加密货币洗钱犯罪治理

■ 俞　亮　张　驰

摘　要　利用加密货币进行洗钱有日益增长的趋势，其通过参与（投资）加密货币挖矿、在不履行反洗钱要求的加密货币市场进行交易、使用混淆交易主体身份（地址）或交易过程的技术方式使放置、分层、整合等三个阶段的洗钱手段变得更为复杂，也更难被发现和认定。我国目前的“禁止式”监管模式不但无法实际阻止利用加密货币进行洗钱活动，而且也损失了获取此类线索的常规、稳定渠道，更无法建立明确、健全的监管、打击机制。未来治理加密货币洗钱犯罪的基本思路应当以加密货币与法定货币兑换接口为反洗钱监管的重点，同时加强以破解加密货币洗钱过程中的匿名性难题为目标的技术手段开发，并构建更为有效的监管合作框架。

关键词　加密货币　反洗钱　犯罪治理

加密货币（Cryptocurrency）是“一种可以电子数据形式交易，具有交易媒介和（或）计价单位及（或）价值存储功能，但在任何法域不具有法定货币地位的数字形式价值”。其主要形式包括比特币（Bitcoin）、莱特币（Litecoin）和以太币（Ether）等。与传统的硬币和纸币一样，其首先是一种价值的数字表示形式，同时又可作为交换媒介，既可以进行数字交易或转让，也可用于支付或投资。加密货币是通过被称为加密挖矿的过程以数字方式创建的，先由被称为矿工的个人来解决复杂的数学算法，然后，加密货币被存储在一个类似于虚拟账户，并可存在于用户计算机、手机应用程序或云存储中的数字形式加密货币钱包中。每个钱包的功能与用户非常相似，都被分配有包括名称及密码的唯一身份认证（ID），用于登录该钱包并访问其中的数字资产。用户可以使用这种钱包相互购买和发送加密货币，或简单地以与传统货币几乎相同的方式管理他们的加密货币。加密货币也可依赖于类似于商品交易所的在线交易平台获取和交易，在那里可以使用传统货币买卖加密货币，也可交易与加密货币价值相关的期货合约和其他衍生

作者：俞　亮，北京工商大学法学院教授；张　驰，最高人民检察院第六厅三级高级检察官

基金项目：本文得到国家留学基金资助。

产品。

从形式上看，加密货币实际上是无形的“数字签名链”。其所依赖的区块链技术是一种在分布式账本上存储、访问和传输信息的方式，且其数据库上的更新信息与所有用户共享，并通过加密机制进行验证。加密货币无需一个如中央银行一样的中央管理者来发行和维护支付账本，其交易可以在对等方之间直接进行，从而提供了一种无需中介或中心化实体即可处理交易的机会，即完全去中心化的生态系统，并由分布式共识方法对其安全性加以维护。根据所依赖的相关区块链的非公开性质或公开程度，加密货币会有不同的匿名程度。

一方面，几乎所有的加密货币地址都不记录用户信息，如购买者和销售者的姓名和身份，但如比特币一类的部分加密货币的区块链是公开的，公众可以在这个永久的、固定的和公共的账本（即电子记录簿）查询任何交易的流程和时间。但也有部分加密货币使用隐私程度更高的区块链，这些类型被称为隐私币或匿名增强型加密货币，其交易变得不透明且更难追踪，这包括达世币（Dash）、毛内罗币（Monero）和再世币（Zcash）等以及其他更多正在开发中的新型加密货币。区块链技术和加密货币自 2009 年以来，其所衍生的技术生态系统就开始快速增长，截至 2021 年，加密货币市场中约有 4737 种加密货币，其总流通供应的全球加密货币市值约为 2. 07 万亿美元。

由于犯罪分子总会倾向于利用或滥用一种新兴行业或技术所带来的信息不对称，且加密货币交易具有不可逆转且即时处理的属性，同时较容易进行匿（伪）名化和跨境交易，因此往往成为犯罪分子隐藏、洗白和转移犯罪收入的便捷手段。2019 年，网络犯罪分子从加密货币相关犯罪中净赚 43 亿美元，导致大量肮脏网络资金需要清洗。从罪犯的角度看，相比使用无记名股票债券或开设瑞士银行账户等传统隐藏资金方式，使用加密货币的额外好处是可以消除中介机构的管理费用和可能被迫公开账户信息的风险，从而使其成为隐藏或转移资金的有利方法。

