DOI:10.16136/j.joel.2023.08.0348

基于深度残差网络的庞氏骗局合约检测方法

葛 斌*,袁 政,任 萍,彭曦晨,夏晨星

(安徽理工大学 计算机科学与工程学院,安徽 淮南 232001)

摘要:现有针对庞氏骗局智能合约的检测方法大多基于合约操作码特征和账户特征,对初步部署合约检测效果一般。对此,提出一种基于深度残差网络的庞氏骗局合约检测方法。首先,通过分析智能合约操作码特点,提出单点词嵌入编码算法(single word embedding coding algorithm,SWEC),对智能合约进行重新编码。然后,利用关键操作码提取方法,提取关键操作码(critical operation code,CO)及权重值,并以此设计关键操作码权重模块,改进深度残差网络用于合约检测。最后,在公开数据集上进行相关实验,实验结果表明,基于深度残差网络的庞氏骗局合约检测方法具有99.7%的查准率和99.9%的查全率,相比现有方法有较大提升,能够更加准确地识别庞氏骗局合约。

关键词:智能合约;庞氏骗局;以太坊;深度残差网络

中图分类号:TP309.2 **文献标识码**:A **文章编号**:1005-0086(2023)08-0882-08

Ponzi scheme contract detection method based on deep residual network

GE Bin*, YUAN Zheng, REN Ping, PENG Xichen, XIA Chenxing

(School of Computer Science and Engineering, Anhui University of Science and Technology, Huainan, Anhui 232001, China)

Abstract: The existing detection methods for Ponzi scheme smart contract are mostly based on the operation code features and account features, but using these methods to detect initially deployed contracts is ineffective. Therefore, a Ponzi scheme contract detection method based on deep residual network was proposed. Firstly, by analyzing the characteristics of smart contract, the single word embedding coding algorithm (SWEC) was proposed. Then the contract was recoded by this algorithm. Secondly, critical operation code and its weight were extracted and the weight module of critical operation code (CO) was designed to improve the deep residual network. Finally, the experiments were carried out on public data sets, the experimental results show that the Ponzi scheme contract detection based on deep residual network had 99.7% precision and 99.9% recall. Compared with the existing methods, Ponzi scheme contract was detected more accurately.

Key words: smart contract; Ponzi scheme; ethereum; deep residual network

0 引 言

随着区块链技术[1]的发展,智能合约[2]爆发式增长的同时带来诸多安全问题,庞氏骗局合约就是其中之一[3]。庞氏骗局合约是以庞氏骗局思想为内核部署于区块链上的智能合约,以高回报为噱头虚假宣传,骗取后入投资者资金用于回报先前投资者。该类型骗局合约已造成上千万美元资金流失[4],严重影响区块链环境健康。

众多学者针对庞氏骗局合约展开研究。BARTOLETTI等[4]通过分析手动获取的庞氏骗局合约,提出四条庞氏骗局合约评判准则,并以待检测合约与庞氏骗局合约字节码相似度,判断其是否为庞氏骗局合约。该方法以归一化莱文斯坦

* E-mail:421862726@qq.com

收稿日期:2022-05-12 修订日期:2022-07-17

基金项目:国家自然科学基金(6210071479)、国家重点研发计划(2020YFB1314103)和安徽省自然科学基金(2108085QF258)资助项目

距离(normalized Levenshtein distance,NLD)作为判断依据,但是其阈值设置未经过科学证明,说服力不足,检测精度不高。庞氏骗局合约账户具有区别于普通合约账户的明显特征,为更加精准检测庞氏骗局合约,更多学者开始结合账户特征对合约进行检测。CHEN 等[5-6]挖掘操作码特征和账户特征,将二者结合作为实验数据,利用训练后的极端梯度提升(extreme gradient boosting,XGBoost)和随机森林(random forest,RF)检测庞氏骗局合约,获得较好效果。FAN 等[7]通过有序目标统计的方法处理账户和操作码特征,结合有序增强思想,基于决策树(decision tree,DT)构造一个无偏残差模型检测合约。张艳梅等[8]引入深度学习用于庞氏骗局合约的检测,相比基于传统机器学习的检测方法,进一步提升检测精度。WANG 等[9]通过合成少数类过采样技术(synthetic minority over-sampling technique,SMOTE)合成庞氏骗局合约,解决数据集不均衡问题,基于操作码特征和账户特征,利用长短期记忆网络(long short-term memory network,LSTM)检测庞氏骗局合约。

