Market Talks
교육 센터

블록체인 · 초급 · 13강 중 10강

수탁: 거래소 계정이냐, 내 지갑이냐

내 코인을 실제로 누가 보관하는지, 두 선택에 대해 역사는 무엇을 말해 주는지, 그리고 대부분의 트레이더가 둘을 어떻게 나누는지

읽는 시간 5분　　퀴즈 6문항, 정답 포함

블록체인 · 초급 · 13강 중 10강

수탁: 거래소 계정이냐, 내 지갑이냐

한 문장 요약

거래소에 암호화폐를 두면 키는 거래소가 갖고 나는 약속만 갖습니다. 내 지갑에 두면 키와 모든 책임을 내가 갖습니다. 두 선택은 서로 다른 위험으로부터 나를 지켜 줍니다.

같은 비트코인을 보유하는 두 가지 방법

수탁(custody)이란 간단히 말해 개인 키를 누가 가지고 있느냐입니다. 기본 모델은 두 가지입니다.

- **위탁 보관.** 거래소나 다른 회사가 키를 가지고 있습니다. 나는 비밀번호로 로그인하고, 내 잔고는 5강에서 본 것처럼 회사 자체 데이터베이스의 숫자입니다. 출금할 때는 회사가 나를 대신해 거래에 서명합니다.
- **자기 수탁.** 내가 키를 가지고 있으며, 보통 9강의 시드 문구로 백업한 지갑에 보관합니다. 누구도 내 코인을 옮기거나 내가 옮기는 것을 막을 수 없지만, 내가 키를 잃어버려도 누구도 구해 줄 수 없습니다.

블록체인 위에는 거래소의 '내 계정'이라는 것이 존재하지 않습니다. 거래소의 주소들이 모든 고객의 코인을 한데 보관하고, 거래소 데이터베이스가 그 더미 중 얼마가 각 고객의 몫인지 기록할 뿐입니다.



그림 1. 거래소 계정에서는 회사가 키를 가지고 있고, 나는 회사를 거쳐 블록체인에 닿습니다. 내 지갑에서는 내가 키를 가지고 블록체인과 직접 거래합니다.

비유: 외투 보관소

붐비는 행사장에서 외투를 보관소에 맡기고 번호표를 받습니다. 편리하고, 대개 외투는 돌아옵니다. 하지만 그날 저녁 내 손에 있는 것은 외투가 아니라 번호표입니다. 보관소가 털리거나, 일찍 문을 닫거나, 몰래 외투를 다른 사람에게 빌려줬다면, 번호표의 가치는 카운터 뒤에 있는 사람들의 신용만큼일 뿐입니다. 외투를 입고 있으면 덜 편하지만, 나 말고는 아무도 그것을 잃어버릴 수 없습니다.

거래소에 대해 역사가 말해 주는 것

대부분의 거래소는 망하지 않습니다. 하지만 큰 거래소가 무너졌을 때 고객들은 몇 년을 기다렸고, 돈의 상당 부분을 잃는 경우가 많았습니다.

거래소	무슨 일이 있었나	고객들이 겪은 일
Mt. Gox (2014)	당대 최대의 비트코인 거래소가 해킹과 부실 경영으로 약 85만 BTC를 잃음	남은 자산의 상환은 10년 뒤인 2024년 7월에야 시작됨
QuadrigaCX (2019)	창업자가 사망했고, 그 혼자만 관리하던 콜드 월렛은 거의 비어 있었음	약 7만 6천 명의 사용자가 약 2억 1,500만 캐나다달러를 받지 못함
FTX (2022)	계열 트레이딩 회사가 고객 자금을 써 버렸고, 며칠 만에 출금이 멈춤	수십억 달러의 고객 자금이 사라졌고, 창업자는 이후 사기 혐의로 유죄 판결을 받음

세 경우 모두 화면에는 마지막 순간까지 평소와 같은 잔고가 표시되었습니다. 거래소의 잔고는 그 회사에 대한 청구권일 뿐, 코인이 실제로 있다는 증거가 아닙니다.

직접 보관할 때의 위험

자기 수탁은 회사를 그림에서 빼 주지만, 모든 일을 나에게 넘깁니다. 사람들이 스스로 코인을 잃는 가장 흔한 경우는 다음과 같습니다.

- **백업 분실.** 시드 문구를 잃어버리고 기기까지 고장 나면 코인은 영원히 잠깁니다. Chainalysis 연구진은 2017년, 이미 약 280만에서 380만 개의 비트코인이 이렇게 사라졌다고 추정했는데, 당시까지 채굴된 전체 코인의 약 5분의 1에 해당합니다.
- **백업 유출.** 가짜 사이트나 앱에 입력한 시드 문구는 9강에서 본 것처럼 모든 것을 도둑에게 넘겨줍니다.
- **송금 실수.** 8강에서 본 것처럼 잘못된 주소나 네트워크는 되돌릴 수 없습니다.

