Web3 反欺诈手册

Web3 反欺诈手册

2024.10

目录

前言

嗨，所有读到这本 Web3 反欺诈手册的朋友们，你好。

当下 Web3 行业的规模体量已经得到了极大的扩张，根据 @CMC 的数据统计，截至本手册开始写作的 2024 年 8 月末，加密市场总规模已经达到 2 万亿美元，相当于英伟达总市值的三分之二，或者港股总市值的一半。

加密资产总市值

而这些快速增长的产业大多发生在不受监管的场景下，一定程度上不可避免地招致了违法犯罪活动的污染。因此，不论你是刚刚才开始了解加密货币的新人小白，还是已经有非常丰富链上交互经验的 OG，相信你都或多或少会对来自内部或外部对加密行业的负面批评——诸如「加密货币是洗钱工具」、「加密货币钱包并不安全」、「诈骗空气币横行」等言论有所耳闻。

尽管这类指责通常过分夸大甚至扭曲事实，但对任何一个普通 Web3 用户而言，这个市场都不像传统金融市场那样安全，稍不注意，一笔交易甚至一个签名都有可能让你损失掉账户地址里所有的钱。

为此我们写作了这本反诈防骗手册，尝试通过对不同阶段用户会遭遇的欺诈手段进行详细拆解，以帮助读者朋友们识别并规避这些威胁，相信会对新手小白与币圈老手都有所帮助。

接下来，让我们开始。

糟糕的信息来源：你可能从一开始就被骗了

许多投资者第一次接触 Web3 相关概念，都是在社交网站、自媒体平台、网络社群等场景，这类场景往往鱼龙混杂，成熟的投资者尚且需要在大量噪音与谣言中寻找真正有效的信息，经验不足的投资者很难不被欺诈信息所干扰。

正因如此，许多不法分子利用客观存在的信息壁垒，对缺乏相关知识的圈外用户进行欺诈，手段包括扭曲或虚构事实、偷盗账户密钥、骗取账户权限等，这也是行业被污名化的重要原因。

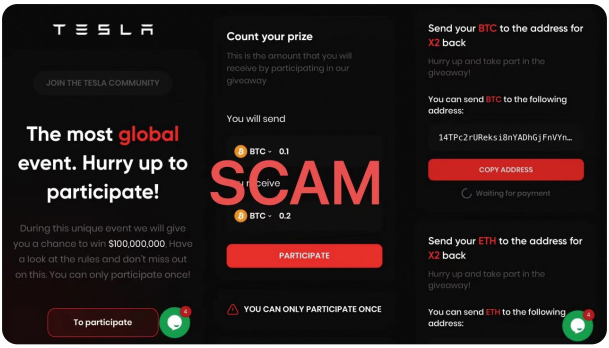
短视频二维码欺诈

诱导受害人扫描二维码跳转第三方欺诈网站是经典的欺诈手段，在传统的场景下，受害人往往会被要求提交隐私信息，安装有害软件，或者进入欺诈网络社群。近年来随着加密经济规模的快速扩张，这个手法在行业内也得到了应用。

以下是典型的冒充埃隆·马斯克的欺诈案例——

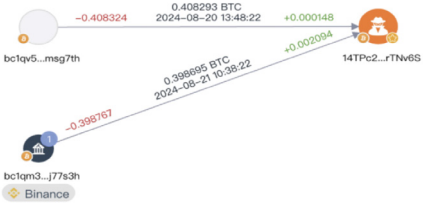
这位影响力巨大的名人因近期频繁提及区块链相关概念，而对加密货币二级市场造成了较大的冲击。有不法分子利用人工智能工具伪造了一段影像，其中「马斯克」声称观众扫描视频中出现的二维码，将能够参与由特斯拉公司发起的比特币返利活动。欺诈者通过向 Youtube 投稿或发起直播的形式，向网友们投放这个欺诈视频。

访问欺诈网站 teslainc2x[.]org 后，网站会要求受害人向某个特定的地址转账，并声称在活动期间仅有一次机会获取双倍的回报。



欺诈信息

这是非常典型的投资返利诈骗，通过 BitracePro 区块链数据分析画布可以看到，已经有两名受害人向欺诈地址转入了比特币，然而并没有收到“双倍返还”。



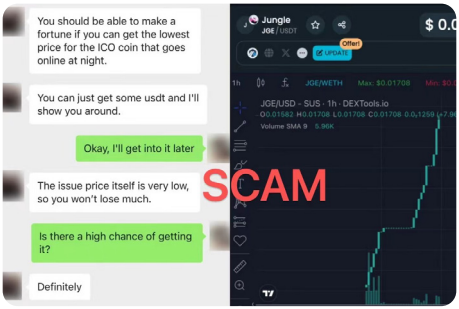
视频二维码欺诈案例资金分析

社交媒体诈骗

除了通过投放欺诈信息等待猎物上钩外，也存在大量投资理财类诈骗活动是通过社会工程学方法精细运作的，欺诈者往往会以「带你赚钱」为由，一步步教导受害人创建钱包、购买加密货币、参与投资赚钱，最后伺机窃走或骗走受害人账户里的资金。

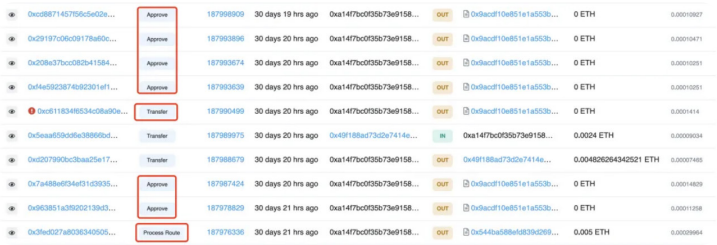
在下面这个案例中，我将为你介绍一个典型手法——

受害人在 TikTok 刷到一条关于比特币的介绍视频（实际上是骗子制作并发布的）并留言评论，不久后便收到视频发布者的私信，对方声称能够教他投资比特币。受害人欣然同意，但由于是完全的新手，过程中的每一步都截图由欺诈者进行指导，导致助记词在其不了解的情况下泄漏。



欺诈者与受害人的聊天记录

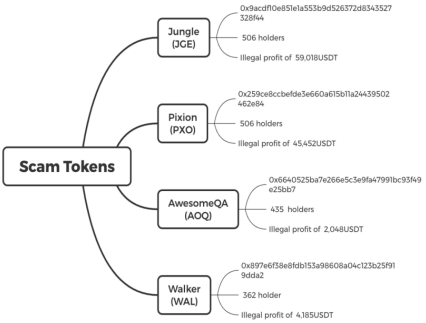
欺诈者推荐的第一个项目是一个名为 Jungle（JGE）的所谓 ICO 代币（官网 itsjungle[.]me 现已无法访问，官方推特也已注销），受害人成功从这笔交易中赚取了 50% 的利润。



多个受害者的链上操作记录

但事实上链上真实发生的故事是，这是一个「貔貅币」，其他不慎购入的受害人正在链上焦急地四处给不同的 DEX 授权以尝试将代币卖出，该受害人的「盈利」只是因为欺诈者给他的地址设置了权限白名单，仅他能够卖出而已。这是特意为他设计的代币池，只是为了让他尝到甜头后加大投入。

果然，次日欺诈者再次邀请受害人参与另一代币的交易，在受害人存入 2.39 ETH 后，欺诈者利用早前获取的助记词，将受害人地址中的资产尽数盗取。



欺诈团伙发行的多个欺诈代币

事后 Bitrace 对 JGE 代币的发布地址进行了调查，发现该团伙已经至少发行了四个欺诈代币，获利超过 130K，如果加上通过非法手段盗取的加密资产，损失数值会更大。

情感诈骗

情感诈骗是一种结合了投资理财类诈骗与交友婚恋类诈骗的欺诈手段，受害人通常为不具备 Web3 知识的圈外高净值群体，欺诈者会通过详细的背景调查后虚构人设投其所好，以网络恋爱的方式要求受害人参与某个并不存在的投资项目。

在「投资」活动的开始，受害人的「投资收益」就会快速上涨，然而当受害人想要提取收益，非法平台便会以「交税」、「滞纳金」、「手续费」、「锁定期」等诸多理由拒绝并要求受害人加大投入。在这个过程中，受害人会被榨干钱财，甚至被要求去借贷，直到再无资金可榨取。

不法分子并不同情这些受害人，他们称后者是「猪」，伪造的人设材料与话术是「猪饲料」，培养感情阶段是在「喂猪」，最后的收割自然也就是「杀猪」了。因此，这类骗局往往也被称为杀猪盘（pig butchering scams），受害人会受到财物与情感的双重损失。

