Market Talks
교육 센터

암호화폐 · 초급 · 15강 중 10강

안전하게 보내고 받기: 네트워크, 주소, 메모 태그

출금 화면의 각 항목이 무엇을 뜻하는지, 왜 양쪽 네트워크가 같아야 하는지, 언제 메모나 태그가 필요한지, 그리고 비슷하게 생긴 주소로부터 자신을 어떻게 지키는지

읽는 시간 10분 퀴즈 8문항, 정답 포함

암호화폐 · 초급 · 15강 중 10강

안전하게 보내고 받기: 네트워크, 주소, 메모 태그

한 문장 요약

암호화폐 전송은 되돌릴 수 없으므로, 모든 출금은 네 가지를 정확히 맞추는 데 달려 있습니다. 코인, 네트워크, 주소, 그리고 필요할 때는 메모나 태그입니다.

되돌리기 버튼은 없습니다

엉뚱한 계좌로 보낸 은행 송금은 때로 되돌릴 수 있습니다. 블록체인 트랜잭션은 그럴 수 없습니다. 일단 확인되면 네트워크도, 여러분의 지갑도, 대개는 거래소도 되돌리지 못합니다. 암호화폐를 검열에 강하게 만드는 바로 그 특성이며, 전송 버튼을 누르기 전에 모든 세부 사항이 정확해야 한다는 뜻이기도 합니다.

다행히 큰 손실로 이어지는 실수는 거의 모두 한 화면에 있는 몇 가지 항목에서 생깁니다. 이 강의에서는 그 항목들을 하나씩 살펴봅니다.

출금 화면 뜯어보기

거래소에서 출금하든 자기 지갑에서 보내든, 채우는 항목의 종류는 같습니다.

- **코인:** USDT처럼 무엇을 보내는지입니다.
- **네트워크:** Tron(TRC-20)이나 Ethereum(ERC-20)처럼 전송에 어떤 블록체인을 쓸지입니다.
- **주소:** 어디로 보내는지입니다. 반드시 같은 네트워크의 주소여야 합니다.
- **메모 또는 태그:** 일부 코인과 일부 받는 쪽에만 필요한 추가 숫자나 텍스트입니다.
- **수량:** 얼마를 보낼지입니다.
- **수수료:** 네트워크 수수료나 출금 수수료로, 수량에서 빠지거나 수량에 더해집니다.

확인 전에 대부분의 거래소는 무엇이 도착할지 요약을 보여 줍니다. 그 요약을 천천히 읽는 것이 이 강의에서 가장 유용한 습관입니다.



그림 1. 일반적인 출금 화면. 코인, 네트워크, 주소는 실수했을 때 손실이 가장 큰 세 항목입니다.

양쪽 네트워크가 같아야 합니다

5강에서 USDT가 Tron, Ethereum, BNB Chain, Solana 등에 각각 별도의 토큰으로 존재한다는 것을 보았습니다. 보낼 때 고르는 네트워크는 받는 쪽이 그 코인에 대해 지원하는 네트워크여야 하고, 주소도 그 네트워크의 것이어야 합니다.

언제나 받는 쪽에서 시작하세요. 받는 거래소나 지갑에서 코인을 고르고, 그다음 네트워크를 고른 뒤, 표시되는 입금 주소를 복사합니다. 그런 다음 보내는 쪽에서 정확히 같은 네트워크를 고릅니다.

네트워크가 맞지 않으면 어떻게 될까요?

- Ethereum 네트워크에 Tron 주소를 넣는 경우처럼 주소 형식이 다르면, 보통 앱이 전송을 거부합니다. 운이 좋은 경우입니다.
- Ethereum과 BNB Chain처럼 두 네트워크가 같은 **0x** 주소 형식을 쓰면 전송은 이루어지지만, 받는 쪽이 지켜보지 않는 네트워크로 갈 수 있습니다. 자기 지갑으로 보낸 자금은 지갑에 그 네트워크를 추가하면 찾을 수 있는 경우가 많습니다. 거래소로 보낸 자금은 복구 요청이 필요할 수 있으며, 몇 주가 걸리거나 수수료가 들거나 거절될 수도 있습니다.



그림 2. 양쪽 네트워크가 같아야 합니다. 주소 형식이 다르면 보통 거부되지만, 0x 형식을 함께 쓰는 네트워크는 전송을 받아들이기 때문에 자금이 묶일 수 있습니다.

