Market Talks
ОБРАЗОВАТЕЛЬНЫЙ ЦЕНТР

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 6 ИЗ 13

Блоки и хеширование простыми словами

Короткие коды, которые скрепляют цепочку, что на самом деле лежит в блоке и почему майнинг похож на гигантскую игру в угадайку

7 мин чтения Вопросов в тесте: 6, с ответами

БЛОКЧЕЙН · НАЧАЛЬНЫЙ · УРОК 6 ИЗ 13

Блоки и хеширование простыми словами

СУТЬ В ОДНОМ ПРЕДЛОЖЕНИИ

Хеш представляет собой короткий код, вычисленный из любых данных. Стоит хоть немного изменить данные, и код меняется полностью. Каждый блок хранит хеш предыдущего, поэтому правка старой истории разрывает все последующие звенья.

Короткий код вместо любых данных

В уроке 3 мы говорили, что каждая запись в цепочке несёт цифровой отпечаток предыдущей. У этого отпечатка есть точное название: **хеш**.

Хеш-функция представляет собой вычисление, которое берёт любые данные, будь то слово, договор или целый блок транзакций, и превращает их в короткий код фиксированной длины. Хеш-функция биткоина называется **SHA-256**. Её результат всегда состоит из 64 символов: цифр от 0 до 9 и букв от a до f. Неважно, что на входе, одно слово или целая библиотека. Результат всегда занимает 64 символа.

Любой компьютер вычисляет хеш за долю секунды, и каждый, кто хеширует одни и те же данные, получает ровно тот же результат. Поэтому хеш позволяет быстро проверить, одинаковы ли две копии чего-либо, не сравнивая их строка за строкой.

ПОПРОБУЙТЕ НА НАШЕМ НАЗВАНИИ

Вот хеш SHA-256 для текста *Market Talks*:

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

А вот хеш для *Market talks*, где всего одна буква стала строчной:

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

Одно маленькое изменение, и результаты выглядят совершенно не связанными. Вы можете проверить их сами в любом бесплатном онлайн-инструменте SHA-256.

Четыре гарантии хорошей хеш-функции

- **Одни данные, один результат.** Одни и те же данные всегда дают один и тот же хеш, на любом компьютере в любой точке мира.
- **Крошечное изменение, совсем другой результат.** Замена одного символа перемешивает весь результат, как показывает пример выше. Это называется **лавинным эффектом**.
- **Только в одну сторону.** Получить хеш из данных легко. Восстановить исходные данные по хешу практически невозможно. Единственный способ найти данные под нужный хеш состоит в том, чтобы угадывать снова и снова.
- **На практике без совпадений.** Теоретически у двух разных входов может оказаться один хеш, но для SHA-256 такую пару ещё никто не нашёл. Число возможных результатов состоит из 78 цифр, это примерно столько же, сколько, по оценкам, атомов в наблюдаемой Вселенной.

Вместе эти четыре правила позволяют хешу служить печатью на данных. Если хеш совпадает, данные не менялись. Если не совпадает, что-то изменили, пусть даже одну запятую.

> **АНАЛОГИЯ: СМУЗИ**
>
> Положите в блендер банан, немного молока и пять клубничин. Любой, кто следует тому же рецепту, получит тот же смузи. Добавьте одну лишнюю клубничину, и вкус изменится. Но никто не сможет превратить смузи обратно в целый банан и пять отдельных ягод. Хеш работает так же: его легко сделать, он чувствителен к каждому ингредиенту, и его невозможно обратить вспять.

Что содержит блок

Блок биткоина состоит из двух частей. Большая часть называется **телом**: это список транзакций, обычно несколько тысяч. Меньшая часть называется **заголовком**, это краткая сводка, в которую входят:

- **Хеш предыдущего блока.** Именно эта связь превращает блоки в цепочку.
- **Сводка всех транзакций блока.** Транзакции хешируются вместе в один код, поэтому изменение любой из них меняет сводку. На среднем уровне мы покажем, как именно она строится.
- **Метка времени**, примерно показывающая, когда создан блок.
- **Целевая сложность**, которая задаёт, насколько трудна задача майнинга в данный момент.
- **Нонс**, число, которое майнеры меняют снова и снова в поисках подходящего блока. Подробнее об этом ниже.

Собственный хеш блока вычисляется из его заголовка. Поскольку заголовок содержит и сводку транзакций, и хеш предыдущего блока, этот единственный код зависит от всего содержимого блока и от всего, что было до него.

Как хеши запирают цепочку

Теперь всё складывается. Блок 102 хранит хеш блока 101. Блок 103 хранит хеш блока 102. И так далее, вплоть до генезис-блока.