目前我国对加密货币活动采取“禁止式”监管模式。根据中国人民银行等有关部门发布的《关于防范比特币风险的通知》《关于整治虚拟货币“挖矿”活动的通知》《关于防范代币发行融资风险的公告》《关于进一步防范和处置虚拟货币交易炒作风险的通知》等相关文件的规定，与虚拟货币相关的“挖矿”、首次代币融资发行（ICO）、交易等所有活动在中国境内都不具有合法性，并以切断境内外加密货币合法交易途径的方式来保护投资者免受加密货币欺诈和价格波动影响，进而维护国家金融安全和社会稳定。

一、加密货币用于洗钱犯罪的特殊形式

根据金融行动特别工作组（FAFT）提供的权威定义，所谓洗钱是指将犯罪活动所得重新注入金融系统，并使其在形式上变得合法化的行为，其过程通常可以被分为以下三个阶段：

一是置入阶段（placement）。即将犯罪活动所得及其收益引入金融系统，尤其是将其注入到合法资金账户的阶段，其形式往往是将大额资金拆分成较小、不太显眼的金额后存入银行账户或用于购买一系列金融工具，然后再将这些资金转移并分配到其他地方账户中。二是分层阶段（layering）。即将资金引入金融系统后将其与来源分开，使

其具有合法外表的阶段，并混淆或打破审计线索。过程往往是购买和出售投资工具进行资金形式转换，或者利用一系列不同银行账户将资金进行汇款。三是整合阶段（integration）。即通过投资将被“洗白”的资金重新引入合法经济，如通过购买合法商业资产或收购可以产生资本收益和股息收入的金融工具进行合法投资。

借助在线服务的广泛使用和可用性，加密货币为犯罪组织提供了一种避免被发现、保持匿名和具有全球影响力的额外方法，从而将传统洗钱带入网络洗钱领域。由于在世界许多地方使用数字前端或空壳公司建立在线身份相对简单，犯罪组织可以在分层过程中建立多个在线账户或空壳公司，将资金分散到各个地点和司法管辖区，然后再通过空壳公司的账户、收入、付款、利润、服务和产品等看起来合法的方式将货币融入到合法的金融体系当中。当然，运用加密货币洗钱也可能比传统的洗钱步骤更少。由于加密货币本身也具有交易媒介和价值存储功能，因此诈骗、勒索、盗窃等财产犯罪也可能直接以加密货币为对象。

作为犯罪收益的加密货币可能只经历分层和整合阶段，甚至可能只存在于分层阶段，从而使此类犯罪的整个洗钱过程都只在加密货币的生态环境范围内进行。但无论是哪种类型，其核心目的都是掩盖以法定货币或加密货币形式体现的犯罪收益之真实性质和来源，即掩盖加密货币产生、交易、兑现过程中相关主体的真实身份，以及加密货币交易的准确路径和数量信息。目前，常见的加密货币洗钱手段有以下形式：

（一）掩盖加密货币交易主体真实身份的洗钱方式

一是参与（投资）加密货币挖矿。根据加密货币产生的基本原理，许多加密货币都是通过“工作证明”挖掘过程创建的。加密货币“矿工”们通过使用计算机解决加密机制中内置的复杂数学问题来验证交易的准确性，然后竞相将交易添加到区块链中，第一个解决该数学问题的矿工将获得系统所新创建的数字加密代币。由于加密货币矿工的身份极为广泛和分散，且往往无需验证购买者的身份，因此洗钱者可以通过将犯罪所得支付给加密货币“矿工”，即购买新产生的加密货币的方式来完成违法资金的置入。

二是通过未经许可、未注册或不符合合法交易所遵循的反洗钱／反恐怖融资（AML/CFT）标准和监管要求的加密货币交易所（市场）交易加密货币交易所（市场）的业务，包括将加密货币兑换成法定货币，将一种形式的加密货币兑换为另一种形式的加密货币，或将其他类型的资产兑换成不同的加密货币，以及进行以上交易的反向操作。洗钱分子往往利用此类交易所不验证客户真实身份的便利来完成犯罪所得与加密货币之间的匿名兑换，即对资金的置入和整合。可以说，加密货币交易所是最容易受到加密货币洗钱交易影响的领域。此外，场外加密货币经纪人（over-the-counter broker）的出现也为洗钱者提供了一个巨大的机会，其中一些加密货币经纪人对遵守反洗钱合规控制和了解客户身份（KYC）流程的遵守程度最低。

