Market Talks
교육 센터

암호화폐 · 초급 · 15강 중 15강

실제로 시작하는 법: 거래소, KYC, 지갑

거래소 고르기, KYC 통과, 계정 보안 설정, 첫 매수, 자기 수탁 지갑 만들기, 그 지갑으로 자금 옮기기까지 첫 실전 단계가 어떻게 이루어지는지 살펴봅니다

읽는 시간 12분 퀴즈 8문항, 정답 포함

암호화폐 · 초급 · 15강 중 15강

실제로 시작하는 법: 거래소, KYC, 지갑

한 문장 요약

대부분의 사람은 중앙화 거래소에서 암호화폐를 시작하고, 나중에 스스로 통제하는 지갑을 더합니다. 이 강에서는 각 단계가 무엇을 포함하는지, 흔한 실수는 어디서 생기는지 하나씩 살펴봅니다.

암호화폐를 보관하는 두 가지 방법

계정을 열기 전에, 암호화폐를 보관하는 기본적인 두 가지 방법을 알아 두면 도움이 됩니다.

- **거래소에 보관(수탁형):** Binance나 Coinbase 같은 회사에 계정을 엽니다. 개인 키는 거래소가 보관하고, 내 잔고는 은행 계좌 속 돈처럼 그 회사 데이터베이스에 적힌 숫자입니다. 간단하고, 비밀번호를 잊어버려도 거래소가 다시 접속하도록 도와줄 수 있습니다.
- **내 지갑에 보관(자기 수탁):** MetaMask 같은 지갑을 설치하거나 Ledger 같은 하드웨어 기기를 씁니다. 키는 시드 문구를 통해 내가 가집니다. 누구도 내 코인을 동결하거나 대신 잃어버릴 수 없지만, 누구도 대신 되찾아 줄 수도 없습니다.

둘의 차이를 요약하는 유명한 말이 있습니다. **"내 키가 아니면 내 코인이 아니다"**(not your keys, not your coins). 많은 사람이 둘 다 씁니다. 사고팔 때는 거래소를, 블록체인 위에서 암호화폐를 보관하고 쓸 때는 지갑을 씁니다(9강과 12강, 블록체인 과정 9강).



그림 1. 거래소에서는 회사가 키를 보관하고, 자기 수탁 지갑에서는 내가 보관합니다.

예시: 거래소가 무너질 때

2022년 11월 거래소 FTX가 파산했고, 고객들은 오랫동안 자금을 출금하지 못했습니다. 2025년 2월에는 FBI가 북한과 연계되었다고 밝힌 해커들이 Bybit에서 약 **15억 달러** 상당의 이더를 훔쳤습니다. Bybit는 출금을 계속 열어 두었고 고객 손실을 보전하겠다고 밝혔지만, 두 사례가 보여 주는 점은 같습니다. 거래소에 있는 코인은 그 회사의 보안과 정직성에 달려 있습니다.

거래소 고르기

중앙화 거래소(9강)는 일반 화폐가 암호화폐로 바뀌는 곳으로, 가장 흔한 진입로입니다. 사람들이 흔히 비교하는 점은 다음과 같습니다.

- **이용 가능 여부와 인허가:** 그 거래소가 내가 사는 나라의 이용자에게 서비스할 수 있는지, 어느 규제 기관이 감독하는지.
- **입금 방법:** 은행 송금, 카드, 현지 결제 수단, 그리고 지원하는 통화.
- **코인과 네트워크:** 어떤 코인이 상장되어 있는지, 입출금에 어떤 네트워크를 지원하는지(5강).
- **수수료:** 거래 수수료, 카드 수수료, "간편 매수"의 스프레드, 출금 수수료.
- **이력:** 해킹이나 출금 중단을 겪은 적이 있는지, 준비금 증명을 공개하는지.

거래소	특징
Binance	거래량 기준 세계 최대 거래소, 매우 많은 상장 코인
Coinbase	미국 상장 기업, 간단한 앱, 미국과 유럽에서 강세
OKX	자기 수탁 지갑이 내장된 글로벌 거래소
Bybit	파생상품 거래로 인기 있는 글로벌 거래소
Kraken	가장 오래된 거래소 중 하나, 미국과 유럽에서 강세
Upbit	한국 최대 거래소, 원화로 거래

이 이름들은 널리 쓰이는 서비스의 예시일 뿐이며, **추천이 아닙니다**. 서비스와 규칙은 바뀌고, 모든 거래소를 모든 나라에서 이용할 수 있는 것도 아닙니다. 한국처럼 일부 국가에서는 현지 거래소가 제휴 은행의 실명 확인 입출금 계정(real-name bank account)도 요구합니다.

