Market Talks
教育中心

加密货币 · 初级 · 第10课，共15课

安全收发：网络、地址与备注标签

提现页面上每个栏位的含义，为什么收发双方的网络必须一致，什么时候需要填写备注或标签，以及如何防范仿冒地址

阅读约10分钟　8道测验题，附答案

加密货币 · 初级 · 第10课，共15课

安全收发：网络、地址与备注标签

一句话概括

加密货币转账无法撤回，所以每一次提现都取决于四件事是否正确：币种、网络、地址，以及在需要时填写的备注或标签。

没有撤销按钮

转错账户的银行转账，有时还能追回。区块链交易却不行。交易一旦确认，任何人都无法撤销，网络不能，你的钱包不能，通常交易所也不能。正是这一特性让加密货币能够抵抗审查，但这也意味着，在按下发送之前，每个细节都必须正确。

好消息是，几乎所有代价高昂的错误，都出在同一个页面上的少数几个栏位。这一课会逐一讲解。

一次提现的组成部分

无论是从交易所提现，还是从自己的钱包发送，你要填写的都是同样几类栏位：

- **币种：**你要发送的是什么，例如USDT。
- **网络：**这笔转账走哪条区块链，例如Tron（TRC-20）或以太坊（ERC-20）。
- **地址：**转到哪里。它必须是同一网络上的地址。
- **备注或标签：**一个额外的数字或文字，只有某些币和某些收款方才需要。
- **数量：**要发送多少。
- **手续费：**网络费或提现费，会从数量中扣除，或者另外加上。

在确认之前，大多数交易所会显示一份到账摘要。慢慢读完这份摘要，是这一课里最有用的一个习惯。



图1. 一个通用的提现页面。币种、网络和地址是出错代价最高的三个栏位。

收发双方的网络必须一致

第5课讲过，USDT在Tron、以太坊、BNB Chain、Solana等网络上是各自独立的代币。发送时，你选择的网络必须是收款方支持该币种的网络，而地址也必须属于这个网络。

一定要从收款方开始。在接收的交易所或钱包里，先选币种，再选网络，然后复制它给出的充值地址。接着在发送方，选择完全相同的网络。

如果两边不一致，会发生什么？

- 如果地址格式不同，比如在以太坊网络上填了一个Tron地址，应用通常会拒绝这笔转账。这算是幸运的情况。
- 如果两个网络使用相同的**0x**地址格式，比如以太坊和BNB Chain，转账会成功，但到了一个收款方可能并不监控的网络上。如果发到的是你自己的钱包，往往只要在钱包里添加那个网络就能找到资金。如果发到的是交易所，可能需要提交找回申请，这可能要花上几周、收取费用，甚至被拒绝。



图2. 收发双方的网络必须一致。地址格式不同通常会被拒绝，但共用0x格式的网络会接受这笔转账，资金可能因此滞留。

备注与标签

对于某些币种，交易所会让许多客户共用同一个充值地址。为了知道一笔充值属于哪位客户，它们会附加一个简短的数字或文字，称为**备注**（memo）、**标签**（tag）或**目标标签**（destination tag）。常见的例子有使用目标标签的XRP，以及使用备注或留言的Stellar（XLM）、TON和Cosmos（ATOM）。

如果接收的交易所在地址旁边显示了备注或标签，你在发送时**必须**把它复制到备注栏里。没有它，币会到达交易所的共用地址，但没有人能看出这些币是你的。要找回它们，通常需要带着证明联系客服，而且不一定成功。