三是使用虚拟专用网络（VPN）、代理服务器（Proxy Servers）和洋葱路由器（Tor）等工具来混淆网络协议（IP）地址。通常 IP 地址是加密货币交易中唯一的识别信息，但加密货币用户可以利用 VPN 来掩盖他们的地理位置，营造互联网活动来自不同国家的假象。这既可以为他们提供访问被屏蔽网站的权限，同时也可以阻碍执法部门的互联网

跟踪。同样，寻求更大匿名性的加密货币用户可以使用代理服务器来隐藏他们的 IP 地址。代理服务器可以充当访问特定网站人的中间人，使访问网站看起来是代理 IP 地址，而不是实际用户的真实 IP 地址。至于 Tor 则是一种更复杂、更安全的代理，它使用多个 Tor 节点并同时加密节点间的流量。由于连接的计算机只能检测到前一个节点的 IP 地址，因此该软件可以隐藏原始 IP 地址和后续踪迹。此外，利用 Tor 还可以创建“深度网络”，由只能使用 Tor 浏览器访问的网站组成，近一步加强使用该技术进行加密货币交易用户的匿名性。

四是使用加密货币自动提款机（BTM）。与普通 ATM 机不同，一些针对特定加密货币的自动取款机提供了更大的匿名性。特别是那些具有双向功能的 BTM 可以实现加密货币和传统货币的交换，客户可直接使用移动设备购买或出售加密货币，也可用纸币形式进行交易，为加密货币交换提供了一个易于使用的物理接入点。尽管 BTM 通常也被要求向特定的金融管理机构注册，并遵循相应的反洗钱要求，但一些 BTM 缺乏可靠的高质量客户身份验证，或者没有任何客户身份验证，为犯罪分子洗钱提供了便利。

（二）混淆特定加密货币交易与交易主体之间真实对应关系的主要洗钱方式

一是使用所谓的加密货币搅拌器（mixer）/ 不倒翁（tumbler）。其通过复杂的和半随机的虚拟交易重新安排加密货币的交易路径，并将收入交易与许多其他交易混合，或将特定客户的加密货币分发到属于搅拌器 / 不倒翁中所包含的数十万个钱包中，从而使该加密货币具有更为复杂和不同的交易历史。不倒翁通过将一个钱包地址的加密币与其他钱包地址的加密币混合来切断特定加密货币交易发起者与该笔交易之间的联系，然后将新钱包中的新加密货币提供给所有参与交易的人。这样“干净”的加密货币就将被转移回发送者或新所有者。此外，不倒翁还可随机确定交易量并增加交易时间延迟，甚至将这些服务转移到暗网上匿名运行，进一步增加了加密货币交易的匿名性。

二是使用新型隐私币（privacy coin）。隐私币是一种具有更高级别匿名性的加密货币，它可以加密收件人的公共地址，并通过区块链机制创建虚假地址来混淆真实发件人的信息。例如，当用户发起涉及隐私币的交易时，钱会从原始钱包地址发送到一个新地址，在那里它与来自其他无关钱包地址的交易进行混合，从而无法从这个“被偷的地址”上发现与最初发起交易用户的明显联系。

三是使用多个钱包地址。由于新钱包的创建速度非常快，每个钱包可以为每次交易生成新的公共地址，因此交易者还可以通过使用多个钱包地址获得更大的匿名性。拥有多个钱包地址可以让交易主体在这些钱包之间汇款，而这些钱包之间没有明显联系。因此，即使调查人员确定了其中一个钱包的所有者，他们也不一定能了解其他钱包的所有者的情况，从而无法将交易相互联系起来。

四是使用加密除尘技术。该技术是由加密货币搅拌器或洗钱者向多个加密货币钱包发送少量加密货币，通过给人留下该地址与洗钱有关印象的方法来玷污所有接收加密货币地址的声誉。具有严格反洗钱法规的加密货币交易所将因怀疑其参与非法活动而监控所有这些可能的良性账户。这会影响区块链算法分析工具发现洗钱迹象的能力，从而为实际洗钱活动的发生制造烟幕弹。

