Bitget 反欺诈月研究报告（2025）摘要

加密货币欺诈已迈入 AI 深度伪造、社会工程学与虚假项目包装驱动的新纪元。本报告由 Bitget、慢雾（SlowMist）与 Elliptic 联合撰写，剖析2024至2025年初常见欺诈手法，并提出用户与平台联防对策。

当前三大高危欺诈类型：

1.深度伪造冒充——利用合成视频推广虚假投资；

2.社会工程学欺诈——涵盖求职木马、钓鱼机器人及虚假质押方案；

3.现代庞氏骗局——伪装成 DeFi、NFT 或 GameFi 项目。

现代欺诈正从技术漏洞转向信任与心理漏洞的双重攻击。从钱包劫持到数百万美元级欺诈，攻击呈现高度个性化、高度欺骗性与隐蔽化趋势。

Bitget 为此推出“反欺诈”行动页（Anti-Scam Hub），升级平台防护体系，并联合慢雾与 Elliptic 实现链上赃款追踪、钓鱼网络瓦解及跨链欺诈行为标记。

报告内含真实案例解析、欺诈红标清单及用户及机构防护指南。
核心结论：当 AI 可完美复刻任何人时，安全防线必须以质疑为起点，以集体防御为终点。

目录

1. 核心摘要
   AI 辅助加密欺诈威胁升级现状，及 Bitget、慢雾与 Elliptic 联合反制机制。

2. 引言：威胁演进态势
   DeFi 发展、AI 普及与跨境便利性如何催生新型欺诈温床，以及其中蕴含的风险。

3. 现代加密欺诈解剖
   当下最危险欺诈解析：
      3.1 深度伪造冒充
      3.2 社会工程学策略
         - AI 套利机器人
         - 木马求职陷阱
         - 社交媒体钓鱼
         - 地址投毒攻击
         - 貔貅盘代币骗局
         - 虚假质押返利平台
         - 空投陷阱
      3.3 Web3 时代的庞氏骗局

4. 加固数字防线：**Bitget** 多层安全架构
   Bitget 实时威胁检测、代币尽调、双审计机制及3亿美元保护基金详解。

5. 链上欺诈追踪与资金取证（**Elliptic** 撰文）
   交易监控、跨链桥追踪与行为分析如何识别并阻断赃款流动。

6. 防护建议与最佳实践（慢雾撰文）
   用户与企业实操指南：从钓鱼识别到防诈习惯养成及企业级响应框架。

7. 结论：未来路径规划
   加密安全如何从孤立防御转向网络免疫，以及 Bitget 如何在不断升级的威胁中领先一步。

洞察前沿：揭秘加密领域欺诈新趋势

1. 核心摘要

2025年1月，香港警方捣毁深度伪造诈骗集团并逮捕31人，该团伙通过冒充加密货币高管窃取3400万美元——这只是第一季度在亚洲破获的87起同类案件之一（慢雾，《2025加密犯罪报告》）。而这些，都是无可辩争的事实。从新加坡总理 AI 合成视频到马斯克"虚假代言"，深度伪造信任攻击已成为日常威胁。

由三方共同完成的本报告揭示加密欺诈如何从粗糙钓鱼诈骗进化为 AI 增强的心理操控：2024年近40%的高额诈骗案涉及深度伪造技术。无论是木马求职陷阱还是庞氏"质押平台"，背后都是社会工程学对信任、恐惧与贪婪的精准利用。

加密欺诈不只是骗取钱财——它正在侵蚀行业信任根基。

Bitget 安全系统每日拦截大量信任滥用行为：登录异常、钓鱼攻击、恶意软件下载。为此我们推出反欺诈中心，开发主动防护工具，并联合慢雾、Elliptic 等全球性领头平台瓦解诈骗网络及追踪赃款。

本报告绘制威胁演变图谱，揭示当前高危手法，并为用户及机构提供实用防御策略。当 AI 可以复刻任何人的面容时，安全机制必须从根本上具备质疑精神。

2. 引言：威胁演进态势

加密货币的无国界特性既是最大的优势，也是最大的风险。随着去中心化协议锁定总价值超过980亿美元，机构参与度也不断提升，推动创新的同一技术也在助长新一波加密货币欺诈的出现。

这已非过往出现的初级钓鱼攻击。2023-2025年欺诈规模与精密性剧增：2024年全球用户因欺诈损失超**46**亿美元，同比增长**24%**（Chainalysis，《2025年加密犯罪报告》）。从深度伪造冒充到伪装成"质押收益"的庞氏生态，诈骗分子正利用 AI、心理操控及社交平台欺骗资深用户。

三大主流攻击手法：

- 深度伪造，伪造成公众人物代言虚假平台。
- 社会工程学骗局，包括木马求职测试及钓鱼推文等。
- 庞氏骗局变体，如经 DeFi/GameFi/NFT 包装后的骗局。