现有方法大多基于操作码特征和账户特征,以文本形式处理操作码序列,能够有效表示操作码,但损失了远距离关联操作码上下文联系,训练后模型对不存在账户特征的初步部署合约检测效果一般。

对此,提出一种新的检测方法。该方法以初步部署合约的唯一特征操作码为出发点,根据其特点提出一种针对合约操作码的新编码算法,该方法能够有效表示操作码序列,极大保留远距离关联操作码联系,突显关联操作码的联系特征。然后,提出一种庞氏骗局合约操作码序列中的关键操作码(critical operation code,CO)提取方法,以此提取 CO 及权重值,并设计 CO 模块,结合深度残差网络,提出一种用于检测合约的关键残差网络(critical residual network,CResNet)。最后,通过训练后的模型,检测合约是否为庞氏骗局合约。

1　基本原理

1.1　智能合约操作码及 CO

以太坊平台对部署运行的智能合约并未强制要求提供源码,合约作者将源码通过以太坊编译器编译为字节码后,即可将其部署于以太坊运行。以太坊平台运行智能合约数量超过两百万,具有源码合约数量不足 1%。将源码作为特征提取源的模型,对于无源码合约将无法实施检测。为能够对所有合约都进行有效检测,选取合约运行的前提条件字节码为检测对象。

合约字节码是由操作指令和操作数两部分组成的十六进制序列[10],操作指令集合代表着整个合约运行动作。所有操作指令构成整个合约运行逻辑,庞氏骗局合约和普通合约操作指令有逻辑上的区别,可以通过操作指令判别合约性质。将合约字节码操作指令提取,反汇编成操作码序列。

对庞氏骗局合约和非庞氏骗局合约的操作码序列进行统计以观察二者操作码差异。

统计方法为庞氏骗局合约和非庞氏骗局合约分别统计,对一类合约中某一操作码进行频率统计后除以该类合约总数,即最后频率为该类合约中该操作码在每条合约的平均出现频率。

庞氏骗局合约和非庞氏骗局合约整体操作码数量级存在差异,非庞氏骗局合约操作码数量是庞氏骗局合约 1.4 倍左右,为更明显展示数据差异,额外统计同一操作码在庞氏骗局合约和非庞氏骗局合约中频率之间的关系,由非庞氏骗局合约中频率除以庞氏骗局合约频率倍数确定。

表 1 为庞氏骗局合约和非庞氏骗局合约的操作码频率及频率之间关系。智能合约操作码数量较多,表 1 仅展示部分操作码数据,为操作码在庞氏合约中的频率前十位以及部分频率关系异常操作码。

表 1　庞氏骗局合约和非庞氏骗局合约部分操作码频率及关系

Tab. 1　Partial operation code frequency and multiple of Ponzi scheme contract and non-Ponzi scheme contract

Operation code	Word frequency of Ponzi scheme contract	Word frequency of non-Ponzi scheme contract	Multiple
PUSH	373	535	1.43
DUP	241	342	1.41
SWAP	195	261	1.34
JUMPDEST	78	120	1.53
POP	73	100	1.36
ADD	62	84	1.35
JUMPI	47	70	1.48
MSTORE	47	75	1.60
SLOAD	45	43	0.96
ISZERO	39	61	1.56
CALLVALUE	10	16	1.6
CALLDATALOAD	8	14.9	1.86

由表 1 可见,大部分操作码频率关系维持在整体合约字节码数量级的1.4倍左右,如 PUSH、DUP、SWAP、POP、AND 等,此类操作码频率关系在 1.35—1.45 的合理数量级之间。

但是存在部分频率异常的操作码如 JUMPDEST、JUNPI、MSTORE、ISZERO、CALLVALUE、CALLDATALOAD 等,该类操作码在庞氏骗局合约中数量过少,以及 SLOAD 等操作码在庞氏骗局合约

