

虚拟币犯罪联盟链侦查研究

包海勇

(中国人民公安大学, 北京 100038)

【摘要】 虚拟币犯罪是近年来出现的新型犯罪, 涉案金额不断飙升, 危害后果由最初的财产损失上升为扰乱金融秩序进而威胁国家经济、金融安全。此类犯罪侦查中存在着效能不足、规范性薄弱、潜在风险高和公信力不足等问题。联盟链侦查因兼顾私密性和兼容性、链上资源融合、侦查功能增强及规范性提高等优势, 是提升侦查效能的有效路径。具体思路为: 搭建多节点、多层级的联盟链网络平台, 设计契合侦查需求的联盟链系统架构, 部署多视角的具体侦查应用场景, 嵌入外部引智和自主研发相结合的模型算法。依此, 在链上研判数据获取可靠案源, 运用“可编程侦查”和“可信侦查”查清事实, 通过地址标签和聚类分析等技术刻画嫌疑人, 开展链上、云上等溯源取证和链上链下相结合的赃款追踪等, 实现虚拟币犯罪的高效侦查。

【关键词】 虚拟币犯罪; 联盟链侦查; 联盟链网络平台

【中图分类号】 D918

【文献标志码】 A

【文章编号】 2096-3165 (2024) 06-0008-11

虚拟币犯罪是近年来经济、金融领域出现的严重扰乱金融秩序、危害经济安全的新型犯罪, 涉及多个类型、多个罪名, 其发案数难以准确统计。笔者依据裁判文书网公开的刑事案件裁判数和个别区块链服务公司及一些办案民警的访谈, 获取发案的相对数。检索中国裁判文书网, 以“虚拟币”为关键词, 选择刑事案由, 时间为2011年1月1日至2024年9月28日, 检索结果为1951份,^①各年度的文书数量如图1所示。人民法院裁判的涉虚拟币刑事案件数量逐年上升, 特别是2018年至2021年, 年均数百起。当然, 2022年下降应当与国家颁布禁令有关。2021年9月15日, 中国人民银行、中央网信办、最高人民法院、最高人民检察院、公安部等多部门联合发出《关于进一步防范和处置虚拟货币交易炒作风险的通知》, 明确虚拟币不能作为货币在

市场上流通使用, 因而境内涉虚拟币裁判案件数下降。此后境内犯罪分子选择境外交易所继续疯狂作案, 2023年裁判文书数再次呈上升走势, 2024年前9个月为250份, 全年总量或超过2023年。另外, 据国内某区块链技术服务公司发布的《中国(大陆)2023年度虚拟货币犯罪形态分析报告》, 该公司2022年和2023年共协助全国各地司法机关办理了大量虚拟币犯罪案件, 且2023年数量远高于2022年。当前, 国内此类公司累计有十多家, 均协助司法办案, 数量不可低估。另外, 笔者访谈了多名虚拟币案件的办案民警, 均指出当前虚拟币犯罪黑数很高, 进入法院审判环节并被如期判决的仅是一少部分, 公安机关侦查环节存在诸多难点。据此, 虚拟币犯罪的实际态势更加复杂、严峻, 探索新型侦查方式、提升侦查打击效能成为重要课题。

【基金项目】 中国人民公安大学侦查学双一流专项 (2023SYL02)。

【作者简介】 包海勇 (1979—), 男, 中国人民公安大学博士研究生, 中国人民公安大学侦查学院副教授。

① 参见中国裁判文书网 <https://wenshu.court.gov.cn>。

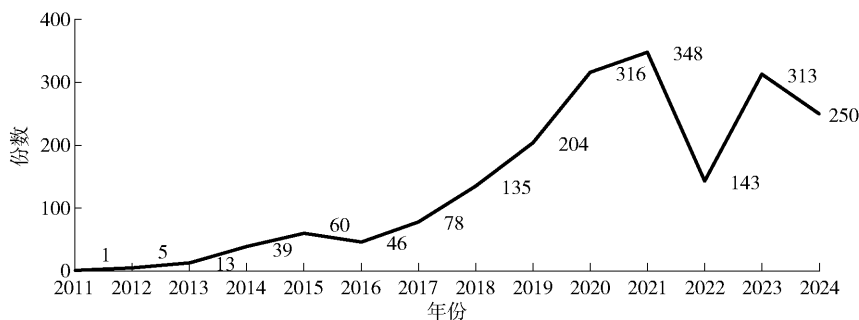


图1 2011年1月—2024年9月虚拟币刑事裁判文书数量图

一、虚拟币犯罪联盟链侦查概述

（一）虚拟币犯罪类型

虚拟币犯罪是新型犯罪，具体是指行为人实施的与虚拟币相关的一切违反刑事法律规范、危害社会、应受刑罚处罚的行为总称。此类犯罪既非个罪，也非类罪，而是发生在与虚拟币有关的多个领域内的所有犯罪的总和。通常包括以下几类：一是以虚拟币为对象的犯罪。如盗窃、诈骗、抢劫、抢夺、侵占虚拟币等，罪名累计近10种。如曾是日本最大的比特币交易所的Coincheck，2018年被黑客成功攻击并盗窃价值5.3亿美元的虚拟币^[1]。二是以虚拟币为工具或手段的犯罪。如利用虚拟币洗钱、集资诈骗、组织领导传销、网络赌博、非法吸收公众存款、非法经营、帮助恐怖活动等。特别是虚拟币洗钱犯罪，发案量近几年呈几何倍数增长，少数境外虚拟币交易所大有取代传统地下钱庄之势，成为新型洗钱犯罪的天堂。三是发生在虚拟币交易空间的犯罪。如在虚拟货币交易所或相应的区块链技术应用场景中实施的敲诈勒索、网络诽谤、损害商业信誉等犯罪。四是与虚拟币相关的技术型犯罪，最典型的就是智能合约犯罪。既有以智能合约为对象的犯罪，也有以智能合约手段的犯罪；既有非法获利型，也有非法破坏型，还有非法持有或非法修改型^[2]。如非法获取他人合约私钥进而窃取他人虚拟财产，或利用他人合约漏洞非法修改编码获取不当利益等；或编制合约代码实施诈骗、伤害、报复陷害甚至雇佣杀人等各类犯罪^[3]。五