最令人警觉的是心理操控升级：受害者非单纯受骗而是被逐步说服。诈骗者不仅会窃取密码，更会针对行为盲点设计陷阱。

当然，防御体系也在同步进化：生态内协同创新正在加速推进。

Bitget 行为分析系统实时标记可疑模式；Elliptic 跨链取证追踪多链资产；慢雾威胁情报助力铲除亚洲钓鱼团伙。

本报告融合实战案例、实地调研及三方运营数据，剖析当前资产损失的主因，并为用户、监管方及平台提供反制策略。

诈骗手法持续进化，但防御机制也在同步升级。本报告详细阐述了具体方案。

3. 现代加密欺诈解剖：2024 - 2025 十大骗局

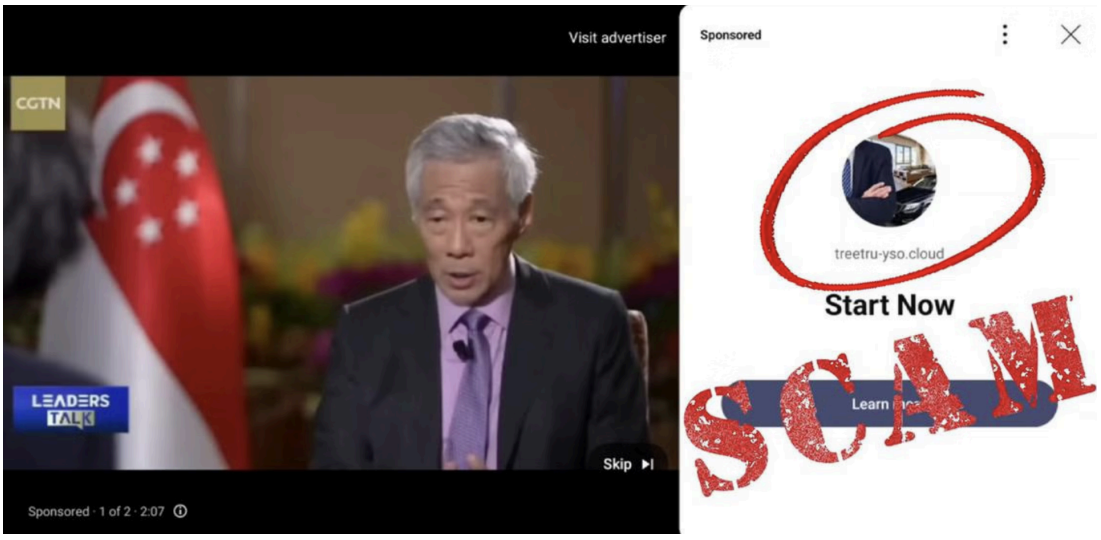
随着区块链技术普及与加密资产越发增值，诈骗越来越复杂、隐蔽且精密，呈现“高技术伪装+心理操控+链上诱导”新特征。过去两年诈骗者融合 AI、社会工程学与传统欺诈模型，构建更具欺骗性及破坏性的诈骗生态。其中，深度伪造、社会工程学与庞氏变体最为猖獗。

3.1深度伪造：信任体系的崩塌

2024-2025年生成式 AI 催生新型信任诈骗：一种利用深度伪造技术进行基于信任的诈骗。攻击者使用 AI 合成工具伪造知名项目创始人、交易所高管或社区 KOL 的音视频误导用户。伪造素材往往可以以假乱真——模仿目标面部表情与声线，甚至生成含“官方标识”背景的视频，令普通用户难辨真伪。典型场景：

（1）名人深度伪造推广投资

诈骗者利用深度伪造技术轻松“邀请名人站台”。案例：新加坡总理李显龙与副总理黄循财也被制作了深度伪造视频，用来推广“政府背书加密平台”。



https://www.zaobao.com.sg/realtime/singapore/story20231229-1458809

特斯拉 CEO 马斯克频现虚假投资奖励骗局。

https://www.rmit.edu.au/news/factlab-meta/elon-musk-used-in-fake-ai-videos-to-promote-financial-scam

此类视频通过 X/Facebook/Telegram 等社媒平台广泛传播，诈骗者常关闭评论功能营造“官方权威”假象，诱使用户点击恶意链接或投资特定代币。这种攻击方式利用了用户对“权威人士”或“官方渠道”的固有信任，具有很强的欺骗性。

(2)绕过身份认证

诈骗者利用 AI 伪造动态人脸视频(可响应语音指令)，结合受害者照片突破交易所/钱包平台身份认证系统，劫持账户窃取资产。

(3)虚拟身份投资诈骗

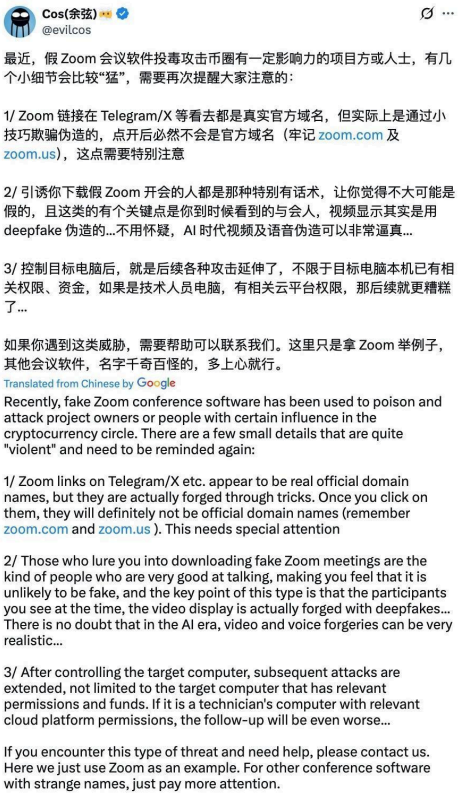
2024-2025年香港及新加坡警方连续捣毁多个深度伪造诈骗集团。例如，2025年初，香港警方在一起涉案金额高达3400万港元的案件中逮捕了31名嫌疑人，受害者遍布新加坡、日本、马来西亚和其他亚洲国家和地区。犯罪组织特征：

- 招募传媒专业毕业生构建丰富的虚拟身份与背景；
- 在 Telegram 上创建大量钓鱼群，以“高学历、温柔、友好人设”接触目标；
- 通过“交友→引导投资→提现障碍”话术诱导用户在虚假平台投资；
- 伪造聊天记录/客服对话/收益截图营造真实感，可信任的假象；
- 以“激活算力”和“提现审核”等名目为由诱导持续充值(庞氏架构)。

https://user.guancha.cn/main/content?id=1367957

(4)深度伪造 +Zoom 钓鱼

诈骗者冒充 Zoom 发送伪造会议邀请链接，诱骗用户下载含木马的"会议软件"。会议中"参会者"使用深度伪造视频冒充高管或技术专家，操控受害者进一步点击，进行授权或转账。设备被控制后，诈骗者就会开始远程控制设备，窃取云数据或私钥。



Cos(余弦)
@evilcos

最近，假 Zoom 会议软件投毒攻击币圈有一定影响力的项目方或人士，有几个小细节会比较"猛"，需要再次提醒大家注意的：

1/ Zoom 链接在 Telegram/X 等看去都是真实官方域名，但实际上是通过小技巧欺骗伪造的，点开后必然不会是官方域名（牢记 zoom.com 及 zoom.us），这点需要特别注意

2/ 引诱你下载假 Zoom 开会的人都是那种特别有话术，让你觉得不大可能是假的，且这类的有个关键点是你到时候看到的与会人，视频显示其实是用 deepfake 伪造的...不用怀疑，AI 时代视频及语音伪造可以非常逼真...

