区块链3.0时代虚拟货币洗钱犯罪情报分析研究

王 燕[1] 潘振生[2] 贾林鹏[3]

(1. 中国人民公安大学法学院 北京 100038; 2. 北京市西城区人民检察院 北京 100035;
3. 中国科学院 计算技术研究所 北京 100190)

摘 要:[**研究目的**]提出针对虚拟货币洗钱犯罪的情报分析工具和方法,以增强执法机关打击此类犯罪的能力,旨在响应区块链技术快速发展背景下,虚拟货币洗钱犯罪日益增多且侦查难度加剧的挑战。[**研究方法**]综合运用文献分析、比较分析和逻辑分析方法,梳理国内外关于虚拟货币洗钱犯罪情报相关研究,总结区块链3.0时代虚拟货币洗钱的技术和特点,提炼虚拟货币洗钱犯罪情报分析的一般流程与重点技术。[**研究结论**]混币服务、去中心化交易和跨链技术成为当下虚拟货币洗钱应用的主要技术,应优化情报分析工具、技术和流程:情报分析工具呈现专业化和应用性特点;人工智能在情报分析技术中发挥愈加重要的作用;情报分析流程应注重一般流程的构建,包括数据收集与预处理、地址间分析、地址与主体关系分析、主体与行为分析,助力虚拟货币洗钱犯罪的追踪和分析。

关键词:虚拟货币洗钱犯罪;区块链;情报分析;人工智能

中图分类号:G353.1 **文献标识码:**A **文章编号:**1002-1965(2024)08-0059-07

引用格式: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,2024,43(8):59-65.

DOI:10.3969/j.issn.1002-1965.2024.08.008

Analysis on Virtual Currency Money Laundering Crime Intelligence in the Blockchain 3.0 Era

Wang Yan[1] Pan Zhensheng[2] Jia Linpeng[3]

(1. Law School, People's Public Security University of China, Beijing 100038;
2. People's Procuratorate of Xicheng District, Beijing 100035;
3. Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190)

Abstract: [**Research purpose**] This study proposes intelligence analysis tools and methods for combating virtual currency money laundering crimes, aiming to enhance law enforcement agencies' capabilities in response to the increasing challenges of virtual currency money laundering crimes amidst the rapid development of blockchain technology. [**Research method**] A comprehensive approach utilizing literature analysis, comparative analysis, and logical analysis is employed to review domestic and international research related to intelligence on virtual currency money laundering crimes. The study summarizes the technologies and characteristics of virtual currency money laundering in the era of blockchain 3.0, and extracts the general process and key technologies of intelligence analysis for virtual currency money laundering crimes. [**Research conclusion**] Coin-mixing services, decentralized transactions, and cross-chain technologies have become the main technologies used in current virtual currency money laundering applications. Intelligence analysis tools, technologies, and processes should be optimized; intelligence analysis tools exhibit specialization and applicability; artificial intelligence plays an increasingly important role in intelligence analysis technology; the intelligence analysis process should focus on constructing a general framework, including data collection and preprocessing, address interlink analysis, address-entity relationship analysis, and entity-behavior analysis, to facilitate the tracking and analysis of virtual currency money laundering crimes.

Key words: virtual currency money laundering crime; blockchain; intelligence analysis; artificial intelligence

收稿日期:2023-12-21 修回日期:2024-01-30

作者简介:**王 燕**,女,1990年生,博士研究生,研究方向:网络犯罪、刑事司法;**潘振生**,男,1997年生,研究方向:网络犯罪、公安情报学;**贾林鹏**,男,1995年生,助理研究员,研究方向:区块链、虚拟货币。

0 引 言

自 2008 年区块链技术诞生以来,经历了三个重要的发展阶段:技术起源、数字货币和智能合约[1]。在智能合约被广泛采用的区块链 3.0 时代,虚拟货币的种类和使用范围不断扩大。虚拟货币的发明与发展具有双重性:一方面,它使得互联网上的安全交易更加便捷;另一方面,虚拟货币被广泛用于促进各种网络犯罪。据 Chainalysis 的《2022 年加密货币犯罪报告》估计,自 2017 年以来,网络犯罪分子利用虚拟货币洗钱的金额已超过 330 亿美元[2]。在 2021 年,通过虚拟货币洗钱的金额达到 86 亿美元,同比增长 31%[3]。我国近年来的虚拟货币犯罪也日益严重,2022 年涉案金额高达 348.49 亿人民币[4]。因此,对虚拟货币洗钱犯罪进行情报研究具有重要意义。

