数币洗钱日益猖獗 中国监管科技卡位发力

近年来，随着数字货币和暗网交易逐渐为人所知，全球范围内利用数字货币进行洗钱的规模也节节攀升。区块链技术路线上的去中心化选择和点对点转账的隐匿性特征，被部分犯罪分子加以利用，沦为诈骗、赌博、贩毒、涉黄、贩卖人口甚至恐怖行为等违法行为的洗钱工具，据 DEA 报告称，中国已成为洗钱计划的重要中心。

日益猖獗的新型洗钱犯罪，给监管带来了一定挑战。欧美国家解决问题的路径是“政府+民间”，即政府出台法规，加强监管，民间提供技术支持。在中国，如何有效监控数字货币洗钱，还处于各方力量的积极探索阶段，但也正逐渐显现出一些可喜的成果。

欧美政府出台数字货币相关法案，加强数字货币监管力度

欧洲刑警组织(Europol)总干事 Rob Wainwright 在 2017 年曾经表示，欧洲罪犯获得的非法收益中，约有 3-4%是用数字货币洗钱的。每年用于洗钱的秘密资金达 42 亿至 56 亿美元。美国缉毒局(U.S. Drug Enforcement Administration)的报告也显示，国际犯罪集团正利用数字资产作为第三种洗钱工具。应对新型犯罪趋势，欧美警方严阵以待，纷纷出台了一系列法律法规加以防范。

以美国为例，联邦层面，主要由美国金融犯罪执法网络（Fin CEN）负责虚拟货币的反洗钱监管。Fin CEN 将比特币等虚拟货币按照“货币服务业”进行反洗钱监管。美国《银行保密法案》（Bank Secrecy Act, 1970）对“货币服务业”（money service business, MSB）进行了明确的反洗钱规定。该法案要求被监管对象对某些交易进行记录、提交报告，并由 Fin CEN 进行收集和分析，为执法机构的稽查提供支持。2013 年 3 月，该局发布《监管规定适用于管理、交换和使用虚拟货币的说明》，其中规定，除非有特别限制或者豁免条款，管理员或者交易商需要

遵守货币服务业的登记、报告并保存记录的规定。Fin CEN 对比特币等虚拟货币交易平台也提出了监管要求。2014 年 10 月，Fin CEN 进一步明确比特币等虚拟货币交易平台属于资金转移机构，必须遵守金融犯罪执法网络的各种规定，包括但不限于反洗钱政策和程序，以及记录保留、报告和交易监管。同时，还特别提出三项具体要求：一是客户资金（包括美元和比特币）需要存入公共账户，与公司运营账户分离；二是不允许第三方注入资金或将客户资金转移到第三方；三是使用匹配引擎促进美元对比特币在用户间的直接交易。概括来说，Fin CEN 对数字货币的监管覆盖了从持有到交易的所有环节，同时也覆盖了传统金融机构和数字货币交易所。

州政府层面，多数州按照现有的货币转移法律进行监管，纽约州于 2015 年 6 月在传统的货币转移法的基础上出台专门针对虚拟货币的《虚拟货币监管法案》，将监管力度集中于比特币发行、储存和兑换环节，不包括消费、支付环节。其中，第十五条对反洗钱工作做了专门要求，第十二条对登记和记录也作出了配套规定。该法案对反洗钱的监管主要体现在客户身份识别、交易记录保存、大额和可疑交易报告、建立内部反洗钱控制系统等方面。

随着政府对数字货币犯罪打击的力度不断加强，一些商业机构也找到了服务社会痛点的机会。美国公司 Chainalysis 顺应市场监管需要，开发了产品，将其命名为比特币跟踪器，其官网介绍，欧洲一半以上的警察部队都与他们有合作；2015 年巴克莱加速器计划之后，Chainalysis 开始在银行业扩大其客户群。在英国，Elliptic 也开始通过数据分析服务加密货币公司，金融机构和政府机构。不难看出，欧美链上数据公司的服务都立足于和政府合作，在数字货币反洗钱领域释放其技术能力。

