Market Talks
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 13 ИЗ 13

Мифы и реальность

Шесть вещей, в которых люди часто ошибаются насчёт блокчейнов, в обе стороны, и что на самом деле показывают факты

5 мин чтения Вопросов в тесте: 6, с ответами

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 13 ИЗ 13

Мифы и реальность

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Блокчейны не являются ни волшебством, ни мошенничеством. Они очень хороши в нескольких конкретных задачах, например в переводе ценности без посредника и в ведении общей записи, которую трудно изменить, и слабы в других. Понимание того, где что, защищает и от ажиотажа, и от огульного отрицания.

Миф 1: «Биткоин анонимен»

Реальность: он псевдонимен, как объяснялось в уроке 5. К адресам не привязаны имена, но каждый платёж между ними навсегда остаётся публичным. Как только один адрес связывают с человеком, например через биржу, которая проверила его личность, большую часть его истории можно отследить.

Наглядный случай произошёл в июне 2021 года. После атаки программы-вымогателя на Colonial Pipeline, которая нарушила поставки топлива на восточном побережье США, Министерство юстиции США проследило выкуп по блокчейну и вернуло 63,7 из 75 уплаченных биткоинов. Публичный реестр оказался плохим укрытием.

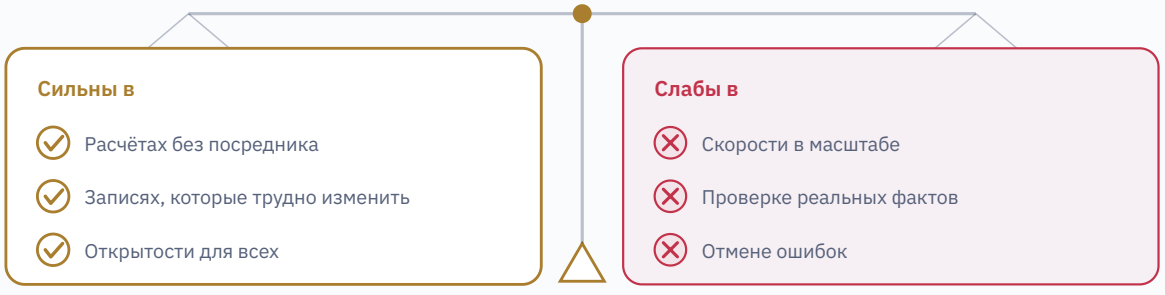


Рисунок 1. Блокчейны сильны в нескольких конкретных задачах и слабы в других. Большинство мифов возникает, когда забывают одну из сторон этих весов.

АНАЛОГИЯ: ПСЕВДОНИМ В СТЕКЛЯННОМ ДОМЕ

Представьте, что вы подписываете каждое письмо псевдонимом, но все ваши письма приколоты к стене стеклянного здания на оживлённой улице. Сначала никто не знает вашего настоящего имени. Но как только кто-то увидит, как вы вешаете одно письмо, он сможет прочитать и все остальные письма с тем же псевдонимом.

Миф 2: «Криптовалюта используется в основном для преступлений»

Реальность: преступность существует, но её доля в общей активности невелика. Аналитическая компания Chainalysis подсчитала, что незаконные адреса получили в 2025 году не менее 154 миллиардов долларов. Это огромная сумма, но всё же меньше 1% от всего отслеживаемого ею объёма криптотранзакций. Значительная часть этой суммы пришлась на обход санкций и кражи, совершённые группировками, которые поддерживают государства.

Важны обе половины. Доля мала, но суммы достаточно велики, чтобы регуляторы, биржи и банки относились к криптопреступности серьёзно. Именно поэтому биржи просят пройти проверку личности.

Миф 3: «Блокчейны невозможно взломать»

Реальность: сам реестр биткоина ни разу не был переписан, но почти всё вокруг него можно атаковать. Крупнейшие потери случаются на краях: на биржах, в кошельках, в смарт-контрактах и в **мостах**, которые переносят токены между цепочками. В марте 2022 года злоумышленники вывели около 625 миллионов долларов из моста Ronin, которым пользовалась игра Axie Infinity, получив контроль над большинством ключей, одобрявших выводы средств. Позже Министерство финансов США связало эту кражу с северокорейской группировкой Lazarus.

Второе слабое место представляют собой небольшие цепочки. Если за сетью стоит мало вычислительной мощности или мало застейканных средств, переписать последние блоки может быть по карману, это так называемая атака 51%. Безопасность зависит от того, сколько стоит обман, а эта стоимость у разных цепочек очень разная.

