



Технология блокчейн: что это такое простыми словами

Термин «блокчейн» в большинстве случаев связывают с криптовалютой. Однако эта технология применяется не только в этой сфере. Эксперты активно разрабатывают схемы ее использования в маркетинговых стратегиях, компьютерных развлечениях, создании систем сбора, хранения и анализа персональных сведений и идентификации личности. Что это на самом деле и как это работает, подробно расскажем в статье.

Что такое блокчейн простым языком

Дословно blockchain переводится как цепочка из связанных друг с другом блоков. В таких «ячейках» содержится информация, зашифрованная в цифровом виде.

Представим некоего Вазгена, который продает мандарины. У него обязательно есть книга учета приходов и расходов, куда он каждый вечер аккуратно записывает информацию по каждой сделке. Исправить или стереть эти данные никак нельзя — все транзакции должны быть учтены. В амбарную книгу можно лишь добавить новые сведения.

Если фруктов стало меньше (замерзли, испортились, были съедены грызунами-гурманами), то Вазген может легко узнать, сколько их было изначально: то, что было записано ранее, нигде не исчезает, но на страницах появляются новые данные — сколько мандаринов есть сейчас в наличии и сколько пропало. Подобные записи — примитивный пример блокчейна. Его еще называют технологией распределенных реестров: подробная цепочка сделок и список ее владельцев хранятся на компьютерах разных пользователей. Если на одном или нескольких ПК

произойдет сбой, сведения никуда не пропадут, и при необходимости их можно будет легко восстановить.

Чтобы понять, как устроена эта технология, разберем основные термины, которые применяются при обсуждении блокчейна.

Актив



Кадр из фильма «Кремниевая долина»

Это обязательно что-то ценное, например, денежные средства, движимое и недвижимое имущество или даже важная информация. Активы бывают реальными / материальными (авто, квартира, ценные бумаги) и полностью цифровыми.

Транзакция

Если выдуманный Вазген отдает свои мандарины (активы) покупателю, значит, он совершает транзакцию. Ситуация, когда происходит передача прав собственности на товар — это тоже транзакция. Такое может быть, если наш предприниматель решит ненадолго отойти от дел и уехать в отпуск в жаркие страны: по сути мандарины останутся в магазине, но владеть ими будет уже Гиви — родной брат Вазгена. Его главной задачей станет тщательный контроль всех других транзакций.

Учет транзакций

Под учетом понимают фиксацию всех движений активов (или прав на них) — собственно, этим и должны заниматься Вазген и Гиви. В этой системе передачи есть один важный момент — насколько она надежна, стабильна и соответствует ли критериям конфиденциальности. В нашем примере у Вазгена есть несколько вариантов передачи прав. Он может просто сказать об этом своему компаньону или

назначить его на должность приказом. При этом босс обязан сообщить всем сотрудникам, кто будет его заместителем и какие обязанности он будет выполнять — в базе данных компании должна появиться соответствующая запись.

Допустим, что вся информация фиксируется в большой и толстой тетради. Что будет, если кто-то случайно оставит ее на улице, и она попадет под дождь? Правильно, все записи исчезнут. Как теперь Гиви докажет свои права собственности? Будет сложно и, к сожалению, такое может произойти не только с нашими героями.

У вас есть друг, который уехал отдыхать за рубеж, не рассчитал бюджет и остался без денег. Он просит перевести две сотни евро. Помешать этому могут разные факторы: атаки хакеров, системные проблемы банков, ошибки сотрудников — записи о транзакциях могут просто испариться, а их проведение окажется невозможным. Такое случится, если информация хранится только в одном месте. Блокчейн же в разы уменьшает риски, потому что позволяет контролировать активы и вести учет транзакций на основе распределенных реестров.

Распределенные реестры



Особенность блокчейн в том, что реестр владельцев данных никогда не размещается на одном сервере — одновременное обновление копий происходит сразу на нескольких компьютерах, которые объединены в единую интернет-сеть. В нашем случае с Вазгеном и Гиви это должно выглядеть так: все сотрудники магазина открывают свои блокноты и отмечают, что на время отпуска обязанности руководителя будет выполнять другой человек. Даже если кто-то потеряет записи, информация сохранится у остальных. Блокчейн-реестры, содержащие сведения о владельцах и распределителях активов, нельзя подделать, ведь они хранятся не на одном носителе. У всех заинтересованных лиц должна быть одинаковая, полная и достоверная «картина», и для этого используется понятие консенсуса.

Консенсус

В блокчейне под ним понимают простую процедуру достижения согласия, которая позволяет восстановить правильные данные. Если кто-то из пользователей выключит свой ПК, не дождавшись отображения транзакции, то это никак не повлияет на работу всей сети. Вернемся к нашему примеру. Что будет, если кто-то из сотрудников магазина намеренно или случайно внесет в свой блокнот неверную информацию? В этом случае необходимо поступить следующим образом: прежде чем сделать следующую запись, надо, чтобы все сверили свои блокноты. Вариант, который зафиксирован у большинства, считается единственно верным.

