单位代码：10359　　密　级：公开
学　　号：2022180187　　分类号：TP393.08

合肥工業大學

Hefei University of Technology

硕士学位论文

MASTER'S DISSERTATION

论文题目：	基于全局图结构与局部语义的区块链欺诈检测方法相关研究
学位类别：	专业硕士
专业名称：	网络与信息安全
作者姓名：	张升
导师姓名：	凌能祥 教授
完成时间：	2025 年 6 月

合　肥　工　业　大　学

专业硕士学位论文

基于全局图结构与局部语义的区块链欺诈检测方法相关研究

作者姓名： 张升

指导教师： 凌能祥 教授

学科专业： 网络与信息安全

研究方向： 区块链安全

2025 年 6 月

A Dissertation Submitted for the Degree of Master

A Study on Blockchain Phishing Detection methods Based on Global Graph Structures and Local Semantics

By

Zhang Sheng

Hefei University of Technology

Hefei, Anhui, P.R.China

June, 2025

学位论文独创性声明

本人郑重声明：所呈交的学位论文是本人在导师指导下进行独立研究工作所取得的成果。据我所知，除了文中特别加以标注和致谢的内容外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得 合肥工业大学 或其他教育机构的学位或证书而使用过的材料。对本文成果做出贡献的个人和集体，本人已在论文中作了明确的说明，并表示谢意。

学位论文中表达的观点纯属作者本人观点，与合肥工业大学无关。

学位论文作者签名：张升　　签字日期：2025 年 5 月 30 日

学位论文版权使用授权书

本学位论文作者完全了解 合肥工业大学 有关保留、使用学位论文的规定，即：除保密期内的涉密学位论文外，学校有权保存并向国家有关部门或机构送交论文的复印件和电子光盘，允许论文被查阅或借阅。本人授权 合肥工业大学 可以将本学位论文的全部或部分内容编入有关数据库，允许采用影印、缩印或扫描等复制手段保存、汇编学位论文。

（保密的学位论文在解密后适用本授权书）

学位论文作者签名：张升　　指导教师签名：

签名日期：2025 年 5 月 30 日　　签名日期：2025 年 5 月 30 日

论文作者毕业去向

工作单位：

联系电话：　　E-mail：

通讯地址：　　邮政编码：

合 肥 工 业 大 学

本论文经答辩委员会全体委员审查，确认符合合肥工业大学专业硕士学位论文质量要求。

答辩委员会签名（工作单位、职称、姓名）

主席：中国科学院合肥物质科学研究院　　研究员

委员：合肥工业大学　　教授

合肥工业大学　　教授

合肥工业大学　　副教授

合肥工业大学　　副教授

导师：合肥工业大学　　教授

致　谢

这三年过得很快，也很充实。这三年来，求学的足迹走过了合肥、宁波、杭州、新加坡，在此期间也结识了不少良师：凌老师、浙江大学的许老师和王师兄、东方理工的姜老师、新加坡管理大学的段老师以及美国圣地亚哥州立大学的李老师。也结识了不少益友：上海交通大学的段博士、香港理工大学的贺博士等等。我为我能在硕士三年和各位一起工作表示感激。

也感谢项目资助机构为本研究提供的资金支持，为实验与数据采集提供了坚实保障。

最后，衷心感谢我的家人，感谢父母无条件的理解与支持，你们的关爱是我前行的不竭动力。

谨以此致谢，献给所有在我硕士求学历程中给予帮助的师长和挚友。

作者：张升

2025 年 4 月 1 日

摘　要

随着区块链技术的出现，智能合约在金融领域得到了广泛应用。这项革命性技术通过密码学算法构建的去中心化信任机制，有效解决了传统金融交易中存在的中介依赖性强、流程透明度不足、合约执行效率低下等痛点问题。然而，现有的欺诈检测方法在捕捉交易网络中的全局结构模式以及交易数据中蕴含的局部语义关系方面存在局限性。大多数现有模型仅单独关注结构信息或语义特征，导致在检测复杂欺诈模式时效果不尽如人意。为此，本文提出了一种动态特征融合模型，该模型结合了基于图的表示学习和语义特征提取方法来进行区块链欺诈检测。具体来说，我们构建了全局图表示以对账户关系进行建模，并从交易数据中提取局部上下文特征。同时，我们引入了一种动态多模态融合机制，用以自适应地整合这些特征，从而使模型能够有效捕捉结构性和语义性的欺诈模式。

此外，我们还开发了一套完整的数据处理流程，包括图构建、时间特征增强和文本预处理。基于大规模真实区块链数据集的实验结果显示，在准确率、F1 分数和召回率等指标上，我们的方法均超过了现有的基准方法。该研究的核心价值在于揭示了结构关系与语义相似性协同分析的必要性。通过融合账户网络拓扑特征与交易文本语义特征，模型能够突破单一特征分析的局限性。这种融合思路为区块链安全领域提供了新的技术路径，特别是在应对智能合约漏洞利用、钓鱼攻击等新型欺诈手段时展现出扩展性潜力。实验数据表明，同时考虑结构与语义特征的检测框架能够显著提升复杂场景下的欺诈识别效果。

关键词：区块链；欺诈检测；多模态融合；安全

ABSTRACT

With the emergence of blockchain technology, smart contracts have been widely applied in the financial sector. This revolutionary technology, through decentralized trust mechanisms built by cryptographic algorithms, effectively addresses pain points in traditional financial transactions such as high dependency on intermediaries, insufficient process transparency, and low contract execution efficiency. However, existing fraud detection methods exhibit limitations in capturing global structural patterns within transaction networks and local semantic relationships embedded in transaction data. Most current models focus solely on structural information or semantic features independently, resulting in suboptimal performance when detecting complex fraudulent patterns. To address this, this paper proposes a dynamic feature fusion model that combines graph-based representation learning with semantic feature extraction for blockchain fraud detection. Specifically, we construct global graph representations to model account relationships and extract local contextual features from transaction data. Additionally, we introduce a dynamic multimodal fusion mechanism to adaptively integrate these features, enabling the model to effectively capture structural and semantic fraudulent patterns.

Furthermore, we developed a complete data processing pipeline comprising graph construction, temporal feature enhancement, and text preprocessing. Experimental results on large-scale real blockchain datasets demonstrate that our method surpasses existing baseline approaches in accuracy, F1 score, and recall rate. The core value of this research lies in revealing the necessity of synergistic analysis between structural relationships and semantic similarities. By integrating topological features of account networks with semantic features of transaction texts, the model overcomes the limitations of single-feature analysis. This fusion approach provides a novel technical pathway for blockchain security, particularly demonstrating scalability potential in addressing emerging fraudulent techniques such as smart contract exploits and phishing attacks. Experimental evidence indicates that detection frameworks considering both structural and semantic features significantly enhance fraud identification effectiveness in complex scenarios.

KEYWORDS: Blockchain; Fraud Detection; Multimodal Fusion; Security

目 录

插图清单

表格清单

符号说明

$\mathbf{A}$ 交易账户图的邻接矩阵，$\mathbf{A}[i,j]$ 表示账户 i 到 j 的交易权重，由交易金额与时间特征加权计算

$\tilde{\mathbf{A}}$ 添加自环的邻接矩阵，$\tilde{\mathbf{A}} = \mathbf{A} + \mathbf{I}$

$\tilde{\mathbf{D}}$ 邻接矩阵的度矩阵，对角线元素为节点度数

ΔT_n n-gram 时间差，$\Delta T_n = T_i - T_{i-(n-1)}$，表示当前交易与前 $n-1$ 个交易的时间间隔

w_k 交易权重，$w_k = \text{value}_k \cdot \sum_{n=1}^{N} \alpha_n \Delta t_{n,k}$，由交易金额与时间聚合特征线性组合

α_n n-gram 时间差权重系数，$\alpha_n = \frac{1/n}{\sum_{j=1}^{N}(1/j)}$，强调短期交易爆发模式

$\mathbf{H}^{(l)}$ 第 l 层 GCN 节点特征矩阵，初始 $\mathbf{H}^{(0)}$ 为账户初始特征

$\mathbf{W}^{(l)}$ 第 l 层 GCN 可学习权重矩阵

$\mathbf{E}_{\text{BERT}}$ BERT 嵌入表示，包含词向量、位置向量和段落类型向量

$\mathbf{E}_{\text{Fusion}}$ 动态融合嵌入，$\mathbf{E}_{\text{Fusion}} = g_1\mathbf{E}_{\text{BERT}} + g_2\mathbf{E}_{\text{GCN}} + g_3(\alpha\mathbf{E}_{\text{BERT}} + (1-\alpha)\mathbf{E}_{\text{GCN}})$

g_i 动态融合门控权重，通过 Gumbel-Softmax 计算，τ 控制权重分布的尖锐程度

$\mathbf{W}_{\text{fusion}}$ 分类器权重矩阵，$\mathbf{y} = \text{Softmax}(\mathbf{W}_{\text{fusion}}\mathbf{H}_{\text{fusion}} + \mathbf{b}_{\text{fusion}})$

第一章 引言

1.1 研究背景及意义

(1) 研究背景

区块链技术近年来在全球范围内迅速发展，成为多个行业变革的驱动力。作为一种去中心化的分布式账本技术，区块链能够在没有中央管理机构的情况下确保数据的安全性和透明性。特别是在金融行业，区块链的引入使得支付、交易、证券、供应链金融等多个领域发生了深远变化[1]。在传统的支付系统中，跨境支付通常需要通过多个中介，这不仅增加了成本，也降低了交易的速度。而通过区块链，支付可以直接在参与者之间完成，无需中介，从而大幅度提升了交易的速度和透明度。

然而，随着区块链技术的普及，相关的安全问题和欺诈行为也随之增多。由于区块链本身具有匿名性和去中心化特点，恶意用户能够通过伪造身份、篡改交易记录等手段进行欺诈[2]。尤其在加密货币交易中，黑客通过利用智能合约的漏洞进行攻击，造成了大量的财务损失[3]。此外，随着区块链技术在供应链管理、物联网等领域的应用增加，相关的欺诈行为呈现多样化趋势，给社会和经济带来了严峻挑战[2]。

尽管区块链技术具有明显的优势，但也面临着包括隐私泄露、法律监管滞后等一系列挑战。由于区块链的交易信息公开透明，任何人都可以查看交易的全过程，这虽然为提高透明度提供了保障，但同时也暴露了用户的隐私和敏感信息[4]。此外，区块链技术虽然提高了交易的安全性，但其在监管方面的挑战仍然突出。许多国家和地区的法律体系尚未完全适应区块链带来的新问题，导致相关的监管法规滞后，增加了非法活动的风险[3]。

在供应链管理中，区块链的应用虽然提升了透明度和可追溯性，但由于供应链的复杂性和跨行业的参与方，仍然面临较大的欺诈风险。例如，某些不法分子利用供应链中的信息不对称，通过虚假数据篡改来掩盖其不正当行为[5]。这些问题引发了对区块链技术安全性的广泛关注，并迫使学者和行业专家加强对区块链安全性的研究。

此外，区块链技术在金融领域的应用尤其复杂，因为金融交易通常伴随着极高的风险。在面对跨境支付、证券交易、数字货币等高风险操作时，区块链技术的安全性和防护能力显得尤为重要。尽管区块链的去中心化特点有助于降低传统金融系统中的单点故障风险，但它也可能成为攻击者的新目标，例如通过 51% 攻击、智能合约漏洞等方式进行恶意篡改[3]。

(2) 研究意义

为了应对这些问题，学者们提出了多种区块链安全防护方案，其中包括基于人工智能的欺诈检测技术[6]。近年来，人工智能和机器学习在区块链安全中的应用取得了显著进展，尤其是在欺诈行为的识别与预测方面，成为了研究的重点[2]。在以太坊中的钓鱼检测长期以来一直依赖图神经网络（GNNs）[7] 来对交易图中的资金流进行建模。图神经网络作为处理图结构数据的有效工具，能够在区块链网络中通过分析账户之间的资金流动关系，挖掘出潜在的欺诈行为。具体来说，GNN 通过对区块链交易数据中的图结构进行学习，可以发现资金流动中的异常模式，从而识别潜在的钓鱼行为[8]。这种方法的核心优势在于其能够自动捕捉和学习图中的节点之间的依赖关系，且无需人工设计特征，使得图神经网络在金融欺诈检测中获得了广泛应用。

然而，尽管图神经网络（GNN）在捕捉全局交易结构方面具有显著优势，当前的图神经网络方法依然面临一些挑战。最显著的问题之一是交易关系的二值性和邻居采样策略的局限性。在传统的 GNN 模型中，交易关系通常被视为存在或缺失，而这种二值化处理方式很难捕捉到账户行为的细微差异，尤其是在高频交易和周期性转账等情形下。例如，在许多钓鱼攻击中，恶意账户会通过频繁的小额交易来掩盖其真实意图，这种行为模式在普通 GNN 模型中容易被忽视[9]。

此外，图神经网络的邻居采样策略通常是基于节点的邻接信息进行采样，而对于大规模的区块链网络而言，节点的邻接信息可能会被稀疏化，导致邻居采样的效果不尽如人意。这种情况下，GNN 无法有效捕捉到账户之间的复杂交互关系，尤其是在存在多个相似节点或者多个交易对手的情况下，如何准确地识别出恶意账户，成为了一个亟待解决的难题[10]。

为了克服这些问题，近年来一些方法开始引入序列建模技术，如 Transformer 和 LSTM 等，来对账户的交易序列进行上下文建模，从而捕捉交易行为中的时序模式[11]. 通过对账户的交易行为进行序列化处理，序列模型能够从完整的交易记录中捕捉到更为细致的上下文信息，例如周期性转账、固定对手方偏好以及特定时间窗口内的交易激增。这些信息通常能揭示出钓鱼账户在短时间内的异常行为模式，如频繁的资金转移、金额相似的交易等，正是这些行为的异常性让传统的基于图结构的模型难以捕捉[12]。

然而，序列模型在解决上述问题时也带来了一些新的挑战。最主要的一个问题是，序列模型无法直接利用区块链交易图中的拓扑结构信息。虽然序列模型可以有效捕捉到账户的行为序列，但对于账户间的全局结构关系和交易模式，序列模型无法进行充分的建模。这导致了一个显著的局限性：尽管可以识别出局部的交易模式，但对于跨账户之间的关联关系和复杂的行为网络，序列模型往往表现得较为薄弱。因此，目前的研究工作往往试图将图神经网络和序列模型结合，以期

实现更为全面的欺诈检测。

局部语义相似性信息是当前研究中的一个重要方向。正常账户和钓鱼账户的交易行为在局部模式上存在显著差异。正常账户通常表现为较为随机的行为，其交易频率较低，且金额和时间间隔不规则，因此这些账户之间的语义关联性较弱[13]。与此相对，钓鱼账户则表现出一致性特征——短时间内频繁交易、金额相近或存在重复行为。这些特点通常反映了钓鱼账户的自动化行为，即试图通过频繁的小额交易或与特定账户的重复交互，掩盖其真实意图。当前的检测方法往往难以捕捉这些局部的语义相似性，限制了其在识别复杂欺诈行为时的准确性。