以「高瑞商学院」杀猪盘案为例——

受害人是一名稍有资产的年轻女性，在 2023 年 2 月于社交软件中结识一名年轻多金的男网友，对方自称正在各地考察投资，会把自己去全国各地考察、投资的照片发给受害人，照片中不经意夹杂着几张自拍照，照片里的他开着豪车戴着名表，加以日常嘘寒问暖，令受害人为之倾心。

网恋过程中，欺诈者反复提及所谓的「高瑞商学院」，并声称这是一个区块链投资项目，参与者需要自行购买泰达币（USDT）用于认购份额，到期后便可连本带利获取高额收益。

欺诈者自称已经参与过多期投资，并赚取了较大收益，为了让受害人也参与，欺诈者甚至采用了 PUA 手段。

欺诈者与受害人的聊天记录

受害人花光了自己的资产，并向亲友大量借贷后，累计向该项目投入超过 20 万 USDT，最终网恋对象消失，自己血本无归。

错误的资管方法：位于加密之旅起点的大坑

不同于传统 Web2 平台中心化的账户登录与验证体系，加密货币钱包等 Web3 基础设施并不保留用户的身份信息、账户权限，也不存在传统互联网软件平台常见的销户、换绑、身份信息找回等设定。这意味着 Web3 用户需要自行保管地址密钥，一旦丢失将导致永久失去对链上身份的控制，或者因泄漏而导致链上资产被窃取。

在 Web3 钱包管理方面，我们应当首先简单理解什么是地址私钥和钱包助记词。

地址私钥是一串由数字与字母组成的字符串，用于揭秘数据或者签署交易，通过导入私钥，用户可以在任何钱包程序中「登陆」自己的加密地址并获得完整的账户权限。私钥通过特定的密码学方法可以单向推导出另一串特定规则的字符串，后者被称为地址公钥，也即我们日常互相转账时填写的资金收付对手方。不难看出，公钥就像对外公布的家庭住址，私钥则像由主人管理的房门钥匙。

助记词是私钥的另一种形式，由来源于特定词库的 12、24 或者其他个数的单词组成，因而具备更高的可读性与记忆便利性。通过助记词，钱包可以通过特定的标准派生并管理一组或多组公私钥对，例如颇受用户欢迎的 imToken 、TokenPocket 钱包，允许用户在同一组助记词下创建多个区块链地址，包括同一区块链下的多个地址，以及不同区块链下的多个地址。通过将助记词导入支持这类标准的钱包，用户将能够找回自己的链上资产。

而在地址私钥之外，部分钱包软件也支持导出二维码格式的密钥，这是一种钱包便利度设置，但其重要性不亚于私钥或助记词明文。

部分盗币者利用部分投资者对区块链钱包的不了解，会通过各种方式骗取助记词、私钥，或者钱包操作权限，进而盗取资产。

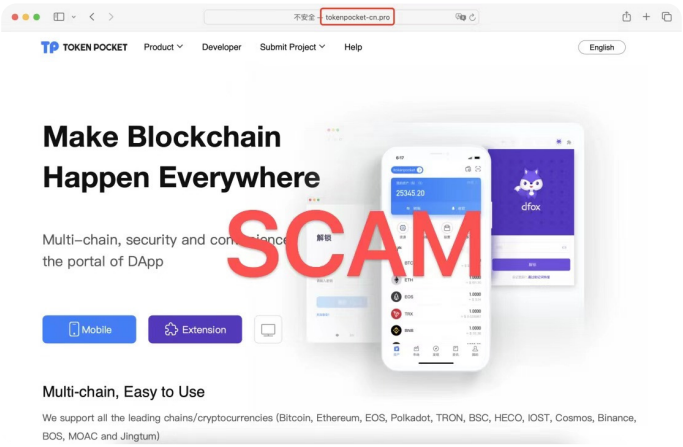
假钱包 APP 盗币

盗版 APP 是一种常见的恶意软件应用，通过盗用正版软件的 LOGO、名称、页面素材等方式，诱导受害人下载并使用，以实现危害网络安全、窃取用户信息、擅自使用付费业务等目的。

在加密货币行业，钱包 APP 是被高仿重灾区。盗币者通常的做法是，在真实钱包 APP 的代码文件中植入恶意代码，一旦有人安装了这一恶意软件并导入自己的助记词、私钥，APP 背后的盗币者就能够第一时间知晓受害人的助记词、私钥，进而非法转移受害人的资产。

当下最流行的假钱包 APP 的推广方式是通过搜索引擎、假钱包官网、假社交媒体账户的形式实现的——

在搜索引擎渠道，欺诈者会制作 Crypto 主题的文章或短视频，在嵌入恶意软件下载链接后通过 SEO 或 SEM 的方式进行推广，当潜在受害人通过搜索引擎搜索相关关键词——尤其是特定钱包品牌名称时，这类欺诈链接就有可能展现在搜索结果首页甚至首页第一条。未能分辨真伪的受害人会因此失去自己的资产。



假网站

假钱包官网与假钱包 APP 是配套存在的，通过制作高仿钱包网站并部署在高仿域名中，相比于普通的 SEO 手段更具迷惑性。例如针对 Tokenpocket 钱包的虚假官网 tokenpocket-cn[.]com，该域名就是真实官方域名 tokenpocket.pro 的高仿，意在诱导投资者下载假钱包 APP。

假 X(Twitter) 账户

假社交媒体账户也颇为流行，尤其是在 X 等 Web3 用户常用的社交平台上，活跃着大量以「imToken 中文客服 / 官方」、「imToken SupportTeam」等为名称的账户，意图对平台资讯进行污染以推广盗币 APP。

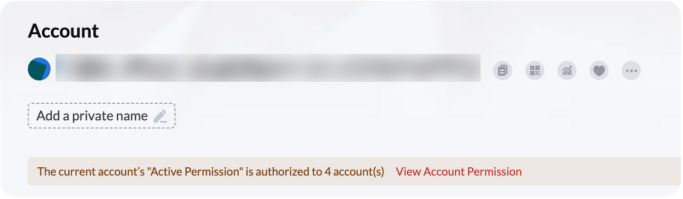
多签案例

多重签名钱包是一个重要的资产安全解决方案，区别于普通钱包，多签钱包需要多个私钥来进行操作，例如最常见的 2 对 3 多签钱包，要求三个私钥持有者中的至少两个签名，才能够发起一笔交易。其安全性在于，至少需要两个私钥同时泄漏，才会对所保管的资产有所威胁。

但这一解决方案反而被盗币团伙所利用，形成了一个新型变种——多签盗币。

在传统的假钱包骗局中，黑客通过假钱包后台获取地址私钥，与用户共享地址操作权限，双方都可以将地址内资金转出。在此类骗局中，盗币者有两类选择，一是当下实施盗窃，清空地址资产，用户发现地址余额归零后便不再使用该钱包；二是冒着用户可能会转出资金的风险，不立即转出，而是等待用户囤积，这种操作被不法分子称为「养鱼」。

这种场景下盗币者往往不会特别耐心，会不论大小尽快将资金转走。



多重签名诈骗中权限被更改的受害者账户

而在多签骗局中，由于用户失去了自己的账户权限，在这段时间里地址会一直处于「只进不出」的状态，理论上只要用户不操作转出，他将永远不会发现自己已经处在被盗的边缘。对盗币者而言，只需要等待不明真相的受害人持续向钱包转账。

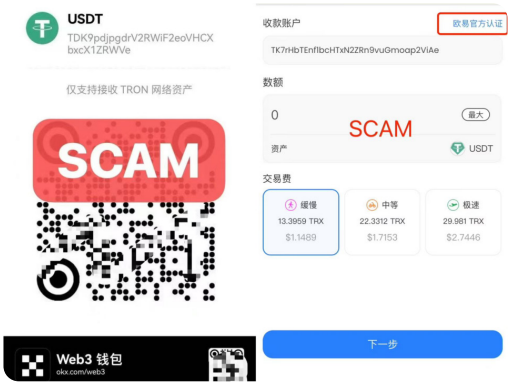
显然，多签骗局手法更加隐蔽，成功非法获取的比例更高，威胁也更大。

支付授权骗局

而除了多重签名会导致投资者失去钱包控制权限外，针对特定加密资产的授权盗币也更加普遍。其原理在于，区块链允许用户将自己地址内一定数量的代币的操作权限让渡给另一个地址，这是通过智能合约实现的，需要用户执行一笔链上交易。

