



北京警察学院学报
Journal of Beijing Police College
ISSN 2095-5758, CN 10-1116/D

JOURNAL OF BEIJING POLICE COLLEGE

《北京警察学院学报》网络首发论文

题目: 理性选择理论视角下利用虚拟货币洗钱犯罪防控对策研究——以裁判文书网 283 份判决书为样本
作者: 罗正青, 张雍锭
DOI: 10.16478/j.cnki.jbjpc.20251020.001
收稿日期: 2025-04-23
网络首发日期: 2025-10-20
引用格式: 罗正青, 张雍锭. 理性选择理论视角下利用虚拟货币洗钱犯罪防控对策研究——以裁判文书网 283 份判决书为样本[J/OL]. 北京警察学院学报.
<https://doi.org/10.16478/j.cnki.jbjpc.20251020.001>



网络首发: 在编辑部工作流程中, 稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定, 且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式(包括网络呈现版式)排版后的稿件, 可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定; 学术研究成果具有创新性、科学性和先进性, 符合编辑部对刊文的录用要求, 不存在学术不端行为及其他侵权行为; 稿件内容应基本符合国家有关书刊编辑、出版的技术标准, 正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性, 录用定稿一经发布, 不得修改论文题目、作者、机构名称和学术内容, 只可基于编辑规范进行少量文字的修改。

出版确认: 纸质期刊编辑部通过与《中国学术期刊(光盘版)》电子杂志社有限公司签约, 在《中国学术期刊(网络版)》出版传播平台上创办与纸质期刊内容一致的网络版, 以单篇或整期出版形式, 在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊(网络版)》是国家新闻出版广电总局批准的网络连续型出版物(ISSN 2096-4188, CN 11-6037/Z), 所以签约期刊的网络版上网络首发论文视为正式出版。

理性选择理论视角下利用虚拟货币洗钱犯罪防控对策研究

——以裁判文书网 283 份判决书为样本

罗正青, 张雍锭

(中国人民公安大学, 北京 100038)

摘 要:以近十年裁判文书网中的 283 份利用虚拟货币洗钱犯罪案件判决书为样本, 揭示我国此类洗钱行为多依托帮信罪、掩隐罪等罪名完成, 并呈现操作主体年轻化, 犯罪集团大量利用社会经济地位边缘化的青年群体作为犯罪工具, 地域集聚显著, 初高中学历居多的五大特征。其行为成因归结于潜在行为人在有限理性下, 因认知偏差和逐利动机而产生犯罪意图, 对于被招募的底层人员而言, 其感知的犯罪成本远低于其感知的收益, 形成了强烈的短期诱惑, 虚拟货币的技术匿名性与监管穿透力失衡提供了作案条件。理性选择理论中的“理性”应理解为行为人在有限信息与认知约束下, 以自我利益为考量进行的成本收益计算, 其决策未必符合社会规范, 却在其自身主观层面具有“合理性”。可以通过破除“技术匿名”认知误区, 强化司法案例震慑的犯罪倾向干预措施; 建立链上资金穿透式追踪与跨国协查机制的犯罪机会阻断措施; 压缩 OTC 交易渠道, 实施虚拟货币——法币兑换全域监管的犯罪收益压制措施构建三位一体的防控体系。

关键词:虚拟货币; 理性选择理论; 区块链; 犯罪治理; 洗钱

随着互联网技术的飞速发展, 以比特币为代表的虚拟货币发展成为一种被越来越多民众知晓的金融新主张。这类虚拟货币具有去中心化、记账留痕、数量恒定、国际化和抗通胀等特殊属性,^[1]这既是它受追捧的原因, 同时也是滋生犯罪的温床, 其中以比特币为代表的虚拟货币尤为典型。根据全球虚拟货币行业大数据平台 CoinCarp 的统计数据显示, 截至 2025 年 2 月 7 日, 虚拟货币种类达到 3 万 3 千多种, 交易所 355 家, 全球虚拟货币流通总市值达到 4.0 万亿美元, 其中比特币占总市值的 48.0%。与 2024 年 9 月的 2.1 万亿美元相比, 全球虚拟货币流通总市值在短短半年内增长接近一倍。^[2]从风险传染速度来看, 换手率是金融资产流通速度的度量衡。根据全球稳定币权威机构 StablecoinIndex 发布的数据, USDT, 又称稳定币^①, 交易换手率常年居高不下, 单日可高达 99.17%, 其他主流稳定币的换手率也均高于 30%, 日交易额可达五百亿至千亿美元。^[3]这种

收稿日期: 2025-04-23 修回日期: 2025-09-27

作者简介:罗正青(2001—), 男, 中国人民公安大学 2024 级犯罪学专业硕士研究生, 研究方向为犯罪学; 张雍锭(1989—), 男, 中国人民公安大学犯罪学院副教授, 研究方向: 少年司法、犯罪学、罪犯矫正。

^①稳定货币是一种与法定货币兑换价格相对稳定的虚拟货币。它锚定某一国家的法定货币或其他资产, 每发行一个单位量, 便会有相应的资产储备。

畸高换手率，具有任何金融产品都无法比拟的流动性。高流通性再加上虚拟货币本身的匿名性、跨区域性的特点，致使以虚拟货币作为犯罪对象或犯罪手段、犯罪工具的刑事风险也日渐凸显。^[4]

相较于传统洗钱犯罪模式，基于区块链技术的虚拟货币洗钱行为^①，因分布式账本架构的匿名性、链上交易不可逆性及去中心化节点特征，呈现出技术壁垒高、隐蔽性强的双重特性，在很大程度上使得虚拟货币脱离传统的金融监管体系，给执法部门带来了巨大的挑战。据欧科云链研究院统计，洗钱、诈骗、传销、赌博是 2022 年最常见的四种虚拟货币犯罪形式，其中高达 54.72% 的虚拟货币犯罪与洗钱相关。^[5]2025 年 1 月 10 日，公安部新闻发言人张明在新闻发布会上表示，当前诈骗集团利用区块链、虚拟货币、人工智能（AI）等新技术手段持续升级犯罪工具，涉虚拟货币电信网络诈骗犯罪形势严峻复杂。对此，公安机关将深入推进“云剑”“断流”“拔钉”等专项行动，始终保持严打高压态势。^[6]2025 年 1 月 13 日，最高人民检察院在全国检察长会议上强调，检察机关将依法加大惩治洗钱犯罪力度，重点打击利用虚拟货币等新型手段非法向境外转移资产的犯罪行为。^[7]本文旨在运用理性选择理论，剖析利用虚拟货币洗钱犯罪的生成机制，并提出针对性的防控对策。

一、利用虚拟货币洗钱犯罪的概念厘定

对利用虚拟货币洗钱犯罪进行精准界定，是展开后续路径与规制研究的前提。而理解这一犯罪，首先必须厘清其核心犯罪工具虚拟货币的法律性质与基本分类，并明确其被用于洗钱活动时的特殊含义。

（一）虚拟货币的法律属性与分类框架

在我国，法律上如何界定虚拟货币的法律性质，在理论界和实务界均存在较大的争议，其中最主要的三种争论分别是财产说、货币说和证券说。财产说是我国的主流学说，大部分学者认为虚拟货币应当属于《民法典》第 127 条规定的网络虚拟财产。^[8]在人民法院案例库的参考案例的裁判要旨中，明确提出“虚拟货币具有刑法意义上的财产属性，可以成为财产犯罪的对象”。^②可见，虚拟货币被定性为一般法律意义上的财产（商品）。在现行司法实践中，除比特币（BTC）、

