E-Commerce Letters 电子商务评论, 2025, 14(11), 3144-3150
Published Online November 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14113790

Hans汉斯

区块链智能合约对电子商务的效能优化分析

刘　欢

浙江理工大学法学与人文学院，浙江　杭州

收稿日期：2025年10月10日；录用日期：2025年10月28日；发布日期：2025年11月28日

摘　要

本文旨在系统分析智能合约对电子商务的效能优化作用及其面临的挑战。研究表明，智能合约通过其自动化执行、去中心化与不可篡改的技术特性，在商品溯源、支付结算及构建自治市场等核心环节能有效提升交易效率与透明度，推动电商模式从“平台中介”向“协议中介”的范式转变。然而，其广泛应用仍受限于技术瓶颈、法律监管不确定性及消费者权益保护难题。为此，本文提出应从技术完善、法律规制与标准建设三个层面协同推进，以促进智能合约在电子商务领域的健康与可持续发展。

关键词

智能合约，电子商务，去中心化，法律规制

Analysis of Efficiency Optimization in E-Commerce through Blockchain Smart Contracts

Huan Liu

School of Law and Humanities, Zhejiang Sci-Tech University, Hangzhou Zhejiang

Received: October 10, 2025; accepted: October 28, 2025; published: November 28, 2025

Abstract

This paper aims to systematically analyze the efficiency optimization effects of smart contracts in e-commerce and the challenges they face. Research indicates that, through features such as automated execution, decentralization, and tamper resistance, smart contracts can significantly enhance transaction efficiency and transparency in key areas like product traceability, payment settlement, and the construction of autonomous markets. This drives a paradigm shift in e-commerce from “platform intermediation” to “protocol intermediation”. However, widespread application remains

文章引用: 刘欢. 区块链智能合约对电子商务的效能优化分析[J]. 电子商务评论, 2025, 14(11): 3144-3150.
DOI: 10.12677/ecl.2025.14113790

constrained by technical bottlenecks, regulatory uncertainties, and challenges in consumer protection. Therefore, this paper proposes a coordinated approach across three dimensions—technical refinement, legal regulation, and standard development, to promote the healthy and sustainable integration of smart contracts in the e-commerce sector.

Keywords

Smart Contracts, E-Commerce, Decentralization, Legal Regulation

1. 引言

传统的电子商务模式高度依赖中心化平台(如淘宝、亚马逊)作为信任中介，处理交易撮合、资金托管与信用担保。此模式虽促进了电商的早期发展，但也引发了高额佣金、数据垄断、单点故障风险以及议价能力失衡等问题。区块链技术的大规模普及不仅极大地改变了传统的交易模式[1]，还催生了一批依托区块链技术的各种应用，其中，智能合约(smart contract)无疑是最成功的应用之一。作为一种运行在区块链上的分布式应用[2] [3]，随着区块链技术的成熟，智能合约作为一种可编程、自动执行的数字化协议，为构建去中心化、高效透明的新型电商生态系统提供了潜在解决方案。智能合约的核心价值在于通过代码逻辑降低信任成本，实现交易流程的自动化。然而，其在电商领域的应用仍处于探索阶段，面临技术可靠性、法律定性及监管适配性等多重挑战。基于此，本研究旨在系统回答以下核心问题：智能合约如何通过其技术特性优化电子商务的核心流程？其在落地过程中面临哪些关键挑战？以及如何通过多维度对策推动其健康发展？本文将通过剖析智能合约的技术原理与应用场景，并针对性地提出治理框架，以期为相关理论与实践提供参考。

2. 智能合约的核心原理与对电子商务的价值

(一)、智能合约的技术原理与核心特征

智能合约的概念最早于 20 世纪 90 年代由计算机科学家兼密码学家尼克·萨博提出。他将智能合约界定为“一套以数字化形式定义的承诺，涵盖合约参与方能够在其上执行这些承诺的协议”。然而，直至区块链技术发展成熟，尤其是以太坊平台问世，这一构想才得以切实付诸实践。

1) 智能合约的自动化执行

智能合约本质上是部署在区块链上的一些可执行代码，可不依赖中心机构自动代表各签署方执行合约[4]智能合约的自动化执行，指的是将合约条款编码为特定程序代码，部署于去中心化或分布式账本之上，在预设条件被触发时，由计算机网络节点无需中介干预而自主、确定性地执行相应操作的计算范式。智能合约的自动化执行，本质上是将合同条款编码为确定性代码并部署于区块链上，在预设条件触发时由网络节点自动执行。这一机制将传统合约的“被动执行”转变为“主动履行”，显著降低了执行成本与信任摩擦。其技术基础是区块链的共识机制，确保所有节点对执行结果的一致性确认。从学术视角看，这代表了一种从“被动执行”到“主动履行”的范式转变。传统法律合约依赖于缔约方的诚信与第三方权威机构(如法院、银行)的监督与强制执行，其执行是事后的、被动的且成本高昂。而智能合约通过将“承诺”内化为“代码逻辑”，并与数字资产(如加密货币、通证化资产)直接绑定，实现了合约义务的“事前