메모와 태그

일부 코인의 경우 거래소는 여러 고객에게 하나의 공용 입금 주소를 씁니다. 입금이 어느 고객의 것인지 알기 위해 **메모**, **태그** 또는 **데스티네이션 태그**라는 짧은 숫자나 텍스트를 덧붙입니다. 흔한 예로 데스티네이션 태그를 쓰는 XRP, 그리고 메모나 코멘트를 쓰는 Stellar(XLM), TON, Cosmos(ATOM)가 있습니다.

받는 거래소가 주소와 함께 메모나 태그를 보여 준다면, 보낼 때 그것을 메모 칸에 **반드시** 복사해 넣어야 합니다. 메모가 없으면 코인은 거래소의 공용 주소에 도착하지만, 아무도 그것이 여러분의 것인지 알 수 없습니다. 되찾으려면 보통 증빙을 갖춰 고객 지원에 연락해야 하며, 돌려받는다는 보장도 없습니다.

자신의 개인 지갑으로 보낼 때는 주소가 여러분만의 것이므로 대개 메모가 필요 없습니다.

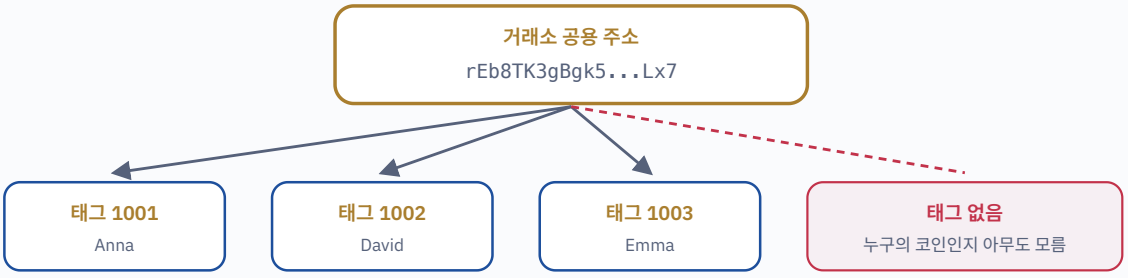


그림 3. XRP 같은 코인에서 거래소는 여러 고객에게 같은 주소를 주고 태그로 고객을 구분하는 경우가 많습니다. 태그 없는 입금은 누구와도 연결할 수 없습니다.

주소 지키기

암호화폐 주소는 길어서 외울 수가 없고, 공격자들은 이 점을 크게 두 가지 방식으로 악용합니다.

- **주소 포이즈닝:** 공격자는 여러분이 쓰는 주소와 앞뒤 글자가 같은 주소를 만든 뒤, 아주 적은 금액이나 가짜 트랜잭션을 보내 그 주소가 여러분의 거래 기록에 나타나게 합니다. 나중에 여러분이 기록에서 실수로 엉뚱한 주소를 복사하게 됩니다. 2024년 5월 한 트레이더는 진짜 주소와 앞뒤가 일치하는 주소를 복사했다가 이런 식으로 약 6,800만 달러어치인 1,155 WBTC를 잃었습니다. 공격자는 협상 끝에 나중에 자금을 돌려주었는데, 이는 극히 드문 일입니다.
- **클립보드 악성코드:** 컴퓨터나 휴대폰에 숨어 있다가 여러분이 붙여 넣는 순간 복사해 둔 주소를 공격자의 주소로 바꿔치기하는 악성 소프트웨어입니다.

간단한 습관으로 둘 다 막을 수 있습니다. 주소는 거래 기록이 아니라 받는 쪽의 입금 페이지에서 복사하고, 절대 손으로 입력하지 말고, 붙여 넣은 뒤에는 앞, 가운데, 끝의 글자를 확인하고, 자주 보내는 주소는 거래소의 **출금 주소 화이트리스트**나 지갑의 주소록을 이용하세요.

