Market Talks
교육 센터

블록체인 · 초급 · 13강 중 3강

비트코인 이전: 디지털 현금 실험들

25년에 걸친 시도와 아쉬운 실패들, 그리고 각각이 비트코인에 남긴 조각들

읽는 시간 8분 퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 3강

비트코인 이전: 디지털 현금 실험들

한 문장 요약

비트코인은 갑자기 나타난 것이 아닙니다. 이전 디지털 현금 프로젝트들의 아이디어를 결합했고, 그 대부분을 무너뜨린 단 하나의 약점을 피하도록 설계되었습니다.

웹 브라우저보다 오래된 꿈

1강과 2강에서 우리는 두 가지 문제를 만났습니다. 디지털 화폐는 복사될 수 있고, 한 주체가 운영하는 시스템은 동결되거나 폐쇄되거나 부패할 수 있다는 것입니다. 비트코인이 나오기 훨씬 전부터 암호학자와 기업가들은 이미 이 두 문제를 함께 풀려고 노력하고 있었습니다.

그들의 프로젝트는 1980년대 초부터 2000년대 중반까지 이어졌습니다. 일부는 실제 고객을 둔 실제 사업이 되었고, 일부는 끝내 종이 위에만 머물렀습니다. 완전히 성공한 것은 하나도 없었지만, 거의 모든 프로젝트가 훗날 비트코인이 사용하게 될 무언가를 더했습니다. 이들의 이야기를 따라가 보는 것이 비트코인이 왜 지금과 같은 방식으로 만들어졌는지 이해하는 가장 좋은 방법입니다.



그림 1. 비트코인 이전에 25년이 넘는 디지털 현금 실험이 있었습니다. 각 실험은 최종 설계의 한 조각을 남겼습니다.

DigiCash: 프라이버시는 있었지만 한 회사가 운영

1982년, 암호학자 데이비드 차움(David Chaum)은 **은닉 서명**(blind signature)이라는 기법을 제시했습니다. 이 기법을 쓰면 은행은 자신이 어떤 코인에 서명하는지 보지 않고도 디지털 코인에 서명해 그 유효성을 확인해 줄 수 있습니다. 그 결과, 은행이 결제를 코인을 인출한 사람과 연결할 수 없기 때문에 현금처럼 익명으로 쓸 수 있는 디지털 화폐가 탄생합니다.

차움은 이 아이디어를 제품으로 만들기 위해 1989년 DigiCash를 설립했고, 1995년 세인트루이스의 마크 트웨인 은행이 고객들에게 DigiCash의 eCash를 제공하기 시작했습니다. 기술은 작동했습니다. 사업은 그렇지 못했습니다. 참여한 은행과 가맹점이 너무 적었고, DigiCash는 1998년 파산을 신청했습니다.

더 근본적인 약점은 구조에 있었습니다. 모든 코인은 여전히 중앙 은행이나 회사가 발행해야 했고, 이중 지불을 확인하는 것도 바로 그 중앙 주체였습니다. 회사가 무너지자 돈도 함께 무너졌습니다.

e-gold: 실물 담보, 단일 실패 지점

1996년에 출시된 e-gold는 다른 길을 택했습니다. 모든 단위는 금고에 보관된 실물 금으로 뒷받침되었고, 사용자들은 금으로 뒷받침되는 잔고를 몇 초 만에 전 세계 누구에게나 보낼 수 있었습니다. 성장은 빨랐습니다. 2006년에는 연간 20억 달러가 넘는 결제를 처리하고 있었습니다.

하지만 e-gold는 하나의 회사였고, 그래서 하나의 표적이 되었습니다. 신원 확인이 없다는 점이 범죄자들을 끌어들였고, 미국 당국은 2007년 회사와 이사들을 기소했습니다. 2008년 이들은 자금 세탁 공모와 무허가 송금업 운영 혐의를 인정했고, 2009년에는 송금이 중단되었습니다. 계좌 보유자들은 자금을 돌려받는 절차가 마련되기까지 수년을 기다려야 했습니다.

2강의 교훈이 현실에서 그대로 드러났습니다. 단일 통제 지점은 곧 단일 실패 지점이기도 합니다. 그 원인이 해커든, 파산이든, 법원 명령이든 마찬가지입니다.