가입과 KYC

규제를 받는 거래소는 고객이 누구인지 확인해야 합니다. 이를 **KYC**라고 하며, "know your customer"(고객 확인)의 줄임말입니다. 대부분의 나라에서 자금세탁방지(AML) 법의 일부입니다. 일반적인 가입 과정은 다음과 같습니다.

1. **계정:** 이메일 또는 휴대폰 번호와 비밀번호.
2. **개인 정보:** 이름, 생년월일, 주소, 국적.
3. **신분증:** 여권, 신분증, 운전면허증 중 하나의 사진.
4. **셀카 또는 영상 확인:** 앱이 얼굴이 신분증과 일치하는지, 실제 사람이 있는지 확인합니다.
5. **승인:** 몇 분 안에 끝나는 경우가 많고, 며칠이 걸리기도 합니다. 일부 거래소는 더 높은 한도를 위해 나중에 주소 증명이나 자금 출처 증빙을 요청합니다.

트래블룰(Travel Rule)이라는 관련 규칙에 따라, 많은 나라의 거래소는 거래소 사이의 큰 금액 전송에 대해 보내는 사람과 받는 사람의 정보도 공유하며, 출금하려는 지갑의 소유자가 누구인지 물을 수도 있습니다.

KYC는 거래소가 민감한 개인 정보를 보관한다는 뜻이기도 합니다. 진짜 사이트인지가 중요한 이유 중 하나입니다. 가짜 거래소 사이트도 신분증 사진을 수집합니다(14강).



그림 2. 거래소 계정을 열 때 거치는 일반적인 KYC 단계입니다.

계정 보안 설정

거래소 계정은 공격의 표적이 되기 때문에, 거래소는 여러 겹의 보호 장치를 제공합니다. 가장 먼저 켜는 경우가 많은 것들은 다음과 같습니다.

- **2단계 인증(2FA):** 로그인과 출금에 필요한 두 번째 코드입니다. Google Authenticator 같은 인증 앱, 패스키나 보안 키는 SIM 스와프로 가로챌 수 있는 SMS 코드보다 훔치기 어렵습니다.
- **피싱 방지 코드:** 내가 정한 단어로, 거래소가 보내는 모든 진짜 이메일에 들어갑니다. 이 단어가 없는 이메일은 거래소가 보낸 것이 아닙니다.
- **출금 주소 화이트리스트:** 미리 저장해 둔 주소로만 출금이 허용되며, 새 주소에는 대기 기간이 붙는 경우가 많습니다.

- **기기와 로그인 알림:** 누군가 새 기기나 새 위치에서 로그인하면 알림이 옵니다.
- 다른 곳에서는 쓰지 않는 **고유하고 강력한 비밀번호**.

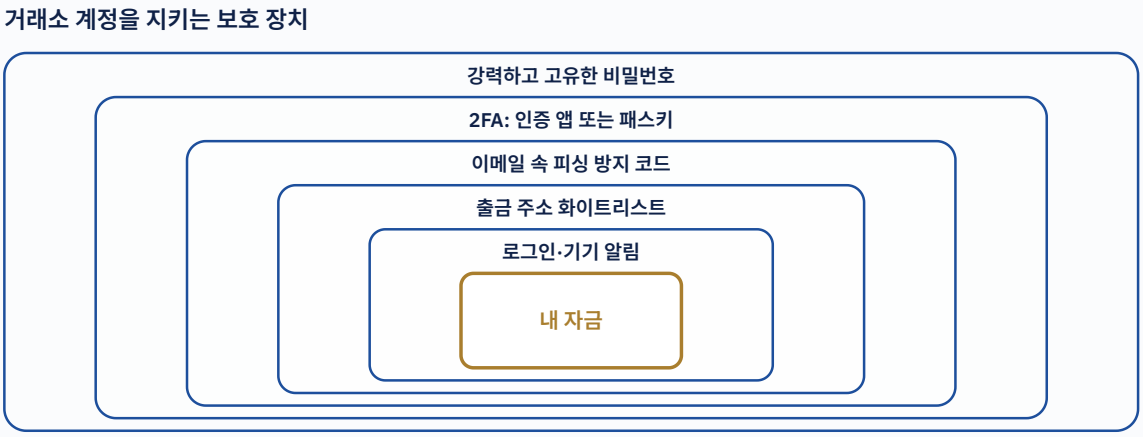


그림 3. 거래소는 여러 겹의 계정 보호 장치를 제공합니다.

