E-Commerce Letters 电子商务评论, 2025, 14(12), 1657-1664
Published Online December 2025 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2025.14124036

Hans汉斯

区块链技术对网络支付安全性的提升研究

陈佳钰

贵州大学公共管理学院，贵州 贵阳

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

在数字化时代，网络支付已成为经济活动的核心环节，但支付安全问题如影随形，严重制约着行业发展。区块链技术以其去中心化、不可篡改、分布式账本等特性，为网络支付安全困境提供了破局之道。本文系统剖析区块链技术提升网络支付安全性的内在逻辑，全面阐述其在各类支付场景的应用实践，深入探讨面临的技术、法律、隐私等挑战，并对未来发展趋势进行展望，以期为网络支付安全领域的理论研究与产业实践提供更具深度的参考。

关键词

区块链技术，网络支付，安全性，分布式账本，智能合约

Research on the Improvement of Blockchain Technology to Online Payment Security

Jiayu Chen

School of Public Administration, Guizhou University, Guiyang Guizhou

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

Abstract

In the digital era, online payment has become a core component of economic activities. However, payment security issues persist as significant constraints on industry development. Blockchain technology, with its characteristics of decentralization, immutability, and distributed ledger, offers a groundbreaking solution to the security challenges of online payments. This paper systematically analyzes the inherent logic of how blockchain technology enhances the security of online payments, comprehensively elaborates on its application in various payment scenarios, and deeply discusses the technical, legal, and privacy challenges it faces. Furthermore, it prospects future development trends, aiming to provide more in-depth references for theoretical research and industrial practices in the

文章引用: 陈佳钰. 区块链技术对网络支付安全性的提升研究[J]. 电子商务评论, 2025, 14(12): 1657-1664.
DOI: 10.12677/ecl.2025.14124036

field of online payment security.

Keywords

Blockchain Technology, Online Payment, Security, Distributed Ledger, Smart Contract

1. 引言

互联网的普及与数字经济的崛起，推动网络支付实现了从无到有、从局部到全球的跨越式发展。如今，小到日常的线上购物、线下扫码，大到跨国企业的跨境贸易结算，网络支付都已成为不可或缺的工具。其便捷性极大地缩短了交易时间、降低了交易成本，但与此同时，支付安全风险也日益凸显。传统网络支付体系基于中心化架构，依赖银行、第三方支付平台等中心机构进行交易验证与数据存储。这种模式下，中心机构既是交易的核心枢纽，也成为了安全风险的集中点。黑客攻击、内部人员违规操作、系统漏洞等因素，都可能导致支付数据泄露、资金被盗刷等严重后果。据相关机构统计，每年因网络支付安全问题造成的经济损失数以百亿计，且呈逐年上升趋势，这不仅损害了用户的财产权益，也极大地削弱了公众对网络支付的信任。

区块链技术的出现，为网络支付安全带来了革命性的变革可能。它摒弃了传统的中心化信任机制，通过分布式网络、密码学算法等技术手段，构建起一种全新的信任体系。这种体系下，交易的安全性不再依赖单一机构，而是由整个网络共同保障。因此，深入研究区块链技术对网络支付安全性的提升，对于维护数字经济的健康发展、保障公众财产安全具有至关重要的意义。

2. 网络支付安全现状及面临的风险

2.1. 网络支付安全现状

当前，网络支付市场呈现出多元化、规模化的发展态势。网络支付即第三方支付，它是以网络发展为基础，以健全的信用体系为保障的新型付款方式[1]。第三方支付平台如支付宝、微信支付占据了国内移动支付的主要份额，而国际上则有 PayPal 等平台在跨境支付领域发挥重要作用。同时，银行也在不断拓展线上支付业务，推出了各类网上银行支付服务[2]。

