刑事司法科学与治理
Criminal Justice Science & Governance
2025 年 第 6 卷 第 2 期

跨境虚拟货币洗钱犯罪的“猫鼠游戏”破局

——基于云端智库多源数据融合的治理路径优化

李超逸

中南财经政法大学刑事司法学院，武汉

摘　要 | 当前跨境虚拟货币洗钱犯罪呈现技术迭代加速化、资金转移瞬时化、犯罪主体隐蔽化特征，传统“监管主体—犯罪组织”二元对抗模式陷入取证固证难、资金溯源难、司法认定难的治理困局。本文提出构建基于云端智库的多源数据融合体系，通过区块链交易图谱分析、跨链资金流向追踪、暗网地址聚类关联三大技术模块，实现犯罪网络动态监测、可疑交易智能预警、匿名账户穿透识别的三重突破；采用联盟链架构的分布式数据节点可提升链上链下数据协同效率，结合联邦学习算法对链上地址标签库、交易所KYC数据库、暗网论坛语料库进行联合建模，能够形成“资金—行为—身份”三位一体的证据链闭环；建立链上特征数据与链下实体信息的动态映射机制，构建犯罪组织反侦查行为与监管科技演进的动态博弈模型，推动形成“技术治理—法律协同—国际协作”三位一体的治理新格局，为打击跨境虚拟货币洗钱犯罪、维护国家金融安全秩序提供坚实的司法保障与技术支撑。

关键词 | 虚拟货币；跨境洗钱犯罪；链上治理；云端智库

在经济全球化深度演进的时代语境下，各国间经济协作与交往的密度显著提升，跨境经济活动的频次与规模亦呈几何级增长。这一进程在推动全球经济体系持续稳定发展的同时，亦助长了洗钱犯罪的国际化趋势。虚拟货币的出现，使得网络洗钱成为新的犯罪形式，这种洗钱模式与传统模式有所不同，具有反侦查性、证据难固定、参与人员广泛及跨国性等特征，导致这种网络洗钱的行为具有极大的社会危害性。[1] 在数字经济与全球化深度互嵌的时代语境下，以比特币为典型代表的虚拟货币，因其去中心化架构、匿名交易特性及跨境流通优势，已成为跨境洗钱犯罪的新型载体。该类犯罪呈

［1］王美琪，金泓序．虚拟货币洗钱犯罪研究［J］．河北公安警察职业学院学报，2024，24（1）：32–36.

现的跨区域流动性、技术隐蔽性与监管套利性特征，对传统反洗钱治理体系构成颠覆性挑战。当前，在我国的实践中，公安部大力推进的科技强警战略与中国人民银行反洗钱风险预警系统的持续迭代升级，共同构筑了立体化的反洗钱治理体系，传统洗钱犯罪在境内的生存空间被大幅压缩。基于犯罪经济学的成本收益逻辑，犯罪分子为维系非法利益链条，逐渐将犯罪目标转向境外金融犯罪治理效能较弱的地区，跨境洗钱遂成为洗钱犯罪的新型选择[1]。虚拟货币凭借其跨境支付的高效性、低交易成本属性及抗通货膨胀的技术特性，在贸易全球化浪潮中重塑了全球金融交易的底层逻辑。然而，区块链技术的去中心化架构与匿名性特征，客观上为洗钱犯罪开辟了技术赋能的新通道。据全球知名区块链分析机构Chainalysis发布的2024年度报告显示，当年全球通过虚拟货币实施的洗钱规模已突破200亿美元，其中跨境洗钱占比高达60%以上。与传统洗钱模式相异，虚拟货币洗钱借助区块链技术的匿名性与跨司法管辖区特性，使得资金流向追踪、电子证据固定及司法管辖权认定等司法实务环节面临技术性困境。尽管我国采取了坚定的反洗钱禁止性政策，并通过制度创新与技术革新持续优化治理体系，在一定程度上实现了对境内洗钱犯罪生态的有效压制，但现有政策框架与技术手段尚未能充分应对虚拟货币洗钱的固有风险。事实上，这种治理张力反而催生了虚拟货币交易的地下化与跨境化演进趋势[2]。有鉴于此，构建更具针对性与实效性的治理体系已成为当务之急。本文拟聚焦跨境虚拟货币洗钱犯罪的治理困境，通过典型案例的规范分析与技术逻辑的解构，尝试从体系建设角度提出优化路径。

一、跨境虚拟货币洗钱犯罪特征及运作模式

（一）虚拟货币区别传统货币的特征

当前世界范围内，主流的虚拟货币包括以比特币（BTC）、以太坊（ETH）为代表的“加密货币”，币安币（BNB）、SOL（Solana）为代表的“平台代币”，门罗币（XMR）、Zcash（ZEC）为代表的“隐私币”等。虽然依据货币的呈现形式，以泰达币（USDT）、美元币（USDC）为代表的“稳定币”和以数字人民币（e-CNY）为代表的“央行数字货币”也属于虚拟货币的范畴，但是二者核心特点为中心化发行，具备法偿性或与法币、黄金挂钩，价格相对稳定。与上述几种虚拟货币的核心特点差异性较大，且这些特征使其不具备较高洗钱犯罪风险，故本文不将其列为高危虚拟货币的讨论范畴。虚拟货币是区块链技术在金融科技领域的创新应用，具有去中心化、匿名性和跨国性等特点，易被利用实施诈骗、传销、洗钱、非法集资、网络赌博、敲诈勒索和暗网交易等违法犯罪活动。[3]国际清算银行2023年研究报告显示，全球约78%的虚拟货币交易所支持至少5种法币的即时兑换服务，这种特性极大降低了跨境洗钱的时空成本。此外，智能合约的可编程性赋予其自动执行交易的能力，特别是在去中心化金融（DeFi）生态中，洗钱者通过对流动性池、闪电贷等金融工具的组合运用，洗钱者可实现资金路径的智能伪装。值得注意的是，虚拟货币的价值储存功能具有高度波动性，2024年比特币价格振幅达到67%，这种特性既为洗钱者提供套利空间，也增加了涉案资产追缴的折算风险。上述技术特征与传统货币的本质差异，构成了虚拟货币洗钱犯罪异化的底层逻辑。

