

虚拟货币跨境洗钱形势严峻

中国新闻周刊记者/徐天

发于2021.4.26总第993期《中国新闻周刊》

因涉嫌集资诈骗，陈丽的丈夫出逃至澳大利亚，并授意陈丽将诈骗所得转移至海外。而当陈丽到案时，警方其实并不掌握她是如何把大额资金转给逃至海外的丈夫的。警方翻查她的银行流水，发现她在前几天汇了几十万元给陌生人。出逃时的重要资金来源，不可能无缘无故汇给不相干的人。陈丽后来供述，钱打给了两个比特币矿工，兑换密钥，给了丈夫。

这起案件发生在2018年，承办该案的上海市浦东新区公检法部门，都是第一次碰到用虚拟货币洗钱的情况。2021年3月19日，最高人民检察院、中国人民银行联合发布6个惩治洗钱犯罪典型案例，该案成为其中之一。相关负责人指出，利用虚拟货币跨境兑换，将犯罪所得及收益转换成境外法定货币或者财产，是洗钱犯罪的新手段。

中国通信工业协会区块链专委会轮值主席、火币大学校长于佳宁告诉《中国新闻周刊》，从2020年开始，在全球范围内，无论是诈骗、网络攻击和勒索、赌博、洗钱、地下钱庄这类黑产，还是跑分等灰色产业，有一部分开始利用具有匿名性、复杂性和跨国性的虚拟货币实施犯罪。在国际上，也出现了恐怖组织转向虚拟货币领域融资以支持其活动。

根据区块链安全公司 PeckShield 发布的“2020年年度虚拟货币反洗钱报告”显示，2020年，中国未受监管的跨境流动虚拟货币价值达175亿美元，较2019年增长51%，且仍在快速增长。激增的洗钱“新通道”，给中国反洗钱机制带来巨大的挑战。

黑灰产盯上虚拟货币

2020年11月底，江苏省盐城市中级人民法院发布了一份二审刑事裁定书，驳回上诉，维持原判。备受瞩目、总值超400亿元的“币圈第一大案”告一段落。

两年多以前，被告人以区块链为概念，策划搭建PlusToken平台，对外宣称该平台拥有“智能狗搬砖”功能，即能同时在不同数字货币交易所进行套利交易、赚取差价，许诺给投资者10%到30%的月息。平台会根据发展下线数量和投入资金数量，将会员分等级，按等级高低发放相应奖励和返现。2019年6月，PlusToken平台被曝出提币困难。后经警方查证，该平台没有任何经营活动，也不具备“智能狗搬砖

”功能。警方将该案定性为“以比特币等数字货币为交易媒介的网络传销案”。截至案发，PlusToken平台的注册会员账号269.3万个，会员的最大层级为3293层，涉案的比特币等数字货币总值逾400亿元。

利用区块链、数字货币进行传统犯罪，在近几年已成趋势。区块链安全公司 PeckShield在接受《中国新闻周刊》采访时指出，随着区块链核心技术被上升到国家战略高度，公众对区块链领域也愈发关注，各式骗局应运而生，其中以区块链概念包装的资金盘、杀猪盘最为层出不穷。

PeckShield曾统计过从2017年至2020年在虚拟货币行业发生的重大安全事件，诈骗案件的数量变化非常明显。2017年和2018年，虚拟货币行业分别发生了3起和4起诈骗案件。2019年，诈骗案件增长了4倍，达20起。到2020年时，案件激增至151起。

诈骗案件激增与比特币暴涨有着直接关系。欧科云链集团的技术负责人于志翔告诉《中国新闻周刊》，牛市有造富效应，市场越好就有越多的人想涌入，而新人没有足够的渠道来了解虚拟货币，很容易被骗。PeckShield也指出，对普通用户而言，虚拟货币的技术和参与门槛相对较高，给了投机分子炮制各种骗局的可能性。