国外研究文献的收集是通过谷歌学术和“Web of Science”数据库完成的,涉及虚拟货币洗钱和犯罪情报相关主题筛选出 81 篇有效文献。研究主要集中在虚拟货币洗钱的特点和原理、情报分析、技术监测以及人工智能在反洗钱领域的应用等方面。如金融行动特别工作组(Financial Action Task Force,简称“FATF”)分析了虚拟货币被应用于洗钱的情况,并提出使用监测虚拟货币交易、使用区块链分析工具等方式来发现洗钱活动[5];Furneaux 对虚拟货币调查、区块链证据的提取分析进行了较为全面的研究[6];Seo 等提出比特币混合服务和反洗钱策略,强调分析和追踪资金流动的重要性[7];Kuet 等对深度学习与人工智能用于可识别洗钱交易进行了分析,并提出未来的研究方向为数据预处理、对大数据进行模型评估、图挖掘和社交网络分析、应用可解释的 AI 技术等[8]。国内的研究主要来源于中国知网,集中在虚拟货币洗钱的监管和犯罪侦查研究上。吴云的研究提供了虚拟货币洗钱犯罪情报研究的理论基础[9];陈亮构建了基于情报主导的洗钱犯罪威胁评估模型[10];李涛提出了虚拟货币犯罪侦查策略[11]。虽国内外对虚拟货币洗钱犯罪有一定研究,但专门从情报领域进行系统研究的文献较少。本文将从虚拟货币洗钱犯罪的技术原理以及情报分析工具、流程和技术等方面进行探讨,旨在通过情报分析研究助力虚拟货币洗钱犯罪的发现、追踪和取证。

1 虚拟货币与洗钱犯罪

1.1 虚拟货币概述

2009 年 1 月 3 日,首个成功应用区块链技术的虚拟货币——比特币诞生。虚拟货币是基于密码学技术的数字资产,可用作交易媒介、价值存储和投资工具。随着以太坊等项目的发展,虚拟货币种类不断增加,如 USDT、ETH、TRX、BNB、BUSD 及非同质化代币 NFT 等。其核心特点包括去中心化、匿名性、不可篡改性、可追溯性和全球可兑换性。去中心化指虚拟货币不依赖于中央机构,通过分布式网络运行。虚拟货币系统还可以在互联网上交易,允许匿名资金资助[5]。所有交易均记录在不可篡改的区块链上,确保交易历史的可追溯性。虚拟货币为金融系统带来新机遇,同时也增加了犯罪监管和侦查的难度。

1.2 虚拟货币洗钱的新特点与新趋势

洗钱是隐匿或掩饰犯罪所得财物的真实性、来源、流向的行为[12]。在区块链 3.0 时代,虚拟货币洗钱的主要特点如下:

1.2.1 虚拟货币洗钱成为新趋势,涉案金额巨大

虚拟货币洗钱已成为全球洗钱犯罪的新方式,每年超过 90% 的洗钱活动未被察觉[13]。虚拟货币洗钱包括放置、分层和整合三个阶段。放置是将资金引入的过程,如果在不遵守反洗钱法律的交易所进行转换,黑钱可以轻松的被匿名洗白。分层是指将资金分散的过程,该阶段本可通过监控区块链的交易来跟踪其流转轨迹,但仍可以使用匿名化途径隐藏资金来源。整合是网络洗钱的最后阶段,此时的货币已不再直接与犯罪相关,已经提升到无法轻松追踪的程度。虚拟货币使洗钱活动更隐蔽、难以发现。

1.2.2 区块链技术发展快,洗钱方式不断升级

区块链技术的去中心化和匿名性特点使虚拟货币成为洗钱的理想工具。随着技术进步,洗钱手段从组织“币农”和场外交易演变为混币平台、去中心化交易和跨链等新技术应用。例如,Bisq 等去中心化交易所允许用户在无需注册的情况下交易[14],根据有关虚拟货币和洗钱活动的最新研究,洗钱者越来越多地转向 DeFi 协议[3]。这些技术的发展导致虚拟货币洗钱犯罪的隐蔽性增强,侦破难度增大。

2 虚拟货币洗钱犯罪的技术原理

2.1 区块链技术:虚拟货币洗钱的基础技术

以比特币为代表的虚拟货币基于区块链技术实现,区块链是一种特定数据结构,按时间顺序将区块以链表形式组合,并通过密码学保证数据不可篡改和伪造的去中心化共享总账[15]。涉及分布式账本、非对称加密、共识机制和智能合约等技术。每个货币都有一个由公钥和私钥组成的地址,公钥用于标记每个货币,私钥由所有者保管。用户转移资金时,发送方创建消息并用私钥签名。区块链技术已发展到 3.0 版本。区块链 1.0 最具代表的应用是比特币,区块链 2.0 最具代表的是以太坊。以太坊是一种开放的区块链平台,具有强大的智能合约功能,为区块链 3.0 去中心化的