例如 Alice 的地址里拥有 1000 枚 USDT，她通过调用智能合约发起了一笔链上交易，交易细节为将自己地址内 100 额度的 USDT 操作权限让渡给 Bob 的地址，成功后 Bob 即可通过自己的地址发起交易，将 Alice 地址中不超过 100USDT 进行转移，而无需 Alice 的再次同意。

盗币者利用了这一点，通过将授权链接转换为二维码，向受害人声称这是一个转账支付二维码，受害人只要扫码并发起交易便会将特定代币的全部额度操作权限让渡给盗币者。



支付授权骗局

以近期较流行的高仿转账盗币为例。请注意，上图右部的界面并非 OKX Web3 钱包的系统转账界面，而是盗币者高仿的网页，真实 OKX Web3 钱包的转账界面并非如此，更不会标记某个地址为「欧意官方认证」（OKX official certification）。

其真实目的在于，在诱导受害人通过钱包浏览器打开钓鱼网站后，通过高仿页面误导受害人以为自己正在执行转账，但实际上提交的交易内容是代币授权。如果钱包不对交易内容做校验并提醒，受害人几乎不可能发现自己已经上当。等到他们意识到的时候，诈骗者已经完全获得了钱包内资产操作的权限。

这种授权诈骗方法构成了重大威胁，因为它利用了智能合约交互的复杂性和受害者对技术交易细节的不熟悉，使其成为诈骗者利用的非常有效的工具。

假 TG 骗局

Telegram 是 Web3 用户常用的重要社交软件之一，因其较高的匿名性而颇受 OTC 商的青睐，也因此盗币者定向针对这一群体开发了假 Telegram APP。

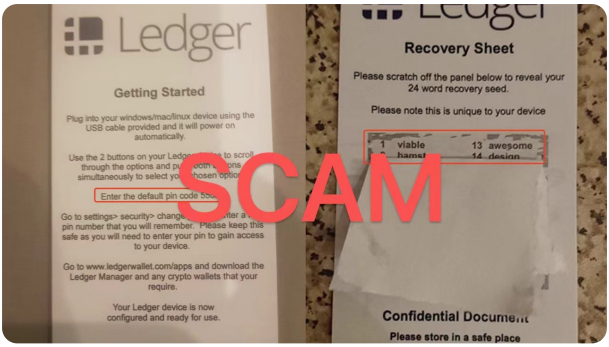
该手法类似前面所提及的假钱包 APP，同样是在 Telegram APP 代码文件中添加恶意代码，目的有二——

其一是获取受害人所有的聊天记录，部分受害人会通过 Telegram 传输或保存自己地址的助记词、私钥，通过这种方式盗币者可以直接窃取资产；

其二是篡改受害人发送的信息，其原理在于自动识别输入内容，将其中特定形式的信息（例如 0x 开头的字符串）进行替换，发送地址的人在本地客户端不会察觉任何异常，但另一端的人所收取的则是被替换的地址。这种替换活动一旦发生在常见的转账场景下，就会出现一方将加密资产转入盗币者地址的情况。

硬件钱包说明书欺诈

硬件钱包是广受推崇的资产存储方式，通过隔离网络与助记词、私钥，理论上投资者能够免受密钥泄露的风险，但仍然存在特定的方式实现盗窃。接下来我将介绍一种社会工程学盗币手法——



欺诈团队制作的假硬件钱包手册

受害人于第三方电商平台购入某品牌硬件钱包一台，打开包装后，按照「说明书」上标注的「初始 Pin 码」打开了硬件钱包，并在备份了「说明书」上印制的「助记词」后，向钱包地址存入了大量资金，最终失窃。

其原因并非钱包在硬件层面遭到破解，而是被盗币者提前激活获取地址助记词，而后伪造虚假说明书进行二次封装，再通过非官方的渠道将已激活的硬件钱包销售给受害人。这表明识别官方电商店铺，重要性等同于识别官方网址。

通过操纵用户对硬件钱包的信任，并利用这些设备本质上是安全的假设，诈骗者能够通过这种精心设计但有效的社会工程策略窃取资产。

当你开始交易加密资产

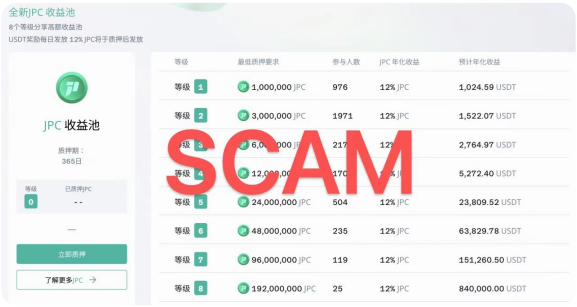
截至目前，你已经可以识别并避开那些虚假信息渠道，并对那些不安全的资产存储方式有所了解，成功让自己度过了艰难的「新手期」，接下来就要开始面对真正的挑战——用自己的真金白银去市场上参与交易。

你是否认为加密市场上存在可持续的年化收益超过 50% 的理财项目？是否认为用手中闲置的稳定币去某个「矿池」里「质押」就能稳定赚到钱？是否认为购买某个代币去参与「交易所官方」的质押活动就能轻松赚钱？如果你的答案都是「是」，那么你可能危险了。

高收益的交易所理财骗局

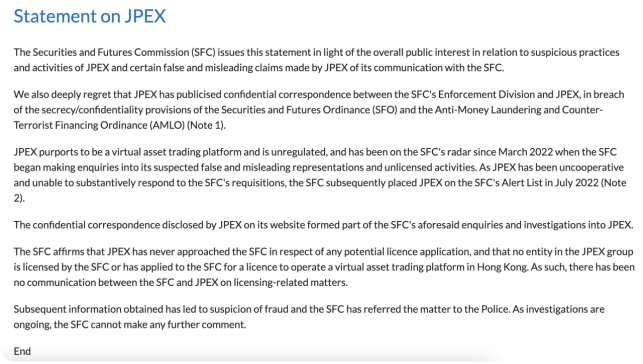
在中心化加密货币交易平台购买加密资产是最常见的投资方式之一，部分中心化交易平台的运营方为了吸引更多的用户资金留存，会推出一些理财产品，例如最常见的质押代币获取更多同种或者其他代币。这类理财产品通常收益率不高且存在额度限制，正常展业的平台也不会将这类理财产品作为主要经营项目。

但某些欺诈平台会虚构理财产品超高收益，吸引大量非专业投资者购买参与，并诱导设置较长的质押周期以限制客户赎回。等到质押结束，这类理财产品或是无法兑付，或是所兑付代币已极大贬值，甚至是平台直接跑路（rug），给投资者造成财产损失。



JPEX 高收益骗局

以 2023 年 9 月暴雷的 JPEX 交易所为例。该所的经营方式非常激进，采用余额返点而非交易手续费返点的邀请模式，鼓励投资者大量存入加密资产并邀请亲朋好友。平台还发行了名为 JPC 的代币，声称该代币系平台的治理代币，持有者能够参与所谓的「节点质押」获取至少 12% 的稳定年化收益率，通过增加参与资金与锁定期限，该收益率还会上升。



Statement on JPEX

The Securities and Futures Commission (SFC) issues this statement in light of the overall public interest in relation to suspicious practices and activities of JPEX and certain false and misleading claims made by JPEX of its communication with the SFC.

We also deeply regret that JPEX has publicised confidential correspondence between the SFC's Enforcement Division and JPEX, in breach of the secrecy/confidentiality provisions of the Securities and Futures Ordinance (SFO) and the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO) (Note 1).

JPEX purports to be a virtual asset trading platform and is unregulated, and has been on the SFC's radar since March 2022 when the SFC began making enquiries into its suspected false and misleading representations and unlicensed activities. As JPEX has been uncooperative and unable to substantively respond to the SFC's requisitions, the SFC subsequently placed JPEX on the SFC's Alert List in July 2022 (Note 2).

The confidential correspondence disclosed by JPEX on its website formed part of the SFC's aforesaid enquiries and investigations into JPEX.

The SFC affirms that JPEX has never approached the SFC in respect of any potential licence application, and that no entity in the JPEX group is licensed by the SFC or has applied to the SFC for a licence to operate a virtual asset trading platform in Hong Kong. As such, there has been no communication between the SFC and JPEX on licensing-related matters.

Subsequent information obtained has led to suspicion of fraud and the SFC has referred the matter to the Police. As investigations are ongoing, the SFC cannot make any further comment.

