Artificial Intelligence and Robotics Research 人工智能与机器人研究, 2025, 14(4), 855-867
Published Online July 2025 in Hans. https://www.hanspub.org/journal/airr
https://doi.org/10.12677/airr.2025.144081

Hans汉斯

基于权益证明共识机制的用户攻击行为检测

向　诉[1]，宋鹃侃[2]，罗　颂[3]

[1]重庆理工大学两江人工智能学院，重庆
[2]成都市公安局锦江区分局信息通信科，四川 成都
[3]重庆理工大学计算机科学与学院，重庆

收稿日期：2025年5月9日；录用日期：2025年7月2日；发布日期：2025年7月11日

摘　要

随着区块链技术的快速发展，其去中心化、不可篡改和可追溯等特性在金融、供应链管理和物联网等领域得到了广泛应用。然而，区块链生态系统的开放性和匿名性也为攻击者提供了可乘之机，导致欺诈交易、恶意套利、跨链洗钱等安全问题频发，严重威胁区块链网络的稳定性和用户资产安全。现有的检测方法在应对复杂的交易模式和时序特征等方面仍存在检测精度不足、模型泛化能力有限、实时性较差等问题。因此，研究高效、精准的用户攻击行为检测方法，对提升区块链系统的安全性、增强交易可信度具有重要的现实意义。本文以以太坊平台为研究对象，结合其共识机制特点，联合卷积神经网络和双向长短期记忆网络，构建检测模型。通过利用卷积神经网络提取交易数据的局部特征，双向长短期记忆网络捕捉交易中用户行为的时间依赖关系，并引入注意力机制强化关键特征的权重分配。实验结果表明，该模型在以太坊交易网络检测中达到了很好的效果，实现了对复杂交易模式和异常行为的精准识别。

关键词

区块链安全，攻击行为检测，共识机制，机器学习

User Attack Behavior Detection Based on PoS Consensus

Su Xiang[1], Juanni Song[2], Song Luo[3]

[1]School of Artificial Intelligence, Chongqing University of Technology, Chongqing
[2]Information and Communication Department, Jinjiang District Branch of Chengdu Public Security Bureau, Chengdu Sichuan
[3]College of Computer Science and Engineering, Chongqing University of Technology, Chongqing

Received: May 9th, 2025; accepted: Jul. 2nd, 2025; published: Jul. 11th, 2025

文章引用: 向诉, 宋鹃侃, 罗颂. 基于权益证明共识机制的用户攻击行为检测[J]. 人工智能与机器人研究, 2025, 14(4): 855-867. DOI: 10.12677/airr.2025.144081

Abstract

With the rapid development of blockchain technology, its decentralized, tamper resistant, and traceable characteristics have been widely adopted in fields such as finance, supply chain management, and the Internet of Things. However, the openness and anonymity of blockchain ecosystems also create opportunities for attackers, leading to frequent security issues such as fraudulent transactions, malicious arbitrage, and cross-chain money laundering, which severely threaten the stability of blockchain networks and user asset security. Existing detection methods still face challenges including insufficient detection accuracy, limited model generalization capabilities, and poor real-time performance when addressing complex transaction patterns and temporal features. Therefore, researching efficient and precise methods for detecting user attack behaviors holds significant practical importance for enhancing blockchain system security and transaction credibility. In this paper, we take the Ethereum platform as the research object, combine the characteristics of its consensus mechanism, unite the convolutional neural network and bidirectional long and short-term memory network to construct the detection model. By using convolutional neural network to extract the local features of transaction data, bidirectional long and short-term memory network captures the time-dependence of user behaviors in transactions, and introduces the attention mechanism to strengthen the weight allocation of key features. Experimental results show that the model achieves good results in Ethereum transaction network detection, realizing accurate identification of complex transaction patterns and abnormal behaviors.

Keywords

Blockchain Security, Attack Behavior Detection, Consensus Mechanism, Machine Learning

1. 引言

随着共识机制的发展，以太坊的共识机制也从工作量证明[1]机制逐步转向权益证明机制[2]，利用持币权益来验证交易和生成区块，这不仅在节能方面具有显著优势，还提高了系统的可扩展性。然而，权益证明(Proof of Stake, PoS)的出现虽然减少了矿工消耗的资源，却面临新的安全挑战，尤其是权益集中的问题，使得部分用户可能利用手中权益对网络发起恶意攻击。这些攻击行为包括权益积累后的双花攻击[3]、网络垄断、洗钱等，不仅威胁到网络的公平性，还可能影响整个系统的交易可靠性[4]-[7]。因此，及时发现和检测用户的异常行为，特别是在交易网络中识别潜在的攻击行为，对于保障 PoS 共识机制的有效性至关重要。

在以太坊的交易网络中，由于用户通过匿名地址进行交易，恶意用户可能借助多地址、假地址甚至隐蔽路径来隐藏其真实身份，增加了攻击检测的复杂性。同时，以太坊的交易数据量庞大且具有时间序列特征，数据呈现动态变化，因此对于用户攻击行为的检测需要具备搞笑的数据处理和准确的异常识别能力。传统的基于规则的检测方法难以识别复杂的关联模式，而深度学习模型可以通过学习大量数据中的潜在模式来更准确地识别异常行为。

在 2019 年，Xu 等人[8]提出了检测以太坊的交易网络中是否存在日蚀攻击的第一个智能检测器，该检测模型基于随机森林的分类算法，它能够检测以太坊的交易网络上是否存在日蚀攻击。OstaPoWicz 等

