Market Talks
教育中心

加密货币 · 初级 · 第14课，共15课

骗局、跑路与警示迹象

最常见的加密货币骗局如何运作，从跑路和拉盘砸盘，到虚假投资平台、冒充者和钱包盗取工具，以及它们共有的警示迹象

阅读约11分钟　　8道测验题，附答案

加密货币 · 初级 · 第14课，共15课

骗局、跑路与警示迹象

一句话概括

加密货币骗局每年卷走数十亿美元。其中大多数遵循少数几种模式，一旦你能认出这些模式，警示迹象就容易看清得多。

为什么骗局在加密世界如此常见

加密货币交易速度快、全球通行，而且无法撤销。没有银行可以打电话要求退款，也没有一个中央部门能冻结已经离开你钱包的付款。让加密货币有用的这些特点，同样让它对骗子很有吸引力。

涉及的金额很大。区块链分析公司Chainalysis估计，2025年加密货币骗局卷走了**超过170亿美元**，创下纪录。仅在美国，FBI下属的互联网犯罪投诉中心（IC3）在2025年收到的与加密货币相关的投诉中，报告的损失约为**114亿美元**，比前一年增加22%。其中约72亿美元来自虚假投资骗局。

骗局也越来越专业化。Chainalysis发现，冒充类骗局在2025年增长了1,400%以上，每笔付款被骗走的平均金额从约782美元升至约2,764美元。如今许多诈骗团伙使用AI来撰写消息、翻译对话和制作虚假视频。

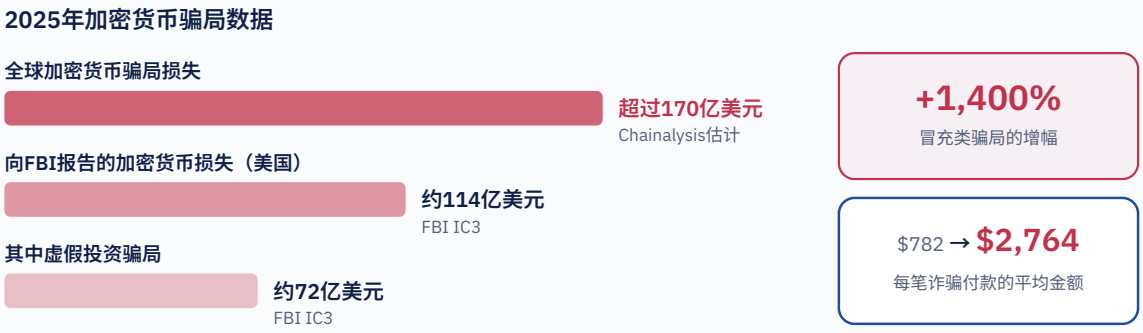


图1. 2025年加密货币骗局创下纪录。数据为Chainalysis的估计和向FBI报告的投诉。

跑路与貔貅盘

跑路（rug pull，字面意思是“抽地毯”）是指某个代币或项目背后的人突然卷走资金并消失，就像把买家脚下的地毯一下子抽走。它在去中心化交易所的新代币中最为常见，因为在那里任何人都能在几分钟内创建一个代币和一个交易池（第7课和第9课）。

常见的形式包括：

- **撤走流动性：**创建者把资金从交易池中撤出。池中没有了可供交易的资金，代币价格会暴跌到几乎为零。
- **团队抛售：**创建者持有很大一部分供应，并一次性全部卖给市场。
- **貔貅盘**（honeypot）：代币的智能合约被设计成只能买、不能卖。价格图表只涨不跌，因为除了创建者之外，谁都卖不出去。



图2. 鱿鱼游戏代币跑路事件的简化示意。价格上涨时持有者无法卖出，随后创建者抽干了资金池。

例子：鱿鱼游戏代币，2021年

2021年底，一个以热门电视剧《鱿鱼游戏》命名的非官方代币出现在去中心化交易所PancakeSwap上。它的价格在几天内上涨了数万个百分点，并在2021年11月1日突破**2,850美元**。买家很快发现自己卖不出去。随后，创建者卖掉了手中的代币并抽干了资金池，几分钟内价格就跌到约**0.002美元**。创建者带着约338万美元离开。这部剧的制作方与此毫无关系。

拉盘砸盘

在**拉盘砸盘**（pump and dump）中，一伙人先悄悄买入一种交易清淡的小币，然后通过社交媒体帖子、付费网红或聊天群大肆宣传。随着新买家蜂拥而入，价格飙升。接着组织者把自己的币卖给（“砸”给）这些后来的买家，价格随之回落，常常跌到比起点还低。

