小 型 微 型 计 算 机 系 统
Journal of Chinese Computer Systems
DOI:10.20009/j.cnki.21-1106/TP.2025-0357
2026 年 4 月 第 4 期
Vol.47 No.4 2026

以太坊钓鱼诈骗检测研究综述

吴国栋,黄苗苗,谢东辰,李景霞

[1](安徽农业大学 信息与人工智能学院,合肥 230036)
[2](农业农村部农业传感器重点实验室,合肥 230036)
[3](智慧农业技术与装备安徽省重点实验室,合肥 230036)
E-mail:8978850@qq.com

摘 要: 以太坊是一个全球性的、开源的和去中心化的区块链平台,近年来以太坊上的钓鱼诈骗事件频发,不仅造成用户资产损失,还影响区块链的健康发展.有效检测出以太坊上的钓鱼诈骗,对保护用户资产安全以及维护区块链平台生态健康等方面具有重要意义.本文基于不同检测方法的数据表示视角,从非图结构、图结构以及非图结构与图结构相结合三方面对已有以太坊钓鱼诈骗检测研究进行深入探讨,分析了本领域现有研究取得的进展与不足.在此基础上,总结了以太坊钓鱼诈骗检测研究常用的数据集及主要评价指标;同时指出了现有以太坊钓鱼诈骗检测研究存在的数据不平衡、资源消耗高和检测实时性不足等问题;最后展望了本领域未来主要研究方向.

关 键 词: 以太坊;钓鱼诈骗;检测;非图;图;图神经网络
中图分类号: TP311 **文献标识码:** A **文 章 编 号:** 1000-1220(2026)04-0960-14

Review of Research on Ethereum Phishing Fraud Detection

WU Guodong, HUANG Miaomiao, XIE Dongchen, LI Jingxia
[1](College of Information and Artificial Intelligence, Anhui Agricultural University, Hefei 230036, China)
[2](Key Laboratory of Agricultural Sensors, Ministry of Agriculture and Rural Affairs, Hefei 230036, China)
[3](Anhui Provincial Key Laboratory of Smart Agriculture Technology and Equipment, Hefei 230036, China)

Abstract: Ethereum is a global, open-source and decentralized blockchain platform. In recent years, phishing scams on Ethereum have occurred frequently, not only causing losses of users' assets but also affecting the healthy development of the blockchain. Effectively detecting phishing scams on Ethereum is of great significance for protecting users' asset security and maintaining the healthy ecosystem of the blockchain platform. Based on the data representation perspective of different detection methods, this paper conducts an in-depth discussion on the existing research on phishing scam detection on Ethereum from three aspects: non-graph structure, graph structure, and the combination of non-graph and graph structures. It analyzes the progress and shortcomings of the current research in this field. On this basis, it summarizes the commonly used datasets and main evaluation indicators in the research of phishing scam detection on Ethereum; at the same time, it points out the problems existing in the current research, such as data imbalance, high resource consumption, and insufficient detection real-time performance; finally, it looks forward to the main research directions in this field in the future.

Keywords: ethereum; phishing scams; detection; non-graph; graph; graph neural network

0 引 言

2008 年,中本聪发表了一篇名为《比特币:一种点对点的电子现金系统》[1]论文,描述了比特币这一去中心化数字货币的概念.随着比特币的兴起,区块链作为其底层实现技术也逐渐受到广泛关注.区块链上的数据由网络上的众多节点共同维护,无需第三方介入,具有去中心化特性,增强了数据的可信度和安全性.当前区块链相关技术被广泛应用到金融、数字货币和保险等诸多领域.以太坊是一个基于区块链技术构建的平台,其上引入了智能合约功能,被称为区块链 2.0,进一步扩展了以太坊的应用范围.由于以太坊的飞速发展及其广泛的应用场景,其具有极大的价值和潜力.然而这也成为很多欺诈行为滋生的土壤,各类欺诈事件频发.全球最大的 NFT 交易所 OpenSea 曾遭到钓鱼攻击,黑客通过给用户发送钓鱼邮件诱导用户将自己的钱包授权,进而盗取用户资产.根据慢雾科技发布的《2024 上半年区块链安全与反洗钱报告》[2]显示,2024 年上半年共发生 223 件安全事件,造成 14.3 亿美元的损失,其中以太坊平台上损失最多,达到了 4 亿美元.

钓鱼诈骗是以太坊上最常见的诈骗行为之一,造成以太

收稿日期:2025-09-02 收修改稿日期:2025-10-20 基金项目:国家自然科学基金项目(32371993)资助;安徽高校自然科学研究重点项目(2024AH050443)资助;安徽省自然科学基金项目(2108085MF209)资助;安徽省科技重大专项项目(202103b06020013)资助. 作者简介:**吴国栋**,男,1972 年生,博士,副教授,CCF 会员,研究方向为人工智能、图神经网络及智慧农业等;**黄苗苗**,女,2002 年生,硕士研究生,研究方向为区块链技术、图神经网络等;**谢东辰**,男,2001 年生,硕士研究生,研究方向为推荐系统等;**李景霞**,女,1976 年生,博士,讲师,研究方向为智能推荐、服务计算等.

坊上巨大资产损失. 为促进以太坊平台的健康发展,检测以太坊上的钓鱼诈骗已成为一个亟待解决的重要课题. 针对以太坊钓鱼诈骗检测,目前已有相关工作进行研究,并取得一定进展. 边玲玉等人[3]从以太坊交易记录中得到手工特征和统计特征,并将二者融合成为新的特征,使用轻量级梯度提升机算法(Light Gradient Boosting Machine,LightGBM)有效检测以太坊上的恶意账户. Chen 等人[4]提出一种基于区块链交易的钓鱼账户检测方法,采用图级联方法从交易图中提取特征,并使用基于 LightGBM 的双采样集成算法模型来识别钓鱼账户. Kanezashi 等人[5]在实际的以太坊交易数据集使用不同类型图神经网络识别以太坊钓鱼账户,并评估不同模型的性能.

随着以太坊钓鱼诈骗检测技术的不断发展,已有文献对以太坊钓鱼诈骗研究工作进行综述. 2023 年,蔡召等人[6]总结了以太坊钓鱼诈骗检测的数据集及评价指标,并从基于交易信息、基于图嵌入和基于图神经网络 3 个方面总结了现有的以太坊钓鱼诈骗检测方法,但该文献由于发表较早,未能涵盖当前以太坊钓鱼诈骗检测的最新研究进展,例如自然语言模型以及非图方法与图方法的结合. 2024 年,李广等人[7]总结了区块链上的 8 种欺诈行为,并分析讨论了每一类欺诈行为相应的识别技术,但其从主要从链上和链下两个角度整理区块链钓鱼诈骗识别技术,未能对其进行深入分析. 同年,李梦等人[8]针对以太坊上的传销、诈骗和蜜罐合约 3 种非法交易行为,从通用检测和特殊检测两个方面对其进行总结,但同样未能涵盖以太坊钓鱼诈骗检测的最新研究进展. 2025 年,李嘉乐等人[9]从区块链层次角度出发,分析每一层出现的恶意交易及其检测技术,但其侧重于整体框架描述,对以太坊钓鱼诈骗检测这一具体领域的探讨不足.

综上所述,已有综述对以太坊钓鱼诈骗检测技术缺乏全面总结与深入分析. 因此,结合当前以太坊钓鱼诈骗检测技术的最新发展,本文基于不同检测方法的数据表示视角,将现有的以太坊钓鱼诈骗检测研究分为非图结构、图结构以及非图和图结构相结合 3 类. 同时,本文在不同数据表示视角下,根据检测方法对当前以太坊钓鱼诈骗检测进行进一步地细致分类与深入分析总结,具体如图 1 所示. 在此基础上,指出了当前以太坊钓鱼诈骗检测领域存在的主要问题和未来研究方向.

1　以太坊钓鱼诈骗及检测

1.1　以太坊钓鱼诈骗

钓鱼诈骗是一种常见的网络犯罪行为,钓鱼者通过虚假网站或发送钓鱼邮件等方式获取用户敏感信息,如用户的账户名和密码等. 在以太坊中,钓鱼诈骗通常通过伪装成可信实体获取正常用户的信任,引诱用户向钓鱼地址转账,直接诈骗以太坊用户的资产.

与传统钓鱼诈骗获取用户隐私信息或钱财不同,以太坊钓鱼诈骗更倾向于直接诈骗用户资产,且以太坊钓鱼诈骗的方式更加多样,没有固定的模式. 此外,由于以太坊的匿名性,难以获取以太坊钓鱼者的具体信息. 因此传统的钓鱼诈骗检测方法难以直接应用到以太坊钓鱼诈骗检测中.

1.2　以太坊钓鱼诈骗检测

以太坊钓鱼诈骗检测是指通过分析以太坊账户的交易数据来识别其中的钓鱼账户. 以太坊钓鱼诈骗检测可定义为:$M(d_i,y):D\rightarrow\{0,1\}$,表示通过相关检测模型 M 发现可能是钓鱼账户的以太坊账户 d_i. 其中,d_i 是包含不同交易记录信息的以太坊账户,$d_i\in D$. $D=\{d_1,d_2,\cdots,d_n\}$ 表示账户集合;$y\in\{0,1\}$ 表示账户的标签,其中 0 表示正常账户,1 表示钓鱼账户.

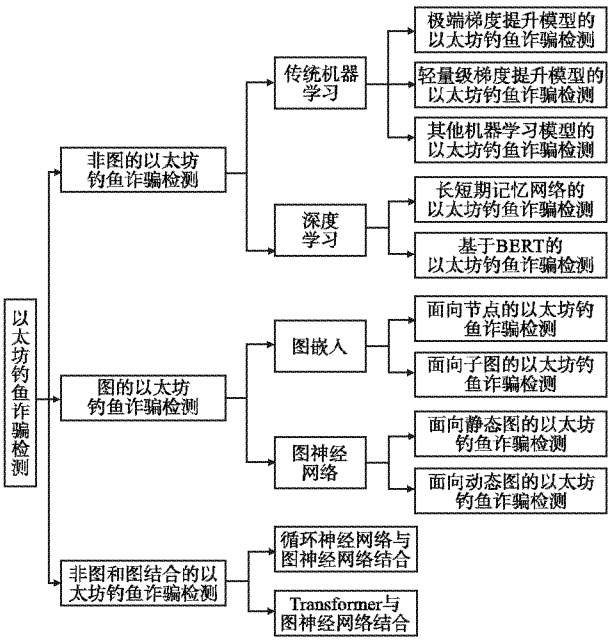

图 1　以太坊钓鱼诈骗检测主要研究

Fig. 1　Main research on Ethereum phishing fraud detection

目前已有一些检测以太坊钓鱼诈骗的工具. 文献[10]提出一种名为 TxPhishScope 的,能自动检测以太坊上 TxPhish 钓鱼诈骗的系统,该系统能够实时检测并报告可疑网站. He 等人[11]从以太坊钓鱼合约角度进行实证研究,并将研究成果应用到 Phalcon Compliance APP 中,帮助机构检测钓鱼地址.

以太坊钓鱼诈骗检测关键技术主要涉及传统机器学习、深度学习、图嵌入和图神经网络等方法. 传统机器学习方法主要通过对原始交易数据进行特征工程,进而采用机器学习算法识别钓鱼账户. 深度学习的以太坊钓鱼诈骗检测一般使用深度神经网络模型从原始数据中自动学习并提取包含丰富语义的特征. 图嵌入和图神经网络方法主要基于交易数据构建图结构数据,通过不同图算法识别钓鱼账户.