3/ 控制目标电脑后，就是后续各种攻击延伸了，不限于目标电脑本机已有相关权限、资金，如果是技术人员电脑，有相关云平台权限，那后续就更糟糕了...

如果你遇到这类威胁，需要帮助可以联系我们。这里只是拿 Zoom 举例子，其他会议软件，名字千奇百怪的，多上心就行。

Translated from Chinese by Google

Recently, fake Zoom conference software has been used to poison and attack project owners or people with certain influence in the cryptocurrency circle. There are a few small details that are quite "violent" and need to be reminded again:

1/ Zoom links on Telegram/X etc. appear to be real official domain names, but they are actually forged through tricks. Once you click on them, they will definitely not be official domain names (remember zoom.com and zoom.us). This needs special attention

2/ Those who lure you into downloading fake Zoom meetings are the kind of people who are very good at talking, making you feel that it is unlikely to be fake, and the key point of this type is that the participants you see at the time, the video display is actually forged with deepfakes... There is no doubt that in the AI era, video and voice forgeries can be very realistic...

3/ After controlling the target computer, subsequent attacks are extended, not limited to the target computer that has relevant permissions and funds. If it is a technician's computer with relevant cloud platform permissions, the follow-up will be even worse...

If you encounter this type of threat and need help, please contact us. Here we just use Zoom as an example. For other conference software with strange names, just pay more attention.

https://x.com/evilcos/status/1920008072568963213

从技术层面上讲，诈骗者采用 Synthesia、ElevenLabs、HeyGen 等 AI 合成工具在分钟级的单位里生成高清音视频，并通过 X/Telegram/YouTube Shorts 等平台扩散。

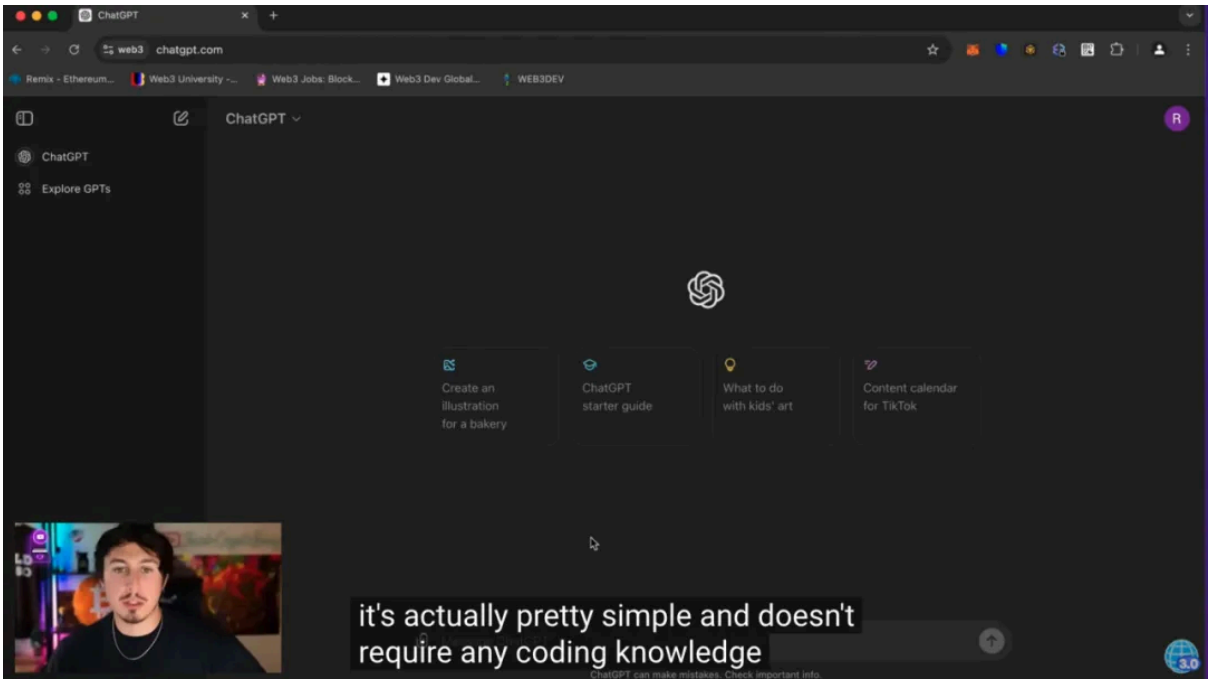
深度伪造技术已成为 AI 驱动诈骗的核心组件。视觉与听觉内容的可信度在 AI 时代急剧下降。用户必须通过多通道验证资产操作类"权威信息"，避免盲目相信"熟悉的面孔或声音"。同时，项目团队应认识到 AI 伪造所带来的品牌风险，建立唯一可信的信息传播渠道，或采用链上签名广播进行身份认证，从而从机制上抵御伪造攻击。

3.2社会工程学策略：利用心理漏洞

与高科技手段相辅相成的，是那些低技术但极高效的社会工程学攻击。人性是最薄弱也是最容易被忽视的环节，导致许多用户低估了社会工程学带来的威胁。骗子往往通过伪装、引导、恐吓等手段操纵用户行为，利用用户的心理弱点逐步达到诈骗目的。