拉盘砸盘之所以能得逞，是因为小币的流动性很差（第8课），不多的买盘就能让价格大幅变动。突然冒出大量关于某个无名币、说法如出一辙的帖子，常常还带着倒计时和目标价，这是一种典型的迹象。

虚假投资平台与“杀猪盘”

损失最大的一类来自虚假投资骗局。其中一种广为人知的形式叫做**杀猪盘**（pig butchering），这个名称来自骗子们自己的行话：他们先用信任把受害者“养肥”，然后再“宰杀”。

它通常从一条看似无害的消息开始：一条“发错号码”的短信、交友软件上的一次配对，或社交媒体上的一个新联系人。在几周时间里，骗子会建立起友谊或恋爱关系。最终，他们会提到自己炒加密货币赚了不少钱，并提出可以教你怎么做。

受害者被引导到一个看起来很专业、实则是假的交易网站或应用。屏幕上的余额增长得很快，早期的小额提现甚至可能成功，这会建立信任。存款越来越多。当受害者想取出一大笔钱时，平台突然要求先缴纳一笔“税”、“手续费”或“解冻保证金”。付完之后，平台和那位朋友都消失了。

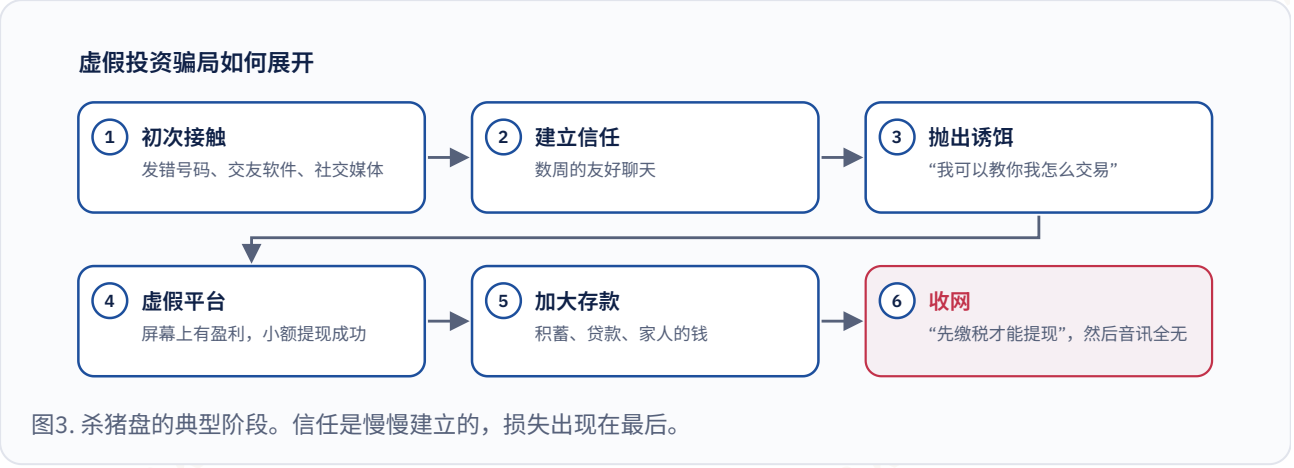


图3. 杀猪盘的典型阶段。信任是慢慢建立的，损失出现在最后。

例子：从内部看是什么样子

Laura收到Michael发来的一条短信：“嗨，David，周六的高尔夫还照常吗？”她回复说他发错号码了。Michael道了歉，两人开始聊天。六周后，他给她看自己交易盈利的截图，并帮她在自己使用的一个平台上开了账户。她最初的1,000美元在屏幕上涨到了1,600美元，一笔200美元的提现也到了她的钱包。她存入了25,000美元。当她申请提现时，客服说她必须先为盈利缴纳20%的“税”。屏幕上的数字从来都不是真的。

冒充者、假客服与追款骗局

许多骗局靠冒充你信任的人来得逞：

- **假客服：**你在公开论坛或聊天群里发了一个问题之后，有人私信你，自称是交易所或钱包的客服团队。真正的客服团队不会主动发起私聊，也绝不会索要助记词或密码。
- **假冒交易所或政府人员联系：**一通电话、一封邮件或一条短信称你的账户有风险，你必须立刻把资金转到一个“安全”钱包。

- **假名人和假赠送活动：**一段视频或一篇帖子显示某位名人承诺，你发给他多少加密货币，他就返还双倍。如今AI生成的深度伪造（deepfake）视频让这些内容看起来很逼真。真正的赠送活动没有一个是这样运作的。
- **追款骗局：**有人亏钱之后，一位“追款专家”或一家假律师事务所提出可以帮忙追回，但要先付费。这类骗局专门针对已经被骗过一次的人。