是与虚拟币相关的其他类型犯罪，如“挖矿”过程中盗窃电力，以及贩毒、军火交易、色情服务、黑灰产业及暗网^①中的虚拟币交易等。黑龙江、河南等数个省市就是全国虚拟币盗窃电力的重灾区^[4]，上述分类及常见罪名见表1。粗略统计，因虚拟币引发的犯罪高达50种以上，且部分罪名是典型的危害经济安全、社会安全、公民人身及财产安全甚至国家安全的高发、常发犯罪。

表1 虚拟币犯罪主要类型及常见罪名

犯罪类型	常见罪名	罪名数量
对象型	盗窃、诈骗、抢劫、抢夺、侵占等	约10种
工具手段型	洗钱、集资诈骗、组织领导传销、赌博（网络）、非法吸收公众存款、非法经营（买卖外汇）、帮助恐怖活动（融资）等	10种以上
交易空间型	敲诈勒索、网络诽谤、损害商业信誉等	6、7种
相关技术型	盗窃（合约盗窃）、诈骗（合约诈骗）、伤害、报复陷害、杀人（雇佣）等	10种以上
其他	盗窃（电力）、贩卖毒品、非法买卖枪支弹药、组织卖淫等	10种以上

（二）虚拟币犯罪特点

一是犯罪数额高。虚拟币犯罪多属财产犯罪，以获取经济利益为目标，但因其具有去中心化、无国界、监管难、投机炒作等特点，犯罪金额与传统财产犯罪相比异常高。类案方面，如2021年，虚拟币网络赌博犯罪的平均案值最高，为21.49亿元，虚拟币传销犯罪次之，为10.92亿元。^②个案

① 暗网，又被称为深网或隐藏网，是指那些任何搜索引擎均没有索引注册的网站，正常的访问链接无法直接访问，必须使用特殊的暗网访问浏览器方能访问的网络资源，是互联网的深层次信息。

② 参见知帆科技公开发布的《2021年区块链和虚拟货币犯罪趋势研究报告》。

方面，如2022年内蒙古警方侦破一起虚拟币洗钱犯罪案件，涉案金额高达120亿元^[5]。2023年，湖北荆门公安机关破获的一起虚拟币洗钱犯罪，平台资金流水4000亿余元，均以虚拟币形式流向境外^[6]。可见，相较传统财产犯罪，虚拟币犯罪的案值非常高。二是常见类型相对稳定，涉及罪名有不断扩大趋势。纵观近几年发生的虚拟币犯罪，常见类型相对集中。据知帆科技公司司法协助办案数量统计，2021年，虚拟币犯罪发案数量由高到低排名前五位的分别是洗钱（占比30.7%），传销（29.2%），盗币（11.5%），电诈（7.1%），网赌（6.3%），累计占有所有虚拟币案件的85.8%。2022年，发案数量前五位的分别是洗钱（30.5%），网赌（12.3%），传销（11.8%），盗币（11.2%），电诈（10.7%），累计占有所有虚拟币案件的76.5%。^①此外，近几年涉案罪名不断扩大，出现勒索、贩毒、侵犯公民信息等犯罪，以及涉黄、涉枪、非法经营、破坏计算机信息系统等犯罪。三是犯罪手段科技化、智能化。如，有的犯罪分子利用区块链的匿名性特点，通过伪匿名标识符研究开发多重匿名技术，除身份匿名外，还能隐藏交易价格等其他关键数据^[7]。再如，在虚拟币洗钱犯罪中，犯罪分子利用混币^②、跨链^③等技术混淆资金链路，增加资金追踪难度。还有，在虚拟币传销犯罪中，犯罪分子依托去中心化金融（DeFi）技术，编制高水准传销项目智能合约部署上链，自参与者上链之时，后续犯罪行为全部自动执行，手法隐蔽、效率高，还节约传销的技术维护、财务管理等人力成本。2021年底，安徽池州公安机关破获一起虚拟币犯罪，犯罪分子李某伙同他人开发了两款链上项目合约代码，一款功能正常，另一款带有“后门”功能，即未经投资者同意可任意链上提取投资者质押的虚拟币。正式上线后在微信群开展虚假宣传，待投资者将虚拟币投入项目，犯罪分子利用带“后门”功能的合约代码直接将受害人所投虚拟币全部转移至场外变现、提现^[8]。

二、虚拟币犯罪联盟链侦查的必要性

（一）虚拟币犯罪侦查现状及存在问题

1. 虚拟币犯罪侦查现状。一是网络犯罪常规侦查理念的运用取得基本成效。虚拟币犯罪是网络犯罪的一种，从已经侦破的各类虚拟币犯罪案件来看，侦查部门多采用网络犯罪的常规侦查思路。案源多来自关联罪名串并，如反洗钱或网络赌博专项整治行动中发现线索；事实查证多趋同于传统网络犯罪的“四流”（资金流、信息流、人员流、物流）查证；在线取证亦以数据调取、截屏录屏为主，辅以必要的外部调证等等。数年来的侦查实践表明，这种思路和理念大体上能够应对当前虚拟币犯罪的客观态势。二是建立了侦查部门和区块链公司协同办案模式。虚拟币犯罪专业性强，对于案情简单、资金链路不复杂的案件，公安机关依法独立侦办，处于“摸着石头过河”的探索阶段，呈现出“办案中学习、学习中办案”的典型特征。而对于案情和资金链路相对复杂的重大、疑难案件，办案人员须取得专业的区块链技术服务公司的支持和配合，协同开展资金分析、地址锁定、链上调证、资产查扣等案件侦办工作，并建立了比较成熟的协同模式。三是多维数据和人工研判相结合的数据导侦模式。针对虚拟币犯罪，侦查员常根据侦查需求，线上运用算法和模型分别检索、分析、研判数据，结合人工汇总和分析，寻找数据间的关联关系。如虚拟币传销犯罪侦查中，侦查员先通过链上资金数据穿透，还原传销组织各成员间的资金收支路径，确定入盟费、提成；再从人员通讯、出行轨迹等数据中分析犯罪团伙的分工，绘制人员关系图^[9]。同理，依托其他类型数据，人工汇总，综合研判，分析得出结论，是人工研判主导下的多维数据导侦模式。四是破获一批大案要案，总结了一些侦查战法。如2020年江苏盐城公安机关侦破当时轰动全国的“币圈第一大案”——Plus Token平

