技术原理与溯因归责:区块链洗钱犯罪的刑事治理

付玉明　李　想*

内容摘要　区块链技术为洗钱犯罪提供了隐蔽的技术支撑,也加剧了犯罪行为的复杂性。利用虚拟货币实施的洗钱活动已突破传统金融监管框架,呈现技术驱动、跨国协作及产业链条化等特征。区块链洗钱引发的刑事归责与监管困境包括:一、匿名性导致共同犯罪"意思联络"难以认定;二、现行法律对区块链洗钱行为的界定滞后与法益争议;三、跨境管辖权冲突与监管技术不足制约执法效能。为此,应当完善专项立法以明确区块链的"特定非金融机构"属性,并扩展洗钱罪上游犯罪的范围;引入片面共犯理论解决技术帮助行为的归责难题;通过分级属地管辖与跨境数据协作优化刑事管辖权适用。同时,建议构建多部门协同治理机制,强化区块链交易的身份溯源与智能合约合规审查,借助大数据技术实现全链条精准打击。

关键词　区块链技术　虚拟货币　洗钱罪　共同犯罪　刑事管辖权

在当前数字化时代,随着互联网技术的普及和高质量发展,人们生活水平不断提升的同时,传统的洗钱犯罪也在朝着新型的高科技犯罪方向演进。常见的互联网洗钱渠道有:网上银行、第三方/第四方支付平台、网络赌博、电商平台交易、虚拟货币、网络赌博、P2P 网络借贷、网络集资洗钱、网络炒汇炒金、网络传销、网络非法股权融资等。而区块链技术作为一种去中心化、安全可信的分布式账本系统,已经在各个领域展现出巨大的潜力和影响力,正因如此,随着其应用范围的不断扩大,区块链技术被犯罪分子逐渐发展成高效隐蔽的作案工具,在互联网洗钱犯罪中发挥作用。

一、问题提出:区块链洗钱对传统犯罪的冲击

洗钱犯罪作为一种严重的跨国犯罪行为,通过将非法获得的资金运用一系列复杂的交易和支付手段,使其表面上看起来具有合法性,以此来掩盖资金的真实来源。而区块链技术所具有的匿名性、不可篡改性和跨境性等诸特性,使其成为洗钱犯罪分子的理想犯罪工具之一。最为典型的案例便是 Silk Road(丝绸之路)案件。① Silk Road 是一个匿名的暗网市场,在 Tor 网络运作上,允许用户匿名购买和出售各种非法商品和服务,包括毒品、假币、假证件、黑客工具等。Silk Road 之所以备受关注,是因为它的商业模式和技术手段使得参与者在进行非法交易时几乎可以完全匿名。用户可以通过 Tor 网络访问

* 付玉明,西北政法大学刑事法学院教授、博士生导师,刑事法律科学研究中心主任;李想,西北政法大学刑事法学院博士研究生,刑事法律科学研究中心助理研究员。

① US v. Ulbricht, 31 F. Supp. 3d 540－Dist. Court, SD New York 2014－Google Scholar.

Silk Road，并使用比特币进行交易，而 Tor 网络和比特币均具有匿名性和隐私性，使得用户的身份和交易记录难以被追踪。这种匿名性使得 Silk Road 很快成为吸引全球黑市交易的中心之一。美国联邦调查局（FBI）于 2013 年展开对 Silk Road 的调查，并于同年 10 月关闭了该网站，该网站创始人被控多项罪名，包括洗钱、贩卖毒品、计算机黑客入侵等。在调查过程中，FBI 揭露了 Silk Road 网站的庞大规模和背后的犯罪网络。据估计，Silk Road 网站每天的交易额达到数百万美元，涉及数万名用户。网站的营业额被认为高达数十亿美元，使其成为当时最大的暗网市场之一。Silk Road 案件也成为区块链技术在黑市交易和洗钱方面的一个典型案例。尽管区块链技术本身具有许多优势，如去中心化、安全可信等，② 但它也为洗钱犯罪提供了便利条件，需要加强监管和防范措施以确保技术的合法良性使用。

国内也有许多关于利用虚拟货币进行洗钱犯罪的案例。例如，在崔某、杨某强走私、贩卖、运输、制造毒品案③中，崔某多次使用网络虚拟货币比特币进行毒品交易，后将毒资比特币转换成人民币加以使用的行为。在胡某颖、李某德等洗钱案④中，被告人提供资金账户并通过购买加密数字货币等方式协助资金转移。以及在雷某洗钱案、陈某洗钱案、谭某洗钱案、陈某某洗钱案、施某君洗钱案等案件中，所涉及的都是相关被告人利用虚拟货币转移资金或犯罪所得的行为。⑤ 同时，在薛某开设赌场案、杨某掩饰、隐瞒犯罪所得案、邓某掩饰、隐瞒犯罪所得案等案件⑥中，虽然法院并未认定被告人构成洗钱罪，但被告人无一例外都通过区块链技术进行了资金转移的行为。由此可见，在国内，传统的洗钱犯罪也在受到新型技术带来的挑战和冲击，利用虚拟货币进行洗钱的犯罪方式愈发成为洗钱罪的主要形式，随着区块链技术的逐渐完善，犯罪分子通过区块链实施洗钱活动将会成为当下亟须解决的实务难题。

如何有效治理区块链洗钱犯罪成为当今亟须解决的重要问题。首先，区块链技术作为新型高科技手段，普遍民众缺乏直观了解，没有对区块链技术产生全面认知和深入运用，对于区块链技术的底层逻辑和特性也没有做到完全掌握，从而无法剖析区块链技术如何被洗钱犯罪分子利用。其次，区块链洗钱犯罪中关于共同犯罪的认定存在界定盲区，当行为人通过具有匿名性和跨境性的区块链进行洗钱交易时，是否能被认定为具有“意思通谋”还有待商榷。再次，我国司法体系中对于区块链洗钱犯罪没有明确的界定，法律法规存在一定的滞后性，洗钱罪所保护的法益亦需要进一步厘清，不同法域中针对虚拟货币的相关条文也不能很好地覆盖区块链这种新兴技术，包括对刑事管辖权的冲击，区块链的跨境性导致管辖权在实践中适用艰难。最后，执法部门应当审视当前法律法规对区块链洗钱犯罪的监管漏洞，区块链技术使跨国境的洗钱犯罪更加具备隐蔽性和匿名性，现有的侦查技术不足以应对最新的洗钱手段，这不仅涉及技术层面的创新和完善，更需要跨国合作、政策法规的制定和执行以及社会各界的共同努力。

