

## 利用虚拟币“跑分”为犯罪团伙洗钱 10人“洗钱”被判刑

与传统通过多级银行卡层层转账洗钱不同，为逃避打击，不法分子开始将目光瞄向虚拟币，将“黑钱”通过“买卖”形式兑换成虚拟币再卖出，一来二去，“黑钱”便洗成了“白钱”。2022年12月29日，由江苏省句容市人民法院提起公诉的一起利用虚拟币掩饰、隐瞒犯罪所得案获一审判决，张某、李某等10名被告人分别被判处有期徒刑四年至七个月不等刑罚，并处罚金九万元至一千元不等。

### 上游团伙花式诈骗套路多

2020年10月，在北京出差的张先生从酒店房间地上看到色情小卡片，于是产生找“小姐”的想法。后通过百度搜索、微信扫码方式加上客服微信，先以支付包夜费、路费、体检费、服装费、小姐安全保证金等名义转账，后客服以下单未成功为由让他办理会员卡，再次转账后客户还是称还是达不到办卡要求，感觉不对的张先生便要求退款，谁知退款程序仍要支付多笔费用，张先生几小时共计支付各种“费用”72.6万元。但等了两天仍未收到退款，受骗的张先生于是报警。

刷单挣钱、申请保险理赔、提供卖淫上门服务……你能想到的诈骗套路全都有。和张先生有类似经历的不在少数，本案中查实的被害人就多达19人，被骗资金共计227.5161万元。

### “黑钱”去哪了

因账户实名制要求，犯罪分子不会让赃款在银行账户停留太久以免被公安机关冻结，因此，具有匿名性、去中心化特点的虚拟币便成了犯罪团伙洗钱的重要媒介。

“黑钱”一转入上游团伙提供的一级银行账户后，立即转入找来的前端团伙的二级账户，由前端团伙迅速提现至支付宝、微信等第三方平台，后用绑定的账户在交易软件上用“黑钱”买成虚拟币再提币到指定账户，由另一伙后端人员将指定账户中的虚拟币卖出，整个洗钱过程快速又难以追踪，加上前、后端人员互不联系，追踪“黑钱”去向更是难上加难。

2020年12月底，一名句容被害人向公安机关报警，经反查资金流向，被骗资金最终流入肖某（另案处理）的银行账户，而肖某曾在火币“USDT”app（一

种虚拟币，和美元挂钩，1USDT=1 美元）上多次卖币，该资金是买家用来向其买币的钱。经肖某供述，其是听从上家安排将上家转给其的火币卖出后取现。经对火币交易账户进行溯源，发现卖出的火币均是从同一个混币资金池（注：即流入和流出资金很难找出对手端，隐藏交易路径及身份信息，阻断资金之间的关联）中流出，资金池的火币金额高达 1200 万余元，而部分火币是从另一伙人的火币账户中卖出，经公安机关通过技术手段将前端团伙李某等 10 名被告人抓获归案。

#### “跑分群”找商机，沦为洗钱帮凶

2020 年 8 月，李某从之前的加入“跑分”群中看到关于收 USDT 虚拟币的消息，也就是找人“洗黑钱”。为了赚取佣金，便和上家“雷神”在火币平台上做买卖虚拟币生意，即由李某将自己的银行账户发给“雷神”，“雷神”将买币的钱转到李某的银行账户，由李某用这笔钱在平台上买币，最后按照要求将火币通过扫码或指定链接方式转出到指定账户，而最终火币均会流入一个总的资金池，每买 1 万元佣金 70 元。为了逃避监管，二人平时都在“蝙蝠”“飞机”“BK”等境外软件上交流。因每个火币账户每天只能买 2-3 万的 USDT，李某又找到 3 人“跑分”。另外一伙买币的张某等 6 人团伙也进行同样“跑分”操作。

该案移送审查起诉后，由于资金链条复杂，打印出来的银行流水及火币交易记录达 500 余页，且混币资金池下分多个分级账户，资金溯源难度非常大。检察机关组建专业化办案团队，对案件侦破经过、人员关系及地位作用、资金流向多次分析研判，抽丝剥茧，最终查明李某等人共计参与洗钱 7.8255 万元，张某等人共计参与洗钱 87.4864 万元，均构成掩饰、隐瞒犯罪所得罪。

为全力挽回被害人经济损失，承办检察官多次督促各被告人主动退赃，最终上述被告人共计退出赃款人民币 40.1255 万元发还被害人，并自愿认罪认罚。综合全案情节，句容市人民法院采纳检察机关的全部量刑建议，并作出上述判决。

（来源：人民日报客户端，转引自：复旦大学中国反洗钱研究中心，网址：<http://www.ccamls.org/newsdetail.php?did=43938>。时间：2023 年 1 月 13 日。访问时间：2023 年 1 月 18 日 17:05。）