一是去中心化。去中心化的本质特征是“权力分散”和“规则自治”：权力分散指决策权从中心机构转移至网络节点（如矿工、验证者、普通用户），即不存在集中式发行机构，而是通过网络协议实现单个节点与其他节点的直接交互[4]；规则自治则是通过代码（如共识算法、智能合约）自动执行协议，规避金融部门监管，减少人为干预。正是因权力分散和规则自治的存在，大大增加虚拟货

[1] 詹文蔚. 利用虚拟货币跨境洗钱犯罪的行为规制研究[D]. 无锡：江南大学，2024.

[2] 卢建平，刘嘉. 虚拟货币洗钱犯罪的治理方案——基于风险视角的分析[J]. 北京社会科学，2025（2）：105-116.

[3] 陈潮，吴建峰，徐歆. 数字经济背景下虚拟货币犯罪模式分析与多维治理研究[J]. 浙江警察学院学报，2024（6）：20-34.

[4] 邓宁江. 虚拟货币洗钱犯罪分析及治理对策研究[J]. 北京警察学院学报，2023（6）：92-101.

币洗钱犯罪的发生风险。虚拟货币的去中心化和匿名性特征，导致交易账户难以有效关联，侦查部门无法快速锁定涉案账户。此外，虚拟货币可实现全球流通和虚拟传输，单一主权国家难以对虚拟货币在全球范围内的流动情况进行实时监测。[1]

二是匿名性。基于匿名性这一特征，虚拟货币相较于传统金融货币能够更好地保护用户隐私权。在现有中心化财产登记制度下，用户通过传统货币进行交易，所有账户交易数据都将储存于银行系统，其中包括交易用户的个人信息、交易数额、交易次数等。现实交易中，不可避免地因为数据保管不当而造成用户信息的泄漏，这些数据被不法分子利用后，造成用户的隐私权受到严重侵犯。虚拟货币则是提供不记名的金融交易环境，该环境下的每一笔交易均满足公钥与私钥衔接的条件，同时在每一笔交易完成后都会自动产生新的公钥与私钥，因此虚拟货币交易具有较强的隐私保护功能[2]。虽然通过虚拟货币交易在一定程度上可以减少经济领域滥用个人信息情况的发生，但是虚拟货币交易的不记名性为犯罪分子进行暗网交易、转移赃款提供极大的便利。虚拟货币交易独立于传统中心化交易监管体系，源于虚拟货币的交易地址在不断动态变化中且无需进行实名认证。虚拟货币通过随机选出256位二进制数字，进而形成私钥，然后通过加密函数生成26位至34位的交易地址[3]。随着加密技术的不断发展，门罗币（XMR）、Zcash（ZEC）为代表的“隐私币”应运而生，极大增强了交易隐秘性。因此精确定位犯罪交易地点和追踪虚拟货币流向，成为阻碍侦查活动进行的难题之一。

三是跨境流通便利性。虚拟货币的流通便利性主要体现在：交易过程中系统会自动生成虚拟交易站，通过虚拟交易站促成不同用户之间的OTC交易（场外交易），犯罪分子可以轻易地通过虚拟货币将违法所得转换为法币等合法金融货币，从而实现洗钱的犯罪目的。虚拟货币通过单一P2P网络节点确认，便可在全球范围内广泛流通，即只要存在接受虚拟货币支付的第三方，交易便会自动完成，不再受地域和政府监管。基于此，全球接受虚拟货币交易的商户和第三方支付渠道数量呈现持续增长趋势。例如，美国贝宝（Paypal）就允许其用户通过虚拟货币在其有贸易往来的2600万名商户处进行购物结算；闪电网络（Lightning Network）作为第三方交易渠道，用于比特币交易支付，被萨尔瓦多政府列为法定支付方式。这种上升趋势的最主要原因，是中心化模式下的外币兑换通常需要支付较高的手续费用且存在数额限制，而以比特币为代表虚拟货币的兑换不存在限额规定，且不会收取较高的手续费用。比特币当前普遍收取的手续费比例只有千分之二，没有第三方机构的监管，即用户与用户、用户与商家、商家与商家间的跨境交易无需向银行等监管机关报备。犯罪分子正是利用这一便利条件，随意进行跨境转账洗钱活动，给全球各国打击此类经济犯罪造成严重困扰。

