E-Commerce Letters 电子商务评论, 2025, 14(12), 1697-1703
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124041

Hans汉斯

网络支付场景下电子商务财务风险智能识别与防控路径研究

金　锟

上海理工大学财务处，上海

收稿日期：2025年10月30日；录用日期：2025年11月14日；发布日期：2025年12月11日

摘　要

随着网络支付在电子商务领域深入渗透，线上交易便捷性和财务风险复杂性同步增长，本文依据财务风险管理理论与智能决策理论，深入探讨网络支付场景下电子商务财务风险的智能识别与防控路径。研究表明引入大数据分析、人工智能算法、区块链技术等智能化手段，得以构建包含交易行为监测、风险特征识别、异常模式预警、协同响应处置的全流程智能风控体系，在此基础上本文设计了多维系统化防控路径，为提升电子商务财务安全水平、促进数字经济健康发展提供理论支撑和实践指引。

关键词

网络支付，电子商务，财务风险，智能识别，风险防控

Research on Intelligent Identification and Prevention Pathways for Financial Risks in E-Commerce under Online Payment Scenarios

Kun Jin

Financial Department, University of Shanghai for Science and Technology, Shanghai

Received: October 30, 2025; accepted: November 14, 2025; published: December 11, 2025

Abstract

With the deep penetration of online payment in the e-commerce domain, the convenience of online

文章引用: 金锟. 网络支付场景下电子商务财务风险智能识别与防控路径研究[J]. 电子商务评论, 2025, 14(12): 1697-1703. DOI: 10.12677/ecl.2025.14124041

transactions and the complexity of financial risks have increased synchronously. Drawing on financial risk management theory and intelligent decision-making theory, this study delves into the intelligent identification and prevention pathways for financial risks in e-commerce under online payment scenarios. The research demonstrates that the integration of intelligent tools such as big data analytics, artificial intelligence algorithms, and blockchain technology enables the construction of a comprehensive intelligent risk control system encompassing transaction behavior monitoring, risk feature identification, anomalous pattern alerting, and coordinated response handling. Building on this foundation, the study designs multidimensional systematic prevention pathways, thereby providing theoretical support and practical guidance for enhancing the financial security of e-commerce and promoting the healthy development of the digital economy.

Keywords

Online Payment, E-Commerce, Financial Risks, Intelligent Identification, Risk Prevention

1. 引言

网络支付作为电子商务价值实现的关键环节，已成为连接消费者、商户、金融机构的核心纽带[1]。从早期的网上银行转账到当前移动支付的全面普及，线上支付方式的迭代升级深刻改变了商业交易的时空结构与资金流转模式。在企业电子商务领域，线上支付不仅覆盖 B2C、C2C 等零售场景，更延伸至 B2B 采购、供应链金融等产业互联网场景，成为企业资金管理与财务运作的重要载体[2]。在高校等事业单位，网络支付同样呈现快速发展态势，学费缴纳、科研经费支付、校园消费等场景的线上化水平显著提升，财务管理的网络化转型不断深化。

然而，网络支付在带来效率革命的同时，也催生了新型财务风险的集聚与扩散。近年来，网络支付领域的财务风险事件频发，从个人账户盗刷、商户恶意套现，到第三方支付平台资金池风险、跨境支付洗钱风险，风险形态呈现多样化与复杂化趋势。在企业层面，恶意退款、刷单套现、虚假交易等风险行为侵蚀企业利润，扰乱市场秩序；在高校等机构层面，科研经费网络支付中的虚假报销、资金挪用等问题影响了财政资金使用效益，损害了公共利益[3]。

基于上述情况，本文重点关注网络支付场景下电子商务财务风险这一关键问题，深入分析智能化技术如何为电子商务财务风险的精准识别和实时预警发挥赋能作用，同时探讨如何设计系统化的风险防控路径来保障电子商务线上交易的财务安全，目的是丰富网络支付和财务风险管理方面的理论研究，并为电子商务交易主体以及监管部门提供决策方面的参考依据。

2. 理论基础

2.1. 财务风险管理理论

财务风险管理理论属于企业财务管理学范畴，它的核心是应用系统化方法识别并应对可能影响财务目标实现的不确定性因素，传统财务风险理论主要关注市场、信用、流动性和操作等类型的风险，强调通过分散、转移和规避等策略降低财务风险[4]。

