Криптовалюта без паники

Понятный гид для начинающих



Павел Красников

Павел Красников

Криптовалюта без паники

https://litres.ru/74749712
SelfPub; 2026

Аннотация

Что именно происходит, когда вы отправляете криптовалюту? Кто контролирует доступ к кошельку? Почему токен с названием «стейблкоин» не обязательно сохраняет цену, а подтверждённый блокчейном перевод не всегда можно отменить?

Эта книга простым языком объясняет основы Bitcoin и Ethereum, устройство блокчейна, различия между монетами и токенами, работу кошельков, комиссий и криптосервисов. На практических примерах читатель разберёт распространённые ошибки, мошеннические схемы и способы проверять информацию о проектах.

В книге есть словарь терминов, чек-лист безопасности, ответы для самопроверки, упражнения и план обучения на 30 дней. Для знакомства с темой не нужно покупать криптоактивы или совершать реальные переводы.

Это образовательный гид, а не инвестиционная рекомендация, руководство по быстрому заработку или юридическая и налоговая консультация. Правила и доступность сервисов зависят от страны и могут меняться.

Содержание

Введение. Зачем разбираться в криптовалюте 6
Что вы сможете сделать после чтения 8
Чего эта книга не обещает 9
Границы темы 10
Как читать книгу 11
1. Что такое криптовалюта 12
Цифровая запись, а не файл с монетой 13
Что означает слово «криптовалюта» 14
Откуда возникает доверие 15
Три слоя, которые не следует путать 16
Почему существуют криптовалюты 17
Цифровой актив и электронные деньги 18
Разбор двух учебных ситуаций 20
Кейс: один перевод — разные записи 21
Кейс: цифровой жетон и право на вещь 23
Почему баланс на экране не всегда равен контролю 24
Кому доверяет участник сети 26
Что важно запомнить 27
Вопросы для самопроверки 28
Для дальнейшего чтения 29
2. Как работает блокчейн 30
Блоки и ссылки между ними 31

Узлы и одинаковые правила 32
Как сеть договаривается о состоянии 33
Подпись и проверка права на действие 35
Транзакция — это запрос на изменение состояния 36
Публичность и конфиденциальность 37
Блокчейн не решает все задачи 38
Разбор учебных ситуаций 39
Кейс: два запроса и один доступный остаток 40
Кейс: две версии следующего блока 42
Подтверждение и финальность простыми словами 44
Как меняются правила и кто их применяет 45
Узел не обязан принимать любое мнение большинства 47
Как оценить изменение протокола 49
Вымышленный пример: два разных значения слова «одобрено» 50
Что важно запомнить 51
Вопросы для самопроверки 52
Для дальнейшего чтения 53
3. Bitcoin, Ethereum и другие проекты 54
Bitcoin: платежная сеть и единица BTC 55
Ethereum: сеть для программируемых операций 57
Сравниваем устройство, а не цены 60
Сквозной пример: Лена разбирается, что ей 62

предлагают
Базовая сеть, дополнительный уровень и сервис 64
Другие проекты: задавайте одинаковые вопросы 66
Как сеть вознаграждает участников 68
Частые путаницы 69
Что важно запомнить 70
Вопросы для самопроверки 71
Первоисточники и документация 72
4. Криптовалюта, токены и стейблкоины 73
Нативная монета сети 74
Токен 75
Стейблкоины 76
Вопросы о «привязке» 78
Токенизация реальных активов 79
Что может произойти с токеном после выпуска 80
Разные функции токенов 81
Один токен — три разных описания 82
Переводимость и погашение — не одно и то же 84
Конец ознакомительного фрагмента. 85

Павел Красников
Криптовалюта без паники

Введение. Зачем разбираться в криптовалюте

О криптовалютах легко услышать раньше, чем понять, что за ними стоит. В одном разговоре Bitcoin называют цифровыми деньгами, в другом — способом сохранить капитал, в третьем — технологией, которая изменит интернет. Рядом с серьёзными объяснениями встречаются обещания быстрой прибыли, тревожные истории о потерях и термины, которые звучат так, будто их специально придумали, чтобы отпугнуть новичка.

Эта книга поможет отделить устройство технологии от рекламных обещаний и рыночных прогнозов. Мы разберём, что именно записывает блокчейн, почему для отправки средств нужны ключи, чем отличаются сеть и актив, как работают токены и смарт-контракты, какие ошибки приводят к потере доступа и как распознавать мошеннические схемы.

Книга рассчитана на читателя без технической подготовки. Сложные вещи будут объясняться через бытовые примеры, а после важных разделов появятся вопросы для самопро-

верки. Если какой-то термин встретится впервые, его можно будет найти в словаре в конце книги.

Что вы сможете сделать после чтения

После чтения вы сможете объяснить разницу между публичной сетью, токеном и сервисом; понять, почему адрес и сеть надо проверять одновременно; распознавать ситуации, в которых кошелёк просит перевести деньги или дать контракту разрешение; отличать первичную документацию от рекламного пересказа.

Вы также сможете составить карту рисков для конкретного сценария и задать вопросы, на которые должен ответить оператор или эмитент токена. Эти навыки не требуют покупки криптоактивов. Если в конце книги вы решите, что ваша задача проще решается обычным сервисом, это тоже обоснованный результат.

Книга намеренно не приводит пошаговые инструкции по конкретным биржам и кошелькам. Интерфейсы и правила меняются. Вместо этого мы будем учиться проверять текущие инструкции и понимать, что именно скрыто за кнопкой подтверждения.

Чего эта книга не обещает

Это не инструкция по быстрому заработку и не список монет для покупки. Здесь не будет прогнозов курса, рекомендаций вложить определённую сумму или утверждений, что какая-либо технология обязательно победит. Никто не может надёжно гарантировать доходность криптоактива. Цена может резко вырасти или упасть, а сам проект — столкнуться с технической, организационной или правовой проблемой.

Образовательный материал также не заменяет индивидуальную юридическую, налоговую или финансовую консультацию. Правила, доступность сервисов и комиссии меняются в зависимости от страны и времени. Перед практическим действием проверяйте актуальные сведения у первоисточника и в официальных источниках и правилах страны, где вы находитесь.

Границы темы

Книга объясняет общие принципы публичных блокчейнов и цифровых активов, а не правовой режим конкретной страны. Условия сервиса, доступность площадок, налоговые обязанности и правила обращения с активами могут различаться и меняться. Часть материалов по безопасности и защите потребителей взята у американских органов SEC, FTC и CFTC; она иллюстрирует общие подходы и не описывает российские или иные местные правила. Перед реальным действием проверяйте официальные источники и требования страны, где вы находитесь.

Термин «криптовалюта» также используют неодинаково. В книге мы будем различать нативные монеты блокчейнов, токены, стейблкоины, кошельки и сервисы. Если в новости слово употреблено шире, сначала уточняйте, какой объект обсуждается.

Часть глав посвящена рискам, потому что они возникают не только при покупке. Даже бесплатная раздача, просмотр сайта или подписание сообщения могут раскрыть данные или дать приложению дополнительные права. Не воспринимайте учебные примеры как приглашение проверять описанное на реальных средствах.

Как читать книгу

Если вам нужен общий обзор, читайте главы по порядку. Если вы хотите понять конкретный вопрос, можно перейти сразу к нужной части: главы о кошельках и переводах рассказывают о повседневном использовании, а разделы о рисках и мошенничестве помогают выстроить защиту.