① 参见知帆科技公开发布的《区块链和虚拟货币犯罪趋势研究报告（2021、2022年度）》。

② 混币，字面意思就是币币混合，是区块链技术支撑下的一种虚拟币隐私功能，通常是运用混币器将不同地址间的虚拟币以少量多次的方式，短时间内汇集到一个地址，类似资金池，后拆散资金并通过多个其他地址多次转出，从而成功割裂这些虚拟币的输入地和输出地，增加追踪涉案币流向的难度。

③ 跨链是指通过常用的跨链技术将本应在同一条链上交易、转移的虚拟币，成功实现在不同链之间转移、记录，提高流通性。

台组织、领导传销案，参与人员 200 余万人，层级关系多达 3000 余层，涉案虚拟币总值逾 400 亿元。多年来的侦查破案，办案民警总结了一些侦查经验和战法，如链上资金流穿透法、链上高危钱包地址归类法等，并培养了一批办案能手。

2. 虚拟币犯罪侦查存在的问题。一是侦查打击效能不足。如，案源发现滞后，犯罪黑数高。犯罪分子借助互联网、密码学、混币、跨链等技术，资金流呈现的不再是传统二维平面，而是三维立体，通过针对法定账户的资金查控技术获取案源几乎不现实^[10]，部分被害人在此类犯罪（如虚拟币传销等）中也可能涉嫌犯罪，存在畏罪等心理而选择不报案^[11]。再如，借助区块链的匿名性特点，链上犯罪人的身份认定历来是难题。门罗币更以“匿名币”著称，在完全匿名的环境中交易，查明交易者的身份难上加难^[12]。有些犯罪团伙，黑市购买他人身份、手机、银行卡、第三方支付等信息（俗称“四件套”）用以作案，对抗侦查。还有，资金追踪不力。犯罪分子开通多个钱包地址，资金反复流转，形成“迷宫”般的交易网络，并结合复杂的混币和跨链等技术，借助暗网操作等，追踪阻力巨大^[13]。此外，对于数据资源运用而言，人工挖掘线上分散数据并确定关联关系还只是寻找数据间的弱关联，是大数据侦查的初级形态。二是执法规范性相对薄弱。虚拟币犯罪的空间背景、时间轨迹、人员身份、资产流转等均存在明显的特殊性和差异性，网络犯罪常规侦查方法常出现理论供给明显不足的境遇。大量案件都需要开辟新途径、提炼战法，民警摸索性办案的特点突出，规范性薄弱。如侦查取证环节，针对链上原生证据和链外需要上链证据，办案民警往往一案一尝试，有的在线调取交易哈希，有的录屏截屏资金链路等等，获取的证据往往需要补强。再如，资产查扣和处置工作，同样面临规范性被质疑的尴尬。虚拟币是存储在钱包地址的一串数字符号，既无法像传统银行账户那样在线冻结，也无法像传统实物资产那样扣押、拍卖变卖等。三是办案潜在风险高。对于疑难、复杂虚拟币犯罪案件，公安机关联合区块链技术服务公司协同办案，目前来看，仅是一种权宜之计而非最优组合。区块链公司的协助行为已经实质性履行了部分侦查权，如链上资金链路分析、链上嫌疑人特征刻画、钱包地址多层级穿透等，存在越权之嫌。如果区块链公司将办案数据公开或挪作他

用，将存在不可估量的风险。此外，实践中个别地区办案民警出现过自开热钱包暂存涉案虚拟币现象，存在一定的道德风险，不排除民警借办案产生贪污、挪用的可能，且暂管期间出现价格波动时难以应对^[14]。四是侦查公信力需要提升。近年来，各地侦查部门虽全力开展虚拟币犯罪案件查处、损失挽回、秩序维护等工作，然而侦查办案质效时常受到质疑。如，质疑办案周期，当事人习惯性将虚拟币案件等同于传统网络犯罪案件，希望能够快侦快办。但该类案件复杂多变，侦查周期远比传统网络犯罪长。再如，质疑涉链证据能力。无论是公安机关自行取证，还是委托调证，涉链证据的真实性和可采性时常遭受质疑。还有，质疑追赃挽损率。从目前办案的现实状况而言，挽损率整体上达不到受害人的心理预期。以上质疑直接降低侦查办案公信力。

（二）虚拟币犯罪联盟链侦查的优势分析

联盟链侦查是侦查领域的一个新兴概念，目前学术界鲜有科学的界定，近一两年才提出与之相关的概念。如区块链侦查，李晓东 2023 年提出，区块链侦查是依托区块链技术为底层架构，综合运用哈希算法、时间戳、智能合约及非对称加密等技术开展高效侦查，以保障侦查工作合法性、科学性及安全性的侦查生态系统^[15]。再如，基于联盟链的区块链侦查，潘嘉瞳 2024 年提出，基于联盟链的区块链侦查是指以联盟链技术为支撑的所有侦查场景的综合，如警务联盟链、公检法司联盟链、国际司法合作链、区块链取证平台等^[16]。

上述概念，事实上都是区块链侦查概念，区别在于前者是区块链侦查的总体概念，后者限定于与联盟链相关的区块链侦查概念，二者是种属关系，前者属概念，后者是种概念。联盟链是区块链的一种类型，故联盟链侦查，亦是区块链侦查的种概念，其与基于联盟链的区块链侦查相比较，从字面意义而言，无论是内涵还是外延，研究范畴均小于基于联盟链的区块链侦查这一概念。故，区块链侦查、基于联盟链的区块链侦查、联盟链侦查，三者可大体视为宏观、中观和微观三个不同层面的概念。

本文中的联盟链侦查，是指依托区块链技术，搭建侦查联盟链并在链上开展线索研判、案源生成、链上侦查、链上取证及链上追赃等一切侦查工作的总和。其应用于虚拟币犯罪侦查，具备明显的优势。

1. 兼顾私密性和兼容性，契合侦查需求。区块链分为公链、私链和联盟链。公链完全去中心化，节点自由加入或退出，但私密性不强，运行速度慢。而私链，中心化、仅少量节点加入，安全性和私密性强，速度快，但参与节点受限，行业应用率过窄。应用率较高的是联盟链，相较公链，联盟链私密性强，链上节点仅为经许可的单位或个人。相较私链，联盟链兼容性强，只要链上节点同意，任何单位或个人均可上链，应用率较高。目前广泛应用于经济、金融、行政管理、司法等领域，侦查破案是部分单位和个人参与、涉密性强的专职工作，联盟链是最佳选择。