大量应用奠定基础。区块链 3.0 代表了区块链技术的进一步发展和演进,实现了智能合约的广泛应用和跨链互操作性,其典型代表是去中心化金融(DeFi)、非同质化代币 NFT 的快速发展,为涉案资金的转移提供了新的隐匿方式,使得洗钱犯罪更难以被追踪和治理。

2.2　区块链 3.0 下虚拟货币洗钱应用的新技术

2.2.1　混币服务

由于虚拟货币交易在公链上可查询,为保护用户隐私产生了混币服务(Bitcoin Laundry)。混币服务的原理是通过整合无关交易实现交易匿名性。一种是如门罗币等匿名增强型虚拟货币使用环签名和隐秘地址技术,发送方、接收方和交易金额都被混淆,难以追踪。另一种是通过混币器来实现,如混币器通过一系列复杂的、半随机的虚假交易来发送交易,使得特定的虚拟货币(地址)与特定交易之间极难建立联系[16]。混币器 Tornado Cash 曾是犯罪分子的首选工具,但已受到制裁(2022 年美国财政部下属的外国资产控制办公室以 Tornada Cash 被犯罪分子自 2019 年利用清洗了价值超过 70 亿美元的虚拟货币为由列入制裁名单)。

2.2.2　去中心化应用

基于智能合约的去中心化交易模式广泛应用于区块链 3.0。由于中心化交易所(CEX)需实名登记,洗钱方式转向去中心化交易所(DEX)。去中心化交易所是运行在区块链上的智能合约,提供点对点交换机制,用户在无中介情况下交易代币。除此之外还有去中心化金融 DeFi,其允许用户将一种代币换成另一种新代币,且大多数的 DeFi 项目缺乏 KYC(Know-Your-Customer)要求,在这些协议上追踪资产移动存在难度。

2.2.3　跨链技术

跨链行为通过中间技术在不同区块链上转移虚拟货币,其底层技术是区块链的跨链技术,使用智能合约促成交换。正常独立的两条区块链是独立的分布式账本,跨链技术实现二者共通。跨链结束将 A 链虚拟货币转移到 B 链上,在公链上只显示 A 链资金转入合约,不显示 B 链资金信息,从而实现匿名化交易。跨链作为洗钱“分层”技术,增加匿名层。据统计,通过跨链的链跳洗钱已超过 7.5 亿美元,跨链已成为流行的洗钱技术[17]。

3　虚拟货币洗钱犯罪情报分析工具

虚拟货币洗钱犯罪频发,相关部门对链上数据的获取和分析需求十分迫切。针对虚拟货币洗钱的情报分析工具应运而生。本文对国内外提供区块链数据服务及打击虚拟货币洗钱活动的分析工具进行了梳理与分析。根据分析工具的功能和价值,将其分为查询类、监测类、追踪取证类。查询类工具在情报分析中扮演重要角色,通过收集、整理和可视化区块链及交易的多样数据,为用户提供了全面的视角。监测类工具则是通过实时监测、交易追踪、实体联系等提供强大的实时监控和风险评估功能,为用户及时应对潜在的洗钱活动提供支持。追踪类工具专注于追踪区块链上资金流动,通过链分析数据利用、跨链调查等实现匿名服务交易追踪、案件线索筛查、一站式多维度识别及调证固证支持(见表 1)。

表 1　国内外虚拟货币洗钱犯罪情报分析工具

类别	分析工具	主要功能	可用性及价值分析
查询类	Elliptic 研发的 Wallet Screening	识别钱包的所有者、资金的来源、目的地和行为	实现交易筛选、多资产筛选与跨链溯源;识别加密地址或钱包是否由特定虚拟货币交易所、受制裁实体等控制
	CipherTrace 研发的 Armada	揭示与虚拟货币相关的交易	允许查看与风险和欺诈相关的数据;将法定名称和帐号映射到虚拟资产服务提供商(VASP),帮助发现用于风险和欺诈模型的虚拟货币交易
	Coinmetrics 研发的 Network Data、Market Data	提供去中心化加密情报	提供链上交易流量、财富区间、资金规模、时间指标和交易明细;提供来自 30 多家现货和衍生品加密交易所的数据
	区跨链数据和智能平台 Glassnode	利用工具套件来分解和理解区块链数据	Studio 可以显示链上活动、实体、地址等内容;Metrics 涵盖了一系列资产的众多链上指标;Insights 提供市场动向、交易所活动报告
	欧科云链研发的链上天眼	区块链大数据监测和交易行为可视化工具	一键式地址挖掘、交易图谱展示和 NFT 溯源;通过多维度数据监测和历史事件分析,建立安全监测模型和指标体系
	成都链安研发的链必知	区块链安全舆情平台	实时获取区块链行业资讯,对情报内容进行自动实时分析;自动推送资讯消息、多维度关联检索、自定义专题等
监测类	Chainalysis 研发的 Chainalysis KYT	识别高风险的交易并提示预警	对虚拟货币资产进行交易监控;追踪资金流,并将可疑活动与现实世界的实体联系起来;优化警报以暴露未知风险
	Elliptic 研发的 Transaction Monitoring	揭示资产通过不同区块链和资产时的移动情况	同时跟踪整个虚拟货币资产生态系统的交易;通过数字风险评分及时了解钱包情况,可在平台内进行自定义设置阈值,超过特定数值后触发警报
	Ciphertrace 研发的 Ciphertrace Sentry	监控虚拟货币反洗钱交易	赋予 VASP 自动筛选交易可疑活动功能;赋予开发人员利用数据实现交易监控
	Coinfirm 研发的 Coinfirm Analytics	监测交易和钱包的区块链分析平台	筛选并评估区块链交易的所有地址;可用其数据库中的模型分析验证风险

