利用虚拟货币披上一层隐蔽外衣，成为近几年犯罪分子的惯用新手段。

被“神化”的荐股大师、“一对一VIP”的会员服务、“低风险高回报”的投资平台……随着投资理财热情高涨，各类荐股骗局层出不穷，不少投资者明知有风险，却还沉迷在骗子编织的骗局里，幻想“一夜回本”，结果陷入虚假平台的投资陷阱。

现在，这类“杀猪盘”“虚拟盘”“网恋陷阱”产生的黑钱向更隐蔽的虚拟货币平台转移，一条利用虚拟货币洗钱的非法产业链逐渐浮出水面。

传统“荐股”套路，新型洗钱手段

4月26日，萧山区人民法院审结了一起涉境外诈骗集团诈骗案，诈骗数额高达770万余元，其中，为首的被告人柳某获刑十一年四个月。

诈骗金额虽然巨大，但柳某及其团伙的骗术其实也是“老套路”了。

2019年9月的一天晚上，吴先生收到了一条微信好友添加申请，通过后，对方自称爱好炒股，有赚钱门路，随后便将吴先生拉入一个炒股群，还向他推荐了一位炒股老师。

这位炒股老师每天都会在群内讲课、分享炒股信息，群内其他成员经常向老师反馈赚钱的“捷报”。时间久了，吴先生也不免有些动心。他按照老师的教程操作，开始的确顺利赚了几笔钱，他对炒股老师的信任也开始提升。

没过多久，老师表示现在股票行情不好，推荐大家炒“数字货币”，吴先生不疑有他，又按照老师的推荐下载了某APP，并在其中充值购买了所谓的“数字货币”。

可惜，同年11月4日至8日，短短4日内，吴先生先后四次充值19万元均未能获得收益。两周后，吴先生发现，该APP账户已无法提现，这才幡然醒悟，随即报警。

后经警方调查，除了吴先生外，陆某、张某等20余人均遭遇了同样的“套路”，被骗数额有数万元至上百万元不等。随着柳某、李某甲、刘某、李某乙等人被抓获，一个境外电信网络诈骗犯罪集团的幕后骗术也浮出水面。

法院判决书显示，2019年8月至9月期间，被告人柳某、李某甲、刘某、李某乙等人经他人邀请或网络招聘，加入了马来西亚某境外诈骗犯罪集团。该诈骗犯罪集团有着一套明确的“工作机制”：

先将新招募的成员分为不同小组，以小组为单位实施电信网络诈骗。其中，被告人柳某作为诈骗犯罪集团总监，负责管理各诈骗小组、下发话术、统计业绩等。

各小组成员手握大量微信号，一边随机添加吴先生这样的被害人，一边假装成“投资人”加入由该犯罪集团组建的大量微信群中。在微信群内，被告人李某甲等各小组组长冒充炒股老师，被告人刘某、李某乙等其他组员分别冒充老师助理、虚假投资者等角色，小组成员之间有一套成熟的交流话术，互相配合。

在取得被害人信任后，以“某数字货币可以获得高额利益”的说法，诱导被害人下载其所操控的投资平台，并通过后台操作制造出升值的假象，直至非法占有被害人的充值钱款。

经查，被告人柳某等人参与的诈骗小组共骗取钱款770万余元。

法院审理认为，被告人柳某、李某甲、刘某、李某乙结伙，以非法占有为目的，虚构事实、隐瞒真相，通过电信网络骗取他人财物，数额特别巨大，应当以诈骗罪定罪处罚。根据四被告人的犯罪情节和认罪态度，以诈骗罪判处被告人柳某有期徒刑十一年四个月，并处罚金11万元；判处被告人李某甲有期徒刑六年六个月，并处罚金5万元；判处被告人刘某有期徒刑三年十一个月，并处罚金2万元；判处被告人李某乙有期徒刑三年十个月，并处罚金2万元。

赃款流入境外交易所“漂白”