中数量较多。

庞氏骗局合约和非庞氏骗局合约中所包含的操作码及其频率倍数不同，某些频率倍数异常的操作码对合约性质存在关键影响。将对智能合约性质起着关键性作用的操作码称为CO[11]。

智能合约类别分布失衡，合约长度不一，常规操作码高频率出现，以词频大小作为判断CO依据不具有科学性。

逆文档频率（inverse document frequency，*IDF*）[12]是文本分析领域用来衡量某一词条在该研究对象中重要程度的一种计算方法，以该词条出现的语句数量和整体语句数量关系计算。

基于计算*IDF*的数学模型，提出一种庞氏骗局合约CO权重计算方法。

该方法分为计算操作码的初步权重值和权重归一化处理两部分。

第一部分，首先统计包含操作码o的智能合约数量，记为N_o。

然后，统计所有智能合约数量记为N。

最后，计算操作码o的初步权重IDF_o，计算方法为式(1)：

$$IDF_o = \log\left(\frac{N}{N_o+1}\right)。\tag{1}$$

将所有操作码及初步权重计算完毕后，进行第二步归一化处理，具体操作步骤如下：

首先，确定操作码中初步权重最大值记为Max。

然后，确定操作码中初步权重最小值记为Min。

最后，计算操作码o的最终权重值$IDF_{o\,\mathrm{normalization}}$，计算公式见式(2)：

$$IDF_{o\,\mathrm{normalization}} = \frac{IDF_o - Min}{Max - Min}。\tag{2}$$

利用提出的庞氏骗局合约CO权重计算方法，可得操作码及权重值，结果见表2。表2展示部分CO及其权重结果。

表2　关键操作码权重部分输出结果

Tab. 2　Partial outputs of CO weight

Operation code	Weight
DUP	0.000 029 486 5
POP	0.000 178 389 0
AND	0.000 124 499 6
JUMP	0.000 076 867 5
STOP	0.000 154 398 3
CALL	0.002 859 483 3
OR	0.003 370 708 0
GAS	0.007 166 674 8
MOD	0.034 781 035 9

1.2　单点词嵌入编码

现有庞氏骗局合约检测方法大多使用文本表示方法，如独热编码、词向量等[13]。该方法可以有效表示合约操作码序列，对于序列中存在关联操作码、距离较近的关联操作码在特征提取的时候，其关联性可以同时被有效提取。但是，随着关联操作码距离提升，检测模型对其关联性感知变弱，关联特征变模糊。对此，提出一种单点词嵌入编码算法（single word embedding coding algorithm，SWEC），在有效表示操作码序列的前提下，极大缩短操作码序列中关联操作码距离，加强相关联操作码上下文联系，突显关联操作码的联系特征。

算法如下：

首先，将智能合约整体映射到操作码空间，对操作码空间的操作码进行有效统计（有效统计指：如操作码PUSH和操作码PUSH1是具有相同动作的操作码，将其看作同一操作码，作为同一操作码处理）。

然后，将每个操作码映射为不同的数字标量。

最后，每条操作码序列按照操作码对应标量，转为标量序列，操作码标量序列嵌入自适应矩阵。

此编码方法能够有效缩短合约操作码序列中操作码之间的欧氏距离。

长度为n的操作码序列，最大的操作码之间欧氏距离为n，采用SWEC表示的操作码序列，最大操作码欧氏距离缩短至$\sqrt{2n}$。普通表示的操作码序列，某一操作码序列在尺寸为m的卷积核第一轮卷积后，会提取到该操作码及其距离最近的$2(m-1)$个操作码的联系。以SWEC方法表示的操作码序列可以提取到某一操作码及其距离最近的$[2(m-1)+1]^2-1$，即$4m(m-1)$个操作码的联系，其检测数量可以提升$2m$倍。

以一段智能合约操作码为例。

操作码序列为：PUSH PUSH MSTORE CALLDATASIZE ISZERO PUSH JUMPI PUSH PUSH PUSH EXP PUSH CALLDATALOAD DIV AND PUSH DUP EQ PUSH JUMPI DUP PUSH EQ PUSH JUMPI DUP PUSH EQ PUSH JUMPI DUP PUSH EQ PUSH JUMPI DUP