人[9]也在实验中提出了关于大规模的以太坊账户中是否存在欺诈账户的检测方法。他们通过使用监督学习技术来进行检测，实验结果表明它们能较好的检测出欺诈账户是否存在，但召回率很低。Tan 等人[10]提出了一种通过挖掘以太坊的交易记录来检测是否存在欺诈交易的方法，该方法通过使用图神经网络的组合来进行检测，但该模型的 F1 分数也只能达到 0.75 左右。Elmougy 等人[11]通过检测比特币和以太坊的交易网络中的异常来识别欺诈性交易和欺诈性账户是否存在。利用机器学习模型：支持向量机、随机森林和逻辑回归，最终得到 0.802 的准确率和 0.835 的召回率。Kumar 等人[12]通过在账户的交易数据中使用基于监督学习的方法来检测是否存在恶意节点。Dahiya 等人[13]提出了一种基于神经网络的方法用于以太坊的欺诈检测，并将所提出的模型与同类模型进行了比较，实验结果证明神经网络的表现比那些模型更好。Farrugia 等人[14]提出了一种基于以太坊网络的检测器，该检测器通过使用 XGBoost 分类器对非法账户进行检测。

权益证明机制是为了解决基于工作量证明区块链的系统所需的大量能源消耗、硬件要求、区块生成速度。但是，尽管权益证明机制在防止安全漏洞和降低能耗方面效率很高，但它仍然容易受到一系列攻击。Akbar 等人[15]提出了工作量证明和权益证明的分布式混合解决方案，但是他们的解决方案受到可扩展性和共识更加集中的限制。Tas 等人[16]提出了一种解决方案，使用比特币哈希算力来增强基于权益证明机制的区块链的安全性，这种解决方案的缺点是它需要矿工拥有 Babylon 软件。Sanda 等人[17]提出一种在权益证明机制的区块链上，关于数据集节点分类的深度学习新方法，将节点分类为恶意或非恶意节点，以高精度缓解远程攻击。

本研究联合卷积神经网络和双向长短期记忆网络构建 CNN_BiLSTM 模型，结合以太坊的共识机制为权益证明的特点，展开用户攻击行为的检测实验，有以下几点贡献：

(1) 构建了一个在以太币交易场景下，根据以太坊的权益证明机制的特点，联合卷积神经网络和长短期记忆网络，用于检测系统中是否存在用户恶意的攻击行为的模型：CNN_BiLSTM 模型。

(2) 提出了利用长短期记忆网络捕捉交易行为中的时间依赖关系，能够识别到交易网络中节点的长期依赖关系，将短期异常行为与长期异常行为结合起来，提高模型的检测精度。

(3) 同样，通过在真实的以太币交易数据集上进行大量实验表明，与现有的检测方法相比，本章提出的检测方法更有效。从而验证了 CNN_BiLSTM 模型的有效性，以及证明了联合卷积神经网络算法对节点特征的有效提取和长短期记忆网络对时间依赖关系的捕捉，为用户攻击行为检测提供了一种更有效的方法。

2. 方法

2.1. 评价指标

对于本研究，需要通过计算模型的精确率(Precision)、召回率(Recall)、准确率(Accuracy)和 F1 Score 作为模型的评价指标。

对于这四个指标的计算，首先需要了解混淆矩阵(Confuse Matrix)：针对一个二分类问题，即将实例分成正类(Positive)或负类(Negative)，在实际分类中会出现以下四种情况：

如果实际为正类，同时被预测为正类，即为真正类 TP (True Positive)；

如果实际为正类，同时被预测为负类，即为假负类 FN (False Negative)；

如果实际为负类，同时被预测为正类，即为假正类 FP (False Positive)；

如果实际为负类，同时被预测为负类，即为真负类 TN (True Negative)；

混淆矩阵的每一行是样本的预测分类，每一列是样本的真实分类。

在了解了混淆矩阵之后，精确率、召回率、准确率和 F1 值都是通过混淆矩阵中的真正类、假负类、

假正类、真负类来进行计算的。

精确率：以预测结果为判断依据，预测为正类的样本中实际为正类的比例。该评价指标重点关注预测结果的可靠性，衡量模型减少误报的能力。其公式如下所示：

$$\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \tag{1}$$

召回率：以实际样本为判断依据，实际为正类的样本中被预测正确的比例。该评价指标重点关注模型捕捉正类的全面性，衡量模型减少漏报的能力。其公式如下所示：

$$\text{Recall} = \frac{\text{TP}}{\text{TP} + \text{FN}} \tag{2}$$

准确率：表示分类正确的样本数占总样本个数的比例，即预测为正类且实际为正例的情况加上预测为负类且实际也为负类的情况，在总样本个数的百分比是多少。其公式如下所示：

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \tag{3}$$

F1 值是中和了精确率和召回率的指标，其公式如下所示：

$$\text{F1} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} \cdot \text{Recall}} \tag{4}$$

2.2. 卷积神经网络

卷积神经网络(Convolutional Neural Network, CNN)作为深度学习模型，通过引入卷积操作，实现了对空间结构信息的捕捉。CNN 主要用于处理具有网格结构的数据(如图像、时间序列等)，通过局部连接、权重共享以及池化操作等特点，在图像分类、目标检测、语音识别等领域取得了显著的成功。对卷积神经网络的研究可追溯到日本学者 Fukushima 提出的“Neocognitron”模型[18]。1980 年，他仿造生物的视觉皮层设计了以“Neocognitron”命名的神经网络，该神经网络是最早被提出的深度学习算法之一。1998 年，Yann Lecun 等人提出了 LeNet-5，他们将 BP 算法应用到神经网络结构的训练上，就形成了当代卷积神经网络的雏形[19]。CNN 的基本结构通常由以下几个主要组成部分构成：

卷积层，它是 CNN 的核心组成部分，负责提取数据中的局部特征。在卷积操作中，网络通过卷积核(或滤波器)与输入数据进行卷积，计算局部区域的加权和，从而得到特征图。卷积操作具有权重共享的特点，这意味着同一卷积核在不同位置共享相同的参数，大大减少了模型的参数数量，同时也提高了模型的泛化能力。

