 или 64 символа. SHA-256 существует в рамках набора хэш-функций SHA-2, пришедшего на смену ныне криптографически неполноценному SHA-1. SHA-3 также был представлен в 2015 году на основе криптографического примитива Keccak.

Изменение одного символа в хэше, например, добавление запятой во втором входе, полностью изменит результат и покажется наблюдателям совершенно случайным.

**Симметричное шифрование**

Симметричное шифрование (оно же шифрование с использованием секретных ключей) предполагает использование общего секретного ключа, который отправитель и получатель используют для шифрования и расшифровки сообщений. Симметричное шифрование является быстрым и эффективным, но при этом возникает проблема безопасного обмена секретным ключом через Интернет. Хотя обмен можно осуществлять лично, этот метод не является глобально масштабируемым, поскольку требует формальных отношений с каждым контрагентом. Другая проблема заключается в том, что если секретный ключ скомпрометирован, то любой, кто его использует, рискует расшифровать все предыдущие и будущие сообщения. Именно поэтому многие интернет-протоколы, использующие симметричное шифрование, такие как TLS, также используют протоколы обмена ключами для безопасного создания общего секретного ключа без его передачи через интернет.

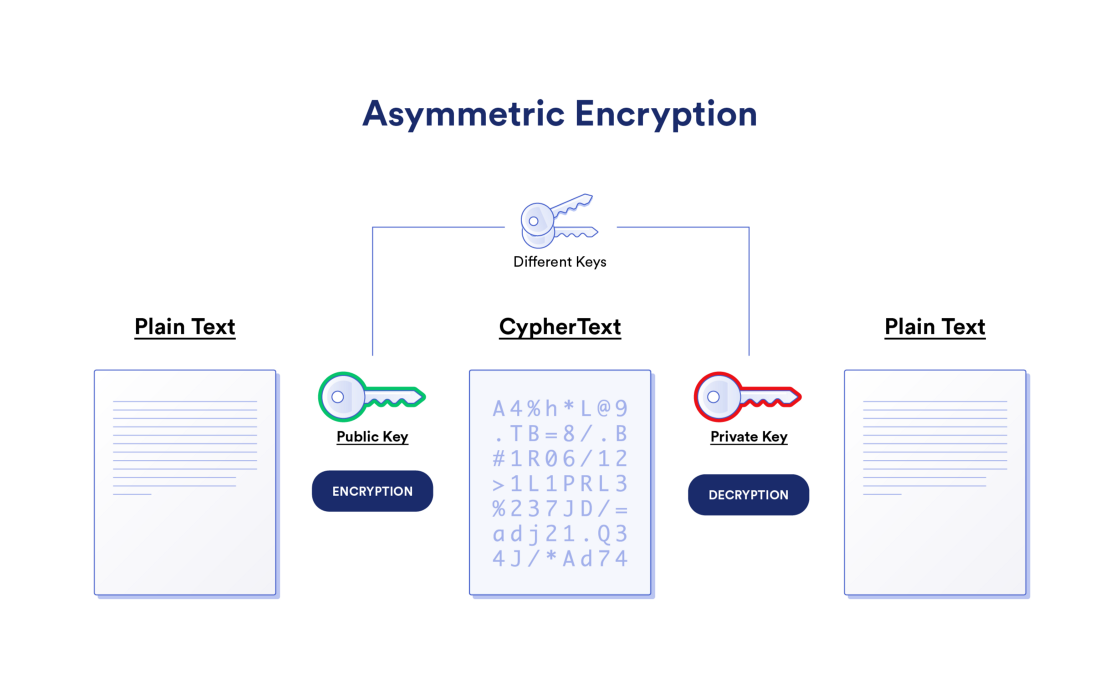
Наиболее популярным симметричным шифром является Advanced Encryption System (AES). AES предлагает ключи длиной 128, 192 и 256 бит — существенное улучшение по сравнению с 56-битными ключами, используемыми в предыдущем и ныне небезопасном стандарте шифрования данных (DES). Для сравнения, 56-битный ключ имеет 256, или 72 квадриллиона, возможных ключей, которые можно взломать перебором менее чем за 24 часа. В противном случае, для того чтобы перебрать 2 в степени 128 возможных ключей, даже при объединении всех компьютеров мира, потребуется триллионы и триллионы лет.

Симметричное шифрование использует один и тот же секретный ключ для шифрования и расшифровки сообщений.

# Криптография с открытым ключом(Асимметричное шифрование)

Асимметричное шифрование (оно же криптография с открытым ключом) дает каждому пользователю пару открытого и закрытого ключей. Открытый ключ виден всем, в то время как закрытый ключ известен только его владельцу. Пользователи могут шифровать сообщения с помощью своего закрытого ключа, который может расшифровать любой человек с открытым ключом. Это известно как цифровая подпись, поскольку она доказывает знание секрета без раскрытия самого секрета (т.е. у пользователя есть закрытый ключ к адресу открытого ключа). Пользователи также могут шифровать сообщения с помощью чужого открытого ключа, который может расшифровать только человек с закрытым ключом (т.е. отправка конфиденциальной информации).

Наиболее популярными алгоритмами асимметричного шифрования являются RSA (названный в честь его изобретателей Рамиса, Шамира и Адлемана), ECC (Elliptic Curve Cryptography), Diffie Hellman (популярный протокол обмена ключами) и DSS (Digital Signature Standard). Некоторые алгоритмы асимметричного шифрования устойчивы к квантованию, а другие — нет, и в будущем их, возможно, придется модернизировать или отказаться от них.

Асимметричное шифрование требует, чтобы у каждого пользователя была пара открытый/закрытый ключ.

**Криптография в блокчейн**

Блокчейн использует две основные формы криптографии: криптографию с открытым ключом и хэш-функции. Однако все чаще используются и другие криптографические методы для обеспечения масштабирования, конфиденциальности и внешних подключений к блокчейну. Ниже перечислены некоторые способы использования криптографических функций в блокчейн.

# Обработка транзакции

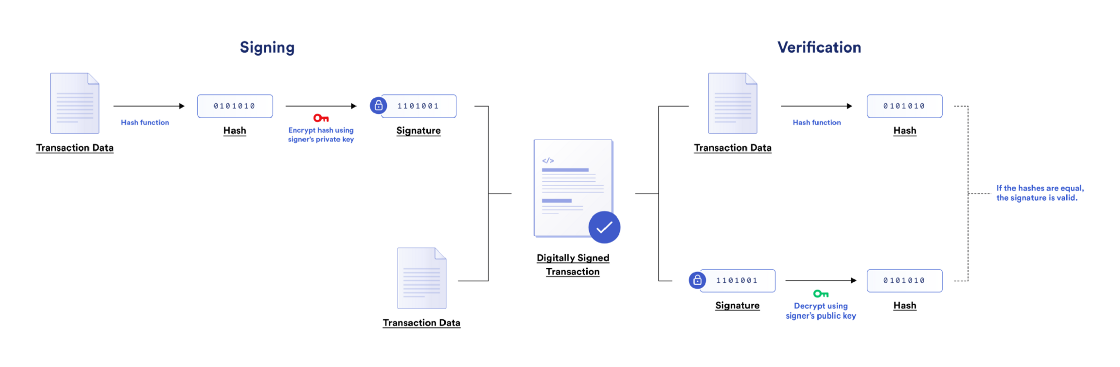
**Аутентификация и верификация транзакций**

Каждый пользователь блокчейна должен иметь пару открытый/закрытый ключ и адрес блокчейна, чтобы отправлять транзакции в сети. Закрытый ключ используется для генерации открытого ключа, а открытый ключ используется для генерации адреса блокчейна — как правило, это хэш открытого ключа с последними 20 байтами, добавленными к префиксу, например 0x. Обратите внимание, что многие блокчейн-кошельки и традиционные биржи абстрагируются от создания пары открытый/закрытый ключ и взаимодействия пользователя с ней.

