

区块链欺诈行为识别技术综述

李 广, 陈梓钿, 卞 静, 周杰英, 吴维刚

中山大学 计算机学院 广州 中国 510006

摘要 近年来, 区块链技术和产业的迅速发展为经济和技术创新注入了新的活力, 但随之而来的是不断涌现的欺诈行为。这些欺诈行为不仅对用户造成了经济损失, 也对区块链技术的信誉和发展带来了威胁。因此, 识别和预防欺诈行为对于保障区块链技术和产业创新的良性发展至关重要。另一方面, 区块链欺诈行为变化快、匿名性强, 具有多样性和复杂性, 给识别工作带来了巨大挑战。针对这些挑战, 目前已提出了相当多的技术方法。本文整理归纳了近五年来的相关文献, 清晰呈现区块链欺诈行为识别技术的最新进展。考虑到识别技术的多样性, 本文采用了两层的分类框架对其进行归纳。首先从业务场景出发, 划分出不同类型的欺诈行为, 涉及区块链洗钱、非法代币发行、庞氏骗局和钓鱼诈骗等八种行为。进而, 再针对每一类欺诈行为, 分析讨论对应的识别技术。通过对识别技术解析与归纳, 本文将识别技术从具体场景中抽象出来, 构建出一般化的识别技术体系。并基于这一体系对识别技术展开详细讨论, 包括: 区块链交易图构建技术、特征工程方法以及欺诈行为识别方法与模型。在识别方法上, 本文重点关注了近年流行的区块链去中心化生态下的一些反欺诈识别工作, 包括: 跨链洗钱识别、去中心化平台的代币骗局识别等, 此类欺诈行为具有较高的复杂性和识别难度, 与之相关的识别技术还较少, 亟待得到更多的关注。最后, 本文依据当前区块链欺诈行为识别工作所面临的挑战和困难, 分析了未来技术趋势。

关键词 区块链; 反欺诈; 欺诈识别; 钓鱼识别; 洗钱识别

中图法分类号 TP391 DOI号 10.19363/J.cnki.cn10-1380/tn.2024.07.01

Blockchain Fraud Behaviors Detection Technology: A Survey

LI Guang, CHEN Zitian, BIAN Jing, ZHOU Jieying, WU Weigang

School of Computer Science and Engineering, Sun Yat-Sen University, Guangzhou 510006, China

Abstract In recent years, the rapid development of blockchain technology and industry has engendered fresh vigor for economic and technological innovation. However, this also catalyzed the proliferation of fraudulent practices, which have posed a threat to the technology's reputation and progression as well as brings financial loss to subscribers. As a result, it is crucial to detect and prevent fraud behaviors to safeguard the benign development of blockchain technology and application. On the other hand, blockchain fraud behaviors is anonymous, diverse and complex, which poses enormous challenges to the detection methods, and quite many different approaches have been proposed to address these challenges. This paper summarizes the relevant literature in the past five years, to clearly present the latest progress of blockchain fraud behavior detection technologies. In consideration of the diversity of detection technologies, this paper adopts a two-level classification framework. Firstly, the fraud behaviors are classified into different categories based on business scenarios, involving blockchain money laundering, initial coin offering, Ponzi schemes and phishing scams, and totally eight types behaviors. And then, for each category, the corresponding detection techniques are analyzed and discussed. By analyzing and summarizing, this paper views the detection technologies from specific scenarios and constructs a generalized technical architecture. The detection technologies are discussed in detail based on this architecture, covering blockchain transaction graph construction technologies, feature engineering technologies, fraud behavior detection technologies and models. This paper also discusses the fraud behavior detection efforts in the decentralized ecosystem of blockchain, including cross-chain money laundering, decentralized platform token scam, etc, which has become popular in recent years. These fraud behaviors have high complexity and detection difficulty, and related detection technologies are still lacking, which urgently require more attention. Finally, this paper analyzes the future technology trends based on the challenges and difficulties faced by the current blockchain fraud behavior detection work.

Key words blockchain; Anti-Fraud; fraud detection; money laundering detection; phishing detection

通讯作者: 吴维刚, 教授, 博士生导师, Email: wuweig@mail.sysu.edu.cn.

本课题得到广东省重点领域研发计划项目(No. 2020B0101090005)资助。

收稿日期: 2022-10-17; 修改日期: 2023-02-28; 定稿日期: 2024-04-09

1 引言

区块链被认为是信息领域最具革命性的新兴技术之一,近年来得到了快速发展。区块链技术发源于以比特币为主的数字加密货币,其核心原理是以对等网络为物理基础、以共识机制建立去中心化的信任模型、以密码学技术为身份安全认证三者合为一体的去中心化分布式账本,具有共识信任、不可篡改以及可追溯等突出特性,对金融等诸多行业而言极具颠覆性,具有非常广阔的应用价值。

从区块链应用发展历程看,区块链历经了以数字加密货币为代表的区块链 1.0 形态,以智能合约主导去中心化应用的区块链 2.0 形态,而当前的区块链 3.0 形态正逐渐超越货币、金融的应用范围,与物联网等其他技术相结合,为社会、经济、文化提供价值证明与保障支持。典型的应用场景有数字资产管理^[1-3]、智能电网^[4-5]、供应链溯源^[6-7]等。同时,相关机构也研发了不少区块链系统,如国家工信部支持的星火·链网工业互联网服务平台^①、中国人民银行贸易金融区块链平台^②、央行数字票据交易平台^③等。

在区块链应用蓬勃发展的背后,各种欺诈行为也层出不穷。在已披露的区块链欺诈事件中,以加密货币违法犯罪最为常见,主要包括:洗钱、钓鱼诈骗、庞氏骗局、非法套利、暗网交易、非法代币发行、蜜罐诈骗和勒索软件 8 种。这些区块链欺诈事件所牵扯的资金量通常十分庞大(见表 1),且形式变化多样。具体地,就庞氏骗局这一行为而言,诈骗者善于利用区块链投资热点构造投资骗局,通过变换投资噱头和手段以反复诱骗投资者。在 2019 年 Plustoken 案件中,诈骗者利用刚流行起来的加密货币投资热,以传销手段结合高利润回报的方式运作 Plustoken 虚拟币平台欺诈投资者,吸引了境内外会员逾 300 万人,诈骗金额高达 400 余亿。而在 2020 年数字货币公司 Mirror Trading International 的庞氏骗局事件中,诈骗者则转向更受欢迎的 AI 算法驱动外汇交易为投资噱头,吸收了 26 万会员,涉及资金 5.88 亿美元。另外,在 2021 年 AnubisDAO 庞氏骗局案件中,诈骗者利用其时去中心化稳定币的金融热点,在发行稳定币 ANKH 仅仅 20 h 后,诈骗者就停止了项目,并将项目的流动资金卷走,以“一夜之间卷走 6000 万美元”成为 2021 年最受关注的 Rug Pull

案件。在这些案件中,庞氏骗局的外在形式跟随着区块链产业的发展而变化,即从最初的传统加密货币,到量化投资,再到去中心化金融,我们难以预测下一次它又以何种方式卷土重来,但其高收益陷阱的内在特征是未变化的,而这些内在特征则为提前识别此类欺诈行为,并进一步规避损失提供了技术上的可行性。

区块链反欺诈工作已开始受到越来越多的关注,众多研究者和优秀的加密货币数据分析企业,如:Chainalysis、Elliptic,加入到区块链反欺诈行列中,并为区块链反欺诈社区提供了大量的数据与案例。各国政府与相关监管部门也对区块链生态提出了一系列监管政策,2018 年美国证券交易委员会(Securities and Exchange Commission, SEC)和商品期货交易委员会(Commodity Futures Trading Commission, CFTC)联合发布了《关于对虚拟货币采取措施的联合声明》,监管虚拟货币中可能出现的违规行为。2020 年欧洲委员会(European Committee, EC)公布了区块链监管沙盒计划,计划于 2024 年在欧盟内建立一个全面的监管框架,以便将分布式账本技术(Distributed Ledger Technology, DLT)和加密资产转为受监管的金融工具。2021 年中国七部委联合发布了《关于防范代币发行融资风险的公告》,严格禁止各类代币发行融资活动。这些都为打击区块链生态中的欺诈行为产生了重要作用。

尽管区块链监管需求迫切,但是去中心化、匿名性、开放性、多样性给区块链监管带来了巨大挑战,区块链监管远未形成有效体系。具体地,区块链监管面临着以下技术难题。

(1)变化快。自比特币诞生以来,到以太坊智能合约,再到去中心化金融,区块链欺诈几乎伴随着每一次技术的进步而变化。同时,不同欺诈行为间的标识性特征有的差异极大,当欺诈者改变违法机制后,识别方法很可能失去效用。欺诈行为变化快,使得对识别技术的泛化性要求很高。

(2)匿名性强。专提供匿名性的区块链(如:Zcash)、混币服务、去中心化跨链服务等丰富的匿名服务为欺诈者提供了不同程度的匿名性,由于匿名性问题,如何从海量数据的区块链生态活动中识别出少量的非法活动面临着极大的挑战。

(3)样本少。目前区块链欺诈行为数据主要来源于链下的碎片化社交论坛、市场交易,网络地址等,

① <http://www.bitfactory.cn/>.

② <https://www.safe.gov.cn/shenzhen/2019/1114/593.html>.

③ https://news.ifeng.com/a/20170205/50650776_0.shtml.

表 1 部分区块链欺诈事件
Table 1 Some blockchain fraud behavior events

年份	类型	事件	涉及金额	事件关键字
2018	非法洗钱	Shapeshift 洗钱事件	300 万美元	Cross-Cryptocurrency;
2019	非法洗钱	Binance 被盗资金洗钱事件	4000 万美元	Mixing Service;
2020	非法洗钱	英国毒贩洗钱事件	100 万英镑	OTC;
2021	非法洗钱	Spartan Protocol 事件	3000 万美元	De-Fi;
2021	非法洗钱	Lazarus 黑客洗钱事件	9135 万美元	De-Fi;
2019	庞氏骗局	Plustoken 事件	60 亿美元	Traditional Cryptocurrency;
2020	庞氏骗局	Mirror Trading International 事件	5.88 亿美元	AI Investment;
2021	庞氏骗局	AnubisDAO 事件	6000 万美元	De-Fi;
2018	钓鱼攻击	Coinhoarder 事件	5000 万美元	DNS;
2021	钓鱼攻击	Badger 钓鱼事件	1.5 亿美元	DeFi; ERC-20
2022	钓鱼攻击	OpenSea 钓鱼事件	170 万美元	NFT; MetaVersa
2022	钓鱼攻击	UniSwap V3 空投钓鱼事件	800 万美元	DeFi;

并大多聚焦于加密货币交易,无法支撑通用性的区块链应用,未形成较完备的知识库,不能支持多维高效的反欺诈识别。另外,欺诈行为标注样本少给机器学习类解决方案带来了类别不平衡的问题,这导致机器学习识别模型在实际应用中所能起到的作用受到限制。

(4)验证困难。区块链欺诈在链下取证十分困难,当前区块链反欺诈识别技术大都基于公开的反欺诈数据集、欺诈行为投诉举报、公开披露的案例等内容进行验证,上述取证信息来源只是众多欺诈信息中的冰山一角,识别结果验证困难这一挑战,对反欺诈识别技术提出了极高的可解释性要求。

围绕上述技术难点,区块链反欺诈研究工作近年来得到快速发展,在前期相关研究工作中,主要依据比特币公开的交易记录,人工发现异常交易地址集群并展开对这些集群的去匿名化分析^[8-10]。其后,研究者们开始将机器学习算法引入区块链欺诈行为识别^[11-14],能够自动地识别出区块链中的一些非法实体及其交易模式,但这些算法的识别准确率一定程度上依赖于特征工程的效率,并难以扩展到其他类型的行为识别中。在此问题上,图神经网络技术具备自动聚合并优化特征等特性,当前被广泛用于区块链欺诈行为识别工作中^[12, 15],并在各类欺诈行为上取得了较高的识别准确率,但由于神经网络的弱可解释性,以及欺诈行为在现实世界取证的困难性,使得此类算法的真实性能难以验证。另外,一些研究者还提出了具有通用性的区块链欺诈行为识别算法^[12-13],此类算法并不对特定的行为类别进行识别,而是通过挖掘出行为间的共性特征来识别出可能的欺诈行为,具备更好的扩展性和应用潜力。

近期,一些学者对区块链一般化数据分析^[16]、区

块链特定行为识别技术^[17]进行了综述,但对区块链各类欺诈行为识别技术进行综合全面总结和探讨的综述仍为空白。为此,本文梳理了近5年以来(2017—2022年)的区块链欺诈行为识别工作,考虑其多样性,本文采用了两层的分类框架(见图1)对现有欺诈行为识别方法进行了归纳和分析,首先从业务场景出发,按欺诈行为类型分类,分为区块链非法洗钱行为识别技术、区块链庞氏骗局识别技术、区块链钓鱼行为识别技术和其他欺诈行为识别技术。然后,再针对每一类欺诈行为,根据不同的行为特征与行为场景,分析讨论各场景下的识别技术。

通过对欺诈识别技术方法的归纳梳理,本文将识别技术从具体场景中抽象出来,提取出一套三层的技术体系(见图2),包括:数据层、交易图和特征层以及欺诈行为识别层。数据层涵盖了识别算法中常用到的数据来源,包括链上交易数据与各种链下行为数据。交易图和特征层在数据层的基础上,总结了各种常用的区块链交易信息图以及特征提取方法。欺诈行为识别层则归纳了各类行为的识别方法与模型,以及对一些非法案例的识别分析。基于这一技术体系,本文以交易图和特征层、欺诈行为识别层两个核心技术层的研究现状展开了详细介绍。

内容结构方面,本文第2节介绍了主要的区块链欺诈行为类型;第3节提出了区块链欺诈行为识别技术的分类框架以及三层结构的一般化技术体系;第4节围绕技术体系第二层中的区块链交易图构建,详细介绍了识别技术中常用的交易信息图及其构建过程;第5节介绍了技术体系第二层中的特征工程方法与各类欺诈行为的标识特征;第6节就技术体系中的欺诈行为识别层,分类介绍了各类主要的技术;在第7节和第8节中,给出了区块链欺诈行为识

别工作的未来技术趋势,并总结全文。

2 区块链欺诈行为类型

区块链欺诈行为识别任务很大程度上因行为类型而异,在识别过程中,研究人员首先关注的是欺诈行为类别,因此,在对识别方法进行分析讨论前,需要进一步明确相关的欺诈行为类型。本文将涉及区块链加密货币交易的非法活动共总结为 4 大类型,分别为:非法洗钱、庞氏骗局、钓鱼诈骗和其他欺诈行为。下面具体介绍各类非法活动的特点,并给出相应非法活动的典型案例分析,以助了解区块链欺诈行为识别的研究关键和挑战。

1)非法洗钱

非法洗钱是指将犯罪或其他非法违法行为所获得的违法收入,通过各种手段掩饰、隐瞒、转化,使其在形式上合法化的行为。根据当前已知的洗钱模式,存在 3 种主要的洗钱渠道:(1)通过中心化交易所变现。但这种渠道存在身份暴露风险,因此,出现了一些专门为犯罪分子提供洗钱服务的场外经纪商(Over The Counter, OTC),他们借用自身与交易所的关联为犯罪分子清洗掉污点货币,以避开洗钱者与交易所的直接接触。(2)通过专门的混币服务提供商完成洗钱。混币服务通过聚合分离多笔互不相干的交易,制造一长链的复杂交易以混淆加密货币的来源,而经过混币后的加密货币最终在中心化交易所或 OTC 手中完成变现。(3) NFT、去中心化金融(Decentralised Finance, De-Fi)等新兴去中心化应用平台为洗钱提供了新渠道。首先,以数字藏品为主的 NFT 平台具备无汇率波动、价格易操纵的特性,而这些特性容易被洗钱者利用,比如:拍出天价数字藏品交易来掩盖大额洗钱。其次,DeFi 平台提供的跨链交易服务为洗钱者提供了跨链洗钱的便利性,洗钱者首先在 DeFi 平台上通过质押获取跨链 BTC 或 ETH 代币,再利用两个或两个以上专门进行跨链交易的 DeFi 协议,将资金跳转到以太坊区块链打包转换,换取新的 BTC 和 ETH 变现。

典型案例:混币服务是洗钱的常用手段。在 2019 年加密货币交易所 Binance 遭受的黑客攻击中^①,有 7074 个比特币被盗,价值 4000 万美元。一个月后,盗窃者开始通过加密混币服务 Chipmixer 清洗赃物,在对被盗交易的追踪上,7074 个比特币被转移到了 44 个输出地址,其中 21 个是本地 Segwit 地址,随

后,这 44 个地址的资金又被转移到 7 个地址中,其中 6 个持有 1060.6 个比特币,1 个地址持有 707.1 个比特币。

另外,与交易所关联的场外经纪人也是洗钱的渠道之一。在 2020 年英国曼彻斯特警方查获的毒品案件^②中发现,该贩毒集团将比特币网络作为资金转移系统,采用与场外经纪人合作的方式清洗毒资。该团伙的处理方式是:首先将毒品分销给街头毒贩,在变卖为现金后送回贩毒集团。随后,由快递员收集这些现金,交付到一个经纪人手中,然后由该经纪人负责将这些现金转换为比特币,并发送到贩毒团伙制定的地址上来完成洗钱。对区块链交易记录的追踪表明,共有 100 万英镑的毒资得到清洗。

在 2021 年,去中心化金融领域开始成为洗钱的新渠道。著名的黑客组织 Lazarus 在 2021 年 5 月对加密货币交易所 Liquid 发起了攻击^③,共盗取了 67 个不同 ERC-20 代币以及大量的以太币和比特币。随后,攻击者就利用去中心化协议对这些非法所得进行了清洗,他们首先将所有的 ERC-20 代币通过去中心化交易所转换成以太币,然后利用加密混币服务对这些以太币分散。被混淆的以太币又通过去中心化交易所转换为比特币。经过新一轮的混币,最终转移到法定加密货币交易所的存款地址一一变现,结果表明大约有 9135 万美元被 Lazarus 清洗。

2)庞氏骗局

庞氏骗局是一种金融欺诈手段,经营者将后期参与者的投入兑现给前期参与者,建立起参与者对获取持续回报的信心,在一段时间后终止兑现并将大部分资产占为己有。加密货币平台上的庞氏骗局通常以智能合约的形式呈现,利用其中复杂的程序逻辑以及自动执行的特性,掩盖诈骗意图并阻碍参与者退出。Rug Pull 是近年来在区块链去中心化应用平台上兴起的庞氏骗局代名词,寓意“如果有人成功从你身下拉走地毯——你就跌倒了(他们拿走了你的投资,让你一无所有)”。其通常用于指代加密货币项目的开发人员(通常是新的代币)突然放弃项目,并卷走所有投资资金。比如:在一些去中心化交易所(DEXes)中,项目开发商可以无需代码审计就让新代币上市,这使得创建新代币和启动流动性池十分容易,而持有代币的投资者认为他们的资产受合约保护,但实际上,项目代码存在漏洞且未被审计,这使得开发者有机会盗走投资人全部资金。

① <https://cointelegraph.com/news/bitcoin-stolen-in-binance-hack-moved-to-seven-addresses>.