2　非图的以太坊钓鱼诈骗检测

2.1　传统机器学习的以太坊钓鱼诈骗检测

传统机器的以太坊钓鱼诈骗检测主要依赖于人工提取的特征,即从以太坊交易数据中手动提取特征,然后采用机器学习算法进行训练对以太坊账户进行分类. 根据使用的机器学习算法不同,将传统机器学习的以太坊钓鱼诈骗检测分为基于极端梯度提升模型的方法、基于轻量级梯度提升的方法和基于其他机器学习的方法.

2.1.1　极端梯度提升模型的以太坊钓鱼诈骗检测

极端梯度提升模型(eXtreme Gradient Boosting, XGBoost)是由陈天奇等人[12]在2016年提出的一种基于梯度提升决策树的机器学习算法,集成了多个决策树,提升了处理任务时的效率和准确率.

为高效精准地从众多以太坊数据中检测出异常账户,文献[13]从以太坊账户交易数据中为账户提取出42个特征,使用XGBoost分类器检测分类以太坊上的非法账户,实验结果表明XGBoost方法能够高效地检测出非法账户.虽然上述方法取得了较好的结果,但主要聚焦于XGBoost算法的精度上,未能与其他算法进行对比.因此,周健等人[14]在使用XGBoost算法检测以太坊欺诈账户时,采用与文献[13]相同的特征工程方法提取出41个特征,并进一步地与其他机器学习算法进行了详尽的对比,证明XGBoost算法的有效性.同时引入SHAP[15]来对XGBoost机器学习模型进行解释分析,得出识别以太坊欺诈账户的关键因素.但该方法未考虑交易的实时性问题以及特征工程和特征选择方面未做进一步探索.

2.1.2 轻量级梯度提升模型的以太坊钓鱼诈骗检测

LightGBM[16]也是一种基于梯度提升决策树的机器学习算法,与XGBoost相比,其训练速度更快,所占内存更小.Aziz等人在文献[17]中使用LGBM算法检测以太坊上的异常交易,并与其他机器学习算法如随机森林、多层感知机和XGBoost等进行比较,结果表明LGBM的检测性能最优.此外,由于以太坊数据集中钓鱼账户数量远少于正常账户数量,这种数据不平衡性影响模型正确识别交易的能力.因此该文献中使用合成少数类过采样技术(Synthetic Minority Oversampling Technique, SMOTE)[18]来缓解数据不平衡问题,SMOTE技术通过合成新的样本增加少数样本的数量,大大减少了过拟合的风险,提升模型检测性能.

尽管LightGBM在检测以太坊欺诈交易任务上表现良好,但其检测性能受限于数据集规模.LightGBM通常在数据集规模充足时表现出色,但当数据集规模较小时容易出现过拟合的情况,导致模型检测效果不佳.因此,针对这一问题,文献[19]提出一种面向小样本数据的LightGBM算法检测以太坊异常交易账户,通过特征选择减少特征数量和网格搜索方法优化模型的超参数等方法防止模型过拟合.与上述仅使用手工特征不同,边玲玉等人[3]在使用LightGBM识别恶意账户时,将手工特征与自动特征构造工具提取的统计特征融合作为输入特征.实验表明,融合特征有效提升了模型检测恶意账户的能力.

2.1.3 其他机器学习模型的以太坊钓鱼诈骗检测

除XGBoost和LightGBM算法外,还有如随机森林、决策树和支持向量机等技术应用于以太坊钓鱼诈骗检测研究.以太坊中存在外部账户和合约账户2种账户类型,以往工作大多仅关注以太坊外部钓鱼账户的检测,忽略了对合约账户合法性的检测.因此,Kumar等人[20]根据以太坊中外部账户和合约账户的不同特性分别提取相应特征,使用随机森林、决策树、XGBoost和k近邻4种机器学习模型进行恶意地址检测.结果显示,外部账户和合约账户的检测精度最终分别达到了96.54%和96.82%.

当前以太坊钓鱼诈骗检测研究中存在数据不平衡、特征工程过于复杂和低准确率等问题,因此Kabla等人[21]提出一种基于机器学习的以太坊钓鱼诈骗检测(Ethereum Phishing Scam Detection, Eth-PSD)方法来检测以太坊中的钓鱼地址.Eth-PSD方法通过随机过采样方法增加少数类样本来平衡数据集,创新地使用基于投票的特征工程技术选择重要的特征,并选择决策树和k近邻等算法检测钓鱼诈骗.同样为了缓解数据不平衡问题,文献[22]采用6种机器学习模型检测以太坊上的非法活动时,使用SMOTE技术合成少数类样本,相比于随机复制少数类样本,降低了模型过拟合风险.

尽管上述研究证明了多种机器学习技术检测以太坊钓鱼诈骗的有效性,但其未能比较不同重采样技术对检测结果的影响.文献[23]采用逻辑回归、支持向量机和随机森林等机器学习算法检测以太坊恶意实体,并采用多种重采样技术平衡数据集.该方法考虑了不同机器学习的检测效果,分析对比了不同重采样技术对检测结果的影响并解决了数据不平衡问题,但未考虑到模型可解释性问题.

当前基于传统机器学习的以太坊钓鱼诈骗检测研究在数据不平衡问题上已取得了一定进展,但很少有研究能够同时考虑到数据不平衡和模型可解释性问题.虽然机器学习能够给出检测结果,但缺少对决策过程的透明性和可解释性.模型的可解释性可以分析特征对模型预测结果的影响性,帮助人们更好地理解模型做出的决策,增强模型的透明性、公开性和公平性.因此,文献[24]采用了多种过采样技术平衡数据集并评估其有效性,引入SHAP值解释模型决策过程中的特征重要性和贡献度,并采用多种机器学习如决策树和随机森林等检测区块链上的欺诈行为.实验结果表明过采样技术对提升模型检测性能的有效性,未来可考虑使用其他方法来解释模型以及关注检测的实时性问题.

上述传统机器学习的以太坊钓鱼诈骗检测方法对交易数据进行手工特征提取,这些特征很好地描述了交易细节信息.传统机器学习的检测方法还具有训练时间短,计算成本低等优点,在以太坊钓鱼诈骗检测任务上取得了不错的效果.但传统机器学习方法很大程度上依赖于手动提取的特征,检测效果取决于选择的特征,但选择有效合适的特征需要丰富的专家经验,仍然是一个挑战.除此之外,以太坊账户之间的关系日益复杂,手工提取难以从交易记录中挖掘出深层次有效特征.且不法分子实施犯罪的手段越发隐蔽,手工特征很难捕捉其中的细微差别和隐藏模式.因此,传统机器学习方法在检测钓鱼账户任务上具有一定的局限性.

2.2 深度学习的以太坊钓鱼诈骗检测

随着技术的不断发展,深度学习逐渐被应用到以太坊钓鱼诈骗检测领域.深度学习的以太坊钓鱼诈骗检测主要通过使用深度学习算法从以太坊交易数据中自动提取特征,无需手动提取和选择特征.根据使用神经网络不同,将当前深度学习的以太坊钓鱼诈骗检测研究分为基于长短期记忆网络的方法和基于BERT模型的方法.在上述两类方法研究中,通常将以太坊账户的交易记录数据构建为序列数据,再使用深度学习进行特征提取和账户检测.

2.2.1 长短期记忆网络的以太坊钓鱼诈骗检测

作为循环神经网络(Recurrent Neural Network, RNN)一种变体,长短期记忆网络(Long Short-Term Memory, LSTM)引入门控单元来控制信息的遗忘和更新,不仅缓解了RNN处

理长序列数据时容易发生梯度消失的问题,还能够捕捉序列数据中的依赖关系. 因此,已有研究将 LSTM 应用以太坊钓鱼诈骗检测领域,旨在利用 LSTM 的时序建模能力学习账户的潜在交易模式. Wen 等人[25]提出了一种基于混合深度神经网络的钓鱼诈骗账户检测模型(LSTM-FCN and BP Neural Network-Based Phishing Scam Accounts Detection Model,LBPS),将手动特征工程和基于交易记录分析的方法相结合. LBPS 采用滑动窗口对账户交易记录进行采样来获得交易序列,利用 LSTM-FCN[26]从交易序列中提取有效的时序特征,并使用 BP 神经网络处理手工提取的账户特征以挖掘账户特征之间的隐含关系. 最终将由 LSTM-FCN 和 BP 神经网络学习得来的特征进行拼接,并输入到全连接层中对账户进行分类. LBPS 模型通过学习和拼接多种特征,实现了对特征的全面挖掘,提升了模型检测性能. 未来可考虑构建更大的数据集,将 LBPS 方法应用于其他区块链平台.

LSTM 模型虽然能够很好地处理序列数据,但只能处理单向的信息,这种单向性限制了模型对上下文信息的全面捕捉. 因此,引入双向长短期记忆网络(Bidirectional Long Short-Term Memory Networks,BiLSTM)应对 LSTM 存在的上述局限性. 通常单层 BiLSTM 模型由两个 LSTM 模型组成,分别处理正向和反向的序列信息. 这种双向结构使得 BiLSTM 模型能够同时考虑序列的前后文信息,增强模型的表达能力. 因此,Tang 等人[27]将 BiLSTM 模型应用到以太坊钓鱼账户检测研究中,提出一种基于注意力机制的 BiLSTM 方法——BiLSTM4DPS 检测以太坊钓鱼账户,模型整体架构如图 2 所示.

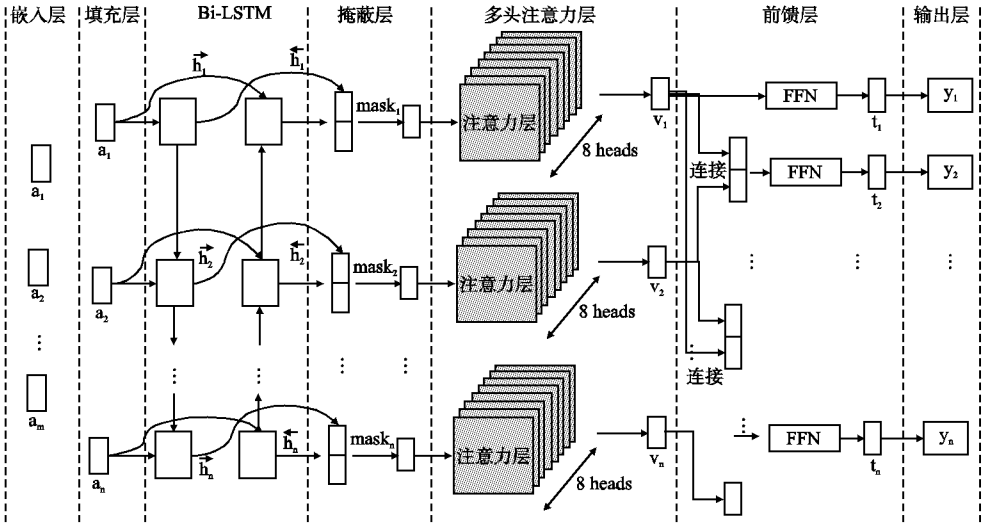

图 2　BiLSTM4DPS 架构图

Fig. 2　BiLSTM4DPS architecture diagram

该工作将以太坊账户的交易记录构建成时间序列交由 BiLSTM4DPS 处理,并引入多头注意力机制动态地为经过掩蔽技术处理的数据分配注意力权重,从而增强模型对关键信息的关注. BiLSTM4DPS 模型在不同的数据集上进行了大量的实验,结果表明该模型处理交易时间序列能够获取更丰富更有效的信息,在以太坊钓鱼账户检测任务上具有较好的性能. 但模型复杂度较高,且可能会出现过拟合等问题. 此外,由于数据中存在噪声,BiLSTM4DPS 模型的泛化能力和检测能力可能会被影响.