Адрес блокчейна похож на реальное имя, связанное с банковским счетом пользователя (например, Pay to the Order…), только в блокчейне это псевдоанонимная строка цифр и букв. Адрес блокчейна — это место, где пользователь хранит средства и развертывает смарт-контракты. Закрытый ключ сродни пин-коду, который пользователь должен ввести, чтобы совершить действия со своим счетом, например, перевести средства или внести изменения в смарт-контракты. Открытый ключ похож на номер банковского счета пользователя и используется для проверки подписей закрытого ключа.

При отправке транзакций пользователь посылает в сеть сообщение со своего адреса в блокчейне, содержащее данные о транзакции и цифровую подпись. Данные транзакции описывают действие, которое пользователь хочет совершить в сети, а цифровая подпись подтверждает подлинность этого действия. Цифровая подпись генерируется из двух входных данных: хэша данных транзакции пользователя и его закрытого ключа. Затем цифровая подпись присоединяется к данным транзакции, образуя транзакцию с цифровой подписью.

Майнеры/валидаторы и полные узлы, которые управляют блокчейном, запускают протокол проверки цифровой подписи, чтобы проверить действительность транзакции. Протокол проверки берет исходные данные транзакции и хэширует их. Он также расшифровывает цифровую подпись с помощью открытого ключа пользователя, чтобы получить хэш. Если эти два хэша совпадают, то транзакция считается действительной. Благодаря сочетанию хэширования и криптографии с открытым ключом для поддержки цифровых подписей блокчейн гарантирует, что только владелец закрытого ключа может получить доступ к средствам, хранящимся на соответствующем адресе блокчейна.

Блокчейн использует цифровые подписи для аутентификации и проверки транзакций пользователей.

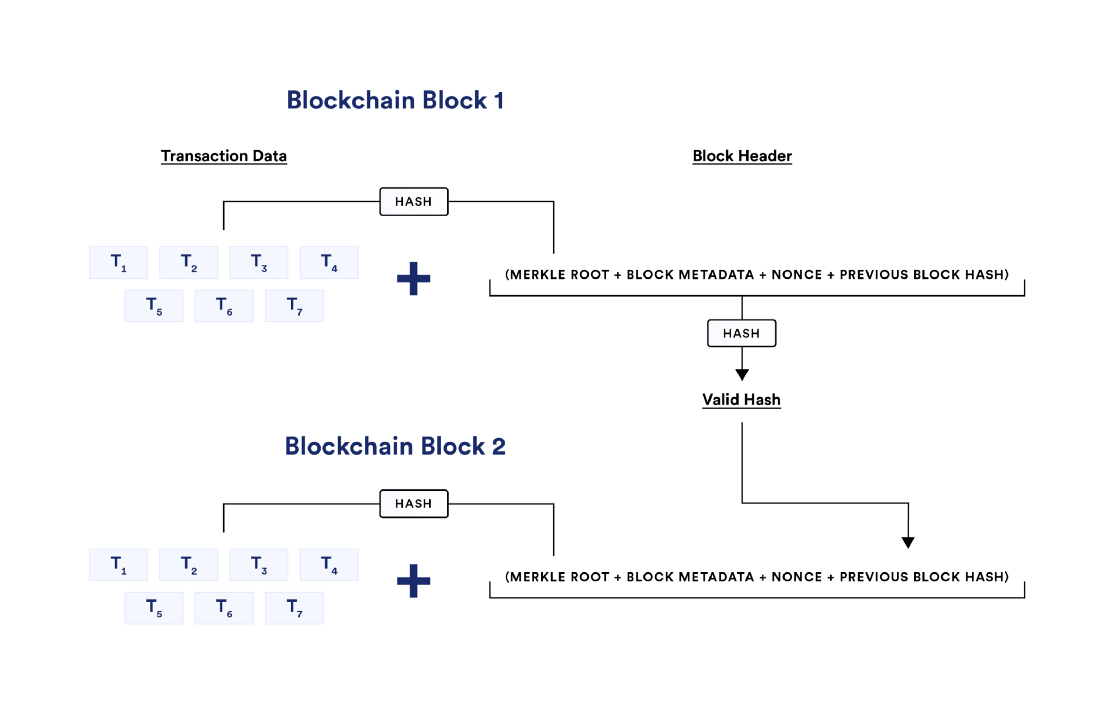
# Атака Сивиллы

**Производство блоков, устойчивость к атаке Сивиллы и финализация**

Производство блоков — это процесс, в ходе которого майнеры/валидаторы объединяют ожидающие транзакции в структуры данных, называемые блоками, и предлагают их в сети. Блок обычно состоит из списка всех транзакций, включенных в блок, и заголовка блока, содержащего метаданные блока. Чтобы создать блок, майнер/валидатор должен сгенерировать правильный хэш блока, иначе блок будет отклонен.

В блокчейнах Proof-of-Work (PoW) (например, в Bitcoin) проводится открытое соревнование между майнерами, где первый, кто сгенерирует достоверный хэш (т.е. хэш, начинающийся хотя бы с определенного количества нулей) методом перебора, будет выбран для предложения своего блока в реестр. Блокчейн PoW использует хэш-функции в производстве блоков для обеспечения устойчивости к атакам Сивиллы — защиты от того, что один субъект контролирует процесс производства блоков, подделывая альтернативные личности. Поскольку мощность хэширования — единственный способ для майнера PoW увеличить свои шансы стать автором блока, получение контроля над большей мощностью хэширования в сети сопровождается пропорциональными финансовыми затратами в виде выполнения большего количества вычислений. Это не только предотвращает атаки типа “отказ в обслуживании”, но и требует от майнеров “работы”, чтобы даже получить шанс на вознаграждение.

Блокчейн Proof-of-Stake (PoS), такой как Ethereum 2.0, также генерирует хэши при производстве блоков, но этот процесс специально разработан таким образом, чтобы быть легким, поскольку нет конкуренции между валидаторами. Вместо этого валидаторы PoS обычно выбираются в качестве авторов блоков случайным образом, часто на основе веса их доли. Блокчейн PoS создает устойчивость к атаке Сивиллы, требуя от валидаторов внесения криптовалюты (т.е. ставки) для участия в производстве блоков. Таким образом, валидаторы PoS должны вкладывать финансовые ресурсы, чтобы увеличить свои шансы быть выбранными в качестве автора блока. Зачастую их доля подлежит сокращению (т.е. конфискации), если они нарушают определенные правила протокола, например, включают в свой блок недействительные транзакции или подписывают два блока на одной высоте.

Блоки состоят из данных транзакции, корня Меркла, других метаданных блока, действительного ключа (nonce) и хэша предыдущего блока.

Как правило, правильный хэш блока должен иметь следующие исходные данные:

* Корень Меркла — хэш всех включенных в блок транзакций, содержащийся в структуре данных дерева Меркла.
* Nonce (это сокращение от number used once «число, используемое один раз») — произвольное число/буквенное сочетание, которое создает действительный хэш, удовлетворяющий текущей цели сложности. Блокчейны PoW периодически регулируют сложность угадывания Nonce для достижения определенной частоты блоков (например, каждые десять минут), в то время как в сетях PoS Nonce относительно легко генерируются.
* Дополнительные метаданные блока — в разных блокчейнах они разные, но могут включать в себя следующее: текущую версию программного обеспечения блокчейна, метку времени, целевую сложность майнинга, корень состояния всей цепи или номер текущего блока.
* Хэш предыдущего блока — действительный хэш блока, который был проверен ранее.