End

香港证券及期货事务监察委员会（证监会）关于 JPEX 的声明

基于这种经营模式，JPEX 吸引了大量非专业投资者的资金，参与者遍布香港、台湾、内地、新加坡等地，最后恶意 Rugpull。据香港警方披露，案发后有超过 2000 名受害人报案，涉及金额高达 13 亿港币。

此类高收益投资骗局非常危险，因为它们利用看似安全、丰厚的回报和成熟交易平台的信誉的诱惑来瞄准非专业投资者。

貔貅币欺诈

「只能买不能卖」的骗局除了会发生在中心化平台以外，在去中心化交易所（DEX）里也会发生，但其原因并不在于 DEX，而在于代币的发行者。

开发者在区块链上根据特定标准发行一个代币（Token）时，不仅能够设置一些基本参数，例如代币名称、代码、数量上限等，还可以限制特定地址对该代币的访问权限，例如让这些地址无法转账或卖出所发行代币等。而当限制范围几乎囊括了所有地址仅有少数发行者自身地址能够访问时，我们称这个代币为「貔貅币」（honeypot token）。

文如其名，不在白名单列表里的地址，在买入或者获取这类代币后，无法通过常规的手段在 DEX 交易对里将代币出售，只能眼看着代币涨跌无法退出。这类骗局有许多变种——

一种是简单的限制卖出手法。欺诈者发行貔貅币并在 DEX 中建立流动性池后，会通过社交平台污染、网络社群广播、向知名地址空投等方式推销这个代币，同时利用多个地址反复交易快速拉升币价。此时如有不明就里的受害人买入，就会发现自己的账户头寸价值迅速上涨，但却无法卖出获利。最后在有足够多受害人买入代币后，欺诈者再通过撤回流动性的方式，有效地耗尽所有资金，让受害者只剩下毫无价值的代币。

一种是结合了杀猪盘手法的权限可修改貔貅币。欺诈者在发行貔貅币后，通过社会工程学手段诱骗新手投资者购买，在早期一到两个项目中，将目标对象的地址加入白名单允许其卖出获利，从而骗取受害人的信任。但当受害人加大投入后，欺诈者就不再允许其卖出，完成欺诈。

这种方法具有很强的欺骗性，因为受害者根据最初的成功交易而认为他们正在进行合法的投资。

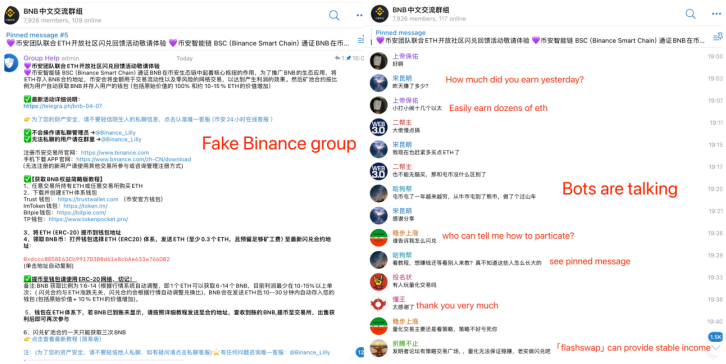
还有一种是针对「聪明钱」地址跟随者的猎杀。所谓聪明钱，指的是链上投资胜率较高的地址，由于区块链公开透明的特性，任何人都能够观察到所有地址的交易活动，因此有交易员或情报分析公司会对这类高胜率地址密切关注，当聪明钱地址买入某个代币时，部分交易员也会选择跟随买入。

于是针对这批追随者地址的貔貅币骗局出现了，欺诈者在发行代币并建立流动性池后，会通过调用特定智能合约的方法发起一笔交易将资金池中的代币发送给聪明钱地址，部分监控机器人可能会将这笔交易错误识别为聪明钱地址的买入行为，进而误导其他跟随者买入。

这导致一系列来自不知道代币是貔貅币的交易员的后续购买。然后，骗子等待足够数量的受害者买入，然后再撤回流动性，让追随者陷入无法出售的代币的困境。

假币安矿池骗局

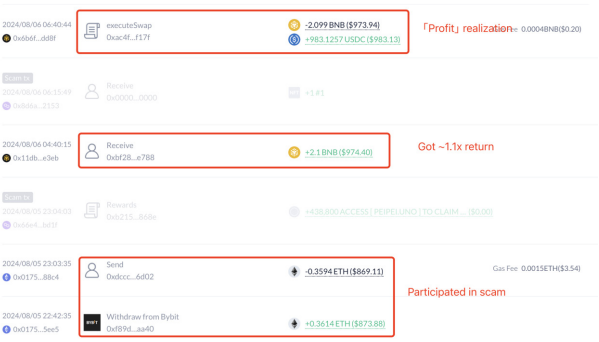
在前面我们提到了冒充特斯拉的「双倍返还」欺诈手法，这种骗局的主要受众是不了解区块链知识的圈外用户，接下来我会介绍主要针对圈内用户更具迷惑性的「假币安矿池」欺诈。



假币安群聊天记录

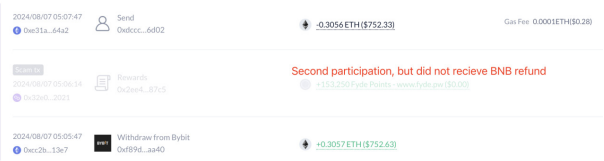
这是一类历史悠久的欺诈方式，欺诈者通常会以「币安交易所交流群」、「币安回馈福利群」等名称创建 Telegram 社群，随后填充数千到数万 Bots 账户，以冒充币安官方社群，通常这个群只有受害者一个人是真人。

欺诈者接着会以「币安客服」的名义，在假社群中发布信息称币安交易所与以太坊基金会合作，正在开展用户回馈营销活动，允许用户使用 ETH 以高于市场汇率的价格换取 BNB 进而赚取差价收益。社群中也会有大量 Bots 模仿真人聊天，宣称他们通过闪兑（flashswap）赚到了许多钱。



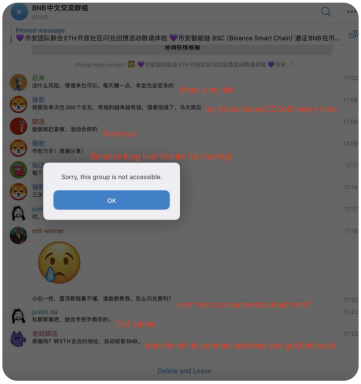
欺诈性诱饵

按照欺诈者的要求，受害人首先需要在以太坊网络中，向一个智能合约账户转一定数量的 ETH，接着受害人会在 BSC 区块链上收到大约价值 1.1 倍的 BNB 返还，超出市场价格的部分就是受害人的「收益」。



受害者链上操作记录

尝到甜头的受害人如果再次参与的话，就不会收到 BNB 返还，接着如果受害人在社群内说自己被骗，就会马上被管理员封禁并解散群组，至此整个骗局完成。



假币安群聊天记录

假 OKX 公链持 USDT 领 OKT 骗局

流动性挖矿是加密行业在 DeFi 时代所流行的事物，用户通过将一定数量的代币存入某些智能合约地址，便能够参与 Dapp 治理、获取投票权、借钱给其他人、为链上协议提供安全性等。在这些活动中，存入代币的用户可以获取一定的收益。

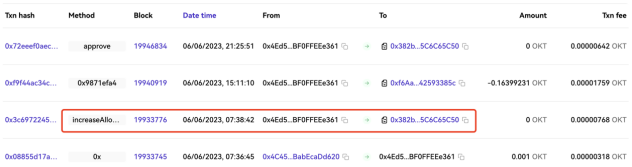
因此有欺诈者假借「流动性挖矿」的名义，设计了大量不同形式的欺诈手法，这里以针对新手用户的「假 OKX 公链持 USDT 领 OKT 」骗局为例进行介绍。

欺诈信息

这一骗局声称，用户只需要在钱包里存放 USDT，就能持续获得超高年化收益率的 OKT，并且不存在代币锁定期，用户随时可以转移地址里的资金。

欺诈信息

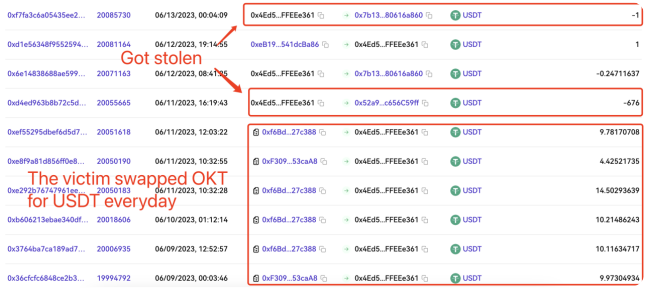
按照欺诈者宣称的规则计算，即使是最低一档，参与者的年化收益率也将达到 475%，许多刚刚参与 Crypto 投资，对区块链不甚了解的新手用户很容易被高收益所欺骗。