^①本文探讨的洗钱犯罪，指的是通俗语境下广义的洗钱犯罪行为，即不限缩于《刑法》第 191 条所规定的洗钱罪行为类型，其外延涵盖所有类型掩饰、隐瞒各类犯罪所得及其收益的关联行为。

^②参见最高人民法院案例库入库案例：陈某等诈骗案（入库编号：2024-04-1-222-007）。

以太坊（ETH）、泰达币（USDT）等具有市场共识的虚拟货币外，境外市场中流通的虚拟货币种类已逾万种。笔者主张，仅主流虚拟货币可被纳入刑法第 92 条所规定的“财物”范畴予以保护，其他非主流虚拟货币的刑法属性需审慎认定：其一，非主流币种因发行机制混乱、技术标准模糊及生态体系脆弱等特征，尚无法形成统一的司法认定标准；其二，司法实务中，山寨币多作为传销组织、非法集资类犯罪的犯罪工具出现，行为人通过以太坊智能合约或自建链发行虚拟货币，实则系以虚假技术概念包装的非法资金盘，其价格操控空间显著、市场流通性及价值稳定性存疑，故不宜直接赋予其刑法意义上的财产属性。对于虚拟货币案件展开司法评估时，需要构建起一个多维度审查体系，此审查体系重点关注的内容包括底层技术逻辑、实际应用场景、项目团队所呈现出的表现，以及是否契合交易所的流动性指标和变现途径，结合具体个案的证据来综合确定其属性。

虚拟货币、数字货币、央行数字货币以及电子货币的概念界定乃是研究虚拟货币犯罪的前提条件，长久以来，学术界对于这些概念一直缺乏统一的认知，笔者借助构建分类框架（如图 1 所示）可清晰地呈现各类数字货币的隶属关系以及核心差异。

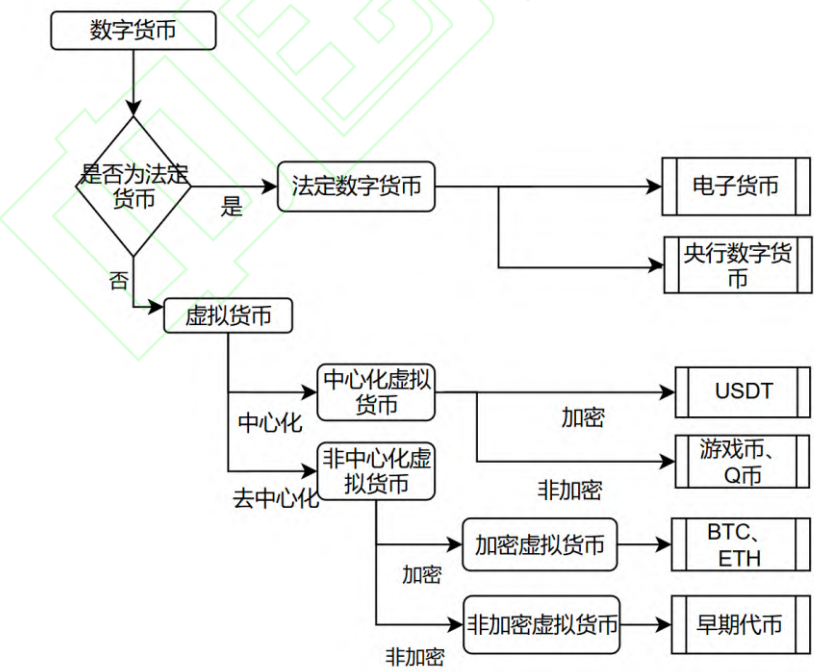


图 1 数字货币分类框架

据此，本图以法定属性为核心标准，将数字货币划分为两大类别，并进一步通过中心化程度与技术特性细化分类。在区块链技术诞生之前，中心化虚拟货币是指 Q 币、游戏币等只能在特定场景内使用，无法直接在场景外主体之间实现转移的货币，在区块链技术诞生之后，诞生了诸如泰达币等基于区块链技术作为底层架构的虚拟货币；去中心化虚拟货币通常由私人主体发布，没有国家或地区的信用作为担保，其信任基础来自于区块链技术，此类虚拟货币不具备法定货币地位，但具有支付、结算功能，通常被用于洗钱犯罪当中。

对于虚拟货币的定义，各国尚无统一的标准。在通俗语境中，广义的虚拟货币可泛指游戏币、数字货币、加密货币等多种虚拟货币。而在国内国外的相关文件中，虚拟货币的语义则相对狭小。我国现行法律并未明确定义虚拟货币，仅在特定文件中将比特币视为“一种特定的虚拟商品”。^①美国金融犯罪执法网络（FinCEN）定义虚拟货币为一种交换媒介，其使用和流转是具有合法性的，可以类似货币进行流通，但不具备货币属性。^[9]日本 2016 年立法将虚拟货币定义为“通过电子信息系统处理，可以在不特定主体之间用于清偿债务、既非法定货币也不以法定货币计价的财产性价值”。^[10]根据欧洲银行管理局（EBA）的定义，虚拟货币是“价值的一种数字表达”，非由中央银行或公共权威机构发行，也不一定与法定货币挂钩，但被自然人或法人接受为支付手段，可进行电子化转移、存储或交易。^[11]根据反洗钱金融行动特别工作组（FATF）发布的相关文件，虚拟货币不具备法定地位的数字化价值表达，具有转移与交易的功能，可用于支付、投资。^[12]总之，虚拟货币可定义为：由私人或者社群发行，借助区块链技术达成去中心化或者中心化流通，依靠一定算法保证交易安全，于特定社群或者开放网络之中承担支付、投资以及权益凭证功能，以数字化形式存在的价值载体。

（二）对利用虚拟货币洗钱犯罪的界定

“利用虚拟货币洗钱犯罪”在本质上并未脱离传统洗钱罪的范畴，其核心仍是对刑法第一百九十一条所规定的上游犯罪所得及其收益进行“掩饰、隐瞒”，使其在形式上合法化。该犯罪的特殊性在于，其以去中心化、匿名性或准匿名性、

^①参见中国人民银行、工业和信息化部、原中国银行业监督管理委员会、原中国证券监督管理委员会、原中国保险监督管理委员会于 2013 年 12 月 3 日联合发布的《关于防范比特币风险的通知》（银发〔2013〕289 号）。该文件是我国首部对比特币等加密货币进行系统性风险提示的规范性文件，明确比特币不具有法定货币地位，并禁止金融机构开展相关业务。

全球可兑换性等作为核心特征的虚拟货币作为核心工具与通道。犯罪分子通过将非法所得转换为虚拟货币，并利用其跨国界、点对点传输的特性，再结合链上混币、跨链桥、去中心化交易所等区块链特有生态，实施资金转移、混淆路径与最终变现，从而极大地增加了资金链路的追踪与监管难度，构成了信息时代下洗钱活动的新范式。综上，我们可以对“利用虚拟货币洗钱犯罪”进行概念界定。它指的是洗钱犯罪分子利用虚拟货币作为工具或通道，试图掩饰、隐瞒犯罪所得及其收益的来源和性质，使其在形式上合法化的犯罪行为。

二、利用虚拟货币洗钱犯罪路径分析

虚拟货币凭借其匿名性、跨境流动便捷性及交易不可逆性等核心特性，天然降低了洗钱活动的门槛和风险，从而被犯罪分子利用作为新型洗钱工具。区块链技术的匿名性滋生了虚拟货币洗钱犯罪，其跨境流通性进一步加剧治理难度，与虚拟货币相关的犯罪近些年才涌现，而当前我国《刑法》尚未规定虚拟货币犯罪这一罪名乃至类罪，学术界对此类犯罪的概念也未形成共识，本文认为虚拟货币洗钱犯罪，是指犯罪分子利用虚拟货币的匿名性、跨境性和易变现性，将非法所得及其产生的收益通过多次交易或转换，掩饰、隐瞒其来源和性质，使之合法化的行为。^{[13]60}