（二）虚拟货币洗钱犯罪运作模式

虚拟货币洗钱犯罪，指利用虚拟货币的匿名性、去中心化及跨国流通特性，通过技术手段掩饰、隐瞒犯罪所得及其收益的来源，使其在形式上合法化的犯罪行为。当前全球社会高度关注网络洗钱犯罪活动，国际上反洗钱金融行动特别工作组（FATF）在《虚拟资产与反洗钱指南》（2019年修订版）中将虚拟货币纳入反洗钱监管范围，要求各国将其定义为“虚拟资产”（VA）并实施监管。我国《中华人民共和国刑法》第一百九十一条中明确为“协助将资金转换为虚拟货币”列为洗钱犯罪行为；中国人民银行等十部门联合发布的《关于进一步防范和处置虚拟货币交易炒作风险的通知》，强调禁止虚拟货币相关业务，并强调打击利用虚拟货币实施的洗钱犯罪行为。根据洗钱采用的技术手段，可将虚拟货币洗钱分为以下三种路径。

1. 匿名钱包洗钱

虚拟货币因为其匿名性、去中心化、交易模式复杂多变等特点，而备受地下钱庄等洗钱组织青睐。在虚拟货币洗钱犯罪中，全球流通性和去中心

---

［1］程聪聪，王秋菊．利用虚拟货币洗钱犯罪的侦查困境及破解对策［J］．江苏警官学院学报，2024，39（4）：102-110.

［2］邹锦圣．打击虚拟货币跨境洗钱犯罪国际合作法律问题研究［D］．广州：广东外语外贸大学，2020.

［3］邓宁江．虚拟货币洗钱犯罪分析及治理对策研究［J］．北京警察学院学报，2023（6）：92-101.

化的特性不但缩短了洗钱周期，更让虚拟货币洗钱不会留下跨境交易痕迹，外汇监管机构很难追踪资金流向[1]。当前匿名钱包主要包括Wasabi Wallet、Samourai Wallet，其功能在于隐匿待洗白资金的来源，通过无KYC（Know Your Customer，即客户身份识别）验证、Coin Join技术、分层架构等方式，切断资金与用户真实身份的关联，切断金融机构、公安机关对资金来源和流转路径的追踪，从而实现洗钱的犯罪行为并逃避法律制裁。其中，KYC验证是金融机构和受监管实体为识别客户身份、评估风险，并防止洗钱、恐怖融资等非法活动而实施的合规流程，核心要求包括身份验证、风险评估、持续监控等。在传统金融体系中，KYC验证具有强制性，即只有事先通过KYC验证，用户间交易才可进行。基于此，在我国反洗钱风险预警系统24小时持续监管下，传统洗钱犯罪的发生率呈总体下降趋势。但在虚拟货币领域，以TER等去中心化交易所（DEX）和匿名钱包为主的平台或服务，允许用户在不提供身份信息的情况下进行交易，为匿名钱包洗钱行为提供了便利。加之Coin Join技术可将多个用户的资金交易混合打包，使外部观察者无法分辨资金来源与流向。例如，Wasabi Wallet的“零链”混合功能，通过多次混合（默认至少5轮）扩大匿名范围及规模，使外部监管机构难以通过统计学分析追踪资金流向；合并分层隐匿架构将匿名钱包和Tor网络结合，隐藏用户IP地址与交易时间戳，实现链下隐私增强，再通过分层交易操作，增加资金追踪复杂度。

2. 跨链桥与 DeFi 洗钱

DeFi（去中心化金融）平台是基于区块链技术建构的金融生态系统，旨在通过智能合约和去中心化协议替代传统金融机构，提供无需信任中介的金融服务。在DeFi平台从事交易，相较于传统金融平台而言收取的服务费较低，因此也更受用户的青睐。DeFi平台去中心化的特点，使其不受银行、公安等实体机构的监管，逐渐沦为犯罪分子实施洗钱活动的工具。加之DeFi平台缺乏KYC验证要求和用户自主权限制，导致了DeFi在识别和冻结非法资金方面存在重大缺陷。跨链桥与DeFi平台主要通过以下路径协助洗钱：首先，犯罪分子利用跨链桥（如Polygon Bridge）将资产转移至不同区块链网络，脱离原链监管范围；其次，通过DeFi平台（如Uniswap、Curve）将赃款兑换成其他代币，无需KYC且流动性高；最后，通过质押、借贷等DeFi操作，将非法资金包装为“投资所得”。

3. 暗网洗钱

暗网作为以互联网为基础，依托匿名通信技术构建并通过特定软件访问的加密网络系统，为多种非法活动提供了隐蔽空间[2]。犯罪分子常通过暗网平台，利用隐私币交易实施洗钱犯罪。隐私币通过加密技术实现交易不可追踪，从而隐匿赃款转移路径。以门罗币（XMR）为例，其采用的“环签名”技术会混淆发送方身份，使交易签名来自一组随机地址，且每次交易都会生成一次性地址，阻断对接收方的关联；门罗币交易遵循zk-SNARKs协议，通过零知识证明技术隐藏交易金额参与方信息，仅验证交易合法性；其具有抗链上分析特性，即隐私币区块链浏览器无法显示具体交易详情。

利用暗网实施洗钱犯罪的全过程可以大致划分为如下三个阶段[3]：第一阶段：投放。在这一阶段，非法所得资金被投入去中心化交易所进行混币交易，旨在使虚拟货币地址间的关联变得难以追踪，从而隐匿洗钱犯罪行为；第二阶段：分层。此阶段旨在将资金转换为其他货币形式，并构建多层次的虚拟货币交易网络，掩盖资金的原始来源和流动路径；第三阶段：整合。基于前两阶段实施的资金转化，赃款已成功融入正常的经济交易体系，此阶段旨在将洗白资金以小额、多次、不连续的方式进行提取，避免受到金融监督机构的异常预警，从而实现洗钱的最终目的。

---

［1］苏伟光，张冬冬．虚拟货币犯罪模式剖析及治理对策研究［J］．网络安全技术与应用，2023（2）：139-143.