为保障支付安全，行业采取了多种技术手段，如 SSL 加密、数字证书、动态口令、生物识别(指纹、人脸识别)等。这些技术在一定程度上提升了支付的安全性，但随着网络攻击技术的不断演进，传统安全防护手段的局限性逐渐暴露。例如，SSL 加密虽能保护数据传输过程，但无法防止数据在中心服务器被篡改[3]；生物识别技术也存在被伪造的风险，如高精度的指纹模具、人脸照片等都可能欺骗识别系统[4]。

2.2. 面临的主要风险

1. 数据篡改风险

在中心化网络支付系统中，所有交易数据最终都存储在中心机构的服务器中。一旦服务器遭受攻击，如 SQL 注入、缓冲区溢出等，攻击者就可能非法访问并篡改数据[5]。此外，内部人员也可能利用权限之便，对交易数据进行篡改，这种“内部”行为往往具备极强的隐蔽性和破坏性，如 2020 年不法分子与某

快递公司多位心存侥幸者“合作”，非法获取 40 万条个人信息，从而导致信息的大量泄露[6]。

2. 身份伪造问题

网络支付的身份认证环节是安全防护的关键，但传统认证方式存在诸多漏洞。密码认证容易因用户设置简单密码、密码被盗取等原因被突破；数字证书虽然安全性较高，但证书的管理、存储也存在风险，如证书文件被恶意拷贝、私钥泄露等。近年来，利用身份伪造进行的网络支付诈骗案件频发，犯罪分子通过非法获取用户身份信息，伪造身份进行大额支付操作，给用户造成了巨大的经济损失[7]。譬如，部分网络钓鱼者利用篡改网站、将欺诈性电子邮件发送给网民、仿冒 URL 地址等途径进行网络钓鱼活动，一般情况下网络钓鱼者选择知名银行或知名企业作为伪装对象，通过与真实网站还原度极高的网站违建，让用户在违建网页的产品选购和支付中，输入银行卡账号、真实原网站的登录密码、用户名、支付口令等重要信息，被钓鱼者盗取信息进而造成个人财产损失[8]。

3. 交易抵赖现象

由于缺乏有效的不可篡改、可追溯的交易记录，部分用户在完成支付后，可能会以“未进行过该交易”“交易金额有误”等为由否认交易行为。尤其是在跨境支付、大宗商品交易等场景中，交易双方可能分处不同国家和地区，一旦发生交易抵赖，取证和维权难度极大，不仅会给商家带来损失，也会影响支付平台的声誉[9]。

4. 中间环节安全隐患

网络支付通常涉及多个中间环节，如支付网关、清算机构、收单机构等。这些中间环节的系统安全防护水平参差不齐，成为了支付安全的薄弱环节[10]。例如，支付网关作为连接用户与银行的桥梁，若其安全防护措施不到位，可能会被黑客利用，截获用户的支付信息[11]；清算机构在处理大量交易数据时，若系统出现故障或被攻击，可能会导致交易延迟、资金清算错误等问题[12]。网络支付成为黑客攻击的重灾区，他们利用自己高超的计算机技术操控着用户，利用网络的安全漏洞谋取非法的经济利益，利用病毒、网络钓鱼、木马等攻击盗用他人的账号密码非法从网络上转走他人的存款，2015 年就有新闻报导有一黑客团伙盗了千万个支付账户，涉及数亿资金，而受害人银行卡未离身，但资金已经不翼而飞了，保障网络信息安全面临着严峻的挑战，由于是通过网络犯罪，黑客的犯罪地不受局限，有的甚至转移到国外，在打击上也存在着难度，资金的损失很难追偿[13]。

3. 区块链技术提升网络支付安全性的原理

3.1. 去中心化

区块链采用分布式对等网络架构，网络中的每个节点都拥有平等的地位和完整的账本副本[14]。当进行网络支付交易时，交易请求会被广播到整个网络，由多个节点共同进行验证和确认，而不是依赖单一的中心机构。这种去中心化的结构，彻底改变了传统网络支付中中心机构“一言堂”的局面，避免了因中心节点被攻击或出现故障而导致整个支付系统瘫痪的风险[15]。同时，由于没有中心机构对交易进行垄断性控制，也减少了因中心机构自身问题带来的安全隐患。