Hashcash: 일부러 비용을 들게 만들기

1997년, 암호학자 애덤 백(Adam Back)은 스팸 메일을 막는 방법으로 **Hashcash**를 제안했습니다. 메시지를 보내기 전에 발신자의 컴퓨터는 작은 퍼즐을 풀어야 했고, 여기에는 잠깐의 연산 작업이 들었습니다. 이메일 한 통에는 그 비용이 눈에 띄지 않습니다. 하지만 수백만 통을 보내는 스패머에게는 비용이 빠르게 쌓입니다.

핵심은 비대칭성입니다. 퍼즐은 푸는 데 오래 걸리지만 확인은 즉시 가능합니다. 이메일을 받은 사람은 누구나 그 작업을 다시 하지 않고도 작업이 이루어졌음을 확인할 수 있습니다. 이 아이디어를 **작업 증명**(proof of work)이라고 부르며, 비트코인 백서는 Hashcash를 직접적인 영향을 준 사례로 언급합니다.

> **비유: 스도쿠 테스트**
>
> 어려운 스도쿠는 푸는 데 한 시간이 걸릴 수 있지만, 완성된 칸을 확인하는 데는 1분이면 충분합니다. 누군가 다 푼 퍼즐을 건네면, 그 사람이 푸는 모습을 보지 못했더라도 노력을 들였다는 것을 알 수 있습니다. 작업 증명은 이 아이디어를 어떤 컴퓨터든 검증할 수 있는 디지털 노력 도장으로 바꿉니다.

b-money, Bit Gold, RPOW: 설계도

1998년, 두 가지 제안이 문서상으로는 비트코인에 놀라울 만큼 가까이 다가갔습니다. 컴퓨터 엔지니어 웨이 다이(Wei Dai)가 설명한 **b-money**에서는 모든 참여자가 누가 무엇을 소유하는지에 대한 사본을 보관하고, 새로운 돈은 연산 문제를 풀어서 만들어집니다. 비슷한 시기에 법학자이자 컴퓨터 과학자인 닉 재보(Nick Szabo)는 **Bit Gold**를 제안했습니다. 이는 작업 증명의 답을 타임스탬프와 함께 사슬처럼 이어, 희소하고 생산 비용이 큰 무언가, 일종의 디지털 금을 만드는 방식이었습니다.

둘 다 실제로 출시되지는 않았습니다. 그리고 둘 다 중요한 질문 하나를 남겼습니다. 서로 독립적인 많은 사람이 기록을 보관한다면, 책임자 없이 어떤 기록이 옳은지 어떻게 합의할 수 있을까요?

2004년, 암호학자 할 피니(Hal Finney)는 작업 증명 토큰을 사람에서 사람으로 넘길 수 있게 하는 **RPOW**(재사용 가능한 작업 증명)를 만들었습니다. 이 시스템은 실제로 작동했지만, 이중 지불을 막기 위해 특수 보안 하드웨어에서 돌아가는 신뢰할 수 있는 서버에 의존했습니다. 중심에는 여전히 신뢰받는 하나의 주체가 있었습니다. 5년 뒤, 피니는 한 사람이 다른 사람에게 보낸 최초의 비트코인을 받게 됩니다.

타임스탬프의 사슬

또 하나의 조각은 화폐의 세계 밖에서 왔습니다. 1991년, 연구자 스튜어트 하버(Stuart Haber)와 W. 스콧 스토르네타(W. Scott Stornetta)는 디지털 문서가 언제 만들어졌는지, 그리고 그 이후로 변경되지 않았음을 어떻게 증명할 수 있을지 고민했습니다.

그들의 답은 기록을 사슬로 연결하는 것이었습니다. 새로운 기록마다 바로 앞 기록의 디지털 지문을 담기 때문에, 오래된 기록 하나를 바꾸면 그 뒤의 모든 연결 고리가 끊어집니다. 그렇게 역사는 **변조 흔적이 드러나는** (tamper-evident) 구조가 됩니다. 여전히 고쳐 쓰려고 시도할 수는 있지만, 모두가 그 사실을 알게 됩니다. 비트코인 백서는 이들의 연구를 세 번 인용하며, 이렇게 기록을 잇는 아이디어가 블록체인의 '체인'(chain)이 되었습니다. 이 지문이 정확히 어떻게 작동하는지는 6강에서 설명합니다.

실제 사례

사슬을 몰래 고쳐 쓰는 것이 불가능하도록, 하버와 스토르네타의 회사는 1995년부터 최신 기록의 지문을 뉴욕타임스 안내 광고란에 게재하기 시작했습니다. 누구나 인쇄된 신문과 사슬을 비교할 수 있었고, 이미 인쇄된 수천 부를 나중에 바꿀 수 있는 사람은 아무도 없었습니다.