通过SWEC，对智能合约所有操作码进行统计，共计74种操作码。将74种操作码映射为标量，如PUSH对应标量为1，DUP对应标量为2，SWAP对应标量为3等。

根据映射规则,该操作码序列可以表示为数组 a =[1 1 7 38 10 1 8 1 1 1 15 1 19 22 9 1 2 16 1 8 2 1 16 1 8 2 1 16 1 8 2 1 16 1 8 2]。

数组 a 的所有对象存放入自适应矩阵 $\boldsymbol{M}$。矩阵 $\boldsymbol{M}$ 即为该操作码序列的最终呈现形式。

$$\boldsymbol{M}=\begin{bmatrix}1 & 1 & 7 & 38 & 10 & 1\\ 8 & 1 & 1 & 1 & 15 & 1\\ 19 & 22 & 9 & 1 & 2 & 16\\ 1 & 8 & 2 & 1 & 16 & 1\\ 8 & 2 & 1 & 16 & 1 & 8\\ 2 & 1 & 16 & 1 & 8 & 2\end{bmatrix}。$$

合约操作码片段中第 13 个操作码 CALLDATALOAD 和第 25 个操作码 JUMPI 之间存在一定依赖关系。以普通文本表示的方法,其依赖联系可能无法被有效获取。以 SWEC 方法表示的操作码序列,其欧氏距离由 11 被缩短至 2,二者联系能够被有效获取。

完整合约操作码序列长度更长,存在更多距离更远的关联操作码,其联系特征被提取概率更低。本文提出的编码方法,在完整操作码序列上表现更为突出。

1.3　CResNet

庞氏骗局合约中异于非庞氏骗局合约的操作码会对合约性质起更加重要作用。以操作码及其权重为基础,设计 CO 权重模块。

CO 模块基于 CO 权重,对不同的操作码赋予不同的权重,权重计算方式来自上文庞氏骗局合约 CO 权重计算方法。

权重模块 y_o 表示为:

$$y_o = w_o A_o\ , \tag{3}$$

式中,w_o 为操作码 o 的权重,A_o 为操作码 o 以 SWEC 中的表示方式。结合深度残差网络[14],提出 CResNet。CResNet 结构见图 1,CO 模块位于输入层之后,通过关键码操作权重模块对操作码加权。然后进入卷积层进行特征提取,通过最大池化层后依次进入各残差层,最后经平局池化后,通过全连接层,在 softmax 层完成最终分类,最后输出结果。

CResNet 模型中各残差层以何凯明团队[15]提出的残差结构为基础。采用多层残差模块(residual module,RM)和降采样残差模块(subsampling residual module,SRM)交替叠加构建。

