区块链赋能数据存储安全服务研究进展

张瑶瑶,周 圆,杨青林,颛孙晨露,陈 凯,李 意,刘 园*,田志宏
(广州大学网络空间安全学院,广东广州 510555)

摘 要: 随着数字经济的高速发展,数据存储已成为数据要素全生命周期管理的核心环节,在完整性、隐私性、可用性等安全属性上面临多重挑战. 区块链依托分布式账本数据结构与密码学共识机制,构建起覆盖数据全生命周期可信存储的基座,为破解安全挑战提供创新技术路径. 然而现有区块链技术在可扩展性、效率优化和安全加固等方面仍存在局限,亟需系统梳理区块链赋能数据安全的技术路径与能力边界. 本文围绕数据安全服务"数据上链、服务访问、授权管理、生态运营"等关键业务,系统性调研区块链赋能数据安全研究进展,并面向数据安全利用和价值流通等数据产业安全发展指明技术发展趋势. 具体地,本文首先从数据上链存储环节出发,分析影响数据完整性的共识机制、可编辑区块链以及完整性审计技术现状;其次在服务访问环节,分析拒绝服务(Denial-of-Service,DoS)攻击和低效率功能两类威胁的攻击原理,并对比当前存储可用性方案的优缺点;面对授权管理环节,从身份管理和密文存储两方面讨论数据跨域和非法访问问题及分析现有解决方案;面对数据存储安全服务生态运营需求,探索可扩展性的共识协议和分片机制两类技术,分析其成本、效率与适配性等方面瓶颈;最后,讨论区块链在数据安全领域赋能大语言模型(Large Language Model,LLM)安全的能力,并展望区块链在抗量子密码算法的能效优化机制、基于联邦学习的区块链弹性扩展架构,以及可信数据要素驱动的大语言模型等研究方向的发展趋势.

关键词: 区块链;数据安全;存储;安全服务;大语言模型

基金项目: 国家自然科学基金(No.62172085);国家重点研发计划(No.2022YFB3102700);广东省工业控制系统安全重点实验室项目(No.2024B1212020010)

中图分类号: TP309.2 **文献标识码:** A **文章编号:** 0372-2112(2025)10-3794-23

电子学报 URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20250347

Research Progress on Blockchain-Empowered Data Storage Security Service

ZHANG Yao-yao, ZHOU Yuan, YANG Qing-lin, ZHUANSUN Chen-lu,
CHEN Kai, LI Yi, LIU Yuan*, TIAN Zhi-hong
(*School of Cyberspace Security*, *Guangzhou University*, *Guangzhou*, *Guangdong* 510555, *China*)

Abstract: With the rapid growth of the digital economy, data storage has become a critical component in the whole management cycle, but it encounters several critical security challenges, such as content integrity, privacy preservation, and sustainable availability. Benefiting from the distributed ledger structure and cryptographic consensus mechanisms, blockchain technology provides a trustworthy solution for addressing these security challenges. Given the fact that the current blockchain systems remain constrained by scalability, efficiency, and security limitations, it is essential to conduct a systematic review of their data storage service capacities and analyze their security boundaries. This paper provides a comprehensive survey of research progress in blockchain-enabled data security by investigating its key procedures, including data on-chain storage, service access, authorization management, and ecological operation to identify emerging technical trends towards secure data utilization and value exchange. Specifically, this paper begins by examining the data on-chain storage phase, analyzing the current state of consensus mechanisms, editable blockchains, and integrity auditing technologies that impact data integrity. Next, in the service access phase, it analyzes the attack principles of two types of threats - DoS (Denial-of-Service) attacks and inefficient functionality - and compares the strengths and weaknesses of existing storage availability solutions. Regarding the authorization management phase, it discusses cross-domain data and unauthorized access issues

收稿日期:2025-04-30;录用日期:2025-10-24;责任编辑:覃怀银
*通讯作者:刘园

from the perspectives of identity management and ciphertext storage, while analyzing existing solutions. In response to the ecological operation needs of data storage security service, it explores two types of technologies — scalable consensus protocols and sharding mechanisms — analyzing their bottlenecks in terms of cost, efficiency, and adaptability. Finally, it discusses blockchain's capability to empower LLM (Large Language Models) in the field of data security and looks ahead to research trends, including energy-efficient optimization mechanisms for post-quantum cryptographic algorithms, blockchain elastic scaling architectures based on federated learning, and trusted data element-driven LLMs.

