Market Talks
교육 센터

블록체인 · 초급 · 13강 중 4강

2008년과 비트코인의 탄생

아홉 쪽짜리 논문, 첫 블록에 숨겨진 신문 헤드라인, 그리고 홀연히 떠난 창시자

읽는 시간 8분 퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 4강

2008년과 비트코인의 탄생

한 문장 요약

2008년, 사토시 나카모토라는 이름의 정체불명 저자가 이전 실험들의 조각을 하나로 모아, 그 누구도 풀지 못했던 문제를 해결했습니다. 바로 책임자 없이 서로 모르는 사람들이 하나의 역사에 합의하는 방법입니다.

위기 한가운데의 아홉 쪽

2008년 9월, 투자은행 리먼 브라더스가 무너졌고 전 세계 정부들은 공적 자금으로 자국 은행을 구제하기에 바빴습니다. 금융 시스템에 대한 신뢰는 바닥을 쳤습니다.

6주 뒤인 2008년 10월 31일, 암호학자들이 구독하는 메일링 리스트에 한 통의 메시지가 올라왔습니다. **사토시 나카모토**(Satoshi Nakamoto)라는 이름을 쓴 작성자는 신뢰할 수 있는 제3자 없이 사용자들 사이에서 직접 작동하는 새로운 전자 현금을 발표했습니다. 메시지에는 짧은 논문 링크가 붙어 있었습니다. 제목은 *Bitcoin: A Peer-to-Peer Electronic Cash System*, 분량은 단 아홉 쪽이었습니다.

논문은 자신의 뿌리를 숨기지 않았습니다. 3강에서 만난 b-money, Hashcash, 타임스탬프 연구를 인용했습니다. 새로 더한 것은 중심에 회사도, 은행도, 신뢰할 수 있는 서버도 없이 이 부품들을 함께 작동시키는 방법이었습니다. 리스트의 많은 독자들은 회의적이었습니다. 결코 충분한 결제를 처리하지 못할 것이라는 의견도 있었고, 아예 무시한 사람들도 있었습니다.

빠진 조각을 풀다

3강은 하나의 열린 질문으로 끝났습니다. 수천 대의 독립된 컴퓨터가 각자 기록의 사본을 가지고 있다면, 책임자가 없을 때 어떤 버전이 옳은지 어떻게 합의할 수 있을까요? 비트코인의 답은 세 부분으로 이루어집니다.

첫째, 결제는 **블록**이라는 묶음으로 모이고, 각 블록은 3강의 타임스탬프 사슬처럼 바로 앞 블록과 연결됩니다. 둘째, 다음 블록을 추가할 권리는 Hashcash가 처음 사용한 아이디어인 **작업 증명**으로 얻습니다. **채굴자**라고 불리는 컴퓨터들이 퍼즐을 풀기 위해 경쟁하고, 나머지 모두가 승자의 블록을 확인한 뒤 그 위에 이어서 쌓습니다. 셋째, 만약 두 가지 버전의 역사가 경쟁하게 되면 모든 컴퓨터는 가장 많은 작업이 쌓인 체인을 따릅니다.

이 규칙들이 합쳐지면 부정행위의 비용이 매우 커집니다. 이미 체인 깊숙이 묻힌 결제를 고쳐 쓰려면, 공격자는 그 블록과 그 뒤의 모든 블록에 대한 작업을 다시 해야 하며, 그것도 나머지 네트워크 전체를 합친 것보다 빨라야 합니다. 승리한 채굴자는 새로 만들어진 비트코인을 보상으로 받습니다. 그래서 기록을 지키는 바로 그 작업이 돈을 발행하는 역할도 합니다. 두 가지 일 모두 회사가 필요 없습니다.



그림 1. 때로는 두 채굴자가 거의 동시에 블록을 찾습니다. 네트워크는 가장 많은 작업이 쌓인 체인 위에 계속 쌓아 가고, 경쟁 블록은 버려집니다.

비유: 비싼 추첨

한 번에 한 사람만 쓸 수 있는 공유 노트를 떠올려 보세요. 다음 쪽을 누가 쓸지 정하기 위해 모두가 추첨권을 사는데, 추첨권 한 장마다 실제 전기 요금이 듭니다. 대략 10분마다 한 명의 당첨자가 뽑힙니다. 지난 쪽을 위조하려는 사람은 몇 번이고 계속 당첨되어야 하는데, 이는 나머지 모두를 합친 것보다 많은 추첨권을 사야 한다는 뜻입니다. 정직한 참여자들이 훨씬 많기 때문에 계속 당첨되는 쪽은 그들입니다.

