DOI 10.15302/J-SSCAE-2024.11.025

区块链系统中反洗钱技术研究综述

刘乐源[1]，李湘叶[2]，蓝天[2]，程亚坤[3]，陈伟[1]，李智鑫[3]，曹晟[2]，韩伟力[3,4]，张小松[2*]，柴洪峰[3,4]

（1. 电子科技大学信息与软件工程学院，成都 610054；2. 电子科技大学计算机科学与工程学院， 成都 611731；3. 复旦大学计算机科学技术学院，上海 200433；4. 复旦大学金融科技研究院，上海 200433）

摘要：在全球金融格局深刻变化的背景下，区块链技术成为Web 3.0金融的重要基础设施、全球金融科技发展的制高点，不法分子也在利用区块链技术规避监管审查、进行洗钱等非法交易，威胁着国家和全球金融安全；亟需梳理现有的反洗钱技术研究进展，前瞻区块链系统中反洗钱技术研究方向，更好应对区块链技术应用伴生的新型金融安全挑战。本文阐述了传统反洗钱模式、区块链系统中的洗钱模式等反洗钱技术研究背景，辨识出反洗钱任务面临的迫切挑战；按照设置交易参数的阈值、地址与实体关联分析、跨链关联分析等基于规则的反洗钱方法，支持向量机、逻辑回归、决策树、随机森林、k均值聚类、结合链下信息等基于传统机器学习的反洗钱方法，卷积神经网络、循环神经网络、图神经网络、Transformer等基于深度学习的反洗钱方法的分类，全面梳理了区块链系统中反洗钱技术的研究现状，辨识了相关技术的应用特性，讨论了支持反洗钱研究的常用数据集。展望区块链系统中反洗钱技术发展，需在面向不平衡数据、不确定性标注的反洗钱数据集构建，可信反洗钱算法研究，针对隐蔽交易的反洗钱机制研究，兼顾隐私性和可监管性的新技术研发等方面开展部署，提高我国区块链系统中反洗钱技术能力，保障数字经济安全发展。

关键词：反洗钱；区块链系统；机器学习；深度学习；数据集；Web 3.0

中图分类号：TP391　　**文献标识码：**A

A Survey on Anti-Money Laundering Techniques in Blockchain Systems

Liu Leyuan[1], Li Xiangye[2], Lan Tian[2], Cheng Yakun[3], Chen Wei[1], Li Zhixin[3], Cao Sheng[2], Han Weili[3,4], Zhang Xiaosong[2*], Chai Hongfeng[3,4]

(1. School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China; 2. School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China; 3. School of Computer Science, Fudan University, Shanghai 200433, China; 4. Institute of Financial Technology, Fudan University, Shanghai 200433, China)

Abstract: As the global financial landscape undergoes profound transformation, the blockchain technology has emerged as a cornerstone of Web 3.0 finance and a pivotal frontier in financial technology innovation. However, its decentralized and pseudonymous nature has also been exploited by malicious actors to circumvent regulatory oversight, facilitate money laundering, and conduct other illicit financial activities, posing substantial risks to both national and global financial security. Consequently, there is an urgent need to systematically

收稿日期：2024-11-19；**修回日期：**2025-02-20

通讯作者：*张小松，电子科技大学计算机科学与工程学院教授，研究方向为计算机系统与网络安全；E-mail: johnsonzxs@uestc.edu.cn

资助项目：国家自然科学基金项目(U2336204, 62472075)；中国工程院咨询项目“金融法治智能化协同建设的战略研究”(2023-JB-09)

本刊网址：sscae.engineering.org.cn

assess the current progress in anti-money laundering (AML) research, anticipate future directions in blockchain-based AML technologies, and develop effective countermeasures to mitigate the evolving financial security challenges associated with blockchain applications. This study provides a comprehensive review of AML research in blockchain systems, examining the foundational AML frameworks, including traditional AML models and blockchain-based money laundering methodologies. It categorizes existing AML techniques into three primary approaches: rule-based methods, such as transaction parameter threshold setting, address-entity association analysis, and cross-chain association analysis; machine learning-based approaches, including support vector machines, logistic regression, decision trees, random forests, *k*-means clustering, and combining off-chain information; and deep learning-based methodologies, encompassing convolutional neural networks, recurrent neural networks, graph neural networks, and transformer-based models. Furthermore, this study discusses the practical applications of these techniques and reviews commonly used datasets that support AML research. Looking ahead, the advancement of AML technologies in blockchain systems necessitates progress in several critical areas: the construction of AML datasets capable of addressing data imbalance and annotation uncertainty, development of trusted AML algorithms, design of detection mechanisms for covert financial activities, and formulation of privacy-preserving yet regulation-compliant AML solutions. Strengthening these capabilities will enhance the effectiveness of AML frameworks within blockchain ecosystems and contribute to the secure and sustainable development of the digital economy.

Keywords: anti-money laundering; blockchain system; machine learning; deep learning; data set; Web 3.0

一、前言

自比特币概念于2008年[1]提出后，区块链作为分布式账本的支撑技术得到迅速发展，推动了数字经济转型发展。区块链也是Web 3.0生态体系的核心支撑，以去中心化、透明、不可篡改、匿名等特征，为新一代互联网架构提供了技术底座[2~5]。Web 3.0催生了去中心化金融、数字资产交易、去中心化身份验证等新兴应用，加速了全球数字经济发展[3,6]。不可忽视的是，区块链的安全性面临严峻挑战：区块链的匿名性、无国界特性、监管缺失为不法分子从事违法活动提供了条件，智能合约与去中心化交易所也为非法资金的流转与“洗白”创造了便利。例如，仅在2024年上半年全球即发生223起相关的安全事件，损失达到14.3亿美元[7]。

在与区块链系统相关的众多安全问题中，洗钱尤为突出。按照国际定义[8]，洗钱指通过金融交易等手段将非法所得伪装为合法来源的行为，反洗钱则是通过法律框架与监管机制来遏制洗钱及其衍生金融犯罪的系统性实践。国际货币基金组织估算，全球洗钱活动造成经济损失约为2万亿美元/年，占全球国内生产总值的2%~5%[9,10]。在区块链环境下，匿名账户、跨链转移、混币器、隐私币、赌博服务等手段叠加，使洗钱活动更加隐蔽和复杂。例如，有黑客通过多次资金转移和跨链操作，将被盗资金从山寨币逐步转换为以太币、比特币，最终分散至泰达币等稳定币，跨越了比特币、以太坊、Solana、波场币4个区块链网络[11]。

鉴于洗钱行为的严重危害性，各国在法律、技术层面均采取应对措施。在法律层面，美国《银行保密法》[12]、日本《金融商品交易法》[13]、《中华人民共和国反洗钱法》[14]等相继发布，金融机构、服务提供商也在加强实施客户尽职调查（KYC）策略，以遏制洗钱活动滋生。在技术方面，传统基于规则的反洗钱方法虽然易于部署，但依赖先验知识、对新型洗钱手段的适应性不足，限制了应用成效。与此同时，机器学习、深度学习虽然能够提升检测的灵活性，但仍受数据可及性、模型可解释性的制约。近年来，已有文献开展反洗钱研究进展综述，但主要围绕传统金融体系或早期的区块链应用展开，而对当前区块链环境下的反洗钱关键技术、数据集、发展趋势等关注不足[15~17]。尤其是在Web 3.0、区块链技术持续演进的背景下，多模态数据融合、跨链追踪、高隐蔽性洗钱手段业已出现，进一步增加了面向区块链系统开展反洗钱研究综述、支持深入技术研究的迫切性。

仅从已有文献检索可知，未见全面总结区块链系统中反洗钱技术的综述研究。本文围绕这一选题，对现有的反洗钱技术进行全面梳理与比较分析。从技术角度出发，将反洗钱方法分为基于规则、基于传统机器学习、基于深度学习3类进行讨论，并分析常用的公开数据集，进一步就当前研究的局限性、未来发展方向等开展前瞻探讨。

二、反洗钱的背景与应对挑战

（一）传统洗钱模式

反洗钱方法有多种类型（见图1），而洗钱行为通常划分为放置、混淆、整合3个关键步骤（见图2）[18,19]。在放置阶段，洗钱者将非法所得引入金

融系统，一般将大笔现金拆分成小额现金或金融票据，直接存入银行账户。在混淆阶段，洗钱者将资金投入各种掩饰性交易，隐藏资金原始来源。在整合阶段，经过层层掩饰的资金以看似合法的收入或资产形式重新回归到实体经济中（如合法的商业投资、房地产、金融资产等）。

（二）区块链系统中的洗钱模式

在区块链系统中，洗钱行为更趋隐蔽。以比特币为代表的加密货币快速兴起，颠覆了传统银行业的格局，用户无需央行授权即可实现匿名的无现金交易。用户可同时拥有多个假名地址，大量的加密货币亦不涉及国别与监管，显著削弱了传统金融体系中的KYC机制，也为洗钱等非法活动提供了隐蔽空间，增加了全球金融监管的难度。

区块链上的洗钱过程在整体框架上与传统模式类似，同样包括放置、混淆、整合3个阶段，但在混淆阶段引入了剥离链、跨链、混币器、隐私币、赌博服务等技术，显著削弱甚至抵消了传统反洗钱手段的效力（见图3）。不法分子既能够通过去中心化交易所将非法所得转化为加密货币进入区块链体系，又可以在整合阶段应用不受监管的交易所或去中心化金融平台使资金重新回归实体经济，从而规避监管和追踪[20]。区块链上的新技术类型多样，但不法分子在实际操作中会同时采用多种技术实施隐匿洗钱行为。