续表1 国内外虚拟货币洗钱犯罪情报分析工具

类别	分析工具	主要功能	可用性及价值分析
监测类	CertiK 研发的 Skynet 及 Sky-Insights	区块链智能平台、Web3 安全分析及数据研究工具	主动监测链上和链下数据实现实时预警;为虚拟货币安全和监管环境提供实时风险监控
	Peck Shield 研发的 coinholmes 平台	提供区块链数据、分析服务和反洗钱解决方案	实时监控和识别异常交易;通过其能了解全球资产分布,降低潜在风险
	欧科云链研发的链上 AML	数字货币交易监测及大数据风险评估	监控充提币交易风险、识别恶意地址并生成警报;针对链上地址的风险类型进行识别、分析、测算和分类
	成都链安研发的链必控	安全态势感知平台	监控链上运行状态、实时交易行为,自动识别异常交易;基于人工智能技术,结合开源情报线索实现交易风险实时感知
追踪类	Chainalysis 研发的 Chainalysis Reactor	追踪区块链上资金流动的调查软件	通过链分析数据和地址标签,将区块链上的活动与现实联合起来;跨链调查允许用户在单个图表中追踪多个资产的资金
	Elliptic 研发的 Crypto Investigations	可跨区块链和资产进行调查	使用人工智能和机器学习技术来跟踪和定位区块链上的可疑交易;帮助执法机构获取有关加密货币犯罪的线索和证据
	Coinfirm 研发的 Coinfirm Investigator	可对通过匿名服务的交易进行追踪	实时追踪、自动追踪资金流向;生成总结跟踪结果的表格证据,为调查工作提供证据
	慢雾科技(SlowMist)研发的 MistTrack 追踪服务	集追踪、调证、分析证据为一体的平台	分析资金链路情况、监控案件关联地址;根据追踪情况形成分析报告;协助警方联系可调证交易平台,对涉案的交易平台充值地址进行调证冻结
	成都链安研发的链必追	利用人工智能技术的研判平台	利用人工智能算法智能筛查案件线索;实现交易地址的精准刻画、多地址多币种追踪及关联分析、一键调查取证;出具司法鉴定固证报告[18]
	中科链源研发的安士	结合AI模型、大数据溯源追踪、链上地址穿透等技术的区块链信息作战系统	实现任意地址来源及去向追踪、不同币种的交易资金链路追踪、去向关联分析;一站式多维度识别犯罪嫌疑人

4 虚拟货币洗钱犯罪情报分析流程

虚拟货币洗钱犯罪情报分析流程是针对洗钱犯罪情报分析的步骤与过程,可分为一般流程和特殊流程。一般流程程是指一般情况下的洗钱犯罪情报分析,始于数据收集、处理,进行识别洗钱模式,锁定取币地址,并最终分析出洗钱犯罪主体,如图1所示。特殊流程则是由于线下冷钱包交易导致缺乏必要的分析数据,只能通过链下数据和特殊的侦查手段进行情报分析。本文重点对虚拟货币洗钱犯罪情报分析的一般流程进行归纳,同时指出目前对特殊流程的依赖趋势也在逐步增强。