② <https://www.birminghammail.co.uk/news/midlands-news/nearly-140-years-jail-multi-14543064>.

③ <https://go.chainalysis.com/2022-crypto-crime-report.html>.

典型案例: 2019 年的 Plustoken 案件^①是加密货币领域有史以来造成损失最大的庞氏骗局, 犯罪者以传销手段结合高利润回报的方式运作 Plustoken 虚拟币平台欺诈投资者, 吸引了境内外会员逾 300 万人, 诈骗金额高达 400 余亿, 其崩盘后的巨量套现操作甚至造成了比特币在当年 9 月的价格下跌。

2020 年, 美国联邦调查局牵头对一家位于南非的数字货币公司 Mirror Trading International 展开庞氏诈骗调查^②, 该公司自 2018 年对外宣称使用 AI 算法驱动外汇交易来产生投资收益, 用户只需存入至少价值 100 美元的比特币, 就可以实现 0.5% 的每日回报, 从而转化为 500% 的年收益。至崩盘前, 该公司共吸收了 26 万会员, 涉及资金 5.88 亿美元。

2021 年, AnubisDAO “一夜之间卷走 6000 万美元”成为当年最受关注的 Rug Pull 案件^③, 该项目于 2021 年 10 月 28 日推出, 计划提供一种由一篮子资产支持的去中心化、自由浮动的货币, 并自称是 OlympusDAO (一种去中心化稳定币) 的分支。该项目甚至没有发布网站和白皮书, 有的只是一个 Twitter 账号和一张用于推销用的犬类图像, 但投资者仍然在项目最初的代币销售中投入了 6000 万美元以换取项目发行的 ANKH 代币, 并认为自己找到了下一个 Dogecoin。而项目仅仅在销售 20 h 后, 所有资金就从流动资金池中消失, 转移到了其他地址, 随后, 项目唯一的 Twitter 账号也停用下线, 很快, ANKH 的价值暴跌至 0。

3) 钓鱼诈骗

钓鱼诈骗与传统网络钓鱼窃取用户信息的目的不同, 区块链钓鱼者一般以加密货币为目标, 采取各种手段引诱用户转账。加密货币的用户大部分具有投资倾向, 因此, 伪装成官方网站或官方人物散播有利可图的钓鱼诈骗信息很容易在加密货币平台上得到流行。最常见的包括: 网址克隆、预付款陷阱、代币空投等。除此之外, “冰钓攻击”是近年活跃于智能合约和 DeFi 生态中的一种钓鱼新模式, 它攻击的目标并不是受害者的钱包私钥, 而是试图欺骗受害者签署交易, 从而将用户代币的批准权交给犯罪分子, 一旦批准交易被签署、提交, 攻击者就可以使用这些资金, 进行代币交换。

典型案例: 钓鱼网站和邮件是区块链钓鱼犯罪

者最常用的手段。2018 年, 思科网络安全团队发现了出自乌克兰的 Coinhoarder 犯罪集团在利用 Google Adword 以 blockchien.info 等域名假冒成著名比特币钱包网站 blockchain.info 诱骗投资人^④, 骗取投资人的钱包登录凭证, 从而席卷了价值 5000 万美元的比特币。

此外, 在 2022 年, NFT 平台 OpenSea 遭到了钓鱼诈骗者的邮件攻击^⑤, 该诈骗者假冒 OpenSea 平台, 给 OpenSea 平台用户发送了大量的 opensea-team.io 钓鱼链接, 骗取了价值 170 万美元的 NFT 产品。在冰上钓鱼案件中, 最引人注目的是发生在 2021 年 DeFi 平台 Badger 的入侵事件, 攻击者通过破坏 Badger 前端以获得对 Cloudflare API 密钥的访问, 其定期将恶意脚本注入到 Badger 应用程序中, 这些脚本拦截了 Badger 交易并提示用户允许外国地址对其钱包中的 ERC-20 代币进行操作, 最终, 攻击者从获得批准的用户的钱包中抽走了 1.5 亿美元。

4) 其他欺诈行为

在现有区块链欺诈行为案例中, 还囊括了许多其他的欺诈行为, 但现有的针对这些欺诈行为的研究工作还未形成体系, 因此, 在本文中将其归纳为一类进行考察。根据现有研究工作, 在此类中主要考虑其他 5 种欺诈行为: a) 非法代币发行(Initial Coin Offering, ICO), 是初创公司的募资手段之一, 在推行前公开相应的 ICO 白皮书和网站, 投资者使用法定货币或市场价格相对稳定的其他加密货币, 换取由该公司发行的新型加密货币, 其去中心化以及便捷的特性得到了市场的呼应, 但接近三分之一的新型加密货币在半年内会因发行方的恶意抛售而大幅贬值, 给投资者造成巨大损失。b) 蜜罐诈骗, 是指看似具有漏洞但包含深层陷阱的智能合约, 部署者借此引诱那些认为自己能从中获益的用户。“蜜罐”通常建立在智能合约执行平台一些易受忽视的特性的基础上, 或者利用公共信息的不完备完成。c) 暗网交易, 暗网指必须通过特殊软件、获得特殊授权才能访问的万维网站点, 是 globally 从事非法活动的人员进行沟通、交易的媒介之一。区块链加密货币因其匿名性和便捷性受到这些团体的青睐, 在各个暗网市场中被广泛使用。d) 市场操纵, 加密货币交易价格的巨大波动与相应的套利空间是其受到公众广

① <https://news.cctv.com/2021/04/09/ARTISnSGEG1wmXOVfXOCTyaG210409.shtml>.

② <https://news.bitcoin.com/mirror-trading-international-named-biggest-crypto-scam-of-the-year-after-raking-in-589-million/>.

③ <https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/>.

④ <https://blogs.cisco.com/security/talos/coinhoarder-tracking-a-ukrainian-bitcoin-phishing-ring-dns-style>.

⑤ <https://www.jinse.com/blockchain/1181839.html>.

泛关注的重要原因,这种明显的投机属性为相关利益方进行市场操纵提供了足够的动机。2014 年大型比特币交易所 Mt. Gox 的数据遭受泄露,其中存在的一些市场操纵模式已被验证。e) 勒索软件,是一种传统但威胁极大的网络犯罪行为,受害者因面临重要数据丢失、泄露的风险,不得不向数据的窃取者或加密者支付指定的加密货币。来自 Chainalysis 的分析表明,近年来企业远程办公形式兴起,针对商业数据的勒索行为也随之活跃。

典型案例: 2018 年的 Pincoin ICO^①是众多恶意 ICO 项目之一,其创始人团队由 7 名越南人组成,推出自称为 Pincoin 的 ERC-20 代币,向投资人承诺持续的收益回报,然而,该团队在募集了 6.6 亿美元之后就消失的无影无踪,给超过 32000 名投资者带来了重大经济损失。

在暗网黑市方面,全球最大的暗网黑市 Hydra 在 2022 年的一次多国联合行动中被查封,一并没收了存放在服务器中价值 2500 万美元的比特币。据区块链分析公司 Elliptic 称,Hydra 自 2015 年上线,在短短 7 年内的加密货币交易量就超过了 50 亿美元。

加密货币是现代勒索软件最受青睐的支付渠道,Wannacry^②是 2017 年最令人难忘的勒索软件,攻击

者利用微软 EternalBlue 漏洞在 150 个国家大规模发布勒索软件 Wannacry,受害者需要支付 600 美元的比特币才能关闭软件,否则将被删除电脑数据。据估计,Wannacry 从全球受害者中获得了不少于 40 亿美元的勒索费。

3 分类框架与技术体系

由于识别技术类型比较多,本文采用了一个两层的分类框架(如图 1)对现有识别技术进行归纳整理。在对不同识别技术的整理中可以发现:尽管不同欺诈行为类型在行为特征上可能有相当大的差异,但在技术层面的抽象上,则存在一定的相通性。对此,本文在对识别方法的归纳中,概括提炼出了一套具有一般性的区块链欺诈行为技术体系(如图 2),从而在这一基础上,展开后文对区块链交易图构建技术、特征工程方法以及欺诈行为识别方法与模型的详细介绍。

3.1 识别技术分类框架

本文对现有区块链欺诈行为识别技术的分类方法如图 1 所示。首先按照欺诈行为类型划分,即:区块链非法洗钱行为识别技术、区块链庞氏骗局识别技术、区块链钓鱼行为识别技术和其他欺诈行为识别技术。

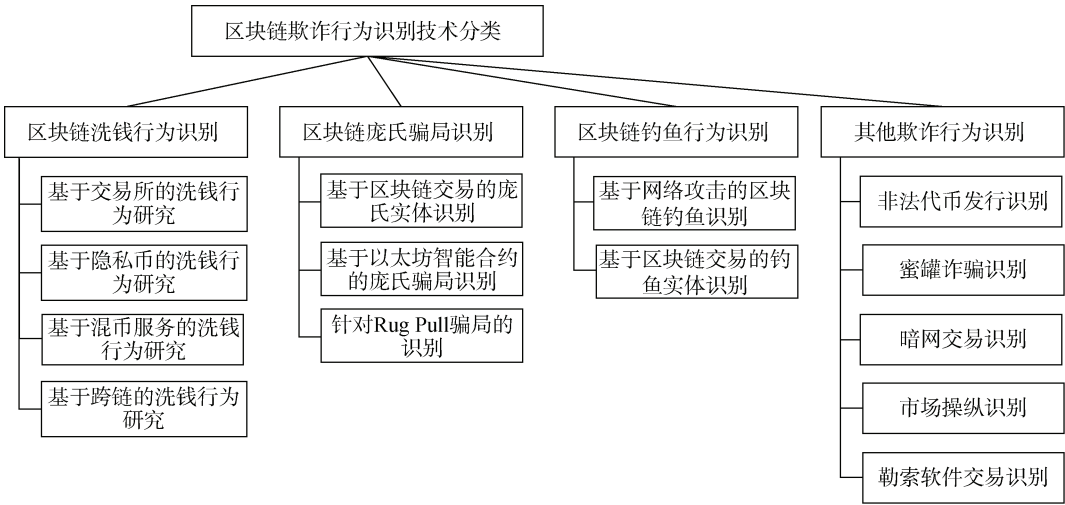


图 1 区块链欺诈行为识别技术分类

Figure 1 Blockchain fraud behavior detection technology classification

每类区块链欺诈行为,根据不同的行为特征与行为场景,细分出不同的技术类型。具体地,根据区块链非法洗钱所涉及的 3 种洗钱渠道:中心化交易所、混币服务和跨链交易服务,将现有区块链洗钱行为识别技术划分为基于交易所的洗钱行为研究、基

于混币服务的洗钱行为研究和基于跨链的洗钱行为研究。根据现有区块链庞氏骗局识别技术所涉及的 3 种类型:庞氏实体(地址/账户)识别、庞氏智能合约识别以及区块链去中心化生态中的代币骗局识别,将现有区块链庞氏骗局识别技术划分为基于区块链交

① <https://www.cryptoground.com/a/660-million-pincoin-ifan-ico-fraud-vietnam>.

② <https://www.malwarebytes.com/wannacry>.

易的庞氏实体识别、基于以太坊智能合约的庞氏骗局识别以及针对 Rug Pull 骗局的识别。根据区块链钓鱼行为所涉及的 2 类方案: 黑客攻击方案和社会工程方案, 将现有区块链钓鱼行为技术划分为基于网络攻击的区块链钓鱼识别、基于区块链交易的钓鱼实体识别。最后, 关于其他欺诈行为识别技术, 则按所包含的区块链 ICO 诈骗、区块链蜜罐诈骗、暗网交易、市场操纵、勒索软件分别介绍。

3.2 识别技术体系

本文根据现有识别方法的归纳, 构建了区块链欺诈行为识别的一般化技术体系, 具体如图 2 所示, 由上至下分别为数据层、交易图与特征层、欺诈行为识别层。

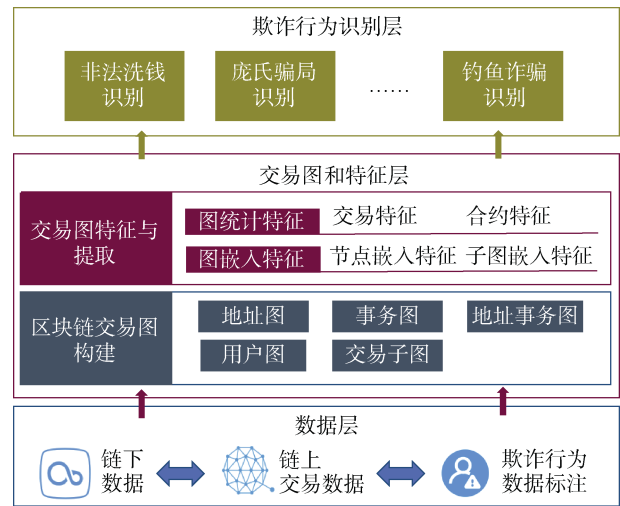


图 2 区块链欺诈行为识别一般化技术体系
Figure 2 Blockchain fraud behavior detection generalized technology architecture

数据层, 区块链交易数据通常以链式或网状结构呈现, 用于描述交易双方间的交易属性与交易关系。数据层总结了当前欺诈行为识别研究使用的数据资料、数据来源, 为识别模型提供数据实例, 主要包括链上交易数据、欺诈行为标注数据、链下行为数据等。本文第 4 节(相关数据资料与来源)对数据层展开了相应介绍。

交易图与特征层, 是在链式交易数据的基础上, 进一步构建出有助于计算的矩阵图结构, 同时, 提取出有利于区块链欺诈行为识别的属性与关系特征。本层总结了欺诈行为识别工作中常用的交易图构建技术与特征提取方法。根据任务目标, 交易数据将被构建成不同类型的图结构, 包括: 地址图、事务

图、地址事务图、实体图、交易子图等。

常用特征主要包括交易特征和合约特征。交易特征通过在构建的交易图上计算图统计特征用于衡量交易节点属性以及发现网络中不同寻常的节点关系, 如: 节点度、中心性、聚类系数等特征, 合约特征则包括在合约代码上提取的字节码特征与抽象的语义特征。同时, 图嵌入技术(如: 图神经网络), 一种聚合特征表示的优化方法, 可用更低维的向量保留尽可能多的图结构信息和潜在特性, 被广泛应用于当前的识别工作, 从而纳入此层特征提取方法中。最终, 这些特征将作为识别模型的重要推断依据。本文第 5 节(区块链交易图构建)和第 6 节(交易图特征与提取技术)分别对本层的区块链交易图、交易图特征展开了相应介绍。

欺诈行为识别层, 是在特征提取完成后, 进一步形成自动化识别区块链欺诈行为的模型或启发式算法。在此层中, 受到不同欺诈行为类型的影响, 如: 非法洗钱的识别通常与混币服务交易有关, 而庞氏骗局的识别通常源自对智能合约的分析, 针对这些行为所形成的识别模型与算法通常只针对某一特定的或某一类相似的欺诈行为。最终, 所建立的欺诈行为识别模型将在实验数据集以及掌握的欺诈行为案例中验证方法有效性。本文第 7 节(欺诈行为识别技术)对本层展开了相应介绍。

4 数据来源与数据集

数据是区块链欺诈行为识别工作的基座, 下游识别方法需要针对不同的识别目标而综合考虑各种数据来源。但与此相关的数据来源种类多、数据质量不一, 同时有标注的样本少。如何获取需要的数据, 以及基于哪些数据构建目标模型, 通常是识别任务的难点。为此, 本节总结了有关数据来源以方便了解到各类数据的获取。同时, 本节从模型构建的数据策略上, 提供了相应的公开数据集作为参考。

4.1 数据来源

本文依据数据功能将已知的数据来源分类为: 1)链上交易数据, 2)链下行为数据, 3)欺诈行为标注数据, 其中 1)和 2)的数据来源被默认为无标注。

1)链上交易数据。指经认证上链后的区块链交易详情数据、部署在链上的合约及其日志数据。可通过区块链客户端完成数据同步后解析获取, 常见的区块链客户端如 Bitcoin-core^①(比特币)、Geth^②(以太

① <https://bitcoin.org/en/bitcoin-core/>.
② <https://geth.ethereum.org/>.

