Market Talks
교육 센터

블록체인 · 초급 · 13강 중 5강

블록체인이란 정확히 무엇인가

쉬운 정의, 모든 블록체인이 가진 세 가지 구성 요소, 그리고 사실이 아닌 흔한 주장들

읽는 시간 7분 퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 5강

블록체인이란 정확히 무엇인가

한 문장 요약

블록체인은 수많은 독립된 컴퓨터가 함께 관리하는 거래 기록입니다. 새 항목은 서로 연결된 묶음으로 추가되고, 오래된 항목은 몰래 바꿀 수 없으며, 무엇을 넣을지는 회사가 아니라 공유된 규칙이 결정합니다.

실제로 쓸 수 있는 정의

지난 네 강의에서 우리는 하나의 문제와 그 해결책을 찾는 긴 여정을 따라왔습니다. 이제 그 해결책에 제대로 이름을 붙일 수 있습니다. 과장을 걷어 내면 블록체인은 이렇습니다.

수많은 독립된 컴퓨터가 함께 관리하는 거래 기록으로, 새 항목은 서로 연결된 묶음으로 추가되고, 오래된 항목은 몰래 바꿀 수 없으며, 무엇을 추가할지는 공유된 규칙이 정합니다.

이 문장의 모든 부분이 중요합니다. '수많은 독립된 컴퓨터'는 1강의 중개자를 없애는 부분입니다. '서로 연결된 묶음'은 3강의 타임스탬프 연구에서 나온 블록의 사슬입니다. '공유된 규칙'은 4강에서 본 합의 방식입니다. 이 중 하나라도 빠지면, 비트코인이 처음 선보인 의미의 블록체인이라고 할 수 없습니다.

이런 종류의 기록을 **원장**(ledger)이라고 합니다. 누가 누구에게 무엇을 언제 보냈는지를 적은 목록입니다. 블록체인은 원장을 관리하는 하나의 특정한 방식으로, 참여자들이 서로를 완전히 믿지 못하는 상황을 위해 만들어졌습니다.

함께 작동하는 세 가지 구성 요소

모든 퍼블릭 블록체인을 세 개의 층이 쌓인 구조로 생각하면 이해하기 쉽습니다.

- **기록.** 거래는 블록으로 묶이고, 각 블록은 바로 앞 블록을 가리키며 맨 첫 블록까지 이어집니다. 이 연결이 정확히 어떻게 만들어지는지는 6강에서 보여 드립니다.
- **네트워크. 노드**(node)라고 불리는 수천 대의 컴퓨터가 각자 기록의 전체 사본을 보관하며, 새 거래와 블록을 서로 전달합니다. 7강에서 자세히 살펴봅니다.
- **규칙.** 모든 노드는 새 블록을 받아들이기 전에 같은 규칙으로 확인합니다. 규칙을 어긴 블록은 누가 보냈든 거부됩니다. 다음 블록을 추가할 사람을 정하는 방식을 **합의**(consensus)라고 하며, 비트코인의 방식은 4강에서 만난 작업 증명입니다.

이 구성 요소 중 어느 것도 그 자체로 새로운 것은 아닙니다. 데이터베이스, 네트워크, 규칙 확인은 2008년 훨씬 이전부터 있었습니다. 블록체인을 다르게 만드는 것은 이들의 결합, 그리고 어느 한 주체도 셋 중 무엇 하나 통제하지 못한다는 점입니다.

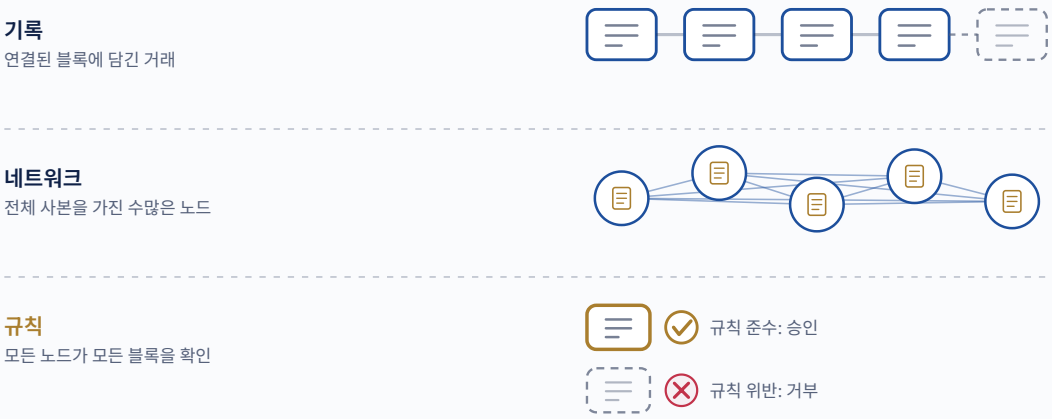


그림 1. 블록체인은 세 부분을 결합합니다. 연결된 블록으로 이루어진 기록, 독립된 사본들의 네트워크, 그리고 모든 노드가 새 블록을 받아들이거나 거부할 때 쓰는 공유된 규칙입니다.