Блок

За определенный промежуток времени в блокчейн-сетях одновременно совершается несколько транзакций. Данные о них включаются в блок. В этой «ячейке» содержится полная информация о том, кто, когда, кому и сколько перевел активов. Последовательные блоки образуют цепочку.

Цепь



Ее невозможно разорвать, так как в каждом блоке находится отсылка на предыдущий. Сами блоки не получится стереть или изменить, можно только добавить новые «кирпичики» системы. Такая «механика» открывает дверь в историю транзакций: в любой момент пользователь может узнать, когда активы одного владельца перешли в руки другого. Наш Вазген установил простое, но строгое правило — сотрудникам магазина нельзя изменять свои записи в блокнотах (исправлять или зачеркивать). Данные о транзакциях всегда постоянные! Передачу прав на управление бизнесом на время отпуска невозможно отыграть назад. В случае с криптовалютой новые блоки в цепочку добавляют майнеры.

Майнеры

Их функции не ограничены созданием блоков. Вращаясь в системе, майнеры проверяют и подтверждают транзакции, зарегистрированные другими пользователями, а также сохраняют копии блокчейна, защищая данные от подделки, потери и хищения. Майнеров может быть сколько угодно, и чем их больше, тем лучше — разрушить такую сеть ой как сложно! Она станет максимально надежной. Чтобы стать майнером, нужны две вещи — мощный компьютер и специальное программное обеспечение.

А что же у нас? Что, если Вазген решил проявить великодушие и передать права на управление не только Гиви, но и Оганесу? В blockchain-магазине так сделать не получится, ведь только одному предпринимателю разрешено регистрировать транзакции. Обязанность остальных — внести данные в свои блокноты и свериться со всем другими.

Награда



За фиксацию новых транзакций и поддержку работы сети блокчейн майнеры получают вознаграждение — комиссию определенного размера от всех участников, зарегистрированных в блоке, а также поощрение от самой сети, которые генерируется специальным алгоритмом. Зачем Гиви следить за порядком в магазине? А затем, чтобы получать зарплату (награду): чем больше он продаст, тем больше будет итоговая сумма, которую он сможет потратить на собственные развлечения. У Гиви прямой интерес вызвать «мандариновую лихорадку».

То же самое происходит и в криптомире. Награда в нем — это непосредственно криптовалюты, которые, в прямом смысле, появляются из ниоткуда и зачисляются на персональный счет майнера. Таким образом выпускаются новые крипто-единицы — общее количество виртуальных денег увеличивается. Однако здесь есть свои

ограничения: как только сумма достигает максимального значения, монеты перестают «синтезироваться», и майнеры работают только за награду от сетевых участников.

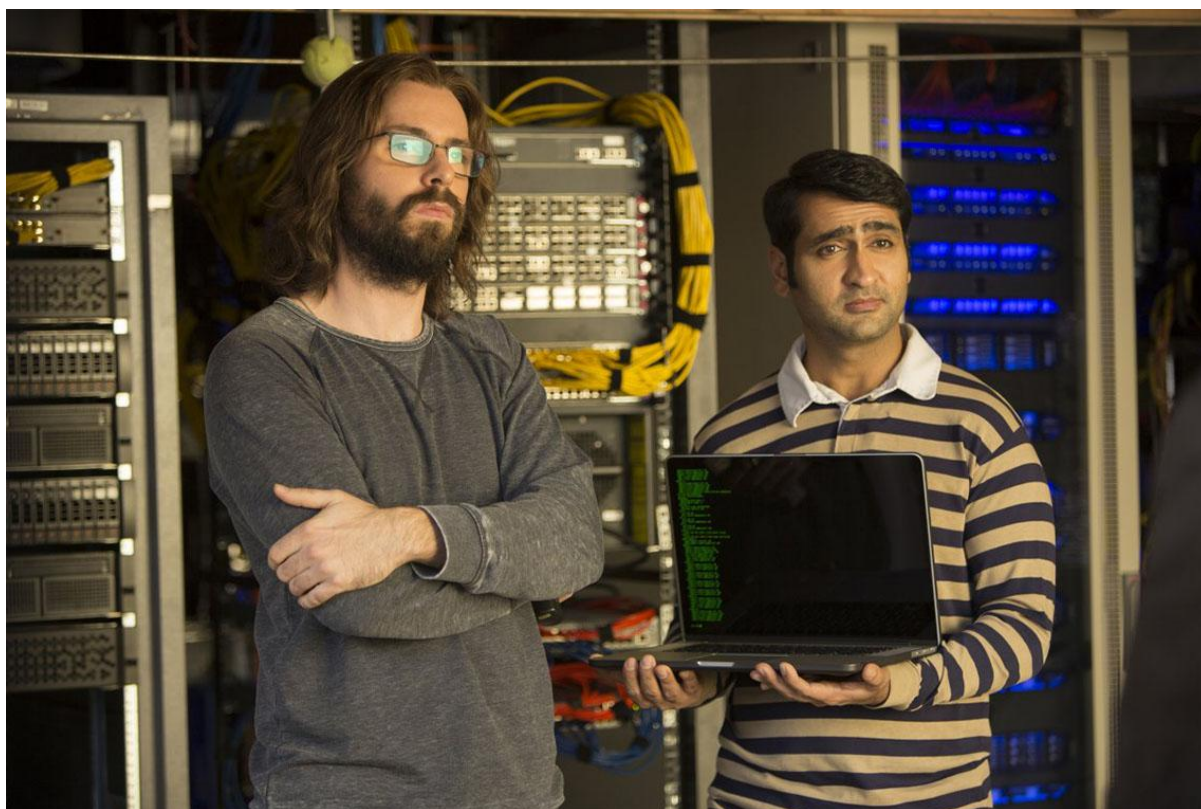
Блокчейн-цепочка выглядит так: в каждой ячейке прописаны время и итог предыдущих транзакций. Алгоритмы системы позволяют майнерам каждые 10 минут добавлять в цепь новый блок, добывая при этом 5 единиц виртуальной валюты. Кто же тот счастливчик, которому удастся положить «кирпичик» и получить за него награду? Для этого в blockchain создаются специальные задачи.

