文章编号:1674-2974(2022)10-0119-11 DOI:10.16339/j.cnki.hdxbzkb.2022288

数字货币交易所洗钱行为检测

钟增胜[1,2],朱纯瑶[1],杨逸飞[1],廖忻橙[1],王任之[1],赵颖[1†],周芳芳[1],施荣华[1],秦拯[3]
(1. 中南大学 计算机学院,湖南 长沙 410075;
2. 重庆工商大学 人工智能学院,重庆 400067;
3. 湖南大学 信息科学与工程学院,湖南 长沙 410082)

摘 要:数字货币交易中的洗钱行为区别于传统金融犯罪形态,传统反洗钱技术手段难以直接适用.针对数字货币交易所面对的洗钱行为检测需求和检测难点,通过定义交易行为,构建了一个层次化加权的交易行为特征描述体系,提出了一个结合孤立点检测和小类簇检测的数字货币交易行为异常检测方法,实现从交易行为到交易用户的洗钱可疑程度的量化度量.在真实数字货币交易所数据集上进行评估实验,结果显示,异常交易行为、可疑洗钱用户、显著性异常交易行为和隐蔽性异常交易行为的检测准确率分别为96.02%、95.05%、95.83%和95.81%,均优于基准算法.同时,本文算法的特征体系能对检测结果做出有效解释,帮助数字货币交易所安全员快速开展后续调查和取证工作.

关键词:数字货币;异常检测;反洗钱;孤立点检测
中图分类号:TP391.7 **文献标志码**:A

Money Laundering Detection for Cryptocurrency Transactions

ZHONG Zengsheng[1,2], ZHU Chunyao[1], YANG Yifei[1], LIAO Xincheng[1], WANG Renzhi[1], ZHAO Ying[1†], ZHOU Fangfang[1], SHI Ronghua[1], QIN Zheng[3]
(1. School of Computer Science and Engineering, Central South University, Changsha 410075, China;
2. School of Artificial Intelligence, Chongqing Technology and Business University, Chongqing 400067, China;
3. College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China)

Abstract: Money laundering in cryptocurrency transactions is differentiated from traditional financial crimes due to its strong anonymity and decentralization. The existing anti-money laundering techniques cannot be directly applied to cryptocurrency transactions. Considering the traceability, interpretability, and measurability of money laundering crime forensics, this paper designs a four-stage money laundering detection approach: (1) defining a set of transactions of a user in a period as a transaction behavior; (2) constructing a set of features to characterize transaction behaviors; (3) adopting outlier detection and small cluster detection methods to find out loud and subtle anoma-

* **收稿日期**:2021-06-23
基金项目:国家自然科学基金资助项目(61872388, 62072470), National Natural Science Foundation of China(61872388, 62072470);湖南省自然科学基金资助项目(2021JJ30881), Natural Science Foundation of Hunan Province(2021JJ30881)
作者简介:钟增胜(1974—),男,江西萍乡人,中南大学博士研究生
† 通信联系人,E-mail: zhaoying@csu.edu.cn

lous transactions; (4) analyzing the suspicious score distributions of users and calculating a suspected-launderer value for each of them. To evaluate the performance of our proposed method, a real-world money laundering dataset is obtained and experimentally evaluated. The experiment results show that our approach obtains 96.02%, 95.05%, 95.83%, and 95.81% accuracy in terms of abnormal transaction behaviors, suspected money launderers, loud abnormal transactions, and subtle abnormal transactions, respectively, all better than benchmark algorithms. Moreover, the carefully-designed features of transaction behaviors can offer supportive interpretations for the detection results and help exchange security officers to carry on further investigations and crime forensics.

Key words: cryptocurrency; anomaly detection; anti-money laundering; outlier detection

洗钱是一种常见金融犯罪行为,它将非法所得的金融资产通过投资或交易等手段进行掩饰,使其在形式上合法化[1]. 洗钱通常分为浸泡、分层和集成三个阶段. 在浸泡阶段,洗钱者将非法资金投入金融体系;在分层阶段,洗钱者通过多层金融交易使非法所得脱离其来源;在集成阶段,清洗过的非法所得与合法收入混合,再次进入合法金融账户. 传统洗钱手段主要有地下钱庄清洗赃款和空头公司虚假贸易等,洗钱过程通常伴有大额交易、高频交易、关联交易、闲置账户被突然启用、开户后立即销户等行为[2]. 这些行为可以通过规则匹配、数据挖掘、图分析等技术和方法,在银行、保险和证券等传统金融形态的交易记录中分析出来,因此洗钱犯罪难以完全隐匿.

近几年,数字货币交易开始成为新洗钱手段. 数字货币交易所是交易数字货币的主要场所,它采用完全不同于传统金融形态的运行与管理机制,主要特点包括:7×24 小时服务、全网络化交易、无严格真实身份认证、无清算中心集中处理数据与监控交易. 这种低成本、快速、强匿名、去中心化的金融交易场所给投资者带来了便捷和商机[3],也滋生了新的洗钱行为手段.

洗钱者用法币购买数字货币或向交易所个人账户充入数字货币以完成非法资金入场,然后通过币币交易分散资金并利用币种间差价赚取利润以混合非法资金和合法收入,最后卖出数字货币获得法币或直接从交易所转出数字货币,完成非法资金出场. 洗钱者为了隐匿行踪,往往会进行错综复杂的入场、币币交易与出场操作,并减少大额与频繁交易. 再加上数字货币交易具有强匿名和去中心化等特点,传统反洗钱技术手段难以直接适用,这给挖掘洗钱线索、鉴别洗钱行为和打击洗钱犯罪带来了新的挑战.

本文通过与S数字货币交易所的合作,共同探索面向数字货币交易的洗钱行为检测方法. 首先,梳理业务特点、设计需求和设计难点. 然后,从交易行为定义、交易行为建模、异常行为检测和可疑用户识别四阶段来检测洗钱行为. 最后,进行多组对比实验. 结果显示,本文方法在显著性和隐蔽性洗钱行为检测以及可疑洗钱用户识别方面都优于参考算法.