첫 매수하기

계정 인증이 끝나면 돈을 입금하고 암호화폐로 바꿉니다.

- **입금:** 보통 은행 송금이 가장 저렴합니다. 카드는 더 빠르지만 몇 퍼센트의 비용이 드는 경우가 많습니다. 일부 거래소는 이용자끼리 거래소를 통해 직접 거래하는 P2P 마켓도 제공합니다.
- **"매수" 또는 "전환" 버튼:** 가장 간단한 방법입니다. 금액을 입력하면 견적이 나옵니다. 수수료는 더 넓은 가격 차이(스프레드)에 숨어 있는 경우가 많습니다.
- **현물 시장:** 호가창이 있는 거래 화면입니다(9강). 시장가 주문은 가능한 가장 좋은 가격에 사고, 지정가 주문은 내가 정한 가격을 기다립니다. 이곳의 수수료는 보통 더 낮습니다.

매수가 끝나면 코인은 거래소 계정에 있습니다. 그곳에서 그대로 둘 수도, 팔 수도, 지갑으로 출금할 수도 있습니다.

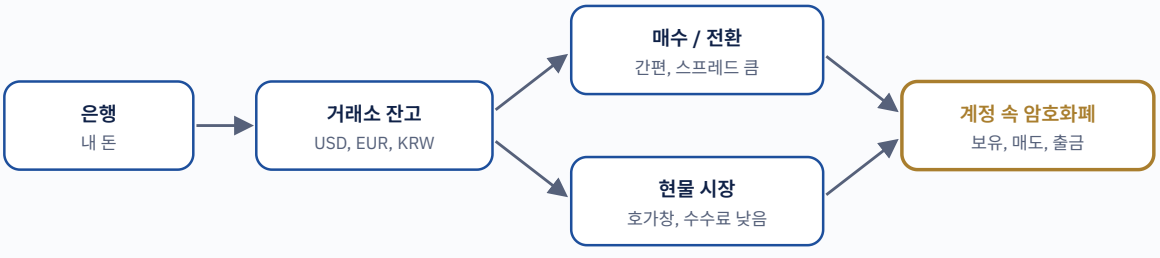


그림 4. 돈을 입금한 뒤 거래소에서 매수하는 두 가지 방법입니다.

예시: 두 가지 매수 방법

Sophie는 은행 송금으로 500달러를 입금합니다. 간단한 "매수" 버튼으로 250달러어치 비트코인을 사는데, 견적에 약 1%의 스프레드가 포함되어 있어 예상보다 조금 적게 받습니다. 나머지 250달러로는 현물 시장에서 시장가 주문을 넣고, 0.1%인 약 25센트의 거래 수수료를 냅니다. 둘 다 평범한 매수 방법이며, 차이는 주로 비용과 거래 화면을 얼마나 다루고 싶은지에 있습니다.

지갑: 핫 월렛, 콜드 월렛, 흔히 쓰이는 이름들

자기 수탁 지갑은 키를 저장하고 트랜잭션에 서명하는 앱이나 기기입니다(블록체인 과정 9강). 주요 유형은 다음과 같습니다.

- **핫 월렛**은 인터넷에 연결되어 있습니다. 모바일 앱과 브라우저 확장 프로그램이 여기에 속합니다. 무료이고, 일상적으로 쓰거나 디파이 앱에 연결하기에 편리합니다.
- **콜드 월렛**은 키를 오프라인에 두며, 보통 작은 하드웨어 기기를 씁니다. 트랜잭션은 기기의 버튼을 눌러 승인하므로, 컴퓨터에 있는 악성코드가 혼자 서명할 수 없습니다.

