

本报记者 李晖 北京报道

对虚拟货币渐成围剿之势，但监测和干预此类绕道传统金融体系的新型支付工具仍存较大挑战。

“十一”前夕，中国人民银行联合多部门下发《关于进一步防范和处置虚拟货币交易炒作风险的通知》，严厉打击虚拟货币交易炒作。被市场认为国内对虚拟货币产业链雷霆整肃的又一里程碑。

监管对虚拟货币的整顿由来已久，自2017年以来，相关表态和措施持续出台。在近期的第十届支付清算论坛上，中国人民银行支付结算司司长温信祥在演讲时首次明确提出虚拟货币对支付体系带来的主要三项挑战——脱离支付体系封闭运行、分流银行和支付机构的支付业务、被用于非法行动。

上述“三宗罪”可以一窥监管大力整顿虚拟货币炒作与交易的部分动因。虚拟货币是如何绕道传统金融体系侵蚀跨境支付业务的？其如何通过隐秘的资金路径参与非法行动？需要看到，目前监管主要着眼于“虚拟货币”与传统金融体系的连接环节，采用“断支付”等措施，但如何进行监测、干预、阻止、惩治，还需要法律依据和技术手段的创新应用。

未受监管资金流出汹涌

因开设互联网金融平台非法集资、数字货币交易平台发行虚拟币被警方侦查立案后，陈某波2018年出逃澳大利亚。此后，其授意尚在国内的妻子陈某枝变卖以非法集资款购买的车辆，将数十万元赃款转移到境外供其使用。

今年上半年，最高人民检察院和中国人民银行联合披露了多起典型洗钱案例。但在上述由上海浦东公安部门破获侦办的案件中，警方最初并不掌握陈某枝如何把大额资金转给在逃海外的丈夫。从银行交易记录看，陈某枝只是汇了几十万元给两位陌生人，与其丈夫并无直接资金往来，洗钱的资金链中断了。

此后，人民银行指导商业银行反洗钱部门排查可疑交易，通过穿透资金链、分析研判可疑点，向公安机关移交了相关证据。经过审讯后，陈某枝交代是通过转账给两位比特币矿工，矿工再将比特币密钥提供给其丈夫，将赃款转移到了境外。公安机关根据利用虚拟货币洗钱犯罪的交易特点收集运用证据，包括比特币地址、密钥，行为人与比特币持有者的联络信息和资金流向数据等，最终实现了对其定罪。

上述典型案例一定程度反映了国内监管对虚拟货币交易炒作零容忍的动因。京衡律师事务所互联网法律部副主任张豪在接受《中国经营报》记者采访时表示：虚拟货

币具有三大非法应用场景。其一是跨境支付，为跨境结算、跨境赌博等非法活动提供了支付结算途径；其二是跑分洗钱，比传统跑分更难追踪；其三是偷税漏税，虚拟货币的交易记录税务机关很难稽查。

事实上，在此次“924”监管再升级之前，自2017年以来，在持续监管整肃下，原先在国内活跃的众多虚拟货币交易所纷纷远走境外，将交易所服务器迁址到直布罗陀等监管较为宽松的国家和地区。但仅凭此，并不能彻底阻击虚拟货币市场运行和未受监管资金的流出。

区块链安全服务公司杭州派盾信安科技有限公司（以下简称“派盾科技”）发布的《数字货币反洗钱暨 DeFi 行业安全报告（2021年上半年）》显示，2021年上半年，以虚拟货币形式从国内交易所（用户主要分布于中国内地和香港的四家交易所）流出至国外交易所未受监管出境的资金规模达到283亿美元，是2020年全年流出的资金总量1.6倍。2021年5月至6月，由于国内政策在挖矿、交易上加强监管力度，未受监管的虚拟货币流出资本金量下降了近40%。

需要看到的是，目前炒作虚拟货币的方式已在悄然转移。上海方达律师事务所资深律师、反洗钱专家汪灵罡曾经在多家国际银行反洗钱岗位工作，他告诉记者：随着近年来监管升级，目前国内个人和机构进行的主流虚拟货币交易方式，比较常见的方式一类是投资者之间的场外交易，类似于线下的面对面“一手交钱、一手交货”；一类是以境外资金账户、在境外交易平台进行的离岸交易。

而随着此次监管再度收紧，多家大型数字货币交易所作出关闭内地服务的决定。这在打击虚拟货币交易的同时，是否能进一步扼制不受监管的资金出境仍需观察。

隐秘复杂的交易链路

此轮监管升级，一方面是源自挖矿等高耗能行业背离低碳目标。另一方面则是伴随资金流出汹涌的同时，虚拟货币被频繁用于洗钱、诈骗、赌博等非法交易之中，其资金路径隐秘性更强而难以监管。