Задачи

Допустим, Вазген решил провести конкурс среди сотрудников — кто же станет ИО директора. Он предлагает решить математический пример, и тот, кто первым напишет правильный ответ в свой блокнот, займет вакантное место.

В блокчейне то же самое: майнеру нужно первым справиться с предложенной задачей и создать новый блок, чтобы получить поощрение. Успех зависит от мощности оборудования, которым он обладает. Зависимость прямая — чем выше производительность ПК, тем больше шансов заработать.

Кошелек



Майнерские цифровые переводы попадают в кошельки — особые идентификаторы, в которых хранятся данные о состоянии счета участника. При этом на том счете не обязательно могут быть деньги, но и любые другие активы. Здесь также размещается полная история транзакций. О том, [как вывести криптовалюту и не нарваться на комиссию](#), читайте в нашей статье.

Кошельки всегда анонимные — нельзя узнать имя владельца, принимающего или отправляющего активы.

В магазине Вазгена всегда «маскарад» — все сотрудники носят маски и не разглашают свои настоящие имена. Никто не знает, что в костюме пчелы ходит Арам, а медведь — это Бедрос.

Анонимность — это хорошо, но в то же время она таит и опасность. Если хозяин кошелька забудет его номер, то у него не будет никаких шансов доказать принадлежность счета. Все, что хранится на балансе, окажется потерянным навечно.

Шифрование

Информация об электронных кошельках и транзакциях в блокчейне защищена специальными средствами шифрования. Подтвердить перевод или принятие активов пользователь может только криптографическим ключом, в котором содержится уникальный цифровой код.

Вазген, назначая Гиви на новую должность, сообщает, сколько килограммов мандаринов необходимо доставить по определенному адресу. Если говорить на языке блокчейна, хозяин дает исполнителю так называемый открытый ключ. У Гиви теперь есть собственный ключ, но закрытый. Именно он позволит открыть склад и взять нужное количество фруктов.

Как узнать последовательность цифр в коде? Никак! Благодаря этой технологии блокчейн можно назвать одним из лучших и надежных вариантов для защиты финансовых операций. Однако случаи взлома кошельков есть, поэтому опытные майнеры рекомендуют подключать их к сети только на момент проведения транзакции.

Смарт-контракты



В системе blockchain они занимают не последнее место. Понятие предложено американским программистом Ником Сабо. Он определяет смарт-контракт как

своеобразный компьютерный алгоритм, который необходим для создания, управления, контроля и предоставления сведений о владении чем-либо.

Интеллектуальный контракт как особый программный протокол позволяет участнику системы забрать то, за что он заплатил. Простая аналогия этого процесса — кофейный автомат: вы кидаете монету, нажимаете кнопку и получаете выбранный напиток. В этой цепочке нет посредников (продавца, кассира, официанта и т. д.) — все автоматизировано. То же и со смарт-контрактами.

Нужно отметить, что они находятся под максимально возможной защитой — по мнению некоторых экспертов они являются надежным местом для хранения данных. За счет чего обеспечивается такая безопасность? Высокий уровень поддерживается благодаря размещению информации в распределенной блокчейн-сети, где не получится что-то изменить или подделать. Сам контракт иногда подвергается шифрованию, создавая полную анонимность для сторон соглашения.

Блокчейн в криптовалюте



В 2008 году некий Сатоши Накамото придумал первую крипту Bitcoin. Это не деньги, а определенный алгоритм, протокол, инструкция — своеобразный свод правил, которым должны следовать все участники системы, осуществляющие транзакции. В основе этих протоколов лежит блокчейн-технология, причем она затрагивает не только биткойны, но и другие виды криптовалюты (в статье [Альткойн: список монет, набирающих популярность в 2022 году](#) мы подробно рассказывали о них).