② 参见张淑芳、肖峰：《数字治理视野下的软法及其功能变迁》，载《法治现代化研究》2025 年第 3 期，第 133 页。

③ 参见辽宁省辽阳市中级人民法院（2022）辽 10 刑终 182 号刑事判决书。

④ 参见江苏省苏州市吴中区人民法院（2020）苏 0506 刑初 579 号刑事判决书。

⑤ 参见江苏省扬州市江都区人民法院（2023）苏 1012 刑初 523 号刑事判决书；上海市宝山区人民法院（2023）沪 0113 刑初 573 号刑事判决书；四川省天全县人民法院（2020）川 1825 刑初 71 号刑事判决书；上海市浦东新区人民法院（2019）沪 0115 刑初 4419 号刑事判决书；浙江省杭州市富阳区人民法院（2019）浙 0111 刑初 438 号刑事判决书。

⑥ 参见河南省新密市人民法院（2023）豫 0183 刑初 689 号刑事判决书；山东省海阳市人民法院（2023）鲁 0687 刑初 259 号刑事判决书；陕西省靖边县人民法院（2021）陕 0824 刑初 249 号刑事判决书。

二、区块链洗钱的技术原理

(一) 区块链技术的底层逻辑和应用特点

区块链是一种分布式数据库技术,它通过多个节点之间的协作来存储和管理数据,其核心思想是将数据分割成块,然后链接这些块形成一个不断增长的链式结构。区块链的概念体系于2008年由中本聪(Satoshi Nakamoto)提出(他也是比特币的创始人),区块链具备完整的运行机制,主要包括分类账、共识机制、智能合约等机制,其技术架构系统划分为基础设施、基础组件、账本、共识、智能合约、接口、应用、操作运维和系统管理等九个部分,这九个部分发挥着为上层提供物理资源、计算驱动,为网络提供通信机制、数据和密码库等功能。⑦ 区块链技术的核心特征包括:去中心化、匿名性、不可篡改性、智能合约、加密算法等。

1. 去中心化

区块链的去中心化,是指在整个系统中没有一个单一的中心权威或控制点,其运行的权力和决策是分布在网络的多个节点之间的,这也是比特币底层技术中最主要的特征。区块链的去中心化始于其分布式节点网络,在传统的中心化系统中,数据通常存储在单一实体的服务器或数据中心中,由该实体进行管理和控制,区块链通过将网络分布到众多节点,每个节点都拥有一份完整的账本,从而消除了中心化的单一控制点,每个节点都参与到网络中,通过点对点的连接进行通信。这种网络结构的优势在于,即使部分节点发生故障或受到攻击,整个系统依然能够正常运行。节点之间通过共识机制协调一致,保持账本的同步和一致性。区块链网络采用对等网络结构,每个节点都是平等的,没有特权节点,所有节点都能够参与交易验证和区块生成的过程,共同维护整个网络的稳定性和一致性。对等网络结构消除了单一中央实体对系统的控制,使得网络更为分散和自主。与传统货币相比,去中心化的特点主要体现在没有货币的中央发行机构,基于节点之间的相互对接,资金通过网络协议直接实现各个节点的交互,资金不再需要中央发行机构和中央服务器等第三方接手,交易也不再受专门机构监管和负责,与传统的中心化金融模式形成鲜明的对比。

2. 匿名性和透明度

区块链具备先进的加密技术,确保了交易的安全性和参与者的匿名性,每个参与者在网络中有一个唯一的身份标识,通过公钥和私钥的组合,实现对身份信息的加密和解密,从而在网络上进行交易不会暴露个人身份。同时,区块链上的交易是通过智能合约进行的,不需要中介机构的干预,大大降低了用户被追踪的可能性。虽然交易平台上的信息是公开的,但不同节点和个体用户却很难联系到一起,而且还存在用户个体修改网络地址的可能性。一些区块链项目通过引入匿名货币(门罗币和黑暗币)和混币技术进一步提升匿名性,其中匿名货币使用零知识证明等技术确保交易的隐私性,混币技术通过混淆交易路径,使得交易更难被追踪。

区块链的透明度,首先体现在分布式账本上,每笔交易都会被记录在一个区块中,当各个区块链接在一起时会形成不可篡改的链条,确保所有参与者都能够查看和验证交易的发生。其次,智能合约是区块链的重要组成部分,智能合约的代码也是公开可见的,任何人都可以审查,这种开放性保障了合约的透明

⑦ 参见张莉莉等:《"区块链"技术下洗钱类犯罪治理机制建设》,载《广州市公安管理干部学院学报》2022年第1期,第35页。

度，确保了合约的执行是公平和可验证的。最后，区块链上的交易是实时更新的，所有参与者都可以随时查看最新的交易信息，大大提高了区块链货币交易的透明度。

3. 加密算法与不可篡改性

区块链使用多种加密算法来确保数据的机密性和完整性，其中最常见的是哈希函数、非对称加密和对称加密。哈希函数是将任意长度的输入数据转换为固定长度的输出值算法，每个区块中都包含前一区块的哈希值，其哈希值就是由该区块的数据和前一区块的哈希值计算而得。这种单向哈希关系使得修改一个区块的数据会导致整个链的哈希值发生变化，因此任何篡改都会被迅速检测到，从而确保区块链上的数据不可被篡改。区块链中一般使用非对称加密算法来管理数字签名和密钥对。每个用户都有一对公钥和私钥，公钥用于加密信息，而私钥用于解密。数字签名则是通过私钥对数据进行加密生成，其他用户可以使用对应的公钥来验证签名的有效性。⑧ 这确保了只有持有正确私钥的用户才能对区块链进行操作，保护了数据的安全性。对称加密算法是使用相同的密钥来进行加密和解密。在区块链中，对称加密通常用于加密数据的传输过程，以确保数据在传输过程中不被窃取或篡改，虽然对称加密速度较快，但由于密钥的安全传输和管理问题，一般与非对称加密结合使用。

区块链的不可篡改性，是指一旦数据被写入区块链，就很难修改或者删除，其主要由加密算法和共识机制保障。首先，哈希函数是不可逆的，即无法从哈希值还原出原始数据。这意味着一旦数据被哈希后写入区块链，就无法通过哈希值逆向推导出原始数据，这种不可逆性保障了数据的不可篡改性。区块链通过共识机制确保所有节点对于区块链的状态达成一致。常见的共识机制包括工作量证明(PoW)和权益证明(PoS)。在这些机制中，节点需要通过一定的算法验证新区块的合法性，然后通过竞争或者按照拥有的权益进行添加，只有通过共识的区块才能被添加到链上，这样就防止了恶意节点的篡改行为。

4. 可兑换性与跨境性

可兑换性是指不同的区块链网络之间能够交互和合作的能力。在传统的区块链系统中，由于采用不同的共识机制、加密算法、智能合约语言等，导致不同区块链之间存在着一定的隔阂。为了实现区块链网络之间的可兑换性，业界逐渐形成了一些标准化的协议和接口。其主要在于允许不同的支付网络互相连接，实现跨链支付，或者允许不同区块链上的数字资产直接进行兑换，而无须通过中介。可兑换性还体现在智能合约方面，智能合约是区块链中的自动化执行代码，跨链智能合约则允许在不同区块链上执行，这意味着可以通过智能合约实现跨链资产的锁定、解锁和转移，从而实现不同区块链上的资产互通。与传统货币相比，虚拟货币可以实现全球范围内自由流通，不受地域的、中央的控制，并且虚拟货币之间、虚拟货币与传统货币之间都可以自由兑换结算。

