

以太坊钓鱼诈骗检测技术综述

蔡召, 荆涛, 任爽

(北京交通大学计算机与信息技术学院, 北京 100044)

摘要: 随着区块链技术的广泛应用, 网络钓鱼诈骗成为区块链平台上的一大威胁。由于区块链交易具有不可逆性、匿名性和难以篡改性等特点, 网络钓鱼攻击往往具有高度的欺骗性和隐蔽性, 给用户和企业带来了巨大损失。其中, 以太坊平台因其智能合约功能而备受瞩目, 并吸引了众多“加密货币”投资者。然而, 这种广泛流行也导致了一些不法分子的涌入, 滋生了许多网络犯罪行为。其中, 钓鱼诈骗是以太坊平台上主要的诈骗形式之一。针对这种情况, 以太坊网络钓鱼检测技术应运而生, 研究者在该领域取得了众多成果, 但对这些研究成果的系统分析和总结相对较少。深入分析了以太坊上网络钓鱼诈骗的现状, 对已有的钓鱼诈骗检测数据集和评价指标进行了全面总结。在此基础上, 进一步综述了以太坊钓鱼诈骗检测的方法, 包括基于交易信息、基于图嵌入和基于图神经网络的方法。其中, 基于交易信息的方法是最为常见的, 通过分析交易数据的输入地址、输出地址和数额等信息, 来判断交易是否存在异常。基于图嵌入和基于图神经网络的方法则更加注重对整个交易网络的分析, 通过构建图结构来分析节点之间的关系, 从而更加精准地识别钓鱼攻击。对比分析了各方法的优缺点, 说明了各方法的适用范围和局限性。进一步指出了以太坊钓鱼诈骗检测面临的挑战, 并展望了以太坊钓鱼诈骗检测未来的研究趋势。

关键词: 区块链; 以太坊; 钓鱼检测; 图神经网络

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023018

Survey on Ethereum phishing detection technology

CAI Zhao, JING Tao, REN Shuang

School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China

Abstract: With the widespread application of blockchain technology, phishing scams have become a major threat to blockchain platforms. Due to the irreversibility, anonymity, and tamper-proof nature of blockchain transactions, phishing attacks often have a high degree of deception and concealment, causing significant losses to both users and businesses. Ethereum platform, with its smart contract functionality, has attracted many crypto currency investors. However, this widespread popularity has also attracted an influx of criminals, leading to the rise of cybercrime activities. Among them, phishing scams are one of the main forms of fraud on the Ethereum platform. To tackle this

收稿日期: 2022-06-28; 修回日期: 2023-02-19

通信作者: 任爽, sren@bjtu.edu.cn

基金项目: 国家自然科学基金 (62072025)

Foundation Item: The National Natural Science Foundation of China (62072025)

引用格式: 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.

Citation Format: 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.

issue, researchers have developed Ethereum network phishing identification technology, achieving significant progress in this field. However, there has been relatively little systematic analysis and summary of these research results. The current state of phishing fraud on the Ethereum network was analyzed. Moreover, a comprehensive summary of existing phishing detection datasets and evaluation metrics were provided. On this basis, methods for detecting phishing on Ethereum were reviewed, including those based on transaction information, graph embedding and graph neural networks. Transaction information-based methods are the most common, analyzing information such as input and output addresses and amounts in transaction data to determine whether a transaction is abnormal. Methods based on graph embedding and graph neural networks place more emphasis on analyzing the entire transaction network, constructing a graph structure to analyze the relationships between nodes, and more accurately identifying phishing attacks. In addition, a comparative analysis of the advantages and disadvantages of various methods was conducted, explaining the applicability and limitations of each method. Finally, the challenges facing Ethereum phishing detection were pointed out, and the future research trends for Ethereum phishing detection were predicted.

Keywords: blockchain, Ethereum, phishing detection, graph neural network

0 引言

区块链是一种开放式的分布式账本,可以高效、可追溯、可验证、永久地记录双方之间的交易^[1-3]。区块链在经济学中非常重要和著名的应用之一是数字资产^[4-5](或“加密货币”),“加密货币”通过密码学技术来保证交易的安全性。比特币是第一个成功大规模应用区块链技术的“加密货币”。最近,以太坊凭借其自身的去中心化、安全性、匿名性等特点,成为被广泛采用的“加密货币”交易平台,并在区块链技术驱动的各种应用中得到进一步发展。以太坊是目前支持智能合约最大的区块链平台,其相应的“加密货币”以太币(ETH)是第二大“加密货币”^[6]。由于“加密货币”具有匿名性、无监管组织等特点,“加密货币”市场不可避免地滋生了许多犯罪行为^[7]。

首次“代币”发行(ICO, initial coin offering)是在区块链上进行融资的一种方式,指通过发行“代币”(token)募集启动资金。然而,据报道称,以太坊上发布的 10% 以上的 ICO 遭受了各种各样的骗局,包括庞氏骗局和钓鱼诈骗等^[8]。虚拟货币风险管理软件提供商 Chainalysis 的报告显示,在以太坊上的各种诈骗中,钓鱼诈骗是最具欺骗性的诈骗形式。根据 2018 年钓鱼诈骗的统计数据,仅仅在一个月的时间里,诈骗者通过钓鱼诈骗取得非法利润就超过了 300 万美元。

以太坊上的网络犯罪包括黑客攻击、漏洞攻

击、网络钓鱼和庞氏骗局等,据报道称,自 2017 年以来,在以太坊上的各种网络犯罪中,网络钓鱼诈骗占 50% 以上,此类诈骗已成为以太坊上交易安全的重大威胁^[9]。Bee Token, 一个基于区块链技术的家庭共享服务平台,于 2018 年 1 月 31 日进行 ICO,在正式进行 ICO 之前,网络钓鱼者向潜在的 ICO 投资人员发送虚假电子邮件,承诺在接下来的 6 h 内为所有投资者提供额外奖励,还承诺在接下来的两个月内将“代币”价值翻倍。这个网络钓鱼骗局最终在短短 25 h 内骗取了近 100 万美元。

网络钓鱼诈骗的泛滥会导致人们对区块链技术的安全性产生怀疑,从而阻碍相关技术的健康发展^[10]。因此,研究人员越来越重视区块链中的交易安全问题,并提出了各种检测网络钓鱼诈骗的方法。本文首次对以太坊钓鱼检测技术进行了全面的归纳和总结,详细分析了以太坊钓鱼诈骗检测技术的研究现状,并对今后可能的研究方向进行了讨论。

1 以太坊

受比特币的启发,Buterin^[11]于 2013 年提出了以太坊的概念,以太坊是区块链 2.0 的典型代表,其特点是能实现可编程金融,是区块链技术的进阶版本。以太坊最大的特点是增加了对智能合约的支持。智能合约的概念很早就被提出,一般来说,智能合约可以被当成一台图灵机,能够按照一定的规则自动执行代码逻辑,但由于缺乏