记者注意到，温信祥在前述论坛上披露了今年上半年河南侦破的一起利用虚拟货币转移赌资的案件，该案涉案金额高达51亿元。央行在现场调研时发现，转移资金链路具有“钱币分离”和“先钱后币”特点——通过多个参与主体、多次资金流转，设计了颇为复杂的资金链路。“其中，有团伙专门承担类中央对手方（CCP）角色，对接赌博平台与币圈群体；有犯罪团伙与币圈提供人民币与虚拟货币的钱币对付机制，并在内部形成‘大户—散户’的双层结构。虚拟货币的钱币对付机制、交易信任机制、币圈双层结构等特点。”温信祥表示。

虽然上述案件尚未被相关部门详细公开，但通过“跑分”形式转移赌资或实施诈骗的套路却并不陌生。而借助虚拟货币通道，资金的转移更加复杂且高速。派盾科技在对一起利用虚拟货币诈骗的“杀猪盘”案件进行技术分析时发现，在诱骗被害人将虚拟货币充值到虚假平台或地址后，资金从归集地址进入诈骗分子钱包后随即产生了多次转移和混淆，诈骗平台的充币地址和243个交易所地址产生了交互，受害人的虚拟货币迅速通过洗钱团伙处理或者流入境外去中心化交易所。

派盾科技方面相关负责人表示在接受记者采访时表示：近年来虚拟货币非法交易的结构日益复杂，特点是拉长整个交易的链条进而提高整个洗钱环节的复杂性。这类案件的侦查取证难点在于：一是犯罪团伙利用多个虚假身份开设交易所账户，使KYC认证信息失效，难以锁定真实嫌疑人；二是通过比较复杂的拆分、转移、归置，将一些主观上没有洗钱意图的用户和OTC（场外交易）卷入网络；三是中间的核心环节往往由境外的犯罪控制，为闭环整个非法交易的链条制造困难。

一位虚拟货币交易所从业人士透露：特别是有时候资产流入某个新开地址，而这个地址几乎没有过交易数据，极难判断账户性质或持有者，而洗钱的步骤是以毫秒级的速度运行，响应、追查起来非常艰难。

传统“断支付” 仍存挑战

虚拟货币的交易之所以难监测难干预，是由于其脱离了现有的监管体系。银行和支付机构仅靠内部交易系统监控可疑资金、账户，无法解决跨行、跨平台甚至跨国的交易跟踪问题。

据记者采访了解，目前，支付宝、微信支付对待此类大多以黑名单性质进行管理，对重点网站和账户建立巡查制度，一经发现立即封堵；通过加强支付交易环节风险监测，部署风险算法模型，加强异常交易监测，对嫌疑付款方风险提示、收款方进行限权。

国内的金融机构基本也只能从可疑交易的维度来进行约束。汪灵罡告诉记者：国内银行机构的反洗钱交易监测系统并不是专门针对虚拟货币交易监测而设置。目前，各金融机构都充分重视虚拟货币交易相关的洗钱风险，但由于洗钱手法众多，通过虚拟币交易洗钱的规模在整个洗钱行为中所占的份额可谓沧海一粟。

“更多的技术投入必然带来更高的合规成本，由于虚拟币交易洗钱的规模仍较小，只是个案看起来数额比较大。金融机构通常不会为虚拟币洗钱监测投入更多资源。”他表示。

更多的反诈反洗钱措施，显然需要数字货币交易所“扛起重任”。派盾科技结合已

有的1亿个地址标签，对包括资金盘地址、暗网地址、赌博地址等多种高风险地址进行追踪、监控时发现，这些黑产地址和交易所地址存在频繁的交互行为。

据记者了解，主流交易所通常有严格的KYC认证，除此之外更多反诈反洗钱措施也开始出现。一些交易所此前曾披露设置了风险隔离期政策，风险用户需要T+1日取现。此外，基于涉币人群动态开源情报大数据分析的链上资产追踪系统近两年已经被利用在对于虚拟货币欺诈、洗钱的追踪。

记者注意到，包括派盾科技、火币、欧科云链等机构都先后推出了类似系统，以跟踪资金在链上的流动情况——链上监控功能普遍涉及“地址监控”和“交易监控”，通过监控某些地址的动态和监控某笔交易中涉及的资金来实现动态跟踪。

不过，如果这些资金最终去向非主流交易所则可能让上述追踪机制也力有不逮。随着 DeFi

（去中心化金融）生态的发展，更复杂的用虚拟货币洗钱的模式已经出现。

在汪灵罡看来，这种模式不做KYC认证也找不到具体运营方，即使在国际上对此的监管研究和措施也远远不够。

派盾科技相关负责人向记者透露，除了常用的中心化混币服务、利用协议实现自动化混币的去中心化的混币服务器的出现，为犯罪分子持有的虚拟货币加上了多层保护膜。而此次监管升级之后的新变化也仍需要继续调研。