［2］肖恩，阮能文．暗网毒品犯罪亟须多维治理［EB/OL］．（2021-09-06）［2025-05-24］．https://www.spp.gov.cn/spp/llyj/202109/t20210906_528587.

［3］林海文，谢瑜，郑上坚．暗网洗钱犯罪的治理困境与出路［J］．浙江警察学院学报，2024（3）：101-112.

二、我国跨境虚拟货币洗钱犯罪治理困境

（一）区块链技术难以确定账户身份

区块链的分布式账本技术虽能确保交易记录的不可篡改性，但其底层架构天然排斥中心化身份认证体系。虚拟货币账户由非对称加密算法生成的哈希地址构成，这种由随机数生成器创造的26～34位字符组合，与用户真实身份之间不存在法定强制关联。我国在区块链分析技术领域取得显著进展：当前北京海存科仪的链上资金追踪系统可识别门罗币环形签名交易，2024年在“12·05”跨境洗钱案中，该系统通过分析3000万条交易记录，成功锁定犯罪团伙资金流向；美亚柏科“取证云平台V2.0”的“虚拟货币分析中心”支持交易所App云探测，输入手机号即可检索全球主流交易所注册记录，2024年协助冻结资金达5亿元；AI智能取证工具广泛应用，联腾正道系统的动态关联碰撞算法可实时分析交易图谱，该系统通过关联10万条链上交易记录和500个链下账户，72小时内即可完成证据链构建。

然而，技术对抗形势严峻。门罗币的环形签名算法通过随机选择多个公钥形成签名环，使得交易发起者身份难以追踪。在2020年Plus Token网络传销洗钱案中，犯罪团伙利用门罗币混币服务转移资金，导致链上交易无法关联到真实账户。混币服务单次涉及3000个账户，变现渠道监管缺失，23%的资金流向“去中心化交易所”，取证难度极大。虚拟货币犯罪活动隐蔽性较高是多因素共同导致的：虚拟货币交易具有较高自由度和便捷性，天然的去中心化和匿名性特征使审查及监管难度提升；在实施犯罪过程中，犯罪分子还会借助混币器、跨链桥、匿名币等工具，进一步提高犯罪行为的隐蔽性。[1]虚拟货币的匿名性加大了犯罪主体的锁定难度。私人虚拟货币的注册是开放的模式，网络服务平台仅进行形式审查。在中国人民银行等七部门联合出台《关于防范代币发行融资风险的公告》，全面禁止我国交易平台开展虚拟货币运营业务后，虚拟货币平台基本迁向境外，因整个交易过程完全匿名，用户可以使用多个匿名地址，且没有集中的交易平台与服务运行器，交易信息绝对加密，犯罪分子仅有可能在区块链中留存痕迹，而具有现金价值的虚拟货币基本上都通过技术手段设置了隐私信息保护屏障，这就导致侦查机关难以锁定犯罪主体身份。[2]例如，作为世界规模最大虚拟货币的比特币，其协议并不要求提供参与者的身份识别和验证，也不生成与现实世界身份相关的交易历史记录。换言之，即使发送方与接收方均未进行充分的身份识别，系统大概率依旧会进行交易操作。这也意味着，若警方追踪犯罪者行踪，平台方可提供的用户信息仅限于手机号码及昵称，此举无疑是人为切断了犯罪者与资金流的关系，为警方调查犯罪行为增加了难度[3]。当前，我国司法机关在办案实践中还面临链上与链下数据协同难题。国家互联网应急中心2023年的数据显示，区块链地址虽可通过网络层IP溯源，但混币器与Tor匿名网络的叠加使用，使得IP定位误差率高达64%。即便通过大数据分析锁定可疑地址，依据《区块链信息服务管理规定》调取交易所用户数据时，也常因境外服务商拒绝配合导致证据链断裂。这种技术特性与法律管辖权的双重障碍，构成了虚拟货币洗钱犯罪治理的深层技术困境。

（二）匿名技术导致电子证据难以认定

虚拟货币洗钱犯罪中电子证据的认定困境，源于区块链技术的双重属性。一方面，区块链的分布式账本技术使得交易记录具有不可篡改性，理论上能够形成完整的证据链条；另一方面，混合加密算法、零知识证明等隐私保护技术的迭代升级，使得交易主体身份与行为轨迹的关联性被系统性割裂。以Zcash为代表的零知识证明协议，允许交易双方在不透露地址余额、转账金额等核心信息的前提下完成交易验证，这种“有效性验证而非信息披露”的机制，导致侦查机关即使获取区块链数据，也难以形成具备完整证明力的电子证据链。涉虚拟货币

［1］李大猛，孙杰，蒋照生，等．虚拟货币犯罪态势及安全治理研究综述［J］．警察技术，2023（2）：33-41.

［2］吕晗．虚拟货币相关刑事犯罪的惩治困境与法律保障［J］．中国政法大学学报，2023（4）：173-184.