激活函数，它用于引入非线性因素，帮助网络学习复杂的模式。常用的激活函数包括 ReLU、Sigmoid、Tanh 等。

池化层，它用于对特征图进行下采样，以减少特征图的尺寸，降低计算量，并增强模型的空间不变性。常用的池化方法有最大池化、平均池化。池化操作可以有效提取图像中的重要特征，忽略不重要的信息。

全连接层，在卷积特征提取与空间下采样操作完成后，通常会引入全连接网络层实施特征空间映射。该层通过权重矩阵乘法实现高维张量的全局表征融合，将局部感受特征升维为任务导向的判别性特征向量。最终通过 softmax 函数或回归器实现监督学习目标。

2.3. 长短期记忆网络

长短期记忆网络(Long Short-Term Memory, LSTM)是一种特殊的循环神经网络，能够有效地学习和捕

捉序列数据中的长期依赖关系。LSTM 是由 Hochreiter 等人于 1997 年首次提出[20]，通过设计特殊的门结构来控制信息流，有效克服了传统循环神经网络在时序数据建模中存在的梯度消失和梯度爆炸问题。LSTM 的核心在于其“记忆单元”，这个单元能够通过特殊的门控制来有效地控制信息流动，如图 1 所示。其结构可以通过以下几个关键组成部分来理解：

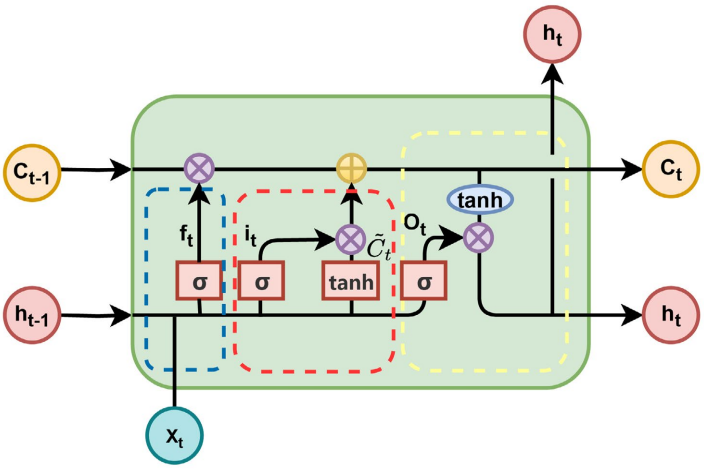


Figure 1. LSTM with memory cells and gates
图 1. 带有存储单元和门的 LSTM

输入门，它决定当前输入信息的多少将被添加到单元状态中，即图中的红色虚线框处。输入门由两部分组成：一个是通过 sigmoid 激活函数输出的值，决定了输入信息的“重要性”；另一个是通过 tanh 激活函数生成的候选值。它是当前时间步的输入信息。

遗忘门，它控制从“记忆单元”中丢弃多少信息，即图中的蓝色虚线框处。该门的输出通过 sigmoid 激活函数生成一个介于 0 和 1 之间的值，表示哪些信息应该被遗忘。当遗忘门的输出接近 0 时，表示“遗忘”操作强烈；接近 1 时，则表示“记忆”操作强烈。

输出门，它决定哪些信息从“记忆单元”传递到下一个时间步，即图中的黄色虚线框处。该门通过 sigmoid 激活函数生成输出值，用来决定何时输出信息。同时，LSTM 会基于当前的单元状态和输出门的激活值，利用 tanh 激活函数对最终的输出进行调制。

3. 实验

3.1. 总体架构

本研究是联合卷积神经网络和双向长短期记忆网络算法，针对以太币交易数据，构建的用户攻击行为检测模型。总体架构如图 2 所示。

3.2. 数据集

本研究使用开源的以太坊的交易数据集：Ethereum Fraud Detection Dataset，该数据集包含了在以太坊的交易网络中通过以太币进行的已知欺诈和有效交易的数据，大约 720 万笔交易。数据集中每笔交易包含 44 种不同的输入特征，可以很好地使用特征数据，对交易是否存在欺诈可能性进行判断。数据集中列出的特征包括但不限于以太坊账户地址、账户发送交易的平均间隔时间(分钟)、账户收到交易的平均间隔时间(分钟)、第一个和最后一次交易之间的时间差(分钟)等[13]。