Для безопасного знакомства не нужно начинать с отправки денег. Сначала полезно научиться читать адреса, понимать разницу между сетями, находить первоисточник информации и замечать ситуации, в которых вас торопят. Практическая осторожность здесь важнее технической смелости.

Главный принцип книги прост: понимать, что именно вы делаете, кто контролирует ключи и что произойдёт, если что-то пойдёт не так. Когда эти вопросы ясны, незнакомые слова перестают быть магией. Они становятся деталями системы, которые можно изучить и оценить.

1. Что такое криптовалюта

Представьте, что вы переводите деньги знакомому через банковское приложение. Вы вводите сумму и получателя, а банк проверяет, что у вас достаточно средств, списывает их со счёта и сообщает банку получателя, что нужно зачислить перевод. В этой привычной схеме участники доверяют посредникам: банку, платёжной системе и правилам, по которым они работают.

Криптовалютная сеть предлагает другой способ вести учёт цифровых единиц. Участники используют программное обеспечение, которое проверяет правила и распространяет сведения о транзакциях между узлами сети. В некоторых системах для этого не требуется один центральный оператор, ведущий единственную базу данных. Но «без центрального оператора» не означает «без правил», «без разработчиков» или «без риска».

Цифровая запись, а не файл с монетой

Когда человек говорит «у меня есть биткоины», он обычно имеет в виду, что сеть считает определённый объём средств доступным для расходования владельцем соответствующего ключа. На компьютере не хранится отдельный файл с монетой, как фотография в папке. Кошелёк помогает управлять ключами и читать состояние сети, а сама запись о транзакциях хранится участниками блокчейна.

Это различие важно. Если устройство сломалось, средства не обязательно исчезают вместе с ним: доступ можно восстановить, если надёжно сохранены необходимые ключи или фраза восстановления. И наоборот, красивый интерфейс кошелька сам по себе не доказывает, что именно пользователь контролирует средства. Иногда ключи хранит сервис, и тогда пользователь зависит от его работы и правил.

Что означает слово «криптовалюта»

Термином часто называют сразу несколько вещей: собственную единицу блокчейн-сети, токен в смарт-контракте, стейблкоин, цифровой актив на торговой платформе или весь набор связанных с ними технологий. Для точного разговора полезно уточнять, о чём именно идёт речь.

Криптография — область математики и информатики, изучающая способы защищать информацию. В криптовалютных системах криптографические методы помогают проверять подписи и связывать данные. Они не превращают любую монету в надёжное вложение, не гарантируют честность создателей проекта и не обеспечивают защиту от обмана пользователя.

Слово «валюта» тоже может вводить в заблуждение. Некоторые активы задуманы как средство передачи ценности; другие используются для оплаты вычислений в сети, доступа к приложению или управления параметрами проекта. Даже если у токена есть рыночная цена, это не обязательно означает, что им удобно расплачиваться в магазинах или что его стоимость стабильна.

Откуда возникает доверие

В обычных платёжных системах доверие часто сосредоточено в организации, которая ведёт счёт и может отменять или исправлять операции в рамках своих правил. В открытой блокчейн-сети доверие распределяется между программным кодом, криптографическими проверками, механизмом согласования состояния сети, участниками и инфраструктурой, через которую человек взаимодействует с блокчейном.

Это не исчезновение доверия, а его другая организация. Пользователь всё ещё может зависеть от разработчиков кошелька, биржи, провайдера сети, смарт-контракта, моста между блокчейнами или человека, который объясняет ему, что подписывать. Децентрализация бывает разной степени: проект может использовать публичный блокчейн, но иметь небольшую группу разработчиков, администраторские ключи или единственную компанию-оператора.

Поэтому полезнее задавать не вопрос «децентрализован ли проект?», а несколько более точных вопросов: кто может менять правила; кто проверяет транзакции; кто может остановить сервис; у кого находятся ключи; какие действия можно отменить; откуда приложение получает информацию.

Три слоя, которые не следует путать

Чтобы не запутаться в новостях, разделяйте три уровня:

1. **Протокол и сеть.** Правила и программное обеспечение, которые определяют, какие операции действительны и как участники согласуют состояние.

2. **Актив.** Цифровая единица, связанная с сетью или приложением. У неё могут быть разные функции и разные риски.

3. **Сервис.** Биржа, кошелёк, сайт, платёжное приложение или компания, через которые человек получает доступ к активу или сети.

Например, сбой сайта биржи не всегда означает остановку блокчейна. И наоборот, сеть может продолжать работать, пока сервис, которым пользуется конкретный человек, недоступен. Цена актива, техническое состояние сети и надёжность сервиса — три отдельные вещи.

Почему существуют криптовалюты

В исходной статье о Bitcoin автор предложил систему электронных платежей между участниками сети, которая не полагается на финансовую организацию для ведения общего списка операций. Позже появились сети, предназначенные не только для передачи цифровых единиц, но и для выполнения программного кода, выпуска токенов и работы приложений.

Эти идеи привлекают людей по разным причинам: открытый доступ к сети, возможность проверять публичные записи, программируемые операции, международная передача цифровых активов. Но между технической возможностью и полезным массовым продуктом часто лежит большой путь. Система может быть интересной инженерам и при этом неудобной, дорогой или рискованной для обычного пользователя.

Цифровой актив и электронные деньги

Электронный баланс в банковском приложении и токен в блокчейне могут одинаково выглядеть как число на экране, но за этим числом стоят разные отношения. Банковский баланс — запись в системе финансовой организации и обязательство, которое регулируется условиями счёта и применимыми правилами. Криптоактив может быть записью в публичном реестре, контролируемой ключом, или внутренней записью посредника. Степень юридической защиты и возможность оспорить операцию отличаются.

Это сравнение не означает, что один способ всегда безопаснее другого. Банковская система тоже может иметь задержки, ограничения или ошибки. Криптоактив может дать больше самостоятельного контроля, но пользователь несёт дополнительные обязанности по хранению ключей и проверке адресов. Полезно выяснить не только, «где баланс», но и кто обязан вернуть средства при ошибке и по какой процедуре.

Если продукт называет актив «цифровыми деньгами», «цифровой валютой» или «электронной наличностью», спросите, кто выпускает единицы, чем они погашаются и какие права у держателя. Маркетинговое название не заменяет

этих ответов.

Разбор двух учебных ситуаций

Имена и примеры вымышлены.

Кейс: один перевод — разные записи

Представим, что Ирина хочет передать знакомому Максиму цифровую единицу. Они могут сделать это через централизованный сервис или напрямую через блокчейн-сеть. Внешне оба действия выглядят похоже: Ирина выбирает получателя, вводит сумму и нажимает кнопку. Однако за экраном могут происходить разные процессы.

В централизованном сервисе Ирина и Максим могут иметь аккаунты на одной площадке. Если Ирина нажимает «Перевести», компания вправе просто уменьшить число в её внутреннем учёте и увеличить число в учёте Максима. Публичная блокчейн-транзакция при этом может не появиться. Для пользователей перевод состоялся внутри сервиса, но они зависят от того, что оператор правильно ведёт учёт и разрешает им пользоваться своими балансами.