剥离链主要在“未花费的交易输出”模式的区块链上进行，通常将一笔大额资金通过一系列小额转账分散开来，每次转账都只剥离出少量资金，再将剩余的资金不断转移至新的地址（见图4）。这种链式转账可以将资金逐渐“稀释”，降低被追踪的可能性。

跨链将一种加密货币兑换成其他加密货币，再将现有的加密货币转移到其他区块链上，通常表现为大量、快速执行的交易方式（见图5）。

混币器指专门设计的用于支持匿名化、混淆、

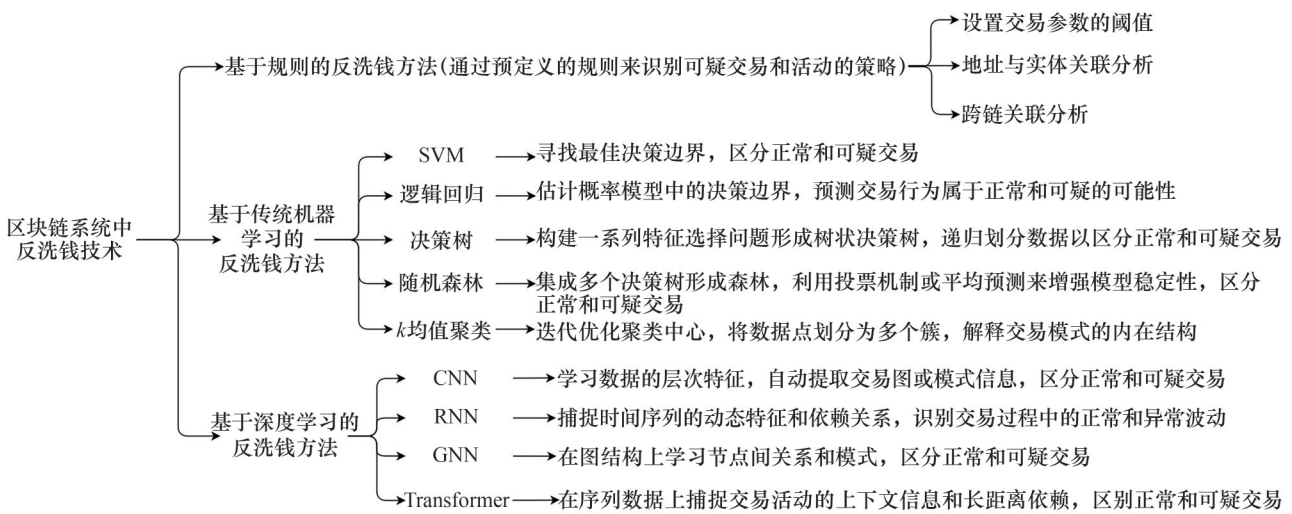

图 1　区块链系统中反洗钱技术分类

注：SVM表示支持向量机；CNN表示卷积神经网络；RNN表示循环神经网络；GNN表示图神经网络。

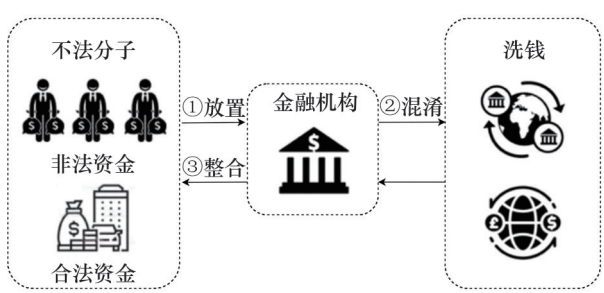

图2　传统洗钱的流程

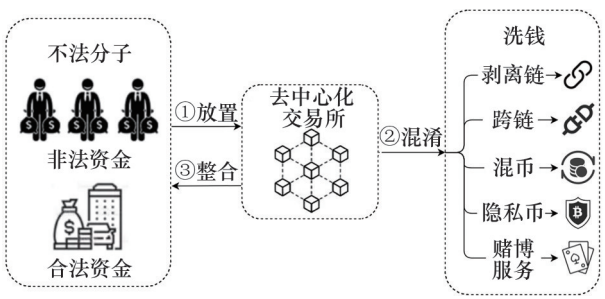

图 3　加密货币洗钱的流程

分散加密货币交易过程的服务，如Tornado Cash（见图6）[21]。相关分析案例表明，监管机构在监督和追踪区块链系统中的交易时面临挑战[22]。

隐私币指特别设计、用于保护用户交易隐私的加密货币（见图7），以Monero[23]为代表。Monero采用多种措施来提高用户及其交易的匿名性，使用环签名[24]来隐藏交易的来源，可将历史交易的虚假输出进行组合；还采用环机密交易技术[25]以隐藏交易金额，并使用一次性地址（又称隐形地址）。

赌博服务通常起到中介作用，接受玩家的数字货币存款并在赌博平台上进行交易，将非法资金与其他客户的资金混在一起。

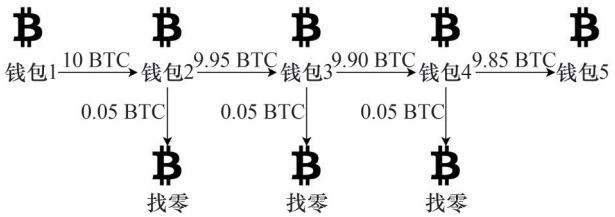

图 4　剥离链示意图

注：BTC表示比特币。

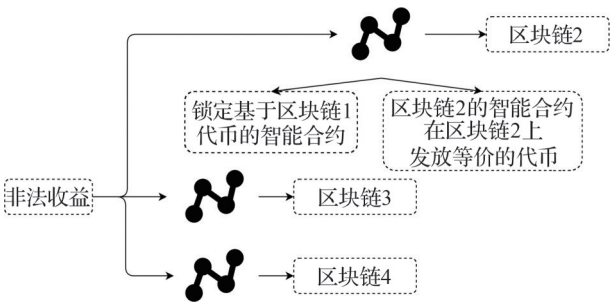

图 5　跨链示意图

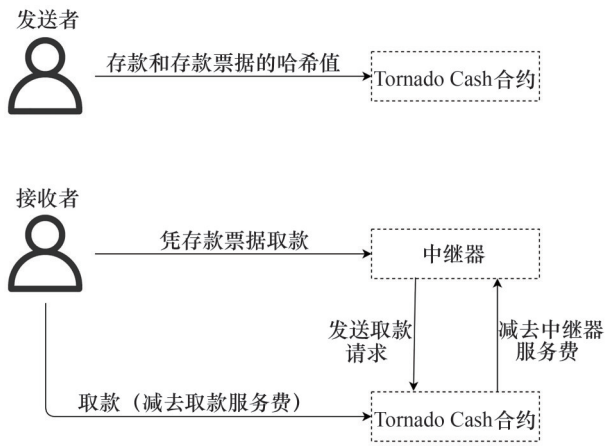

图 6　混币器示意图（以Tornado Cash为例）

（三）反洗钱面临的挑战

1. 网络稀疏性

在区块链反洗钱任务中，受隐私政策的限制，不同机构通常仅能访问各自的内部数据，导致跨平台交易数据碎片化，形成了稀疏网络。在此情景下，传统机器学习和深度学习模型的信息传播与特征聚合能力受到限制，难以充分学习代表性特征，更易出现过拟合和不稳定，也就降低了面向新数据的泛化能力。

2. 交易数据量巨大且不平衡

在区块链反洗钱任务中，解决交易量巨大且数据不平衡的问题至关重要。例如，微众银行的日活跃用户数为百万量级，蚂蚁金服的日活跃账户为数亿个[26,27]，庞大的交易规模对深度学习模型的训练时间、表达能力等构成了严峻挑战；仅有约0.02%的账户被标记为可疑，数据的不平衡性进一步降低了监督学习模型的检测效果。

3. 模型可解释性不佳

基于神经网络的黑箱模型在检测准确性上优于传统方法，但结果的可解释性面临挑战。银行等金融机构在应用这些模型时，需向监管机构提供合理依据以证明标记可疑交易的合法性。然而，深度神经网络的决策过程不透明，使监管机构难以理解模型的判断逻辑，实际上构成新技术方法在反洗钱应用的关键障碍。

4. 公开数据集缺乏

尽管已有Elliptic等常用数据集，但反洗钱研究仍面临公开数据集不足的挑战，制约了深度学习模型在区块链反洗钱任务中的深入应用。区块链具有

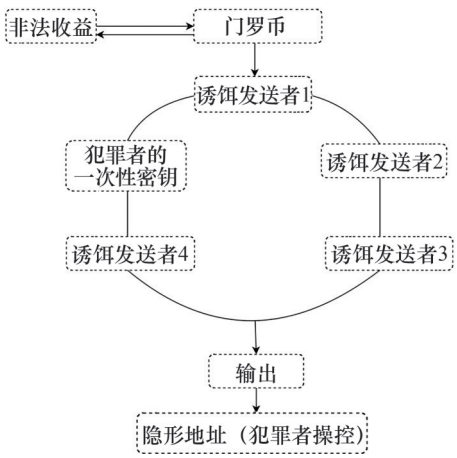

图 7　隐私币示意图

的匿名性、隐私保护技术能力，加大了追踪洗钱行为的难度，导致标记数据不足，难以有效训练并验证监督学习模型。数据匮乏迫使相关研究只能依赖假阳性率较高的无监督方法，如聚类、异常检测等。数据的敏感性也使金融机构不愿意公开信息，形成的“数据孤岛”不利于技术进步。需要通过数据共享推动学术界、工业界、监管机构的联合研究，同时确保数据收集和使用符合法律与隐私保护的要求。