传统的跨境交易通常需要多个中介、复杂的结算过程和高昂的手续费。区块链通过去中心化和智能合约的特性，可以实现实时、透明、低成本的跨境交易，并且能够促进缺乏传统金融服务的地区更容易地接入全球金融系统，由此可见，区块链技术支持的虚拟货币交易打破了地理位置的限制，用户群体和账户都分散在世界各地，为跨境洗钱犯罪提供了极大的便利。

(二) 区块链洗钱的常见类型

区块链洗钱犯罪主要依靠加密货币开展，其具有去中心化、匿名性、可兑换性、跨境性等特点，区块链技术为洗钱犯罪提供了高效、隐秘、安全的环境，同时也为洗钱犯罪创造了多种多样的行为手段。

⑧ 参见[美]布莱恩·S. 哈尼：《区块链：后量子安全与法律经济学》，杨安卓、吴媛译，载《法治现代化研究》2022 年第 5 期，第 182 页。

1. 代买虚拟货币

代买虚拟货币属于最为常见的区块链洗钱犯罪手段,指的是犯罪分子通过组织大量的"币农"购买虚拟货币来达到将赃款洗白的目的。首先,犯罪组织通过委托或者招募的方式,组织大量的"币农";其次,通过注册或者购买他人身份信息的方式,产生大量的虚拟货币交易账户;随后,"币农"利用这些账户用需要洗白的赃款购买虚拟货币,再将这些虚拟货币打散,在不同交易所之间反复转移,以实现赃款在多个账户间的分散和交换;最后,"币农"将反复转移的虚拟货币转入到犯罪组织指定的地址,犯罪组织再通过欠缺监管的小型交易所或场外的承兑商,将虚拟货币兑换为现金完成洗钱行为。

2. 混币平台洗钱

混币平台是一种提供加密货币混合服务的在线平台,这类服务旨在增强用户对数字货币交易的隐私性,通过混合或混淆交易记录,使得这些记录难以追踪到特定的发件人或接收者。基本上,混币服务通过将来自多个用户的加密货币合并在一起,然后再重新分发给这些用户,以使得整个过程更难以被监测和分析。这样的服务通常用于提高数字货币交易的匿名性,犯罪组织充分利用混币平台的隐蔽性,将赃款(虚拟货币)转移到混币平台,再通过平台自身的混合和混淆,最后兑换成已经洗白的虚拟货币或现金。

3. 跑分洗钱

跑分洗钱是指利用信用卡或其他支付方式,在虚构或合法的方式下进行多次交易,目的是将非法获得的资金转移到合法的经济系统中,以掩盖其非法来源。这种行为的目标是混淆资金流动路径,使其难以被追踪,从而使犯罪分子能够在经济系统中洗白其非法所得。犯罪组织通常会通过虚构的交易来创建看似合法的资金流动,包括虚构的购物、服务支付或其他类型的交易。为了不引起注意,犯罪组织往往会选择多次多个账户的小额交易,并且还会利用合法的商户进行跑分洗钱活动。典型的虚拟货币跑分就是"USDT(泰达币)跑分",即以稳定币 USDT 为跑分媒介,跑分参与者到跑分平台购入泰达币作为保证金,参与跑分抢单。因为 USDT 跑分平台在收取抵押的 USDT 币后极容易演变为资金盘,时机不对就携币撤离,所以实践中,更多的是代买形式的非典型性跑分。⑨

4. 通过专门网站和平台洗钱

目前犯罪组织常用的洗钱网站主要是暗网(Dark Web)和各类赌博网站。通过暗网进行洗钱是指利用暗网平台的匿名化技术,以隐藏身份并进行非法资金交易的行为。暗网是互联网的一部分,但其内容不被传统搜索引擎所索引,用户需要特定的软件或访问协议(如 Tor 网络)才能访问。由于暗网独特的匿名性和隐秘性,犯罪组织直接在暗网上交易赃款和虚拟货币,可以绕过虚拟货币交易所,免去洗白的步骤,实现赃款持有者和虚拟货币持有者的单独交易,从而达成销赃的效果,以规避法律和执法机构的监控。随着虚拟货币流通的盛行,全球多数赌博网站已经允许用加密货币当作赌资,这类赌博网站属于监管的灰色地带,大多都不要求用户进行实名注册,犯罪组织注册成为赌博网站的会员,将赃款转入会员账户中,通过多次小额的参与赌博活动,在不涉及 KYC(Know Your Customer)环节的情况下,完成赃款洗白为赌博收益的目的。

5. 其他快速洗钱手段

除了以上常见的区块链洗钱手段外,还存在一些其他快速洗钱的方式。比如,利用虚拟货币"搬砖套利"洗钱,是指通过在不同交易平台或市场上迅速买卖数字资产,因为不同平台的数字资产存在价格差异,从而利用平台差价获利,这一过程涉及将数字资产快速移动,被犯罪组织滥用以掩盖非法来源资金。此外,犯罪组织还会利用 NFT(Non-Fungible Token),即非同质化代币进行快速洗钱。其原理在于犯罪

⑨ 参见邓宁江:《虚拟货币洗钱犯罪分析及治理对策研究》,载《北京警察学院学报》2023 年第 6 期,第 6 页。

分子创建大量虚假的 NFT 项目，然后通过内部交易方式来转移非法资金，达到快速洗钱目的。再比如，利用 DeFi(Decentralized Finance)，即去中心化金融的方式洗钱，犯罪组织通过 DeFi 领域内基于区块链搭建的众多贷款平台，可以在不涉及中心化授权的情况下，极短时间内借出大量资金，然后进行复杂操作后，再迅速偿还贷款完成洗钱的过程。

三、区块链洗钱的治理困境

在数字时代之前，侦查机关通过对金融、证券、会计等行业的监管和约束能够较为有效地打击洗钱犯罪，但随着区块链技术日新月异的变化和虚拟货币形式多样的广泛应用，犯罪组织洗钱犯罪的手段进一步升级。犯罪组织依靠区块链技术的去中心化、匿名性、加密算法、跨境性等特点，实施区块链洗钱犯罪，在极大提升洗钱效率和降低成本的同时，还能更容易地规避司法机关监管的风险。由此可见，区块链洗钱犯罪作为新兴犯罪手段，已然成为国家打击洗钱犯罪的最大挑战，司法机关和侦查机关需要调整现有法律规范和改进传统侦查手段，才能充分迎接区块链洗钱犯罪对我国司法体系和金融市场的风险冲击。