在网络支付场景下，财务风险所体现出的新形式与新特征对传统的风险管理理论构成了新挑战——

网络交易的虚拟特性加大了交易主体信用风险的识别难度[5]，线上支付的即时性与不可逆性使得传统的事后补救机制难以发挥作用，操作风险一旦发生就很有可能无法挽回损失，第三方支付平台介入则改变了传统电商的资金流转路径，催生出平台沉淀资金风险和技术风险等新型风险[6]。所以需要在传统财务风险管理理论的基础上，结合网络支付的技术特征与业务逻辑来完善适用于线上场景的财务风险管理理论。

2.2. 智能决策理论

智能决策理论着重借助数据分析、算法优化以及模型构建等技术手段，以此提升决策的科学性、精准性以及时效性，从而达成从经验决策向数据驱动决策的转变[7]。在财务风险管理领域，智能决策理论的应用主要体现在风险识别的自动化、风险评估的量化、风险预警的实时化以及风险应对的智能化等方面[8]。

就网络支付的财务风险管理来看，智能决策理论的价值具体体现在：在数据层面依靠整合多源数据构建全景式风险感知体系，以弥补单一数据源局限；在算法层面组合使用多种算法以应对不同类型风险的识别需求，同时提升风险判断准确率；在系统层面通过构建实时计算平台与智能决策引擎，实现风险的秒级识别与自动化处置，以满足线上交易高并发、低延迟的实际要求[9]。需要注意的是，智能决策并非完全由智能系统替代人工判断，而是通过人机协同来整体提升决策质量，机器所处理的是标准化风险，而复杂疑难风险则交由人类专家进行研判。

3. 电子商务财务风险智能识别机制构建

3.1. 基于交易行为分析的异常识别机制

交易行为是体现电子商务财务风险的重要载体，借助对于线上交易行为数据的深度分析，智能识别机制能够发现隐藏的风险信号，并在海量交易数据中捕获正常交易与异常交易在行为模式上的差异。

在企业电商场景里，正常交易一般均具备相对稳定的供应商选择与合理的采购周期等特征，若某笔交易涉及之前从未合作过的供应商、采购金额远超历史水平、采购时间异常集中，就有可能存在虚假交易或舞弊嫌疑；在 C2C 场景里，正常消费者购物行为通常具有一定规律性，如果其账户在短时间内连续进行大额转账、转账对象频繁变化、且交易设备与常用设备不符，则有可能存在账户被盗用的风险；在高校报销场景里，科研经费的正常支付通常与科研进度及合同约定相匹配，如果某个项目在短期内集中报销大量费用、报销凭证格式异常统一、报销商户高度重复，则有可能存在虚假报销风险。

机器学习算法在交易行为异常识别过程中起到了核心作用，其中监督学习算法借助对标注的历史欺诈案例开展训练，学习欺诈交易的行为特征并构建分类模型来对新交易进行风险判断，无监督学习算法则通过对未标注数据进行聚类分析，发现数据当中的异常点与离群值以揭示其可能对应的潜在风险交易。需要强调的是，交易行为分析不应局限于单笔交易的静态特征，更要关注交易序列的动态模式，如多个看似独立的账户之间若存在频繁的资金往来，则有可能构成线上洗钱或套现的资金链条，通过构建交易网络图谱并应用关键节点识别等算法，能够揭示出这些隐蔽的关联关系[10]。

3.2. 基于多维特征融合的风险评估机制

单一维度的数据分析很难全面刻画电子商务财务风险的复杂性，因此需要整合多源数据来构建立体化的风险评估体系。在网络支付场景下，除交易行为数据之外还有用户属性数据、网络行为数据、外部信用数据等多种数据源，这些数据从不同角度反映出交易主体的风险特征，其中用户属性特征包含用户的注册信息、实名认证信息、历史信用记录等，这些静态特征反映了用户的基本风险水平；网络行为特征涵盖用户的浏览轨迹、点击行为、停留时长等线上操作数据，这些数据能够反映用户的真实意图与行

为习惯；外部信用数据则来源于第三方征信机构、行业黑名单、公共信用信息平台等，这些数据提供了用户在更广泛范围内的信用表现[11]。

基于多维特征融合，可以构建精细化的风险评分体系。对每笔交易计算综合风险分值，根据分值高低划分风险等级，对不同风险等级采取差异化的处置策略——低风险交易自动放行，高风险交易拦截或转人工审核，中等风险交易采取增强验证措施。动态风险评分机制能够根据用户的实时行为不断更新风险判断，当用户风险水平发生显著变化时及时调整风控策略。这种精细化、动态化的风险评估机制，既能有效识别风险，又能避免对正常电子商务交易的过度干扰，在安全与体验之间实现平衡。

