分类号：　　密　　级：公开

学　号：20232008004　　单位代码：10759

石河子大学

硕 士 学 位 论 文

基于区块链的隐私保护和异常行为检测协同方法研究

学 位 申 请 人	庞晋鹏
指 导 教 师	高攀
申请学位门类级别	工学硕士
学科、专业名称	网络空间安全
研 究 方 向	信息内容安全
所 在 学 院	信息科学与技术学院

中国·新疆·石河子

2026 年 5 月

分类号：　　密　　级：公开

学　号：20232008004　　单位代码：10759

石河子大学

硕 士 学 位 论 文

基于区块链的隐私保护和异常行为检测协同方法研究

学 位 申 请 人	庞晋鹏
指 导 教 师	高攀
申请学位门类级别	工学硕士
学科、专业名称	网络空间安全
研 究 方 向	信息内容安全
所 在 学 院	信息科学与技术学院

中国·新疆·石河子

2026 年 5 月

Research on Collaborative Method for Privacy Protection and Anomaly Detection Based on Blockchain

A Dissertation Submitted to

Shihezi University

In Partial Fulfillment of the Requirements

for the Degree of

Master of Engineering

By

Pang Jin-peng

（Cyberspace Security）

Dissertation Supervisor: Prof. Gao Pan

May, 2026

石河子大学学位论文独创性声明及使用授权声明

学位论文独创性声明

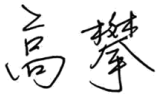
本人所呈交的学位论文是在我导师的指导下进行的研究工作及取得的研究成果。据我所知，除文中已经注明引用的内容外，本论文不包含其他个人已经发表或撰写过的研究成果。对本文的研究做出重要贡献的个人和集体，均已在文中作了明确的说明并表示谢意。

研究生签名：  时间：2026 年 5 月 24 日

使用授权声明

本人完全了解石河子大学有关保留、使用学位论文的规定，学校有权保留学位论文并向国家主管部门或指定机构送交论文的电子版和纸质版。有权将学位论文在学校图书馆保存并允许被查阅。有权自行或许可他人将学位论文编入有关数据库提供检索服务。有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

研究生签名：  时间：2026 年 5 月 24 日

导师签名：  时间：2026 年 5 月 24 日

摘要

政务数据是数字政府建设的重要基础资源，其安全治理与高效利用对提升政府治理能力、释放数据要素价值具有重要意义。然而，在电子政务联盟链场景下，区块链虽提升了数据可信性，但加大了数据机密性、属性隐私和验证过程隐私的保护难度；同时，区块链数据兼具时序逻辑与拓扑关联且异常样本稀缺，增加了异常行为检测的难度。此外，单一技术难以兼顾隐私保护与异常检测，而二者在数据形态、处理方式和响应路径上的差异又增加了协同治理的复杂性。针对以上问题，本文围绕区块链环境下的隐私保护、异常行为检测及协同响应机制展开研究，旨在构建兼顾安全性、可信性与治理效能的数据安全治理方法，为政务数据安全保障与风险防控提供参考。

本文主要研究工作如下：

（1）在隐私保护方面，设计了融合变色龙哈希 Merkle 树（CH-Merkle）、密文策略属性基加密（CP-ABE）、零知识可扩展透明知识论证（zk-STARKs）、密钥和数据封装机制（KEM/DEM）混合加密的多阶段隐私保护架构，实现权限状态的原地原子化更新与密文环境下的细粒度访问控制，实验结果表明，本方案端到端延迟稳定在 524~527ms 区间，交易区分成功率为 53.1%，操作模式熵为 3.31 bits，Bhattacharyya 值为 0.9931；

（2）在异常检测方面，设计了时空多视图融合网络（ST-MFN），网络由 GraphSAGE 图结构分支和 Transformer 时序分支组成，并结合自适应门控、多尺度特征增强等方法，以提升类别极度不平衡场景下异常行为识别的精度与鲁棒性，实验结果表明，ST-MFN 在 Elliptic 数据集上的 Precision 为 0.8776，F1-Score 为 0.7505，AUC-ROC 为 0.901；

（3）在协同治理方面，设计了满足本地差分隐私约束的多视图特征投影算子，以解决隐私保护与异常检测之间输入域不兼容的问题，同时设计了风险自适应有限状态机与承诺—揭示分布式共识协议，形成从隐私映射、协同检测到分级响应的协同治理流程，实验结果表明，当隐私预算为 2.0 时，检测模型效用退化率为 3.4%，在 40%恶意节点投毒环境下，全局共识偏差为 1.89%，在突发攻击场景下，R-FSM 的累积安全损失为 4.77，用户干扰率为 3.2%。