(一) 洗钱罪在区块链技术下的演变

1. 匿名性和隐蔽性的挑战

在数字时代背景下，互联网支付功能并未完全实名制，仍然是通过密钥、数字签名、电子证书等方式进行核验确认，其中以区块链上的交易方式最为复杂和隐蔽。区块链具备先进的加密技术，交易都是通过密码学技术实现的，这种方式只能核实用户的私钥身份和交易金额，无法核实交易资金的属性和来源，犯罪组织只需要具备相应的私钥就可以完成交易，不需要再提供个人身份信息，充分隐匿了交易用户的个人信息资料，同时区块链上的交易是通过智能合约进行的，又排除了中介机构的干预和追踪。与线下洗钱相比，区块链上进行洗钱不需要经过各类人员的层层询问，也不需要使用现有金融体系中的工具，从而可以规避金融体系中的监管机构。

区块链上的交易主要是通过虚拟货币实现的，犯罪组织往往为了更好地不被侦查机关追踪，在一般虚拟货币的基础上采用了隐蔽性更强的匿名货币，匿名货币的设计初衷就是为了提供更高程度的用户匿名性，这类货币通常采用特殊的隐私保护技术，确保用户在进行交易时更难被关联到具体身份。比如区块链交易中最常用的比特币，是将代码数据作为数字签名，再将该数字签名隐藏从而达到匿名的作用，但目前侦查机关通过技术解密已经可以追踪到交易方的具体信息，而匿名货币则是在虚拟货币匿名化的基础上采用了一些隐私保护技术，这些技术可以使得交易参与者能够在交易中证明某个事实而不需要透露具体信息，与传统洗钱犯罪相比，犯罪组织可以在交易时不用担心身份泄露从而完成洗钱活动，为侦查机关的追踪工作带来极大的挑战和困扰。

2. 去中心化的风险

传统洗钱犯罪常常因某一笔交易被侦查人员查获从而牵扯出整个洗钱犯罪团伙，但犯罪组织通过区块链进行洗钱活动就能避免这种情况的发生，即使某一节点上的交易被追踪或查处，也能保证其他节点上的洗钱活动顺利完成。区块链交易去中心化的设计避免了传统监管模式的数据整合处理分析，政府的监管体系无法及时对发生交易的区块链节点进行识别和分析，从而使洗钱行为逃避政府监管。

去中心化的另一特点就是虚拟货币没有中央发行机构，不受相关机构的监督和保护。传统洗钱犯罪常不能避免与银行打交道，在洗钱过程中需要想尽办法逃避中央发行机构和银监会的监管，侦查机关只

需将金融机构或第三方支付单位纳入司法监管网络即可掌握资金链流向。[10] 但犯罪组织通过区块链洗钱可以直接实现各个节点上的资金流通，基于各个节点的单独交互，赃款不需要再经过中央发行机构和相关第三方机构的接手，可以轻松绕开专门监管机构的监督。

3．智能合约的潜在滥用

智能合约是区块链交易中基于区块链技术的自动执行合约程序，其执行依赖于预先定义的规则和条件，本质上是为了应对区块链上烦琐的密码学技术和各节点中庞大的资金流通，为区块链交易提供便捷的服务功能，但其潜在漏洞也被犯罪组织所利用，比如犯罪组织通过创建匿名合约、利用技术手段隐匿智能合约中的地址信息或使用匿名货币的地址，确保交易不被跟踪，同时犯罪组织为了不泄露私钥信息会采用匿名私钥的形式为智能合约签名，包括在匿名合约中引入多个交易和地址提高交易的混淆度，并且设计多层结构的匿名合约使得每一层都执行不同的逻辑和操作，从而增加整个交易过程的复杂性，以规避追踪路径的作用。

除了创建匿名合约外，犯罪组织还会在智能合约中用到一些隐私保护技术，比如匿名货币常用的零知识证明技术，通过该技术，在不需要透露具体信息的情况下证明某些陈述为真，确保交易条件的成立而不揭示相关具体数据；再比如在智能合约中使用环签名方式，即某一签名者的身份被隐藏在一个签名者的集合中，从而无法确定具体签署者实现交易的匿名性；犯罪组织在设计智能合约时还可以选择以接受匿名货币作为支付，以增强交易的匿名性，使监管机构更难追踪资金流动。

（二）区块链洗钱罪共同犯罪归责问题

我国《刑法》第25条规定，“共同犯罪是指二人以上共同故意犯罪”。共同故意，是指行为人之间对共同实施的犯罪进行沟通谋划，共同参与该犯罪的行为人具备意思联络，意思联络一直被视作二人以上犯罪故意得以有机统一的纽带以及认定共同故意的前提。[11] 由于区块链技术的匿名性与去中心化，区块链通过公私钥加密机制和分布式账本技术，导致交易双方身份难以追溯，比如利用混币的方式，可以将赃款分散至多个匿名钱包，达到切断赃款流向的关联性，购买者极有可能出现不知道所购资产为洗钱所得的情况，即缺乏主观上的认知；而即便购买者在客观上将资产变现帮助了洗钱活动，但二人因网络空间的匿名性和距离性，比如“矿工”“交易所”这些区块链的参与者，通常与洗钱正犯无直接沟通，其“矿工”处理涉及混币服务的交易或“交易所”验证交易的技术行为在无意中协助洗钱，但主观上无法识别资金来源，并无共同故意的意思联络，不能被认定为共同犯罪。并且，单纯的购买行为，比如正常交易虚拟货币，通常不构成“掩饰、隐瞒犯罪所得”的客观行为。故而，按照传统的共犯理论，难以认定区块链洗钱共同犯罪的成立，但如此处置在实务中必然会产生打击犯罪的漏洞，大量区块链技术帮助行为得以脱罪，导致刑法法益保护功能虚化，不利于网络洗钱犯罪的整治。

当前学界的通说虽不承认片面共犯，但仍存在例外情形，即若购买者明知行为人是利用其进行洗钱交易，仍然配合完成交易，则存在认定为片面共犯的空间。片面正犯需要行为人明知他人正在实施犯罪，并单方面提供帮助或促成犯罪结果，而被帮助者对此不知情。那么，在区块链洗钱犯罪中，比如，区块链网络中去中心化交易所的智能合约会自动执行洗钱交易，其开发者和使用者是否能构成片面帮助犯？在智能合约驱动的洗钱场景中，犯罪行为的实施主体可能完全由代码执行，赃款转入智能合约后，按预设比

⑩ 参见王熠：《论匿名货币洗钱模式的刑法规制——以区块链技术的结构特征为导向》，载《安徽行政学院学报》2019年第6期，第96页。

⑪ 参见陈兴良：《共同犯罪论》，中国人民大学出版社2023年版，第309－310页。

例自动拆分至多个匿名钱包，此时开发者编写代码的行为是否构成帮助行为？若代码被滥用，开发者是否因“技术预见可能性”而承担片面共犯责任？可见，即使采取片面共犯理论规制洗钱罪共同犯罪，在实际操作中也存在一定的障碍有待厘清。