2020年初，一名温州女子在某个婚恋网认识自称投资精英的男士杨某，杨某赢取该女子好感后，便开始让其在某个不知名交易平台帮忙购买比特币。按照杨某的指导，女子也从该平台买入了一批比特币，提现时却需要缴纳保证金。陆陆续续向平台缴纳了保证金、激活金、比特币等在内的40.7万余元后，女子意识到这是典型的杀猪盘骗局，选择报警。江苏常州警方也曾破获类似案件，在广东、福建、云南等地抓获犯罪嫌疑人17名，该团伙在全国近300个地市作案370多起，全是杀猪盘，涉案总金额达1.2亿元。

PeckShield告诉《中国新闻周刊》，2020年，因诈骗案件造成的损失共有31.3亿美元。这类案件往往以投资名义让受害人先到正规交易平台用现金购买虚拟货币，再诱骗对方将已买的虚拟货币转移至诈骗分子指定的虚假平台或地址。一旦转移，虚拟货币会迅速通过洗钱团伙处理或者流入境外交易所，为追回资金造成极大的难度。诈骗类安全事件已经成为区块链世界最大的安全威胁。

除了“杀猪盘”，黑客攻击、勒索攻击也占较大份额。2020年，虚拟货币行业的黑客攻击事件有170起，较2019年增长300%。

另外，随着银行体系越来越严格的反洗钱和反恐怖融资机制，国际的恐怖组织也开始转向虚拟货币领域融资。2020年8月，美国查封并公布了一批由“基地”组织、伊斯兰国(ISIS)等恐怖组织拥有和使用的虚拟货币账户，价值超200万美元。PeckS

hield指出，账户地址的资产和数十个主流虚拟货币交易所发生交互，变现渠道遍布全球。

于佳宁指出，正是因为虚拟货币具备匿名性、复杂性和跨国性的特征，黑灰产开始转向该领域实施犯罪。作为这些上游犯罪的“链条下游”，通过虚拟货币交易的方式来洗白犯罪所得的黑币、黑钱，也已呈趋势。

更隐秘的资金走向

在最高检、央行发布的用虚拟货币洗钱的典型案例中，陈丽与丈夫选择这一方式洗钱，出于一个非常现实的考量：绕过外汇管制。

该洗钱案的承办检察官、上海市浦东新区人民检察院检察官朱奇佳告诉《中国新闻周刊》，陈丽丈夫出逃中国香港及澳大利亚期间，陈丽分几次给丈夫随身携带的银行卡打了300万元人民币，丈夫带着银行卡出走澳大利亚。而他出境后，取现涉及每人每年一定限额的外汇管制。因此，丈夫主动提出，要兑换虚拟货币。

陈丽丈夫所涉罪名是集资诈骗，起因就是因为发行虚拟货币的固定理财，自建模型、自己控制涨跌。他在行业内本就有熟人，于是轻车熟路找来“矿工”，将妻子拉入，建了微信群。他负责谈判价格，“矿工”同意后，陈丽汇款，“矿工”将密钥给丈夫。身处澳大利亚的他，可以直接将虚拟货币兑换澳币。

该案的审判长、上海市浦东新区人民法院法官刘娟娟告诉《中国新闻周刊》，虚拟货币洗钱虽然是有技术与专业性的新方式，但其查证路径与传统洗钱，归根结底是一致的，黑钱转出，洗白的钱转回来。其取证难点在于，踪迹更难寻，且极有可能发生在境外。

朱奇佳透露，在该案中，资金的走向十分隐蔽。查洗钱案，通常要跟着资金的流向查。该案中，明面上的资金流向却是中断的。陈丽将钱从银行账户打给“矿工”，“矿工”的银行账户和陈丽丈夫并无来往，无法构成完整的洗钱链条。如果不是陈丽的口供以及微信聊天记录，公安机关并不知晓，这笔钱已经转换成了比特币，打给了丈夫。

彭启劲是广东省广州市公安局白云区分局刑警大队四级警长，常常会接触诈骗、洗钱案件。去年碰到的一起用虚拟货币洗钱的案子，也让他对如何分析资金流，有了新看法。

该案的上游犯罪同样是一起利用虚拟货币诈骗的案件。2020年2月底，谢某报案称，自己在网上认识了一位金融投资老师，对方指导他在一个叫“币齐”的网站进行

比特币投资，陆陆续续投了310万元。后来，该老师称，投资平台爆仓，310万元血本无归。谢某怀疑对方是恶意操作，故意让自己亏掉钱，因此来报案，并提供了嫌疑人操作的11个一级账户。