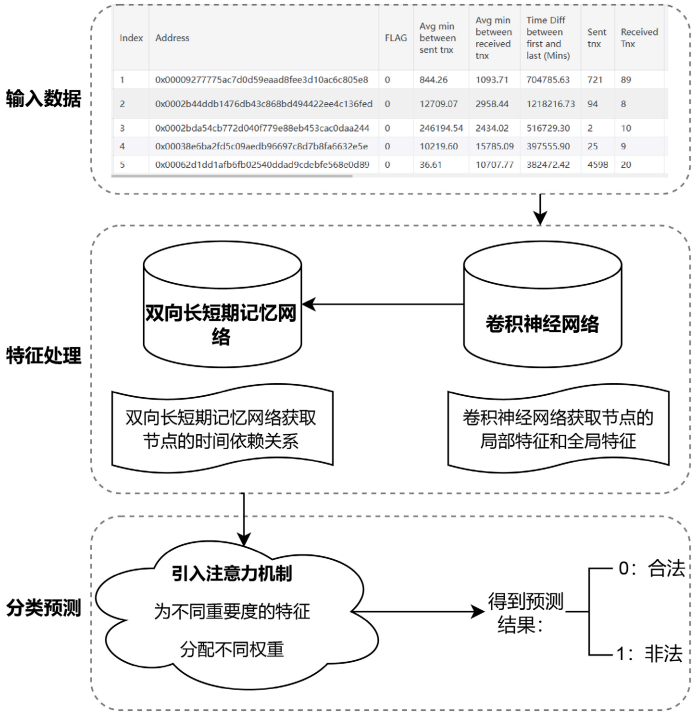


Figure 2. Experimental architecture diagram
图 2. 实验架构图

同时为了更好的完成实验，对于数据集中的异常值、缺失值，需要进行一系列的填补或删除等操作。在解决数据集中的异常值、缺失值之后，对于其中的无用特征值也可以进行直接删除。对于数据集中类别不平衡问题，通常采用 SMOTE 算法，通过生成合成样本来平衡数据集中欺诈与非欺诈类别的样本数量。通过生成多样化的欺诈类别样本，扩展了欺诈类别的特征空间，使得模型能够更好地捕捉其特性，从而提高泛化能力。

3.3. 用户攻击行为检测模型

对于以太坊网络中，交易场景下用户是否发起攻击行为的检测，本研究设计了一种联合卷积神经网络和长短期记忆网络的用户攻击行为检测模型。同时，为了让模型能够实现更好的检测效果，对于模型的构建，还引入了注意力机制，对交易数据中的特征信息进行更充分有效地学习，有效地提取其更复杂、更深层的特征信息。

联合卷积神经网络和长短期记忆网络，再加入注意力机制的用户攻击行为检测模型能够更好地学习以太币的交易数据的局部特征信息和数据的时序相关性。该模型由多层结构组成，包括卷积层、池化层、双向长短期记忆网络层、随机失活层，注意力层、平铺层和全连接层，其模型的结构图如图 3 所示。

3.3.1. 特征提取模块

在特征提取模块，需要卷积神经网络从对已经完成数据清洗等预处理操作的以太币交易数据中提取局部特征。CNN 能够有效地捕捉这些局部特征，通过卷积操作提取出具有判别力的深度特征。样本数据需要依次进入隐藏层中的卷积层、池化层，其中卷积层是提取特征的关键，它能够通过训练交易数据得到一组具有最小损失的最优卷积核，再利用卷积核自动提取复杂的交易数据特征。本模型采用一维卷积，按照单一的时域方向进行卷积。

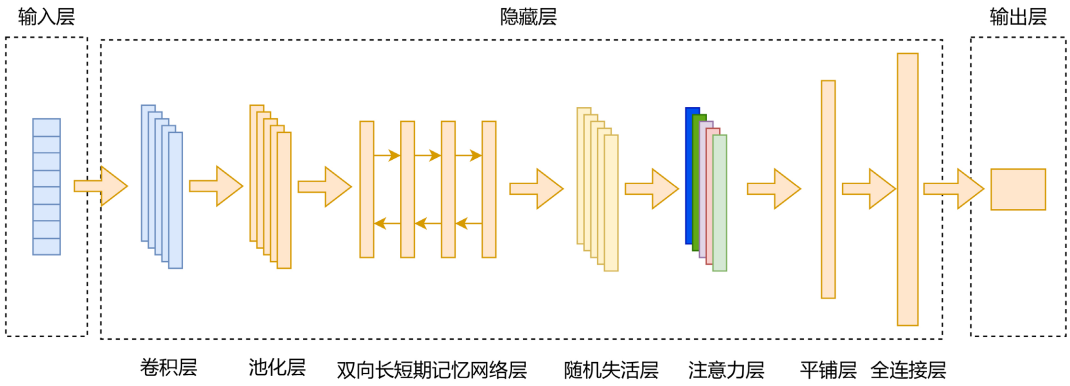


Figure 3. Model structure diagram
图 3. 模型结构图

在本研究的实验中，设置一维卷积层对其进行特征提取，卷积层中包含 64 个滤波器。同时，在完成数据预处理之后的数据集中，每个样本都包含 16 个特征，因此，实验将时间步数 t 设为 16，特征维度 n 记为 1，卷积核大小 k 为 3。设波器个数为 64，该参数通过控制模型复杂度与训练效率的平衡确定，意味着该层会生成 64 个不同的特征图，每个特征图都是对输入数据的一种变换，反映了输入的不同方面。同时，设置输入输出宽度一致的填充方式，维持了时间序列的完整性。

为了提高特征提取的效率，在网络中加入了池化层，减少了特征维度并增强了模型的泛化能力。池化层通常用于：减少数据的维度，从而降低计算复杂度和模型参数的数量(降采样)、帮助模型获得一定程度上的平移、旋转或其他变换的不变性(特征不变性)、通过减少参数数量和控制模型容量来减少过拟合风险(防止过拟合)，常用的池化方法是最大池化和平均池化。本研究使用最大池化层对卷积层的特征向量的最大值进行合并，得到最终的特征值。在卷积层后面加入一个最大池化层，池化窗口大小设为 2。经过了卷积层和池化层的操作之后，最终会得到一个 1*n 维的数据特征，这个特征作为 LSTM 模型的输入。

3.3.2. 时间依赖关系捕捉模块

在完成特征提取任务之后，引入长短期记忆网络对特征数据进行时间依赖关系捕捉。LSTM 是一种特殊的递归神经网络，它通过独特的门控机制(输入门、遗忘门和输入门)有效地学习并记住长期的历史信息。在使用卷积层提取局部特征之后，添加 LSTM 层能够帮助模型在这些局部特征的基础上进一步整合全局的时间依赖关系。这样可以获得更深层次的理解，并提升模型的表现力。

在本研究中，选择双向长短期记忆网络(Bidirectional Long Short Term Memory, BiLSTM)对其进行训练。BiLSTM 是 LSTM 的一种变体，它不仅具有 LSTM 的学习能力，还可以同时考虑序列的正向和反向信息，使得模型的性能更好。其结构包含了输入层、正向隐层、反向隐层和输出层。