Txn hash	Method	Block	Date time	From	To	Amount	Txn fee
0x72eeef0aec...	approve	19946834	06/06/2023, 21:25:51	0x4Ed5...BF0FFEEe361	0x382b...5C6C65C50	0 OKT	0.00000642 OKT
0xf9f44ac34c...	0x9871efa4	19940919	06/06/2023, 15:11:10	0x4Ed5...BF0FFEEe361	0xf6Aa...42593385c	-0.16399231 OKT	0.00001759 OKT
0x3c6972245...	increaseAllo...	19933776	06/06/2023, 07:38:42	0x4Ed5...BF0FFEEe361	0x382b...5C6C65C50	0 OKT	0.0000768 OKT
0x08855d17a...	0x	19933745	06/06/2023, 07:36:45	0x4C45...BabEcaDd620	0x4Ed5...BF0FFEEe361	0.001 OKT	0.00000318 OKT

恶意授权

通常，欺诈者会要求受害人第一时间交互欺诈合约以参与「挖矿」，实际上该合约是给欺诈者地址的无限额度 USDT 的授权。



0xf7fa3c6a05435ee2...	20085730	06/13/2023, 00:04:09	0x4Ed5...FFEEe361	0x7b13...80616a860	USDT	-1
0xd1e56348ff552594...	20081164	06/12/2023, 19:14:55	0xeB19...541dcBa86	0x4Ed5...FFEEe361	USDT	1
0x6e14838688ae599...	20071163	06/12/2023, 08:47:35	0x4Ed5...FFEEe361	0x7b13...80616a860	USDT	-0.24711637
0xd4ecf963b8b72c5d...	20055665	06/11/2023, 16:19:43	0x4Ed5...FFEEe361	0x52a9...c656C59ff	USDT	-676
0xef55295dbef6d5d7...	20051618	06/11/2023, 12:03:22	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	9.78170708
0xe8f9a81d856ff0e8...	20050190	06/11/2023, 10:32:55	0xF309...53caA8	0x4Ed5...FFEEe361	USDT	4.42521735
0xe292b76747961ee...	20050183	06/11/2023, 10:32:28	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	14.50293639
0xb606213ebae340df...	20018606	06/10/2023, 01:12:14	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	10.21486243
0x3764ba7ca189ad7...	20006935	06/09/2023, 12:52:57	0xf6Bd...27c388	0x4Ed5...FFEEe361	USDT	10.11634717
0x36cfcfc6848ce2b3...	19994792	06/09/2023, 00:03:46	0xF309...53caA8	0x4Ed5...FFEEe361	USDT	9.97304934

受害者链上操作记录

在最初的几天，受害人每天都会收到一定数量的 OKT，一旦他加大投入或者长期未增加投入，欺诈者就会调用 transferfrom 方法，将受害人地址中所有的 USDT 转走，完成欺诈。

流动性退出骗局

自动做市商（AMM）是最主要的一类去中心化交易平台（DEX），其业务实现原理为通过智能合约为用户自动报价，而无需点对点撮合。因此需要流动性提供者（LP）向合约中按照特定汇率放入成比例的两种代币，用户的每次兑换行为都会影响合约中的两种代币汇率，进而对价格造成影响。例如某个资金池中同时有一定数量的 A、B 两种代币，用户使用自己持有的 A 代币兑换了一些 B 代币，使得资金池中 A 代币数量增加，B 代币数量减少，将导致以 A 为价格单位的 B 代币价格上升。

利用这一特点，欺诈者设计了基于 AMM 的流动性退出骗局——

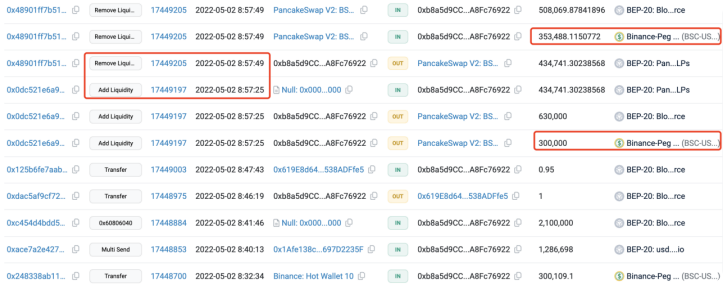
欺诈者首先会在链上发行一个代币（成本不会超过 100 美金），并去主要的 DEX 上为代币提供流动性，通常会与 WETH 或者 USDT 配对。

接着通过其他手段——例如前文所提到的那些，令其他投资者相信这一代币是有升值潜力的，进而诱导受害者们买入。

然后，由于受害者们的买入，导致欺诈者发行代币的价格上升。

最后，欺诈者只需要撤回流动性，就能够从资金池中提取大量 WETH 或者 USDT（取决于配对的代币是什么），相对于这一系列操作极低的手续费成本，欺诈者几乎是一本万利。

2024 年 2 月 20 日，河南南阳高新技术产业开发区人民法院判决了一起加密货币欺诈案件，被告人因发行虚假加密货币并误导他人充值 5 万 USDT，后迅速「撤回资金」造成他人损失，而被判诈骗罪。



0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	PancakeSwap V2: BS...	IN	0xb8a5d9CC...A8Fc76922	508,069.87841896	BEP-20: Blo...rce
0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	PancakeSwap V2: BS...	IN	0xb8a5d9CC...A8Fc76922	353,488.1150772	Binance-Peg ... (BSC-US...)
0x48901ff7b51...	Remove Liqui...	17449205	2022-05-02 8:57:49	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	434,741.30238568	BEP-20: Pan...LPs
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	Null: 0x000...000	IN	0xb8a5d9CC...A8Fc76922	434,741.30238568	BEP-20: Pan...LPs
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	630,000	BEP-20: Blo...rce
0x0dc521e6a9...	Add Liquidity	17449197	2022-05-02 8:57:25	0xb8a5d9CC...A8Fc76922	OUT	PancakeSwap V2: BS...	300,000	Binance-Peg ... (BSC-US...)
0x125b6fe7aab...	Transfer	17449003	2022-05-02 8:47:43	0x619E8d64...538ADFfe5	IN	0xb8a5d9CC...A8Fc76922	0.95	BEP-20: Blo...rce
0xdac5af9cf72...	Transfer	17448975	2022-05-02 8:46:19	0xb8a5d9CC...A8Fc76922	OUT	0x619E8d64...538ADFfe5	1	BEP-20: Blo...rce
0xc454d4bdd5...	0x60806040	17448884	2022-05-02 8:41:46	Null: 0x000...000	IN	0xb8a5d9CC...A8Fc76922	2,100,000	BEP-20: Blo...rce
0xace7a2e427...	Multi Send	17448853	2022-05-02 8:40:13	0x1Afe138c...697D2235F	IN	0xb8a5d9CC...A8Fc76922	1,286,698	BEP-20: usd...io
0x248338ab11...	Transfer	17448700	2022-05-02 8:32:34	Binance: Hot Wallet 10	IN	0xb8a5d9CC...A8Fc76922	300,109.1	Binance-Peg ... (BSC-US...)

欺诈者链上操作

据区块链浏览器显示，2022 年 5 月 2 日，欺诈者于 UTC 时间 8:41:46 发行了 BFF 代币，并于 8:57:25 在 DEX 中创建了 BFF-USDT 交易对，初始投入 30 万 USDT 与 63 万 BFF 进资金池，但仅在 24 秒后，欺诈者便撤回了所有流动性。由于在此期间已有受害人大量购入，导致资金池汇率发生变化，欺诈者撤回流动性的行为为他带来了超过 5 万 USDT 的非法所得，全程仅花费 25 分钟。

而同类型的欺诈手法无时无刻不在链上发生，且不是每次都能够幸运追回损失资金，这提醒普通投资者在参与链上交易前，务必要了解其中风险。

疯狂的网络钓鱼：病毒式增长

网络钓鱼（Phishing）是一种通过发送欺骗性邮件、短信、电话或网站，意图引诱用户泄露敏感信息或进行恶意操作的攻击方式。在传统互联网时代，这类钓鱼活动通常都是为了牟取受害人现金资产或虚拟资产，而近年来随着加密经济的发展，越来越多的欺诈者开始盯上 Web3 行业。