실제로 안에 들어 있는 것

흔히들 동전이 가득한 거대한 금고를 떠올립니다. 실제 모습은 아주 긴 송금 목록에 더 가깝습니다. 비트코인 블록에는 주로 거래가 들어 있는데, 각 거래는 사실상 '이 코인이 여기서 저기로 옮겨 간다'는 내용이며, 여기에 이전 블록과 연결해 주는 작은 헤더가 붙습니다.

'앨리스는 2비트코인을 가지고 있다'는 줄은 어디에도 없습니다. 지갑은 내 주소와 관련된 모든 과거 거래를 살펴서 잔고를 계산합니다. 잔고는 기록의 결과일 뿐, 누군가 따로 저장해 두고 고칠 수 있는 숫자가 아닙니다.

이름도 저장되지 않습니다. 거래는 글자와 숫자로 된 긴 문자열인 **주소**를 가리킵니다. 그래서 비트코인은 익명이 아니라 **가명성**을 띱니다. 누구나 각 주소가 무엇을 했는지 볼 수 있지만, 그 뒤에 누가 있는지는 자동으로 알 수 없습니다. 주소가 어디서 오는지는 8강에서 설명합니다.

직접 확인해 보세요

사람과 사람 사이의 첫 결제, 즉 2009년 1월 사토시가 할 피니에게 보낸 10비트코인은 170번 블록에 있습니다. 아무 무료 블록 탐색기 사이트를 열고 블록 170을 검색하면, 17년이 넘은 지금도 그대로인 거래를 찾을 수 있습니다. 전 세계의 모든 풀 노드가 여전히 바로 그 거래를 보관하고 있습니다.

중요한 네 가지 특성

비트코인 같은 퍼블릭 블록체인에는 일반적인 시스템에 보통 없는 네 가지 특성이 있습니다.

- **추가 전용.** 새 항목은 끝에 추가할 수 있지만, 오래된 항목은 절대 수정하거나 삭제하지 않습니다. 실수는 이전 거래를 지우는 대신 새 거래로 바로잡습니다.
- **복제.** 똑같은 전체 기록이 여러 나라의 수천 대 기기에 존재합니다. 그중 일부가 사라져도 아무것도 달라지지 않습니다.
- **투명성.** 누구나 허락받지 않고 기록을 내려받아, 지금까지 이루어진 모든 거래를 읽을 수 있습니다.
- **무허가성.** 누구나 가입이나 승인 없이 거래를 보내거나 노드를 운영할 수 있습니다. 그렇지 않은 프라이빗 블록체인은 12강에서 다룹니다.

비유: 아무도 수정할 수 없는 단체 채팅방

모든 멤버의 휴대폰이 전체 대화 기록을 보관하고, 메시지는 절대 수정하거나 삭제할 수 없으며, 새 메시지는 대부분의 휴대폰이 단체방 규칙에 맞는지 확인한 뒤에야 올라오는 단체 채팅방을 상상해 보세요. 내 휴대폰에서 앱을 지울 수는 있지만, 대화는 다른 모든 곳에서 계속 이어집니다. 작년에 한 말을 바꾸려면 수천 대의 휴대폰에서 동시에 바꿔야 합니다.

블록체인이 아닌 것

블록체인에는 거창한 주장이 따라붙곤 합니다. 그중 몇 가지는 일찍 바로잡아 둘 만합니다.