白云警方对一级账户进行穿透调查，获得了12个与一级账户来往密切的二级账户。他们选取了事主所投资金中的100万元，来跟踪深挖接下来的资金去向。

彭启劲告诉《中国新闻周刊》，这100万元，从一级账户汇给了二级账户，而从二级到五级账户，这笔钱分拆、掩藏、转移、汇总，从五级到六级账户，走账的资金却从100万元变成了140万元，从六级到七级账户，资金更是增至900万元，规模变化极大。警方发现，二级至五级账户的开卡人彼此关联，基本都是广东省一个镇上的。警方以此为切入点做进一步调查，发现了一个多达20人、有100多张银行卡的家族式洗钱“水房”。

主犯张辛落网后，警方才从他的供述中得知，原来这个团伙利用虚拟货币洗钱。张辛是某数字交易平台的商家，2020年2月，有人找到张辛，以市场价买他手上的泰达币，转账100万元，这就是被诈骗的那笔钱从一级账户汇入二级账户的过程，诈骗者已经将100万元顺利转换成泰达币。而这笔钱此后从二级账户到五级账户的流转，都是张辛认为这笔钱恐怕是“黑钱”，有可能被警方冻结，因此做出的“反冻”腾挪举动。

彭启劲感慨，如果仅仅对银行账户的资金流进行追踪，警方既不知道他们实际上使用了虚拟货币洗钱，也不知道竟然早在资金从一级账户流转至二级账户时，这笔钱已经转换成了虚拟货币，回到一级账户持有者手中。从事主的100万元人民币汇入一级账户，到一级账户持有者拿到虚拟货币，整个过程只有6分钟。

复旦大学经济学院副教授、中国反洗钱研究中心执行主任严立新告诉《中国新闻周刊》，这实际上充分体现了虚拟货币其运行机制有着特别鲜明的去中心化、虚拟性、匿名性、实时性、难篡改等特征，无须金融机构的参与就可以完成交易。去中心化使得追踪一笔虚拟资产交易远比中心化状态下更为艰难，因为线索不易获取，完整的证据链也极难收集；实时性则意味着洗钱的步骤可以是毫秒级的运行速度，在全球任何一个地方发起并完成，监管机关或执法部门几乎没有足够的响应时间去及时阻断以防止损失或负面影响的发生。

抓获了张辛为主犯的洗钱“水房”，警方的调查并未结束。一级账户的持有者是实施诈骗的人吗？张辛卖出的泰达币流向了哪里？诸多问题还待解答。在对11个一级账户进行行为习惯的分析之后，警方发现，一级账户仍非诈骗者，而是另一拨从事洗钱的人，跑分客。

跑分，是这些年的新兴事物。跑分平台是指通过第三方支付平台合作银行及其他服务商等接口，非法对(赌博、淫秽色情、诈骗等)提供支付结算业务的网上平台。跑分客，就是在这些平台注册账户，提供自己的支付宝、微信、银行等支付渠道收款码，为他人代收款并转款至指定账户，从中收取佣金的人。

近几年来，随着反洗钱行动的深入，跑分平台也开始通过虚拟货币洗钱。彭启劲介绍，在前述案件中，事主在“币齐”这个网站投资，充值时，网站会自动而隐秘地跳转至跑分平台。事主充值的310万元，并未进入诈骗者的账户，而是直接进入了该跑分平台各跑分客的账户。根据跑分平台工作人员的指挥，这批资金通过虚拟货币的方式“洗白”。

彭启劲感慨，虚拟货币是黑钱的载体，跑分平台是一条快速通道，境外聊天软件则是一条安全带，黑钱在这个过程中高速流转。“我们开着一台捷达警车在后面追赶，能追上吗？即便能追上，也是一些已经来回跑了好几圈的跑手，抓了这些跑手，我们能处理吗？”彭启劲指出，非常有必要花时间、精力对这类新型洗钱模式、指挥模式作探讨。