2.2.2　基于 BERT 的以太坊钓鱼诈骗检测

BERT 是一种基于 Transformer 架构的预训练语言模型,能够捕捉语句中的双向上下文关系,获取丰富的语义表示. BERT 的训练主要分为预训练和微调两阶段. 在预训练阶段,模型在大量无标注数据上进行训练,训练任务包括掩码语言建模和下一句预测. BERT 通过预训练任务学习了通用的语言表示并得到模型的权重. 在微调阶段,将预训练后的 BERT 模型根据下游任务进行微调,以适应下游任务的需求. BERT 模型自提出以来,在多个自然语言处理任务上表现出色. 因此,已有研究将 BERT 模型应用于以太坊钓鱼诈骗检测任务上,以期通过其强大的序列建模能力和双向捕捉能力有效识别以太坊钓鱼账户.

针对以太坊交易数据的高重复性、分布偏斜和异质性特点,文献[28]提出 BERT4ETH 模型,用于以太坊上钓鱼账户检测和去匿名化任务. BERT4ETH 模型中采用了去重和高掩码率等策略以缓解上述以太坊交易特点对模型识别能力造成的负面影响. BERT4ETH 整体架构如图 3 所示,将以太坊账户的交易序列作为模型的输入,特征嵌入层为每个交易生成相应的特征表示,随后 Transformer 编码层对特征表示进行编码,捕捉交易序列中的上下文信息. 实验结果表明 BERT4ETH 在钓鱼账户检测和去匿名化任务上相比其他模型有显著的性能提升,其采用的 3 种策略有效缓解了以太坊交易特性给模型训练带来的挑战.

虽然文献[28]表明 BERT 模型凭借其强大的时序建模能力在以太坊钓鱼账户检测任务上取得了出卓越的成效,但 BERT 在处理海量数据的任务时存在占用内存高和计算成本过高等问题,限制了其在大规模实际应用场景中的可行性. 因此,文献[29]提出了 ZIPZAP 框架,旨在为在大规模交易数据上训练语言模型时达到参数减少和计算效率提升的目的. ZIPZAP 主要通过频率感知压缩和非对称训练两种策略来达成这一目标. 频率感知压缩技术根据地址出现的频率动态调

整嵌入向量的维度,减少了参数数量;非对称训练在预训练阶段采用交易丢弃和跨层参数共享两种方法来加速预训练过程,在微调阶段恢复标准训练方法. 实验表明 ZIPZAP 为训练语言模型在处理大规模数据集的有效性以及高效率性. 相较于文献[28],此方法有效减少了模型参数并优化了预训练和微调的效果,模型的计算效率得到了有效提升.

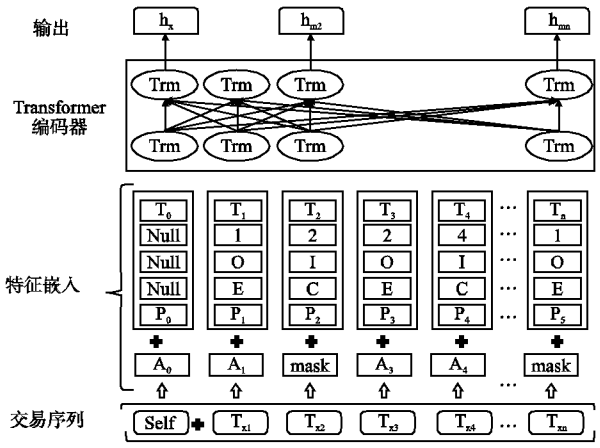

图 3 BERT4ETH 架构图

Fig. 3 BERT4ETH architecture diagram

相比于传统机器学习的以太坊钓鱼诈骗检测,深度学习的以太坊钓鱼诈骗检测能够自动从交易数据中提取特征,挖掘交易记录中的特征和复杂关联,无需手动提取. 但深度学习方法也存在一定的局限性,深度学习模型往往涉及到众多参数,面临着训练时间长、占用内存高和计算成本过高等问题. 除此之外,当前深度学习的以太坊钓鱼诈骗检测大多将以太坊账户交易记录构建成序列数据作为模型的输入,虽然能够捕捉交易时序和潜在交易模式,但序列数据无法有效表示以太坊账户之间的拓扑关系.

表 1 从不同方法及其优缺点方面总结了基于非图的以太坊钓鱼诈骗检测研究主要工作.

表 1 非图的以太坊钓鱼检测主要研究

Table 1 Main research on non-graph Ethereum phishing detection

类别	子类	主要文献	采用方法	优点	缺点
传统机器学习的以太坊钓鱼诈骗检测	XGBoost 的检测	[13]、[14]	手动提取特征,使用 XGBoost 识别钓鱼账户	鲁棒性较好,灵活性较高	参数调优较为复杂
	LightGBM 的检测	[17]、[19]、[3]	对交易数据进行手动特征提取,使用 LightGBM 进行检测	训练速度快,占用内存资源少	对数据噪声敏感
	其他机器学习模型的检测	[20]、[21]、[22]、[23]、[24]	手动提取特征,使用不同机器学习检测,并比较分析	缓解数据不平衡问题和模型可解释性问题	泛化能力和鲁棒性存在不足、缺乏对数据实时性的考虑
深度学习的以太坊钓鱼诈骗检测	长短期记忆网络的检测	[25]、[27]	将交易记录构建成时间序列,使用 LSTM 处理序列数据提取特征进行检测	挖掘交易时序信息,丰富节点表示	数据集规模有限,模型复杂,存在过拟合风险
	基于 BERT 的检测	[28]、[29]	采用基于 BERT 的模型处理以太坊交易数据构建的序列数据进行账户检测	具有强大的建模能力,捕捉上下文关系	计算成本和占用内存过高

3 图的以太坊钓鱼诈骗检测

3.1 图嵌入的以太坊钓鱼诈骗检测

图嵌入的以太坊钓鱼诈骗检测对交易数据的处理主要根据账户的交易记录构建图数据,以账户为节点,账户之间的交易为边. 图嵌入是一种将图中的节点或边转换为低维向量表示的技术,旨在将数据降维,并保留图的拓扑结构和语义信息. 根据分类任务不同,将当前图嵌入的以太坊钓鱼诈骗检测研究分为面向节点的以太坊钓鱼诈骗检测和面向子图的以太坊钓鱼诈骗检测.

3.1.1 面向节点的以太坊钓鱼诈骗检测

面向节点主要是将以太坊钓鱼诈骗检测视为节点分类任务,在由以太坊交易数据构成的交易图上进行随机游走生成节点序列,对序列进行处理得到节点的嵌入向量. DeepWalk[30]和 node2vec[31]是两类经典的基于随机游走的图嵌入方法. DeepWalk 通过在图上进行无偏深度优先随机游走得到节点序列,再采用 skip-gram 方式训练词嵌入,最终得到嵌入向量. node2vec 与 DeepWalk 思想相似,但区别在于 node2vec 是有偏随机游走,通过控制参数来调整随机游走策略,能够更灵活地探索图的结构,生成丰富的嵌入表示.

文献[32]提出一种基于 node2vec 的以太坊钓鱼账户检测方法. 将获取到的以太坊交易记录构建成图,使用 node2vec 方法在图上进行有偏随机游走从而获得节点表示,随后采用单类支持向量机对节点进行分类. 此方法是较早将图嵌入方法应用于以太坊钓鱼账户检测任务上的尝试,与非图方法相比考虑了节点的邻近信息并保留了局部结构特征,提升了检测性能. 但其忽略了交易信息和账户属性等重要信息,在检测效果上仍有提升空间. 因此,文献[33]提出 trans2vec 图嵌入算法检测以太坊钓鱼账户,创新性地将交易记录中交易金额和交易时间戳两种交易属性融入随机游走过程,实现有偏随机游走 trans2vec 中使用搜索偏差 a 平衡交易金额和时间对随机游走的影响,随机游走中从节点 u 到其邻居节点 x 的转移概率公式如式(1)所示:

$$\pi_{ux}(a) = PA_{ux}^{a} \cdot PT_{ux}^{1-a} \tag{1}$$

PA^{α}_{ux}表示在基于金额的有偏采样下,从源节点 u 到其邻居节点 x 的概率;$PT^{1,-\alpha}_{ux}$表示在基于时间的有偏采样下,从源节点 u 到其邻居节点 x 的概率,a 的取值是 0 ~ 1 之间的闭区间. 实验结果表明时间和金额等交易信息对识别钓鱼账户具有重要影响. trans2vec 方法虽然考虑了基于交易金额和交易时间戳进行有偏随机游走,但其无法捕捉到交易网络中的交易的时序性和重复性特征. 因此,Xiao 等人[34]提出了一种基于信息素的图嵌入算法(Pheromone-based Graph Embedding Algorithm,PGEA)检测以太坊钓鱼诈骗. PGEA 将信息素机制应用到随机游走中,将交易金额和交易频率概念化为信息素,使得游走更倾向于选择高信息素浓度的节点,有效捕捉了以太坊交易网络中交易的时序性和重复性特征. 此外,为避免随机游走陷入局部最优,设计了禁忌列表机制,降低重新访问已访问过节点的概率,增强算法捕捉图结构的能力. 实验表明,PGEA 检测以太坊钓鱼诈骗的能力优于其他基线模型.

上述以太坊钓鱼诈骗检测方法将交易信息融入到随机游走中提取了更全面的特征,但其都只考虑了源节点与其一阶邻居节点之间的关系,忽略了其他源节点对上述邻居节点的影响,使得检测模型难以捕获账户的拓扑结构,模型的检测能力可能会受到影响. 因此,Luo 等人[35]针对以太坊钓鱼账户检测问题构建交易图时,计算源节点与其一阶邻居节点之间的平均交易金额和平均交易时间作为节点与其邻居节点之间边的附加权重,用于后续有偏采样. 随后对 trans2vec 和 T-EDGE[36]中的有偏采样进行改进,提出一种名为 bias2vec 的随机游走算法,其引入不同参数平衡交易金额和时间之间的影响以及原始交易与附加权重之间的影响. 实验表明引入的附加权重相比于原始交易信息在识别以太坊钓鱼账户方面更为关键,证明了该改进方法的有效性.