以下我们将介绍三种常见的，以不特定对象的加密资产为目标的网络欺诈手法。

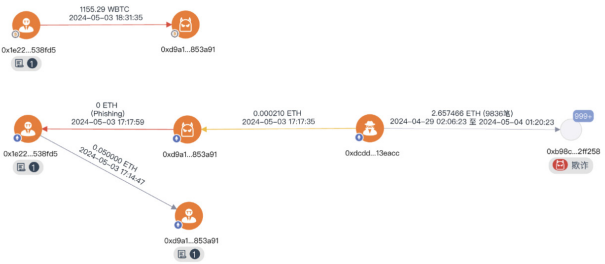
地址投毒

如果你拥有一个正在使用中的区块链地址，那么你一定会发现自己的地址时不时就会收到一笔极小金额的转账，这些转账并不会对你的地址使用造成任何影响，它们只是静静待在你的转账记录里。

这其实是当前非常流行的地址投毒钓鱼，主要的实现形式是向目标对象转账极小金额的ETH、USDT、TRX等代币，从而污染对方的转账记录，假如目标对象的钱包使用习惯不好，就有可能在转账的时候从记录中复制错误的地址，进而将资金错误转账给欺诈者。

如果更深入考察发起转账的投毒地址，会发现它尾部的字符与目标对象的主要交互对手方是一致的，这正是这个骗术的核心障眼法——用来钓鱼的地址是针对目标对象定制的同尾号地址。

其实现原理是通过特定程序批量生成区块链公私钥对，保留那些有特定意义的地址，例如尾号全都是 6、8 等大众喜爱的数字，这类账户通常醒目而有趣，我们称之为「虚荣地址」或者「靓号」。这种技术同样可以应用在地址投毒活动中，只不过批量生成的地址是对目标对象地址的模仿。



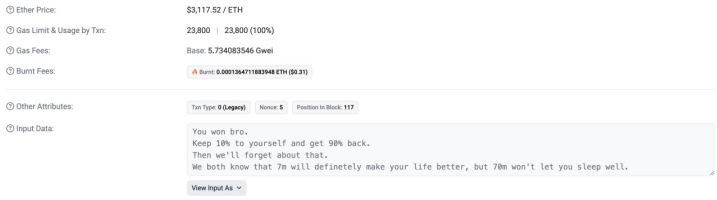
地址投毒相关分析

例如发生在 2024 年 5 月 3 日的史上最大的地址投毒惨案，受害人错误向投毒地址转移了 1155 枚比特币，当时价值 6800 万美金。复盘这个案例不难发现，受害人 0x1e22 在当天向自己的新地址 0xd9a1b0b1e1ae382dbdc898ea68012ffcb2853a91 转入了 0.05ETH 用于购买 DAI，这一行为迅速被钓鱼团伙识别，3 分钟后便利用 0xd9a1c3788d81257612e2581a6ea0ada244853a91 向受害人发起 0 转账。75 分钟后，受害人复制到错误的地址，向钓鱼地址转移了 1155 枚比特币。

对钓鱼地址手续费进行溯源不难发现，上游地址已作案 9836 次，而这只是这类钓鱼活动的冰山一角。

广告代币

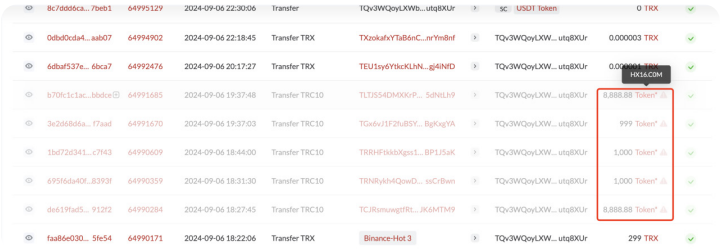
区块链转账的时候，通常都可以在交易之外携带一些与交易本身无关的信息，例如以太坊官方浏览器就支持解析并展示用户的链上留言，这种浏览是公开非加密的，因此所有人都可以看见其内容。



钓鱼受害者通过链上交易给诈骗者留言

在前面提到的 1155BTC 被钓鱼事件中，受害人就第一时间通过留言功能向钓鱼团伙发声，声称只要退换 90% 就不追究其责任，后续双方以此建立了联系，并最终达成了退还协作，在这过程中双方都是匿名的。

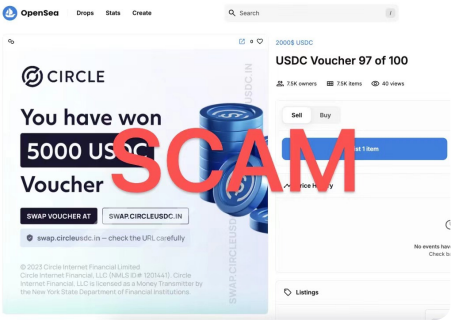
但这种需要工具解析的信息传递形式，对于广告投放者而言仍然不够醒目直接，为此他们开始通过将代币符号设置为域名的形式传递广告内容。



广告代币

例如主流公链之一的 Tron Network，其网络交易中就存在着大量广告代币的转账，这些广告的宣传对象包括但不限于网赌网站、色情网站、能量租用网站等，也存在大量欺诈链接，收到这类代币的投资者若出于好奇进入网站并交互，就存在资金损失的可能。

而随着 NFT 经济的崛起，这类广告钓鱼形式也在非同质化代币上得到了应用。NFT 玩家想必时常会遇到账户被空投陌生 NFT 的经历，这些空投而来的 NFT 大部分都是欺诈网站批量发起的，它们制作精良，会在海报上强调你获得了数千美元的奖励，需要进入钓鱼网站领取。有的欺诈者还会煞有介事地操纵欺诈 NFT 的价格，使得它们的地板价看上去真的非常昂贵。

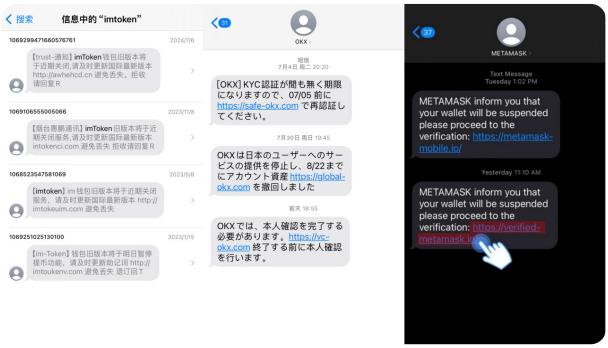


钓鱼 NFT

例如上图中的欺诈 NFT，名为「2000$USDC」，它声称你有资格获取 5000USDC 的奖励，是一百个幸运儿中的一个。但实际上他给 7500 个地址都空投了，显然这是一个骗局，访问海报中出现的网站，只会导致自己的资金损失。

清退短信

冒充公检法或者行业机构，对普通投资者投放钓鱼链接，是非常流行的 应用于 Web3 行业的欺诈手法之一。



欺诈短信

在个人信息泄露的情况下，投资者会收到大量欺诈短信或邮件，其核心手法为声称「旧版本软件需要更新」，请受害人访问钓鱼网站。对于钱包类型的钓鱼短信，通常会被要求下载假钱包 APP，对于交易所类型的钓鱼短信，则通常是杀猪盘。

假钱包钓鱼

Bitrace 曾调查过一起案件，2023 年 11 月，知名中心化交易平台 Binance 的联合创始人赵长鹏被捕入狱，有欺诈者声称将资金存放在中心化交易平台并不安全，有受害人出于害怕将资金从 OKX 交易所转出，过程中私钥被骗取，导致最终损失 166.7ETH。

这类手法的核心是，利用普通投资者对行业政策的不了解，通过诉诸权威进而恐吓、诱骗的方式拿到受害人的钱包助记词或私钥。

产业分工的尽头：Crypto Drainer

依据李嘉图的比较优势理论，在市场经济下，各个经济部门之间总会自发进行分工以提高生产效率，这一理论在 Web3 欺诈领域同样适用。

其典型特征在于，位于欺诈产业链最前端的技术开发部门不再参与实际的欺诈软件推广工作，而是直接面向代理商提供软件运营服务（SaaS），并从中抽取分成。这种模式使得各类欺诈活动的发起门槛急剧降低，欺诈者仅需专注于软件推广。

对于这类 SaaS 提供者，我们称他们为 Crypto Drainer。

盗币代理模式

前文中所提到的假钱包 APP 盗币活动背后，正是在庞大盗币需求市场中野蛮生长的 Crypto Drainer。他们会对主流加密货币钱包软件进行逆向分析，并修改特定代码用以获取目标助记词，为了帮助代理商管理庞大的助记词，还会开发专门的管理后台，使得代理商能够一键划转受害人的资金或者多签受害人的地址。

类似传统互联网 SaaS 提供商，假钱包类 Crypto Drainer 通常也会有多种代理模式——

例如最常见的直接推广 Crypto Drainer 的木马链接，这种模式无后台，代理商只需要通过社交软件、搜索引擎、自媒体平台等渠道引流即可，由 Drainer 执行盗窃并按照比例给代理商分成。