综上，本文构建了面向电子政务联盟链的政务数据安全治理方法与协同框架，实现了隐私保护、异常行检测到分级联动响应的协同联动，所提方法能够在隐私约束条件下兼顾数据安全与治理有效性，为政务数据安全治理与风险防控提供了可行的技术方案。

关键词：区块链；隐私保护；异常行为检测；协同治理

ABSTRACT

Government data constitutes a vital foundational resource for the development of a digital government; its secure governance and efficient utilisation are of great significance for enhancing government governance capabilities and unlocking the value of data as a key factor. However, in the context of e-government consortium blockchains, whilst blockchain technology enhances data credibility, it also increases the difficulty of protecting data confidentiality, attribute privacy and the privacy of the verification process. At the same time, blockchain data combines temporal logic with topological relationships, and the scarcity of anomalous samples further complicates the detection of anomalous behaviour. Furthermore, it is difficult for a single technology to address both privacy protection and anomaly detection simultaneously, whilst the differences between the two in terms of data format, processing methods and response pathways further increase the complexity of collaborative governance. In response to these issues, this thesis investigates privacy protection, anomaly detection and collaborative response mechanisms within a blockchain environment, aiming to construct a data security governance methodology that balances security, trustworthiness and governance effectiveness, thereby providing a reference for the security assurance and risk prevention of government data.

The main research contributions of this thesis are as follows:

(1) In terms of privacy protection, a multi-stage privacy protection architecture was designed that integrates Chameleon Hash Merkle Trees (CH-Merkle), Ciphertext-based Attribute-based Encryption (CP-ABE), Zero-knowledge Scalable Transparent Arguments of Knowledge (zk-STARKs), and Key and Data Encapsulation Mechanisms (KEM/DEM). This architecture enables in-place atomic updates of permission states and fine-grained access control within a ciphertext environment. Experimental results indicate that the end-to-end latency of this scheme remains stable within the range of 524–527 ms, with a transaction discrimination success rate of 53.1%, an operation mode entropy of 3.31 bits, and a Bhattacharyya measure of 0.9931;

(2) In the area of anomaly detection, a Spatio-Temporal Multi-View Fusion Network (ST-MFN) was designed. The network comprises a GraphSAGE graph structure branch and a Transformer temporal branch, and incorporates methods such as adaptive gating and multi-scale feature enhancement to improve the accuracy and robustness of anomaly behaviour recognition in scenarios with extreme class imbalance. Experimental results show that ST-MFN achieves a Precision of 0.8776 on the Elliptic dataset, an F1-score of 0.7505, and an AUC-ROC of 0.901;

(3) In terms of collaborative governance, a multi-view feature projection operator satisfying local differential privacy constraints was designed to resolve the incompatibility between the input domains of privacy protection and anomaly detection. Concurrently, a risk-adaptive finite-state machine and a commitment-disclosure distributed consensus protocol were devised, forming a collaborative governance workflow spanning privacy mapping, collaborative detection, and tiered response. Experimental results indicate that when the privacy budget is 2.0, the detection model's utility degradation rate is 3.4%; in an environment with 40% malicious node poisoning, the global consensus bias is 1.89%; and in a sudden attack scenario, the cumulative security loss of the R-FSM is 4.77, with a user interference rate of 3.2%.

In summary, this thesis constructs a governance methodology and collaborative framework for government data security tailored to e-government consortium blockchains, achieving coordinated interaction from privacy protection and anomaly detection to tiered joint response. The proposed method balances data security and governance effectiveness under privacy constraints, providing a viable technical solution for government data security governance and risk prevention and control.

Key words: Blockchain; Privacy protection; Anomaly detection; Collaborative governance

目录

第一章 绪论

1.1 研究背景和意义

数字政府建设是网络强国战略重要实践，是数字中国建设关键一环，同时，对数据进行高效利用，实现数据的最大化价值，是在数字经济时代掌握数据核心资产的关键[1]，政务数据是政府部门进行社会治理的重要记录与呈现，具有较高的政治、经济、科学、文化和社会价值，在国民经济建设和国家安全战略体系中发挥着越来越重要的作用。《国务院关于加强数字政府建设的指导意见》指出要求依法依规促进数据高效共享和有序开发利用，充分释放数据要素价值，确保各类数据和个人信息安全，因此，结合数字政府建设背景，研究政务数据安全和隐私保护的实现机制变得尤为重要。