Key words: blockchain; data security; storage; security service; large language models

Foundation Item(s): National Natural Science Foundation of China (No.62172085); National Key Research and Development Program of China (No.2022YFB3102700); Project of Guangdong Key Laboratory of Industrial Control System Security (No.2024B1212020010)

1 引言

在数字经济深度发展的今天,数据已跃升为关键生产要素,其价值贯穿于生产、流通、分配的全生命周期,具有价值共享、低成本批量复制、即时传输、无限供给等特点[1]. 然而数据的低成本可复制性决定了在扩大数据流通范围的同时,也加剧了数据安全的风险. 数据安全覆盖价值流通全生命周期,而数据存储作为数据全生命周期的核心环节,直接影响着数据的完整性、隐私性[2]、可用性以及可扩展性[3].

区块链技术作为一种分布式账本,通过哈希验证数据结构与共识机制实现去中心化信任,是存储领域的创新性技术[4]. 该技术已广泛应用于金融科技、医疗健康、政务服务、智能制造及能源管理等关键领域,尤其在分布式数据存储场景中展现出了独特价值. 在金融科技领域,区块链通过分布式账本记录交易数据并形成链式结构,重构传统信任机制,实现跨境支付与结算的高效性与透明性[5];同时,资产所有权信息通过代币化存储于区块链,结合智能合约自动执行交易规则,推动资产证券化与数字资产管理的发展[6]. 在医疗健康领域,区块链实现了去中心化的隐私安全数据存储. 患者的加密数据存储于分布式节点,中继信息写入区块链,确保病例管理的安全性与可追溯性[7];药品供应链中产生的数据经节点共识验证后存储于区块链,实现了全流程溯源[8];实验室数据实时上传并利用智能合约设定访问规则,进一步保障实验结果的可信管理. 在政务服务领域,区块链记录公共数据,政府公文的哈希值存储于区块链,原始文件存于分布式服务器,有效增强政府公信力[9]. 在工业制造领域,区块链实现全生命周期数据的可信溯源[10]. 在零部件生产中,生产数据实时写入区块链并支持跨企业数据共享,以此降低产品召回成本[11];同时,区块链为设备提供唯一标识,确保设备与身份绑定,防止设备注入虚假数据;供应链为数据存储提供全流程追踪和审计,提升工业制造的透明度与效率. 在储能领域,区块链存储能源生产与消费数据,同时采用智能合约实现自动结算,提高资源利用效率[12];储能设备的性能状态数据上链存储,便于实时监控与维护[13],链上存储储能数据为多单元调度与充放电优化提供数据基础;能源的来源与流向信息记录于区块链,确保能源可追溯性与透明度. 区块链通过其在存储阶段的应用,为各行业数据管理提供了安全、可信、高效的解决方案,推动了数字化转型的深入发展.

然而,区块链技术的大规模应用仍面临扩展能力不足、效率低下和数据安全风险等多重挑战. 与此同时,数据要素市场正经历着从"数据洪流"到"智能涌现"再到"价值重构"的范式转变. 在此过程中,数据质量作为大语言模型训练与部署的核心要素,其安全治理、可信来源认证以及部署优化需求与区块链技术形成深度耦合. 这些需求与去中心化金融(Decentralized Finance, DeFi)、非同质化货币(Non-Fungible Token, NFT)、去中心化自治组织(Decentralized Autonomous Organization, DAO)等新兴计算范式共同推动着区块链技术向着高质量服务、跨域协同、效率增强、安全加固等方向加速演进. 值得注意的是,当前研究前沿已延伸至量子增强算法、大语言模型赋能以及共识算法等深层次领域,这些突破性进展推动区块链基础理论研究进入新阶段. 基于技术演进和市场需求的双向驱动,亟需系统性分析区块链技术如何赋能数据安全,为区块链的进一步发展点明方向.

在区块链赋能数据安全服务研究方向上,当前领域已经积累了较丰硕的理论研究和技术成果. 为理清研究现状与空白,本文采用内容分析法分析了有关区块链赋能数据安全的近十年综述文献,针对现有综述研究,在区块链核心技术与优化、区块链赋能场景和区块链安全服务三个纬度方向进行对比分析,优点和不足如表1所示.