지갑	유형	주요 네트워크
MetaMask	브라우저 확장 프로그램, 모바일 앱	이더리움과 BNB Chain, Base, Arbitrum 같은 다른 EVM 네트워크, 이제 Solana와 비트코인도 지원
Trust Wallet	모바일 앱, 확장 프로그램	BNB Chain, 이더리움, 비트코인을 포함한 여러 네트워크
Phantom	모바일 앱, 확장 프로그램	Solana 중심, 이더리움, Base, 비트코인도 지원
Ledger	하드웨어 지갑	여러 네트워크, 자체 앱 Ledger Live나 다른 지갑과 함께 사용
Trezor	하드웨어 지갑	여러 네트워크, 자체 앱 Trezor Suite나 다른 지갑과 함께 사용

다시 말하지만, 이들은 흔한 예시일 뿐이며 추천이 아닙니다. 지갑 앱은 가짜가 특히 많이 만들어지는 대상이어서, 사람들은 보통 공식 웹사이트나 그곳에 걸린 링크를 통해서만 내려받습니다. 하드웨어 지갑은 중고 기기나 조작된 기기가 안전하지 않을 수 있어서 보통 제조사에서 직접 구입합니다.

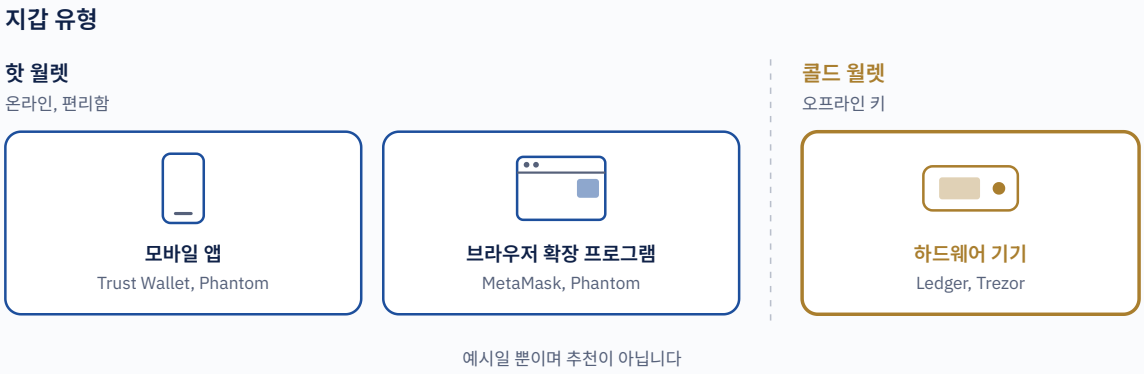


그림 5. 핫 월렛은 온라인이라 편리하고, 콜드 월렛은 키를 오프라인에 보관합니다. 이름은 예시일 뿐이며 추천이 아닙니다.

지갑 설정과 시드 문구

새 지갑을 만들면 12개 또는 24개 단어로 된 **시드 문구**(복구 문구라고도 합니다)가 표시됩니다. 이 단어들만 있으면 호환되는 어떤 앱이나 기기에서든 지갑의 모든 키를 다시 만들 수 있습니다. 그 의미는 다음과 같습니다.

- 시드 문구를 본 사람은 누구든 지갑 속 모든 것을 가져갈 수 있습니다.
- 휴대폰을 잃어버렸는데 시드 문구도 잃어버렸다면 자금은 영영 사라집니다. 지갑 회사는 사본을 가지고 있지 않으며 재설정할 수도 없습니다.

일반적인 관행은 단어를 종이에 적거나 금속판에 새기고, 꼼꼼히 확인한 뒤, 오프라인의 안전한 곳에, 때로는 두 곳에 나누어 보관하는 것입니다. 스크린샷, 사진, 클라우드 메모, 이메일, 온라인으로 동기화되는 비밀번호 관리자는 시드 문구가 도난당하는 흔한 경로입니다. 진짜 지원 담당자, 앱, 웹사이트는 결코 시드 문구를 필요로 하지 않습니다(14강).

