本刊记者/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。

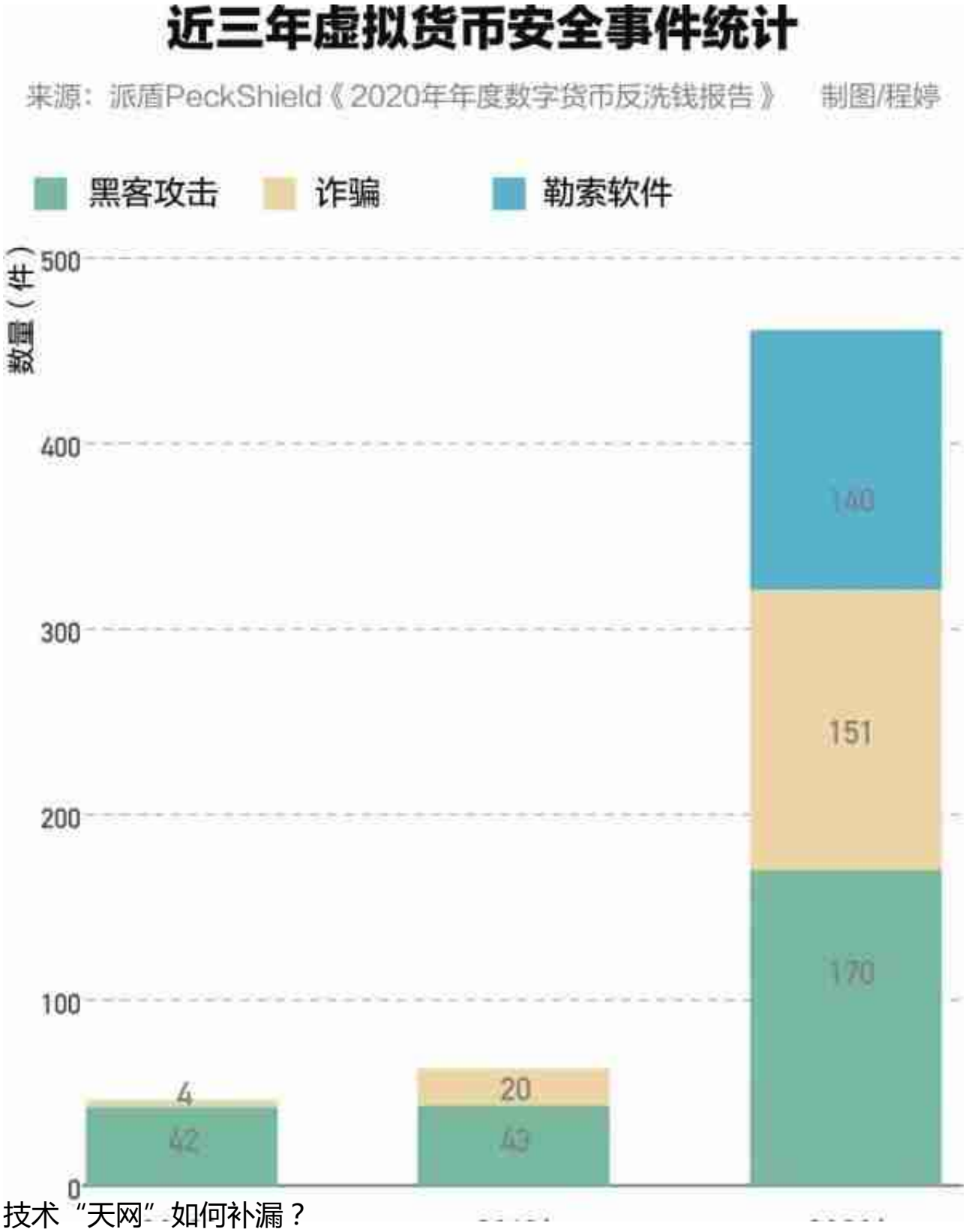
2020年初，一名温州女子在某个婚恋网认识自称投资精英的男士杨某，杨某赢取该女子好感后，便开始让其在一个不知名交易平台帮忙购买比特币。按照杨某的指导，女子也从该平台买入了一批比特币，提现时却需要缴纳保证金。陆陆续续向平台缴纳了保证金、激活金、比特币等在内的40.7万余元后，女子意识到这是典型的杀猪盘骗局，选择报警。江苏常州警方也曾破获类似案件，在广东、福建、云南等地抓获犯罪嫌疑人17名，该团伙在全国近300个地市作案370多起，全是杀猪盘，涉案总金额达1.2亿元。

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。PeckShield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。



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对的挑战。

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。