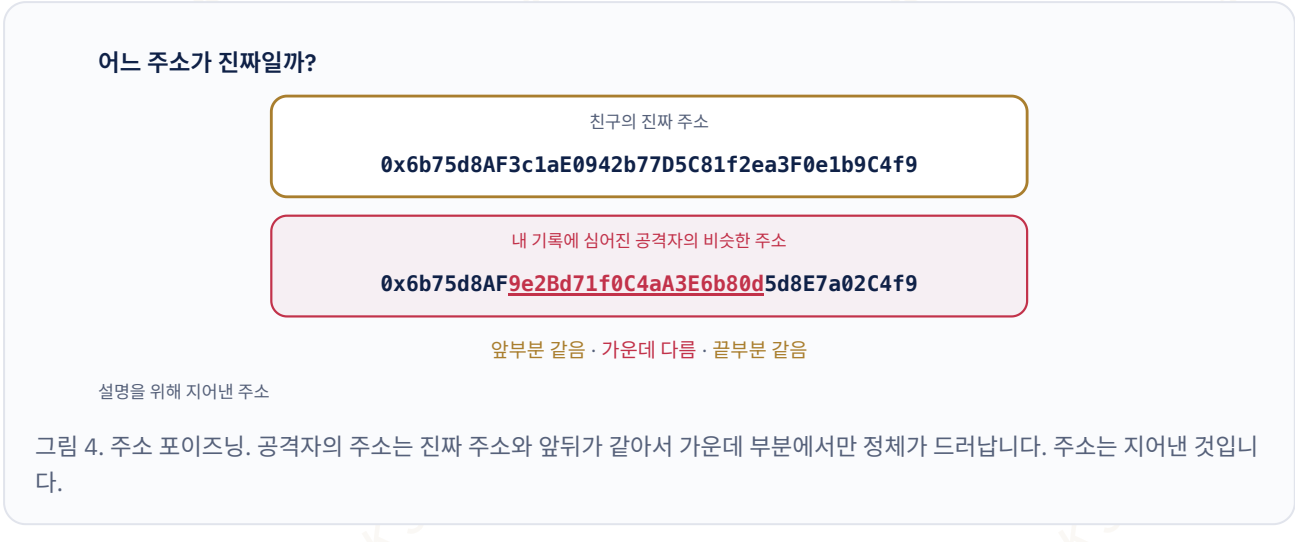


그림 4. 주소 포이즈닝. 공격자의 주소는 진짜 주소와 앞뒤가 같아서 가운데 부분에서만 정체가 드러납니다. 주소는 지어낸 것입니다.

먼저 시험하고, 그다음 추적하기

새 주소로 처음 보낼 때 경험 많은 이용자들은 먼저 소액의 **테스트 전송**을 보내고, 도착할 때까지 기다린 뒤에야 나머지를 보내는 경우가 많습니다. 추가 수수료는 실수의 대가에 비하면 대개 작습니다.

보내고 나면 **트랜잭션 해시**, 즉 TxID를 받습니다. 여러분의 전송을 식별하는 고유한 코드입니다. 이것을 그 네트워크의 블록 탐색기, 예를 들어 Ethereum은 Etherscan, Tron은 Tronscan에 붙여 넣으면 전송이 확인되었는지, 어디로 갔는지 볼 수 있습니다. 거래소는 정해진 횟수의 **확인**(컨펌)이 끝난 뒤에야 입금을 반영하므로, 블록체인에서는 완료로 표시된 전송이 몇 분 뒤에야 계정에 나타날 수 있습니다.

그래도 문제가 생겼다면 빨리 움직이세요. 트랜잭션 해시를 보관하고, 받는 플랫폼의 웹사이트나 앱을 통해 공식 고객 지원에 연락하고, 자금을 되찾아 주겠다며 연락해 오는 사람은 무시하세요. 그런 제안은 거의 언제나 두 번째 사기입니다.

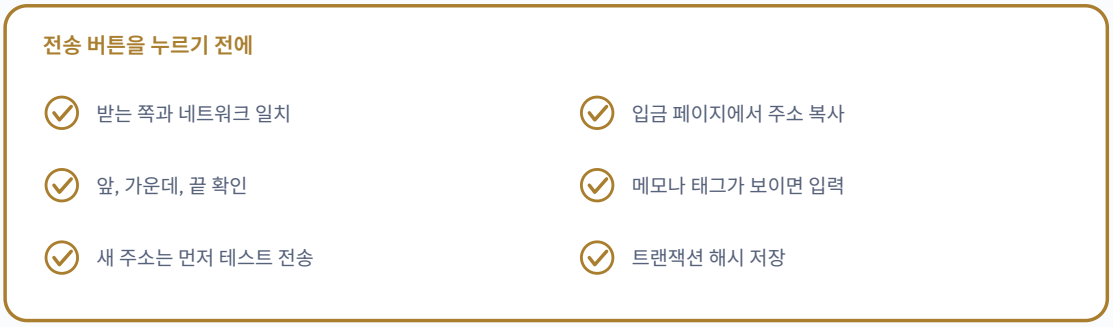


그림 5. 모든 전송에 쓸 수 있는 짧은 체크리스트.