5. 隐私币、混币、跨链影响反洗钱任务

隐私币、混币服务、跨链技术显著提高了资金流动的匿名性，增加了追踪与监管的复杂性。隐私币利用环签名、零知识证明等技术来隐藏交易双方的身份和金额，几乎不可能开展区块链上的追踪。混币服务以混合、分散多笔资金的形式切断资金来源与去向的关联性，尤其是去中心化的混币服务进一步加剧了相关问题。跨链交易允许洗钱者在不同的区块链之间频繁转移资金以规避监管，去中心化的跨链桥[28]、链间数据不兼容进一步增加了监控难度。这些服务和技术的结合应用，不仅削弱了传统反洗钱方法的有效性，还对管理部门的侦察、取证、监管等构成了严峻挑战。

6. 区块链的匿名性对监管构成挑战

区块链的匿名性既可保护用户身份，也为洗钱等违法活动提供了隐蔽性。区块链上的交易记录是公开的，但交易双方的身份难以识别，显著增加了对非法资金流动开展追踪和监管的难度。区块链采用的加密算法可以提升数据安全性，但也增加了监控并分析可疑交易的难度。

三、区块链系统中基于规则的反洗钱方法

在区块链系统中，基于规则的反洗钱方法仍然是核心策略之一[29,30]，尤其是在智能合约框架下具有实践价值[31]。所用规则主要涉及设置交易参数的阈值、地址与实体关联分析、跨链关联分析等方面。

（一）设置交易参数的阈值

设立阈值规则和异常交易模式，可实现对可疑行为的预警[32]。基于以太坊交易网络的应用进展，研究者提出了拓扑可疑性、时间可疑性、金额可疑性3类指标，用于识别洗钱者及资金流动路径，为更复杂场景下的规则设计提供了借鉴[33]。此类方法可以快捷部署，也能够以较低的资源消耗在可疑交易的早期即发出预警。当前，金融机构普遍采用“设置交易参数的阈值+风险评分”的混合模式，在规则层快速过滤99%的正常交易，再采用其他方法对剩余1%的高风险交易进行深度分析，兼顾控制运营成本、提升整体检测效率。然而，混合模式应用时依赖洗钱行为的先验知识，导致规则制定具有滞后性，在部署后规则不具备自适应性，容易被新的洗钱方式规避。设置阈值规则的方法面临日益严峻的技术挑战，但仍是当前反洗钱体系的核心基础，在短期内难以替代。

（二）地址与实体关联分析

通过智能合约、钱包地址规则验证数字身份，再运用黑 / 白名单、启发式规则将数字身份与实际账户关联起来[34]。基于“未消费交易输出”模型的交易验证机制支持嵌入细粒度的规则，适用于比特币的地址聚类分析。设置启发式的规则分析，对1个实体的多个地址之间关联性进行评估。几乎所有的启发式地址聚类方法都属于多输入启发式聚类。例如，使用启发式聚类，根据共享权限的证据对比特币钱包进行分组[35]，形成区块链系统中的行为模式聚类算法[36]；结合区块链信息、链外信息的聚类方法，使用共同消费、一次性找零等启发式方法来处理地址重用问题[37]；采用启发式方法，对LocalBitcoins.com上进行的比特币托管交易进行去匿名化处理[38]；通过排除后来被重用的地址（非找零地址）来检测一次性找零地址的启发式聚类方法[39]、用于判断比特币地址之间关系的启发式聚类方法，可以更好地发现比特币用户之间的关系[40]；基于多种启发式条件的比特币地址聚类方法，用于分析比特币交易和地址之间的关联，能够更准确地聚类大量的地址，揭示比特币交易实体之间的潜在关系[41]；基于多条件识别一次性找零地址的聚类方法，针对链上比特币交易数据取得良好的结果[42]。此外，比较多输入启发式算法、影子启发式算法、消费者启发式算法、最优找零启发式算法的性能后发现，钱包软件无法很好地保护用户的隐私[43]。整体上，相关研究进展良好，可在一定程度上揭示可疑洗钱账户之间的关联，但仅适用于“未花费交易输出”协议的区块链系统；在区块链系统隐私保护技术不断发展的情况下，尤其是在Tornado Cash混币服务获得

应用后，相关方法的应用成效面临极大的挑战。

（三）跨链关联分析

在多链网络趋于普遍的情况下，分析跨链交易的时序特征和链间交互规则，可以阐明潜在的跨链洗钱路径[44]。在应用层面，Elliptic[45]、Chainalysis[46]、CipherTrace[47]等区块链分析工具，较多基于规则来设定交易的风险阈值和特定行为模式，能够实时标注高风险账户、可疑资金来源、异常交易行为；依据规则定义风险阈值、过滤特定金额或地址来源，与黑白名单筛选机制联合使用，为合规审计提供潜在的证据链和基础数据。在当前的跨链交易中，出于用户隐私的考虑而越来越多地对跨链交易数据、智能合约、资产状态、跨链桥日志文件等信息进行加密，也倾向于使用零知识证明等技术，而现有的跨链关联分析方法无法从加密数据中获得有用的信息。不可忽视的是，基于规则的方法存在局限性[48]：构建过程高度依赖人工经验、已知模式，对复杂、多变的洗钱策略反应迟缓；不法分子规避已知规则，可使预警功能失效并产生大量无法管理的数据；针对新型洗钱手段被动制定规则的流程冗长低效[49]。在前沿研究和实际应用中，基于规则的方法逐步与机器学习方法融合，确保规则对已知模式的快速识别，兼顾对未知威胁的自适应性，成为应对加密货币犯罪行为的新解决方案。例如，在Elliptic、Chainalysis、CipherTrace等区块链分析软件的规则过滤基础上，引入机器学习模型对更复杂的可疑行为进行精细化检测。

四、区块链系统中基于传统机器学习的反洗钱方法

区块链中的数据（如交易记录、用户行为、社交网络交互）规模和复杂度快速增长，机器学习技术在反洗钱方面应用不断拓展。相较依赖先验规则的传统反洗钱方法，机器学习通过演绎推理可实现更灵活的模式发现[50]，由此弥补预定义规则的刚性与滞后性[51]，在识别新型拓扑结构和隐藏模式时表现出更高的检测率、更低的假阳性[52]。有研究者认为，基于机器学习的方法可在极少量标注数据的条件下，获得较基于规则的方法更有效的洗钱行为甄别效果[53]。基于机器学习（含深度学习）的反洗钱方法可分为异常检测、分类[54]：前者依托无监督或半监督学习技术，从大规模未标注的数据中挖掘偏离正常模式的交易行为；后者采用监督学习模型，根据标注数据训练分类器以识别高风险交易。各类机器学习方法的特点、在反洗钱任务中的应用进展等如表1所示。

表1　基于传统机器学习的反洗钱方法

传统机器学习方法	优点	缺点	反洗钱任务中的应用	处理方法	数据集
SVM	对高维空间问题具有良好的泛化能力	对大规模数据训练慢，对参数和核函数的设计敏感	寻找最优决策界，区分正交易与可疑交易	基于交易数据流	Elliptic数据集
逻辑回归	解决二分类问题	对于大的特征空间易欠拟合，难处理多类特征／变量	利用估计概率模型中的决策边界，预测交易正常或可疑的概率	标签稀缺情况下基于交易数据流	Elliptic数据集
				基于交易数据流	Elliptic数据集
决策树	解决分类问题，尤其适合决策分析	对于大多特征空间易过拟合，处理不平衡数据的能力有限	构建特征选择问题，形成树状决策模型，递归划分数据，区分正常和可疑交易	标签稀缺情况下基于交易数据流	Elliptic数据集
				基于自适应堆叠极端梯度提升	Elliptic数据集 Ethereum Illicit Accounts数据集
				图基级联特征提取方法	爬取的以太坊区块链数据
				基于LightGBM的双采样集成算法	
				基于交易数据流	Elliptic数据集

续表

传统机器学习方法	优点	缺点	反洗钱任务中的应用	处理方法	数据集
随机森林	解决分类或回归问题，处理高维数据	模型的可解释性较差，对噪声敏感，内存消耗大	集成多个决策树形成森林，用投票 / 平均预测增强稳定性和准确性，区分正常和可疑交易	标签稀缺情况下基于交易数据流	Elliptic 数据集
				基于 Scikit-learn 库的随机森林分类器	爬取的以太坊区块链数据
k 均值聚类	识别异常模式、处理大规模数据	*k* 值难确定，对初值敏感，不适用高维和稀疏数据	迭代并优化聚类中心，将数据点划分为多簇，揭示交易模式结构	使用期望最大化算法进行聚类分析	爬取的以太坊区块链数据
				基于交易数据流	Elliptic 数据集
结合链下信息的传统机器学习方法的应用	融合不同数据来源的信息，增强对洗钱行为的检测能力和分析深度	依赖客户的链下信息，攻击者可通过伪造交易记录、使用虚假身份信息、更换互联网协议地址等方式绕过模型的检测	结合社交网络特征增强对洗钱行为的检测能力和分析深度	基于账户信息和交易数据流	软件工具生成、模拟银行客户的交易数据
				基于账户的活跃性、时间序列特征和空间特征	即时通信软件的数据集

（一）支持向量机

SVM 是一种具有统计评估功能的学习方法，用于解决分类和回归问题[55]，在应对高维特征空间和复杂模式识别时的性能优异，被视为反洗钱的有效解决方案之一。相较许多传统模型，SVM 具有稳定、可重复、局部最优的抵抗力等特点，是反洗钱任务中的基线应用方法。引入特征选择、核函数转换、集成预测策略，进一步提高了 SVM 的适应性与准确性[56~61]。改进的径向基函数在应对异构数据、识别可疑交易方面效果良好，但需要采用 K 折交叉验证，显著增加了计算成本[60]；采用的数据集包含 3.2×10^5 个实例，对于 SVM 应用而言已是规模较大的数据集。