［3］张郁，侯文瑾，柳滨．虚拟货币犯罪分析及治理对策研究［J］．浙江警察学院学报，2022（6）：78-87.

犯罪是在网络空间内实施的，而网络空间与虚拟货币均有匿名性，且涉虚拟货币犯罪各环节多是独立操作，多重因素叠加导致公安机关在侦查时查找犯罪主体相对困难。实践中，公安机关接到报案后，往往根据资金链条查到实体银行账户的户主，而大多数案件侦查到这一步线索即中断了，因为犯罪分子会采用多种手段弱化资金链与其真实身份的关联性[1]。

虚拟货币洗钱犯罪的追溯性差、隐蔽性高，加之区块链技术本身的复杂性、作案地点分散等特点，相较于传统的取证技术要求更高。电子数据的提取与固定对案件的整体走向和犯罪事实的最终认定起到重要的作用，是案件能否成功破获的关键。由于电子数据具有易失性、时效性、易篡改性等特点，如不能及时提取和保全，将对后续的侦查工作产生不利的影响。[2]实践中，门罗币环形签名算法每18个月升级一次，而我国区块链取证工具平均3年更新一次，导致技术对抗失衡。数据碎片化与云存储技术的普及，使得电子数据完整性难以保障。虚拟货币洗钱犯罪产业化形成完整链条，跑分平台日均处理10万笔交易，如2025年湖北鄂州刘某某案中，犯罪团伙通过“取现换U币”模式，3个月内洗钱9.5万元，涉及3000个匿名账户；同时云存储服务商因数据覆盖导致证据灭失，致使案件被迫退查两次。

我国在区块链存证技术领域取得一定进展，2024年发布的《区块链和分布式记账技术存证通用服务指南》国家标准，规范了电子数据存证的关键流程。但该标准未强制要求进行哈希值存证，导致链上交易记录因未进行哈希值存证被法院排除在外。核心技术受制于人的问题依然存在，如门罗币的环形签名算法依赖特定加密库，而我国目前尚未形成自主可控的替代方案。

三、打击虚拟货币洗钱犯罪的优化路径

（一）数智赋能区块链取证技术与云端智库的双轮驱动

数智赋能区块链技术诞生发展，源于哈希算法的创造性使用。这种数学函数，将任意长度的字串，完整压缩成固定长度的二进制数据，这种现象被称为哈希值或散列值；哈希表则是数据存储类型库，以键值为索引，帮助找到相应的库。因此数智赋能区块链技术因其不易篡改性的特点，利用哈希值固定犯罪嫌疑人的手机、犯罪集团电脑以及勾结的第三方网络平台的信息后，便可保存下来，并能有效地防止电子数据在运输过程中或因储存不当而受到损坏，对固定网络犯罪证据起到极大促进作用[3]。加之区块链去中心化的特点，在完成收集证据后，犯罪嫌疑人或勾结的第三方网络平台要想再毁灭或破坏证据就变得尤为困难，使得证据的真实性、安全性得到极大的提升。

云端数据库通过建立类似于人脑工作系统的“神经链条”，从而连接不同种类案件的数据源。侦查取证机关通过对实时证据的锁定与提取，将相关信息上传至数智赋能云端数据库。数据入库后，在取证联盟链机制的协同运作和相应的管理节点的监管下，能够允许相关司法机关按照权限进行构件资源的查询、检索、上传与下载[4]。同时，充分利用多样化的管理节点的管理职能，规范取证与提证程序，有效提高情报资源的质量，保证电子证据在总链中循环流动的构件资源下载即可使用，提高情报资源的复用性与情报工作的效率。

（二）区块链固定洗钱犯罪电子罪证后上传至联盟链云端智库

缅北跨境犯罪集团实施的网络贩毒、虚拟货币洗钱等非法资金流动活动，需依托国内外大型金融机构的区块链记账系统、证券交易系统、基金托管系统及银行核心业务系统完成资金流转。上述

---

［1］张涛．涉虚拟货币犯罪的代际演变、发展态势及应对之策［J］．河南警察学院学报，2023，32（5）：51–59.

［2］邓宁江．虚拟货币洗钱犯罪分析及治理对策研究［J］．北京警察学院学报，2023（6）：92–101.

［3］宋宝燕，丁俊翔，王俊陆，等．基于变色龙哈希和可验证秘密共享的联盟链修改方法［J］．计算机应用，2024，44（7）：2087–2092.

［4］蔡鸿宇，徐宗煌，张伟，等．基于区块链思维的情报构件资源共享机制研究［J］．情报杂志，2024，43（1）：176–182.