2. 便于链上侦查资源高效融合。虚拟币犯罪侦查涉及公安机关、金融监管、检察院、法院等多个部门。传统线下协商弊端突出，联盟链可契合各部门需求，上链成为节点并将合作意向部署为链上合约，明确权利和义务，即可突破行业壁垒，实现高效协作；联盟链亦由数据层、网络层、共识层等几部分构成，所有交易均记录在链上数据层和网络层，包括虚拟币犯罪行为轨迹^[17]，不可篡改。构建联盟链，链上侦查节点就可在数据层和网络层整合各类数据资源，发挥多重数据资源优势。

3. 侦查环节功能显著。如链上锁定犯罪嫌疑人。联盟链上存储着犯罪嫌疑人的钱包地址、交易规律等数据，侦查节点综合运用地址标签等多种技术，可快速查证嫌疑人身份信息，锁定物理位置。再如链上存证。链上证据受技术加持而强化了数据的真实性，“采用去中心化的分布式存储技术、多节点共享的读取技术、严格的入链后防篡改技

术”^[18]，使证据上链后真实性得到可靠保障，改变电子证据取证多、采信少的司法窘境，大幅提升证据的证明力。还有，链上资金追踪。链上侦查节点依托联盟链，运用区块链浏览器，有效查询钱包地址下的资金、交易记录等信息，以及项目通证、代币人数、项目风险等合约地址信息。还可结合数据溯源技术，实现数据从产生到发展变化等全流程记录、保存和留痕，便于逆向查对和核准^[19]，实现精准追踪。此外，联盟链还可嵌入一些区块链服务公司研发的链上追踪专业软件（如“无匿”“链必追”“链上天眼”等），资金追踪效果更佳。

4. “可编程侦查”和“可信侦查”助推智慧侦查。侦查节点将需要开展的数据收集、流转和存储等侦查工作，编制为智能合约上链，在联盟链中自动执行，实现既定的侦查目的^[20]，即可编程侦查。必要时，依据个案的特殊侦查需求，适当调整合约代码，修订共识规则，打造“个案订制侦查”，是典型的“自侦查”范式。同时，基于联盟链打造“可信侦查”^[21]，依托联盟链，数据上链即固化，修改其中任何一条数据均需要全网节点超过51%的算力，无法篡改。该技术成功地“解决了人类信赖危机，使得双方交易处于‘机器信任’状态”^[22]。侦查节点的一切工作亦能实现链上信任。相较传统侦查和数据侦查，可编程侦查和可信侦查是侦查思维的迭代和升级，是高阶智慧侦查。如果将传统侦查界定为侦查1.0时代，数据侦查为侦查2.0时代，可编程侦查和可信侦查就是侦查3.0时代，在侦查理念、模式、方案、手段及证据认定等方面具有显著优势（见表2）。

表2 传统侦查、数据侦查和可编程侦查、可信侦查的区别

	传统侦查	数据侦查	可编程侦查和可信侦查
侦查理念	被动侦查	主动侦查为主+被动侦查为辅	链上自侦查为主、数据侦查为辅
侦查空间	线下	线上+线下	链上+线上+线下
侦查模式	从案到人	从数到案到人	从链到案到人
侦查方案	侦查员主观拟定	数据导侦	类案模型和机器语言
侦查手段	线下调查、取证	在线数据研判+线下调查	合约自运行为主+人工操作为辅
证据认定	人工审查	数据鉴定为主+人工审查为辅	自信任、司法共享、直接适用
结果精确度	较高，但偶有错案	很高，错案很少	非常高，理论上无错案

5. 提高侦查规范性，降低办案风险。联盟链侦查是一种趋向于标准化、程式化的侦查思维，形成“共性侦查为主+个性侦查为辅”的侦查范式。

如链上资金穿透和追踪、链上取证和存证等侦查工作是共性侦查，个案不同的侦查策略和战法是个性侦查。侦查工作在获取案源、启动侦查、调查取

证、追赃挽损等各环节形成比较成熟的路径和方法。链上侦查节点以此为指引，开展各环节侦查取证，实现标准化、规范化执法办案，有效减少随意性和盲目性，降低执法风险。此外，联盟链侦查全程链上进行，处处留痕，便于执法监督，必要时可以在联盟链上进一步搭建侦查监督侧链，全面提升侦查规范性水平。

三、虚拟币犯罪侦查联盟链的搭建

侦查联盟链应当由网络平台、系统架构、应用场景、模型算法四部分组成。其中网络平台用于搭建类似于局域网的联盟链网络，并确定上链节点及其权限；系统架构是区块链技术架构在虚拟币犯罪侦查中的具体适用，如增加管理层等；应用场景是在搭建的系统架构中部署具体的侦查应用情景，侦查任务不同，应用场景亦不同；模型算法是在具体应用场景中嵌入相应的数据分析和研判工具。

（一）多节点、多层级的联盟链网络平台规划

打击虚拟币犯罪涉及公、检、法、金融监管及被害人、证人等多方主体，构建侦查联盟链，将以上主体作为参与方上链成为节点，以合约方式明确

职责权限。其中公、检、法和金融监管等部门是必备节点，而被害人、证人以及其他相关方作为可选节点，依据不同案情，允许上链参与，构成联盟链的一级网络，犯罪嫌疑人及辩护人也可视案情需要设置为可选节点。同时，公、检、法、金融监管各部门内部相关机构，如公安机关经侦、治安、刑侦、派出所等在一级网络架构下，上链成为必备子节点，与所属公安机关成为联盟链的二级网络。同理，检察院内部的批捕、公诉，法院内部的审判、执行，具有虚拟币监管职责的国家金融监管总局、中国人民银行、国家网信办等也成为必备子节点，分别与所属主管部门构建联盟链的二级网络。此外，公安机关内部经侦、治安、刑侦等机构与检察院内部的批捕、公诉，法院内部审判、执行及国家金融监管总局、中国人民银行等，依托一级、二级网络，构建三级联盟网络。该联盟链架构如图2所示，其中链上节点分为全节点、半节点和轻节点三类，每个节点均赋予可信数字身份。公安机关作为侦查主体，是全节点，享有链上一切权限；检察院、法院和金融监管部门是半节点，享有部分权限；被害人、证人、犯罪嫌疑人和其他相关主体是轻节点，视案情需要开通少量权限。