根据表1综述分析所示,区块链核心技术与优化通过共识算法、智能合约等技术保证数据的完整性、隐私性和可扩展性[14~19];区块链技术在工业物联网、6G等场景的应用验证了技术落地的可行性[20~24];安全服务研究则集中在加密、存储优化等方面构建数据保护框架[25~28]. 然而,核心技术与优化虽强化了数据完整性、

表1 本文与其他相关综述文章对比

调查维度	文献	时间	优点	不足/局限
区块链核心技术与优化	文献[14]	2023	综述可编辑区块链文献,保证数据完整性	对数据可用性论述和调研不够深入
	文献[15]	2023	综述共识协议的安全性,保障区块链系统的安全性	
	文献[16]	2023	综述关键字搜索技术,保证数据隐私性	
	文献[17]	2024	综述智能合约安全,保证数据完整性	
	文献[18]	2024	综述基于区块链的身份共享技术,保证数据隐私性	
	文献[19]	2025	综述共识协议可扩展性,提高区块链系统性能	
区块链赋能场景	文献[20]	2022	综述区块链在工业物联网(Industrial Internet Of Things,IIOT)中的应用	尚未分析区块链对于通用场景的赋能边界
	文献[21]	2022	综述区块链在智能制造中的应用现状和挑战	
	文献[22]	2023	综述数字孪生驱动IIOT的方案	
	文献[23]	2023	综述区块链和智能网络技术赋能元宇宙	
	文献[4]	2024	综述区块链赋能6G网络	
	文献[24]	2024	探讨区块链在海运行业的网络安全挑战	
区块链安全服务	文献[25]	2018	综述基于区块链的安全服务方法,讨论加密和身份验证服务、隐私服务、数据来源服务以及完整性服务	未覆盖存储全流程安全的保护方案
	文献[26]	2020	从流程、数据和基础设施层面研究区块链安全状况	
	文献[27]	2024	总结区块链存储优化方案,并从基于复制、基于密文和基于内容的优化三个角度进行分析	
	文献[28]	2024	归纳分析区块链与数据安全的交叉解决方案	

隐私性与可扩展性,但对数据可用性的探索普遍薄弱;领域应用研究主要关注区块链赋能单一场景,并未分析区块链赋能通用场景的边界;安全服务研究成果呈现碎片化,未见覆盖数据存储全流程的系统性保护方案. 上述问题凸显了从单项技术到全局性安全服务体系的迫切需求. 因此,本文开展综述研究以期系统性回答以下三个研究问题:

(1)区块链在存储阶段具备哪些安全能力?

(2)当前存储安全体系存在哪些薄弱环节?

(3)在大语言模型通用智能场景下区块链如何赋能数据安全?

为了回答上述问题,本文聚焦当前区块链相关论文最关注的完整性、可用性、隐私性和可扩展性四大数据安全服务属性,通过对区块链相关文献的系统梳理,从数据存储阶段的安全效能切入,针对区块链数据安全能力的关键问题展开研究. 首先,通过分析数据上链全流程,系统论证了区块链保障存储完整性的技术路径及其潜在安全风险;其次,在访问管理层面,揭示了影响数据可用性的持续性威胁;围绕授权管理环节,从身份管理和密文存储两方面入手讨论数据存储隐私问题;然后,为了保证系统生态运营,在基础架构方面,分析系统可扩展性;在应用层面,从数据安全治理、模型可信增强以及部署优化三方面着手分析区块链赋能大语言模型;最后,基于上述分析内容,本文回答了所提出的三个问题,并分析讨论未来研究方向,为构建下一代可信区块链系统奠定了研究基础. 本文主要贡献包括:

(1)基于最关注的数据安全服务属性维度,以“数据上链、服务方案、授权管理、生态运营”为路径,分析区块链在存储过程中的安全能力和薄弱环节,为区块链赋能数据安全理清技术路径和能力边界.

(2)本文深入分析了区块链赋能大语言模型场景下的数据安全,深入研究了区块链赋能大语言模型的安全能力以及面临的安全问题,明确区块链赋能大语言模型的能力边界.

(3)分析展望了量子密码增强、区块链性能和大语言模型赋能区块链三个研究方向,助推区块链技术在数据安全领域的深化应用,对推动数字经济高质量发展具有重要意义.

本文其余部分的结构如下. 第二章阐明调研方法;第三章到第六章分别从四个安全服务属性展开深度分析;第七章从应用层面分析区块链赋能大语言模型的安全能力. 最后,第八章回答了本文要解决的三个问题并讨论总结未来的发展情况. 本文组织架构如图1所示.

2 调研方法

本文选择使用系统性文献综述方法[29]来研究区块链赋能数据安全. 首先本文以区块链、安全为关键字,在谷歌学术数据库、dblp和IEEE中进行文献检索,查找近十年的论文,共找到符合条件的论文280篇,后筛选出高相关度文章190篇. 从数据赋能角度,选出92篇与数据存储相关的论文. 然后,本文将这些论文根据数据安全服务属性进行分类,经调查发现数据安全服务属性中排前4的属性是数据完整性、可用性、可扩展性、隐私性,具体数据安全服务属性及其解释如表2所示.