Bitcoin и blockchain можно назвать взаимозаменяемыми, но между ними есть разница. Основа биткойна — это та самая технология блокчейна. Многие по ошибке используют эти понятия как равнозначные, однако blockchain применяется не только в сфере крипты.

Bitcoin представляет собой централизованную валюту, которая изначально создавалась для проведения интернет-транзакций. Сегодня она имеет статус цифрового актива, который можно перевести в реальные деньги. Биткойн-блокчейн, находящийся в публичном доступе, создает и управляет централизованным реестром. Его копии хранятся на многочисленных серверах, размещенных по всему миру. Серверы выступают в роли финансовых учреждений: на них, как в банки, поступают сведения о совершенных в разное время и разном месте транзакциях. Единственное отличие — у банков есть только данные о деньгах клиентов. Любой может назначить один из серверов узлом — создать собственный биткойн-банк вместо открытия счета.

В bitcoin-сетях цифровые деньги добываются через майнинг. Здесь под ним понимается процесс решения зашифрованных уравнений, необходимый для формирования новых блоков. Все транзакции открыто распространяются по сети, и почти каждые 10 минут майнеры составляют эти блоки. Они, в свою очередь, встраиваются в систему блокчейн, которая играет роль конечного реестра для Bitcoin.

Описанный процесс требует высоких временных затрат — необходимо иметь мощные компьютеры. Майнеры собирают специальные сети для повышения вычислительных ресурсов (подробно об этом мы рассказывали в статье [Майнинговая ферма: что это такое простыми словами](#)). «Добытчики» за свою работу получают не так уж и много криптовалюты. Майнеров можно сравнить с клерками или менеджерами, которые за определенные комиссионные регистрируют сделки.

Блокчейн и базы данных



Блокчейн не надо путать с базами данных (БД). Рассматриваемая технология находится выше и является особой системой, позволяющей управлять этими базами и имеющей более широкие возможности. Среди основных отличий выделяют следующие:

- блокчейн лишен централизованного контроля, чего нельзя добиться в других системах БД;
- у участников сделки нет возможности использовать БД совместно, а в сети blockchain у каждого есть собственная копия реестра, и соответствие между ними поддерживается на автоматическом уровне;
- любую БД можно редактировать (изменять, удалять сведения), в блокчейн информация только добавляется.

Блокчейн и облако

Blockchain-сети — это также и не облачные хранилища данных. Облако представляет собой вычислительный онлайн-сервис. Провайдеры-«облачники» предоставляют доступ к своей инфраструктуре и оборудованию, и это больше, чем просто управление базами данных. Чтобы попасть в публичную blockchain-сеть, пользователь должен сообщить сведения об имеющемся аппаратном обеспечении. Это необходимо для создания копии реестра.

Где и как применяется технология блокчейн



Ротшильд как-то сказал: «Кто владеет информацией, тот владеет миром». И он прав. Сегодня информация — это основа всего: государства, социума, да и всей цивилизации. Она необходима для описания произошедших событий, анализа имеющейся ситуации и прогноза на будущее. Во всех смыслах данные, сведения, информация должны быть максимально точными и достоверными. Если в физической формуле пропустить хотя бы одну букву или цифру, реальность перестанет быть правдивой и, соответственно, полезной. Так можно говорить о любом деле, будь то прогноз или план, составленные на основе ложных данных.

Есть три основных принципа, на которых базируется хранение информации. Она обязана быть:

1. Правдивой (объективно отражать происходящее).
2. Читаемой (ею можно воспользоваться).
3. Существенной (от данных, которые в силу каких-либо причин были утеряны, нет никакой пользы).

Раньше люди хранили разные сведения в своей голове, пересказывая их другим. Постепенно мысли обретали форму — появились слова и письменность: из летописей мы можем знать, что происходило в прошлые времена. Архивы существуют повсеместно: в государственных есть данные о каждом из нас (имя, дата рождения, адрес), в банковских — информация о финансах, из реестров можно узнать об имуществе, а в поликлинике — о состоянии здоровья. В век технологий сведения постепенно приобретают цифровую форму, при этом перенос информации происходит на основании тех принципов, о которых мы говорили чуть выше.

Сведениям важно обеспечивать надежное хранение: бумажный архив может сгореть, и велика вероятность изменения данных. Сохранность зависит, прежде всего, от человека, а не от непосредственного носителя. С появлением компьютерной техники возникла возможность автоматизировать процессы хранения. Пользователь вносит данные, система ПК сортирует их, создает копии и защищает от постороннего вмешательства. Казалось бы, ничего не нарушится. Но тот, у кого есть доступ и определенные знания, легко может изменить записи.

Блокчейн — способ хранения информации



До 2008 года для размещения огромных массивов сведений использовались базы данных. Благодаря отцу биткойна Сатоши Накамото появились блокчейны — принципиально новое «хранилище». Технология предполагает разбивку информации на несколько блоков и связывание последних в единую цепочку. Если что-то изменить хотя бы в одной ячейке, нарушится вся система. Выявить этот факт очень легко, так как данные записываются в автоматическом режиме, а пользователь только посылает запрос на формирование нового блока и запись новых сведений.