嵌入”与“事中自执行”，从而在特定领域内极大地降低了信任成本与执行摩擦。智能合约在本质上是运行于区块链之上的一个确定性状态机。其内部状态(存储的数据)和状态转移函数(合约函数)对所有网络节点公开且一致。当一笔有效交易(即“输入”)调用合约函数时，所有验证节点会基于相同的初始状态和输入数据，独立地执行代码，并必须就最终的状态变更达成共识。这种确定性是自动化执行结果可信的基础。智能合约的刚性自动化执行引发了关于“代码即法律”的哲学与法学辩论。支持者认为这实现了最高程度的规则客观性。反对者则指出，代码可能包含漏洞或无法涵盖现实世界的复杂性与例外情况，导致不公正的结果。因此，学术界正在探索将柔性治理、争端解决机制与自动化执行相结合的“混合智能合约”。

智能合约的自动化执行，作为一种革命性的合约履行机制，通过将信任从个体和机构转移至密码学与分布式共识算法，为构建可编程经济与去中心化应用奠定了基石。它体现了“执行即验证”的新型计算范式，在提升效率、降低信任成本方面具有巨大潜力。然而，其发展仍面临技术可靠性、法律合规性以及与现实世界复杂系统融合的挑战。

2) 智能合约的去中心化

智能合约的去中心化，并非一个单一维度的概念，而是一个在架构、控制权和信任模型上实现从单点集权向多点分布的系统性范式转移。它指的是智能合约的部署、验证、执行与状态维护的全过程，并非由单一中心化实体掌控，而是由一个分布式的节点网络，通过共识机制协同完成。智能合约的去中心化体现在其部署、验证与执行过程由分布式网络共同维护，而非单一中心化实体控制。通过共识算法与密码学技术，它将传统由中介机构掌握的信任权力分散至整个网络，从而构建了一个高容错、抗单点故障的信任环境。其核心内涵在于，将传统合约中由“可信第三方”所垄断的权力(如解释权、仲裁权、执行权)，解构并分散到整个网络之中，最终通过算法与密码学来重构信任。这创造了一种全新的、不依赖于特定机构背书的客观信任环境智能合约的代码与数据在成千上万个网络节点上进行冗余存储。不存在一个中心化的数据中心或服务器，单个或部分节点的故障不会导致整个合约系统的瘫痪，从而具备了极高的容错性和抗单点故障能力。一旦智能合约被部署到区块链上，其代码逻辑在绝大多数情况下(除非预设了可升级机制)对于包括创建者在内的任何一方都无法被修改或删除。这消除了中心化机构单方面变更规则的可能性。合约的执行由预设条件和公开交易触发，无需经过任何中央网关的审批。控制权从“人治”转移到了“代码自治”。对于合约的关键参数修改或升级，可能通过去中心化自治组织(DAO)进行社区治理投票来决定，而非由开发团队单独决策[4]。

(二)、对电子商务的价值

传统电子商务建立在“平台中心化”范式之上。平台(如 Amazon、阿里)作为强大的中介，聚合流量、制定规则、处理支付、解决纠纷，并因此收取高额佣金、掌控核心数据。智能合约引入的颠覆性价值在于，它使得一种新的“去中心化协议”范式成为可能。在这种范式下，电子商务不再由一个中心化组织运营，而是由一系列开源、透明的智能合约作为底层协议，自动化地执行交易规则，并将权力和价值返还给生态参与者[5]。降低信任成本无需完全依赖平台信用背书，买卖双方可直接建立信任。自动化流程消除了中间环节，实现了“交易即结算”。加密技术和分布式账本有效防止了数据篡改和欺诈行为。催生了去中心化市场、微支付、资产通证化等新业态。

3. 智能合约在电子商务中的核心应用场景

(一)、商品溯源与防伪

传统商品溯源与防伪系统面临核心痛点在于中心化信任危机。数据存储于企业或机构的私有数据库中，存在被篡改、伪造或选择性披露的风险。消费者难以验证信息的真实性，整个链条的透明度不足。