SVM 在处理高维数据时表现良好，但训练复杂度为 $O(n^2)$~$O(n^3)$，其中 n 是样本数量。可见，对于大规模的区块链交易数据而言，SVM 的训练和推理过程会非常耗时。此外，SVM 对输入数据的微小变化较为敏感，攻击者可通过生成对抗样本（如微调交易金额、时间、地址）的方式来欺骗模型。

（二）逻辑回归

逻辑回归是统计学、机器学习方面的基础方法[62]，可视为一种单层神经网络，擅长处理输入数据由多个变量组成、数据集中存在许多异常值的任务，具有线性结构特征，对反洗钱决策的影响易于阐明[63]。

逻辑回归的训练复杂度较低，通常为 $O(n\cdot d)$，其中 d 是节点特征维度，但当数据量极大时（如区块链的全局交易记录）仍然面临计算瓶颈。在数据集严重不平衡时，逻辑回归的决策边界会向多数类倾斜。反洗钱任务的数据集一般都存在严重的不平衡问题，逻辑回归在反洗钱任务中表现不佳[64]。逻辑回归对输入数据的微小变化同样较为敏感，易被攻击者欺骗。然而，作为经典的基线算法之一，逻辑回归仍是反洗钱研究中开展初步评估的良好选择。

（三）决策树

决策树是基于逻辑判断的经典机器学习方法，常用于构建可解释的决策路径[65]，相关研究起源于 ID3 算法[66]、C4.5 算法[67]，性能及适应性也得到逐步提高。决策树结构简单、易解释、具有自动特征选择功能，在当前的反洗钱任务中仍被广泛应用；逐层划分数据的规则设计，直观揭示特征之间的因果关系，利于开展监管和模型可视化[68]。

决策树在反洗钱任务中具有优势：规则结构便于识别异常交易特征，对噪声数据具有鲁棒性，可

高效处理大规模、多类型的数据集。为了改进传统的决策树模型，引入XGBoost算法[69]显著提高了Elliptic数据集上的检测性能，显现出在区块链上反洗钱的应用潜力；优化了计算和内存管理，具有较强的可伸缩性，在实时数据流中表现出良好的适应性；建立增量学习、滑动窗口机制，减少了模型对数据漂移的敏感性。采用LightGBM算法[70]并结合双重采样集成策略，有效提升了钓鱼账户检测的准确性及效率，验证了基于决策树的梯度提升框架在复杂区块链环境中的适用性；在涉及约5.4×10^5个地址、近8×10^6条交易记录的以太坊数据集中进行实验，展现出良好的可伸缩性，说明可在大规模数据集上快速训练并有效处理类不平衡问题。

决策树的训练复杂度较低，通常为$O(n\cdot d)$，与逻辑回归类似，但在数据量极大时（如区块链的全局交易记录）仍可能面临计算瓶颈。决策树的结果具有较好的可解释性，但规则易被逆向工程，便于攻击者设计可规避检测的交易模式。

（四）随机森林

随机森林作为决策树的集成方法，构建多个随机决策树并进行多数投票，在大规模反洗钱任务中展现出良好的准确性与稳定性[71~74]；尽管可解释性略逊于单棵决策树[75,76]，但在多维特征处理、关键因素识别方面表现更优。例如，利用无监督学习的期望最大化算法、随机森林算法，对区块链上大规模钱包数据进行了异常检测[77]；尽管对离线数据的处理效果良好，但在实时交易监控中仍需提高模型的响应速度。

反洗钱任务通常需要处理包含大量特征的数据集，如交易金额、时间、地点、账户类型等。随机森林算法可高效地处理高维数据，并能有效识别对预测结果影响最大的特征。随机森林集成多个决策树，提供较单一模型更高的准确性和稳定性，有助于更准确地检测并识别可疑交易行为。

随机森林的训练复杂度为$O(m\cdot n\cdot d\cdot \log n)$，其中$m$是决策树的数量。对于区块链数据，随机森林的训练和推理成本较高。与决策树类似，随机森林虽有较高的可解释性，但规则易被逆向工程，使攻击者设计可规避检测的交易模式。

（五）k均值聚类

k均值聚类算法早在1957年即提出，起初用于信号处理中的向量量化，1982年正式发表[78]，在数据挖掘、模式识别方向得到广泛应用。k均值聚类是一种经典的无监督学习方法，将样本划分为k个簇，最大化簇内样本的相似性、最小化簇间样本的差异性。k均值聚类算法在反洗钱任务中展现出显著优势：高效处理大规模的数据集，揭示异常交易模式，对复杂交易网络进行初步分组和风险评估；算法结构简单、易于实施，具有较高的可解释性；得到的聚类结果可作为客户和交易的分层风险分析依据，支持金融、监管机构优化反洗钱策略。例如，利用k均值算法对etherscan.io网站收集的38 526个加密货币钱包进行聚类分析，将钱包划分为7个集群[77]；相关结果揭示了不同类别交易模式之间的特性差异，展示了k均值聚类算法在识别加密货币交易模式与异常行为方面的潜力。

k均值聚类的训练复杂度为$O(n\cdot k\cdot d\cdot t)$，其中$k$是聚类数量，$t$是迭代次数。在区块链场景中，交易数据的较大规模和动态变化可能导致聚类算法难以收敛或计算开销过大。k均值聚类方法依赖数据分布的相似性，攻击者可构造与正常交易相似的交易模式，将之混入正常聚类后即可规避检测。

（六）结合链下信息的传统机器学习方法

研究者正在积极探索多模态方法，期望为区块链系统中的洗钱行为识别提供更全面的分析视角。相关工作集中在多模态数据与多种传统机器学习方法相结合，融合不同数据来源的信息，增强对洗钱行为的检测能力和分析深度。例如，将客户档案的关联数据与社会网络特征相结合，运用社会网络分析、k均值聚类、基于规则的方法，揭示可疑客户之间的复杂关系[79]；但方法应用依赖客户的个人信息和交易历史，如果攻击者操控交易数据（如伪造交易记录、使用虚假身份信息）可能会绕过模型的检测。

在处理多模态数据时，部分社交网络自身带有虚拟或加密货币交易功能，导致金融交易沿着社交网络进行流通。面向某类即时通信软件收集的操作数据，应用基于传统机器学习的反洗钱方法[80]，提取账户的活跃性、时间序列特征（如马尔科夫链）、空间特征（如账户关联特征），结合SVM、随机森林等模型，有效识别出可疑账户和异常交易行为。然而，该方法依赖账户的历史数据和交易模式，攻击者通过频繁更换互联网协议地址、使用不同设备

进行操作等方式即可改变这些数据，会降低模型的检测能力。

多模态融合在一定程度上显著提高了对异常交易模式的检测精度。然而，不同的数据源可能具有不同的特征分布，多模态学习在整合不同来源的数据时可能导致信息丢失或产生冲突。区块链的匿名性进一步增加了多模态数据融合的难度，从多源数据中提取有价值信息变得更有挑战性。

在区块链上的反洗钱任务中，传统机器学习方法对于特定数据集和场景具有一定的成效，但存在泛化能力不足、假阳性率偏高、难以应对新型洗钱策略等问题。为此，可将经典算法用作基准方法来衡量新方案的有效性，如针对决策树、随机森林、SVM 等监督学习算法，就区块链交易所反洗钱系统中的应用性能进行评估[81]。

区块链是一个分布式账本，交易数据量庞大（如比特币、以太坊的链上数据为数百吉字节甚至更多）；区块链数据处于动态增长状态，新的交易也不断添加到链上。传统机器学习算法在处理此类数据时往往面临计算资源不足、训练时间过长等问题。区块链交易数据的特征提取及选择对模型性能至关重要，但实施过程需要大量的计算资源和领域知识，进一步限制了机器学习方法的可伸缩性。区块链具有去中心化架构，机器学习通常需要集中化数据处理模式，两者存在冲突而限制了算法的可扩展性。新型洗钱技术层出不穷，导致区块链上的交易模式存在变化，如果机器学习模型未能及时更新，其检测性能可能下降。为此，需要引入分布式计算、在线学习、高效的特征工程方法，以提升模型对大规模、动态环境的适应能力。这也驱动学术界、产业界逐步将研究重心转向深度学习，以获得更优的检测性能与自适应能力。

五、区块链系统中基于深度学习的反洗钱方法

在区块链反洗钱任务中，深度学习相较传统机器学习展现出更优的应用潜力：具有强大的自动特征提取能力，利于从原始数据中捕捉高层抽象特征；可处理非结构化、多模态的数据，更适应复杂交易场景；自带多层非线性结构，可揭示隐藏在巨量交易网络中的复杂模式。当前，研究者广泛采用 CNN、RNN、GNN、Transformer 等深度学习架构，在捕捉交易结构、时间关联、潜在关系方面取得显著进展（见表 2）。

表 2　基于深度学习的反洗钱方法

深度学习方法	优点	缺点	反洗钱任务中的应用	处理方法	所用数据集
CNN	自动学习并提取交易数据的层次特征，泛化能力强	序列特征提取能力有限，可能忽视全局上下文	学习数据的层次结构特征，提取交易图像和模式的关键信息，有效识别并区分正常与可疑交易行为	基于交易数据	Elliptic 数据集
RNN	具有出色的序列数据处理能力和记忆功能	在处理长序列时易出现梯度消失 / 爆炸，计算效率较低	捕捉时间序列动态特征和长期依赖，识别正常和异常的交易模式	基于交易数据和客户信息 基于交易数据、钱包地址数据和时间序列数据	Spar Nord Bank 数据集 Elliptic++数据集
GNN	可高效捕捉并分析金融交易图中的复杂关系和模式	高度依赖图的结构和质量，难以有效捕捉实时动态交易	学习图结构节点关系和模式，区分网络中的正常与可疑交易	基于交易网络 基于亲和性的边 基于节点特征的边 基于用户行为和交易模式	Elliptic 数据集 Elliptic 数据集 DBLP Citation Network 数据集 Al-E’mari 等提供的数据集
Transformer	可并行化处理，捕捉长距离依赖关系	模型参数庞大，对位置的敏感性不强	学习序列数据中的模式和关系，区分数据中的正常与可疑交易	基于交易数据和客户特征	Spar Nord Bank 的数据集