二、我国打击加密货币洗钱犯罪所面临的挑战

（一）加密货币的匿名性加大了调查人员准确认定洗钱行为的难度

加密货币网络一般都有隐匿的账户体系，主要通过以下三个措施进行隐私保护或匿名：一是地址生成无需实名认证；二是通过地址不能对应出真实身份；三是同一拥有者的不同账号之间没有直接关联，无法得知特定用户的全部加密货币数量。这一匿名性特征阻断了特定加密货币与犯罪活动和犯罪主体之间的联系，极大地降低了执法机关认定和追踪加密货币交易过程中和交易完成后资金流向的能力，从而无法准确认定特定资金作为犯罪收益的属性，并适用洗钱犯罪罪名对其进行打击。相较于以往的货币置入和整合模式，加密货币和行为人自身的双重匿名性增加了洗钱犯罪的溯源难度。

加密货币采用的分布式账簿设计并不要求其显示交易者和客户的身份信息，也不要求参与者提供用于验证的身份信息，更不会产生与真实身份相关联的交易记录，如果在加密货币和现实货币之间进行相互转换的接口环节缺乏充分适用了解客户真实身份和反洗钱要求的保障机制，洗钱分子可以利用以虚假身份投资“挖矿”、参与未注册的首次代币发行、选择在暗网或未注册的平台进行交易、使用代理服务器、虚拟专用网络、洋葱路由器来掩盖真实网络协议地址、参与在线拍卖和赌博网站、大型多人在线角色扮演游戏，并通过信用卡、预付卡、储值卡（“智能卡”）、移动支付和数字贵金属等各种工具进行价值交换等方式来隐匿在法定货币与加密货币之间进行转换的交易者真实身份，模糊了加密货币资金的真实所有权人和占有权人。加密货币用户还可以使用来自不同加密货币钱包的多个公共地址或连接到开放无线网络内的其他计算机来隐藏自己的身份。而后者尤其令人担忧，因为毫无戒心、不知情的无辜个人可能会被劫持并参与或无意中支持非法通信和活动。

因此即便可以在区块链分布式记账本上查询到特定加密货币的交易记录和流向，也无法将其与现实世界中的特定犯罪及其收益之间建立起对应的联系。另一方面，加密货币搅拌器、不倒翁、新型隐私币、加密货币除尘、闪电网络等新兴技术的出现使得加密货币交易自身的流转过程也变得更为复杂和隐秘，甚至绕过了传统区块链技术可以提供每笔交易的记录和相关数据，并确定交易真实发起人的功能，从而进一步阻碍了在区块链上追踪加密货币的能力，使得对加密资产进行分层变得更为容易。显然，对虚拟货币洗钱的调查复杂且耗时，通常只有拥有最熟练和技术精湛人员的大型调查机构才有能力进行调查并取得一定程度的成功。调查人员必须彻底了解加密货币和区块链技术以及它们支持的复杂交易方法和算法，且还必须跟上加密货币市场不断加快的创新速度。虽然用户的公钥可以通过交易历史记录进行追踪，但与个人相关联的潜在大量公钥的存在只会使调查任务更加复杂。

总体而言，大量使用加密来支持匿名性及其在数字钱包中的应用显著增加了调查人员识别交易参与者的挑战，且这些调查挑战是加密货币和区块链环境所固有的，是打击利用加密货币进行洗钱过程中无法回避，短期内无法一劳永逸彻底解决的障碍，需要长期持续关注和寻求最新的解决办法。

（二）缺乏获取加密货币洗钱犯罪活动线索的常规、稳定渠道

“禁止式”监管模式虽然有利于在一定程度上防范因虚拟货币本身价值的不稳定性、相关交易的不可撤销性所带来的金融风险，但其所依赖的区块链等新兴技术本身却无法，也不应当被彻底禁止，因此实际上无法禁止掌握该种技术的相关个体将虚拟货币作为一种犯罪工具来继续实施逃税、洗钱等犯罪行为。“禁止式”监管模式使得绝大部分希望合法利用区块链、加密货币技术的科技、金融创新者、投资者和金融消费者等合法使用者被与少部分利用加密货币进行违法犯罪活动的违法人员同等对待，不仅扩大了需要由相关国家机关进行打击的人员范围和活动范围，极大地加重了执法机关的办案负担，也使得那些经过长期积累的，已经较为成熟、有效的，利用被监管的合法金融机构自行建立合规体系，主动了解客户信息，及时向监管部门主动报告可疑交易行为的一系列反洗钱措施失去了可以适用的对象。