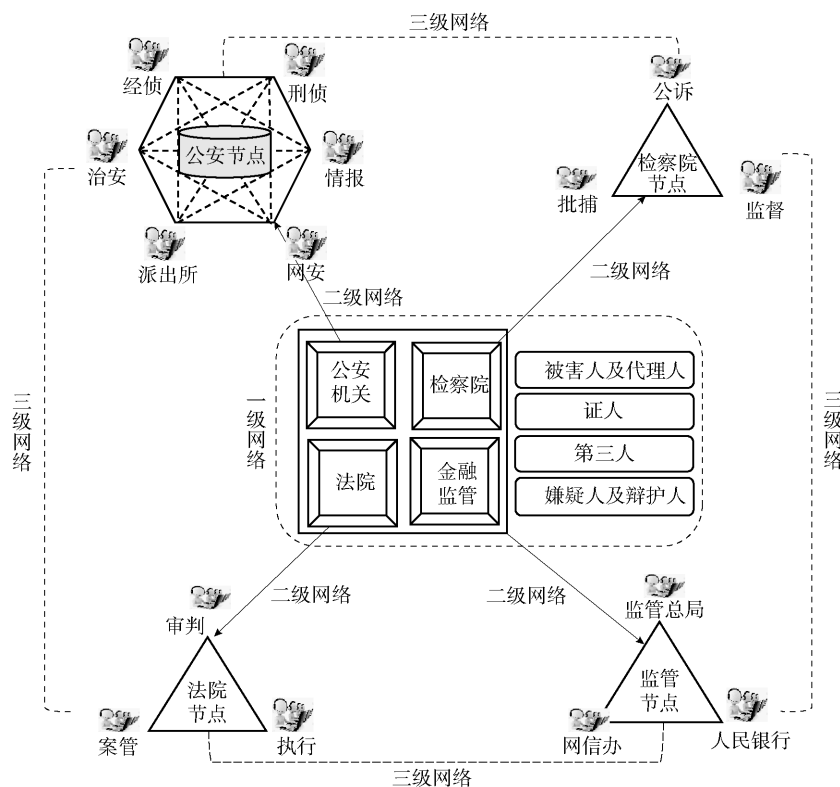


图2 虚拟币犯罪侦查联盟链网络平台图

（二）契合侦查需求的联盟链系统架构设计

联盟链侦查的系统架构，应当在具备区块链系统架构共性的基础上，补充增加实现侦查目标的个性化组件。纵向层面，除包括数据层、网络层、共识层、激励层、合约层、应用层外，还应当增加必要的管理层。横向层面，数据层除包括数据区块、链式结构、时间戳、哈希函数、梅克尔树、非对称加密等区块链基础数据外，还包括侦查联盟链的特有数据，如公安、司法、金融监管、银行、通信等数据；网络层除包括传统的三级网络架构外，还包括应当单向接入的公安专

网、司法局域网及金融监管部门的联网端口；共识层使用 POW 机制；^①激励层包括积分制和奖励办法两部分；合约层除包括常规的合约脚本和合约算法外，还包括侦查联盟链特有的依据《刑事诉讼法》和《公安机关办理刑事案件程序规定》编制的各环节智能合约，如受案合约、立案合约、侦查合约等；管理层包括身份管理、私钥管理和涉密管理；应用层是侦查特色应用，包括可编程侦查、可信侦查及各种犯罪侦查等，如虚拟币洗钱、诈骗、网赌、传销、盗窃、其他等。具体系统架构如图 3 所示。

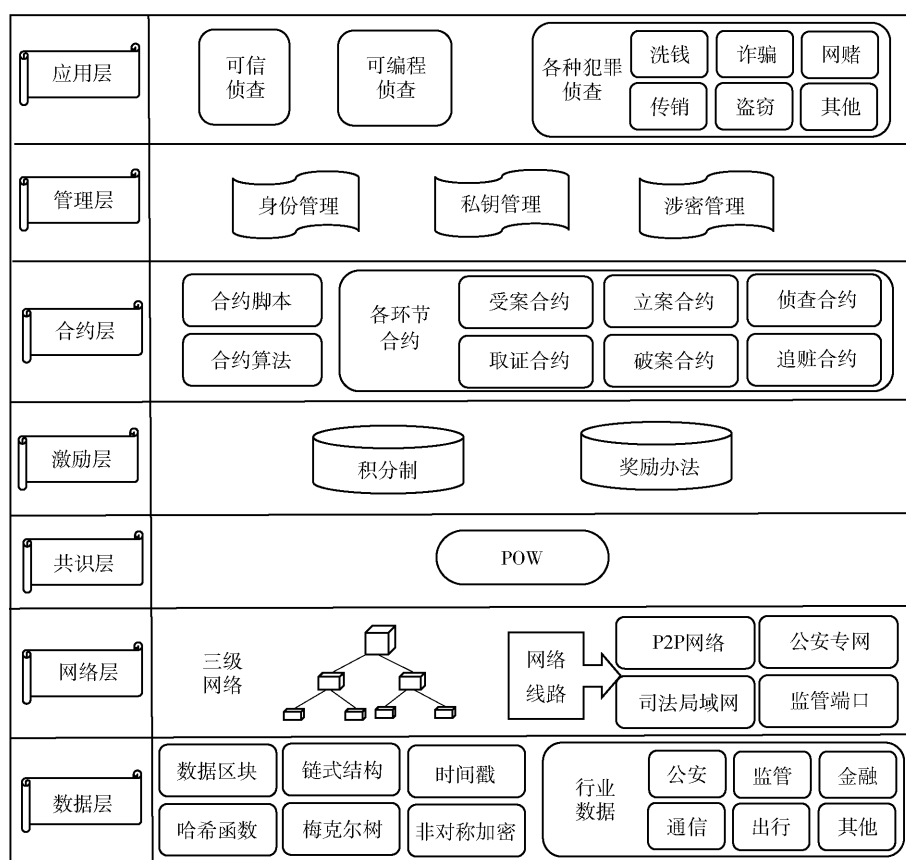


图 3 虚拟币犯罪侦查联盟链系统架构图

（三）多视角联盟链侦查的具体应用场景部署

应用是联盟链的生命力和终极价值，也是当前越来越多行业开始应用联盟链的内在动力。系统内应用场景部署是联盟链侦查应用的重要组成，是侦

查目标实现的具体路径。链上侦查的需求不同，可设计不同的应用场景，如针对错综复杂的链上资金脉络，可设计链上资金追踪场景。再如，针对不同类型的虚拟币犯罪，可设计类案侦查场景等。场景