在对虚拟货币的概念与法律属性进行厘定后，需进一步剖析其被用于洗钱的具体运作模式。本部分旨在衔接上文的技术特性，并为下文分析此类犯罪的现状特征与生成机制奠定基础，核心在于揭示犯罪分子如何利用虚拟货币的匿名性、跨境流动性及交易不可逆性等核心特性。洗钱行为通常包含放置（Placement）、离析（Layering）、融合（Integration）三个阶段。虚拟货币的特性使其在离析阶段尤其高效。其主要洗钱路径如下：

1. 法币—虚拟货币—法币的兑换洗钱路径。这是最为常见的模式。犯罪分子首先将犯罪所得的法定货币通过场外交易（OTC）、交易所或非法兑换点转换为虚拟货币（如 USDT、BTC）。随后，利用虚拟货币的匿名性和跨境性进行多次、跨链、混币交易，以离析资金，切断其与上游犯罪的联系。最后，在境外或其他地区将清洗后的虚拟货币再次兑换成法定货币，并融入合法经济体系。整个路径的核心在于利用虚拟货币作为“中转站”，实现赃款的跨境转移和性质遮掩。

2. 利用隐私币和混币器增强隐匿的路径。为应对链上分析技术，犯罪分子

会采用更高级的隐匿手段。一是直接使用门罗币等隐私币进行交易，利用其原生匿名技术逃避追踪。二是使用混币器（Mixer）或翻滚器（Tumbler），将犯罪资金与大量无关资金混合，打乱资金流向，混淆交易记录，使得执法机构难以追溯资金来源和去向。

3. 基于 DeFi 和跨链桥的复杂化路径。随着去中心化金融（DeFi）的发展，洗钱路径更趋复杂。犯罪分子可以利用跨链桥将资产在不同区块链网络（如从比特币网络到以太坊网络）之间转移，利用不同链的协议差异增加追踪难度。随后，通过在 DeFi 协议中进行质押、借贷、流动性挖矿等操作，进一步模糊资金链条，将非法所得与 DeFi 生态产生的合法收益相混合，完成洗白。

三、我国利用虚拟货币洗钱犯罪现状分析

在中国裁判文书网中使用高级检索功能，通过对涉及虚拟货币洗钱的刑事案件进行检索，^①删除与虚拟货币犯罪无关判决书，共收集到刑事判决书 283 份，覆盖全国 30 个省级行政区，形成具有代表性的全国性样本分析，能比较系统地呈现我国虚拟货币洗钱犯罪的特征。

（一）虚拟货币洗钱犯罪总体呈现上升趋势

随着区块链 3.0 时代的到来，以区块链技术作为底层架构的虚拟货币成为了洗钱犯罪的重要工具，利用虚拟货币进行洗钱的犯罪行为呈现出明显增长的趋势。^[14]我国虚拟货币相关犯罪形势严峻，据 SAFEIS 安全研究院统计，我国在 2023 年已打击涉虚拟货币犯罪案件总量 428 件，较 2022 年减少了 88.9%，但整体涉案金额陡增至 4307.19 亿元人民币，约是 2022 年的 12.36 倍，对我国金融安全造成了穿透性威胁。^[15]根据裁判文书网关于按年统计案件数量结果，为了揭示市场周期与犯罪量的相关性，本文（如图 2 所示）采用双轴叠加呈现。左侧纵轴为十年间的虚拟货币洗钱案件数，右侧为比特币价格曲线。

从案件数量来看，过去十年间，我国虚拟货币洗钱犯罪案件数量呈现高速增长态势，尤其是 2019 年至 2021 年数量激增，2021 年更是达到了 108 起，平均每年涨幅约为 292.7%。相比 2021 年，2022 年判决案件数量快速下降，2024 年判决案件数量又有所反弹。可见，随着虚拟货币在公众追捧下热度不断提升，相关犯罪

^①笔者在“中国裁判文书网”平台上设置如下检索条件：案件类型为“刑事案件”，全文搜索为“虚拟货币”、“洗钱”，案由为“刑事案由”，审判程序为“刑事一审”，文书类型为“判决书”，时间设置为“2015 年 1 月 1 日—2024 年 12 月 31 日”。

案件数量可能会继续保持高速增长。^[16]

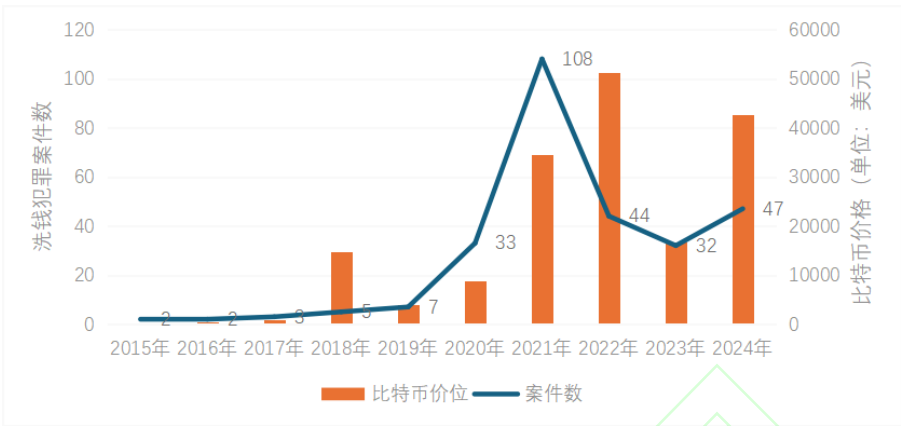


图 2 虚拟货币洗钱犯罪刑事案件判决数量与比特币价位统计图

借助对虚拟货币犯罪趋势与比特币价格走势展开对比,可观察到二者整体的演化态势颇为相似,在 2021 年,二者同时抵达峰值,呈现出一定程度的正相关关系,在市场处于高涨阶段时,像 2024 年等其他年份,比特币价格再度上扬,案件数量也出现了反弹,只是涨幅不像 2021 年那般较大。当价格处于高涨状态时,犯罪分子会更倾向于借助比特币来进行洗钱活动,原因在于市场流动性有所提升,这使得非法活动更易于被掩盖,不过在某些年份,二者的趋势并非一致,举例来说,2018 年比特币价格大幅上升,然而案件数量仅有 5 起,相对而言处于较低水平,这是由于当时虚拟货币的普及程度还不够,并且犯罪手段也尚未成熟。到了 2021 年,随着技术以及工具的成熟,比如 DeFi 和隐私币的出现,洗钱犯罪活动变得更便于实施,案件数量急剧增加。

国内监管政策的变化也是造成这种数据表现的重要原因。自 2020 年 10 月起,全国各地陆续开展严厉打击整治非法租售的电话卡、银行卡违法犯罪活动的专项整治行动。^[17]2021 年 2 月,国务院处置非法集资部际联席扩大会议提出 2021 年需要密切关注打着“区块链”和“虚拟货币”等旗号的新型网络犯罪风险。2021 年 9 月,中国人民银行等十部门联合发布《关于进一步防范和处置虚拟货币交易炒作风险的通知》,再次明确虚拟货币不具有法定货币地位,虚拟货币相关业务活动属于非法金融活动,应当一律禁止和取缔。^[18]2021 年底,火币、币安、OKEx 接连表态退出中国市场,这些举措对遏制虚拟货币犯罪的蔓延趋势起到了积极作用,导致 2022 年、2023 年案件数下降。但 2024 年随着技术对抗的升级,如利