3.3. 基于智能预警的实时监控机制

风险识别的时效性直接影响应对电子商务财务风险的效果，在网络支付的高频交易场景下，实时监控与即时预警至关重要。传统的事后审计模式虽然能够发现风险，但往往损失已经发生，事后追偿难度大、成本高。智能预警机制通过对交易流的实时监测与分析，在风险发生的第一时间触发警报，为风险处置争取宝贵时间。

实时监控系统需要处理海量的并发交易请求，这对系统的计算能力与响应速度提出了极高要求。在网络支付场景下，需要将规则引擎与模型引擎结合应用，以实现运用简单规则进行快速判断与运用复杂模型进行精准预测的有机统一[12]。在企业电商场景中，对大额支付、新供应商首笔交易、异地登录后的支付等高风险操作可设置实时预警；在高校财务场景中，对单日报销金额异常增高、集中报销大量小额发票、报销时间与项目进度不符等情况可设置预警。预警信息应及时推送给相关责任人，通过短信、邮件、系统消息等多种渠道确保信息送达，并提供必要的风险要素与处置建议，帮助决策者快速判断与响应。同时，每一次预警的处置结果都应回流到系统中，作为模型优化的训练数据以实现自我学习和持续改进，不断提升预警系统的准确性。

3.4. 基于区块链技术的交易溯源机制

区块链技术凭借其特有的去中心化、不可篡改以及可追溯等特性，为网络支付的财务风险识别提供了全新技术手段。传统电子商务支付系统的交易记录通常存储在中心数据库里，存在被篡改或者删除的潜在风险，并且不同机构之间的数据难以实现有效共享与验证。区块链运用分布式账本技术，让交易记录由多个节点共同进行记录与验证，任何一方都无法单方面篡改历史记录，这为交易的真实性提供了技术层面的保障。在涉及多方的复杂电子商务交易场景中，区块链所具有的交易溯源价值显得尤为突出[13]。

智能合约属于区块链技术的重要应用形式，通过把业务规则与风控逻辑编码成为可以自动执行的程序，实现了风险控制的自动化与去信任化。在网络支付过程中，可以将支付条件、限额规则以及审批流程等嵌入智能合约，当满足预设条件时便自动触发支付，若不满足则拒绝交易。这种自动执行机制避免了人为干预所存在的随意性，提升了风险控制的刚性与可靠性。在高校科研经费管理工作中，可以将经费使用范围、支出比例限制以及审批权限等规则写入智能合约，当科研人员发起线上支付时，智能合约自动检查是否符合经费管理规定，不符合规定的支付会自动被拒绝，从而有效防范经费违规使用的风险。

4. 电子商务财务风险系统化防控路径设计

4.1. 技术嵌入路径

技术嵌入路径强调将智能风控技术深度融入网络支付的业务流程，实现风险防控的无缝化与自动化。技术嵌入不是简单的技术叠加，而是要基于业务逻辑重构支付流程，让风险识别成为支付过程的内生环节[14]。在支付发起阶段，应嵌入身份认证技术，通过多因子认证和生物特征识别等手段确认支付人的真

实身份，防止账户冒用；在支付处理阶段，应嵌入实时风控引擎，对每笔交易进行毫秒级的风险评分与决策。支付请求在到达清算系统前，先经过风控引擎的检查，根据风险评分结果决定是否放行。对于识别为高风险的交易，可以采取延迟到账、人工审核、要求补充验证等干预措施。这种实时拦截机制能够在资金真正流出前阻断风险，最大限度减少损失。在支付完成后，应嵌入交易监控系统，对已完成的交易进行事后分析，发现可疑的交易模式。事后监控虽然无法阻止单笔交易的风险，但能够发现系统性的风险趋势与欺诈网络，为风险规则的优化提供依据。

企业与高校应根据自身的业务规模与风险特征，选择适配的技术方案，大型企业与平台可以自建完整的风控技术体系，中小企业与高校可以采购第三方风控服务，通过 API 接口嵌入自身的支付系统。技术嵌入是一个持续迭代的过程，随着风险形态的演化与技术的进步，需要不断升级风控技术，保持技术防护能力与风险挑战的动态适配。