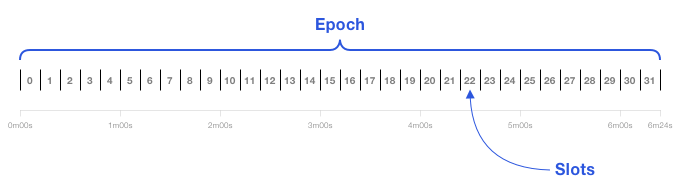
Блоки включают хэш-значение предыдущего блока, чтобы криптографически связать их вместе в цепочку, сохраняя хронологический порядок реестра. Именно поэтому блокчейн считается неизменяемым, так как для отмены ранее подтвержденных блоков, называемых реорганизацией блоков или просто реорганизацией, потребовалось бы много вычислительной мощности и/или финансовых рисков. Даже если изменяется только одна транзакция в блоке, меняется весь хэш этого блока, и, таким образом, другие узлы могут легко заметить его. Обратите внимание, что не все перерегистрации являются злонамеренными; например, перерегистрации 1 блока на вершине цепочки более распространены из-за асинхронных сетевых условий. Однако глубокие перерегистрации могут быть более спорными, и их значительно сложнее осуществить, чем дальше назад они происходят.

В блокчейне PoW майнерам приходится заново генерировать достоверные хэши для всех заменяемых блоков, чтобы провести атаку на перестройку, а в это время другие майнеры тратят вычислительные ресурсы на добавление новых блоков к последнему блоку. Именно здесь вступает в игру логика консенсуса Накамото, согласно которой “самая длинная цепочка с наибольшим количеством работы является действительной”, поскольку она предоставляет майнерам простой способ определения действительной версии реестра.

Именно благодаря этой логике блокчейн PoW имеет вероятностную окончательность, так как чем дальше назад пытаются внести изменения, тем меньше вероятность того, что атака будет успешной. Из вероятностной окончательности вытекает понятие атаки 51% — майнерам требуется 51% или более мощности хэширования, чтобы провести более глубокую атаку на реорганизацию или цензуру блоков других майнеров. Вероятностная окончательность также является причиной того, что централизованные криптовалютные биржи обычно разрешают пользователям тратить внесенные средства только после того, как будет добыто определенное количество последующих блоков поверх блока, включающего их транзакцию (например, обычно 6 блоков в Bitcoin, 32 блока в Ethereum). Это помогает предотвратить атаки двойной траты — когда одна и та же единица валюты обманным путем тратится более одного раза.

В сетях PoS всем или части валидаторов, не производящих в данный момент блоки, часто поручается подтвердить достоверность новых блоков с помощью механизма голосования. Валидатор, пытающийся провести перегруппировку, должен подвергнуть риску свою финансовую долю, причем штраф за нарушение децентрализованного консенсуса (обычно >2/3 валидаторов) увеличивается тем больше, чем глубже атака. Эта обобщенная модель PoS придает криптоэкономические свойства таким алгоритмам консенсуса, как Practical Byzantine Fault Tolerance, Tendermint, Casper и HotStuff.

Некоторые блокчейны PoS также имеют ограничение на то, как далеко назад может быть изменена главная книга блокчейна, по существу устанавливая контрольную точку, в которой каждая транзакция до нее имеет явную окончательность. Например, при объединении цепочки маяков PoS в текущую сеть Ethereum производство и проверка блоков будут разделены на эпохи, причем каждая эпоха имеет 32 слота длиной 12 секунд каждый. В течение каждой эпохи все валидаторы случайным образом делятся на комитеты размером не менее 128, при этом валидаторы в каждую эпоху перемешиваются. Во время каждого слота валидатор предлагает блок, а валидаторы из одного или нескольких комитетов подтверждают этот блок. Это сделано так, чтобы валидаторы подтверждали один предложенный блок за эпоху.



Производство и проверка блоков Ethereum 2.0 будут разбиты на эпохи с 32 слотами, где блок может быть предложен и засвидетельствован в каждом слоте.

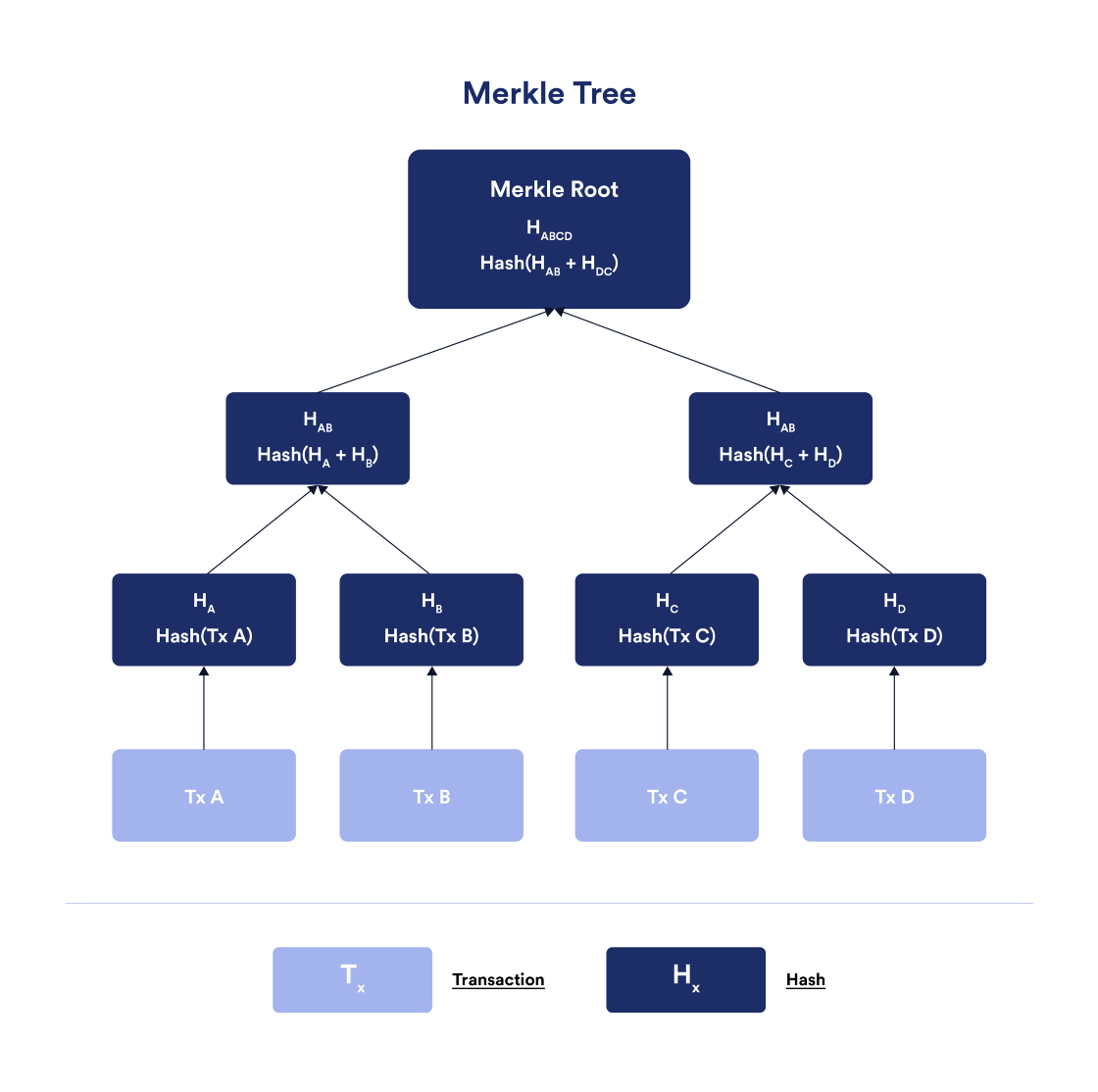
В конце каждой эпохи блоки в рамках предыдущей эпохи считаются обоснованными, если их обоснованность подтверждают не менее двух третей всех валидаторов (т.е. супербольшинство). Если две предыдущие эпохи подряд оправданы, то первая эпоха становится завершенной. При идеальных условиях сети и участии валидаторов завершение транзакции происходит в среднем около 14 минут. После того как эпоха завершена, правила протокола не позволяют отменить ее без внешнего социального консенсуса.