例如，在一些基于图神经网络的模型中，节点之间的关系仅仅通过交易是否发生来判定，而忽略了交易时间的间隔和金额的相似性，这使得模型难以发现那些特定时间内的异常交易行为，尤其是在钓鱼攻击中，攻击者往往通过短时间内的频繁交易来测试不同账户的响应[14]。因此，局部语义信息的提取，尤其是交易行为中时间、金额等因素的综合分析，对于提高欺诈检测模型的精度至关重要。

全体交易账户网络信息的分析则是另一个关键点。正常账户和钓鱼账户在网络结构上存在显著差异。正常账户通常构成稀疏连接的网络，账户之间的聚类较少，呈现出较为随机的交易模式[15]。相比之下，钓鱼账户往往在网络中形成高密度的子网络，这些子网络的节点之间存在紧密的联系，交易行为集中且频繁。通过分析这种高密度子网络的形成，我们可以有效地识别出可能的钓鱼账户。具体来说，钓鱼账户通常会在短时间内产生大量的交易，且这些交易的金额和对象高度相似，形成异常的交易聚集。这些交易聚集的局部高连通性为钓鱼行为提供了有力的指示[12]。

目前，大部分的图神经网络方法已经能够一定程度地捕捉这种结构信息，但仍然存在对于大规模网络数据的处理能力有限的问题。在面对高密度网络和多变的交易模式时，如何更精确地提取出全局网络结构信息，并结合局部交易行为模式进行综合分析，仍然是当前研究中的一个挑战。

1.2 国内外研究现状

1.2.1 基于图的欺诈检测

在区块链网络中，交易数据通常具有复杂的关系结构，而基于图的模型能够有效捕捉这些复杂关系，并在欺诈检测中表现出色。区块链平台的去中心化特性使得每一笔交易都可能涉及多个账户之间的交互，形成了一个动态且多层次的交易网络。这些网络中的节点代表区块链上的账户，而边则表示账户之间的交易行为。通过这种方式，区块链交易数据不仅呈现出明显的图结构特征，而且这些图结构能够反映账户间的交易关系、行为模式及潜在的风险点。基于图的模型尤其在图神经网络（GNNs）方面展现了巨大的潜力，能够通过学习节点和边的特征来有

效地识别欺诈行为，如钓鱼账户和恶意行为者的活动[16]。

图神经网络（GNNs）通过对节点及其邻居的特征进行聚合，从而为每个节点生成高维表示。这种表示能够有效捕捉节点间的复杂关系，并有助于揭示潜在的欺诈行为。在以太坊等区块链平台上，图神经网络（GNNs）已经被广泛应用于检测欺诈行为。例如，Tan[17] 提出了一种基于图卷积网络（GCNs）的模型，用于从以太坊交易记录中检测欺诈。该模型通过构建交易网络和提取节点特征，将地址分为正常和欺诈两类。具体来说，模型首先通过图结构捕捉账户间的交易关系，并将账户特征转化为向量，进而利用图卷积网络进行特征聚合，从而在图的层级上学习账户的潜在行为模式。在此过程中，GCN 能够在多层网络中传播信息，从而捕获到更深层次的账户行为特征，如周期性交易或异常资金流动等。通过这种方式，模型能够准确识别那些行为模式与正常账户有显著差异的钓鱼账户。

此外，Kanezashi[18] 探讨了在以太坊交易网络中使用异构图神经网络的应用，重点关注如何处理大规模网络以及标签不平衡问题。在以太坊网络中，由于正常账户的数量远大于钓鱼账户，导致标签不平衡问题的严重性。为了解决这一问题，Kanezashi 提出了异构图神经网络（HGNN），该方法在构建交易图时，将不同类型的交易行为视为不同类型的边，从而实现更加精准的特征提取。此外，异构图神经网络通过增加额外的边类型，有效增强了模型在处理不同类型账户之间的交互时的表达能力。通过这种方式，模型能够更加灵活地适应区块链网络的多样性，并且能够针对不同类型的欺诈行为进行特定的学习。

在另一个研究中，Li[19] 提出了一个称为 PDGNN 的钓鱼检测框架。该框架基于 Chebyshev-GCN，通过提取交易子图并训练分类模型，能够在大规模以太坊网络中有效地区分正常账户与钓鱼账户。与传统的 GCN 模型相比，Chebyshev-GCN 通过使用 Chebyshev 多项式逼近卷积运算，从而在计算上提高了效率，同时保持了较高的精度。通过这种方式，PDGNN 能够在处理大规模数据时，避免了过度计算和过拟合的问题。此外，Li 提出的交易子图（Subgraph）方法，通过提取与账户行为相关的局部子图，进一步优化了模型的学习过程，使得模型能够更好地捕捉到钓鱼账户的特殊行为模式，如频繁的小额交易、固定对手方偏好等。

Wang[20] 提出了交易子图网络（TSGN）框架，通过构建捕捉交易流关键特征的交易子图来增强以太坊钓鱼检测。与传统的全局图神经网络不同，TSGN 通过在图中划分交易子图，对每个子图进行特征学习。这种方法能够更有效地捕捉交易流中的局部行为特征，尤其是在面对复杂的账户行为时，可以避免全局信息的过度干扰。通过对局部图的关注，TSGN 模型能够更精准地捕捉到钓鱼账户的异常交易模式，如频繁与特定账户交易、相似金额的重复交易等行为，从而显著提升了模型在实际应用中的准确性。

Hou[21] 则提出了一种基于 GCN 和条件随机场（CRF）的以太坊钓鱼检测方

法。该方法首先利用 DeepWalk 为交易图中每个账户节点生成初始特征，然后采用 GCN 学习图结构表示，以捕捉账户间的交易关系。DeepWalk 是一种基于随机游走的节点嵌入方法，通过模拟账户间的交易行为，生成每个节点的初始向量表示。这些初始特征为后续的 GCN 学习提供了丰富的信息。为了进一步提高分类性能，CRF 层被引入模型中，CRF 能够通过条件依赖关系对相似节点进行聚类，从而进一步增强了相似节点之间的联系。这种方法的创新之处在于将图神经网络与条件随机场结合，进一步提高了钓鱼账户的识别能力，尤其是在处理节点间相似性较高时，能够有效避免误分类。

尽管基于图神经网络的方法在欺诈检测中取得了显著进展，但仍然存在一些挑战。首先，区块链交易图的规模非常庞大，尤其是在以太坊等公链中，节点和边的数量极为庞大，这对图神经网络的计算能力提出了较高的要求。如何在保证模型准确性的同时提高计算效率，仍然是当前研究中的一个重要问题。其次，交易图中的标签不平衡问题依然存在，大量正常账户与少数钓鱼账户之间的差异性使得模型的训练过程容易出现过拟合。因此，未来的研究需要更多地关注如何解决大规模数据处理和标签不平衡的问题。

1.2.2 基于时间序列数据的欺诈检测

时间序列数据分析在区块链欺诈检测中扮演着重要角色，尤其是在处理交易记录和检测异常行为方面。随着区块链技术的不断发展，平台上每天产生的交易数量庞大，其中包含了大量有价值的时间序列信息。尤其是在像以太坊这样的大型区块链平台上，交易时间、交易频率、交易金额及其波动等时间序列信息可用于识别潜在的欺诈行为。时间序列数据的独特性和丰富的上下文使得其在检测异常活动、发现可疑模式以及对抗不断演化的欺诈行为中发挥着越来越重要的作用[22]。

(1) LSTM 在时间序列数据中的应用

在区块链欺诈检测领域，长短时记忆网络（LSTM）作为一种强大的序列建模工具，已经被广泛应用于时间序列数据的异常检测。LSTM 能够有效地捕捉时间序列中的长短期依赖关系，对于处理区块链交易数据中如交易频率、时间间隔及金额波动等信息，展现出了显著的优势。Hu[22] 提出了基于 LSTM 的时间序列分析方法，应用于以太坊智能合约中的交易欺诈检测。LSTM 模型能够从历史交易序列中捕捉到异常交易行为的时间特征，如短时间内的交易激增、频繁的重复交易等，这些都是潜在的欺诈行为的表现。

LSTM 通过记忆网络中的门控机制有效解决了传统 RNN 在长时间序列中梯度消失的问题，能够在处理复杂的交易行为时，保持对过去交易的敏感性，从而识别出欺诈行为的潜在规律。例如，在一个多交易者参与的场景下，LSTM 可以追踪账户间的交易模式，检测出有规律的、不寻常的交易行为，尤其是在跨账户大规模转

移资金时，LSTM 可以捕捉到这类行为的时间序列异常，并通过模型的训练将其分类为可能的欺诈行为[23]。

(2) XGBoost 与时间序列特征的结合

除了 LSTM，另一种流行的机器学习方法是 XGBoost，它在许多欺诈检测任务中显示了极高的性能。XGBoost 利用梯度提升算法（GBDT），在对数据进行分类时能够高效地处理特征的非线性关系。Farrugia[23] 提出了结合时间序列特征与 XGBoost 模型用于以太坊非法账户检测的方法。该研究通过提取关键时间序列特征，并与 XGBoost 进行结合，强调了诸如交易时间间隔、交易金额波动等特征在检测非法账户中的重要性。

具体来说，Farrugia 通过提取时间序列的统计特征（如均值、标准差、最大值和最小值）以及交易的时间特征（如每日交易频率、交易时间间隔）来构建特征向量，并输入到 XGBoost 模型中进行训练。与 LSTM 不同，XGBoost 能够快速处理大量的时间序列数据，并在短时间内完成训练，适用于大规模数据集的检测任务。Farrugia 的工作展示了如何结合机器学习算法和时间序列分析方法，提升区块链欺诈检测的精度和效率。通过这种方式，XGBoost 模型不仅能够从历史数据中学习账户行为模式，还能够识别出那些在正常交易行为中不容易察觉的异常模式[24]。

1.2.3 混合方法

混合方法整合了图数据、时间序列数据和语义信息等多种信息，从而实现了更高的检测准确率和鲁棒性，能够有效识别以太坊恶意交易检测中的复杂和动态欺诈模式[25]。近年来，随着区块链技术的快速发展，尤其是以太坊智能合约的广泛应用，欺诈行为在区块链平台中变得越来越复杂多样。为了有效识别这些恶意行为，研究人员提出了多种混合方法，通过融合不同类型的数据和算法，提升了检测的准确性与效率。混合方法的核心思想在于通过多模态数据的综合分析，最大化地发掘其中的潜在欺诈模式，使得模型能够更好地应对多样化的欺诈行为，尤其是在面对交易模式隐蔽、恶意行为高度动态变化的情况下，表现出更强的适应性和准确性。

其中，基于图神经网络（GNN）的混合方法已经成为一种重要的研究方向。图神经网络能够有效地捕捉以太坊交易数据中的复杂关系结构，利用图结构的特性对交易模式进行建模，进而发现其中的异常行为和潜在欺诈。结合其他类型的数据，如时间序列数据和语义信息，可以进一步提升检测系统的鲁棒性和准确率。

Li 等人[26] 提出了用于以太坊钓鱼检测的时序交易聚合图网络（TTAGN），该方法利用时间交易数据来提高检测准确性。TTAGN 结合了时序边表示、边到节点聚合以及结构增强来捕捉交易模式和网络结构，从而能够更好地揭示交易中的潜在欺诈行为。具体而言，TTAGN 模型通过将时间序列信息融入到图结构中，增强

了图神经网络在捕捉交易模式方面的能力。时间边表示在 TTAGN 中扮演了关键角色，它不仅捕捉了交易发生的顺序信息，还为模型提供了交易时序的上下文，有效解决了传统图神经网络在处理时序数据时面临的困难。实验表明，TTAGN 在真实数据集上的表现优于现有方法，尤其在复杂交易模式的识别上具有显著优势。

在 TTAGN 的基础上，Wen 等人[27] 提出了另一种创新的混合特征融合模型，名为 LBPS（LSTM-BP-Sequence），用于以太坊钓鱼检测。LBPS 模型结合了 LSTM-FCN 和 BP 神经网络，通过融合时间序列特征和手工特征工程提取的信息，进一步提升了模型的检测能力。具体来说，LBPS 模型采用 LSTM-FCN 网络来提取交易数据的时序特征，LSTM 用于捕捉长时间依赖关系，FCN 则有助于提高时序特征的表达能力。与此同时，BP 神经网络被用来捕捉交易记录中手工特征与交易结果之间的隐含关系，从而增强了特征的表达能力。通过这种多模态特征融合，LBPS 模型能够在面对不同类型的欺诈模式时，展示出较高的适应性和准确性。实验结果表明，LBPS 模型在多个标准数据集上取得了显著的检测性能，尤其是在处理具有强烈时序特征的钓鱼交易时，优于传统的单一模型方法。

Chen 等人[28] 提出了 DA-HGNN 模型，这是一种结合数据增强的混合图神经网络，用于以太坊钓鱼检测。DA-HGNN 模型通过引入数据增强技术，解决了传统模型在面对数据不平衡问题时的表现欠佳的问题。在这一模型中，Conv1D 和 GRU-MHA 被融合用于提取时序特征。Conv1D 层通过卷积操作有效地提取了交易序列中的局部时序特征，而 GRU-MHA 则在处理长时序依赖时发挥了关键作用，尤其在捕捉交易过程中的动态变化方面具有重要意义。同时，DA-HGNN 利用 SAGEConv 来捕捉交易图中的结构特征，进一步增强了图神经网络的表现力。SAGEConv 作为一种图卷积操作，能够在处理大规模图数据时有效地聚合邻居节点的信息，从而为节点和边的表示提供了更加丰富的上下文信息。通过数据增强的策略，DA-HGNN 模型能够在样本不平衡的情况下提高检测的鲁棒性，增强了模型在实际应用中的泛化能力。

与上述模型相比，我们提出的 ETH-GBERT 模型具有显著优势。不同于纯图基模型（如 GCN[7] 或 GAT[29]），ETH-GBERT 融入了丰富的交易文本语义，使其能够检测出可能不形成明显结构模式的钓鱼账户。纯图神经网络模型，如 GCN，依赖于交易图中的节点和边结构进行欺诈检测，能够有效地捕捉到账户之间的全局交易模式。例如，GCN 在捕捉账户之间的资金流动关系和节点间的密切联系时表现出色[7]，但当欺诈行为不呈现出明显的结构性模式时，GCN 的表现就相对较差。许多钓鱼攻击往往依赖于账户间的频繁、但金额较小的交易，这类行为在结构上可能不具有足够的显著性，导致传统图神经网络方法的检测效果有限。

另一方面，ETH-GBERT 通过结合 BERT 模型的文本特征，使得模型能够不仅捕捉结构信息，还能通过分析交易文本（如合约详情、备注信息、交易额等）深入

挖掘账户行为的语义特征。BERT 模型经过大量文本数据的预训练，能够理解语言的上下文关系，因此，能够揭示出隐藏在交易描述中的语义信息[30]。例如，通过分析交易的智能合约文本或账户备注，BERT 能够识别出包含潜在欺诈行为的语义模式，即使这些模式在图结构中不明显。这样一来，即使是那些依赖于文本暗示、并没有直接显示为交易模式的钓鱼账户，ETH-GBERT 也能够有效识别。