- **더 빠르거나 저렴한 데이터베이스가 아닙니다.** 수천 개의 사본을 일치시키는 일은 의도적으로 느리고 비용이 많이 듭니다. 대부분의 일상적인 소프트웨어에는 일반 데이터베이스가 더 낫습니다.
- **해킹이 불가능한 것이 아닙니다.** 비트코인 기록 자체는 공격하기 매우 어렵다는 것이 입증되었지만, 블록체인을 중심으로 만들어진 거래소, 지갑, 앱은 정기적으로 해킹당합니다. 대부분의 손실은 체인이 아니라 그곳에서 일어납니다.
- **진실을 가려 주는 기계가 아닙니다.** 블록체인은 어떤 항목이 기록되었고 바뀌지 않았다는 것을 증명합니다. 그 항목이 처음부터 사실이었는지는 증명하지 못합니다. 거짓 정보가 들어가면 체인은 거짓 기록을 충실하게 보관합니다.

	일반 데이터베이스	퍼블릭 블록체인
기록을 추가할 수 있는 사람	소유자와 소유자가 승인한 사람	규칙을 따르는 누구나
오래된 기록 수정	가능하며 흔히 드러나지 않음	모두가 알게 되지 않고는 불가능
사본을 보관하는 주체	소유자	수천 개의 독립된 노드
읽을 수 있는 사람	소유자가 허락한 사람	누구나
속도와 비용	빠르고 저렴함	느리고 더 비쌈
운영자가 사라지면	시스템이 멈춤	네트워크는 계속 작동함

트레이더에게 왜 중요한가

- **거래소 잔고는 블록체인 위에 있지 않습니다.** 거래소에서 비트코인을 사면, 그 거래는 거래소 자체 데이터베이스에 기록됩니다. 블록체인은 입금과 출금만 봅니다. 2022년 11월 FTX가 무너졌을 때, 고객들의 화면에는 회사가 지급할 수 없는 잔고가 표시되어 있었습니다. 이 리스크를 어떻게 바라볼지는 10강에서 다룹니다.
- **공개 데이터는 곧 트레이딩 데이터입니다.** 기록이 투명하기 때문에 누구나 대규모 이체, 거래소로 들어가고 나오는 코인, 수년간 잠자던 지갑을 지켜볼 수 있습니다. 많은 트레이더가 이런 온체인 데이터를 활용하며, 고급 과정에 이를 다루는 강의가 따로 있습니다.
- **단어 하나가 시장을 움직이기도 합니다.** 2017년 12월, Long Island Iced Tea Corp.가 회사 이름을 Long Blockchain으로 바꾸자, 실제 블록체인 사업이 전혀 없었는데도 주가가 몇 시간 만에 몇 배로 뛰었습니다. 이후 미국 증권거래위원회(SEC)는 이 주식의 등록을 취소하고 세 명을 내부자 거래 혐의로 기소했습니다. 블록체인이 무엇인지 이해하면 과대광고를 알아보는 데 도움이 됩니다.

핵심 용어

원장	누가 누구에게 무엇을 언제 보냈는지에 대한 기록. 블록체인은 원장을 관리하는 한 가지 방식입니다.
노드	블록체인의 사본을 보관하고, 새 블록을 규칙에 따라 확인하며, 이를 다른 컴퓨터와 공유하는 컴퓨터.
합의	블록체인 네트워크가 다음에 추가할 블록을 정하는 방식. 비트코인은 작업 증명을 사용합니다.

추가 전용	새 항목은 추가할 수 있지만 오래된 항목은 절대 수정하거나 삭제할 수 없는 기록.
가명성	실명 대신 주소에 연결된 상태. 활동은 공개되지만 그 뒤의 사람은 자동으로 알려지지 않습니다.
무허가성	거래를 보내거나 노드를 운영하는 데 가입이나 승인이 필요 없이 누구에게나 열려 있는 상태.

핵심 정리

1. 블록체인은 수많은 독립된 컴퓨터가 함께 관리하는 거래 기록으로, 서로 연결된 묶음으로 추가되며 공유된 규칙을 따릅니다.
2. 모든 퍼블릭 블록체인은 기록, 노드 네트워크, 그리고 무엇을 추가할지 정하는 규칙이라는 세 부분으로 이루어집니다.
3. 블록에는 잔고나 이름이 아니라 거래가 들어 있습니다. 잔고는 내 주소의 전체 거래 기록으로 계산됩니다.
4. 퍼블릭 블록체인은 추가 전용이며, 복제되고, 투명하고, 무허가성을 띱니다.
5. 블록체인은 더 빠른 데이터베이스도, 해킹 불가능한 시스템도, 진실을 가려 주는 기계도 아닙니다. 항목이 바뀌지 않았음을 증명할 뿐, 사실이었음을 증명하지는 않습니다.

실력 점검

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

1. 블록체인을 가장 정확하게 설명한 것은 무엇인가요?