本文的主要创新点包括两个方面:构建了一个数字货币交易所交易行为的特征描述体系;设计了一个面向数字货币交易所的洗钱行为与洗钱用户检测方法. 该特征描述体系和洗钱行为检测方法能为识别数字货币这种新金融形态的洗钱犯罪行为提供技术支持,也能为后续相关研究提供借鉴.

1 相关工作

1.1 洗钱行为检测

早期反洗钱主要采用基于规则的检测模型,例如:Han 等人[4]设置了金融风险阈值来识别大额交易、高频交易等可疑交易行为;Rajput 等人[5]设计了一个基于语义 web 规则语言的反洗钱专家系统. 随着金融活动日趋复杂,许多学者将数据挖掘和机器学习技术用于反洗钱,比如:Rohit 等人[6]提出聚类技术是反洗钱的有力工具;Wang 等人[7]采用最小生成树对银行账户聚类,并利用类簇间差异鉴别洗钱账户;Tai 等人[8]利用支持向量机识别具有快速开销户、启用闲置账户等可疑交易行为的银行账户. 近年来,基于网络模型的反洗钱技术逐步流行,Anacpapa 图分析工具[9]是早期典型代表,随后出现了 Analyst's

Notebook[10]和 Netmap[11]等金融犯罪网络分析工具.然而,现有反洗钱技术主要面向传统金融形态,很难直接应对数字货币这类新兴金融形态.

1.2 数字货币交易数据分析

数字货币交易可以发生在区块链上和数字货币交易所内部,因此交易数据分为区块链交易数据和交易所交易数据.区块链交易数据完全公开且易于获取,近年来有许多研究分析此类数据.

在数字货币的核心特性研究方面,一些学者通过分析区块链交易数据来比较不同数字货币的去中心化[12]、匿名性[13]和安全性[14]等核心特性.在数字货币的交易模式研究方面,有研究从区块链交易数据中分析洗钱交易模式[15]、归纳链式[16]等典型交易模式特征[17].在数字货币的异常交易研究方面,学者们主要关注区块链交易中的勒索[18-19]、空投糖果和贪婪注资[20]等异常现象.

数字货币交易所出现较晚,2017年币安交易所推出了相对丰富且完善的数字货币交易业务后,才逐步带动了交易所的成交量.交易所的交易数据属于私有数据,目前关于此类数据的研究相对较少.有学者通过分析交易所数据来了解交易市场的发展情况,及时预警交易风险.Elbahrawy等人[21]使用统计图表展示2013年4月以来重要数字货币的市场份额分布和成交量;Yue等人[22]设计了可视化分析系统BitExTract,用来分析比特币交易所在交易所市场间的交易模式演变.基于此,本研究与某数字货币交易所展开深度合作,使用该交易所脱敏的交易数据来开展研究.

2 相关概念与数据抽象

2.1 相关概念

数字货币交易所是数字货币间、数字货币与法币间交易撮合的平台,是数字货币交易流通和价格确定的主要场所.S数字货币交易所规定,一个手机号可注册一个交易账号,一个交易账号对应一个交易所数字钱包.钱包记录了某个人用户在S交易所当前持有的数字货币币种及对应余额.

个人账号在数字货币交易所可以进行的交易操作主要有3类:1)买币与卖币(数字货币与法币间的兑换).交易所内的商家用户可以提供数字货币与法币的兑换服务.买币操作是指个人用户用法定货币(人民币、美元等)向商家用户购买数字货币(比特币、莱特币等)并存入数字钱包.卖币操作是个人用户将数字钱包中的数字货币卖给商家用户并获得法定货币.每个商家提供的数字货币和法币的币种、价格、数量、付款方式和汇率会有细微差异并随时间波动.2)充币与提币(同种数字货币间的流转).个人账户数字钱包里的每种数字货币都有一个对应区块链的链上地址.充币是从个人所拥有的其他链上地址或其他交易所数字钱包向该地址充入一定数额的同种数字货币.提币是充币的反向操作.充提币可以实现同种数字货币在不同交易所数字钱包间的流转.3)币币交易(不同数字货币间的交易).币币交易是用一种数字货币作为计价单位去兑换另一种数字货币,比如用BTC(比特币)定价SLU(Silubium)[23]就形成SLU/BTC交易对,该交易对的价格代表买入/卖出1单位SLU需要支付/获得多少单位BTC.币币交易需要确定采用限价或市价交易方式.限价交易需设定买入/卖出价格,待市场价格波动到设定价格便可成交.市价交易即按当前市场上最新成交价成交.

2.2 数据抽象

本文使用的数字货币交易所交易数据(已脱敏)由合作方S数字货币交易所提供.该数据可以抽象为一个多维表格型数据,字段包括:交易序号、用户账号、交易时间、交易类型、交易额、交易币种、交易地址.本文使用数据的时间跨度为2018年4月23日至2020年4月8日,涉及3万个用户,共计1 000多万条真实交易数据.交易数据样例见表1.

表1 数字货币交易所交易数据样例

Tab.1 Samples of transaction data in a cryptocurrency exchange

交易序号	用户账号	交易时间	交易类型	交易额	交易币种	交易地址
1134	338345	2018-05-23 09:03:24	0(充币交易)	6 791.632 74	ETH	0xb75bcf……8ca10c14
1151	389366	2018-05-23 09:04:46	1(提币交易)	7 141.598 21	ETH	0x6ebaf4……8c9b131a
1249	344485	2018-05-23 09:10:11	4(买币交易)	5 000.000 00	CNYT	—
1288	344472	2018-05-23 09:10:34	5(卖币交易)	46 280.500 00	CNYT	—
1408	71662	2018-05-23 09:11:07	3(币币交易)	0.259 48	USDT	—
1409	71662	2018-05-23 09:11:07	3(币币交易)	-1.000 12	SLU	—

3 设计需求与设计难点

本文目标是设计一个面向数字货币交易的自动化洗钱行为检测算法,提高数字货币交易所安全员的日常工作效率.S数字货币交易所安全员指出算法设计要考虑洗钱行为的两大基本特点:组合性和异常性.组合性是指洗钱过程通常由多笔交易组合而成.异常性是指与洗钱相关的少量交易行为必然表现出一定的异常特性.