（一）卷积神经网络

在区块链反洗钱任务中，CNN广泛用于特征提取与分类，凭借高效处理高维数据、自动学习局部特征模式的能力而受到认可[82]。CNN能够快速从非结构化交易数据中提取层次化特征，具有良好的泛化能力，可提高洗钱行为识别的响应速度，支持实时监控复杂的交易动态，提升反洗钱工作的时效性。此外，CNN可扩展应用至图数据分析[83]，为深入理解并监控区块链交易网络提供了新路径。

利用CNN堆叠卷积层与激活层分析比特币交易数据，识别出占市场总量2%~3%的潜在影子交易[84]。相关应用依赖人工构建的72个聚合特征，在更大规模的图中特征计算效率明显降低，且模型性能受到噪声的干扰。进一步发展的CNN变体方案[85]，增强了面向图结构数据的适用性，拓展了CNN在复杂区块链关系分析中的应用范围。

CNN虽然在处理结构化数据（如图像）时表现优异，但区块链中的交易记录通常是时间序列或图结构数据，直接应用CNN需要复杂的特征工程和大量的计算资源。在处理区块链交易时，CNN侧重局部特征，容易忽略全局语境，可能导致对洗钱活动的偏差判断。因此，兼顾局部与全局特征的方法得到更多的关注，将提高对区块链复杂交易生态的整体识别能力及可靠性。

（二）循环神经网络

RNN源于统计力学与神经科学研究，1995年提出的长短期记忆（LSTM）网络[86]极大改善了RNN在长序列处理中的表现。在区块链反洗钱任务中，RNN对时间序列数据具有出色的建模能力，通过记忆关键的历史交易信息，有效识别交易行为中的动态模式与异常特征，减少对人工特征工程的依赖。集成RNN与图分析技术，可进一步提升对复杂洗钱策略的响应能力。

利用门控循环单元（GRU）和自注意力机制构建的RNN模型[87]，在成功降低假阳性的同时保持了较高的真阳性检出率，在区块链反洗钱任务中表现出良好的性能。使用LSTM检测欺诈行为（欺诈被视为与洗钱行为密切相关），评估并分析比特币交易数据[88]，表明RNN在捕捉时序关联和异常行为方面具有优势。然而，这些方法均采用了复杂的模型架构，也需对交易序列进行特征提取和转换，导致训练和推理时间较长，难以开展实际应用。

RNN及其变体（如LSTM、GRU）适合处理时间序列数据（如交易序列），但训练过程是顺序化的，复杂度较高（通常为$O(r \cdot s^2)$，其中r是序列长度，s是隐藏层维度）。对于长序列的区块链交易数据而言，RNN的训练和推理效率较低。未来需优化模型结构、引入新型注意力机制等，提高RNN在区块链反洗钱任务中的可扩展性与实用性。

（三）图神经网络

GNN专门用于处理以图形式表示的数据[89,90]，以图卷积网络（GCN）[85]、图注意力网络（GAT）[91]为代表。金融领域中用户之间的交易流构成了复杂的网络关系，GNN可充分利用图的拓扑结构和邻居信息，支持开展交易网络的特征表征与模式挖掘，为区块链反洗钱提供了新思路。

在区块链反洗钱任务中，GNN具有高效捕捉并分析复杂交易关系的优点，减少了对人工开展特征工程的依赖，能够深度挖掘多维数据的特征，为研究者理解交易行为提供全面的视角。在处理大规模、动态交易数据时，GNN表现出优异的可扩展性和适应性，相应模型决策过程也有可解释性，为监管与合规审查提供了必要的透明度。得益于数据隐私保护、跨领域应用的潜力，GNN成为复杂网络结构数据条件下实施反洗钱任务的理想选择，主要用于解决以下问题。① 应对数据不平衡问题。涉及比特币交易的反洗钱任务中应用了GCN，处理类别不平衡问题成为特别关注点[92]；为此引入Focal Loss损失函数，解决了比特币交易中合法与非法交易标签数量严重不平衡的问题，在提升非法交易检测的准确性、降低误报率方面取得突破性进展。② 不同GNN模型的比较与场景验证。采用Elliptic数据集，对比了GCN、GAT在比特币交易异常检测中的有效性，进而阐明了区块链交易中应用GNN方法进行反洗钱和打击非法融资的良好潜力，突出表现在提升检测精度、降低误报率方面[93]。③ 图数据预处理与图结构优化。新型图预处理技术增强了GNN识别比特币网络中非法交易的性能及鲁棒性[94]，基于Elliptic数据集的实验结果表明，预处理优化后的图数据显著提升了GNN模型的评估指标性能。④ 跨平台与可解释性扩展。GNN在以太坊网络欺诈检测中的应用结果表明，基于以

太坊区块链上的交易历史，GNN 可精确分类欺诈用户[95]；后续研究可与人工智能方法（如 GraphLIME）相结合，进一步洞察用户和交易行为的内在机制，通过定制化的架构来最大化计算过程的准确性及效率。⑤ 模型融合与解构改进。将传统的 GCN 与线性层相结合，再通过多层感知器进行深入处理，在 Elliptic 数据集上显著提升了模型的效率和准确性[64]，展示了 GCN 在处理复杂网络数据方面的良好潜力。

GNN 适合处理区块链上的图结构数据（如交易图），但训练复杂度较高，通常为 $O(m \cdot d^2)$，其中 m 是边数。对于大规模的区块链交易图，GNN 的训练和推理成本偏高。GNN 的性能依赖图结构的质量和准确性，而在区块链交易分析中精确构建图结构并非易事。GNN 对静态图结构的依赖性也限制了捕捉实时动态交易的能力，而这种动态性对于反洗钱任务至关重要。在跨链、混币、新的隐私保护协议用于区块链的背景下，深度学习能够学习到的有效交易特征呈降低趋势，限制了 GNN 在反洗钱任务中的应用成效。此外，对于 GNN，攻击者可通过修改交易图的边或节点特征（如伪造交易关系）的方式来规避检测。

（四）Transformer

CNN、RNN、GNN 虽在区块链反洗钱任务中各有优势，但受制于可疑交易标注数据稀缺、数据存在噪声、交易市场变化频繁等现实因素，面临着容易过拟合、增加维护成本等应用困难。这一困境促使研究者探索兼具高效特征提取与动态适应能力的新型架构，而基于自注意力机制的 Transformer 架构为解决传统模型的局限性提供了新的技术路径。Transformer 模型于 2017 年提出[96]，核心思想是摒弃循环结构、引入多头注意力机制，从而显著缩短了训练时间，相较 RNN 等传统架构更为高效。Transformer 能够有效捕捉交易数据中的长距离依赖关系，具有并行处理数据的能力并可显著加速计算过程，也能从多个维度解析复杂模式与关联，因而在识别洗钱行为模式与潜在关联性方面表现出色，面对海量、多样化的金融数据可保持较高的性能。例如，深度学习方法应用于银行中的反洗钱警报[87]，将预定义的规则替换为从交易序列中自动提取的潜在特征；RNN、Transformer 编码器层的结果比较显示，使用 Transformer 编码器层的模型在减少假阳性方面更为出色，在提高反洗钱检测的准确性及效率上具有良好的潜力。

Transformer 在处理长序列数据时具有优势，但自注意力机制的训练复杂度为 $O(n^2 \cdot d)$。对于大规模的区块链交易数据，Transformer 的计算开销较大。Transformer 是高复杂度的深度学习模型，决策过程难以直观解释，在合规和监管要求严苛的金融环境下推广应用面临挑战。

深度学习方法在区块链反洗钱任务中同样面临可伸缩性问题。区块链数据具有大规模、动态增长、异构的特性，而深度学习模型通常需要将大量数据加载到内存中进行训练，对计算资源、存储能力提出了极高要求。区块链数据的动态性也使深度学习模型需要频繁更新才能适应新的交易模式，进一步增加了模型维护的复杂性。分布式训练、联邦学习等技术可以部分缓解上述问题，但实现过程复杂、需要高效的通信机制，难以完全满足区块链去中心化环境下的应用需求。因此，深度学习方法在处理区块链数据时，仍需在算法优化、硬件支持方面开展攻关。

六、支持反洗钱研究的常用数据集

在反洗钱研究中，数据集是推动方法论演进、支持实证验证的基础，传统以规则驱动的反洗钱策略、基于机器学习的人工智能模型都需要相应的数据集资源来支持算法构建、训练与评估。过去的研究多依赖合成数据集对传统金融体系下的洗钱行为进行模拟与分析，随着区块链、去中心化金融的兴起，相关研究逐渐转向结合区块链特性的交易数据集，更好满足从规则设计到智能算法优化的多层次需求。

在传统金融体系下的反洗钱任务中，合成数据集[97~99]得到较多应用，提供了相对受控的环境，支持各种反洗钱策略和模型的安全测试及评估。合成数据集包含了大量的结构化特征，如交易金额、频率、交易双方关系等，对训练和优化传统反洗钱模型至关重要。然而，区块链上的交易数据集与传统金融交易数据存在显著差异，需要能够反映区块链上交易的真实情况，如交易的匿名性、去中心化性、与其他金融活动的交互性等，才能更准确地训