以太坊中存在不同类型的账户和交易形式. 典型的账户类型如外部账户、智能合约账户和交易所等;交易类型包括调用合约、创建合约以及转账等. 然而以往钓鱼诈骗检测方法大多基于同构图展开,即在建模图时仅包含单一类型的节点和单一类型的边. 同构图忽略了现实以太坊账户和交易的异构性与复杂性,难以有效捕捉不同类型以太坊账户之间的交互模式和交易行为的多样性. 因此,为更精准有效地检测以太坊钓鱼诈骗账户,已有研究采用异构图建模方法. 通过引入多种节点类型和边类型,更细致地刻画交易网络的复杂关系,揭示钓鱼诈骗账户的隐蔽行为模式,提高模型检测能力. Hu 等人[37]在检测以太坊钓鱼账户时,将以太坊交易记录构建为异构图,并考虑以太坊交易网络的异构性和动态性,提出了一种新颖的基于 jump-stay 算法的时间加权有偏游走,将时序依赖性和节点异构性纳入随机游走中. 这种方法不仅考虑了交易网络的异构性和动态性,还结合了交易金额和时间对检测钓鱼账户的影响,捕捉到了更加全面的特征信息. 同样地,为考虑交易时序性和交易网络的异构性,Lin 等人[38]在进行以太坊钓鱼账户检测任务时提出一种名为 Phish2vec 的嵌入算法. 与文献[37]在游走过程中同时考虑异构性和动态性不同,Phish2vec 算法分别考虑图的异构性和时序性. 具体来说,Phish2vec 利用基于时间的序列生成器(Temporal-based Sequences Generator,TSG)和基于异构性的序列生成器(Heterogeneous-based Sequences Generator,HSG)分别生成序列,将二者生成的序列进行拼接生成具有更丰富信息的序列,并将其输入到 word2vec 中得到节点嵌入. 除此之外,为解决交易数量过多和传统采样方法导致标签泄露的问题,研究中采用基于统计采样(Statistics-Based Sampling,SBS)对交易网络进行采样. Phish2vec 算法充分考虑了交易网络的异构性和动态性,将交易的时序性和异构性结合起来,丰富了节点表示.

3.1.2　面向子图的以太坊钓鱼诈骗检测

面向子图的以太坊钓鱼诈骗检测主要以目标节点为中心节点构建一系列子图,目标节点的标签作为整个图的标签,分类模型以子图为输入进行检测任务. 文献[39]从图分类角度,提出采用改进的 Graph2Vec[40]方法检测以太坊上的钓鱼账户. 考虑到之前的研究工作未关注到边的方向信息,因此其将原始图中的边转换为新图的节点,共享公共端点的节点连接成边,最终形成线图作为 Graph2Vec 的输入,达到将边的方向信息融入到 Graph2Vec 模型中的目的. 实验表明,该方法在检测以太坊钓鱼诈骗账户任务上的有效性,但上述工作并没有过多地探讨交易金额和交易方向对以太坊钓鱼账户检测结果的影响.

针对以往工作对交易信息利用不充分的问题,Xia 等人[41]设计了一种重标记策略,即根据交易金额、基于交易次数和交易方向对网络中的节点标签进行重新标记,采用 Graph2Vec 算法从图分类角度检测钓鱼地址. 与文献[39]中的方法相比,这项工作融入了更多交易信息如交易金额等,提高了模型检测的准确率,但未考虑到交易网络中边的多重性. 文献[42]重点关注交易图的构建,受 SGN(Subgraph Network)[43]启发,提出了一种基于交易子图网络(Transaction SubGraph Network,TSGN)的以太坊钓鱼账户识别框架,旨在挖掘更多特征信息. 其将子图网络通过不同的映射机制扩展成相应的 TSGN,同时引入交易的时间和方向形成 Temple-TSGN 和 Directed-TSGN,随后采用 6 种以太坊钓鱼检测模型来检测钓鱼账户. 实验结果表明,TSGN 深入挖掘了以太坊交易的潜在信息,提高了模型检测准确率.

图嵌入的以太坊钓鱼诈骗检测方法将交易记录构建为图结构数据进行检测,通过在图上随机游走等方法有效捕捉账户之间的拓扑关联和结构特征. 但图嵌入方法具有一定局限性,已有的图嵌入方法大多基于随机游走,随机游走过程中产生大量序列,导致计算量庞大. 除此之外,现实世界中以太坊中的交易网络是动态的,涉及到账户以及交易的增加、修改和删除等,但已有的图嵌入以太坊钓鱼诈骗检测方法大多将交易记录建模为静态图,忽略了细粒度的时间信息,无法捕捉图的动态变化,降低模型检测性能.

3.2　图神经网络的以太坊钓鱼诈骗检测

图神经网络的以太坊钓鱼诈骗检测在图构建方面与图嵌入的以太坊钓鱼诈骗检测相似,同样将以太坊账户作为节点,账户之间的交易记录作为边. 但对图数据的处理方法不同. 图神经网络是一种常用于处理图结构数据的深度学习模型,通过聚合邻域特征来不断更新节点表示,进而捕捉图的拓扑结构. 根据图结构是否随时间发生变化,将图神经网络的以太坊钓鱼诈骗检测分为面向静态图的以太坊钓鱼诈骗检测和面向动态图的钓鱼诈骗检测.

3.2.1　面向静态图的以太坊钓鱼诈骗检测

1)基于静态同构图的检测

Patel 等人[44]使用单类图神经网络(One Class Graph Neural Network, OCGNN)[45]检测区块链的异常交易,OCGNN 旨在通过在正常交易数据中学习出一个超球面,将位于超球面之外的数据定义为异常数据,进而识别出区块链的异常交易.但 OCGCN 方法在面对大规模数据集时检测性能仍有一定的局限性.

由于以太坊上的交易量巨大,将整张交易图直接作为模型输入进行训练需要高昂的计算成本,因此,已有一些研究从原始交易网络中提取交易子图作为模型输入进行钓鱼账户识别,以此来减少资源占用. Shen 等人[46]提出一种端到端的基于图神经网络的区块链身份推断模型(Identity Inference on Blockchain using Graph Neural Network, I^2BGNN),模型整体架构如图 4 所示. I^2BGNN 以子图为输入,经过两层图卷积层提取节点嵌入,再使用最大池化层聚合节点获取全图的表示,全连接层对得到的表示向量进行标签预测,判断节点类型. I^2BGNN 模型在交易图上提取交易子图,通过减少图的规模来减少计算成本和资源消耗,并兼顾了可扩展性和端到端学习能力.

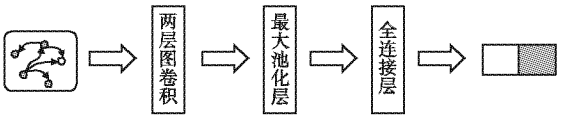

图 4 I2BGNN 架构图

Fig. 4 I2BGNN architecture diagram

Zhang 等人[47]提出一种多通道图分类模型(multi-channel graph classification model, MCGC),将钓鱼诈骗检测转换为图分类任务,利用多个图池化层提取图的不同层次结构信息. 与 I^2BGNN 中简单使用最大池化不同,MCGC 在每个池化层中引入可训练节点重要性权重将节点表示加权聚合为图表示,进一步考虑了不同通道与图表示之间的关系,捕捉了重要的结构信息,提取了丰富的交易模式特征. Li 等人[48]提出一种端到端的钓鱼检测图神经网络(Phishing Detection Graph Neural Network, PDGNN),将原本庞大的交易数据轻量化并从中提取交易子图. PDGNN 方法主要基于 Chebyshev-GCN 来聚合节点信息,随后采用池化层提取目标账户特征,最后输入到全连接层识别钓鱼诈骗账户.

虽然上述研究将钓鱼账户检测作为图分类任务,通过提取账户的交易子图来减小计算复杂度获取账户表示,但这些方法忽略了更细粒度的交易信息,在检测精度上仍有上升空间. 因此,Huang 等人[49]提出了一种于图神经网络增强自我网络的钓鱼检测框架 PEAE-GNN. PEAE-GNN 为账户构建自我网络,设计了一种基于结构特征、交易特征和交互强度的特征特征策略来增强节点特征,将增强后的自我网络输入到图神经网络中进行特征提取和钓鱼诈骗账户检测. PEAE-GNN 在减少资源占用的基础上,对节点特征进行增强,有效缓解了已有的钓鱼诈骗检测方法存在的复杂度高和可扩展性差等问题,提升了模型检测性能.

2)基于静态异构图的检测

静态同构图只能表示出单一类型的节点和边,无法表达出以太坊账户和交易的复杂多样信息,因此基于此类图的以太坊钓鱼诈骗检测方法具有一定的局限性. 相比之下,建模异构图能够捕获交易网络的异构信息有利于得到丰富特征表示. 文献[5]首次将异构图神经网络应用到以太坊钓鱼诈骗账户检测任务中,考虑了以太坊交易网络中的不同节点和边类型. 实验表明,相较于同构图神经网络,异构图神经网络能够捕捉到更丰富的信息,具有更好的检测性能. 此外,文献还指出将额外的交易信息融合到模型中可能会有更好的检测性能. 因此,Huang 等人[50]提出异构交易子图图卷积网络(Heterogeneous Transaction Subnet Graph Convolution Network, HTSGCN)来检测以太坊上的钓鱼账户,其核心思想是充分考虑边上的信息,利用边的异构性和方向来为目标节点选择重要邻居. 具体来说,HTSGCN 为每个账户构建 k 阶异构交易子图,根据边的类型和方向来为边分配不同的权重,进而聚合邻居信息,节点的邻居节点的整体表示如式(2)所示:

$$\boldsymbol{H}_{N_i}^{l}=\sum_{r\in R,d\in D}\sum_{j\in N_i^{r,d}}\frac{1}{C_i^{r,d}}\boldsymbol{W}_{r,d}^{l}\cdot\boldsymbol{h}_j^{(l-1)} \tag{2}$$

其中 $\boldsymbol{W}_{r,d}^{l}$是第 l 层的权重矩阵,$\boldsymbol{h}_j^{(l-1)}$ 表示上一层的嵌入向量,$N_i^{r,d}$ 是结点 i 的类型为 r,方向为 d 的邻居节点的集合,$C_i^{r,d}$ 表示归一化系数. HTSGCN 充分考虑了交易网络的异构性,将边的类型和方向纳入模型中,得到具有丰富语义的节点特征.但此方法也缺乏对动态图的研究,未来可考虑将更多交易属性纳入研究范围.

随着以太坊上犯罪活动越发猖獗,以太坊钓鱼账户的犯罪行为模式也越来越隐蔽. 以太坊钓鱼账户往往通过少量多次地与正常账户交互让本身行为模式与正常账户的交易模式相似,使得欺诈行为更加隐蔽,达到伪装成正常账户的目的,一般的检测方法难以全面有效地识别出欺诈行为. 因此,文献[51]从度量账户之间的相似性角度出发,提出一种基于邻居关系过滤的异构图神经网络 NF-HGNNs 来识别以太坊上的异常账户. NF-HGNNs 使用基于交易信息的随机游走来计算节点之间的相似度,并利用强化学习来选择不同关系下的最优邻居,通过这种方式过滤掉伪装成正常账户的钓鱼账户,获得有效的节点特征表示. NF-HGNNs 充分考虑了图的异构性和节点的伪装性,但模型在避免过拟合方面仍有不足,处理大规模数据时间复杂度较高.

3.2.2 面向动态图的以太坊钓鱼诈骗检测

区块链上的账户和交易随着时间在不断变化,上述静态图忽略了时间因素对网络拓扑造成的影响. 因此静态图分析方法无法捕捉到交易图的动态结构特征,难以得到有效的节点表示,不能准确识别出钓鱼账户. 针对静态图分析方法的局限性,可将交易记录构建成动态图进行特征提取. 根据时间粒度的不同,将现有面向动态图的以太坊钓鱼诈骗检测研究工作从离散时间动态图和连续时间动态图两方面进行深入探讨.