트레이더에게 왜 중요한가

- **자금 이동은 트레이딩의 일부입니다.** 트레이더는 거래소와 지갑 사이로 자주, 때로는 급하게 돈을 옮깁니다. 큰 손실로 이어지는 전송 실수는 대부분 시간에 쫓길 때 일어납니다.
- **네트워크 선택에 따라 속도와 비용이 달라집니다.** Tron이나 Solana의 USDT는 보통 낮은 수수료로 몇 분 안에 도착합니다. 같은 전송이 Ethereum에서는 더 비쌀 수 있고, 비트코인은 확인에 한 시간 이상 걸릴 수 있습니다.
- **거래소는 가끔 네트워크를 멈춥니다.** 업그레이드나 혼잡 중에는 한 네트워크의 입금이나 출금이 중단될 수 있습니다. 보내기 전에 네트워크 상태를 확인하면 자금이 전송 중에 묶이는 일을 피할 수 있습니다.
- **화이트리스트는 안전장치를 하나 더해 줍니다.** 많은 거래소에서 출금을 저장해 둔 주소로만 제한할 수 있으며, 계정이 털렸을 때 도움이 됩니다.

핵심 용어

출금 네트워크	전송을 실어 나를 블록체인으로, 받는 쪽이 그 코인에 대해 지원하는 네트워크여야 합니다.
입금 주소	받는 쪽이 특정 네트워크의 특정 코인에 대해 알려 주는 주소입니다.
메모, 태그, 데스티네이션 태그	공용 주소로 들어온 입금이 어느 고객의 것인지 거래소에 알려 주는 추가 코드입니다.
주소 포이즈닝	비슷하게 생긴 주소를 거래 기록에 심어 두고 여러분이 실수로 복사하기를 노리는 사기입니다.
클립보드 악성코드	복사해 둔 암호화폐 주소를 공격자의 주소로 바꿔치기하는 악성 소프트웨어입니다.

테스트 전송	주소와 네트워크가 맞는지 확인하려고 먼저 보내는 소액 전송입니다.
트랜잭션 해시(TxID)	트랜잭션을 식별하는 고유한 코드로, 블록 탐색기에서 조회할 수 있습니다.
출금 주소 화이트리스트	미리 저장해 둔 주소로만 출금을 허용하는 거래소 설정입니다.

핵심 정리

1. 확인된 암호화폐 전송은 되돌릴 수 없으므로, 보내기 전에 세부 사항이 정확해야 합니다.
2. 출금에는 올바른 코인, 네트워크, 주소, 그리고 필요할 때는 메모나 태그가 있어야 합니다.
3. 받는 쪽에서 시작하세요. 그곳에서 코인과 네트워크를 고르고 입금 주소를 복사한 뒤, 보낼 때 같은 네트워크를 고르세요.
4. 받는 쪽이 메모나 태그를 보여 준다면 반드시 넣어야 하며, 그렇지 않으면 자금이 반영되지 않을 수 있습니다.
5. 주소 포이즈닝과 클립보드 악성코드는 부주의한 복사를 노립니다. 기록이 아니라 입금 페이지에서 복사하고, 앞, 가운데, 끝을 확인하세요.
6. 소액 테스트 전송, 트랜잭션 해시, 블록 탐색기를 이용하면 전송을 단계별로 확인할 수 있습니다.

실력 점검

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

1. 암호화폐를 보낼 때 세부 사항이 그토록 중요한 이유는?

- A 수수료가 매우 비싸서
- B 확인된 트랜잭션은 되돌릴 수 없어서
- C 거래소가 모든 전송을 사람이 직접 확인해서
- D 주소는 한 번 쓰면 만료되어서

2. USDT를 다른 거래소로 옮길 때 가장 안전한 순서는?

A 보내는 쪽에서 아무 네트워크나 고른 뒤 주소를 찾는다
B 받는 쪽에서 코인과 네트워크를 고르고 입금 주소를 복사한 뒤, 보낼 때 같은 네트워크를 고른다
C 기억나는 대로 주소를 입력한다
D 지난번 트랜잭션의 주소를 쓴다

3. BEP-20 USDT를 자신의 Ethereum 지갑 주소로 보냅니다. 그래도 전송이 이루어질 수 있는 이유는?

A USDT는 모든 네트워크에서 자동으로 작동해서
B BNB Chain과 Ethereum이 같은 0x 주소 형식을 써서
C 거래소가 대신 변환해 줘서
D 어떤 경우에도 전송되지 않는다

4. 메모나 데스티네이션 태그는 언제 필요한가요?