与仅基于文本的模型如 BERT4ETH[31] 相比，ETH-GBERT 的优势在于其结合了图神经网络的全局结构信息来增强对复杂交互模式的检测。BERT4ETH 仅使用交易的文本描述进行欺诈检测，而忽视了交易图中的结构信息，这限制了其对账户间复杂交互模式的识别能力。比如，BERT4ETH 虽然能够分析账户的语义层面的信息，但在面对跨账户之间的资金流动，尤其是大规模、多次的资金转移时，模型的表现可能不如基于图结构的模型。由于这些资金流动模式涉及到账户间的网络结构，BERT4ETH 无法有效地从全局结构角度捕捉到账户间的潜在关系，而这正是图神经网络能够发挥其优势的地方。

此外，尽管现有的混合方法（如 TTAGN[26] 和 LBPS[27]）也整合了多种特征类型，但 ETH-GBERT 独特地采用了一种动态融合机制，根据输入复杂性自适应地调整语义信息与结构信息的权重，从而显著提高了在异构区块链环境下的鲁棒性和灵活性。传统的混合模型，如 TTAGN，通过简单地将图嵌入和文本特征拼接在一起进行训练，虽然取得了较好的检测效果，但在面对更加复杂和多样化的区块链环境时，仍然存在一定的局限性。这些方法通常将结构信息和语义信息视为固定的特征，并不考虑输入数据的复杂性和多样性。而 ETH-GBERT 则通过其动态融合机制，能够根据交易的实际情况自适应地调整两类特征的权重，从而最大程度地挖掘每种特征所带来的价值。在某些情况下，语义信息可能更为重要，尤其是当交易行为缺乏明显的结构模式时；而在另一些情况下，图结构信息则能够提供更为直接的欺诈线索。因此，ETH-GBERT 的动态调整机制使得模型能够更好地适应各种复杂的欺诈检测场景。

1.3 主要研究内容

为了解决上述问题，整合多种有用信息成为一个极具前景的研究方向[32]。在本研究中，我们提出了一种基于深度学习的多模态融合框架，用于区块链交易数据的欺诈检测。与传统方法相比，所提出的方法能够同时捕捉交易网络中的全局结构关系和交易记录中蕴含的局部语义模式，从而在检测复杂欺诈行为时实现更高的准确性和鲁棒性。

我们首先构建全局账户交互图来表示区块链交易账户之间的关系。图中每个节点对应一个账户，而边则捕捉交易行为，如交易频率、交易金额和时间模式。为了从该图中提取有意义的结构特征，我们采用了基于图的表示学习方法，该方法

通过聚合邻近账户的信息来捕获交易网络中直接及间接的关系，从而使模型能够发现指示欺诈行为的全局交互模式。

其次，我们利用预训练的文本表示模型对交易数据中蕴含的语义信息进行处理。该模型将交易金额、智能合约细节及其他元数据等文本描述转换为高维特征向量，从而使模型能够识别局部上下文关系，例如重复出现的交易模式或与可疑账户相关的异常文本特征。

为了更好地利用结构和语义信息，我们提出了一种动态特征融合机制，该机制能够自适应地整合这两种特征空间。该机制通过学习平衡全局网络结构和局部交易语义在每笔交易中的相对重要性，使模型能够以更高精度检测出微妙且复杂的欺诈模式。

1.4 本文主要创新点

通过结合全局结构关系和局部语义特征这两种互补视角，我们的方法显著提升了欺诈检测的鲁棒性和精确性。基于真实区块链数据集的实验结果表明，所提出的 ETH-GBERT 模型达到了最先进水平。具体而言，在 Multigraph 数据集上，模型取得了 94.71% 的 F1 分数，显著超过表现最佳的基线方法 Role2Vec（F1 分数为 74.13%），提升幅度达 20.58%；在 Transaction Network 数据集上，ETH-GBERT 的 F1 分数为 86.16%，相较于下一个最佳模型 Role2Vec（F1 分数为 71.39%）也有明显提高（提升了 14.77%）；在 B4E 数据集中，ETH-GBERT 获得了 89.79% 的 F1 分数，超过最高基线方法 Role2Vec（F1 分数为 74.25%）15.54%。此外，该模型在召回率（89.57%）和精确率（90.84%）上也均表现出色，进一步凸显了其在识别钓鱼账户方面的鲁棒性。这些结果充分展示了模型在捕捉复杂欺诈模式、处理不平衡数据分布以及动态整合结构与语义特征方面的优势。

本研究的主要贡献如下：

1. 提出了一种动态多模态融合模型，该模型创新性地将图结构信息与文本语义相似性信息相结合，以提升区块链智能合约中的欺诈检测性能。
2. 开发了一套完整的数据处理流程，包括交易数据的提取、邻接矩阵的生成以及基于 BERT[30] 的文本表示处理，为其他区块链应用提供了有价值的参考。
3. 通过实验验证了所提方法的有效性，结果显示该方法在检测复杂欺诈行为方面表现优异，并显著优于现有的基准模型。

1.5 本文结构

本文结构安排如下：第一章为引言，首先介绍区块链安全与智能合约欺诈检测的研究背景及意义，随后回顾国内外在基于图、基于时间序列及混合方法等方面的研究现状，并概述本文的主要研究内容与创新点，最后给出论文整体结构安排。第二章为背景介绍，分别阐述区块链技术的基本理论、交易数据结构及智能合约

概念，并回顾人工智能与深度学习、BERT 及图卷积网络等相关技术；第三章聚焦于区块链交易数据的预处理方法，详细描述时间聚合特征增强、图数据生成与邻接矩阵构建、文本交易数据生成及清洗流程；第四章提出 ETH-GBERT 模型架构，依次介绍基于图的全局表示模块、基于 BERT 的局部语义提取模块，以及动态多模态融合机制的设计；第五章展示实验设计与结果，包括数据预处理与特征构建、超参数设置、损失函数与优化器选择，以及在多图、交易网络和 B4E 等数据集上的性能评估与对比分析；第六章为结论，总结本文研究贡献，讨论方法局限，并展望未来在实时检测、跨链分析与模型可解释性等方向的进一步工作。

第二章 背景

近年来，随着区块链技术的迅速发展，区块链网络中频繁发生的欺诈行为已成为一个全球性挑战。研究人员和开发者已经开发了各种欺诈检测方法，以应对这些挑战，并确保区块链系统的安全性和可靠性[16]。本节回顾了区块链的基础理论及现有的钓鱼欺诈检测方法，重点关注其技术创新与局限性。

2.1 区块链相关理论介绍

区块链技术作为近年来兴起的一种革命性技术，已经引起了学术界和产业界的广泛关注。其主要特征是去中心化、不可篡改、透明性和高安全性，这些特征使得区块链在多个领域展现出了巨大的应用潜力[33]。在本小节中，我们将介绍区块链的基本概念、工作原理、分类以及在各个领域中的应用。

2.1.1 区块链的定义

区块链是一种分布式数据库技术，旨在通过去中心化的方式保障数据的完整性与安全性。最初，区块链技术是为了解决数字货币（如比特币）的安全问题而被提出的[34]。然而，随着技术的发展，区块链逐渐被广泛应用于金融、供应链管理、医疗、版权保护等领域。区块链的核心理念是通过一系列加密算法和共识机制，确保交易的不可篡改性和透明性，从而减少中介机构的参与，提高效率[35]。

区块链系统由多个节点组成，节点之间通过点对点的网络进行通信，所有的交易和数据都通过区块存储在分布式账本上。每一个区块都包含一组交易记录，并通过加密技术与前一个区块进行连接，形成一个链式结构，因此得名“区块链”[36]。

2.1.2 区块链的工作原理

区块链的工作原理可以从以下几个方面来理解：

- **分布式账本**：区块链的核心是分布式账本，所有节点共享同一份账本，不存在单点故障。每个节点都持有完整的区块链副本，并能通过共识机制保持一致[37]。
- **加密技术**：为了确保数据的安全性和隐私性，区块链采用了先进的加密算法，如哈希算法和公私钥加密技术[38]。每个区块中的交易数据都被加密，以保证数据的不可篡改性。
- **共识机制**：区块链通过共识机制来达成对账本中交易的验证。最常见的共识机制有工作量证明（PoW）、权益证明（PoS）等。通过共识机制，网络中的所有节点能够就区块链的当前状态达成一致，从而防止双重支付等问题的发生[39]。
- **智能合约**：智能合约是区块链技术的一项重要创新。智能合约是由计算机程

序自动执行的一种协议，它能够在区块链上执行预定的合同条款，而不需要依赖第三方中介[33]。

2.1.3 区块链的分类

区块链根据其应用场景和权限管理的不同，通常可以分为以下几类：

- **公有链（Public Blockchain）**：公有链是完全开放的区块链网络，任何人都可以参与其中的节点，并且任何人都可以查看该链上的所有数据。比特币和以太坊都是公有链的典型代表[35]。
- **私有链（Private Blockchain）**：私有链是由单一组织或少数几个组织控制的区块链，网络中的节点权限受到严格控制，通常用于企业内部的数据管理和流程自动化[36]。
- **联盟链（Consortium Blockchain）**：联盟链是由多个组织联合建立和维护的区块链，适用于需要多个企业之间协作但又不希望完全公开的应用场景。联盟链的节点通常是由联盟成员控制，具有较高的隐私保护[37]。

2.1.4 区块链的交易数据

区块链的核心特征之一是交易数据的不可篡改性[39]。每一笔交易都会被记录到区块中，并在网络中传播，最终通过共识机制确认。这些交易数据由若干部分组成，包括但不限于交易发起方、接收方、交易金额、时间戳以及交易的数字签名。区块链的设计确保了交易数据的透明性、安全性和不可更改性，这对于去中心化的网络尤为重要。

(1) 交易数据结构

在区块链中，交易数据通常由以下几个部分组成：

- **交易输入（Transaction Input）**：每个交易输入指定了资金来源，它是前一笔交易的输出的引用。交易输入包含了一个指向之前交易输出的引用（即“UTXO”——未花费交易输出）。
- **交易输出（Transaction Output）**：交易输出指定了交易的目标地址，并包含了相应的金额信息。每个输出是由一个公钥（即地址）加密的，只有该地址的私钥持有者才能解锁这部分资金。
- **交易金额（Amount）**：每笔交易包含一个金额字段，表示该交易的资金转移数量。区块链中的数字货币（例如比特币、以太坊）通常有一个固定的精度单位。
- **时间戳（Timestamp）**：时间戳字段记录了交易发生的时间，通常是自 Unix 时间以来的秒数。这有助于确定交易的顺序。
- **数字签名（Digital Signature）**：数字签名是交易发起方使用私钥对交易进行签名生成的。签名不仅证明了交易的合法性，还保证了交易数据的完整性和

发起者的身份。

(2) 交易验证与共识机制

每笔交易在区块链网络中传播后，首先会由各个节点进行验证。验证过程主要包括:

- **签名验证：**每个节点会验证交易的数字签名，确保交易是由持有私钥的用户发起的，并且交易内容未被篡改。
- **余额验证：**节点会检查交易的输入部分，确保输入的资金没有被重复花费。这是防止双重支付的关键措施。
- **时间戳和顺序验证：**节点还会检查交易时间戳，确保交易按照正确的时间顺序进行处理。

当交易通过验证后，它将被包含在一个区块中，并通过共识机制（如 PoW 或 PoS）得到确认[38]。交易一旦被区块链确认，就无法进行更改或删除，这也是区块链不可篡改性的基础。

(3) 区块与区块链的关系

交易数据被打包成区块，并通过加密技术与前一个区块链接[39]。区块链中的每一个区块都包含了前一个区块的哈希值，这使得每一个区块与前一个区块不可分割，形成了一个线性的链条。每个区块都包含一个区块头和多个交易数据，每个区块的哈希值是通过对交易数据、前一个区块的哈希值以及其他信息（如时间戳、难度值等）进行哈希计算得到的[38]。

2.2 人工智能概述

人工智能（AI）是近年来最具革命性和前景的技术之一，深度学习作为 AI 的重要分支，已经广泛应用于语音识别、图像处理、自然语言处理（NLP）、自动驾驶等领域。深度学习模型通过构建复杂的神经网络来模拟人脑的认知过程，从而解决传统机器学习方法难以处理的高维数据问题。随着计算能力的提升和数据量的增加，深度学习的应用也日益成熟[40]。

在深度学习中，常用的模型有卷积神经网络（CNN）、循环神经网络（RNN）、生成对抗网络（GAN）等。这些网络通过不同的结构和学习机制来捕捉数据的深层特征，从而使得机器在图像识别、语音合成、自动翻译等任务中表现出色[41]。

2.2.1 深度学习（Deep Learning）

深度学习是一类基于人工神经网络的学习方法，特别强调通过多层网络结构进行特征自动提取。在传统机器学习中，特征提取通常依赖专家知识，而深度学习通过逐层学习自动提取特征。深度学习的基础是多层神经网络，其中每一层的输出都是对上一层的输入进行加权和非线性变换的结果[42]。

深度神经网络（DNN）通常包含多个隐藏层，每一层都是一个神经元的集合，

神经元之间通过加权连接相连。深度学习模型通过反向传播算法（backpropagation）来更新每一层的权重，以最小化误差函数。与传统算法相比，深度学习能够在大数据和高维数据的情况下表现得更好，尤其在图像和语音识别方面的应用取得了突破性进展[40]。

深度学习的经典模型包括卷积神经网络（CNN）和循环神经网络（RNN）。CNN 在图像处理和计算机视觉领域中得到了广泛应用，通过局部连接、权重共享和池化等策略来减少参数数量，提高计算效率[43]。RNN 则在处理序列数据（如文本、语音等）时具有优势，能够捕捉数据的时序关系和上下文信息[44]。

2.2.2 BERT（Transformer 的双向编码器表示）

BERT 是自然语言处理（NLP）领域的一个革命性突破[45]。传统的 NLP 模型往往是基于单向的上下文理解，而 BERT 通过采用双向 Transformer 架构，能够同时考虑句子的前后文，从而更准确地理解句子中的语义信息。BERT 的双向性使得它能够在多个 NLP 任务中如情感分析、问答系统、命名实体识别等上超越了传统的模型。

BERT 的训练过程由预训练和微调两个阶段组成。在预训练阶段，BERT 采用了掩码语言模型（Masked Language Model, MLM）和下一个句子预测（Next Sentence Prediction, NSP）两种任务来学习语料库中的上下文信息。掩码语言模型通过随机掩盖输入句子中的某些词汇，要求模型根据上下文预测被掩盖的词汇，进一步提高语言模型的理解能力[45]。

在微调阶段, BERT 通过在特定任务上进行微调来适应实际应用。这使得 BERT 能够在许多 NLP 任务中达到最先进的性能，成为 NLP 领域的重要技术之一[46]。

2.2.3 图卷积网络（GCN）

图卷积网络（Graph Convolutional Networks, GCN）是深度学习在图数据上的一个应用，特别适用于社交网络分析、推荐系统、化学分子分析等任务[47]。GCN 的核心思想是通过卷积操作聚合节点的邻居信息，以此来更新节点的特征表示。