稳定可靠的运行环境, 智能合约并没有被广泛使用。直到区块链技术的出现, 大规模应用智能合约技术才成为可能, 区块链的可靠性和稳定性能够保证智能合约的正确执行。在智能合约的代码中设置确定的触发条件, 然后把智能合约部署到区块链上, 在达到合约的触发条件之后, 区块链就会自动执行合约中预定义的代码逻辑, 最后把执行后的结果保存在区块链中, 并且结果不可更改。智能合约的引入使得以太坊成为继比特币之后的第二大平台, 相比比特币, 以太坊增加了账户的概念, 更方便了用户进行交易。

1.1 以太坊账户

比特币是基于交易的模式, 用户无法直接知道自己账户上的余额, 只能通过查看未花费的交易输出 (UTXO, unspent transaction output) 来计算自己的余额。每次在交易时都必须检查余额是否足够花费。此外, 在交易时需要交易发起人花费掉所有比特币, 如果消费的金额小于比特币的总金额, 需要设置一个地址来接收剩余的比特币金额, 否则这部分差额会被当作手续费送给矿工。可以看到, 基于 UTXO 的交易过程十分烦琐, 对比特币用户非常不友好^[12]。以太坊引入了账户的概念, 类似于银行卡账户, 像日常使用银行卡一样, 在以太坊上进行交易直接扣除余额即可, 不需要其他操作。以太坊上的账户可以分为两类,

一类是外部账户 (EOA, externally owned account), 也叫普通账户; 另一类是合约账户 (CA, contract account)。外部账户由密钥进行控制, 记录了账户的余额和账户发出的交易数量。外部账户可以主动发起一笔交易, 或者调用多个合约账户。合约账户不能主动发起交易, 所有交易必须从外部账户发起。合约账户需要存储合约对应的代码、账户状态和变量值等。

1.2 以太坊交易

比特币中的交易基于 UTXO, 在交易过程中需要说明币的来源, 在输入输出中要表明钱包的公钥地址, 如果产生余额, 还需要在输出中添加存放余额的地址。与比特币只能进行转账不同, 以太坊交易可以完成包括转账、合约创建和合约调用在内的 3 种主要功能。根据交易发送方, 以太坊交易可以分为由 EOA 发起的外部交易和由合约调用触发的内部交易。外部账户之间的转账操作和外部账户创建或调用智能合约的操作都属于外部交易, 如图 1 中的交易 1 和交易 2, 交易 2 是外部账户之间的转账交易, 在进行转账操作时, 只需要指定交易双方的地址和转移的以太数量。交易 1 是由外部账户调用智能合约, 在调用时需要指明调用的方法和该方法的参数, 该合约继而触发了交易 3、交易 4 和交易 5, 这 3 个交易属于内部交易, 内部交易是自动进行的, 不需要由外部账户发起。

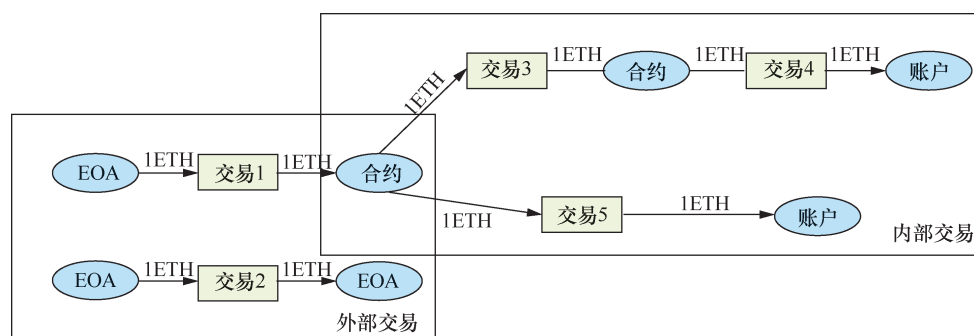


图1 内部交易和外部交易

Figure 1 Internal transactions and external transactions

2 以太坊钓鱼检测的特点、数据集和评价指标

2.1 以太坊钓鱼与传统钓鱼检测的区别

在过去的几十年里, 随着在线业务的兴起, 网络钓鱼诈骗成为交易安全的主要威胁。网络钓

鱼诈骗是指诈骗者通过非法伪造官方网站或联系方式, 获取用户的用户名、密码和地址等隐私信息, 以谋取非法的收益^[13-14]。钓鱼诈骗通常的做法是给受害者发一封看似来自官方的假邮件, 通知其点击链接修改相关信息, 链接实际上指向了一个虚假的诈骗网页, 受害者的信息会在该网站

上泄露,最终被骗子所获得。在实际情况下,这些虚假信息通过电子邮件、广告、论坛和聊天应用程序传播,并且由于成本低,在大多数情况下具有很大的杀伤力。

随着网络钓鱼诈骗受到越来越多的关注,一些研究^[15-18]提出了基于虚拟相似度、关联规则学习和支持向量机的网络钓鱼检测方法。随着研究的不断深入,与钓鱼诈骗相关的各种特征得到了证实和总结,如钓鱼网站的源代码^[19]、链接 URL 的特征^[20]、网站的 CSS 特征^[21]等。由于传统的钓鱼诈骗通常依靠钓鱼邮件和网站来获取用户的敏感信息,现有的大多数钓鱼检测方法基于对邮件和 Web 内容的文本检测。

与传统场景相比,以太坊上的钓鱼诈骗可以通过更多样的方式进行。这种钓鱼诈骗不仅可以通过钓鱼网站获取用户的敏感信息和金钱,还可以通过电子邮件、网站和在线聊天向受害者传播钓鱼地址,直接诈骗钱财。以太坊钓鱼诈骗和传统钓鱼诈骗的区别如图 2 所示。因此,传统的基于网站的钓鱼检测方法不能直接用来解决以太坊上的钓鱼检测问题,因为只有一小部分钓鱼诈骗是通过钓鱼网站实现的。同时,得益于区块链的开放性和透明性,钓鱼诈骗的受害者通常可以找到其诈骗资金去向,并举报可疑的钓鱼地址。此外,以太坊上的所有交易记录都是公开可访问的,可以通过挖掘地址之间的交易行为来识别钓鱼地址。

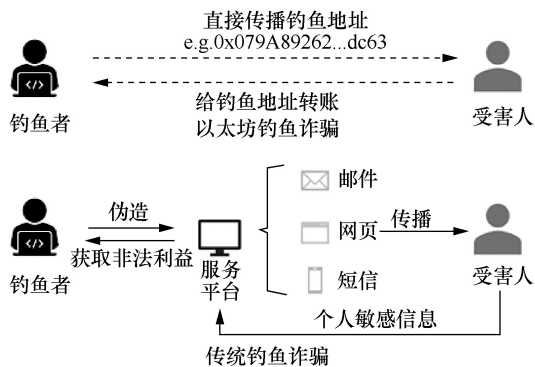


图2 以太坊钓鱼诈骗和传统钓鱼诈骗的区别
Figure 2 The difference between Ethereum phishing scams and traditional phishing scams