当下，政务数据共享开放使得数据流动成为常态，但多环节的信息隐性留存和数据流转环境复杂使数据泄密、数据篡改、非法访问、信息扭曲等政务数据开放后的衍生性问题出现风险增大[2][3]。而区块链技术的出现，为安全高效地跨部门、跨层级政务数据共享提供了新的思路和途径。它通过协商一致的规范和协议，在信息不可篡改和交易可追溯的基础上克服了信任问题。其次，区块链实现了在 IT 系统中引入人类社会治理模式的可能[4]，它将传统中心化系统发展成了完全去中心或多中心的系统，能够让拥有不同数据需求的部门在同一 IT 系统中共享数据，并在共享数据的基础上制定合约提高数据共享服务的质量。

虽然基于区块链不可篡改、交易可追溯等根本特性可以给政务数据共享过程带来数据的可信度，但区块链上数据公开的特点也带了政务数据隐私安全问题。电子政务数据是指用户、企业和政府部门个人在进行政务服务时产生的各种数据，包括身份证明、许可证、税务信息等。这些数据具有高度的敏感性[5],多数情况下需要获得用户授权，同时还必须按照数据共享有关的业务管理规则，在大量政务数据汇聚发挥数据价值的同时，也更容易成为攻击，如果被不法分子窃取或篡改，会给用户造成经济损失[6]、信誉损害甚至法律风险。针对区块链应用于政务数据流转过程中存在的隐私安全问题，常规的解决方法通常会使用结合区块链和密码学的方案，在数据传输过程中使用诸如访问控制、零知识证明等密码学协议以及属性基加密等密码算法保障数据隐私。这些方案可以较为安全高效地保护政务数据自身的隐私。但隐私种类多样，例如在属性基加密访问控制中除了数据自身的隐私还存在访问者身份属性隐私、访问权限属性隐私，在政务数据中还存在数据真实性验证时的隐私以及权限动态更新时的状态一致性等。若只考虑单方面隐

私保护，可能让攻击者通过推理攻击等方式获取政务数据中敏感数据。结合不同密码学方法的隐私保护方案可以解决不同类型的隐私问题，例如密文策略属性基加密（CP-ABE）可以实现基于属性的细粒度数据访问控制，零知识证明可以在不暴露属性明文的前提下完成策略验证，而变色龙哈希等具备陷门特性的密码学原语可以支撑权限状态的动态高效更新。将上述方法结合使用，可以同时覆盖数据机密性、属性隐私性、验证可信性与权限动态性等多方面需求，实现更加全面的隐私保护，进而确保政务数据流转的高效性和可靠性的同时，最大程度地保护用户个人信息和数据安全。这不仅提高了政务数据流转的可信度，还增强了公众对电子政务系统的信任度，有助于推动电子政务的健康发展，最终实现政务服务的优化和提升。

同时，随着区块链技术在电子政务数据安全应用范围不断扩大和多样化，针对电子证照、政务数据管理、公共服务等领域的合规监管与风险控制需求也在不断增加。因此，监管部门迫切需要挖掘区块链系统中有价值的交易信息，在保障数据隐私的前提下检测异常行为，关联背后的合谋团伙，洞察违规数据流向，从而提高政务数据的安全治理效率。然而，现有的异常检测研究在应用到电子政务联盟链场景时，仍面临以下较为突出的困难：（1）数据特征的异构性与单视图局限性：电子政务区块链数据呈现出时空异构特性。一方面，账户间的交互构成了复杂的空间拓扑结构；另一方面，业务流程的流转蕴含着时序逻辑依赖。传统的机器学习或单一的图算法往往顾此失彼：仅关注图结构容易忽略慢速的流程违规，仅关注时序则难以识别隐蔽的团伙合谋。如何将这两种异构视图有效融合，是提升检测精度的重要因素。（2）动态演化与长程依赖的捕捉难题：真实的政务数据网络是动态演化的，节点和边随业务发生实时增删。现有的静态图方法难以捕捉网络结构的时间演变规律，而传统的循环神经网络在处理长周期的政务审批链条时，容易出现梯度消失，难以捕捉长程时序依赖。相较之下，结合了 Transformer 与图神经网络的融合架构更具优势：GraphSAGE 等归纳式图算法能够通过聚合邻居信息高效处理动态节点的空间特征，而 Transformer 的自注意力机制能够并行捕捉序列中的全局长程依赖。