GCN 通过图结构数据进行计算，不同于传统的卷积神经网络（CNN），其输入数据是图数据而非网格数据（如图像）。GCN 的卷积操作并不直接作用于图像像素，而是通过邻接矩阵来传递节点之间的信息，从而捕捉图中节点间的结构信息[48]。

GCN 模型的一个典型应用是节点分类任务，例如在社交网络中预测用户的兴趣，或在分子结构中预测化学反应的性质。GCN 的另一重要特性是其在处理大规模图数据时的计算效率和可扩展性[49]。

第三章 区块链交易数据前处理的相关研究

在本章中，我们详细描述了一种用于区块链交易数据欺诈检测的动态多模态融合方法。所提出的方法整合了基于图的表示学习，以捕捉交易网络中的全局关系，同时利用语义特征提取来识别交易记录中的局部上下文模式。借助动态特征融合机制，该模型能够有效地结合结构和语义信息，从而增强检测复杂欺诈行为的能力，如图 3.1 所示。本章包括我们方法的详细步骤，首先介绍数据生成与预处理，然后对模型架构以及用于优化性能的训练过程进行全面解释。

在处理区块链交易数据集时，每条交易记录通常包含多个字段，如 `tag`、`from_address`（发送方地址）、`to_address`（接收方地址）、`value`（交易金额）和 `timestamp`（交易时间戳）。这些字段描述了交易行为、发生时间以及涉及的各方。为了更有效地分析和建模交易关系，我们需要对交易数据进行适当的分类和重新组织。

具体来说，我们根据发送方和接收方地址对所有交易数据进行分类，构建一个基于账户的交易记录结构。此分类步骤不仅简化了交易数据的存储和访问，同时也为后续图结构构建与局部语义分析奠定了基础。

每笔交易包含两个账户地址，即发送方（`from_address`）和接收方（`to_address`）。我们根据发送方地址（`from_address`）对交易进行分类，将其视为某一账户的交易记录。每笔交易被标记为“转出”交易，其字段 `in_out` 取值为 1。同样，当账户为接收方时，该交易被标记为“转入”交易，其字段 `in_out` 取值为 0。

分类后的交易记录存储在字典 `accounts` 中，键为账户地址，值为该账户所有交易记录的列表。与某个账户关联的列表包含该账户所有的转出和转入交易。通过按账户分离和索引交易记录，我们可以迅速检索任一账户的交易历史，尤其在分析账户行为模式或交易频率时十分有用。

3.1 时间聚合特征增强

为了提高交易数据在时间维度上的信息表达能力，我们在数据生成与预处理阶段特别关注交易的时间聚合特性。通过增强时间聚合特征，我们可以有效捕捉一些潜在的异常账户行为，特别是那些在短时间内进行大量资金交易的账户[50]。这些行为往往是钓鱼账户的典型特征，因此在准确检测欺诈活动时，对时间维度信息的分析和利用至关重要。

在处理每个账户的交易数据时，我们首先根据时间戳对交易记录进行排序。排序的目的是确保后续时间差的计算能反映交易的实际顺序，为时间聚合特征提供基础支持。通过按时间顺序排序交易，我们可以捕捉账户在特定时间段内的资金

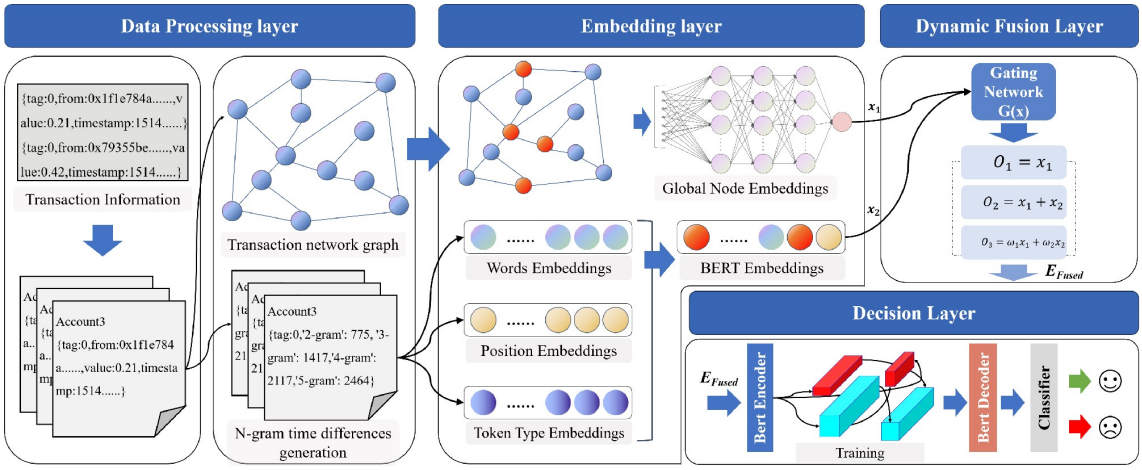

图 3.1　用于区块链钓鱼检测的动态特征融合模型架构

流动情况，并进一步分析其交易行为的频率和密度。

为了量化短时间内频繁交易的程度，我们引入了 n-gram 时间差特征。具体来说，n-gram 时间差通过计算某笔交易与前 $n-1$ 笔交易之间的时间差来衡量交易时间的紧密程度。我们计算了 2-gram 至 5-gram 的时间差，公式如下：

$$\Delta T_n = T_i - T_{i-(n-1)} \tag{3.1}$$

其中 t_i 表示第 i 笔交易的时间戳，$t_{i-(n-1)}$ 表示该账户中第 $i-(n-1)$ 笔交易的时间戳。如果交易数量不足以计算 n-gram，则该时间差设为 0。

n-gram 时间差特征使我们能够捕捉短时间内频繁交易的模式。例如，如果一个账户在几分钟内进行多笔转入和转出交易，则 n-gram 时间差将显著较小，这种时间聚合反映了账户在短时间内的高频交易行为，而这通常与钓鱼行为密切相关。

3.2 图数据生成

为了有效捕捉区块链交易数据中的账户间关系，我们首先构建了一个基于图的数据结构来表示交易网络。在本节中，我们使用邻接矩阵 $\mathbf{A}$ 来量化交易网络中各账户之间的连接权重。生成这种图表示的过程包括以下步骤：

3.2.1 创建零矩阵

我们首先创建一个 $n \times n$ 的零矩阵 $\mathbf{A}$，其中 n 表示唯一账户地址的数量。该邻接矩阵用于存储不同账户之间的连接权重。矩阵 $A[i, j]$ 的元素表示账户 i 与账户 j 之间的交易权重。

$$\mathbf{A} = \mathbf{0}_{n \times n} \tag{3.2}$$

3.2.2 遍历交易记录

为了填充邻接矩阵的各个元素，我们需要遍历所有交易记录 T_k，其中每笔交易 T_k 包含发送方 from_address_k 和接收方 to_address_k。我们使用“address_to_index”字典将这些账户地址映射到邻接矩阵中的索引。

- 发送方地址映射为 from_idx
- 接收方地址映射为 to_idx

公式表示如下：

$$\text{from\_idx} = \text{address\_to\_index}(\text{from\_address}_k) \tag{3.3}$$

$$\text{to\_idx} = \text{address\_to\_index}(\text{to\_address}_k) \tag{3.4}$$

3.2.3 计算交易权重

每笔交易 w_k 的权重反映了交易金额以及交易行为的时间特性。为了有效捕捉时序特征，我们提出了一种基于 n-gram 时间差的权重计算方法。具体来说，每笔交易 w_k 的权重被计算为 n-gram 时间差 (ΔT_n) 的加权和，计算公式如下：

$$w_k = \text{value}_k \times \left(\sum_{n=1}^{N} \alpha_n \cdot \Delta T_n \right) \tag{3.5}$$

其中：

- ΔT_n 表示前面定义的 n-gram 时间差，即 $\Delta T_n = T_i - T_{i-(n-1)}$，代表第 i 笔交易与第 $i-(n-1)$ 笔交易之间的时间间隔。
- α_n 表示对应于不同 n-gram 时间差的权重系数。在我们的实验中，我们经验地将这些权重设置为与 n-gram 阶数成反比，以强调短期内交易激增：

$$\alpha_n = \frac{1/n}{\sum_{j=1}^{N}(1/j)} \tag{3.6}$$

其中 N 是考虑的最大 n-gram（在我们的实验中，$N = 5$）。

此外，交易金额 value_k 也是权重的重要组成部分，我们将其与 n-gram 时间差结合，以进一步调整交易的权重：

$$w_k = \text{value}_k \cdot \left(\sum_{n=1}^{N} \alpha_n \cdot \Delta t_{n,k} \right) \tag{3.7}$$

3.2.4 填充邻接矩阵

一旦计算出每笔交易的权重 w_k，它们就被累加到邻接矩阵 $A[\text{from\_idx}, \text{to\_idx}]$ 的对应位置。具体来说，如果同一对账户之间存在多笔交易，则其权重被累加。该累加过程可以用以下数学公式表达：

$$A[\text{from\_idx}, \text{to\_idx}] = \sum_{k \in \mathcal{T}(from\_idx, to\_idx)} w_k \tag{3.8}$$

其中 $\mathcal{T}(from\_idx, to\_idx)$ 表示从账户 $from\_idx$ 到账户 to_idx 的所有交易集合。因此，邻接矩阵中的每个条目既反映了两账户之间交易的总频率，也反映了总交易金额。

该操作确保当两账户之间发生多笔交易时，相应的权重会累加到邻接矩阵中适当的位置。这一累加过程有效地反映了账户之间交易的频率和总交易金额。最终得到的邻接矩阵 $\mathbf{A}$ 作为图结构表示学习的输入，使得模型能够捕捉并分析交易网络中的全局结构关系。

在实际应用中，“address_to_index”字典的大小取决于所分析的区块链数据集规模，通常范围从数万到数百万个唯一账户地址，尤其是在处理如以太坊这样的大型区块链网络时。当新账户实时出现时，可以增量地为其分配新索引并将其添加到此字典中。因此，邻接矩阵需要通过扩展其维度来动态更新，以容纳这些新账户及其交易。然而，这种动态更新可能在计算效率上带来挑战，因为频繁调整大规模邻接矩阵的尺寸可能耗费大量资源。因此，所提出的方法在当前形式下主要针对离线或批量分析场景。对于实时钓鱼检测，则需要采用增量图更新、近似邻接结构或流式图技术等额外的优化策略。

3.3 文本交易数据生成

在每个账户的交易记录中，from_address、to_address 和 timestamp 字段记录了账户的地址信息和时间戳。虽然这些字段对于交易分类和时间特征增强非常重要，但在文本分析中并不需要，因此我们在生成文本数据之前删除这些字段，以简化数据结构并保留如交易 value 和标签等关键信息.

最近的研究表明，基于 Transformer 的模型，如 BERT，也可以从随机或任意顺序排列的序列训练中获益[51]。我们利用这一特性，通过随机重新排列每个账户的交易列表。这一操作打乱了交易的前后顺序，使模型能够聚焦于交易的内容特征而非时间依赖信息，从而避免可能的噪声干扰.

例如，账户 A 的交易列表在打乱前为 $[T_1, T_2, T_3]$，而在随机打乱后可能变为 $[T_2, T_1, T_3]$.

接下来，我们为每个账户打上总体标签。只要账户中存在标签为 1 的交易，该账户就被标记为欺诈，即整个账户的标签为 1。该标签被赋予该账户的第一条交易记录。为了简化交易日志，其余交易的标签信息被删除，仅保留第一条交易的标签。这是因为即使账户中只有一笔交易与欺诈相关，该账户本身也可能具有潜在风险，甚至可能被用于更大范围的欺诈活动。通常，网络钓鱼账户倾向于通过掩饰多笔正常交易来隐藏其恶意行为。因此，为了确保欺诈检测的安全性和有效性，我们采用了更严格的标准，确保模型能够识别出潜在的高风险账户，并防止它们参与进一步的非法交易。这种标注方法有助于模型更准确地学习账户的风险特征，

表 3.1　特征提取及 TSV 表示总结

字段	描述	示例值
tag	网络钓鱼标签 (1)/合法 (0)	1
value	转账交易金额	5.06854256
in_out	交易方向 (1: 出, 0: 入)	1
2-gram	当前与 t-1 之间的时间差 (秒)	30 (seconds)
3-gram	当前与 t-2 之间的时间差 (秒)	90 (seconds)
4-gram	当前与 t-3 之间的时间差 (秒)	120 (seconds)
5-gram	当前与 t-4 之间的时间差 (秒)	300 (seconds)
TSV 格式示例:		
`tag=1, value=5.0685, in_out=1, 2-gram=30, ...`		

并提高整体检测效果.

在生成文本数据时，我们处理每个账户的交易记录，并将其转换为一行描述性文本。每笔交易的关键字段（例如标签、交易金额等）被组合在一起，形成一个紧凑的文本表示，封装对应账户的交易信息。此步骤生成了原始文本语料库，作为后续通过预训练文本表示模型进行语义特征提取的输入. 该格式可以通过一个具体例子清楚地说明:

网络钓鱼账户示例: `tag=1, value=5.0685, in_out=1, 2-gram:30, 3-gram:60, 4-gram:90, 5-gram:120; value=3.7451, in_out=0, 2-gram:30, 3-gram:60, 4-gram:90, 5-gram:120;`

正常账户示例: `tag=0, value=0.0340, in_out=1, 2-gram:0, 3-gram:0, 4-gram:0, 5-gram:0;`

在这些例子中，最初的标签数字表示账户级标签（`1` 表示网络钓鱼，`0` 表示合法），而后续数据代表以随机排列顺序呈现的交易记录，每个账户实例可能包含多笔独立交易。这种简化的表示方式使模型能够从交易金额中学习语义模式，而不会过度拟合于时间顺序或位置特定偏差.

生成的文本交易数据集按照 80% 训练集、10% 验证集和 10% 测试集的比例进行划分。该数据划分确保模型在训练过程中能够学习足够的特征，并通过验证集进行性能调优，同时在测试集上验证模型的泛化能力.

3.4 提取特征及 TSV 表示总结

为了清晰地展示在实验中使用的最终交易表示中提取并包含的特征，我们在表 3.1 中提供了详细总结。最终 TSV 文件中的每一行对应一个区块链账户，其交易信息以文本描述形式拼接在一起.

这种明确的表示方式促进了基于 Transformer 方法的语义建模，因为交易被编码为同时反映其数值和时间属性的文本序列.