智能合约结合区块链技术，为此带来了一场信任范式转变。它通过构建一个去中心化、不可篡改、可程序化验证的信任基础设施，将商品的“物理流”与信息的“数据流”不可分割地绑定在一起，实现了从“机构信任”到“算法信任”的跨越。为每一件商品或每一批次商品赋予唯一的数字身份，通常以非同质化通证(NFT)或具有唯一标识符的数字化形式存在。该身份与物理世界的锚点(如二维码、RFID、NFC芯片的物理 ID)紧密绑定。初始化上链：商品的生产商作为信任起点，将核心元数据(如原料来源、生产时间、地点、批次号)与该数字身份关联，并作为初始交易记录在区块链上，创建了商品的“数字孪生”[3]。商品在整个供应链中的流转(如出厂、报关、物流、入库、上架)被视为一系列状态转移事件。每个参与方(如物流商、经销商)通过其私钥对商品状态的变更进行签名确认，并将关键信息(如时间、地点、操作者)作为新的交易写入链上。在此过程中，智能合约充当了业务规则执行器和状态守护者。从生产、仓储、物流到销售的每一个环节，信息都被记录在链[6]。智能合约将物流信息与支付条件绑定。当消费者确认收货时，区块链上的信息可作为其验真凭证，同时自动触发支付给卖家，解决了信息不透明问题，有效打击了假冒伪劣品。

(二)、自动化的支付与结算

智能合约在自动化支付与结算中的应用，指的是利用其状态驱动、条件触发的自动化执行能力，对金融合约中支付与结算条款进行编码，从而在满足预设条件时，无需人工干预即可自主、精确地完成价值的转移与所有权的变更。买家下单后，货款被锁定在智能合约中。物流系统将包裹送达并由买家签收后，GPS 或 IoT 设备数据作为触发条件，通知智能合约自动将货款释放给卖家[2]。若超时未收货，合约可自动退款。这代表了对传统支付结算范式的一场深刻革命。传统范式依赖于一系列中介机构(如银行、清算所、证券交易所)进行对账、清算和结算，流程冗长、成本高昂且存在操作风险与对手方风险。智能合约通过将清算逻辑(计算各方头寸)与结算动作(完成资产交割)合二为一，并置于一个确定性的执行环境中，实现了“交易即结算”的理想模式，极大地提升了效率并降低了风险。

智能合约的核心是将复杂的商业逻辑编码为确定性的“if-then”规则。智能合约最革命性的特性之一——原子性。在一次合约调用中，多个操作(如“从 A 账户扣款”和“向 B 账户转账”)被捆绑为一个不可分割的原子单元。要么所有操作全部成功，要么全部回滚，不存在任何中间状态。这彻底消除了本金风险，即一方已支付款项但未收到对应资产的风险。构建了真正的“货到付款”体验，无需第三方托管，资金效率更高。智能合约通过将支付与结算逻辑编码为具有确定性的自动化程序，正在重塑全球价值转移的范式。它通过原子性、透明性和无需许可的特性，创造了一个更高效率、更低风险、更具包容性的金融基础设施。

(三)、去中心化的自治市场

中心化自治市场电商平台，是基于区块链与智能合约构建的、不由中心化组织运营，而是由预先编码的规则和社区治理来驱动的在线交易市场。它旨在消除传统电商平台(如 Amazon、阿里巴巴)作为中心化中介所带来的高额佣金、数据垄断、单边规则制定及审查等问题。智能合约在此扮演了平台底层协议和自动化仲裁者的角色，实现了从“公司制平台”到“社区制协议”的范式转变。其核心是创建一个可信的中立基础设施工厂让买卖双方能够以点对点的方式进行可信交易。基于智能合约构建完全去中心化的电商平台(如 OpenSea)。平台规则由代码定义，交易由合约自动执行，佣金极低甚至为零，社区通过投票参与治理。一个完整的去中心化电商平台由一系列相互协作的智能合约模块构成，每个模块负责特定的功能，共同替代传统平台的中心化服务。

用户(买卖双方)使用其区块链钱包地址作为全局身份，无需在中心化服务器注册，智能合约将交易历史、评价等信誉数据通证化(如以 SBT——灵魂绑定通证的形式)，并存储在链上或去中心化存储网络(如IPFS)中。信誉数据是用户的自有资产，可跨平台移植，打破传统平台的“数据孤岛”。合约可自动计算

并更新信誉分数。每个上架的商品可以表示为一个 NFT 或同质化通证，其中元数据(图片、描述)存储在 IPFS 上，所有权和唯一性由区块链保障。卖家通过调用智能合约函数，支付少量 Gas 费即可上架商品，无需平台审核(在合规框架内)。列表信息全局可见、不可篡改。这是实现“自治”的关键。智能合约本身无法判断是非，但它可以程序化地接入去中心化争议解决协议。当争议发生时，智能合约将案件随机分配给一群匿名的陪审员(由代币持有者或专业解决者扮演)。陪审员在链下评估证据，并在链上进行投票。智能合约根据投票结果，自动执行资金的分配(如全额退款、部分退款等)。这实现了基于算法的仲裁执行。