2009년 1월 3일: 첫 번째 블록

2009년 1월 3일, 사토시는 비트코인 체인의 맨 첫 블록을 만들었습니다. 이를 **제네시스 블록**(genesis block, 최초 블록)이라고 부릅니다. 보상은 50비트코인이었는데, 코드의 특이한 점 때문에 이 코인들은 영원히 쓸 수 없습니다. 6일 뒤 누구나 내려받아 실행할 수 있도록 소프트웨어가 공개되었습니다.

2009년 1월 12일, 사토시는 3강에서 만난 RPOW의 개발자인 암호학자 할 피니에게 10비트코인을 보냈습니다. 네트워크에서 사람과 사람 사이에 오간 첫 결제였습니다. 그 뒤로도 몇 달 동안 사용자는 집 컴퓨터에서 프로그램을 돌리는 소수의 애호가들뿐이었습니다.

첫 블록에 담긴 메시지

사토시는 제네시스 블록에 한 줄의 문장을 적어 넣었습니다. *The Times 03/Jan/2009 Chancellor on brink of second bailout for banks*(더 타임스 2009년 1월 3일: 재무장관, 은행 2차 구제금융 임박). 그날 영국 신문의 1면 헤드라인이었습니다. 3강에서 신문에 실린 지문처럼, 이 문장은 블록이 그 날짜 이전에 만들어졌을 수 없다는 것을 증명합니다. 많은 사람들은 이를 비트코인이 만들어진 이유에 대한 메시지로도 봅니다.

첫날부터 새겨진 규칙

DigiCash나 e-gold와 달리, 비트코인에는 돈을 얼마나 만들지 결정하는 발행자가 없습니다. 공급은 처음부터 소프트웨어에 새겨진 규칙을 따릅니다.

- **약 10분마다 새 블록 하나.** 2,016블록마다, 즉 대략 2주마다 퍼즐이 자동으로 어려워지거나 쉬워져 이 속도를 유지합니다. 채굴자가 장비를 늘리든 줄이든 마찬가지입니다.
- **줄어드는 보상.** 블록당 보상은 50비트코인에서 시작해 210,000블록마다, 대략 4년마다 절반으로 줄어듭니다. 이를 **반감기**(halving)라고 합니다. 2024년 4월 반감기 이후 보상은 3.125비트코인입니다.
- **고정된 한도.** 보상이 계속 절반으로 줄기 때문에 전체 공급량은 결코 2,100만 비트코인을 넘을 수 없습니다. 마지막 조각은 2140년 무렵에 채굴될 것으로 예상됩니다.

이 규칙은 한 사람이 바꿀 수 있는 것이 아닙니다. 네트워크의 모든 컴퓨터는 자신이 실행하는 규칙에 따라 모든 블록을 확인하므로, 규칙을 어긴 블록은 그대로 거부됩니다. 이 컴퓨터들에 대해서는 7강에서 더 자세히 살펴봅니다.

취미에서 첫 가격까지

2009년 대부분 동안 비트코인에는 아예 가격이 없었습니다. 2009년 10월, New Liberty Standard라는 이름을 쓰던 사용자가 첫 달러 환율을 발표했습니다. 1달러에 1,309.03비트코인이었습니다. 그는 자신의 컴퓨터가 코인을 채굴하는 데 쓰는 전기량을 계산해 이 숫자를 얻었습니다.

2010년 5월 22일, 플로리다의 프로그래머 라슬로 하니에츠(Laszlo Hanyecz)는 피자 두 판에 10,000비트코인을 냈습니다. 이 화폐로 실물 상품을 산 최초의 사례 중 하나입니다. 2010년 중에 첫 거래소들이 등장했고, 비트코인은 매일 변하는 시장 가격을 갖게 되었습니다. 하나의 트레이딩 시장이 탄생한 것입니다.

떠나 버린 창시자

사토시는 실명도, 얼굴도, 사는 곳도 밝힌 적이 없으며 포럼 게시물과 이메일로만 소통했습니다. 2010년 동안 사토시는 코드의 관리를 다른 자원봉사 개발자들에게 조금씩 넘겼습니다. 확인된 마지막 메시지는 2011년 4월 23일자 이메일로, 사토시가 "다른 일로 옮겨 갔다"는 내용이었습니다. 그 이름 뒤에 누가 있는지는 지금도 알려지지 않았습니다.