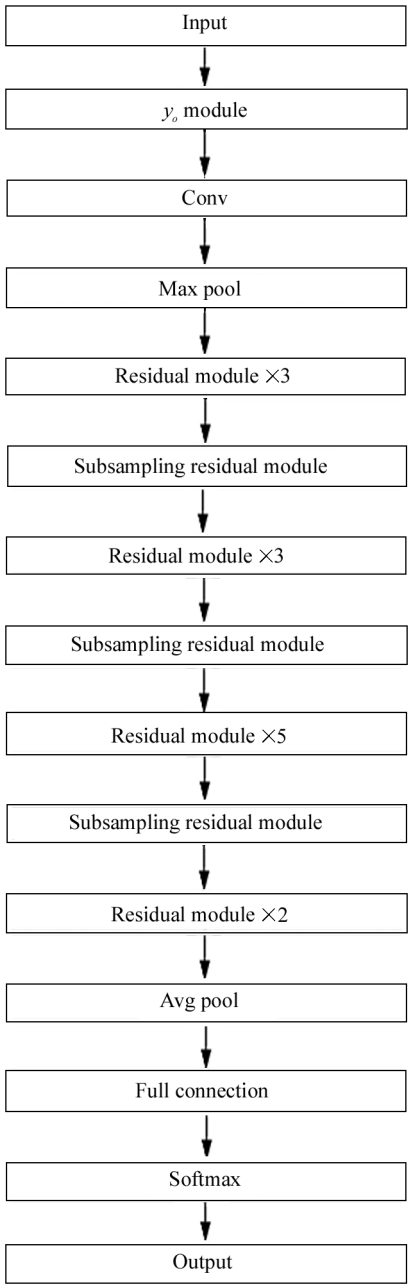

图 1　CResNet 结构

Fig. 1　Structure of CResNet

1.4　检测方法框架

图 2 为基于深度残差网络的庞氏骗局合约检测方法框架,根据数据集中的合约地址从以太坊浏览器(etherscan.io)获取智能合约字节码,根据汇编规则,合约字节码通过反汇编为对应操作码,构建数据集。对数据集进行合适划分,1−n 用于模型训练,余下部分作为测试集,用于模型性能测试(n 大小取值通过实验对比获得)。将数据集通过提出的 SWEC 进行编码处理,将处理后的操作码序列矩阵作为模型的输入。对训练后的 CResNet 模型通过测试集进行测试,最后输出检测结果。

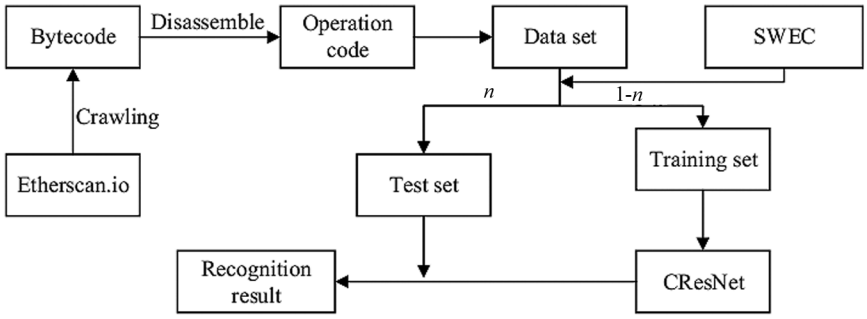

图 2　基于深度残差网络的庞氏骗局合约检测框架

Fig. 2　Structure of Ponzi scheme contract detection based on deep residual network

2　实验结果及分析

2.1　实验设置

2.1.1　数据集

实验数据为中山大学团队制作的公开数据集以太坊庞氏骗局合约数据集[5]。该数据集共计3 793条智能合约地址。去除标签error合约3个，销毁合约4个，可用智能合约共计3 786条，其中庞氏骗局合约200条，非庞氏骗局合约3 586条。

2.1.2　评价指标

实验评价指标为模型准确率 *accuracy*，测试查准率 *precision*，测试查全率 *recall* 和综合指标 $F1$。具体定义如下：

$$accuracy = \frac{TP + TN}{TP + FP + FN + TN}, \tag{4}$$

$$precision = \frac{TP}{TP + FP}, \tag{5}$$

$$recall = \frac{TP}{TP + FN}, \tag{6}$$

$$F1 = 2\,\frac{precision \cdot recall}{precision + recall}, \tag{7}$$

式中，对于真实标签为1的数据，预测标签为1的数据记为 TP，预测标签为0的数据记为 FN；对于真实标签为0的数据，预测标签为1的数据记为 FP，预测标签为0的数据记为 TN。

2.1.3　实验环境

实验系统为64位Windows10，处理器为AMD Ryzen 7 4800H，显卡为RTX2060，内存16 G，深度学习框架为Pytorch。

2.2　实验参数

2.2.1　训练轮数

模型通过训练，学习输入数据特征，通过每一轮回馈结果进一步优化下一轮学习。一定训练轮数即可达到模型最优，过多训练则会导致模型过拟合。适当的训练轮数可以获得模型的最佳效果。