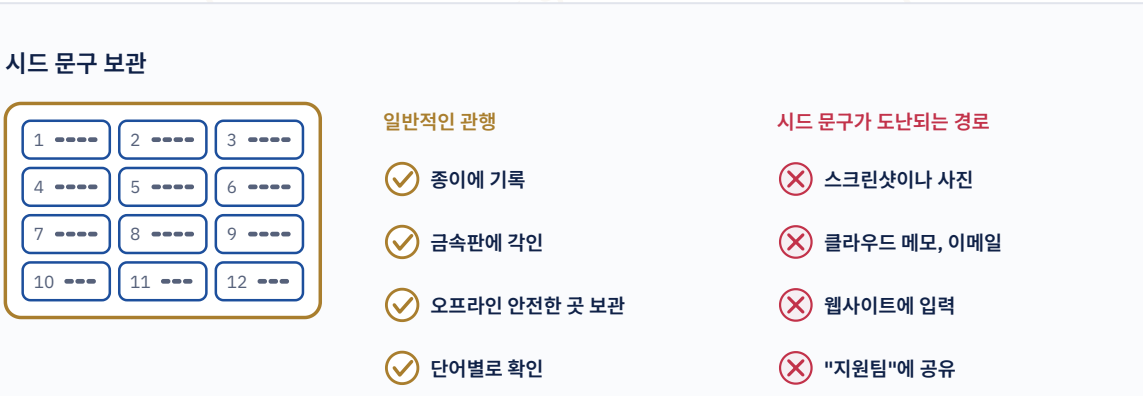


그림 6. 시드 문구가 지갑을 통제합니다. 어떻게 보관하느냐에 따라 누가 자금을 가져갈 수 있는지가 정해집니다.

지갑으로 자금 옮기기와 첫 스왑

거래소에서 내 지갑으로 출금할 때는 10강에서 다룬 내용을 모두 쓰게 됩니다.

1. 지갑에서 올바른 네트워크의 **입금 주소**를 복사합니다.
2. 거래소에서 **출금**을 선택하고, 주소를 붙여 넣은 뒤 **같은 네트워크**를 고릅니다. 메모 태그는 받는 쪽에서 필요할 때만 넣습니다.
3. 주소의 처음과 마지막 글자를 확인합니다.
4. 많은 사람이 먼저 **소액 테스트 전송**을 하고, 그것이 도착하면 나머지를 보냅니다.

그 네트워크에서 지갑을 쓰려면 **가스비로 쓸 기본 코인**도 조금 있어야 합니다. 이더리움의 ETH, BNB Chain의 BNB, Solana의 SOL 같은 것입니다(5강).

탈중앙화 거래소(9강)에서의 첫 스왑은 다음과 같이 진행됩니다. 공식 DEX 사이트를 열고, 지갑을 **연결**하고, 두 토큰을 고르고, 가격 영향과 슬리피지를 확인하고, 요청이 있으면 토큰을 **승인**하고(승인이 왜 중요한지는 14강에서 설명합니다), 마지막으로 지갑에서 스왑을 **확인**하고 가스비를 냅니다.



그림 7. 거래소에서 자기 수탁 지갑으로 자금을 옮긴 뒤, DEX에서 첫 스왑을 하는 과정입니다.

전체 과정을 한눈에

이 강의 내용을 모으면, 일반적인 첫 설정은 여덟 단계로 이루어집니다. 모든 사람이 모든 단계를 거치지는 않습니다. 거래소만 쓰는 사람도 많고, 시간이 지난 뒤 자기 수탁으로 옮겨 가는 사람도 있습니다.

이 강으로 암호화폐 초급 단계가 마무리됩니다. 이제 암호화폐가 무엇인지, 코인과 토큰과 네트워크가 어떻게 다른지, 어디서 거래되는지, 가격이 어떻게 움직이는지, 주요 위험이 무엇인지, 그리고 첫 실전 단계가 어떻게 이루어지는지 알게 되었습니다. 회원용 암호화폐 중급 및 고급 과정에서는 트레이딩, 온체인 데이터, 디파이를 더 깊이 다룹니다.



그림 8. 거래소 계정부터 첫 DEX 스왑까지, 일반적인 첫 설정입니다.