Блокчейн — надежный и защищенный способ хранения информации. Среди его достоинств выделяют:

- данные не удаляются и не корректируются;
- исключен риск ошибки, так как сведения заносятся в сеть в автоматическом режиме;
- информация размещается и хранится не на одном компьютере, а сразу в нескольких местах, поэтому ее нельзя уничтожить, даже если избавиться от какого-то носителя;
- технологию можно масштабировать под любые потребности.

У блокчейна есть и недостатки. Первый заключается в том, что объем блоков ограничен — за один раз не получится добавить большой «пакет» информации. Вторым минусом можно назвать отсутствие единого стандарта. Этот момент часто отталкивает от использования системы. Подробнее на том поговорим позже.

Как видим, плюсов гораздо больше. Многие компании и пользователи оценили преимущества блокчейна и активно применяют технологию в своей деятельности.

Энергетика



Компании, работающие в энергетической сфере, используют blockchain для создания одноранговых платформ, на которых проходят торги. У некоторых фирм есть площадки, созданные на основе blockchain и позволяющие хозяевам домов с солнечными батареями продавать избытки энергии соседям. Сложный процесс автоматизирован: смарт-счетчики самостоятельно формируют транзакцию и отправляют ее для записи в blockchain.

Мультимедиа

Компании из сферы развлечений применяют blockchain, чтобы управлять сведениями об авторских правах. Их контроль имеет важное значение для расчета суммы вознаграждения настоящему автору произведения. Простая фиксация сделок по купле-продаже и передаче контента новому владельцу осуществляется через запись нескольких транзакций.

Финансы

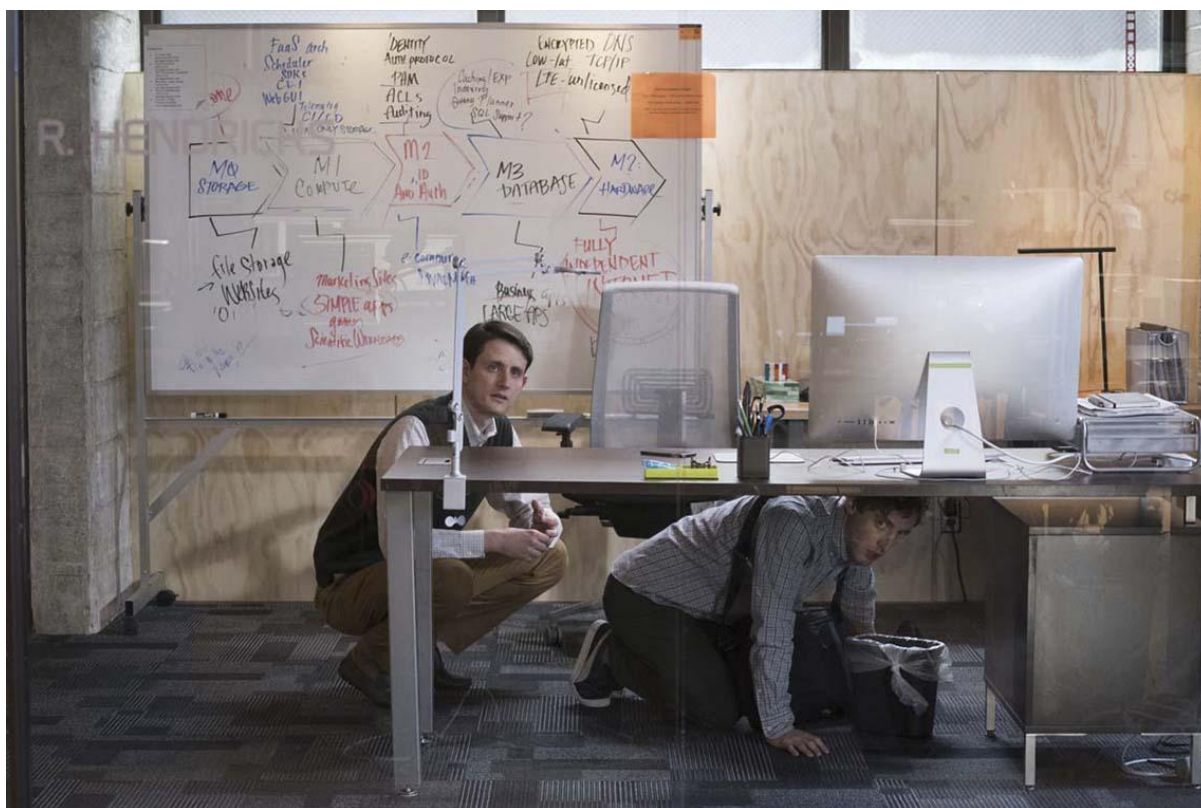
Технология давно внедрилась в системы банковских учреждений и фондовых бирж. Она помогает управлять онлайн-платежами, счетами, рыночной торговлей, а также эффективно проводить расчеты между банками. Внедрение системы — это избавление от проблем, связанных с пакетной обработкой данных и сверкой вручную финансовых транзакций, количество которых может достигать нескольких тысяч.