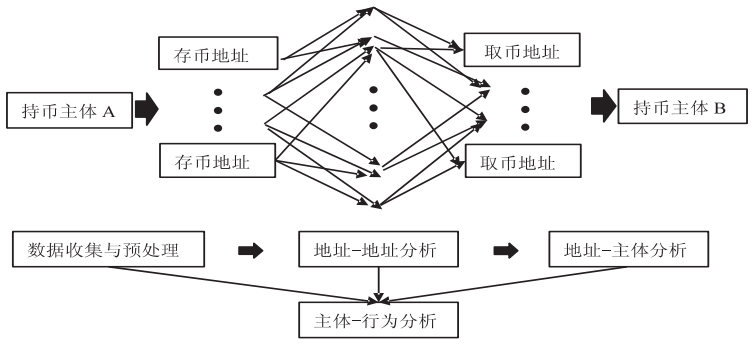

图1 虚拟货币洗钱犯罪情报分析一般流程

4.1 数据收集与预处理

数据收集对于虚拟货币洗钱犯罪情报分析来说尤为重要,决定了后续分析的质量和准确性[19]。虚拟货币交易数据是情报分析的主要数据来源,它包含了虚拟货币交易的所有记录。数据预处理是指基本的数据处理,主要目的在于通过对虚拟货币交易原始数据进行收集、清洗、整理,以便于开展后续分析。虚拟货币洗钱犯罪数据收集与预处理涉及以下几个常见的步骤:

4.1.1 区块链数据获取

区块链是虚拟货币交易的底层技术,所有的交易记录都被记录在区块链上。因此,从区块链中获取数据是情报分析的起点。情报分析师可以通过公开的区块链浏览器获取虚拟货币交易数据。以比特币为例,首先获取比特币区块链的全节点数据,其次获取区块数据,如通过 Bitcoin Core APP、比特币 P2P 网络协议或区块链浏览器的 API 接口来获取并更新区块数据。

4.1.2 虚拟货币交易数据整合与清洗

虚拟货币交易数据通常分布在不同的区块链网络和交易所中,因此需要将这些数据整合在一起。由于区块链数据的庞大和复杂性,需要进行数据清洗和预处理,以提取有用的信息。将不完整数据清洗后,需要对交易所、钱包、智能合约地址、涉案人员高度关联地址等数据进行初步的统计分析,通常包括特征分析、聚类分析等。

4.1.3 链下数据的获取

从当前的虚拟货币洗钱犯罪情报分析实务经验看,越来越多的虚拟货币洗钱犯罪从业人员,特别是单次大额交易,选择使用冷钱包进行线下实物交易以规

避链上数据监管。针对这类“线上转线下”的交易模式,需要执法部门介入,获取一般机构无法获取的链下数据,通过第三方数据库或其他各种合法渠道确认身份信息,如互联网 IP 地址追踪、线下视频比对等方式进行非面对面的交易主体身份识别和验证。

4.2　地址-地址分析:可疑交易模式识别与异常检测

从存币地址追踪到提币地址,需要运用相关数据分析技术,通过标签、建模、迭代识别成千上万次的拆分、混淆、转移、整合。以网络赌博资金利用虚拟货币洗钱为例,其情报分析过程重点识别以下地址:存币地址,又称入金地址,用于赌客充值入场,存在零存整取的特征,存入时间和金额有也一定的规律特征;下分地址:用于给赌客下分兑换筹码,存在上游交易对手数量少且金额大、下游交易对手数量多且金额零散的特征;过渡地址:用于赌博平台整理资金,向下游逃逸,存在上下游交易对手数量少且整进整出的特征;混淆地址:用于交易承接涉案资金,可混淆资金来源,阻碍资金追踪。其特征是,地址数量较多、上下游交易主体众多、交易频次和交易金额极大,往往同时服务于多个洗钱项目;提币地址:又称获利地址,其特征为有大额余额,交易关系简单。

如前文所述,混币服务和基于智能合约的去中心化交易、跨链交易将成为虚拟货币洗钱的主要途径,这些技术的应用大大增加了虚拟货币洗钱犯罪情报分析的难度,虚拟货币交易的去中心化、匿名性进一步增强,但由于虚拟货币交易记录公开记录这一基本特性,虚拟货币追踪的可能性仍未断绝。从智能合约的代码中提取并解析交易的数据,仍可以发现代币发行或虚拟货币交易的底层逻辑,包括智能合约所部署的混币程序。即使混币服务可自动将一笔交易隐藏于成千上万个钱包地址,也能以进出混币服务的地址为起点,进行碰撞和拓展,识别出一些强关联的地址。通过对这些地址进行的迭代追踪,加强情报分析研判以获得更多线索,直至穿透存币地址到提币地址的关联。在某虚拟货币洗钱情报分析案例中,洗钱黑客将虚拟货币转入混币器 TornadoCash 中,反洗钱方 MistTrack 利用存币/提币时间、提币行为、提币数额分布等关联线索进行提币地址分析,最终锁定了一批符合筛选特征的 TornadoCash 提币地址[20]。