^① POW 机制，是区块链共识机制中的一种，全称 Proof of Work 工作量证明，简称 POW。另两种共识机制分别是 Proof of Staked 权益证明，简称 POS；Delegated Proof of Stake 授权股权证明，简称 DPOS。三种机制是专门用来分配和奖励链上节点的一致协议，其中 POW 机制是根据算力来奖励，算力最强、业绩最突出的获得奖励，类似按劳分配机制，另两种则根据持币量或持股量来奖励，目前区块链领域 POW 机制运用最广泛。

内突出侦查重点、目标导向、权限分配、程序规划、运行机制、制度保障等，是链上侦查理念落地应用的微观环境。当前，依据虚拟币犯罪的态势，应当设计并部署上链的侦查应用场景，可分为基础类、措施类和类案类等三类常规场景。基础类如案情分析场景、侦查决策场景、侦查指挥场景、侦查监督场景等；措施类如资金追踪场景、人员定位场景、链上取证场景等；类案侦查场景如洗钱犯罪侦查场景、网赌犯罪侦查场景、传销犯罪侦查场景等。同时，侦查应用场景应呈开放态势，将随着虚拟币犯罪的不断发展、演变及相应侦查工作的调整、更新等客观需求不断拓展和丰富。特别是全面进入区块链3.0时代后，场景内需要大量增加3.0时代的技术特色，进一步提升虚拟币犯罪专业打击能力。

（四）外部引智和自主研发相结合的模型算法嵌入

联盟链侦查应用场景内需要有大量模型算法作为数据武器和工具，开展研判和分析。模型算法来源应坚持外部引智和自主研发相结合的思路。一方面，积极引进市面上已经研发出的先进工具，如前文提及的区块链服务公司研发的“无匿”“链上天眼”“链必追”等专业软件，特色突出、功能强大，已经成为公安机关侦查办案的得力助手，并产生了积极效应。此外，还应积极借助国外虚拟币犯罪调查工具，如取得国际刑警组织支持，依托其研发的“地下黑市交易调查工具”监测虚拟币交易流向、分析跨链交易地址等^[23]。另一方面，公安机关也应当主动作为、大胆创新，依据办案客观需求，自主研发相应的模型算法。其优势在于可借助多年来的办案经验和资源积累，研发出的模型和算法特色更突出、针对性更强，还可满足涉密管理等要求。

四、虚拟币犯罪联盟链侦查的运行

（一）链上案源——链上数据研判生成线索且智能立案

1. 数据上链。大数据的价值在于通过数据现象，寻找数据本质和规律，特别是研发高精度的模

型和算法深入挖掘有价值的信息作为线索^[24]。虚拟币犯罪线索获取以链上为主、链下为辅，需先将数据接入联盟链。一方面，链链对接，即将常发案的链接入侦查联盟链，使这些链上数据在联盟链上时时同步；另一方面，接入链下数据，部分链下实物往往是虚拟币犯罪的道具，如一幅字画可被铸造为NFT^①作品，成为链上传销工具。依托物联网技术，将易涉案物品打上标签，并结合数据识别和传感技术及全球定位系统等，实现物物相连^[25]，再接入侦查联盟链，实现高危物品数据亦在联盟链上同步更新。今后，应建立虚拟币大额和可疑交易报告制度，由交易所将监测出的大额和可疑交易，及时上链并推送给公安机关^[26]。

2. 链上研判生成线索。传统线索生成模式是“模型算法+人工识别”，虽然有效但还不是真正的机器学习。相反，联盟链可实现完全的机器学习，将模型和算法编制为智能合约，嵌入侦查联盟链。此时，“模型加人工”模式转化为智能合约自动执行，无需人为干预即可批量生成线索，且具有极高的准确性，是真正的人工智能生成线索。如虚拟币洗钱犯罪，自赃款上链开始，钱包地址间的所有交易行为均记录在链（包括混币和跨链等），并在侦查联盟链同步数据，当其交易符合洗钱犯罪的类罪特征时，智能合约即可抓取数据、自动研判、机器学习，生成批量可靠的线索和案源。

3. 智能立案。人工立案模式，需人为调取资金记录，结合笔录和管辖规定等，人为判断是否立案，时限长且存在错判等情形。应用侦查联盟链，立案模式升级为犯罪记录同步上链，立案审查亦同步上链，数据可靠、不可篡改，同时将立案标准、管辖规定等内嵌为链上共识机制。一旦链上记录达到立案条件，联盟链智能提示侦查员办理立案手续。侦查员只需在联盟链上授权同意，联盟链即可依托智能合约自动生成立案报批文书，并发送至审批节点，获批同时生成立案决定文书。整个程序呈智能化特点，还能从根本上解决当前公安机关普遍存在的应立不立、不应立而立以及管辖推诿等顽疾。

（二）链上查事——构建可编程侦查和可信侦查以查证事实

1. 可编程侦查。智能合约把实践中侦查所需

① NFT，英文全称是 Non-Fungible Token，即非同质化代币，是一种通过区块链技术铸造的原生数字资产所有权，具有不可分割和不可替代等特性。

的流程以及法律语言抽象为以代码和算法为表达形式的可自动执行的电子合约，众多可编程的智能合约组成脚本语言，通过设置数据自行触发与执行机制，明晰合约触发边界，筛选有价值数据，依托链上智能合约和共识机制自动运行，迅速执行合约中的线上侦查事务，体现“机器学习、智能算法侦查”的准智慧侦查新思路，进而实现线上任务的“自流程、自执行”^[27]。基于可编程侦查，全程运用模型和算法，自动追查涉案资金流向，理清涉案主体间关系，全链条还原事实真相，实时生成相应法律文书等，极大地提高了侦查效率。