Если Ирина отправляет актив из собственного кошелька в публичной сети, операция должна быть подготовлена и подписана ключом, а затем передана узлам сети. После проверки её включают в блок согласно правилам этой сети. Здесь результат зависит не только от приложения-кошелька: имеют значение адрес, выбранная сеть и состояние транзакции. Интерфейс сервиса-посредника может вообще не участвовать.

Представим третий вариант: Ирина смотрит на сайт, который показывает баланс по адресу, но ключи хранит другая организация. Сайт может показывать настоящую запись сети, но Ирина не обязательно контролирует возможность распоряжаться активом. Информация о балансе и возможность подписать расходную операцию — не одно и то же.

Этот пример помогает задавать точные вопросы вместо общего «где лежат мои монеты?»: кто изменяет учётную запись; какой системе виден баланс; кто хранит ключ; где возникает запись о переводе; что именно обещал сервис. У этих вопросов могут быть разные ответы даже в приложениях с похожим дизайном.

Кейс: цифровой жетон и право на вещь

Предположим, художественный фонд выставляет на цифровом аукционе картину и выпускает токен с её фотографией и описанием: «токен представляет право собственности». Запись в блокчейне показывает, что токен можно передать между адресами. Но что именно получает покупатель при такой передаче?

Публичная запись может подтвердить, кому принадлежит токен по правилам сети, но сама по себе не подтверждает право на физическую картину, авторские права на изображение или обязанность фонда передать произведение. Для этого важны договор купли-продажи, документы о происхождении и процедура фактической передачи.

Поэтому фраза «токен — это право» требует уточнения: право на что именно, кто обязан его предоставить и где записаны условия? Блокчейн хранит запись о токене; смысл и исполнение связанного с ним обещания зависят от договора и внешних процедур.

Вопрос для читателя: какую часть обещания можно проверить непосредственно в сети, а какую — только по договору или у организации-эмитента?

Почему баланс на экране не всегда равен контролю

Слово «баланс» может означать разные записи. В самостоятельном кошельке приложение может рассчитывать сумму активов, доступных по ключам в публичной сети. На бирже баланс может быть внутренней записью аккаунта, а не отдельной транзакцией в блокчейне. В платёжном сервисе число может показывать требование клиента к оператору.

Во всех трёх случаях на экране появится сумма, но путь к ней различен. Публичная запись может быть видна всем, тогда как внутренний баланс зависит от учёта компании. Ключ может контролировать сам пользователь или хранитель. Поэтому полезно спросить: кто может распоряжаться активом, кто хранит запись и какие правила действуют, если я хочу вывести средства?

Это не означает, что внутренние балансы обязательно ненадёжны. Они могут облегчать операции и восстановление доступа. Но пользователь должен понимать, что именно ему обещает сервис и какие риски возникают, если компания задержит вывод или прекратит работу.

При чтении описания продукта попробуйте заменить слово «кошелёк» конкретным процессом: «сервис хранит ключи и показывает мой внутренний счёт» или «приложение

подписывает транзакцию моим ключом». Точная фраза часто сразу обнаруживает разницу в контроле.

Кому доверяет участник сети

В блокчейн-продукте доверие часто распределено по цепочке. Пользователь доверяет правильности программы-кошелька, точности адреса, правилам сети и тому, как приложение показывает действие. Если он использует биржу, добавляется оператор, который ведёт внутренний учёт и хранит ключи. Если приложение зависит от оракула, добавляется источник внешних данных. Если актив пришёл через мост, появляется ещё один механизм и его оператор или контракт.

Полезно нарисовать цепочку для конкретной задачи. Например, при получении токена: кто его выпускает; на каком блокчейне он существует; через какой кошелёк он отображается; какой сервис может обменять его; кто сможет остановить доступ. Такая карта не отвечает автоматически, хорош ли продукт, но показывает места, где надо искать документы, условия или независимые проверки.

Чем длиннее цепочка, тем больше возможностей для сбоя — и тем важнее выяснить, какие звенья можно проверить самостоятельно. Децентрализованный базовый протокол не означает, что интерфейс, эмитент и сторонние сервисы тоже распределены.

Что важно запомнить

Криптовалюта — не просто «цифровые деньги» и не единый продукт. Это сочетание сетевых правил, криптографических инструментов, цифровых активов и сервисов. В каждом случае важно выяснить, какая часть системы перед вами и кому вы доверяете.

Перед тем как переходить к кошелькам и транзакциям, попробуйте ответить на вопросы:

Где записано состояние актива — в базовой сети или в приложении?

Кто контролирует ключи, позволяющие распоряжаться активом?

Какую задачу решает сеть или токен?

Какой сервис является посредником и что произойдёт, если он перестанет работать?

Пока ответы неясны, действие можно отложить. В криптовалюте пауза часто оказывается самой полезной функцией.

Вопросы для самопроверки

1. Чем сеть отличается от актива и сервиса?
2. Почему слово «децентрализованный» не означает, что доверие исчезло?
3. Какие вопросы стоит задать до взаимодействия с приложением?

Для дальнейшего чтения

Сатоси Накамото, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008): https://bitcoin.org/bitcoin.pdf

Официальное введение в Ethereum: https://ethereum.org/developers/docs/intro-to-ethereum/

2. Как работает блокчейн

Блокчейн проще представить как общую книгу учёта, копии которой хранятся у многих участников. В неё последовательно добавляют новые записи. Участники проверяют, соответствует ли очередная запись правилам системы, а затем обновляют свои копии. В отличие от таблицы, которой управляет один администратор, публичная блокчейн-сеть распределяет проверку между узлами.

Это сравнение полезно, но у него есть пределы. Блокчейн — не просто электронная таблица, а система с правилами проверки, криптографическими ссылками, механизмом согласования и экономическими стимулами. Конкретные механизмы сильно различаются у разных сетей.

Блоки и ссылки между ними

Транзакции собираются в группы — блоки. В заголовке каждого блока хранится хеш предыдущего блока. Хеш можно вообразить как короткий цифровой отпечаток данных: если изменить исходное содержимое, отпечаток изменится.

Так образуется последовательность связанных блоков. Если кто-то пытается незаметно изменить старую запись, изменится хеш блока, а значит, перестанут совпадать ссылки в следующих блоках. Чтобы сеть приняла переписанную историю, атакующему пришлось бы убедить участников, проверяющих правила, принять эту версию вместо текущей. Насколько это сложно, зависит от архитектуры сети и распределения контроля.

Важно не говорить, что блокчейн абсолютно неизменяем. Точнее сказать, что уже подтверждённые записи обычно становится всё труднее изменить по мере добавления последующих блоков, если сеть работает по ожидаемым правилам. Возможны реорганизации цепочки, ошибки программного обеспечения, атаки, изменения протокола и разделение сообщества на несовместимые версии. «Неизменность» — практическое свойство при определённых условиях, а не магическое обещание.

Узлы и одинаковые правила

Узел — это программа, участвующая в сети. В зависимости от сети и роли узел может хранить данные, проверять блоки, передавать транзакции другим участникам или выполнять другие задачи. Узлы сверяют получаемые записи со своими правилами. Запись, которая нарушает правила, может быть отвергнута независимо от того, насколько убедительно её представляют.

Многие узлы не означают автоматически, что власть распределена равномерно. Важны не только число компьютеров, но и то, кто ими управляет, какие версии программ они используют, насколько легко запустить собственный узел и насколько независимы крупные участники. Если значительная часть инфраструктуры контролируется несколькими организациями, это может создавать точки концентрации влияния.