빠진 조각

2000년대 중반에는 거의 모든 부품이 이미 존재했습니다. 여전히 빠져 있던 것은 가장 어려운 조각이었습니다.

프로젝트	더한 것	여전히 부족했던 것
DigiCash (1989)	프라이버시가 보장되는 디지털 결제	중앙 발행자에 의존
타임스탬프 사슬 (1991)	몰래 바꿀 수 없도록 서로 연결된 기록	화폐용으로 설계되지 않음
e-gold (1996)	대규모 글로벌 송금	폐쇄될 수 있는 하나의 회사
Hashcash (1997)	작업 증명: 만들기는 비싸고 검증은 저렴	화폐가 아닌 도장일 뿐
b-money, Bit Gold (1998)	공유 기록과 작업으로 만들어지는 돈	리더 없이 합의할 방법이 없음; 출시되지 않음
RPOW (2004)	사람들 사이에 넘길 수 있는 작업 증명 토큰	신뢰할 수 있는 서버 하나에 의존

모든 시도는 책임자에게 의존했거나, 책임자 없이 낯선 사람들이 하나의 역사에 합의하는 방법을 끝내 풀지 못했습니다. 2008년, 한 익명의 저자가 이 조각들을 하나로 모으고 빠진 조각을 더했습니다. 그것이 4강의 이야기입니다.

트레이더에게 왜 중요한가

- **중앙 발행자는 익숙한 방식으로 실패합니다.** DigiCash는 파산했고 e-gold는 검찰에 의해 문을 닫았습니다. 같은 패턴이 2013년에 다시 나타났는데, 미국 당국이 또 다른 중앙 운영 디지털 화폐인 Liberty Reserve를 폐쇄한 것입니다. 하나의 발행자에 의존하는 자산은 그 발행자의 사업 리스크와 법적 리스크를 함께 떠안습니다.
- **오늘날의 스테이블코인은 e-gold를 닮았습니다.** 달러 담보 스테이블코인도 비슷한 모델을 따릅니다. 한 회사가 준비금을 보유하고 그에 맞춰 토큰을 발행합니다. 그래서 스테이블코인에 의존하기 전에 발행자의 준비금, 인허가, 법적 지위를 이해해 둘 가치가 있습니다.
- **'디지털 금' 내러티브는 뿌리가 깊습니다.** 만드는 데 비용이 들기 때문에 희소하다는 Bit Gold의 아이디어는 지금도 많은 투자자가 비트코인을 금과 비교하는 방식에 영향을 줍니다. 어떤 내러티브가 어디서 왔는지 알면, 그것이 시장을 움직일 때 얼마나 무게를 둘지 판단하는 데 도움이 됩니다.

핵심 용어

은닉 서명 은행이나 발행자가 어떤 코인인지 보지 않고도 디지털 코인을 승인하는 방법으로, 결제의 프라이버시를 지켜 줍니다.

작업 증명	컴퓨터가 퍼즐을 푸는 데 실제 노력을 들였다는 증거. 만들기는 느리고 확인은 즉시 가능합니다.
자산 담보	발행자가 보유한 금이나 달러 같은 실물 자산이 가치를 뒷받침하는 돈이나 토큰.
타임스탬프	디지털 기록이 언제 만들어졌는지, 그리고 그 이후로 변경되지 않았음을 증명하는 것.
변조 흔적 노출	물리적으로 막을 수는 없더라도, 과거 기록에 대한 어떤 변경이든 모두에게 보이도록 만든 구조.
디지털 희소성	단순히 복사하거나 공짜로 만들어 낼 수 없는, 공급이 제한된 디지털 대상.

핵심 정리

1. 디지털 현금 실험은 1980년대 초, 비트코인보다 25년 이상 앞서 시작되었습니다.
2. DigiCash는 프라이버시를, e-gold는 글로벌 규모를 가져왔지만, 둘 다 하나의 회사에 의존했고 회사와 함께 무너졌습니다.
3. Hashcash는 작업 증명을 도입했습니다. 만들기는 느리지만 검증은 즉시 가능한 노력입니다.
4. b-money, Bit Gold, RPOW는 공유 기록과 작업 기반 화폐의 밑그림을 그렸지만, 신뢰할 수 있는 주체 없이 낯선 사람들이 합의하는 방법은 어느 것도 풀지 못했습니다.
5. 연결된 타임스탬프는 역사를 변조 흔적이 드러나게 만드는 방법을 보여 주었습니다. 비트코인은 이 조각들을 결합하고 빠진 조각을 더했습니다.