트레이더에게 왜 중요한가

- **거래소 선택은 비용에 영향을 줍니다.** 거래 수수료, 스프레드, 펀딩비, 출금 수수료는 거래가 많아질수록 쌓입니다. 수수료 등급은 거래량에 따라 달라지는 경우가 많습니다.
- **거래 상대방 위험은 실제로 존재합니다.** 거래를 위해 거래소에 둔 자금은 그 거래소에 달려 있습니다. 많은 트레이더가 거래에 필요한 만큼만 그곳에 두고 나머지는 다른 곳에 보관합니다.
- **보안 설정이 거래 계정을 지킵니다.** 2FA, 피싱 방지 코드, 출금 주소 화이트리스트가 있으면 도난당한 비밀번호가 공격자에게 훨씬 덜 쓸모 있어집니다.
- **거래소와 지갑 사이의 이동은 일상적인 일입니다.** 올바른 네트워크를 고르고 주소를 확인하는 일은 활발한 트레이더에게 매일의 습관이 됩니다.

핵심 용어

수탁형	거래소 같은 회사가 나를 대신해 개인 키를 보관하는 방식입니다.
자기 수탁	내가 통제하는 지갑에 직접 키를 보관하는 방식으로, 어떤 회사도 자금을 동결하거나 되찾아 줄 수 없습니다.
KYC	Know your customer(고객 확인). 규제를 받는 거래소가 고객에게 서비스하기 전이나 서비스하는 동안 반드시 해야 하는 신원 확인입니다.
트래블룰	특정 전송에 대해 거래소가 보내는 사람과 받는 사람의 정보를 공유하도록 하는 규칙입니다.
2FA	2단계 인증. 비밀번호에 더해 인증 앱의 코드 같은 두 번째 신원 증명을 쓰는 것입니다.

피싱 방지 코드	거래소가 진짜 이메일에 넣어 주는 나만의 단어로, 가짜 이메일을 알아보는 데 쓰입니다.
출금 주소 화이트리스트	계정에서 출금을 받을 수 있도록 허용된 주소만 미리 저장해 둔 목록입니다.
핫 월렛	휴대폰 앱이나 브라우저 확장 프로그램처럼 인터넷에 연결된 기기에 키가 있는 지갑입니다.
콜드 월렛	보통 하드웨어 기기에 키를 오프라인으로 보관하는 지갑입니다.
시드 문구	지갑의 모든 키를 다시 만들 수 있는 12개 또는 24개 단어의 목록입니다.
EVM 네트워크	이더리움 가상 머신(EVM)을 실행하는 블록체인으로, 이더리움과 같은 지갑, 주소, 앱을 쓸 수 있습니다. BNB Chain, Base, Arbitrum, Polygon이 그 예입니다.

핵심 정리

1. 암호화폐는 거래소(수탁형)나 내 지갑(자기 수탁)에 보관할 수 있습니다. 많은 사람이 둘 다 씁니다.
2. 거래소마다 이용 가능 여부, 입금 방법, 코인, 네트워크, 수수료, 이력이 다릅니다. 이 강에 나온 이름은 예시일 뿐이며 추천이 아닙니다.
3. KYC는 자금세탁방지 법에 따라 요구되는 신분증 및 셀카 확인입니다.
4. 인증 앱이나 패스키를 쓰는 2FA, 피싱 방지 코드, 출금 주소 화이트리스트가 주요 계정 보호 장치입니다.
5. 핫 월렛은 편리하고, 콜드 월렛은 키를 오프라인에 둡니다. 시드 문구는 모든 것을 통제하며 재설정할 수 없습니다.
6. 지갑으로 출금하려면 올바른 주소, 같은 네트워크, 가스비로 쓸 약간의 기본 코인이 필요합니다. DEX 스왑은 연결, 승인, 확인으로 이루어집니다.

실력 점검

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

1. "내 키가 아니면 내 코인이 아니다"는 무슨 뜻인가요?

A 거래소에 있는 코인은 언제나 사라진다
B 다른 사람이 키를 보관하면 내 코인은 그 사람에게 달려 있다
C 개인 키는 비트코인에만 필요하다
D 암호화폐를 사려면 하드웨어 지갑이 있어야 한다

2. 규제를 받는 거래소는 왜 신분증과 셀카를 요구하나요?

A 거래 수수료를 정하려고
B KYC와 자금세탁방지 법 때문에
C 네트워크를 고르려고
D 시드 문구를 만들려고

3. 피싱 방지 코드란 무엇인가요?

A 출금용 비밀번호
B 거래소가 진짜 이메일에 넣는 단어
C 모든 로그인을 막는 코드
D 하드웨어 지갑의 한 종류

4. 다음 중 가장 훔치기 쉬운 2FA 방식은?