2. 可信侦查。在智能合约模块增加侦查信任协议，详细列明每个节点的链上权利和义务，上链节点逐一签署，认可侦查节点在链上的行为及记录。同时其他节点如有链上行为，同样全网广播获得全网认可，并存储在相应数据区块中，每个节点主体平等，均同步更新数据，体现去中心化特征，构建一个链上节点信任共同体，实现链上侦查的机器信任。同时，在激励机制中也对应增加激励协议，对履行信任协议突出的节点予以链上激励。此外，还可将《刑事诉讼法》和《公安机关办理刑事案件程序规定》等法律法规也通过技术规则设定在链上，侦查节点链上遵守，从而使侦查程序同样在链上合法、可信。由此，侦查工作可得到链上其他节点的广泛认可，减少质疑，极大提升侦查办案公信力。

（三）链上查人——刻画作案人的真实身份

1. 通过钱包地址和交易痕迹追踪刻画作案人。依托交易哈希，顺线查找交易地址，该地址使用人即是作案人。对此，联盟链侦查节点可利用区块链浏览器，搜索可疑钱包地址的一切交易记录，锁定其链上活动轨迹，并在链上逐一查证与该地址有关的其他钱包地址，绘制关联钱包地址关系图谱。图谱中，有的是新地址，有的是反复交易的关系地址，如虚拟币洗钱，就是在链上不同的地址间往返流转资金、不断清洗漂白，关系地址很可能是受过打击处理的犯罪分子重操旧业。如果查到此类地址，作案人的身份或可直接查明，或能取得查证线索，利于进一步甄别。今后，随着技术进一步发展，可搭建虚拟币匿名犯罪侦查平台，研发身份查证模块，运用“海量钱包地址+精准算法模型+便捷联盟链技术”一键分析，确定嫌疑人身份^[28]。

2. 通过地址标签技术刻画作案人。搭建侦查

联盟链的同时研发地址标签系统，依据联盟链中数据采集模块，实时收集链上数据、科学提取数据特征，特别是区块高度、交易时间、交易金额、钱包地址等关键要素，并打上标签，形成主体标签、身份标签、行为标签、异常标签等。然后，运用机器学习和模型算法对已打标签的地址进行训练，并将标签地址与实体地址建立强关联关系，借助自然语言处理技术，识别其中的关键信息。再深入分析每笔交易中的文本描述，从中确定标签地址对应的实体地址^[29]。

3. 通过聚类分析法缩小摸查范围刻画作案人。聚类分析法很实用，强调将某个领域内的多个分析对象按性质相同或高度相似标准，分为多个群体，同一群体内的成员在属性、身份、行为等方面属于同类。针对虚拟币犯罪，“聚类，即以网络空间内的同类虚拟货币交易痕迹为突破口，以区块链浏览器查询，借助大数据分析，抓取同类异常行为，以此推测可能存在的犯罪主体信息；或以建立虚拟币IP地址为基础，基于启发式聚类方法，综合不同交易聚类特点，对匿名的虚拟币地址进行相关性聚类，分析受同一类团体控制的地址群，根据交易群体，推测犯罪主体”^[30]。据此，可将交易主体缩小至小范围，再结合其他线索，综合分析确定。

（四）链上取证——运用联盟链多层面采集证据

1. 链上数据采集。链上数据产生并记录在链上，取证重点是快速查找和采集，本质是一种溯源取证。理论层面难度较大，技术层面，联盟链是良方。一方面，链上侦查节点实时关注交易数据，发现有证据价值时，及时检索、采集和固定；另一方面，积极研发取证侧链，根据类案取证规则，编制取证合约代码、植入链中，构成取证基础合约集。针对个案，受案后依案情和取证需求，修改、调整合约代码，形成个案取证合约，部署上链。如链中出现有证据价值的钱包地址、区块高度、时间戳、交易哈希值、资金流向等信息时，合约自动抓取、及时存储，形成证据数据集。

2. 链外证据上链。链外证据是与虚拟币犯罪相关但未在联盟链上的各类证据，既包括线上的即时通信、资金流转记录等数据，也包括线下的实物类证据，侦查员均需及时采集上链。对于前者，可通过取证侧链，连接公安、金融监管等部门专网，经数字签名和人脸识别等可信身份认证，开启链外

数据的网络线上取证及同步上链程序，全程录屏并进行哈希运算，哈希值上传云端，实现云上取证^[31]。可以借鉴杭州市余杭区检察院的做法，研发并运行“云上取证”系统，依托区块链、网络传输、人脸识别、屏幕共享、云存储、电子签名、网络视频等技术，实现身份验证、图像截屏、远程录屏、在线取证。针对当前虚拟币犯罪的作案人、网络设备和涉案虚拟币均在境外（俗称“三头在外”）的困境，云上取证能有效解决管辖不明、跨境协作难、证据灭失风险高等难点和痛点。对于线下实物证据，如计算机设备、网络服务器、存储介质等，需要专门的线下取证、上链固定。可借鉴杭州市西湖区检察院的做法，研发类似于执法记录仪的“区块链取证设备”，将区块链技术芯片植入执法记录仪中，现场执法时，边勘验边录像，同步上传入链，分布式存储和验真。公安机关效仿研发“联盟链侦查记录仪”，使线下实物证据取证工作同步上链。

（五）链上追赃——链上资金追踪及合规处置

1. 链上资金追踪。联盟链建成，侦查节点依托联盟链，并运用区块链浏览器及一些区块链公司研发的资金追踪系统，顺线追查每笔资产的流向，确定赃款的去向。其一，运用区块链浏览器。如，以 Vision 区块链浏览器为例，获取可疑交易的哈希值，就可利用该值查询交易明细、详情、发出和接收地址，研判是否为涉案的高危地址，并顺线查询交易上家和下家，形成资金链路。如果作案人使用混币或跨链等技术，依然使用区块链浏览器，结合前文提及的地址聚类 and 标签分析等技术，从混币器中离析每笔交易，或从多个交易链中逐一剥离每笔交易。其二，运用区块链公司研发的资金追踪软件。如前文提到的“链必追”“无匿”等追踪系统，后者将链上地址分为充币地址、提币地址、资金池地址、作案人收割跑路地址等，通过分析，可以清晰、可视化地展示各地址间的资金流转关系^[32]，是资金追踪利器。当然，链上追踪同时也要结合链下追踪和暗网追踪，前者如抓捕犯罪嫌疑人时，从其住宅、工作场所搜查、获取钱包地址或助记词等。后者通过对表网^①及现实空间的仔细筛查，查找暗网交易的地址和轨迹。辩证唯物主义联

