Market Talks
교육 센터

블록체인 · 초급 · 13강 중 8강

키, 주소, 지갑

비트코인의 소유를 실제로 증명하는 것, 돈을 받기 위해 공유하는 것, 그리고 지갑이 실제로 담고 있는 것

읽는 시간 6분　　퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 8강

키, 주소, 지갑

한 문장 요약

비트코인을 소유한다는 것은 결제에 서명할 수 있게 해 주는 비밀 숫자인 개인 키를 가지고 있다는 뜻입니다. 개인 키에서 공유해도 되는 공개 키와 주소가 나옵니다. 지갑은 코인을 전혀 담고 있지 않습니다. 키를 보관하고 그 키로 서명할 뿐입니다.

비밀 하나, 공유해도 되는 것 둘

5강에서 블록체인에는 이름이 없고 주소만 있다는 것을 보았습니다. 그렇다면 네트워크는 어떤 코인이 내 것인지 어떻게 알까요? 답은 서로 연결된 세 가지에 있습니다.

- **개인 키.** 78자리에 이르는, 6강의 해시와 같은 규모의 거대한 범위에서 무작위로 고른 비밀 숫자입니다. 이 숫자를 아는 사람은 그와 연결된 코인을 쓸 수 있습니다.
- **공개 키.** 특별한 종류의 수학으로 개인 키에서 계산한 숫자입니다. 누구에게나 보여 줘도 됩니다.
- **주소.** 공개 키를 해시해서 만든 더 짧은 코드로, 입력 실수를 잡아내는 검사 기능이 들어 있습니다. 사람들이 나에게 돈을 보낼 수 있도록 알려 주는 것이 바로 이것입니다.

각 단계는 한 방향으로만 작동합니다. 개인 키를 공개 키로, 공개 키를 주소로 바꾸는 데 컴퓨터는 1초도 걸리지 않습니다. 거꾸로 돌아가는 것은 사실상 불가능합니다. 그래서 주소를 어디에 공개해도 코인이 위험해지지 않습니다.



각 화살표는 1초도 걸리지 않습니다. 반대 방향으로 돌아가는 것은 사실상 불가능합니다.

그림 1. 개인 키가 공개 키를, 공개 키가 주소를 만듭니다. 각 단계는 한 방향으로만 작동하므로, 주소를 공유해도 개인 키는 절대 드러나지 않습니다.

쓴다는 것은 서명한다는 것

비트코인을 쓰려면 지갑이 거래를 만들고, 개인 키로 만든 **디지털 서명**을 붙입니다. 어떤 노드든 내 공개 키로 그 서명을 확인해, 개인 키 자체는 한 번도 보지 않고도 짝이 맞는 개인 키로 만든 서명임을 확인할 수 있습니다.

서명은 그 거래 하나의 정확한 내용에도 묶여 있습니다. 누군가 금액이나 받는 곳을 한 글자라도 바꾸면 서명이 더 이상 맞지 않아 모든 노드가 거부합니다. 그래서 누구도 네트워크를 지나가는 결제를 가로채 다른 곳으로 돌릴 수 없습니다.

이것이 은행과의 큰 차이입니다. 은행은 내가 누구인지 확인해서 돈을 쓸 수 있는지 결정합니다. 비트코인은 서명이 유효한지만 확인합니다. 이름도, 비밀번호 재설정도, 고객센터도 없이, 오직 수학뿐입니다.

비유: 투입구가 있는 우편함

주소를 앞면에 투입구가 있는 우편함이라고 생각해 보세요. 위치를 아는 사람은 누구나 편지를 넣을 수 있고, 거리의 모든 사람이 편지가 몇 통 오는지 볼 수 있습니다. 하지만 열쇠를 가진 사람만 우편함을 열고 편지를 꺼낼 수 있습니다. 열쇠를 잃어버리면 편지는 영원히 안에 갇힙니다. 누군가 열쇠를 복사하면 우편함을 비울 수 있습니다.

비트코인 주소는 어떻게 생겼나

비트코인은 주소 형식을 몇 차례 바꿨습니다. 모든 형식이 지금도 작동하며, 첫 글자로 구분할 수 있습니다.

시작 문자	종류	도입 연도
1	Legacy, 최초의 형식	2009
3	스크립트 주소, 공동 지갑이나 다중 서명 지갑에 자주 쓰임	2012
bc1q	Native SegWit, 더 작은 거래와 더 낮은 수수료	2017
bc1p	Taproot, 가장 새로운 형식으로 프라이버시와 유연성이 더 높음	2021

다른 블록체인은 저마다의 형식을 씁니다. 예를 들어 이더리움 주소는 *0x* 뒤에 40개의 문자가 붙습니다. 같은 앱에 둘 다 표시되더라도 비트코인 주소를 이더리움 주소로 대신할 수는 없습니다.