고객센터도 없고 비밀번호 재설정도 없습니다. 망하거나 내 자금을 동결할 수 있는 회사가 없다는 것의 대가입니다.

대부분의 사람들이 나누는 방법

많은 사람에게 답은 둘 중 하나가 아닙니다. 흔한 방법은 거래소를 주머니 속 지갑처럼, 자기 수탁을 집 안의 금고처럼 다루는 것입니다.

	거래소 계정	내 지갑
키를 가진 쪽	거래소	나
비밀번호를 잊었을 때	고객지원이 보통 접근을 되찾아 줄 수 있음	시드 문구만이 가능
회사가 망하면	코인이 동결되거나 사라질 수 있음	아무것도 달라지지 않음
적합한 용도	활발한 트레이딩과 곧 쓸 금액	장기 보유와 저축
주요 위험	회사: 해킹, 사기, 동결, 파산	나: 백업 분실, 사기, 실수

거래소에 자금을 둔다면, 오랜 이력을 가진 대형 규제 거래소를 고르고, 제공하는 모든 보안 기능을 켜고, 준비금 증명(proof of reserves)을 정기적으로 공개하는지 확인하세요. 준비금 증명은 특정 시점에 거래소가 보유한 자산을 보여 주지만, 거래소가 갚아야 할 모든 부채까지 항상 보여 주는 것은 아니라는 점을 기억하세요.

트레이더에게 왜 중요한가

- **선물과 마진 거래에는 위탁 보관이 필요합니다.** 무기한 선물을 거래하려면 담보가 거래소에 있어야 합니다. 전 재산이 아니라 포지션에 필요한 만큼만 두고, 트레이딩에 필요 없는 수익은 정기적으로 내 지갑으로 옮기세요.
- **경고 신호를 지켜보세요.** 출금이 느려지거나 중단되는 것, 출금 한도가 갑자기 바뀌는 것, 온체인에서 거래소 밖으로 대량의 코인이 빠져나가는 것은 문제가 터지기 전에 자주 나타났습니다. 2022년 11월 초 FTX의 출금은 느려지다가 며칠 만에 멈췄습니다. 첫 신호에 움직이는 것이 마지막 신호에 움직이는 것보다 쉽습니다.
- **자기 수탁에는 속도라는 비용이 있습니다.** 지갑에서 거래소로 코인을 옮기려면 시간과 네트워크 수수료가 들고, 빠른 장에서는 몇 분이 중요합니다. 변동성이 닥치기 전에, 그 와중이 아니라 미리, 양쪽에 얼마씩 둘지 계획하세요.

핵심 용어

수탁	개인 키에 대한 통제권, 즉 그 키로 열 수 있는 코인에 대한 통제권.
위탁 보관	거래소 계정처럼 회사가 나를 대신해 키를 보관하는 방식.

자기 수탁	내가 통제하는 지갑에 내 키를 직접 보관하는 것으로, 보통 시드 문구로 백업합니다.
거래상대방 위험	내 자산을 보관하는 회사가 파산하거나, 자산을 동결하거나, 돌려주지 않을 위험.
준비금 증명	특정 시점에 거래소가 보유한 자산을 보여 주는 공개 검증으로, 거래소가 갚아야 할 모든 부채를 보여 주지 않을 수 있습니다.
Not your keys, not your coins	'내 키가 아니면 내 코인이 아니다'라는 유명한 말. 다른 사람이 키를 가지고 있다면, 나에게는 코인을 돌려주겠다는 그 사람의 약속만 있을 뿐입니다.

핵심 정리

1. 수탁은 키를 누가 가지고 있느냐입니다. 거래소에서는 회사가, 자기 수탁에서는 내가 가지고 있습니다.
2. 거래소 잔고는 회사 데이터베이스의 숫자이자 그 회사에 대한 청구권이지, 내가 통제하는 코인이 아닙니다.
3. Mt. Gox, QuadrigaCX, FTX는 거래소 파산이 고객 자금을 수년간 묶어 두거나 완전히 날려 버릴 수 있음을 보여 줍니다.
4. 자기 수탁은 회사 위험을 없애지만 개인 위험을 더합니다. 백업 분실, 시드 문구 유출, 송금 실수입니다.
5. 많은 사람이 트레이딩 자금은 믿을 만한 거래소에, 장기 보유 자산은 내 지갑에 둡니다.