1)基于离散时间动态图的检测

离散时间动态图按照一定的时间步将动态图划分成一系列的静态图快照. Patel 等人[52]提出一种动态图卷积神经网络框架(Evolving Anomaly detection Graph Convolutional Network, EvAnGCN)来检测区块链交易网络中的异常节点. EvAnGCN 主要在文献[44]的基础上进一步扩展,将区块链

上的交易构建成离散时间动态图,在每一个时间步长内利用 EvanGCN 捕捉时间信息和结构信息. EvanGCN 模型较好地处理了高度动态的网络,有效捕捉时间信息,但模型缺乏可解释性分析以及忽略了数据不平衡问题.

在以太坊交易图中,交易流向也是识别以太坊异常交易的关键因素,但以往工作通常将边视为无向或忽略方向语义,未能充分考虑动态图中边的方向信息. 针对这个问题,文献[53]提出一种基于图神经网络的以太坊网络多层时序交易异常检测模型(Multi-layer Temporal Transaction Anomaly Detection,MT^2AD). MT^2AD 模型将边的交易信息和方向信息融入到节点属性上,根据边上的时间戳构建一系列快照,并采用带有注意力机制的图卷积编码器获取嵌入向量. MT^2AD 捕捉了以往传统工作忽视的交易时序信息和边的方向信息,提升了模型的检测性能.

2)基于连续时间动态图的检测

连续时间动态图利用一组事件来表示动态图. 与离散时间动态图不同,连续时间动态图中发生节点属性改变或边增加等事件都有一个具体的时间戳,更细粒度地刻画了网络拓扑结构随时间发生的改变.

当交易网络发生快速变化时,离散图快照可能无法精准捕捉到某一时刻的网络状态,造成重要信息的丢失. 针对这个问题,已有研究将时间编码函数引入以太坊钓鱼诈骗账户检测中,利用时间编码函数捕捉动态变化,从而在连续时间域上学习图的演化过程,避免关键结构信息的遗漏. 文献[54]提出一种基于时序图注意力网络的以太坊钓鱼诈骗检测方法——PDTGA. PDTGA 利用 TGAT[55] 学习时间感知的节点嵌入,将时间编码函数与节点特征、边特征和图拓扑结构的交互来对时间信号进行建模. 与以往简单将不同模块中得到的不同类型特征连接起来,PDTGA 通过时间编码函数将节点特征、边特征和图结构之间的相互作用对时间信号进行建模,更符合图中节点和边随时间推移而增加或删除的特性,得到了更丰富的节点表示. 但 PDTGA 方法未考虑到数据不平衡问题和图的异构性,未来可在这两方面作进一步探索. Zhang 等人[56]同样将时间编码技术引入以太坊钓鱼账户检测中,提出一种名为 Grabphisher 的以太坊钓鱼诈骗检测方法. 与 PDTGA 不同的是,Grabphisher 利用基于 TGAT 和 TGN[57] 的方法来捕捉交易过程中节点的动态时序特征信息,并进一步使用 EvolveGCN 学习动态图随时间变化的拓扑结构信息,增强了模型检测钓鱼账户的能力.

图神经网络的以太坊钓鱼诈骗检测方法通过消息传递机制,聚合邻域节点信息更新节点特征. 通过不断迭代捕获节点之间的关系和图结构信息. 已有图神经网络的以太坊钓鱼诈骗检测方法在不同类型图如静态图、动态图、同构图和异构图上均取得一定进展. 但同样地,使用图神经网络检测以太坊钓鱼诈骗也具有一定局限性. 当涉及到大规模数据即大规模图时,图神经网络训练时间长、计算资源消耗过高. 除此之外,图神经网络还存在可解释性不足的问题,难以解释模型的决策过程,模型透明度较低. 最后,以太坊交易数据存在类别不平衡问题,钓鱼账户数量远远少于正常账户数量,图神经网络在这样的数据上检测效果不佳.

表 2 从不同方法及其优缺点等方面总结了基于图的以太坊钓鱼诈骗检测研究相关工作.

表 2　图的以太坊钓鱼诈骗检测主要研究

Table 2　Main research on graph Ethereum phishing fraud detection

类别	子类	主要文献	采用方法	优点	缺点
图嵌入方法的以太坊钓鱼诈骗检测	面向节点	[32]、[33]、[34]、[35]、[37]、[38]	在交易图上进行游走生成节点序列来学习节点表示	保留局部结构特征	面对大规模网络时,计算复杂度高
	面向子图	[39]、[41]、[42]	构建子图,使用 Graph2Vec 获得图的表示向量	有效减小图规模,降低计算成本,捕获潜在的交易模式	子图采样可能会丢失重要信息
图神经网络方法的以太坊钓鱼诈骗检测	面向静态图	[44]、[46]、[47]、[48]、[49]、[5]、[50]、[51]	将交易记录构建为静态图,使用图神经网络检测以太坊钓鱼账户	迭代更新节点表示,捕捉图的拓扑结构特征	未考虑图的动态性、可解释性较差
	面向动态图	[52]、[53]、[54]、[56]	将交易记录构建为动态图,使用图神经网络检测以太坊钓鱼账户	捕获了交易图的结构特征和动态时序特征信息、增强节点表示	缺乏可解释性,计算成本较高,模型鲁棒性有待探索

4　非图与图结合的以太坊钓鱼诈骗检测

非图方法和图方法在以太坊钓鱼诈骗检测任务上各有优势,但同时也存在着各自的不足之处. 非图方法中深度学习的钓鱼诈骗检测虽然能够有效捕捉账户交易的动态序列模式,但其无法捕捉账户之间的复杂交互结构;图方法虽然能够捕捉节点之间的交互关系,但其可能无法捕捉节点的长距离依赖. 因此,为进一步提高检测准确性,可将非图方法与图方法结合以充分利用两者的优势,弥补单一方法的局限性. 根据使用方法不同,将混合方法分为循环神经网络与图神经网络结合方法和 Transformer 与图神经网络结合方法.

4.1　循环神经网络与图神经网络结合的以太坊钓鱼诈骗检测

循环神经网络能够处理序列数据,有效提取交易的时序特征,图神经网络在处理图结构数据方面具有显著优势,能够捕捉图的结构信息,将两者结合可以协同利用时序信息和图

的结构信息,获得更丰富全面的节点表示.

鉴于以往研究工作存在缺乏考虑时间序列交易信息和节点表示不足等问题,Li 等人[58]针对以太坊钓鱼诈骗检测问题,提出一种时间交易聚合图网络(Temporal Transaction Aggregation Graph Network,TTAGN). TTAGN 将交易记录建模为序列数据输入到 LSTM 中捕捉节点对之间的交互模式并生成边表示,且使用注意力机制为节点的边表示分配不同权重进行聚合获得交易特征. 随后在结构增强模块中将节点统计特征和交易特征结合作为 GCN 的输入来获取节点的结构特征,最后将统计特征,交易特征和结构特征结合作为节点的最终表示. TTAGN 整体架构如图 5 所示.

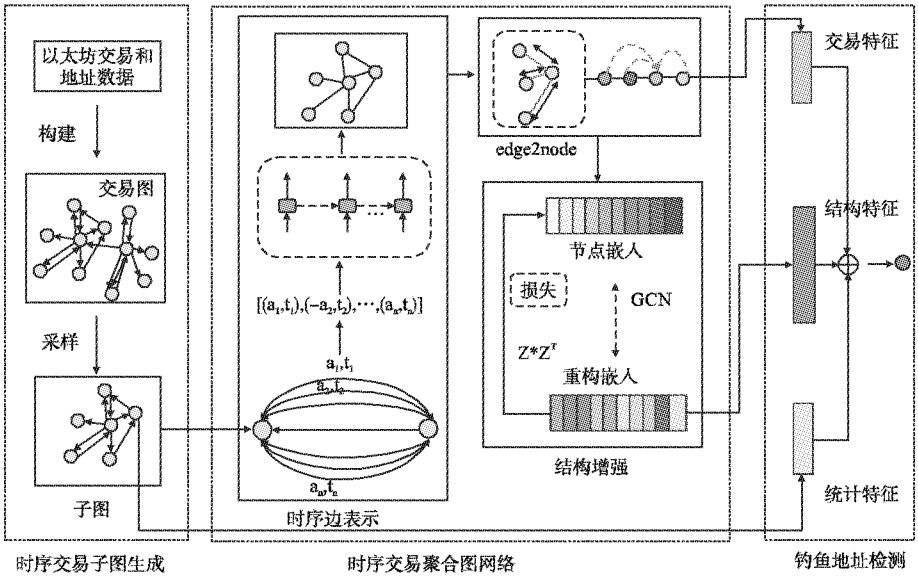

图 5 TTAGN 架构图

Fig. 5 TTAGN architecture diagram

TTAGN 方法充分捕获了节点之间交易记录的时序特征,将统计特征、时序特征和拓扑特征融入到节点表示中,丰富了节点表示,提高模型检测的准确性. 但模型需考虑交易中存在的噪声以及模型的鲁棒性等问题. 与 TTAGN 不同,文献[59]提出的 DIAM 模型将节点的入边和出边分别按照时间戳排序形成序列,并利用 GRU 学习序列表示,有效捕捉不同方向的交易模式. 同时,文献还指出传统的图神经网络模型存在同质性假设,即认为一条边连接的两个节点具有相似的特征. 但这在以太坊钓鱼账户检测中并不适用,因为在以太坊交易图中存在钓鱼账户大多和正常账户进行交互的情况,导致正常用户与欺诈节点之间缺乏特征差异性,模型检测效果不佳. 因此 DIAM 设计了一个多图差异模块捕捉传递正常账户与非法账户之间的特征差异性. DIAM 学习了保留正常节点与非法节点之间的特征差异性的节点特征,提高模型检测准确率.

在 TTAGN 基础上,后续研究做出各种改进和优化. 文献[60]提出一种多特征融合方法(Three-Stream Feature Fusion,TSFF)增强节点表示来检测以太坊钓鱼诈骗. 首先针对 TTAGN 中使用随机游走采样子图忽略交易多重性,可能导致信息丢失的问题,TSFF 提出一种基于节点状态的随机游走采样子图来减少子图中非钓鱼节点的引入. 其次,TSFF 在使用 LSTM 提取交易时序特征时加入对比学习来学习更丰富的特征表示;随后,将残差块与 GCN 结合,捕捉更全面的表示. TSFF 与 TTAGN 相比,捕捉了更精细的结构和时序特征. 但 TSFF 方法也存在一定的不足,比如模型仍然难以处理数据类别不平衡问题和大规模图. 因此,针对上述研究方法存在的数据不平衡问题,Tang 等人[61]提出 EthGAN 框架进行以太坊账户分类,其采用与 TTAGN 相似的方法将多种特征结合形成节点特征. 但与 TTAGN 不同的是,EthGAN 在获得丰富节点特征表示后,利用 GAN[62]合成少数类样本以增加少数类样本数量. EthGAN 不仅增强了节点特征表示,还有效缓解数据类不平衡问题,提升模型检测精度.