系统在联盟链架构中形成具有特定功能的情报子链网络。通过情报组件资源池、实时数据采集模块、组件数据复核机制、管理节点认证体系与跨链数据交换协议的协同运作，构建起覆盖全产业链的电子罪证查证网络。云端智库作为联盟链生态的智能中枢，通过多维度数据链路连接异构数据源，公安机关通过实时证据固化技术，将加密哈希值、交易元数据等关键信息上传至分布式存储节点。

数据入库后，联盟链凭借其适度去中心化的分布式账本架构，在管理节点的共识机制约束下，允许司法机关按照最小权限原则实施组件资源的查询、检索、上传与下载操作。具体而言，管理节点通过智能合约固化的权限管理机制，实现对情报组件设计标准、功能边界的全生命周期管控，通过数据质量校验算法提升组件资源的可信性，确保总链中流通的情报组件满足“即取即用”的业务需求，显著提升组件资源的复用率与刑事侦查情报工作的协同效率。该机制通过管理节点的认证网关、数据交换的加解密隧道与操作行为的审计追踪，构建起“采集—存储—分析—应用”的闭环证据管理体系，有效破解跨境犯罪证据链碎片化难题。联盟链架构下情报子链网络及数据管理结构如图1所示。

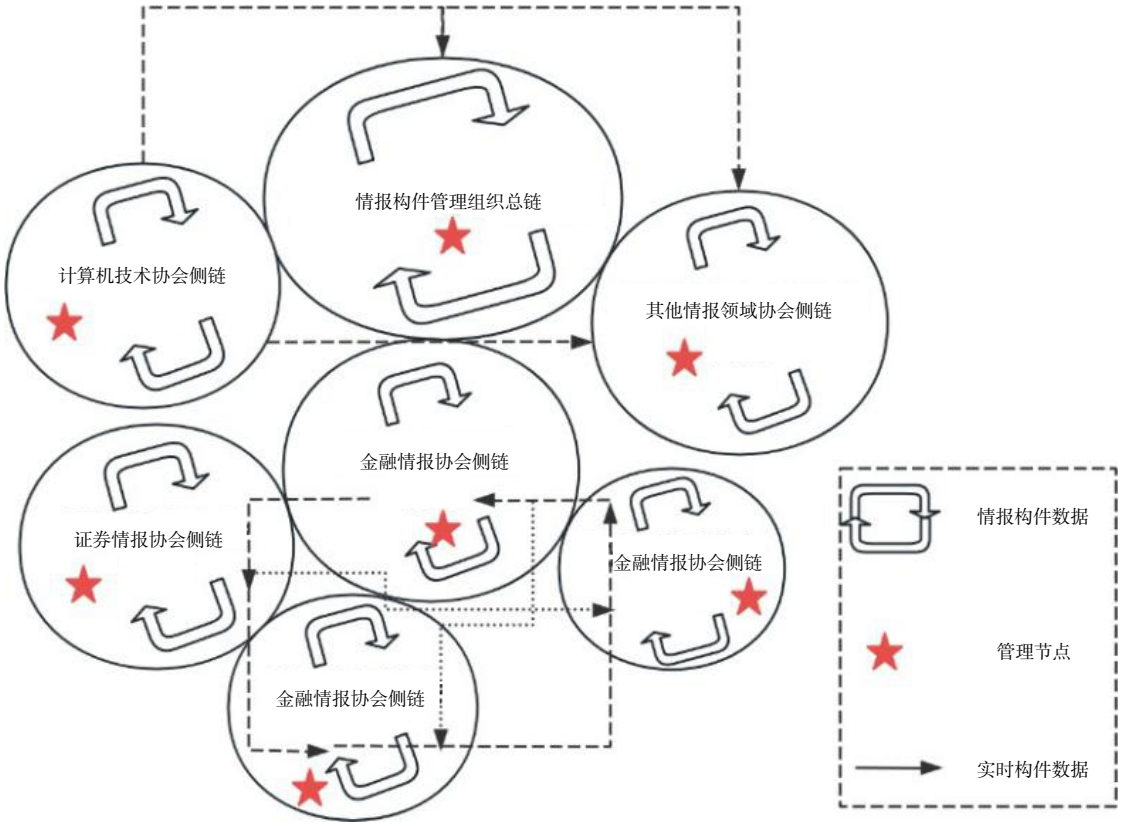

图 1　联盟链架构下情报子链网络及数据管理结构示意图

云端智库大数据并行连接查询流程如图2所示，上传至云端智库的数据后依靠共识机制进行运作，其功能就是要保证情报构件的信息资源的一致性与安全性，决定了情报构件的使用价值与共享机制的平稳运行。区块链固定虚拟货币洗钱电子证据后，联盟链分布式记账方式存在的问题就是很难在众多节点上达成共识。因此，需在公检法联盟链中建立专业性共识机制，即基于共识算法建立统一管理源数据点，并对分数据链开放的信息交互体系，保证情报构件资源的质量，并提高情报构件资源共享平台的运行效率。