Розничная торговля

Блокчейн помогает быстро отслеживать движение товара от продавца к покупателю, а также проверять подлинность продукции, которая представлена в онлайн-каталоге. На крупных интернет-платформах (например, Amazon) поставщик, благодаря системе распределенного реестра, может отобразить свою цепочку поставок, при этом у других

участников (изготовителей, курьеров, потребителей) также есть право добавлять события (разрешается после официальной регистрации в сертификационном центре).

Разработка приложений



Программное обеспечение, в основе которого лежит технология блокчейн, обеспечивает:

- безопасное сетевое администрирование, где невозможны хакерские атаки по типу MITM;
- надежное хранение цифровых сертификатов;
- максимально защищенный доступ пользователей к веб-ресурсам (отсутствие риска перехвата пароля);
- точную фиксацию времени внесения новых записей и документов.

Типы блокчейнов

Выделяют несколько разновидностей «блочной» сети.

Название	Особенности
Приватный	Эксклюзивный блокчейн, создаваемый, главным образом, для ведения частного бизнеса. Основные характеристики —

	<p>закрытость, централизованность. Поддержка и контроль осуществляются со стороны создателя. Система подчиняется внутренним целям корпорации. Чтобы «включиться» в систему, требуется учитывать заданные условия. Заниматься майнингом разрешено только сертифицированным пользователям.</p>
Публичный	<p>Войти в сеть и начать майнить криптовалюту может любой желающий. Роль администратора выполняет само сообщество участников.</p>
Гибридный	<p>Сочетает возможности и функции двух блокчейнов, описанных выше. В одной компании может быть и частная, и публичная система — такой комплекс позволяет тщательно контролировать доступ к некоторым данным реестра, но при этом разрешает его к другой информации. В этих схемах используются смарт-контракты. С их помощью участники могут проверить, была ли выполнена частная транзакция.</p>
Консорциумы	<p>Этими блокчейнами управляют целые группы организаций. Ответственность за работоспособность системы распределяется заранее, как и определяются права доступа к информации. Предпочтение консорциумам отдают так называемые фирмы-единомышленники, которые могут извлечь определенную выгоду из общей ответственности.</p>

Принцип работы

Рассмотрим механизм блокчейна подробнее. Он простой, и его можно представить как несколько последовательных шагов.

#1 Фиксация транзакции



Транзакция — это любое движение активов (цифровых или материальных) от одного сетевого пользователя к другому. В blockchain такая информация записывается как блок с данными. В ячейке находятся разные сведения:

- кто принимал участие в сделке;
- что случилось в момент операции;
- когда была совершена сделка;
- место ее проведения;
- почему она была нужна;
- какое именно количество активов было передано;
- какие условия были соблюдены сторонами.

#2 Консенсус

Участники, включенные в блокчейн, обязаны подтвердить, что записанная транзакция достоверна. Правила соглашения в разных типах сети отличаются, но они всегда устанавливаются и закрепляются еще в начале процедуры.

#3 Установление связи между блоками

Как только участники придут к консенсусу, транзакция будет зафиксирована в блоке. Вместе с ней в «ячейку» добавляется специальный шифровальный (криптографический) хеш. Его задача — связать все блоки в единую цепочку. Если

данные в блоке изменятся, то поменяется и значение хеша — это простой, но важный сигнал о том, что информация была подделана (случайно или целенаправленно).

Блоки связаны как звенья стальной цепи, и как-то отредактировать эту связь не получится. Каждая следующая «ячейка» — своеобразный маркер для проверки предыдущей, а, значит, и всей blockchain-системы. Такую структуру можно сравнить с возведением высокой башни из нескольких сегментов: их можно укладывать только сверху (друг на друга), а если вынуть один средний сектор, сломается вся конструкция.

#4 Публичный доступ к реестру



Последний шаг — автоматическая «рассылка» последней копии реестра всем участникам сети.

Чтобы лучше разобраться в принципах работы блокчейна, рассмотрим их на простом примере биткоинов, тем более что технология изначально разрабатывалась именно для этой криптовалюты.

Деньги будут ценными, только если их «изобретатель» сможет дать 100% гарантию, что валюту никто не подделает. В целях обеспечения защиты на бумажные банкноты наносят водяные знаки, голограммы, номера серии, а в электронных базах данных указывают конкретную сумму и место, где она хранится. В системе Bitcoin известно точное количество монет, причем оно ограничено. Каждая операция с ними моментально фиксируется в блоках. Если расшифровать цепочку, то мы узнаем, сколько виртуальных денег находится в конкретном кошельке.