3.2. 不可篡改

区块链中的交易数据以区块为单位进行存储，每个区块包含了一定时间内的所有交易记录，并且每个区块都通过密码学哈希函数与前一个区块相连，形成一条不可逆转的链条[16]。哈希函数具有单向性和雪崩效应，即输入数据的微小变化都会导致哈希值的巨大变化。如果有人试图篡改某个区块中的交易数据，那么该区块的哈希值就会发生改变，从而破坏整个区块链的连续性[17]。由于区块链的分布式特性，要成功篡改数据，需要同时控制网络中超过 51%的节点，并对这些节点的账本进行修改，这在计算资源

和时间成本上是极其高昂的，几乎不可能实现[18]。因此，区块链的不可篡改特性确保了网络支付交易数据的真实性和完整性。

3.3. 分布式账本

区块链的分布式账本技术意味着交易信息会被同步存储在网络中的多个节点上[19]。当一笔网络支付交易发生时，交易信息会被实时广播到所有节点，每个节点都会对交易进行验证，并将验证通过的交易记录添加到自己的账本中[20]。这样，任何一笔交易都可以在多个节点上进行查询和验证，实现了交易信息的透明化和可追溯性。即使某个节点出现故障或数据损坏，也可以通过其他节点的账本进行数据恢复，保证了支付数据的可靠性和连续性。这种分布式存储方式，也使得黑客难以通过攻击单一节点来破坏整个支付系统的数据[21]。

3.4. 智能合约

智能合约是区块链上的一段自动执行的计算机程序，它以代码的形式将交易规则和条件固化下来[22]。在网络支付场景中，智能合约可以根据预设的条件自动触发支付操作[23]。例如，在电商交易中，当买家确认收到商品后，智能合约会自动将货款从买家账户划转到卖家账户；在跨境支付中，智能合约可以根据汇率波动情况，自动完成货币兑换和资金清算。智能合约的自动执行特性，减少了人为干预的环节，避免了因人工操作失误或恶意篡改而导致的支付安全问题。同时，智能合约的执行过程是公开透明的，所有节点都可以对其进行监督，进一步增强了支付的安全性和可信度[24]。

3.5. 密码学技术的应用

区块链技术广泛应用了多种密码学技术，如非对称加密、数字签名等，为网络支付安全提供了坚实的技术基础[25]。非对称加密使用公钥和私钥对数据进行加密和解密，用户的公钥可以公开，用于加密交易信息，而私钥则由用户自己保管，用于解密信息和进行数字签名[26]。数字签名则可以确保交易的真实性和不可抵赖性，当用户发起支付交易时，会用自己的私钥对交易信息进行签名，其他节点可以用用户的公钥对签名进行验证，从而确认交易的发起者身份以及交易信息的完整性[27]。这些密码学技术的应用，使得网络支付交易在传输和存储过程中得到了有效的保护，防止了信息被窃取、篡改和伪造。

4. 区块链技术在网络支付安全中的应用场景

4.1. 跨境支付

传统跨境支付流程复杂，通常需要经过多个中间银行，涉及多个环节的审核与清算，不仅耗时较长，而且手续费高昂，同时还存在着汇率风险、资金被挪用等安全隐患。

利用区块链技术进行跨境支付，可实现点对点的直接交易。交易双方通过区块链网络直接进行支付操作，无需中间银行参与。区块链的分布式账本技术使得交易信息在全球范围内的节点实时同步，所有参与方都可以实时查看交易进度，提高了交易的透明度。智能合约可以自动处理汇率转换、资金清算等环节，当交易满足预设条件(如双方身份验证通过、交易信息确认无误)时，智能合约自动执行资金划转，大大缩短了跨境支付的时间(可缩短至几分钟甚至几秒)，降低了手续费成本。此外，区块链的不可篡改特性确保了跨境支付交易记录的真实性，有效防范了资金被挪用、汇率被恶意操纵等风险。