钱包盗取工具、授权与假空投

有些骗局并不需要你发送任何东西。它们会诱骗你授权一个恶意智能合约转移你的代币。

使用DeFi应用时，钱包常常会请你**授权**某个合约替你花费某种代币（第12课）。一个假网站，常常以免费**空投**、铸造或领取奖励为名，要求你连接钱包并签名。你实际签署的是一份授权，有时额度不限，它让骗子的合约可以拿走你的代币。这类工具叫做**钱包盗取工具**（wallet drainer）。

其他常见手法包括：在你输入助记词时将其窃取的假钱包应用和浏览器插件、外观相似的网址，以及地址投毒（第10课）。正如区块链课程第9课所讲，任何拿到你**助记词**的人都能完全控制你的钱包。旧的授权在被移除之前一直有效，Revoke.cash等工具和一些区块浏览器可以显示一个钱包给出过哪些授权。



图4. 钱包盗取工具不会要求你发送资金，而是让你签署一项许可，好让它把资金拿走。

大多数骗局共有的警示迹象

故事会变，但警示迹象总是反复出现：

- **保证收益或极高回报**，例如“每天2%”或“零风险”。
- **制造紧迫感和压力：**马上行动，优惠今晚结束，你的账户将被关闭。
- **索要你的助记词或私钥**，无论出于什么理由。
- **不请自来的联系**，慢慢转向投资话题。
- **一个不知名的平台**，由一位新认识的网友推荐，或者一个不是通过官方渠道找到的应用。

- **提现前需要先付费。**
- **“发送加密货币，返还双倍”。**
- **卖不出去的代币**、持有大部分供应的匿名团队，或未锁定的流动性。

单一的警示迹象并不能证明就是骗局，但几个同时出现就是一个强烈的警告。



图5. 大多数加密货币骗局共有的常见警示迹象。

骗局发生之后

由于区块链转账是最终的，发给骗子的钱很少能追回。有时，如果资金很快到达受监管的交易所，该交易所可以将其冻结，Tether和Circle等稳定币发行方也曾在一些案例中冻结被盗资金。

FBI等机构所描述的步骤包括：向警方报案，在美国还包括向IC3报告；告知被利用的交易所或平台；保留交易哈希、钱包地址、消息和网站链接等记录；以及撤销已经给出的钱包授权。许多人如果认为旧钱包已经暴露，还会把剩余资金转到一个使用新助记词的新钱包里。

相关机构还警告说，报告损失的人事后常常会被追款骗子联系，因此第一次损失之后可能紧接着第二次。

这对交易者为何重要

- **快速上涨会吸引骗局。**单日涨幅巨大的新代币，正是跑路、貔貅盘和拉盘砸盘发生的地方。检查一个代币能否卖出、供应由谁持有、流动性是否锁定，是许多交易者所做基本研究的一部分。
- **“跟我下单”类的提议。**承诺提供私人交易提示或代管账户、以换取存款的群组，是虚假平台常见的切入点。
- **授权会越积越多。**活跃的DeFi用户随着时间推移可能积累许多旧的代币授权。一旦相关合约被攻破，每一个都可能成为风险。
- **同样的安全习惯也能保护交易账户。**交易所账户同样是目标：钓鱼邮件、假登录页面和SIM卡调换都意在接管账户并提走资金。第15课会讲解交易所提供的基本保护措施。

关键术语

跑路（rug pull）	项目创建者突然卷走资金，例如撤走流动性或抛售手中的代币，让代币几乎一文不值。
貔貅盘（honeypot）	一种代币，其智能合约允许买入，但除创建者外禁止所有人卖出。
拉盘砸盘（pump and dump）	组织者买入一种小币，通过炒作推高价格，再卖给后来的买家。
杀猪盘（pig butchering）	一种长期骗局，骗子花几周时间建立信任，再引导受害者在虚假投资平台上存入大笔资金。
网络钓鱼	模仿真实服务的虚假消息、邮件或网站，用来骗取密码、验证码或助记词。
钱包盗取工具（wallet drainer）	假网站上的恶意代码，诱骗用户签署授权或交易，把代币转给骗子。
代币授权	你签署的一项许可，让某个智能合约可以从你的钱包中花费某种代币，额度可以设定，也可以不限。
深度伪造（deepfake）	通常用AI制作的虚假视频或音频，显示某个真实的人说了他从未说过的话。
追款骗局	一种后续骗局，针对已经亏钱的人，承诺只要预先付费就能把钱追回来。