4.2. 制度重构路径

技术手段需要与制度安排相结合方能发挥最大效能，因此制度重构路径强调通过完善内部控制制度、优化财务管理流程、明确责任边界等制度性安排，为网络支付风险防控提供组织保障与规则约束。内部控制制度是财务风险管理的基础，在网络支付场景下，需要针对线上支付的特点重新设计内部控制流程。不相容职务分离原则在网络环境中同样适用，支付发起、审批、执行、核对等环节应由不同人员或不同系统模块负责，形成相互制约[15]。

在企业电商场景中，应建立多级审批制度，根据支付金额、支付对象、支付紧急程度等因素设置差异化的审批流程。小额日常支付可以授权一线人员审批，大额重要支付需要经过财务负责人乃至企业负责人审批。审批流程应在线上系统中固化，通过工作流引擎实现审批流转的自动化，审批记录全程留痕便于事后追溯。在高校财务场景中，应完善科研经费网络支付的管理制度，明确不同类型经费的使用范围、审批权限、报销标准。科研人员通过线上系统发起报销申请时，系统自动检查是否符合经费管理规定，不符合的申请无法提交。财务部门对线上报销进行审核时，应重点核查电子凭证的真实性与合规性。

在制度建设方面，要着重关注应急处置机制的完善，以便在发生重大支付风险事件时能快速启动应急响应流程，及时止损并且追溯相关责任，同时要建立风险事件的复盘机制，对每次风险事件的发生原因、处置过程以及改进措施进行系统总结，把经验教训转化为制度优化与流程改进的动力，内部审计部门需定期对网络支付的风险防控制度执行情况进行检查，及时发现制度漏洞与执行偏差来推动制度持续完善。此外，还需要高度重视人员管理与教育培训，因为网络支付的风险防控最终依靠人来执行，人员的风险意识与专业能力直接影响制度落实效果，要加强对财务人员、业务人员的风险教育，提升他们对网络支付风险的认知水平与防范意识，对于高风险岗位人员要建立定期轮岗制度，避免权力过度集中带来道德风险，对于违反风险管理制度的行为要建立明确的责任追究机制，通过问责强化制度的约束力。

4.3. 流程优化路径

流程优化路径着重于对网络支付业务流程进行系统梳理和再造，以此消除流程里的风险隐患与管理漏洞，进而提升流程的规范性和风险可控性。流程优化的首要步骤是开展流程梳理工作，要全面识别网络支付所涉及的各个环节并绘制出完整的流程图，在进行流程设计时，应当遵循简洁高效和风险可控相结合的原则，依据不同支付场景的风险特征来设计差异化的流程，对于小额高频的日常支付可简化流程从而提升效率，对于大额低频的重要支付则需设置更为严格的审核环节，在整个流程当中还应嵌入关键控制点，借助自动化的风险检查确保每个控制点都能得到有效执行[16]。

流程优化路径需重点关注线上线下流程衔接，线上支付在网络支付的众多场景里仅仅是完成了资金

划转，后续还有实物交付等线下环节，若线上线下流程衔接不畅就有可能产生新的风险。针对这一情况，应建立线上支付与线下业务关联机制，保证支付信息准确传递到后续环节以避免信息断层。具体而言，企业电商在线上支付完成后应自动触发库存更新和物流发货等后续流程，高校财务在线上报销完成后则应自动生成会计凭证并更新项目预算余额。

流程优化路径还需要基于数据分析来持续评估流程的效率指标和风险指标，及时发现耗时过长、审批通过率过低等流程设计上可能存在的问题，并在此基础上依据数据反馈不断调整优化流程参数，按照业务发展和风险态势变化持续迭代，以保持流程的适应性和先进性。

4.4. 生态协同路径

网络支付风险防控仅仅依靠某一主体的独自努力很难达成，需要构建多方协同的风险防控生态体系。因此，生态协同路径通过平台、商户、用户、监管机构等电子商务多元主体之间的协作联动来形成风险防控合力。在数据协同领域，不同主体掌握着不同维度的风险信息，借助数据共享能够构建更全面的风险视图。具体而言，支付平台掌握着资金流数据，电商平台掌握着交易行为数据，物流平台掌握着商品流数据，把这些数据整合分析可更为精准地识别欺诈行为，但数据共享面临隐私保护与商业竞争双重约束，需要在合规框架下探索数据共享可行模式[17]。

在规则协同层面，应推动行业风控标准统一，防止不同平台的风控规则差异被欺诈者利用。对此，行业协会可发挥协调作用，组织制定网络支付风险分类标准、评估方法及处置流程等行业规范，以此提升整个行业的风险防控水平，同时要建立跨平台的欺诈账户黑名单库，一旦某个账户在一个平台实施欺诈被识别，其他平台能及时发出预警。