安全员还指出算法设计要考虑洗钱犯罪取证的三大基本要求:可追溯性、可解释性和可度量性.可追溯性是希望算法给出一个从用户到行为的二层体系,即能提供可疑洗钱用户及其相关洗钱行为.可解释性是希望算法能对检测结果给出一定的解释性理由,以辅助开展调查取证.可度量性是希望算法能定量给出用户可疑程度和交易行为异常程度,使得后续调查取证能有序展开.

算法设计需要满足的基本需求包括五个需求:(T1)定义组合性交易行为;(T2)对交易行为进行可解释性特征建模;(T3)找出异常交易行为;(T4)找出可疑洗钱用户和相关异常交易行为;(T5)能对用户可疑程度和交易行为异常程度进行量化度量.

然而,设计一个满足这五大需求的算法并不容易,面临两大设计挑战.

特征建模难(C1).预定义交易行为特征体系可以让洗钱行为检测结果具有更好的可解释性.作为新金融形态,数字货币具有全新的交易体系,不能直接借鉴面向传统金融形态的交易行为特征建模体系.因此,新算法的交易行为特征建模过程中必须与数字货币反洗钱专家深度合作,充分借鉴专家知识,并进行反复实验验证.

隐蔽性洗钱行为检测难(C2).根据专家经验,与洗钱相关的交易行为有显著性和隐蔽性两类.显著性洗钱交易行为一般会在某些特征上具有极端取值,其产生原因是急于洗钱,快进快出.但它们也可能是工作人员或职业操盘手的正常交易行为.隐蔽性洗钱交易行为会在某些特征或特征组合上表现出与正常交易行为的轻微差异,它们由沉稳的洗钱者操纵.新算法要能有效找到显著性和隐蔽性洗钱交易行为,并排除正常的显著性交易行为.

4 数字货币交易洗钱行为检测方法设计

4.1 总体流程

本文采用自底向上的思路设计数字货币交易洗钱行为检测方法,该方法的基本流程如图1所示.首先,将一个用户一段时间内的连续交易记录视作一个交易行为,并对交易行为进行特征建模;然后,将交易行为作为检测单元进行异常检测;最后,综合交易行为异常检测结果识别出可疑洗钱用户.该算法可以同时输出可疑洗钱用户及与其相关异常交易行为,帮助安全员完成自顶向下的取证过程,即:先选出可疑洗钱用户,再确定异常交易行为/时段,最后对相关交易进行逐笔人工分析.

为了满足算法设计需求(T1~T5)实现自底向上的洗钱行为检测,应对算法设计中面临的两大挑战(C1~C2),算法设计引入了多属性决策特征赋权机制、改进的局部异常因子算法和多项去噪策略等.

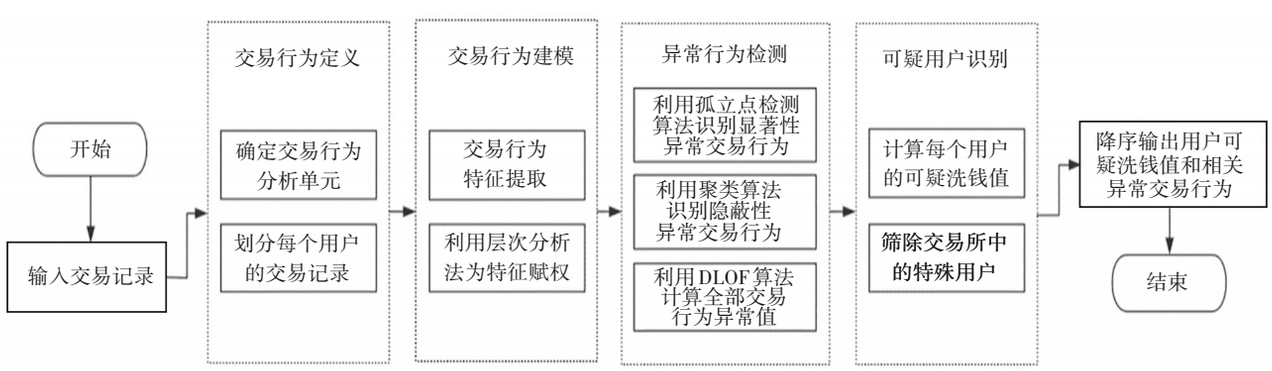

图1 自动洗钱行为检测流程图

Fig.1 Flow chart of automatic money laundering behavior detection

4.2 交易行为定义

交易行为定义主要是确定交易行为的分析单元(T1),分析单元一般可以是单次交易或组合交易.洗钱行为通常具有组合性,并且单次交易提供的信息

非常有限,因此,选择以组合交易作为分析单元.思路是将一个用户固定时间间隔内的交易集合作为分析单元,间隔设置为 10 d,这一设定基于四方面考虑:1)洗钱过程有一定时间跨度,短则几天,长则十天甚至数月;2)固定时间间隔有利于建立比较基准;3)根据S数字货币交易所提供数据的统计情况,大部分账户交易频率平均每天不足 1 笔,以 10 d 为单位可以保证每个分析单元中有多笔交易记录,便于提取交易行为的统计特性;4)金融领域经常以 10 d 为单位来进行政策调控和风险管理.

在数字货币交易所中每个用户的每一次交易会生成对应的交易记录,首先获取每个用户在其交易时间段$[t_s, t_e]$的交易数据,即其所有交易记录$\{S_1, S_2, S_3, \cdots, S_n\}$.将每个用户的交易时间段$[t_s, t_e]$划分为长度相同的 m 个分段,每段的时间间隔为 10 d,然后将第 i 号用户在第 j 个时间分段 t_j 的所有交易记录的组合,作为该用户的第 j 个交易行为,记为$T_{i_j}(1 \leqslant j \leqslant m)$.

4.3 交易行为建模

4.3.1 交易行为特征提取

交易行为特征提取是将交易数据表征为统一的、可解释的特征形态(T1),便于后续算法处理.同时,预定义特征体系可以让算法结果具有更好的可解释性(T2).本部分的难点是不能直接借鉴传统金融风险防控经验,需要重新探索数字货币交易特征描述体系(C1).通过与数字货币专家和反洗钱专家深度合作,构建一个交易行为特征描述体系.