**Хранение данных**

Блокчейн — это реестр, содержащий все транзакции, которые когда-либо происходили в сети блокчейн в хронологическом порядке (хотя некоторые блокчейны изучают возможность обрезки исторических данных после определенной контрольной точки). Чем дольше работает блокчейн, тем больше становится реестр и тем дороже узлам обходится ее хранение и синхронизация. Чрезмерные требования к хранению и пропускной способности ставят под угрозу децентрализацию сети блокчейн, поскольку увеличивают аппаратные требования к работе всего узла, что потенциально позволяет небольшой группе субъектов нарушить работу сети.

Для эффективного и безопасного кодирования данных реестра блокчейн использует структуры данных, называемые деревьями Меркла. В дереве Меркла каждая транзакция пользователя хэшируется, затем сопоставляется с другой хэшированной транзакцией и снова хэшируется. Хеши постоянно сопоставляются и хешируются вверх по дереву, пока не образуется единый хеш всех хешей, называемый корнем Меркла.

Биткойн использует дерево Меркла для транзакций на основе модели “Неизрасходованный выход транзакции” (UTXO), а Ethereum использует деревья Меркла для транзакций, состояния и квитанций (например, журналов и событий) в так называемой модели учётной записи с обобщенной поддержкой смарт-контрактов.

Деревья Меркла — это эффективный способ хранения данных о транзакциях в блокчейн.

Деревья Меркла полезны, поскольку занимают меньше дискового пространства по сравнению с другими структурами данных и способствуют эффективной проверке целостности данных и включению данных в распределённый реестр. Кроме того, поскольку корни Меркла включаются в заголовки блоков, они позволяют легким клиентам, подключенным к доверенному полному узлу, быстро и безопасно проверить, что конкретная транзакция была включена в блок, не загружая весь блокчейн.

**Другие криптографические техники, используемые в блокчейн**

Некоторые из других криптографических примитивов, используемых в блокчейн, включают:

* Доказательства нулевого знания (ZKPs) — метод, позволяющий пользователю (проверяющему) доказать другой стороне (проверяемому), что он обладает знаниями о конкретной части информации, не раскрывая фактической информации, лежащей в основе. Например, в блокчейне Zcash полные узлы могут доказать, что транзакции действительны, не зная ни отправителя, ни получателя, ни суммы транзакции.
* Доверенные среды выполнения (TEEs) — использование доверенного оборудования, такого как Intel SGX, для выполнения конфиденциальных вычислений, где целостность вычислений может быть доказана с помощью криптографических сертификатов. В качестве примера можно привести блокчейн Oasis, где все узлы-валидаторы используют доверенные среды выполнения для обеспечения конфиденциального и проверяемого выполнения смарт-контрактов.
* Пороговые схемы подписи (TSS) — форма распределенной генерации и подписания ключей, используемая для аутентификации вычислений, выполняемых децентрализованной сетью, с помощью одной криптографической подписи, для подписания которой требуется только пороговый набор участников. Например, транзакция, которую должны подписать только 10 из 15 узлов, чтобы она считалась действительной.

# Блокчейн консенсус

**Истина генерируется на основе децентрализованного консенсуса**

Теория игр — это математический подход к стратегии, основанный на предсказании действий рациональных участников в определенном соревновании. В рамках теории игр разработка механизмов — это искусство использования стимулов для достижения желаемых результатов в рамках стратегических взаимодействий.

Блокчейн использует механизм проектирования для стимулирования децентрализованной сети рациональных, незаинтересованных узлов к поддержанию точному, неизменному, всегда доступному, устойчивому к цензуре реестру. Этот желаемый результат иногда называют достижением честного большинства — большинство узлов в сети блокчейн участвуют честно, что позволяет пользователям последовательно доверять консенсусу сети.

**Структура игры**

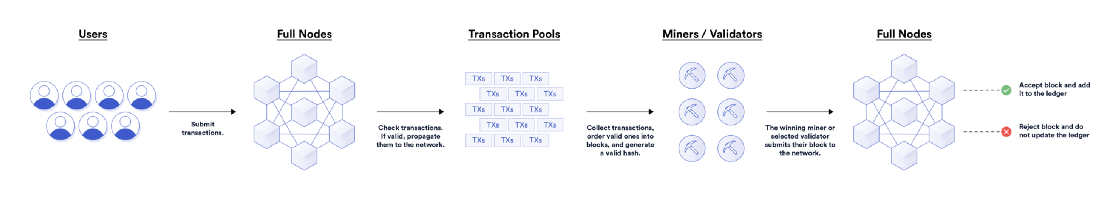
Блокчейн — это прозрачный реестр с открытым исходным кодом, то есть все участники могут просматривать всю историю реестра и проверять, как функционирует код. Участники сети блокчейн делятся на пять основных групп:

Пользователи совершают транзакции в сети либо по личным причинам, либо для размещения приложений. В блокчейн-цепочках без разрешений любому человеку разрешается отправлять транзакции в сеть в любое время.

Майнеры/валидаторы расширяют реестр, создавая новые блоки из транзакций пользователей. В некоторых блокчейнах майнером/валидатором может стать любой желающий, в то время как в других блокчейнах количество участников ограничено. Некоторые компенсируют это ограничение, позволяя пользователям голосовать или делегировать долю валидаторам.

Полные узлы выполняют несколько функций в сетях блокчейн. Во-первых, полные узлы предоставляют конечные точки RPC, которые позволяют пользователям читать из блокчейна и писать в него. Конечные точки RPC могут быть созданы на самостоятельно размещенных узлах или доступны через сторонних поставщиков (например, Infura). При записи данных в блокчейн (т.е. отправке транзакций) полные узлы либо передают их в публичный мемпул, либо хранят в частных пулах транзакций. Это связано с тем, что в одноранговой децентрализованной сети не существует единого пула транзакций, а каждый полный узел имеет свой собственный пул транзакций.

Полные узлы также проверяют действительность транзакций пользователей перед передачей их в сеть или перед распространением транзакций других узлов в сети. Кроме того, полные узлы проверяют новые блоки, предложенные майнерами/валидаторами, что служит способом самопроверки блокчейна. Если они считают блок действительным, они добавляют его в свою копию реестра. Если они не считают его действительным, они отклоняют блок и не обновляют свою книгу. Консенсус среди децентрализованной сети полных узлов представляет собой текущее состояние реестра — совокупность всех адресов блокчейна, их балансов, развернутых смарт-контрактов и связанных с ними хранилищ. Любой человек может управлять полным узлом, хотя требования к аппаратному обеспечению в разных сетях различны. Майнеры/валидаторы часто участвуют в работе полных узлов.



Блокчейн разделяет роли майнеров/валидаторов и полноценных узлов для повышения безопасности сети.

Поставщики услуг — это внешние организации, которые предоставляют услуги блокчейн или создают услуги на основе содержимого блокчейн. К ним относятся оракулы, протоколы индексирования, централизованные биржи, легкие клиенты, архивные узлы, исследователи блоков и многие другие. Эти организации обычно имеют бизнес-модели, которые требуют взаимодействия с блокчейном. Например, централизованные биржи обеспечивают переход между криптовалютами и традиционной финансовой системой, легкие клиенты позволяют пользователям проверять информацию, отправленную с полных узлов, без необходимости иметь полную копию реестра, а оракулы предоставляют ключевые внешние ресурсы для приложений смарт-контрактов.