（1）AI 套利机器人骗局

AI 已成为提高生产力的一项标志性技术，诈骗者迅速抓住了这一趋势，用"ChatGPT 生成"（听起来尖端又可信的流行语）标签包装骗局，降低用户戒心。



骗局通常以详细的视频教程开始。在视频中，骗子声称套利机器人的代码通过 ChatGPT 生成，它可以部署在以太坊等区块链上，监控新代币的发布和价格波动，通过闪电借贷或价格差异进行套利。他们强调"机器人会自动为您完成所有逻辑运行，您只需等待利润生成即可"。这种说法与许多用户"人工智能=轻松赚钱"的先入为主的观念非常吻合，进一步降低了他们的警惕性。

诈骗者通过降低用户技术门槛的包装语言，引导用户访问高度仿真的 Remix IDE 界面（实际上是一个假页面）。单从界面上看，真假难辨。用户被要求粘贴所谓的“由 ChatGPT 编写的合约代码”。部署完成后，用户被告知需向合约地址注入启动资金作为初始套利本金，而诈骗者则暗示“投资越多，回报越高”。用户完成这些步骤并点击“开始”按钮后，等待他们的不是源源不断的套利利润，而是再也找不回资金。因为用户复制和粘贴的代码中已经包含了诈骗逻辑：合约激活后，充值的 ETH 就会立即转移到骗子预设的钱包地址中。换句话说，整个“套利系统”本质上就是一个包装精美的敛财工具。

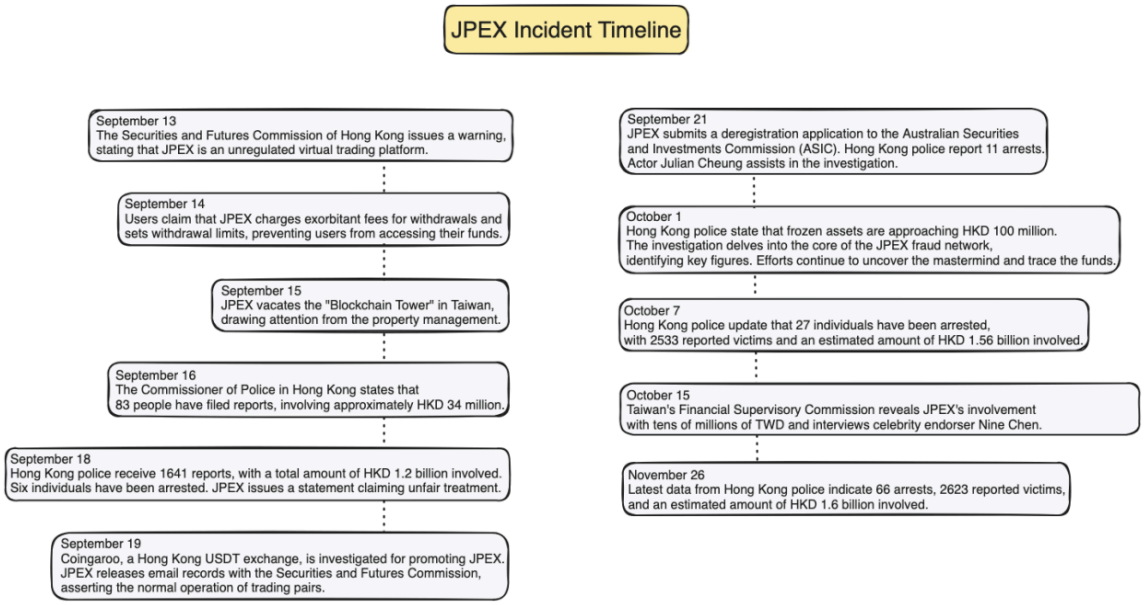
慢雾分析表明，此类骗局采用“广撒网、小诱饵”策略，导致单个用户损失数十至数百美元。虽然单个用户被诈骗的金额相对较小，但诈骗者通过大规模传播教程，诱使众多用户上当，仍能获得稳定可观的非法利润。由于每个受害者损失金额不大，且操作看似“自主完成”，而不是直接的欺诈性转账，大多数受害者都选择沉默，不再进一步调查。更令人担忧的是，这些骗局很容易改头换面重新上线：只需要更改机器人名称或更换几个页面模板，骗子就能重新上线继续行骗。

其他社会工程学套路包括：木马求职陷阱、虚假面试编程任务、 推文/Telegram 私信钓鱼链接、相似地址投毒攻击、阻断卖出的“貔貅盘”代币、伪装质押平台的返利骗局。这些攻击通过信任（私聊接触）、贪婪（高收益承诺 ）或困惑（伪造界面和聊天记录 ），不断更换包装形式，通过隐蔽、让用户主动配合的方式导致用户资金损失。

3.3庞氏骗局：新瓶装旧酒

加密生态发展迅速，传统的庞氏骗局也如影随形，并未消失。它们利用链上工具、社交病毒式增长和人工智能驱动的深度伪造，进行了一场“数字进化”。这些骗局通常伪装成 DeFi/NFT/GameFi 项目进行募资、流动性挖矿或平台币质押。本质仍是“新钱补旧账”的庞氏结构，现金流断裂或操盘者卷钱跑路即崩盘。