좋은 지갑은 받기를 요청할 때마다 새 주소를 만들어 줍니다. 이 주소들은 모두 같은 지갑에 속하며, 예전 주소도 계속 작동합니다. 새 주소를 쓰면 낯선 사람이 내 결제들을 서로 연결하기가 더 어려워집니다.

지갑이 실제로 담고 있는 것

이름과 달리 지갑은 코인을 담고 있지 않습니다. 코인은 블록체인 위의 기록으로만 존재합니다. **지갑**은 내 키를 보관하고, 블록체인을 읽어 잔고를 보여 주며, 거래를 만들고 서명하는 도구입니다.

지갑은 크게 두 가지로 나뉩니다.

- **핫 월렛**은 휴대폰 앱이나 데스크톱 프로그램처럼 인터넷에 연결된 기기에 키를 보관합니다. 일상적으로 쓰기 편하지만, 그 기기를 공격할 수 있는 모든 것에 키가 노출됩니다.
- **콜드 월렛**은 키를 오프라인으로 보관합니다. **하드웨어 지갑**은 키를 내부에 보관하고, 키를 컴퓨터에 한 번도 드러내지 않은 채 거래에 서명하는 작은 기기입니다. 사용은 더 느리지만 해킹하기는 훨씬 어렵습니다.

코인이 거래소에 있다면 키는 내가 아니라 거래소가 가지고 있습니다. 두 가지 선택은 10강에서 비교하고, 모든 키를 한꺼번에 지켜 주는 백업은 9강에서 다룹니다.

실제 사례: 쓰레기 매립지의 하드 드라이브

2013년, 웨일스의 컴퓨터 엔지니어 제임스 하월스는 몇 년 전에 채굴한 8,000비트코인의 개인 키가 담긴 낡은 하드 드라이브를 실수로 버렸습니다. 드라이브는 시의 쓰레기 매립지로 갔습니다. 그는 10년 넘게 매립지를 파게 해 달라고 요청했습니다. 2025년 1월 영국 법원은 그의 소송을 기각했고, 같은 해 3월 항소도 기각되었습니다. 코인은 여전히 블록체인 위에 있어 누구나 볼 수 있지만, 아무도 쓸 수 없습니다.

트레이더에게 왜 중요한가

- **매번 주소 전체를 확인하세요.** 주소 오염(address poisoning) 사기에서 공격자는 내가 쓰는 주소와 거의 똑같아 보이는 주소에서 아주 적은 금액을 보내, 다음번에 내가 거래 내역에서 그 주소를 복사하기를 노립니다. 2024년 5월 한 트레이더는 약 6,800만 달러에 해당하는 래핑 비트코인(WBTC) 1,155개를 그런 주소로 보냈습니다. 공격자가 협상 끝에 대부분을 돌려주었지만, 이는 매우 드문 결말입니다.
- **주소뿐 아니라 네트워크도 맞추세요.** 거래소는 같은 코인을 여러 네트워크에서 지원하는 경우가 많습니다. 받는 쪽이 지원하지 않는 네트워크로 보내면 자금을 되찾기가 매우 어렵거나 불가능할 수 있습니다. 확인을 누르기 전에 네트워크와, 필요하다면 메모나 태그를 확인하세요.
- **먼저 소액으로 테스트하세요.** 큰 금액이나 처음 하는 송금이라면, 소액 테스트 송금에 드는 수수료는 약간이지만 전체 금액을 지킬 수 있습니다. 많은 트레이더가 거래소 계정에 출금 주소 화이트리스트도 함께 사용합니다.

핵심 용어

개인 키	보유자가 거래에 서명하고 그와 연결된 코인을 쓸 수 있게 해 주는 무작위 비밀 숫자.
공개 키	개인 키에서 계산한 숫자로, 공유할 수 있으며 서명을 확인하는 데 쓰입니다.
주소	공개 키로 만든 더 짧은 코드로, 다른 사람이 나에게 코인을 보낼 수 있도록 공유합니다.

디지털 서명	개인 키로 만들어 특정 거래 하나를 승인하는 증명으로, 누구나 공개 키로 확인할 수 있습니다.
지갑	내 키를 보관하고, 블록체인을 바탕으로 잔고를 보여 주며, 거래를 만들고 서명하는 도구.
하드웨어 지갑	개인 키를 오프라인으로 보관하고, 키를 컴퓨터에 노출하지 않고 거래에 서명하는 작은 기기.