Допустим, кто-то изменил одну транзакцию в блоке 101. Меняется сводка транзакций, а значит, меняется и хеш блока. Но блок 102 по-прежнему хранит старый хеш, связь между ними больше не совпадает, и любой узел сразу это видит.

Чтобы скрыть правку, злоумышленнику пришлось бы пересчитать блок 101, затем блок 102, затем каждый последующий. А как покажет следующий раздел, для создания каждого такого блока нужно огромное количество попыток угадать. Тем временем честная сеть продолжает добавлять сверху новые блоки. Вот почему платёж становится надёжнее с каждым блоком, добавленным после него.

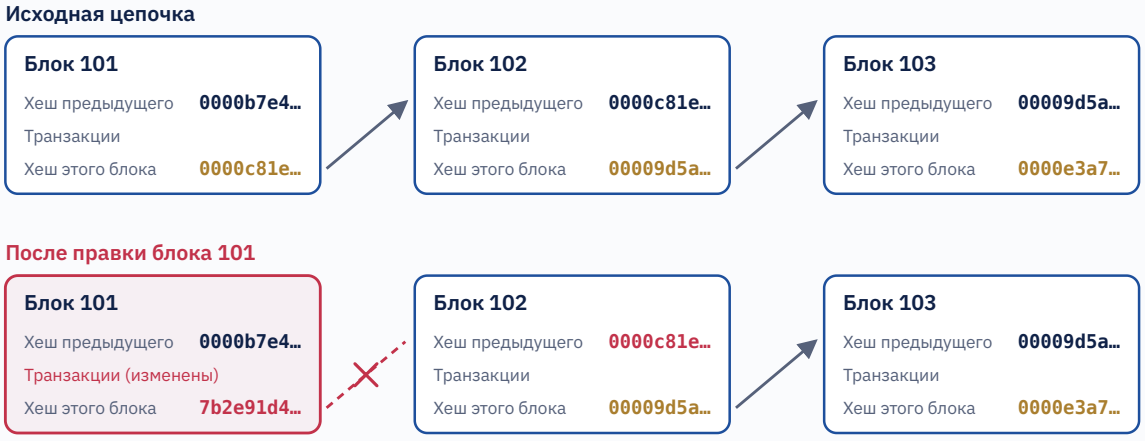


Рисунок 1. Каждый блок хранит хеш предыдущего. Правка блока 101 меняет его хеш, связь с блоком 102 перестаёт совпадать, и все видят, что цепочку подделали.

Майнинг: гигантская игра в угадайку

В уроке 4 говорилось, что майнеры соревнуются в решении задачи. Вот в чём эта задача состоит на самом деле. Чтобы блок был действительным, его хеш должен быть меньше целевого числа, заданного сетью. Проще говоря, хеш должен начинаться с определённого количества нулей.

Поскольку хеши работают только в одну сторону, хитрого способа получить хеш с множеством нулей нет. Майнеры меняют нонс, хешируют заголовок, проверяют результат и пробуют

снова, миллиарды раз в секунду. Каждый дополнительный обязательный ноль делает поиск примерно в 16 раз труднее.

Мы провели этот эксперимент сами: хешировали *Market Talks* с добавленным порядковым числом, пока результат не начинался с нужного количества нулей:

Нужно нулей	Сколько попыток понадобилось нам	Ожидаемое среднее число попыток
1	15	16
2	262	256
3	5931	4096
4	120 539	65 536
5	129 996	1 048 576
6	13 591 130	16 777 216

Обратите внимание на строку с пятью нулями: нам повезло. Майнинг похож на лотерею, и выиграть может любая отдельная попытка. Но в среднем объём работы растёт очень быстро. Самому первому блоку биткоина нужен был хеш, начинающийся с 10 нулей. Сегодняшним блокам нужно около 19 или 20, поэтому вся сеть сейчас делает около миллиарда триллионов попыток в секунду.

Почему это важно трейдерам

- **У каждой транзакции тоже есть хеш.** Он называется **идентификатором транзакции**, или TXID. Когда биржа или контрагент говорит, что платёж отправлен, попросите TXID и найдите его в блок-эксплорере. Там видно, существует ли транзакция, сколько отправлено и сколько новых блоков уже легло поверх неё.
- **Хешрейт служит показателем здоровья сети.** Хешрейт означает общее число попыток, которые сеть делает в секунду. Хешрейт биткоина впервые превысил один зеттахеш в секунду, это единица с 21 нулём, в апреле 2025 года. Растущий хешрейт означает, что майнеры вкладываются в сеть. Резкое падение, как в январе 2026 года, когда зимний шторм в США заставил майнеров отключить большую часть машин, может создать для майнеров давление.
- **Майнеры под давлением могут стать продавцами.** Майнеры платят за электричество и оборудование, часто продавая добытые биткоины. Когда их доход падает, одни продают больше, другие отключаются. Поэтому некоторые трейдеры следят за индикаторами на основе хешрейта вместе с графиками цены.

