## Что такое блокчейн?

Блокчейн — это особая база данных, которую также называют децентрализованным цифровым реестром. Он поддерживается множеством компьютеров по всему миру. Данные блокчейна хранятся в блоках в хронологическом порядке и защищены с помощью криптографии.

Первая модель блокчейна была создана в начале 1990-х годов, когда специалист по информатике Стюарт Хабер и физик У. Скотт Сторнетта решили использовать криптографию в цепочке блоков для защиты цифровых документов от фальсификации.

Хабер и Сторнетта вдохновили многих программистов и любителей криптографии, что в конечном итоге привело к созданию Биткоина — первой криптовалюты на основе технологии блокчейна. С тех пор блокчейн стал набирать популярность, и сейчас число пользователей криптовалют неуклонно растет по всему миру.

Технология блокчейна обычно используется для записи криптовалютных транзакций, но она также подходит для записи других видов цифровых данных и может выполнять множество задач.

## Что такое децентрализация в блокчейне

Децентрализация в блокчейне означает, что контроль и полномочия по принятию решений в сети распределены между ее пользователями, а не принадлежат одному субъекту, такому как правительство или корпорация. Децентрализация может быть полезна в ситуациях, когда пользователям необходимо координировать свои действия с незнакомыми людьми или когда они хотят обеспечить безопасность и целостность своих данных.

В децентрализованной сети блокчейна нет центрального органа или посредника, контролирующего поток данных или транзакций. Вместо этого транзакции проверяются и записываются распределенной сетью компьютеров, которые вместе поддерживают целостность сети.

При этом блокчейн — это не только база данных. Он также обеспечивает работу различных сервисов, таких как криптовалюты и невзаимозаменяемые токены (NFT). С его помощью пользователи могут сотрудничать и совершать сделки друг с другом без участия центрального органа власти.

## Как работает блокчейн

Блокчейн — это цифровой реестр, который надежно записывает транзакции между двумя сторонами и защищает эти записи от несанкционированного доступа. Данные о транзакциях записываются распределенной сетью специальных компьютеров со всего мира, называемых нодами.

Когда пользователь инициирует транзакцию, например отправляет определенную сумму криптовалюты другому пользователю, эта транзакция транслируется в сеть. После этого каждая нода проверяет подлинность транзакции, изучая цифровые подписи и другие данные транзакции.

Если транзакцию одобрили, она добавляется в блок вместе с другими проверенными транзакциями. Блоки соединяются в цепочку с помощью криптографических методов и образуют блокчейн. Для проверки транзакций и добавления их в блокчейн используется механизм консенсуса. Механизм консенсуса — это набор правил, с помощью которого ноды координируют свои действия и приходят к соглашению о состоянии блокчейна и одобрении транзакций.

Чтобы запись транзакций была надежной, прозрачной и устойчивой к взлому, блокчейн использует криптографию. Одним из важнейших криптографических методов является хеширование — процесс, который преобразует входные данные любого размера в строку символов фиксированной длины.

Хеш-функции в блокчейне обычно устойчивы к коллизиям. Это означает, что вероятность найти две части данных, которые произведут один и тот же результат, невероятно мала. При этом любое изменение входных данных полностью изменит результат хеширования.

Еще один криптографический метод, который часто используют в блокчейне, — это криптография с открытым ключом, или асимметричная криптография. Она помогает устанавливать безопасные и проверяемые транзакции между пользователями.

Работает это так. У каждого пользователя есть уникальная пара ключей: приватный ключ, который необходимо держать в тайне, и публичный ключ, который находится в открытом доступе. Когда пользователь инициирует транзакцию, он подписывает ее с помощью своего приватного ключа, создавая цифровую подпись.

Затем другие пользователи сети могут проверить подлинность транзакции, применив публичный ключ отправителя к цифровой подписи. Такой подход обеспечивает безопасность транзакций, поскольку инициировать транзакцию может только настоящий владелец приватного ключа, но проверить подписи с помощью публичного ключа может кто угодно.

