Market Talks
교육 센터

블록체인 · 초급 · 13강 중 6강

# 블록과 해시, 쉽게 풀어 보기

체인을 단단히 묶어 주는 짧은 코드, 블록 안에 실제로 들어 있는 것, 그리고 채굴이 거대한 추측 게임인 이유

읽는 시간 7분  퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 6강

# 블록과 해시, 쉽게 풀어 보기

한 문장 요약

해시는 어떤 데이터에서든 계산해 낸 짧은 코드입니다. 데이터가 조금만 바뀌어도 코드는 완전히 달라집니다. 각 블록은 이전 블록의 해시를 저장하므로, 과거 기록을 고치면 그 뒤의 모든 연결 고리가 끊어집니다.

## 어떤 데이터든 대신하는 짧은 코드

3강에서 우리는 체인의 각 기록이 바로 앞 기록의 디지털 지문을 담고 있다고 했습니다. 이 지문에는 정식 이름이 있습니다. 바로 **해시**(hash)입니다.

**해시 함수**는 단어 하나, 계약서 한 장, 혹은 거래가 가득 담긴 블록 하나까지 어떤 데이터든 받아서 길이가 고정된 짧은 코드로 바꾸는 계산입니다. 비트코인의 해시 함수는 **SHA-256**이라고 합니다. 그 결과는 항상 0부터 9까지의 숫자와 a부터 f까지의 글자로 이루어진 64자입니다. 입력이 단어 하나든 도서관 전체든 상관없이 결과는 언제나 64자입니다.

어떤 컴퓨터든 1초도 안 되어 해시를 계산할 수 있고, 같은 데이터를 해시하면 누구나 정확히 같은 결과를 얻습니다. 그래서 해시는 두 사본이 완전히 같은지 한 줄씩 비교하지 않고도 빠르게 확인하는 방법이 됩니다.

우리 이름으로 해 보기

다음은 *Market Talks*라는 글자의 SHA-256 해시입니다.

`16e127cc0d60a230a1f1f80040012fc10164f835b2a99ab8f42b2ea457d9964c`

그리고 다음은 한 글자만 소문자로 바꾼 *Market talks*의 해시입니다.

`79eaca857fb12aa6db2d1ab5c896ae9a3241eb2c96f99dd0640f2c6517a5a972`

작은 변화 하나에 두 결과는 전혀 관련이 없어 보입니다. 무료 온라인 SHA-256 도구로 직접 확인해 볼 수 있습니다.

## 좋은 해시 함수가 보장하는 네 가지

- **같은 입력, 같은 결과.** 같은 데이터는 어느 컴퓨터에서, 세계 어디에서 계산하든 항상 같은 해시를 냅니다.
- **작은 변화, 완전히 다른 결과.** 글자 하나만 바꿔도 결과 전체가 뒤섞입니다. 위의 예가 바로 그렇습니다. 이를 **눈사태 효과**라고 합니다.

- **한 방향으로만.** 데이터에서 해시를 구하기는 쉽습니다. 해시에서 원래 데이터를 되찾기는 사실상 불가능합니다. 어떤 해시와 맞는 입력을 찾는 유일한 방법은 계속해서 추측하는 것뿐입니다.
- **현실적으로 겹치지 않음.** 이론상으로는 서로 다른 두 입력이 같은 해시를 가질 수 있지만, SHA-256에서 그런 쌍을 찾은 사람은 아직 없습니다. 가능한 결과의 수는 78자리 숫자로, 관측 가능한 우주에 있는 원자 수의 추정치와 비슷한 규모입니다.

이 네 가지 규칙이 합쳐지면 해시는 데이터 위에 찍힌 봉인처럼 작동합니다. 해시가 여전히 일치하면 데이터는 바뀌지 않은 것입니다. 일치하지 않으면 쉼표 하나라도 무언가가 바뀐 것입니다.

> **비유: 스무디**
>
> 믹서기에 바나나 하나, 우유 약간, 딸기 다섯 개를 넣어 보세요. 같은 레시피를 따르면 누구나 같은 스무디를 얻습니다. 딸기 하나만 더 넣어도 맛이 달라집니다. 하지만 스무디를 다시 바나나 한 개와 딸기 다섯 개로 되돌릴 수 있는 사람은 없습니다. 해시도 마찬가지입니다. 만들기 쉽고, 재료 하나하나에 민감하며, 되돌릴 수 없습니다.