用混币器通过将用户的加密货币与其他用户的加密货币进行混合洗钱、使用跨链桥协议实现资产匿名置换等方法使得交易路径变得模糊不清,这些手段使得洗钱案件数再次上升。这说明监管措施能在短期内抑制犯罪,但监管措施的效果倒逼犯罪技术迭代,使得犯罪手段也在不断进化,可能导致后续洗钱案件数量反弹。

（二）我国虚拟货币洗钱犯罪的特点

根据 2015 年至 2024 年中国裁判文书网判决书的统计分析,通过对不同案由的检索,虚拟货币犯罪案件共计 278 件。可以发现,掩饰、隐藏犯罪所得、犯罪所得收益罪最多,共 133 件,占 47.84%;其次是帮助信息网络犯罪活动罪,达 59 件,占 21.22%;再次是诈骗罪,共 43 件,占 15.47%。此外,近年来网络赌博、开设网络赌场类犯罪日益猖獗,网络赌场经营者往往也会利用虚拟货币进行洗钱,逐渐成为虚拟货币洗钱犯罪的另一大资金来源。^[19]

表 1 案件类型分布

案件罪名	案件数量（件）	案件数量占（%）
掩饰、隐瞒犯罪所得、犯罪所得收益罪	133	47.84
帮助信息网络犯罪活动罪	59	21.22
诈骗罪	43	15.47
开设赌场罪	12	4.32
洗钱罪	6	2.16
非法吸收公众存款罪	3	1.08
妨害信用卡管理罪	3	1.08
集资诈骗罪	2	0.71
窃取、收买、非法提供信用卡信息罪	2	0.71
敲诈勒索罪	1	0.36
其他	14	5.04
总计	278	100

1. 行为主体低龄化与高风险决策偏好

犯罪人多为青壮年。18 岁至 29 岁年龄段的人是当前虚拟货币洗钱犯罪的主要群体,占 40.58%,其次为 30 岁至 39 岁,占 26.43%,而 40 岁以上所有罪犯

占比仅有为 10.09%，该年龄分布特征反映了不同群体在有限理性下的差异化决策偏好。18 至 39 岁的青年群体对新技术接受度高，学习能力强，能快速掌握虚拟货币钱包、混币器等操作工具，其决策更易受短期高收益预期的驱动。同时，该年龄段个体往往处于经济压力较大的人生阶段，对合法收入的预期收益评估较低，而对非法收入的乐观偏见较强。青壮年普遍存在的风险偏好强、惩罚预期低的心理特征，使其在成本—收益计算中，显著低估了利用虚拟货币洗钱的长期法律风险，而高估了其便捷性和隐匿性带来的短期收益，从而更倾向于选择该行为。

表 2 犯罪人年龄分布

罪犯年龄	人数（人）	人数占比 （%）	罪犯年龄	人数（人）	人数占比 （%）
18-29	390	40.58	60-69	无	0
30-39	254	26.43	70-79	1	0.10
40-49	68	7.08	不详	220	22.89
50-59	28	2.91	总计	961	100

2. 行为技能低门槛化与有限理性约束

犯罪人多为初高中学历。数据显示，初中学历罪犯占比最高，达 37.46%，其次为高中和大专学历，分别占 11.65%和 11.55%，本科和研究生学历占分别为 0.31%和 8.12%。高中及以下学历合计超 50%，低学历化特征揭示了此类洗钱行为的去技术化和产业化分工本质。犯罪团伙通过层级化、组织化运作，将复杂的洗钱流程拆解为出租银行卡、场外兑换等低技能、标准化任务。对于低学历主体而言，在其有限理性的决策框架内，无需理解区块链技术原理，只需执行简单指令即可获得远高于其合法劳动所得的报酬。这种“低技能门槛—高经济回报”的强烈对比，极大地扭曲了其成本—收益计算，驱动其选择参与犯罪。而本科及以上学历者虽占比少，但多充当技术骨干和组织者，其决策更基于对技术漏洞的深刻理解和利用，是另一种形式的“理性”选择。

表 3 犯罪人学历分布

罪犯学历	人数（人）	人数占比 （%）	罪犯学历	人数（人）	人数占比 （%）

研究生	3	0.31	初中	360	37.46
本科	78	8.12	小学	64	6.66
大专	111	11.55	文盲	1	0.10
高中	112	11.65	不详	129	13.42
中专	103	10.72	总计	961	100.00

3. 行为地域集聚化与犯罪机会传导

犯罪人户籍地呈现出明显的地域集聚性。一是从案件审判机关所属地域来看,全国有 30 个省级区域出现了虚拟货币犯罪案件,出现 10 件以上的有 5 个省,分别是湖南、河南、甘肃、陕西、四川,二是从涉案人员户籍地分布情况来看,湖南籍罪犯人数最多,共 174 人,占 18.11%,其次是河南省,共 124 人,占 12.90%,再次是四川籍 71 人,占 7.39%。地域集聚性并非偶然,它反映了犯罪机会通过地缘、亲缘社会网络的传导效应。在理性选择过程中,个体不仅评估行为的抽象成本与收益,更依赖于其可接触的信息和机会。当某一地区出现利用虚拟货币洗钱的“成功”案例后,其操作模式、犯罪工具和销赃渠道会通过本地社会关系网络迅速扩散,显著降低了潜在行为人的学习成本和入行门槛。这种身边人的示范效应,为其提供了清晰的犯罪路径和“安全”错觉,使其在决策时更容易获得正面的收益预期和低风险评估,从而形成地域性的行为选择偏好。

表 4 犯罪人户籍地分布

籍贯	人数(人)	人数占比(%)	籍贯	人数(人)	人数占比(%)
湖南	174	18.11	广东	20	2.08
河南	124	12.90	山西	17	1.77
四川	71	7.39	新疆	16	1.66
黑龙江	62	6.45	河北	13	1.35
安徽	60	6.24	贵州	12	1.25
甘肃	47	4.89	辽宁	11	1.14
江苏	38	3.95	上海	9	0.94
浙江	36	3.75	宁夏	9	0.94
吉林	35	3.64	山东	7	0.73
福建	32	3.33	天津	6	0.62

陕西	30	3.12	青海	5	0.52
江西	26	2.71	海南	2	0.21
湖北	26	2.71	重庆	2	0.21
广西	24	2.50	北京	1	0.10
内蒙古	22	2.29	其他	3	0.31
云南	21	2.19	总计	961	100

4. 行为动机经济化与边际收益抉择

犯罪人多为无业和务工人员。无业人员占比最高，达 40.27%，务工与农民群体次之，占比之和达到 19.15%，自由职业者和个体户也是虚拟货币洗钱犯罪的高发群体，占比达到 7.91%。职业分布特征深刻揭示了行为选择的经济动机。无业、务工及农民群体在合法劳动力市场中面临边际收益递减的困境，其合法收入的预期价值较低。而当其评估利用虚拟货币洗钱的收益时，犯罪团伙许诺的“高额佣金”形成了巨大的诱惑力。在其主观理性的权衡中，从事合法工作的机会成本远低于从事犯罪活动的预期收益。因此，即使面临法律风险，他们也更倾向于选择能带来即时、高额经济回报的洗钱行为。对于自由职业者和个体户，其职业的灵活性使其更易接触到黑灰产信息，从而拥有了更多的犯罪机会，其决策更基于对边际收益的精确计算，将参与洗钱视为一种“创收”渠道。