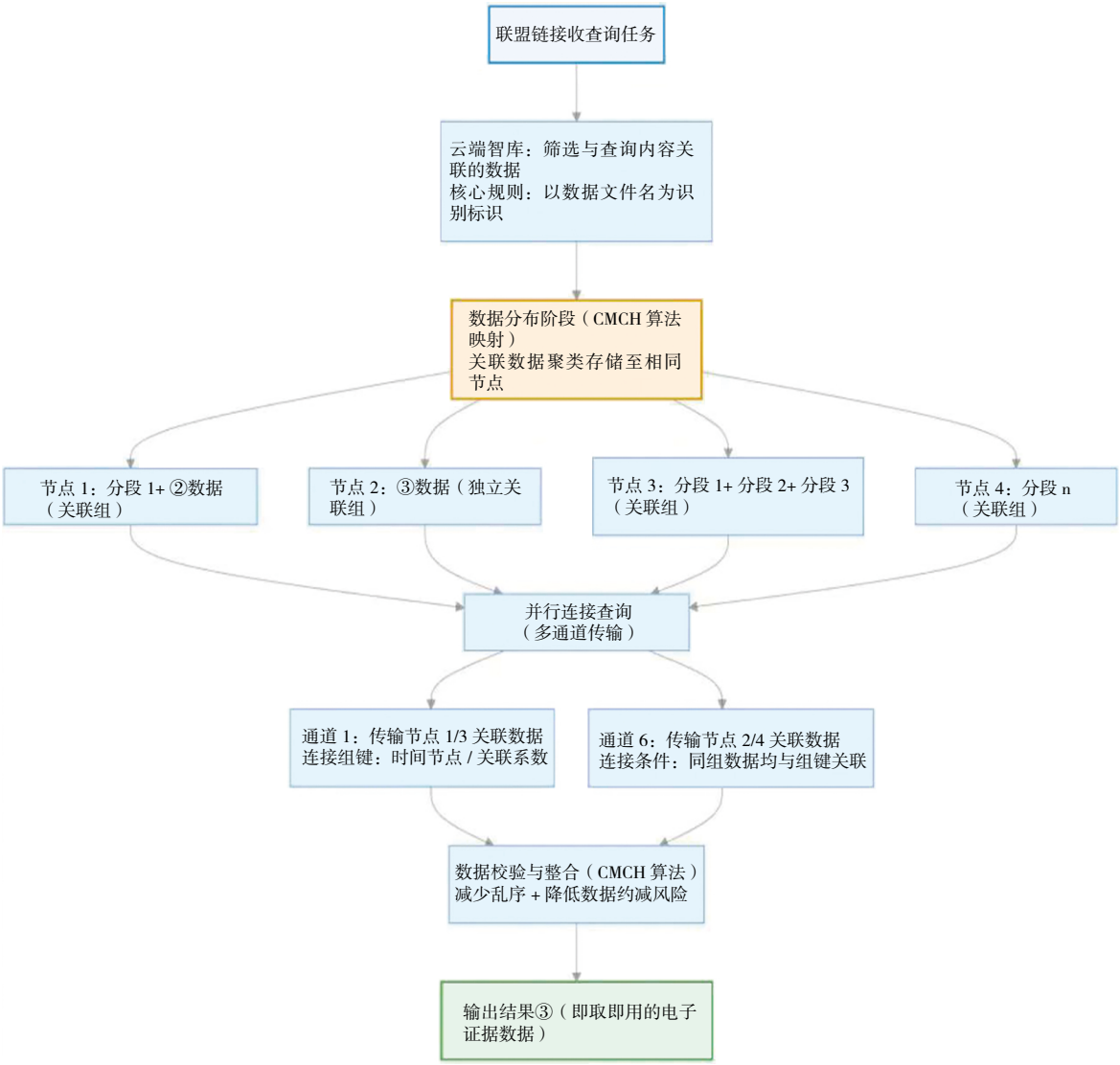

图 2　云端智库大数据并行连接查询流程

（三）“赋能处理”区块链所固定的虚拟货币洗钱犯罪的电子证据

“数智赋能处理云端智库”采用基于数据相关性的多副本一致性哈希数据存储算法（CMCH），对区块链固定的虚拟货币洗钱犯罪电子证据进行大数据并行连接查询，使电子证据及其相关数据在传输过程中减少乱序情况的发生，降低电子证据的数据约减风险。云端智库在映射阶段充分考虑到数据间的关联性，将关联数据排列在相同数据节点，然后进行数据连接，具体过程如图3所示。