2.2 常用数据集

由于公有链的开放性,每个客户端在以太坊上都可以获得所有的交易记录,从而获得以太坊

交易网络的数据集。Etherscan^[22]是以太坊区块浏览器,可以查看区块链上的任何交易信息,包括区块高度、时间戳、交易数量、矿工信息、区块奖励和挖矿难度等。对于每一笔交易,可以看到交易的哈希值、交易发送方、交易接收方、所属区块、交易时间、交易金额和 Gas 汽油费等信息。其中,比较重要的是交易双方地址、交易时间和交易金额。

目前,以太坊钓鱼检测研究大多是通过网络爬虫获取以太坊上的交易信息,形成以太坊数据库。为了检测网络钓鱼诈骗,需要获得足够多的经过验证的网络钓鱼地址作为阳性样本,Etherscan 提供了一份钓鱼地址列表,这些地址是真实审计后标记的。网站 Etherscamdb^[23]报道了以太坊上的各种骗局,包括钓鱼诈骗等。Xblock^[24]是被学术界广泛使用的区块链数据平台,收集了当前的主流区块链数据,并且所有区块链数据集都被以标准化的方式清洁和分类,包括区块链交易数据集、以太坊交易数据集和智能合约数据集等。

2.3 常用评价指标

以太坊钓鱼检测的目标是从包含钓鱼节点和正常节点的数据集中检测出钓鱼节点,本质上是一个二分类问题。在二分类问题中,共有 4 种分类情况,常用混淆矩阵(如表 1 所示)衡量分类的准确性。

表1 混淆矩阵
Table 1 Confusion matrix

实际节点类型	预测为钓鱼节点	预测为正常节点
	的数目	的数目
实际为钓鱼节点	TP	FN
实际为正常节点	FP	TN

其中,TP 表示将钓鱼节点正确预测为钓鱼节点的数目,FN 表示将钓鱼节点错误地预测为正常节点的数目,FP 表示将正常节点错误地预测为钓鱼节点的数目,TN 表示将正常节点正确预测为正常节点的数目。

1) 灵敏度(sensitivity): 将钓鱼节点预测为钓鱼节点的能力,见式(1)。

$$\text{sensitivity} = \frac{TP}{TP+FN} \quad (1)$$

2) 特异度 (specificity): 将正常节点预测为正常节点的能力, 见式(2)。

$$\text{specificity} = \frac{TN}{FP+TN} \quad (2)$$

3) 误检率 (FPR, false positive rate): 将正常节点错误地预测为钓鱼节点的比例, 见式(3)。

$$\text{FPR} = \frac{FP}{FP+TN} \quad (3)$$

4) 漏检率 (FNR, false negative rate): 将钓鱼节点错误地预测为正常节点的比例, 见式(4)。

$$\text{FNR} = \frac{FN}{TP+FN} \quad (4)$$

5) 准确率 (P, prediction): 在所有预测为钓鱼节点的节点中, 实际钓鱼节点所占的比例, 见式(5)。

$$P = \frac{TP}{TP+FP} \quad (5)$$

6) 召回率 (R, recall): 召回率是覆盖面的度量, 等价于 sensitivity, 见式(6)。

$$R = \frac{TP}{TP+FN} \quad (6)$$

7) F -measure: 准确率 P 和召回率 R 有时候会出现矛盾的情况, 就得综合考虑它们。 F 是 P 和 R 的加权调和平均数, 计算如式(7)所示。其中 β 是参数, 如果 $\beta=1$, 即为常见的 F_1 值, 见式(8)。

$$F_\beta = \frac{(1+\beta^2)PR}{\beta^2 P + R} \quad (7)$$

$$F_1 = \frac{2PR}{P+R} \quad (8)$$

8) 精确度 (ACC, accuracy): 钓鱼节点和正常节点正确预测的比例, 见式(9)。

$$\text{ACC} = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

3 钓鱼节点检测技术

3.1 基于交易信息

基于交易信息的以太坊钓鱼检测方法主要利用历史交易信息。在以太坊的交易过程中, 每一次交易都会涉及交易发送方、交易接收方、交易时间、交易金额以及交易产生的手续费等账户信息。同时, 复杂网络分析方法可以应用到以太坊

上^[25-27], 可以把以太坊上的交易抽象为交易网络, 把以太坊中的账户抽象为节点, 将节点之间的关系抽象为边, 再提取账户的入度、出度等网络信息。常用的账户特征如图3所示, 利用这些账户信息和网络信息来描述每一个账户节点, 进而区分钓鱼节点和正常节点。基于交易信息的以太坊钓鱼检测流程如图4所示。

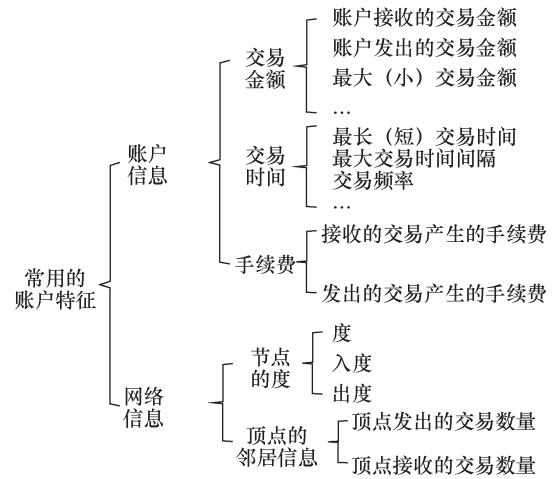


图3 常用的账户特征
Figure 3 Common account features

Chen 等^[28]根据交易信息构造了一个交易图, 图中的节点代表账户, 边代表账户之间的交易, 接着提取了账户的8个特征, 包括节点的度、交易金额、邻居的数量和交易频率等信息。Farrugia 等^[29]构造了42个特征来进行账户分类, 最后根据特征重要性分析, 发现前3个最重要的特征分别是最长交易间隔、总的交易金额和收到的最小交易金额。构造完特征之后选择分类器进行节点分类。对于下游分类任务所用的模型, 可以采用LGBM^[30]、CatBoost^[31]、XGBoost^[32]等。更进一步, Ibrahim 等^[33]采用相关系数分析方法将42个特征精简到了6个特征, 然后在下游的分类任务中使用决策树、 K 近邻和随机森林等方法进行节点分类, 也取得了较好的效果。

除了使用人工提取的特征, 也可以自动构造特征。文献[34]通过收集以太坊上的交易数据进行特征提取。特征由两部分组成: 一部分是基于以太坊上的交易历史总结归纳的手工特征, 包括交易数量、交易总额、交易平均价值、以太坊手续费等; 另一部分是使用自动特征构造工具