在失去了可以依靠的日常监管渠道和线索来源的情况下，现有对加密货币的监管措施只能依赖于定期或不定期的运动式打击。但由于那些本来可以作为有效线索来源的普通科技人员、金融从业者和金融投资者因为担心自身行为也可能涉及违法并受到处罚，其主动或积极配合国家执法机关工作的意愿并不强烈，反而加大了有关部分发现、打击加密货币洗钱犯罪活动的难度。在此背景下，对加密货币洗钱活动的打击将不得不更加依赖于刑事司法机关和刑事侦查手段，从而形成以刑事司法机关为主导，以金融监管部门为辅助的治理模式。这种模式既不利于对此类违法犯罪活动“抓早”、“抓小”的源头治理目标，也不利于提高打击效率和节约有限的司法资源，甚至超出了目前阶段部分刑事司法机关在专业知识、技术设备、数据获取渠道等方面的能力，极大地削弱了打击此类犯罪活动的效果。

（三）缺乏打击加密货币洗钱犯罪的明确、健全机制

由于我国已经明确取消了加密货币的合法地位，因此其规制方式必然面临着规范性不足的挑战，进而也给相关司法机关在办案过程中如何适用强制性侦查措施、如何进行合法处置、如何进行跨界执法合作带来了一系列问题。虽然利用加密货币进行洗钱逐渐成为主流趋势，但我国法律还缺乏关于加密货币的明确规定，对于加密货币、虚拟资产等核心概念的内涵和外延也缺乏清晰、权威的定义，使得加密货币应该被界定为去中心化的虚拟货币、特定类型的资本资产、证券、商品，甚至是一种全新的事物还没有权威的定论，进而导致对其监管机构的确定、监管模式、监管手段、交易机制、交易规则等一系列相关问题长期无法得到充分解决。其定性问题上的分歧不但直接导致对加密货币交易所的直接监管机构有所不同，而且将加密货币被归类为证券也会比将其归类为货币导致更为繁琐的规则及更为严格的监管。

虽然我国当前的禁止式监管模式暂时压制了回应此类问题的需求，但也妨碍了国内日常主管部门和正常监管体制的建立，现有各相关部门的职责、权限也得不到科学、合理地划分和调整。由于禁止式监管模式必然会妨碍我国对这一新兴金融产品及相关科学技术的研究和开发，甚至会对相关数字经济、数字产业的发展造成一定的不利影响，未来一旦在某些领域、某种程度上对其重新开放，则当前我国的相关理论研究、规则储备、基础机制等方面显然还没有充分的准备。另一方面，禁止式监管模式并不能杜绝利用加密货币进行洗钱活动的发生。尤其是在跨境洗

钱活动日益增长的形势下，这一模式只能使本已较为混乱、复杂的相关国际执法活动变得更为困难。虽然我国已制定了《中华人民共和国反洗钱法》，并确立了针对金融机构的标准化反洗钱框架，但以加密货币为代表的网络洗钱活动往往并非发生在传统金融机构中，而禁止式监管模式甚至无法将包括加密货币交易平台在内的相关主体纳入到有权参照金融机构采取相应反洗钱措施的主体当中，这就造成境内对利用加密货币进行洗钱活动的控制力进一步下降，对外也无法参与和利用现有国际反洗钱合作机制的困境。

事实上，加密货币本身的多面性已经导致各国对待加密货币的方法大相径庭，大多数关于加密货币和网络洗钱的监管计划和立法政策都已支离破碎，缺乏标准化的反网络洗钱框架已经严重阻碍了我国执法机关和合法利益相关者之间的合作、调查和起诉工作，特别是在涉及跨境、跨司法管辖区的案件中遇到的困境尤为明显。

三、应对加密货币洗钱犯罪的基本思路

（一）加强加密货币与法定货币兑换接口的反洗钱监管

实践中发现，禁止式监管模式下金融机构的“严防死守”并不足以杜绝虚拟资产洗钱，而有效预防和打击与使用加密货币有关的任何非法活动的最相关因素是加密货币和法定货币之间的接口。一方面，加密货币归根结底只是一种用于洗钱的工具，除少数情形之外，绝大多数被用于洗钱的加密货币最终仍然需要被转换为法定货币或在合法市场上进行投资或交易。一旦洗钱资金的“所有者”想要成为合法市场的积极、公开的参与者，有关涉嫌犯罪活动人员的奢侈、不寻常的购买或投资就会引起当局的注意，并可能引发调查以确定资金的来源，因此关照加密货币与实体经济兑换接口的异常交易活动仍然是发现洗钱的重要途径。