A 인증 앱
B 하드웨어 보안 키
C SMS 코드
D 패스키

5. 핫 월렛과 콜드 월렛의 주된 차이는 무엇인가요?

A 핫 월렛은 비트코인만 보관한다
B 콜드 월렛은 키를 오프라인에 둔다
C 핫 월렛에는 시드 문구가 없다
D 콜드 월렛은 트랜잭션을 보낼 수 없다

6. Anna는 휴대폰을 잃어버렸고, 시드 문구를 적어 둔 적이 없습니다. Anna의 자기 수탁 지갑은 어떻게 되나요?

A 지갑 회사가 재설정해 준다
B 거래소가 복구해 준다
C 더 이상 자금에 접근할 수 없다
D 블록체인이 코인을 돌려보낸다

7. Lucas는 거래소에서 BNB Chain에 있는 자기 지갑으로 USDT를 출금합니다. 거래소에서 어떤 네트워크를 골라야 하나요?

A 아무 네트워크나, 모두 같다
B 가장 큰 네트워크인 이더리움
C 지갑 주소와 같은 네트워크인 BNB Chain
D 비트코인

8. Lucas의 USDT는 도착했지만, 수수료를 낼 수 없어서 스왑이 실패합니다. 무엇이 빠졌나요?

A 시드 문구
B 가스비로 쓸 약간의 BNB
C KYC 승인
D 피싱 방지 코드

정답 및 해설

1 B

다른 사람이 키를 보관하면 내 코인은 그 사람에게 달려 있다

거래소에서는 회사가 키를 보관하므로, 내 잔고는 그 회사의 보안과 정직성에 달려 있습니다.

2 B

KYC와 자금세탁방지 법 때문에

KYC 확인은 대부분의 나라에서 규제를 받는 거래소의 법적 의무입니다.

3 B

거래소가 진짜 이메일에 넣는 단어

거래소가 보냈다는 이메일에 내 코드가 없다면 진짜가 아닙니다.

4 C

SMS 코드

SMS 코드는 공격자가 내 전화번호를 자기 SIM 카드로 옮기는 SIM 스와프로 가로챌 수 있습니다.

5 B

콜드 월렛은 키를 오프라인에 둔다

핫 월렛은 인터넷에 연결된 기기에 키를 두고, 콜드 월렛은 키를 오프라인에 둔 채 기기에서 트랜잭션을 승인합니다.

6 C

더 이상 자금에 접근할 수 없다

키를 다시 만들 수 있는 것은 시드 문구뿐입니다. 시드 문구가 없으면 누구도 자금을 되찾을 수 없습니다.

7 C

지갑 주소와 같은 네트워크인 BNB Chain

보내는 네트워크와 받는 네트워크가 일치해야 합니다. 그렇지 않으면 자금을 잃거나 되찾기 어려울 수 있습니다(10강).

8 B

가스비로 쓸 약간의 BNB

네트워크의 모든 트랜잭션은 그 네트워크의 기본 코인으로 비용을 냅니다. 여기서는 BNB Chain의 BNB입니다.

출처

- TRM Labs, Bybit 해킹: 북한 최대 규모의 탈취 추적: https://www.trmlabs.com/post/the-bybit-hack-following-north-koreas-largest-exploit
- TechTarget, FBI: 15억 달러 Bybit 탈취의 배후는 Lazarus Group: https://www.techtarget.com/cybersecurity/news/366619872/FBI-Lazarus-Group-behind-15-billion-Bybit-heist
- The Block, MetaMask 멀티체인 전환: 하나의 계정으로 EVM, Solana, 곧 비트코인까지 지원: https://theblock.co/post/376450/metamask-multichain-account
- Cointelegraph, MetaMask 비트코인 지원 추가: https://cointelegraph.com/news/metamask-adds-bitcoin-support-after-teasing-february

- Tiger Research, 2026년 한국 암호화폐 시장: https://reports.tiger-research.com/p/2026-korea-cryptocurrency-market-eng

Market Talks

계속 학습하기

이 강의는 MARKET TALKS 교육 센터의 암호화폐 과정에 속합니다. 초급 강의는 무료이며 강의마다 퀴즈와 다운로드 가능한 PDF가 제공됩니다. 중급과 고급 강의는 회원 전용입니다.

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.