3.5 文本数据清洗

生成文本交易数据后，进一步的预处理步骤被应用以确保与下游语义表示模型所需输入格式的兼容。这些步骤包括读取生成的 TSV 文件、将文本分割为子词单元以及转换成适合基于深度学习训练的格式。

我们首先读取生成的 train.tsv 和 dev.tsv 文件，这些文件包含了处理后的训练集和验证集数据。为了确保模型在训练过程中接触到多样的数据分布，我们随机打乱数据顺序，以避免模型对特定数据顺序产生过拟合。此外，测试集数据从 test.tsv 中读取，并同样进行了随机打乱。

在读取并打乱数据后，训练集、验证集和测试集被合并为一个统一的数据框。从中提取出两个关键列：交易文本描述（corpus）和账户标签 (y)。交易文本描述捕捉了账户的交易行为，而标签则表明该账户是否涉及欺诈活动。此操作生成了后续语义特征提取和模型训练所需的输入语料及相应的监督信号（标签）。

文本语料随后使用 BERT 的 WordPiece 分词器被分割为子词单元。在这个分词过程中，令牌通过将所有字符转为小写并应用标准 Unicode 规范化 (NFKC) 进行归一化，遵循原始 BERT 预处理建议[30]。这一归一化过程确保了令牌表示的一致性，减少了词汇冗余并提高了模型效率。随后，分词后的序列被转换为令牌 ID，这些 ID 作为文本处理模型嵌入层的输入用于后续训练。为了确保鲁棒性，文档的顺序被有意打乱，使模型在训练过程中暴露于无序且多样化的输入。此外，标签数据 y 与分词后的句子对齐，并作为有监督学习过程中的监督信号。

随后进行了一个分词过程，将每个文档分割为一系列令牌（子词单元），这些令牌随后根据需要进行了归一化和编码。此步骤确保交易文本被转换为适合语义表示模型的格式，从而生成一系列令牌 ID。这些令牌 ID 作为文本处理模型嵌入层的输入用于后续训练。为了保证鲁棒性，文档顺序被有意打乱，使得模型在训练过程中接触到无序且多样化的输入。此外，标签数据 y 与分词后的句子对齐，并用作有监督学习过程中的监督信号。

上述步骤生成的数据集包含全局交易关系和局部交易语义信息，为后续模型训练提供了多模态输入。

第四章 ETH-GBERT 模型架构的研究

为了解决区块链交易中检测复杂欺诈活动的挑战，我们提出了 ETH-GBERT 模型，这是一种深度学习框架，旨在同时捕捉全局结构关系和局部语义相似性。虽然交易网络包含反映账户交互的丰富全局模式，但交易记录蕴含的局部上下文细节能够指示欺诈行为。现有方法往往只侧重于某一方面，未能发挥两者的互补优势。

在本研究中，我们采用图卷积网络（GCN）来捕捉嵌入在账户交互图中的全局交易关系。图卷积网络特别适合从基于图的数据中提取结构特征，因此非常适合对区块链交易网络中的关系进行建模。同时，我们使用预训练的 BERT 模型来分析交易文本数据中存在的局部语义特征，有效捕捉交易细节中的上下文含义和细微模式。

通过采用多模态融合机制整合这两个组件，ETH-GBERT 模型将全局结构特征与局部语义表示相结合，从而提升欺诈检测性能。以下各节对 ETH-GBERT 模型组件的架构和设计进行了详细说明。

4.1 模型架构

ETH-GBERT 模型集成了两个核心模块：一个针对交易账户图的 GCN 模块和一个针对文本交易数据的 BERT 模块。具体来说，我们使用以下架构配置:

- **BERT 组件:** 预训练的 BERT-base 模型，由 12 层 Transformer 编码器构成，隐藏层大小为 768，注意力头数量为 12。
- **GCN 组件:** 一个两层图卷积网络，每层的隐藏维度大小为 128。
- **门控网络:** 该架构采用一个两层多层感知机 (MLP)，隐藏维度为 128 并使用 ReLU 激活，能够自适应生成概率向量，以确定融合的多模态嵌入表示中各视角的相对贡献权重。

整体模型结构可分为以下部分:

i. **基于图的表示模块**: 主要捕捉交易网络中的全局关系。通过 GCN 层，对交易账户之间的关系进行卷积运算，从而生成包含全局语义信息的节点嵌入（账户嵌入）。

ii. **语义特征提取模块**: 从交易文本数据中提取局部语义信息。BERT 模型对每个账户的交易记录进行深层表示，并生成高维文本嵌入。

iii. **多模态融合**: 将 GCN 生成的全局账户嵌入和 BERT 生成的局部文本嵌入融合，形成一个多模态嵌入向量。该融合使模型能够同时利用交易网络结构和文本特征进行欺诈检测。

iv. **分类器**: 将融合后的嵌入向量传递至全连接层进行分类，输出预测结果以确

定账户是否与欺诈行为相关。

4.2 基于图的表示模块设计

邻接矩阵输入。GCN 模块的输入是交易账户图的邻接矩阵 $\mathbf{A}$，其中元素 $A[i, j]$ 表示账户 i 和账户 j 之间的交易权重。该邻接矩阵是从前述的图数据生成步骤中获得的，并结合了交易金额和时间特征。

图卷积层（GCN 层）。在 GCN 模块中[7]，交易账户图通过多层图卷积层进行特征提取。每层的卷积操作由下式表示：

$$\mathbf{H}^{(l+1)} = \sigma\left(\tilde{\mathbf{D}}^{-\frac{1}{2}}\tilde{\mathbf{A}}\tilde{\mathbf{D}}^{-\frac{1}{2}}\mathbf{H}^{(l)}\mathbf{W}^{(l)}\right) \tag{4.1}$$

其中：

- $\mathbf{H}^{(l)}$ 表示第 l 层的节点特征矩阵（即账户嵌入矩阵），初始 $\mathbf{H}^{(0)}$ 为交易账户的初始特征;
- $\tilde{\mathbf{A}} = \mathbf{A} + \mathbf{I}$ 为带自环的邻接矩阵;
- $\tilde{\mathbf{D}}$ 为邻接矩阵的度矩阵;
- $\mathbf{W}^{(l)}$ 为第 l 层的权重矩阵;
- σ 是非线性激活函数，例如 ReLU.

通过多次卷积操作，模型逐层聚合交易网络的全局信息，最终生成包含全局交易关系的节点嵌入。

4.3 语义特征提取模块设计

文本输入及初始嵌入. BERT 模块的输入为交易文本数据。经过清洗和分词处理后，文本数据被转换为令牌序列。这些令牌序列通过 BERT 的词嵌入、位置嵌入和标记类型嵌入层进行嵌入处理[30]：

$$\mathbf{E}_{\text{BERT}} = \mathbf{E}_{\text{word}} + \mathbf{E}_{\text{position}} + \mathbf{E}_{\text{token\_type}} \tag{4.2}$$

与图嵌入的融合. 在经过 Transformer 编码器处理之前，来自 BERT 的嵌入 $\mathbf{E}_{\text{BERT}}$ 被动态地与基于图的嵌入融合，以生成融合嵌入 $\mathbf{E}_{\text{Fused}}$。详细的融合机制及其自适应加权策略将在下一小节 (4.4) 中详细阐述.

BERT 编码层. 融合后的嵌入 $\mathbf{E}_{\text{Fused}}$ 随后被输入到 BERT 的多层 Transformer 编码器中，以生成更高级的表示。形式上，该编码步骤定义为：

$$\mathbf{H}_{\text{fusion}} = \text{TransformerEncoder}(\mathbf{E}_{\text{Fused}}) \tag{4.3}$$

生成的 $\mathbf{H}_{\text{fusion}}$ 作为最终分类模块的输入.

4.4 多模态融合

在模型的多模态融合阶段，我们引入了一种受 DynMM[52] 启发的**动态特征融合机制**，该机制自适应地确定每个输入实例中 BERT 与 GCN 嵌入的贡献比例.

融合策略. 我们的方法采用一个**门控网络** $G(x)$ 来生成针对实例的融合权重。这使得模型能够动态决定从现有嵌入中提取多少信息。具体而言，考虑了三种融合策略:

- **仅 BERT 嵌入** E_{BERT}: 仅使用文本信息进行预测.
- **GCN 增强的 BERT 嵌入** $E_{\text{GCN\_Enhanced}}$: 整合了结构化图信息并融合了 BERT 上下文特征的 GCN 嵌入.
- **BERT 与 GCN 嵌入的加权组合**:

$$E_{\text{Fusion}} = \alpha \cdot E_{\text{BERT}} + (1 - \alpha) \cdot E_{\text{GCN\_Enhanced}} \tag{4.4}$$

其中 α 是一个可学习参数，初始值设为 0.5.

动态权重计算. 门控网络 $G(x)$ 以拼接后的特征 $[\mathbf{E}_{\text{BERT}}, \mathbf{E}_{\text{GCN\_Enhanced}}]$ 作为输入，并输出对应于三种融合策略的融合权重 $g = [g_1, g_2, g_3]$:

$$g_i = \frac{\exp\left((\log G(x)_i + b_i)/\tau\right)}{\sum_{j=1}^{3} \exp\left((\log G(x)_j + b_j)/\tau\right)}, \quad i \in \{1, 2, 3\} \tag{4.5}$$

其中 $b_i \sim \text{Gumbel}(0, 1)$ 表示 Gumbel 噪声，τ 是控制输出概率分布陡峭度的温度参数。具体而言，当 τ 较大时，输出分布较平滑，趋近于均匀分布，从而使三种融合策略的权重更加平衡或相等。反之，当 τ 较小时，分布变得更陡峭，最终趋向于 one-hot 分布，明显偏向于单一融合策略。在实际操作中，我们调整 τ 以在探索（均衡融合）与利用（选择性融合）之间达到最佳平衡，从而增强我们动态融合机制的适应性.

为了处理不同任务复杂性和数据特征，门控网络 $G(x)$ 可采用不同的架构实现，例如多层感知机 (MLP)、Transformer 层或卷积网络.

在本工作中，我们将门控网络实现为 **多层感知机 (MLP)**，由两层全连接层组成，并采用 ReLU 激活函数.

最终融合的嵌入 E_{Fused} 计算公式为:

$$E_{\text{Fused}} = g_1 \cdot E_{\text{BERT}} + g_2 \cdot E_{\text{GCN\_Enhanced}} + g_3 \cdot E_{\text{Fusion}} \tag{4.6}$$

自适应融合机制. 这一动态融合机制使得模型能够根据输入复杂度自适应地调整计算资源及融合策略:

- 对于 **简单输入**，门控网络会为较简单的策略（如 E_{BERT} 或 $E_{\text{GCN\_Enhanced}}$）分配更高的权重，从而降低计算成本.

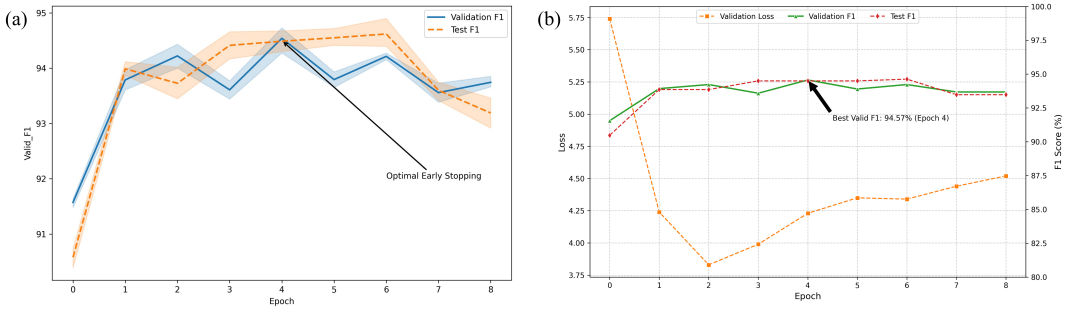

图 4.1　ETH-GBERT 训练动态（在第 4 个 epoch 采用早停）. (a) 训练损失曲线显示模型在 4 个 epoch 后收敛; (b) 验证集的 F1 分数曲线在第 4 个 epoch 达到峰值.

- 对于 **复杂输入**，门控网络会增加加权组合 E_{Fusion} 的贡献，使模型能够有效整合来自两种模态的信息.

虽然融合机制引入了额外的计算成本，但我们的实验表明训练时间仍然在可控范围内。例如，当禁用早停机制时，ETH-GBERT 模型每个 epoch 大约需要 19 分钟——40 个 epoch 总计 12.5 小时（754 分钟）。值得注意的是，如图 4.1 所示，模型在第 4 个 epoch 达到了最高的验证加权 F1 分数（94.565%），此后性能指标趋于稳定。鉴于显著高于基线方法的 F1 分数带来的巨大性能提升，这一计算成本是合理的，尤其在检测准确性至关重要的场景中.

在实际应用中，权重 g_1、g_2 和 g_3 会根据输入复杂度自适应调整。对于较为简单、语义集中的交易，模型可能分配如 $[0.8, 0.1, 0.1]$ 的权重，从而偏向于基于 BERT 的语义嵌入。相反，涉及多个账户的结构复杂交易可能会产生如 $[0.2, 0.3, 0.5]$ 的权重，更加侧重于混合嵌入 $\mathbf{E}_{\text{Fusion}}$.

尽管 $\mathbf{E}_{\text{Fusion}}$ 已经是动态加权的，但通过 g_1、g_2 和 g_3 所提供的额外门控机制，增加了更高层次的自适应决策层。这一额外的灵活性使模型能够在单一模态嵌入（BERT 或 GCN 增强）与混合嵌入之间动态选择，从而提高其对异构区块链数据的适应性。我们的实验结果证实，这种动态门控显著提高了模型的整体性能和灵活性.