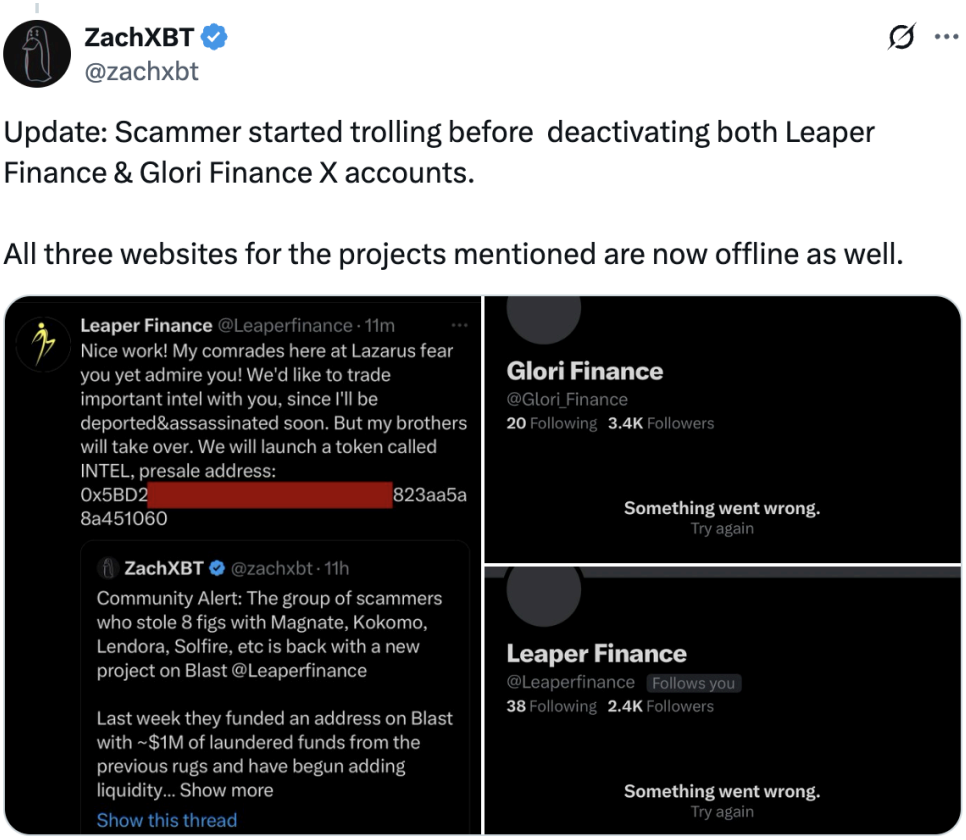
2023年震动香港的 JPEX 事件就是典型案例。该平台自称“全球交易所”，通过线下广告与明星代言推广平台币 JPC 并承诺“高额稳定收益”，在无监管批准及信息披露缺失下吸纳大量用户。2023年9月，香港证监会将平台标记为“高度可疑”，警方“铁关行动”逮捕多人。截至2023年底涉案16亿港元，2600余名受害人，或成香港史上最大金融诈骗案之一。



此外，链上庞氏项目的典型模式也在不断演变。2024年区块链分析师 ZachXBT 曝光诈骗团伙在 Blast 链部署 Leaper Finance 项目。该团伙曾运作 Magnate、Kokomo、Solfire 以及 Lendora 等项目窃取数千万美元，他们伪造身份认证文件与审计报告，预洗资金并人为刷高链上数据引诱用户投资，TVL 达数百万美元后迅速抽逃流动性，卷钱跑路。

更令人震惊的是，该团伙多次瞄准多个主流链，包括 Base、Solana、Scroll、Optimism、Avalanche 和以太坊，采用快速"换皮和重塑品牌"的轮换诈骗方式。

例如，他们部署在 Base 链上的 Zebra 借贷项目的 TVL 曾一度达到31万美元以上；在 Arbitrum 上，他们的 Glori Finance 项目的 TVL 曾达到140万美元的峰值。这两个项目都是 Compound V2 的分叉。这些项目利用从 Crolend、HashDAO 和 HellHoundFi 等其他骗局中提取的资金作为种子资金，形成了一个诈骗闭环。



与传统的庞氏骗局相比，数字骗局具有以下新特点：

- 更隐蔽的技术伪装：借开源合约/NFT 包装/链上数据积累营造“技术创新”假象，误导用户相信这些都是合法合规的 DeFi 产品。
- 返利结构复杂化：以“流动性挖矿”、“质押奖励”、“节点分红”掩盖资金流，实际多层抽取资金与内外盘操控。
- 社交裂变传播：依赖微信群/Telegram 频道/KOL 直播驱动用户拉新，形成典型的传销式传播模式。
- 游戏化界面与身份伪造：许多项目采用游戏 UI 与 NFT 项目 IP 塑造“年轻化”及“合法”形象。有些项目甚至结合 AI 换脸和深度伪造技术，伪造项目创始人或代言人的图像或视频，从而提高可信度。

例如，2025年2月黑客劫持坦桑尼亚富豪 Mohammed Dewji 的 X 账号，用深度伪造视频推广虚假代币 $Tanzania，数小时内募资148万美元。类似的造假技术已被广泛用于伪造创始人视频、编造会议截图和伪造团队照片，使受害者越来越难以辨别真伪。

以下诈骗红标对照表总结了核心预警标志和简单防范措施，供用户参考。

诈骗类型	危险信号	防护措施
深度伪造冒充	CEO/官员/KOL“官方”视频推广投资	通过官网/公告渠道二次验证

AI 套利机器人骗局	YouTube 教程声称使用 ChatGPT 生成的代码创建"自动盈利"机器人	请勿部署未知代码或盲目投入资金
木马求职陷阱	附带紧急测试链接或克隆编码任务的领英消息	沙盒环境运行代码，直联公司确认
钓鱼评论（X 平台）	推文回复含虚假空投链接或质押页面	请勿点击社交评论链接，确保验证来源
地址投毒攻击	来自相似钱包地址的小额转账	请使用地址簿，逐笔交易二次确认
貔貅盘代币	新币暴涨但无法卖出	请在买入前查验合约功能，切勿相信高额稳定收益
虚假质押/矿工返利	Telegram"双倍返利"话术、虚假页面或数据、伪造用户聊天	请规避无链上逻辑的充值返利项目
空投陷阱	钱包出现免费代币，引导用户访问钓鱼链接或恶意合约	请勿与来源不明的代币或要求授权的网站进行互动

如何保障安全：对可疑或来源不明的内容保持警惕——无论是通过领英、Telegram 还是电子邮件；请勿运行陌生代码或安装不明文件（尤其是在以工作测试或应用演示为借口的情况下）；收藏官方网址；使用 Scam Sniffer 等浏览器插件；请勿连接钱包至未知链接。加密世界的信任需主动验证而非被动给予。

4. 加固数字防线：Bitget 多层安全架构

面对日益复杂的数字资产威胁，Bitget 构建了一个全面安全框架，旨在保护每个平台用户。本节介绍了在账户保护、投资审查和资产保护方面实施的战略措施。

1. 账户保护：实时阻断未授权访问

Bitget 采用一整套实时监测工具来检测和提醒用户注意任何异常活动。从新设备登录时，用户会收到详细的电子邮件通知，其中包括防钓鱼码、验证码、登录位置、IP 地址和设备详情。这种即时反馈使用户能够及时发现和处理未经授权的访问。