## 블록에 담기는 것

비트코인 블록은 두 부분으로 이루어집니다. 더 큰 부분은 **본문**으로, 보통 수천 건에 이르는 거래 목록입니다. 더 작은 부분은 **헤더**로, 다음 내용을 담은 짧은 요약입니다.

- **이전 블록의 해시.** 블록들을 체인으로 만드는 연결 고리입니다.
- **모든 거래의 요약.** 거래들을 함께 해시해 하나의 코드로 만들기 때문에, 그중 하나만 바뀌어도 요약이 바뀝니다. 이 요약이 정확히 어떻게 만들어지는지는 중급 과정에서 보여 드립니다.
- **타임스탬프**, 블록이 대략 언제 만들어졌는지 보여 줍니다.
- **난이도 목표**, 그 시점의 채굴 퍼즐이 얼마나 어려운지 정합니다.
- **논스**(nonce), 채굴자들이 유효한 블록을 찾는 동안 계속 바꾸는 숫자입니다. 아래에서 자세히 설명합니다.

블록 자체의 해시는 헤더로 계산합니다. 헤더에는 거래 요약과 이전 블록의 해시가 모두 들어 있으므로, 이 코드 하나가 블록 안의 모든 것과 그 이전의 모든 것에 좌우됩니다.

## 해시가 체인을 잠그는 방법

이제 조각들이 맞춰집니다. 블록 102는 블록 101의 해시를 저장합니다. 블록 103은 블록 102의 해시를 저장합니다. 이렇게 제네시스 블록까지 거슬러 올라갑니다.

누군가 블록 101의 거래 하나를 고쳤다고 해 봅시다. 거래 요약이 바뀌니 블록의 해시도 바뀝니다. 그런데 블록 102에는 여전히 예전 해시가 저장되어 있어 둘 사이의 연결이 더 이상 맞지 않고, 모든 노드가 즉시 이를 알아챕

니다.

수정을 숨기려면 공격자는 블록 101을 다시 계산하고, 이어서 블록 102, 그리고 그 뒤의 모든 블록을 다시 계산해야 합니다. 다음 절에서 보듯이 그런 블록을 하나 만드는 데에도 엄청난 양의 추측이 필요합니다. 그동안 정직한 네트워크는 그 위에 새 블록을 계속 쌓아 갑니다. 그래서 결제는 그 뒤에 블록이 하나씩 추가될 때마다 더 안전해집니다.




그림 1. 각 블록은 바로 앞 블록의 해시를 저장합니다. 블록 101을 고치면 해시가 바뀌어 블록 102와의 연결이 맞지 않게 되고, 누구나 체인이 조작되었음을 알 수 있습니다.

## 채굴: 거대한 추측 게임

4강에서 채굴자들이 퍼즐을 풀기 위해 경쟁한다고 했습니다. 그 퍼즐의 실체는 이렇습니다. 블록이 유효하려면 블록의 해시가 네트워크가 정한 목표값보다 작아야 하는데, 쉽게 말해 해시가 일정한 개수의 0으로 시작해야 한다는 뜻입니다.

해시는 한 방향으로만 계산되므로, 0이 많은 해시를 만들어 내는 요령 같은 것은 없습니다. 채굴자들은 논스를 바꾸고, 헤더를 해시하고, 결과를 확인하고, 다시 시도하기를 초당 수십억 번 반복합니다. 필요한 0이 하나 늘어날 때마다 탐색은 약 16배 어려워집니다.

우리는 이 실험을 직접 해 보았습니다. *Market Talks* 뒤에 하나씩 커지는 숫자를 붙여 해시하면서, 결과가 충분한 개수의 0으로 시작할 때까지 반복했습니다.

| 필요한 0의 개수 | 실제로 걸린 추측 횟수 | 평균 기대 추측 횟수 |
|---|---|---|
| **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 |

0이 다섯 개인 줄을 보세요. 운이 좋았습니다. 채굴은 복권과 같아서 어떤 추측이든 당첨될 수 있습니다. 하지만 평균적으로 작업량은 아주 빠르게 늘어납니다. 비트코인의 맨 첫 블록은 0이 10개로 시작하는 해시가 필요했습니다. 오늘날의 블록에는 약 19개나 20개가 필요하며, 그래서 지금 네트워크 전체는 초당 약 10해 번의 추측을 하고 있습니다.

