Market Talks
教育中心

区块链 · 初级 · 第6课，共13课

区块与哈希，简单讲清楚

把链条牢牢连在一起的短代码，区块里到底装了什么，以及为什么挖矿是一场巨型猜数字游戏

阅读约7分钟　　6道测验题，附答案

区块链 · 初级 · 第6课，共13课

区块与哈希，简单讲清楚

一句话概括

哈希是从任意数据计算出的一段短代码。数据哪怕只改动一点点，代码也会完全改变。每个区块都保存着前一个区块的哈希，因此改动旧的历史会破坏其后的每一个环节。

代表任意数据的一段短代码

在第3课中我们提到，链中的每条记录都带着前一条记录的数字指纹。这个指纹有一个正式的名字：**哈希**（hash）。

哈希函数是一种计算方法：它接收任意数据，可以是一个单词、一份合同，或是一整个区块的交易，并把它变成一段长度固定的短代码。比特币的哈希函数叫作**SHA-256**，它的结果永远是64个字符，由数字0到9和字母a到f组成。无论输入是一个词还是一整座图书馆，结果始终是64个字符。

任何电脑都能在不到一秒的时间内算出哈希，而且每个人对同样的数据计算哈希，得到的结果都完全相同。因此，哈希是检查两份东西是否完全一致的快捷方法，不必逐行比对。

用我们的名字试试

这是文本*Market Talks*的SHA-256哈希：

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

这是*Market talks*的哈希，只把一个字母改成了小写：

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

一个小小的改动，结果却看不出任何关联。你可以用任意免费的在线SHA-256工具亲自验证。

好的哈希函数保证的四件事

- **输入相同，输出相同。**同样的数据永远得到同样的哈希，无论在哪台电脑上、在世界的哪个角落。
- **微小改动，结果全变。**只改一个字符，整个结果就会被打乱，正如上面的例子所示。这被称为**雪崩效应**。
- **只能单向。**从数据算出哈希很容易，从哈希还原出原始数据则几乎不可能。想找到与某个哈希对应的输入，唯一的办法就是一次又一次地猜。

- **实际上不会重复。**理论上两个不同的输入可能得到同一个哈希，但对于SHA-256，至今没有人找到过这样的一对。可能结果的数量是一个78位数，大约相当于可观测宇宙中原子的估计数量。

这四条规则合在一起，使哈希可以像封条一样保护数据。哈希依然吻合，说明数据没有变；不吻合，说明有东西被改了，哪怕只是一个逗号。

> **类比：奶昔**
>
> 把一根香蕉、一些牛奶和五颗草莓放进搅拌机。任何人照同样的配方，都会得到同样的奶昔。多加一颗草莓，味道就变了。但没有人能把奶昔变回一整根香蕉和五颗完整的草莓。哈希也是如此：做起来容易，对每一种原料都很敏感，而且无法还原。

一个区块里有什么

一个比特币区块由两部分组成。较大的部分是**区块体**：一份交易清单，通常有几千笔。较小的部分是**区块头**，一份简短的摘要，其中包括：

- **前一个区块的哈希。**正是这个链接让区块连成了链。
- **本区块全部交易的摘要。**所有交易被一起哈希成一个代码，所以改动其中任何一笔都会改变这个摘要。中级阶段会具体展示这个摘要是如何生成的。
- **时间戳**，大致表明区块创建的时间。
- **难度目标**，决定当时挖矿谜题的难度。
- **随机数**（nonce），矿工在寻找有效区块时一次又一次修改的数字。下文会详细说明。

区块自身的哈希由区块头计算而来。由于区块头既包含交易摘要，也包含前一个区块的哈希，这一个代码就同时取决于区块里的一切以及之前的一切。

哈希如何锁住整条链

现在各个部分拼到了一起。区块102保存着区块101的哈希，区块103保存着区块102的哈希，依此类推，一直到创世区块。

假设有人改动了区块101中的一笔交易。它的交易摘要会变，于是它的哈希也会变。但区块102保存的仍是旧的哈希，两者之间的链接就对不上了，每个节点都能立刻发现。

为了掩盖这次改动，攻击者必须重新计算区块101，再计算区块102，然后是之后的每一个区块。而正如下一节所示，生成每一个这样的区块都需要海量的猜测。与此同时，诚实的网络还在不断往上添加新区块。这就是为什么一笔支付之后每多一个区块，它就更安全一分。



图1. 每个区块都保存着前一个区块的哈希。改动区块101会改变它的哈希，与区块102的链接就对不上了，所有人都能看出链被篡改过。

挖矿：一场巨型猜数字游戏

第4课说过，矿工们竞相解一道谜题。下面就是这道谜题的真面目：一个区块要有效，它的哈希必须低于网络设定的目标数值，简单来说，就是哈希必须以一定数量的零开头。

由于哈希只能单向计算，没有任何巧妙的办法能直接造出一个开头有很多零的哈希。矿工只能修改随机数、对区块头做哈希、检查结果，然后再试，每秒数十亿次。每多要求一个零，搜索难度就增加约16倍。

我们亲自做了这个实验：在*Market Talks*后面加上一个递增的数字进行哈希，直到结果以足够多的零开头：

要求的零的个数	我们实际猜了多少次	平均预期次数
1	15	16
2	262	256
3	5,931	4,096
4	120,539	65,536
5	129,996	1,048,576
6	13,591,130	16,777,216

注意五个零那一行：我们运气不错。挖矿就像抽奖，任何一次猜测都可能中奖。但平均来看，工作量增长得非常快。比特币的第一个区块需要一个以10个零开头的哈希，如今的区块需要大约19到20个零，这就是为什么整个网络现在每秒要进行大约十万亿亿次猜测。