当前的循环神经网络与图神经网络结合的以太坊钓鱼诈骗检测方法,主要是分别使用循环神经网络处理交易序列数据提取交易时序特征,图卷积神经网络提取结构特征,再将统计特征、交易时序特征和结构特征结合作为最终的节点表示. 这种结合方式增强了节点特征表示,提升模型检测能力. 但这种结合检测方法仅仅是简单地将不同网络生成的特征拼接在一起,忽略了不同特征对模型检测精度的影响. 除此之外,不同网络方法之间缺乏交互,不能实现不同方法之间的潜在协同作用.

4.2 Transformer 与图神经网络结合的以太坊钓鱼诈骗检测

相较于循环神经网络,Transformer 能够捕捉序列中的长距离依赖关系. 除此之外,不同于循环神经网络中信息的串行处理,Transformer 并行处理数据,提高了计算效率. 将 Transformer 与图神经网络结合进行以太坊钓鱼诈骗检测,可协同捕捉图的拓扑结构特征和账户的全局时序行为.

在当前以太坊交易网络中,钓鱼账户和非钓鱼账户在某些时刻表现出相似的行为模式,且用户行为具有稀疏性,导致难以有效识别出钓鱼账户. 因此,文献[63]将图神经网络和

Transformer 结合,提出一种以太坊钓鱼诈骗检测方法 CATALOG. CATALOG 从用户的局部行为和全局行为之间的相关性和用户交易行为在连续时间窗口内的演变相关性两个关键因素出发,捕捉用户行为的局部和全局时间依赖性,以此增强模型区分钓鱼账户和非钓鱼账户的能力. 具体来说,CATALOG 为账户构建基于滑动时间窗口的加权有向自我网络,使用图神经网络获得账户初始嵌入,并引入双交叉注意力机制和 Transformer 等方法捕捉用户行为的细微变化和长期依赖关系. CATALOG 缓解了以太坊钓鱼诈骗检测任务中存在的数据稀疏性、数据泄露和数据规模过大等问题,并增强了节点表示,有效识别出与正常账户具有相似行为模式的钓鱼账户. 但 CATALOG 仍然存在一些不足,如训练时间复杂度高、计算成本高和模型可解释性低,且需要大量的标记数据. 同样为了捕捉账户的局部和全局行为,文献[64]将图神经网络与 Transformer 结合,提出一种创新的局部-全局感知(Local-Global Awareness,LGA)框架. LGA 框架由一个局部感知模块和一个全局感知模块组成,局部感知模块提取节点的子图,并将局部自注意力机制应用到子图中的每个节点,再使用图池化聚合得到节点表示,捕捉了复杂的交易模式. 但局部感知模块的感受野有限,只能捕捉到局部范围内的结构信息. 对此,全局感知模块中以局部感知模块编码得到的节点表示为输入,引入全局自注意力机制来识别节点间的长距离依赖关系,扩展了模型的感受野并增强其表达能力. LGA 协同利用账户局部结构信息和全局关系依赖,实现了不同方法的优势互补,增强模型的检测能力.

与 CATALOG 侧重于捕捉用户行为的时序依赖与演变不同,Sun 等人[65]关注到交易的语义信息,提出一种以太坊欺诈检测方法 TLMG4Eth. TLMG4Eth 将交易语言模型与基于图的方法结合,开创性地利用语言模型学习交易的语义信息,对交易相似性建模. TLMG4Eth 通过将交易数据转换为交易句子、构建交易属性相似图和账户交互图,分别使用不同模型捕捉交易数据中的语义特征、交易相似性和结构信息. 值得注意的是,TLMG4Eth 联合训练多头注意力网络和图卷积神经网络. 与之前仅将特征结合,使用单一预测结果不同,TLMG4Eth 还将两种模型得到的预测结果进行线性插值,融合多种预测结果对节点进行分类. TLMG4Eth 充分利用模型之间的协同效益,提高模型检测能力. 但 TLMG4Eth 方法同样存在一些不足,例如模型复杂,计算成本高和资源消耗大等. Zhang 等人[66]同样关注到交易数据的语义信息,但其侧重于如何将结构信息与语义信息更好地融合在一起,提出一种结合全局图结构和局部语义信息的区块链欺诈检测模型 ETH-GBERT. ETH-GBERT 引入一种动态融合机制,将图卷积神经网络从账户交互图中捕获的全局结构特征和 BERT 模型从交易文本数据中提取的局部语义特征动态融合. 动态融合机制通过一个门控网络,根据输入的不同特征,自适应地调整语义信息和结构信息的融合权重,提高了模型检测复杂欺诈活动的准确性和鲁棒性.

总而言之,Transformer 与图神经网络方法共同应用在以太坊钓鱼诈骗检测任务上,通过结合两者各自的优势,能够有效捕捉账号行为的局部和全局特征. 然而,Transformer 与图神经网络结合的方法在实际检测任务中仍面临一定挑战:由于模型结构复杂,模型在训练过程中往往需要占用大量的内存资源;此外,模型的可解释性较差.

非图与图结合的以太坊钓鱼诈骗检测利用多种方法,综合学习了多种特征. 这种方法不仅丰富了节点的特征表示,还弥补了不同方法各自的局限性,增强了模型检测能力,在一定程度上减少了漏检测或误报的风险. 但同时,这种方法也存在一定局限性. 例如模型的结构复杂,参数量大,可能会导致计算效率低,训练困难等问题. 除此之外,如何更有效地融合不同特征也是一个需要考虑的问题,错误的特征融合方式可能会引入噪声以及重要信息丢失,从而导致模型检测性能反而下降.

表 3 从不同方法及其优缺点等方面总结了非图和图结合的以太坊钓鱼诈骗检测研究相关工作.

表 3　非图和图结合的以太坊钓鱼诈骗检测主要研究

Table 3　Main research on Ethereum phishing fraud detection combining non-graph and graph methods

类别	子类	主要文献	采用方法	优点	缺点
循环神经网络与图神经网络结合的检测	-	[58]、[59]、[60]、[61]	将循环神经网络提取的序列特征和图神经网络捕捉的结构特征结合	融合多种特征,增强节点特征表示	仅拼接特征,忽略不同特征的权重
Transformer 与图神经网络结合的检测	-	[63]、[64]、[65]、[66]	Transformer 与图神经网络结合提取特征	捕捉了结构特征和长距离依赖	模型复杂,消耗资源大,可解释性差

5　以太坊钓鱼诈骗检测相关数据集及评价指标

5.1　以太坊钓鱼诈骗检测研究主要数据集

数据集是模型训练和评估的基础. 随着以太坊钓鱼诈骗检测技术的不断发展,研究人员构建了多种数据集. 在此,选取其中的一些钓鱼账户数据集作为以太坊钓鱼诈骗检测的数据集进行介绍.

文献[33]中贡献了数据集,从 EtherScamDB 和 Etherscan 两个网站上收集关于以太坊钓鱼诈骗行为的数据,包括 1259 个钓鱼账户和 1259 个未标记账户,并以这些账户为源节点提取一阶邻居以及其之间的连接作为一个子网络,子网络中平均包含超过 6 万个节点和 20 万条边.

Chen 等人[67]提供数据集,该数据集通过从被标记为钓鱼账户的节点开始,进行两层的广度优先搜索得到,是一个有向加权的多重图交易网络. 数据集中包含了 2973382 个节点和 13551214 条边,其中被标记为钓鱼节点的节点数量为 1157.

文献[63]提供了一个新的数据集,不同于上述数据集主

要关注以太坊 1.0 的交易,该数据集收集了以太坊 2.0 的交易,反映了以太坊 2.0 上的网络当前状态. 该数据集包含了从 2024 年 8 月 1 日到 2024 年 10 月 9 日的交易,共有 270 个钓鱼账户和 20194 个非钓鱼账户以及 60713 条交易.

5.2 以太坊钓鱼诈骗检测相关评价指标

评价指标是衡量模型检测能力的重要评判工具,以太坊钓鱼诈骗检测可视为一个二分类问题,即判断一个以太坊账户是否属于钓鱼账户. 因此,采用精确率(Precision)、准确率(Accuracy)、召回率(Recall)、F1 分数和 ROC-AUC 作为模型检测的评价指标. Precision 指被识别为钓鱼账户的样本中实际为钓鱼账户的比率;Accuracy 是指被正确识别的账户的数量占总体账户数量的比率;Recall,也称查全率,为总体钓鱼账户中被正确识别为钓鱼账户的比率;F1 分数是 Precision 与 Recall 的调和平均值;ROC-AUC 为 ROC 曲线下的面积,ROC 曲线由假阳率为横坐标、真阳率为纵坐标绘制而成,ROC-AUC 的值越大,代表模型的检测能力越好. 上述 5 种评价指标计算公式如式(3)~式(6)所示:

$$\text{Precision} = \frac{TP}{TP + FP} \tag{3}$$

$$\text{Accuracy} = \frac{TP + TN}{TP + FP + TN + FN} \tag{4}$$

$$\text{Recall} = \frac{TP}{TP + FN} \tag{5}$$

$$\text{F1} = 2 \times \frac{\text{Precision} \times \text{Recall}}{\text{Precision} + \text{Recall}} \tag{6}$$

其中,TP 表示实际为钓鱼账户,也被检测为钓鱼账户的样本数;FP 表示实际为正常用户,却被检测为钓鱼账户的样本数量;TN 表示实际为正常用户,也被检测为正常用户的样本数;FN 表示实际为钓鱼账户,却被检测为正常用户的样本数. 除这 5 种常用评价指标外,还有一些指标用来衡量模型的检测能力,包括假阳率、PR-AUC 和 Kappa 系数. 假阳率是指被是被识别成钓鱼账户的正常账户占总体正常账户的比率. PR-AUC 是 PR 曲线下的面积,PR 曲线由 Recall 为横坐标,Prcision 为纵坐标绘制而成. PR-AUC 评估了模型检测正样本的能力,适用于类别不平衡的任务场景,PR-AUC 的值越大,对正类样本的分类能力越好. Kappa 系数衡量了模型分类能力,在类别不平衡的情况下,惩罚模型对多数类的偏好,克服准确率失真的缺陷,能够更真实地反映模型实际的检测能力.

除了上述主要关注了模型的分类结果的评价指标,模型的检测效率也是一个重要评价指标. 模型的运行时间衡量了模型的检测效率,运行时间越短,代表模型的检测效率越高.

6 以太坊钓鱼检测研究存在的主要问题及未来研究方向

6.1 主要问题

1)数据不平衡问题. 以太坊中的钓鱼账户数量远远少于正常账户数量,分类器在对账户进行分类时易倾向多数类,导致分类结果出现偏差. 因此,数据不平衡仍是以太坊钓鱼诈骗检测中存在的主要问题之一. 缓解数据不平衡问题的方法可分为两类,分别是数据层面和算法层面. 数据级方法主要通过采样技术改变数据集中的正负样本数量,使其类别分布均衡,算法级方法主要通过调整模型算法使其更适合处理不平衡数据集. 在当前的研究工作中,数据层面解决数据不平衡问题采用最多的方法是过采样、欠采样和 SMOTE 技术,这些方法虽然能在一定程度上缓解数据不平衡问题,但容易造成信息丢失和过拟合的风险,影响模型识别异常交易的能力. 算法层面应对数据不平衡问题无需对不平衡数据集进行预处理,但有一定的局限性,如难以处理高维数据,泛化能力下降和计算成本过高等. 为此,在解决数据不平衡问题时需根据实际情况综合考虑使用数据层面和算法层面,并对其进行调整优化.