在监管协同层面，监管部门需要加强对网络支付财务风险的监测与引导，通过建立网络支付财务风险监测平台来实时掌握行业风险态势，针对系统性风险要做到及时预警。面对新型风险与新型欺诈手段，监管部门要及时发布风险提示以指导企业与机构加强防范，并不断完善网络支付的法律法规体系，明确参与各方的责任和义务，加大对违法违规行为打击力度来营造良好市场环境，企业与高校应当主动配合监管部门的检查与指导，及时报告重大风险事件。

在用户教育层面，提升用户的风险防范意识亦是生态协同的重要环节，很多风险事件发生是因为用户风险意识太过淡薄，给了欺诈者以可乘之机。对此，电子商务平台与机构要加强用户安全教育，通过多种渠道普及网络支付安全知识，提醒用户注意保护个人信息与支付账户安全，当用户出现高风险操作情况时，系统要及时弹出风险提示来引导用户谨慎操作，同时要建立便捷的风险举报与投诉渠道，鼓励用户发现风险时及时报告，以形成全民参与的风险防控格局。

5. 结语

本文依据财务风险管理理论和智能决策理论，系统探讨了网络支付场景下电子商务财务风险的识别与防控问题。结果表明：借助大数据分析、人工智能算法、区块链技术等智能化手段，能够构建基于交易行为分析、多维特征融合、智能实时预警、区块链溯源的全方位智能识别机制，从而显著提升电子商务财务风险识别的精准性和时效性。在此前提之下，本文提出技术嵌入、制度重构、流程优化、生态协同四位一体的系统化防控路径，为网络支付风险的有效防控提供理论框架与实践指引，致力于在技术创新与制度完善的双轮驱动之下持续提升电子商务财务安全水平，为数字经济的健康发展保驾护航。

参考文献

[1] 许军. 面向大数据的移动网络支付安全与对策分析[J]. 电信快报, 2025(1): 44-47.

[2] 刘昕. 融合支付在多元化场景中的应用研究[J]. 上海企业, 2025(10): 70-72.
[3] 杨萌. 网络环境下事业单位财务风险防控策略[J]. 合作经济与科技, 2025(7): 161-163.
[4] 冀奕博. 新时代背景下财务风险管理的理论与实践[J]. 中国商界, 2025(2): 140-141.
[5] 谢潇. 数字经济视阈内网络虚拟财产的识别标准与类型构造[J]. 法商研究, 2025, 42(3): 49-65.
[6] 张健维. 互联网财务模式下的企业财务风险管理[J]. 产业创新研究, 2025(12): 139-141.
[7] 董玉成, 范莎, 陈霞, 等. 诺贝尔经济科学奖与决策理论及其对数据驱动智能决策的研究启示[J]. 管理科学学报, 2025, 28(4): 174-190.
[8] 赵军. 人工智能在财务管理中的应用与智能决策支持研究[J]. 中国市场, 2025(11): 159-162.
[9] 李茉. 数据驱动模式对智能财务决策精准度的影响研究[J]. 现代营销, 2025(24): 140-142.
[10] 袁富江, 梁波, 武琦, 等. 基于多层感知机模型的金融交易洗钱风险预测[J]. 金融科技时代, 2025, 33(3): 23-29.
[11] 蔡晓华. 基于机器学习的异常流量检测在智慧审计中的应用研究[J]. 网络安全和信息化, 2025(5): 54-56.
[12] 刘静. 基于网络安全的移动支付系统设计[J]. 信息与电脑(理论版), 2024, 36(7): 209-211.
[13] 张煜, 王昊, 叶昊. 区块链技术在网络安全中的应用与挑战[J]. 网络安全技术与应用, 2025(9): 19-23.
[14] 史官清, 赵倚林, 黄婉秋. 智能技术嵌入管理沟通的发展脉络、双向影响与强化路径[J]. 上海管理科学, 2025, 47(5): 45-49.
[15] 施志晖, 陆岷峰. 从稳定币到数字货币桥: 跨境支付体系的制度重构与中国企业的应对策略[J]. 改革与战略, 2025, 41(4): 185-194.
[16] 商俊凤. 大数据技术在企业财务决策流程优化中的应用[J]. 商业文化, 2025(11): 119-121.
[17] 杨一军. 支付数据安全生态化治理与技术迭代演进[J]. 中国信用卡, 2025(6): 38-43.