虚拟货币流转不留痕，具有匿名性、复杂性、跨国性特征，无需金融机构参与即可完成操作，难以追溯资金去向，已成为不法分子为赃款“漂白”的新利器。

利用虚拟货币进行非法集资、洗钱等犯罪行为的案件也不断增加。据中国裁判文书网统计，2018年，我国虚拟货币的传销类案件多达166起，而2017年为94起，2016年为46起，2015年为10起，2014仅有5起，近几年的案件年均增长率超过100%。2020年以来，国内各地警方破获关于虚拟货币犯罪的案件频繁被媒体披露。

北京德和衡（上海）律师事务所合伙人安宁表示，他接触的虚拟货币洗钱案件主要分为两类，一类是以虚拟货币作为幌子，开设虚假的交易平台等，进行诈骗的案件；另一类是以虚拟货币作为转移赃物的媒介，涉及洗钱罪，掩饰、隐瞒犯罪所得罪等。

以往，犯罪团伙较多采用提供资金账户进行转账或取现，通过购买理财产品，买卖房屋、车辆等方式协助转移资金。但这类资金转移方法能追踪到流水记录，而利用虚拟货币洗钱的新型犯罪手法则更隐蔽，洗钱团伙一旦将黑钱转去境外交易所，便

给追回资金造成极大难度。

2020年3月，在上海市浦东新区公检法部门公布的一起虚拟货币洗钱典型案例中，一名涉嫌利用虚拟货币平台诈骗的嫌疑人集资诈骗了上千万元后，出逃澳大利亚，并授意妻子陈某将诈骗所得转移至海外。该名妻子供述，钱通过银行卡打给了两个比特币矿工，兑换密钥，给了丈夫，从而将资金绕过外汇管制。身处澳大利亚的他，可以直接将虚拟货币兑换成澳元。

夫妻双方里应外合的境外洗钱操作，将两类诈骗手段都发挥得淋漓尽致。

业内人士认为，虚拟货币洗钱有可能成为区块链世界长时间的犯罪威胁。加密虚拟货币的去中心化属性，让侦查部门面临资金难以查控、操作人员难以关联、电子证据难以获取等多方面困难。

对此，侦查部门应以区块链技术为依托，优化反洗钱系统，完善电子证据取证工作，健全反洗钱数据监测预警体系。

“网恋”对象教导为犯罪团伙洗钱

赃款流入虚拟货币交易所的重要通道，是流经不易被识别的信用卡账户。福州警方近期侦破的洗钱案中，嫌疑人李某则是因“网恋”稀里糊涂被带入了洗钱圈套。

2020年春节，待业在家的李某通过抖音App认识了一位女网友小陈，双方很快坠入爱河。小陈告诉李某，手机刷单能赚钱，李某想也没想就向小陈请教“经验”。根据小陈的指示，李某下载了聊天软件App、绑定了银行卡和身份信息后便开始了第一笔的“刷单”。仅一天便赚取了2000元。尽管他觉得事有蹊跷，但并未停下刷单的“手速”。

今年1月，福州三叉街派出所民警在侦办一起网络投资诈骗案时，发现李某名下一张银行卡资金流水竟然多达500多万元，民警立即出动将李某抓捕归案。面对自己银行卡打出的资金流水，李某只能低头认罪。他在小陈的指导下，通过出租、出借、出售银行卡，帮助犯罪分子用虚拟货币“漂白”了一部分赃款，成为了犯罪分子的帮凶。

安宁说，要减少这类信用卡被犯罪团伙利用成为洗钱工具的行为，监管部门要从三方面加强管理：

一是加强银行卡的管理。近些年，犯罪分子经常购买、借用、冒用他人身份申领银行卡，并用于犯罪活动，公安部等部门近期开展“断卡”行动，目标就是打击此类

行为。

二是加强对资金异动的监控。银行等金融机构，要加强对资金交易行为的实时监控，对有异动的资金流转，要及时采取临时限制措施。

三是加强对第三方支付平台、网络科技公司的监管和法治宣传，强化对第三方支付、网络科技公司的合规经营义务，防止为犯罪分子提供资金通道和技术手段。

栏目主编：顾万全 文字编辑：程沛 题图来源：图虫 图片编辑：苏唯

来源：作者：21财闻汇