表 5 犯罪人职业分布

罪犯职业	人数（人）	人数占比 （%）	罪犯职业	人数（人）	人数占比 （%）
无业	387	40.27	经商	17	1.77
务工	100	10.41	职工	26	2.70
农民	84	8.74	法人代表	9	0.94
自由职业	52	5.41	其他	262	27.26
个体	24	2.50	总计	961	100.00

四、理性选择理论视角下利用虚拟货币洗钱犯罪生成机制阐释

在对虚拟货币洗钱的原因分析的研究上，笔者以古典犯罪学派中的理性选择

理论作为理论依据。理性选择理论（Rational Choice Theory）的假设前提是存在一个理性的经济人，其行动旨在通过最小的经济代价获取最大的经济利益。^[21]理论选择理论认为首先需要存在具备犯罪动机的犯罪人，犯罪人出于主观意志而进行犯罪，某种具体犯罪是犯罪行为特性与犯罪人特性相结合的产物，二者相互作用，决定了犯罪人的行为选择。^[22]理性选择理论源于古典犯罪学，其核心假设是犯罪人是理性的决策者。不过，这里所说的“理性”并非古典经济学中那种全知全能、完全理性的“经济人”假设，而是强调有限理性与主观理性。有限理性的核心观点是，个体决策并非在理想条件下进行，而是会受到信息不对称、认知偏差、时间压力与知识局限等因素的制约。他们并非追求“最优解”，而是在自身认知和能力范围内寻求满意解。例如，虚拟货币洗钱犯罪人可能高估技术的匿名性，低估执法部门链上追踪的技术能力，从而在“有限”的认知下做出了“理性”的犯罪选择。主观理性是指决策的“理性”标准是主观的，是基于犯罪人自身的价值观念、风险偏好和所处的环境设定的。一个在外部看来高风险、低收益的行为，在犯罪人自身的主观评估中可能是合理的。综合来看，影响犯罪行为产生的关键因素有三个：犯罪人的犯罪倾向、犯罪人的犯罪机会和犯罪结果的诱惑力。^[23]

（一）犯罪动机生成中的高收益驱动因素

犯罪人的犯罪倾向是指犯罪人个人的个性、能力等心理要素，虚拟货币洗钱犯罪人的犯罪倾向主要体现在对非法收益的强烈牟利动机、技术能力对其价值观的异化以及对风险偏好的高容忍度，他们基于无业、经济压力的自身处境和技术至上、低估风险的认知，对“犯罪”这一选项给出了高于“守法”的主观效用值，正是犯罪人观理性的集中体现。具体可从以下三方面分析：

1. 犯罪人高度认同非法收益的巨额性与便捷性

如果一个人没有令人满意的合法的赚钱途径，认为非法途径取得的利益很大，那么他就会趋向于实施犯罪。在有限理性的框架下，犯罪人的决策深受其社会经济地位和信息环境的制约。样本中无业（占 40.27%）、务工（占 10.41%）与农民（占 8.74%）群体占比较高，这表明该群体在合法劳动力市场中可能面临投入产出比低、社会资源匮乏的困境。在其主观理性的评估中，合法途径的边际收益显著低于非法途径。虚拟货币洗钱犯罪所承诺的高额报酬在其自身受限的认

知和处境下，构成了一个极具诱惑力的“满意解”。他们并非全知全能地评估所有风险，而是基于其可见的、迫切的经济压力，主观地赋予了犯罪收益极高的效用值，从而驱动了犯罪意图的形成。例如，杨某，无业，听说找银行卡将黄色网站上别人充值、打赏的钱转出来，一晚上最多能赚两万元的高额报酬，于是迅速准备好洗钱所需的押金，下载了“飞机”聊天软件，组建“车队”群开始洗钱。^①相较于合法职业的微薄收益，犯罪人对非法收入的预期更为乐观，此种主观认知构成了其利用虚拟货币洗钱的心理动因。

2. 区块链技术催生犯罪人价值观异化

技术能力在塑造犯罪人的主观理性方面扮演了关键角色。部分掌握区块链技术的犯罪人（如样本中的本科及以上学历者），长期沉浸于“代码即规则”的技术语境中，其有限理性表现为一种技术认知的偏差。他们将复杂的法律与社会规范简化为可操纵的技术参数，将“去中心化”理念主观地曲解为“去监管化”，甚至认为技术凌驾于法律之上。这种价值观的异化，使其在决策时对技术挑战成功和规避监管予以极高的主观效用，而低估了法律后果的严重性。虚拟货币洗钱相比于传统洗钱模式，具有一定的门槛，需要犯罪人研究监管漏洞，设计“虚拟货币+跑分平台”、“游戏代币跨境结算”等新型模式，利用虚拟货币的匿名性规避追踪，以及开发混币平台、自动化交易机器人等工具，掌握区块链技术、加密通信工具及混币服务的操作技能。具备一定区块链、金融知识，容易产生利用虚拟货币的匿名性规避追踪的犯罪动机。例如，张某，大学文化，通过买手在境外平台注册匿名账户，利用热钱包与冷钱包交替转移资金，甚至借助跨链技术将比特币转换为门罗币等匿名币以规避追踪，张某利用其负责客户端开发的工作便利，在火币钱包 IOS 客户端植入代码非法窃取用户私钥及助记词 6437 条，成功转换 5680 个数字钱包地址，并通过混币技术转移赃款，规避追踪后转入自有钱包。^②张某原负责火币客户端开发，掌握植入请求用户私钥和 RSA 加密算法代码的技术手段，在其主观理性的权衡中，技术成功的成就感与经济利益可能远远超过了其有限认知中所评估的法律风险。原本作为保障用户资产安全的加密算法和私钥管理机制，在他的技术思维中被理解为可操控的后台参数和数据流、现实世界的财产规则被虚拟世界的技术逻辑所取代，最终驱使他在错误认知下迈出犯罪

^①参见（2023）苏 0722 刑初 642 号。

^②参见（2024）沪 0104 刑初 74 号。

步伐。可见，潜在犯罪人掌握一定区块链技能对于实施虚拟货币犯罪的倾向较为明显。

3. 犯罪人风险偏好强且惩罚预期低

风险偏好是主动追求风险，喜欢收益的波动性胜于收益的稳定性的态度。当预期收益相同时，风险偏好越强的人越会选择风险大的决策，因为这会给他们带来更大的效益。学习和经验也会影响犯罪人的选择，当犯罪人有一定经验时，便能察觉和比较犯罪的风险和利益，因此知道何时应该冒险，何时应该小心，犯罪人对风险的评估是主观且有限的。从犯罪人的年龄结构来看，18至29岁的人群最多，占比40.58%，其次是30至39岁，占26.43%，青年犯罪人往往存在“乐观偏见”，其决策基于不完整的信息。他们看到的是虚拟货币洗钱平均涉案金额高达数万元的巨额收益，以及链上追踪的技术难度，从而主观地低估了被查获的概率和惩罚的严厉程度。这种“低惩罚预期”是其有限理性决策的一个关键输入变量。他们并非完全理性地计算全局风险，而是在其信息视野内犯罪团伙的鼓吹、对早期成功案例的观察，得出了一个主观上低风险、高收益的结论，进而强化了犯罪倾向。根据研究，虚拟货币洗钱案件的平均涉案金额高达2845万元，^[24]但实际破案率却不高，大量资金通过境外交易所或混币平台流向不可追踪的暗网钱包。不少犯罪人认为，即使被查获，司法机关也难以完整追溯资金链路，证明其主观故意，从而形成低风险高收益的心理认知。