핵심 정리

1. 비트코인을 소유한다는 것은 개인 키를 통제한다는 뜻입니다. 키를 가진 사람이 코인을 쓸 수 있습니다.
2. 공개 키와 주소는 개인 키에서 계산되며, 어느 것도 개인 키로 되돌릴 수 없습니다.
3. 코인을 쓰려면 정확한 거래에 묶인 디지털 서명이 필요하며, 모든 노드는 개인 키를 보지 않고도 이를 확인할 수 있습니다.
4. 비트코인 주소는 종류에 따라 1, 3, bc1q, bc1p로 시작하며, 지갑은 결제마다 새 주소를 만들 수 있습니다.
5. 지갑은 코인이 아니라 키를 담습니다. 핫 월렛은 편리하고, 콜드 월렛은 키를 오프라인에 두어 훨씬 안전합니다.

실력 점검

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

1. 누군가에게 비트코인을 쓸 수 있는 힘을 주는 것은 무엇인가요?

- A 주소를 아는 것
- B 개인 키를 가지고 있는 것
- C 거래소 계정을 가지고 있는 것
- D 거래 ID를 아는 것

2. 주소를 공개적으로 공유해도 안전한 이유는 무엇인가요?

A 주소는 한 번 쓰면 만료되기 때문
B 네트워크가 주소를 다른 사람에게 숨기기 때문
C 누구도 주소에서 개인 키로 거슬러 올라갈 수 없기 때문
D 주소가 암호화되어 있기 때문

3. 서명된 거래의 금액을 누군가 바꾸면 어떻게 되나요?

A 서명이 더 이상 맞지 않아 노드들이 거부한다
B 바뀐 금액으로 거래가 처리된다
C 서명이 자동으로 갱신된다
D 채굴자가 어느 금액을 쓸지 정한다

4. 암호화폐 지갑이 실제로 보관하는 것은 무엇인가요?

A 내 코인
B 블록체인 전체의 사본
C 내 은행 정보
D 내 키

5. bc1q로 시작하는 비트코인 주소는 어떤 종류인가요?

A Legacy
B Native SegWit
C 이더리움
D Taproot

6. 하드웨어 지갑의 가장 큰 장점은 무엇인가요?

A 거래를 더 빠르게 한다
B 모든 수수료를 없앤다
C 개인 키를 오프라인에 두고, 키를 노출하지 않고 서명한다
D 잘못된 주소로 보낸 코인을 되찾게 해 준다

정답 및 해설

1 B

개인 키를 가지고 있는 것

결제에 서명하는 것은 개인 키입니다. 이를 가진 사람은 누구나 코인을 쓸 수 있으므로 반드시 비밀로 지켜야 합니다.

2 C

누구도 주소에서 개인 키로 거슬러 올라갈 수 없기 때문

개인 키에서 공개 키, 주소로 가는 각 단계는 한 방향입니다. 다른 사람은 내 주소로 보낼 수는 있지만, 그 주소로 개인 키를 찾아낼 수는 없습니다.

3 A

서명이 더 이상 맞지 않아 노드들이 거부한다

서명은 거래 하나의 정확한 내용에 묶여 있습니다. 한 글자라도 바뀌면 서명은 무효가 됩니다.

4 D

내 키

코인은 블록체인 위에만 존재합니다. 지갑은 내 키를 보관하고, 체인에서 잔고를 읽고, 거래에 서명합니다.

5 B

Native SegWit

bc1q로 시작하는 주소는 2017년에 도입된 Native SegWit입니다. Taproot 주소는 bc1p로, Legacy 주소는 1로 시작합니다.

6 C

개인 키를 오프라인에 두고, 키를 노출하지 않고 서명한다

하드웨어 지갑은 키를 기기 안에 보관하고 서명된 거래만 내보내므로, 컴퓨터의 악성 코드가 키를 읽을 수 없습니다.

출처

- 사토시 나카모토, Bitcoin: A Peer-to-Peer Electronic Cash System (2008): https://bitcoin.org/bitcoin.pdf
- 위키백과, 뉴포트 매립지에 묻힌 비트코인: https://en.wikipedia.org/wiki/Bitcoin_buried_in_Newport_landfill
- Cointelegraph, 주소 오염 사기로 6,800만 달러를 잃은 트레이더 (2024년 5월): https://cointelegraph.com/news/trader-loses-68-million-address-poisoning-scam
- Cointelegraph, 협상 끝에 자금을 돌려준 공격자: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations

Market Talks

계속 학습하기

다음: 9강
시드 문구와 백업

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.