为了减少可能由诈骗引起的冲动行为，Bitget 设立了动态冷静期。该机制由异常登录位置或可疑交易等指标触发，对提现实施1-24小时的临时停用，以便用户重新评估和确认账户活动是否正常。

此外，Bitget 提供官方验证通道，使用户能够验证通信内容并有效防范钓鱼攻击。

2. 投资审查：数字资产严格评估

Bitget 认识到加密市场中高风险代币的激增，因此为资产上架制定了详尽的尽职调查流程，其中包括对项目团队进行全面背景调查、深入分析代币经济学、评估估值和分配模式，以及评估社区参与程度。

为进一步确保评估准确，Bitget 实施了双层安全审计系统。内部区块链安全工程师会进行彻底的代码审查，以找出漏洞。同时，第三方权威机构会进行复审，确保审查到位。
资产上线后，Bitget 的专有链上监测系统将持续实时监控交易和合约互动情况。该系统旨在适应新的安全威胁，不断演变并更新其威胁模型，以迅速应对新出现的风险。

3. 资产保护：全面保护用户持有资产

Bitget 采用双钱包策略，同时采用热钱包和冷钱包来提高安全性。大多数数字资产都存储在离线、多签名的冷钱包中，大大降低了遭受网络攻击的风险。
此外，Bitget 还设有价值超过3亿美元的巨额保护基金，用于在发生与平台相关的安全事件时向用户进行赔付。

对于 Bitget Wallet 用户，平台额外采用了部分安全功能，包括钓鱼网站警报、内置合约风险检测工具和创新的 GetShield 安全引擎。GetShield 可持续扫描去中心化应用、智能合约和网站，在用户交互之前检测出潜在威胁。

通过这种多重安全架构，Bitget 不仅保护了用户的资产安全，还增强了用户对其平台的信任，为加密货币交易所行业的安全标准树立了标杆。

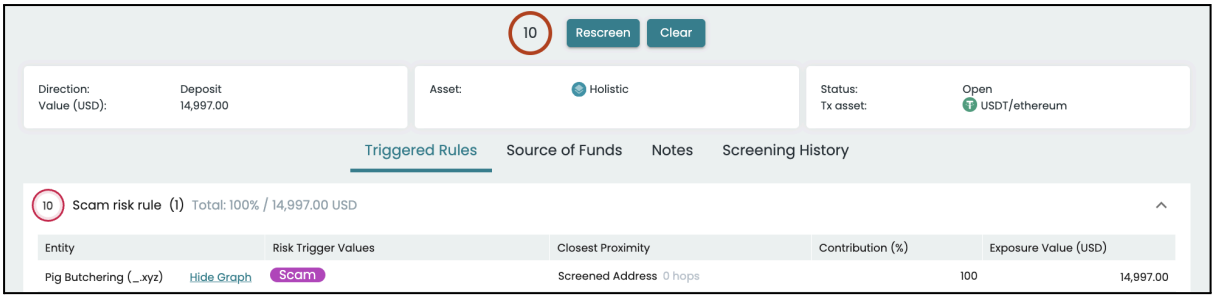
5.链上诈骗资金追踪与标记

本报告前几节介绍了诈骗者如何通过不同手段骗取加密货币，包括使用深度伪造技术。诈骗者通常会尝试转移赃款并最终兑换为法币。这些资金流动可被追踪——区块链分析工具在此过程中至关重要。此类工具主要分为三类：交易监测、地址筛查及调查工具。本节重点解析交易监测工具如何检测并标记诈骗相关资金，增加赃款利用难度。

交易监测工具已被 Bitget 等加密货币交易所广泛采用。该工具通过扫描进出交易识别并标记潜在风险。典型应用场景包括检查所有用户充值，以识别潜在风险。多数正常用户充值不会被标记为高风险，资金自动处理并及时入账用户账户；但若充值资金源自已知诈骗地址，资金将被标记为高风险。

我们可以看看交易监测的实际案例。下图显示的是交易监测工具对用户在加密货币交易所充值的分析。如图所示，某交易所用户充值被识别为“杀猪盘”投资诈骗关联地址转账。

工具给出10/10最高风险评分，触发人工审核流程——用户资金不会自动入账，该活动将移交合规团队手动核查。



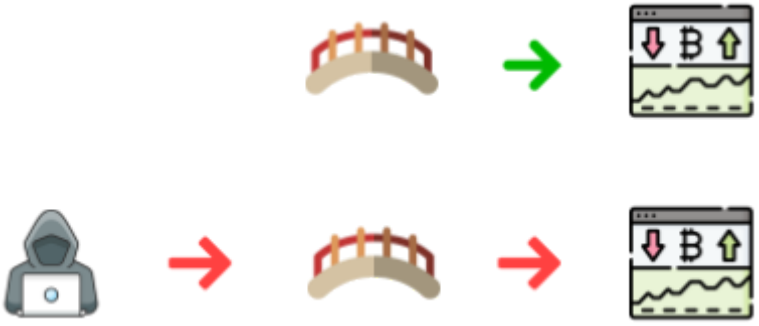
高级犯罪组织熟知交易监测机制，常采用特定链上操作混淆（即隐藏）资金路径。典型手法即"资金分层"：通过多级中间地址转移赃款，试图切割其与源头的联系。先进交易监测工具可穿透无限层级中间地址，精准定位资金犯罪源头。犯罪组织亦日益频繁使用跨链桥，下小节将重点解析。

5.1跨链桥

过去几年里，市场上已经推出了各种区块链。用户可能由于某个区块链承载着特定的加密货币或去中心化应用或其他服务而被吸引。跨链桥使用户能近乎实时地将价值跨链转移。虽然普通区块链用户是跨链桥主要使用者，但诈骗者正日益利用其在区块链间转移赃款。诈骗者使用跨链桥通常有以下动因：