2)资源消耗高问题. 以太坊上的交易日益增长,导致交易数据数量庞大. 由交易数据构建成的图规模庞大,且节点和边的类型众多,导致图具有复杂的网络结构. 若将整个图输入模型中进行处理,则不可避免地会造成极大的内存消耗以及过高的计算成本. 为缓解这一问题,现有的研究主要采用子图采样的方法来减少图的规模,以期降低模型的计算负担,但这些采样策略可能会丢失重要信息,导致模型的学习效果变差,最终影响模型的检测性能.

3)检测技术实时性和适应性问题. 以太坊上每秒可产生大量交易,钓鱼诈骗对以太坊生态安全造成严重威胁,导致用户损失大量资金. 实时性检测可及时捕捉异常交易并阻止,降低用户的财产损失. 此外,以太坊上的钓鱼诈骗的模式会随着时间而改变,因此检测方法需具备实时性和适应性,能够学习并识别新的钓鱼诈骗交易模式. 现有的以太坊钓鱼诈骗检测方法虽然已有一定的研究进展,但在实时性方面仍然比较缺乏.

4)检测模型的可解释性问题. 在以太坊钓鱼诈骗检测相关研究中,当前检测方法大多仅仅直接输出以太坊账户的分类标签. 用户对模型的决策过程是不可见的,难以理解模型的检测结果,可能会导致对检测结果的不信任. 因此,需采取一定措施提升模型的可解释性,增强用户对检测结果的信任度,推动以太坊钓鱼诈骗检测领域的发展.

5)钓鱼账户伪装性问题. 钓鱼诈骗犯罪分子其常与正常账户交互模仿正常账户的交易频率与金额,这些行为使得钓鱼账户看起来更像是正常账户,实现了自然伪装,模糊了正常账户与钓鱼账户之间的界限. 这种伪装性给模型准确检测钓鱼账户带来了挑战. 因此,为有效识别出钓鱼账户,未来需研究更为先进的检测技术,深入了解伪装账户的内在模式,捕捉其与正常账户的差异,增强模型对自然伪装账户的检测能力.

6.2 未来主要研究方向

1)大语言模型的以太坊钓鱼诈骗检测. 大语言模型是一种具有大量参数的基于深度学习的人工智能模型,通过在海量数据上进行训练,从而捕捉和学习数据复杂的模式和特征. 大语言模型具有实时处理和学习大规模数据的能力,并且拥有强大的时序建模能力,而以太坊上的大规模交易数据对现有的检测方法仍是一个难点,将大语言模型应用到以太坊钓鱼诈骗检测领域上具有广泛的前景. 从非图方面来看,大语言模型能够从由交易数据建模成的序列数据中挖掘出丰富的语义信息和时序特征,实时高效地识别出以太坊钓鱼诈骗账户. 在图方面,大语言模型能够捕捉节点的文本信息,生成丰富的图节点表示.

2)增量学习的以太坊钓鱼诈骗检测. 增量学习,也被称为终身学习,是一种能够在学习新知识的同时又能保留旧知

识的机器学习算法.现有模型处理任务时常常遇见灾难性遗忘问题,即模型在学习新的知识之后会遗忘掉大部分的旧知识,导致模型在原任务上的性能不佳.而增量学习能够让模型保留对旧知识的记忆,是缓解灾难性遗忘问题的一个重要方法.此外,增量学习允许模型在学习新知识时逐步学习,不必重新训练模型,提高模型学习效率.以太坊上的交易数据规模庞大且增长迅速,现有的检测方法处理以太坊交易数据仍有一定的局限性,对此,可引入增量学习来进行以太坊钓鱼诈骗检测.增量学习在非图和图方法中均有所应用,其核心目的是避免模型灾难性遗忘以及持续学习新的数据.Li 等人[68]提出使用自监督增量深度图学习方法检测以太坊上的钓鱼欺诈,其中采用增量训练方法,每次只输入部分交易数据进行训练,不仅有效缓解了数据规模过大带来的挑战,还帮助模型适应新的数据分布.将增量学习应用到以太坊钓鱼诈骗检测中,有助于提升模型训练效率,降低计算成本.

3)以太坊钓鱼诈骗检测模型的可解释性.模型的可解释性能够增强模型的透明度,帮助用户理解模型的决策过程以及最终的检测结果,对推动检测模型的发展至关重要.目前以太坊钓鱼诈骗检测领域中关于模型可解释性方面的工作较少,通常引入 SHAP 方法衡量特征对模型检测的贡献度.未来需考虑更多方法来提升模型的可解释性,如在图方法方面,使用 GNNexplaine[69]等方法对图神经网络模型的检测结果提供可解释性.

4)动态异构图的钓鱼诈骗检测.目前大多基于图的以太坊钓鱼诈骗检测研究工作主要是围绕静态图和同构图开展的,很少同时考虑到图的动态性和异构性.动态异构图中包含更多信息,更有利于图分析技术挖掘信息生成丰富特征表示.但动态异构图同时也具有更复杂的结构,如何利用图分析技术更有效地处理动态异构图获得丰富的节点表示是未来研究的一个重要方向.

5)图对比学习的钓鱼诈骗检测.图对比学习是一种自监督学习方法,通过对比学习任务来学习高质量的节点特征表示,无需依赖标签,有效缓解以太坊账户标签稀缺的问题.文献[70,71]中使用图对比学习检测以太坊钓鱼诈骗,通过不同对比任务学习并增强节点特征表示,缓解了数据稀疏问题和钓鱼节点的伪装性问题带来的挑战.目前图对比学习的以太坊钓鱼诈骗检测相关研究工作较少,在未来仍有较大的发展空间.

6)图与非图结合的以太坊钓鱼诈骗检测.基于非图的以太坊钓鱼诈骗检测能够高效细粒度地提取到账户的信息,但容易忽略账户之间的交互结构信息.基于图的以太坊钓鱼诈骗检测能够捕捉图中的结构特征,但容易忽略其他的细粒度信息.对此,可将基于非图和图的方法结合以发挥两者各自的优势,例如大语言模型与图神经网络的结合,以期提高模型检测能力.未来,非图与图结合的以太坊钓鱼诈骗检测是一个重要方向.

7　结束语

本文从不同检测方法的数据表示视角出发,对当前以太坊区块链的钓鱼诈骗检测研究从非图、图以及非图和图结构相结合 3 个方面对其现有研究工作展开分析,指出了当前以太坊钓鱼诈骗检测研究存在的数据不平衡、大规模数据处理和实时性等问题,最后对以太坊钓鱼诈骗检测未来研究方向进行了展望,旨在为后续以区块链相关钓鱼诈骗检测研究提供一定借鉴.

References:

[1] Nakamoto S, Bitcoin A. A peer-to-peer electronic cash sytem[EB/OL]. https://bitcoin.org/bitcoin.pdf, 2008.

[2] Slowmist. 2024 blockchain security and AML annual report[EB/OL]. https://www.slowmist.com/report/f-irst-half-of-the-2024-report(CN).pdf, 2024-07-15.

[3] BIAN L Y, ZHANG L L, ZHAO K, et al. Ethereum malicious account detection method based on lightGBM[J]. Netinfo Security, 2020, 20(4): 73-80.

[4] Chen W, Guo X, Chen Z, et al. Phishing scam detection on ethereum: towards financial security for blockchain ecosystem[C]//International Joint Conferences on Artificial Intelligence Organization (IJCAI), 2020: 4506-4512.

[5] Kanezashi H, Suzumura T, Liu X, et al. Ethereum fraud detection with heterogeneous graph neural networks[J]. arxiv preprint arxiv: 2203.12363, 2022. doi: 10.48550/ arXiv.2203.12363.

[6] CAI Z, JING T, REN S. Survey on ethereum phishing detection technology[J]. Chinese Journal of Network and Information Security, 2023, 9(2): 21-32.

[7] LI G, CHEN Z T, BIAN J, et al. Blockchain fraud behaviors detection technology: a survey[J]. Journal of Cyber Security, 2024, 9(4): 1-30.

[8] LI M, LIANG G J, YIN J, et al. A Survey of ethereum illegal detection methods[J]. Journal of Cyber Security, 2024, 9(5): 189-216.

[9] LI J L, LI L X, LIN H, et al. A review of hierarchical research on malicious transactions in blockchain[J]. Journal of Frontiers of Computer Science and Technology, 2025, 19(10): 2559-2586.

[10] He B, Chen Y, Chen Z, et al. TxPhishScope: towards detecting and understanding transaction-based phishing on ethereum[C]//Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, 2023: 120-134.

[11] He B, Hu X, Hu Y, et al. Phishing tactics are evolving: an empirical study of phishing contracts on ethereum[J]. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2025, 9(2): 1-24.

[12] Chen T, Guestrin C. XGBoost: a scalable tree boosting system[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016: 785-794.

[13] Farrugia S, Ellul J, Azzopardi G. Detection of illicit accounts over the ethereum blockchain[J]. Expert Systems with Applications, 2020, 150: 113318. doi: 10.1016/ j.eswa.2020.113318.

[14] ZHOU J, ZHANG J, YAN S. Research on blockchain fraud account detection based on data on chain[J]. Application Research of Computers, 2022, 39(4): 992-997.

[15] Lundberg S M, Lee S I. A unified approach to interpreting model predictions[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems, 2017: 4768-4777.

[16] Ke G, Meng Q, Finley T, et al. LightGBM: a highly efficient gradient boosting decision tree[C]//Proceedings of the 31st International Conference on Neural Information Processing Systems, 2017:

3149-3157.

[17] Aziz R M, Baluch M F, Patel S, et al. LGBM: a machine learning approach for Ethereum fraud detection[J]. International Journal of Information Technology, 2022, 14(7): 3321-3331.

[18] Chawla N V, Bowyer K W, Hall L O, et al. SMOTE: synthetic minority over-sampling technique[J]. Journal of Artificial Intelligence Research, 2002, 16(1): 321-357.

[19] WANG Z Q, WANG Z Y, WANG Q D, et al. Research on blockchain abnormal transaction detection technology based on LightGBM[J]. Journal of Information Security Research, 2023, 9(9): 877-883.

[20] Kumar N, Singh A, Handa A, et al. Detecting malicious accounts on the ethereum blockchain with supervised learning[C]//Cyber Security Cryptography and Machine Learning: 4th International Symposium(CSCML), 2020: 94-109.

[21] Kabla A H H, Anbar M, Manickam S, et al. Eth-PSD: a machine learning-based phishing scam detection approach in ethereum[J]. IEEE Access, 2022, 10: 118043-118057, doi: 10.1109/ACCESS.2022.3220780.

[22] Obi Okoli C, Jogunola O, Adebisi B, et al. Machine learning algorithms to detect illicit accounts on ethereum blockchain[C]//Proceedings of the 7th International Conference on Future Networks and Distributed Systems, 2023: 747-752.

[23] Poursafaei F, Hamad G B, Zilic Z. Detecting malicious ethereum entities via application of machine learning classification[C]//2nd Conference on Blockchain Research & Applications for Innovative Networks and Services(BRAINS), 2020: 120-127.

[24] Ravindranath V, Nallakaruppan M K, Shri M L, et al. Evaluation of performance enhancement in Ethereum fraud detection using oversampling techniques[J]. Applied Soft Computing, 2024, 161, doi: 10.1016/j.asoc.2024.111698.