系学说和空间转移理论认为，网络与现实、表网与暗网总是不停地发生着各种各样的联系，并在相应空间留下轨迹。

2. 资金合规处置。处置虚拟币主要包括冻结、变现两个环节。冻结需要准确区分虚拟币是热钱包还是冷钱包。前者由侦查部门直接向境外交易所申请冻结，目前火币、币安、欧易等几大交易所，均接受刑事司法协助申请。如果是冷钱包，交易所也无能为力，只能依托线下缉捕、搜查时现场查扣冷钱包，如嫌疑人随身手机、电脑、智能手表等。采集内部数据，审查是否安装钱包应用软件，从数据中寻找钱包地址或助记词，必要时结合讯问获取。虚拟币变现是当前的办案难点。境内禁止交易，公安机关也不能作为交易主体参与境外交易。综合当前的司法境况，建议由办案机关委托境内公司代为变现。需注意：一是变现对象是比特币、币安币等价值波动较大的虚拟币，以期保值；而价值相对稳定的泰达币，不建议变现，结案后再定；二是与境内公司签订代为变现合同时，务必明确权利和义务，强调正规途径，严禁地下钱庄参与；三是变现全程尽可能同步上链，减少风险隐患。

结语

随着联盟链技术的不断普及和落地应用，“联盟链+行业应用”将成为今后科技研发的制高点。公安机关应尽早接轨，探索构建“联盟链+各警种业务”，这也是公安机关技术发展的必由之路。对侦查领域而言，“联盟链+侦查”是亟须大力研究和推进的关键技术，公安机关应倾力将其打造为引领新时代侦查工作的技术引擎。针对虚拟币犯罪，积极探索和构建以“链上技术自侦查为主、链下人工侦查为辅”的联盟链侦查新模式，令涉币犯罪无处可遁，还链上生态安全，并成为其他类型犯罪联盟链侦查的试金石，技术层面真正实现“准智慧侦查”。将以人为本的传统侦查和以数为本的数据侦查，迭代升级为以机器学习、人工智能、合约代码为本的高阶型和前沿型侦查，必将为法治侦查和平安中国建设作出积极的贡献。

① 表网，是与暗网相对应的一个名词，就是互联网上登记注册、接受正常监管的网站资源，也是广大网民日常使用的网络资源。

【参考文献】

- [1] 黄泽政,李双其. 回应犯罪演变的智慧侦查[J]. 湖南警察学院学报,2022(2):5-11.
- [2] 杨玉晓. 区块链智能合约犯罪刑事司法应对研究[J]. 法律适用,2020(15):145-156.
- [3] 颜卉,朱刚. 区块链智能合约涉诈骗犯罪中数字货币的定性及价值衡量[J]. 人民检察,2022(18):73-74.
- [4] 石宝兰. 数字货币衍生犯罪及其治理[J]. 铁道警察学院学报,2021(2):93-98.
- [5] 向志强,吴梓溢. 虚拟币犯罪现新特点,打击力度持续加大[N]. 经济参考报,2023-06-13(7).
- [6] 史乐蒙. 洗钱成为最普遍的涉虚拟币犯罪形式[N]. 期货日报,2023-08-21(7).
- [7] DYSON S, BUCHANAN J W, BELL L. The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime. arXiv:1907.12221v1 [cs. CY] 29 Jul 2019.
- [8] 吴贻伙,刘晨,唐菲菲. 投资者的虚拟货币被他们从“后门”偷走了[N]. 检察日报,2023-03-21(4).
- [9] 付勇康,徐永新. 区块链虚拟货币传销犯罪侦防研究[J]. 中国人民警察大学学报,2024(2):14-19.
- [10] 高尚. 加密货币犯罪的防范及监管研究[D]. 北京:中国政法大学,2022.
- [11] 刘家豪. 虚拟货币传销犯罪侦查难点与应对[J]. 四川警察学院学报,2024(2):57-64.
- [12] 刘德塘. 利用虚拟货币洗钱犯罪的侦查困境及治理路径研究[J]. 上海公安学院学报,2024(2):39-48.
- [13] 谢玲. 暗网犯罪刑事治理研究[J]. 学术论坛,2020(5):13-24.
- [14] 田力男. 刑事涉案虚拟财产强制处分论[J]. 中国法学,2023(5):111-127.
- [15] 李晓东. 论区块链侦查[D]. 武汉:中南财经政法大学,2023.
- [16] 潘嘉瞳. 区块链侦查研究[D]. 北京:中国人民公安大学,2024.
- [17] 王燕,潘振生,贾林鹏. 区块链3.0时代虚拟货币洗钱犯罪情报分析研究[J]. 情报杂志,2024(8):59-65.
- [18] 刘品新. 论区块链证据[J]. 法学研究,2021(6):130-148.
- [19] 高明,等. 数据世系管理技术研究综述[J]. 计算机学报,2010(3):373-389.
- [20] 马明亮. 基于区块链的大数据侦查:价值、场景与协同规制[J]. 公安学研究,2022(4):1-18.
- [21] 丁鹏. 区块链技术与场景[M]. 北京:电子工业出版社,2021:26.
- [22] 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.
- [23] 兰立宏. 论虚拟货币的犯罪风险及其防控策略[J]. 南方金融,2018(10):33-40.
- [24] 王燃. 大数据时代侦查模式的变革及其法律问题研究[J]. 法制与社会发展,2018(5):110-129.
- [25] 姚前. Web3.0:渐行渐近的新一代互联网[J]. 中国金融,2022(6):14-17.
- [26] 师秀霞. 利用虚拟货币洗钱犯罪的防控策略[J]. 中国人民公安大学学报(社会科学版),2016(1):1-11.
- [27] 李康震,陈刚,周芮. 区块链技术在侦查领域中的应用研究[J]. 信息资源管理学报,2018(3):81-92.
- [28] 马明亮. 区块链司法的生发逻辑与中国前景[J]. 比较法研究,2022(2):15-28.
- [29] 李大猛,孙杰,蒋照生,彭延荣. 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.
- [30] 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.
- [31] 赵东方. 区块链技术在网络犯罪侦查中的应用研究[D]. 北京:中国人民公安大学,2021.
- [32] 黄奕翔,王容刚. 利用虚拟货币传销犯罪模式及侦查对策研究[J]. 网络安全技术与应用,2023(7):152-154.

(责任编辑 徐艳宏)