## 트레이더에게 왜 중요한가

- **모든 거래에도 해시가 있습니다.** 이를 **거래 ID**, 즉 TXID라고 합니다. 거래소나 거래 상대방이 송금했다고 말하면 TXID를 요청해 블록 탐색기에서 찾아보세요. 거래가 실제로 있는지, 얼마가 보내졌는지, 그 위에 새 블록이 몇 개나 쌓였는지 확인할 수 있습니다.
- **해시레이트는 건강 신호입니다.** 해시레이트는 네트워크가 초당 하는 추측의 총 횟수입니다. 비트코인의 해시레이트는 2025년 4월 처음으로 초당 1제타해시, 즉 1 뒤에 0이 21개 붙은 수를 넘어섰습니다. 해시레이트가 오르면 채굴자들이 네트워크에 투자하고 있다는 뜻입니다. 2026년 1월 미국의 겨울 폭풍으로 채굴자들이 장비의 상당 부분을 꺼야 했던 것처럼 갑자기 떨어지면 채굴자들이 압박을 받을 수 있습니다.
- **압박받는 채굴자는 매도자가 될 수 있습니다.** 채굴자들은 전기료와 장비 비용을 대개 채굴한 비트코인을 팔아서 냅니다. 수입이 줄면 일부는 더 많이 팔거나 장비를 끕니다. 그래서 일부 트레이더는 가격 차트와 함께 해시레이트 기반 지표도 지켜봅니다.

## 핵심 용어

**해시** 어떤 데이터에서든 계산해 낸, 길이가 고정된 짧은 코드. 같은 데이터는 항상 같은 해시를 냅니다.

| | |
|---|---|
| **SHA-256** | 비트코인이 쓰는 해시 함수. 결과는 항상 64자입니다. |
| **눈사태 효과** | 입력이 아주 조금만 바뀌어도 완전히 다른 해시가 나오는 성질. |
| **블록 헤더** | 블록 맨 앞의 짧은 요약. 이전 블록의 해시, 거래 요약, 타임스탬프, 논스가 들어 있습니다. |
| **논스** | 목표를 만족하는 블록 해시를 찾는 동안 채굴자들이 거듭 바꾸는 숫자. |
| **해시레이트** | 네트워크가 초당 하는 해시 추측의 총 횟수. 채굴 능력을 재는 흔한 척도입니다. |

## 핵심 정리

1. 해시는 어떤 데이터에서든 계산해 낸, 길이가 고정된 짧은 코드입니다. 비트코인은 결과가 64자인 SHA-256에 의존합니다.
2. 좋은 해시는 일관되고, 어떤 수정에도 완전히 바뀌며, 되돌릴 수 없고, 현실적으로 겹치지 않습니다.
3. 블록은 거래로 이루어진 본문과, 이전 블록의 해시 및 거래 요약을 담은 헤더로 구성됩니다.
4. 각 블록이 바로 앞 블록의 해시를 저장하므로, 오래된 블록을 고치면 그 뒤의 모든 연결 고리가 끊어집니다.
5. 채굴은 블록 해시가 충분한 개수의 0으로 시작할 때까지 논스를 추측하는 일이며, 0이 하나 늘 때마다 탐색은 약 16배 어려워집니다.

## 실력 점검

각 문제에 답을 하나씩 표시하세요. 해설이 포함된 정답은 다음 페이지에 있습니다. markettalks.info에서 온라인으로 퀴즈를 풀고 바로 점수를 확인할 수도 있습니다.