4.3　地址-主体分析:洗钱组织结构与关键成员识别

虚拟货币交易的匿名性是虚拟货币洗钱犯罪情报分析的另一道关卡,需要从虚拟货币洗钱网络结构图出发,找到虚拟世界与现实世界的连接,“按图索骥”般分析地址背后的真正交易主体。虚拟货币洗钱犯罪的匿名性障碍主要体现在:一是注册虚拟货币钱包地址不需要实名认证;二是通过“IP 代理”或域名系统(Domain Name System,DNS)服务商来掩饰域名的真实所有者[21];三是使用蝙蝠(BatChat)、电报(Telegram)等加密的聊天软件进行单线沟通。因此,这一过程首先需要数据监控、网站定位、个人信息追踪等技术对重点地址进行梳理,从域名 IP、登录设备、支付信息、电话信息、网络使用痕迹等进行多维度的关联分析和数据交叉比对碰撞,寻找虚拟货币地址与其真实持有人身份之间的联系。其次是判断涉案人员在洗钱团伙中的层级、角色、犯罪参与程度。根据交易情况、相同 IP/电子设备登录情况、聊天记录、文件账本、到案犯罪嫌疑人口供情况等,将交易账户建立起群组关系,通过社交网络技术分析判断出犯罪团伙的组织结构与关键成员。

4.4　主体-行为分析:洗钱行为推测与识别

洗钱犯罪是典型的下游犯罪,可以结合犯罪嫌疑账户中虚拟货币与法定货币等的关联关系,对可能存在的上游犯罪事实及行为进行逻辑推演。不同上游犯罪、不同的资金链路来源,也会影响虚拟货币洗钱模式的选择。对上游犯罪行为的推论是虚拟货币洗钱犯罪情报分析的自然延展。某虚拟货币洗钱犯罪情报分析案例中,根据资金链路情况,通过交易所回函信息及区块链数据信息进行交叉比对,后又根据交易情况、同 IP/设备情况、到案犯罪嫌疑人口供情况,锁定涉案交易所账户 5 个,其中 1 个无身份认证信息,3 个为外籍人员,1 个为中国籍人员。后将上述 5 个账户建立起群组关系,最终判断出这是一个由中国籍人员 L 为组织头目,盘踞在菲律宾的一个从事跨境网络赌博及洗钱活动的犯罪团伙[22]。

5　虚拟货币洗钱犯罪情报分析技术

虚拟货币洗钱犯罪情报分析技术是由虚拟货币洗钱犯罪的特点和情报分析流程所决定的。虚拟货币洗钱犯罪情报分析实质上是广义的数据挖掘,关键是在所有交易数据中识别洗钱模式。虚拟货币洗钱犯罪情报分析涉及的技术较多,本文基于技术价值将虚拟货币洗钱犯罪情报分析技术分为网络分析技术、人工智能技术和辅助类技术三类。

5.1　网络分析技术

对洗钱方法的类型化研究是从个案到一般的过程,是将反洗钱案例上升为监测模型的关键步骤。虚拟货币洗钱犯罪是一种特殊的虚拟货币交易,可以被看作是一种复杂的网络关系图,每个节点代表一个虚拟货币地址,每条边代表交易。因此,一系列基于图论发展而来的技术可应用于虚拟货币洗钱犯罪的情报分

析中。本文根据应用不同将其分为两类,一类是针对交易账户的虚拟货币交易网络图谱分析,另一类是针对交易主体的洗钱犯罪团伙社交网络分析。

5.1.1 虚拟货币交易网络图谱分析

知识图谱在犯罪情报分析领域,常被用于人员身份核查、线索查证分析、受害者画像和犯罪行为描述与分析等[23]。利用图论和复杂网络理论的方法,进行节点度中心性、节点之间的路径和距离、社区结构等分析[24]。事实证明,通过这些情报分析,可以发现洗钱网络中的关键节点、洗钱路径和洗钱模式,从而有助于制定相应的反洗钱策略。

5.1.2 虚拟货币洗钱犯罪社交网络分析

社交网络分析(Social Network Analysis,简称SNA)是一种研究人际关系和网络结构的方法。现有研究表明,社交网络分析可以用来研究和分析犯罪组织的网络结构以及成员之间的关系[25]。在虚拟货币洗钱犯罪情报分析中,社交网络分析可以对犯罪人员进行网络结构分析、识别核心成员和挖掘组织结构,确定洗钱组织内部的层级和角色分工,从而更有针对性地打击洗钱活动。

5.2 人工智能技术

网络分析技术能够为虚拟货币洗钱模式的识别提供基本建模观念和方法,但由于虚拟货币数据量过于庞大,虚拟货币的洗钱账户在一段时间内容易被反复使用,参与交叉转账、来回转账[26],仅靠节点追踪和人工建模已无法有效应对,人工智能技术则通过数据搜集、归纳校验、特征提取、解释修正、聚类整理等对区块链数据及已经带有标签的地址进行训练,建立监测模型,进而分析可疑地址及账户之间的关联,发现洗钱模式和异常行为,甚至能够提前发现潜在的洗钱行为。