Как сеть договаривается о состоянии

Распределённой системе нужно решать, какой блок считать следующим, особенно когда сообщения приходят не мгновенно и разные участники могут одновременно предложить новые блоки. Для этого применяются механизмы консенсуса — правила, по которым сеть выбирает и подтверждает историю.

В Bitcoin используется proof of work, или доказательство выполнения работы: участники, которых называют майнерами, соревнуются в поиске подходящего результата вычислений. Это требует ресурсов, а проверка найденного результата обходится намного дешевле. В Ethereum используется proof of stake (PoS, доказательство доли): самостоятельный запуск валидатора требует внести 32 ETH в депозитный контракт и поддерживать необходимое программное обеспечение. Пулы позволяют участвовать иначе, но добавляют посредников и связанные с ними риски. Стейк обеспечивает экономический стимул соблюдать правила, а за некоторые виды недобросовестного поведения часть средств валидатора могут уничтожить. Конкретные параметры сети могут меняться, поэтому проверяйте документацию перед практическими действиями. proof of work (PoW, доказательство вы-

полнения работы) и PoS различаются по устройству, стимулам и рискам; их не стоит сводить к короткому рейтингу «лучше — хуже».

Консенсус в техническом смысле означает, что сеть достигает согласованного состояния по правилам протокола. Это не всеобщее одобрение проекта и не гарантия, что его экономическая модель разумна. Сеть может корректно исполнять программу, которая приносит пользователям убытки из-за ошибки или плохого дизайна.

Подпись и проверка права на действие

Чтобы сеть приняла транзакцию, отправителю обычно нужно доказать, что он уполномочен совершить действие. В распространённой схеме пользователь создаёт цифровую подпись с помощью закрытого ключа. Остальные участники проверяют подпись открытым ключом или адресом, не получая сам секретный ключ.

Это похоже на печать, которую можно проверить, но нельзя восстановить по её оттиску. Если закрытый ключ попал к постороннему, он может подписать операцию от имени владельца. Сеть не знает, кто человек за клавиатурой; она проверяет подпись и соблюдение правил. Поэтому украденная подпись обычно выглядит для блокчейна как действительная команда.

Ключи и кошельки подробно рассматриваются в отдельной главе. Здесь достаточно запомнить: блокчейн защищает правильность проверки подписи, но не способен отличить добровольную подпись от подписи, полученной под давлением или обманом.

Транзакция — это запрос на изменение состояния

В простом случае транзакция может передавать цифровую единицу от одного адреса к другому. В программируемой сети она может запускать код смарт-контракта: изменить баланс токена, записать данные или выполнить условие. Узлы проверяют запрос, выполняют предусмотренные правила и сохраняют новое состояние.

Транзакция не обязательно означает «перевод денег человеку». Иногда это разрешение приложению взаимодействовать с токеном, участие в голосовании, обмен через смарт-контракт или запись данных. Кошелёк показывает пользователю подпись, но интерфейс может не объяснить её последствия понятным языком. Поэтому проверяйте, что именно вы подтверждаете.

Публичность и конфиденциальность

Многие публичные блокчейны позволяют любому желающему просматривать записи. Адреса обычно не содержат имя владельца, поэтому такую систему иногда называют псевдонимной. Псевдонимность не равна полной анонимности: если адрес удаётся связать с человеком через биржу, публикацию в соцсети или анализ его операций, другие связанные действия могут стать видимыми.

Не помещайте в публичную транзакцию личную информацию в расчёте на то, что она останется скрытой. Даже если отдельное поле не содержит имени, набор метаданных может раскрыть больше, чем кажется.

Блокчейн не решает все задачи

Записи в общей базе трудно исправлять, а каждое действие требует согласования и ресурсов. Это полезно, когда нескольким сторонам нужно проверяемое общее состояние без единого владельца базы. Но для обычной системы, которой управляет одна организация и где важны скорость, конфиденциальность и простота исправления ошибок, блокчейн может оказаться лишним усложнением.

У технологии есть ограничения: пропускная способность, комиссии, задержки подтверждения, риск ошибок контрактов, сложность интерфейсов и зависимость приложений от внешних данных. Смарт-контракт сам по себе не узнает, выиграла ли команда матч или пришла ли посылка; ему нужен источник данных, которому приходится доверять.

Разбор учебных ситуаций

Примеры ниже упрощены и не описывают точный алгоритм конкретной сети.

Кейс: два запроса и один доступный остаток

Представим очень упрощённую учебную сеть. На адресе А есть одна условная единица. Почти одновременно владелец создаёт два запроса: в первом отправляет её адресату Б, во втором — адресату В. Оба запроса подписаны ключом владельца, поэтому подпись сама по себе не говорит, какой из них должен победить. Если бы сеть приняла оба, одна и та же единица была бы потрачена дважды.

Участники сети применяют общие правила к новой истории. После того как первая операция включена в выбранную историю, остатка для второй операции уже нет. Узлы, которые проверяют правила, должны отвергнуть попытку потратить тот же остаток повторно. Так возникает задача упорядочивания: сеть должна прийти к общей истории, где операция занимает определённое место.

Это и есть причина, по которой блоку недостаточно быть просто набором красивых строк. Он должен быть допустимым согласно правилам и встроенным в историю способом, который признают участники. Разные системы достигают этого по-разному; в примере выше нет описания точной процедуры конкретного блокчейна.

Также важно, что подпись подтверждает контроль над

ключом, но не объясняет намерение человека. Если обманщик заставил владельца подписать запрос, сеть может увидеть корректную подпись и всё же обработать нежелательное действие. Проверка протокола отвечает на вопрос «разрешено ли это правилами?», а не «понимал ли пользователь последствия?».

Кейс: две версии следующего блока

В распределённой сети сообщения между участниками не приходят всем одновременно. Представим, что почти в одно время два участника предлагают допустимые блоки, оба продолжающие одну и ту же предыдущую историю. Часть узлов сначала видит блок X, другая часть — блок Y. На короткое время разные участники могут считать разными кандидатами следующий блок.

Механизм консенсуса задаёт способ продолжать работу и в итоге согласовать историю по правилам конкретной сети. В сети с доказательством выполнения работы участникам приходится затрачивать вычислительные ресурсы, а другим участникам проще проверить результат. В сети с доказательством доли участия валидаторы выполняют роли по правилам, связанным с залогом и протокольными стимулами. Эти предложения намеренно упрощены: реальная логика включает дополнительные правила, и детали различаются между сетями.

Слово «консенсус» здесь не означает, что каждый человек одобряет сделку, знаком с её участниками или уверен в экономическом смысле операции. Оно описывает согласование допустимой истории между программами и участника-

ми, работающими по правилам протокола. Если программа корректно исполнила невыгодное для человека действие, согласие сети не отменяет последствий.

Подтверждение и финальность простыми словами

После того как транзакция попала в блок, она ещё не обязательно обладает одинаковой степенью окончательности во всех системах. В сетях proof of work новые блоки поверх старого делают альтернативную историю всё дороже для переписывания. Это часто называют вероятностной финальностью: уверенность повышается, но не выражается единственным универсальным числом для всех ситуаций.

В Ethereum и других сетях proof of stake протокол может использовать отдельное понятие финализированных контрольных точек. Валидаторы подтверждают историю по правилам сети; изменение финализированной записи требует нарушения экономических условий протокола и может повлечь потерю стейка. Временные проблемы связи или недостаток активных голосов могут задержать финальность.