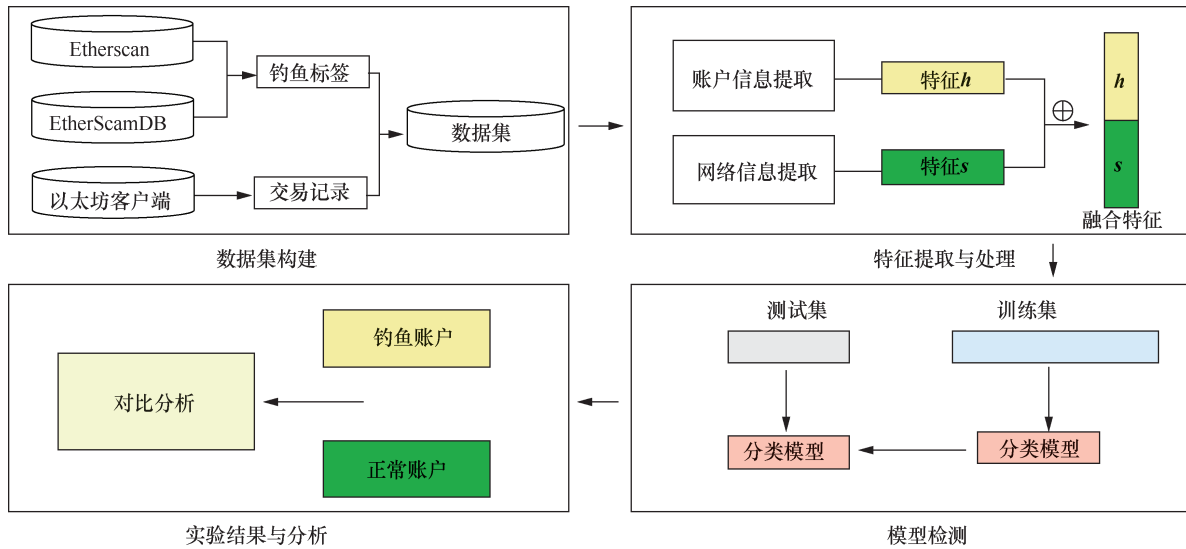


图 4 基于交易信息的以太坊钓鱼检测流程

Figure 4 The process of Ethereum phishing detection based on transaction information

featuretools 提取与交易有关的统计特征, 选取了 86 个有效特征作为统计特征。然后, 作者将两部分特征进行融合, 最后为了对比模型分类检测效果, 文中采用 6 种监督机器学习方法来检测钓鱼账户, 结果表明, LightGBM 模型效果最好, F_1 值可达 94%。该方法的缺点是没有考虑到以太坊交易网络的结构特征, 因为点对点的交易最终会组成一个交易网络, 仅仅考虑单个节点的特征会产生局限性, 同时该方法不能很好地解决数据不平衡的问题。

为了解决上述问题, Chen 等^[35]采用基于图的级联特征提取的方法来构建账户特征, 该方法能够很好地考虑到交易网络的结构信息。作者在构造交易图时, 给每条边赋予两个属性 (交易时间和交易金额), 不仅使用账户自身的信息, 而且提取账户邻居的信息, 或者邻居的邻居 (即 2 阶邻居) 的信息, 当然也可以扩展成多阶邻居。在提取交易信息时, 主要采用统计方法, 如求最大值、最小值、平均值和中位数等。通过在不同阶段采用不同的统计方法, 可以提取节点与整个网络相互作用的丰富信息。作者共提取了 200 个特征。同时为了解决样本不平衡的问题, 选取 LightGBM 作为基础模型, 采用双采样集成方法来区分正常节点和钓鱼节点。Poursafaei 等^[36]融合了节点的交易特征、邻居特征和结构特征, 更好地表征了每一个节点。

为了增强模型的鲁棒性, 在网络中加入对抗性攻击是有必要的。对抗性攻击是指在原始网络中注入一些扰动 (如修改拓扑和特征信息) 来误导相应的机器学习模型, 从而得到错误的答案^[37-40]。Wen 等^[41]对以太坊交易记录增加了一些扰动, 就是在账户之间插入不存在的交易。作者用单向隐藏策略对原始网络进行扰动得到扰动网络, 在扰动网络中提取新的交易特征, 最后将扰动后的特征送入分类器进行训练, 从而得到鲁棒性好的检测模型。

3.2 基于图嵌入

图嵌入属于表示学习, 主要目的是将图中的节点表示成低维的向量形式, 使得到的向量能够做进一步的推理, 以更好地实现下游任务。基于图嵌入方法的以太坊钓鱼检测流程如图 5 所示, 首先将数据构造成交易图, 其中每个节点表示一个交易账户, 每条边表示账户之间发生的交易, 再利用图嵌入的方法把图中的节点表示成低维向量, 这些向量包含了节点的拓扑信息, 最后根据这些向量进行节点分类。图嵌入的方法主要有矩阵分解、随机游走和深度学习。在以太坊上进行节点嵌入主要有随机游走和深度学习的方法。

3.2.1 基于随机游走的图嵌入方法

随机游走是从一个或一系列节点开始的图的遍历过程。在任意一个节点, 该节点会以一定的概率移动到其相邻的节点, 并随机跳转到图中的

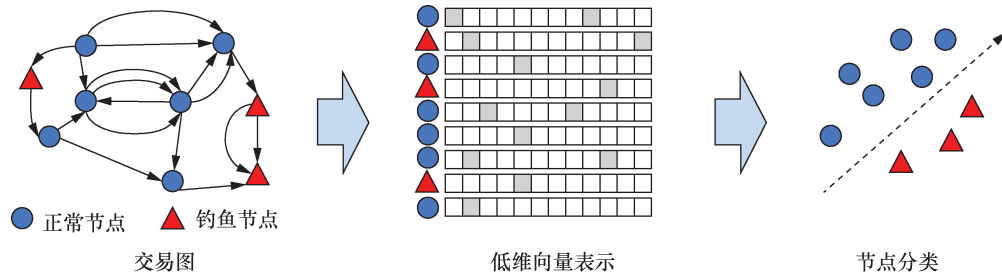


图5 基于图嵌入方法的以太坊钓鱼检测流程
Figure 5 The process of Ethereum phishing detection based on graph embedding method

任意一个节点。在每一步之后都会得到一个概率分布。这个概率分布表示每个节点被访问的概率,将这个概率值作为输入继续重复这一过程,满足一定条件后直至收敛达到稳定,最终的概率分布可以刻画图的结构特征。

DeepWalk^[42]是一种基于随机游走的网络表示学习方法,其灵感来自 Word2Vec^[43],它的过程是首先选择一个特定的节点作为起始节点,随机游走得到节点的序列,然后把得到的序列当作一个句子,用 Word2Vec 学习得到节点的表示向量。这是因为通过随机游走得到的序列分布类似于自然语言中词的分布,并遵循幂律。Node2Vec^[44]是 DeepWalk 的扩展,DeepWalk 随机均匀地选择下一个节点,但 Node2Vec 是深度优先搜索(DFS, depth first search)和广度优先搜索(BFS, breadth first search)的动态组合,该模型设置了两个参数 p 和 q 来控制选择 DFS 和 BFS 的概率。 p 和 q 一般需要通过半监督学习来确定,但也可以手动设置。Yuan 等^[45]采用 Node2Vec 对以太坊钓鱼账户进行识别,取得了较好的效果。Line^[46]定义了一阶相似度和二阶相似度,可以很容易地扩展到具有数百万个节点和数十亿条边的网络。