A 모든 비트코인 전송에
B XRP, XLM, TON 같은 코인에서 받는 거래소가 입금 주소와 함께 보여 줄 때
C 10,000달러가 넘는 전송에만
D 필요 없다, 선택 사항이다

5. 필요한 메모를 빠뜨리면 어떻게 되나요?

A 전송이 자동으로 환불된다
B 코인은 거래소에 도착하지만, 고객 지원에 연락하지 않으면 여러분의 계정과 연결되지 않는다
C 코인이 파괴된다
D 아무 일도 없다, 메모는 참고용일 뿐이다

6. 주소 포이즈닝은 어떻게 작동하나요?

A 블록체인을 바이러스로 감염시킨다
B 앞뒤가 같은 비슷한 주소를 거래 기록에 심어 실수로 복사하게 만든다
C 개인 키를 바꾼다
D 네트워크 수수료를 올린다

7. 받는 주소를 복사하기에 가장 안전한 곳은?

A 자신의 거래 기록
B 모르는 사람이 보낸 메시지
C 받는 쪽의 공식 입금 페이지나 저장해 둔 주소록
D 소셜 미디어의 스크린숏

8. 트랜잭션 해시로 무엇을 할 수 있나요?

A 트랜잭션을 되돌린다
B 블록 탐색기에서 조회해 전송이 확인되었는지, 어디로 갔는지 본다
C 받는 주소를 바꾼다
D 수수료를 환불받는다

정답 및 해설

1 B

확인된 트랜잭션은 되돌릴 수 없어서

블록체인 전송은 일단 확인되면 최종적입니다. 누구도 대신 되돌려 줄 수 없습니다.

2 B

받는 쪽에서 코인과 네트워크를 고르고 입금 주소를 복사한 뒤, 보낼 때 같은 네트워크를 고른다

받는 쪽에서 시작하면 그쪽이 지원하는 네트워크이고 주소도 그 네트워크의 것임이 보장됩니다.

3 B

BNB Chain과 Ethereum이 같은 0x 주소 형식을 써서

같은 0x 주소가 두 네트워크에 모두 존재합니다. 자기 지갑이라면 BNB Chain을 추가해 확인할 수 있는 경우가 많지만, 거래소라면 복구가 느리거나 거절될 수 있습니다.

4 B

XRP, XLM, TON 같은 코인에서 받는 거래소가 입금 주소와 함께 보여 줄 때

이런 코인에서는 거래소가 여러 고객에게 하나의 공용 주소를 씁니다. 메모가 그 입금이 여러분의 것임을 알려 줍니다.

5 B

코인은 거래소에 도착하지만, 고객 지원에 연락하지 않으면 여러분의 계정과 연결되지 않는다

자금은 공용 주소에 도착하지만 아무도 그것이 여러분의 것인지 모릅니다. 고객 지원을 통한 복구가 가능한 경우도 있지만 보장되지는 않습니다.

6 B

앞뒤가 같은 비슷한 주소를 거래 기록에 심어 실수로 복사하게 만든다

공격자는 여러분이 쓰는 주소의 앞뒤 글자를 흉내 냅니다. 2024년 5월 한 트레이더는 이런 식으로 약 6,800만 달러를 잃었습니다.

7 C

받는 쪽의 공식 입금 페이지나 저장해 둔 주소록

기록에서 복사하는 것이 바로 주소 포이즈닝이 노리는 행동입니다. 공식 입금 페이지나 저장해 두고 검증한 주소를 쓰세요.

8 B

블록 탐색기에서 조회해 전송이 확인되었는지, 어디로 갔는지 본다

해시는 여러분의 전송을 식별합니다. 그 네트워크의 블록 탐색기가 상태와 확인 횟수를 보여 줍니다.

출처

- CoinDesk, 공격자가 주소 포이즈닝으로 6,800만 달러어치 암호화폐를 훔치다: https://www.coindesk.com/business/2024/05/03/exploiter-steals-68m-worth-of-crypto-through-address-poisoning
- Cointelegraph, WBTC 주소 포이즈닝 공격자가 협상 끝에 자금을 돌려주다: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations
- Stablecoin Insider, USDT 2026년 2분기 보고서 (네트워크별 USDT): https://stablecoininsider.org/usdt-q2-2026-report-supply-regulation-and-the-two-tier-market/

Market Talks

계속 학습하기

다음: 11강 현물과 파생상품: 선물, 무기한 계약, 레버리지 첫걸음

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.