特征描述体系从入场操作(买币和充币)、出场操作(卖币和提币)与币币交易这3种交易操作角度描述交易行为特征,共计40个特征.入场操作是一笔资金在交易所内一系列活动的起点,是分析洗钱用户交易行为的首要切入点;出场操作通过卖币与提币实现资金出场,是一笔资金在交易所内一系列操作的终点;币币交易是用一种数字货币作为计价单位去兑换另一种数字货币,是用户主要的交易活动.完整的特征描述体系见表2.

4.3.2 交易行为特征赋权

在使用特征时需要考虑不同特征在具体场景中的重要程度,因此需要给每一个特征赋权值以反映其在反洗钱场景中的重要性(T1).特征赋权需要充分考虑专家知识(C1).层次分析法[24]是解决赋权问题的常见方法,它主要有三大优点:通过两两比较的方法确定特征的相对重要性;专家可以利用自身经

表 2　数字货币交易行为特征描述体系

Tab.2　Description system of cryptocurrency transaction behavior features

序号	特征名称	分类	操作
1	入场总额	概括型	入场操作
2	入场总次数		
3	入场额均值		
4	入场频率		
5	入场币种数		
6	入场额占总交易额比	比例型	
7	入场次数占总交易次数比		
8	非工作时段入场次数占入场总次数比		
9	入场小众币种数占入场币种数比		
10	单笔最大入场额	最值型	
11	入场最大额与最小额差值		
12	最多持续入场次数		
13	最长入场间隔天数		
14	入场额离散系数	其他	
15	入场额为整数的交易次数		
16	入场额大于一万的交易次数		
17	出场总额	概括型	出场操作
18	出场总次数		
19	出场额均值		
20	出场频率		
21	出场币种数		
22	出场天数		
23	出场额占总交易额比	比例型	
24	出场次数占总交易次数比		
25	非工作时段出场次数占出场总次数比		
26	出场小众币种数占出场币种数比		
27	单日最大出场额	最值型	
28	单笔最大出场额		
29	出场最大额与最小额差值		
30	连续最多出场次数	其他	
31	出场额小于与大于均额的次数差		
32	出场后数字钱包余额为零的次数		
33	币币交易总额	概括型	币币交易
34	币币交易次数		
35	币币交易交易对数量倒数		
36	币币交易涉及币种数倒数		
37	币币交易频率		
38	币币交易次数占总交易次数比	比例型	
39	币币交易币种数占总交易币种数比		
40	非工作时段币币交易次数占该交易总次数比		

验判断特征的相对重要性;计算简单快速.因此,选用层次分析法来定量地为特征赋权,本文的特征赋权主要包括4个步骤:1)建立层次结构;2)构造判断矩阵;3)层次单排序及一致性检验;4)层次总排序及一致性检验.

第1)步中的层次框架结构以洗钱可疑度作为目标层,描述交易行为特征的入场操作、出场操作、币币交易这三个维度是中间层,40个交易行为特征作为最底层,即因素层.在第2)步中,专家比较了入场操作、出场操作和币币交易这三类交易行为特征在洗钱可疑度判断上的相对重要度,构造了第1个矩阵,然后分别对每一维度下的多个特征比较相对重要度,构造了3个矩阵.通过前两步得到的4个判断矩阵进行第3)和第4)步的计算,最终可得到特征权值矩阵.

专家认为通过层次分析法得出的权值结果能基本反映各特征对可疑洗钱交易行为判定的影响程度.从最终权值排序结果来看,最多持续入场次数和入场额大于一万的交易次数的权值最高.专家表示,这两个特征也是他们在日常反洗钱工作中最关注的,洗钱行为通常都具有持续性多次入场以及大额交易入场的特性,绝大多数洗钱行为都会在这两个特征上取值较高.而币币交易总额和非工作时段币币交易次数占该交易总次数比的权值最低,专家解释,尽管有些洗钱用户为了模糊审计线索和伪装正常用户,会进行币币交易,但也存在不少洗钱用户为了实现资金快速出入场,很少甚至不进行币币交易,这导致币币交易总额对判定可疑洗钱交易行为的影响并不大,非工作时段币币交易次数的影响则更小.

4.4 异常行为检测

根据第3节所述,洗钱行为具有异常性,因此洗钱行为检测问题可以转化为对交易行为的异常检测问题,即在交易行为特征化的基础上,通过自动化算法找到数字货币异常交易行为(T3)并量化度量异常程度(T5),为进一步识别可疑洗钱用户提供基础(T4).异常交易行为检测的难点是同时有效检测显著性和隐蔽性洗钱交易行为(C2).另外,异常交易行为检测还需要考虑到当前数据没有标签的现状,人工标记需要耗费交易所专家大量精力,而且洗钱者常常变换洗钱方式,这使数据标记工作更为困难.

本文采用无监督的孤立点检测和小类簇检测相结合的方法,解决异常交易行为检测的难点问题.孤立点检测用于识别显著性洗钱交易行为;小类簇检测用于识别隐蔽性洗钱交易行为;两者结合共同确定每个交易行为的异常程度.因此,本文的异常行为检测方法分为三个基本步骤:检测孤立点、检测小类簇和确定交易行为的异常值.

4.4.1 数字货币交易行为的孤立点检测

本文使用孤立点检测识别显著性洗钱交易行为,因为显著性洗钱行为在某些特征上具有极端取值,形成远离正常交易行为的孤立交易行为,很容易被孤立点检测方法捕获.本文采用局部异常因子(Local Outlier Factor,LOF)孤立点检测算法[25],主要考虑到以下三点因素:1)它使用相对密度来检测孤立点,适合本文的数据分布不均匀场景;2)它可以量化交易行为的异常程度;3)计算速度快、可解释性强并且应用成熟.

在S数字货币交易所提供的交易数据中,存在一定量的显著性洗钱交易行为,它们的LOF值很高.然而,低LOF值交易行为中可能存在隐蔽性洗钱交易行为.隐蔽性洗钱交易行为一般没有极端的特征取值,不容易被LOF算法检测到,因此需要进一步检测这类异常交易行为.