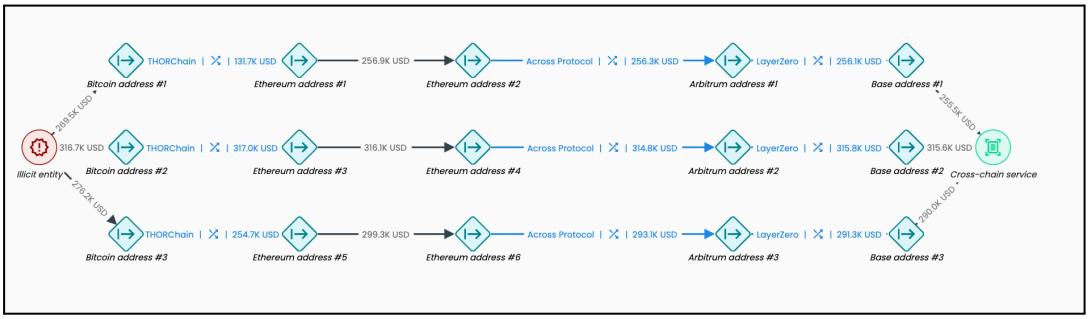
- 获取混淆机会：特定混淆工具仅支持特定区块链（如多数混币器网站仅处理比特币 ）。犯罪组织常跨链至目标区块链使用混淆服务后再次转移至其它区块链。
- 增加追踪难度：跨链转移显著提升资金追踪复杂度。即便调查员能手动追踪单次跨链行为，重复跨链操作将极大延缓调查进度，而且如果资金被拆分，调查员手动追踪所有线索的可行性也会降低（下文案例显示，专用工具可实现跨链资金无缝追踪）。

犯罪组织深知部分自动化交易监测工具在跨链桥处会终止追踪。下图上半部分展示此类工具在识别非法活动时止步于跨链桥，导致交易所仅可见来自桥接地址的资金，无法追溯前序路径。下图下半部分为 Bitget 采用的 Elliptic 交易监测工具，其自动穿透跨链桥完整还原资金路径，暴露出相关非法实体。



下方案例研究描述了非法实体如何利用一系列跨链桥和区块链，大规模、有计划地试图对加密货币进行洗钱，以及如何从某些工具中识别该活动。

案例研究：下图Elliptic 调查工具截图显示某犯罪组织如何利用跨链桥在多个区块链上转移资金，然后最终将资金存入加密货币服务平台。



资金从比特币链发起（左侧），跨链至以太坊，以太坊切换地址进行内部转移，跨链至Arbitrum，再跨链至Base 链，最终存入加密货币服务平台。图片还突出显示了另外两个具有相同模式的实例。虽然没有完整显示，但同样的套路还出现了十余次，反映出洗钱行为的系统性。

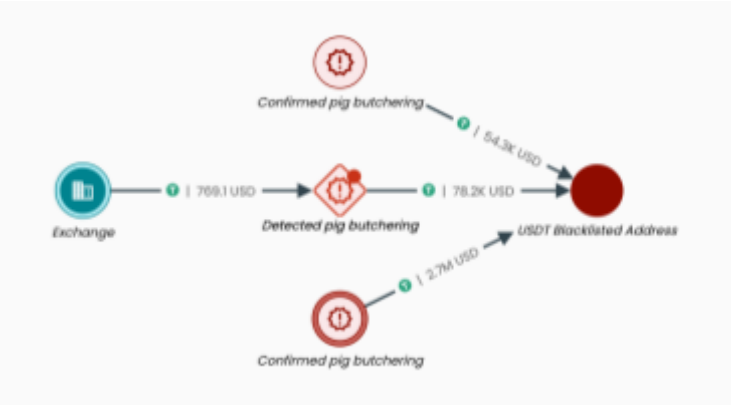
此行为目的有二：延缓调查员追踪速度或进行干扰；阻止接收方交易所识别资金非法源头。然而，支持自动跨链桥追踪的区块链调查工具可无缝还原完整路径。具备跨链追踪能力的交易监测工具（如Bitget 采用的Elliptic 系统）能自动识别资金与犯罪组织的原始关联。

5.2 如何利用行为和模式侦查诈骗资金

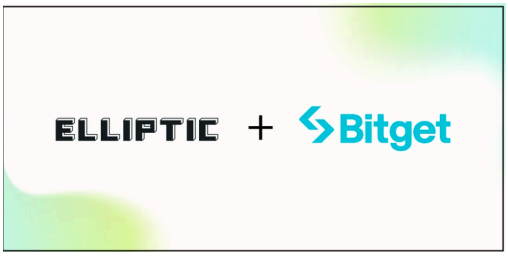
前文案例依赖已知非法加密货币地址标签（如杀猪盘地址），这些地址标签通常来自受害者报案、执法协作等多渠道数据采集。但诈骗规模膨胀（加之受害报案率低等因素）导致无法覆盖所有地址。

因此部分先进交易监测工具引入行为检测作为补充防线。通过自动分析行为和模式，系统可推断某特定地址是否进行符合诈骗特征的链上操作，并对相关交互进行风险标记。此类行为分析通常由专业行为检测模型执行（部分采用机器学习技术）。截至目前，Elliptic 行为检测可识别15余种诈骗类型（含杀猪盘、地址投毒、冰钓攻击等），且检测能力持续扩展。

下方示例展示行为检测如何阻止用户向诈骗地址转账：该示例中存在三个杀猪盘相关地址。顶部与底部地址经受害者报案识别并确认。处于中间的那个地址虽未被举报，但行为检测模型将其标记为潜在杀猪盘关联地址。



该地址随后收到了某交易所的转账。若该交易所启用行为检测警报，转账前即可识别风险从而避免用户资金损失。最终这三个杀猪盘地址资金均流向同一地址，该地址后被 Tether 官方冻结，列入黑名单。该地址持有的 USDT 均被冻结，进一步证实了所涉资金的非法性质。