另一方面，由于加密货币具有复杂性和分散性，其基本上不受单点故障的影响，对加密货币网络的监管很困难。与其试图控制特定加密货币网络的所有方面，不如通过简化的成本效益分析方法确定哪些方面最适合监管，而最有效和最有希望的则是对加密货币交易所的监管。交易所通过用户信心和交易量获得信誉，如果交易所很少有用户愿意交易，或者交易所不值得信赖，其业务量将受到极大影响。鉴于此，交易所可能不那么分散，因此更容易成为监管对象，而对其的监管也可以最少的资源投入产生最大的效果。域外经验表明一些加密货币交易所已表现出主动性，并根据当前的反洗钱计划注册为需要履行类似于银行反洗钱义务的金融服务机构（MSB）。如果所有加密货币交易所都遵守相关的了解客户及反洗钱法规，那么使用匿名加密货币就不会成为问题，因为任何想要将资金兑换成货币的加密货币用户首先必须说明他们如何获得这些资金，且用户、商家和公司需要说明交易历史才能兑换。

此外，如将记录历史交易过程的义务交给交易所，再由交易所转嫁给用户，那么犯罪分子的交易成本必然会增加，从而降低其洗钱意愿。当然，由于加密货币依赖的是点对点技术，场外交易仍可行，但加密货币的买家将面临难以说明资金来源的困难。由于去中心化交易所没有法定货币网关（fiat gateway），用户需要亲自记录他们的交易过程，以便在将资金兑换为法定货币时向交易所提供此信息。一旦用户想要在中心化交易

所将资金转换为加密货币，他们仍然可能会被要求解释这些资金的来源和交易历史。

因此，未来需要重点监管的是加密货币交易所，而不是加密货币。对法定货币与虚拟货币兑换接口的有效监管或监控将不但有助于增加非法活动的成本，也有利于节约监管成本和执法资源。根据金融行动特别工作组的建议，未来各国反洗钱政策的主要重点应该放在加密货币和法定货币之间的转换上，并暗示所有司法管辖区都应确保加密货币提供商遵守反洗钱法规以及注册和许可，同时将禁止使用匿名交易工具，如搅拌器和不倒翁、隐私币和 VPN，以加强加密货币交易监控。而欧盟在 2018 年推出的关于加密货币监管的《第五条反洗钱指令（5AMLD）》也要求各成员国应在加密货币和法定货币之间的交换服务提供商问题上进行立法。根据该指令对成员国施加的义务，加密货币交易所需要获得许可和注册，同时合法的交易所也被允许访问加密货币地址与加密货币所有者身份的关联信息。

此外，处理无边界、去中心化加密货币在洗钱方面风险的另一种方法是实施全球范围内对下载钱包软件的用户也要履行客户尽职调查（CDD）监管。由于钱包是参与去中心化加密货币系统的先决条件，从技术上讲，其对于通过网络接收和发送交易是必不可少的。如果下载钱包软件也需履行了解客户流程，则会建立单一的可观察法定货币和加密货币兑换的出口点，以及去中心化系统中现实世界身份和加密货币账户之间的联系。当然，对加密货币的钱包下载实施强制性身份识别会与加密货币系统的开源特性及其与排除中央权力监管和影响的价值观和目标之间具有天然的矛盾，因此其落实会很困难，但如果采用由国家建设，私人购买并经许可使用系统的方式，实现这种监管也是可行的。

（二）加强技术手段开发，破解加密货币洗钱过程中的匿名性难题

与传统的货币转移相比，加密货币没有实物材料可供观察或拦截以证明非法活动，从而给相应的反洗钱工作增加了另一层复杂性。如果不能有效破解加密货币洗钱的匿名性难题，仍会导致对洗钱犯罪过程证明链条的中断，无法实现在司法层面上对此类犯罪的有效打击。由于缺乏必要的技术手段和知识储备，目前我国实践中对运用加密货币洗钱的证明还主要依赖于被追诉人的自我供述，因此与立法上所要求的核心待证事实要有不同来源的证据相互印证、达到超过合理怀疑的证明标准还有一定的差距。