MEV-боты — это субъекты, которые стремятся повлиять на то, как упорядочиваются транзакции во время добычи блоков, в частности майнеры и разработчики MEV. Извлекаемая майнерами стоимость (MEV), также называемая максимальной извлекаемой стоимостью, основана на способности майнеров/валидаторов выбирать, какие транзакции будут включены в блок и как эти транзакции будут упорядочены. Затем они могут использовать эту привилегию в своих интересах для извлечения стоимости, например, опережая или атакуя пользователей и используя возможности ликвидации и арбитража. MEV-боты обычно работают через частные пулы транзакций и офф-чейн аукционы в блокчейне, хотя могут действовать и самостоятельно.

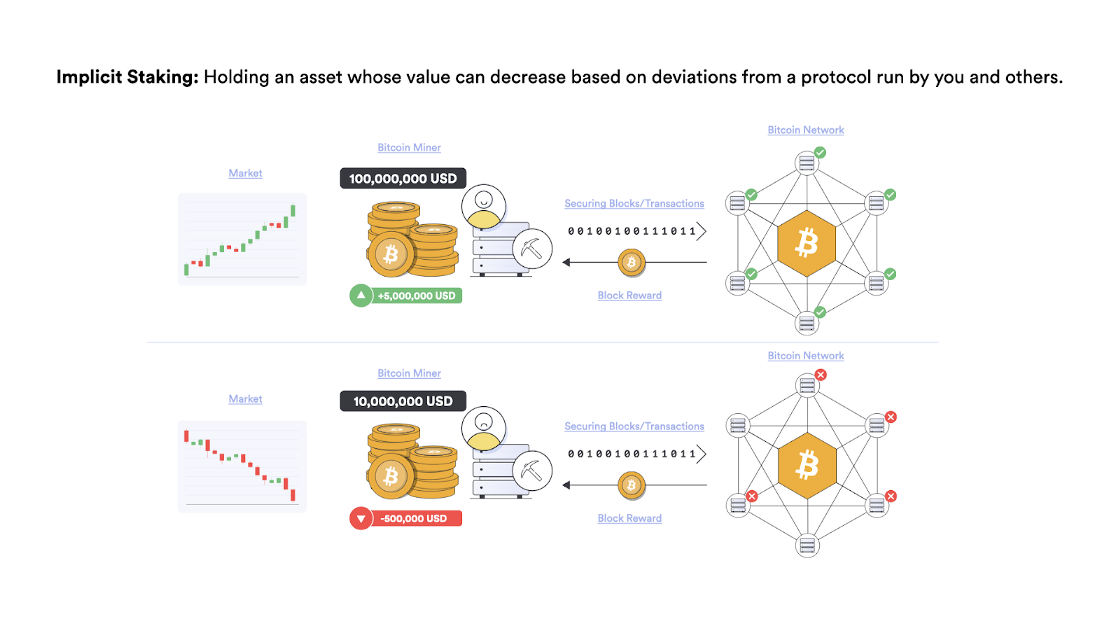
**Игровые стимулы**

Стимулы делятся на две большие категории: неявные и явные. Явные стимулы — это прямые вознаграждения или наказания за действия, совершенные в игре, например, обязательный платеж за доступ к услуге или жестко закодированный штраф за нарушение правил протокола. Неявные стимулы — это косвенные вознаграждения и наказания, вытекающие из игры, например, упущенные участниками возможности получения будущих доходов или затраты труда без гарантированной компенсации.

Наиболее очевидными стимулами в блокчейн являются вознаграждение за блок и плата за транзакции, выплачиваемая майнерам/валидаторам за создание одобренных блоков. Вознаграждение за блок обычно стандартизировано по количеству, в то время как плата за транзакции может колебаться в большую или меньшую сторону в зависимости от текущего спроса на ограниченное пространство блока. В процессе производства блоков также существуют стимулы для заказа транзакций определенным образом, которыми MEV-боты пытаются воспользоваться для получения финансовой выгоды.

Блокчейн также использует финансовые санкции через механизмы, устойчивые к атаке Сивиллы, такие как PoW и PoS; т.е. майнеры/валидаторы должны сделать вычислительную или финансовую ставку, чтобы получить шанс заработать вознаграждение, которое может быть потрачено впустую или сокращено, если они идут против консенсуса сети. Еще одним преимуществом требования к производителям блоков делать вычислительную или финансовую ставку является то, что это стимулирует децентрализацию. В частности, потому, что майнеру/валидатору становится все дороже получать больший контроль над хэш-мощностью сети или долей.

Блокчейн также платит майнерам/валидаторам в их собственной криптовалюте. Это создает неявный стимул для майнеров/валидаторов честно участвовать в работе сети, поскольку безопасная и надежная сеть, скорее всего, привлечет больше пользователей. Большее количество пользователей ведет к увеличению комиссий за транзакции, а также к потенциально более высокой цене на зарабатываемую ими криптовалюту. Более высокая цена криптовалюты может означать больший доход от каждого блока и увеличение личных средств.

Биткойн имеет форму неявного стейкинга, когда майнеры получают вознаграждение в виде актива (BTC), который сохраняет свою ценность и покрывает их расходы только в том случае, если они поддерживают безопасность сети.

Хотя явного стимула для запуска полного узла в протоколе обычно нет, существует множество неявных стимулов для этого. Для начала, полные узлы необходимы для работы сети, поэтому, как минимум, майнеры должны их запускать. Пользователи, приложения и поставщики услуг также должны запускать полные узлы или иметь к ним доступ, чтобы отправлять и проверять статус ожидающих транзакций. Таким образом, для поддержки экосистемы существует несколько моделей бесплатных узлов и узлов как услуги.

Помимо финансовых стимулов, полные узлы критически важны для целостности реестра, поскольку отсутствие децентрализации дает меньшей группе участников контроль над сетью. Скомпрометированный реестр повлияет на поставщиков услуг и децентрализованные приложения, бизнес-модели которых зависят исключительно от предположения о честном большинстве в блокчейн.

Децентрализованная сеть с полным узлом также помогает отделить генерацию блока от его верификации, обеспечивая подотчетность майнеров/валидаторов за счет снижения их способности произвольно изменять правила протокола. Кроме того, организации, управляющие собственным полным узлом, имеют наибольшую степень устойчивости к цензуре и гарантии безопасности, поскольку им не нужно доверять третьим лицам для чтения или записи в блокчейн. Эти неявные стимулы побуждают пользователей и ключевых экономических субъектов запускать полные узлы.

**Результат игры**

Внедрение этих стимулов в рамках заявленной структуры игры приводит к желаемым результатам блокчейн:

* Точность — децентрализация блокчейн, неявные/явные затраты, стоящие на кону, и простота обнаружения недействительных транзакций стимулируют майнеров/валидаторов и полные узлы к достижению честного консенсуса относительно действительности транзакций.
* Неизменность — финансовые затраты и риск при попытке изменить ранее одобренный блок делают это нежелательным, особенно когда поверх целевого блока создаются новые блоки.
* Доступность — достаточное вознаграждение помогает майнерам/валидаторам постоянно генерировать блоки, а наличие значительной суммы, поставленной на карту, стимулирует создание полноценных сетей узлов, которые расширяются за пределы майнеров/валидаторов.
* Устойчивость к цензуре — механизмы защиты от сибилов, финансовые вознаграждения и возможность беспрепятственного участия делают невероятно дорогостоящими попытки любой централизованной структуры цензурировать транзакции, особенно в течение длительного периода времени.

Благодаря этим желаемым свойствам у пользователей появляется больше стимулов для взаимодействия с сетью блокчейн. Не только использование сети может возрасти, но и пользователям станет удобнее хранить на блокчейне большие суммы ценностей и использовать свои активы на сети в приложениях смарт-контрактов.

Однако следует отметить, что, хотя блокчейн в целом устойчив к цензуре и точен, упорядочение транзакций по времени отправки или уплаченной комиссии не гарантируется из-за MEV. Именно поэтому Chainlink разрабатывает Fair Sequencing Services (FSS) — сервис оракула для децентрализованного упорядочивания транзакций для блокчейн, сетей второго уровня и приложений на основе времени их получения.

