

虚拟货币犯罪无法追踪？想多了！

在数字化浪潮的推动下，虚拟货币依托区块链技术诞生，逐渐成为在网络空间流通的数字化代币。一些人因其“去中心化”“点对点传输”的技术特性，产生了一种危险的错觉：只要不使用银行卡，改用虚拟货币接收境外资金，就能切断与个人身份的关联，实现真正的“匿名交易”，借助其“无法溯源”的特点逃脱法律制裁。但事实上，虚拟货币并非法外之地，其所谓的“匿名性”不过是表象，其带来的风险不容忽视。

衍生隐患莫轻视

虚拟货币因其流转隐蔽、监管难度大等特性，已成为不法分子从事各类违法犯罪活动的重要工具，滋生多个方面的安全风险。

——洗钱犯罪的“温床”。电信诈骗、网络赌博、跨境走私等违法所得，通常借助虚拟货币进行拆分和转移，进而规避金融监管，完成赃款“洗白”与跨境流动，严重扰乱国家外汇管理秩序，危害国家经济安全和金融安全。

——网络攻击的“掩体”。网络黑客、非法攻击者普遍借助虚拟货币实施犯罪活动。他们发动勒索病毒攻击、网络入侵等非法活动后，往往只接受虚拟货币缴纳赎金，借助其交易隐蔽的特点隐藏身份、躲避追查。

——间谍窃密的“帮凶”。境外间谍情报机关鼓吹虚拟货币流转隐蔽、难以核查等特性，以此打消被拉拢策反人员的顾虑，并通过虚拟货币输送间谍经费，对我国国家秘密安全构成严重威胁。

匿名交易是假象

不法分子大肆炒作虚拟货币“匿名交易”“不可追踪”，以此作为推广噱头，但从技术原理来看，区块链本身具备公开透明、链上数据不可篡改等核心特点，虚拟货币的所谓“匿名属性”从根本上就是伪命题。同时，区块链完整留存交易记录等数据，为全链路溯源提供了依据。

——看账本：交易全程留痕迹。任何一笔虚拟货币交易，无论金额大小、无论发生在何时何地，都会被永久、公开地记录在虚拟货币的“公共账本”上。区块链技术的分布式记账特性，决定了交易信息一旦上链便无法删除、无法篡改。

虚拟货币体现出的地址匿名效果，仅实现了钱包地址与使用者真实身份的临时隔离，并非真正意义上的身份隐匿。

——查链路：真实身份难藏匿。虽然钱包地址是一串乱码，但虚拟货币与法定货币的兑换、虚拟货币之间的兑换均需经过交易平台和支付接口，进而留下设备编码、网络 IP 等痕迹。专业机构可以依托链上数据分析和大数据比对等技术手段，溯源钱包地址背后的实际使用人，还原资金流转全过程。

——论私钥：资产安全无兜底。在区块链体系中，私钥如果由个人保管，它就是支配虚拟货币的唯一凭证，不存在挂失、找回渠道。一旦私钥遗失、泄露、被窃取，持有人就会失去对虚拟货币的控制权。如果将私钥交由交易平台保管，虽可通过申诉找回账号密码，但需要承担平台倒闭和失联的风险。

擦亮双眼筑防线

虚拟货币不仅潜藏财产损失风险，还常被境外反华敌对势力、不法分子利用，从事破坏金融秩序、危害国家安全的各类违法犯罪活动。对此，我们务必认清本质、提高警惕、主动防范。

——认清非法金融属性。在我国，虚拟货币不具有与法定货币等同的法律地位，任何涉及虚拟货币的非法金融活动均不受法律保护。2026 年 2 月，中国人民银行等多部门发布通知重申：比特币、以太币、泰达币等虚拟货币不应且不能作为货币在市场上流通使用；虚拟货币相关业务活动属于非法金融活动，一律严格禁止，坚决依法取缔。

——警惕高薪兼职陷阱。对承诺高回报且操作灵活的兼职应保持高度警惕，特别是要求使用虚拟货币结算、前往敏感区域拍照搜集资料、提供内部文件数据等任务，极有可能是境外间谍情报机关的圈套。天下没有免费的午餐，远高于市场薪酬的兼职背后，往往是危害国家安全的违法犯罪深渊。

——发现线索及时举报。如遇到以虚拟货币为诱饵，诱导提供涉密敏感信息、协助转移可疑资金等情况，请及时通过 12339 国家安全机关举报受理电话、网络举报受理平台（www.12339.gov.cn）、国家安全部微信公众号或直接向当地国家安全机关进行举报。

（来源：国家安全部微信公众号，转引自：新华网，网址：<https://www.news.cn/20260928/71441d4e8ef3430f9447845b8b448cdb/c.html>。时间：2026 年 9 月 28 日。访问时间：2026 年 10 月 9 日 16:30。）