在实验中，指定了 64 个 BiLSTM 单元，该层用于学习前面卷积输出得到的 64 个不同的特征向量。与卷积层的滤波器数量一致，确保特征维度匹配以避免信息损失。同时，设置 LSTM 层会为输入序列中的每个时间步返回一个输出(即输出整个序列)，而不是只返回最后一个时间步的输出，这样可以使得下一层能够接收到完整的序列信息。BiLSTM 通过其双向结构捕捉数据中的前后时序依赖关系，以捕捉交易数据中的长期趋势和动态模式，更加全面地学习到数据中的序列特征。

3.3.3. 引入注意力机制模块

最后，为了进一步提升模型的检测能力，在 BiLSTM 的输出基础上加入注意力机制。该机制通过自动为输入特征分配权重，帮助模型关注与攻击行为相关的关键特征。具体而言，注意力机制能够根据不

同时间步和特征的重要性动态调整其权重，使模型更倾向于关注异常交易行为的信号。特别是在面对不平衡的攻击数据时，注意力机制能够有效提高对少数类攻击流量的检测率。通过这种方式，模型能够更加准确地聚焦于对攻击行为具有判别力的特征，进一步增强其在实际应用中的有效性和鲁棒性。

在实验中，将注意力机制放在 BiLSTM 后面，其本质上是求最后一层 LSTM 输出向量的加权平均和。对于注意力层的计算过程主要有以下几个关键步骤：

扩展查询维度：查询 query 作为一个向量，表示当前解码器的时间步状态，为了与编码器输出 values 的形状相匹配，需要在时间轴上扩展 query。

计算得分：得分是衡量查询与每个编码器输出之间相似度的关键，注意力机制是使用一个双线性函数(即两个线性变换后加上非线性激活)来计算这些得分。

其中 W_1 和 W_2 表示可训练的权重矩阵，分别应用于 query 和 $value_t$，V 是另一个可训练的向量，用于将激活后的结果投影到单一标量得分。

归一化得分：使用 softmax 函数对所有时间步的得分进行归一化，得到注意力权重。

计算上下文向量：上下文向量是通过将注意力权重应用到对于的编码器输出上并求和得到的，它可以看作是对输入序列的一个加权平均。

最终，注意力机制会返回上下文向量以及注意力权重，并将这个值输入到全连接层，得到检测结果。

4. 实验结果与分析

4.1. 模型解释性分析

实验对特征完成了基于 SHAP 值的量化分析，图 4 表示 SHAP 值为前 15 的特征名称，这些特征对于检测结果的影响相较于其他特征更大。这里解释前五个特征的含义及模型如何根据该特征信息判断用户是否发起攻击行为。Avg min between sent tnx 表示用户发起交易的平均间隔时间，正常用户的发起交易间隔稳定，若某节点想要发起高频恶意操作(如闪电贷攻击)，该节点的这个特征值就比较小。MaxValueSentToContract 表示单次向合约发送的最大值，普通用户向合约发送金额较小，若出现单次发送过大的情况，则可能为闪电贷中的资金聚合。NumberofCreated_Contracts 表示创建的智能合约总数，

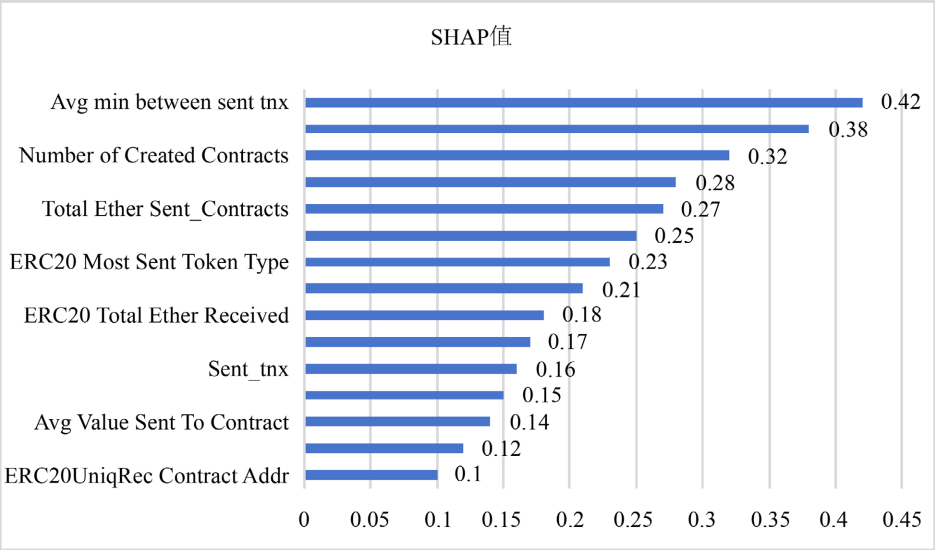


Figure 4. Characteristics of the top 15 SHAP values
图 4. SHAP 值前 15 的特征

普通用户很少主动创建合约，但如果某节点短时间密集创建，则它可能会发起重入攻击或多合约协作攻击。ERC20UniqSentTokenName 表示地址发送不同 ERC20 代币类型的数量，用户通常使用少数几种代币，若某用户发送多种代币，则该用户为混淆资金流向，隐藏洗钱的攻击行为。TotalEtherSent_Contracts 表示地址向所有合约地址发送的以太币总和，普通用户一般发送的金额都比较低。若该特征出现异常高值，则有可能发生恶意合约部署或资金池操作。