练并评估区块链系统中反洗钱模型，进而可靠识别并预防区块链上的洗钱行为。

（一）EthereumHeist数据集

EthereumHeist数据集是首个针对以太坊平台的洗钱行为数据集，提供了能力全面的分析工具，支持研究者深入理解区块链上洗钱活动的复杂机制[100]。EthereumHeist数据集包含了超过1.6×10^5个与洗钱行为相关的以太坊地址，构建了庞大且详尽的资源库；详细记录了交易的时间戳和金额，提供了关于服务提供商地址的分类标签；标注出洗钱地址在层级结构中的位置，为研究者提供了洞察洗钱活动复杂性和层级性的新视角。相关详细信息支持研究者精确分析和模拟区块链上的洗钱模式，对揭示洗钱过程中涉及的角色和实体至关重要，也为制定有效的反洗钱策略提供了直接支持。

（二）Elliptic数据集

Elliptic数据集是基于比特币区块链构建的图网络，利用公开可获取的信息并结合人工制作的特征[64]，成为规模较大、经过标记的比特币交易公开数据集之一。Elliptic数据集具有匿名化特点，呈现了比特币区块链中的交易网络，将相关交易活动分为合法、非法两类：前者包括标准的交易行为、钱包服务提供商、矿工活动、提供合法服务的交易，后者指涉及欺诈、恶意软件、勒索软件、庞氏骗局等的非法金融活动。

Elliptic数据集中的交易图网络包含了代表独立的比特币交易的203 769个节点、指示交易间支付流向的234 355条有向边。在所有的节点中，有2%被标记为非法交易，21%被标记为合法交易，77%被标记为未知交易。每个节点配置了166个特征，其中前94个特征描述局部交易信息（如交易时间、交易输入/输出的数量、交易费用、输出的比特币总量，以及输入/输出的平均比特币接收和支出量、交易计数等进一步的统计数据），后72个特征基于以中心节点为出发点的一跳交易信息，提供了前向、后向交易的聚合特征（如邻居交易的输入/输出数量和交易费用的最小值、最大值、标准差、相关系数等）。此外，每个节点关联于1个时间步，该时间步代表了交易确认的估计时间点。Elliptic数据集包含49个相关的时间步，每个时间步平均间隔两周，这种设计有助于分析交易行为随时间的演变过程。

（三）Elliptic++数据集

Elliptic++数据集是Elliptic数据集的扩展形式，为比特币网络中的欺诈检测、金融取证提供了多维度分析框架[88]。Elliptic++数据集整合的特征信息较为丰富，不仅可用于识别可疑交易，还能支持检测并识别非法的比特币地址；包含了超过8.22×10^5个比特币钱包地址，每个地址配置了56个详细的特征，共记录了1.27×10^8次时间交互。数据集中的交易以时间序列图的形式呈现，涵盖了49个不同的时间步骤，包括203 769笔交易、234 355条有向边，每笔交易都被标记为非法、合法、未知类别。此外，Elliptic++数据集利用了交易到交易图、地址到地址交互图、地址–交易图、用户实体图等类型的图数据，进一步增强分析能力，支持深入理解交易和地址之间的关系。

七、区块链系统中反洗钱技术研究展望

当前，Web 3.0驱动数字经济迅猛发展，在区块链系统上越来越多地部署去中心化金融应用。区块链的去中心化、匿名性、金融全球化等特性，为洗钱等违法活动带来了规避监管的“便利性”，给数字经济的健康发展造成了极大隐患。基于规则和机器学习的反洗钱方法，虽然取得了一定的应用效果，但在具体实施中仍面临网络稀疏、数据不平衡、模型可解释性差、难以识别隐蔽交易等技术挑战。鉴于反洗钱技术发展存在滞后效应，区块链系统中的洗钱犯罪行为、反洗钱技术存在长期的动态博弈关系。未来的反洗钱技术研究需着力在以下4个方面采取行动，以为我国数字经济安全发展提供坚实保障。

（一）面向不平衡数据、不确定性标注的反洗钱数据集构建

创建高质量的反洗钱数据集对于区块链上的反洗钱任务而言至关重要，但数据不平衡、标注具有不确定性是两大直接挑战。洗钱行为在数据集中通常属于少数类，模型会偏向于识别正常交易，这就限制了洗钱检测的有效性。可探索采用过采样、权重调整、数据增强等技术，稳妥处理数据不平衡问

题，从而增强模型对少数洗钱样本的识别能力。人工标注数据存在一定的局限性，难以充分保证标注数据的准确性和一致性，当许多交易仅是疑似洗钱行为时更是如此。可引入多标签标注机制来提高数据标注的质量，再与半监督学习、自监督学习方法相结合，利用大量未标注数据、少量标注数据共同进行模型训练，从而增强模型的泛化能力。应用上述方法将支持构建更高质量的数据集、开发更有效的反洗钱系统，进而提高洗钱检测的综合效能。

（二）可信反洗钱算法研究

可信机器学习指构建的机器学习系统在真实环境下应用时具有可靠性、安全性，同时符合伦理、法律和社会规范。在反洗钱任务中，模型的可信度依赖模型的透明性、稳定性、对潜在风险的控制能力，因而可解释性、公平性成为确保模型可信的关键因素。在金融领域中，基于深度学习的算法虽有出色的性能表现，但在分析客户交易时可解释性、公平性往往存在不足。可采用基于注意力权重的层次化解释框架，在Transformer架构中嵌入可解释性模块，从而支持金融机构、监管部门理解模型的决策过程。公平性对于反洗钱活动同样重要，需要确保模型不会因数据中的偏见而对特定群体做出不公平的判断；可在模型训练时引入公平性正则化项，以互信息最小化的方式约束模型决策与受保护属性（如性别、年龄、其他不相关特征）的统计独立性。研究可信反洗钱算法，构建具有良好可解释性和公平性的可信反洗钱模型，确保相应决策过程的可追溯，将增强反洗钱系统在金融行业中应用的合规性和透明性。

（三）针对隐蔽交易的反洗钱机制研究

近年来，用于非法活动的比特币份额有所下降，而隐私币（如门罗币）等新型加密货币热度不减，暗网市场中的交易量有所增加[101]，相关变化导致区块链上的洗钱行为更具有隐蔽性[102]。现有的反洗钱机制多源自传统的金融系统设计，难以有效应对去中心化、匿名性的区块链交易；严格的KYC以及针对区块链系统的去匿名化处理，虽然对预防并打击洗钱活动有所帮助，但这些措施也可能引发用户隐私泄露的担忧，也会抑制Web 3.0时代的金融创新和活力。因此，需要设计面向混币、跨链、隐私币等技术应用的洗钱交易追踪方法，更好挖掘不法分子的洗钱犯罪行为；甚至构建新的区块链交易机制，在保护隐私、维护经济活力、实施有效监管、预防并打击洗钱活动之间取得平衡。例如，基于零知识简洁非交互知识论证方法构建可验证合规断言，允许交易方证明资金流转符合反洗钱规则，而无需暴露完整交易图谱。

（四）兼顾隐私性和可监管性的新技术研发

区块链技术为用户提供了强大的隐私保护功能，但也便利不法分子进行洗钱活动，在隐私保护、监管需求之间形成了矛盾。直观的研究方向是在隐私性、监管之间达成平衡，在保护用户隐私的同时，赋予监管机构追踪可疑交易的能力。零知识证明、同态加密、多方安全计算等新技术的出现，为解决上述矛盾提供了机遇。① 基于零知识证明设计可验证合规断言智能合约，交易方生成合规证明（如证明交易金额未超过监管阈值、资金来源已通过KYC验证），监管机构通过链上验证合约来检查合规证明的有效性，无需获取交易的明文数据。② 同态加密允许在加密数据上进行计算而无需解密数据本身，金融机构可在不暴露客户敏感信息（如账户余额、交易内容等）的情况下进行加密计算。可构建同态加密驱动的协同分析系统，金融机构上传经Paillier加密的交易特征（如地址度数、时间序列模式），监管机构直接对密文执行聚合运算。③ 多方安全计算允许多个数据拥有者在不访问彼此私人数据的情况下进行协作计算，进而构建三方可验证的安全多方计算框架：交易所持有地址标签数据，银行掌握交易流水，监管机构维护黑名单库。通过Beaver三元组协议实现分布式模型推理，各方在本地计算梯度份额，最终聚合得到洗钱风险评分（不泄露原始数据）。这种方法能克服现有反洗钱系统中跨机构的信息共享受到隐私保护法规、行业规范的限制，适合跨机构的反洗钱调查；也使银行、监管机构等可以共享计算结果而无需暴露敏感数据，利于增强机构之间的信任度，提高反洗钱任务的效率和透明度。

利益冲突声明

本文作者在此声明彼此之间不存在任何利益冲突或财务冲突。

Received date: November 19, 2024; **Revised date:** February 20, 2025

Corresponding author: Zhang Xiaosong is a professor from the School of Computer Science and Engineering, University of Electronic Science

and Technology of China. His major research fields include computer systems and network security. E-mail: johnsonzxs@uestc.edu.cn

Funding project: National Natural Science Found Project (U2336204, 62472075); Chinese Academy of Engineering project "The Strategic Study on the Intelligent and Collaborative Construction of Financial Rule of Law" (2023-JB-09)

参考文献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. [2025-02-15]. https://courses.csail.mit.edu/6.857/2015/files/L07-nakamoto-bitcoin-a-peer-to-peer-electronic-cash-system.pdf.

[2] Ethereum white paper [EB/OL]. [2025-02-15]. https://ethereum.org/en/whitepaper/.

[3] DApps: What Web 3.0 looks like [EB/OL]. [2025-02-15]. https://gavwood.com/dappsweb3.html.

[4] Staff E. Blockchains: The great chain of being sure about things [J]. The Economist, 2016, 18(7): 1–5.

[5] Bonneau J, Miller A, Clark J, et al. SoK [R]. San Jose: Proceedings of the 2015 IEEE Symposium on Security and Privacy, 2015.