（二）犯罪实施条件中的低成本因素

犯罪机会的存在，为犯罪人在有限理性下的决策提供了客观的可行性基础。犯罪人并非能利用所有技术漏洞，但他们能接触和理解的工具，恰恰构成了其主观决策环境中的机会集合。

1. 技术特性支撑的隐匿条件

虚拟货币的匿名性设计直接消解了传统金融监管的抓手，一方面，门罗币（XMR）等采用环签名技术的虚拟货币，犯罪资金可完全脱离身份绑定，基于虚拟货币的匿名性与去中心化特性，其钱包地址无需实名认证，交易通过点对点完成，脱离传统金融机构监管；另一方面，泰达币等稳定币凭借与法币的锚定关系，在跨境流动中既保持价值稳定，又利用区块链的即时到账特性，虚拟货币可瞬时转移至境外交易所，规避外汇管制，成为跨境洗钱的主要媒介。例如，吴某

接收泰达币作为犯罪报酬，通过欧易 APP 交易兑换人民币并转入亲属账户，依托区块链点对点匿名交易特性，使资金脱离身份认证及金融机构监管。^①犯罪人基于其有限的技术知识，主观地将虚拟货币的匿名性视为一种安全保证。他们可能并不完全理解链上分析技术的穿透能力，但门罗币的环签名、泰达币的跨境流动性等特性，在其认知中已被标记为高效的隐匿工具，显著降低了其主观评估中的犯罪心理成本和行为成本。

2. 监管协作存在的执行障碍

反洗钱监测分析在整个洗钱犯罪治理中处于核心与基础地位，只有监测效能提高，各部门的数据沟通与共享监管协作顺畅，才能适应虚拟货币领域反洗钱工作的要求。反洗钱局隶属于中国人民银行，负责组织协调反洗钱工作，牵头拟订反洗钱政策规章，监督检查金融机构履行反洗钱义务情况等。但其层级较低且缺乏跨部门协调权，难以整合公安、海关、网信办等部门的资源，且虚拟货币洗钱涉及链上交易、跨境支付、社交平台通信等多环节，但各部门数据共享机制缺失，导致追踪资金流时出现境内与境外之间的监测盲区。2025 年修订的《反洗钱法》虽强化了跨境协作框架，由于各国对洗钱罪的法律定义、构成要件及量刑标准存在结构性差异，如欧盟将虚拟货币交易平台纳入严格监管框架，而部分离岸金融中心仍允许匿名账户存在，这种法律冲突导致跨国案件法律定性困难。中国全面禁止虚拟货币交易平台，而美国、日本等国允许其合法运营并采用分级监管，这种制度鸿沟导致洗钱团伙将服务器和交易平台设在境外（如菲律宾、新加坡），利用监管宽松地区完成境内黑钱到境外法币的转换洗钱，而中国执法机构因“双重犯罪”原则限制难以跨境追责。例如，2021 年广州白云警方侦破的“币齐”平台洗钱案中，上游犯罪团伙依托境外服务器逃避打击，资金流向涉及东南亚多国。^②犯罪人将服务器设置于境外监管宽松地区的行为，可归因于其对各国监管政策差异的有限理性利用。这并非建立在对国际司法协作体系的全面认知之上，而是基于“国外管得松，钱好出去”这一简单信息。此种主观机会认知，构成了其犯罪决策的关键支撑。

3. 犯罪工具的产业化供给

^①参见（2023）湘 8602 刑初 19 号。

^②《轻信直播间“投资高手”市民“炒币”被骗近 500 万元》，载央视网新闻网，<https://news.cctv.com/2021/04/01/ARTI3HLg9aIutmPREMuGZvnG210401.shtml>，2025 年 4 月 29 日访问。

犯罪生态呈现专业化分工特征，一方面，由于跑分平台与加密通讯的猖獗，犯罪分子通过社交媒体招募买手，利用“天马跑分”等平台实现赃款与虚拟货币的快速兑换，佣金高达 10%—15%，吸引社会人员参与赃款清洗。另一方面，随着开源工具与教程普及，暗网流通的混币脚本、批量地址生成器等开源工具，配合详细操作教程，形成从工具供应、技术指导到人员招募的完整犯罪支持链条，大幅降低了犯罪技术门槛。例如，被告人张某作为上线提供诈骗链接，明某负责培训及转发，关某等三人以虚假身份在微信群推广，使用欧易 APP 进行虚拟货币结算，形成层级化分工，通过 QQ 群招募人员，发布操作脚本及动态二维码规避封控，配套教程指导删除记录、更换广告模板，并以高额佣金吸引参与者。^①跑分平台、加密通讯教程和开源混币工具的产业化，极大地降低了犯罪的技术门槛。这在犯罪人的有限理性决策中，意味着他们无需掌握高深技术也能参与犯罪，其主观评估的能力成本和学习成本大幅下降，从而使得更多潜在犯罪人将犯罪视为一个可操作的选项。

（三）成本收益失衡对犯罪决策的促成作用

犯罪收益的诱惑力大小，同样取决于犯罪人主观的、有限的“成本—收益”计算。这种计算往往是片面的，聚焦于直接的经济得失，而忽略或低估了其他成本。具体表现为：

1. 直接成本低廉且惩罚概率低

从犯罪实施环节看，虚拟货币洗钱的技术成本显著低于传统洗钱模式，租用境外服务器、购买匿名 SIM 卡等费用远低于传统洗钱所需的物理场所与人力成本。从司法实践效果看，2022 年中国涉虚拟货币洗钱案件仅破获 259 起，与虚拟货币链上实际交易规模存在明显落差，大量资金通过冷钱包离线存储逃避冻结。例如，黄某等人通过每套 3000 元的价格购买廉价银行卡三件套、租用境外加密聊天软件及火币网账户即可实施洗钱，技术成本远低于实体场所，其使用 14 个账户频繁划转资金、冷钱包离线存储规避冻结，大量涉案账户在交易异常时才被部分冻结，2396 万元赃款中仅 645 万元被查实，^②犯罪人使用廉价的银行卡、匿名 SIM 卡实施犯罪，其主观评估的直接经济成本极低。更重要的是，他

^①参见（2022）辽 0423 刑初 137 号。

^②参见（2021）闽 0902 刑初 296 号。

们基于如低破案率等的不完整的案例信息，主观判定犯罪的预期成本（被惩罚的概率×惩罚的严厉程度）处于低位。这种在有限信息下得出的低成本结论，与高额收益形成鲜明对比，构成了强大的诱惑力。

2. 犯罪收益规模化与可持续性

虚拟货币洗钱的获利空间巨大，通过发展多层级代理跑分体系，犯罪团伙可构建规模庞大的资金归集网络，快速扩大资金池。犯罪分子通过虚拟货币来进行套利，赚取市场波动红利。例如，卢某参与搭建的 MOS 代币项目形成 17 层 10742 个用户的传销层级，通过编写合约代码将用户资金兑换为代币，设置 LP 用户收益分成及 NFT 算力奖励机制，形成了基于虚拟货币的传销资金增值体系，^①犯罪收益在犯罪人的主观理性中被放大。他们不仅看到一次性的洗钱佣金，更看到通过发展下线构建跑分网络带来的规模效应，以及利用 DeFi 质押、跨平台套利实现钱生钱的可持续性。这种对收益增长潜力的主观预期，极大地增强了犯罪行为的吸引力。然而，这种计算是有限的，他们可能沉醉于收益的指数级增长模型，却选择性忽略了随之倍增的法律风险。