随着技术的不断更新，如何破解因搅拌器、隐私币等新型匿名技术所带来的交易主体、金额、路径等犯罪核心事实的同一认定难题只能通过开发相应的识别技术来加以应对，并需要将法律、金融等行业知识与区块链、人工智能、大数据分析等相关科技知识进行有效融合。反加密货币洗钱的技术手段将涵盖从洗钱模型的构建、神经网络的应用、可视化分析方法的开发到人工智能技术的利用等多个方面，同时也包括对混合服务的预防和穿透交易匿名化的追踪等策略，但以下几个方面仍应当成为基本的发展方向：

1．提升跟踪 IP 地址技术

即使非法行为者会使用洋葱路由器这样的隐私保护应用程序来进行交易，仍可能部分跟踪到交易者的 IP 地址。如已经存在一些如 ExoneraTOR 这样的收费工具，它保留了过去和当前使用洋葱路由器进行网络链接的 IP 地址数据库，并允许发现特定 IP 地址是否在特定日期使用了洋葱路由器中转。即使原始 IP 地址仍然无法发现，执法部分也

可以查看正在调查的可疑 IP 地址是否与工具出口中继列表中列出的任何 IP 地址匹配，从而增加实现同一身份认定的能力。

一般来说，追踪 IP 地址的方式主要适用于洗钱者在使用隐私保护工具时缺乏经验，并在使用过程中犯错误的情况，例如浏览器插件安装不当、使用 HTTP 上的明文、允许 cookie 或运行某些类型的应用程序，生成未隐藏或未报告的网络流量等，这些可能发生的技术故障恰恰可以通过计算机取证方法被用来发现个人身份。

2．结合大数据和人工智能技术进行区块链分析

人工智能和洗钱算法可以分析大量交易数据并识别洗钱的模式，并自动标记可疑活动、检测异常并生成警报，而大数据分析则是利用先进的分析技术来处理和分析大量结构化和非结构化数据，通过检查金融交易、社交媒体和在线平台上的各种数据源来识别可疑交易模式，并发现可能表明洗钱活动的隐藏联系，这些技术都可以与区块链技术进行结合来协助金融机构和执法机构检测和防止数字洗钱。由于各种加密货币都使用区块链技术作为交易的公共账本，而其分布式特性使得几乎不可能在不产生高成本的情况下操纵区块链中包含的数据，因此人们高度相信存储在区块链中的数据没有改变。针对区块链交易具有的可追溯、不可变和不可逆的特点，执法机关可以充分利用区块链及其交易历史记录来调查非法活动或推断用户之间的社会关系，如使用 blockchain. info 等工具检查区块链，并验证特定公钥是否批准了某些交易或 IP 地址。

为此，必须使用广泛的数据挖掘和定性及定量分析来检查区块链交易，通过仔细检查区块链的过去和现在的交易数据来建立不可变的审计线索，并推断出基本信息和重要模式，从而实现用户 IP 地址或交易的去匿名化。此外，在支付过程中可以加大对公钥执行行为的分析广度和深度，通过将特定公钥与交易关联，发掘跨数据集和网络的公钥与交易之间的对应关系，从而允许对行为模式进行集群映射。这些追踪模式可以形成关于用户购物和消费习惯以及交易频率的图像，甚至可以识别地理位置，并最终发现特定的网络用户。

3．采用数字身份验证解决方案

尽管域外大规模和规范的加密货币交易所已经开始要求提供用户的详细信息来进行账户验证，但洗钱者的个人身份仍然可能通过使用有清白记录的中介机构来屏蔽，甚至还存在着暗网等领域内的交易经过验证的个人账户的在线市场，这些都威胁着对加密货币用户身份验证的准确性。此外，数字身份盗窃涉及窃取个人信息并使用它来创建欺诈性身份，洗钱者也可以利用这些合成身份开设银行账户、建立空壳公司并进行交易，这使得追踪非法资金的来源变得十分困难。以上难题只能通过实施安全高效的数字身份验证工具来解决，以加强客户尽职调查并防止身份盗窃。总体来看，数字身份验证工具、生物特征认证和数据分析等方案可以实现更为强大的加密货币用户身份识别程序，从而使洗钱者更难伪造身份并进行非法交易。

（三）构建更为有效的监管合作框架

加密货币洗钱活动的去中心化、跨境化特点必然要求有更多的主体共同合作才能更为及时、有效地发现和打击此类犯罪，并通过随时吸收和分享更为先进、及时的科学技术、规范流程、经验措施、案件信息来更好地应对技术进步所带来的挑战。总体来看，要想构建更为有效的加密货币洗钱监管框