技术“天网”如何补漏？

随着全国范围内开展“断卡”行动的推开，越来越多的非法资金开始通过虚拟货币洗钱，境内资产通过虚拟货币转向境外也呈上涨趋势。据PeckShield对资金流动量的计算，2020年1月至10月，每个月从国内交易所流出到国外的比特币数量从8.94万到16.69万枚不等。而在“断卡”行动生效之后，去年11月和12月，比特币流出数量达23.17万和25.41万枚，较此前的最高点还增长了近40%。

更复杂的用虚拟货币洗钱的模式也已出现并使用。于佳宁告诉《中国新闻周刊》，西方研究者总结了典型虚拟货币洗钱犯罪的三个阶段：放置、培植和融合。放置阶段，犯罪分子购买虚拟货币，将非法资金注入所要“清洗”的渠道中；培植阶段，洗钱者利用虚拟币的匿名性进行多层次、复杂化的交易，从而掩饰犯罪所得的性质和来源，或是通过虚拟币的“混币”技术，将待“洗白”的虚拟币掺入“混合池”，以此模糊原始来源；融合阶段，在不断转移和洗白非法所得后，犯罪分子持有的虚拟币已基本不受限制并且相对安全，此时他们只需将虚拟货币提现，基本上就完成了洗钱操作。

作为虚拟货币交易平台，在保护客户隐私的前提下，如何避免平台被犯罪分子所利用，这是各平台从成立之时就面临的挑战。

于志翔告诉《中国新闻周刊》，最初，交易平台像各类传统金融机构一样，平台推出了KYC政策，也就是Know your customer(充分了解你的客户)，强化对账户持

有人的身份审查，即要求个人开户时必须提供身份证明文件，比如身份证、护照等，最大限度地保证账户背后是活生生的、可以触达的人，这是各类传统金融机构反洗钱政策的基石。

这些年，KYC之外的更多反诈反洗钱措施也开始出现。首先是风险隔离期政策，对于一些平台识别出的风险用户，其取现必须经历T+1日的风险隔离期，即其他用户可以T日取现，而这类风险用户需要T+1日取现。这对急于流转资金的洗钱者来说，增加了洗钱难度，甚至不再愿意在该平台取现。另外，平台对大额交易设置了人工审核机制。火币集团告诉《中国新闻周刊》，他们已实现识别并拦截疑似杀猪盘受害人的技术，在2020年，平台提前限制未交易风险账户8090个，打击平台欺诈账户186个。对于被认定为有直接参与或协助洗钱等犯罪行为的用户，火币会直接永久限制该用户的账户及关联账户的全部功能。

更主动的链上资产追踪系统也在近一两年被一批虚拟货币交易平台、区块链安全公司推出，比如火币集团推出了“占星系统”，欧科云链集团推出了“链上天眼”，PeckShield推出了coinholmes系统。这些系统都可以获取资金在链上的流动情况

以“链上天眼”为例，于志翔告诉《中国新闻周刊》，链上监控功能分为“地址监控”和“交易监控”两种，前者可以监控某些地址的动态，后者则可以用来监控某笔交易中涉及的资金。地址监控，通过对互联网数据的挖掘分析，检测出一批与暗网、涉黑涉骗等犯罪相关的虚拟货币地址。一旦这类地址的虚拟货币转移，系统就会感知到，并进行链上追踪。追踪就涉及交易监控的功能，资金流转的每一个地址都可以被追踪还原。对监控系统来说，最佳结果是资产最终流入某个虚拟货币交易平台的账户地址。一般来说，只要平台做了严格的KYC认证，账户和人就可以联系起来，警方立即可以找到犯罪嫌疑人。最坏的结果是资产流入了某个新开地址，此前只有一两笔交易数据，极难判断账户性质，以及背后是何人持有。

于志翔告诉《中国新闻周刊》，区块链技术的匿名性特征注定了从地址到人追踪之难。未来，随着区块链技术越来越普及，支付场景越来越丰富，有可能通过支付习惯来推理地址背后的人。当前，这些链上资产追踪系统已帮助各地公安机关开展了多个反诈骗、反洗钱工作，为其提供技术支持。