Следует также отметить, что блокчейн в конечном итоге является системой, управляемой людьми для обслуживания людей, поэтому если все придут к социальному консенсусу (т.е. офф-чейн соглашению между участниками), что что-то в блокчейне необходимо изменить, то это может быть сделано. Самым ярким примером социального консенсуса, способствующего изменениям, стал хард-форк Ethereum — обновление программного обеспечения, несовместимое с предыдущими версиями, — который восстановил украденные средства после взлома DAO в 2016 году. Общественный консенсус также может иметь обратную сторону, когда участники сообщества препятствуют внедрению предложенных изменений, как, например, отказ от Segwit2x для сети Bitcoin и ProgPoW для сети Ethereum.

С учетом вышесказанного, блокчейн, вероятно, является наиболее эффективной сетью для защиты от нежелательных атак и изменений, которые идут вразрез с большинством общественного консенсуса, особенно с помощью криптографических и экономических механизмов.

**Мир, основанный на криптографической истине**

В конечном счете, криптографическая истина привносит детерминизм, точность и прозрачность в вычисления и ведение записей. Зная, что код приложения будет выполнен так, как задумано, что исторические записи были избыточно проверены и останутся защищенными от взлома, социальные и экономические отношения могут быть основаны на более глубоком уровне истины, чем когда-либо прежде. Наличие прочного фундамента правды ведет к росту экономической активности и укреплению социальной гармонии — мира, который все хотят видеть воплощенным в жизнь. Именно поэтому все мы должны создать и внедрить технологии блокчейна и блокчейн оракула, которые устанавливают криптографическую истину в основных сферах нашего коллективного общества.

# Одноранговые сети (Peer-to-Peer)

**Почему именно «одноранговые»?**

Если рассматривать ситуацию с точки зрения информационных технологий, то одноранговые или пиринговые (от peer-to-peer) сети – это такие сети, в которых отельные элементы (узлы) обмениваются между собой файлами и хранят один и тот же набор данных. Узлы равны по мощности и выполняют одинаковые по смыслу задачи.

*С финансовой точки зрения, одноранговые сети – финансовые платформы, которые позволяют осуществлять финансовые операции купли-продажи без посредников. В некоторых ситуациях, аналогичным образом организуются и процедуры получения и выдачи кредитов.*

В любом случае, о первых эффективных одноранговых сетях начали говорить примерно в девяностых годах прошлого века, когда появились программы для эффективного обмена файлами. Однако основной интерес к ним вспыхнул после появления криптовалютных сетей, основанных на классической P2P-архитектуре. Впрочем, теперь такие сети используются не только в [криптоэкономике](https://exbase.io/ru/wiki/vvedenie-v-kriptojekonomiku), но и при создании поисковых систем, стриминг-платформ, разнообразных онлайн-рынков и в рамках межпланетной файловой системы IPFS.

**Как это работает?**

*Итак*. У нас есть большое количество связанных друг с другом компьютеров. На каждом из них хранится копия всех файлов, содержащихся в сети. Это позволяет одновременно выполнять и роль клиента, и роль сервера. Кроме того, узлы равны в своих правах, так что ни у кого нет преимущества перед остальными, а решения о глобальных изменениях принимаются коллегиально.

Эта ситуация позволяет каждому узлу одновременно закачивать новую информацию и раздавать уже хранящуюся. Процесс этого постоянен и непрерывен, поскольку все узлы обязаны реагировать на любое изменение содержимого сети.

Независимое хранение информации на разных источниках делает всю систему более устойчивой к внешним воздействиям и взломам. Кроме того, в сетях Р2Р нет единой точки отказа, в отличие от централизованных систем.

**Классификация**

Выделяют три основных типа одноранговых сетей.

* **Неструктурированные**. Узлы случайным образом контактируют друг с другом, что обеспечивает высокую активность системы даже при значительной текучке узлов. Относительно просты в построении, однако требуют больших мощностей при работе. Дело в том, что поисковые или любые другие запросы отправляются на максимально возможное число машин одновременно, так что сеть перегружается «пустыми» информационными запросами, которые могут помешать прохождению отзывов.
* **Структурированные**. Узлы объединены в строгую систему со своей архитектурой. В такой системе активно используется поиск по хэш-функциям, что значительно снижает общую интенсивность информационного потока. Однако такие системы в некоторой степени уже являются централизованными, поэтому куда более требовательны к обслуживанию и установке. Да и при временном выпадении большой группы узлов, вся работа системы нарушается.
* **Гибридные**. Комбинация предыдущих вариантов. Например, наличие центрального сервера, упрощающего процесс обмена между отдельными узлами. Как правило, подобные сети отличаются высокой производительностью и устойчивостью.

**Р2Р и блокчейн**

Когда Сатоши Накамото создавал сеть Биткоин, он сформулировал её как «одноранговая платёжная система электронных денежных средств». Это обеспечивалось благодаря работе новой технологии – блокчейн.

Технология позволяла обмениваться цифровой валютой с участниками по всему миру без использования услуг посредников и центральных серверов. Кроме того, любой желающий мог присоединиться к этому процессу.

Роль банков, фиксирующих и гарантирующих подлинность финансовых операций, взял на себя цифровой регистр, в котором фиксируется вся активность и к которому может обратиться любой желающий. Проще говоря, каждый узел, подключенный к сети, хранит всю информацию, содержащуюся в ней, и регулярно связывается с другими узлами, чтобы гарантировать достоверность и актуальность хранимой информации.

Но несмотря на то, что сеть является одноранговой, разные узлы могут брать на себя разные функции. Так, например, существуют так называемые «полные ноды», основная задача которых - проверка транзакций в системе на предмет соответствия их действующим алгоритмам консенсуса. А есть и другие узлы – майнеры, основная задача которых – генерация новых блоков хранения информации.

**Преимущества**

* Высокая устойчивость к DoS-атакам, поскольку информация не хранится в одном месте, а пропускная способность сети позволяет одновременно обрабатывать множество запросов.
* Высокая устойчивость к изменению уже внесённой информации. Чтобы переписать данные на всех машинах сети, нужно мощность, превышающая половину общей мощности системы. Это называется «Атака 51 процента». Довольно редкое явление, особенно в больших сетях.
* Высокая устойчивость к внутренним ошибкам и противоречивым сигналам. Сети Р2Р демонстрируют высокую «византийскую отказоустойчивость».
* Устойчивость к внешней цензуре. Криптовалютные кошельки, например, не могут быть заморожены решением судов и правительств, в отличие от счетов в банках.