上述几个图嵌入方法都是基于随机游走生成节点序列的,将图结构的数据转化为自然语言处理的任务。然而,图结构中节点的关系往往比词上下文的关系更复杂。通常,边具有权重,现有的基于 Word2Vec 的方法无法很好地处理这些权重。此外,存储所有游走序列需要大量空间。

为了解决大规模网络问题,Yuan 等^[47]根据收集到的以太坊交易记录,构建了相应的子图,同时为了获取原始图的结构信息和边信息,作者将

原始图转换为线图,即将原始边转换为新图的节点,并将共享公共端点的节点连接起来构成边,然后保留原边的标签作为其在线图中的对应节点的标签,并将转换后的对应线图放入 Graph2Vec^[48]模型中,得到所有图的表示向量。Graph2Vec 的主要步骤包括以下两部分:提取有根子图,以一组子图的形式表示所有的图;通过 skip-gram 模型学习图的嵌入表示。最后采用支持向量机来区分该地址是否为网络钓鱼账户。

传统的随机游走都是无偏游走,即中心节点转移到邻居节点的概率是相等的,对于以太坊来说,每条交易边上都有重要的信息,显然无偏游走是具有局限性的。Wu 等^[49]改进 DeepWalk,提出了一种新型的游走方式 tran2vec,基于交易金额和交易时间戳来进行有偏游走。Wang^[50]等也采用了这种游走方式,并把表示学习分成节点表示学习、边表示学习和属性表示学习,再把这 3 种表示学习进行结合。

上述方法将交易记录建模为静态简单图,以太坊交易网络是一个多重图,意味着每两个账户之间不一定只发生一次交易,静态简单图无法准确描述以太坊交易网络的时间和重复交易特征。文献[51-52]将以太坊交易网络建模成时间加权多重图,具体来说,给定以太坊交易网络图 $G=(V,E)$,其中 V 是节点集, E 是边集,每条边都是独一无二的且可以表示为 $e=(u,v,w,t)$,其中 u 是源节点, v 是目标节点, w 是交易金额, t 是交易时间戳。这种时间加权多重图更能反映实际的以太坊交易网络。

3.2.2 基于深度学习的图嵌入方法

基于深度学习的方法主要利用神经网络来学

习图中的非线性信息^[53-54]。文献[55]提出了基于交易子图网络(TSGN, transaction sub-graph network)的分类模型来识别以太坊中的钓鱼账户,首先提取每个地址的交易子图,然后根据不同的映射机制将这些子图扩展为对应的 TSGN。此外,通过引入方向属性,Directed-TSGN 可以保留捕获钓鱼诈骗重要拓扑模式的交易流信息。Chen 等^[28]提出了一种基于图卷积网络和自动编码器的检测方法来精确识别网络钓鱼账户。Xia 等^[56]根据以太坊交易记录构造了中心图,对每个中心节点采集 k -hop 有向邻居,并根据金额、交易数量、方向对节点进行重新标记,中心节点的 label 是 0,邻居节点的 label 是 1~12,再对重新标记后的图进行训练。

3.3 基于图神经网络

上述的以太坊钓鱼检测方法都是两阶段分离的,也就是说第一阶段进行特征提取,第二阶段把提取好的特征放入下游检测任务,这种两阶段式检测方法是解耦的,其结果具有局限性,而且上述这些方法大多是作用在单一图上的,是直推式学习,不是归纳式学习,对于像以太坊这种产生海量交易的、不断变化的网络,显然需要的是归纳式学习方法。基于图神经网络的钓鱼检测方法可以很好地解决上述问题,基于图神经网络方法的以太坊钓鱼检测流程如图 6 所示,对于交易图中的节点特征,直接输入图神经网络中进行训练,训练结果不再是节点的向量表示,而是直接输出预测结果。

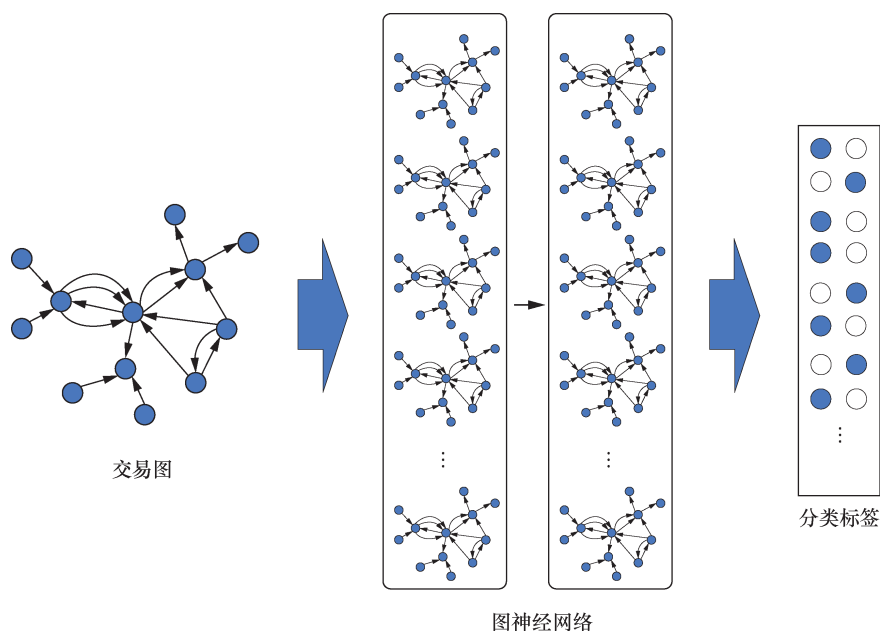


图 6 基于图神经网络方法的以太坊钓鱼检测流程
Figure 6 The process of Ethereum phishing detection based on graph neural network

文献[57]提出了一种多通道图分类(MCGC, multi-channel graph classification)模型来进行钓鱼检测,该模型采用多通道图神经网络(GNN, graph neural network)架构,能够从不同的池化图中自动提取丰富的信息,将节点分类变成图分类。MCGC 通过图池化层的节点聚合操作,将输入图中的节点聚合成新的节点簇,从而得到粗化的池化图结构。多个池化层可以提取输入图的不同关键层次结构信息,这有助于提取多层次的用户交易模式信息。此外,池化层可以与 GNN 结合形成一个端到

端训练模型。Li 等^[58]提出了一种基于 Chebyshev-GCN (graph convolutional network) 的端到端检测模型,该模型选取最大的弱连通子图,根据一定的规则来动态决定采样子图的规模大小,采用 GCN 聚集节点信息,最后用全连接层进行节点分类。