4.4.2 数字货币交易行为的小类簇检测

小类簇检测的目的是找到隐蔽性洗钱交易行为.隐蔽性洗钱交易行为在某些特征或特征组合上表现出与正常交易行为的微小差别.同时,由于洗钱交易行为数量一般很少,因此,隐蔽性洗钱交易行为会在交易行为聚类过程中形成一些规模较小的类簇.本文选了基于密度的噪声应用空间聚类算法[26](Density-Based Spatial Clustering of Applications with Noise,DBSCAN)对所有交易行为聚类,主要有两点考虑:1)数据集聚类成簇的数量未知,该算法无须预先指定簇的个数;2)该算法可以发现任意形状的聚类簇,具有很强的适应能力.

对全部交易行为聚类之后,算法最终会输出簇的划分结果 $C=\{C_1,C_2,\cdots,C_k\}$,簇 C_n 的规模为 $|c_n|$,即簇中包含的交易行为个数.簇内交易行为数量较少的簇称为小类簇,小类簇很可能是由某些具有相似特征的隐蔽性洗钱交易行为聚集而成,因此小类簇是更加需要关心的聚类.但是,并不需要检测出具体的小类簇,这是因为:1)小类簇的规模很难界定;2)更需要一个定量的值加入后续计算,以进一步定量地衡量交易行为的异常程度,因此,每一交易行为所在的聚类簇规模是本研究需要的信息.

根据经验,隐蔽性洗钱交易行为通常会在小类簇中,但DBSCAN聚类结果无法直接提供LOF值,因

此可以利用聚类结果,在已经获得的LOF值的基础上,考虑聚类结果带来的新信息,重新计算全部交易行为的异常值.

4.4.3　数字货币交易行为的异常值计算

通过前两个步骤,已经得到了全部交易行为的LOF值及其所在的聚类簇大小.结合前面两步的计算结果,重新计算全部交易行为的异常值,以更合理地为交易所安全员推荐值得优先关注的交易行为.

交易行为的异常值计算需要解决两个问题:1)保证显著性洗钱交易行为和隐蔽性洗钱交易行为的异常值高于正常交易行为;2)在孤立点检测中,显著性洗钱交易行为和其他交易行为的LOF值差值太大,需要平衡它们的异常值,以使得全部交易行为的异常值在一个合理的区间中.

本文设计了一个DLOF(DBSCAN-LOF)算法,该算法综合利用了孤立点检测和小类簇检测的结果.基于如下的DLOF算法公式对全部交易行为计算最终的异常值DLOF值,公式如下:

$$\mathrm{DLOF}(p)=\frac{\mathrm{LOF}(p)}{\log_2(|c_n|+1)},p\in C_n,\quad n=1,2,\cdots,K \tag{1}$$

由式(1)可知,在正常交易行为中LOF值较低,且正常交易行为一般在大类簇中,因此DLOF值较低.显著性洗钱交易行为LOF值非常高,如果某些显著性洗钱交易行为在规模相对较大的类簇,则可以明显降低其原LOF值;如果某些显著性洗钱交易行为在小类簇,则其DLOF仍然会较大.因此,DLOF算法可以根据类簇信息,平衡显著性洗钱交易行为的异常值.隐蔽性洗钱交易行为LOF值较低,一般在小类簇中,因此其DLOF值会相对较大,在一定程度上高于正常交易行为的DLOF值.

4.5　可疑用户识别

可疑用户识别基于交易行为异常值找出可疑洗钱用户和相关异常交易行为(T4),并对用户的洗钱可疑程度进行量化度量(T5).可疑用户识别的难点是检测可疑洗钱用户的同时需要排除有伪显著性洗钱行为的用户(C2),这类用户可能是特殊用户,比如:他们会持续高频交易,表现出显著性洗钱交易行为,容易被识别为可疑洗钱用户.

首先,计算每个用户的可疑洗钱值并找出相关异常交易行为.取用户前 n 个交易行为DLOF值的均值而非整体均值作为他们的可疑洗钱值,该做法是鉴于洗钱用户只会在某些时段洗钱.其中,n 通过专家的经验知识得到并在可疑用户识别中表现良好且 $n=3$. 因此,本文将第 i 号用户的可疑洗钱值定义为 U_i,计算公式如下:

$$U_i=\frac{\sum_{j=1}^{n}\mathrm{DLOF}(T_{i\_j})}{n} \tag{2}$$

根据上述方法,得到每一用户的可疑洗钱值及其相关异常交易行为.对高可疑洗钱值的用户进行分析,发现其中存在一类特殊用户,这类用户的DLOF值长期处于较高水平.交易所专家表示,他们很可能是交易所工作人员或职业操盘手,几乎每天都会进行大量交易.根据这类用户的交易习惯总结其交易行为特点,具体是:交易行为数量较多、异常值长期较高、异常值波动较小.基于这三个特点,本文设计了一个检测该类用户的方法.首先,对所有高可疑洗钱值的用户,分别计算交易行为数量、异常均值和异常波动值,然后将满足一定条件的用户标记为特殊用户.具体方法如下.

本文定义第 i 号用户的交易行为数量 m_i, 交易行为的异常均值 a_i,异常波动值 z_i. a_i 与 z_i 的计算公式分别如下:

$$a_i=\sum_{j=1}^{m_i}\mathrm{DLOF}(T_{i\_j})/m_i \tag{3}$$

$$z_i=\sum_{j=1}^{m_i}\left\{1-P_N(\mathrm{DLOF}(T_{i\_j}),\mu,\sigma)\right\}\Big/m_i \tag{4}$$

若用户满足 $m_i>k_1$(异常交易行为数量阈值),$a_i>k_2$(异常交易行为均值阈值),$z_i<k_3$(异常交易行为波动值阈值),$k_1=300,k_2=100,k_3=0.4$,则标记该用户为特殊用户.这3个阈值皆由专家的经验指导得出,并在识别交易所特殊用户的实验中表现良好.

5　实验与评估

5.1　实验准备

本实验的PC配置为CPUi9-9900K、32GRAM、机械硬盘1.5T.算法采用python语言实现,软件运行环境是python 3.7.