反洗钱机制面临巨大挑战

虚拟货币交易有着跨国性的特点，对于洗钱团伙及其上游犯罪，进行全链条打击，历来是个难题。彭启劲所在的白云警方，在抓捕了7名跑分客、“搬砖者”之后，对于跑分平台的管理层，以及诈骗公司，无法再继续追查抓捕。原因无他，跑分平台、诈骗公司均在菲律宾。

于佳宁告诉《中国新闻周刊》，犯罪分子可以轻易地选择在监管较为宽松或者不予监管的法域租用服务器、搭建虚拟货币交易网站，或提供虚拟货币存储服务，或通过互联网实施虚拟货币犯罪活动，使得一国的反洗钱和金融监管失效，而主要以双重犯罪为前提的国际司法协助与引渡也难以奏效。

建立国际合作机制对反洗钱类案件至关重要。中国人民大学刑事法律科学研究中心主任时延安告诉《中国新闻周刊》，目前联合国《打击跨国有组织犯罪公约》《反腐败公约》等都就反洗钱国际合作进行了规定。应充分发挥多边合作机制的作用，加强信息情报的交换，尤其是与其他国家执法部门和金融部门的情报交换。另外，也要在承认被请求方应得利益的前提下，加强境外追赃合作。

几位受访专家都指出，加强对虚拟货币洗钱问题的监管，绕不过的一点是对虚拟货币及其交易平台的监管。正如金融机构内部会有反洗钱机制一样，虚拟货币平台也应建立反洗钱机制，并接受主管部门监管，这是当前国内所欠缺的。

但时延安指出，这类平台不具备相应的“支付业务许可证”，既不是金融机构，也不是特定非金融机构。其在实际运营过程中应当遵守何种反洗钱监管规定、履行怎样的反洗钱义务均没有明确规定。

数字货币交易平台，一定程度上脱离了现有的监管体系。2017年，监管部门责令所有境内数字货币交易所限期关闭，并停止新用户注册。然而随着一批服务器设在境外、但能够在境内登录的虚拟货币交易平台为人所知，仅凭境内禁止平台交易已无法阻止虚拟货币市场的运行。中国政法大学民商经济法学院副教授赵炳昊告诉《中国新闻周刊》，一刀切、鸵鸟政策显然是不行的，虚拟货币自诞生至今，才短短十几年，发展速度远远快于传统金融行业。监管部门必须要转变心态，直面现实，逐步探索、循序渐进地找出适合我国实际情况的监管方案。

赵炳昊指出，当前，我国对虚拟货币的监管由中国人民银行牵头，但传统的监管机构和监管权力体系，对于区块链技术下的金融创新有时鞭长莫及。时延安也认为，中国人民银行设有反洗钱局，但反洗钱局只能监管拿到牌照的机构，而虚拟货币洗钱问题，仅靠监管金融机构或特定非金融机构，是无法解决的。反洗钱局隶属于中国人民银行，层级较低，难以沟通协调公安、海关、网信办等多部委合作，而洗钱恰恰是涉及各行业的事。另外，反洗钱局“没有牙齿”，发现可疑线索后，需依靠公安机关调查取证，反洗钱局能做的工作很有限。

在时延安看来，将虚拟货币交易平台纳入我国的金融机构或特定非金融机构，可能性不大。因此，可以考虑将反洗钱局从中国人民银行独立出来，成为国务院的下设机构，一方面提升其地位，另一方面给予其更大的职权，将虚拟货币交易平台纳入监管。

“无论是提前预防、监测，还是及时阻断，从法律依据和实现手段来说，都还存在欠缺。”严立新指出。更大的挑战也已经出现，赵炳昊指出，“去年，去中心化的虚拟货币交易所开始流行，没有运营方、不做KYC认证，这恐怕是虚拟货币的天生反骨会走上的必然之路。但对世界各国的监管机构来说，大家远远没有做好准备。”

(文中提及的所有犯罪分子、犯罪嫌疑人，均为化名)

《中国新闻周刊》2021年第15期

来源：中国新闻周刊