Блок имеет строгую структуру:

- номер;

- подпись;
- данные о транзакции;
- хеш-сумма предшествующей «ячейки»;
- хеш-сумма актуальной «ячейки».

Хеш-сумма представляет собой 16-значное число. Оно формируется после того, как к информации будут применены определенные функции. Сведения прогоняются по специальным алгоритмам и формулам сотни раз и в результате превращаются в бессмысленное на первый взгляд число. Если с данными проделать то же еще раз, получится такое же цифровое сочетание. Когда данные меняются, меняется и хеш-значение. Блок с отредактированными данными не будет совпадать с его же хеш-суммой в следующей «ячейке»: если пользователь скорректирует хеш-сумму блока №1 в блоке №2, изменится хеш-сумма блока №2. Другими словами, удалить или исправить значения задним числом становится невозможно — именно за счет этого обеспечивается надежность хранения данных в блокчейне.

Если участник сети хочет добавить в цепочку новое «звено», он должен его подписать. Подпись представляет собой число, которое получают методом хеширования случайного и бесконечно длинного другого числа. При этом необходимо соблюдать определенные условия, например, в биткойн-системе число должно начинаться с 13 нулей. Их количество напрямую влияет на время, которое майнер должен потратить на поиск задания. Когда это случается, все участники сети получают системное уведомление — кто-то нашел! Они, в свою очередь, начинают проверять, соответствует ли значение установленным требованиям. В блокчейн-схеме формируется новая «ячейка», и в ней фиксируется «призовая» транзакция — размер поощрения, которое выдается за обнаружение числа-подписи. В блок также добавляется информация о других транзакциях и хеш-суммах.

Случайным участникам системы также нужно проверить, правильно ли выполнены транзакции: они должны проанализировать блокчейн-сеть и подтвердить, что в кошельке отправителя есть достаточное количество монет, которые можно перевести. После подтверждения блок автоматически подписывается своим числом и включается в цепочку.

Плюсы и минусы технологии



Ранее мы вкратце говорили о достоинствах и недостатках блокчейна. Пришло время рассмотреть их подробнее.

Blockchain — универсальная система, которую используют в разных сферах жизни, и это ее несомненный плюс. Она открытая, безопасная и защищенная. Внедряя ее на глобальном уровне, можно навсегда избавиться от проблем:

- больших трат на содержание и обслуживание мощных серверных станций и системы защиты данных;
- монополизации рынка;
- необоснованно долгого проведения финансовых операций;
- махинаций с деньгами.

Несмотря на достоинства, скептики находят отрицательные стороны применения системы:

- отсутствие законодательных основ, которые могли бы регулировать статус блокчейн-проектов;
- так называемая Атака 51% неизбежно приведет к сетевому коллапсу;
- невозможность вносить изменения: если появится потребность исправить данные в блоке или отредактировать исходный код, то единственным выходом станет хардфрок:

- если инвестор потеряет приватный ключ, то навсегда лишится доступа к активам, в частности, криптовалюте, хранящейся на виртуальном кошельке;
- некоторые сети нуждаются в «усиленном энергопитании». Чтобы зарабатывать, некоторым майнерам bitcoin необходимы мегаватты электричества.

В blockchain-системах идет негласное «противостояние» опытных пользователей с простыми «массовиками». Старожилы криптовалюты придерживаются определенной концепции, философии, называя новичков «хомяками», которые не вникают в суть. Для них покупка и продажа крипты — увлекательный аттракцион, где все постоянно меняется. Но на «кураже» легко забыть и потерять пароль от кошелька, из-за чего цифровые монеты исчезают навсегда.

Виртуальная валюта «бесхозная» — у нее нет владельца в виде централизованного банка. Некоторые регуляторы пытаются установить контроль над этой сферой и сделать ее более доступной и понятной. На пути систематизации встречаются и довольно печальные примеры. Так, в 2021 году в Китае вступил в силу запрет на криптовалюту. Причем ее не разрешается использовать и в инвестиционных целях. Такой подход государства оправдывается тем, что даже в публичных системах блокчейн невозможно вычислить того, кто проводит транзакцию — все участники действуют анонимно. Другими словами, можно узнать путь движения крипты, но невозможно установить «водителей». Особенно это касается так называемых бартерных ситуаций, когда покупатель переводит монеты продавцу, а тот отдает ему реальные деньги — это одна из распространенных мошеннических схем.

Подобное положение дел не может устраивать регуляторов. Они пытаются массово внедрить специальные алгоритмы позволяющих идентифицировать личность еще до совершения даже самой простой транзакции. Естественно, что биткойн-адептов возмущают такие попытки. Они убеждены, что отсутствие анонимности противоречит философии блокчейна. Отсюда вытекает главный недостаток государственной цифровой валюты — централизованность: в любой момент центральный банк может заблокировать кошельки неугодных лиц.

Блокчейн сейчас



Криптовалюта (в частности, биткойн) была создана как «акт неповиновения». Впервые о ней заговорили после окончания мирового кризиса. Крипту выставляли как мощное и эффективное средство против традиционной системы финансов, несправедливой и коррумпированной.