坊)。也可通过一些区块链浏览器查询和下载, 常见的包括 Blockchain^①、Etherscan^②等。

2)链下行为数据。用于指代发生在链下(通常是 Web), 且包含区块链欺诈行为线索的数据。在现有工作中, 此类数据来源包括: a. 社交网站, 如比特币论坛^③、推特, b. 白皮书发布网站, 如 Icobench^④, c. 交易所买卖数据, 如 Bitfinex^⑤、Mt.Gox^[24], d. 区块链交易 IP 数据^[56]等。

3)欺诈行为标注数据。是经由投诉举报、案件披露、互联网收集、人工验证等方式对区块链账户、交易、合约标注的各类数据。其来源包括 a. 区块链非法地址披露网站, 如 Etherscan、Cryptoscamdb^⑥, b. 实体身份披露网站, 如 Walletexplorer^⑦、Ethonym^⑧, c. 相关的公开数据集(见 4.2)等。

4.2 公开数据集

表 2 整理了已知的公开数据集。依据现有识别方法, 其数据策略被大体分为两类。

1)基于交易。即研究者主要从区块链交易记录中理解交易双方的行为逻辑, 找出目标行为的交易特性, 从而挖掘识别出属于目标行为的交易、账户、合约。表 2 基于交易策略的数据集覆盖的行为包括洗钱^[12, 18]、钓鱼^[19]、庞氏骗局^[20]、勒索软件^[25]。

2)基于合约。合约中的代码逻辑提供了欺诈行为良好的识别基础和可验证性。预先检测和发现合约代码中的漏洞或陷阱, 可以为区块链用户起到预警作用。研究者可以从合约的代码语义特征(如字节码特征)、合约代码执行路径等方面, 构建出目标行为的识别模型。表 2 基于合约策略的数据集覆盖的行为包括庞氏骗局^[21-22]和蜜罐诈骗^[23]。

5 区块链交易图构建

区块链交易图构建技术是基于第 4 节区块链交易数据构建具有拓扑逻辑的图网络, 不同的图网络被用于表征不同的区块链实体间的关联关系。同时, 相关的标注数据以及链下行为特征可以作为节点属性或边属性引入对应的交易图中。因此, 在构建识别模型前选择合适的交易图结构是分析工作的重点。

本节将基于当前最普遍的两种交易模型上, 介绍 5 种交易图构建方法。

表 2 相关的公开数据集
Table 2 Related open datasets

数据策略	公开数据集	总地址/合约数	非法地址/合约数
基于交易	Elliptic ^[12]	203769	4545
	BitcoinMixing ^[18]	12360	---
	Xblock-Phishing ^[19]	2973382	1157
	Bitcoin-Ponzi ^[20]	32	32
	Btcransomware ^[25]	4027	---
基于合约	Contract-Ponzi ^[21]	1382	131
	SADPonzi ^[22]	1528	133
	HoneyBadger ^[23]	857	323

5.1 交易模型

交易模型是各交易信息图构建的底层逻辑。在众多区块链平台中存在两种主流交易模型, 一是以比特币为代表的 UTXO 交易模型, 类似于现实中的找零交易模式。另一种是以太坊为代表的账户交易模型, 类似于现实中的银行账户交易模式。

1)UTXO 交易模型

在比特币中, 交易账户由账户所控制的地址所表示, 如 1CtvVyedKeeqNqibLf4dWYHeZREn53SsnAo。地址可以是一次性的, 因此, 同一账户通常控制着多个地址。比特币交易由若干个转出(输入)账户和若干个接收(输出)账户完成。比特币交易的记账模式使用未花费交易输出(unspent transaction output, UTXO)模型, UTXO 模型类似于购买物品后收到的找零。如果转账的金额小于输入地址的总额, 比特币将自动生成一个找零地址接收余额并用于下一次交易。因此, 每笔交易的输入地址总是来源于上次交易的未消费完的余额地址或出块奖励(coinbase 交易)地址。

图 3 为一个比特币交易图示例, 在交易(T_x)中, 包含了 2 个输入地址(a_1 、 a_2), 3 个输出地址(a_3 、 a_4 、 a_5), 其中 a_5 为找零地址。在该交易图中, 以地址为节点, 地址间的交易连接成边, 边上的权重表示转移的金额。在此交易中, (a_1 、 a_2)作为交易的输入地址, 共转出了 12 个比特币, a_3 、 a_4 作为接收地址, 共接收

① <https://www.blockchain.com/>.
② <https://etherscan.io/>.
③ <https://bitcointalk.org/>.
④ <https://icobench.com>.
⑤ <https://github.com/Nucs/cryptocurrency-ticks-data>.
⑥ <https://cryptoscamdb.org/scams>.
⑦ <https://www.walletexplorer.com/>.
⑧ <https://ethonym.com/>.

了 11 个比特币, 扣除掉 0.2 个比特币的手续费后, 剩余的 0.8 个比特币由找零地址 a_5 接收作为未花费交易可用于下一次交易中。通常, 在比特币交易中, 由于交易的完成都需要交易输入方确认并用私钥签名, 在私钥不泄露的前提下, 会将交易的输入地址都视为由同一实体控制(多输入地址识别), 即: 在图 3 中, a_1 、 a_2 被视为同一实体。另外, 比特币交易的手续费通常是非整数、长度较长且数额较小的一串数字金额, 这导致输入地址所转出的金额不会恰好满足接收方所需要的金额与交易手续费, 从而产生找零地址。找零地址的金额同样也是非整数且长度较长的一串数字, 具有较强的辨识度, 该找零地址与输入方视为由同一实体控制(找零地址识别), 并参与到下一次交易中, 即: 在图 3 中, a_1 、 a_2 、 a_5 被视为同一实体。

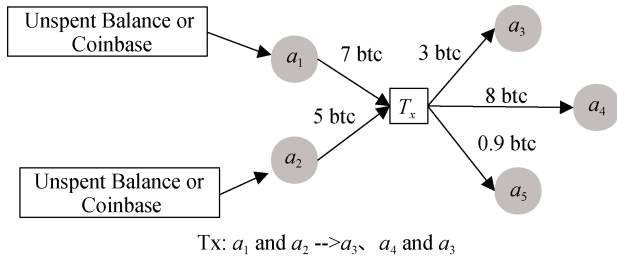


图 3 比特币交易图

Figure 3 Bitcoin transaction graph

2) 账户交易模型

以太坊是一个图灵完备的区块链智能合约平台,

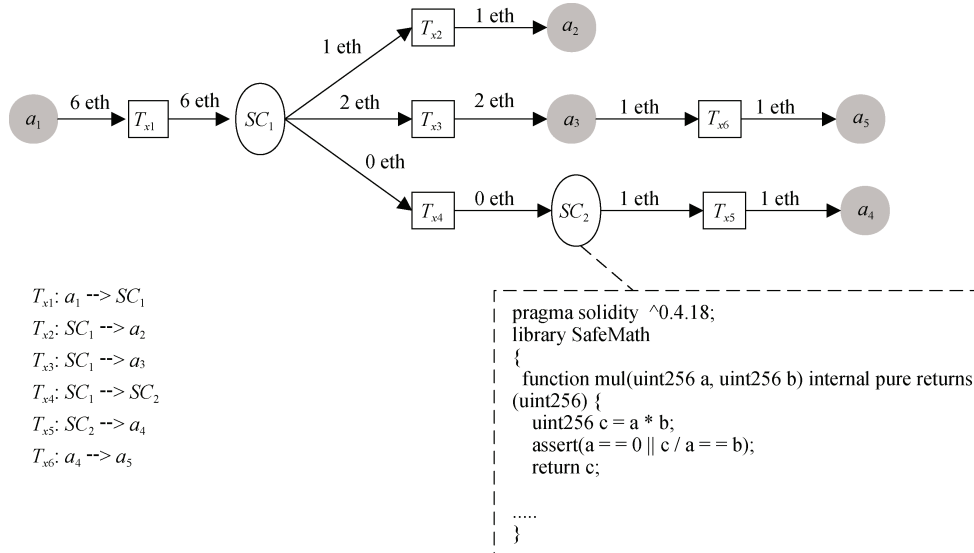


图 4 以太坊交易图

Figure 4 Ethereum transaction graph

5.2 交易信息图构建

现有欺诈行为识别技术中常见的交易信息图包括: 地址图、事务图、地址事务图、用户图、交

智能合约是存储在区块链上的程序, 由各区块链节点执行, 一旦满足合约的触发条件, 预定义的交易逻辑能够自主执行, 执行后的结果上链不可更改^[26]。与比特币不同, 以太坊的记账模式采用与银行记账类似的账户交易模型(账户直接存储余额)。在以太坊中, 存在 2 类账户: 1) 外部账户, 是由人们通过私钥创建的账户, 与比特币系统的账户概念类似, 记录了账户的余额等信息。2) 合约账户, 记录了智能合约的可执行代码, 由外部账户或合约账户建立, 在创建时被自动分配到一个账户地址。合约代码能够被外部账户或者其他合约账户所调用。因此, 以太坊交易不仅发生在外部账户与外部账户之间, 还包括了大量外部账户与合约账户、合约账户与合约账户的交易。另外, 以太坊交易手续费以执行交易消耗的 gas 总额来衡量。以太坊操作指令有着事先规定的 gas 消耗量, 以太坊交易会被拆分为多条操作指令来完成。在一笔交易中, 由用户给定 gas 的单价(如: 4×10^{-8} eth), 交易手续费最终由交易的 gas 消耗量乘上 gas 单价所决定。

图 4 是一个以太坊交易图示例, 共包含 6 笔交易, 每笔交易都是一对一转账。合约账户记录了可执行代码(如 SC_2), 交易可发生在任意的外部账户或合约账户之间, 如: 交易 T_{x1} 发生在外部账户 a_1 与合约账户 SC_1 , 交易 T_{x4} 记录了合约账户 SC_1 调用合约账户 SC_2 的过程, T_{x6} 记录了外部账户 a_3 与外部账户 a_5 之间的交易。

易子图。

地址图用于描述数字货币在地址间的交互信息。常被用作行为识别的初始图, 具有逻辑简单、易

于构造的优点,但地址图通常消耗存储资源大,并不利于大规模交易下的行为识别。

事务图用于表示数字货币在事务间随时间的流动状态。以事务哈希为节点,表达的交易逻辑更简洁,所占资源更少。

地址事务图同时包含了事务和地址信息,具有更丰富的交易信息。

用户图用于表示数字货币在区块链用户之间的流动情况。采用实体聚类的方式在地址图上形成聚群的行为抽象,常被用于识别用户间的行为模式,具有更强的行为逻辑,但其效果通常依赖于实体聚类的性能。

交易子图是交易全图的局部图,被用于在交易图中过滤特定的行为模式。在现有识别方法中常见的交易子图包括 N -ego、 K -motifs 两种。

图 5 描述了各交易信息图间的关系。其中地址图与事务图为最基本的交易信息图,为地址事务图提供地址和事务间的关系信息。交易子图是在交易关系上对交易模式的抽象,主要是从地址事务图抽取基础图元信息获得。用户图是利用地址事务图提供的内在实体逻辑,在匿名化交易上对用户实体的抽象。

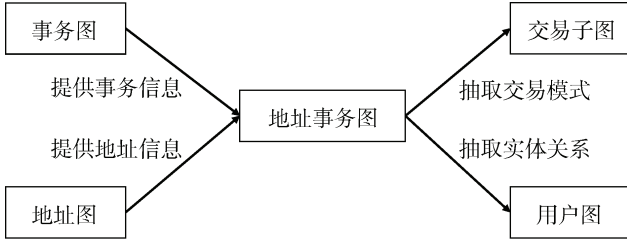


图 5 各交易信息图关系

Figure 5 Relationship of each transaction information graph

1)地址图构建

地址图 $G=(A, E)$ 用于表示数字货币在地址间的交互模式, $A=\{a_1, a_2, \dots, a_n\}$ 为图 G 的顶点集合, $E=\{e_1, e_2, \dots, e_n\}$ 为边集合。每个顶点 a 表示区块链的一个账户地址, 顶点间的有向边 e 代表交易在地址间的流动方向, 交易金额通常作为边的权重。一个典型 UTXO 模型的地址图的构建如图 6 所示。灰色顶点用于表示顶点集合 A 中的账户地址, 灰色有向边用于表示账户地址间的交易关系, 即: 边 e , 图 6 的右下角记录了该地址图所包含的 5 笔交易, 该地址图 G 的顶点集合 $A=\{a_1, a_2, \dots, a_{12}\}$, 共 12 个顶点。边集合 $E=\{e_1, e_2, \dots, e_{12}\}$, 共 12 条有向交易边, 边上

的权重记录了每笔交易的金额。

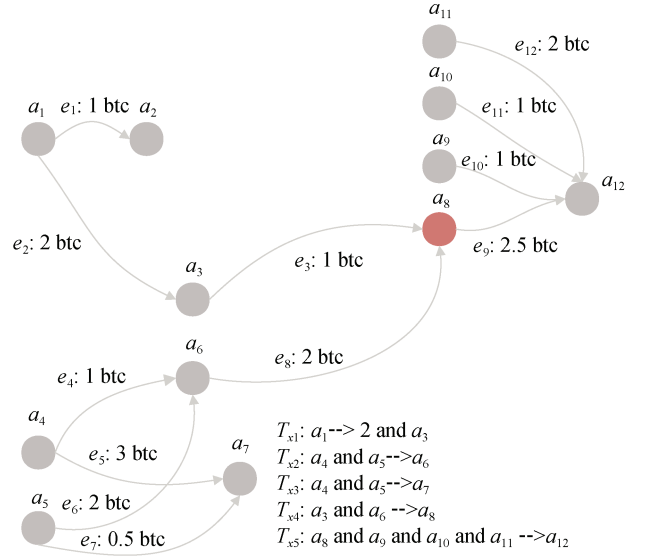


图 6 地址图构建

Figure 6 Address graph construction

地址图有效地表达了区块链最基本的交易逻辑。如: 在交易 T_{x1} 中, 地址 a_1 向地址 a_2 转移了 1 个比特币, 向 a_3 转移了 2 个比特币。地址图的构建方法在逻辑上十分简单,但在多输入输出的 UTXO 模型中,大量的交易记录会使得地址图纷繁复杂,而并不利于分析交易后的实体行为。因此,地址图通常作为区块链欺诈行为识别技术的初始图,并在地址图的基础上,进一步构建出更具行为逻辑的实体图或地址-事务图等。

2)事务图构建

事务图 $G=(T, E)$ 用于表示数字货币在事务间随时间的流动状态。 $T=\{t_1, t_2, \dots, t_n\}$ 为图 G 的顶点集合, 每个顶点 t 代表一个区块链事务, 使用事务哈希 (Transaction Hash) 标识, 如: 一项比特币的事务以哈希 18eac872ba70f10daf6ec0938d01884e24a8a5fca3be09055e1d1c637e3a623d 标识。 $E=\{e_1, e_2, \dots, e_n\}$ 为图 G 的有向边集合, 有向边 e 用于连接输入顶点所来源的事务与输出顶点所去向的事务, 事务间流入流出的金额可作为边 e 的权重。

图 7 是在图 6 交易上构建事务图的过程。右下角记录了 5 笔事务的输入输出情况, 图右侧的黑色方框用于表示一项事务, 并以哈希值标识, 黑色有向边用于连接输入事务与输出事务。构建过程如下, 以事务 T_{x4} 为起始点, 首先, T_{x4} 的输入地址 a_3 来源于事务 T_{x1} , 输入地址 a_6 来源于事务 T_{x2} , T_{x4} 的输出地址 a_8 参与到了下一事务 T_{x5} 。 T_{x1} 、 T_{x2} 作为 T_{x4} 的输入顶点, T_{x5} 则作为 T_{x4} 的输出顶点, 形成了一个事务有向

图。各边 e 的权重情况: 账户地址 a_3 输入了 1 个比特币到 T_{x4} 中(e_1 : 1 btc), a_6 输入了 2 个比特币到 T_{x4} 中(e_2 : 2 btc), 共转出了 2.5 个比特币到 a_8 (e_4 : 2.5 btc), 所以, 最终形成的事务图(以 T_{x4} 为中心的一阶事务图)如图 7 右侧所示。

事务图不存在多重边, 即: 一项事务到另一项事务最多只存在一条边。另外, 由于事务具有唯一性, 事务的输出永远不能作为自身的输入。因此, 事务图不存在自循环, 事务图 G 是一种有向无环图(DAG)。时间区段通常是区块链欺诈行为识别技术构建事务

图的重要参照, 为了聚焦于特定事件的时间区间。譬如以著名的暗网组织——丝绸之路, 被关闭前的 7 个月(2013.03~2013.10)作为时间区段构建比特币事务图, 来重点研究该暗网组织与其他实体(bitcointalker 论坛用户)的关联关系^[8]。另一项事务图的构建方式则是聚焦于目标账户的全生命周期, 以目标账户地址(赌博、勒索软件账户)所参与的最后一项事务为起始点, 逐次地向前迭代, 直到该地址所参与的第一个事务(创世块或 coinbase 交易), 构建比特币事务图, 以研究此类账户的行为特征^[27]。

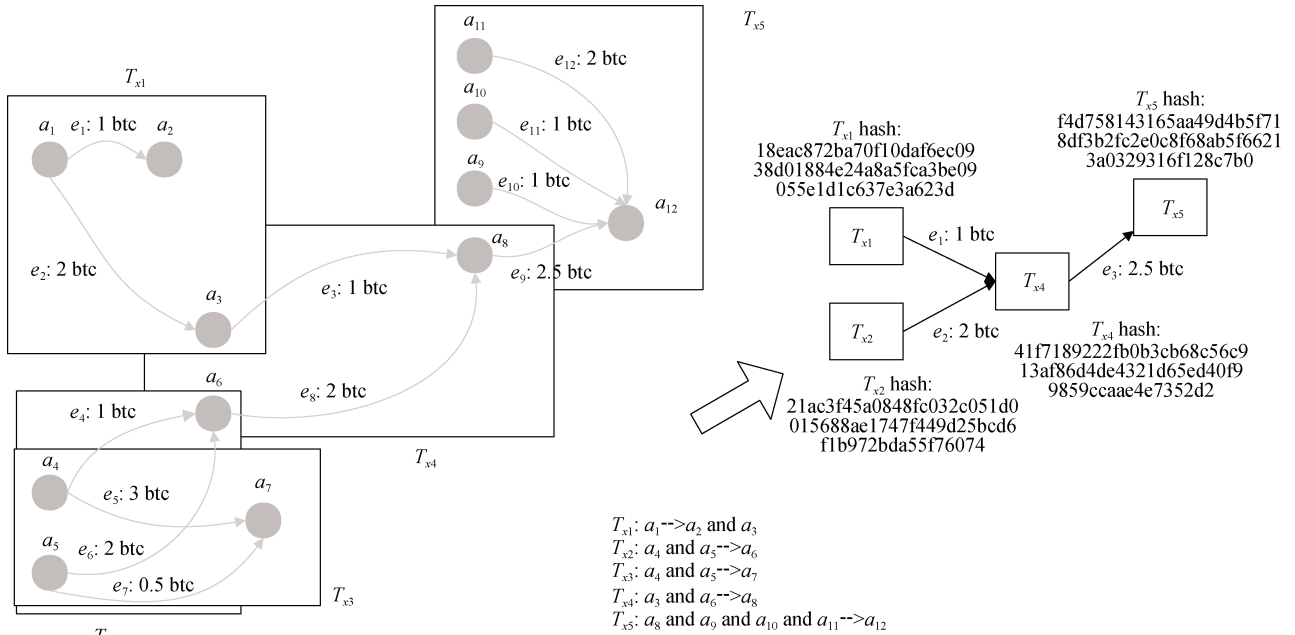


图 7 事务图构建

Figure 7 Transaction graph construction

3) 地址事务图构建

地址事务图 $G=(T, A, E)$ 是将地址引入上述事务图中, 可以看作是事务图的展开形式, 用于描述地址与事务间的二元关系。 G 是一种异构图, 包含两种类型的节点: $T=\{t_1, t_2, \dots, t_n\}$ 和 $A=\{a_1, a_2, \dots, a_n\}$ 。 T 为事务节点集合, 每个节点 t 代表一个区块链事务, t 使用事务哈希标识。 A 为图 G 的地址节点集合, 每个节点 a 代表一个区块链地址。 $E=\{e_1, e_2, \dots, e_n\}$ 为图 G 的有向边集合, 有向边 e 用于连接事务与输入地址、事务与输出地址, 边 e 两端总是一个事务节点和一个地址节点, 边 e 上的权重可以是输入地址的转入金额以及输出地址收到的交易金额。如图 8 所示, 地址事务图在图 7 事务图、图 6 地址图的基础上, 将事务 T_x 相关的输入地址输出地址嵌入到图中, 形成地址事务图, 易于理解, 本文将不再赘述。地址事务图相较于地址图与事务图, 表达了更清晰的地址与事