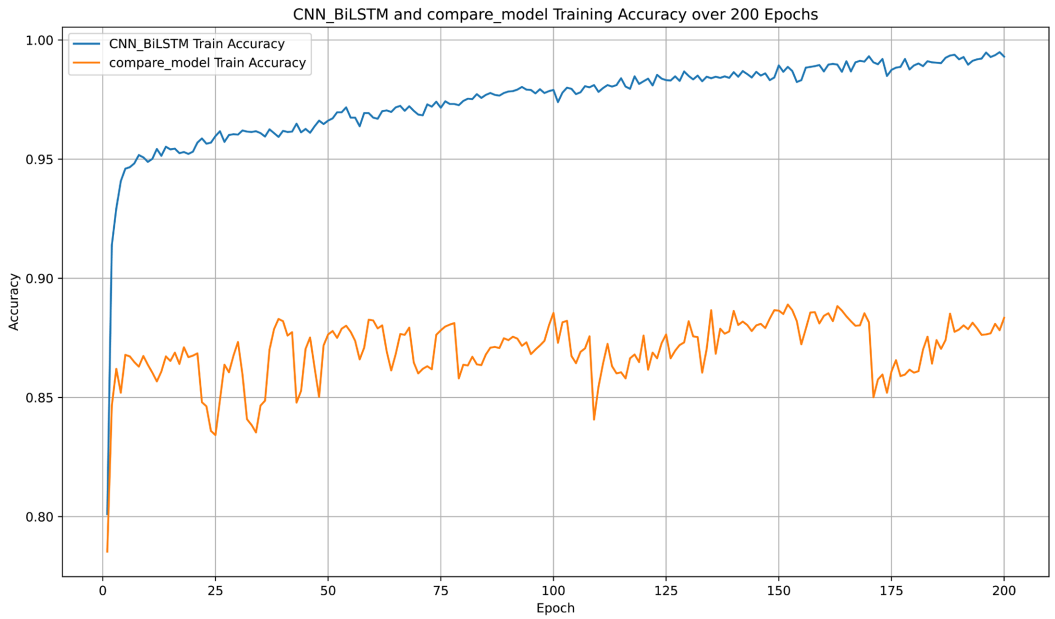
为了验证 SHAP 值高的这些特征的重要性，通过逐一移除特征信息的方法展开特征消融实验。实验结果如表 1 所示，随着特征的 SHAP 越低，F1 值会相应越高，从而更加深入地理解了某个特征对最终结果的影响程度。

Table 1. Characteristic ablation experiments
表 1. 特征消融实验

移除特征	F1 Score	下降幅度
Avg min between sent tnx	0.876	10.4%
MaxValueSentToContract	0.884	9.6%
NumberofCreated_Contracts	0.901	7.9%
ERC20UniqSentTokenName	0.908	7.2%
TotalEtherSent_Contracts	0.914	6.6%

4.2. 有效性评估

对于有效性评估中，将从两个角度对本实验构建的模型 CNN_BiLSTM 进行检验。在实验之初，选择使用卷积神经网络和长短期记忆网络进行结合，对以太坊上的以太币交易数据进行用户攻击行为检测模型的构建。但是，仅仅只是简单地将这两个模型结合起来得到的准确率是远远不够的，因此多次实验尝试之后，构建模型的时候将长短期记忆网络升级为双向长短期记忆网络，同时在其后面引入注意力机制，可以从图 5 看到，在训练集和验证集上，CNN_BiLSTM 模型的性能都非常优秀，在训练集上，准确率达到了 0.99 左右，在验证集上，准确率达到了 0.96 左右。



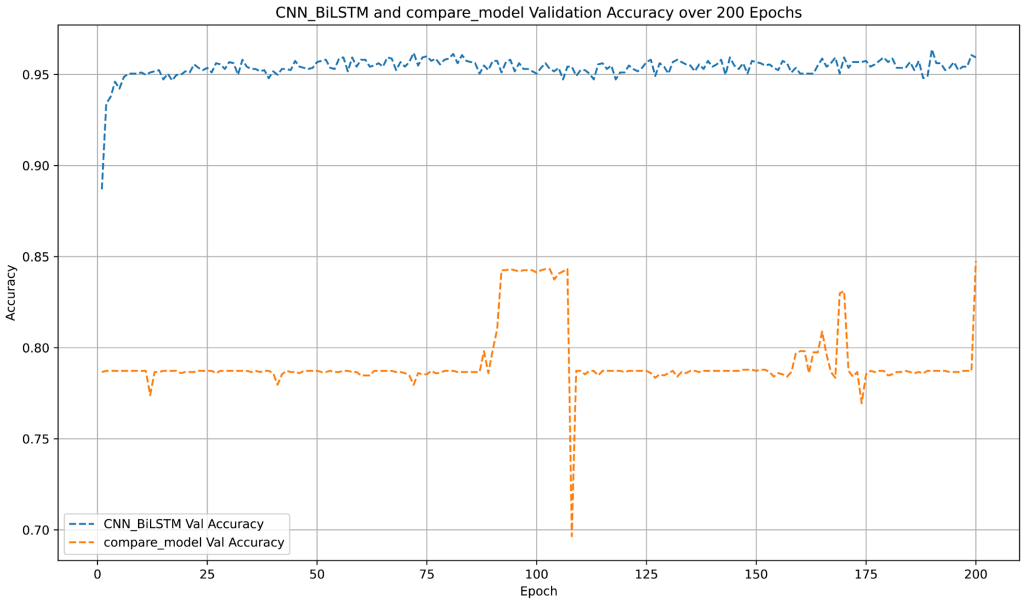
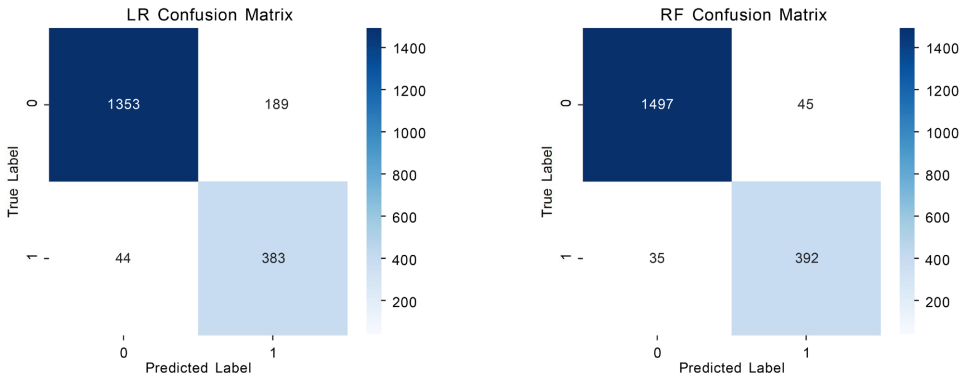