**Недостатки**

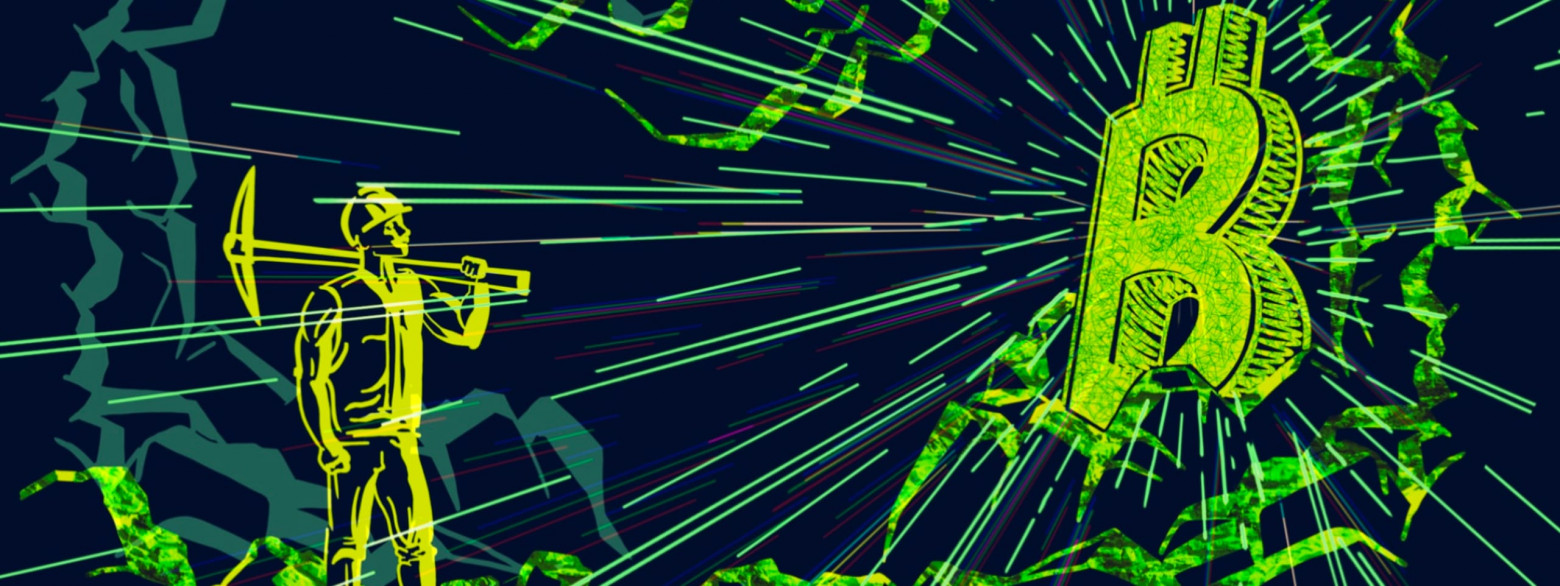
* Чем больше сеть, тем больше вычислительной работы нужно проделать, чтобы обеспечить актуальность хранимой информации. За счёт этого, замедляется общая скорость работы. Эта проблема известна как «проблема масштабируемости». И очень немногие одноранговые сети нашли более-менее приемлемые способы её решения. Примерами этого могут служить Lightning Network, Ethereum Plasma и протокол Mimblewimble.
* Возможна ситуация «разделения» цепочки информации на две – ситуация «хардфорка». В таком случае, оба новых разветвления оказываются уязвимыми перед атакой повторного воспроизведения (достоверная транзакция с одной цепочки дублируется на второй, за счёт чего – снимается в 2 раза больше денег). А если учесть, что подобные хардфорки случаются регулярно, то приходится дополнительно обеспечивать защиту от них.
* Невозможность исправления информации может быть и минусом. Изъять, например, компрометирующие данные из такой сети – крайне сложно. Как и цифровые копии, связанные с нарушением авторских прав.

**Вывод**

Одноранговая архитектура заметно улучшила эффективность хранения информации, сделав обмен более прозрачным, устойчивым и быстрым. Причём не только в рамках криптовалютных сетей, но и при обмене информацией иного рода – от файлов пиринговых сетей, типа torrent, до информации, связанной с крупными торговыми операциями или обработкой больших массивов цифровых данных.

# Proof of Work

Какой консенсус лучше для блокчейна, proof-of-work или proof-of-stake?



**Что такое proof-of-work?**

Proof-of-work (**PoW**) — децентрализованный алгоритм консенсуса, впервые представленный Bitcoin (BTC).

Сеть Bitcoin требует, чтобы ее участники вкладывали в нее вычислительные мощности (например, GPU) для решения математических задач, сгенерированных произвольным образом. Это требуется для защиты сети от единоличного контроля и манипуляций.

Каждая транзакция в сети валидируется перед добавлением в блокчейн. Затем каждый блок валидируется майнерами, получающими вознаграждение в токенах BTC за вложенные вычислительные мощности. Поэтому консенсус и называется proof-of-work — «доказательство выполнения работы».

Этот алгоритм уже проверен временем, с его помощью в сети Bitcoin успешно про валидированы миллиарды транзакций. Поддерживая достоверность и надежность, proof-of-work доказал свою ценность как самый защищенный и децентрализованный алгоритм консенсуса.

**Что такое proof-of-stake?**

Алгоритм консенсуса proof-of-stake (**PoS**) используется блокчейн-сетями как альтернатива алгоритму PoW. В этом алгоритме владельцы криптовалюты *лидируют* транзакции блоков исходя из принадлежащего им числа монет (токенов). Поэтому консенсус называется proof-of-stake — «доказательство доли владения».

Валидаторы здесь выбираются случайным образом. Чтобы иметь возможность стать валидатором, нужно иметь на своем балансе определенное количество токенов, с которыми работает блокчейн-сеть.

Существует много разновидностей алгоритма PoS, например, delegated-proof-of-stake (PoS — «делегированное доказательство доли владения»). Все эти варианты применяются в различных блокчейн-сетях, но в основном работают по схожему принципу.

Когда в сети появляется готовый к обработке блок транзакций, протокол криптовалюты выбирает участника сети для валидации этого блока. Валидатор проверяет точность транзакций в блоке, и после этой проверки блок добавляется в блокчейн. За это валидатор получает вознаграждение в виде токенов сети.

Если же валидатор одобрит блок с неточными данными, он будет оштрафован на некоторое количество токенов сети. Такая ситуация возможна, поскольку в PoS не используется решение криптографических задач с помощью вычислительных мощностей, как в PoW.

**Какой механизм консенсуса лучше и почему?**

И PoW, и PoS созданы, чтобы помогать нодам проверять все транзакции сети. Как только все ноды подтверждают валидность блока транзакций, он добавляется в блокчейн. Каждый алгоритм предлагает для этого свою последовательность действий.

В целом, proof-of-work намного лучше подходит для валидации транзакций, чем proof-of-stake, но здесь возникает вопрос затрат.

**Безопасность и подлинность данных**

**PoW** превосходит PoS с точки зрения безопасности и сохранения подлинности данных. Это связано с тем, что в PoW данные связаны с обоснованным выбором ролей в сети. При проверке каждой отдельно взятой транзакции это обеспечивает защиту от обмана системы. Так реализуется модель нулевого доверия, где 100% транзакций верифицированы и записаны участниками сети в публичный реестр.

Кроме того, высокая степень защиты PoW обусловлена тем, что сеть со временем становится все сложнее, и шанс ее взлома снижается. В конце концов, сеть становится невозможно взломать. Она мониторится участниками, которые материально заинтересованы в ее работе, поскольку вкладывают в нее свои вычислительные ресурсы. Это делает потенциальный взлом чрезвычайно дорогим.

**PoS** более уязвим для взлома и атак. Теоретически, если участник сети или группа участников получат контроль над 51% ее токенов, они смогут контролировать и изменять весь блокчейн. Эта атака известна как «атака 51%».

**Владение сетью**

Модель **PoW** требует значительных затрат на майнинг, что позволяет при ее использовании обеспечить более децентрализованную структуру. Биткоин здесь — отличный пример. Сеть биткоина полностью децентрализована. Ни один человек, организация или страна не контролируют её. Сетью владеют и управляют тысячи нод по всему миру, образуя децентрализованную и защищенную систему.

Инфраструктура на основе **PoS** более централизована. Участники сети, имеющие больше токенов (или средств на их покупку), получают все больший контроль над сетью с каждым новым полученным  токеном.

Это опасно, так как группа участников, получившая 51% токенов, может изменить блокчейн для получения личной выгоды. Разве подобные системы уже не создавали проблем? Откройте глаза — мы живем в подобной системе довольно давно и смотрите, куда это нас привело.

*Число известных форков биткоина действительно гораздо ниже, но к концу этого пункта автор, видимо, уже выходит за предмет обсуждения.*

**Распределение вознаграждений и равенство участников**

Согласно модели **PoW**, майнеры получают дивиденды за решение сложных математических задач — награду за блок и иногда комиссии за транзакции. Это стимулирует участников верным образом, поскольку ноды соревнуются за решение задачи для получения награды.