Миф 4: «Если это в блокчейне, значит, это правда»

Реальность: блокчейн доказывает, что запись не менялась с момента её внесения. Он не доказывает, что запись изначально была верной. Если поставщик напишет «органическое» рядом с ящиком обычных овощей, цепочка добросовестно сохранит это ложное утверждение навсегда.

Это иногда называют **проблемой оракула**: всякий раз, когда факты из реального мира, такие как цены, доставки или право собственности, попадают в блокчейн, кто-то должен о них сообщить, и этому кому-то нужно доверять. Цепочка сильнее всего тогда, когда актив целиком существует в ней, как сам биткоин.

Мифы 5 и 6: «Биткоин впустую тратит энергию» и «Блокчейны быстрые и бесплатные»

Реальность об энергии: майнинг биткоина действительно потребляет много электричества, около 138 тераватт-часов в год по данным кембриджского исследования 2025 года, то есть примерно 0,5% мирового потребления электроэнергии. То же исследование показало, что 52,4% приходилось на устойчивые источники, в основном гидроэнергию, ветер и атомную энергию. Сети на доказательстве доли, такие как Ethereum, потребляют лишь крошечную долю от этого. Стоит ли эта энергия того, остаётся предметом настоящего спора.

Реальность о скорости: публичные блокчейны медленные по своей природе, потому что тысячи компьютеров должны прийти к согласию. В основной цепочке биткоин обрабатывает лишь несколько транзакций в секунду, а комиссии растут при всплесках спроса, как показал урок 11. Поверх создаются более быстрые системы, но каждая из них идёт на компромиссы.

В чём блокчейны сильны	В чём они слабы
Перевод ценности без посредника	Скорость и стоимость в больших масштабах
Записи, которые очень трудно изменить	Проверка истинности данных из реального мира
Открыты для всех, их трудно цензурировать	Ошибки и кражи нельзя отменить
Каждый может проверить правила	Приватность, ведь всё публично

Почему это важно трейдерам

- **Мифы двигают цены.** 12 мая 2021 года Tesla перестала принимать биткоин в оплату автомобилей, сославшись на энергопотребление майнинга, и биткоин в тот день упал примерно на 12%. Истории об энергии, преступности и взломах возвращаются снова и снова, и рынки часто реагируют раньше, чем факты проверены.
- **Взломы бьют по токенам, а не всегда по цепочке.** Когда мост или биржу опустошают, затронутые токены могут обвалиться, а сама сеть продолжает работать как обычно. Прежде чем решать, что это значит для монеты, которая у вас есть, выясните, что именно атаковали.
- **Ажиотаж работает в обе стороны.** «Блокчейн всё исправит» и «блокчейн бесполезен» представляют собой одинаково лёгкие заголовки. Полезный вопрос всегда уже: нужна ли этому проекту открытая общая запись и действительно ли он её использует?

Ключевые термины

Псевдонимность	Использование адресов вместо имён. Активность публична, а личность остаётся скрытой, только пока адрес не связан с человеком.
Мост	Сервис, который переносит токены между двумя блокчейнами и часто хранит крупные суммы в одном месте, поэтому становится частой целью атак.
Атака 51%	Атака, при которой кто-то контролирует большую часть вычислительной мощности или стейка цепочки и использует это, чтобы переписать последние блоки.
Проблема оракула	Трудность переноса информации из реального мира в блокчейн без необходимости доверять тому, кто её сообщает.
Незаконный объём	Стоимость криптовалюты, полученной адресами, связанными с преступлениями, такими как мошенничество, кражи, вымогательство и обход санкций.
Доказательство доли	Способ защиты блокчейна блокировкой монет вместо майнинга, который требует гораздо меньше электроэнергии.

Главное

1. Биткоин псевдонимен, а не анонимен, и платежи можно отследить, как показало возвращение выкупа Colonial Pipeline.
2. Незаконная активность велика в долларах, но остаётся ниже 1% отслеживаемого криптообъёма.
3. Реестр биткоина ни разу не был переписан, но биржи, мосты, смарт-контракты и небольшие цепочки атакуют регулярно.
4. Блокчейн сохраняет записи неизменными, но не может проверить, были ли данные из реального мира верны в момент внесения.
5. Биткоин потребляет много энергии, а публичные цепочки медленны по своей природе. Знание настоящих сильных и слабых сторон защищает от ажиотажа в обе стороны.

Проверьте себя

Обведите один ответ на каждый вопрос. Ответы с пояснениями находятся на следующей странице. Пройти этот тест можно и онлайн на markettalks.info, сразу узнав свой результат.

1. Почему биткоин называют псевдонимным, а не анонимным?