务间的逻辑关系, 如在图 8 中, 地址 a_1 在事务 T_{x1} 中, 转出了 3 个比特币, 其中 1 个比特币发送到了 a_2 , 2 个比特币发送到了 a_3 。相较于地址图 6, 地址事务图 8 用更简洁的拓扑形式表达出了更多的事务信息, 相较于事务图 7, 地址事务图则具备了更丰富的地址交易关系。

4) 用户图构建

用户图 $G=(U, E)$ 用于表示数字货币在区块链用户之间的流动情况, $U=[U_1, U_2, \dots, U_n]$ 为图 G 的用户节点集合, $E=\{e_1, e_2, \dots, e_n\}$ 为边集合, 每个顶点 u 表示区块链的一个用户。这里的用户通常是从区块链地址中采用一些聚类或去匿名化方法抽象出来的, 如 UTXO 模型中的多输入节点和找零节点被识别为同一用户控制(见 2.1 节比特币 UTXO 交易模型)。顶点间的有向边 e 代表交易在用户间的流动方向, 用户间交易的总金额通常作为边的权重。一个典型 UTXO

在用户图的构建中,关键在于对区块链用户的抽象过程,即:地址聚类。通过多输入地址识别、找零地址识别(见 2.1 比特币 UTXO 交易模型)抽象出比特币钱包用户是现有区块链欺诈行为识别技术常用的规则^[8, 28-29]。这一规则在图拓扑上的体现是:图的每个最大连通分量对应于一个用户。但这一规则存在缺陷, Dalal^[27]指出,将这种启发式规则应用到整个比特币区块链时,将得到一个包含 90% 以上地址的超级集群,这其中大多数是由于混币服务造成的,这些服务通过将不同用户的交易结合再打散,以保持交易的匿名性,这导致了上述启发式规则在地址聚类上出现错误。针对这一问题, Dalal 提出:在一定时间窗口内对比特币交易采用局部聚类的方式来获取用户图,可以有效解决这种大集群效应。

5) 交易子图: N -ego 图和 K -motifs 图构建

子图 $G'=(V', E')$, 顾名思义, 是区块链交易全图 G 的局部图, 常被区块链欺诈行为识别技术用于探

索欺诈行为的特征模式。通常, 在交易图中频繁出现的子拓扑结构, 被认为是特定的行为所呈现出来的, 例如: 区块链交易图中形成的自循环、三角结构被认为是与洗钱行为相关^[30]。在子图构建技术中, 最常见的包括有: N -ego 图构建技术与 K -motifs 图构建技术。

子图的构建通常围绕一个中心节点完成。考虑一个无向的 N 阶 ego 图, 一种简单的构建方式是忽略交易的方向, 由该中心节点及其 N 阶交易的邻居节点所形成的子图, 就是该节点的 N -ego。如图 10 是一个无向 1-ego 图构建的过程, 图中 a_8 节点为中心节点(中心节点可以往任意一个节点迭代), 将 a_8 节点的 1 阶邻域所形成的子图, 再去除掉交易方向后, 形成图 10 右侧的 1-ego 图。另外, 有一种简化版的 N 阶 ego 图^[8], 加入了对子图的多重边合并、自循环消除等处理, 可以得到一个简洁子图拓扑, 从而更直观的观察到欺诈行为节点与其同谋、受害者、其他邻居节点的关系。

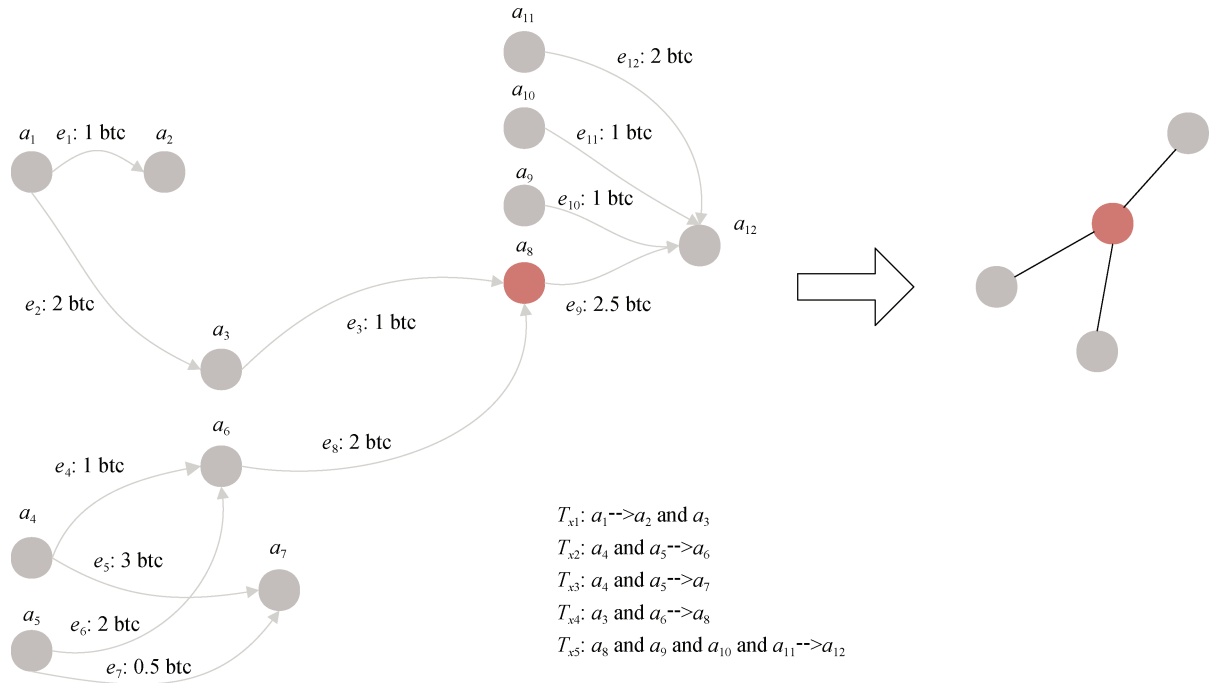


图 10 1-ego 图构建

Figure 10 1-ego graph construction

类似于 N -ego 图, K -motifs 图是包含了 k 条有向边的子图结构。图 11 为地址事务图中提取出的有向 2-motifs 结构, 每个顶点可能是地址节点, 也可能是事务节点, 每条有向边连接了地址与事务的关系。有向 2-motifs 包含了两种类型的边: tail(T)边和 head(H)边。一共可组合成 4 种子交易模式: A、A'、B、C(见图 11 左侧)。具体的, 图 11 的右侧是这 4 种交易模式对应到地址事务图中的情况。所有的交易关系均

可由这 4 种 2-motif 子图连接构成。在 A 模式中, 当 T 边与 H 边所指向的节点集合存在交集时, 将会形成特殊的环状交易模式。在现有的区块链欺诈行为识别技术中, 一种特殊的 2-motifs 模块短粗带^[30](Short Thick Band, STB)被用于挖掘区块链交易所中潜在的洗钱模式, 它通过在 2-motifs 覆盖节点中交易所地址的排布来定义, 分为线性 STB 块和循环 STB 块, 线性 STB 块表示比特币从一个交易所移到另一个交易所

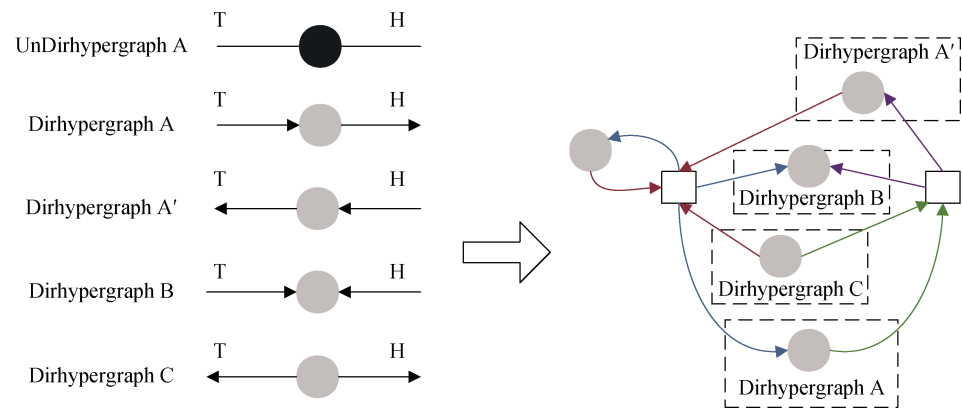


图 11 2-motifs 图构建
Figure 11 2-motifs graph construction

所的模式, 循环 STB 块表示比特币转出又转回到原交易所的模式。在对洗钱行为的研究中发现^[30], STB 模块表现出了比普通 2-motifs 更强的过滤性。

6 交易图特征与提取技术

在交易图结构上建立良好特征工程是下游区块链欺诈识别算法必不可少的一步。本节将介绍现有区块链反欺诈识别技术中, 两种常用的特征工程方法: 图统计特征(属性特征)方法和嵌入特征方法。

6.1 图统计特征

图统计特征是在图的拓扑结构上, 统计出图/节点的拓扑属性和行为指标, 比如节点度、边权重、邻

节点数等, 用于特征化某个图/节点的状态。区块链欺诈行为识别技术中的图统计特征, 引入了更多的交易属性和交易行为指标, 如地址活跃天数、交易周期、发送地址数等。具体地, 表 3 整理了现有区块链欺诈行为识别技术中常用的图统计特征, 按不同级别划分, 共包括 4 种类型特征: 事务(Transaction)节点特征、地址/账户(Address/Account)节点特征、合约(Contract)特征以及子图(Sub-graph)特征。其中, 属性特征是对区块链交易图节点的基本状态的概括, 包括交易属性特征与一般的图属性特征。系数统计特征, 是对节点在中心性、聚类性等系数上的统计, 用于衡量节点在整个交易图中的重要性程度。在这些

表 3 常用的区块链交易特征与合约特征
Table 3 Popular blockchain transaction and contract features

特征类型	Level	特征
交易特征	Address/Account Level	属性统计: 地址生命周期、地址活跃天数、地址参与的总事务数、地址接收事务总数、每周交易的地址数、地址接收与转出交易的最小时间间隔、地址交易平均时间间隔、接收事务的平均间隔、转出交易的平均间隔、地址总交易额、余额、总接收金额、总转出金额、平均接收金额、平均转出金额、接收金额标准差、转出金额标准差、地址连续两天的最大余额差额、地址日最大交易量、转移到地址的不同地址数、地址节点入度、地址节点出度、父子节点个数、既是父节点又是子节点的个数、输出中兄弟节点的个数。 系数统计: 中心性系数、PageRank、聚类系数、Gini 系数。
	Transaction Level	属性统计: 事务时间、事务输入地址数量、事务输出地址数量、输入输出地址数量比例、交易手续费、事务转出金额(sum/mean/std)。
	Actor Level	属性统计: 余额、每天的交易量、连接 coinbase 交易的比例、不同交易量的频率、转出交易中输入和输出的平均地址数量、活跃时间、接收总金额、转出总金额、交易对应时刻的美元总额、按时间窗口计算的交易金额(mean/std/skewness/Kurtosis)、作为接收方的事务总数、作为转出方的事务总数、用于发送和转出的地址总数。
	Sub-graph Level	属性统计: 节点数、边数、交易总金额、接收事务数量、转出事务数量、唯一地址数、作为输入的地址数、作为输出的地址数、交易手续费、存在循环数量、平均邻接度、叶子节点占比平均。 系数统计: 聚类系数、网络密度、平均 betweenness 中心性、平均 closeness 中心性、邻接矩阵最大特征值。
	Bytecode Level	属性特征: 合约余额、付款数量、付款给参与者最大金额、合约特征: JUMPI 和 JUMP 操作码比例、TIMESTAMP 操作码数量。
合约特征	Semantics Level	----

图统计特征中, 区块链欺诈实体所涉及的交易对象、交易金额和交易频率等特征属性, 可能与常规交易大相径庭, 比如: 与洗钱相关的交易在交易图中体现的弱连通分量上有别于常规交易甚至是一些混币服务交易。另外, 常规交易更倾向于跟其强关联的地址进行交易^[31]。

不同区块链欺诈行为的标识特征的差异也可能非常大。比如: 在与暗网相关的区块链交易中, 交易手续费是这类交易的标识特征, 因为暗网交易者会希望交易更快地得到确认, 通常会将手续费设置的更高, 使得矿工优先确认这笔交易。而与勒索软件相关的区块链交易中, 交易金额是此类交易的标识特征, 这是由于勒索软件设定的勒索金额固定, 勒索者地址通常会在一段时间内接收到大量从受害者发送过来的相同交易金额的区块链交易^[32]。表 4 是根据现有区块链欺诈行为识别技术中所披露的特征及其特征重要次序, 整理了不同欺诈类别所对应的标识特征。可以发现, 一些不同区块链欺诈类型, 如: 非法 ICO 和区块链庞氏骗局, 其标识性特征差异非常大, 这也是本文按不同欺诈类别对区块链欺诈行为识别技术分类的原因之一。相反的, 也存在标识特征相似的区块链欺诈行为, 如: 区块链非法洗钱与非法套利, 二者在重要的标识特征上都包括了输入输出比例、输出金额等特征。

6.2 图嵌入技术

图嵌入技术是近年来流行的图表征方法, 其将原始图数据转换到低维空间并保留关键信息, 从而提升节点分类、关系预测、节点聚类下游任务的性能^[33]。在对图节点的特征表示上, 图嵌入技术在节点的领域上聚合更新节点信息, 从而迭代优化对图节点的表征能力^[11]。

图嵌入技术按嵌入类型可大致分为节点嵌入和全图嵌入两种。二者的区别在于: 节点嵌入是学习到一个节点的表征, 如: 学习一个社交用户节点的表征, 常被用于节点分类、节点聚类任务; 而全图嵌入则是学习到对整个图的表征, 如: 学习对分子结构的表征, 被用于图分类、图聚类等任务。嵌入技术的基本原理是学习一个编码器, 将图(节点)映射到低维的嵌入空间中, 并且在嵌入空间中能有着与原图中相似的特性^[32]。图嵌入技术具备自我学习能力, 通常是半监督或无监督的, 这是图嵌入技术的一大优势。由于图嵌入技术并非本文的重点, 感兴趣的读者可参阅图嵌入模型综述^[33-34]。

表 5 整理了近年来区块链欺诈行为识别技术中常用的图嵌入技术。采用的节点嵌入是使用嵌入方

法学习到对各类图节点(实体)的表征, 用于对下游非法节点分类的任务中。节点类别主要包括非法节点与正常节点。因此, 在正常节点嵌入特征和非法节点嵌入特征之间是否具有强辨识度(通常以下游的分类性能表示)是对嵌入方法性能好坏的一种衡量。一种子图嵌入方法^[35]是围绕着中心节点构建出领域子图, 然后使用图嵌入技术学习对此子图进行表征, 最后将区块链欺诈行为识别作为一种图分类任务完成。

表 4 不同区块链欺诈行为的标识特征
Table 4 Identity features of different blockchain fraud behaviors

区块链欺诈行为类别	图统计特征
区块链非法洗钱	输入输出比例、输出金额(sum/mean/std)、弱连通分量数 ^[3] 、兄弟节点交易、子节点交易、父节点交易 ^[1] 。 输出金额的 gini 系数、输入交易量/总交易量之比、输出金额(mean/std)、转移到地址的不同地址数、地址的生命周期和活跃天数 ^[5] ; 智能合约
区块链庞氏骗局	JUMPI 和 JUMP 操作码比例; 智能合约 TIMESTAMP 操作码数量; 收款方在付款前已投资的比例 ^[6] ; 接收/转出事务量、合约最大交易额、合约生命周期 ^[4] 。
区块链非法 ICO	ICO 白皮书文字特征、团队简历特征、web 内容特征、github README 特征 ^[26] 。 接收转出事务块号标准差、转出事务金额中位数和标准差、接收事务金额最小值、输入唯一地址数、接收事务中唯一地址比例 ^[30] 、首末次交易时间戳、输入地址交易数量、接收地址的交易数量、地址交易总数、花费的以太币总额、失败交易总数、输入输出使用的 gas、输出交易占百分比、接收交易平均时差、地址活跃时长、输出接收以太币平均值、接收交易占百分比、交易平均时差、首次交易额、花费以太币总额。
区块链钓鱼诈骗	合约代码行数、编译器补丁版本号、交易额均值/标准差、gas 花费、合约创始者的存款频率 ^[13] 。
区块链蜜罐诈骗	不同量级交易图对应的奇异值分解特征 ^[33] 。
市场操纵	时间、交易金额 ^[34] 、聚类系数、紧密中心性、Coreness ^[35] 。
勒索软件	交易手续费、地址接收与转出交易的最小时间差、花费的平均金额、接收交易的频率 ^[32] 。
暗网交易	

表 5 区块链欺诈行为识别技术中常用的图嵌入技术
Table 5 Graph embedding techniques commonly used in blockchain fraud behavior detection technology

类型	嵌入方法
节点嵌入	node2vec ^[31] 、random walk ^[13, 19] 、deepwalk ^[31] 、skip-gram ^[36] 、GCN ^[12] 、EveloveGCN ^[12] 、Autoencoding ^[37]
子图嵌入	diffpool ^[35] 、graph2vec ^[35]

在图嵌入技术和图统计特征方法的性能方面,

在一些区块链欺诈行为识别任务中, 图嵌入特征表现了比图统计特征更好的性能。如 Hu^[31]分别构造了 node2vec、deepwalk 两种嵌入特征用于识别比特币生态中的洗钱行为, 并与手工提取的特征在相同的分类器 Adaboost 下进行了比较, 实验结果表明: 采用图嵌入特征的分类器在识别准确率上均达到了 90% 以上, 相较图统计特征有更强的性能。同时, Hu 还表示, 在嵌入过程中, 对邻居节点聚合的步长越长, 特征对交易如何传播的了解就越强。与这一结果不同的是, Weber^[12]在对洗钱行为研究中发现, 图嵌入特征与图统计特征二者的结合使用, 输入到下游分类器中训练, 可以获得比单独使用任何一种特征更好的性能。

7 欺诈行为识别技术

上述第 5 节和第 6 节提供了区块链交易图数据, 以及对应的交易结构和属性特征。在此基础上, 一些行为识别模型和方法得以提出。根据使用的数据策

略, 这些方法大体可分为基于交易、基于合约以及涉及链下信息的三类。本节以图 1 中描述的分类框架归纳整理各类区块链欺诈行为的识别技术, 即: 非法洗钱、庞氏骗局、钓鱼诈骗以及其他欺诈行为。