此外，由于政务数据流通过程具有跨层级、跨地域、跨系统、跨部门、跨业务特点，因此需要具有数据归集权、数据使用权、数据管理权[7]的政务数据管理权限所有方发挥各自的职责，对数据安全贡献进行协同管理[8]。随着数字化政府的不断推进以及信息化手段的不断更迭，仅依靠组织协同进行政务数据安全防治会出现因不同部门的数据安全能力和意识参差不齐导致数据泄露或被滥用问题以及因各部门存在自我保护和权限意识导致某些数据不愿共享或共享不完全问题。而在组织协同的基础上引入隐私保护与异常行为检测等技术手段进行协同防治，是一种更可行的做法，但隐私保护与异常检测在技术路径上存在矛盾：前者将敏感数据封装为不可解析的密文形式，后者却依赖可计算的明文特征进行风险研判，两者的直接组合面临输入域不兼容的问题，需要构建专门的

适配机制才能实现有效协同。在此前提下，通过标准化的数据格式、加密传输、身份认证、访问控制、恶意数据检测等技术手段，有效保障数据的安全性、完整性和隐私性，同时还能自动化实现数据流转流程，减少人为干预带来的风险，并通过区块链等分布式技术增强数据透明度与可信度，从而更高效、可靠地打破信息孤岛，促进跨部门的数据安全治理。

1.2 国内外研究现状

本节从基于区块链的隐私保护研究、基于区块链的异常行为检测研究和基于区块链的隐私保护与异常行为检测协同研究三个方面梳理国内外研究现状，并介绍相关典型方案及其存在的问题。

1.2.1 基于区块链的隐私保护研究

随着人工智能、互联网、物联网及数字经济的持续发展，数据已逐渐成为支撑社会运行与经济增长的重要基础资源。在数据采集、存储、传输、处理和共享过程中，往往涉及大量个人隐私信息、商业敏感信息以及工业关键数据，隐私泄露、数据滥用和越权访问等问题日益突出。传统隐私保护方法大多依赖中心化架构，虽然能够在一定程度上实现数据加密和权限控制，但普遍存在单点故障、可信性不足以及数据易被篡改等缺陷，难以满足复杂应用场景下对数据安全、可信共享与隐私保护的多重需求。区块链技术因其去中心化、难篡改、可追溯和多方协同等特点，为数据隐私保护提供了新的解决思路。然而，区块链账本具有公开透明特征，如果缺乏有效的保护机制，也可能引发交易内容、身份关系以及访问行为的隐私暴露问题。因此，如何在保障区块链可信性的同时实现隐私保护，已成为当前研究的重点方向之一[9][10]。目前，围绕区块链隐私保护的研究主要集中在身份认证、交易数据保护、数据共享与访问控制、匿名机制设计以及区块链与隐私计算融合等方面。

在隐私认证研究中，Chen 等人[11]提出了一种面向电动汽车换电场景的智能区块链隐私保护认证协议，该方法利用区块链增强数据存储完整性和交易验证安全性，从而提升了认证过程的安全水平，但其在匿名保护能力和交易验证效率的扩展性方面仍存在优化空间。Naidu 等人[12]将零知识证明技术引入区块链认证系统，构建了兼顾支付认证隐私保护和交易透明追踪的方案，并借助智能合约提升了认证过程的自动化与透明性，但该方案仍在一定程度上依赖外部约束来防止验证者合谋泄露陷门密钥。

在交易数据隐私保护方面，相关研究通常通过引入差分隐私、零知识证明等技术降低交易信息泄露风险。Guo 等人[13]针对去中心化边缘资源交易场景，提出了融合区块链

与差分隐私的资源拍卖系统。该方案利用区块链防止恶意节点篡改交易及合约信息，同时借助差分隐私增强了交易数据的隐私保护能力，兼顾了系统公平性与去中心化特征。Li 等人[14]提出了一种面向飞行操作数据的区块链安全共享方案，通过结合零知识证明和代理重加密技术，实现了飞行数据的隐私保护与安全共享，但在面对海量数据时，其处理效率仍有待提升。Xue 等人[15]则针对数据交易场景设计了隐私增强的可追溯匿名交易方案，利用环签名与 Merkle 哈希树技术优化了签名和验证过程，在一定程度上实现了匿名性与可追踪性的平衡，但随着交易规模扩大，系统在计算效率和扩展性方面仍可能受到限制。