[6] CoinMarketCap. According to CMC H1 2024 [EB/OL]. (2024-07-15)[2024-12-11]. https://coinmarketcap.com/academy/article/according-to-cmc-2024-h1

[7] 慢雾科技. 上半年区块链安全与反洗钱报告 [EB/OL] (2024-07-01)[2024-12-11]. https://www.slowmist.com/report/first-half-of-the-2024-report(CN).pdf.
SLOWMIST. Blockchain security and anti-money laundering report for H1 2024 [EB/OL]. (2024-07-01)[2024-12-11]. https://www.slowmist.com/report/first-half-of-the-2024-report(CN).pdf.

[8] United Nations convention against illicit traffic in narcotic drugs and psychotropic substances, 1988 [EB/OL]. [2025-02-15]. https://www.unodc.org/pdf/convention_1988_en.pdf.

[9] International Monetary Fund. 2023 review of the fund's anti-money laundering and combating the financing of terrorism strategy [EB/OL]. (2023-12-05)[2025-02-15]. https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015.

[10] Jullum M, Løland A, Huseby R B, et al. Detecting money laundering transactions with machine learning [J]. Journal of Money Laundering Control, 2020, 23(1): 173–186.

[11] 慢雾科技. 2024区块链安全与反洗钱年度报告 [EB/OL]. [2025-02-15]. https://www.slowmist.com/report/2024-Blockchain-Security-and-AML-Annual-Report(CN).pdf.
SLOMIST. 2024 blockchain security and AML annual report [EB/OL]. [2025-02-15]. https://www.slowmist.com/report/2024-Blockchain-Security-and-AML-Annual-Report(CN).pdf.

[12] United States Congress. Bank secrecy act: An overview of key provisions and issues [R]. Washington DC: U.S. Department of the Treasury, Financial Crimes Enforcement Network, 1990.

[13] Financial instruments and exchange act (No. 25 of 1948) [EB/OL]. [2025-02-15]. https://www.fsa.go.jp/common/law/fie01.pdf.

[14] 中华人民共和国反洗钱法 [EB/OL]. [2025-02-12]. http://www.pbc.gov.cn/fxqzhongxin/3558093/3558113/5586756/index.html.
Anti-money laundering law of the People's Republic of China [EB/OL]. [2025-02-12]. http://www.pbc.gov.cn/fxqzhongxin/3558093/3558113/5586756/index.html.

[15] Chen Z Y, Van Khoa L D, Teoh E N, et al. Machine learning techniques for anti-money laundering (AML) solutions in suspicious transaction detection: A review [J]. Knowledge and Information Systems, 2018, 57(2): 245–285.

[16] Tiwari M, Gepp A, Kumar K. A review of money laundering literature: The state of research in key areas [J]. Pacific Accounting Review, 2020, 32(2): 271–303.

[17] Alsuwailem A A S, Saudagar A K J. Anti-money laundering systems: A systematic literature review [J]. Journal of Money Laundering Control, 2020, 23(4): 833–848.

[18] Chen J. What is money laundering [EB/OL]. (2024-06-24)[2025-02-15]. https://www.investopedia.com/terms/m/moneylaundering.asp.

[19] Albrecht C, Duffin K M, Hawkins S, et al. The use of cryptocurrencies in the money laundering process [J]. Journal of Money Laundering Control, 2019, 22(2): 210–216.

[20] Trozze A, Davies T, Kleinberg B. Of degens and defrauders: Using open-source investigative tools to investigate decentralized finance frauds and money laundering [J]. Forensic Science International: Digital Investigation, 2023, 46: 301575.

[21] Pertsev A, Semenov R, Storm R. Tornado cash privacy solution version 1.4 [EB/OL]. (2019-12-17)[2025-02-15]. https://berkeley-defi.github.io/assets/material/Tornado%20Cash%20Whitepaper.pdf.

[22] Giannoni C, Medda F. Unlocking transparency: Harnessing blockchain for anti-money laundering in alternative assets. The case of fine art and real estate [J]. SSRN Electronic Journal, 2023: 4662355.

[23] Monero. CryptoNote v 2.0 [EB/OL]. (2013-10-17)[2025-02-15]. https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf

[24] Bender A, Katz J, Morselli R. Ring signatures: Stronger definitions, and constructions without random oracles [J]. Journal of Cryptology, 2009, 22: 114–138

[25] Noether S, MacKenzie A, Research Lab T M. Ring confidential transactions [J]. Ledger, 2016, 1: 1–18.

[26] WeBank. WeBank leads in financial performance and application of AI and blockchain technologies [EB/OL]. (2021-08-04)[2025-02-15]. https://www.theasianbanker.com/updates-and-articles/webank-recorded-best-financial-growth-among-peer-banks-with-excellent-digital-service.

[27] Ant Financial. Ant financial—A global leading techfin company [EB/OL]. (2019-11-13)[2025-02-15]. https://data.alibabagroup.com/ecms-files/1532295521/e263ce74-7a13-44d7-8359-4399b9f7eb81.pdf.

[28] Celer Network. Celer network: Bring Internet scale to every blockchain [EB/OL]. (2018-6-15)[2025-02-15]. https://celer.network/doc/CelerNetwork-Whitepaper.pdf.

[29] Gonzálvez-Gallego N, Pérez-Cárceles M C. Does goodness of governance dissuade citizens from using cryptocurrencies? [J]. Economics & Sociology, 2021, 14(1): 11–27.

[30] Saiedi E, Broström A, Ruiz F. Global drivers of cryptocurrency infrastructure adoption [J]. Small Business Economics, 2021, 57(1): 353–406.

[31] Röscheisen M, Baldonado M, Chang K, et al. The Stanford info-

bus and its service layers: Augmenting the Internet with higher-level information management protocols [EB/OL]. (1997-08-08)[2025-02-15]. http://infolab. stanford. edu/pub/papers/augmenting. pdf#: ~: text=In% 20this% 20paper% 2C% 20we% 20survey% 20the% 20design% 20of, metadata% 20%28SMA% 29%2C% 20search%20%28STARTS%29%2C%20payment%20%28UPAI%29%2C%20and%20r.

[32] Khanuja H K, Adane D S. Forensic analysis for monitoring database transactions [R]. Delhi: Security in Computing and Communications, 2014.

[33] Lin D, Wu J J, Yu Y M, et al. DenseFlow: Spotting cryptocurrency money laundering in ethereum transaction graphs [R]. New York: The ACM Web Conference 2024, 2024.

[34] Grinberg R. Bitcoin: An innovative alternative digital currency [EB/OL]. (2011-11-11)[2025-02-15]. https://sites. cs. ucsb. edu/~rich/class/cs293b-cloud/papers/bitcoin.legal.pdf.

[35] Meiklejohn S, Pomarole M, Jordan G, et al. A fistful of Bitcoins: Characterizing payments among men with no names [J]. Communications of the ACM, 2016, 59(4): 86–93.

[36] Huang B T, Liu Z G, Chen J H, et al. Behavior pattern clustering in blockchain networks [J]. Multimedia Tools and Applications, 2017, 76(19): 20099–20110.

[37] Ermilov D, Panov M, Yanovich Y. Automatic Bitcoin address clustering [R]. Cancun: The 16th IEEE International Conference on Machine Learning and Applications, 2017.

[38] Sabry F, Labda W, Erbad A, et al. Anonymity and privacy in Bitcoin escrow trades [R]. London: The 18th ACM Workshop on Privacy in the Electronic Society, 2019.

[39] Zhang Y H, Wang J, Luo J. Heuristic-based address clustering in Bitcoin [J]. IEEE Access, 2020, 8: 210582–210591.

[40] Zheng B K, Zhu L H, Shen M, et al. Identifying the vulnerabilities of Bitcoin anonymous mechanism based on address clustering [J]. Science China Information Sciences, 2020, 63(3): 132101.

[41] He X, He K T, Lin S W, et al. Bitcoin address clustering method based on multiple heuristic conditions [J]. IET Blockchain, 2022, 2(2): 44–56.

[42] Liu F, Li Z H, Jia K, et al. Bitcoin address clustering based on change address improvement [J]. IEEE Transactions on Computational Social Systems, 2024, 11(6): 8094–8105.

[43] Nick J D. Data-driven de-anonymization in Bitcoin [EB/OL]. (2015-08-09)[2025-02-15]. https://nickler.ninja/papers/thesis.pdf.

[44] Zhang J S, Gao J B, Li Y, et al. Xscope: Hunting for cross-chain bridge attacks [R]. Rochester: The 37th IEEE/ACM International Conference on Automated Software Engineering, 2023.

[45] Fanusie Y, Robinson T. Bitcoin laundering: An analysis of illicit flows into digital currency services [EB/OL]. (2018-01-23)[2025-02-15]. https://cdn2. hubspot. net/hubfs/3883533/downloads/Bitcoin%20Laundering.pdf.

[46] Chainalysis. Transfer impact assessment white paper [EB/OL]. (2023-03-27)[2025-02-15]. https://www.chainalysis.com/wp-content/uploads/2023/03/transfer-impact-assessment-white-paper-march-27-2023.pdf.

[47] Jevans D, Hardjono T, Vink J, et al. Travel rule information sharing architecture for virtual asset service providers [EB/OL]. [2025-02-15]. https://trisa. io/travel-rule-information-sharing-architecture-for-virtual-asset-service-providers-trisa/.

[48] Ketenci U G, Kurt T, Onal S, et al. A time-frequency based suspicious activity detection for anti-money laundering [J]. IEEE Access, 2021, 9: 59957–59967.

[49] United Nations Office on Drugs and Crime. Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes [EB/OL]. (2011-08-31)[2025-02-15]. https://www.unodc.org/documents/data-and-analysis/Studies/Illicit-financial-flows_31Aug11.pdf.