실력 점검

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

1. DigiCash의 핵심 혁신은 무엇이었나요?

- A 금고에 보관된 금
- B 디지털 결제를 비공개로 만든 은닉 서명
- C 스팸을 막기 위한 작업 증명
- D 모든 사용자가 사본을 가진 장부

2. e-gold는 왜 끝나게 되었나요?

A 이를 운영한 단 하나의 회사에 대한 법적 조치
B 금 준비금을 도난당함
C 버그로 사용자가 코인을 복사할 수 있었음
D 사용자들이 비트코인으로 옮겨 감

3. Hashcash는 원래 무엇을 위해 설계되었나요?

A 온라인 결제를 비공개로 만들기
B 금 담보 잔고 보관하기
C 스팸 메일 발송을 비싸게 만들기
D 법률 문서에 타임스탬프 찍기

4. 작업 증명을 유용하게 만드는 특성은 무엇인가요?

A 누구나 즉시 만들 수 있다
B 중앙 서버만 확인할 수 있다
C 복사하기 쉽다
D 만들기는 느리지만 검증은 즉시 가능하다

5. 1991년 하버와 스토르네타의 연구는 무엇을 기여했나요?

A 금 담보 디지털 화폐
B 역사를 바꾸면 드러나도록 기록을 사슬로 연결하는 방법
C 익명 이메일
D 최초의 암호화폐 거래소

6. 2008년 이전에 여전히 빠져 있던 조각은 무엇이었나요?

A 더 빠른 인터넷 연결
B 결제를 비공개로 만드는 방법
C 책임자 없이 낯선 사람들이 하나의 공유된 역사에 합의하는 방법
D 작업 증명을 할 만큼 강력한 컴퓨터

정답 및 해설

1 B

디지털 결제를 비공개로 만든 은닉 서명

데이비드 차움의 은닉 서명 덕분에 은행은 어떤 코인인지 보지 않고도 코인을 승인할 수 있었고, 그래서 결제는 현금처럼 비공개로 유지될 수 있었습니다.

2 A

이를 운영한 단 하나의 회사에 대한 법적 조치

e-gold는 하나의 회사가 운영했습니다. 검찰이 기소한 뒤 회사와 이사들은 2008년 혐의를 인정했고, 2009년 송금이 중단되었습니다. 하나의 회사는 곧 단일 실패 지점을 뜻했습니다.

3 C

스팸 메일 발송을 비싸게 만들기

애덤 백은 스팸에 맞서기 위해 Hashcash를 제안했습니다. 이메일마다 약간의 연산 작업이 필요했는데, 한 통에는 별것 아니지만 수백만 통에는 매우 큰 비용이 됩니다.

4 D

만들기는 느리지만 검증은 즉시 가능하다

다 푼 스도쿠처럼, 작업 증명은 만드는 데 노력이 들지만 확인은 순식간입니다. 덕분에 누구나 작업을 다시 하지 않고도 작업이 이루어졌음을 확인할 수 있습니다.

5 B

역사를 바꾸면 드러나도록 기록을 사슬로 연결하는 방법

각 기록은 이전 기록의 지문을 담고 있어서, 오래된 기록을 바꾸면 그 뒤의 모든 연결 고리가 끊어집니다. 이 아이디어가 블록체인의 '체인'이 되었습니다.

6 C

책임자 없이 낯선 사람들이 하나의 공유된 역사에 합의하는 방법

이전 시스템들은 신뢰할 수 있는 주체에 의존했거나, 서로 독립적인 많은 참여자가 하나의 기록에 합의하는 방법을 끝내 풀지 못했습니다. 비트코인이 그 빠진 조각을 더했으며, 4강에서 이를 설명합니다.

출처

- 미국 법무부, e-gold 유죄 인정 (2008년 7월): https://www.justice.gov/archive/opa/pr/2008/July/08-crm-635.html
- 위키백과, DigiCash: https://en.wikipedia.org/wiki/DigiCash
- 위키백과, e-gold: https://en.wikipedia.org/wiki/E-gold
- Satoshi Nakamoto Institute, 할 피니: RPOW: https://nakamotoinstitute.org/finney/rpow/
- Cointelegraph, 블록체인 공동 발명자가 말하는 자신이 사토시 나카모토가 아닌 이유: https://cointelegraph.com/news/co-inventor-of-blockchain-on-why-he-is-not-satoshi-nakamoto

Market Talks

계속 학습하기

다음: 4강
2008년과 비트코인의 탄생

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.