在数据共享与细粒度访问控制方面，属性加密、代理重加密和链上链下协同存储已成为当前研究的重要技术路径。时雪磊[16]针对电力数据中的用户隐私泄露问题，提出了基于属性加密的隐私保护方案，通过引入云服务商和多个授权中心，实现了电力数据一对多的访问控制与高效计算，但由于数据仍然存储于中心化服务器中，系统依旧存在单点故障和数据被篡改的风险。巫朝霞等人[17]针对云环境下医疗数据存储中的隐私泄露与共享效率不高问题，提出了一种支持多授权机构的属性基加密方案，采用离线计算与外包计算方式提高加解密效率，并实现了细粒度访问控制，但同样未能彻底摆脱中心化存储带来的固有缺陷。Liang 等人[18]提出了基于联盟链的个人数据隐私保护方案，通过改进 Paillier 同态加密机制并结合属性加密访问控制方法，提升了个人数据保护能力，但同态加密本身计算复杂度较高，在大规模数据处理场景下容易造成系统性能下降。Zhang 等人[19]将属性基加密与关键词搜索技术结合，构建了支持可验证性和公平支付的数据共享框架，增强了密文数据检索与共享过程的安全性。翟社平等人[20]针对中心化存储和共享壁垒问题，提出了一种基于区块链的属性代理重加密数据共享方案，采用双链结构分别管理密文数据和索引信息，并通过分布式密钥生成和周期更新机制强化系统安全性，从而实现了较为灵活的细粒度访问控制。Li 等人[21]构建了基于区块链的个人健康记录共享方案，实现了对 PHR 数据的细粒度访问控制和安全共享，但该方案在数据上传和下载过程中的吞吐能力仍然不足。Wang 等人[22]则面向区块链工业物联网场景提出了一种轻量级安全数据共享方案，综合利用代理重加密、身份认证以及链上链下协同存储机制，在保障数据来源可信与防止数据滥用的同时，有效降低了区块链存储开销。Ma 等人[23]面向工业互联网数据共享需求，提出了安全高效、可追踪且可撤销的数据共享方案，将区块链技术与 IIoT 架构相结合，实现了动态域撤销和用户撤销，并在 CP-ABE 基础上引入隐藏策略机制，从而增强了访问控制的灵活性和隐私保护能力。

随着研究的不断深入，学者们逐渐认识到，仅依赖数据加密并不足以全面应对区块链环境下的隐私泄露问题。为隐藏用户身份和交易关系，环签名、零知识证明、一次性地址等匿名技术被引入区块链隐私保护体系之中。Liu 等人[24]提出了一种基于区块链和无证书环签名的物联网数据共享方案 BCRS-DS，该方案利用无证书环签名保护参与者

身份隐私，并引入基于零知识证明的去中心化匿名激励机制，在提高认证效率的同时兼顾了奖励分配过程中的隐私保护需求。这类研究说明，多层次、多维度的隐私保护机制已成为区块链数据共享领域的重要研究方向。

此外，区块链与联邦学习等隐私计算技术的融合也逐渐成为研究热点。Yang 等人[25]提出了一种结合区块链、同态加密和声誉机制的联邦学习方法，通过同态加密保护训练数据隐私，并借助区块链记录模型更新过程及声誉信息，以增强训练过程的安全性和公正性。然而，在数据规模不断扩大的情况下，该方案面临同态加密计算开销较高、数据传输时延较大等问题，从而影响系统训练效率与实时性。这表明，虽然区块链与隐私计算技术的结合能够提升隐私保护水平，但在性能优化和实际部署方面仍有较大的研究空间。

1.2.2 基于区块链的异常行为检测研究

随着图神经网络技术的不断发展，异常检测研究逐渐由传统机器学习方法转向能够刻画复杂结构关系与时序依赖的深度图模型。尤其是在区块链场景中，交易行为具有图结构特征，账户之间的转账关系、交易路径及其时间演化过程，为异常交易识别提供了丰富的信息来源。因此，基于图神经网络、时序建模和多特征融合的区块链异常检测方法已成为当前研究的重点方向。