**1. 해시 함수는 무엇을 하나요?**

- A 주인만 읽을 수 있도록 데이터를 암호화한다
- B 어떤 데이터든 길이가 고정된 짧은 코드로 바꾼다
- C 파일을 압축해 공간을 덜 차지하게 한다
- D 거래를 데이터베이스에 저장한다

**2. 문서의 글자 하나를 바꾸고 다시 해시하면 해시는 어떻게 되나요?**

A 한 글자만 바뀐다
B 그대로다
C 완전히 달라진다
D 길어진다

**3. 해시에서 원래 데이터로 거꾸로 돌아갈 수 없는 이유는 무엇인가요?**

A 해시 함수는 한 방향으로만 작동해서 추측하는 수밖에 없다
B 네트워크가 해시를 비밀로 지킨다
C 해시한 뒤 원래 데이터가 삭제된다
D 채굴자만 되돌리는 열쇠를 가지고 있다

**4. 한 블록을 바로 앞 블록과 연결해 주는 것은 무엇인가요?**

A 같은 채굴자가 두 블록을 만든다
B 두 블록의 타임스탬프가 같다
C 두 블록에 같은 거래가 들어 있다
D 각 블록의 헤더에 이전 블록의 해시가 저장되어 있다

**5. 논스란 무엇인가요?**

A 채굴자가 받는 보상
B 유효한 블록 해시를 찾는 동안 채굴자들이 계속 바꾸는 숫자
C 거래의 ID
D 블록에 담긴 거래의 수

**6. 맨 앞에 필요한 0이 하나 늘어날 때마다 채굴 탐색은 어떻게 되나요?**

A 두 배 어려워진다
B 변하지 않는다
C 약 16배 어려워진다
D 더 쉬워진다

# 정답 및 해설

1 B

**어떤 데이터든 길이가 고정된 짧은 코드로 바꾼다**

해시 함수는 어떤 입력이든 길이가 고정된 짧은 코드로 계산합니다. SHA-256에서는 입력 크기와 상관없이 결과가 항상 64자입니다.

2 C

**완전히 달라진다**

이것이 눈사태 효과입니다. 아무리 작은 변화라도 결과 전체를 뒤섞기 때문에, 아주 작은 수정도 쉽게 알아챌 수 있습니다.

3 A

**해시 함수는 한 방향으로만 작동해서 추측하는 수밖에 없다**

해시는 한 방향으로는 쉽고 반대 방향으로는 사실상 불가능합니다. 바로 그 때문에 채굴은 시행착오로 할 수밖에 없습니다.

4 D

**각 블록의 헤더에 이전 블록의 해시가 저장되어 있다**

모든 헤더에는 이전 블록의 해시가 들어 있습니다. 오래된 블록을 고치면 그 해시가 바뀌어 다음 블록에 저장된 값과 더 이상 맞지 않습니다.

5 B

**유효한 블록 해시를 찾는 동안 채굴자들이 계속 바꾸는 숫자**

채굴자들은 논스를 바꾸고, 헤더를 해시하고, 결과를 확인하는 일을 해시가 충분한 개수의 0으로 시작할 때까지 반복합니다.

6 C

**약 16배 어려워진다**

해시의 각 글자는 16가지 값 중 하나가 될 수 있으므로, 0이 하나 더 필요해지면 유효한 결과가 약 16배 드물어집니다.

출처


- 사토시 나카모토, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- NIST, FIPS 180-4 보안 해시 표준 (SHA-256): https://csrc.nist.gov/files/pubs/fips/180-4/final/docs/fips180-4.pdf
- Forklog, 비트코인 해시레이트 처음으로 1제타해시 돌파 (2025년 4월): https://forklog.com/en/bitcoin-hashrate-surpasses-one-zettahash-for-the-first-time/
- KuCoin, 2026년 비트코인 해시레이트: 추세, 채굴 난이도, 네트워크 보안: https://www.kucoin.com/blog/in-bitcoin-hashrate-in-2026-latest-trends-mining-difficulty-network-security-analysis

Market Talks

계속 학습하기

# 다음: 7강
# 노드와 P2P 네트워크

이 강의는 MARKET TALKS 교육 센터의 무료 블록체인 과정에 속합니다. 초급, 중급, 고급 강의로 구성되며 강의마다 퀴즈와 다운로드 가능한 PDF가 제공됩니다.

**교육 센터**
기초 원리부터 고급 주제까지 다루는 강의

**시장 분석**
주요 시장에 대한 기술적 분석과 기본적 분석

**리포트**
비트코인, 금, 은, SPX 등

**markettalks.info**

텔레그램 @MARKET_TALKS

교육 목적으로만 제공됩니다. 이 문서의 어떤 내용도 투자 조언이 아닙니다. © 2026 MARKET TALKS. 이 PDF는 수정 없이 자유롭게 공유하실 수 있습니다.