设置一个相对较大轮数对模型进行训练，通过观察模型准确率及损失波动判断模型最佳训练轮数范围。图3为模型的训练准确率和测试准确率。图4为模型的训练损失和测试损失。

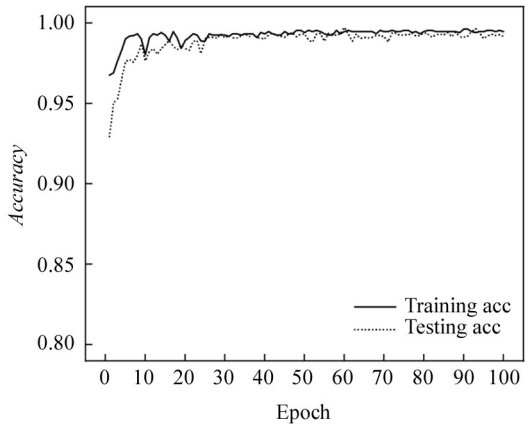

图 3　训练准确率和测试准确率

Fig. 3　Training accuracy and testing accuracy

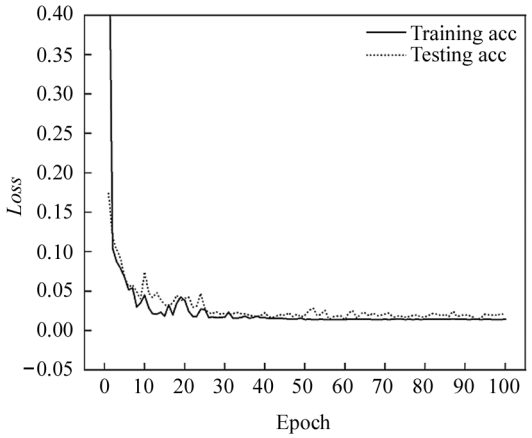

图 4　训练损失和测试损失

Fig. 4　Training loss and testing loss

通过观察,模型在 30 轮左右逐渐收敛,准确率仍保持缓慢上升,损失缓慢下降。60 轮左右模型准确率有小幅度波动,基本维持不再变化,损失值基本降到最低。因此选择 60 轮作为最终训练轮数。

2.2.2　数据集划分

数据集划分比例的不同会对模型准确率有一定影响。不合理的数据集划分甚至可能会导致模型无效训练。

针对庞氏骗局合约相关研究的数据集划分并没有确定比例,大多以不同比例数据集划分训练模型展开多次实验,以实验结果选择最佳划分比例确定最终数据集划分。

本实验同样通过该方法确定训练集和测试集划分比例。由图 5 可知,数据集划分以测试集的比例从 0.25,每次以 0.05 增量递增至 0.45,模型均训练 60 轮后对测试集进行相关测试。实验结果表明,测试集的占比为 0.35 的数据集划分实验效果最好,准确率为 99.6%。测试集的比例增长导致训练样本过少,对测试样本表现逐渐变差。更多训练数据会导致模型泛化性能变差,在测试集上表现变差。因此,选择表现最佳的数据集划分,测试集为 0.35,训练集为 0.65。

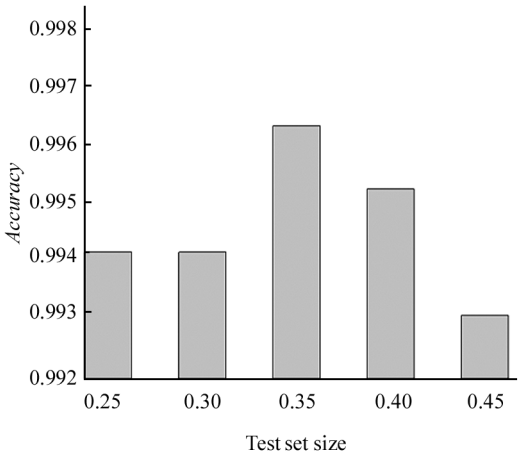

图 5　测试集的不同比例和准确率

Fig. 5　Accuracy on different ratio of test set

2.2.3　批尺寸

批尺寸过小,损失会有较大震荡,模型较难收敛。批尺寸过大,达到相同准确度需要更多训练轮数,训练时间过长。适当的批尺寸大小,模型会有较好收敛,时间最优。表 3 为不同批尺寸下模型的训练时间、准确率及收敛轮数。在批尺寸为 16 和 32 时,模型准确率最高,批尺寸为 16 时,训练轮数更好。综合考虑选择批尺寸为 16。