在图异常检测方法的发展过程中，基于图卷积网络（GCN）的模型逐渐成熟。Deng 等人[26]提出了时空图卷积对抗网络（STGAN），针对复杂时空关联和异常判定标准动态变化的问题，构建了由时空生成器和判别器组成的双重检测机制，并引入图卷积门控循环单元（GCGRU）以及新的异常分数计算方法，从而提升了异常检测性能。尽管该研究主要面向交通场景，但其在动态图表示学习和异常评分设计上的思路，对区块链交易网络异常检测具有重要启发意义。在图注意力网络的改进方面，Huang 等人[27]提出了 DHSEGATs 方法，通过引入编码距离和逐跳结构统计信息对图注意力网络（GAT）进行增强，取得了具有竞争力的检测效果。这一研究说明，仅依靠局部邻居聚合难以充分反映区块链交易网络中的复杂拓扑关系，而结合更丰富的结构信息能够提升异常识别能力。谭朋柳等人[28]则提出融合图注意力网络与支持向量机的 GAS 方法，利用 GAT 聚合目标节点邻居特征，提取节点间复杂关系，再将更新后的节点表示输入 SVM 完成分类，实现了较高效的异常交易检测。这类方法体现出深度表示学习和传统分类器混合范式在区块链异常检测中的实用价值。

面向区块链安全应用，Turner 等人[29]针对加密货币犯罪检测问题，对比特币交易网络中的异常行为识别进行了专门研究。他们并未直接采用通用图嵌入方法，而是结合比特币交易图的实际特征，对 GraphSAGE 算法进行了针对性改进，并引入“暴露度”特

征以量化交易的风险属性。实验表明，该方法不仅在标准数据集上具有较好表现，而且在真实世界中面对复杂多变的勒索软件攻击时仍保持了较强的稳定性与鲁棒性。这为图学习方法在区块链安全领域的应用提供了实践上的参考。

针对区块链交易数据特征复杂、多源异构的问题，研究者开始重视多特征融合建模。林伟[30]提出了多特征融合模型 MFF（Multi Feature Fusion），通过整合区块链交易数据中的多种属性特征，构建拼接特征向量，以提高异常检测的准确率。Liu 等人[31]将 Transformer 架构引入图异常检测任务，弥补了传统方法在复杂时序依赖建模和图结构动态变化刻画上的不足。该方法通过设计时序编码机制，有效捕捉节点在不同时间维度上的行为演变特征，从而能够识别那些表面上正常、但实际上偏离常规行为模式的异常节点。这一研究表明，结合时序建模与图结构学习，是提升区块链异常检测能力的重要方向。

在账户身份识别与交易主体分类方面，Liu 等人[32]提出了过滤与增强图神经网络模型 FA-GNN（Filter and Augment Graph Neural Networks），以区块链交易图结构为核心，在以太坊用户身份分类任务中实现了精确率与召回率的同步提升。Gu 等人[33]则面向 Binance、Coinbase 等大型交易所提出了一个异常交易检测框架，该框架包括爬虫系统、特征工程和深度学习检测模块：首先通过爬虫整合多交易所用户信息，其次提取跨平台共性交易特征，最后利用基于注意力机制的 LSTM 网络对交易数据进行拟合与重构，通过原始值与拟合值之间的差异识别异常交易。这表明，区块链异常检测已逐步从单一链上行为分析扩展到跨平台、多源异构数据联合建模。

在可解释性与样本不平衡问题上，刘现林[34]提出了基于自动化图特征的区块链异常检测框架。该方法结合深度合成特征与高阶图结构特征，并采用 LightGBM 对账户进行分类，在实验中验证了其有效性。同时，为尽可能保留正常样本信息并缓解黑样本不足的问题，该研究还提出基于变分自编码器互补对抗生成网络的数据增强方法，通过完整分布的白样本生成潜在黑样本，从而提升异常检测效果。这一研究体现了区块链异常检测正在从单纯追求识别性能，也开始兼顾解释性与样本质量。

此外，时序序列建模在区块链交易异常检测中也发挥了重要作用。Ding 等人[35]提出了 DNLP-TCT 交易跟踪模型，在自动编码器框架下结合时间自注意力机制与双向长短期记忆网络（Bi-LSTM），以捕捉交易网络中的动态行为与结构特征。Ogundokun 等人[36]采用 LSTM、Bi-LSTM 和 CNN-LSTM 等深度学习方法，对区块链交易网络中的钓鱼攻击进行检测，验证了序列建模方法在处理交易行为时序特征方面具备较高的准确性与鲁棒性。Li 等人[37]提出的 TTAGN 方法则关注时序交易聚合问题，针对现有工作缺乏时序信息建模和节点表征能力不足的问题，通过子图提取、一方面利用 LSTM 建模历史交易记录的时间关系形成时间边表示，另一方面采用图注意力机制聚合周围边表示形成交易特征，最终与统计特征联合用于异常检测任务，增强了模型对时序与结构信息的综合利