要点总结

1. 加密货币付款快速且不可撤销，这让它对骗子很有吸引力。Chainalysis估计，2025年骗局造成的损失超过170亿美元。
2. 跑路、貔貅盘和拉盘砸盘在新的小代币中最为常见。鱿鱼游戏代币在几分钟内从2,850美元以上跌到几乎为零。
3. 虚假投资平台造成的损失最大，受害者往往是经过一段长期的网络友谊被引过去的。虚假余额和早期的小额提现会建立信任。
4. 冒充者会假扮客服人员、交易所、官员和名人。真正的客服绝不会索要助记词。
5. 钱包盗取工具利用你签署的授权，而不是让你发送资金。旧的授权在被移除之前一直有效。
6. 保证收益、制造紧迫感、索要助记词以及提现前收费，是最常见的警示迹象。

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. 为什么加密货币付款对骗子有吸引力？

A 它们总是匿名且不可见
B 它们速度快、全球通行且无法撤销
C 交易所为骗子的利润提供担保
D 它们只能在夜间发送

2. 什么是貔貅盘（honeypot）代币？

A 以真正的蜂蜜作支撑的代币
B 支付高额质押奖励的代币
C 合约允许人们买入但不能卖出的代币
D 与黄金挂钩的稳定币

3. 2021年11月，鱿鱼游戏代币发生了什么？

A 它在各大交易所上市
B 创建者抽干了资金池，价格从2,850美元以上跌到约0.002美元
C 这部剧的制作方买下了全部供应
D 它变成了一种稳定币

4. 在拉盘砸盘中，通常是谁亏钱？

A 最先买入的组织者
B 因炒作而入场的后来买家
C 区块链的验证者
D 没有人，它没有风险

5. 在杀猪盘中，为什么早期的小额提现常常能成功？

A 因为平台是真的
B 为了在更大的存款之前建立信任
C 因为区块链的规则
D 因为银行强制要求

6. 有人私信你，自称来自你的钱包客服团队，并索要你的助记词来解决一个问题。这是什么？

A 正常的客服流程
B 必需的安全检查
C 典型的冒充骗局
D 一次软件更新

7. 钱包盗取工具通常如何拿走代币？

A 猜出你的密码
B 让你在假网站上签署一项授权或交易
C 攻破整个区块链
D 改变代币的价格

8. 以下哪一项是骗局的常见警示迹象？

A 平台要求先付费才能提现

B 可以随时卖出代币

C 一家公开审计结果的知名交易所

D 价格有涨有跌

答案与解释

1 B

它们速度快、全球通行且无法撤销

一笔转账一旦确认，银行或支付公司都无法撤销，而且资金几分钟内就能跨越国界。

2 C

合约允许人们买入但不能卖出的代币

合约阻止普通持有者卖出，所以在创建者套现之前，价格看起来只涨不跌。

3 B

创建者抽干了资金池，价格从2,850美元以上跌到约0.002美元

买家卖不出去，随后创建者卖出代币并拿走流动性，价格在几分钟内崩溃。

4 B

因炒作而入场的后来买家

组织者提前买入，再卖给宣传之后才到来的人，让这些人手里攥着一个不断下跌的币。

5 B

为了在更大的存款之前建立信任

放出一小笔钱能让虚假平台显得真实，受害者于是放心存入多得多的钱。

6 C

典型的冒充骗局

任何拿到你助记词的人都能控制你的钱包。真正的客服团队绝不会索要它。

7 B

让你在假网站上签署一项授权或交易

用户签署了一项许可，它常常被包装成领取空投，让骗子的合约可以转移这些代币。

8 A

平台要求先付费才能提现

在放行提现前要求缴纳税费、手续费或保证金，是虚假平台的典型迹象。

资料来源

- Decrypt，AI 与冒充手段推动 2025 年加密货币骗局损失创下 170 亿美元纪录（Chainalysis）：https://decrypt.co/354624/ai-impersonation-drove-crypto-scam-losses-record-17-billion-2025-chainalysis
- Yahoo Finance，FBI 报告 2025 年加密货币欺诈损失增长 22%: https://finance.yahoo.com/markets/crypto/articles/fbi-reports-22-rise-crypto-191510401.html
- Cointelegraph，受《鱿鱼游戏》启发的加密骗局崩盘，价格从 2,800 美元跌至零: https://cointelegraph.com/news/game-over-squid-game-inspired-crypto-scam-collapses-as-price-crashes-from-2-8k-to-zero
- Cointelegraph，用户无法卖出鱿鱼游戏代币: https://cointelegraph.com/news/users-not-able-to-sell-squid-game-token-clocking-45-000-gains

Market Talks

继续学习

下一课：第15课
真正的入门：交易所、KYC与钱包

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。