本文选择了如下3个参考算法用于对比实验.1)局部异常因子算法(LOF).LOF算法用来识别显著性洗钱交易行为,该实验是为了验证本文引入聚类算法的必要性.参数 $k=20$,该参数为经验值.2)基于K-Means算法的局部异常因子算法(KLOF)[27].K-Means算法是一种基于划分的聚类算法.本实验是为了对比说明选择DBSCAN算法进行聚类的有效性.参数 k 通过经典的手肘法确定,$k=33$. 3)孤立森林算法(DiForest).DiForest算法[28]结合了

DBSCAN 聚类和 iForest 孤立点检测. 本实验是为了验证结合 DBSCAN 聚类和 LOF 孤立点检测的有效性. DBSCAN 算法的参数 $\varepsilon = 4, P = 41$, iForest 算法的参数 $n_{\text{estimators}} = 300, m_{\text{features}} = 0.6$.

上述 3 个算法最后输出的是每一交易行为(用户)的异常得分. 需要给算法结果设定阈值,小于该阈值得分的交易行为(用户)被认定为异常行为(用户). 本实验中,异常交易行为的异常得分阈值 $a = 2\,000$,洗钱用户的异常得分阈值 $b = 500$. 这两个阈值的设定是考虑到该实验的正常样本与异常样本数量具有极大的不平衡性,同时这也是与交易所专家仔细讨论后的结果. 专家强调异常交易行为(洗钱用户)漏检的风险较高,因此应尽可能降低漏检风险.

5.2 数据准备

本研究从 S 数字货币交易所中随机抽取了 1 万个用户的脱敏交易数据作为本实验的测试数据集,并邀请专家对这些数据进行人工浏览、分析和标记. 测试数据集的时间跨度为 2018 年 4 月 23 日至 2020 年 4 月 8 日,共计 300 多万条真实交易记录. 根据专家的标记结果,测试数据集有 9 981 个正常用户(其中包括 230 个特殊用户),47 618 个正常交易行为. 初步发现了 19 个可疑洗钱用户和 42 个异常交易行为(显著性异常交易行为 24 个,隐蔽性异常交易行为 18 个).

5.3 指标说明

本实验通过混淆矩阵对比了 DLOF 算法以及 3 个基准算法的检测性能. 混淆矩阵是机器学习中总结模型检测结果的情形分析表,其中,正例是指异常(可疑洗钱)样本,负例是指正常(非洗钱)样本. 混淆矩阵延伸出准确率(Accuracy)、召回率(Recall)、精确率(Precision)以及 F_1 4 个评价指标.

5.4 实验结果

5.4.1 异常交易行为和可疑洗钱用户检测结果分析

表 3 从交易行为和用户两个层面分别展示了 4 种算法的实验结果. 总的来说,DLOF 算法效果最好,它在检测异常交易行为和可疑洗钱用户上的 4 个评价指标均优于其他算法,LOF 算法的效果次之,DiForest 算法的效果最差.

从指标层面来看,4 个算法的准确率都较高,这是因为正常交易行为(正常用户)数在总交易行为(用户)数中占比非常高;召回率差异较大,因为每个算法检测出的异常交易行为(异常用户)的数量差异较大,DLOF 算法的召回率明显高于参考算法;精确率均较低,其原因一是为了降低漏检风险,优先保证了召回率,二是在交易所的交易数据中异常交易行为(异常用户)极少;较低的精确率导致了较低的 F_1 值.

从单个算法层面来看,DLOF 算法的效果均为最优,这证明了本文算法的有效性. DLOF 算法检测到 29 个异常交易行为. 分析发现未检测到的 13 个异常交易行为大部分具有模式化交易的特征,例如:T_{341490_12} 循环 5 种小众数字货币的买入交易,且每笔交易的间隔时间几乎相等;T_{101022_7} 连续用不同的小众数字货币以币币交易的形式兑换同种数字货币,且以“一次大额交易数次小额交易”的模式循环交易. 算法检测失败的原因可能是在特征提取中没有考虑到与这些模式化交易行为相关的特征. DLOF 算法检测到 12 个可疑洗钱用户,检测到了未被其余 3 个算法检测到的可疑洗钱用户. LOF 算法检测到 19 个异常交易行为和 7 个可疑洗钱用户,它们均具有明显的洗钱特征. LOF 算法只检测到了 2 个隐蔽性异常交易行为,这证明了本研究引入 DBSCAN 算法的必要性. KLOF 算法只检测到 17 个异常交易行为和 6 个可疑洗钱用户,由此可见,K-Means 算法对于隐蔽性异常交易行为检测的效果不如 DBSCAN 算法,且引入 K-Means 算法反而使得对显著性异常交易行为的检测效果变差,这大概率因为它不能有效聚类数字货币交易行为,以至于许多真实的异常交易行为被划分至大类簇中,反而减弱了检测效果.

表 3 异常交易行为和可疑洗钱用户检测实验结果

Tab.3 Experimental results of abnormal transaction behaviors and suspicious traders detection

算法	异常交易行为检测				可疑洗钱用户检测			
	准确率/%	召回率/%	精确率/%	F_1/%	准确率/%	召回率/%	精确率/%	F_1/%
DLOF(本文)	96.02	69.05	1.45	2.84	95.05	63.16	2.40	4.60
LOF	95.98	45.24	0.95	1.86	94.95	36.84	1.40	2.70
KLOF	95.97	40.48	0.85	1.67	94.93	31.58	1.20	2.31
DiForest	95.94	21.43	0.45	0.88	94.89	21.05	0.80	1.54

DiForest算法效果最差,仅检测到9个显著性异常交易行为和4个具有非常显著可疑洗钱特征的用户.分析可能因为该算法对全局离群点敏感,不擅长处理局部异常点,且不适用于高维数据,它每次都是随机选取一个维度切割数据空间,建完树后仍有大量维度信息没有被使用,导致算法可靠性降低.

5.4.2　显著性和隐蔽性异常交易行为检测结果分析

表4为4个算法的显著性和隐蔽性异常交易行为检测的实验结果.DLOF算法的表现仍然最好,LOF和KLOF算法的效果次之,DiForest算法的表现相对较差.

在检测显著性异常交易行为方面,DLOF算法检测到19个显著性异常交易行为,可见DLOF算法在检测显著性异常交易行为上较为有效.分析发现该算法未检测到的5个显著性异常交易行为中有2个的可疑洗钱特征权值较低,而其余3个具有模式化交易特点,然而在本研究的交易行为特征描述中并没有与之相关的特征.LOF算法检测到17个显著性异常交易行为,效果较好但逊于DLOF算法,这证明用LOF算法检测显著性异常交易行为是有效的,也证明了引入DBSCAN聚类算法能更有效地检测显著性异常交易行为.KLOF和DiForest效果较差,分别检测到14个和9个显著性异常交易行为,且这些异常交易行为的显著性表现较强.

