**Блокче́йн** ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *blockchain* или *block chain*) — выстроенная по определённым правилам непрерывная последовательная цепочка блоков ([связный список](https://ru.wikipedia.org/wiki/Связный_список)), содержащих информацию. Чаще всего копии цепочек блоков хранятся на множестве разных компьютеров независимо друг от друга.

## Общие сведения

Впервые термин появился как название полностью [реплицированной](https://ru.wikipedia.org/wiki/Репликация_(вычислительная_техника)) [распределённой базы данных](https://ru.wikipedia.org/wiki/Распределённая_база_данных), реализованной в системе «[Биткойн](https://ru.wikipedia.org/wiki/Биткойн)», из-за чего блокчейн часто относят к [транзакциям](https://ru.wikipedia.org/wiki/Транзакция_(информатика)) в различных [криптовалютах](https://ru.wikipedia.org/wiki/Криптовалюта), однако технология цепочек блоков может быть распространена на любые взаимосвязанные информационные блоки.

## Реализация в системе Биткойн

### **Блок транзакций**

Блок транзакций — специальная структура для записи группы транзакций в системе [Биткойн](https://ru.wikipedia.org/wiki/Биткойн) и аналогичных ей. Транзакция считается завершённой и достоверной («подтверждённой»), когда проверены её формат и подписи, и когда сама транзакция объединена в группу с несколькими другими и записана в специальную структуру — *блок*. Содержимое блоков может быть проверено, так как каждый блок содержит информацию о предыдущем блоке. Все блоки выстроены в одну цепочку, которая содержит информацию обо всех совершённых когда-либо операциях в базе. Самый первый блок в цепочке — *первичный блок* ([англ.](https://ru.wikipedia.org/wiki/Английский_язык) *genesis block*) — рассматривается как отдельный случай, так как у него отсутствует родительский блок.

Блок состоит из заголовка и списка транзакций. Заголовок блока включает в себя свой [хеш](https://ru.wikipedia.org/wiki/Хеш-сумма), хеш предыдущего блока, хеши транзакций и дополнительную служебную информацию. В системе Биткойн первой транзакцией в блоке всегда указывается получение комиссии, которая станет наградой [майнеру](https://ru.wikipedia.org/wiki/Майнинг) за созданный блок. Далее идёт список транзакций, сформированный из очереди транзакций, ещё не записанных в предыдущие блоки. Критерий отбора из очереди задаёт майнер самостоятельно. Это не обязательно должна быть хронология по времени. Например, могут включаться только операции с высокой комиссией или с участием заданного списка адресов. Для транзакций в блоке используется [древовидное хеширование](https://ru.wikipedia.org/wiki/TTH), аналогичное формированию [хеш-суммы](https://ru.wikipedia.org/wiki/Хеш-сумма) для файла в [протоколе BitTorrent](https://ru.wikipedia.org/wiki/BitTorrent_(протокол)). Транзакции, кроме начисления комиссии за создание блока, содержат внутри параметра *input* ссылку на транзакцию с предыдущим состоянием данных (в системе Биткойн, например, даётся ссылка на ту транзакцию, по которой были получены расходуемые биткойны). Операции по передаче майнеру комиссии за создание блока не имеют «входных» транзакций, поэтому в данном параметре может указываться любая информация (для них это поле носит название [англ.](https://ru.wikipedia.org/wiki/Английский_язык) *Coinbase parameter*).

Созданный блок будет принят остальными пользователями, если числовое значение хеша заголовка равно или меньше определённого целевого числа, величина которого периодически корректируется. Так как результат [хеширования](https://ru.wikipedia.org/wiki/Хеширование) функции [SHA-256](https://ru.wikipedia.org/wiki/SHA-256) считается [необратимым](https://ru.wikipedia.org/wiki/Односторонняя_функция), на данный момент нет алгоритма получения желаемого результата, кроме случайного перебора. Если хеш не удовлетворяет условию, то в заголовке изменяется параметр [nonce](https://ru.wikipedia.org/wiki/Nonce) и хеш пересчитывается. Обычно требуется большое количество пересчётов. Когда вариант найден, узел рассылает полученный блок другим подключенным узлам, которые проверяют блок. Если ошибок нет, то блок считается добавленным в цепочку и следующий блок должен включить в себя его хеш.

Величина целевого числа, с которым сравнивается хеш, в системе Биткойн корректируется через каждые 2016 блоков. Запланировано, что вся сеть системы Биткойн должна тратить на генерацию одного блока примерно 10 минут, на 2016 блоков — около двух недель. Если 2016 блоков сформированы быстрее, то цель немного уменьшается и достичь её становится труднее, в противном случае цель увеличивается. Изменение сложности вычислений не влияет на надёжность сети Биткойн и требуется лишь для того, чтобы система генерировала блоки почти с постоянной скоростью, не зависящей от вычислительной мощности участников сети.