（三）区块链洗钱罪界定和监管困境

区块链洗钱作为新兴的犯罪模式，与传统洗钱罪相比最主要的区别在于行为手段，即区块链具有匿名性、隐蔽性、跨境性等特点。这一特点给区块链洗钱在界定和监管方面带来新的挑战和困境。

1. 区块链洗钱罪法域存在滞后性

目前我国对于防范区块链洗钱犯罪的专项文件主要是 2013 年由央行、工信部、银监会、证监会、保监会联合印发的《关于防范比特币风险的通知》（以下简称《通知》）和 2021 年由最高人民检察院、公安部、市场监管总局、银监会、保监会、证监会、外汇局联合印发的《关于进一步防范和处置虚拟货币交易炒作风险的通知》。

其中，2013 年《通知》只是在有关比特币的属性、加强比特币互联网站的管理以及风险防范等方面作了规定，而对于诸如主体公司的资格审查流程以及相关具体内容、交易平台用户进行登记注册时的个人信息核实、交易限度及平台举报、监督机制建设等诸多具体问题方面，并没有明确的细致规定。⑫ 而经调整后的 2021 年《通知》则细化了之前法律文件不足部分，进一步明确了虚拟货币和相关业务活动的本质属性，完善了应对虚拟货币交易炒作的工作机制，针对虚拟货币交易炒作风险加强了监测预警机制等。由此可见，我国对于虚拟货币的态度一直持否定态度，即认为虚拟货币相关业务活动属于非法金融活动，包括法定货币与虚拟货币之间的兑换业务、虚拟货币之间的兑换业务、虚拟货币衍生品交易等，而相关监管机制也得到了改善。但对于新型区块链洗钱犯罪仍然还存在诸多法律问题，比如，该文件只是笼统规定了虚拟货币的兑换、为虚拟货币交易提供信息中介和定价服务、代币发行融资等虚拟货币相关业务活动属于非法活动，构成犯罪的，依法追究刑事责任，但具体如何追究并未明确；同时，该文件规定境外虚拟货币交易所通过互联网向我国境内居民提供服务，同样属于非法金融活动，但区块链是一种去中心化的分布式账本技术，用于记录和验证交易，它是一种数据库的形式，而虚拟货币交易所是一种在线平台，允许用户交易和投资虚拟货币的平台，两者属于不同概念；该文件更多是规制“炒币”“挖矿”等虚拟货币交易活动，对于区块链洗钱行为并无详细规定，存在一定法律空白。

2. 区块链洗钱罪法益界定难题

区块链洗钱罪所侵害的法益存在学说上的争议。目前关于洗钱罪侵犯的法益之争，主要存在侵害金融管理秩序，还是司法机关的正常活动，抑或是二者的复合等观点的争论。若认为洗钱罪侵犯的法益是金融管理秩序，则需要通过金融机构或利用金融服务手段实施洗钱行为，从而影响金融市场稳定，妨害金融管理秩序，但利用区块链技术进行洗钱犯罪并没有涉及金融机构，取代了传统金融机构作为媒介的存在，因此不能简单地认定区块链洗钱罪侵犯了金融管理秩序。若认为洗钱罪侵犯的法益是司法机关的正常活动，也存在一定不恰当之处，我国《刑法》将洗钱罪规制在第三章第四节“破坏金融管理秩序罪”中，显然立法者希望将洗钱罪单独进行评价，同时《刑法修正案（十一）》着重强调了自洗钱入罪，如果立法者支持该罪的法益为司法机关的正常活动，则会出现上游犯罪人的赃物处置行为在缺乏期待可能性的情况下，对自洗钱犯罪不缺乏期待可能性的矛盾局面。⑬ 因此，司法机关的正常活动不应成为洗钱罪所保护

⑫ 参见前引⑦，张莉莉等文，第 35 页。

⑬ 参见张明楷：《洗钱罪的保护法益》，载《法学》2022 年第 5 期，第 71 页。

的法益。若持双重客体观点,则无法解释对上游犯罪的违法所得及收益进行掩饰、隐瞒的行为,为何会因上游犯罪的不同而出现不同的评价结果的问题。⑭

3. 区块链洗钱罪的监管漏洞

区块链上的虚拟货币交易活动在监管方面一直没有得到妥善处理,没有形成完善全面的监管体系,监管技术手段也没有随着数字时代的发展而进化,相应的法规也没有作出及时调整等。比如,智能合约的复杂性(如犯罪组织设计的匿名合约)可能会使得监管机构更难以完全理解和审查其运行的原理或内部逻辑。区块链交易本身具有隐蔽性,而犯罪组织使用匿名地址和匿名货币的交易则更难被监管机构追踪。随着零知识证明、环签名、混币技术等隐私保护技术的不断进步、不断涌现的可能采用了更先进技术的新型加密货币,监管机构需要不断更新技术手段以保持对洗钱活动的监控。目前我国对于区块链洗钱犯罪监管存在漏洞,重要原因之一就在于教育和技术娴熟度不足,缺乏对区块链技术和加密货币知识的掌握,不能及时发现和应对新型的洗钱手段,同时监管机关和执法机关在运用先进技术工具方面也存在一定滞后,导致不能有效分析和监控区块链上的复杂交易。

由于区块链是全球性技术,涉及交易可能跨越多个国家,目前监管机构缺乏有效的国际合作机制,在追踪和打击跨境洗钱行为时面临困难。不同国家对区块链和加密货币的法规和监管差异巨大,犯罪组织可以选择在法规有利的国家进行操作,从而规避某些国家对洗钱犯罪的打击。

(四) 刑事管辖权原则的适用冲突

区块链洗钱犯罪如同其他网络犯罪一样,具有跨境性特点,犯罪分子可以借助互联网在多个法域之间完成洗钱犯罪,可能会出现多个国家对同一案件主张管辖权,也可能会出现没有任何一个国家主张管辖权的情况,导致管辖权的积极冲突与消极冲突。⑮ 目前我国针对网络空间犯罪的管辖问题在理论层面仍然较为保守,在司法实务方面也存在适用紊乱的情形。

1. 属地管辖的碎片化

传统属地管辖原则是以物理空间作为刑事管辖的依据,以"犯罪行为或者结果发生地"为判定核心,但区块链洗钱犯罪全程通过网络空间进行,区块链技术的分布式架构和跨国流通特性,消解了犯罪地要素的物理性,区块链洗钱行为主要靠公私密钥、智能合约等方式实现,这些新型技术通过加密数据传输完成犯罪,不再依赖物理空间,完成犯罪实施行为的虚拟化,其服务器分布、节点运营者国籍、用户 IP 地址等要素分散于多个国家,例如,前文提到的 Silk Road 跨国洗钱案中,赃款通过分布在多个国家的节点完成混币操作,导致美国、立陶宛、瑞典等国均主张属地管辖权。