Создатели виртуальных денег были уверены, что цифровая валюта способна составить конкуренцию «бумажкам» и со временем полностью вытеснит их, а, значит, устранит причины, которые могут вызвать новую кризисную волну.

Неофициальный девиз биткойна простой и звучит как «Верим в криптографию!». В нем заложен определенный смысл: в бедах в экономике виноваты банкиры, посредники и третьи стороны, которым нельзя доверять — большое число участников сделки лишь усложняет проведение транзакций. Биткойн же должен сменить услуги, которые предоставляют посредники, и сделать это он может с помощью методов криптографии и специального кода.

Платеж по ипотечному кредиту — это несколько операций, в ходе которых со счета пользователя списывается определенная сумма. Банк может гарантировать, что со средствами все в порядке, так как у него есть информация, сколько и когда было потрачено. Криптовалюта исключает фоновые операции за счет использования особого программного обеспечения — распределенной базы данных, которая и называется блокчейном.

Технология blockchain также применима к процедурам и процессам, которые не связаны с криптовалютой и движением денежных средств. Можно ли использовать ее, скажем, для установления контакта между людьми, которые сдают квартиру в аренду, и теми, кто ищет жилье? Может ли блокчейн выступать в роли надежного хранилища

мультимедийных файлов и площадки для демонстрации фильмов, телевизионных шоу и других программ СМИ? Способна ли система на автомате проверять авиарейсы и оперативно перечислять денежную компенсацию пассажирами, чьи самолеты задержались? Все реально, и благодаря технологии в лету могут кануть Netflix, Uber и даже страховые компании.

В этих словах нет сомнения. Уже сейчас ведется активная работа, например, на blockchain-платформе Ethereum, которая в дистанционном режиме поддерживает программное обеспечение на одной из распределенных компьютерных систем. Цепочка «ячеек», созданная на криптовалютном эфире, считается самой открытой для экспериментов и проверок гипотез.

Открытость может таить в себе опасность. Каждый день появляются новые блокчейн-схемы. Они, в том числе, разрабатываются корпорациями-гигантами. Так, Microsoft уже сейчас предлагает пользователям определенные инструменты, позволяющие проводить операции с криптой на облаке Azure. Intel и IBM активно контактируют с хабом Hyperledger — публичной площадкой, ориентированной на разработку блокчейнов для бизнеса. Мировые банки работают над созданием собственных версий технологии, стремясь опередить время и стать первыми на рынке. И даже старый и добрый биткоин, практически родоначальник blockchain-систем, проходит этап модернизации для приложений.



Во многих странах технология blockchain обсуждается на государственном уровне. Одни ведут речь о биткоинах и других видах криптовалюты, другие пытаются внедрить цифровые деньги в банковскую систему и операции по международным переводам.

С юридической точки зрения вопрос не решен, что тормозит развитие и применение блокчейна, в том числе и в России. На процесс сильно влияют решения руководства Центробанка, где пытаются четко разграничить понятия blockchain и криптовалюты. Для финансовых учреждений внедрение технологии принесет выгоду относительно

того, что сейчас происходит со SWIFT — избавит от монополии и контроля международных транзакций.

Кроме системы переводов рассматривается и возможность разработки международных баз данных. Эксперты предполагают, что общедоступные ресурсы позволят быстро и своевременно отправлять коллегам и партнерам уведомления о мошеннических действиях, а также формировать «черные» и «белые» списки контрагентов. Рынок России пока не готов к таким нововведениям, но сейчас уже ведутся работы по созданию «национальной», русской криптовалюты, которая будет легальной.

Если говорить о перспективах развития блокчейна, то они открываются только на глобальном уровне. Оптимистично настроенные специалисты прогнозируют, что технология спасет от коррупции и поможет свести к минимуму махинации с деньгами и финансовые правонарушения. Если удастся построить максимально прозрачную систему, пользователи будут вынуждены соблюдать действующее законодательство, так как информация о каждой транзакции станет открытой.

Заключение



Blockchain — это не крипта, не облако, не база данных. Блокчейн для чайников — это особая технология, применяемая для хранения информации. Система представляет собой множество блоков, объединенных в цепочку. В каждом из них прописаны данные, начиная с первого. Новые «звенья» цепи добавляются в конец — система постепенно разрастается подобно снежному кому.

«Ячейки» в блокчейне расположены в строгой хронологии. Связь между ними обеспечивает криптографическая подпись, в основе которой лежат сложные алгоритмы. Актуальное состояние системы загружается в автоматическом режиме,

доступ к реестру открывается одновременно тысячам компьютеров, которые объединены в сеть.

Считается, что блокчейн — надежный способ хранения информации. Сегодня он нашел применение не только в сфере цифровых финансов, но и в энергетике, мультимедиа, банковских системах. Эксперты рисуют радужные перспективы развития технологии за счет ее несомненных преимуществ перед классическими базами данных.