Kanezashi 等^[59]将 GCN 及其变形应用到以太坊钓鱼检测上。GCN^[60]是一种基于图结构数据的神经网络模型,该模型不断聚集邻居的特征向量,将其输入神经网络中。在以太坊网络的钓鱼检测

中，并非所有的邻居节点都与可疑交易相关，在 GCN 模型中，每个节点与所有相邻节点具有相同的权重，GCN 模型不考虑交易属性（时间和金额）作为权重，这可能会对检测钓鱼账户产生影响。

GAT（graph attention network）模型^[61]隐式学习每个邻域的不同权重作为注意力，通过注意力机制，可以更有效地区分正常账户和可疑账户。原始的 GCN 模型不能应用于大型图结构，因为它需要学习所有节点的嵌入向量。GraphSAGE^[62]学习到的聚合函数适用于未知节点，并减少了具有相邻节点采样的大型图的计算量。

4 检测方法总结与展望

4.1 检测方法总结

本文将以太坊钓鱼检测方法分为基于交易信息的检测方法、基于图嵌入的检测方法和基于图神经网络的检测方法，每一类方法都有各自的优缺点，表 2 为以太坊钓鱼检测方法总结，提供了直观的展示，为后续研究工作提供一个明确的指导。

基于交易信息的以太坊检测方法只考虑了以太坊上历史交易记录，特征提取简单，检测时间短，适用于快速检测场景，但是没有考虑到以太

表 2 以太坊钓鱼检测方法总结
Table 2 Summary of Ethereum phishing detection methods

检测方法	典型代表	原理	优点	缺点
基于交易信息的以太坊钓鱼检测方法	基于 XGBoost 的以太坊异常账户检测方法 ^[29]	从 EtherScamDB 和以太坊客户端上获取数据集，通过收集的交易信息提取了 42 个账户特征，使用 XGBoost 分类器进行分类，在训练集上训练模型，在测试集上预测结果，并采用十折交叉验证来评估模型的性能	- 提取特征较为充分，从交易历史记录中提取了 42 个特征 - 使用 XGBoost 检测精度高，平均准确率达到 96.3%，平均 AUC 达到 99.4% - 进行了特征重要性分析，评价了不同的特征对检测结果的影响程度	- 只考虑了节点的账户信息，忽略了节点的网络信息 - 只考虑了交易成功的记录，结果具有一定的局限性
	基于 LightGBM 的以太坊恶意账户检测方法 ^[34]	收集交易记录进行特征构造，一部分是基于交易历史归纳总结的手工特征，一部分是使用自动特征构造工具 featuretools 提取的统计特征，最后采用 6 种监督机器学习方法来检测恶意账户	- 不仅考虑手工特征，还使用自动特征构造工具来提取特征 - 检测结果较好，提出方法的 F1 值达到 94.9%	- 忽略交易网络的结构特征 - 不能解决数据不平衡问题
	级联特征提取和双采样集成方法 ^[35]	将以太坊交易历史记录建模成交易网络，考虑交易时间和交易金额，提取节点的 n 阶邻居信息，采用 LightGBM 作为基准模型进行双采样集成训练	- 解决了数据不平衡问题 - 考虑了交易的网络信息 - 具有可扩展性	- 忽略交易网络的结构特征 - 没有考虑以太坊交易网络的动态特性
基于图嵌入的以太坊钓鱼检测方法	Tran2Vec ^[49]	将交易网络建模成交易图，节点代表账户，边代表交易，采用改进后的有偏游走方式刻画图的结构特征，获得节点的低维向量表示，最后采用单类 SVM 进行检测	- 改进传统游走方式，更能反映以太坊交易网络特点 - 解决数据不平衡的问题	- 忽略以太坊交易网络多重图特性 - 两阶段式方法具有局限性
	基于时间加权多重图的检测方法 ^[51,52]	将以太坊交易网络建模成时间加权多重有向图，每个节点之间可以存在多条边，且边具有交易金额和交易时间戳等权重信息	时间加权多重图更符合以太坊交易网络	- 两阶段式方法具有局限性 - 建模后的网络巨大，不适用于大型图
	构造交易子图 ^[47]	根据目标账户构建交易子图，每个子图包含标签和账户周围的交易网络，用子图反映账户信息获得低维嵌入向量	- 大大缩小网络规模，容易处理大型图 - 图级表示检测效果较好	- 两阶段式方法具有局限性 - 前期交易子图构造过程复杂
基于图神经网络的以太坊钓鱼检测方法	多通道图分类模型 ^[57]	将高复杂度的节点分类任务转化为低复杂度的图分类任务，使用不同池化层提取不同层次的结构信息，最后再聚合池化图信息	- 复杂度低 - 模型精度高	- 依赖数据集的质量 - 检测时间较长
	基于 Chebyshev-GCN 的以太坊钓鱼检测方法 ^[58]	构建了轻量级以太坊交易网络，选取最大的弱连通子图，动态调整子图的大小	- 实现了端到端的检测模型 - 适合大型图	子图采样规则较复杂

坊交易的网络特性,检测结果具有一定的局限性。基于图嵌入的方法可以分为基于随机游走的图嵌入方法和基于深度学习的图嵌入方法,这两种方法在以太坊钓鱼检测上都得到了广泛应用。基于随机游走的钓鱼检测方法能够考虑到以太坊交易图的拓扑结构,把节点映射为低维嵌入向量,再进行下游分类任务,这类方法较多关注目标节点的局部特征。基于深度学习的图嵌入方法主要使用图神经网络来获取节点的非线性信息,经过神经网络的训练能够得到节点的更高阶信息,通常检测精度也较高,但是神经网络的输入端通常要求是小型图,对于以太坊这种大型交易网络,此类方法的通常做法是构建子图,这就会牺牲一些全局信息。

目前的大多数方法是先获取节点特征,通过一些模型训练得到节点的向量表示,再输入下游进行分类或者检测任务,这种两阶段式的方法是上下游解耦的,对于以太坊钓鱼检测任务,显然端到端的模型适用性更好。基于图神经网络的方法可以实现端到端的检测目标,这类方法直接输入以太坊交易图数据,输出节点的标签,检测过程更加高效,也更适应每天产生大量交易的不断变化的以太坊交易网络,但是此类方法的相关研究较少。

4.2 展望

目前,以太坊钓鱼检测研究在特征提取和检测方法上面临着一定的挑战。首先是可用数据集较少,在构建数据集时许多研究需要到特定的网站上爬取相关数据,不同的研究采用不同的数据集,导致评价标准不同,很难进行横向对比。而且在构建数据集的过程中,数据中的正负样本比例悬殊,数据集严重不平衡。同时,以太坊上的交易每天都在进行,不断产生大量交易,现有的研究大多是基于静态图来构造方法的,没有考虑到不断变化的以太坊交易网络,影响所提检测方法的扩展性和实用性。针对现存在的挑战,本文提出如下展望。