表 3　不同批尺寸的训练时间、模型准确率、收敛轮数

Tab. 3　Time cost, *accuracy* and epoch on different batch size

Batch size	Time cost/min	*Accuracy*	Epoch
1	450	0.992	150
8	130	0.995	60
16	120	0.996	60
32	124	0.996	65
64	145	0.995	70
128	141	0.995	70

2.2.4　其他参数

模型优化器选择随机梯度下降(stochastic gradient descent,SGD),该优化器可有效避免较差最优解。学习率为动态学习率,初始为 0.1,每 25 轮训练,缩小至当前学习率的十分之一。

2.3　实验结果与分析

对 CResNet 检测模型进行上文参数训练后,在测试集上表现结果见图 6,其中标签 0 为非庞氏骗局合约,标签 1 为庞氏骗局合约。

测试集中非庞氏骗局合约1255条,检测正确 1 254 条,查准率 0.997,查全率 0.999。非庞氏合约 70 条,检测正确 66 条,查准率 0.985,查全率 0.943。模型准确率 0.996。

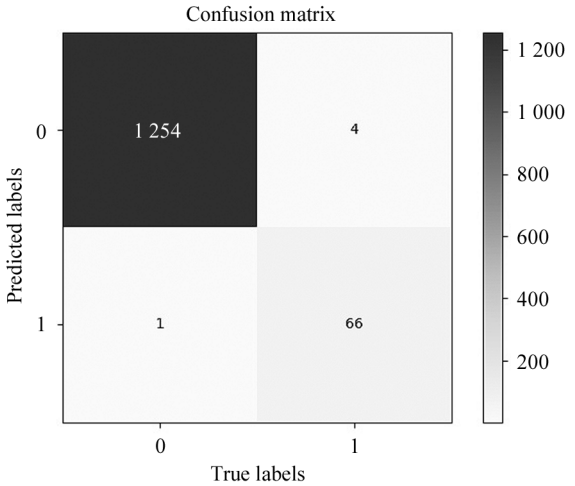

图 6　CResNet 实验结果

Fig. 6　Experimental results of CResNet

对比实验选择文献[5]、文献[6]、文献[9]中的实验方法及一些表现较为突出的传统机器学习算法如一类支持向量机(one class support vector machine,OCSVM)、支持向量机(support vector machine,SVM)、DT。

实验结果见表 4。从实验结果可看出,OCSVM 在查全率方面有最好效果,达到 100%。但是其相当

高的查全率是以将样本大数量归为非庞氏骗局样本的方式获得，其准确率较低。SVM有较高的查准率，DT相对SVM查全率和$F1$较高。文献[5]和文献[6]都有超过90%的查准率和超过80%的$F1$，表现尚佳。文献[9]的实验方法是目前现有方法中效果最佳的方法，有96%的查准率，95%的查全率和95%的$F1$。本文提出的实验方法，相对文献[9]提升了3.7%的查准率和4.9%的查全率。$F1$相比现有方法，达到最高为99.8%。本文方法对初步部署庞氏骗局合约有较好的检测效果。

表4　不同方法的实验结果比较

Tab. 4　Performance comparison of different methods

Algorithm	*Precision*	*Recall*	*F*1
OCSVM	0.06	1.00	0.10
SVM	0.95	0.43	0.59
DT	0.64	0.73	0.68
XGBoost[5]	0.90	0.80	0.84
RF[6]	0.94	0.73	0.82
PSD-OL[9]	0.96	0.95	0.95
CResNet	0.997	0.999	0.998

3　结　论

针对现有庞氏骗局合约检测方法对初步部署合约检测效果一般，提出基于深度残差网络的庞氏骗局合约检测方法。首先，分析智能合约特点，合理选择操作码作为特征提取源，提出SWEC，对操作码进行重新编码表示，增强关联操作码连接性，放大操作码自身特征。然后，根据合约操作码特点，设计CO权重模块，结合残差结构提出用于合约检测的CResNet模型。最后，在相关数据集上展开相关实验，实验结果表明，本文提出的检测方法在查准率、查全率、$F1$等多项考察指标上相比现有检测方法均有较大提升，能够对庞氏骗局智能合约进行准确的检测。

参考文献：

[1] SHAO Q F, JIN C Q, ZHANG Z, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.
邵奇峰，金澈清，张召，等. 区块链技术：架构及进展[J]. 计算机学报，2018，41(5)：969-988.