点击此处了解Bitget 接入Elliptic 区块链分析工具后如何将风险拦截率提升99%——该行业领先工具支持超过50条区块链，具备自动化跨链桥追踪与行为检测能力。

6. 防护建议与最佳实践

面对持续升级的诈骗技术，用户需建立清晰的自我保护意识与技术鉴别能力。为此，慢雾提出以下核心反诈建议：

(1)提升社交媒体内容鉴伪能力
切勿点击评论区或群聊中的任何链接——即便看似"官方"。进行钱包绑定、领取空投、质押操作等关键行为时，务必通过项目官网或可信社区渠道验证。建议安装 Scam Sniffer 等安全插件实时检测并拦截钓鱼链接，降低误触风险。

(2)警惕 AI 工具引入的新型风险
随着大语言模型技术(LLM)迅猛发展，各类新型 AI 工具涌现。模型上下文协议(MCP)标准已成为连接 LLM 与外部工具/数据源的关键桥梁。但 MCP 普及也带来新安全挑战。慢雾已发布系列 MCP 安全研究文章，建议相关项目团队提前自查并加固防御。

(3)善用链上工具识别风险地址与庞氏特征
对疑似跑路或欺诈的代币项目，建议使用 MistTrack 等反洗钱追踪工具查验项目关联地址风险，或通过 GoPlus 代币安全检测工具快速评估。结合 Etherscan/BscScan 等平台查看受害者评论区预警。对高收益项目保持高度警惕——异常高回报往往伴随极高风险。

(4)切勿盲信"规模效应"与"成功案例"
诈骗者常通过大型 Telegram 群组、虚假 KOL 背书、伪造盈利截图营造暴利氛围。一般来说，项目可信度应通过 GitHub 代码库、链上合约审计、官网公告等透明渠道进行验证。用户需培养独立验证信息源的能力。

(5)防范社交信任型"文件诱导"攻击
越来越多的攻击者利用 Telegram、Discord 和领英等平台发送伪装成工作机会或技术测试邀请的恶意脚本，诱使用户操作高风险文件。

用户防护指南：

- 警惕要求从 GitHub 等平台下载/运行代码的可疑工作或自由职业邀约。请务必通过公司官网或邮箱核实发件人身份，请勿轻信"限时高回报任务"话术。
- 处理外部代码时严格审查项目源及作者背景，拒绝运行未经验证的高风险项目。建议在虚拟机或沙盒环境中执行可疑代码以隔离风险。
- 谨慎处理 Telegram/Discord 等平台接收的文件：关闭自动下载功能，手动扫描文件，警惕"技术测试"名义的脚本运行要求。
- 启用多重认证并定期更换高强度密码，避免跨平台密码复用。
- 请勿点击来源不明的会议邀请或软件下载链接，养成核验域名真实性和确认官方平台来源的习惯。
- 使用硬件钱包或冷钱包管理大额资产，减少联网设备敏感信息暴露。
- 定期更新操作系统与杀毒软件，防范新型恶意程序和病毒。

如果怀疑设备被感染，立即断网，转移资金至安全钱包，清除恶意程序，必要时重装系统以最小化损失。

企业防护指南：

- 定期组织钓鱼攻防演练，培训员工识别伪造域名与可疑请求。
- 部署邮件安全网关拦截恶意附件，持续监控代码仓库防范敏感信息泄露。
- 建立融合技术防御与员工意识的钓鱼事件响应机制。这种多层次战略有助于最大限度地降低数据泄露和资产损失的风险。

(6)牢记投资判断的"基本原则"

- 高收益承诺=高风险：任何宣称"稳定高回报"或"保本盈利"的平台均应视为高风险平台。
- 基于拉人头进行病毒式增长即典型红标：设置招募返利机制或"团队收益"分层结构的项目可初步判定为传销。
- 使用链上分析工具识别异常资金流：MistTrack 等平台可追踪大额异常资金动向，分析团队套现路径。
- 核验审计机构与团队透明度：警惕部分项目提供的"虚假审计报告"或小型审计机构形式化背书，用户应确认智能合约是否经可信第三方审计且报告公开。

总之，AI 时代的加密诈骗已从单纯“技术漏洞利用”升级为“技术+心理”双维操控。用户既要提高技术识别能力，也要加强心理防御：

- 多验证，少冲动：请勿因“熟人、权威视频、官方背景”降低戒心。
- 多质疑，少转账：涉及资产操作务必深究底层逻辑，核实来源，确认安全。
- 戒贪婪，常存疑：项目“保本盈利”承诺越诱人，越需提高警惕。

建议研读慢雾创始人 Cos 所著《区块链黑暗森林自救手册》，掌握链上反诈基础技能，增强自我防护。如遇盗窃，用户可寻求慢雾团队的协助。

唯有透彻理解诈骗机制、提升信息甄别力、强化安全工具认知、规范操作习惯，方能在充满诱惑和风险的数字时代风险浪潮中守护资产安全。安全防护无法一劳永逸，需要持续提起注意。构建完整认知体系与基本防御习惯，是在数字时代稳步前行、避开诈骗陷阱的唯一航标。

7.结论：未来路径规划

五年前防诈意味着“勿点可疑链接”，如今则是“所见不为实”。
当 AI 伪造视频、虚假招聘流程与代币化庞氏骗局重新将信任变成伤害用户的手段，加密安全的下一阶段不仅依赖智能技术，更需集体防御。Bitget、慢雾与 Elliptic 正通过共享威胁情报、自动化资金追踪、跨生态风险标记构建联防网络。
结论已然明晰：安全无法依赖孤立措施，必须构建网络化、持续化、用户中心化的体系。
为此 Bitget 将全力推进三大方向：

- **AI** 红队攻防演练：模拟新型诈骗手法测试系统漏洞。
- 合规数据协同网络：携手监管机构与合规伙伴共建情报共享生态。
- 推进安全教育：通过反欺诈中心赋能用户实时威胁感知能力。

诈骗者持续进化，我们也需升级迭代。在这个行业，最珍贵的货币从来不是比特币，而是信任。