7.1 区块链非法洗钱识别

洗钱是所有加密货币犯罪的基础。不法分子在收到非法所得的加密货币后, 面临的首要问题就是“如何转化为合法现金?” 根据当前已知的洗钱模式, 存在四种主要的洗钱渠道: a) 通过中心化交易所变现, 包括与交易所相关的 OTC 场外经纪人, b) 使用匿名性更强的隐私币完成黑币转移, 如 Zcash 和门罗币(Monero)等, c) 通过区块链风险服务实现, 比如: 混币服务、比特币自动取款机和赌博网站, d) 与新型区块链技术结合的洗钱手段, 如: 基于 De-Fi 的跨链洗钱。表 6 是对一些现有区块链非法洗钱识别技术的整理, 按文献年份、数据策略、技术类别上进行了归纳, 表中准确率等指标依据论文数据得出。下文将分别介绍这些区块链洗钱识别技术。

表 6 区块链非法洗钱识别技术
Table 6 Blockchain illicit money laundering detection technology

文献	年份	数据策略	主要技术方法	是否考虑类别不平衡问题	精确率	召回率	F1 分数
Ranshous S, et al. ^[30]	2017		Adaboost	✗	99.71%	99.76%	0.9973
Möser, et al. ^[67]	2017		Heuristic Algorithm	✗	76.75%	--	--
Kappos, et al. ^[65]	2018		Heuristic Algorithm	✗	--	--	--
Hu Y, et al. ^[31]	2019		Ensemble Model	✗	92.3%	93.7%	0.93
Weber M, et al. ^[12]	2019		GCN	✗	97.1%	67.5%	0.796
Yousaf H, et al. ^[38]	2019		Heuristic Algorithm	✗	--	--	--
Joana Lorenz, et al. ^[14]	2020		Active Learning	✓	--	--	0.82
Jiajing Wu, et al. ^[39]	2020	基于交易	PU Learning	✓	--	--	--
Ismail Alarab, et al. ^[15]	2020		Relational-GCN	✗	89.9%	67.8%	0.773
Dylan Vassallo, et al. ^[40]	2020		Xgboost	✓	97.9%	69.3%	0.812
Catarina Oliveira, et al. ^[13]	2021		Random Walk	✗	97%	77%	0.85
Béres, et al. ^[70]	2021		Graph Embedding	✗	--	--	--
Tang, et al. ^[71]	2021		Heuristic Algorithm	✗	--	--	--
Wang, et al. ^[69]	2022		Heuristic Algorithm	✗	37%	100%	0.54
Sun, et al. ^[68]	2022		LSTM	✗	96.6%	96.1%	0.964

1) 基于交易所的反洗钱研究

区块链中心化交易所作为区块链金融的主要载体, 如: Binance^①、Huobi^②, 是洗钱变现的主要渠道。Ranshous^[30]在去匿名化比特币交易所地址的过程中, 就发现与交易所地址相关的交易中存在一种与洗钱

行为有着极大关联的交易模式, 称之为短粗带 STB 子图(一种特殊的 2-motif 子图), 其大量存在于 2011 年到 2015 年的比特币交易中。由于近年来交易所的 KYC(Know Your Customer)监管越来越严格, 洗钱者又绕道于 OTC 场外经纪人来实现在交易所洗钱, 如:

① <https://www.binance.com/>.
② <https://www.huobi.com/zh-cn/>.

在 2019 年, Plustoken 的诈骗者就通过火币的 OTC 经纪人套现了至少 1.85 亿美元非法资金^①。

由于区块链中心化交易所的内部数据具备商业保密性, 如: 数字货币的买卖数据、KYC 身份数据等。因此, 现有针对区块链交易所的反洗钱研究主要是从区块链公开的交易记录着手。研究人员根据已知的区块链交易所地址以及互联网上公开披露的区块链非法洗钱地址作为标注数据, 建立反洗钱数据集, 从而在标注数据集上展开对交易所反洗钱的研究。反洗钱研究中一个常用的数据集是麻省理工学院的 Weber 等人^[12]和区块链数据分析企业 Elliptic 联合公开的 Elliptic 数据集^②。该数据集是目前最大的区块链欺诈行为公开数据集, 它收集了 4545 个非法交易实体(包括: 洗钱、诈骗、恐怖组织等)以及 42019 个合法交易实体(包括: 交易所、钱包提供商、矿场等), 被广泛应用于当前的反洗钱工作中^[11, 33, 35]。在该数据集上, Weber 以 2 周作为一个时间步长构建了 49 个比特币交易事务图(其中: 34 个交易事务图作为分类模型的训练集, 15 个作为测试集), 从中提取了 166 种图统计特征、GCN 嵌入特征和时序 EvolveGCN 嵌入特征, 训练下游分类器 Random Forest, 对比特币中的非法洗钱实体进行识别, 对非法实体的识别准确率达到 97%。

但 Hu^[31]指出, Elliptic 数据集并没有提供真实的标注过程以及所使用的确切特征信息, 这导致算法很难在其他数据集上也产生效果。在 Hu 的工作中, 从 WalletExplorer 等线上资源收集了与洗钱服务相关的比特币钱包地址作为标注数据, 提取了 deepwalk、node2vec 嵌入特征与 14 种交易图统计特征, 以 Adaboost 作为基分类器, 训练多个分类器, 这些分类器使用不同的特征进行训练, 最终, 采用或(OR)和与(AND)两种方式集成这些分类器的结果。实验模型在三种洗钱服务上对比评估: AlphaBay、Bitmixer 和 HelixMixer^[41], 结果表明: “OR” 的集成方式取得了最好的识别准确率(92.3%)和 F1 分数(0.93), 但模型的性能会受到类别不平衡的影响, 只有当欺诈行为标注的数量达到一定程度时, 分类模型才能起到作用。

另外, 在 Elliptic 数据集上, Oliveira^[13]提出了一种基于非法节点的图构建技术, 它由一组种子节点出发, 在比特币交易事务图上以随机游走的方式构图, 直到遇见第一个被标记的非法节点或到达事务的终点。这种构图方式可以提取出新的结构特征, 如:

到达非法节点的步长, 从而提升在 Weber 工作中所提出的洗钱模型的性能, 实验结果表明这种构图方式对比原始特征(91%)可以带来超过 5% 的提升(97%)。并且, 此方法在 Weber 提出的算法性能表现非常差的一段时间区间仍然能够完成很好的识别。这类基于有监督机器学习的反洗钱识别算法可以有效检测出与交易所相关的洗钱模式和非法实体, 但其限制正如 Hu 所说, 类别不平衡和非法标注数量会在一定程度上影响模型在真实场景中发挥作用。

Lorenz^[14]在这一问题上做出了改进。首先, Lorenz 在 Elliptic 数据集上测试了常用的无监督异常检测算法, 包括: KNN、LOF、PCA 以及 OCSVM 等。这些无监督算法的实验结果展现出来的性能很差。然后, 他提出了一种基于主动学习(Active Learning, AL)的半监督反洗钱模型。该算法通过交互式地对数据实例进行标注, 然后使用这些标注重新训练模型, 如果模型性能不令人满意, 则进一步优化标注的增量过程, 以达到解决标签稀缺性限制的目的。其实现结果表明, 这种基于 Active Learning 的反洗钱模型在原数据集 5% 的标注数据量上就可达到 Weber 工作中的模型性能。

一直以来, 交易所都是区块链洗钱的主要渠道。通过机器学习模型对涉及交易所部分的洗钱交易的识别均是十分准确的, 但从算法训练的角度, 相比于 Weber 的工作, Lorenz 基于主动学习的方法对标注数据的依赖程度大大减小, Hu 在集成学习上的设计在类别不平衡问题上可以得到改善。在这些方法中, 特征工程是关键。在 Weber 的实验中, 将嵌入和统计特征结合值得借鉴。上述 Elliptic 数据集覆盖的时间范围在 2020 年以前, 并未披露具体的时间。由于洗钱的形式多变, 数据集多大程度与当前真实分布保持一致, 这是在实际应用中需要着重考量的。

2) 基于隐私币的反洗钱研究

一系列研究表明^[9, 64], 比特币的伪匿名地址并不能提供真正有意义的匿名性。一些区块链分析企业也开始将比特币交易分析作为一项业务提供给监管机构和金融企业, 如 Chainalysis、Elliptic 等, 被用于监控比特币交易行为以及捣毁相关的非法活动, 如关闭丝绸之路。

由于隐私币的匿名性比比特币更强, 一些非法交易市场开始支持隐私币交易, 以隐藏交易身份或洗钱。在这些隐私币中, 最受欢迎的无疑是 Zcash 和 Monero。而早在 2017 年被查获的暗网市场 AlphaBay

① <https://go.chainalysis.com/2020-crypto-crime-report>.

② <https://www.kaggle.com/datasets/ellipticco/elliptic-data-set?resource=download>.

案件^①、Shadow Brokers 黑客组织^②、以及勒索软件 WannaCry 的买卖和清洗交易中就发现了大量 Zcash 和 Monero 上交易记录。

Zcash 是首个具有完全匿名性的数字货币, 采用非交互式零知识证明技术(zero-knowledge succinct non-interactive arguments of knowledge, zk-SNARK), 用于隐藏交易双方的身份、交易的金额以及一切与交易相关的信息, 从而实现完整的隐私保护^[26]。Zcash 包含两个部分, 即公开部分和隐私部分, 公开部分的交易类似于比特币交易, 交易细节完全可见, 本文称为透明池。而隐私部分的交易使用 zk-SNARK 技术确保隐藏, 交易地址和金额不可见, 通常被称为屏蔽池。用户在透明池和屏蔽池内部与外部的交易构成了两类地址和四类交易, 即透明地址和屏蔽地址。透明地址与比特币地址性质相同, 完全可见, 而屏蔽地址不可见。两类地址的组合形成了四类交易。

涉及屏蔽池部分的交易信息具有强匿名性。这对交易行为分析带来了极大的挑战。Kappos^[65]通过分析进入屏蔽池的交易(称为存款), 以及从屏蔽池出来的交易(成为提款), 依据两者在交易金额、交易时间上的特性, 提出了 5 条启发式方法为屏蔽池两端的透明地址建立了关联, 被关联的地址将分为同一用户。继而, 通过对同一用户存款交易与提款交易在交易数量、金额以及时间上的差异, 间接分析该用户在屏蔽池内的行为。发现在屏蔽池内共 8000 余笔交易中, 大部分交易由少数用户完成, 而 BitClub Pool 矿池则至少包含了 1300 笔交易。最后, Kappos 根据黑客组织 Shadow Brokers 的博客中提到的金额与时间信息, 筛选出了高度相关的客户地址集, 很大程度减小了匿名集。

Monero 是一种基于 CryptoNote 协议的加密货币^[66], 采用一次性地址、环签名、环机密交易 3 种技术确保交易的不可追踪、不可链接以及交易数据隐私。Monero 允许用户在交易中加入一定数量的地址作为交易的混合输入以增强隐私。用户在早期 Monero 0.9.0 版本(2016.1.1)以前中可以使用 0 混合, 0 混合匿名性与比特币交易类似。而此之后, Monero 开始强制用户在交易中的混合集大小至少为 2。到 Monero 0.10.0 版本, 推出 RingCT, 允许用户隐藏交易金额。到 Monero 0.11.0 版本, 混合集大小则被提升到了 4 以上。混合集增大以及 RingCT 等技术的引入, 使得 Monero 的匿名性变得更强, 同时对 Monero 的行为分析工作带来了更大困难。

Möser^[67]针对 Monero 对混合集采样策略的两个弱点进行了评估并提出了相应的启发式方法, 即: a. 0 混合交易的输入地址会为之发生的多地址混合交易带来暴露风险, 起到连锁反应。而在 Monero 的所有交易中有 64.04% 的交易是 0 混合交易。b. Monero 交易中最新的输入地址往往是真正的交易地址, 也更小概率被采样为混合集。通过启发式关联属于同一实体的地址集群, 发现在 AlphaBay 运营期间(2014.12 ~ 2017.7), Monero 占其交易量的比例逐步提升。

隐私币从技术本身带来了比比特币更强的匿名性。匿名集大小是衡量其匿名性的主要指标。现有方法从隐私币机制上, 利用交易先验信息减小匿名集大小, 以推测地址间的关联性。这对去匿名化的预处理十分有帮助, 但在精准关联上效果有限。匿名集初始大小可能是此类方法的主要限制。当匿名集地址数量庞大, 尽管可以减少 50% 以上的匿名集, 但仍需在剩余的成百上千个匿名地址中找到关联的地址。如果没有更多的信息, 将很难进一步推断关联性, 也难以产生实际作用。同时, 就像 Monero 在修改了混合集大小后, Möser 所提方法的效果大打折扣。由于隐私币技术上的完整性, 从法律层面要求服务商增强用户信息管理和 KYC 政策也许是更实际的方案。

3) 基于混币服务的反洗钱研究

混币服务是通过自动聚合分离多笔互不相干的交易, 从而达到切断地址链接性的目的, 从而增强用户匿名性。它是现有区块链非法活动中最常用的洗钱和匿名手段。Jawaheri^[42]就在去匿名化暗网服务交易过程中发现, 推特 Tweet、Bitcointalk 论坛用户在与暗网服务的交易中存在了大量的混币操作。识别混币交易中的洗钱行为关键是识别出混币模式。

混币服务有多种不同的实现形式, 根据操作者的不同, 可分为中心化混币、去中心化混币。中心化混币技术需要中心化混币服务提供商参与, 帮助混币用户进行混币操作。去中心化混币技术由所有参与混币的用户按照协议自发进行混币交易。关于这两类混币机制及其隐私攻击(去匿名化)在文献[66]第 2 节中有详细介绍, 可供读者参考。本节则补充介绍其缺少的基于图交易分析的混币模式识别以及近年来流行的基于零知识证明的去中心化混币应用程序。

相较于基于混币机制的去匿名化方法(主要是启发式规则方法), 基于图分析的混币识别方法在召回率上可能更有优势。Wu^[39]在比特币交易的地址图和地址事务图上分别提取了一种时序 motif 子图和一种

① <https://www.justice.gov/opa/press-release/file/982821/download>.

② <http://www.ccert.edu.cn/archives/338>.

ATH(Attributed Temporal Heterogeneous) motifs 子图用于挖掘混币交易模式, 然后从子图中提取网络、账户和交易三个层面的混币标识特征, 构建了一个基于 PU Learning 的半监督模型, 用于识别混币模式。Sun^[68]将比特币交易 DAG 图转化为树形结构。以目标交易作为根节点, 形成两颗树, 其一由目标交易与其前任交易组成, 其二由目标交易与其继任交易组成。通过对树的每一层交易的统计特征聚合作为树的序列化表征, 形成两个长度可能不相同的交易树序列。最后使用 LSTM 向量化两个序列并输入到线性分类器中进行混币交易识别。其实验结果表明这种交易分类方法在召回率上比基于规则的方法更有优势。

基于零知识证明的混币器与 Zcash 机制类似, 即混币用户将固定数量的硬币存入屏蔽池, 随后从屏蔽池中将这些硬币提取到新的地址中, 通过零知识证明保证隐私性的屏蔽池来打破存款地址和提款地址的链接性。Tornado Cash(TC)是以太坊最大的混币器, 至今已完成超过 90 亿美元的混币交易。TC 基于智能合约实现, 是一个可自动执行和去中心化的零知识证明混币器。TC 一共运营了 4 种面额的以太币屏蔽池, 包括 0.1 eth、1 eth、10 eth、100 eth。混币用户在往 TC 存入一笔金额后会获取一张存款单, 在需要提取的时候, 将存款单交由 TC 智能合约验证即可。与 TC 类似的零知识证明混币器还包括 Typhoon Network(主要运行在币安链)、Cyclone(运行在以太坊、币安链、Polygon 多链上)。本节以 Tornado Cash 为重点作为零知识证明混币器的去匿名化介绍。

零知识证明的隐私性通常使用匿名集大小作为衡量。基于 TC 的运行机制, Wang^[69]提出了 5 条启发式规则用于减小匿名集从而关联屏蔽池两端的存取款交易: 1)取款地址如果是存款地址的重用, 那么证明这两笔交易是关联的。2)用户采用提供存款地址发起提款交易, 但指定另一个地址提取资金, 这两个地址被认为是关联的。3)存取款地址不同, 但这两个地址发生过以太坊交易, 将被认为是关联的。4)用户将资金从一个地址分散到多个地址并向池子存款, 这些地址将被认为是关联的。5)存款地址往多个面额的池中存款, 取款地址从相同的面额池中取出相同数量的资金, 这被认为是关联的。通过运用这 5 条启发式规则, 匿名集大小平均可减少 34.18%。另外,

Wang 通过一些公开的非法地址标注, 在 TC 的存取款地址中发现了 87 个非法地址, 其交易量达到 3.7 亿美元, 占总交易量的 4.1%。Tang^[71]对 TC 交易的时间间隔进行了统计分析, 基于分析结果提出了 3 种启发式规则用于减小匿名集, 如存取款时间间隔小于 180s, 将被认为属于同一用户。

Beres^[70]提出了一种基于机器学习的去匿名化方法, 将以太坊账户每天的交易活跃特征、交易花费的 gas 价格以及交易图结构的嵌入特征组成欧式特征向量, 通过距离衡量匿名集中各个候选地址与目标地址的关联性。作者采用 TC 中存取款地址花费的 gas 价格是否相同、是否发生过以太坊交易作为规则, 形成 ground truth 关联对, 以进行评估, 发现这种基于机器学习的去匿名化方法可以提供 1.23 的信息增益, 且将 TC 匿名集大小减小到均值为 400。

现有的大多数方法是依据混币机制而提出基于规则的识别方法。与隐私币不同, 由于这些混币器通常运行比特币、以太坊等公链上, 并不具备完全匿名性, 其混币规律更容易被发现。这些方法在传统的中心化和去中心化混币器上通常能取得很好的效果, 而被应用于各类实际业务上。但其缺点是它们针对于特定规则, 当出现假阳性样本时, 人工难以判断和发现。因此, 对假阳性样本的考虑是选择这类方法的重点。另外, 基于图分析的混币识别方法一定程度上可以提升召回率, 但在准确率上还有待提升。

4) 基于跨链的反洗钱研究

区块链跨链技术是区块链实现互联互通、提升可扩展性的重要手段^[43]。当前主流的跨链技术包括: 公证人机制、侧链/中继、哈希锁定和分布式私钥技术^[44]。这些区块链跨链技术在应用上, 被用于解决不同区块链之间的资产留置、转移问题。一些区块链交易所为用户提供了跨链加密货币转移、交易等服务。最常见的跨链交易所包括: Uniswap^①(提供去中心化的代币自动兑换服务)、dYdX^②、Pancakeswap^③等。

跨链交易为用户提供了在不同区块链转移资产的便利性, 同时, 由于不同区块链之间存在信息孤立性, 跨链交易增强了区块链交易的匿名性, 这为区块链非法洗钱提供了新的工具。区块链数据分析企业 Chainalysis 提到^④: 区块链去中心化金融正在洗钱中发挥更大的作用。同时, Chainalysis 还揭露了

① <https://uniswap.org/>.

② <https://dydx.exchange/>.

③ <https://pancakeswap.finance/>.

④ <https://go.chainalysis.com/2022-crypto-crime-report>.