当你发送到自己的个人钱包时，通常不需要备注，因为这个地址只属于你一个人。

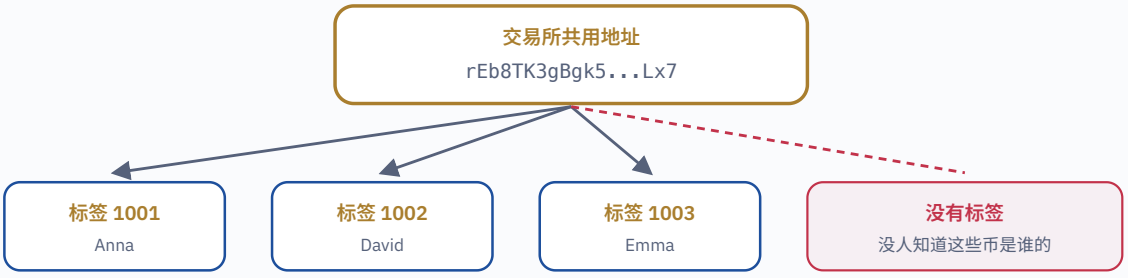


图3. 对于XRP等币种，交易所常常让许多客户使用同一个地址，并用标签来区分他们。没有标签的充值无法对应到任何人。

保护好地址

加密货币地址又长又不可能记住，攻击者主要从两个方面利用这一点：

- **地址投毒：**攻击者生成一个开头和结尾字符都与你常用地址相同的地址，然后给你发一笔极小的或虚假的交易，让它出现在你的历史记录里。之后，你从历史记录中复制地址时，一不小心就复制了错误的那个。2024年5月，一名交易者复制了一个开头和结尾都与真实地址相同的地址，就这样损失了1,155枚WBTC，价值约6800万美元。攻击者后来经过谈判归还了资金，但这种情况极为罕见。
- **剪贴板恶意软件：**电脑或手机上的恶意软件，会在你粘贴的那一刻，把复制的地址换成攻击者的地址。

几个简单的习惯就能同时防范这两种攻击：从收款方的充值页面复制地址，而不是从你的交易历史里复制；绝不手动输入地址；粘贴之后，检查开头、中间和结尾的字符；对于经常转账的地址，使用交易所的**地址白名单**或钱包的地址簿。



图4. 地址投毒：攻击者的地址与真实地址开头和结尾相同，只有中间部分会露出破绽。地址均为虚构。

先测试，再追踪

第一次向一个新地址转账时，许多有经验的用户会先发一笔小额的**测试转账**，等它到账后，才发送其余部分。和犯错的代价相比，多付的手续费通常很少。

发送之后，你会得到一个**交易哈希**，也叫TxID：一个用来识别这笔转账的唯一代码。把它粘贴到该网络的区块浏览器里，例如以太坊的Etherscan或Tron的Tronscan，就能看到转账是否已确认、转到了哪里。交易所要等到达到一定的**确认数**之后才会给充值入账，所以一笔转账可能在区块链上已经显示完成，几分钟后才出现在你的账户里。

如果真的出了问题，要尽快行动：保存好交易哈希，通过官方网站或应用联系接收平台的官方客服，并且不要理会任何主动发消息说能帮你找回资金的人。这类提议几乎总是第二场骗局。



图5. 每次转账都适用的简短检查清单。

这对交易者为何重要

- **转移资金是交易的一部分。**交易者经常在交易所和钱包之间转移资金，有时还很匆忙。大多数代价高昂的转账错误，都发生在时间紧迫的时候。
- **网络的选择会影响速度和成本。**走Tron或Solana的USDT通常几分钟就能到账，手续费也低。同样的转账走以太坊可能更贵，而比特币可能需要一个小时甚至更久才能获得足够的确认。
- **交易所有时会暂停某个网络。**在升级或拥堵期间，某个网络上的充值或提现可能会被暂停。发送前先查看网络状态，可以避免资金卡在途中。
- **白名单多加了一层保护。**许多交易所允许你把提现限制在已保存的地址上，万一账户被盗，这能起到作用。

关键术语

提现网络	选来承载一笔转账的区块链。收款方必须支持该币种在这个网络上的转账。
充值地址	收款方为某个币种在某个网络上提供给你的地址。
备注、标签、目标标签	一个额外的代码，告诉交易所发到共用地址的充值属于哪位客户。
地址投毒	一种骗局：在你的交易历史中植入一个仿冒地址，指望你一不小心复制它。
剪贴板恶意软件	把你复制的加密货币地址替换成攻击者地址的恶意软件。
测试转账	先发送的一小笔转账，用来确认地址和网络都正确。

交易哈希（TxID）	用来识别一笔交易的唯一代码，可以在区块浏览器中查询。
地址白名单	交易所的一项设置，只允许向你事先保存的地址提现。

要点总结

1. 已确认的加密货币转账无法撤回，所以发送前每个细节都必须正确。
2. 一次提现需要正确的币种、网络、地址，以及在需要时填写的备注或标签。
3. 从收款方开始：在那里选好币种和网络，复制充值地址，然后在发送时选择同一个网络。
4. 如果收款方显示了备注或标签，就必须填写，否则资金可能无法入账。
5. 地址投毒和剪贴板恶意软件都利用粗心的复制。要从充值页面复制，绝不从历史记录中复制，并检查开头、中间和结尾。
6. 一笔小额测试转账、一个交易哈希和一个区块浏览器，能让你一步步确认转账情况。

自我测验

请为每道题圈出一个答案。答案及解释在下一页。您也可以在 markettalks.info 在线完成此测验，并立即查看得分。

1. 为什么发送加密货币时细节如此重要？

A 手续费非常高
B 已确认的交易无法撤回
C 交易所会人工检查每一笔转账
D 地址用过一次就会失效

2. 把USDT转到另一家交易所时，最安全的步骤顺序是什么？

A 在发送方随便选一个网络，然后再找地址
B 在收款方选好币种和网络并复制充值地址，然后在发送时选择同一个网络
C 凭记忆输入地址
D 使用上一笔交易里的地址

3. 你把BEP-20 USDT发到了自己的以太坊钱包地址。为什么这笔转账仍然可能成功?