Figure 5. Comparative experiments (upper training set, lower validation set)
图 5. 对比实验(上训练集、下验证集)

然后，将该模型与其他经典机器学习模型进行对比。图 6 是逻辑回归、随机森林、XGBoost 和 CNN_BiLSTM 四种不同模型构成的混淆矩阵的可视化图，用于对比本研究提出来的 CNN_BiLSTM 和其他三种模型在恶意交易检测任务中的性能。通过混淆矩阵可以非常明了地看出，CNN_BiLSTM 模型的表现是最好的，它正确识别了 1517 笔攻击交易，正确判定了 25 笔正常交易，漏报和误判的交易一共仅有 58 笔，表明其对发起攻击行为的节点的捕捉能力更强。

根据表 2，可以观察数据发现：CNN_BiLSTM 模型在这四个评估指标上均取得了最高的分数，特别是作为用户攻击行为检测模型，达到了高准确率和高召回率的要求，得到了 0.98 的准确率和 0.96 的召回率，远超过其他三种模型。由于以太坊的共识机制是 PoS 共识机制，对于攻击者而言，他们发起攻击的条件不仅在于手里权益的多少，还包括该权益在手中的时长。因此，如果需要检测在以太坊的交易数据中，用户是否发起攻击的检测实验，还需要结合时间序列等条件对其进行训练检测。因此，CNN_BiLSTM 模型结合了卷积神经网络和双向长短期记忆网络的特点，利用卷积神经网络可以有效地提取数据的局部特征并进行特征降维，利用双向长短期记忆网络捕捉时间序列中的长期依赖关系。所以结合权益证明共识机制特点对其进行模型设计的方法，能够使得模型在性能方面表现良好。



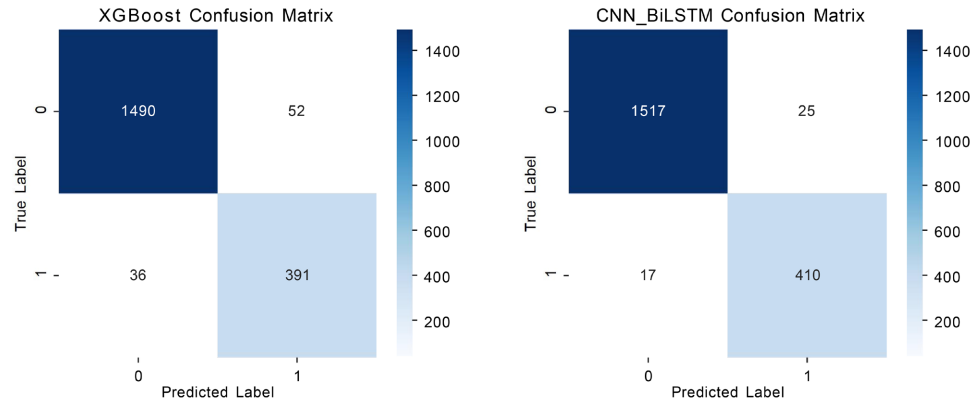


Figure 6. Visualization of confusion matrices for four models
图 6. 四种模型的混淆矩阵可视化

Table 2. Performance comparison of CNN_BiLSTM detection model with other models
表 2. CNN_BiLSTM 检测模型与其他模型的性能对比

Model	Precision	Recall	F1 Score	Accuracy
LR	0.66	0.89	0.75	0.88
RF	0.89	0.91	0.89	0.95
XGBoost	0.88	0.91	0.89	0.95
CNN-BiLSTM	**0.94**	**0.96**	**0.95**	**0.98**

4.3. 实验分析

实验结果表明，CNN_BiLSTM 模型在用户攻击行为检测任务中表现优异，其准确率、精确率、召回率和 F1 值均超过了逻辑回归、随机森林和 XGBoost 等传统机器学习模型。这一实验结果反映了该模型结构在以太坊交易数据中的适用性和优势。

由于以太坊的共识机制是 PoS 共识机制，对于攻击者而言，他们发起攻击的条件不仅在于手里权益的多少，还包括该权益在手中的时长。因此，如果需要检测在以太坊的交易数据中，用户是否发起攻击的检测实验，还需要结合时间序列等条件对其进行训练检测。因此，CNN_BiLSTM 模型结合了卷积神经网络和双向长短期记忆网络的特点，利用卷积神经网络可以有效地提取数据的局部特征并进行特征降维，利用双向长短期记忆网络捕捉时间序列中的长期依赖关系。所以结合权益证明共识机制特点对其进行模型设计的方法，能够使得模型在性能方面表现良好。实验结果显示，CNN_BiLSTM 模型在召回率(0.96)和准确率(0.98)上均表现突出，验证了时间序列建模在以太坊交易场景中的重要性。

5. 总结

本研究提出了在以太币交易场景下，用于检测用户是否存在恶意攻击行为的检测模型：CNN_BiLSTM 模型，通过系统地分析以太币交易网络中合法交易与非法交易的特点，并根据以太坊权益证明机制的特点，联合卷积神经网络和长短期记忆网络，构建了用户攻击行为检测模型，得到较高的准确率和召回率。未来的研究将不仅仅局限于单链环境，而是面向更为复杂和多样化的区块链生态，推动区块链安全防护技术的不断进步和完善。

参考文献

[1] Lamport, L., Shostak, R. and Pease, M. (2019) The Byzantine Generals Problem. In: *Concurrency*: *The Works of Leslie Lamport*, Association for Computing Machinery, 203-226.