4.2. 移动支付

移动支付凭借其便捷性，已成为人们日常生活中最常用的支付方式之一，但移动设备的开放性和移动支付应用的多样性，也使其面临着诸多安全威胁，如移动终端被恶意软件感染、支付信息在传输过程

中被窃取、支付应用存在漏洞等。

区块链技术为移动支付安全提供了有力保障。通过区块链的去中心化身份认证机制，用户可以在不依赖第三方机构的情况下，安全地进行身份验证。用户的身份信息以加密形式存储在区块链上，只有用户自己拥有访问和控制权限，有效防止了身份信息被泄露和伪造。在交易过程中，支付数据通过区块链网络进行传输和存储，利用区块链的不可篡改和分布式存储特性，确保了支付数据的安全性和完整性。即使移动设备丢失或被攻击，只要用户的私钥安全，就可以保证支付账户的安全。例如，一些基于区块链的移动支付应用，通过将用户的支付凭证和交易记录存储在区块链上，极大地提升了移动支付的安全性，受到了用户的广泛欢迎。

4.3. 供应链金融支付

供应链金融涉及供应商、制造商、经销商、物流企业、金融机构等多个参与主体，支付环节是供应链金融的核心环节之一。传统供应链金融支付存在着信息不透明、信任度低、资金周转慢等问题。由于各参与主体之间的信息孤岛现象，金融机构难以全面、准确地了解供应链上的交易情况，导致风控难度大，进而影响了资金的投放效率和安全性。

区块链技术可以构建一个透明、可信的供应链金融支付平台。将供应链上的每一笔交易(如订单签订、货物运输、验收等)都记录在区块链上，实现交易信息的实时共享和透明化。金融机构可以通过区块链实时获取供应链的真实交易数据，准确评估企业的信用状况和还款能力，从而更精准地进行风控，提高资金投放的安全性。同时，区块链的智能合约可以根据供应链交易的进展情况，自动触发支付操作。例如，当货物送达并验收合格后，智能合约自动向供应商支付货款，加快了资金周转速度，降低了企业的融资成本。此外，区块链的不可篡改特性确保了供应链交易数据的真实性，有效防范了虚假交易、重复融资等风险，为供应链金融支付营造了一个安全、可信的环境。

4.4. 公共事业缴费

公共事业缴费(如水电费、燃气费、物业费等)涉及大量的用户和频繁的小额交易，传统缴费方式存在着缴费渠道分散、缴费记录管理混乱、对账困难等问题，同时也存在着缴费信息被篡改、缴费资金被挪用等安全隐患。

利用区块链技术进行公共事业缴费，可实现缴费信息的集中管理和安全存储。用户的缴费记录被完整地记录在区块链上，不可篡改且可追溯，方便用户和公共事业机构进行查询和对账。智能合约可以根据用户的使用情况自动计算费用，并在用户确认后自动完成缴费操作，避免了人工计算和操作带来的错误和风险。此外，区块链的分布式账本技术使得公共事业机构、用户、支付平台等各方都可以实时查看缴费情况，提高了缴费的透明度，有效防范了缴费信息被篡改和缴费资金被挪用的风险。例如，某城市将区块链技术应用于水电费缴费系统，实现了缴费数据的实时同步和安全管理，极大地提升了公共事业缴费的效率和安全性。

5. 区块链技术应用于网络支付安全的现存挑战

5.1. 技术性能问题

目前，区块链技术在处理速度和可扩展性方面还无法满足大规模网络支付的需求。以比特币区块链为例，其每秒只能处理约 7 笔交易，而像支付宝这样的大型支付平台，峰值时期每秒需要处理数十万笔交易[28]。区块链的共识机制(如工作量证明 PoW)是导致其处理速度慢的主要原因之一，PoW 机制需要网络中的节点进行大量的哈希计算来竞争记账权，这不仅消耗大量的计算资源，也限制了交易处理的