### **Цепочка блоков**

Блоки одновременно формируются множеством «[майнеров](https://ru.wikipedia.org/wiki/Майнинг)». Удовлетворяющие критериям блоки отправляются в сеть, включаясь во все [репликации](https://ru.wikipedia.org/wiki/Репликация_(вычислительная_техника)) распределённой базы блоков. Регулярно возникают ситуации, когда несколько новых блоков в разных частях распределённой сети называют предыдущим один и тот же блок, то есть цепочка блоков может ветвиться. Специально или случайно можно ограничить ретрансляцию информации о новых блоках (например, одна из цепочек может развиваться в рамках локальной сети). В этом случае возможно параллельное наращивание различных ветвей. В каждом из новых блоков могут встречаться как одинаковые транзакции, так и разные, вошедшие только в один из них. Когда ретрансляция блоков возобновляется, майнеры начинают считать главной цепочку с учётом уровня сложности хеша и длины цепочки. При равенстве сложности и длины предпочтение отдаётся той цепочке, конечный блок которой появился раньше. Транзакции, вошедшие только в отвергнутую ветку (в том числе по выплате вознаграждения), теряют статус подтверждённых. Если это транзакция по передаче биткойнов, то она будет поставлена в очередь и затем включена в очередной блок. Транзакции получения вознаграждения за создание отсечённых блоков не дублируются в другой ветке, то есть «лишние» биткойны, выплаченные за формирование отсечённых блоков, не получают дальнейших подтверждений и «утрачиваются».

Таким образом, цепочка блоков содержит историю владения, с которой можно ознакомиться, например, на специализированных сайтах.

Блокчейн формируется как непрерывно растущая цепочка блоков с записями обо всех транзакциях. Копии базы или её части одновременно хранятся на множестве компьютеров и синхронизируются согласно формальным правилам построения цепочки блоков. Информация в блоках не шифрована и доступна в открытом виде, но отсутствие изменений удостоверяется [криптографически](https://ru.wikipedia.org/wiki/Криптография) через хэш-цепочки (элемент [цифровой подписи](https://ru.wikipedia.org/wiki/Цифровая_подпись)).

База публично хранит в незашифрованном виде информацию о всех [транзакциях](https://ru.wikipedia.org/wiki/Транзакция_(информатика)), [подписываемых](https://ru.wikipedia.org/wiki/Электронная_цифровая_подпись) с помощью [асимметричного шифрования](https://ru.wikipedia.org/wiki/Криптосистема_с_открытым_ключом). Для предотвращения многократной траты одной и той же суммы используются метки времени, реализованные путём разбиения БД на цепочку специальных блоков, каждый из которых, в числе прочего, содержит в себе [хеш](https://ru.wikipedia.org/wiki/Контрольная_сумма) предыдущего блока и свой порядковый номер. Каждый новый блок осуществляет подтверждение транзакций, информацию о которых содержит и дополнительное подтверждение транзакций во всех предыдущих блоках цепочки. Изменять информацию в блоке, который уже находится в цепи, не практично, так как в таком случае пришлось бы редактировать информацию во всех последующих блоках. Благодаря этому успешная [double-spending](https://ru.wikipedia.org/wiki/Double-spending) атака (повторная трата ранее израсходованных средств) на практике крайне маловероятна.

Чаще всего умышленное изменение информации в любой из копий базы или даже в достаточно большом количестве копий не будет признано истинным, так как не будет соответствовать правилам. Некоторые изменения могут быть приняты, если будут внесены во все копии базы (например, удаление нескольких последних блоков из-за ошибки в их формировании).

Для более наглядного объяснения механизма работы платёжной системы [Сатоси Накамото](https://ru.wikipedia.org/wiki/Сатоси_Накамото) ввёл понятие «*цифровая монета*», определив его как цепочку цифровых подписей. В отличие от стандартизированных номиналов обычных монет, каждая «цифровая монета» имеет свой собственный номинал. Каждому биткойн-адресу может сопоставляться любое количество «цифровых монет». При помощи транзакций их можно делить и объединять, при этом сохраняется общая сумма их номиналов за вычетом комиссии.

До версии 0.8.0 для хранения цепочки блоков основной клиент использовал [Berkeley DB](https://ru.wikipedia.org/wiki/Berkeley_DB), начиная с версии 0.8.0 разработчики перешли на [LevelDB](https://ru.wikipedia.org/w/index.php?title=LevelDB&action=edit&redlink=1).