需要强调的是，反洗钱犯罪在任何一个国家都会被充分重视，尽管国内的数字资产交易所移到境外，作为提供中介服务的数字资产交易平台，应在当地国家

现有的法律框架下活动，不得违反有关反洗钱、外汇管理和支付结算等金融法律法规，对数字资产交易履行审慎核查义务，做好反洗钱和恐怖分子筹资合规审查以及风险防范。

中国探索数字货币监管创新

众所周知，区块链是从中国中央政府到地方政府都非常重视的一项新技术。有迹象表明，有公司使用比特币购买大量“中国制造”商品。然后将这些“中国制造”的货物运往墨西哥和南美的商人，换回当地货币，在这个过程中，可以匿名转移海外价值，绕过中国的资本管制。中国公安大学教授王铎估计，中国利用数字货币进行非法洗钱规模很可能在数百亿元人民币之巨。

任何一项新技术的应用都应该兴利除弊，区块链当然不应该，也不能是监管的法外之地。如是，提高科技在监管实践中的应用，利用大数据、人工智能、云计算等技术，丰富金融监管手段，提高监管能力，建立监管权威就显得十分迫切，同时，监管科技自身的创新也迫在眉睫。

在北京知帆科技（chaidigg）创始人叶茂看来：魔高一尺，则需道高一丈，数字货币兴起衍生出的犯罪现象触发了监管问题，是个全球性问题，技术性强，同样需要科技力量加以震慑。洗钱犯罪行为的特点决定了相关账户或地址的行为与普通的账户交易行为肯定差异很大。知帆科技对链上数据进行收集整理后，通过算法建立链上地址之间，以及链上链下数据之间的关联。通俗的讲，就是通过地址找到人，这种币流追踪在监管实践中的效果非常好，“我们为全国监管部门已经提供了 30 余个案例线索，这些案件涉及的上游犯罪包括赌博、电信诈骗、非法集资等”。

利用数字货币的隐匿性洗钱，将非法收入变为合法收入一度是监管力量难以覆盖的环节，现在，这已经不再是一道无解之题。

2007 年 1 月 1 日，《中华人民共和国反洗钱法》已经开始实施，人民银行同

时出台了《金融机构反洗钱规定》2017年9月13日，国务院办公厅正式发布《关于完善反洗钱、反恐怖融资、反逃税监管体制机制的意见（国办函【2017】84号）》，明确指出反洗钱、反恐怖融资、反逃税监管机制是推进国家治理能力现代化、维护经济社会安全稳定的重要保障，是参与全球治理、扩大金融业双向开放的重要手段。

实际上，部分涉及到数字货币洗钱的案件也已经有了相关判例。来自裁判文书网的资料显示，黑龙江省高级人民法院（2016）黑民终第274号民事判决书里就提及，犯罪分子曾将电信诈骗获得的巨资充值到某数字货币交易平台，分批多次购买比特币，后进行提币操作，将比特币转到比特币钱包，最后在澳门地下钱庄将比特币卖出，完成洗钱活动。该判决同时认定交易平台在KYC环节有漏洞，需承担相应责任。

该案例发生在2014年，判决下来是2016年，对于一个200万案值左右的案子，这个时间跨度还是显得长了些。

侦破涉及数字货币洗钱的案件主要有三难，首先是预防困难，面对成几何倍增长的数字货币交易信息，涉事平台很难及时发现其中与违法犯罪相关的线索，进行必要干预。

其次是查证困难，对于已经发生的数字货币相关案件，由于数字货币的匿名特性，无法追踪其资产流向，无法查找关联钱包及隐匿资产，无法对相关案件进行证据查找及证据固定。而每一个案件的审判过程中，都需要通过证据和证据形成的证据链再现还原事件的本来面目。

最后是执行困难，对于相关违法数字资产，不能非常便利的进行资金冻结以及后续的相关资产处置。

美国的Chainalysis，英国的Elliptic，中国的Chaindigg所做的工作，正是通过大数据分析能力在案件的预防和查证等关键环节形成突破。

由于数字货币犯罪隐蔽强，需要政府各部门通力合作，对此，中央财经大学教授、金融法研究所所长黄震认为，应对用户实名、许可准入、备案管理、反洗钱职责和大额交易限额等方面作出规定，迫切需要工商、公安、金融等部门建立联合监管机制和联动打击机制，“要尽快建立完善统一的数字货币监管体系，把这类违法犯罪扼杀在萌芽状态，保障群众的财产安全。”

相信在各方推动下，中国的监管科技会快速迭代，持续进步，从而使得利用数字货币进行非法洗钱的行为无处藏身。

（来源：经济观察报。转引自：复旦大学中国反洗钱研究中心。时间：2019年1月24日。

网址：<http://www.ccamls.org/newsdetail.php?did=34575>。2019年1月29日 09:04 访问。）