速度。

虽然一些新型的区块链共识机制(如权益证明 PoS、委托权益证明 DPoS 等)在一定程度上提高了处理速度，但与传统中心化支付系统相比，仍有较大差距[29]。此外，区块链的存储容量也是一个问题，随着网络支付交易的不断增加，区块链账本的容量会急剧扩大，这对节点的存储能力提出了很高的要求，也会影响交易的验证和同步速度。如何在保证区块链安全性和去中心化特性的前提下，大幅提升其处理速度和可扩展性，是区块链技术应用于网络支付安全需要解决的关键技术问题。

5.2. 法律法规与监管问题

区块链技术的去中心化、匿名性等特性，与传统的中心化监管模式存在冲突。目前，全球范围内还没有形成统一的、针对区块链技术在网络支付领域应用的法律法规和监管框架。

在法律层面，对于区块链上的智能合约的法律地位、电子签名的法律效力、交易纠纷的管辖权等问题，还缺乏明确的法律规定。例如，当智能合约执行出现问题时，责任该由谁来承担，是合约的编写者、使用者还是区块链平台运营商，在法律上尚未有清晰的界定。

在监管层面，区块链技术的应用可能会带来洗钱、恐怖融资、偷税漏税等金融犯罪风险。由于区块链的匿名性，使得监管机构难以追踪资金的流向和交易主体的身份，给监管工作带来了很大的困难。如何在鼓励区块链技术创新的同时，建立有效的监管机制，防范金融风险，是当前面临的重要挑战。

5.3. 隐私保护问题

区块链技术的透明性是其重要特性之一，区块链上的交易信息对所有节点都是公开可见的。然而，在网络支付中，用户的交易隐私(如交易金额、交易对象、支付习惯等)是需要严格保护的。

虽然区块链采用了加密技术对交易数据进行保护，但交易的发起者、接收者等信息在一定条件下仍可能被追踪和分析。例如，通过对区块链上的交易地址进行关联分析，可以推测出用户的交易行为和资金状况。此外，一些基于区块链的网络支付应用为了提高用户体验，可能会要求用户提供一定的个人信息，这些信息的存储和使用也存在着隐私泄露的风险。如何在保证区块链透明性的同时，有效地保护用户的交易隐私，是区块链技术在网络支付安全领域应用需要解决的重要问题。目前，一些隐私保护技术，如零知识证明、环签名、混币技术等，已经在区块链中得到了一定的应用，但这些技术在实用性和效率方面还有待进一步提升。

5.4. 技术融合与标准化问题

网络支付系统是一个复杂的生态系统，涉及多种技术的融合，如密码技术、网络技术、数据库技术、移动互联网技术等[30]。区块链技术要与现有的网络支付技术进行深度融合，需要解决技术兼容性问题。例如，区块链系统与传统支付系统的数据格式、接口标准可能存在差异，如何实现两者之间的无缝对接，确保数据的准确传输和交互，是一个技术难题。

此外，目前区块链技术还没有统一的标准，不同的区块链平台(如比特币、以太坊、Hyperledger 等)在技术架构、共识机制、智能合约语言等方面存在着很大的差异。这导致不同区块链平台之间的互操作性差，难以进行有效的数据交换和业务协同。在网络支付领域，若采用不同的区块链平台进行支付服务，可能会形成新的信息孤岛，影响支付的效率和安全性。因此，制定统一的区块链技术标准，促进不同区块链平台之间的互操作，是区块链技术在网络支付安全领域广泛应用的必要前提。

6. 相关建议

区块链技术凭借去中心化、不可篡改、分布式账本，以及智能合约、密码学加密等核心特性，为网

络支付安全提供了突破性解决方案。传统网络支付体系面临的数据篡改、身份伪造、交易抵赖等风险，在区块链技术的应用下得到有效缓解——去中心化架构规避了中心节点被攻击或故障的隐患，不可篡改特性保障了交易数据的真实性与完整性，分布式账本实现了交易信息的可追溯与多节点备份，智能合约与加密技术则进一步减少人为干预风险、筑牢信息安全屏障。