#### **Подтверждение транзакций**

Пока транзакция не включена в блок, система считает, что количество биткойнов на некоем адресе остаётся неизменным. В это время есть техническая возможность оформить несколько разных транзакций по передаче с одного адреса одних и тех же биткойнов разным получателям. Но как только одна из подобных транзакций будет включена в блок, остальные транзакции с этими же биткойнами система будет уже игнорировать. Например, если в блок будет включена более поздняя транзакция, то более ранняя будет считаться ошибочной. Есть небольшая вероятность, что при ветвлении две подобные транзакции попадут в блоки разных ветвей. Каждая из них будет считаться правильной, лишь при отмирании ветви одна из транзакций станет считаться ошибочной. При этом не будет иметь значения время совершения операции.

Таким образом, попадание транзакции в блок является подтверждением её достоверности вне зависимости от наличия других транзакций с теми же биткойнами. Каждый новый блок считается дополнительным «подтверждением» транзакций из предыдущих блоков. Если в цепочке 3 блока, то транзакции из последнего блока будут подтверждены 1 раз, а помещённые в первый блок будут иметь 3 подтверждения. Достаточно дождаться нескольких подтверждений, чтобы вероятность отмены транзакции стала очень низкой.

Для уменьшения влияния подобных ситуаций на сеть существуют ограничения на распоряжение только что полученными биткойнами. Согласно сервису *blockchain.info*, до мая 2015 года максимальная длина отвергнутых цепочек была 5 блоков. Необходимое число подтверждений для разблокирования полученного зависит от программы-клиента либо от указаний принимающей стороны. Клиент «Bitcoin-qt» для отправки не требует наличия подтверждений, но у большинства получателей по умолчанию выставлено требование 6 подтверждений, то есть реально воспользоваться полученным обычно можно через час. Различные онлайн-сервисы часто устанавливают свой порог подтверждений.

Биткойны, полученные за создание блока, протокол разрешает использовать после 100 подтверждений, но стандартная программа-клиент показывает комиссию через 120 подтверждений, то есть обычно воспользоваться комиссией можно примерно через 20 часов после её начисления.

#### **«Двойное расходование»**

Если контролировать более 50 % суммарной вычислительной мощности сети, то существует теоретическая возможность при любом пороге подтверждений одни и те же биткойны передать два раза разным получателям — одна из транзакций будет публичной и подтверждаться в общем порядке, а вторая не будет афишироваться, её подтверждения будут происходить блоками скрытой параллельной ветви. Лишь через некоторое время сеть получит сведения о второй транзакции, она станет подтверждённой, а первая утратит подтверждения и будет игнорироваться. В результате не произойдёт удвоения биткойнов но изменится их текущий владелец, при этом первый получатель утратит биткойны без каких-либо компенсаций.

Открытость цепочки блоков позволяет внести в произвольный блок изменения. Но тогда потребуется пересчёт хеша не только изменённого блока, но и всех последующих. Фактически, для такой операции потребуется мощность не меньше той, которая была использована для создания изменённого и последующих блоков (то есть всей текущей мощности), что делает такую возможность крайне маловероятной.

На 1 декабря 2013 года суммарная мощность сети превысила 6000 THash/s. С начала [2014 года](https://ru.wikipedia.org/wiki/2014_год) объединение майнеров (пул) *Ghash.io* длительное время контролирует свыше 40 % суммарной мощности сети «Биткойн», а в начале июня 2014 года в нём кратковременно концентрировалось более 50 % мощности сети.

Двойное расходование биткойнов на практике никогда не было зафиксировано. На май [2015 года](https://ru.wikipedia.org/wiki/2015_год) параллельные цепочки никогда не превышали 5 блоков.

### **Сложность**

За требование к хешам блоков отвечает специальный параметр, называемый «сложность». Так как вычислительные мощности сети непостоянны, этот параметр пересчитывается клиентами сети через каждые 2016 блоков таким образом, чтобы поддерживать среднюю скорость формирования блокчейна на уровне 2016 блоков в две недели. Таким образом, 1 блок должен создаваться примерно раз в десять минут. На практике, когда вычислительная мощность сети растёт — соответствующие временные промежутки короче, а когда снижается — длиннее. Перерасчёт сложности с привязкой ко времени возможен благодаря наличию в заголовках блоков времени их создания. Оно записывается в [Unix-формате](https://ru.wikipedia.org/wiki/UNIX-время) по системным часам автора блока (если блок создается в пуле, то по системным часам сервера этого пула).

## Применение вне сферы криптовалют

В настоящее время к технологии блокчейн проявляют интерес представители самых различных сфер.