2022 年 Spartan Protocol 黑客使用 DeFi 协议和跨链来清洗价值 3000 万美元的 SPARTA 代币的盗窃资金: 黑客首先使用了两个专门用于跨链交易的 DeFi 协议, 将这些代币中的大部分转换为 ETH(以太坊)和 renBTC(一种流通于以太坊网络的比特币锚定币), 然后再将这些资金通过去中心化交易所换成新的 ETH 和 WETH(以太坊的代币化版本), 最后, 这些资金发送到了 Tornado Cash 混币器。

在区块链跨链交易关联问题上, Yousaf^[38]提出了一种跨链交易关联的启发式。通过给定一个阈值窗口, 在存款链和提款链上, 找出时间或金额上相近的两笔交易, 视为两种货币交易的关联。另外, 针对跨链用户之间的关系识别, 存在一种共同关系启发式: 如果两个或多个地址发送到存款链中的同一个地址, 又或者如果两个或多个地址从提款链中同一个地址收到钱, 就说明这些地址之间有着共同的社交关系。通过这些启发式方法, Yousaf 识别了一家名为星景资本 (Starscape Capital) 的公司在完成 ICO 诈骗后使用 ShapeShift 跨链清洗了价值 51.7 万美元的非法收入。星

景资本在 2018.1.19 到 2018.1.21 三天内接收和发送了 2038 个以太坊, 总发送交易共 133 笔, 其中 109 笔交易发往 ShapeShift。在 2018.1.21 这天, ShapeShift 有 103 笔交易发往 monero, 6 笔交易发回了以太坊, 转移到门罗币的地址只有 3 个, 总量共 465.61 个以太坊。

跨链交易为用户带来了与隐私币不同层级上的匿名性, 具备极大的技术难度。Yousaf 提出了首个针对跨链的交易识别方法。方法的有效性依托于跨链交易时间和金额的差异性。因此, 在一些特定的场景下可能会受到很大的限制而出现假阳性样本, 如用户使用跨链服务购买商品, 不同的用户在同等商品上所支付的价格和时间都可能十分相似。

7.2 区块链庞氏骗局识别

Charles Ponzi^①早在 20 世纪初就利用高回报收益诱使美国 4 万波士顿市民蒙受诈骗损失, 此后庞氏之名不绝于耳。自 2011 年比特币市值暴涨以来, 许多人都在追逐着下一个可能带来高收益的区块链加密货币, 庞氏骗局由此在区块链应用中滋生。表 7 对现有区块链庞氏骗局识别技术进行了整理。

表 7 区块链庞氏骗局识别技术
Table 7 Blockchain ponzi scam detection technology

文献	年份	数据策略	主要技术方法	是否考虑类别不平衡问题	精确率	召回率	F1 分数
Massimo Bartoletti, et al. ^[45]	2018	基于交易	Random Forest	✓	65.8%	78.1%	0.714
Shanqing Yu, et al. ^[48]	2021	基于交易	GCN	✗	86.86%	91.59%	0.8907
Pengcheng Xia, et al. ^[52]	2021	基于交易	Xgboost	✗	96.45%	96.79%	0.9662
Weili Chen, et al. ^[21]	2018	基于合约	Xgboost	✗	94%	81%	0.86
Yincheng Lou, et al. ^[46]	2020	基于合约	CNN	✗	98.2%	93.8%	0.959
Shuhui Fan, et al. ^[47]	2020	基于合约	Federated Learning	✗	100%	93.1%	0.9643
Lei Wang, et al. ^[49]	2021	基于合约	LSTM	✓	97%	96%	0.96
Yuzhi Liang, et al. ^[50]	2021	基于合约	Dynamic Graph Embedding	✗	98%	85%	0.91
Giacomo Ibba, et al. ^[51]	2021	基于合约	Abstract Syntax Tree	✗	97%	100%	0.99
Weimin Chen, et al. ^[22]	2021	基于合约	Symbolic Execution	✗	100%	100%	1.00

从识别场景上, 区块链庞氏骗局识别技术主要分为两种类型: a) 账户交易分析, 即: 根据区块链交易记录识别庞氏地址或账户, b) 合约代码分析, 针对利用智能合约进行庞氏诈骗的情况, 从合约代码层面, 识别出以太坊中存在的庞氏骗局合约, c) 代币交易分析, 针对近年来出现的一些“拉地毯(Rug Pull)”骗局项目, 即: 项目起初承诺高回报但最终暴雷的代币, 则是从整个代币的生命周期进行分析, 从而识别出具有 Rug Pull 风险的代币。下文将分别展开这 3 种区块链庞氏骗局识别技术的介绍。

1)基于账户交易的庞氏实体识别

在区块链发展早期, 庞氏诈骗者通过线下或暗网发布投资项目等手段实现诈骗目的, 在这一过程中, 诈骗者会向受害人或社区公开自身的钱包地址。因此, 在早期基于账户交易的庞氏实体识别工作^[20]中, 首先是在互联网上手动或半自动地收集与庞氏骗局相关的加密货币地址, 标注形成庞氏数据集, 然后在这些标注数据上训练出相应的庞氏实体识别模型。但这种收集庞氏地址的方式不再可行, 因为随着诈骗者隐私意识的提升, 它们已经很少再直接公

① https://en.wikipedia.org/wiki/Charles_Ponzi.

开自身的钱包地址^[42]。

在比特币中, Bartoletti^[20]通过比特币论坛(bitcointalker)和社交网络论坛(reddit), 收集了 32 个庞氏实体的比特币储蓄地址。在此基础上提取出地址的交易特征, 采用 Random Forest 作为分类器, 建立了庞氏地址分类模型。同时, 作者考虑了数据集中的类别不平衡问题, 通过随机采样和权重分配的方式来训练模型, 最终在正负样本比 1/200 下成功识别出了 32 个庞氏骗局中的 31 个。

在以太坊中, Yu^[48]从 Etherscan 上收集了 50 个庞氏合约, 并以 Xblock^①中的庞氏合约数据集作为补充, 构建了庞氏合约地址的交易子图, 形成一个对交易地址子图分类任务, 分为两类: 庞氏和常规。采用图卷积网络(Graph Convolutional Network, GCN)提取这些交易子图的嵌入特征, 最终在庞氏数据集上达到了 90%以上的召回率和 85%以上的准确率。

在实际应用中, 基于交易的庞氏实体识别方法对庞氏案件复盘及后续资金追踪有着重要作用。上述识别技术, Bartoletti 考虑到了算法训练中类别不平衡的问题, 在庞氏骗局上的识别上表现很好, 但在非庞氏交易上的检测效果不佳, 可能存在过采样问题。Yu 则采用了技术上更具先进性的图卷积网络方法, 在对以太坊庞氏账户检测的准确率和召回率上体现了方法的优越性。

2) 针对智能合约分析的庞氏合约识别

以太坊智能合约是以高级程序语言 Solidity 编写的代码程序, 运行在以太坊虚拟机(Ethereum Virtual Machine, EVM)之上。编写者将智能合约上链, 首先需要把 Solidity 源代码编译为 EVM 字节码。EVM 字节码由一系列字节组成, 每个字节对应了一项操作, 而操作的集合又被称为操作码, 如: 字节 0x00 对应了 STOP 操作(以太坊黄皮书^②给出了完整的字节码列表)。合约在上链之后, 被部署在以太坊主网络中, 任何人可以查看、调用。

智能合约是庞氏骗局的一个有力工具。因为合约自动执行, 并且一旦部署就无法修改, 这使许多投资者相信, 持续产生收益的项目建立在智能合约之上, 就不会构成骗局风险, 但这是不可能的。诈骗者可以通过在智能合约中埋藏漏洞来卷走投资人的资金。在现有的庞氏合约识别技术中, 主要包含两种: 基于智能合约的操作码和合约交易来识别庞氏合约, 以及基于智能合约的代码语义信

息来检测出庞氏合约。

第一种基于合约操作码与合约交易的识别技术。Chen^[21]从以太坊浏览器 Etherscan 上收集了 1382 个经过验证的智能合约, 并手动检查了潜在的庞氏合约, 形成了一个包含 131 个庞氏合约、1251 个非庞氏合约的数据集。在这一数据集上提取了两类特征: 合约操作码特征和账户特征。合约操作码特征包含了合约中所使用的操作码以及使用频率等信息, 用于分析智能合约潜在的逻辑; 账户特征包含了合约所涉及的交易上的特征, 如: 合约余额、输入地址数、输出地址数等。然后, 庞氏合约识别任务被构建为一个二分类任务, 下游的机器学习庞氏合约识别模型通过 xgboost 实现。最后的实验表明合约操作码特征在模型中的性能表现比账户特征更有效(84%召回率), 而账户特征只能获得很低的召回率(44%)。Wang^[49]在 Chen 的基础上通过 LSTM 技术实现对智能合约庞氏骗局的检测, 并通过过采样的训练方式来缓解数据集类别不平衡问题, 在正负样本比 1:16.9 的数据集下取得了 96%的召回率, 同条件下 Xgboost 方法只有 70%召回。Liang^[50]构建了一个覆盖外部账户和合约账户的以太坊交易网络, 通过动态节点嵌入的方法, 将以太坊交易网络中各个节点的结构信息、智能合约操作码等整合为一个低维的连续向量, 输入到一个多层感知器(Multilayer Perceptron, MLP)中判断节点是否为庞氏合约账户, 最终在实验数据集(131 个庞氏合约以及 1251 个非庞氏合约)上取得了 85%的召回率。

第二种基于合约代码语义信息的识别技术。Bartoletti^[45]根据合约代码对利益分配的逻辑, 在现有的庞氏合约上定义了 4 种类型: a) 基于数组的金字塔方案(Array-based pyramid schemes), 即: 新加入骗局的受害者进入数组队列, 其资金用于按序支付数组中的用户倍增回报。b) 基于树的金字塔方案(Tree-based pyramid schemes), 即: 使用树数据结构记录用户地址, 合约所有者为根节点, 新加入骗局的受害者资金用于在其祖先节点间分配利益。c) 移交方案(Handover schemes), 即: 新加入骗局的受害者需要提供最后一个用户的投资和收益, 移交方案只存储最后一个用户的地址, d) 瀑布方案(Waterfall schemes), 即: 将新加入的投资按固定百分比分配给之前加入的用户, 从第一个用户开始, 直到余额散尽。

Chen^[22]在上述基础上建立了一种静态的庞氏合

① <http://xblock.pro/>.

② <https://ethereum.github.io/yellowpaper/paper.pdf>.

约分析系统, 确定了以太坊中的 835 个庞氏合约, 它通过符号执行技术(Symbolic Execution)生成合约中每条可行路径的语义信息和控制流图, 从而区分出投资者的相关行为, 并将这些行为与上述四种庞氏类型相匹配, 输出最终的庞氏合约检测报告, 在实验数据集上取得了 100%的准确率和召回率, 同条件下基于交易和操作码的机器学习方法只有 57.9%和 85.2%的召回率。Ibba^[51]通过在合约代码中提取出抽象语法树(Abstract Syntax Tree, AST)。在 AST 的基础上解析获取到更高级的合约语义特征, 最终通过朴素贝叶斯模型对智能合约进行分类, 获得了 99%识别庞氏合约的准确率。Lou^[46]将庞氏智能合约的字节码转化为单通道图片数据, 通过对这种数据的分类来实现对庞氏合约的识别。在识别模型上, 作者提出了一种改进后的卷积神经网络(Convolutional Neural Network, CNN), 这种改进版的 CNN 针对字节码的长度不一, 引入了空间金字塔池化, 单通道图片在经过空间金字塔池化后可以形成统一长度的池化向量, 最终可以被 CNN 正常运行, 在实验数据集(包括 132 个庞氏合约和 3642 个非庞氏合约)上取得了 98.2%的准确率和 93.8%的召回率。

通过对庞氏合约的检测, 可以对用户很好的起到预警作用。由于庞氏骗局的行为逻辑比较明确, 基于合约交易特征、基于合约代码语义信息两类识别技术在对庞氏骗局的识别均有着非常高的准确率和召回率。但在实际应用中, 后者在召回率和可解释性上更具优势。在上述合约代码检测方法中, Chen 提出的启发式规则在实验数据集上取得了 100%的准确率和召回率, 体现了该启发式规则的有效性, 但启发式规则的限制在于其针对于特定场景, 鲁棒性不强。Ibba 和 Lou 则提出了基于机器学习的方法, 在识别准确率上也取得了很好的性能, 同时, 在算法鲁棒性上可能更具优势。

3) 针对“Rug Pull”的庞氏项目识别

“拉地毯”(Rug Pull)是近年来出现在去中心化生态中的庞氏骗局的代名词, 用于指代加密货币项目的开发人员(一般是新的代币)突然放弃项目, 并卷走所有投资资金。

去中心化交易所(Decentralized Exchange, DEX)中的代币通常需要有相应的资金流动性池来保证运行, 该资金流动性池一般与另一种加密货币(通常是以太币)挂钩, 并成比例存在。代币在兑换和交易的过程中也按流动性池中两种代币的比例结算, 如: 去中心化交易所 Uniswap 允许任何支持 ERC20 标准的代币进入平台交易。代币的流动性池需要流动性

提供者同时投入按比例的一种加密货币, 获取流动性权证。流动性权证由投入额与流动性池总额的比例来衡量, 流动性权证是流动性提供者的权益代表, 可以为流动性提供者带来交易者手续费收入等回报。在去中心化交易所中, 项目开发商可以无需代码审计就让创建的新代币上市, 这给诈骗者带来了可趁之机。因为创建新代币和启动代币的流动性池十分容易, 而持有代币的投资者认为流动性池中的资产如何使用由他们投票决策, 因此相信开发人员无法非法卷走流动池中的资金。由于项目代码未被审计, 而一旦项目代码存在漏洞, 就可能导致流动资金被盗。

在对“Rug Pull”庞氏骗局的识别技术上, Xia^[52]从不同角度研究了去中心化交易所 Uniswap V2 中存在的“Rug Pull”诈骗项目。作者首先从 The Graph (一个去中心化协议, 用于索引和查询区块链数据)中收集了与 Uniswap 相关的交易事件, 包括: 代币发行(mint)、交换(swap)、销毁(burn)等事件。

根据这些事件进一步收集了 Uniswap 完整的交易信息, 如: 转移的 ETH 数量、输入数据、内部交易和所有的事件日志。这些数据包括了 Uniswap V2 自 2020.5.5(第一笔交易创建)到 2020.12.6, 超过 2000 万条交易、21778 种代币以及 25131 个流动性池。

一些数据分析结果包括: 在流动性池的创建上, 25131 个流动性池共由 17053 个地址建立, 有 3046 个地址建立了超过 2 个流动性池, 120 个地址建立了超过 10 个流动性池。在投资者方面, 共有 548609 个地址参与到了以上交易中, 大约 45%的投资者只与一个流动性池交易, 而超过 90%的投资者与 15 个以内的流动性池交易。

Xia 标注了其中 4048 个诈骗代币和 2397 个官方代币构成机器学习数据集。在此数据集上, 提取了时序特征(如代币的生命周期)、交易特征(如交易数量)、投资者特征(参与流动性池的平均个数)和 Uniswap 特定特征(如涉及代币的总流动性), 以随机森林(Random Forest)作为下游分类器, 训练代币诈骗识别模型, 在实验数据集上取得了 96.45%的准确率和 96.79%的召回率。实验结果表明 Uniswap 上大约 50%的代币都是诈骗代币, 诈骗者从 39762 个受害人手中获利至少 1600 万美元。

Rug Pull 在过去一年造成的经济损失严重, 引起了广泛的关注。Xia 提出了首个在 Uniswap 流动性池中识别诈骗识别的方法, 并取得了不错的识别准确率, 但算法对数据的依赖程度较高, 在性能以及先进性上仍具备提升空间。去中心化平台中对代币的

监管宽松问题还需得到更多的关注。

7.3 区块链钓鱼诈骗识别

钓鱼攻击的危险往往不在于系统中存在漏洞,而在于人类的轻信和疏忽。许多拥有强大安全策略的区块链项目在面对网络钓鱼攻击时束手无策。

据 Chainalysis 研究^①,以太坊钓鱼诈骗是该生态系统中的第一大诈骗,据估计被盗总金额已超过 1.15 亿美元。表 8 对现有的区块链钓鱼诈骗识别技术进行了整理,在这些区块链钓鱼诈骗识别技术中可以大致分为两种类型:侧重于链上交易的钓鱼地

址识别,涵盖了链下内容的钓鱼实体识别。

1)链下区块链钓鱼攻击检测

区块链钓鱼诈骗通常与黑客攻击技术相结合,其手段主要分为两种:社会工程方案和攻击技术方案^[58]。社会工程方案是诈骗者基于欺骗和伪装,向受害者发送虚假信息,以窃取受害者资金,常见方式包括克隆网络钓鱼、社交网络钓鱼等。攻击技术方案则是利用系统漏洞以及软件和基础架构的缺陷窃取受害者资金,常见方式包括基于 DNS 的网络钓鱼、基于恶意软件的网络钓鱼等。

表 8 区块链钓鱼识别技术
Table 8 Blockchain phishing detection technology

文献	年份	数据策略	主要技术方法	是否考虑类别不平衡问题	精确率	召回率	F1 分数
Artsiom Holub, et al. ^[53]	2018	涉及链下信息	Attack Analysis	✗	--	--	--
Phillips Ross, et al. ^[56]	2020	涉及链下信息	DBSCAN	✗	--	--	--
Zihao Yuan, et al. ^[54]	2020	基于交易	Graph2Vec	✗	69%	77%	0.73
Weili Chen, et al. ^[55]	2020	基于交易	Dual-sampling LightGBM	✓	81.9%	80.5%	0.8122
Qi Yuan, et al. ^[36]	2020	基于交易	Skip-gram	✓	87.1%	82.2%	0.846
Chen Liang, et al. ^[19]	2020	基于交易	Random Walk	✗	72.9%	14.5%	0.2357
Haixian Wen, et al. ^[57]	2021	基于交易	Adaboost with Hidden Strategies	✗	83%	66%	0.74
J. Wu, et al. ^[10]	2022	基于交易	Trans2vec	✓	92.7%	89.3%	0.908

预付金诈骗是区块链钓鱼诈骗者使用社会工程手段的一种,是指行骗者在获取受害者的信任之后,向受害者承诺会给受害者很大的一笔资金,但是需要受害者预先支付一些所谓的“手续费”来提取这笔资金。若受害者支付“手续费”,行骗者可能会要求受害者继续支付更多费用,也有可能直接消失^②。受害者通常被社交媒体上的链接引导到这些预付金网站,如:诈骗者使用假 Elon Musk 社交账户宣称提供免费的加密货币,但在此之前需要先支付一笔小的预付金。

Elliptic^[56]对超过 1000 个加密货币预付费网站进行了追踪。首先,针对网站内容进行了聚类,将这些诈骗网站分为不同类型,随后在这些不同类别的网站上再基于网站活动进行聚类,比如 IP 地址、注册地址、注册时间等。结果发现有 51 个网站使用相同的 IP 地址,这一结果表明:这些诈骗网站背后的操控者可能为同一实体。然后,作者通过分析与这些网站关联的链上交易以检测不同的诈骗集群之间是否存在重用,发现同一控制实体使用了不同的操作运行着多个诈骗活动,并且加密货币在这些不同的诈

骗集群间来回流动。作者针对这一行为给出的分析是:这似乎是诈骗者的宣传行为,为了诱使受害者相信骗局是真的。

思科^[53]研究了乌克兰黑客组织 COINHOARDER 在加密货币钱包和交易所上设置的域名(Domain Name System, DNS)钓鱼攻击。COINHOARDER 通过 DNS 攻击手段仿冒加密货币钱包或交易所官网和 URL(见图 12),然后通过 google 广告将其置顶,从而诱使受害者使用并窃取资金。思科首先通过 NLP 和 ML 系统检测到网络钓鱼域,再者使用思科的 Umbrella 解析器追踪到了这些域里面的钓鱼网站及

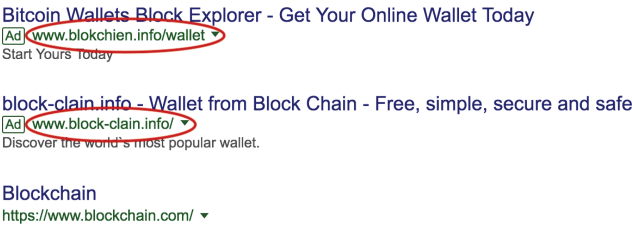


图 12 在 Blockchain.com 上设置的 URL 钓鱼^[53]
Figure 12 URL fishing set on blockchain.com^[53]

① <https://blog.chainalysis.com/the-rise-of-cybercrime-on-ethereum/>.
② <https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/advance-fee-schemes>.