6.1. 技术性能优化

创新共识机制组合应用，采用混合共识模式，在核心交易验证环节保留安全性，非核心环节简化计算流程，将单链交易处理速度提升至每秒千笔以上，适配大规模支付场景需求。推行分层存储与分片技术，将高频小额交易数据存储于轻量节点，核心交易数据同步至全节点，同时按交易地域、类型进行分片处理，降低单节点存储压力与验证延迟。研发高效数据压缩算法，对区块链账本中的重复交易信息、冗余字段进行智能压缩，减少存储容量占用，提升数据同步与查询效率。

6.2. 法律法规与监管完善

明确智能合约法律地位，制定《区块链智能合约管理规范》，界定合约编写者、使用者、平台运营商的责任划分，建立合约漏洞认定标准与纠纷解决机制。

构建“技术 + 监管”协同框架，要求区块链支付平台嵌入监管接口，实现交易数据实时脱敏上报，运用大数据分析技术追踪资金流向，防范洗钱、恐怖融资等犯罪行为。出台跨境支付区块链应用指导意见，统一不同国家和地区的交易验证标准、资金清算规则，明确跨境交易的管辖权归属与争议解决途径。

6.3. 隐私保护强化

推广零知识证明与环签名技术落地，在支付交易中默认启用隐私保护模式，仅向交易双方与监管机构开放必要信息，屏蔽无关节点对交易金额、主体身份的追溯可能。建立用户隐私权限分级管理体系，允许用户自主设置交易信息可见范围，明确平台对个人信息的存储期限与使用边界，严禁超范围采集支付习惯、消费偏好等敏感数据。定期开展隐私安全审计，要求区块链支付平台每季度委托第三方机构进行渗透测试，排查隐私泄露风险点，形成审计报告并向监管部门备案。

6.4. 技术融合与标准化推进

制定跨系统数据交互标准，统一区块链与传统支付系统的数据格式、接口协议，开发适配性中间件，实现交易数据在不同平台间的无缝传输与准确映射。建立行业统一技术规范，由监管机构联合头部企业、科研机构，明确区块链支付的共识机制、智能合约语言、加密算法等核心技术参数，推动不同平台(比特币、以太坊等)的互操作性。搭建技术融合试点平台，选取移动支付、公共事业缴费等场景开展试点，测试区块链与生物识别、物联网等技术的融合效果，形成可复制的技术融合方案并逐步推广。

7. 结论

区块链技术通过其去中心化、不可篡改、分布式账本及智能合约等核心特性，为构建更安全、透明、高效的新型网络支付体系提供了强大的技术支撑。研究表明，该技术能有效应对传统支付模式中的数据篡改、身份伪造与交易抵赖等核心风险，在跨境支付、移动支付等多个场景中展现出巨大应用潜力。

然而，其广泛应用仍面临技术性能、法律法规、隐私保护及技术标准等方面的挑战。未来，需通过持续的技术创新、健全的法规监管、强化的隐私保护方案以及行业标准的统一，方能克服障碍，充分发挥区块链技术在保障网络支付安全、推动数字经济稳健发展中的革命性作用。

参考文献

[1] 张颖楠. 网络支付平台风险分析[J]. 赤峰学院学报(自然科学版), 2020, 36(9): 101-103.

[2] 王磊. 第三方支付平台监管: 进展、问题与完善建议[J]. 价格理论与实践, 2021(8): 28-34.

[3] 刘明达, 拾以娟, 赵波, 等. 一种基于手机令牌的移动支付认证协议[J]. 武汉大学学报(理学版), 2016, 62(2): 110-116.

[4] 才华, 肖普山. 生物识别技术在金融支付领域应用探索[J]. 计算机应用与软件, 2021, 38(4): 106-111+158.

[5] 杨志勇. 大数据云计算下网络安全技术实现的路径[J]. 电脑知识与技术, 2025, 21(12): 67-69.

[6] 任彦君. 电信网络诈骗犯罪的防控难题与对策分析[J]. 浙江警察学院学报, 2024(5): 113-124.