1) 数据集的质量决定了检测方法的好坏,为了提高检测的性能,减少研究人员前期收集数据的工作量,有必要构造一些高质量的数据集。目前现存数据集面临着实时性和数据不平衡的问

题。以太坊交易网络每天都会产生新的交易,导致公开的数据集的实时性受到挑战。因此,未来可通过收集最新的交易样本构建新鲜数据集。同时,以太坊钓鱼检测中正负样本比例悬殊,对检测结果造成了较大影响,当遇到不平衡数据时,传统的分类算法会过多关注多数类样本,从而使得少数类样本的分类性能下降。未来可以探索适用于以太坊交易网络的数据不平衡处理方法,如进行数据采样,使得正负样本数量接近,或者把分类模型改成异常检测模型,只关注某一类等。

2) 对钓鱼检测方法进行融合。现有方法会在某一方面给出较好的性能结果,基于交易信息的检测方法容易提取特征,检测时间短,但是较多依赖先验知识;基于图嵌入的方法能够很好地提取网络的结构特征,刻画交易的拓扑结构;基于图神经网络的方法能够实现端到端检测,但是检测时间较长。不同识别方法具有各自的优缺点,存在很强的互补性,可以在检测过程中融合不同模型之间的优点,来提高整个检测框架的准确率和实时性。因此,不同模型之间的融合可能是以太坊钓鱼检测的发展方向之一。

3) 不同研究者提出了很多检测模型,在相关数据集上产生了很好的效果,但是模型的鲁棒性有待验证,使用生成对抗样本添加扰动可以提高模型的检测性能,因此,选择特征生成对抗性样本从而测试已有钓鱼检测系统的鲁棒性可以作为未来探索方向之一。

4) 除了网络钓鱼诈骗,以太坊上还存在诸多犯罪类型,如黑客攻击、漏洞攻击和庞氏骗局等。这些犯罪行为涉及以太坊上的交易,在进行犯罪行为检测时,除了分析各个犯罪行为具有的特点,对于以太坊交易网络的分析是共通的,未来可以在现有研究的基础上,对其他以太坊网络犯罪行为进行研究。

5 结束语

以太坊网络钓鱼检测引起了研究人员的广泛关注。针对这一问题,本文介绍了以太坊钓鱼检测问题的研究背景和相关概念,并详细阐述了以太坊钓鱼检测问题的特点、常用的数据集和评价指标等。此外,针对现有的钓鱼检测方案进行了

详细的分析和评估, 并对今后可能的研究方向进行了讨论。

参考文献:

- [1] ZHENG Z, XIE S, DAI HN, et al. Blockchain challenges and opportunities: a survey [J]. *International Journal of Web and Grid Services*. 2018, 14(4): 352-375.
- [2] MONRAT A A, SCHELÉN O, ANDERSSON K. A survey of blockchain from the perspectives of applications, challenges, and opportunities[J]. *IEEE Access*. 2019, 7: 117134-117151.
- [3] YUAN Y, WANG FY. Blockchain and cryptocurrencies: Model, techniques, and applications[J]. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. 2018, 48(9): 1421-1428.
- [4] CROSBY M, PATTANAYAK P, VERMA S, et al. Blockchain technology: beyond bitcoin[J]. *Applied Innovation*. 2016, 2(6-10): 71.
- [5] YANG Z, YANG K, LEI L, et al. Blockchain-based decentralized trust management in vehicular networks[J]. *IEEE Internet of Things Journal*. 2018, 6(2): 1495-1505.
- [6] WANG S, OUYANG L, YUAN Y, et al. Blockchain-enabled smart contracts: architecture, applications, and future trends[J]. *IEEE Transactions on Systems, Man, and Cybernetics*: 2019, 49(11): 2266-2277.
- [7] HOLUB A, O'CONNOR J. Tracking a ukrainian bitcoin phishing ring DNS style[C]//*Proceedings of 2018 APWG Symposium on Electronic Crime Research (eCrime)*. 2018: 1-5.
- [8] Ethereum under siege: scammers make \$700,000 in 6 days from slack and reddit phishing attacks[EB].
- [9] CONTI M, KUMAR E S, LAL C, et al. A survey on security and privacy issues of bitcoin[J]. *IEEE Communications Surveys & Tutorials*, 2018, 20(4): 3416-3452.
- [10] BARTOLETTI M, CARTA S, CIMOLI T, et al. Dissecting ponzi schemes on ethereum: identification, analysis, and impact[J]. *Future Generation Computer Systems*. 2020, 102: 259-277.
- [11] BUTERIN V. A next-generation smart contract and decentralized application platform[J]. *Ethereum White Paper*, 2014, 3(37): 2-1.
- [12] 傅丽玉, 陆歌皓, 吴义明, 等. 区块链技术的研究及其发展综述[J]. *计算机科学*, 2022, 49(S1): 447-461, 666.
FU L Y, LU G H, WU M Y, et al. A review of the research and development of blockchain technology[J]. *Computer Science*, 2022, 49(S1): 447-461, 666.
- [13] 付溪, 李晖, 赵兴文. 网络钓鱼识别研究综述[J]. *网络与信息安全学报*, 2020, 6(5): 1-10.
FU X, LI H, ZHAO X W. Survey on phishing detection research[J]. *Chinese Journal of Network and Information Security*, 2020, 6(5): 1-10.
- [14] 张茜, 延志伟, 李洪涛, 等. 网络钓鱼欺诈检测技术研究[J]. *网络与信息安全学报*, 2017, 3(7): 7-24.
ZHANG X, YAN Z W, LI H T, et al. Research of phishing detection technology[J]. *Chinese Journal of Network and Information Security*, 2017, 3(7): 7-24.
- [15] ABDELHAMID N, AYESH A, THABTAH F. Phishing detection based associative classification data mining[J]. *Expert Systems with Applications*, 2014, 41(13): 5948-5959.
- [16] HAN W, CAO Y, BERTINO E, et al. Using automated individual white-list to protect web digital identities[J]. *Expert Systems with Applications*, 2012, 39(15): 11861-11869.
- [17] JAIN A K, GUPTA B B. Two-level authentication approach to protect from phishing attacks in real time[J]. *Journal of Ambient Intelligence and Humanized Computing*, 2018, 9(6): 1783-1796.
- [18] RAO R S, PAIS A R. Jail-phish: an improved search engine based phishing detection system[J]. *Computers & Security*, 2019, 83: 246-267.
- [19] ZOUINA M, OUTTAJ B. A novel lightweight URL phishing detection system using SVM and similarity index[J]. *Human-centric Computing and Information Sciences*, 2017, 7(1): 1-13.
- [20] SAHINGOZ OK, BUBER E, DEMIR O, et al. Machine learning based phishing detection from URLs[J]. *Expert Systems with Applications*, 2019, 117: 345-357.
- [21] MOGHIMI M, VARJANI A Y. New rule-based phishing detection method[J]. *Expert Systems with Applications*, 2016, 53: 231-242.
- [22] Etherscan[EB].
- [23] Etherscan[EB].
- [24] Xblock[EB].
- [25] CHEN Z, WU J, XIA Y, et al. Robustness of interdependent power grids and communication networks: a complex network perspective[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2017, 65(1): 115-119.
- [26] CHEN G, LOU Y, WANG L. A comparative study on controllability robustness of complex networks[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2019, 66(5): 828-832.
- [27] ZHOU J, YU X, LU J A. Node importance in controlled complex networks[J]. *IEEE Transactions on Circuits and Systems II: Express Briefs*, 2018, 66(3): 437-441.
- [28] 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.
- [29] FARRUGIA S, ELLUL J, AZZOPARDI G. Detection of illicit accounts over the Ethereum blockchain[J]. *Expert Systems with Applications*, 2020, 150: 113318.
- [30] AZIZ RM, BALUCH MF, PATEL S, et al. LGBM: a machine learning approach for Ethereum fraud detection[J]. *International Journal of Information Technology*, 2022: 1-11.
- [31] 周健, 闫石, 张杰, 等. 基于交易特征对以太坊多类型非法账户的分析与预测[J]. *计算机应用研究*, 2022(3).
ZHOU J, YAN S, ZHANG J, et al. Analysis and prediction of multi-type illegal accounts of ethereum based on transaction characteristics[J]. *Application Research of Computers*. 2022(3).
- [32] 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.
ZHOU J, ZHANG J, YAN S. Research on detection of fraudulent accounts in blockchain based on on-chain data[J]. *Application Research of Computers*, 2022, 39(4): 992-997.
- [33] IBRAHIM R F, ELIAN A M, ABABNEH M. Illicit account detection in the ethereum blockchain using machine learning[C]//*Proceedings of 2021 International Conference on Information Technology (ICIT)*. 2021: 488-493.
- [34] 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.
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.
- [35] CHEN W, GUO X, CHEN Z, et al. Phishing scam detection on ethereum: towards financial security for blockchain ecosystem[C]//*Proceedings of IJCAI*. 2020: 4506-4512.
- [36] POURSAFAEI F, RABBANY R, ZILIC Z. SigTran: signature Vectors for detecting illicit activities in blockchain transaction net-