실력 점검

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

1. 암호화폐에서 수탁(custody)이란 무슨 뜻인가요?

- A 개인 키를 누가 가지고 있는가
- B 어느 거래소의 수수료가 가장 낮은가
- C 코인을 얼마나 오래 보유할 계획인가
- D 어느 나라가 코인을 규제하는가

2. 거래소 계정에 1 BTC가 있습니다. 실제로 가지고 있는 것은 무엇인가요?

A 내 이름으로 저장된 개인 키
B 거래소 데이터베이스에 기록된, 거래소에 대한 청구권
C 나만 통제하는 개인 주소의 코인
D 거래소가 보관하는 하드웨어 지갑

3. QuadrigaCX 고객들이 돈을 돌려받지 못한 핵심 이유는 무엇인가요?

A 비트코인 네트워크가 멈췄다
B 고객들이 시드 문구를 잃어버렸다
C 창업자 혼자 지갑을 관리했고, 그가 사망했을 때 지갑은 거의 비어 있었다
D 정부가 캐나다의 모든 거래소를 압수했다

4. 자기 수탁은 어떤 위험을 없애 주나요?

A 시드 문구를 잃어버릴 위험
B 잘못된 주소로 보낼 위험
C 피싱 위험
D 거래소가 내 코인을 동결하거나 잃어버릴 위험

5. 두 모델 사이에 자금을 나누는 흔한 방법은 무엇인가요?

A 편의를 위해 전부 거래소에 둔다
B 트레이딩 자금은 믿을 만한 거래소에, 장기 저축은 내 지갑에 둔다
C 선물 담보까지 포함해 전부 자기 수탁한다
D 가능한 한 많은 거래소에 똑같이 나눈다

6. 준비금 증명이 보여 주지 못할 수 있는 것은 무엇인가요?

A 거래소가 보유한 코인
B 거래소의 지갑 주소
C 거래소가 고객과 대출자에게 갚아야 할 모든 부채
D 검증한 날짜

정답 및 해설

1 A

개인 키를 누가 가지고 있는가

개인 키를 가진 사람이 코인을 통제합니다. 수탁은 그 사람이 누구냐는 질문일 뿐입니다.

2 B

거래소 데이터베이스에 기록된, 거래소에 대한 청구권

거래소는 공용 주소의 키를 가지고 있습니다. 내 잔고는 거래소가 나에게 얼마를 빚지고 있는지에 대한 기록입니다.

3 C

창업자 혼자 지갑을 관리했고, 그가 사망했을 때 지갑은 거의 비어 있었다

한 사람이 키를 통제했고 자금이 유용되었기 때문에, 그가 사망한 뒤 대부분의 돈을 되찾을 방법이 없었습니다.

4 D

거래소가 내 코인을 동결하거나 잃어버릴 위험

내 키를 직접 가지고 있으면 어떤 회사도 내 코인을 동결하거나, 빌려주거나, 잃어버릴 수 없습니다. 남는 위험은 내 실수와 사기입니다.

5 B

트레이딩 자금은 믿을 만한 거래소에, 장기 저축은 내 지갑에 둔다

트레이딩에는 거래소에 자금이 있어야 하고, 저축은 내 지갑에 있어야 회사 위험으로부터 더 안전합니다. 각자 잘하는 일을 맡는 것입니다.

6 C

거래소가 고객과 대출자에게 갚아야 할 모든 부채

준비금 증명은 특정 시점의 자산을 보여 줍니다. 부채 전체를 보여 주지 않으면 거래소가 모두에게 갚을 수 있다는 것을 증명할 수 없습니다.

출처

- The Block, Mt. Gox 2024년 7월부터 비트코인 상환 시작: https://www.theblock.co/post/301448/mt-gox-to-distribute-9-billion-of-bitcoin-bitcoin-cash-repayments-from-beginning-of-july
- Crowdfund Insider, QuadrigaCX 관재인 보고서: 사용자 7만 6천 명, 2억 1,500만 달러 손실: https://www.crowdfundinsider.com/2019/05/147401-quadrigacx-trustees-final-report-finds-not-much-left-for-76-000-exchange-users-who-lost-215-million/
- 위키백과, FTX 파산: https://en.wikipedia.org/wiki/Bankruptcy_of_FTX
- Cointelegraph, 최대 400만 개의 비트코인이 영원히 사라졌을 수 있다 (Chainalysis 추정): https://cointelegraph.com/news/up-to-four-million-bitcoins-gone-forever

Market Talks

계속 학습하기

다음: 11강
거래가 처리되는 과정

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.