[7] 阎二鹏, 杨敏杰. 第三方支付模式下网络侵财的类型归结、界限厘清与路径选择[J]. 海南大学学报(人文社会科学版), 2022, 40(4): 115-122.

[8] 郑俞鑫. 新媒体与电子商务融合下的支付安全问题探讨[J]. 中国集体经济, 2021(4): 157-158.

[9] 皮勇, 汪恭政. 新机会理论视角下第三方网络支付平台洗钱犯罪及其防控[J]. 广西大学学报(哲学社会科学版), 2018, 40(2): 33-41.

[10] 劳东燕. 非法经营罪中支付结算业务的界定[J]. 法学, 2024(9): 76-92.

[11] 卢剑权, 邢梦平, 张晶. 网络攻击下多智能体系统一致性安全与隐私保护研究综述[J]. 控制与决策, 2025, 40(11): 3201-3219.

[12] 李欢. 数据资产出资适格性的检视与完善[J]. 东方法学, 2025(4): 107-123.

[13] 张少军. 网络支付安全问题的防范研究[J]. 行政事业资产与财务, 2016(36): 91+3.

[14] 罗振华, 唐寅. 基于区块链的政务数据共享方案研究[J]. 现代电子技术, 2025, 48(18): 22-28.

[15] 关芳. 基于网络交易的区块链安全技术探究[J]. 网络安全技术与应用, 2019(3): 77-78.

[16] 刘旸, 陈以欣. 区块链技术对于解决电子商务信用问题的应用研究[J]. 大连大学学报, 2022, 43(5): 79-85+101.

[17] 颜世露, 相里朋, 崔巍. 区块链在量子时代的机遇和挑战[J]. 电子科技大学学报, 2022, 51(2): 162-169.

[18] 苏楠, 王青梅, 司海平, 等. 基于区块链的优质作物种质资源数据存储模型研究[J]. 农业大数据学报, 2025, 7(3): 343-352.

[19] 李守伟, 张嘉政, 何海波, 等. 基于区块链的大模型数据监管体系设计[J]. 信息安全研究, 2025, 11(8): 682-692.

[20] 荆云华. 基于区块链技术下的财务管理问题研究[J]. 商业经济, 2025(5): 162-165.

[21] 李胜, 陈枫, 罗娜, 等. 面向量子计算威胁的区块链技术综述[J/OL]. 计算机科学与探索, 1-25. https://link.cnki.net/urlid/11.5602.TP.20251014.1232.008, 2025-12-09.

[22] 胡甜媛, 李泽成, 李必信, 等. 智能合约的合约安全和隐私安全研究综述[J]. 计算机学报, 2021, 44(12): 2485-2514.

[23] 孙浩. 加密货币技术与金融基础设施创新——从去中心化金融到金融互联网[J]. 金融监管研究, 2025(6): 91-114.

[24] 杨建霞. 基于区块链技术的企业财务透明化与安全性研究[J]. 太原城市职业技术学院学报, 2025(9): 28-30.

[25] 陈文, 洛桑丁增, 董应海, 等. 区块链技术在电网可靠性评估中的应用研究[J]. 电气技术与经济, 2025(8): 47-50.

[26] 黄清朗. 数据加密技术在计算机网络安全中的应用研究[J]. 科技资讯, 2025, 23(16): 10-12.

[27] 郝嘉琨, 向鹏, 何逸飞, 等. 基于去中心化身份的跨域数据交易系统[J]. 计算机研究与发展, 2024, 61(10): 2570-2586.

[28] 丁晓蔚. 数字金融时代的金融情报学: 学科状况、学科内涵和研究方向[J]. 情报学报, 2021, 40(11): 1176-1194.

[29] 韩益亮, 宋超越, 吴旭光, 等. 区块链与隐私计算融合技术综述[J]. 科学技术与工程, 2024, 24(28): 11945-11963.

[30] 任兵, 陈志霞, 张茂茂. 迈向数智时代的城市元宇宙: 概念界定与框架构建[J]. 电子政务, 2023(6): 88-99.