Для пользователя практический вывод таков: слово «подтверждено» без указания сети и процедуры недостаточно. Биржа или сервис-получатель устанавливает свои требования к числу подтверждений либо финальности. Следуйте актуальным правилам получателя и не считайте первый видимый статус универсальной гарантией необратимости.

Как меняются правила и кто их применяет

У блокчейна нет одного руководителя, который вручную утверждает каждую транзакцию. Но развитие сети зависит от людей: разработчики предлагают код, операторы узлов выбирают версии, а майнеры или валидаторы действуют по правилам протокола.

Полезно разделить два уровня:

Проверка операций по действующим правилам. Узел получает блок или транзакцию и проверяет, допустимы ли они по установленной им версии протокола.

Изменение самих правил. Сообщество и операторы программ решают, принять ли новую версию клиента или иной протокольный набор.

Первое происходит автоматически в программном обеспечении. Второе включает обсуждения, выпуск кода, координацию и выбор участников. Пользователь обычно не голосует за каждый параметр напрямую, но его выбор узлов и сервисов тоже влияет на распространение изменений.

Это различие помогает ответить на вопрос «кто управляет блокчейном?». Часто ответ — не один владелец и не полное отсутствие управления, а несколько групп с разными полномочиями и интересами. Важно выяснить, кто мо-

жет предложить изменение, кто его реализует, кто должен установить новое программное обеспечение и что произойдёт, если участники не договорятся. Сети различаются: обновления могут пройти незаметно для пользователя, потребовать действий от оператора или привести к устойчивому разделению истории.

Узел не обязан принимать любое мнение большинства

В публичных сетях часто говорят о «большинстве» майнеров, валидаторов или узлов. Нужно уточнять, о каком большинстве идёт речь. Большинство вычислительной мощности, большинство застейканного капитала, большинство узлов, большинство бирж и большинство пользователей — не обязательно одни и те же участники. Их интересы могут расходиться.

В Bitcoin полный узел самостоятельно проверяет получаемые блоки по правилам своего программного обеспечения. Узел не принимает недопустимый блок только потому, что тот создан крупным майнинг-пулом. В Ethereum проверка транзакций и выбор цепочки также распределены между клиентами и валидаторами согласно своим протокольным правилам. Это не отменяет влияния крупных операторов или инфраструктуры, но показывает, почему «кто может предложить блок» и «кто определяет допустимость правил» — разные вопросы.

Для новичка полезно отличать три утверждения:

«Этот блок включён в цепочку, которую показывает мой обозреватель» — описание наблюдения.

«Крупные участники поддерживают новую версию» —

утверждение о конкретной группе и её доле.

«Всё сообщество одобрило изменение» — гораздо более широкое заявление, которому нужны ясные критерии.

Как оценить изменение протокола

Представим, что знакомый сообщает: «Завтра сеть обновляется, нужно срочно переместить токены». Прежде чем следовать инструкции, нужно понять, что означает обновление. Это может быть изменение протокола, обновление приложения, переход на новую версию кошелька, миграция контракта или просто объявление о продукте. Эти события требуют разных действий.

Откройте первичное объявление самой сети или команды клиента и найдите дату, затронутые компоненты и требования к пользователям. Уточните, нужно ли владельцу самостоятельного кошелька выполнять действие или обновление происходит на уровне узлов без участия конечного пользователя. Если речь о миграции токена, выясните, кто выпускает новую версию и как проверить правильный адрес контракта. Не подключайте кошелёк к странице, присланной в личном сообщении, только из-за слова «обновление».

Также важно проверить, кто опубликовал сообщение. Ссылка на документ разработчика может быть подлинной, но комментарий рядом с ней — чьё-то толкование. Отделяйте техническое описание изменения от инструкции, которую предлагает сторонний сайт.

Вымышленный пример: два разных значения слова «одобрено»

Проект «Север» объявляет, что пользователи одобрили предложение о снижении комиссии. На сайте голосования действительно видны тысячи голосов. Но в репозитории клиента пока нет нового правила, операторы узлов ничего не обновляли, а изменение касается только внутренней комиссии приложения. Нельзя делать вывод, что базовый протокол всей сети изменился. Уточнив предмет голосования, читатель видит, что речь идёт о настройке сервиса, а не о консенсусных правилах блокчейна.

Этот пример не говорит, что голосование было бесполезным или нечестным. Он показывает, что слово «одобрено» надо связывать с конкретным объектом: кем, каким способом и для какого уровня системы принято решение.

Что важно запомнить

Блокчейн — это способ хранить и согласовывать историю цифровых операций по общим правилам. Его свойства возникают из взаимодействия криптографии, программного обеспечения, участников и стимулов. Он повышает проверяемость некоторых операций, но не устраняет доверие, не гарантирует безопасность продукта и не отменяет человеческие ошибки.

При чтении описания проекта задайте себе вопросы: кто проверяет новые записи; какой механизм согласования используется; что требуется для изменения старой истории; кто контролирует программный код и инфраструктуру; какие данные публичны; кто предоставляет сведения из внешнего мира.

Вопросы для самопроверки

1. Зачем блоки ссылаются на предыдущие?
2. Что проверяют узлы и чего консенсус сам по себе не подтверждает?
3. Почему «неизменяемость» лучше понимать как практическое свойство при определённых условиях?

Для дальнейшего чтения

Bitcoin, исходное описание сети: https://bitcoin.org/bitcoin.pdf

Ethereum, техническое введение: https://ethereum.org/developers/docs/intro-to-ethereum/

Ethereum, proof of stake и требования к валидаторам: https://ethereum.org/developers/docs/consensus-mechanisms/pos/

Ethereum, обзор смарт-контрактов: https://ethereum.org/developers/docs/smart-contracts/

3. Bitcoin, Ethereum и другие проекты

Названия Bitcoin и Ethereum постоянно встречаются в новостях и разговорах о криптовалютах. Иногда ими называют сети, иногда цифровые активы, иногда даже компании или приложения. Чтобы разбираться в теме, полезно каждый раз уточнять, о каком слое идёт речь: о правилах сети, о токене, который учитывается в этих правилах, или о сервисе, через который человек взаимодействует с сетью.

В этой главе мы сравним Bitcoin и Ethereum как два известных, но очень разных примера. Цель сравнения — не решить, какой из них «лучше», и не оценить их рыночную цену. Мы посмотрим на задачи, устройство и ограничения каждого, а затем применим эти идеи к условной истории новичка.

Bitcoin: платежная сеть и единица BTC

В 2008 году под именем Сатоси Накамото вышла статья *Bitcoin: A Peer-to-Peer Electronic Cash System*. В ней описывалась электронная система расчётов между участниками, которая позволяет передавать платежи через сеть без того, чтобы одна финансовая организация вела единственный список транзакций. Сеть Bitcoin запустилась в 2009 году.

Здесь важно различать **Bitcoin** и **bitcoin (BTC)**. Bitcoin — это протокол, программное обеспечение и сеть участников, которые проверяют транзакции по общим правилам. BTC — цифровая единица, которую эта сеть учитывает. В обычной речи название сети и её актива часто совпадает, но при объяснении лучше называть вещи отдельно.