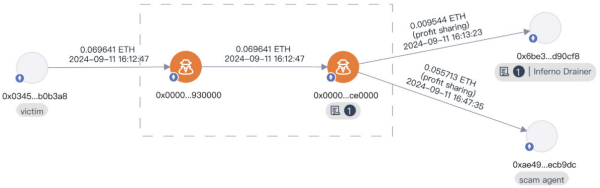
还有针对较大代理商的独立部署方案，在这个模式下代理商可以自行管理盗币后台，完成推广、转化、盗窃等全部流程，也可以进一步转包给更下一层级的代理商，以赚取分成费用。

不同模式下的分成比例不同，代理商群体亦有差别，表明盗币类 SaaS 市场在当下已经相当繁荣。

钓鱼代理模式

地址投毒、假冒官方社交账户、套利骗局等以骗取受害人代币权限的钓鱼欺诈手法背后，同样是专业的 Crypto Drainer 在提供技术甚至运营支持。

以知名的 Inferno Drainer 为例，该团伙通过电报频道推广服务，由开发者提供给诈骗分子需要的钓鱼网站以支持其诈骗活动，一旦受害者扫描钓鱼网站上的二维码并连接钱包，Inferno Drainer 就会检查并定位钱包中最有价值且易于转移的资产，发起一笔恶意交易。



Drainer 模式分析

受害者确认这些交易后，资产便会被非法转移并处置，其中被盗资产的一定比例归 Inferno Drainer 的开发者所有，其他部分则归诈骗分子所有。

再以经典的「带你赚钱」类型的钓鱼欺诈为例，这类骗局的欺诈者通常会在短视频平台、媒体平台、社交软件中寻找目标对象，然后主动接近并告知自己有赚取高额收益的渠道，而方法不外乎前文所提及的杀猪盘、虚假矿池等，在受害人产生资金损失后，欺诈者与 SaaS 提供商会分配这笔收益。

这类骗术技术门槛较低，更强调欺诈话术的使用，因此部分 Drainer 在招募代理商的时候，还会提供额外的欺诈 SOP 教学。

场外交易欺诈：最薄弱一环

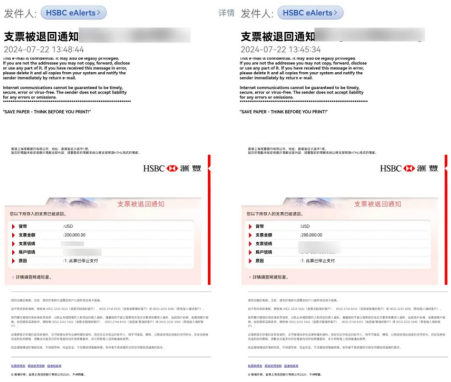
在部分国家或地区，场外交易（OTC）是加密货币投资者群体最常用的转换法币与 Crypto 的交易方式，这类 OTC 活动可以发生在中心化平台、网络群组、线下等多种场景，但不论是何种场景，OTC 活动都存在着遭受欺诈的风险。包括但不限于法币被骗，加密资金被骗，甚至人身安全受到威胁等，以下我们将列举出一些常见的欺诈手法。

交易所币商欺诈

对大部分普通投资者而言，在中心化交易平台的 C2C 交易区与币商进行买卖交易，是最常见的出入金形式。在这个渠道里，交易所起到了类似担保平台的作用，除了会对平台内的 C2C 商家进行约束与管理外，还会建立完善的交易程序。

通常的流程是，卖家将预备卖出的代币交给平台托管，当买卖双方互相确认钱款已支付到账后，平台再将代币划转给买家。但即便如此，仍然有欺诈的存在空间，以投资者向币商卖币的场景为例——

一种常见的骗局是币商伪造支付记录。例如通过技术手段修改支付工具的信息显示，或者甚至只是给手机屏幕截图进行伪造，声称款项已经支付并催促卖家尽快确认交易。投资者一旦轻信，不加以验证并允许平台划转代币，就会损失这部分资金。



支票欺诈

另一种是利用银行支票可撤回特性进行欺诈的案例。同样的交易场景，买家通过银行支票进行支付，在卖家误认为资金已完全到账确认放币后，再撤回支票骗取代币。这类欺诈手法的主要对象是不流行使用银行支票的国家的民众。

线下交易欺诈

有大量场外交易是发生在线下的，部分新手投资者认为网络上容易被骗，更加信任面对面的场景，因而甚至会出现驱车前往数百公里外的某个地点进行交易的情况。

目前针对这类对象的欺诈手法有——

欺诈者向受害人收购代币，要求通过现金支付，然后在交易现场收到代币后，向受害人支付了一袋假币，甚至是冥币（祭奠逝者所用的仿钞）；

欺诈者向受害人收购代币，使用线上支付工具，但自己并不直面受害人，而是通过匿名软件雇佣一名第三方人员前往交易地点假装自己。受害人前期出于谨慎连续小额交易，在多次成功后放松警惕，一次向收款地址转账了大量代币，但这一笔最大的交易并不会收到现金。受害人意识到被骗后通常会试图拦住交易对手方并报警，但这不会有作用，因为对方并不知情，且在欺诈完成后欺诈者会删除所有聊天记录，无所对证；

欺诈者向受害人出售低价代币，并要求受害人使用现金交易，但到达现场后会有数名暴徒冲出，将受害人手中的现金抢走。这类手法本质上是利用低价代币作为诱饵的抢劫，性质十分恶劣，甚至会对受害人人身安全造成威胁。

线下多签欺诈

前文我们提到，假钱包盗币者会通过假钱包 APP 盗取受害人的助记词或私钥，从而非法获取钱包中的资产，而近年来我们也注意到一类发生在线下场景的多签盗币手法。

欺诈者与代币买家约定在线下某地进行交易，见面后，欺诈者会以「你的地址上有风险资金」、「你的钱包可能被植入了木马」等理由，要求受害人另外创建区块链钱包用以收款，否则便拒绝交易。受害人通常是驱车从外地前来交易，已经产生了大量的时间跟精力，为了交易顺利进行只得照做。

而在受害人创建钱包过程中，欺诈者会在身后偷偷拍下受害人新钱包的助记词，并发送给同伙。同伙收到后，会立即将受害人的地址设置为多重签名地址。

接着交易会非常顺利地完成，受害人的地址内收到了欺诈者发来的代币，欺诈者也收到了受害人发来的转账或者现金。但在交易完成后，受害人才会发现自己根本没有办法操作这个钱包地址，最后只能眼睁睁看着欺诈者将资金转走。

这种欺诈手法将钱包地址多签的原因，与假钱包手法中的情况一样，都是为了不让受害人将资金转走。

一些安全建议

不要让恐惧、贪婪等情绪操控自己

相对于其他领域，Web3 行业具备更高的门槛，这些门槛既包括技术原理方面的理解门槛，也包括基础设施使用方面的上手成本，以及获取准确信息的门槛，盲目自信无视这些壁垒的新人往往会因此掉入陷阱。

例如所谓「黑 U 检测」类型的欺诈，部分受害人对于不法分子利用加密货币进行洗钱的事情有所耳闻，也知道执法部门会对案件中的加密货币资金进行追踪，出于恐惧会点击欺诈者提供的钓鱼链接以检测自己的地址是否安全，进而被授权盗币。但实际上检测地址资金风险的 KYA、KYT 工具根本不需要连接钱包，输出地址即可查询，这便是知其然而不知其所以然的坏处，也是让恐惧情绪操控自己的苦果。

对于新手投资者，最好的选择永远是更多地待在自身的认知边界内，在充分学习了解的基础上进行小成本的试错，这是避免欺诈对自己造成重大损害的有效方法。

不要盲目信任，要去验证

盲目自信之外，盲目他信也是损失的来源。包括相信搜索引擎的钱包下载链接展现，相信社交平台中博主给出的空投链接，相信主动给你搭讪的网友会带你赚钱等。

欺诈方式五花八门，但究其根本都是缺乏验证。如果你有收藏权威 Web3 数据平台、官方社媒账户、官方网站，那么当你想要下载钱包 App 时，就至少有三个渠道能够交叉验证网友给你的或者你自己在网上搜到的下载链接是不是安全的；如果你保持了良好的交互习惯，你就会在每次重要交易提交前，在浏览器上查看合约的历史交互记录，这样就能够第一时间发现异常现象；如果你进了一个群，人人都说自己在赚钱并极力邀请你加入，那么你至少应该使用 KYA、KYT 工具考察一下相关地址，看是否已经被标记为欺诈，而不是盲目冲入。