五、理性选择理论视角下利用虚拟货币洗钱犯罪的防控对策

基于理性选择理论的分析，潜在犯罪人是在权衡犯罪收益的诱惑与犯罪成本的制约后做出决策。因此，防控体系的核心在于系统性地重塑其成本—收益计算，通过压制非法收益以降低诱惑力，通过抬升综合成本以增强威慑力，最终使其做出“得不偿失”的理性选择。

（一）强化资金追踪与非法收益阻断

本层次对策旨在针对性地降低潜在犯罪人对犯罪经济回报的预期效用，使其无利可图或获利甚微，从而从根源上抑制犯罪动机。

1. 强化资金链的溯源与阻断，降低收益“落袋为安”的预期

强化公安机关内部侦查协作指的是侦查机关和其他部门之间和不同地域侦查机关之间在刑事侦查工作中为发现犯罪、搜集证据、缉拿罪犯而相互配合和共同协助的一种侦查措施。^[25]虚拟货币洗钱有跨国性特征，要构建多维度监管框架，司法机关要和区块链技术公司以及虚拟货币交易平台创建协作机制，依靠他们的技术优势来追踪涉案资金的流向，确定交易操作的节点，查封与洗钱相关联

^①参见（2023）豫 0781 刑初 473 号。

的账户，并且要定期更新反洗钱技术工具库，提高对新型混币协议、隐私币种的监测能力。侦查机关和其他部门需集中力量打破信息壁垒，通过搭建跨部门实时数据共享平台整合银行机构、虚拟货币交易所及第三方支付机构的资金流水、链上交易记录和 IP 登录信息。强化公安机关内部经侦、网安、技侦等警种的协同分工，由网安部门追踪虚拟货币混币后的链上流转路径，经侦部门核查法币提现账户关联性，技侦部门固定电子证据，同时与境内外合规交易所建立快速协查通道，要求其配合冻结涉案钱包地址并提供用户实名信息。针对跨区域案件由公安部统一协调，涉案地侦查机关同步调取本地关联数据，制定跨省资金流向追踪和钱包私钥移交的操作规范。利用区块链分析工具穿透匿名交易、定位混币服务平台，结合第三方支付机构的异常交易预警模型锁定高频小额转账等可疑行为，通过跨地区警力协作与技术公司提供的交易线索分析工具，形成从链上地址溯源到法币资金闭环验证的全链条打击模式，最终建立全国统一的虚拟货币犯罪情报库和标准化侦查流程，提高跨区域案件的侦破效率。在协作机制层面，建立跨国司法数据共享平台，完善涉案钱包地址的快速冻结机制，依托 FATF 监管框架推动全球交易所合规化进程，压缩跨境资金转移的监管套利空间，缩短跨境资金追踪周期，并利用国际组织（如 FATF）推动全球交易所合规化，要求其配合冻结涉案钱包地址。^[26]

2. 压缩非法资金流转空间，减少犯罪收益

通过限制虚拟货币洗钱的流通渠道与价值变现能力，压缩操作空间、强化法律威慑，从源头降低犯罪收益预期，从而打击虚拟货币洗钱犯罪。

在主体层面，中心化交易所作为虚拟货币交易的主要渠道之一，掌握大量关键数据，例如账户注册信息、账户交易信息和其他关键信息，以上信息包括昵称、实名、身份证号、手机号、邮箱、用户对应充币地址、关联银行卡与第三方支付信息、OTC 交易信息、充币、提币交易信息、合约交易信息等，这些信息对涉案资金流、信息流、人员流的认定及案件能否及时侦办起到关键作用。^[13]⁶⁶ 可组建专门对接中心化交易所的协查调证机构，规范调证流程，畅通调证渠道，^[27]严控交易所与 OTC 服务商，将虚拟货币交易平台、场外交易经纪人纳入反洗钱义务主体，^[28]强制其执行实名认证，要求钱包地址与身份证、人脸识别绑定。对未履行客户身份识别义务的平台，采取职业禁止、吊销牌照等行政处罚。

在制度层面，建立《虚拟货币场外交易商户特许经营管理办法》，实施严格的牌照准入机制。申请主体需缴纳至少 100 万元风险准备金并在央行备案，强制接入国家区块链监管平台接受穿透式监测，同时要求每笔交易实时绑定人脸信息与公安部身份系统交叉核验，个人单日交易限额 5 万元、商户单笔上限 50 万元，超限交易自动推送反洗钱中心复核。强制第三方支付机构部署动态风控模型，对单账户日交易超 5 笔或 72 小时内更换 3 个以上 IP 登录等小额多次交易行为实施智能熔断，同步冻结账户并留存完整资金链证据。

在资金通道层面，禁止金融机构为虚拟货币交易提供清结算服务，强化对跑分平台、电商礼品卡等新型变现渠道的穿透监管，从而切断法币兑换路径，通过强制电商平台封锁虚拟货币礼品卡充值接口阻截资金套现，并要求金融机构穿透监测跑分平台多级账户资金归集链条，构建第三方支付平台智能风控系统，对高频小额交易、多 IP 登录等异常行为实施交易拦截与账户冻结，并加强对跑分平台、电商代充等看似合法的场景的监管，冻结涉案资金账户，同步适用洗钱罪刑事推定规则实现全渠道刑事威慑。

（二）提升犯罪技术难度与法律风险

本层次对策旨在全方位提高犯罪行为的客观实施难度和主观风险感知，涵盖经济成本、心理成本、法律成本及技术成本，使其知难而退。

1. 升级链上追踪技术与数据共享，提高被发现和查获的概率

针对虚拟货币交易的匿名性与跨境流动性，建立链上资金流向可视化系统。一是地址关联性分析，整合区块链浏览器、交易所交易数据库与钱包地址数据库，开发支持比特币、门罗币等多币种的追踪工具，通过地址生成时间、交易频次等特征建立地址关联记录，破解混币技术的路径混淆；二是要监控跨链交易，针对 USDT 等稳定币跨链转移行为，部署跨链桥交易监控模块，结合相应的技术手段，识别高频、大额跨链交易中短时间资金流转的可疑交易账户。三是共享联盟链数据，由央行牵头建立覆盖交易所、支付机构、社交平台的反洗钱联盟链，实时共享频繁更换 IP 登录的交易所账户等可疑账户信息和资金异动数据。着重围绕虚拟货币与法定货币的兑换节点固定证据，囊括行为人购买虚拟货币的交易记录、和虚拟币平台或中间商的通讯信息以及法定货币兑换密钥的流转路径等方面，司法人员要提高对数字取证技术的敏感度，熟悉虚拟货币洗钱常见手段，^[29]规范