5.2.1 机器学习

常见的机器学习方法,如决策树、支持向量机、随机森林和贝叶斯网络等,其核心在于构建分类器,使用大型标注的数据集对欺诈交易进行分类。如前文所述,利用虚拟货币洗钱有放置、分层和整合三个步骤。这些数据驱动的方法通常用于放置和分层阶段。整合阶段的最后阶段很难检测,因为资金已经通过了欺诈检测机制。

5.2.2 深度学习

与传统的机器学习方法相比,深度学习方法可以从原始数据中学习特征表示。深度学习在各种人工智能任务中,包括自然语言理解、图像识别和语音识别方面,已经超越了许多传统的机器学习方法。深度学习算法在虚拟货币洗钱犯罪情报分析中的主要应用包括以下几个方面:

a. 建立网络分析模型。深度学习算法可以直接用于建立虚拟货币洗钱网络分析模型,通过对交易数据的网络结构进行学习,可以发现洗钱行为背后的关联关系和隐藏模式。

b. 挖掘潜在关联信息。利用深度学习技术可以从大量的虚拟货币交易数据中挖掘潜在的关联信息。例如,通过分析交易的时间、地点、金额等特征,可以发现犯罪分子的交易模式、转移路径等,从而帮助执法部门追踪和打击洗钱活动。

c. 研判异常交易情报。通过深度学习模型对大量的虚拟货币交易数据进行分析,可以构建异常交易检测模型,进而可以识别出与正常交易行为不符的模式,如大额交易、频繁转账、集群交易等。

常用的算法通常是基于无监督的社交网络节点排序和社区发现算法,以及半监督或者有监督的图嵌入或社交网络表示学习算法[27]。

5.2.3 自然语言处理

自然语言处理(NLP)是人工智能的一个子领域,可用于跨境网络犯罪社交媒体文本分析和情报研究[28],具体应用包括:其一,实体识别分析。识别和提取虚拟货币交易中的实体,如个人、组织和虚拟货币地址。其二,威胁情报分析。从虚拟货币社交媒体平台、论坛和聊天记录中提取数据,进行语义理解分析,进而识别潜在威胁和洗钱犯罪的迹象,监测和预测洗钱行为。从当前大语言模型(如 ChatGPT)的发展趋势看,其必然将成为虚拟货币洗钱犯罪情报分析的重要技术。

5.3 相关辅助技术

相关辅助技术是指在虚拟货币洗钱犯罪情报分析中随时使用的基础性技术,主要包括可视化技术和数据挖掘技术。

5.3.1 可视化技术

在虚拟货币洗钱犯罪情报分析中,可视化功能成为各类虚拟货币情报分析工具的标配。将洗钱犯罪相关数据和分析结果进行可视化展示,帮助研究者更直观地理解虚拟货币交易的流动和人员关系。

5.3.2 数据挖掘技术

狭义的数据挖掘技术指简单的数据分析技术,可用于虚拟货币交易数据预处理、特征分析、节点追踪等,为网络技术分析和建立人工智能模型提供基础支撑。

6 结 语

随着区块链技术的演进,虚拟货币洗钱犯罪的形态和手段将变得更加复杂。为应对这些挑战,我们需要不断更新和调整情报分析技术。本研究深入探讨了虚拟货币洗钱犯罪的新特点和趋势,并系统性地介绍

了相关的技术原理、分析工具、流程及技术应用,强调了人工智能在虚拟货币洗钱犯罪情报分析中的重要作用。未来,人工智能技术的发展将使得对大规模虚拟货币交易数据的分析更加准确和高效。因此,未来的研究将在技术、方法和合作等方面取得新的突破,更好地服务于执法机关,应对不断变化的虚拟货币犯罪形势。

参 考 文 献

[1] 中国人民银行反洗钱局课题组. 区块链技术在反洗钱工作中的应用前景研究[J]. 金融电子化,2020(10):11-13.

[2] Chainalysis. The 2022 crypto crime report[EB/OL]. [2023-12-19]. https://www. sgpjbg. com/baogao/85462. html.

[3] Guidara A. Cryptocurrency and money laundering: A literature review[J]. Corporate Law & Governance Review ,2022,4(2): 36-41.

[4] SAFEIS 安全研究院. 2022 年涉虚拟货币犯罪趋势研究报告[EB/OL]. [2024-01-26]. https://safeis-official-resource. oss-cn-beijing. aliyuncs. com/pdf/2022 年虚拟货币犯罪趋势研究报告. pdf.