第五章 实验与结果

在本实验中，我们选择了三类常用的基线模型进行对比：

1. 基于随机游走的图嵌入方法，包括 DeepWalk[53]、Trans2Vec[54]、Dif2Vec[55] 和 Role2Vec[56-57]；
2. 图神经网络 (GNN) 模型，包括 GCN[7]、GraphSAGE[58] 和 GAT[29]；
3. BERT4ETH，一种专门用于检测以太坊欺诈行为的模型[31]。

DeepWalk 通过在图上进行随机游走生成节点序列，并采用 skip-gram 模型来学习节点的低维表示。Trans2Vec 在 DeepWalk 的基础上融入了交易异质性和时间特征，专为检测以太坊网络中的钓鱼账户而设计。Dif2Vec 在随机游走过程中调整节点的采样概率，通过增加低度节点的采样来增强嵌入表示的多样性。Role2Vec 则侧重于学习节点的结构角色，而不仅仅关注邻近关系，从而生成更具泛化能力的嵌入表示。

对于基于 GNN 的模型，GCN 通过卷积操作聚合邻居节点的特征来学习节点表示，使其适用于节点分类等任务。GraphSAGE 通过对邻居节点进行采样和特征聚合生成新的节点嵌入，从而使其能够处理大规模图数据。GAT 则引入了注意力机制，对每个节点的邻居动态分配权重，从而更有效地聚合节点信息。

BERT4ETH 专门用于检测以太坊网络中的欺诈活动，利用 BERT 以及以太坊网络中的交易数据特征来识别区块链交易中的欺诈行为。

在我们的实验中，所有基线模型，包括 BERT4ETH、DeepWalk、Trans2Vec、Dif2Vec、Role2Vec、GCN、GraphSAGE 和 GAT，均按照各自论文中规定的原始配置实现，从而确保了不同模型之间性能比较的公平性。

5.1 预处理与训练设置

在本节中，我们详细描述了 ETH-GBERT 模型的预处理配置、初始参数、损失函数及实验中使用的评价指标。

5.1.1 数据预处理

在训练之前，数据集被划分为训练集、验证集和测试集，分别占总数据的 80%、10% 和 10%。我们使用 PyTorch 的 `DataLoader` 以小批量方式加载数据，并在训练过程中对数据进行随机打乱。训练集用于更新模型参数，验证集用于评估模型的泛化能力，测试集则用于最终的性能评估。为了保证模型在不同数据分布下的鲁棒性，我们对数据进行了标准化处理，确保每个特征的均值为 0，方差为 1，避免了不同特征之间的量纲差异对模型训练的影响。

5.1.2 特征构建

在数据处理过程中，除了提取常规的交易数据特征外，还包括了交易时间差、交易频次等与时间相关的特征。这些特征能够帮助模型识别交易行为的时序规律，进一步提升对欺诈行为的敏感性。此外，我们还构建了基于区块链交易网络的邻接矩阵，帮助模型捕捉账户之间的交互关系，为图神经网络（GNN）提供了丰富的结构信息。

5.2 超参数设置

在模型训练过程中，我们对以下超参数进行了调节，并采用了最优配置进行实验：

- **学习率**: 初始学习率设置为 8×10^{-6}，并采用学习率调度器动态调整学习率。通过实验验证，我们发现这种调整策略能够有效避免训练过程中因学习率过大导致的梯度爆炸问题，同时提高了收敛速度。
- **正则化系数**: 为了防止过拟合，我们采用了 L2 正则化，系数设为 $\lambda = 0.001$。正则化项有助于惩罚过于复杂的模型，从而提高模型的泛化能力。
- **批量大小与梯度累积**: 批量大小设置为 32。由于训练数据较大，我们采用梯度累积，每 2 个小批量更新一次模型参数，以节省内存。这种策略使得模型能够在有限的内存条件下处理大规模数据。
- **Epoch 数**: 我们将最大 Epoch 数设置为 40。根据已有工作[28]，类似任务的模型通常在 30 到 50 个 Epoch 内可以收敛，40 个 Epoch 既能保证训练的充分性，又能避免过拟合现象。

5.3 损失函数与优化器

为了确保分类任务的有效性，我们采用了交叉熵损失函数进行训练。交叉熵损失函数通常用于二分类问题，在处理不平衡数据集时，能够有效优化分类模型的性能。损失函数的定义如下：

$$\mathcal{L} = -\frac{1}{N} \sum_{i=1}^{N} \left(y_i \log(p_i) + (1 - y_i) \log(1 - p_i) \right) \tag{5.1}$$

其中 N 为批量大小，y_i 为真实标签，p_i 为预测概率。

优化器采用 AdamW，AdamW 是基于 Adam 的优化器，结合了自适应学习率和通过权重衰减实现的 L2 正则化。AdamW 的更新规则如下：

$$\theta_{t+1} = \theta_t - \eta \cdot \frac{m_t}{\sqrt{v_t} + \epsilon} \tag{5.2}$$

其中 m_t 和 v_t 分别为梯度的一阶和二阶矩，ϵ 为避免除零的小常数。

5.4 评价指标

为了全面评估模型性能，我们采用精确度、召回率和 F1 分数等多种指标。在每个 Epoch 结束时，模型在验证集上的性能通过以下指标进行评估：

- **精确度**:

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

- **召回率**:

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

- **F1 分数**:

$$\text{F1 Score} = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{\text{Precision} + \text{Recall}}$$

其中，TP、TN、FP 和 FN 分别代表真正例、真反例、假正例和假反例的数量。通过这些评价指标，我们可以全面了解模型在欺诈检测任务中的分类效果，确保模型在不同数据集和场景下的表现。

表 5.1　ETH-GBERT 与各基线模型在不同数据集上的性能对比

模型	多图			交易网络			B4E		
	F1 分数	召回率	精确度	F1 分数	召回率	精确度	F1 分数	召回率	精确度
BERT4ETH	67.11	61.25	74.21	64.21	62.17	66.39	64.26	63.58	64.95
DeepWalk	58.44	58.21	58.67	59.21	58.31	60.14	54.51	55.38	53.67
Trans2Vec	52.13	51.36	52.92	54.28	56.26	52.43	55.31	54.96	55.66
Dif2Vec	65.27	64.21	66.37	62.11	62.54	61.69	63.25	63.54	62.96
Role2Vec	74.13	74.52	73.74	71.39	71.58	71.20	74.25	74.25	74.25
GCN	42.29	74.07	29.59	41.12	73.37	28.56	64.71	72.68	58.31
GSAGE	35.47	34.77	36.20	33.79	32.99	34.64	53.28	60.47	47.62
GAT	39.98	79.82	26.67	41.61	77.56	28.43	61.50	85.20	48.12
ETH-GBERT	**94.71**	**94.71**	**94.71**	**86.16**	**87.82**	**84.56**	**89.79**	**89.57**	**90.84**

5.5 性能表现

为了评估我们提出的 ETH-GBERT 模型在检测区块链交易数据中欺诈行为的有效性，我们将其性能与若干基线模型进行了比较，这些模型包括 BERT4ETH、DeepWalk、Trans2Vec、Dif2Vec、Role2Vec、GCN、GSAGE 和 GAT。这些模型分别应用于三个不同的数据集：多图、交易网络和 B4E。比较主要侧重于 F1 分数、召回率和精确度等关键指标，如表 5.1 所示。

5.6 模型性能概述

从实验结果可以看出，ETH-GBERT 在 F1 分数、召回率和精确度方面均明显优于所有基线模型。

- **在多图数据集上**，ETH-GBERT 达到了 94.71 的 F1 分数，比 GAT（84.35）高出约 10 分。这表明 ETH-GBERT 能够有效地结合图结构和语义信息，从而实现卓越的欺诈检测性能.

- **在交易网络数据集上**，ETH-GBERT 的 F1 分数为 86.16，召回率为 87.82，精确度为 84.56。与 GAT（F1 分数为 83.27）和 GCN（F1 分数为 83.29）相比，ETH-GBERT 在捕捉交易关系复杂性方面展现了更高的准确性.
- **在 B4E 数据集上**，ETH-GBERT 达到了 89.79 的 F1 分数，超越了所有基线模型。特别是其召回率高达 89.57，突显了模型在识别潜在欺诈案例方面的敏感性.

5.7 与基线模型的比较

从与基线模型的比较中可以得出以下几个关键见解：

1. **BERT4ETH**: 虽然 BERT4ETH 在提取局部语义信息方面表现尚可，但其在多图和交易网络数据集上的 F1 分数（分别为 67.11 和 64.21）明显低于 ETH-GBERT，这突显了引入全局结构信息的重要性，而 BERT4ETH 缺乏这一特性.
2. **GCN 与 GSAGE**: GCN 和 GSAGE 难以获得具有竞争力的 F1 分数, 其中 GCN 在多图数据集上仅得 42.29，在交易网络数据集上仅得 41.12。这些模型虽然在捕捉全局交易关系方面表现不错，但缺乏整合局部语义信息的能力，限制了其在欺诈检测任务中的表现.
3. **GAT**: GAT 模型受益于其自注意力机制，在召回率方面较为突出（如在多图数据集上达到 79.82）。但其 F1 分数依然较低（多图为 39.98，交易网络为 41.61），这归因于其在建模文本特征和复杂欺诈模式时的局限性.
4. **ETH-GBERT**: 我们提出的 ETH-GBERT 模型在所有数据集上均显著优于各基线模型。在多图、交易网络和 B4E 数据集上，其 F1 分数分别达到了 94.71、86.16 和 89.79。这一性能表现证明了 ETH-GBERT 能够动态融合全局交易网络信息与交易文本局部语义特征，从而实现卓越的欺诈检测能力.

表 5.2　通过多模态动态融合的性能提升分析

模型	**多图**			**交易网络**			**B4E**		
	F1 分数	**召回率**	**精确度**	**F1 分数**	**召回率**	**精确度**	**F1 分数**	**召回率**	**精确度**
仅 BERT	90.10	90.07	90.15	80.87	78.12	83.82	85.19	83.05	87.44
差异 (%)	*-4.61*	*-4.64*	*-4.56*	*-5.29*	*-9.70*	*-0.74*	*-4.6*	*-6.52*	*-3.40*
仅 GCN	42.29	74.07	29.59	41.12	73.37	28.56	64.71	72.68	58.31
差异 (%)	*-52.42*	*-20.64*	*-65.12*	*-45.04*	*-14.45*	*-56.00*	*-25.08*	*-16.89*	*-32.53*
简单组合	84.55	84.15	86.29	83.27	83.75	83.55	85.35	88.16	82.71
差异 (%)	*-10.16*	*-10.56*	*-8.42*	*-2.89*	*-4.07*	*-1.01*	*-4.44*	*-1.41*	*-8.13*
加权组合	92.43	92.51	92.47	85.21	83.75	**86.73**	88.23	86.34	90.20
差异 (%)	*-2.28*	*-2.20*	*-2.24*	*-0.95*	*-4.07*	*+2.17*	*-1.56*	*-3.23*	*-0.64*
ETH_GBERT	**94.71**	**94.71**	**94.71**	**86.16**	**87.82**	**84.56**	**89.79**	**89.57**	**90.84**

表 5.3　不同正常与欺诈比例下的性能表现

比例	多图			交易网络			B4E		
	F1 分数	召回率	精确度	F1 分数	召回率	精确度	F1 分数	召回率	精确度
1:9	78.50	80.10	77.90	75.20	76.90	74.50	70.30	72.20	69.80
2:8	81.30	82.40	80.20	77.80	79.50	76.70	73.10	74.80	72.90
3:7	83.70	84.50	82.90	80.30	81.80	79.90	75.40	77.20	74.60
4:6	87.50	88.20	86.70	84.10	85.40	83.82	79.10	80.70	78.90
5:5	**94.71**	**94.71**	**94.71**	**86.16**	**87.82**	**84.56**	**89.79**	**89.57**	**90.84**
6:4	89.30	90.20	88.70	83.80	85.10	82.90	81.18	82.60	79.80
7:3	85.60	86.50	84.80	80.90	82.30	79.10	77.20	78.80	76.50
8:2	82.30	83.40	81.60	77.60	79.10	76.40	73.90	75.50	73.20
9:1	80.10	81.20	79.30	75.40	76.83	74.60	71.30	72.80	70.50

5.8 多模态动态融合下的性能提升分析

表 5.2 展示了多模态动态融合带来的性能提升，比较了**单模态模型**、**静态融合方法**和**动态融合**的不同表现。以下是对各方法的深入分析：

- **单模态模型：** 仅使用 BERT 的模型在语言特征建模方面展现出强大的能力，特别是在多图数据集上，取得了较高的 F1 分数（90.10）。BERT 作为一种强大的预训练语言模型，能够捕捉到丰富的上下文信息和语言模式，因此在纯文本任务中有显著优势。然而，在图数据集（如交易网络和 B4E 数据集）上，BERT 的表现较差（F1 分数分别为 80.87 和 85.19），这表明其在处理图结构数据时存在局限性。这种局限性主要源自 BERT 缺乏对节点间复杂关系的建模能力，图数据中的节点关系和结构信息无法充分融入 BERT 的学习过程中。BERT 模型的优劣表明，单一模型无法同时处理语言特征和图结构特征，这为后续的融合方法奠定了理论基础。相比之下，GCN（图卷积网络）模型通过聚合邻居节点的信息，在图数据集上展现了较好的性能，尤其是在图结构特征的建模上表现出色。然而，GCN 在处理纯文本任务时显得力不从心，因为它无法有效地捕捉文本中的语言特征。因此，单模态模型的表现局限于各自的优势领域，无法实现跨领域的良好表现。GCN 模型的表现进一步证明了单一数据源的模型在处理跨领域任务时的局限性，突显了多模态融合的必要性。
- **静态融合方法：** 静态融合方法将 BERT 与 GCN 结合，以期同时利用图结构信息与文本语义特征。这种方法为融合模型的初步探索，尽管在某些数据集上有所提升，但由于固定的融合机制，其融合过程未能充分发挥两者优势。静态融合的主要问题在于没有动态权重调整能力，导致在不同任务中，BERT 和 GCN 的贡献未能得到有效平衡。例如，静态融合方法在多图数据集上的 F1 分数为 84.55，而 BERT 仅为 90.10，这反映了静态融合无法应对复杂数据模式的局限性。静态融合方法也表明，基于固定模型结构的融合在面对动态变化的任务时，可能无法有效捕捉各部分特征的重要性差异，导致整体性能

的提升受限。静态融合方法的另一问题在于，在某些特定任务中，由于 BERT 和 GCN 在信息融合时的冲突，静态融合甚至未能超越单模态模型的表现。例如，在交易网络数据集上的性能提升就十分有限，F1 分数仅为 83.27，较为平庸。静态融合的方法未能通过动态调整来弥补图结构特征和文本特征在不同任务中的优势差异，导致其在特定场景下未能实现理想的效果。

- **动态融合（ETH-GBERT）：**ETH-GBERT 模型通过动态融合 BERT 与 GCN，表现出了跨数据集的卓越性能。动态融合机制使得模型能够在每一层的计算过程中根据任务需求动态调整 BERT 与 GCN 的贡献比例，从而能够根据图结构特征与文本特征的复杂性调整其学习策略。这一优势在多图数据集上得到了充分体现，F1 分数达到 94.71，较静态融合提升了 2.28 分，显示了动态融合方法在处理多模态信息时的适应性和灵活性。通过动态调整模型的学习策略，ETH-GBERT 能够在不同任务中灵活地整合各类特征，从而提升模型的性能。在交易网络和 B4E 数据集上，ETH-GBERT 也展现了明显的优势，尤其在 B4E 数据集上，F1 分数为 89.79，较静态融合提升了 1.56 分，突显了该方法在复杂欺诈行为模式检测中的应用潜力。动态融合使模型能够处理更多维度的特征，动态地平衡图结构信息和文本信息，使得 ETH-GBERT 不仅能从语言中提取有价值的信息，还能通过图结构提供有力的补充，最终提升了模型的总体性能。ETH-GBERT 的表现证明了在多模态学习中，如何通过动态调整和融合不同来源的信息，可以显著提升模型在各种任务中的效果。

这些结果进一步验证了单模态模型和静态融合方法的局限性，尤其是在面对复杂多模态数据时，单一模型的表现常常无法全面捕捉所有特征。而 ETH-GBERT 通过动态融合，能够更加精准地调配各个特征的贡献，在不同的数据集上展现了明显的性能优势。这一发现也表明，未来的多模态学习方法可以借鉴这种动态融合机制，以在更多复杂任务中取得优异的表现。动态融合在多模态学习中的应用前景广阔，尤其是在图像、文本、语音等多个领域都具有较强的适应性。

5.9 正常与欺诈比例对模型性能的影响

在本小节中，我们评估了数据集中正常交易与欺诈交易比例的变化如何影响 ETH-GBERT 模型在三个不同数据集（多图、交易网络和 B4E）上的性能。通过这种评估，我们能够更好地理解数据不平衡对模型性能的具体影响，并为未来的应用提供指导。