在检测隐蔽性异常交易行为方面,DLOF算法检测到10个隐蔽性异常交易行为,例如,T_{74654_13}无极端特征值、均在工作时间交易、连续8次出现同种交易模式(1次出场后5至6次入场)、入场额为整数的交易次数占总入场次数的60%;T_{295847_27}大额资金入场与小额资金入场交替进行、每笔交易时间间隔均为5 min左右、连续出现相同交易额的出场交易.而LOF和KLOF只分别检测到了2个和3个隐蔽性异常交易行为,DiForest算法没有检测到.该结果体现了DLOF算法检测隐蔽性异常交易行为效果较好.

表4　显著性和隐蔽性异常交易行为检测的实验结果

Tab.4　Experimental results of significant and covert abnormal transaction behaviors detection

算法	显著性异常交易行为检测				隐蔽性异常交易行为检测			
	准确率/%	召回率/%	精确率/%	F_1/%	准确率/%	召回率/%	精确率/%	F_1/%
DLOF	95.83	79.17	0.95	1.88	95.81	55.56	0.50	0.99
LOF	95.82	70.83	0.85	1.68	95.77	11.11	0.10	0.20
KLOF	95.81	58.33	0.70	1.38	95.78	16.67	0.15	0.30
DiForest	95.79	37.50	0.45	0.89	95.76	0.00	0.00	0.00

5.4.3　特殊用户检测结果分析

特殊用户是指交易所中的工作人员或职业操盘手,他们几乎每天都会进行大量交易,这导致他们的异常值容易处在较高水平,非常容易被算法检测为可疑洗钱用户,因此需要排除这类用户对交易所安全员反洗钱工作的干扰.

DLOF算法做了特殊用户筛除,然而其余3个算法并没有这一步骤.在9 981个正常用户中,特殊用户总共有230个,DLOF、LOF、KLOF与DiForest算法最终输出的可疑洗钱用户数分别占特殊用户总数的12.61%、87.39%、90.87%和95.22%,分别占算法输出的可疑洗钱用户数的5.80%、40.2%、41.8%以及43.8%.由此可见,DLOF算法最终输出的可疑洗钱用户中特殊用户占比非常少,而其他3个算法输出的可疑洗钱用户中特殊用户均占有非常大的比例,这会给交易所安全员的反洗钱工作带来严重障碍,该实验结果充分证明了在算法中加入特殊用户筛除这一步骤的必要性.

除此之外,本研究还进行了一个对比试验,即在其他3个算法中也加入特殊用户筛除这一步骤,实验结果如表5所示.4个算法对特殊用户的筛除率都较高,其中DLOF算法效果最好,筛除了230个特殊用户中的201个,4个算法筛除的相同特殊用户数达154个,这些特殊用户的日均交易次数均超过500次,日均交易额均超过10 000 CNYT(折算),该实验结果充分证明了本文特殊用户筛除方法的有效性.

表5　特殊用户检测实验结果

Tab.5　Experimental results of special traders detection

算法	准确率/%	召回率/%	精确率/%	F_1/%
DLOF	96.71	87.39	41.20	55.07
LOF	96.57	84.35	38.80	53.15
KLOF	96.53	83.48	38.40	52.60
DiForest	96.31	78.70	36.20	49.59

DLOF算法在上述2个特殊用户筛除实验中的表现均为最优,这证明了该算法可以有效降低特殊用户对安全员判断可疑洗钱用户的干扰,提高他们反洗钱工作的效率.

6 小 结

本文提出了一种面向数字货币交易所的洗钱行为检测方法,来帮助交易所安全员快速且有效地确定可疑洗钱用户及其相关洗钱交易.首先,定义了用户的交易行为,综合考虑了交易时间、交易额、交易币种、交易类型、重要程度等信息,构建了层次化加权的交易行为特征描述体系.然后,提出了一种改进的LOF算法检测出异常交易行为并量化度量异常程度.最后,综合交易行为的异常检测结果识别出可疑洗钱用户.为了评估提出的异常检测方法,本文使用真实的S数字货币交易所数据集进行实验,证明了该方法在检测异常交易行为和识别可疑洗钱用户中的有效性.

但是,本研究还存在一些局限性,具体如下:

1)参数设定困难.在本研究中,DLOF算法有3个参数,分别为 k、ε、P,其中,参数 P 描述 ε 距离内交易行为的数量,该参数极小的变化都会带来完全不同的实验结果.若该参数设置过小,则无法有效聚类具有相似特征的交易行为;若设置过大,则密度较大的两个邻近簇可能被合并为同一个簇,显著性与隐蔽性异常交易行为无法得到有效聚类,因此该参数是否设置适当对交易行为的聚类结果有较大影响.本研究的这一参数值主要根据传统方法如突变点取参法与反复实验经验得来,但该参数值未必适用于其他场景数据,研究者仍需根据场景数据的具体情况来设置该值.

2)交易行为特征描述不完全.与交易所专家深入交流讨论,确定了本文目前的交易行为特征描述体系.但是洗钱者在数字货币交易所中的行为复杂多样且可能有新的洗钱手法出现,因此,获得一个相对完整的特征体系非常困难,而且特征体系还需要定期更新.

3)实验数据集来源单一.通过与S数字货币交易所合作,得到了该交易所的交易数据,并将其用于研究.但难以获取其他交易所的交易数据.因此本研究的数据来源较为单一,无法确定算法是否具有较好的适应性.

在未来工作中,将继续研究数字货币交易所洗钱行为检测这一课题,着力解决现有的局限性,同时也希望本文的检测方法能激发更多相关的研究和应用.

参 考 文 献

[1] BRYANS D. Bitcoin and money laundering: mining for an effective solution[J]. Indiana Law Journal, 2014, 89(1): 441-472.

[2] ALEXANDER K. The international anti-money-laundering regime: the role of the financial action task force[J]. Journal of Money Laundering Control, 2001, 4(3): 231-248.