[5] FATF. Guidance for a risk-based approach to virtual assets and virtual asset service providers [R]. [2023-11-06]. https://www. fatf-gafi. org/en/publications/fatfrecommendations/documents/guidance-rba-virtual-assets-2021. html.

[6] Furneaux N. Investigating cryptocurrencies: Understanding, extracting, and analyzing blockchain evidence[M]. John Wiley & Sons, 2018:117-274.

[7] Seo J, Park M, Oh H,et al. Money laundering in the bitcoin network: Perspective of mixing services[C]// 2018 International Conference on Information and Communication Technology Convergence (ICTC). IEEE,2018:1403-1405.

[8] Kute D V, Pradhan B, Shukla N, et al. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering - a critical review[J]. IEEE Access,2021, 9:82300-82317.

[9] 吴　云,薛宏蛟,朱　玮,等. 虚拟货币洗钱问题研究:固有风险、类型分析与监管应对[J]. 金融监管研究,2021(10):1-19.

[10] 陈　亮. 基于情报主导的洗钱犯罪威胁评估模型研究[J]. 信息资源管理学报,2021,11(5):27-37.

[11] 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),2022,38(4):40-52.

[12] 孟建华. 洗钱与银行业机构反洗钱[M]. 福州:福建人民出版社,2006:4.

[13] Wronka C. "Cyber-laundering": The change of money laundering in the digital age[J]. Journal of Money Laundering Control, 2022,25(2): 330-344.

[14] Marques. E. G. Cryptocurrencies: Threats and investigative opportunities for law enforcement[D]. Charles Univesity,2018.

[15] 成都链安. 虚拟货币犯罪研究与实战(2023 版)[R]. 成都:成都链安,2023.

[16] FATF . Virtual currencies: Key definitions and potential AML/CFT risks[EB/OL]. [2023-12-19]. https://www. fatf-gafi. org/en/publications/methodsandtrends/documents/virtual - currency-definitions-aml-cft-risk. html.

[17] Elliptic . The state of cross-chain crime[EB/OL]. [2023-10-20]. https://hub. elliptic. co/reports/the-state-of-cross-chain-crime-2022/.

[18] 网盾安全学院. 成都链安推出 Beosin-AML 虚拟资产调查取证和反洗钱合规系统[EB/OL]. [2023-11-20]. https://chuanpuyun. com/article/2719. html.

[19] Van Wegberg R, Oerlemans J J, van Deventer O. Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin[J]. Journal of Financial Crime, 2018, 25(2): 419-435.

[20] Zero. MistTrack 案例一:TornadoCash 提款分析[EB/OL]. [2024-01-20]. https://mp. weixin. qq. com/s/U03CUJDk1ZOZoPLfxAZY5Q.

[21] 李思佳. FATF 建议下虚拟货币反洗钱法律问题研究[J]. 河北法学,2021,39(10):166-187.

[22] 施竣鹏. 以虚拟货币为载体的犯罪活动浅析[EB/OL]. [2024-01-20]. https://mp. weixin. qq. com/s/NuTk16FrqTB8NYAvqXnlLA.

[23] 漆桂林,高　桓,吴天星. 知识图谱研究进展[J]. 情报工程,2017,3(1):4-25.

[24] Wu Y, Tao F, Liu L, et al. A bitcoin transaction network analytic method for future blockchain forensic investigation[J]. IEEE Transactions on Network Science and Engineering, 2020, 8(2): 1230-1241.

[25] 陈　鹏,袁宏永. 犯罪组织结构的社会网络分析[J]. 清华大学学报(自然科学版),2011,51(8):1097-1101.

[26] 谢　玲. 遏制电诈犯罪虚拟货币跨境洗钱研究—以资金流查控为视角[J]. 中国人民公安大学学报(自然科学版),2022,28(4):67-74.

[27] 霍丽霞,曹荣鑫,邱宗炽,等. 电子数据取证工作中虚拟货币的调查分析与思路探讨[J]. 中国安防,2022(Z1):77-82.

[28] 白　云,李白杨,王施运. 面向新型跨境网络有组织犯罪的开源情报获取与利用方法[J]. 信息资源管理学报,2022,12(2):65-75.

(责编:王育英;校对:贺小利)

(上接第 71 页)

[36] 中国政府网. 中共中央办公厅国务院办公厅印发《关于加强科技伦理治理意的意见》[EB/OL]. http://www. gov. cn/zhengce/2022-03/20/content_5680105. htm.

[37] 阎国华. 技术应用不确定性的道德治理何以可能[J]. 理论学刊,2022(5):135.

[38] 王小伟. "道德物化"与现代科技伦理治理[J]. 浙江社会科学,2023(1):119.

(责编:王平军;校对:贺小利)