2. 属人管辖的局限性

属人管辖是主权国家基于行为人的国籍或特定身份关系,对本国公民或特定主体实施的犯罪行为行使刑事管辖权的法律原则。在传统洗钱犯罪中,犯罪嫌疑人较为明确,容易掌控其身份信息和行动轨迹,即使逃脱出境也可以基于属人管辖原则对其进行引渡。但区块链洗钱犯罪最大的特点便是其匿名性,在匿名钱包、隐私货币、匿名机制等技术的层层规避下,难以分析追溯到犯罪嫌疑人的真实身份,甚至嫌疑人若采取混币手段进行洗钱,其赃款会被拆分至多个地址,更难以定位嫌疑人的真实信息。无法确定嫌疑人的身份信息就不能基于属人管辖原则对其进行刑事管辖,极大限制了属人管辖对洗钱罪的适用。

⑭ 参见安凯:《区块链技术下打击虚拟货币洗钱犯罪的司法困境及解决路径》,载《法治论坛》2022 年第 4 期,第 97 页。

⑮ 参见马赛:《区块链技术应用的刑事风险及其应对——以数字货币洗钱犯罪为视角》,载《四川警官学院学报》2020 年第 3 期,第 112 页。

3. 普遍管辖的实践障碍

针对洗钱犯罪的普遍管辖,《联合国反腐败公约》第三章第 42 条将洗钱罪纳入普遍管辖范畴,但司法实践中却难以实现。首先,2024 年通过的《联合国打击网络犯罪公约》中,中国、印度等国对公约中的数据共享条款提出了保留,这种数据主权的排他性导致司法机关跨境取证的效率被严重限制。其次,部分国家比如阿联酋、伊拉克、阿根廷等国未将区块链洗钱行为入罪,这导致双重犯罪原则在适用过程中出现困境,普遍管辖无法启动。最后,实务中普遍管辖的适用需要一定的技术能力支持,目前只有小部分国家拥有相应的区块链分析和追踪数据的技术能力,这同样导致普遍管辖在实践中存在一定障碍。

四、区块链洗钱的刑事规制

(一) 完善区块链洗钱的法律规范

完善法律规范需要以区块链和匿名货币技术为导向,推动立法转型。目前我国司法体系中针对洗钱犯罪主要的法律依据是《刑法》第 191 条洗钱罪和《中华人民共和国反洗钱法》,但两者无法满足数字时代下区块链洗钱犯罪的治理需求,而《关于防范比特币风险的通知》和《关于进一步防范和处置虚拟货币交易炒作风险的通知》等专项文件只是央行等多部门印发的行政规范性文件,法律效力不足以应对区块链洗钱带来的司法挑战。立法机关应当重视区块链技术对洗钱罪和其他经济犯罪造成的冲击影响,为了预防区块链技术和匿名货币带来的二次冲击,我国立法机关应当就区块链和匿名货币的特点、形态和底层逻辑等方面进行考究,出台相应的专项法律文件。同时,将用于交易的区块链作为“特定非金融机构”,明确其法律义务和责任。区块链技术作为贯穿洗钱犯罪整个过程的链条,连接着网络与现实的接口,经由赃款和数字货币在链条上进行交易完成洗钱犯罪,但区块链不属于传统金融机构和交易平台,不能被现有法律条文所规制,因此为更好地监管新型洗钱犯罪,应当将用来交易的区块链认定为“特定非金融机构”,纳入金融秩序管理范畴中,与金融机构一起构建完整的反洗钱监管体系,弥补洗钱犯罪立法上的缺失。

完善法律规范的另一个方向在于增扩洗钱犯罪的规制范围。目前我国洗钱罪的上游犯罪包括毒品犯罪、黑社会性质的组织犯罪、恐怖活动犯罪、走私罪等 7 项罪名,随着数字时代对我国经济体系的冲击,洗钱犯罪的成本和门槛在逐渐降低,上游犯罪的范围已经不能很好地应对当前局面,应当进行一定的增扩,但仍需要保持刑法的谦抑性,即以毒品犯罪、恐怖活动犯罪、走私罪等现行刑法已经采取的限定关键词作为洗钱罪上游犯罪的关涉范围,同时将“其他严重犯罪”作为兜底条款纳入上游犯罪的范围,此处的“其他严重犯罪”的危害程度应当与其他上游犯罪程度相当,从而达到谨慎增扩的目的。另一方面,尽管《刑法》在第 191 条第 5 项规定了“以其他方法掩饰、隐瞒犯罪所得及其收益的来源”的兜底条款,并在司法解释中进一步明确其行为类型,但当下通过区块链和匿名货币技术实施洗钱的行为已然超过了相关条文和司法解释的范围,是否可以“名正言顺”地纳入兜底条款,仍有疑问,与其如此,不如在立法论上将利用区块链和匿名货币进行洗钱的犯罪行为列入《刑法》第 191 条第 1 款中作为典型参考。

(二) 区块链洗钱共同犯罪认定路径

如前所述,行为人利用区块链技术进行洗钱犯罪活动难以被认定为共同犯罪,因为传统共同犯罪理论以“双向意思联络”为核心,强调共犯间的心理互动,但区块链洗钱中的技术行为天然消解了“合意”的

存在空间,购买人和销赃者之间通过匿名手段在区块链上完成洗钱交易,很难认定两者间存在意思联络。为此,有必要承认"片面共犯理论"。2019 年"两高"《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第 12 条将"明知他人利用网络实施犯罪"而提供技术支持的行为独立入罪,实质上承认片面帮助的可罚性,为区块链洗钱归责提供参照。片面共犯实则仅及于片面者一方的归责问题,其归责的基础在于片面者与不知情者共同引发了法益侵害结果,片面者介入法益侵害流程并作出了不容忽视的因果力,单方面改变了不知情者实行行为的单数形态,影响了犯罪结果的客观归属。⑯

在认定洗钱罪片面共犯的框架中,若开发者或使用者提供的技术工具客观上显著降低洗钱难度或扩大犯罪规模,即使缺乏与上游犯罪人的直接沟通,仍可能被认定为帮助行为。可以将客观指标进行量化处理,对交易频率、资金路径、地址关联等方面予以限制,比如规定单日跨链转账数量上限,对混币与隐藏币种的交易进行重点监控,以及屏蔽与暗网市场或赌博平台地址交互的交易,如若出现突破上述规范的行为,司法机关可根据客观情形推定行为人具备主观故意,存在被认定为洗钱罪片面共犯的可能性。