[2] Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T. and Dutkiewicz, E. (2019) Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities. *IEEE Access*, **7**, 85727-85745. https://doi.org/10.1109/access.2019.2925010

[3] Yan, C., Zhang, C., Lu, Z., Wang, Z., Liu, Y. and Liu, B. (2022) Blockchain Abnormal Behavior Awareness Methods: A Survey. *Cybersecurity*, **5**, Article No. 5. https://doi.org/10.1186/s42400-021-00107-4

[4] Lin, I.C. and Liao, T.C. (2017) A Survey of Blockchain Security Issues and Challenges. *International Journal of Network Security*, **19**, 653-659.

[5] Salman, T., Zolanvari, M., Erbad, A., Jain, R. and Samaka, M. (2019) Security Services Using Blockchains: A State of the Art Survey. *IEEE Communications Surveys & Tutorials*, **21**, 858-880. https://doi.org/10.1109/comst.2018.2863956

[6] Conti, M., Sandeep Kumar, E., Lal, C. and Ruj, S. (2018) A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials*, **20**, 3416-3452. https://doi.org/10.1109/comst.2018.2842460

[7] Li, X., Jiang, P., Chen, T., Luo, X. and Wen, Q. (2020) A Survey on the Security of Blockchain Systems. *Future Generation Computer Systems*, **107**, 841-853. https://doi.org/10.1016/j.future.2017.08.020

[8] Xu, G., Guo, B., Su, C., Zheng, X., Liang, K., Wong, D.S., *et al*. (2020) Am I Eclipsed? A Smart Detector of Eclipse Attacks for Ethereum. *Computers & Security*, **88**, Article 101604. https://doi.org/10.1016/j.cose.2019.101604

[9] Ostapowicz, M. and Żbikowski, K. (2019) Detecting Fraudulent Accounts on Blockchain: A Supervised Approach. In: *Lecture Notes in Computer Science*, Springer, 18-31. https://doi.org/10.1007/978-3-030-34223-4_2

[10] Tan, R., Tan, Q., Zhang, P. and Li, Z. (2021) Graph Neural Network for Ethereum Fraud Detection. 2021 *IEEE International Conference on Big Knowledge* (*ICBK*), Auckland, 7-8 December 2021, 78-85. https://doi.org/10.1109/ickg52313.2021.00020

[11] Elmougy, Y. and Manzi, O. (2021) Anomaly Detection on Bitcoin, Ethereum Networks Using GPU-Accelerated Machine Learning Methods. 2021 31*st International Conference on Computer Theory and Applications* (*ICCTA*), Alexandria, 11-13 December 2021, 166-171. https://doi.org/10.1109/iccta54562.2021.9916625

[12] Kumar, N., Singh, A., Handa, A. and Shukla, S.K. (2020) Detecting Malicious Accounts on the Ethereum Blockchain with Supervised Learning. In: *Lecture Notes in Computer Science*, Springer, 94-109. https://doi.org/10.1007/978-3-030-49785-9_7

[13] Dahiya, M., Mishra, N. and Singh, R. (2023) Neural Network Based Approach for Ethereum Fraud Detection. 2023 4*th International Conference on Intelligent Engineering and Management* (*ICIEM*), London, 9-11 May 2023, 1-4. https://doi.org/10.1109/iciem59379.2023.10166745

[14] Farrugia, S., Ellul, J. and Azzopardi, G. (2020) Detection of Illicit Accounts over the Ethereum Blockchain. *Expert Systems with Applications*, **150**, Article 113318. https://doi.org/10.1016/j.eswa.2020.113318

[15] Akbar, N.A., Muneer, A., ElHakim, N. and Fati, S.M. (2021) Distributed Hybrid Double-Spending Attack Prevention Mechanism for Proof-of-Work and Proof-of-Stake Blockchain Consensuses. *Future Internet*, **13**, Article 285. https://doi.org/10.3390/fi13110285

[16] Tas, E.N., Tse, D., Yu, F., *et al*. (2022) Babylon: Reusing Bitcoin Mining to Enhance Proof-of-Stake Security.

[17] Sanda, O., Pavlidis, M., Seraj, S. and Polatidis, N. (2023) Long-Range Attack Detection on Permissionless Blockchains Using Deep Learning. *Expert Systems with Applications*, **218**, Article 119606. https://doi.org/10.1016/j.eswa.2023.119606

[18] Fukushima, K. (1980) Neocognitron: A Self-Organizing Neural Network Model for a Mechanism of Pattern Recognition Unaffected by Shift in Position. *Biological Cybernetics*, **36**, 193-202. https://doi.org/10.1007/bf00344251

[19] Lecun, Y., Bottou, L., Bengio, Y. and Haffner, P. (1998) Gradient-Based Learning Applied to Document Recognition. *Proceedings of the IEEE*, **86**, 2278-2324. https://doi.org/10.1109/5.726791

[20] Hochreiter, S. and Schmidhuber, J. (1997) Long Short-Term Memory. *Neural Computation*, **9**, 1735-1780. https://doi.org/10.1162/neco.1997.9.8.1735