我们在不同正常与欺诈交易比例下（从 1:9 到 9:1）训练了 ETH-GBERT 模型，并对每个数据集的性能进行了跟踪，评估了关键评价指标——F1 分数、召回率和精确度。实验结果表明，数据集的正常与欺诈比例对模型的学习效果产生了显著影响。

- **平衡数据集 (5:5 比例):** 在数据集正常与欺诈交易比例平衡时，ETH-GBERT 模型的性能最佳。此时，模型不仅能够均衡地学习正常交易与欺诈交易的特征，还能更有效地捕捉两者之间的细微差异。特别是在 **多图**数据集上，模型的 F1 分数达到了 94.71，远超其他比例下的表现。这种平衡数据集的训练有助于避免模型在过拟合某一类别数据上的问题，从而提升了整体分类性能。平衡数据集提供了一个较为理想的训练环境，有助于模型从数据中学习到最有价值的特征，从而提高了检测的准确性。
- **不平衡数据集:** 随着数据集正常与欺诈交易比例的逐渐不平衡，模型的性能有所下降，特别是在正常交易占比过高的情况下。例如，当比例为 9:1 时，F1 分数降至 80.10，这表明模型在面对大量正常交易时，可能忽略了对欺诈行为的有效学习。这种情况在交易网络和 B4E 数据集中尤为明显，F1 分数下降较为显著，特别是在 B4E 数据集（F1 分数为 71.30）中，性能的下降幅度更为明显。数据不平衡导致模型在训练时对少数类别的学习不充分，容易使得欺诈行为的特征被忽略或低估。
- **复杂数据集的影响:** 在 **B4E** 数据集上，由于正常与欺诈交易之间的交互较为复杂，模型对于细微特征的识别显得尤为重要。当数据比例严重失衡时，模型的学习策略可能会被偏向正常交易数据, 导致其对欺诈交易的敏感度下降。这一问题在 B4E 数据集中表现得尤为突出，在比例为 9:1 时，F1 分数降至 70.50，表现出了模型在复杂模式中的适应性问题。复杂的数据交互增加了数据的不确定性, 模型需要更加精准的训练策略来识别欺诈行为中的微小差异。

尽管在不平衡数据集上，ETH-GBERT 模型的表现有所下降，但其鲁棒性依旧较强。模型能够在不平衡数据上训练时，依靠其多模态动态融合的机制，依然能够捕捉到大部分的欺诈行为特征，尤其是在数据集中的欺诈交易较为稀少的情况下，模型能够较好地处理较少的欺诈样本。ETH-GBERT 的设计能够有效应对数据不平衡带来的挑战，展现了其强大的适应性。

这些结果表明，虽然数据不平衡会影响模型性能，ETH-GBERT 仍展现出强大的适应性和鲁棒性。对于实际应用中的欺诈检测任务，保持数据集的平衡或使用相关策略进行数据采样，能有效提升模型的准确性和召回率。此外，在实际应用中，针对数据不平衡问题采取合适的采样策略（如过采样、欠采样或生成对抗网络）可以进一步提升模型的性能。

5.10 实验结果讨论

在本章中，我们进一步分析实验结果，以深入了解不同数据集和融合策略下性能变化的原因，并探讨模型表现的差异性。

- **多图数据集:** 在**多图数据集**上，仅使用 BERT 的模型表现非常出色，F1 分数

高达 90.10。BERT 能够通过预训练学习到大量语言模式和上下文信息，使其在处理交易文本时能有效捕捉到其中的欺诈行为模式。交易文本中的语义信息在多图数据集中可能是较为重要的线索，特别是在文本数据能够提供明确的欺诈信号时。ETH-GBERT（F1 = 94.71）与 BERT 模型相比，性能有所提升，表明 ETH-GBERT 能够更好地结合图结构信息，提升钓鱼检测能力。ETH-GBERT 不仅利用了交易文本的语义特征，还通过图卷积网络（GCN）处理了交易数据中的结构关系。尽管仅使用 BERT 时文本特征的表达力强，但图结构信息的缺乏使得模型在处理更复杂的交易模式时可能表现不足。然而，当我们进一步深入分析**交易网络数据集**时，我们发现仅使用 BERT 的模型表现显著下降，F1 分数降至 80.87，这与多图数据集上的表现形成鲜明对比。交易网络数据集的复杂性主要体现在交易间的关系结构上，BERT 无法有效处理图结构中的关系信息。因此，文本特征单独使用时，未能充分表达数据中的复杂关系模式。相比之下，ETH-GBERT 通过动态融合 BERT 和 GCN 的优点，提升了模型在捕捉交易模式、节点关系及语义信息方面的能力，在该数据集上实现了 F1 分数 86.16 的提升。这一差距突显了图结构信息在复杂交易模式识别中的重要性，进一步证明了 ETH-GBERT 在多模态融合中的优势。

- **融合策略的比较:** 关于融合策略，简单组合方法在**多图数据集**上表现较为有限，F1 分数为 84.55，远低于 ETH-GBERT（F1 = 94.71）。这种性能差距表明，简单组合方法并未充分利用两种模态之间的互补优势，尤其是在多图数据集中。多图数据集可能需要更复杂的动态加权机制，以根据任务的需求动态调整文本特征和图结构特征的贡献比例。简单组合方法的固定权重无法灵活应对不同任务中的需求，导致其无法发挥最大潜力。相比之下，ETH-GBERT 通过动态融合机制，有效地调整了文本与图结构信息之间的权重，从而显著提升了性能。在**交易网络和 B4E 数据集**上，简单及加权组合方法（F1 分数约为 83-86）与 ETH-GBERT（分别为 86.16 和 89.79）的性能差距相对较小。尤其是在交易网络和 B4E 数据集上，图结构的作用更加显著，而文本信息则提供了补充。因此，在这些数据集中，简单组合方法和加权组合方法能够捕捉到部分有效的信息，且性能提升较为有限。这些发现表明，动态融合带来的增量性能提升在那些具有明显模态优势或结构与语义异质性较高的数据集中尤为明显。而在这些数据集中的某些情况下，简单的组合方法也能带来一定的性能提升，尤其是在图特征对整体任务贡献较大的情况下。
- **多模态融合的重要性:** 从这些实验结果可以得出结论，ETH-GBERT 的动态融合策略相较于简单的组合方法和加权组合方法，在不同数据集中的性能差异尤为显著。尤其在多图数据集上，动态融合的优势更为突出，这表明多模态融合不仅仅是将不同类型的信息拼接在一起，而是需要根据任务的特点动态

调整不同信息源的权重。特别是在处理具有强结构特征和复杂语义信息的数据集时，动态融合方法能够更好地应对不同模态之间的异质性，充分挖掘每种模态的潜力。此外，简单的融合方法，虽然在某些数据集上表现不如动态融合，但在一些结构相对简单且语义信息主导的任务中，可能依然能够带来一定的性能提升。比如，在交易网络数据集中的加权组合方法，与 ETH-GBERT 相比虽然存在性能差距，但通过静态的权重调整，模型仍然能够利用不同模态的信息进行一定的优化。这进一步强调了针对不同数据集设计合适的融合策略的重要性。

综上所述，本实验展示了在多模态学习任务中，如何通过精心设计的动态融合机制来提升模型的性能，尤其是在涉及复杂数据集时。虽然简单的融合方法在某些特定情形下也能提供有益的性能提升，但动态融合显然更适合处理那些包含异质性特征的复杂任务。未来的工作可以进一步探索如何在更广泛的应用场景中推广这种动态融合的思路，尤其是在需要处理更加多样化和复杂的多模态数据时。

5.11 局限性与未来研究方向

虽然所提出的 ETH-GBERT 模型在区块链交易数据中的钓鱼检测上取得了显著提升，但仍需明确以下局限性，并为未来的研究指明可能的发展方向：

- **对其他欺诈类型的泛化：** 当前的 ETH-GBERT 模型主要聚焦于钓鱼检测，针对的是特定类型的欺诈行为。钓鱼行为通常依赖于假冒交易、虚假地址和账户控制等特征，而这类特征可能在其他类型的区块链欺诈中并不完全适用。例如，庞氏骗局（Ponzi Scheme）和洗钱行为通常表现为资金流转的复杂性、用户之间的隐蔽互动和资金转移的异常模式，而这些行为更难通过简单的交易文本或单一的图结构来捕捉。因此，当前方法的泛化能力在应对不同类型的欺诈行为时存在一定局限。未来的研究可以探索如何根据不同欺诈类型的特征，设计特定的特征提取机制或模型架构，使得 ETH-GBERT 能够在不同类型的欺诈行为检测中发挥作用。尤其是，对于洗钱或勒索支付等行为，可能需要在现有框架中集成更多的业务层面的规则和模式识别方法，而非单纯依赖图和文本数据。进一步的工作可以通过扩展数据集，涵盖更多的区块链欺诈类型，来测试模型的泛化能力。例如，开发一种联合模型，可以在同一个框架内同时检测多种欺诈类型，而不仅仅局限于单一的钓鱼攻击。这一方向的研究将为区块链安全领域提供更全面的解决方案，帮助识别复杂的跨链欺诈活动。
- **实时检测与离线分析：** 目前，ETH-GBERT 模型主要面向离线或批量分析场景，这一模型的计算复杂性较高，尤其是在多模态嵌入融合及邻接矩阵构建过程中。该模型的训练和推理过程需要处理大量的图数据和文本数据，因此

在大规模区块链交易数据的离线分析中表现出色。然而，在实际应用中，区块链交易的实时性要求非常高，实时检测对于欺诈行为的识别至关重要，尤其是在金融应用和反洗钱等场景中。将 ETH-GBERT 模型应用于实时检测时，可能面临增量图更新和实时嵌入推断的巨大挑战。随着区块链交易量的不断增加，实时处理需求变得更加迫切。为了解决这个问题，未来的研究可以探索增量学习方法，允许模型在新交易数据到达时实时更新而无需重新训练整个模型。这种增量学习可以使得模型在不断增长的交易数据中有效地跟踪变化，同时减轻计算负担。此外，实时嵌入推断技术的研究也至关重要，可以通过高效的图卷积网络（GCN）推理算法来加速实时数据处理过程，从而确保模型能够在实时监控场景中得到有效应用。对于增量图更新和嵌入推断，未来的研究可以重点关注如何在保证检测精确度的同时，减少计算和存储资源的消耗，提升系统的实时性和可扩展性。

- **跨链数据融合与多链分析：**目前的模型主要聚焦于单一区块链的欺诈检测。然而，随着去中心化金融（DeFi）和跨链协议的普及，越来越多的区块链和加密资产跨链互通，数据的跨链流动使得单一链的数据不再能够完全反映整个欺诈行为的全貌。在这种背景下，ETH-GBERT 模型可能需要扩展为跨链数据融合模型，能够处理来自多个区块链的交易数据。这一研究方向可以探索如何通过多链数据融合，识别跨链洗钱、跨链诈骗等复杂的欺诈行为模式。在跨链分析中，数据源的异质性和链间的通信方式也会成为研究的重点。如何在多链环境下进行有效的信息融合，确保不同区块链的交易数据能够在一个统一的模型中进行处理，是未来研究的重要方向。这将需要进一步探索区块链间的协议转换、数据对齐以及跨链欺诈行为模式的识别。
- **模型解释性与可解释性：**尽管 ETH-GBERT 在性能上取得了显著提升，但其作为深度学习模型的“黑箱”特性使得其在实际应用中的可解释性存在挑战。在金融领域和安全领域，尤其需要确保模型的决策过程可以被追溯和理解，特别是在处理涉及法律、监管或用户资金安全的欺诈案件时。未来的研究可以结合可解释性人工智能（XAI）方法，探索如何使得 ETH-GBERT 模型在输出欺诈判断时，能够提供清晰的解释，帮助分析人员理解模型为何判断某个交易或账户为欺诈行为。这不仅有助于提升模型的透明度，也能够增加系统的可信度，尤其是在实际应用中，提供可信的证据支持对欺诈行为的识别和处罚。通过引入如 SHAP、LIME 等可解释性方法，未来的 ETH-GBERT 研究可以在不牺牲模型性能的前提下，增强模型的可解释性，以适应更复杂的实际环境。

综上所述，虽然 ETH-GBERT 在钓鱼检测方面表现出色，但仍有许多挑战需要克服。未来的研究可以在扩展模型应用范围、提高实时检测能力、增强模型解释

性等方面取得更大进展。随着区块链技术的发展，如何在更复杂的欺诈场景中应用多模态学习方法，如何提高模型的实时响应能力，如何提升跨链数据分析能力，将是未来研究的核心课题。

第六章 结论

本文提出了一种新颖的动态多模态融合模型（ETH-GBERT），用于区块链交易中的欺诈检测。该模型通过自适应地整合来自交易网络的全局结构特征和交易文本中的局部语义信息，有效解决了现有方法的局限，实现了计算效率与表示学习能力之间的更好平衡。ETH-GBERT 模型不仅在结构特征和语义特征的结合上进行了创新，还通过动态调整两者的贡献，提升了模型在复杂场景中的性能。

本文的研究工作具有重要的理论和实际意义，尤其是在区块链安全和欺诈检测领域。区块链技术作为去中心化金融（DeFi）和加密货币的重要支柱，伴随而来的却是大量的欺诈行为，传统的欺诈检测方法难以应对区块链特有的交易复杂性和多样性。因此，本文提出的 ETH-GBERT 模型不仅提供了一种新的欺诈检测思路，而且为解决区块链数据中的多模态信息融合问题提供了一个有效的解决方案。

为支持所提出的模型，我们开发了一套完善的数据处理管道，包括用于捕捉账户间关系的图构建和利用 n-gram 时间差提取时间特征。该管道使模型能够同时分析交易数据中所蕴含的全局结构模式和局部上下文信息。在实际应用中，这种双重特征分析能力对于提升区块链欺诈检测的准确性和效率具有至关重要的作用，尤其是在处理复杂的交易模式时，能够捕捉到更多细微的异常行为。

此外，本文引入的动态融合机制根据交易背景自适应调整结构和语义特征的贡献，从而提升了模型在检测复杂欺诈活动时的准确性和鲁棒性。这一机制的创新在于其能够根据任务和数据的变化灵活地调整特征的加权，使得模型能够更好地适应不同的欺诈检测场景。通过这种自适应的融合方式，ETH-GBERT 能够在动态变化的区块链环境中持续保持高效的检测性能。

通过在大规模区块链数据集上进行的广泛实验，我们的模型在多个评估场景中均显著优于现有基准方法，实现了最高的 F1 分数，验证了所提出方法的有效性。实验结果表明，ETH-GBERT 不仅能在传统钓鱼检测中取得良好表现，还能够在更复杂的欺诈行为（如跨链欺诈、洗钱等）中提供有效的检测支持，证明了该模型的广泛适用性和强大性能。