同时,区块链的自动化特性使共犯责任链条无限延伸,在整个区块链交易环节中,"矿工"的验证交易、节点的同步区块、交易所上架资产以及用户的匿名交易,各个环节参与者的技术行为在客观上形成洗钱犯罪的闭环。按传统刑法理论,所有的参与者都有可能被视作洗钱犯罪的帮助犯,这恐怕会导致责任范围泛化,违背刑法谦抑性,因此,针对该情况可以采取实质性贡献标准,仅对核心技术的实施者进行追责,避免刑法打击过度化。

针对智能合约在自动执行洗钱交易过程中各参与者归责的问题,需综合技术功能、预见可能性及合规措施进行实质判断。首先,在洗钱活动中赃款通过智能合约自动拆分成多个匿名钱包的行为,符合洗钱罪中"掩饰、隐瞒犯罪所得"的客观要件。其次,开发者编写代码的行为是否构成帮助行为,需要结合代码功能与设计目的进行考量,若智能合约在交易活动中仅提供诸如资产兑换、信息认证、数据计算等基础的交易功能,则不宜认定为洗钱犯罪的帮助犯;若开发者所设计的代码明显服务于洗钱活动,如跨链转移功能、自动混币功能、跳过安全验证功能等,具有较强的洗钱犯罪意向,则应当认为其协议的设计主要服务于非法目的,存在实质帮助行为,构成帮助犯。再次,判定使用者的责任边界应当重视主观明知的证明与抗辩,若用户仅进行合法交易,即使客观上存在协助洗钱的行为,但因缺乏主观故意,不构成犯罪;若用户明知资金非法仍利用智能合约实施交易活动,则属于洗钱罪的片面正犯。最后,对于智能合约的技术治理与合规路径,笔者认为,开发者在编写智能合约代码时应当秉持认真负责态度,具备一定的合规义务。比如对编写的代码进行审计,可以与专业的安全机构合作排查可能存在的技术漏洞,避免出现技术滥用的情形。在区块链上设置监控机制,能够及时对违规操作进行反馈和报警,可随时对高风险的交易进行追踪,并且在设计的智能合约中添加反洗钱模组,在用户触发疑似风险交易时对账户进行冻结,从而达到功能上的限制。开发者可以通过以上技术手段,自证其设计的智能合约的合规性,降低法律风险。

(三)厘清区块链洗钱犯罪的法律适用

首先,厘清区块链洗钱犯罪的法律适用,需要先对洗钱罪的法益、区块链洗钱行为所侵害的法益进行评价。如前所述,对于存在交易的区块链可视为"特定非金融机构",在区块链上进行虚拟货币交易就相当于在交易平台进行的洗钱活动,可以将其视为与虚拟货币相关的金融服务,便于央行和侦查部门监管和规制。因此,犯罪组织利用区块链技术进行洗钱活动,如同利用金融机构进行洗钱一样,会严重损害我

⑯ 参见杨滨蔓:《归责视角下共犯意思联络的规范理解》,载《中国人民公安大学学报》(社会科学版)2024 年第 4 期,第 58 页。

国市场经济，对金融管理秩序造成扰乱和冲击，区块链洗钱犯罪所侵犯的法益是金融管理秩序。

其次，惩治区块链洗钱行为的国际协作问题。数字时代下的洗钱犯罪已经突破了地域限制，尤其是利用区块链技术轻松实现跨境的洗钱活动。因此对于涉及多个国家都享有管辖权的问题，应当积极寻求国际协作配合，共同探索适应国际打击洗钱犯罪的管辖制度。比如，在有国际合作的国家之间对洗钱罪的上游犯罪共同视为享有管辖权，即洗钱犯罪组织在某合约签订国被查处逮捕，该国法域外进行的上游犯罪在该国内视为具有刑事管辖权，也就是说，该国同时对犯罪组织的洗钱犯罪和上游犯罪都享有管辖权，但管辖权并不是突破传统域外管辖的双重犯罪原则，而是为了追究跨境区块链洗钱犯罪的刑事责任，并不具备实际管辖审判上游犯罪的条件。⑰

（四）区块链洗钱罪的刑事管辖

区块链洗钱犯罪作为新型的互联网犯罪，需结合区块链的特点分析每个刑法空间适用原则在司法实践中的阻碍，对刑事管辖权的适用性进行重构。

属地原则在区块链洗钱中的难点在于犯罪行为的分散性和跨国性。针对属地管辖的碎片化，笔者认为，应当将属地管辖进行细化分级，即分为核心关联和次级关联。核心关联，是指直接涉及该国物理基础设施或造成法定货币损失的情形；而次级关联，是指通过境内 IP 地址访问区块链网络、使用境内支付通道或洗钱行为对境内金融秩序产生可量化的系统性风险的情形。依据《刑法》第 6 条属地管辖权规定之精神，利用区块链进行洗钱的行为，只要资金流、信息流或技术服务的任一环节涉及中国境内，就可以适用中国刑法。倘若行为满足核心关联的条件，则司法机关可以直接依据属地管辖原则对行为人进行刑事管辖；若行为人触及两个以上次级关联条件，亦可主张属地管辖权。比如，犯罪分子使用境内的云端服务器进行区块链洗钱活动的；或犯罪分子将赃款通过境内支付通道兑换货币，导致虚拟货币价格波动对境内金融市场造成溢出效应的情形，皆可基于属地管辖，适用我国刑法。

普遍管辖同样应对区块链洗钱犯罪带来的挑战。首先，根据《联合国打击网络犯罪公约》的争议焦点，部分国家对数据共享条款持保留立场，为保障跨境数据取证的合法性且便于普遍管辖的适用，笔者认为，可以对跨境调取的数据实施分级保护，比如将用户注册信息、用户浏览信息、用户喜好模型等低敏感数据，允许在一定范围内根据公约缔约国的“提交令”并通过司法审查程序后调取。我国应该坚持“提交令”措施的立场，反对未经我国政府同意直接调取储存在我国境内的电子数据。⑱ 将交易内容相关的数据列为高敏感数据，应当严格遵循数据储存地相关法规和意见，按照约定的司法程序，通过国际刑事司法协助渠道获取。其次，对双重犯罪原则的适应性做出调整，推动国际立法协调，提倡各国将区块链洗钱行为明确入罪，并根据相关公约达成统一标准。对于《联合国反腐败公约》第 42 条规定的洗钱行为，在双重犯罪审查中，根据实际情况可以基于“实质危害相当性”认定其符合双重犯罪要求，启动普遍管辖。最后，面对技术上的鸿沟问题，应当由技术领先国家牵头建立区块链数据追踪开源平台，提供先进的技术和工具，提升技术落后国家对混币技术、跨链交易等区块链洗钱手段的分析和辨别能力，以及要求各国统一区块链数据记录格式，方便跨国数据的整合，弥补各国打击区块链洗钱犯罪的技术差距，便于普遍管辖的适用。