[50] Canhoto A I. Leveraging machine learning in the global fight against money laundering and terrorism financing: An affordances perspective [J]. Journal of Business Research, 2021, 131: 441–452.

[51] Savage D, Wang Q M, Chou P, et al. Detection of money laundering groups using supervised learning in networks [EB/OL]. (2016-08-02)[2025-02-15]. https://arxiv.org/abs/1608.00708v1.

[52] Wang Y, Wang H, Gao C S J, et al. Intelligent money laundering monitoring and detecting system [R]. London: European, Mediterranean and Middle Eastern Conference on Information Systems, 2008.

[53] Lorenz J, Silva M I, Aparício D, et al. Machine learning methods to detect money laundering in the Bitcoin blockchain in the presence of label scarcity [R]. New York: The First ACM International Conference on AI in Finance, 2021.

[54] Turner A B, McCombie S, Uhlmann A J. Analysis techniques for illicit Bitcoin transactions [J]. Frontiers in Computer Science, 2020, 2: 600596.

[55] Cortes C, Vapnik V. Support-vector networks [J]. Machine Learning, 1995, 20(3): 273–297.

[56] Wu P C, Dietterich T G, Wu P C, et al. Improving SVM accuracy by training on auxiliary data sources [R]. Banff: The Twenty-First International Conference on Machine Learning, 2004.

[57] Gabrilovich E, Markovitch S. Text categorization with many redundant features: Using aggressive feature selection to make SVMs competitive with C4.5 [R]. Banff: The Twenty-first International Conference on Machine Learning, 2004.

[58] Segata N, Blanzieri E. Operators for transforming kernels into quasi-local kernels that improve SVM accuracy [J]. Journal of Intelligent Information Systems, 2011, 37(2): 155–186.

[59] Chen Z Y, Selere O O, Seng N L C. Equipment failure analysis for oil and gas industry with an ensemble predictive model [R]. Singapore: Proceedings of the 9th International Conference on Computational Science and Technology, 2023.

[60] Liu K Y, Yu T T. An improved support-vector network model for anti-money laundering [R]. Wuhan: 2011 Fifth International Conference on Management of e-Commerce and e-Government, 2011.

[61] Tang J, Yin J. Developing an intelligent data discriminating system of anti-money laundering based on SVM [R]. Guangzhou: 2005 International Conference on Machine Learning and Cybernetics, 2005.

[62] Cox D R. The regression analysis of binary sequences [J]. Journal of the Royal Statistical Society Series B: Statistical Methodology, 1958, 20(2): 215–232.

[63] Sperandei S. Understanding logistic regression analysis [J]. Biochemia Medica, 2014, 24(1): 12–18.

[64] Alarab I, Prakoonwit S, Nacer M I, et al. Comparative analysis using supervised learning methods for anti-money laundering in Bitcoin [R]. Beijing: The 2020 5th International Conference on Machine Learning Technologies, 2020.

[65] Edwards W, Von Winterfeldt D. Decision analysis and behavioral research [M]. Cambridge: Cambridge University Press, 1986.

[66] Quinlan J R. Induction of decision trees [J]. Machine Learning, 1986, 1(1): 81–106.

[67] Salzberg S L. C4.5: Programs for machine learning by J. Ross Quinlan. Morgan Kaufmann Publishers, Inc., 1993 [J]. Machine Learning, 1994, 16(3): 235–240.

[68] Zhang Y, Trubey P. Machine learning and sampling scheme: An empirical study of money laundering detection [J]. Computational Economics, 2019, 54(3): 1043–1063.

[69] Vassallo D, Vella V, Ellul J. Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies [J]. SN Computer Science, 2021, 2(3): 143.

[70] Chen W L, Guo X F, Chen Z G, et al. Phishing scam detection on ethereum: Towards financial security for blockchain ecosystem [R]. Yokohama: The Twenty-ninth International Joint Conference on Artificial Intelligence, 2020.

[71] Heath D, Kasif S, Salzberg S. k-DT: A multi-tree learning method [R] Harpers Ferry: The International Workshop on Multistrategy Learning, 1993.

[72] Ho T K. Random decision forests [R]. Montreal: The 3rd International Conference on Document Analysis and Recognition, 1995.

[73] Breiman L. Random forests [J]. Machine learning, 2001, 45: 5–32.

[74] Kotz S, Johnson N L. Breakthroughs in statistics: Methodology and distribution [M]. New York: Springer New York, 1992.

[75] Madeh P S, El-Diraby T E. Using machine learning to examine impact of type of performance indicator on flexible pavement deterioration modeling [J]. Journal of Infrastructure Systems, 2021, 27(2): 04021005.

[76] Hastie T, Tibshirani R, Friedman J. The elements of statistical learning: Data mining, inference, and prediction [M]. New York: Springer New York, 2009.

[77] Baek H, Oh J, Kim C Y, et al. A model for detecting cryptocurrency transactions with discernible purpose [R]. Zagreb: 2019 Eleventh International Conference on Ubiquitous and Future Networks (ICUFN), 2019.

[78] Steinhaus H. Sur la division des corps matériels en parties [J]. Bulletin of the Polish Academy of Sciences Technical Sciences, 1956, 1: 801.

[79] Shaikh A K, Al-Shamli M, Nazir A. Designing a relational model to identify relationships between suspicious customers in anti-money laundering (AML) using social network analysis (SNA) [J]. Journal of Big Data, 2021, 8(1): 20.

[80] Zhou Y D, Wang X M, Zhang J J, et al. Analyzing and detecting money-laundering accounts in online social networks [J]. IEEE Network, 2018, 32(3): 115–121.

[81] Pettersson R E, Angelis J. Combating money laundering with machine learning-applicability of supervised-learning algorithms at cryptocurrency exchanges [J]. Journal of Money Laundering Control, 2022, 25(4): 766–778.

[82] Schmidhuber J, Schmidhuber J. Multi-column deep neural networks for image classification [R]. Providence: The 2012 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2012.

[83] Defferrard M, Bresson X, Vandergheynst P, et al. Convolutional neural networks on graphs with fast localized spectral filtering [R]. Barcelona: The 30th International Conference on Neural Information Processing Systems, 2016.

[84] Kolesnikova K, Mezentseva O, Mukatayev T. Analysis of Bitcoin transactions to detect illegal transactions using convolutional neural networks [R]. Nur-Sultan: 2021 IEEE International Conference on Smart Information Systems and Technologies (SIST), 2021.

[85] Kipf T N, Welling M. Semi-supervised classification with graph convolutional networks [EB/OL]. (2016-09-09)[2025-02-15]. https://arxiv.org/abs/1609.02907.

[86] Hochreiter S, Schmidhuber J. Long short-term memory [J]. Neural Computation, 1997, 9(8): 1735–1780.

[87] Jensen R I T, Iosifidis A. Qualifying and raising anti-money laundering alarms with deep learning [J]. Expert Systems with Applications, 2023, 214: 119037.

[88] Elmougy Y, Liu L, Elmougy Y, et al. Demystifying fraudulent transactions and illicit nodes in the Bitcoin network for financial forensics [R]. Long Beach: The 29th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2023.

[89] Wu L F, Cui P, Pei J, et al. Graph neural networks: Foundation, frontiers and applications [R]. Washington DC: The 28th ACM SIGKDD Conference on Knowledge Discovery and Data Mining, 2022.

[90] Scarselli F, Gori M, Tsoi A C, et al. The graph neural network model [J]. IEEE Transactions on Neural Networks, 2009, 20(1): 61–80.

[91] Velickovic P, Cucurull G, Casanova A, et al. Graph attention networks [EB/OL]. (2017-10-30)[2025-02-15]. https://arxiv. org/abs/1710.10903.

[92] Humranan P, Supratid S. A study on GCN using focal loss on class-imbalanced Bitcoin transaction for anti-money laundering detection [R]. Krabi: 2023 International Electrical Engineering Congress (iEECON), 2023.

[93] Pocher N, Zichichi M, Merizzi F, et al. Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics [J]. Electronic Markets, 2023, 33(1): 37.

[94] Nicholls J, Kuppa A, Le-Khac N A, et al. FraudLens: Graph structural learning for Bitcoin illicit activity identification [R]. Austin: The 39th Annual Computer Security Applications Conference, 2023.

[95] Tan R N, Tan Q F, Zhang P, et al. Graph neural network for ethereum fraud detection [R]. Auckland: 2021 IEEE International Conference on Big Knowledge (ICBK), 2021.

[96] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need [R]. Long Beach: The 31st International Conference on Neural Information Processing Systems, 2017.

[97] Altman E, Blanuša J, von Niederhäusern L, et al. Realistic synthetic financial transactions for anti-money laundering models [R]. New Orleans: The 37th International Conference on Neural Information Processing Systems, 2023.

[98] Jensen R I T, Ferwerda J, Jørgensen K S, et al. A synthetic data set to benchmark anti-money laundering methods [J]. Scientific Data, 2023, 10(1): 661.

[99] Weber M, Chen J, Suzumura T, et al. Scalable graph learning for anti-money laundering: A first look [EB/OL]. (2018-11-30)[2025-02-15]. https://arxiv.org/abs/1812.00076.

[100] Wu J J, Lin D, Fu Q S, et al. Toward understanding asset flows in crypto money laundering through the lenses of ethereum heists [J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 1994–2009.

[101] Childs A. How cryptomarket communities navigate marketplace structures, risk perceptions and ideologies amid evolving cryptocurrency practices [J]. Criminology & Criminal Justice, 2023: 17488958231213012.

[102] Wu J J, Liu J L, Chen W L, et al. Detecting mixing services via mining Bitcoin transaction network with hybrid motifs [J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2022, 52(4): 2237–2249.