Bitcoin не хранит пользовательские счета так, как это делает банк. Для упрощения можно представить сеть как историю операций и набор ещё не потраченных выходов транзакций. Когда кошелёк показывает баланс, он рассчитывает, какие выходы, согласно истории блокчейна, можно потратить ключом пользователя. Техническое название такой модели — UTXO, то есть «неизрасходованные выходы транзакций».

Представим, что у Лены есть один выход номиналом 0,01 BTC. Она хочет отправить Илье 0,003 BTC. Кошелёк форми-

рует транзакцию, которая использует доступный выход как вход и создаёт новые выходы: один Илье, другой — сдача Лене. Из суммы также вычитается комиссия, если она предусмотрена транзакцией. Это не буквальный перевод монеты из одного электронного кармана в другой, а новая запись, которая указывает, какие предыдущие выходы расходуются и какие создаются. Реальная конструкция может быть сложнее, но такая аналогия помогает понять, откуда берётся баланс.

Транзакция подписывается цифровым ключом, который подтверждает право выполнить операцию. После этого её передают узлам сети. Узлы проверяют транзакцию по правилам Bitcoin, а майнеры могут включить её в блок. Майнеры соревнуются в выполнении вычислительной работы — proof of work (PoW). Когда к блоку добавляются следующие блоки, изменить уже записанную историю обычно становится сложнее. Это не означает, что риск равен нулю или что каждый перевод мгновенно окончателен: практическая уверенность растёт со временем и зависит от обстоятельств.

BTC — нативный актив сети. Он используется в транзакциях Bitcoin, а также участвует в экономических стимулах, связанных с созданием блоков и обработкой операций. Правила выпуска BTC встроены в программный протокол. Ограниченность выпуска часто называют важным свойством, но она сама по себе не гарантирует спроса, стабильной цены или дохода владельца.

Ethereum: сеть для программируемых операций

Ethereum создавался как сеть, в которой можно не только передавать нативный актив, но и исполнять программы. Такие программы называют **смарт-контрактами**. Название не означает, что это обязательно юридический договор. Это код с заданными условиями и состоянием, который исполняется в среде Ethereum.

Здесь тоже есть два близких названия: **Ethereum** — сеть и программная среда, а **ether (ETH)** — её нативный цифровой актив. ETH применяется для оплаты вычислений и операций в сети; он также используется в механизме proof of stake (PoS). Поэтому, если кто-то говорит «купить Ethereum», обычно он имеет в виду ETH, хотя технически это название актива и название сети — разные понятия.

Упрощённо Ethereum можно представить как общий вычислительный журнал. Пользователь отправляет транзакцию, а сеть проверяет её и исполняет. Обычная транзакция может передать ETH. Другая транзакция может вызвать функцию смарт-контракта: например, изменить баланс токена, выполнить обмен или записать результат голосования. Каждый узел, проверяющий соответствующую часть сети, должен прийти к согласованному результату выполнения

правил.

За вычисления платят комиссию, которая связана с количеством ресурсов, использованных операцией. В Ethereum для этих ресурсов применяется понятие gas. Простая передача и сложный вызов контракта могут требовать разного объёма вычислений. Поэтому пользователю важно смотреть не только на сумму, но и на условия транзакции и её комиссию. Размер комиссии и доступность операций меняются во времени и зависят от состояния сети.

Смарт-контракты сделали возможными разные приложения: обменные сервисы, кредитные протоколы, игровые механики, токены и цифровые предметы. Однако код исполняет только заложенную логику. Он не понимает, что «имел в виду» пользователь, не исправляет ошибку автоматически и не знает внешних фактов без отдельного источника данных. Неудачный дизайн или ошибка в контракте способны привести к блокировке либо потере активов.

Ethereum использует proof of stake. Валидаторы вносят ETH в механизм стейкинга, запускают программное обеспечение и проверяют предлагаемые блоки. Протокол поощряет корректное участие и предусматривает штрафы за некоторые виды неправильного поведения. Такой механизм отличается от майнинга Bitcoin: он опирается на заблокированный капитал и процедуры выбора и подтверждения блоков, а не на соревнование по вычислению proof of work.

Пользоваться Ethereum не означает лично быть валидато-

ром. Обычный владелец кошелька отправляет транзакции, а сеть обрабатывает их через участников и программное обеспечение протокола. Также не следует путать ETH со всеми токенами, которые работают в Ethereum. Токен, созданный смарт-контрактом, — отдельный актив со своими правилами и рисками.

Сравниваем устройство, а не цены

Bitcoin и Ethereum имеют общие элементы: криптографические подписи, публичные записи операций, сеть узлов и правила проверки. Но задачи и механизмы у них различаются.

Основной фокус. Bitcoin обычно рассматривают как сеть для передачи и учёта BTC с ограниченным набором базовых операций. Ethereum — как программируемую сеть, в которой смарт-контракты могут управлять цифровыми активами и приложениями.

Модель операций. Bitcoin использует транзакции с входами и выходами. Ethereum хранит состояние аккаунтов и контрактов; транзакция может не только передать ETH, но и вызвать код.

Согласование истории. Bitcoin использует proof of work. Ethereum Mainnet использует proof of stake.

Комиссии. В обеих сетях за операции может взиматься плата. Её размер, расчёт и зависимость от нагрузки отличаются; нельзя переносить привычки из одной сети в другую.

Приложения и токены. В Ethereum смарт-контракты — обычный способ создавать токены и приложения. В экосистеме Bitcoin тоже существуют дополнительные протоколы и уровни, но их устройство и место в системе нужно оценивать отдельно от базового протокола.

Это краткое сравнение не означает, что один проект ограничен только одной функцией или что другой автоматически удобнее. В каждом случае важно понять, на каком уровне происходит операция: в базовой сети, дополнительном протоколе, смарт-контракте, кошельке или централизованном сервисе.

Сквозной пример: Лена разбирается, что ей предлагают

Представим, что Лена хочет получить небольшой цифровой платёж от знакомого. Тот говорит: «Я отправлю тебе криптовалюту, установи кошелёк». Прежде чем нажимать на первую ссылку, Лена может разобрать предложение по слоям.

Первый вопрос — какой именно актив и сеть? Если речь о BTC, это перевод в сети Bitcoin. Если речь об ETH, это операция в Ethereum. Если знакомый называет токен в долларах или присылает тикер, этого мало: нужно узнать сеть и точный актив. Одно и то же или похожее обозначение может встречаться у разных токенов.

Второй вопрос — кто контролирует кошелёк? Если Лена регистрируется на бирже, ключи могут храниться у оператора, а отображаемый баланс будет записью внутри его сервиса. Если она создаёт самостоятельный кошелёк, контроль зависит от сохранности её ключей и фразы восстановления. Эти варианты различаются удобством и рисками.

Третий вопрос — что именно нужно сделать? Получение платежа обычно не требует от Лены сообщать закрытый (приватный) ключ, фразу восстановления или оплачивать «разблокировку входящего перевода». Ей достаточно

понять официальные реквизиты получения в поддерживаемой сети. Если же сайт просит подключить кошелёк и подписать непонятную операцию, это уже не просто «получить перевод».

Четвёртый вопрос — что она сможет подтвердить? Она может посмотреть статус транзакции в обозревателе правильной сети по идентификатору, если он у неё есть. Но сам факт появления записи не гарантирует, что токен имеет ценность или что его можно обменять. Техническое зачисление, рыночная стоимость и возможность вывести актив — разные свойства.