4. 智能合约在电子商务应用中面临的挑战

(一)、技术瓶颈

代码漏洞与安全性：合约代码一旦部署难以修改，任何漏洞都可能被黑客利用，导致巨额资产损失。代码漏洞的存在，源于智能合约编程的复杂性与开发者的经验差异。部分合约因逻辑设计缺陷或未充分考虑边界条件，易成为攻击目标。例如，重入攻击利用合约在执行过程中的状态不一致性，通过递归调用窃取资金；整数溢出则可能导致计算结果错误，引发意外行为。安全性问题还涉及密码学算法的选择与实现，若采用已被证明不安全的算法或密钥管理不当，同样会威胁合约安全。此外，智能合约与区块链底层协议的交互也可能引入风险，如共识机制的分叉或网络延迟，可能导致合约执行结果的不确定性。

性能与可扩展性：区块链网络的吞吐量与延迟限制了智能合约的处理能力。以以太坊为例，其每秒处理交易数(TPS)有限，难以支撑大规模电子商务应用的高并发需求。当交易量激增时，网络拥堵导致 Gas 费飙升，增加了合约执行成本。此外，智能合约的存储与计算资源消耗也制约了其复杂性。复杂的商业逻辑需要更多的状态存储与计算步骤，可能超出区块链节点的处理能力，导致执行失败或延迟。可扩展性解决方案如分片技术、状态通道与 Layer 2 扩容方案虽在发展中，但尚未完全成熟，无法满足所有场景的需求。

互操作性与标准化：电子商务涉及多方参与与复杂流程，智能合约需与多种系统(如支付网关、物流系统、ERP)交互。然而，当前智能合约平台(如以太坊、EOS)与外部系统的互操作性有限，缺乏统一的标准与接口。不同区块链网络之间的互操作性问题更为突出，跨链通信与资产转移仍面临技术障碍。此外，智能合约的编程语言(如 Solidity)与开发工具缺乏标准化，导致合约质量参差不齐，增加了集成与维护的难度。标准化组织的努力(如 ERC 标准)虽在一定程度上促进了生态统一，但整体互操作性仍需进一步提升。

(二)、法律与监管困境

法律主体地位不明确：智能合约是否构成法律意义上的“合同”？其自动执行的性质如何与《民法典》中的合同撤销、变更等条款协调？在现行法律框架下，智能合约的“代码即法律”特性与传统合同法的人为主观判断存在根本冲突。当合约条款因外部环境变化(如政策调整、不可抗力)需要修改时，自动化执行的刚性可能引发法律争议。

监管适配性不足：智能合约的去中心化特征与现有金融监管的“机构主体”监管模式存在矛盾。传统监管要求明确责任主体(如银行、支付机构)，但智能合约的代码开发方、部署方、使用方往往分散且难以追溯。例如，某去中心化交易所的智能合约因代码漏洞导致用户资产损失，监管机构难以确定责任方是开发者、审计方还是用户自身。此外，跨境智能合约应用的监管套利问题突出，不同司法管辖区的规则差异可能导致“监管洼地”效应。

证据认定难题：智能合约的执行记录存储在区块链上，其作为电子证据的合法性、真实性认定存在障碍。虽然区块链的不可篡改特性理论上可保证数据完整，但司法实践中对“链上证据”的采信标准尚未统一。例如，某合同纠纷中，一方主张链上交易记录被篡改，但法院因缺乏技术鉴定能力而难以判别。

此外，智能合约的代码逻辑透明性可能涉及商业秘密保护问题，如何在举证时平衡透明度与保密性需法律进一步明确。

5. 推动智能合约在电子商务中发展的对策建议

(一)、技术层面

针对代码漏洞与安全性问题，需建立严格的智能合约开发规范与审计机制。推行代码审查标准化流程，要求开发者遵循最佳实践(如输入验证、边界检查)，并引入第三方安全审计公司对合约进行全面渗透测试。同时，开发智能合约保险产品，为高风险合约提供资产损失补偿，降低开发者与使用者的后顾之忧。在性能与可扩展性方面，应推动分层架构设计，将高频交易与复杂计算剥离至 Layer 2 网络，减少主链负担。例如，采用状态通道技术实现买卖双方间的离线交易，仅在争议发生时提交主链仲裁。此外，支持跨链互操作协议(如 Polkadot、Cosmos)的开发，使智能合约能调用其他区块链的资产与数据，拓展应用场景。对于互操作性与标准化，需由行业协会牵头制定统一接口标准，明确智能合约与外部系统(如支付网关、物流 API)的数据格式与通信协议。鼓励开源社区开发通用合约模板库(如 ERC-20 代币标准)，降低开发者重复造轮子的成本。同时，推动编程语言与开发工具的标准化，例如将 Solidity 升级为更安全的版本，或推广形式化验证工具，通过数学证明确保合约逻辑无漏洞。