- works[C]//Proceedings of Pacific-Asia Conference on Knowledge Discovery and Data Mining. 2021: 27-39.
- [37] SUN L, DOU Y, YANG C. et al. Adversarial attack and defense on graph data: a survey[J]. arXiv preprint arXiv:1812.10528, 2018.
- [38] DAI H, LI H, TIAN T, et al. Adversarial attack on graph structured data[C]//Proceedings of International Conference on Machine Learning. 2018: 1115-1124.
- [39] ZÜGNER D, AKBARNEJAD A, GÜNNEMANN S. Adversarial attacks on neural networks for graph data[C]//Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining. 2018: 2847-2856.
- [40] ZHANG Q, FANG J, ZHANG J, et al. Cross entropy attack on deep graph infomax[C]//Proceedings of 2020 IEEE International Symposium on Circuits and Systems (ISCAS). 2020: 1-5.
- [41] WEN H, FANG J, WU J. et al. Transaction-based hidden strategies against general phishing detection framework on ethereum[C]//Proceedings of 2021 IEEE International Symposium on Circuits and Systems (ISCAS). 2021: 1-5.
- [42] 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.
- [43] MIKOLOV T, SUTSKEVER I, CHEN K. et al. Distributed representations of words and phrases and their compositionality[J]. Advances in Neural Information Processing Systems, 2013, 26.
- [44] 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.
- [45] YUAN Q, HUANG B, ZHANG J. et al. Detecting phishing scams on ethereum based on transaction records[C]//2020 IEEE International Symposium on Circuits and Systems (ISCAS). 2020: 1-5.
- [46] TANG J, QU M, WANG M. et al. Line: large-scale information network embedding[C]//Proceedings of the 24th International Conference on World Wide Web. 2015: 1067-1077.
- [47] YUAN Z, YUAN Q, WU J. Phishing detection on ethereum via learning representation of transaction subgraphs[C]//Proceedings of International Conference on Blockchain and Trustworthy Systems. 2020: 178-191.
- [48] NARAYANAN A, CHANDRAMOHAN M, VENKATESAN R, et al. Graph2Vec: learning distributed representations of graphs[J]. arXiv preprint arXiv:1707.05005, 2017.
- [49] 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.
- [50] WANG Y, LIU Z, XU J, et al. Heterogeneous network representation learning approach for ethereum identity identification[J]. IEEE Transactions on Computational Social Systems, 2022.
- [51] LIN D, WU J, YUAN Q, et al. Modeling and understanding ethereum transaction records via a complex network approach[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2020, 67(11): 2737-2741.
- [52] 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.
- [53] WANG D, CUI P, ZHU W. Structural deep network embedding[C]//Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. 2016: 1225-1234.
- [54] CAO S, LU W, XU Q. Deep neural networks for learning graph representations[C]//Proceedings of the AAAI Conference on Artificial Intelligence. 2016, 30(1).
- [55] WANG J, CHEN P, YU S, et al. Tsgn: transaction subgraph networks for identifying ethereum phishing accounts[C]//Proceedings of International Conference on Blockchain and Trustworthy Systems. 2021: 187-200.
- [56] 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, 69(5): 2538-2542.
- [57] ZHANG D, CHEN J, LU X. Blockchain phishing scam detection via multi-channel graph classification[C]//Proceedings of International Conference on Blockchain and Trustworthy Systems. 2021: 241-256.
- [58] LI P, XIE Y, XU X, et al. Phishing fraud detection on ethereum using graph neural network[J]. arXiv preprint arXiv: 2204.08194, 2022.
- [59] KANEZASHI H, SUZUMURA T, LIU X, et al. Ethereum fraud detection with heterogeneous graph neural networks[J]. arXiv preprint arXiv:2203.12363, 2022.
- [60] KIPF TN, WELLMING M. Semi-supervised classification with graph convolutional networks[J]. arXiv preprint arXiv:1609.02907, 2016.
- [61] VELIČKOVIĆ P, CUCURULL G, CASANOVA A, et al. Graph attention networks[J]. arXiv preprint arXiv:1710.10903, 2017.
- [62] HAMILTON W, YING Z, LESKOVEC J. Inductive representation learning on large graphs[J]. Advances in Neural Information Processing Systems, 2017, 30.

[作者简介]



蔡召（1998—），男，安徽宿州人，北京交通大学硕士生，主要研究方向为区块链交易网络、网络表示学习。



荆涛（1969—），男，吉林吉林人，北京交通大学教授、博士生导师，主要研究方向为网络与信息安全、人工智能。



任爽（1981—），男，吉林长春人，北京交通大学副教授、博士生导师，主要研究方向为区块链、人工智能。