Соответственно, еще одной особенностью блокчейна является прозрачность. Любой желающий может проверить на публичных сайтах данные блокчейна, включая всю информацию о транзакциях и блоках.  Например, на сайтах обозревателей блокчейна можно увидеть каждую транзакцию, когда-либо записанную в сети Биткоина, включая идентификаторы отправителя и получателя, сумму перевода и список владельцев любого биткоина.

## Что такое механизм консенсуса

Алгоритм консенсуса — это механизм, с помощью которого пользователи и программы могут координировать свои действия в распределенной сети. Он обеспечивает достижение согласия между всеми участниками сети о текущем состоянии данных, даже если некоторые ноды выходят из строя. Такой алгоритм гарантирует, что все ноды сети имеют одну и ту же копию реестра, содержащую запись всех транзакций. Механизмы консенсуса — неотъемлемая часть блокчейнов, ведь у них нет центрального органа, который бы проверял транзакции и поддерживал целостность сети.

Когда десятки тысяч нод хранят копию данных блокчейна, могут быстро возникнуть проблемы, например, из-за несогласованных данных и вредоносных нод. Поэтому для обеспечения целостности блокчейна существуют различные механизмы консенсуса, которые определяют, как ноды сети достигают соглашения. Рассмотрим основные из них.

## Типы механизмов консенсуса

### Что это такое

Proof of Work (PoW) — это механизм консенсуса, используемый во многих сетях блокчейна для проверки транзакций и поддержания целостности блокчейна. Это самый первый механизм консенсуса, который появился и действует в Биткоине.

В PoW майнеры соревнуются в решении сложной математической задачи за право добавить в блокчейн следующий блок. Для этого они осуществляют майнинг. Первый майнер, решивший задачу, получает вознаграждение в виде криптовалюты.

Майнеры должны использовать мощные компьютеры, чтобы решать математические задачи, создавать новые монеты и обеспечивать безопасность сети. Поэтому процесс майнинга требует значительных вычислительных мощностей и, следовательно, энергии.

### Что такое Proof of Stake

Proof of Stake (PoS) — это механизм консенсуса, разработанный для устранения некоторых недостатков Proof of Work (PoW). В системе PoS нет майнеров, которые соревнуются в решении сложных математических задач для подтверждения транзакций и добавления новых блоков в блокчейн. Вместо этого в системе действуют валидаторы, которые добавляют в стейкинг криптовалюту и выбираются на основе предоставленной суммы.

Для участия в процессе консенсуса валидаторы добавляют в стейкинг определенное количество криптовалюты, то есть удерживают ее в качестве залога. Затем они случайным образом выбираются для создания новых блоков и подтверждения транзакций в зависимости от размера их доли в стейкинге. За создание новых блоков валидаторы получают комиссии за транзакции, которые мотивируют их действовать в интересах сети.

### Другие популярные механизмы консенсуса

Proof of Work и Proof of Stake являются наиболее распространенными алгоритмами консенсуса, но они не единственные в своем роде. Существует множество других алгоритмов: одни из них объединяют элементы двух вышеупомянутых систем, а другие открывают совершенно новые способы достижения консенсуса.

Например, Delegated Proof of Stake (DPoS) похож на PoS, но в PoS право создавать новые блоки есть у всех валидаторов, а в DPoS держатели токенов избирают набор делегатов, которые создают блоки от их имени.

А в Proof of Authority (PoA) учитывают репутацию или личность валидатора, а не его количество удерживаемой криптовалюты. Валидаторы выбираются на основе надежности и могут быть удалены из сети за вредоносные действия.

## Преимущества блокчейна

### 1. Децентрализация

Благодаря децентрализации в блокчейне нет единой точки контроля или отказа, поэтому децентрализация может повысить безопасность и устойчивость к атакам или утечке данных.

### 2. Прозрачность

Транзакции на блокчейне видны всем желающим, поэтому отслеживать и проверять транзакции довольно легко.

### 3. Неизменность

После добавления транзакции в блокчейн ее нельзя изменить или удалить. Но посмотреть ее может любой желающий, потому что на блокчейне ведется постоянная запись всех одобренных транзакций. Этим он значительно отличается от традиционных систем, в которых транзакции можно отменить.