[3] 封思贤,丁佳. 数字加密货币交易活动中的洗钱风险:来源、证据与启示[J]. 国际金融研究,2019(7):25-35.
FENG S X, DING J. Money laundering risk of cryptocurrency transaction activities: source, evidence and inspiration[J]. Studies of International Finance, 2019(7): 25-35. (In Chinese)

[4] HAN J W, PEI J, YIN Y W, *et al*. Mining frequent patterns without candidate generation: a frequent-pattern tree approach[J]. Data Mining and Knowledge Discovery, 2004, 8(1): 53-87.

[5] RAJPUT Q, KHAN N S, LARIK A, *et al*. Ontology based expert-system for suspicious transactions detection[J]. Computer and Information Science, 2014, 7(1): 103-114.

[6] ROHIT K D, PATEL D B. Review on detection of suspicious transaction in anti-money laundering using data mining framework[J]. International Journal for Innovative Research in Science & Technology, 2015, 1(8): 129-133.

[7] WANG S N, YANG J G. A money laundering risk evaluation method based on decision tree[C]//2007 International Conference on Machine Learning and Cybernetics. Hong Kong: IEEE, 2007: 283-286.

[8] TAI C H, KAN T J. Identifying money laundering accounts[C]//2019 International Conference on System Science and Engineering (ICSSE). Dong Hoi, Vietnam: IEEE, 2019: 379-382.

[9] XU J J, CHEN H. CrimeNet explorer: a framework for criminal network knowledge discovery[J]. ACM Transactions on Information Systems, 2005, 23(2): 201-226.

[10] WANG J, STEIN T C, HEET T, *et al*. A WebGIS for Apollo analyst's notebook[C]//2010 Second International Conference on Advanced Geographic Information Systems, Applications, and Services. Saint Maarten, Netherlands Antilles: IEEE, 2010: 88-92.

[11] SCHIFFER E, HAUCK J. Net-map: collecting social network data and facilitating network learning through participatory influence network mapping[J]. Field Methods, 2010, 22(3): 231-249.

[12] GENCER A E, BASU S, EYAL I, *et al*. Decentralization in bitcoin and ethereum networks[C]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer Berlin Heidelberg, 2018: 439-457.

[13] MÖSER M, BÖHME R, BREUKER D. An inquiry into money laundering tools in the Bitcoin ecosystem[C]//2013 APWG

eCrime Researchers Summit. San Francisco, CA, USA: IEEE, 2013:1-14.

[14] 魏松杰,吕伟龙,李莎莎. 区块链公链应用的典型安全问题综述[J]. 软件学报,2022,33(1):324-355.
WEI S J, LÜ W L, LI S S. Overview on typical security problems in public blockchain applications[J]. Journal of Software, 2022, 33(1):324-355.(In Chinese)

[15] RANSHOUS S, JOSLYN C A, KREYLING S, *et al*. Exchange pattern mining in the bitcoin transaction directed hypergraph[C]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2017: 248-263.

[16] RON D, SHAMIR A. Quantitative analysis of the full bitcoin transaction graph[C]//Financial Cryptography and Data Security. Berlin, Heidelberg: Springer, 2013: 6-24.

[17] ISLAM R, FUJIWARA Y, KAWATA S, *et al*. Analyzing outliers activity from the time-series transaction pattern of bitcoin blockchain[J]. Evolutionary and Institutional Economics Review, 2019, 16(1):239-257.

[18] KHARRAZ A, ROBERTSON W, BALZAROTTI D, *et al*. Cutting the gordian knot: a look under the hood of ransomware attacks[C]//Detection of Intrusions and Malware, and Vulnerability Assessment. Berlin, Heidelberg: Springer, 2015: 3-24.

[19] PAQUT-CLOUSTON M, HASLHOFER B, DUPONT B. Ransomware payments in the bitcoin ecosystem[J]. Journal of Cybersecurity, 2019, 5(1):1-11.

[20] 沈蒙,桑安琪,祝烈煌,等. 基于动机分析的区块链数字货币异常交易行为识别方法[J]. 计算机学报,2021,44(1):193-208.
SHEN M, SANG A Q, ZHU L H, *et al*. Abnormal transaction behavior recognition based on motivation analysis in blockchain digital currency[J]. Chinese Journal of Computers, 2021, 44(1): 193-208.(In Chinese)

[21] ELBAHRAWY A, ALESSANDRETTI L, KANDLER A, *et al*. Evolutionary dynamics of the cryptocurrency market[J]. Royal Society open science, 2017, 4(11): 170623.

[22] YUE X W, SHU X H, ZHU X Y, *et al*. BitExTract: interactive visualization for extracting bitcoin exchange intelligence[J]. IEEE Transactions on Visualization and Computer Graphics, 2019, 25(1):162-171.

[23] ZHONG Z S, WEI S R, XU Y T, *et al*. Silkviser: A visual explorer of blockchain-based cryptocurrency transaction data[C]// Proceedings of the IEEE Conference on Visual Analytics Science and Technology. Salt Lake City: IEEE, 2020: 121-138.

[24] 刘晓悦,杨伟,张雪梅. 基于改进层次法与CRITIC法的多维云模型岩爆预测[J]. 湖南大学学报(自然科学版),2021,48(2):118-124.
LIU X Y, YANG W, ZHANG X M. Rockburst prediction of multi-dimensional cloud model based on improved hierarchical analytic method and critic method[J]. Journal of Hunan University (Natural Sciences), 2021, 48(2):118-124.(In Chinese)

[25] BREUNIG M M, KRIEGEL H P, NG R T, *et al*. LOF: identifying density-based local outliers[C]//Proceedings of the 2000 ACM SIGMOD international conference on Management of data. New York: ACM Press, 2000: 93-104.

[26] SCHUBERT E, SANDER J, ESTER M, *et al*. DBSCAN revisited, revisited[J]. ACM Transactions on Database Systems, 2017, 42(3):1-21.

[27] GAO J, HU W M, LI W, *et al*. Local outlier detection based on kernel regression[C]//Proceedings of the 20th International Conference on Pattern Recognition. Istanbul: IEEE, 2010: 585-588.

[28] IJAZ M F, ATTIQUE M, SON Y. Data-driven cervical cancer prediction model with outlier detection and over-sampling methods[J]. Sensors, 2020, 20(10):2-9.