[25] Wen T, Xiao Y, Wang A, et al. A novel hybrid feature fusion model for detecting phishing scam on Ethereum using deep neural network[J]. Expert Systems with Aplication, 2023, 211: 118463, doi: 10.1016/j.eswa.2022.118463.

[26] Karim F, Majumdar S, Darabi H, et al. LSTM fully convolutional networks for time series classification[J]. IEEE Access, 2017, 6: 1662-1669, doi: 10.1109/ACCESS.2017.2779939.

[27] Tang M, Ye M, Chen W, et al. BiLSTM4DPS: an attention-based BiLSTM approach for detecting phishing scams in ethereum[J]. Expert Systems with Applications, 2024, 256: 124941, doi: 10.1016/j.eswa.2024.124941.

[28] Hu S, Zhang Z, Luo B, et al. BERT4ETH: a pre-trained transformer for ethereum fraud detection[C]//Proceedings of the ACM Web Conference, 2023: 2189-2197.

[29] Hu S, Huang T, Chow K H, et al. ZIPZAP: efficient training of language models for large-scale fraud detection on blockchain[C]//Proceedings of the ACM on Web Conference, 2024: 2807-2816.

[30] Perozzi B, Al Rfou R, Skiena S. DeepWalk: online learning of social representations[C]//Proceedings of the 20th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2014: 701-710.

[31] Grover A, Leskovec J. node2vec: scalable feature learning for networks[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2016: 855-864.

[32] Yuan Q, Huang B, Zhang J, et al. Detecting phishing scams on ethereum based on transaction records[C]//IEEE International Symposium on Circuits and Systems(ISCAS), 2020: 1-5.

[33] Wu J, Yuan Q, Lin D, et al. Who are the phishers? Phishing scam detection on ethereum via network embedding[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 52(2): 1156-1166.

[34] Xiao S, Zhang L, Tian Z, et al. Pheromone-based graph embedding algorithm for Ethereum phishing detection[J]. Computer Networks, 2025, 260: 111123, doi: 10.1016/j.comnet.2025.111123.

[35] Luo J, Qin J, Wang R, et al. A Phishing account detection model via network embedding for ethereum[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2023, 71(2): 622-626.

[36] Lin D, Wu J, Yuan Q, et al. T-EDGE: temporal weighted multidigraph embedding for ethereum transaction network analysis[J]. Frontiers in Physics, 2020, 8: 204, doi: 10.3389/fphy.2020.00204.

[37] Hu J, Cao M, Zhang X, et al. Temporal weighted heterogeneous multigraph embedding for ethereum phishing scams detection[C]//26th International Conference on Computer Supported Cooperative Work in Design(CSCWD), 2023: 1208-1213.

[38] Lin Z, Xiao X, Hu G, et al. Phish2vec: a temporal and heterogeneous network embedding approach for detecting phishing scams on ethereum[C]//20th Annual IEEE International Conference on Sensing, Communication, and Networking(SECON), 2023: 501-509.

[39] Yuan Z, Yuan Q, Wu J. Phishing detection on ethereum via learning representation of transaction subgraphs[C]//Blockchain and Trustworthy Systems: 2nd International Conference, BlockSys, 2020: 178-191.

[40] Narayanan A, Chandramohan M, Venkatesan R, et al. graph2vec: learning distributed representations of graphs[J]. arxiv preprint arxiv: 1707.05005, 2017, doi: 10.48550/arXiv.1707.05005.

[41] Xia Y, Liu J, Wu J. Phishing detection on ethereum via attributed ego-graph embedding[J]. IEEE Transactions on Circuits and Systems, II. Express Briefs, 2022(5): 69, doi: 10.1109/TCSII.2022.3159594.

[42] Wang J, Chen P, Yu S, et al. TSGN: transaction subgraph networks for identifying ethereum phishing accounts[C]//International Conference on Blockchain and Trustworthy Systems, 2021: 187-200.

[43] Xuan Q, Wang J, Zhao M, et al. Subgraph networks with application to structural feature space expansion[J]. IEEE Transactions on Knowledge and Data Engineering, 2019, 33(6): 2776-2789.

[44] Patel V, Pan L, Rajasegarar S. Graph deep learning based anomaly detection in ethereum blockchain network[C]//International Conference on Network and System Security, 2020: 132-148.

[45] Wang X, Du Y, Cui P, et al. OCGNN: one-class classification with graph neural networks[J]. arxiv preprint arxiv: 2002.09594, 2020, doi: 10.48550/arXiv.2002.09594.

[46] Shen J, Zhou J, Xie Y, et al. Identity inference on blockchain using graph neural network[C]//Blockchain and Trustworthy Systems: 3rd International Conference, BlockSys, 2021: 3-17.

[47] Zhang D, Chen J, Lu X. Blockchain phishing scam detection via multi-channel graph classification[C]//Blockchain and Trustworthy Systems: 3rd International Conference, BlockSys, 2021: 241-

256.
[48] Li P,Xie Y,Xu X,et al. Phishing fraud detection on ethereum using graph neural network [C]//International Conference on Blockchain and Trustworthy Systems,2022:362-375.
[49] Huang H,Zhang X,Wang J,et al. PEAE-GNN:phishing detection on Ethereum via augmentation ego-graph based on graph neural network[J]. IEEE Transactions on Computational Social Systems,2024,11(3):4326-4339.
[50] Huang B,Liu J,Wu J,et al. Ethereum phishing fraud detection based on heterogeneous transaction subnets[C]//IEEE International Symposium on Circuits and Systems(ISCAS),2023:1-5.
[51] Liu Z,Wang Y,Wang S,et al. Heterogeneous graphs neural networks based on neighbor relationship filtering[J]. Expert Systems with Applications,2024,239:122489,doi:10.1016/j.eswa.2023.122489.
[52] Patel V,Rajasegarar S,Pan L,et al. EvAnGCN:evolving graph deep neural network based anomaly detection in blockchain[C]//International Conference on Advanced Data Mining and Applications,2022:444-456.
[53] Han B,Wei Y,Wang Q,et al. MT2AD:multi-layer temporal transaction anomaly detection in ethereum networks with GNN[J]. Complex & Intelligent Systems,2024,10(1):613-626.
[54] Wang L,Xu M,Cheng H. Phishing scams detection via temporal graph attention network in Ethereum[J]. Information Processing & Management,2023,60(4):103412,doi:10.1016/j.ipm.2023.103412.
[55] Xu D,Ruan C,Korpeoglu E,et al. Inductive representation learning on temporal graphs[J]. arxiv preprint arxiv:2002.07962,2020,doi:10.48550/arXiv.2002.07962.
[56] Zhang J,Sui H,Sun X,et al. GrabPhisher:phishing scams detection in ethereum via temporally evolving GNNs[J]. IEEE Transactions on Services Computing,2024,17(6):3727-3741.
[57] Rossi E,Chamberlain B,Frasca F,et al. Temporal graph networks for deep learning on dynamic graphs[J]. arxiv preprint arxiv:2006.10637,2020,doi:10.48550/ arXiv.2006.10637.
[58] Li S,Gou G,Liu C,et al. TTAGN:temporal transaction aggregation graph network for ethereum phishing scams detection[C]//Proceedings of the ACM Web Conference,2022:661-669.
[59] Ding Z,Shi J,Li Q,et al. Effective illicit account detection on large cryptocurrency multigraphs[C]//Proceedings of the 33rd ACM International Conference on Information and Knowledge Management,2024:457-466.
[60] Hou W,Cui B,Chen Y,et al. TSFF:a triple-stream feature fusion method for ethereum phishing scam detection[J]. IEEE Internet of Things Journal,2025,12(3):2623-2632.
[61] Tang X,Yao Z,Zhong H,et al. EthGAN:improving ethereum account classification accuracy via data augmentation[C]//International Joint Conference on Neural Networks(IJCNN),2024:1-8.
[62] Goodfellow I J,Pouget Abadie J,Mirza M,et al. Generative adversarial nets[C]//Neural Information Processing Systems,2014:2672-2680.
[63] Ghosh M,Srivastava S,Upadhyaya A,et al. CATALOG:exploiting joint temporal dependencies for enhanced phishing detection on ethereum[C]//Proceedings of the ACM on Web Conference,2025:969-977.
[64] Huang J,Huang T,Dong C,et al. Hierarchical network with local-global awareness for ethereum account de-anonymization[J]. IEEE Transactions on Systems,Man,and Cybernetics:Systems,2025,doi:10.1109/TSMC.2025.3571795.
[65] Sun J,Jia Y,Wang Y,et al. Ethereum fraud detection via joint transaction language model and graph representation learning[J]. Information Fusion,2025,120:103074,doi:10.1016/j.inffus.2025.103074.
[66] Sheng Z,Song L,Wang Y. Dynamic feature fusion:combining global graph structures and local semantics for blockchain phishing detection[J]. IEEE Transactions on Network and Service Management,2025:1-1,doi:10.1109/tnsm.2025.3576130.
[67] Chen L,Peng J,Liu Y,et al. Phishing scams detection in ethereum transaction network[J]. ACM Transactions on Internet Technology(TOIT),2020,21(1):1-16.
[68] Li S,Xu F,Wang R,et al. Self-supervised incremental deep graph learning for ethereum phishing scam detection[C]//Proceedings of the 31st ACM International Conference on Multimedia(MM'23),2023:8881-8890.
[69] Ying R,Bourgeois D,You J,et al. GNNExplainer:generating explanations for graph neural networks[C]//Proceedings of the 33rd International Conference on Neural Information Processing Systems,2023:9244-9255.
[70] Li S,Gou G,Liu C,et al. TGC:transaction graph contrast network for ethereum phishing scam detection[C]//Proceedings of the 39th Annual Computer Security Applications Conference,2023:352-365.
[71] Sui H,Zhang J,Chen B,et al. EPAD:ethereum phishing scam detection via graph contrastive learning[J]. Expert Systems with Applications,2025:128227,doi:10.1016/j.eswa.2025.128227.

附中文参考文献:

[2] 慢雾科技.2024 上半年区块链安全与反洗钱报告[EB/OL]. https://www.slowmist.com/report/first-half-of-the-2024-report(CN).pdf,2024-07-15.
[3] 边玲玉,张琳琳,赵　楷,等.基于 LightGBM 的以太坊恶意账户检测方法[J].信息网络安全,2020,20(4):73-80.
[6] 蔡　召,荆　涛,任　爽.以太坊钓鱼诈骗检测技术综述[J].网络与信息安全学报,2023,9(2):21-32.
[7] 李　广,陈梓钿,卞　静,等.区块链欺诈行为识别技术综述[J].信息安全学报,2024,9(4):1-30.
[8] 李　梦,梁广俊,印　杰,等.以太坊非法交易检测方法综述[J].信息安全学报,2024,9(5):189-216.
[9] 李嘉乐,李雷孝,林　浩,等.区块链恶意交易的层次化研究综述[J].计算机科学与探索,2025,19(10):2559-2586.
[14] 周　健,张　杰,闫　石.基于链上数据的区块链欺诈账户检测研究[J].计算机应用研究,2022,39(4):992-997.
[19] 王志强,王姿旖,王庆德,等.基于 LightGBM 的区块链异常交易检测技术研究[J].信息安全研究,2023,9(9):877-883.