(二)、法律与监管层面

针对法律主体地位不明确的问题，需推动立法机关明确智能合约的法律效力。可通过修订《民法典》合同编或出台专门司法解释，界定智能合约在合同成立、生效、履行及违约救济中的法律地位。例如，规定智能合约可作为书面合同的电子形式，其自动执行条款视为当事人对履约方式的特别约定，但允许在特定条件下(如不可抗力、情势变更)通过法定程序暂停或终止执行。同时，建立智能合约纠纷的专门仲裁机制，允许当事人约定由区块链仲裁机构根据链上数据与代码逻辑进行快速裁决，减少对传统法院的依赖。在监管适配性方面，需构建“功能监管”框架，突破传统机构监管的局限。监管机构可要求智能合约开发方、部署方及关键节点运营者履行备案义务，建立代码白名单制度，对涉及资金转移、用户数据处理的合约实施强制审计。针对跨境智能合约，推动国际监管协调，例如通过 G20、FATF 等平台制定统一标准，要求合约部署方披露管辖地信息，防止监管套利。此外，可探索“监管沙盒”机制，允许合规创新项目在限定范围内测试，及时调整监管规则。对于证据认定难题，需完善电子证据规则。司法机关可引入区块链取证工具，将链上交易记录、代码逻辑及操作日志转化为可采信的证据形式。同时，建立技术鉴定机构名录，为法院提供代码审计、数据恢复等专业支持。在商业秘密保护方面，允许当事人对合约核心逻辑申请知识产权保护，并在举证时通过零知识证明等技术提交加密证据，既保障透明度又防止信息泄露。消费者权益保护需多管齐下。一方面，强制智能合约嵌入“冷静期”条款，允许消费者在交易后一定期限内通过链下机制(如客服介入)撤销订单，资金原路退回。另一方面，要求合约开发者以通俗语言披露关键条款，并通过交互式界面引导用户确认，解决“算法黑箱”问题。此外，可借鉴欧盟《数字市场法案》，要求大型电商平台为智能合约交易提供默认的消费者保护选项(如退货保障)，平衡去中心化与用户权益。对电商数据的安全展开分析，并从零知识证明、多级身份认证等方面入手，构建适用于电商平台的安全认证框架，对保障电商平台的数据安全具有重要意义[7]。对于数据隐私，强制采用同态加密、差分隐私等技术处理用户数据，并限制合约对个人信息的过度收集。

6. 结论

智能合约代表着电子商务未来演进的一个重要方向，它有潜力通过技术编码信任，构建一个更加透明、高效、公平的全球数字市场。然而，从理想走向大规模商用，必须跨越技术、法律和认知上的多重障

碍。这需要技术开发者、法律学者、监管机构、电商企业和社会各界的共同努力，以审慎而开放的态度，协同构建一个既能激发创新活力又能保障各方权益的治理框架。智能合约并非要完全取代传统电商模式，而是在特定场景下为其提供强大的补充和优化，最终共同推动电子商务生态的繁荣与演进。

参考文献

[1] Wang, R., Lin, Z. and Luo, H. (2018) Blockchain, Bank Credit and SME Financing. *Quality & Quantity*, **53**, 1127-1140. https://doi.org/10.1007/s11135-018-0806-6

[2] Buterin, V. (2024) A Next-Generation Smart Contract and Decentralized Application Platform. White-Paper. https://github.com/ethereum/wiki/wiki/

[3] 欧阳丽炜, 王帅, 袁勇, 等. 智能合约: 架构及进展[J]. 自动化学报, 2019, 45(3): 445-457.

[4] Szabo, N. (1996) Smart Contracts: Building Blocks for Digital Markets. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinter-school2006/szabo.best.vwh.net/smart_contracts_2.html

[5] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[6] 孙国茂, 李猛. 智能合约的法律性质与规制路径[J]. 中国法学, 2019(3): 100-115.

[7] 林小洁. 电子商务平台中基于区块链的数据加密与安全认证技术研究[J]. 信息与电脑, 2025, 37(23): 88-90.