Этот сценарий показывает, зачем различать сеть, актив и сервис. Если Лена смешает их, она может принять токен-клон за настоящий актив, отправить адрес не той сети или доверить секрет поддельной поддержке. Если же она задаёт вопросы по одному, предложение становится понятнее, а подозрительные шаги видны раньше.

Базовая сеть, дополнительный уровень и сервис

В криптосреде часто упоминают «второй уровень» или Layer 2. Обычно так называют отдельные системы, построенные поверх базовой сети и использующие её в той или иной форме для расчётов или обеспечения безопасности. Они могут обрабатывать операции по своим правилам, а затем передавать сводные данные или доказательства в базовую сеть. Конкретная архитектура зависит от проекта: нельзя считать все решения второго уровня одинаковыми или автоматически наследующими все свойства основной сети.

Для пользователя это означает ещё один набор вопросов. Как актив перемещается между уровнями? Кто управляет мостом или механизмом вывода? Есть ли задержка перед возвратом средств? Какие данные публикуются в базовой сети? Работает ли система, если её сайт или оператор недоступен? Эти детали становятся важны, когда приложение предлагает «дешёвую сеть» или просит перевести токен через мост.

Не путайте дополнительную сеть с биржевым внутренним балансом. В обоих случаях пользователь может видеть актив в интерфейсе, но контроль и механизм учёта различаются. В одном случае речь идёт о самостоятельной сети со свои-

ми правилами и участниками; в другом — о записи в базе компании. Название сети в меню ещё не говорит, где именно лежит запись и кто контролирует вывод.

Другие проекты: задавайте одинаковые вопросы

Существует множество блокчейнов и приложений. Одни выпускают собственный нативный актив, другие создают токены поверх существующей сети, третьи предоставляют мосты или сервисы. Громкое название само по себе не объясняет, что именно создано.

Для любого проекта задавайте одинаковые вопросы:

1. Какую задачу решает сеть или приложение?
2. Что такое его нативный актив и для чего он используется?
3. Где именно работает токен и как проверить адрес его контракта?
4. Кто проверяет операции и как сеть согласует состояние?
5. Кто управляет обновлениями, ключами администратора и интерфейсом?
6. Какие внешние сервисы нужны для работы и что случится при их отказе?
7. Что из заявлений подтверждается кодом и данными, а что является обещанием команды?

Если проект использует мост, задайте дополнительные вопросы: кто блокирует исходный актив, кто выпускает его

представление в другой сети и что произойдёт при сбое моста. Перевод «между сетями» часто включает отдельную инфраструктуру, поэтому его не следует считать обычной транзакцией без дополнительных рисков.

Как сеть вознаграждает участников

Сети применяют разные экономические механизмы для обеспечения проверки. В Bitcoin майнеры соперничают за право предложить следующий блок и могут получать вознаграждение по правилам протокола вместе с комиссиями. Это не зарплата, гарантированная отдельной организацией: результат зависит от вычислительной работы, затрат и правил сети.

В Ethereum валидаторы вносят стейк и получают вознаграждения за корректную работу; при некоторых нарушениях протокол может уменьшить их стейк. Участие в пуле меняет распределение обязанностей и добавляет оператора или контракт. Поэтому слова «майнинг» и «стейкинг» обозначают разные процессы, а не одинаковые способы получать доход.

Обе модели имеют технические и экономические компромиссы. proof of work требует вычислений и энергии; proof of stake требует правил управления залогом, валидаторами и штрафами. Сравнивать их надо с учётом конкретного протокола и не делать вывод о доходности для пользователя только по факту наличия вознаграждения.

Частые путаницы

«Ethereum и ETH — одно и то же». В повседневной речи такое сокращение встречается часто, но при разборе операций важно отличать сеть от её нативного актива.

«Токен в Ethereum равен ETH». Нет. Токен — запись смарт-контракта со своими правилами. ETH может понадобиться для комиссии при взаимодействии с ним, но токен и ETH — не один актив.

«Если блокчейн работает, приложение безопасно». Нет. Сеть может корректно исполнять код уязвимого контракта. Безопасность приложения зависит от его кода, управления, интерфейса и внешних компонентов.

«Если цену называют в долларах, она стабильна». Нет. Цена на экране может быть котировкой, ориентиром или обещанием эмитента. Модель стейблкоинов и связанные риски разобраны в следующей главе.

«Большая известность означает отсутствие риска». Известность может упростить поиск информации, но не отменяет волатильность, технические ошибки, фишинг и риск сервисов.

Что важно запомнить

Bitcoin и Ethereum — не взаимозаменяемые названия для одной технологии. Bitcoin — сеть с нативным активом BTC и моделью транзакций UTXO, использующая proof of work. Ethereum — программируемая блокчейн-сеть с нативным активом ETH, аккаунтами, смарт-контрактами и механизмом proof of stake. Оба примера требуют различать сеть, актив, приложение и сервис.

Это описание помогает ориентироваться в принципах, но конкретные технические детали могут меняться с обновлениями. Перед практическим действием проверяйте актуальную документацию нужной сети и точные реквизиты. Не принимайте слова «проверено блокчейном» за гарантию ценности или безопасности продукта.

Вопросы для самопроверки

1. Чем Bitcoin как сеть отличается от BTC как актива?
2. Почему баланс BTC можно описать через неизрасходованные выходы транзакций, а не через банковский счёт?
3. Для чего Ethereum использует ETH, если в сети работают также токены?
4. В чём простое различие между proof of work в Bitcoin и proof of stake в Ethereum?
5. Почему работающий блокчейн не гарантирует, что приложение на нём безопасно?
6. Какие сведения нужно уточнить у человека, который обещает отправить вам «криптовалюту»?

Первоисточники и документация

Сатоси Накамото, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008): https://bitcoin.org/bitcoin.pdf

Bitcoin Developer Guide, транзакции и модель UTXO: https://developer.bitcoin.org/devguide/transactions.html

Bitcoin.org, частые вопросы о транзакциях и подтверждениях: https://bitcoin.org/en/faq

Ethereum.org, техническое введение в Ethereum: https://ethereum.org/developers/docs/intro-to-ethereum/

Ethereum.org, аккаунты Ethereum: https://ethereum.org/developers/docs/accounts/

Ethereum.org, транзакции: https://ethereum.org/developers/docs/transactions/

Ethereum.org, proof of stake: https://ethereum.org/developers/docs/consensus-mechanisms/pos/

4. Криптовалюта, токены и стейблкоины

В новостях слово «криптовалюта» часто используют как общий ярлык для любого цифрового актива. Но между нативной монетой блокчейна, токеном смарт-контракта и стейблкоином есть различия, которые важны и для понимания технологии, и для безопасности.

Нативная монета сети

Нативная монета — это актив, учёт которого встроен в правила базовой сети. BTC является нативным активом Bitcoin, а ETH — Ethereum. Такой актив может использоваться для оплаты комиссий и участия в механизмах сети. Это не означает, что каждый нативный актив имеет одинаковые свойства: правила выпуска, подтверждения транзакций и применения различаются.

Если приложение сообщает, что для операции нужна монета сети, выясните, в какой именно сети будет происходить действие. Похожее обозначение тикера не всегда означает один и тот же актив. Криптоактивы могут существовать в нескольких сетях в виде обёрнутых или мостовых представлений, и между ними могут быть технические и контрагентские риски.