A USDT自动在所有网络上通用
B BNB Chain和以太坊使用相同的0x地址格式
C 交易所会替你转换
D 无论如何都不会成功

4. 什么时候必须填写备注或目标标签?

A 每一笔比特币转账
B 当接收的交易所在充值地址旁显示了备注或标签时，适用于XRP、XLM或TON等币种
C 只有转账金额超过10,000美元时
D 从来不需要，它是可选的

5. 如果漏填了必需的备注，会发生什么?

A 转账会自动退回
B 币会到达交易所，但不联系客服就无法对应到你的账户
C 币会被销毁
D 什么都不会发生，备注只是参考信息

6. 地址投毒是如何运作的?

A 用病毒感染区块链
B 在你的历史记录中植入一个开头和结尾相同的仿冒地址，让你一不小心复制它
C 更改你的私钥
D 提高网络手续费

7. 从哪里复制收款地址最安全?

A 你的交易历史
B 陌生人发来的消息
C 收款方自己的充值页面，或你已保存的地址簿
D 社交媒体上的截图

8. 交易哈希可以用来做什么?

A 撤回交易

B 在区块浏览器中查询，看转账是否已确认、转到了哪里

C 更改收款地址

D 退回手续费

答案与解释

1 B

已确认的交易无法撤回

区块链转账一旦确认就是最终的。没有人能替你撤回。

2 B

在收款方选好币种和网络并复制充值地址，然后在发送时选择同一个网络

从收款方开始，就能确保所选网络是它支持的，而且地址属于这个网络。

3 B

BNB Chain和以太坊使用相同的0x地址格式

同一个0x地址在两个网络上都存在。在自己的钱包里，往往添加BNB Chain就能看到资金；在交易所，找回可能很慢，甚至被拒绝。

4 B

当接收的交易所在充值地址旁显示了备注或标签时，适用于XRP、XLM或TON等币种

对于这些币种，交易所让许多客户共用一个地址。备注告诉它们这笔充值是你的。

5 B

币会到达交易所，但不联系客服就无法对应到你的账户

资金到了共用地址，但没有人知道它们是你的。在某些情况下可以通过客服找回，但不能保证。

6 B

在你的历史记录中植入一个开头和结尾相同的仿冒地址，让你一不小心复制它

攻击者模仿你常用地址的开头和结尾字符。2024年5月，一名交易者就这样损失了约6800万美元。

7 C

收款方自己的充值页面，或你已保存的地址簿

从历史记录复制，正是地址投毒所利用的漏洞。请使用官方充值页面或已保存并核实过的地址。

8 B

在区块浏览器中查询，看转账是否已确认、转到了哪里

哈希能识别你的转账。该网络的区块浏览器会显示它的状态和确认数。

资料来源

- CoinDesk，攻击者通过地址投毒盗走价值 6800 万美元的加密货币: https://www.coindesk.com/business/2024/05/03/exploiter-steals-68m-worth-of-crypto-through-address-poisoning
- Cointelegraph，WBTC 地址投毒者经谈判归还全部资金: https://cointelegraph.com/news/wbtc-address-poisoner-all-funds-negotiations
- Stablecoin Insider，USDT 2026 年第二季度报告（各网络上的 USDT）: https://stablecoininsider.org/usdt-q2-2026-report-supply-regulation-and-the-two-tier-market/

Market Talks

继续学习

下一课：第11课
现货与衍生品：初识期货、永续合约与杠杆

本课属于 MARKET TALKS 教育中心的加密货币课程。初级课程免费，每课都配有测验和可下载的PDF。中级和高级课程面向会员开放。

教育中心
从基本原理到高级主题的课程

市场分析
主要市场的技术面与基本面分析

报告
比特币、黄金、白银、SPX等

markettalks.info

Telegram @MARKET_TALKS

仅供教育用途。本文件的任何内容均不构成投资建议。© 2026 MARKET TALKS。欢迎在不作修改的前提下分享本PDF。