本研究的主要贡献如下：

- **提出了一种动态多模态融合框架**，通过自适应整合结构与语义信息，提升了区块链欺诈检测能力。该框架解决了传统方法在处理多模态数据时的融合困难，并能够根据数据的不同背景动态调整各特征的贡献。
- **开发了一套稳健且高效的数据处理管道**，同时捕捉全局交易关系与时间行为模式。通过图构建和时间特征提取，本文提供了一种多维度、多角度的分析方法，极大地增强了模型的泛化能力和性能。
- **引入了动态特征融合机制**，自适应平衡各特征的贡献，提高了在不同情境下

的检测精度与效率。该机制能够在不同数据集和欺诈行为场景下，灵活调整各特征的权重，从而进一步提升模型的适应性和鲁棒性。

- **通过实验验证了所提出方法的有效性**，其在多个真实世界数据集上显著超越了最先进的模型。实验结果表明，ETH-GBERT 在处理复杂欺诈行为检测时，尤其是在多模态数据融合上表现出色，并在精度、召回率及 F1 分数等多个指标上取得了显著提升。

尽管 ETH-GBERT 模型在多个场景中表现优异，但仍然存在一定的局限性。例如，模型在处理实时交易数据时的计算效率仍有待提高，且模型的泛化能力在应对其他类型欺诈（如跨链欺诈）时需要进一步验证。此外，ETH-GBERT 的动态融合机制虽然在大多数测试中表现出色，但在极端数据情况下仍然可能出现性能波动，因此，未来的研究可以考虑进一步优化这一机制，使其在更多复杂情境下保持稳定的性能。

未来的研究可以进一步探索以下几个方向：

- **扩展模型的应用范围**，将 ETH-GBERT 模型应用于不同类型的区块链欺诈检测中，尤其是针对其他复杂的欺诈行为（如庞氏骗局、洗钱等），提高模型的泛化能力。
- **提升实时检测能力**，针对区块链交易的实时性需求，开发增量学习和实时图更新机制，提升 ETH-GBERT 在实时监控中的应用性能。
- **跨链数据融合与多链分析**，随着跨链技术的发展，ETH-GBERT 可进一步扩展至跨链欺诈检测，探索如何有效融合来自多个区块链的数据，提升跨链欺诈识别能力。
- **模型解释性与可解释性**，未来的研究可以进一步提升模型的透明度和可解释性，使得模型在实际应用中不仅提供准确的判断结果，还能给出清晰的决策依据。

总体而言，ETH-GBERT 模型为区块链欺诈检测提供了一种新的有效方法，并为区块链安全领域的发展做出了积极贡献。随着技术的不断进步，ETH-GBERT 将有望在更多的实际应用中展现其巨大的潜力，推动区块链技术在安全领域的进一步发展。

参考文献

[1] Pal A., Tiwari C.K., Behl A. Blockchain technology in financial services: a comprehensive review of the literature[J]. Journal of Global Operations and Strategic Sourcing, 2021, 14(1): 61-80.

[2] Bhowmik M., Chandana T.S.S., Rudra B. Comparative study of machine learning algorithms for fraud detection in blockchain[A]. 2021 5th international conference on computing methodologies and communication (ICCMC)[C]. IEEE, 2021: 539-541.

[3] Lai J.Y., Wang J., Chiu Y.H. Evaluating blockchain technology for reducing supply chain risks [J]. Information Systems and e-Business Management, 2021, 19(4): 1089-1111.

[4] Wenhua Z., Qamar F., Abdali T.A.N., Hassan R., Jafri S.T.A., Nguyen Q.N. Blockchain technology: security issues, healthcare applications, challenges and future trends[J]. Electronics, 2023, 12(3): 546.

[5] Bhutta M.N.M., Khwaja A.A., Nadeem A., Ahmad H.F., Khan M.K., Hanif M.A., et al. A survey on blockchain technology: Evolution, architecture and security[J]. Ieee Access, 2021, 9: 61048-61073.

[6] Givargizov I. Unstable financial and economic factors in the world and their influence on the development of blockchain technologies[J]. International Humanitarian University Herald. Economics and Management, 2023.

[7] Kipf T.N., Welling M. Semi-supervised classification with graph convolutional networks[J]. arXiv preprint arXiv:1609.02907, 2016.

[8] Ancelotti A., Liason C. Review of blockchain application with graph neural networks, graph convolutional networks and convolutional neural networks[J]. arXiv preprint arXiv:2410.00875, 2024.

[9] Su S., Zhang X., Xiao S., Li Z. Unraveling the deception of web3 phishing scams: Dynamic multiperspective cascade graph approach for ethereum phishing detection[J]. IEEE Transactions on Computational Networks, 2024.

[10] Galdeman A., Al-Harbi H. Scalable blockchain fraud detection using spatial-temporal graph neural networks[J]. Frontiers in Applied Physics and Mathematics, 2025.

[11] Fan S., Xu H., Fu S., Luo Y., Xu M. Edge-feature modeling-based topological graph neural networks for phishing scams detection on ethereum[J]. IEEE/ACM 32nd International Conference on Blockchain, 2024.

[12] Jin S., Yang Q., Chen S., Zhang H. Neighborhood subgraph-based illicit transaction detection in cryptocurrency networks[J]. IEEE Internet of Things (IIKI) Conference, 2024.

[13] Cui B., Wang G. Ponzi scheme detection based on cnn and bigru combined with attention mech-

anism[J]. IEEE Transactions on Computer Science, 2024.

[14] Latifi S. Itng 2024: 21st international conference on information technology-new generations [M]. Springer, 2024.

[15] Harper A., Lee M. Fraud detection in cryptocurrency using spatial-temporal graph neural networks[J]. IEEE Access, 2025.

[16] Osterrieder J., Chan S., Chu J., Zhang Y., Misheva B.H., Mare C. Enhancing security in blockchain networks: Anomalies, frauds, and advanced detection techniques[J]. arXiv preprint arXiv:2402.11231, 2024.

[17] Tan R., Tan Q., Zhang P., Li Z. Graph neural network for ethereum fraud detection[A]. 2021 IEEE international conference on big knowledge (ICBK)[C]. IEEE, 2021: 78-85.

[18] Kanezashi H., Suzumura T., Liu X., Hirofuchi T. Ethereum fraud detection with heterogeneous graph neural networks[J]. arXiv preprint arXiv:2203.12363, 2022.

[19] Li P., Xie Y., Xu X., Zhou J., Xuan Q. Phishing fraud detection on ethereum using graph neural network[A]. International Conference on Blockchain and Trustworthy Systems[C]. Springer, 2022: 362-375.

[20] Wang J., Chen P., Xu X., Wu J., Shen M., Xuan Q., et al. Tsgn: Transaction subgraph networks assisting phishing detection in ethereum[J]. arXiv preprint arXiv:2208.12938, 2022.

[21] Hou W., Cui B., Li R. Detecting phishing scams on ethereum using graph convolutional networks with conditional random field[A]. 2022 IEEE 24th Int Conf on High Performance Computing & Communications; 8th Int Conf on Data Science & Systems; 20th Int Conf on Smart City; 8th Int Conf on Dependability in Sensor, Cloud & Big Data Systems & Application (HPCC/DSS/SmartCity/DependSys)[C]. IEEE, 2022: 1495-1500.

[22] Hu T., Liu X., Chen T., Zhang X., Huang X., Niu W., et al. Transaction-based classification and detection approach for ethereum smart contract[J]. Information Processing & Management, 2021, 58(2): 102462.

[23] Farrugia S., Ellul J., Azzopardi G. Detection of illicit accounts over the ethereum blockchain[J]. Expert Systems with Applications, 2020, 150: 113318.

[24] Pan B., Stakhanova N., Zhu Z. Ethershield: Time-interval analysis for detection of malicious behavior on ethereum[J]. ACM Transactions on Internet Technology, 2024, 21(1): 1-30.

[25] Sun J., Jia Y., Wang Y., Tian Y., Sheng Z. Ethereum fraud detection via joint transaction language model and graph representation learning[J]. Information Fusion, 2025: 103074.

[26] Li S., Gou G., Liu C., Hou C., Li Z., Xiong G. Ttagn: Temporal transaction aggregation graph network for ethereum phishing scams detection[A]. Proceedings of the ACM Web Conference 2022[C]. 2022: 661-669.

[27] Wen T., Xiao Y., Wang A., Wang H. A novel hybrid feature fusion model for detecting phishing

scam on ethereum using deep neural network[J]. Expert Systems with Applications, 2023, 211: 118463.

[28] Chen Z., Liu S.Z., Huang J., Xiu Y.H., Zhang H., Long H.X. Ethereum phishing scam detection based on data augmentation method and hybrid graph neural network model[J]. Sensors, 2024, 24(12): 4022.

[29] Veličković P., Cucurull G., Casanova A., Romero A., Lio P., Bengio Y. Graph attention networks [J]. arXiv preprint arXiv:1710.10903, 2017.

[30] Devlin J., Chang M.W., Lee K., Toutanova K. Bert: Pre-training of deep bidirectional transformers for language understanding[A]. Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies[C]. 2019: 4171-4186.

[31] Hu S., Zhang Z., Luo B., Lu S., He B., Liu L. Bert4eth: A pre-trained transformer for ethereum fraud detection[A]. Proceedings of the ACM Web Conference 2023[C]. 2023: 2189-2197.

[32] Liu S., Cui B., Hou W. A survey on blockchain abnormal transaction detection[A]. International Conference on Blockchain and Trustworthy Systems[C]. Springer, 2023: 211-225.

[33] Tapscott D., Tapscott A. Blockchain revolution: How the technology behind bitcoin and other cryptocurrencies is changing the world[M]. Penguin Random House, 2016.

[34] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[Z]. 2008.

[35] Swan M. Blockchain: Blueprint for a new economy[M]. O'Reilly Media, Inc., 2015.

[36] Zohar A. Blockchain technologies: Principles and applications[M]. Springer, 2018.

[37] Yli-Huumo J., Ko D., Choi S., Park S., Smolander K. A survey of blockchain technology applications in various industries[J]. Future Generation Computer Systems, 2016, 58: 30-41.

[38] Wood G. Ethereum: A secure decentralised generalised transaction ledger[Z]. 2014.

[39] Buterin V. A next-generation smart contract and decentralized application platform[Z]. 2013.

[40] LeCun Y., Bengio Y., Hinton G. Deep learning[J]. Nature, 2015, 521: 436-444.

[41] Hinton G., Srivastava N., Krizhevsky A., Sutskever I., Salakhutdinov R. Improving neural networks by preventing co-adaptation of feature detectors[J]. arXiv preprint arXiv:1207.0580, 2012.

[42] He K., Zhang X., Ren S., Sun J. Deep residual learning for image recognition[J]. IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016: 770-778.

[43] Krizhevsky A., Sutskever I., Hinton G. Imagenet classification with deep convolutional neural networks[J]. Advances in Neural Information Processing Systems (NeurIPS), 2012, 25: 1097-1105.

[44] Hochreiter S., Schmidhuber J. Long short-term memory[J]. Neural Computation, 1997, 9: 1735-1780.

[45] Devlin J., Chang M., Lee K., Toutanova K. Bert: Pre-training of deep bidirectional transformers

for language understanding[J]. arXiv preprint arXiv:1810.04805, 2018.

[46] Sun T., Wang X., Wang Y., Li J. How to fine-tune bert for text classification?[J]. arXiv preprint arXiv:1905.05583, 2019.

[47] Kipf T., Welling M. Semi-supervised classification with graph convolutional networks[A]. Proceedings of the International Conference on Learning Representations (ICLR)[C]. 2017.

[48] Bruna J., Zaremba W., Szlam A., LeCun Y. Spectral networks and deep locally connected networks on graphs[J]. arXiv preprint arXiv:1312.6203, 2013.

[49] Hamilton W., Ying R., Leskovec J. Inductive representation learning on large graphs[J]. Proceedings of the Neural Information Processing Systems (NeurIPS), 2017, 30.

[50] Chen W., Zheng Z., Ngai E.C.H., Zheng P., Zhou Y. Exploiting blockchain data to detect smart ponzi schemes on ethereum[J]. IEEE Access, 2019, 7: 37575-37586.

[51] Clarke M. Arbitrary-order sampling and hand motion modeling with transformers[D]. Open Access Te Herenga Waka-Victoria University of Wellington, 2023.

[52] Xue Z., Marculescu R. Dynamic multimodal fusion[A]. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition[C]. 2023: 2575-2584.

[53] Perozzi B., Al-Rfou R., Skiena S. Deepwalk: Online learning of social representations[A]. Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining[C]. 2014: 701-710.

[54] Wu J., Yuan Q., Lin D., You W., Chen W., Chen C., et al. Who are the phishers? phishing scam detection on ethereum via network embedding[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2020, 52(2): 1156-1166.

[55] Rozemberczki B., Sarkar R. Fast sequence-based embedding with diffusion graphs[A]. Complex Networks IX: Proceedings of the 9th Conference on Complex Networks CompleNet 2018 9[C]. Springer, 2018: 99-107.

[56] Ahmed N.K., Rossi R., Lee J.B., Willke T.L., Zhou R., Kong X., et al. Learning role-based graph embeddings[J]. arXiv preprint arXiv:1802.02896, 2018.

[57] Béres F., Seres I.A., Benczúr A.A., Quintyne-Collins M. Blockchain is watching you: Profiling and deanonymizing ethereum users[A]. 2021 IEEE international conference on decentralized applications and infrastructures (DAPPS)[C]. IEEE, 2021: 69-78.

[58] Hamilton W., Ying Z., Leskovec J. Inductive representation learning on large graphs[J]. Advances in neural information processing systems, 2017, 30.

攻读硕士学位期间的学术活动及成果情况

1）参加的学术交流与科研项目

（1） 2024 5th International Conference on Signal Processing and Computer Science（SPCS 2024）

2）发表的学术论文（含专利和软件著作权）

（1） Zhang Sheng, Tan Kia Quang, Kai Li, Yue Duan. Understanding and Characterizing Obfuscated Funds Transfers in Ethereum Smart Contracts[C]. Submitted to Internet Measurement Conference 2025 (IMC 2025). Published in: arXiv preprint arXiv:2505.11320, 2025.

（2） Sun J, Jia Y, Wang Y, Zhang S, et al. Ethereum fraud detection via joint transaction language model and graph representation learning[J]. Information Fusion, 2025, 120: 103074.

（3） Sheng Z, Song L, Wang Y. Dynamic Feature Fusion: Combining Global Graph Structures and Local Semantics for Blockchain Fraud Detection[J]. IEEE Transactions on Network and Service Management.

（4） Sheng Z, Duan L, Jiang H. Accelerating Gaussian beam tracing method with dynamic parallelism on graphics processing units[J]. Computer Physics Communications.

（5） Sheng Z, Zhu H. Optimizing acoustic field rendering through heterogeneous computing[C]//Fifth International Conference on Signal Processing and Computer Science (SPCS 2024). SPIE, 2025, 13442: 316-321.

（6） 张升, 段礼沭, 姜汉博. 一种基于 GPU 动态并行高斯波束追踪方法: 浙江省, CN118565603A[P]. 2024-08-30 [发明专利]

3）获得的学术奖励

（1） Asia-Pacific Mathematical Modeling Contest (APMCM) Second Prize, 2022.