Токен

Токен — это цифровая запись, созданная по правилам определённой платформы или смарт-контракта. На Ethereum распространён стандарт ERC-20: он задаёт интерфейс, по которому совместимые приложения могут читать текущий общий объём токенов и балансы, переводить единицы и выдавать разрешение на списание. Дополнительные функции выпуска, сжигания, замораживания или обновления зависят от конкретного контракта. Стандарт облегчает взаимодействие программ, но не проверяет, стоит ли проект доверия и имеет ли токен реальную ценность.

Токен может представлять игровую единицу, баллы, право доступа, цифровой предмет, долю в проекте или обещание, связанное с внешним активом. Что именно получает держатель, зависит от кода, документов проекта и применимых правил. Само название токена и его описание на сайте не создают автоматически юридического права или возможности обмена.

У одного проекта может быть несколько контрактов-токенов с одинаковым названием и символом. Поэтому при проверке токена важно сверять сеть и точный адрес контракта через официальные первоисточники. Поиск по одному тикеру недостаточен: похожее обозначение может использовать посторонний токен.

Стейблкоины

Стейблкоинами называют токены, дизайн которых стремится поддерживать цену около некоторого ориентира, например доллара США или другой валюты. «Стремится поддерживать» — ключевая оговорка: привязка не делает цену неизменной и не превращает токен в банковский вклад.

Упрощённо выделяют несколько моделей:

Обеспечение резервами вне блокчейна. Эмитент заявляет, что держит денежные средства или другие активы и позволяет погашать токены по установленным правилам. Пользователь зависит от эмитента, качества и ликвидности резервов, аудиторов, банков и доступности погашения.

Криптообеспечение. Контракт удерживает другие криптоактивы, иногда с избыточным обеспечением. Резкое падение стоимости залога, ошибки контрактов или перегрузка сети могут нарушить работу механизма.

Алгоритмический механизм. Система пытается удерживать цену через программные стимулы и связанный токен либо другие механизмы. Такая модель может оказаться хрупкой, особенно при потере доверия и одновременном выходе участников.

Эти названия описывают общие идеи, а не гарантию качества. Конкретная система может сочетать разные механизмы, менять условия и зависеть от централизованных органи-

заций.

Вопросы о «привязке»

Если токен заявляет привязку к валюте, задайте несколько вопросов: кто выпускает токен; как создаются и уничтожаются единицы; можно ли обменять их напрямую у эмитента и на каких условиях; где и кем хранятся резервы; кто проверяет отчётность; какие права есть у пользователей; какие риски у банков, кастодианов и блокчейна.

Цена на торговой площадке и право погашения — разные вещи. Наличие активного рынка не доказывает, что каждый держатель может потребовать у эмитента базовый актив. И наоборот, заявление о резерве не заменяет независимой проверки того, что именно хранится и насколько оно доступно.

Стейблкоин может торговаться ниже или выше ориентира, если рынок теряет уверенность, ликвидность ухудшается или возникают ограничения на обмен. Возможны блокировки адресов, сбои сети, ошибки контракта и ограничения доступа. Слова «стабильный» и «обеспеченный» следует читать как гипотезу, которую надо проверять.

Токенизация реальных активов

Иногда токен описывают как цифровое представление золота, недвижимости, облигации или другого внешнего объекта. Блокчейн может фиксировать передачу токена, но сам по себе не гарантирует, что держатель получит соответствующий объект или юридически признаваемое право на него. Для этого важны договоры, реестр собственности, хранитель актива и механизм разрешения споров.

Полезно разделять три вопроса: что записано в коде; какое обязательство дал эмитент; как это обязательство будет исполнено в реальном мире. Ответ на первый вопрос можно искать в блокчейне, на второй — в договоре и документах, а на третий — в применимом праве и фактических процедурах.

Что может произойти с токеном после выпуска

Путь токена может включать несколько этапов: контракт создаёт единицы, команда распределяет их по адресам, часть блокируется на период, часть становится доступна для передачи, а держатели взаимодействуют с приложением. Условия распределения могут быть прописаны в коде, отдельном расписании разблокировок или документах проекта.

Если токен можно сжечь, заморозить или выпустить дополнительно, выясните, кто имеет такое полномочие и как оно применяется. Администраторская функция может быть предусмотрена ради исправления ошибок или соблюдения правил, но она означает, что держатель зависит от управляющей стороны. Отсутствие такой функции тоже не гарантирует безопасность: ошибочный контракт иногда невозможно исправить.

Проверьте, какие части токена уже доступны для перемещения, а какие заблокированы. Дата разблокировки не означает, что держатели обязательно продадут активы, но она может изменить предложение на рынке. Не используйте календарь выпуска как точный прогноз цены; считайте его одним из параметров модели проекта.

Разные функции токенов

Токены могут выполнять разные функции. Одни взаимозаменяемы и используются как цифровые единицы внутри приложения. Другие имеют уникальный идентификатор и связаны с отдельным объектом. Некоторые дают возможность голосовать за предложения проекта, другие используются для оплаты комиссии или доступа к сервису.

Названия «служебный», «управленческий» и «игровой» описывают заявленную функцию, но не гарантируют, что она востребована, что держатель имеет юридически защищённое право или что актив будет ликвиден. Токен, дающий право голосовать, не обязательно даёт возможность определять все ключевые решения. Голосование может быть консультативным, а техническое исполнение — оставаться в руках администраторов.

Сначала найдите точное описание прав в коде, условиях использования и документах эмитента. Затем выясните, что можно сделать с токеном сейчас, а что заявлено только на будущее. Слова «владение», «доля» и «участие» требуют уточнения: они могут иметь техническое значение, не совпадающее с обычным юридическим пониманием.

Один токен — три разных описания

Когда человек читает о токене, перед ним могут быть сразу три разных источника. Код показывает, какие технические операции доступны и кто имеет полномочия выпускать или ограничивать токены. Документы проекта объясняют замысел: для чего актив создан, кто им пользуется и какие права ему приписывают. Договор эмитента, если он существует, может задавать юридические условия: кто вправе погасить токен, какие ограничения действуют и как подать требование.

Эти источники не заменяют друг друга. Интерфейс ERC-20 позволяет совместимым приложениям читать баланс и текущее общее предложение токенов, переводить единицы и выдавать разрешение на списание. Сам стандарт не удостоверяет, что у эмитента есть резерв, что токен погашается по номиналу или что держатель имеет юридическое требование к конкретной организации.

Можно сказать, что интерфейс стандарта делает токен удобнее для совместимых приложений, но не проверяет его экономическое содержание. Это похоже на стандартный формат файла: совместимость программ не сообщает, соответствует ли документ истине и имеет ли он юридическую

силу.

Переводимость и погашение — не одно и то же

Переводимость означает, что код сети или контракта допускает перемещение записи между адресами. Погашение означает, что держатель может обменять токен на какой-либо внешний объект, валюту или услугу по установленным условиям. Эти свойства могут сосуществовать, но одно не следует из другого.

Например, токен может свободно передаваться между адресами, но эмитент принимает заявки на погашение только от клиентов, прошедших проверку и находящихся в определённых странах. Или торговая площадка может обменивать токен на валюту, хотя сам эмитент не принимает его напрямую у всех держателей. Цена и ликвидность в таком случае зависят от рынка и правил посредника.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, купив полную легальную версию на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.