⑰ 参见李阜蒙、李昊：《“互联网 3.0”时代网络洗钱犯罪的防控对策研究》，载《中国价格监管与反垄断》2023 年第 4 期，第 79－80 页。

⑱ 参见李哲、朱晓琴：《〈联合国打击网络犯罪公约〉的中国立场与核心问题》，载《北京师范大学学报》（社会科学版）2024 年第 5 期，第 132 页。

属人管辖原则在区块链洗钱犯罪中较难被适用，究其原因在于区块链的匿名性对查明身份信息带来困扰，无法锁定区块链上购买和销赃的用户就无法适用属人管辖。解决问题的核心在于实现犯罪人身份从国籍身份到数字身份的突破。一方面加强技术上的跨越，通过 IP 关联、交易所访问记录、虚拟钱包地址等途径建立线上数字信息与线下真人的对应关系，从而锁定犯罪嫌疑人。另一方面，可以借鉴美国《反海外腐败法》经验，要求境外交易所对具有中国国籍的用户履行反洗钱报告义务，由平台承担部分的责任。

（五）区块链洗钱罪的综合治理

实现区块链洗钱罪的综合治理，需要多部门间的协调合作。建立反洗钱的部门协调机制，形成由公安牵头、人民银行、外汇局参与的三位一体联动机制，联合银监会、财政、税务、市场监管、海关、监察等部门，强化反洗钱的综合治理能力。⑲ 围绕信息资源共享原则，健全内部数据信息沟通共享机制，明确内部数据责任划分和使用数据的权限，极大提高应对洗钱犯罪的侦查调查和审判追踪的效率。在设立全方位反洗钱工作机构和内控机构的基础上，对侦查人员开展专业数字技能培训，提升从业人员的反洗钱意识和对交易的鉴别能力。

基于区块链和匿名货币技术独特的运行机制，侦查机关有必要采取专门的技术手段应对利用此类技术的洗钱活动。区块链作为一种技术手段并非金融机构，但基于打击洗钱犯罪的需要，区块链交易也应当履行构建用户身份识别、报告可疑交易、保存交易记录的反洗钱义务。对于区块链交易匿名的问题，侦查机关需要着重落实真实身份验证，比如涉及数字货币的交易都应当登记备份，同时加强对金融机构和交易所的资质审查，并定期开展实质审查。另外，必须改变侦查模式，因为上游犯罪持续不断地为洗钱犯罪提供空间，且上下游犯罪链条呈现产业化、集团化特征，想要打击洗钱犯罪必须整条犯罪链共同打击，从以往的个案化、片面化的侦查模式转变为宏观掌控的全方面打击模式，通过多部门协调配合积极进行案件串并，从包括违法搭建 VPN 和区块链、借用或假注银行卡、买卖公民个人信息等违法行为入手，牢牢把握虚拟货币交易流数据和资金流数据两条线，运用数据化情报导侦思维，深化数据挖掘和关联分析，及时锁定链上身份，进而锁定相应的犯罪主体，⑳ 实现全链条全覆盖打击。

在数字化背景下，侦查机关应当运用大数据和人工智能等高新技术成果打击区块链洗钱犯罪。一方面，利用区块链技术搭建智能化综合治理数字平台，基于区块链技术的数据唯一性、高效性、去中心化等特点，侦查机关可以将上游犯罪的数据和信息高效整合，再采取数据碰撞和挖掘等方式，迅速发掘异常信息起到报警预警作用，同时能够在复杂烦琐的信息中提取关键线索，更好地将合法资金与上游犯罪非法资金进行区分，便于办案人员进行分析和研判实现精准打击。另一方面，结合区块链特征，实行“以链治链”的方式，比如利用数字验证技术收集交易数据，并与用户的身份信息相匹配，若在匹配过程中发现异常可以及时上报监管机构；还可以利用区块链先进的密码学技术，在区块链上设立智能辨识系统实现对可疑交易和匿名智能合约的监控预警，并自动展开追踪分析；对于匿名或存在缺陷的智能合约试图验证区块链交易的行为，侦查部门应当及时发现并进行拦截，否定相关交易，并对原智能合约进行修改，避免犯罪组织开展洗钱活动，确保资产安全。

⑲ 参见胡云腾、翟辉：《〈反有组织犯罪法〉的立法特色与理解适用》，载《法治现代化研究》2023 年第 1 期，第 3 页；前引⑰，李阜蒙、李昊文，第 80 页。

⑳ 参见前引⑨，邓宁江文，第 6－13 页。

五、结 语

区块链技术的去中心化架构与匿名化特性在重塑金融生态的同时，亦为洗钱犯罪提供了新型技术工具，其引发的刑事治理挑战已超越传统法律框架的应对范畴。本文通过解构区块链洗钱的技术逻辑与行为模式，揭示此类犯罪在匿名交易、智能合约滥用及跨境流通等维度的技术本质。并指出现行刑事规制体系在共同犯罪归责、法益界定及管辖权适用等方面存在的显著滞后。作为解决之道，本文主张以“技术—法律”协同治理为核心理念，重构区块链洗钱的刑事规制范式。在立法层面，亟须将区块链交易纳入“特定非金融机构”监管范畴，并通过扩大洗钱罪上游犯罪范围、细化虚拟货币相关行为的刑事评价标准，填补法律漏洞。在司法适用层面，引入片面共犯理论破解技术帮助行为的归责难题，同时构建分级属地管辖规则与国际数据协作机制，破解跨境管辖冲突。此外，强化区块链交易的身份溯源能力、完善智能合约的合规审查机制、推动侦查技术的智能化升级，是实现全链条精准打击的必要路径。

Abstract: Blockchain technology provides covert technical support for money laundering crimes and increases the complexity of criminal behavior. Money laundering activities involving virtual currencies have surpassed traditional financial regulatory frameworks, exhibiting characteristics such as being technology-driven, involving cross-border collaboration, and forming industrial chains. The criminal attribution and regulatory challenges posed by blockchain money laundering include: (1) anonymity complicates the identification of “mutual intent” in joint crimes; (2) existing laws lag in defining blockchain money laundering and addressing the disputes over protected legal interests; (3) cross-border jurisdiction conflicts and insufficient regulatory technology constrain enforcement effectiveness. To address these issues, special legislation should clarify blockchain's designation as a “specific non-financial institution” and expand the scope of predicate offenses for money laundering. The theory of unilateral accomplice liability should be introduced to resolve attribution challenges for technical assistance behaviors. Additionally, criminal jurisdiction should be optimized through stratified territorial jurisdiction and cross-border data collaboration. A multi-agency collaborative governance mechanism is recommended, enhancing identity tracing in blockchain transactions and compliance review of smart contracts. Big data technologies should be leveraged to achieve precise, full-chain enforcement against money laundering activities.

Key words: blockchain technology; virtual currency; money laundering crime; joint crime; criminal jurisdiction

[学科编辑：王彦强 朱梁伟 责任编辑：周瑞莹]