这对交易者为何重要

- **每笔交易也有一个哈希。**它叫作**交易ID**，即TXID。当交易所或交易对手说款项已经发出时，向对方要TXID，并在区块浏览器上查询。你能看到这笔交易是否存在、发送了多少，以及它上面已经叠加了多少个新区块。
- **算力是网络的健康信号。**算力（hashrate）是网络每秒进行的猜测总次数。比特币算力在2025年4月首次突破每秒1泽哈希，也就是1后面跟21个零。算力上升意味着矿工在加大对网络的投入。突然下跌，例如2026年1月美国一场冬季风暴迫使矿工关掉了大量机器，则可能让矿工承受压力。
- **承压的矿工可能变成卖家。**矿工需要支付电费和设备费用，往往靠卖出挖到的比特币来支付。收入下降时，有些矿工会卖得更多，或者干脆关机。这就是为什么有些交易者会在看价格图表的同时，关注基于算力的指标。

关键术语

哈希	从任意数据计算出的一段长度固定的短代码。同样的数据总是得到同样的哈希。
SHA-256	比特币使用的哈希函数。它的结果总是64个字符长。
雪崩效应	输入的微小变化会产生完全不同的哈希的特性。
区块头	区块开头的简短摘要，包含前一个区块的哈希、交易摘要、时间戳和随机数。
随机数（nonce）	矿工为寻找符合目标的区块哈希而反复修改的数字。
算力	网络每秒进行的哈希猜测总次数，是衡量挖矿力量的常用指标。

要点总结

1. 哈希是从任意数据计算出的长度固定的短代码。比特币依赖SHA-256，其结果长度为64个字符。
2. 好的哈希结果稳定，任何改动都会让它完全改变，无法逆推，而且在实际中不会重复。
3. 区块由交易组成的区块体和区块头构成，区块头包含前一个区块的哈希和本区块交易的摘要。
4. 由于每个区块都保存着前一个区块的哈希，改动一个旧区块会破坏其后的每一个环节。

5. 挖矿就是不断猜随机数，直到区块哈希以足够多的零开头，而每多一个零，搜索难度就增加约16倍。

自我测验

请为每道题圈出一个答案。答案及解释在下一页。您也可以在 markettalks.info 在线完成此测验，并立即查看得分。

1. 哈希函数的作用是什么？

- A 加密数据，只有所有者才能读取
- B 把任意数据变成一段长度固定的短代码
- C 压缩文件，让它们占用更少空间
- D 把交易存进数据库

2. 你改动了文档中的一个字母，然后重新计算哈希。哈希会怎样？

- A 改变一个字符
- B 保持不变
- C 变得完全不同
- D 变得更长

3. 为什么无法从哈希逆推出原始数据？

- A 哈希函数是单向的，只能靠猜
- B 网络对哈希保密
- C 原始数据在哈希后会被删除
- D 只有矿工拥有逆推的密钥

4. 是什么把一个区块和前一个区块连接起来？

- A 两个区块由同一位矿工创建
- B 两个区块的时间戳相同
- C 两个区块包含相同的交易
- D 每个区块的区块头都保存着前一个区块的哈希

5. 随机数（nonce）是什么?

A 矿工获得的奖励

B 矿工在寻找有效区块哈希时反复修改的数字

C 交易的ID

D 区块中的交易数量

6. 每多要求一个开头的零，挖矿搜索会发生什么变化?

A 难度变为两倍

B 没有变化

C 难度增加约16倍

D 变得更容易

答案与解释

1 B

把任意数据变成一段长度固定的短代码

哈希函数从任意输入计算出一段长度固定的短代码。使用SHA-256时，无论输入多大，结果总是64个字符。

2 C

变得完全不同

这就是雪崩效应。任何改动，无论多小，都会打乱整个结果，所以即使极小的修改也很容易被发现。

3 A

哈希函数是单向的，只能靠猜

哈希在一个方向上很容易，反方向则几乎不可能。正因如此，挖矿只能靠反复试错。

4 D

每个区块的区块头都保存着前一个区块的哈希

每个区块头都包含前一个区块的哈希。如果旧区块被改动，它的哈希就会变化，与下一个区块保存的哈希不再吻合。

5 B

矿工在寻找有效区块哈希时反复修改的数字

矿工修改随机数、对区块头做哈希并检查结果，如此反复，直到哈希以足够多的零开头。

6 C

难度增加约16倍

哈希的每个字符都有16种可能的取值，所以多要求一个零，有效结果的出现概率就会降低约16倍。

资料来源

- 中本聪，Bitcoin: A Peer-to-Peer Electronic Cash System（2008）: https://bitcoin.org/bitcoin.pdf
- NIST，FIPS 180-4安全哈希标准（SHA-256）: https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog，比特币算力首次突破1泽哈希（2025年4月）: https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin，2026年比特币算力：趋势、挖矿难度与网络安全: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

继续学习

下一课：第7课
节点与点对点网络

本课属于 MARKET TALKS 教育中心免费的区块链课程，涵盖初级、中级和高级课程，每课都配有测验和可下载的PDF。

教育中心
从基本原理到高级主题的课程

市场分析
主要市场的技术面与基本面分析

报告
比特币、黄金、白银、SPX等

markettalks.info

Telegram @MARKET_TALKS

仅供教育用途。本文件的任何内容均不构成投资建议。© 2026 MARKET TALKS。欢迎在不作修改的前提下分享本PDF。