Ключевые термины

Хеш	Короткий код фиксированной длины, вычисленный из любых данных. Одни и те же данные всегда дают один и тот же хеш.
SHA-256	Хеш-функция, которую использует биткоин. Её результат всегда имеет длину 64 символа.
Лавинный эффект	Свойство, при котором крошечное изменение входных данных даёт совершенно другой хеш.
Заголовок блока	Краткая сводка в начале блока. В ней хранятся хеш предыдущего блока, сводка транзакций, метка времени и нонс.
Нонс	Число, которое майнеры многократно меняют в поисках хеша блока, удовлетворяющего целевому значению.
Хешрейт	Общее число попыток хеширования, которые сеть делает в секунду. Распространённая мера мощности майнинга.

Главное

1. Хеш представляет собой короткий код фиксированной длины, вычисленный из любых данных. Биткоин опирается на SHA-256, результаты которой имеют длину 64 символа.
2. Хорошие хеши постоянны, полностью меняются при любой правке, необратимы и на практике не повторяются.
3. Блок состоит из тела с транзакциями и заголовка, в который входят хеш предыдущего блока и сводка его транзакций.
4. Поскольку каждый блок хранит хеш предыдущего, правка старого блока разрывает все звенья после него.
5. Майнинг означает перебор нонсов, пока хеш блока не начнётся с нужного количества нулей, и каждый лишний ноль делает поиск примерно в 16 раз труднее.

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. Что делает хеш-функция?

- A Шифрует данные, чтобы их мог прочитать только владелец
- B Превращает любые данные в короткий код фиксированной длины
- C Сжимает файлы, чтобы они занимали меньше места
- D Хранит транзакции в базе данных

2. Вы изменили одну букву в документе и снова вычислили хеш. Что произойдёт с хешем?

- A Изменится на один символ
- B Останется прежним
- C Станет совершенно другим
- D Станет длиннее

3. Почему по хешу нельзя восстановить исходные данные?

A Хеш-функции работают только в одну сторону, поэтому остаётся лишь угадывать
B Сеть держит хеш в секрете
C Исходные данные удаляются после хеширования
D Ключ для обратного преобразования есть только у майнеров

4. Что связывает блок с предыдущим блоком?

A Оба блока создаёт один и тот же майнер
B У обоих блоков одинаковая метка времени
C Оба блока содержат одни и те же транзакции
D Заголовок каждого блока хранит хеш предыдущего блока

5. Что такое нонс?

A Награда, которую получает майнер
B Число, которое майнеры меняют снова и снова в поисках подходящего хеша блока
C Идентификатор транзакции
D Количество транзакций в блоке

6. Что происходит с поиском при майнинге, когда требуется ещё один ведущий ноль?

A Он становится вдвое труднее
B Ничего не меняется
C Он становится примерно в 16 раз труднее
D Он становится проще

Ответы

1 B

Превращает любые данные в короткий код фиксированной длины

Хеш-функция вычисляет короткий код фиксированной длины из любых входных данных. У SHA-256 результат всегда составляет 64 символа, каким бы ни был размер входа.

2 C

Станет совершенно другим

Это лавинный эффект. Любое изменение, даже самое маленькое, перемешивает весь результат, поэтому даже крошечные правки легко обнаружить.

3 A

Хеш-функции работают только в одну сторону, поэтому остаётся лишь угадывать

Хешировать легко в одну сторону и практически невозможно в обратную. Именно поэтому майнинг приходится вести методом проб и ошибок.

4 D

Заголовок каждого блока хранит хеш предыдущего блока

В каждом заголовке есть хеш предыдущего блока. Если старый блок изменить, его хеш изменится и перестанет совпадать с тем, что хранит следующий блок.

5 B

Число, которое майнеры меняют снова и снова в поисках подходящего хеша блока

Майнеры меняют нонс, хешируют заголовок и проверяют результат снова и снова, пока хеш не начнётся с достаточного количества нулей.

6 C

Он становится примерно в 16 раз труднее

Каждый символ хеша может принимать одно из 16 значений, поэтому ещё один обязательный ноль делает подходящий результат примерно в 16 раз реже.

ИСТОЧНИКИ

- Сатоси Накамото, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- NIST, FIPS 180-4, стандарт безопасного хеширования (SHA-256): https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog, хешрейт биткоина впервые превысил один зеттахеш (апрель 2025): https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin, хешрейт биткоина в 2026 году: тренды, сложность майнинга и безопасность сети: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

ПРОДОЛЖАЙТЕ ОБУЧЕНИЕ

Далее: урок 7
Узлы и одноранговая сеть

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.