Получить награду становится все сложнее, поскольку решение каждой следующей задачи требует все больше вычислительной мощности. Это делает сеть более защищенной, а потенциальные атаки на нее — более затратными.

Ценность криптовалюты растет, соответственно, растет и награда участникам сети. Каждый майнер имеет равные шансы получить награду, что обеспечивает безопасность и устойчивость сети. Алгоритм стимулирует правильное поведение и предотвращает форки — альтернативные цепочки, которые могут возникнуть при обновлении протокола.

В модели **PoS** участники стремятся получить вознаграждение, только чтобы увеличить свой баланс и в будущем иметь еще большие шансы на вознаграждение. Это ведет к централизации сети, когда участники с бо́льшим балансом получают больший контроль над блокчейном. В блокчейнах, которые не мониторятся, это ведет к росту угроз безопасности и уязвимости даже для сравнительно недорогих атак.

*Этот довод справедлив и для PoW, где майнеры точно так же вкладывают деньги в увеличение мощностей своего майнинг-пула и тем самым делают всю сеть более централизованной.*

**Проверка временем**

Алгоритм **PoW** прошел проверку временем, и сеть Bitcoin — наглядное тому доказательство. За 13 лет эта сеть ни разу не была взломана и скомпрометирована. Это самая мощная сеть в мире, сохранившая подлинность данных, надежность и безопасность.

С другой стороны, модели **PoS** появились позднее и все еще находятся на ранних этапах развития как с технической точки зрения, так и в процессе принятия рынком. Многие сомневаются в моделях консенсуса на основе PoS, поскольку многие из них пока не успели полностью протестировать.

**Энергопотребление**

Избыточное энергопотребление сетей на консенсусе **PoW** обсуждают широко. Это негативно влияет на окружающую среду и приводит к дополнительным тратам. Да, это действительно так: сети на основе PoW потребляют гораздо больше энергии, чем на PoS. Это связано с тем, что сеть становится сложнее и требует все больше вычислительных мощностей для решения все более сложных математических задач. Такова цена функционирования хорошо защищенной сети.

Любая финансовая система, которая ставит безопасность во главу угла, потребляет много энергии. Фиатные валюты, к примеру, потребляют гораздо больше энергии, чем системы на основе консенсуса PoW. Привычная экономика опирается на бумажные деньги, их производство требует ресурсы и вносит большой вклад в загрязнение окружающей среды. Если вы посчитаете, сколько энергии потребляют банки, их офисы, хранилища, транспорт и другие элементы инфраструктуры, традиционная банковская система становится куда менее экологичной по сравнению с сетью Bitcoin.

Сеть, основанная на консенсусе PoW, не требует никаких физических ресурсов — лишь вычислительные мощности для поддержания блокчейна. Таким образом, хоть Bitcoin и потребляет много энергии, он гораздо более экологичен по сравнению с традиционными фиатными валютами. Это шаг вперед. Переезд финансовых систем в сеть Bitcoin не только сделает их более эффективными и защищенными, но и позволит эффективнее бороться с глобальным потеплением.

PoW — это отличная система, сама по себе поощряющая инновации в том числе и в сфере энергетики.

# Смарт-контракты Blockchain

**История смарт-контрактов**

Принцип интеллектуальных контрактов был описан американским криптографом и программистом Ником Сабо еще в 1996 году задолго до появления технологии blockchain. Согласно концепции Сабо, интеллектуальные контракты — это цифровые протоколы для передачи информации, которые используют математические алгоритмы для автоматического выполнения транзакции после выполнения установленных условий и полного контроля процесса. Это определение, которое опережало свое время более чем на десять лет, остается точным и по сей день. Однако в 1996 году эта концепция не могла быть реализована: в то время необходимые технологии не существовали, в частности, распределенная книга.

  
В 2008 году появился bitcoin, появилась первая криптовалюта, созданная на основе революционной технологии blockchain, которой ранее не хватало децентрализованной книги. Blockchain биткоина не позволяет устанавливать условия для совершения транзакции в новом блоке, поскольку он содержит только информацию о самой транзакции. Тем не менее появление технологии послужило толчком для разработки смарт-контрактов. Спустя пять лет блочная платформа Ethereum позволила использовать смарт-контракты на практике. Сегодня рынок предлагает множество платформ, которые позволяют использовать смарт-контракты, но Ethereum остается одним из самых распространенных.

**Как работают смарт-контракты?**

Как уже упоминалось выше, интеллектуальные контракты — это компьютерные протоколы или, проще говоря, компьютерный код.

Код используется для ввода всех условий договора, заключенного между сторонами сделки, в blockchain. Обязательства участников предоставляются в интеллектуальном контракте в форме «если- то» (например: «если Сторона А переводит деньги, тогда Сторона В, передает права на квартиру»). Могут быть два или более участников, и они могут быть отдельными лицами или организациями. Как только данные условия будут выполнены, смарт-контракт самостоятельно выполняет транзакцию и гарантирует, что соглашение будет соблюдаться.

  
Смарт-контракты позволяют обменять деньги, товары, недвижимость, ценные бумаги и другие активы. Контракт хранится и повторяются в децентрализованной книге, в которой информация не может быть сфальсифицирована или удалена. В то же время шифрование данных обеспечивает анонимность сторон соглашения. Важной особенностью интеллектуальных контрактов является то, что они могут работать только с активами, находящимися в их цифровой экосистеме. Как подключить виртуальный и реальный мир в настоящее время является одной из основных трудностей работы со смарт-контрактами. Это является причиной существования «оракулов», специальных программ, которые помогают компьютерным протоколам получать необходимую информацию из реального мира.

**Преимущества смарт-контрактов**



* **Скорость.**Обработка документов вручную занимает много времени и задерживает выполнение задач. Смарт- контракты предполагают автоматизированный процесс и в большинстве случаев не требуют личного участия, что экономит драгоценное время.
* **Независимость.**Смарт-контракты исключают возможность вмешательства третьих сторон. Гарантия на транзакцию — сама программа, которая, в отличие от посредников, не даст основания сомневаться в ее целостности.
* **Надежность.** Данные, записанные в blockchain, не могут быть изменены или уничтожены. Если одна сторона сделки не выполняет свои обязательства, другая сторона будет защищена условиями интеллектуального договора.
* **Нет ошибок**— Автоматическая система для выполнения транзакций и удаления человеческого фактора обеспечивает высокую точность при выполнении контрактов.
* **Сбережения.** Смарт-контракты могут обеспечить значительную экономию за счет устранения расходов для посредников и сокращения операционных расходов, а также возможность для сторон работать вместе на более выгодных условиях.

**Недостатки Smart Contracrs**

Несмотря на их перспективный потенциал, у умных контрактов также есть свои недостатки:

* **Отсутствие регулирования.** В международно-правовой области отсутствуют концепции «blockchain», «умный контракт» и «криптовалюты».
* **Сложность реализации.** Интеграция интеллектуальных контрактов с элементами реального мира часто занимает много времени, денег, и усилия.
* **Невозможность изменения интеллектуального контракта.** Парадоксально, что один из главных плюсов интеллектуальных контрактов также можно рассматривать как конфликт. Если стороны достигают более выгодного соглашения или возникают новые факторы, они не смогут изменить контракт. По этой причине варианты дополнительных соглашений должны быть реализованы по мере разработки новых blockchain платформ.

**Где можно использовать смарт-контракты?**

Смарт-контракты могут изменять разные области. Мы можем выделить несколько отраслей, в которых интеллектуальные контракты будут наиболее эффективными:

* Финансы
* Страхование
* Электронная коммерция
* Аудит и налогообложение
* Выборы