초기 블록을 연구한 사람들은 많은 이들이 사토시로 보는 한 명의 채굴자가 첫해에 약 110만 비트코인을 모았다고 추정합니다. 증거는 정황에 불과하며, 이 코인들은 한 번도 움직인 적이 없습니다.

이 사라짐은 결과적으로 중요했습니다. DigiCash와 e-gold에는 파산하거나 기소되거나 압박을 받을 수 있는 창업자와 회사가 있었습니다. 비트코인에는 둘 다 없습니다. 문을 닫을 본사도, 모두가 따라야 하는 결정을 내리는 리더도 없습니다.

이전의 약점	비트코인의 답
디지털 화폐를 복사할 수 있었다	모든 결제를 하나의 공유된 역사와 대조해 확인한다
회사가 돈의 양을 결정했다	새 코인은 소프트웨어의 고정된 규칙으로만 생긴다
신뢰받는 서버 하나가 이중 지불을 막았다	수천 대의 독립된 컴퓨터가 모든 블록을 확인한다
리더 없이 합의할 방법이 없었다	작업 증명으로 다음 블록을 추가할 사람을 정하고, 가장 많은 작업이 쌓인 체인이 이긴다
기소되거나 압박받을 수 있는 창업자	떠나 버린 익명의 창시자

트레이더에게 왜 중요한가

- **위기는 이야기의 일부입니다.** 비트코인은 은행 위기 한가운데에서, 첫 블록에 구제금융 헤드라인을 담고 출발했습니다. 이 이야기는 은행이 압박을 받을 때마다 다시 떠오릅니다. 2023년 3월 미국 은행 여러 곳이 무너졌을 때, 일부 투자자들이 은행 시스템 밖의 자산을 찾으면서 비트코인은 크게 올랐습니다. 이런 내러티브는 오래가지 않더라도 가격을 움직일 수 있습니다.
- **공급 일정은 공개되어 있습니다.** 모든 반감기 날짜는 몇 년 앞서 추정할 수 있고, 많은 트레이더가 그 전후의 약 4년 주기를 추적합니다. 이미 알려진 이벤트는 가격에 선반영되었을 수 있고, 과거의 주기가 다음 주기를 보장하지 않는다는 점을 기억하세요.
- **오래된 코인은 늘 주목받습니다.** 초창기 코인은 움직일 때마다 뉴스가 됩니다. 2026년 9월, 2010년에 채굴된 600비트코인이 16년 만에 움직였고, 분석가들은 곧 사토시와의 뚜렷한 연관성이 없다는 것을 확인했습니다. 헤드라인에 반응하기 전에 온체인 증거부터 확인하면 소문에 휩쓸린 매매를 피할 수 있습니다.

핵심 용어

백서	새로운 시스템이나 프로젝트가 어떻게 작동하도록 설계되었는지 설명하는 짧은 문서. 비트코인 백서는 아홉 쪽이었습니다.
제네시스 블록	블록체인의 첫 번째 블록. 비트코인의 제네시스 블록은 2009년 1월 3일에 만들어졌습니다.
채굴자	보상을 받기 위해 작업 증명을 수행하며 다음 블록을 추가하려고 경쟁하는 컴퓨터 또는 그 운영자.

블록 보상	승리한 채굴자가 블록을 추가한 대가로 받는 새 비트코인. 모든 새 비트코인은 이렇게 만들어집니다.
반감기	210,000블록마다, 대략 4년마다 블록 보상이 절반으로 줄어드는 것.
최대 작업 체인	역사의 여러 버전이 경쟁할 때, 네트워크가 가장 많은 작업 증명이 쌓인 버전을 따른다는 규칙.

핵심 정리

1. 사토시 나카모토는 은행 위기가 한창이던 2008년 10월 31일, 아홉 쪽짜리 비트코인 백서를 공개했습니다.
2. 비트코인은 사슬로 연결된 블록, 작업 증명, 최대 작업 규칙을 결합해 책임자 없이 서로 모르는 사람들이 하나의 역사에 합의할 수 있게 했습니다.
3. 2009년 1월 3일의 제네시스 블록에는 은행 구제금융에 관한 신문 헤드라인이 담겨 있어, 만들어진 날짜를 증명합니다.
4. 새 비트코인은 대략 4년마다 절반으로 줄어드는 블록 보상으로만 생기며, 총량은 결코 2,100만을 넘을 수 없습니다.
5. 사토시는 정체를 밝히지 않은 채 2011년에 떠났고, 문을 닫게 할 창업자도 회사도 남기지 않았습니다.

실력 점검

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

1. 비트코인 백서는 언제 공개되었나요?