- A 디지털 코인을 보관하는 안전한 금고
- B 수많은 독립된 컴퓨터가 공유된 규칙에 따라 함께 관리하는 거래 기록
- C IT 기업이 운영하는 더 빠른 데이터베이스
- D 사람들이 암호화폐를 사고파는 웹사이트

2. 모든 퍼블릭 블록체인이 결합하는 세 가지 구성 요소는 무엇인가요?

A 코인, 지갑, 거래소
B 채굴자, 은행, 규제 기관
C 기록, 노드 네트워크, 규칙
D 비밀번호, 서버, 백업

3. 지갑은 내 비트코인 잔고를 어떻게 알까요?

A 내 주소와 관련된 모든 과거 거래를 합산한다
B 각 블록에 저장된 잔고 줄을 읽는다
C 비트코인을 운영하는 회사에 물어본다
D 블록체인에서 내 이름을 찾는다

4. '추가 전용'이란 무슨 뜻인가요?

A 승인된 사용자만 기록을 추가할 수 있다
B 기록은 일정 시간이 지나면 삭제된다
C 가장 최근 블록만 읽을 수 있다
D 새 항목은 추가할 수 있지만 오래된 항목은 절대 수정하거나 삭제하지 않는다

5. 비트코인을 익명이 아니라 가명성을 띤다고 하는 이유는 무엇인가요?

A 거래가 대중에게 숨겨져 있기 때문
B 활동은 공개되고 주소에 연결되지만, 실명과는 자동으로 연결되지 않기 때문
C 사용자가 실명으로 가입해야 하기 때문
D 채굴자만 거래를 볼 수 있기 때문

6. 블록체인에 대한 설명 중 옳은 것은 무엇인가요?

A 블록체인은 그 안의 정보가 사실임을 증명한다
B 블록체인은 일반 데이터베이스보다 빠르고 저렴하다
C 블록체인은 항목이 바뀌지 않았음을 증명하지만, 입력될 때 사실이었는지는 증명하지 못한다
D 블록체인을 중심으로 만들어진 것은 무엇도 해킹당할 수 없다

정답 및 해설

1 B

수많은 독립된 컴퓨터가 공유된 규칙에 따라 함께 관리하는 거래 기록

블록체인은 공유된 원장입니다. 수많은 독립된 컴퓨터가 사본을 보관하고, 새 항목은 연결된 블록으로 추가되며, 공유된 규칙이 무엇을 넣을지 정합니다.

2 C

기록, 노드 네트워크, 규칙

기록에는 연결된 블록이 담기고, 노드 네트워크는 사본을 보관하고 공유하며, 규칙은 어떤 블록을 받아들일지 정합니다.

3 A

내 주소와 관련된 모든 과거 거래를 합산한다

블록에는 잔고가 아니라 송금이 저장됩니다. 잔고는 내 주소로 들어오고 나간 모든 거래의 기록으로 계산됩니다.

4 D

새 항목은 추가할 수 있지만 오래된 항목은 절대 수정하거나 삭제하지 않는다

추가 전용 기록에서는 역사가 늘어나기만 합니다. 실수는 오래된 거래를 고치는 대신 새 거래로 바로잡습니다.

5 B

활동은 공개되고 주소에 연결되지만, 실명과는 자동으로 연결되지 않기 때문

누구나 한 주소가 한 모든 거래를 볼 수 있습니다. 자동으로 알 수 없는 것은 그 주소 뒤에 있는 실제 사람입니다.

6 C

블록체인은 항목이 바뀌지 않았음을 증명하지만, 입력될 때 사실이었는지는 증명하지 못한다

블록체인은 기록이 바뀌지 않도록 보호합니다. 거짓 정보가 입력되면 그 거짓 기록도 똑같이 충실하게 보관합니다.

출처

- 사토시 나카모토, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- 기네스 세계 기록, 최초의 비트코인 거래: https://guinnessworldrecords.com/world-records/696243-first-bitcoin-transaction
- Fortune, Long Blockchain 사명 변경 관련 SEC 내부자 거래 기소 (2021년 7월): https://fortune.com/2021/07/09/sec-insider-trading-long-blockchain
- CoinDesk, SEC의 Long Blockchain Corporation 주식 상장 폐지: https://www.coindesk.com/long-blockchain-corporation-shares-delisted-sec

Market Talks

계속 학습하기

다음: 6강
쉽게 설명하는 블록과 해시

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.