- A Транзакции скрыты от всех, кроме майнеров
- B У адресов нет имён, но каждая транзакция публична и её можно отследить
- C Блокчейн видят только биржи
- D Пользователи должны регистрировать свои имена в блокчейне

2. Что Chainalysis выяснила о незаконной криптоактивности в 2025 году?

- A Она составляла большую часть всего криптообъёма
- B Она сократилась до нуля после новых правил
- C Она составила не менее 154 миллиардов долларов, но всё равно меньше 1% отслеживаемого объёма
- D Её нашли только в биткоине

3. Что было атаковано при взломе Ronin в марте 2022 года?

A Сам блокчейн биткоина
B Мост, через захват большинства ключей, одобрявших выводы средств
C Все кошельки Ethereum одновременно
D Оборудование майнера

4. Поставщик записывает в блокчейн ложную информацию. Что гарантирует блокчейн?

A Информация будет исправлена автоматически
B Информация верна, раз она в блокчейне
C Запись не будет изменена позже, хотя она и ложная
D Майнеры отклонят ложные данные

5. Какую примерно долю мирового потребления электроэнергии использует майнинг биткоина по данным кембриджского исследования 2025 года?

A Около 0,5%
B Около 5%
C Около 25%
D Больше половины

6. Взломан мост, в котором хранится популярный токен. Какой первый вопрос разумнее всего задать трейдеру?

A Перестал ли работать весь блокчейн?
B Нужно ли немедленно продать все свои монеты?
C Правда ли, что теперь все блокчейны небезопасны?
D Что именно атаковали и каких токенов это касается?

Ответы

1 B

У адресов нет имён, но каждая транзакция публична и её можно отследить

Реестр полностью публичен. Как только адрес связан с человеком, его прошлые платежи можно проследить, как это сделали следователи с выкупом Colonial Pipeline.

2 C

Она составила не менее 154 миллиардов долларов, но всё равно меньше 1% отслеживаемого объёма

Сумма в долларах была большой, но по сравнению со всей отслеживаемой активностью её доля осталась ниже 1%.

3 B

Мост, через захват большинства ключей, одобрявших выводы средств

Злоумышленники захватили ключи, которые одобряли выводы из моста. Сами блокчейны продолжали работать как обычно.

4 C

Запись не будет изменена позже, хотя она и ложная

Блокчейн защищает записи от последующих изменений. Он не может знать, было ли утверждение о реальном мире верным в момент внесения. Это и есть проблема оракула.

5 A

Около 0,5%

Исследование оценило потребление примерно в 138 тераватт-часов в год, около 0,5% мирового потребления электроэнергии, причём чуть больше половины приходилось на устойчивые источники.

6 D

Что именно атаковали и каких токенов это касается?

Большинство взломов бьют по сервисам вокруг цепочки, а не по самой цепочке. Понимание того, что именно атаковали, показывает, какие активы действительно под угрозой.

ИСТОЧНИКИ

- NPR, США вернули миллионы выкупа, уплаченного хакерам Colonial Pipeline (июнь 2021): https://www.kunc.org/npr-news/2021-06-07/u-s-has-recovered-some-of-the-millions-paid-in-ransom-to-colonial-pipeline-hackers
- The Block, криптопреступность в 2025 году превысила 150 млрд долларов (Chainalysis): https://www.theblock.co/post/384753/crypto-crime-150-billion-usd-2025-state-actors-scale-onchain-chainalysis
- TechCrunch, власти США связали северокорейских хакеров Lazarus с кражей 625 млн долларов из Ronin: https://techcrunch.com/2022/04/15/us-officials-link-north-korean-lazarus-hackers-to-625m-axie-infinity-crypto-theft
- Cambridge Judge Business School, доля устойчивой энергии в майнинге биткоина растёт (апрель 2025): https://jbs.cam.ac.uk/2025/cambridge-study-sustainable-energy-rising-in-bitcoin-mining/
- SiliconANGLE, цена биткоина обвалилась после отказа Tesla от платежей в биткоине (май 2021): https://siliconangle.com/2021/05/12/bitcoin-price-plunges-elon-musk-pulls-support-citing-environmental-concerns/

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Этот урок входит в бесплатный курс «Блокчейн» Образовательного центра MARKET TALKS: уроки начального, среднего и продвинутого уровней, в каждом из которых есть тест и PDF для скачивания.

Образовательный центр
Уроки от базовых принципов до продвинутых тем

Анализ рынков
Технический и фундаментальный анализ ключевых рынков

Отчёты
Биткоин, золото, серебро, SPX и другое

markettalks.info

Telegram @MARKET_TALKS

Только в образовательных целях. Ничто в этом документе не является финансовой рекомендацией. © 2026 MARKET TALKS.
Вы можете свободно делиться этим PDF без изменений.