- A 2009년 1월
- B 2008년 10월 31일
- C 2010년 5월
- D 2011년 4월

2. 블록체인의 두 버전이 경쟁하면 네트워크는 어느 쪽을 따르나요?

A 가장 오래된 컴퓨터가 만든 쪽
B 거래소들이 투표로 고른 쪽
C 가장 많은 작업 증명이 쌓인 쪽
D 가장 많은 결제가 담긴 쪽

3. 제네시스 블록의 신문 헤드라인은 무엇을 증명하나요?

A 블록이 2009년 1월 3일 이전에 만들어졌을 수 없다는 것
B 은행이 비트코인을 승인했다는 것
C 사토시가 영국에 살았다는 것
D 최초의 비트코인이 파운드로 뒷받침되었다는 것

4. 새 비트코인은 어떻게 만들어지나요?

A 중앙은행이 필요할 때 찍어 낸다
B 사토시가 매년 풀어 준다
C 수요가 늘면 거래소가 만든다
D 채굴자가 블록을 추가한 보상으로 받는다

5. 반감기에는 무슨 일이 일어나나요?

A 비트코인 가격이 절반으로 떨어진다
B 블록을 추가하는 보상이 절반으로 줄어든다
C 전체 비트코인의 절반이 소각된다
D 블록이 두 배 빠르게 추가된다

6. 사토시의 사라짐은 왜 비트코인에 도움이 되었나요?

A 비트코인 채굴이 더 저렴해졌다
B 시스템의 모든 규칙이 사라졌다
C 문을 닫게 하거나 압박할 수 있는 창업자나 회사를 남기지 않았다
D 사토시가 몰래 코인을 팔 수 있게 되었다

정답 및 해설

1 B

2008년 10월 31일

사토시는 리먼 브라더스 파산 약 6주 뒤인 2008년 10월 31일, 암호학 메일링 리스트에 아홉 쪽짜리 논문을 공유했습니다.

2 C

가장 많은 작업 증명이 쌓인 쪽

모든 컴퓨터는 가장 많은 작업이 쌓인 체인을 따릅니다. 이를 대체하려면 공격자는 나머지 네트워크 전체를 합친 것보다 큰 연산 능력이 필요합니다.

3 A

블록이 2009년 1월 3일 이전에 만들어졌을 수 없다는 것

그 헤드라인은 2009년 1월 3일에 인쇄되었으므로 블록이 그보다 오래되었을 수 없습니다. 사토시가 누구였고 어디에 살았는지는 여전히 알려지지 않았습니다.

4 D

채굴자가 블록을 추가한 보상으로 받는다

블록 보상은 새 비트코인이 생겨나는 유일한 방법입니다. 소프트웨어의 고정된 규칙을 따르므로 누구도 더 발행하기로 결정할 수 없습니다.

5 B

블록을 추가하는 보상이 절반으로 줄어든다

210,000블록마다, 대략 4년마다 블록 보상이 절반으로 줄어듭니다. 그래서 전체 공급량은 결코 2,100만을 넘을 수 없습니다.

6 C

문을 닫게 하거나 압박할 수 있는 창업자나 회사를 남기지 않았다

DigiCash와 e-gold는 회사와 함께 무너졌습니다. 알려진 리더가 없기 때문에 비트코인에는 문을 닫을 본사도, 모두가 따라야 하는 한 사람도 없습니다.

출처

- 사토시 나카모토, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- 암호학 메일링 리스트, Bitcoin P2P e-cash paper (2008년 10월 31일): https://www.metzdowd.com/pipermail/cryptography/2008-October/014810.html
- Cointelegraph, 제네시스 블록 기념일에 열 살이 된 비트코인: https://cointelegraph.com/news/bitcoin-turns-ten-on-anniversary-of-genesis-block
- Bitcoin Magazine, 첫 달러 가격 이후 65억 퍼센트 오른 비트코인: https://bitcoinmagazine.com/culture/bitcoin-is-up-6-5-billion-percent-since-it-was-first-priced-in-usd
- The Defiant, 사토시 나카모토가 마이크 헌에게 보낸 마지막 이메일 (2011년 4월 23일): https://thedefiant.io/news/people/bitcoin-creator-satoshi-nakamoto-sent-final-email-to-mike-hearn-on-april-23-2011-6735013c

- Cointelegraph, 사토시는 정말 100만 비트코인을 갖고 있을까?: https://cointelegraph.com/news/big-questions-does-satoshi-actually-own-1-million-bitcoin

Market Talks

계속 학습하기

다음: 5강
블록체인이란 정확히 무엇인가

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.