架，其内容应该至少包括以下关键方面：

一是制定适用于传统和数字金融服务的明确和全面的反洗钱法规，以涵盖虚拟货币、在线支付系统和用于金融交易的其他新兴技术，搭建健全和标准化的技术监管框架。二是加强国际合作和信息共享，使执法机构、金融情报部门和监管机构之间的合作信息、情报和最佳实践的交流成为可能，提高反洗钱工作的有效性。三是加强金融机构与执法部门之间的合作和公私伙伴关系。金融机构、执法机构和监管机构之间的合作对于共享与可疑活动有关的信息和情报至关重要，建立开放的沟通和信息交换渠道可以显著提高反洗钱工作的有效性。四是搭建识别和获取受益所有权信息合作机制。洗钱者经常利用不透明的公司载体来隐瞒犯罪所得并将其重新注入金融体系，因此建立一个广泛的、跨国的、基于区块链的分布式数据库，汇总可靠、可验证的公司所有权结构信息，将有助于执法机构和税务机关识别责任人和最终受益人。区块链技术在洗钱领域的有效应用不仅应包括能够提供跨部门和跨国家的必要透明度和协作的可靠交易处理数据库，还应该包括在国际背景下实现有益的所有权的可靠注册中心。

参考文献：

[1]The Financial Action Task Force (FATF) .Virtual Currencies: Key Definitions and Potential AML/CFT Risks.2019.3

[2]Jake Frankenfield.“Cryptocurrency”.Investopedia.2021.5

[3]Michael W. Calafos, George Dimitoglou, Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency. Principles and Practice of Blockchains.2022

[4]Ana Alexandre. “Cyber Criminals Netted $4.3B from Crypto-Related Crime in 2019: Study”. Cointelegraph.2019.8

[5]柯达．虚拟货币“禁止式”监管：法理反思与制度优化[J]．华东政法大学学报．2024．3

[6]“Bitcoin Money Laundering: How Criminals Use Crypto (and How MSBs Can Clean Up their Act)”. Elliptic(blog).2019.9

[7]R. van Wegberg, J.-J. Oerlemans, and O. van Deventer. “Bitcoin money laundering: mixed results? An explorative study on money.laundering of cybercrime proceeds using bitcoin” Journal of Financial Crime.2018.3

[8]Edited by Deborah R. Meshulam and Michael Fluhr. Cryptocurrency and Digital Asset Regulation.American Bar Association.2022

[9]Risk and Vulnerabilities of Virtual Currency Cryptocurrency as a Payment Mothod. 2017 Public-Private Analytic Exchange Program

[10]Jake, Crypto Dusting Is a New Type of Blockchain Spam that Corrodes Reputations and Impacts Cryptocurrency AML. CipherTrace.2018.12

[11]赵炳昊．数字时代加密货币洗钱犯罪的防治 [J]．中国刑事法杂志．2022

[12]王若平．虚拟货币洗钱问题的监管研究 [J]．北方金融．2018．7

[13]Ola M. Tucker.The Flow of Illicit Funds. A Case Study Approach to Anti-Money Laundering Compliance, Georgetown University Press.2022

[14]J. B. a. Sykes, Virtual currencies and money laundering: legal background.enforcement actions.and legislative proposals. Congressional Research Service.2018

[15]The Money Laundering Market : Regulating the Criminal Economy.edited by Killian J. McCarthy. Agenda Publishing. 2018

[16]Edited by Killian J. McCarthy.The Money Laundering Market : Regulating the Criminal Economy.Agenda Publishing.2018

[17]Keidar. R. “ e key to overcoming the AML challenge in crypto-currency”. 2017

[18]Michael W. Calafos, George Dimitoglou.Cyber Laundering: Money Laundering from Fiat Money to Cryptocurrency. Principles and Practice of Blockchains. 2022

[19]Brantly. A. F.Money Laundering and Digital Identity Theft. In A. F. Brantly (Ed.).Identity Theft Handbook: Detection. Prevention, and Security.3. 2018

[20]Wirtschaftsuniversität Wien Global Tax Policy Center (WUGTPC) . “Blockchain 101 for governments: a note prepared for the Committee of Experts on International Cooperation in Tax Matters”. 2017

责任编辑 韩笑尘