### **Банковский сектор**

В российском банковском секторе к технологии проявляют интерес такие компании как [ВТБ](https://ru.wikipedia.org/wiki/Банк_ВТБ) и [Сбербанк](https://ru.wikipedia.org/wiki/Сбербанк).

О разработках и планах использования технологии блокчейн заявили платёжные системы [VISA](https://ru.wikipedia.org/wiki/VISA_(платёжная_система)), [Mastercard](https://ru.wikipedia.org/wiki/MasterCard), [Unionpay](https://ru.wikipedia.org/wiki/China_UnionPay) и [SWIFT](https://ru.wikipedia.org/wiki/SWIFT).

В июле 2017 года [S7 Airlines](https://ru.wikipedia.org/wiki/S7_Airlines) и [Альфа-банк](https://ru.wikipedia.org/wiki/Альфа-банк) запустили в эксплуатацию блокчейн-платформу автоматизации торговых операций с агентами на базе [Ethereum](https://ru.wikipedia.org/wiki/Ethereum).

### **Земельный реестр**

Швеция, Украина и ОАЭ планируют вести земельный реестр при помощи технологии блокчейн.

Правительство Индии борется с земельным мошенничеством при помощи блокчейн.

В первом полугодии 2018 года будет проводиться эксперимент по использованию технологии блокчейн в целях мониторинга достоверности сведений Единого государственного реестра недвижимости (ЕГРН) на территории Москвы.

### **Удостоверение личности**

В 2014 году основана компания [Bitnation](https://ru.wikipedia.org/wiki/Bitnation), предоставляющая услуги традиционного [государства](https://ru.wikipedia.org/wiki/Государство), такие как [удостоверение личности](https://ru.wikipedia.org/wiki/Удостоверение_личности), [нотариат](https://ru.wikipedia.org/wiki/Нотариат) и ряд других.

В июне 2017 [Accenture](https://ru.wikipedia.org/wiki/Accenture) и [Microsoft](https://ru.wikipedia.org/wiki/Microsoft) представили систему цифровых удостоверений личности на блокчейне.

В августе 2017 правительство Бразилии начало тестирование системы удостоверений личности на блокчейн[.](https://ru.wikipedia.org/wiki/Блокчейн" \l "cite_note-37)

Финляндия идентифицирует беженцев при помощи блокчейн-технологий.

В Эстонии работает блокчейн-система электронного гражданства.

**В Активном Гражданине**

#### **Блокчейн, хранящий состояния и транзакций**

Чтобы добавить способность выполнять программы, блокчейн был модифицирован таким образом, что каждый его блок теперь содержит не только данные о последних транзакциях, но и актуальное состояние программ, получивших название «умные контракты». Информация о состоянии контрактов обновляется вместе с добавлением нового блока согласно записанным в нем данным о транзакциях. В качестве гарантии того, что предоставленные программам инструкции не будут выполняться вечно, было введено специальное ограничение: инициирующая контракт сторона должна платить специальные знаки денежной ценности, количество которых зависит от числа инструкций и уровня потребления контрактом памяти системы.

#### **Контракты-счета**

У каждого контракта в блокчейн есть постоянный адрес, назначаемый ему во время создания и позволяющий идентифицировать его в системе. Каждый контракт содержит баланс, выражаемый в виде некоторого количества основных денежных единиц сети Ethereum, получивших название ether.  
  
Если контракт не включает в себя ни одну программную инструкцию, он выступает в роли счета, у которого есть адрес и баланс. Счета могут обмениваться ether’ами с другими счетами или контрактами.

#### **Контракты в виде децентрализованных исполняемых программ**

Каждому контракту для выполнения требуется ether. Эта мера призвана исключить ситуации с бесконечной работой программ, так как их выполнение прекращается как только выделенные во время вызова ether’ы заканчиваются. Сам вызов контракта также требует небольшого количества ether, которое в конечном счете достается тому узлу, которому удастся успешно отправить в блокчейн следующий блок. Тем не менее существует возможность прямо отправить некоторое количество ether тому или иному контракту во время его вызова для перевода баланса, например, в целях оплаты.  
  
Выполнение тех или иных действий программы возможно благодаря передаче параметров в методы программных инструкций. Выполнение метода может изменить состояние контракта с помощью корректировки значений одного или нескольких его полей. Контракт также может обладать набором событий, используемых для уведомления заинтересованных сторон о результатах тех или иных событий на протяжении всего срока действия контракта. По умолчанию срок жизни любого нового контракта в системе ничем не ограничен. Тем не менее при создании контракта его инициатор может задать возможность самоуничтожения, когда по прошествии определенного времени или выполнения неких условий контракт перестает существовать, а весь его ether-баланс переводиться на другой счет.