其底层基础设施,发现 COINHOARDER 集团至少从 2015 年就一直从事加密货币窃取行为,并注意到该集团以非洲国家和其他发展中国家受害者为潜在目标。因为这些国家的银行业务更加困难,与数字资产相比,当地的货币更加不稳定,同时,第一语言不是英语的国家也更容易成为目标。

通过 IP 和 DNS 可以很好的追踪钓鱼诈骗者的实体身份以及链下活动详情,可以很好的满足监管要求。但在实际应用中,想要获取钓鱼者相关的 IP 和 DNS 信息往往是十分困难的,尤其是钓鱼者开始将链下活动转入 Tor 暗网。因此,在采用此类方法进行钓鱼行为分析时,具备丰富的互联网路由资源是十分重要的条件。

2)链上钓鱼交易识别

所有区块链钓鱼行为最终都要落在加密货币的交易上。基于链上交易的钓鱼地址识别是通过公开的区块链交易记录,完成对钓鱼账户或地址交易模式的识别。

Yuan^[36]提出了一种基于机器学习的以太坊钓鱼检测框架,该框架包括三个步骤:在以太坊交易记录上构建交易事务图,在构建好的事务图上提取出嵌入特征,将特征输入到下游分类器中进行钓鱼地址检测,该方法在正负样本比采样为 1:1 下,获得了 87.1%的准确率和 82.2%的召回率。

Chen^[55]提出了一种基于事务特征及联融合的方法。该方法根据节点的第 N 阶邻居节点的历史事务计算出相应的统计量,如:灰色矩阵(grey rectangle)。这一统计量将作为第 $N-1$ 阶邻居节点的数据再次计算出一个统计量出来,以树形结构及联传递到节点本身。这种方法可以提取出一个节点与整个网络交互的更丰富的信息。另外,Chen 采用了 LightGBM 双采样集成算法来解决类别不平衡问题,以建立钓鱼账户识别模型,在正负样本比高达 1:1600 之上的情况下,取得了 81.9%的准确率和 80.5%召回率。

Yuan^[54]构建了一种二阶事务子图,通过 Graph2Vec 方法学习事务节点的子图嵌入特征,以训练出一个以太坊钓鱼地址分类器,作者指出该方法在大规模网络的训练成本上更占优势。同时,该方法在二阶子图和一阶子图上的性能进行了比较。Yuan 指出由于二阶事务图保留了更多邻居信息,这使得二阶图在各方面都有着比一阶子图更好的性能,该方法在实验数据集(801 个钓鱼地址)中取得了 69%的准确率和 77%的召回率。

Chen^[19]基于随机游走的方法从交易记录中采样出节点事务子图,然后采样出来的子图被输入到一

个无监督的图卷积网络提取出该子图的嵌入特征表示,最后,作者使用了一个树模型 LightGBM 分类器,在包含 2973382 个节点(1157 个钓鱼节点),13551214 条边的交易图上获得了 64.7%的准确率和 15.5%的召回率。

Li^[37]针对区块链钓鱼诈骗标注的稀缺性以及数据可扩展性的场景需求,提出了一种自监督增量深度图学习模型。该方法分为两个步骤。首先,作者采用自监督学习算法(基模型是图卷积神经网络)从大量无标签的交易数据中学习节点的嵌入表示,其中自监督学习算法采用节点在时间和空间上的约束条件作为损失函数,即:从空间上,认为节点与节点频繁交易的邻节点有着相近的特征表示,从时间上,认为这一时刻发生的交易会影响到下一时刻节点的行为。在提取出节点嵌入特征后,作者通过增量训练的方式来更新自监督编码器的参数,同时,将钓鱼节点识别作为对嵌入特征向量的一个异常检测任务完成。Li 构建了一个包含 75382756 条边(6588 个钓鱼账户)的交易图,将其切分为 5 个子图。将前 4 个子图用于与训练和增量学习,在第 5 个子图上进行评估,获得了 67.7%的准确率和 40.7%的召回率。

在数据策略上,基于链上交易的钓鱼识别方法比基于链下的钓鱼检测方法更容易开展。数据标注稀缺与类别不平衡是基于链上交易的识别方法的一大挑战,尽管 Chen^[55]与 Li^[37]在算法设计上做出了改善,但在准确率和召回率上的表现仍有较大提升空间。同时,由于钓鱼数据的标注稀缺,基于监督的图神经网络方法^[19, 37, 54]也并没有在识别准确率上体现出明显的优越性。因此,如何克服算法对数据的依赖性,是在未来工作中需要解决的问题之一。

7.4 其他欺诈行为识别

如表 9 所示,本节将介绍 ICO 骗局、勒索软件、暗网交易、市场操纵、蜜罐诈骗这 5 类欺诈行为识别技术。尽管针对这些行为的相关工作并不太多,但这些对行为的识别对反欺诈研究中同样十分重要。

1)ICO 骗局

非法代币发行(Initial Coin Offering, ICO)骗局主要依赖于链下白皮书、项目网站运作来实施“拉高抛售”的计划,从而骗取投资人资金。Bian^[59]针对这些线上发布的 ICO 白皮书、github 项目文档、团队简历、网站内容等文本信息,使用 LSTM 等自然语言模型提取出文本主题、关键词等特征,并建立了一种基于监督学习的 ICO 评级系统。系统将一个 ICO 项目的特征作为输入,将其映射到二进制变量[0, 1]指示是否为骗局,最后在 1482 个 ICO 项目中,成功识

别了其中 82%ICO 项目, 并获得了 77%的召回率。除此之外, Bian 还通过为不同主题的 ICO 项目计算一阶导数显著性(First-derivative Saliency), 量化对 ICO

项目的评分, 并排序。实验结果发现游戏、赌博和娱乐主题的 ICO 项目比交换、支付、智能合约主题有更大的可能是骗局。

表 9 其他欺诈行为识别技术
Table 9 Other fraud behavior detection technologies

文献	年份	数据策略	主要技术方法	行为类型	是否考虑类别不平衡问题	精确率	召回率	F1 分数
Shuqing Bian, et al. [59]	2018	涉及链下信息	LSTM	ICO 骗局	×	83%	77%	0.80
Mauro Conti, et al. [25]	2018	基于交易	Heuristic Algorithm	勒索软件	×	--	--	--
S. Dalal, et al. [27]	2021	基于交易	Stacking Model	勒索软件	×	85.37%	85.66%	0.8551
C. F. Torres, et al. [23]	2019	基于合约	Heuristic Algorithm	蜜罐诈骗	×	--	--	--
R. Camino, et al. [60]	2020	基于合约	Xgboost	蜜罐诈骗	×	--	--	--
K. Kanemura, et al. [32]	2019	基于交易	Voting based method	暗网交易	×	--	--	--
WL Chen, et al. [24]	2019	涉及链下信息	Singular Value Decomposition	市场操纵	×	--	--	--
S. Dalal, et al. [27]	2021	基于交易	Stacking Model	勒索软件	×	85.37%	85.66%	0.8551

总体而言, 算法取得了较好的识别性能。但算法在耦合性上存在欠缺, 体现在对白皮书、github 文档、团队简历等各类数据资料的处理由不同数据模型完成, 复用性较差。同时对各类信息的结合也只是简单的拼接。

2)蜜罐诈骗

蜜罐诈骗通过部署看似存在漏洞的合约来引诱受害者掉入陷阱, 这种合约称为蜜罐合约。针对此类合约, Torres^[23]根据其操作面将蜜罐合约分为了三种类型: a) 基于以太坊虚拟机的蜜罐合约。这类合约利用以太坊虚拟机的异常行为来欺骗用户, 通过合约中看似不合理且有利可图的代码逻辑来暗示误导用户。b) 基于 Solidity 编译器的蜜罐合约。这类蜜罐合约受益于 Solidity 编译器问题。虽然一些编译器问题是众所周知的, 但仍有一些问题没有记录, 如果用户没有仔细分析智能合约或没有在现实条件下对其进行测试, 则可能会忽视这些合约漏洞。c) Etherscan 浏览器上的蜜罐合约。Etherscan 是最为人所知的以太坊浏览器, 很多用户完全相信 Etherscan 中的数据展示。这类合约利用了 Etherscan 中没有被展示出来的内容制造漏洞, 以引导用户调用合约。如: Etherscan 只显示一定宽度的合约代码, 超出这一宽度的代码将被隐藏, 只能通过水平滚动可见, 由此诈骗者通过一串长空格来隐藏蜜罐代码, 使得用户陷入漏洞。Torres 使用符号分析和现金流分析的方法针对每类蜜罐合约给出了启发式自动检测组件, 来找出这三类合约在执行过程中的判别特征, 如: 基于以太坊虚拟机的蜜罐合约可以通过检测合约的控制流图中的可行路径外的基本块函数调用来识别。

Camino^[60]在 Torres 的工作上提出了一种基于机

器学习的蜜罐检测方法 HONEYBADGER, 除了从合约编译信息上提取特征之外, 还考虑了合约、合约创建者、交易发送者、其他参与者之间的资金流动特征, 最后这些特征被用于训练一个 Xgboost 蜜罐合约分类模型, 通过对以太坊 151935 个智能合约检测, HONEYBADGER 共检测出了 460 个蜜罐合约, 通过对识别结果的检验, 发现其中只有 41 个假阳性样本。

Camino 提出了一个性能优越的蜜罐检测器, 在大多数蜜罐类型中都表现出了很高的识别准确率。但算法在先进性设计、以及假阳性样本出现的 3 种蜜罐类型上进行仍然存在提升空间。

3)暗网交易

打击暗网是一场打地鼠游戏, “当一个暗网关闭时, 另一个暗网就会冒出来取而代之, 纵使数字货币价格变动, 对暗网参与者的影响也十分有限”。因此, 持续化地揭露区块链中的暗网实体是打击此类活动的关键。

Kanemura^[32]提出了一种基于比特币交易记录的投票分类模型用于自动识别暗网交易实体。该方法首先收集到去匿名化的暗网实体的比特币地址和对应的交易记录, 由于一个暗网实体可能有多个比特币地址, 通过提取这些地址的交易特征输入到决策树分类器中, 模型将会对属于同一实体的多个地址分别进行投票分类, 当这些地址的投票结果中被投“非法”类别的票数与投“正常”类别的票数比例大于一定阈值时, 则将该实体判定为暗网交易实体。Kanemura 指出交易手续费是识别此类行为的关键特征, 这可能是由于暗网交易者急于确认交易而设置出更高的手续费。

该方法在超过 20 万个比特币地址的实验数据集取得了 70% 以上的准确率和 60% 以上的召回率, 性能仍然有较大的提升空间。同时, 在数据类别不平衡(暗网实体只有 372 个)问题上, 算法也没有做出更合理的设计。

4) 市场操纵

加密货币市值快速上涨的事实背后是否存在市场操纵行为? Chen^[24]基于 2013 年 Mt.Gox 事件泄露的交易所记录, 研究了 Mt.Gox 交易所中三类账户的交易模式: 极大额交易账户、极小额交易账户和普通账户, 通过对这三类账户的交易图矩阵进行奇异值分解, 以捕捉三类账户的交易特征。然后作者根据这三类账户的奇异向量与比特币价格的对数变换序列求取皮尔逊相关系数, 发现极大极小两种异常账户交易都与比特币价格密切相关, 而普通账户的相关系数小。最后, Chen 对奇异向量排序提取出核心异常账户, 通过研究这些账户的基础交易网络, 发现了一些异常交易模式, 如: 自循环、双向、三角, 这些模式被认为是在 Mt.Gox 交易所中存在市场操纵的证据。

5) 勒索软件

加密货币因其突出的隐匿性而常被作为勒索软件的支付工具。Conti^[25]针对 2013 年到 2017 年出现过的勒索软件, 在比特币交易上进行了模式分析, 发现这些勒索软件对应的地址涉及的交易金额通常是固定的, 且交易集中在一段时间内。因此, 从时间和勒索金额两个属性上, 就可以较好的区分出这些勒索软件资金流。但勒索软件与赌博平台在区块链上的交易模式十分相似, 由于比特币网络的匿名性, 这使得对二者区分存在困难。

Dalal^[27]针对上述问题, 提出了针对 CoinJoin 混币交易的启发式识别方法, 在去除掉比特币交易中 CoinJoin 的影响后, 通过一种以比特币事务子图作为训练输入的堆栈机器学习模型, 建立了对勒索软件实体的识别模型, 可以更好的识别比特币交易中的勒索软件地址, 并在 82 个测试子图中取得了 85.7% 的准确率和 85.4% 的召回率, 体现了较好的识别性能, 但算法对子图特征的运算上可能会消耗较多的计算和时间资源, 这值得进一步考虑和改善。

8 技术现状分析与未来技术趋势

8.1 技术现状分析

区块链欺诈行为复杂多样, 为识别工作带来了样本少、行为变化快、匿名性强和验证困难等诸多困难。研究者们通过对各类欺诈行为机制进行剖析,

挖掘行为的标识特征, 最终形成相应的识别方法和模型。从行为类别以及每类行为的技术类别两个方面对这些方法和模型进行, 可以发现: a. 在数据资料方面, 这些方法主要以区块链交易数据、智能合约数据等链上数据为主。b. 在特征层面, 取决于行为类别, 一些欺诈行为的标识特征十分相近, 而一些则存在较大差别。c. 在技术方面, 它们以启发式学习和机器学习算法为主要识别技术, 对挖掘出的标识特征进行分析与识别。

尽管这些识别技术对各类欺诈行为的识别均取得了较高的准确率, 但其在实际应用上仍存在不足, 这体现在基于启发式学习的识别方法受到的条件限制多、自动化识别程度低。基于机器学习的识别方法则主要在可解释性以及模型训练等方面受到限制。这些不足之处具体表现为以下几点:

(1) 机器学习类的识别方法对标注数据需求大, 可解释性需要加强。由于区块链参与者的隐私意识越来越高、欺诈行为变化快, 对各类欺诈行为标注样本进行完整性收集的难度很大。当前机器学习类的识别方法仍以完全监督学习为主, 其识别性能对标注样本有较大依赖性。一些研究者在此问题上进行了改进, 提出了基于半监督学习^[39]、主动学习^[14]、增量学习^[37]的欺诈行为识别技术, 使得识别方法对标注数据的依赖降低, 但在识别准确率以及场景限制上仍需要进一步提升。另外, 此类识别方法大都基于提取的统计特征进行分类。这些统计信息的粒度集中于交易或行为层面, 比较粗放, 所提供的可解释性说服力不强。尤其是神经网络方法, 参数化的嵌入特征以及黑盒模型下的识别结果, 难以在实际监管取证中得到应用。

(2) 识别方法具有较多限制条件, 如特定行为、特定平台。针对不同的行为和平台, 需要重新训练新的模型。而当欺诈行为发生变化时, 这类方法则很有可能失效或性能下降, 无法适应监管的发展, 难以应用于宏观层面欺诈行为系统性风险的捕获。一些系统性的应用, 通常侧重于判断某笔交易或某个实体是正常亦或非法, 而非必要识别出此交易或实体归属何种特定的欺诈行为, 这要求识别方法需要把握欺诈行为的共性特征, 同时具有较强的泛化性能。一些研究者对具有通用性的识别方法进行了探索^[12-13], 这些方法不对行为类别加以区分, 提取潜在的共性交易特征, 从而将交易实体分为非法节点和正常节点两种。目前这些方法的识别查错率表现欠佳, 需要进一步改善。

(3) 一些特别的行为仍缺少相关的研究。如跨链

洗钱、去中心化金融诈骗,正在扮演欺诈行为中更为重要的角色。此类行为并不是孤立存在,通常与多个区块链平台,以及现实中的实体存在关联。由于区块链账户的匿名性,以及不同区块链数据异构不互通,跨域数据的大容量和数据失衡的特点,使得一般识别方法并不适用于此类行为的检测。跨链、跨域行为的分析复杂度高,技术挑战大,主要体现在链间以及链上和链下如何形成关联的问题上。在现有的少数方法中使用到的关联方法有:通过IP关联链上链下信息^[56],通过交易金额与交易时间关联链与链之间的交易^[38]。而在遇到IP变换等问题时,通过IP关联链上链下的方法在准确性上难以得到保证^[61-63]。通过交易信息关联多链则存在一定的偶然性,如在相近时间内,出现其他相近数额的交易,就可能会出现判断失误。如何实现更可靠的跨链与链上链下关联,还需要进一步探索。

8.2 未来技术趋势

基于上述分析,当前区块链欺诈行为识别技术在穿透性、通用性和可解释性上还需要进一步提升,同时,解决标注数据的限制问题仍是识别技术的关键问题。因此,这要求未来区块链欺诈行为识别技术将不再局限于完全有监督的场景,不再局限于单一链上数据,不再局限于特定行为,要求识别技术更深入地把握行为的本质特征。基于这些需求,本文给出了一些未来技术趋势以供参考。