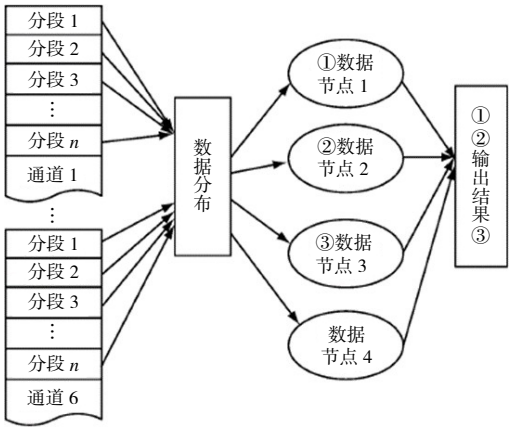

图 3　云端智库数据分布图

（1）当联盟链接收查询任务时，云端智库自动筛选出与查询内容有关联的数据；

（2）云端智库可将固定的虚拟货币洗钱电子证据的时间节点或关联系数作为连接组键进行连接查询；

（3）云端智库以数据文件名作为数据源中虚拟货币洗钱犯罪电子证据数据记录的识别标识；

（4）连接虚拟货币洗钱相关电子证据数据的条件是：同组内的数据都与连接组键具有关联性[1]。

在缅北跨境犯罪生态中，犯罪集团的违法活动已形成涵盖网络贩毒、电信诈骗、虚拟货币洗钱等多维度危害国际金融安全的犯罪链条。为实现非法资金流通并规避国际执法机关的电子证据溯源与信息追踪，犯罪分子在洗钱过程中常对区块链智能合约进行技术性篡改，这一现象即区块链技术应用于虚拟货币洗钱电子证据固定时面临的“智能合约异化”问题。经区块链技术固定的洗钱犯罪电子证据以数字代码形式传入云端智库系统后，需在联盟链各节点间完成共识验证。尽管验证节点可识别代码的哈希编码形态，但其真实语义因加密技术被遮蔽，而经恶意篡改的“异化代码”更呈现语义解构特征，导致自然语言系统与计算机语言系统形成认知断层——这正是犯罪集团通过专业技术人员利用代码语义隐蔽性掩盖违法意图的核心技术路径。以以太坊生态中的The DAO事件为例，其智能合约因代码逻辑漏洞遭黑客攻击，导致价值约6000万美元的加密资产流失。从智能合约运行原理分析，其“代码即法律”的执行机制决定了合约状态的不可逆性，这意味着云端智库若遭入侵，可能引发全库数据不可逆销毁的灾难性后果。数智技术对云端智库的赋能，本质上是在系统入口构建动态密钥验证机制：针对存在异化风险的哈希编码，通过多链访问控制技术实施二次证据固定，实时关闭异常侧链的读写权限，并基于神经网络算法对代码动态进行语义解析。该技术路径通过联盟链共识机制与可信计算技术的协同运作，可在确保电子证据完整性的前提下，实现对洗钱犯罪链的全链路追踪。

（四）数智赋能联盟链调取固定在云端智库中的电子证据

在公检法联盟链体系中，电子犯罪证据的调取呈现显著的技术异化特征，云端智库存储的证据形态已超越传统物证、书证等法定形式，转化为基于区块链技术的数字代码集合。该代码库遵循区块链技术架构的四层技术栈模型，分别为：基础数据层、网络传输层、共识机制层与应用服务层。其中，基础数据层作为区块链技术底座，集成链式数据结构、时间戳服务、梅克尔树算法、哈希加密函数及非对称密钥体系等核心技术要素；网络传输层构建P2P分布式通信网络，实现节点间数据传播的去中心化共识；共识机制层作为技术核心，支持工作量证明（POW）、权益证明（POS）等多种分布式共识算法；应用服务层则聚焦区块链技术的现实场景落地，涵盖区块链金融、供应链管理等垂直领域[2]。

在联盟链环境下调取虚拟货币洗钱犯罪的电子证据时，需借助“区块链数据溯源技术”实现证据链的重构。该技术通过时间戳对齐算法与数据源匹配模型，在侧链网络中完成同时间节点、相似数据源的代码筛选，并基于密码学排序规则构建完整的数据链路。其核心技术路径具体表现为：首先通过哈希值比对锁定异常交易数据段；其次运用智能合约实现跨链数据协同验证，进而通过数据串重组算法完成代码逆向解析；最后将加密代码还原为可被司法系统识别的原始证据形态。数智技术对区块链溯源的赋能，本质上是构建基于大数据分析的全息追踪模型——通过将海量数据节点纳入知识图谱，运用机器学习算法实现数据流动的全生命周期可视化，从而在联盟链环境中建立“代码—证据”的双向映射机制。

四、结语

跨境虚拟货币洗钱犯罪的治理是一场技术革新与制度博弈并行的持久战，其匿名性、跨国性与技术复杂性对传统反洗钱框架提出了颠覆性挑战，但亦倒推全球监管体系向更开放、协同的方向演进。

［1］李伟平．云计算环境下取证及证据管理模型研究［D］．保定：河北大学，2016.

［2］陈平祥，姜琪，朱冠琳．论运用区块链技术提取和审查刑事电子数据［J］．网络信息法学研究，2019（1）：157-170，336-337.

破解这一困局，需不断提高电子数据的取证能力、完善取证流程，从而形成标准化取证范式。未来，随着数智赋能、AI溯源等技术的突破，跨境虚拟货币洗钱犯罪的“攻防战”将进入更高维度。唯有以动态治理思维融合技术创新与制度韧性，方能实现“魔高一尺，道高一丈”的制衡，为全球金融安全筑牢防线，也为数字经济时代的法治化治理提供中国智慧与中国方案。

（责任编辑：蒋修能）

Breaking the “Cat and Mouse Game” of Cross-Border Virtual Currency Money Laundering Crime — Path Optimization Based on Multi-Source Data Fusion of Cloud Think Tank

Li Chaoyi

School of Criminal Justice, Zhongnan University of Economics and Law, Wuhan

Abstract: In the era of deep integration between the digital economy and globalization, virtual currencies represented by Bitcoin, with their decentralized architecture, anonymous transaction characteristics, and cross-border circulation advantages, have become a new carrier for cross-border money laundering crimes. Statistics show that the global virtual currency money laundering scale exceeded the $20 billion threshold in 2024, with cross-border money laundering accounting for 60%. The cross-regional mobility, technological concealment, and regulatory arbitrage characteristics of such crimes pose a subversive challenge to the traditional anti-money laundering governance system. Through in-depth deconstruction of the four core models of virtual currency money laundering—anonymous wallet mixing services, cross-chain bridging and decentralized finance (DeFi) operations, and darknet trading ecosystems—it is evident that they face governance dilemmas in electronic data forensics, such as massive and decentralized data storage and enhanced anonymity technology countermeasures. In response to the new patterns of money laundering crimes in the big data era, public security and judicial authorities need to break down industry barriers, establish cross-departmental judicial collaboration mechanisms, and promote the construction of cloud-based think tank systems. These measures will significantly improve the efficiency and accuracy of electronic data forensics, providing a solid judicial guarantee and technical support for combating cross-border virtual currency money laundering crimes and safeguarding national financial security and order.

Key words: Virtual currency; Cross-border money laundering crimes; On-chain governance; Cloud think tank