### 4. Эффективность

Транзакции в блокчейне могут быть более быстрыми и эффективными, поскольку блокчейну не нужны посредники, такие как банки.

### 5. Более низкие комиссии

Блокчейн может снизить стоимость транзакций и повысить эффективность некоторых бизнес-операций, устраняя посредников и автоматизируя процессы.

### 6. Не требует доверия

Технология блокчейна позволяет совершать прозрачные транзакции, которые проверяются и подтверждаются самими участниками сети без навязанных посредников.

## Типы сетей блокчейна

### Публичный блокчейн

Публичный блокчейн — это открытая децентрализованная сеть, доступная всем желающим. Обычно такие сети используют открытый исходный код, действуют прозрачно и не требуют доверия, то есть получить к ним доступ и использовать их может кто угодно. Примерами публичных блокчейнов являются Биткоин и Ethereum.

### Приватный блокчейн

Приватный блокчейн, как следует из названия, — это закрытая сеть блокчейна. Обычно она находится под контролем одной организации и используется для ее целей и способов применения.

Приватные блокчейны контролируют доступ и устанавливают правила, которые определяют, кто может видеть и записывать транзакции в блокчейне. Они не являются децентрализованными, поскольку в них действует четкая иерархия управления. Однако они могут быть распределенными и поручать многим нодам хранить копию блокчейна на своих компьютерах.

### Блокчейн-консорциум

Блокчейн-консорциум — это гибрид публичного и приватного блокчейнов. В блокчейн-консорциуме несколько организаций объединяются для создания общей сети блокчейна, которая управляется и контролируется совместно. В зависимости от потребностей участников такие сети могут быть как открытыми, так и закрытыми.

В отличие от открытой системы, где проверять блоки может любой пользователь, или закрытой системы, где создателей блоков выбирает одна организация, в блокчейн-консорциуме валидаторами выступают несколько одинаково влиятельных сторон.

Следовательно, правила системы гибкие: просматривать блокчейн могут либо все пользователи, либо только валидаторы. Если валидаторы могут достичь консенсуса между собой, вносить изменения довольно просто. И пока определенная часть участников сети действует честно, у системы блокчейна не возникнет проблем.

## Для чего используется блокчейн?

Хотя технология блокчейна еще находятся на ранней стадии развития, ее уже применяют во многих отраслях. Обычно она используется в следующих сферах:

### 1. Криптовалюты

Технология блокчейна поддерживает создание криптовалют и запись их транзакций в безопасном и децентрализованном реестре.

### 2. Цифровая идентификация

Блокчейн можно использовать для создания безопасной и защищенной от взлома цифровой идентификации, которая нужна для проверки личной информации и других конфиденциальных данных. Цифровая идентификация может стать очень востребованной, ведь наша личная информации и активы постепенно переходят в интернет.

### 3. Голосование

Технология блокчейна позволяет проводить безопасные и прозрачные голосования, которые исключают возможность мошенничества. Ведь блокчейн предоставляет децентрализованный и защищенный от взлома реестр всех голосов.

### 4. Управление цепочками поставок

Технологию блокчейна можно использовать для создания реестра всех транзакций в цепочке поставок. В таком случае каждая транзакция будет записана в виде блока на блокчейне, который обеспечит неизменность и прозрачность всех записей о процессах цепочки поставок.

### 5. Смарт-контракты

Смарт-контракты — это самоисполняющиеся программы, которые могут автоматически выполнять заданные действия при определенных условиях. Технология блокчейна позволяет создавать и исполнять смарт-контракты безопасным и децентрализованным способом. Они могут применяться в разных сферах, наиболее перспективные из которых — децентрализованные приложения (DApp) и организации (DAO).

## В заключение

Технология блокчейна предлагает безопасный и прозрачный способ записи транзакций и хранения данных. Она способна произвести революцию во многих сферах за счет нового уровня доверия и безопасности в цифровом мире.

Блокчейн открывает целый мир возможностей: позволяет совершать одноранговые транзакции, создавать новые формы цифровых активов и развивать децентрализованные приложения. Поскольку эта технология продолжает развиваться и набирать популярность, скорее всего, в ближайшие годы у нее появятся новые инновационные сценарии использования.