[2] HE H W, YAN A, CHEN Z H. Survey of smart contract technology and application based blockchain [J]. Journal of Computer Research and Development, 2018, 55(11): 2452-2466.
贺海武，延安，陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展，2018，55(11)：2452-2466.

[3] SUN G Z, LI Z, XIAO R Y, et al. Research on blockchain transaction security[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition) 2021, 41(2): 41-53.
孙国梓，李芝，肖荣宇，等. 区块链交易安全问题研究[J]. 南京邮电大学学报(自然科学版)，2021，41(2)：41-53.

[4] BARTOLETTI M, CARTA S, CIMOLI T, et al. Dissecting ponzi schemes on ethereum: identification, analysis, and impact[J]. Future Generation Computer Systems, 2020, 102(1): 259-277.

[5] CHEN W L, ZHEN Z B, CUI J H, et al. Detecting ponzi schemes on ethereum: towards healthier blockchain technology[C]//2018 World Wide Web Conference, April 23-27, 2018, Lyon, France. Geneva: International World Wide Web Conferences Steering Committee, 2018: 1409-1418.

[6] CHEN W L, ZHENG Z B, NGAI E, et al. Exploiting blockchain data to detect smart ponzi schemes on ethereum [J]. IEEE Access, 2019, 7(3): 37575-37586.

[7] FAN S, FU S, XU H, et al. AI-SPSD: anti-leakage smart ponzi schemes detection in blockchain [J]. Information Processing and Management, 2021, 58(4): 102587.

[8] ZHANG Y M, LOU Y C. Deep neural network based ponzi scheme contract detection method [J]. Computer Science, 2021, 48(1): 273-279.
张艳梅，楼胤成. 基于深度神经网络的庞氏骗局合约检测方法[J]. 计算机科学，2021，48(1)：273-279.

[9] 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(1): 107312.

[10] OUYANG L W, WANG S, YUAN Y, et al. Smart contracts: architecture and research progress[J]. Acta Automatica Sinica, 2019, 45(3): 445-457.
欧阳丽炜，王帅，袁勇，等. 智能合约：架构及进展[J]. 自动化学报，2019，45(3)：445-457.

[11] ZHANG H X, WANG Q, WANG D Y, et al. Honeypot contract detection of blockchain based on deep learning[J]. Journal on Communications, 2022, 43(1): 194-202.
张红霞，王琪，王登岳，等. 基于深度学习的区块链蜜罐

陷阱合约检测[J].通信学报,2022,43(1):194-202.

[12] YANG W D, TIAN Y X, WAN F, et al. On-board screen text detection and recognition based on deep learning [J]. Journal of Optoelectronics · Laser, 2021, 32(4): 395-402.
杨伟东,田永祥,万峰,等.基于深度学习的车载屏幕文本检测与识别研究[J].光电子·激光,2021,32(4):395-402.

[13] XIONG W, AI M H, YANG D C, et al. Research on scene text detection algorithm based on deep learning[J]. Journal of Optoelectronics · Laser, 2021, 32(7): 728-734.
熊炜,艾美慧,杨荻椿,等.基于深度学习的场景文本检测算法研究[J].光电子·激光,2021,32(7):728-734.

[14] LIU Y N, YU T T, QI W, et al. Study on classification method for dynamic ecg signal based on optimized resnet residual network[J]. Journal of Optoelectronics · Laser, 2021, 32(8): 894-901.
刘亚楠,于婷婷,漆伟,等.基于优化残差网络的动态心电信号分类算法研究[J].光电子·激光,2021,32(8):894-901.

[15] HE K M, ZHANG X Y, REN S Q, et al. Deep residual learning for image recognition[C]//2016 IEEE Conference on Computer Vision and Pattern Recognition, June 27-30, 2016, Las Vegas, Nevada, USA. New York: IEEE, 2016: 770-778.

作者简介:

葛　斌　(1975—),男,博士,教授,硕士生导师,主要从事信息安全、物联网方面的研究.