电子证据提取流程，保障证据链完整且合法。同时，公安机关要通过加强与第三方支付机构和技术公司的深度合作，能够显著提升对虚拟货币洗钱犯罪的打击效率。

2. 完善法律法规与跨境协作，提高惩罚力度并堵塞漏洞

在虚拟货币洗钱犯罪治理中，确立混币服务商的刑事责任边界是提升法律成本的关键突破点。当前司法实践面临的核心困境在于，对混币器开发者主观明知的证明往往陷入技术中立性与犯罪帮助性的争议漩涡。例如美国 Tornado Cash 洗钱案中，因无法直接证明开发者对用户具体犯罪行为的认知，最终仅处罚使用者，而开发者脱责，暴露出法律对技术赋能者的规制盲区。为破解这一难题，笔者认为需构建以客观行为推定主观明知为核心的法律责任体系。在制度设计层面，应当在《反洗钱法实施细则》中增设阶梯式推定条款：当混币服务商存在未向监管部门登记备案技术协议、未留存用户交易日志或日志保存不足 180 天、用户单地址累计混币额超等值 50 万美元未触发风控等情形时，司法机关可直接推定其主观明知；若同时触发两项以上情形且涉案金额超过 100 万美元，则应适用不可反驳的严格推定，应直接认定为洗钱罪帮助犯，依法追究刑事责任。这一规则借鉴了最高人民法院关于洗钱罪司法解释中“推定明知”的立法技术。此外，可以根据 2024 年《关于办理洗钱刑事案件适用法律若干问题的解释》，明确虚拟货币交易作为洗钱手段的入罪条件，针对混币服务、匿名币兑换等新型手法，细化“明知”认定规则，通过交易频次、资金规模、技术隐蔽性等间接证据形成完整证据链；由于虚拟货币洗钱的核心目标是将非法所得通过交易所、钱包服务商等渠道转换为法币进行流通，公安机关可依托第三方支付机构掌握的跨境资金流动数据、异常交易预警模型等技术优势，快速锁定涉案账户的提现记录和资金流向。如知帆科技研发的“逐迹”虚拟货币追踪查证平台即可对区块链上的资金进行可视化层级分析及关联分析，通过与区块链安全企业加强合作，联合中科链安、知帆科技等区块链企业，建立警企联合实验室，可直接获取涉案虚拟货币的链上交易线索、混币服务穿透分析报告等技术支撑，从而掌握交易地址、交易账户的追溯方法，精准追踪 BTC、USDT 等主流币种的跨平台流转路径。这种合作机制不仅突破了传统侦查手段在 IP 地址溯源、匿名钱包关联等方面的技术瓶颈，更高效率实现了从链上数据抓取到法币资金闭环验证的全链条证据固定。

3. 深化技术合规普法与构建司法震慑体系，增加心理与道德成本

司法行政机关需联合央行分支、区块链服务企业与金融机构，开展定向普法。犯罪年龄的集中化证明青少年普法教育和犯罪预防工作的必要性，针对青少年对虚拟货币洗钱追溯存在侥幸心理，误认为利用虚拟货币洗钱难以追溯的现状，基层司法所可以在高校、公司、社区和网络上举办全国洗钱犯罪宣传周活动，增设主题展览和知识竞赛，尤其是针对高校、职校学生开展虚拟货币犯罪警示宣传。行为经济学中的“损失厌恶”理论是指人们在面对损失时往往比面对收益更加敏感和痛苦。通过引入“损失厌恶”原理，设计量刑风险模拟工具，输入特定洗钱金额即可生成对应的刑期预测（例如“转移 100 万美金将面临 7 年监禁”），将未来可能发生的刑罚“损失”具象化、前置化，击破侥幸心理，使其消失在萌芽中。重点解析帮助他人买卖虚拟货币可能构成洗钱共犯这类法律边界的界定，消除年轻群体对虚拟货币的“去中心化”“匿名性”等技术特性存在的认知偏差，使他们重新审视洗钱犯罪的法律风险。针对区块链开发者、矿工、OTC 商家等高危群体设计专项普法，通过区块链浏览器演示资金溯源技术，揭露非接触式洗钱的技术漏洞，破除犯罪的侥幸心理。在宣传内容上，针对虚拟货币洗钱高度依赖技术匿名性的特点，聚焦虚拟货币非完全匿名的技术特性，直击犯罪核心逻辑，明确公链地址可追溯、交易所 KYC 规则等核心要点，结合《刑法》第 191 条洗钱罪及“两高”司法解释，阐明利用暗网混币器、跨链桥接、伪造 DeFi 交易等新型洗钱手法的定罪标准、刑责范围及资金全链追缴规则。

参考文献：

- [1] 葛燕.虚拟货币监管入刑化趋势解读[C]//《上海法学研究》集刊 2022 年第 12 卷——中伦律师事务所卷.中伦律师事务所,2023:187-206.
- [2] CoinCarp Com.全球加密货币总市值走势图及加密货币最新涨跌分布[EB/OL]. (2023-05-20)[2025-04-21]. <https://www.coincarp.com/zh/charts/>.
- [3] 郑丁灏.全球稳定币的系统性风险:监管挑战与应对[J].税务与经济,2021(2):79-88.
- [4] 王熠珏.我国虚拟货币规制的嬗变与反思[J].重庆交通大学学报:社会科学版,2019(3):8-14.
- [5] 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.
- [6] 周倩.打击电诈专项工作取得阶段性重大战果[N].工人日报,2025-01-11(003).
- [7] 李先硕.要点来了! 全国检察长会议强调这些事[EB/OL].(2025-01-14)[2025-04-21]. https://www.spp.gov.cn/spp/zd gz/202501/t20250114_679646.shtml.
- [8] 尹云枫.买卖虚拟货币行为刑法定性研究[D].中南财经政法大学,2023.
- [9] 顾辰欣.数字经济时代涉虚拟货币洗钱风险研究[J].开发研究,2022(2):153-160.

- [10] 郭旨龙.侵犯虚拟货币刑法定性的三层秩序观——从司法秩序、法秩序到数字经济秩序[J].政治与法律,2023(5):49-68.
- [11] 柴用栋,姜雪,洪娟.网络虚拟货币的研究综述与展望[J].技术经济与管理研究,2015(5):106-110.
- [12] 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(4):102-110.
- [13] 陈键钊,吴照美.利用虚拟货币转移涉诈资金犯罪侦查研究[J].湖北警官学院学报,2023(4):58-68.DOI:10.19828/j.issn1673-2391.2023.04.006.
- [14] 李涛,邱归港.虚拟货币洗钱犯罪侦查对策研究[J].中国人民公安大学学报:社会科学版,2022(4):40-52.
- [15] 杨凯.虚拟货币司法处置须规范化[N/OL].人民法院报,2024-09-03(03)[2024-09-03].
<https://www.chinacourt.org/article/detail/2024/09/id/123456.shtml>.
- [16] 田扬畅,付顺顺.虚拟货币犯罪实证研究——以中国裁判文书网 367 个判例为样本[J].公安学刊(浙江警察学院学报),2021(5):89-96.
- [17] 张竞宇.“断卡行动”以来的银行个人账户风险管理研究[J].中国银行业,2022(12):73-75.
- [18] 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.
- [19] 李漠涵.虚拟货币洗钱案件侦查困境及对策研究[D].中国人民公安大学,2024.
- [20] 张云飞,陈亮.DeFi 虚拟货币传销犯罪侦查方法与治理对策[J].中国人民警察大学学报,2025(6):23-29,63.
- [21] 李星,张雍锭.网络空间侵犯著作权犯罪刍议[J].犯罪与改造研究,2024(9):43-51.
- [22] 吴宗宪.西方犯罪学[M].北京:法律出版社,1999:392.
- [23] 李明琪.几种主要的犯罪原因[M]//李明琪.犯罪学(一).北京:中国人民公安大学出版社,2013:213.
- [24] SAFEIS 安全研究院.2022 年涉虚拟币犯罪研究报告[EB/OL].(2023-01-16)[2025-04-21].
<https://news.sina.com.cn/sx/2023-01-16/detail-imyakieq5788169.shtml>.
- [25] 刘涛,杨郁娟.侦查措施[M].北京:中国人民大学出版社,2015:170-171.
- [26] 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.
- [27] 王晓伟.虚拟货币洗钱犯罪打击难点与治理对策[J].人民论坛,2022(24):112-114.
- [28] 李兰英.虚拟货币洗钱犯罪的风险剖析及治理策略[J].贵州省党校学报,2021(2):78-91.
- [29] 马伊蕾.涉虚拟货币洗钱犯罪的司法困境及对策研究[J].福建警察学院学报,2024(4):100-108.

责任编辑：张小米