拒绝轻易相信他人，并持续保持验证，会让你的加密之旅变得平坦。

大多数 Crypto Scams 都是老骗术

正如绝大部分 Web3 协议并没有对传统互联网的同类型业务带来创新一样，Crypto Scam 也同样没有脱离传统互联网欺诈的框架。

目前为止，绝大部分涉币欺诈手法都能够在传统互联网上找到原型，区别仅仅只是使用区块链技术优化了原有的骗术，或者骗术本身就是以 Crypto 为目标。

例如冒充公检法的骗局，传统做法是要求受害人将法币转给欺诈者的银行卡，现在会要求受害人去买币并转给特定地址；又例如很多人都知道「双倍返还」是老骗术，可一旦这个骗术披上区块链技术与 Musk 的外包装，许多人又不认识了，还以为是技术创新。

深入学习已有的互联网欺诈手法，将对你识别 Crypto Scam 有所帮助。

沉没成本不是成本

中国有一句古话叫做“来都来了”，这句话的意思是某人在实现目标的过程中遇到了一些未曾预料的变动，为了不让之前的付出被浪费，而选择继续进行下去。这一心理特点，遭到了欺诈者的广泛利用。

前文提到的线下多签欺诈便是如此。受害人从银行取出大额现金，和朋友一起驱车前往数百公里外的地点，一路小心谨慎，没想到在到达现场后欺诈者会要求他下载新钱包否则不予交易。受害人此时本可以选择原路返回，但为了不让之前的辛苦白费，而坚持参与交易，最后被欺诈者得手。

近期高发的加密货币杀猪盘 (Romantic Scam) 也是如此。受害人在开始怀疑对方之前，往往就已经投入了较多的资金，欺诈者利用受害人想要取回本金的心理，以缴税、凑额度等为由要求加大投入，最终导致受害人越陷越深。

沉没成本不是成本，在面对自己认为是可能的骗局时，及时放弃也不失为止损的好方法，不应让过去的付出成为未来决策的依据。

遭遇欺诈后该怎么办

遭遇 Crypto Scam 后挽回损失的最重要方式是寻求执法部门的帮助，因此受害人在意识到被骗后的所有挽回行为都应当为成功立案调查服务。

及时止损

在发现资产损失的第一时间，及时发起反制，能够或多或少减少损失扩大，这些必要的动作包括——

- 如果是助记词丢失，需快速将其余资产转移到安全的场所。这里的「其余资产」包括同一条链的其他代币或 NFT，同一组助记词派生的其他区块链地址的资产，与被盗区块链地址在同一部智能设备中的其他地址的资产等；
- 如果是投资理财类欺诈，则立即停止进一步的投入，并提款退出；
- 如果是授权盗币，则需要尽快去取消所有地址的可疑授权。

当然，这些反制措施在进行过程中都要遵守前文提到的安全原则，否则存在遭遇其他欺诈的可能。

保护现场并报案

许多人在发现自己被骗、被盗后，第一反应是把被盗钱包、欺诈 App 、欺诈者聊天方式删除，甚至是将设备格式化，地址助记词也不保留。这种过激行为是无法帮助挽回损失的，一则这并不能从根本解决问题，二则会给后续的调查造成困扰。例如——

- 删除钱包 APP 将导致安全公司难以验证是否为假钱包；
- 欺诈 APP 文件中可能会包含一些调查线索；
- 对立案、办案过程中的取证环节造成影响。

受害人在止损过程中，必须要保护好案发现场。

寻求相关方帮助

这里的相关方包括与被盗资产存在关联的平台，以及能够提供分析服务的安全公司。

假如你的链上地址被盗了，你应当时刻保持对资金转移的关注，一旦发现资金有流入中心化交易平台的情况，便立即联系平台客服，要求平台对这个充值地址进行冻结。在你提交的证据足够清晰的情况下，平台通常会对该账户提起 2–7 天的临时风控，在这期间账户资金无法转移。此时你再去请求执法部门向相关平台发函配合调查即可。

假如你和你身边的朋友都缺乏对链上资金的追踪能力，那么你可以寻求专业的区块链安全公司或者数据分析公司（例如 Bitrace）帮你找到被盗、被骗的原因，以及后续资金去向，甚至在案件侦查过程中提供一些帮助。

但不要到处找网友求助，一方面是绝大多数网友的言论都是噪音，对资产找回无益，另一方面目前有许多骗子也会冒充虚拟资产找回专家、某某平台官方客服等身份。

最后

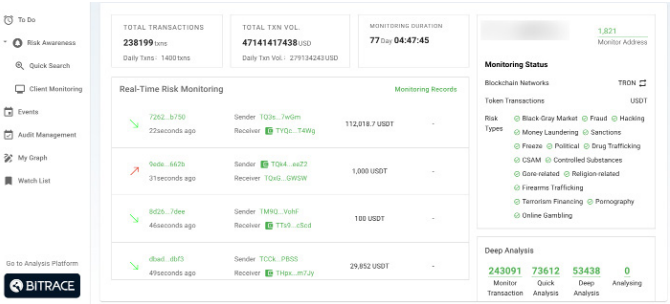
在这本手册中，我们首先按照普通新手的投资生命周期，分阶段介绍了不同时期可能会遇到的欺诈手法，接着对不同类别欺诈背后的原理与防范手段进行了解读，最后罗列了发现被欺诈后挽回损失的方法，旨在将常见的以及损害巨大的骗术进行揭露，防止更多普通投资者遭受损失。

如果你或你身边的朋友不幸遭到 Crypto Scam，也欢迎联系 Bitrace，我们将为受害人提供基本的分析帮助。

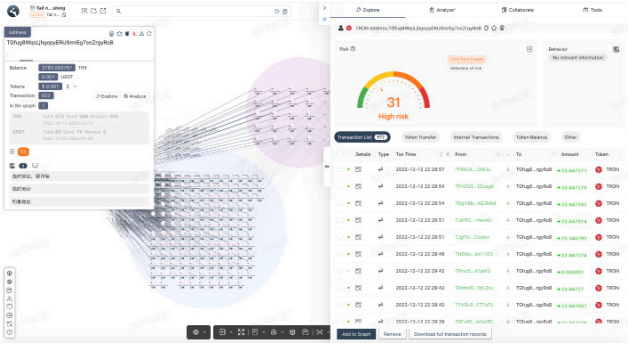
对于有加密资金风险检测需求的用户，也欢迎使用我们的产品，来更好地实现风险识别和预防。

对于个人，您可以访问 https://detrust.bitrace.io/detrust-blacklist/ 使用由 Bitrace 团队推出的免费 KYA 小工具，一键查询对手方地址是否具备任何风险，并基于地址风险评分决定是否要与对方产生资金交互。

对于存在较高交易频率的机构（例如交易所、支付平台、OTC 商等），则可以使用企业版 Detrust 链上风险资金监测管理平台，对平台业务地址的全部交易完成监控覆盖。当风险交易——包括风险资金流入与资金流出至风险地址发生时，风控人员将通过邮件、社群机器人等渠道收取实时提醒，以及时处理已经发生或即将发生的用户风险活动。



对于有加密资金追踪分析需求的团队或执法机构，Bitrace Pro 可以为您提供可视化分析、实体识别、地址聚类、多方协作、智能监控警报等强大的功能，帮助您快速了解犯罪模式、追踪资金流动、识别异常并发现新线索，帮助更快、更精准地开展调查。



您可以随时联系我们，获取产品 Demo。

关于 Bitrace

Bitrace 是一家以加密货币风险数据分析为核心的监管科技（Regtech）企业，我们致力于运用 AI 与大数据技术更准确高效地识别、监测链上的风险和犯罪活动，为客户提供领先的监管、合规、调查工具产品与服务支持。

我们聚焦于加密犯罪调查领域，目前已与多国执法机构、Web3 企业进行协作与对接，完成数千起案例服务支持，累计监测数千亿风险资金，并成功挽回数十亿美元的损失。

网站：bitrace.io
邮箱：support@bitrace.io
X（推特）：@Bitrace_team
LinkedIn：@Bitrace Tech

免责声明

本手册仅用于公众教育和提高意识的目的。它是一个非营利性项目，旨在帮助个人更好地了解和防范加密货币欺诈。所提供的信息并不构成法律、财务或专业建议。尽管我们努力确保内容的准确性，作者和出版商对内容的完整性或可靠性不作任何保证。Bitrace 及其关联方对因使用本手册而导致的任何损失或损害概不负责。建议读者根据具体情况寻求专业建议。如有任何问题，欢迎随时联系我们。