(1)半/无监督的区块链欺诈行为识别技术。基于半/无监督的识别方法在实际应用中具有极大的便利性,现有的一些工作从半监督学习、主动学习、增量学习的角度尝试了减少识别算法的数据限制,但大都只是简单的引入了机器学习中半/无监督的训练技巧或算法,并未从特征等角度给出更具有解释性的方法。而区块链欺诈行为通常验证困难,此类方法在实际应用中难以取证验证。如何更合理的减少识别方法对标注数据的依赖,仍然是欺诈行为识别方法需要攻克的问题。

(2)跨链和链上链下结合的多维识别方法。区块链发展到目前为止,存在大量的区块链系统。一些欺诈行为并不是孤立存在于单个区块链中,而是与多个区块链平台以及链下实体存在关联。其行为场景复杂多样,所采用的技术也存在很多不同。这就使得此类行为在不同的区块链系统与链下平台中的信息具有较大的复杂性。相应地,这些不同平台的数据具有明显的多源性、异构性。这样的多源异构性,再叠加区块链系统的匿名性、开放性,使得此类行为模式复杂、隐蔽。这些问题在现有方法的解决方案中都

难以确保关联的准确性。如何实现跨域跨链多源数据融合关联以及如何识别跨链跨域的真实模式,是识别技术中亟待解决的关键问题之一。

(3)具有通用性(非特定行为)的识别技术。通用性识别方法并不局限于行为类别,而是通过挖掘不同欺诈行为的共性特征,以实现非法/常规实体的识别,可以很好的应用于一般性的行为识别与态势分析中。现有的一些通用性识别方法在识别查错率上会出现性能较差的情况,这可能是对共性特征的重要性不加区分所导致的。由于一些欺诈行为在特征上的差异非常大,如:洗钱和庞氏骗局。而一些行为的特性则很相似,如:钓鱼与庞氏骗局。如何更有效的提取并利用共性特征,从而实现通用性欺诈行为识别,是一个值得探讨的问题。

9 总结

区块链监管是目前广受各界关注的研究领域。本文总结了现有区块链欺诈行为识别工作与进展,包括:提出了一个区块链欺诈行为识别框架,用于总结区块链反欺诈研究方法;从不同行为类别对现有研究工作进行了归纳整理;针对现有区块链欺诈行为识别工作面临的重大挑战,探讨了未来区块链欺诈行为识别技术的发展趋势。

参考文献

- [1] Zhu Y, Qin Y, Zhou Z Y, et al. Digital Asset Management with Distributed Permission over Blockchain and Attribute-Based Access Control[C]. 2018 IEEE International Conference on Services Computing, 2018: 193-200.
- [2] Dilley J, Poelstra A, Wilkins J, et al. Strong Federations: An Interoperable Blockchain Solution to Centralized Third-Party Risks[EB/OL]. 2016: arXiv: 1612.05491. <http://arxiv.org/abs/1612.05491>.
- [3] Lundbaek L N, D'Iddio A C, Huth M. Optimizing Governed Blockchains for Financial Process Authentications[EB/OL]. 2016: arXiv: 1612.00407. <http://arxiv.org/abs/1612.00407>.
- [4] Biswas K, Muthukumarasamy V. Securing Smart Cities Using Blockchain Technology[C]. 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems, 2016: 1392-1393.
- [5] Lee B, Lee J H. Blockchain-Based Secure Firmware Update for Embedded Devices in an Internet of Things Environment[J]. The Journal of Supercomputing, 2017, 73(3): 1152-1167.
- [6] Kim H M, Laskowski M. Toward an Ontology-Driven Blockchain Design for Supply-Chain Provenance[J]. Intelligent Systems in Accounting, Finance and Management, 2018, 25(1): 18-27.
- [7] Wüst K, Gervais A. Do you Need a Blockchain? [C]. 2018 Crypto Valley Conference on Blockchain Technology, 2018: 45-54.

- [8] Fleder M, Kester M S, Pillai S. Bitcoin Transaction Graph Analysis[EB/OL]. 2015: arXiv: 1502.01657. <http://arxiv.org/abs/1502.01657>.
- [9] Mikkel A H, Haohua S Y, Klaus C L, et al. Breaking Bad: De-Anonymising Entity Types on the Bitcoin Blockchain Using Supervised Machine Learning[C]. *Hawaii International Conference on System Sciences*. 2018, 1-10.
- [10] Wu J 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*, 2022, 52(2): 1156-1166.
- [11] Hamilton W L. Graph Representation Learning[J]. *Synthesis Lectures on Artificial Intelligence and Machine Learning*, 2020, 14(3): 1-159.
- [12] Weber M, Domeniconi G, Chen J, et al. Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics[EB/OL]. 2019: arXiv: 1908.02591. <http://arxiv.org/abs/1908.02591>.
- [13] Oliveira C, Torres J, Silva M I, et al. GuiltyWalker: Distance to Illicit Nodes in the Bitcoin Network[EB/OL]. 2021: arXiv: 2102.05373. <http://arxiv.org/abs/2102.05373>.
- [14] 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[C]. *The First ACM International Conference on AI in Finance*, 2020: 1-8.
- [15] Alarab I, Pragoonwit S, Nacer M I. Competence of Graph Convolutional Networks for Anti-Money Laundering in Bitcoin Blockchain[C]. *The 2020 5th International Conference on Machine Learning Technologies*, 2020: 23-27.
- [16] Chen W L, Zheng Z B. Blockchain Data Analysis: Current Situation, Trends and Challenges[J]. *Journal of Computer Research and Development*, 2018, 55(9): 1853-1870.
(陈伟利, 郑子彬. 区块链数据分析: 现状、趋势与挑战[J]. *计算机研究与发展*, 2018, 55(9): 1853-1870.)
- [17] Bartoletti M, Lande S, Loddo A, et al. Cryptocurrency Scams: Analysis and Perspectives[J]. *IEEE Access*, 2021, 9: 148353-148373.
- [18] Wu L, Hu Y F, Zhou Y J, et al. Towards Understanding and Demystifying Bitcoin Mixing Services[C]. *The Web Conference 2021*, 2021: 33-44.
- [19] Chen L, Peng J Y, Liu Y, et al. Phishing Scams Detection in Ethereum Transaction Network[J]. *ACM Transactions on Internet Technology*, 21(1): 10.
- [20] Bartoletti M, Pes B, Serusi S. Data Mining for Detecting Bitcoin Ponzi Schemes[C]. *2018 Crypto Valley Conference on Blockchain Technology*, 2018: 75-84.
- [21] Chen W L, Zheng Z B, Cui J H, et al. Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology[C]. *The 2018 World Wide Web Conference on World Wide Web - WWW'18*, 2018: 1409-1418.
- [22] Chen W M, Li X R, Sui Y T, et al. SADPonzi: Detecting and Characterizing Ponzi Schemes in Ethereum Smart Contracts[J]. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 5(2): 26.
- [23] Torres C F, Steichen M, State R. The Art of the Scam: Demystifying Honeypots in Ethereum Smart Contracts[C]. *The 28th USENIX Conference on Security Symposium*, 2019: 1591-1607.
- [24] Chen W L, Wu J, Zheng Z B, et al. Market Manipulation of Bitcoin: Evidence from Mining the Mt. Gox Transaction Network[C]. *IEEE INFOCOM 2019 - IEEE Conference on Computer Communications*, 2019: 964-972.
- [25] Conti M, Gangwal A, Ruj S. On the Economic Significance of Ransomware Campaigns: A Bitcoin Transactions Perspective[J]. *Computers and Security*, 2018, 79(C): 162-189.
- [26] Cai X Q, Deng Y, Zhang L, et al. The Principle and Core Technology of Blockchain[J]. *Chinese Journal of Computers*, 2021, 44(1): 84-131.
(蔡晓晴, 邓尧, 张亮, 等. 区块链原理及其核心技术[J]. *计算机学报*, 2021, 44(1): 84-131.)
- [27] Dalal S, Wang Z H, Sabharwal S. Identifying Ransomware Actors in the Bitcoin Network[EB/OL]. 2021: arXiv: 2108.13807. <http://arxiv.org/abs/2108.13807>.
- [28] Reid F, Harrigan M. An Analysis of Anonymity in the Bitcoin System[M]. *Security and Privacy in Social Networks*. New York: Springer, 2013: 197-223.
- [29] Jourdan M, Blandin S, Wynter L, et al. Characterizing Entities in the Bitcoin Blockchain[C]. *2018 IEEE International Conference on Data Mining Workshops*, 2018: 55-62.
- [30] Ranshous S, Joslyn C A, Kreyling S, et al. Exchange Pattern Mining in the Bitcoin Transaction Directed Hypergraph[C]. *International Conference on Financial Cryptography and Data Security*, 2017: 248-263.
- [31] Hu Y N, Seneviratne S, Thilakarathna K, et al. Characterizing and Detecting Money Laundering Activities on the Bitcoin Network[EB/OL]. 2019: arXiv: 1912.12060. <http://arxiv.org/abs/1912.12060>.
- [32] Kanemura K, Toyoda K, Ohtsuki T. Identification of Darknet Markets' Bitcoin Addresses by Voting Per-Address Classification Results[C]. *2019 IEEE International Conference on Blockchain and Cryptocurrency*, 2019: 154-158.
- [33] Yuan L N, Li X, Wang X D, et al. Graph Embedding Models: A Survey[J]. *Journal of Frontiers of Computer Science and Technology*, 2022, 16(1): 59-87.
(袁立宁, 李欣, 王晓冬, 等. 图嵌入模型综述[J]. *计算机科学与探索*, 2022, 16(1): 59-87.)
- [34] Goyal P, Ferrara E. Graph Embedding Techniques, Applications, and Performance: A Survey[J]. *Knowledge-Based Systems*, 2018, 151: 78-94.
- [35] Wang J H, Chen P T, Yu S Q, et al. TSGN: Transaction Subgraph Networks for Identifying Ethereum Phishing Accounts[C]. *International Conference on Blockchain and Trustworthy Systems*, 2021: 187-200.
- [36] Yuan Q, Huang B Y, Zhang J, et al. Detecting Phishing Scams on Ethereum Based on Transaction Records[C]. *2020 IEEE International Symposium on Circuits and Systems*, 2020: 1-5.
- [37] Li S C, Xu F Y, Wang R C, et al. Self-Supervised Incremental Deep Graph Learning for Ethereum Phishing Scam Detection[EB/OL]. 2021: arXiv: 2106.10176. <http://arxiv.org/abs/2106.10176>.

- [38] Yousaf H, Kappos G, Meiklejohn S. Tracing Transactions across Cryptocurrency Ledgers[C]. *The 28th USENIX Conference on Security Symposium*, 2019: 837-850.
- [39] 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.
- [40] 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.
- [41] de Balthasar T, Hernandez-Castro J. An Analysis of Bitcoin Laundry Services[C]. *Nordic Conference on Secure IT Systems*, 2017: 297-312.
- [42] Al Jawaheri H, Al Sabah M, Boshmaf Y, et al. Deanonymizing Tor Hidden Service Users through Bitcoin Transactions Analysis[J]. *Computers & Security*, 2020, 89: 101684.
- [43] Li F, Li Z R, Zhao H. Research on the Progress in Cross-Chain Technology of Blockchains[J]. *Journal of Software*, 2019, 30(6): 1649-1660.
(李芳, 李卓然, 赵赫. 区块链跨链技术进展研究[J]. *软件学报*, 2019, 30(6): 1649-1660.)
- [44] Yuan Y, Wang F Y. Blockchain: The State of the Art and Future Trends[J]. *Acta Automatica Sinica*, 2016, 42(4): 481-494.
(袁勇, 王飞跃. 区块链技术发展现状与展望[J]. *自动化学报*, 2016, 42(4): 481-494.)
- [45] Bartoletti M, Carta S, Cimoli T, et al. Dissecting Ponzi Schemes on Ethereum: Identification, Analysis, and Impact[J]. *Future Generation Computer Systems*, 2020, 102(C): 259-277.
- [46] Lou Y C, Zhang Y M, Chen S P. Ponzi Contracts Detection Based on Improved Convolutional Neural Network[C]. *2020 IEEE International Conference on Services Computing*, 2020: 353-360.
- [47] Fan S H, Xu H R, Fu S J, et al. Smart Ponzi Scheme Detection Using Federated Learning[C]. *2020 IEEE 22nd International Conference on High Performance Computing and Communications; IEEE 18th International Conference on Smart City; IEEE 6th International Conference on Data Science and Systems*, 2020: 881-888.
- [48] Yu S Q, Jin J, Xie Y Y, et al. Ponzi Scheme Detection in Ethereum Transaction Network[C]. *International Conference on Blockchain and Trustworthy Systems*, 2021: 175-186.
- [49] Wang L, Cheng H, Zheng Z B, et al. Ponzi Scheme Detection via Oversampling-Based Long Short-Term Memory for Smart Contracts[J]. *Knowledge-Based Systems*, 2021, 228: 107312.
- [50] Liang Y Z, Wu W J, Lei K, et al. Data-Driven Smart Ponzi Scheme Detection[EB/OL]. 2021: arXiv: 2108.09305. <http://arxiv.org/abs/2108.09305>.
- [51] Ibba G, Pierro G A, Di Francesco M. Evaluating Machine-Learning Techniques for Detecting Smart Ponzi Schemes[C]. *2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain*, 2021: 34-40.
- [52] Xia P C, Wang H Y, Gao B Y, et al. Trade or Trick?[J]. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 2021, 5(3): 1-26.
- [53] Holub A, O'Connor J. COINHOARDER: Tracking a Ukrainian Bitcoin Phishing Ring DNS Style[C]. *2018 APWG Symposium on Electronic Crime Research*, 2018: 1-5.
- [54] Yuan Z H, Yuan Q, Wu J J. Phishing Detection on Ethereum via Learning Representation of Transaction Subgraphs[C]. *International Conference on Blockchain and Trustworthy Systems*, 2020: 178-191.
- [55] Chen W L, Guo X F, Chen Z G, et al. Phishing Scam Detection on Ethereum: Towards Financial Security for Blockchain Ecosystem[C]. *The Twenty-Ninth International Joint Conference on Artificial Intelligence*, 2020: 4506-4512.
- [56] Phillips R, Wilder H. Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites[C]. *2020 IEEE International Conference on Blockchain and Cryptocurrency*, 2020: 1-8.
- [57] Wen H X, Fang J Y, Wu J J, et al. Transaction-Based Hidden Strategies Against General Phishing Detection Framework on Ethereum[C]. *2021 IEEE International Symposium on Circuits and Systems*, 2021: 1-5.
- [58] Andryukhin A A. Phishing Attacks and Preventions in Blockchain Based Projects[C]. *2019 International Conference on Engineering Technologies and Computer Science*, 2019: 15-19.
- [59] Bian S Q, Deng Z P, Li F, et al. IcoRating: A Deep-Learning System for Scam ICO Identification[EB/OL]. 2018: arXiv: 1803.03670. <http://arxiv.org/abs/1803.03670>.
- [60] Camino R, Torres C F, Baden M, et al. A Data Science Approach for Detecting Honey pots in Ethereum[C]. *2020 IEEE International Conference on Blockchain and Cryptocurrency*, 2020: 1-9.
- [61] Neudecker T, Hartenstein H. Could Network Information Facilitate Address Clustering in Bitcoin? [C]. *International Conference on Financial Cryptography and Data Security*, 2017: 155-169.
- [62] Fanti G, Viswanath P. Deanonymization in the Bitcoin P2P Network[C]. *The 31st International Conference on Neural Information Processing Systems*, 2017: 1364-1373.
- [63] Biryukov A, Feher D. Privacy and Linkability of Mining in Zcash[C]. *2019 IEEE Conference on Communications and Network Security*, 2019: 118-123.
- [64] Androulaki E, Karame G O, Roeschlin M, et al. Evaluating User Privacy in Bitcoin[C]. *International Conference on Financial Cryptography and Data Security*, 2013: 34-51.
- [65] Kappos G, Yousaf H, Maller M, et al. An Empirical Analysis of Anonymity in Zcash[C]. *The 27th USENIX Conference on Security Symposium*, 2018: 463-477.
- [66] Zhang A, Bai X Y. Survey of Research and Practices on Blockchain Privacy Protection[J]. *Journal of Software*, 2020, 31(5): 1406-1434.
(张奥, 白晓颖. 区块链隐私保护研究与实践综述[J]. *软件学报*, 2020, 31(5): 1406-1434.)
- [67] Möser M, Soska K, Heilman E, et al. An Empirical Analysis of Traceability in the Monero Blockchain[EB/OL]. 2017: arXiv: 1704.04299. <http://arxiv.org/abs/1704.04299>.
- [68] Sun X W, Yang T, Hu B. LSTM-TC: Bitcoin Coin Mixing Detection Method with a High Recall[J]. *Applied Intelligence*, 2022, 52(1): 780-793.
- [69] Wang Z P, Chaliasos S, Qin K H, et al. On how Zero-Knowledge Proof Blockchain Mixers Improve, and Worsen User Pri-

vacy[EB/OL]. 2022: arXiv: 2201.09035. <http://arxiv.org/abs/2201.09035>.

- [70] Béres F, Seres I A, Benczúr A A, et al. Blockchain is Watching You: Profiling and Deanonimizing Ethereum Users[C]. *2021 IEEE International Conference on Decentralized Applications and Infrastructures*, 2021: 69-78.

- [71] Tang Y J, Xu C, Zhang C, et al. Analysis of Address Linkability in Tornado Cash on Ethereum[C]. *China Cyber Security Annual Conference*, 2022: 39-50.

- [72] Akcora C G, Purusotham S, Gel Y R, et al. How to not Get Caught when you Launder Money on Blockchain? [EB/OL]. 2020: arXiv: 2010.15082. <http://arxiv.org/abs/2010.15082>.



李广 于电子科技大学获得硕士学位。现于中山大学攻读博士学位。CCF 学生会员, 研究兴趣包括区块链, 数据挖掘, 机器学习, 图模式识别。Email: liguang7@mail2.sysu.edu.cn



陈梓钊 于中山大学获得学士学位。现于中山大学攻读硕士学位。研究兴趣包括区块链, 图数据挖掘。Email: chenzd8@mail2.sysu.edu.cn



卞静 于中山大学获得博士学位, 中山大学副教授, 硕士生导师。CCF 专业会员, 研究领域为机器学习, 区块链技术, 网络空间安全。Email: mcsbj@mail.sysu.edu.cn



周杰英 于中山大学获得博士学位, 中山大学副教授, 硕士生导师。CCF 专业会员, 研究领域为网络空间安全, 计算机网络, 车联网路由协议, 边缘计算, 区块链。Email: isszjy@mail.sysu.edu.cn



吴维刚 于香港理工大学获得博士学位, 中山大学教授, 博士生导师。CCF 专业会员, 研究领域为网络与分布式计算, 云计算, 分布式机器学习, 区块链。Email: wuweig@mail.sysu.edu.cn