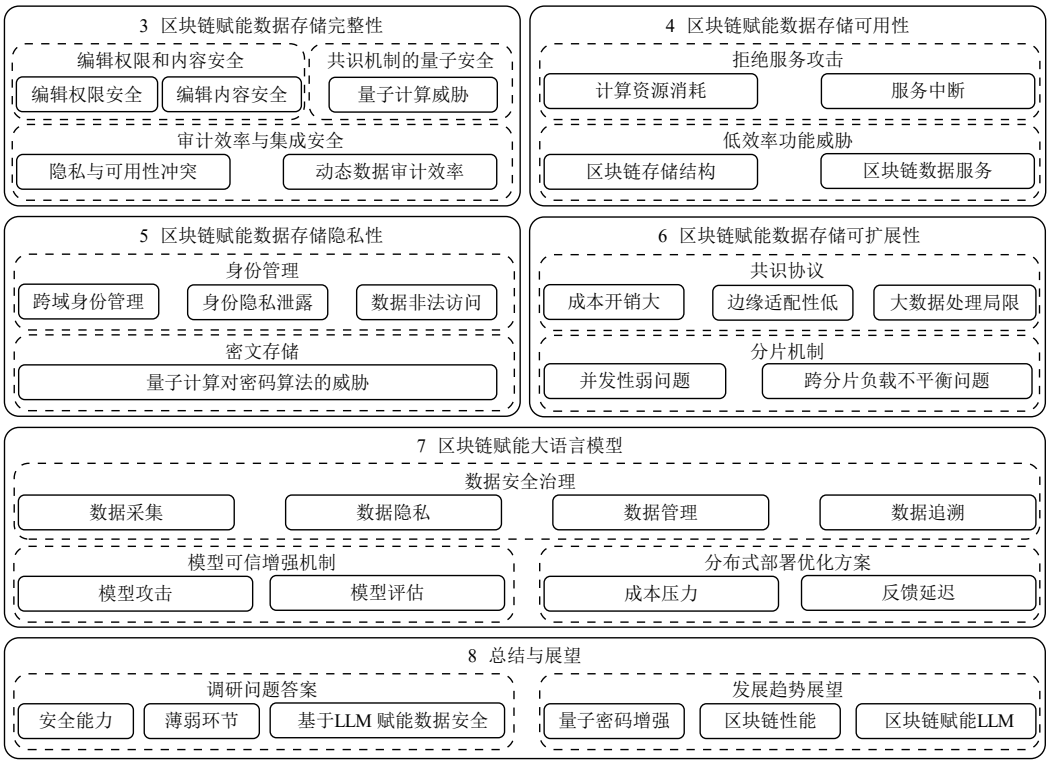

图1　本文内容组织架构

表2　数据安全服务属性及其解释

安全服务	释义
完整性	完整性指数据的一致性,确保数据从共识到审计整个过程中不被恶意破坏或篡改
可用性	可用性指保障数据被合法用户访问,且高效、无阻碍地进行读写
可扩展性	可扩展性指系统在不进行重大改动的情况下,能够处理不断增加的负载或数据量
隐私性	隐私性指数据拥有者通过定义相应的数据访问规则,控制隐私数据资源不被未经授权的用户访问

为了更好地量化研究者们对安全服务属性的重视程度,本文定义了区块链数据存储安全相关的数据服务特性比例,如式(1)所示:

$$X_j=\frac{i}{n} \tag{1}$$

其中,i表示当前存储阶段安全服务j的篇数;n表示论文总量.

根据式(1),本文计算并筛选出4个占比最高的数据服务属性来探讨区块链是否能够适应存储阶段的数据安全需求,图2为面向存储阶段数据安全服务属性的文献占比分析. 在本文研究中,“完整性”的研究热度显著高于其他属性. 其原因在于区块链通过分布式共识机制、链式结构及密码算法,减少了对单一中心化机构的信任依赖,建立了一种基于密码学验证和分布式共识的去中心化信任机制[30],使得数据完整性成为系统存续的关键因素. 随着应用场景向金融、医疗等领域延伸,在保障完整性的前提下,突破扩展性瓶颈成为亟待解决的关键挑战[31,32]. 相较之下,隐私性的研究数量虽低于完整性和可扩展性,但其对于建立用户信任与满足法律合规要求至关重要[33]. 在技术演进初期,区块链主要依赖分布式冗余存储提供的基础容灾能力来保障基本可用性. 然而,针对更深层次的可用性威胁,其系统性防护和优化方案的研究深度往往依赖于底层核心架构的成熟与稳定,加之研究资源更多聚焦于构建信任基石与突破性能瓶颈,导致对深层可用性威胁的防护研究相对滞后.

3　区块链赋能数据存储完整性

传统区块链存储方案多采用链上链下协同机制,通过链下存储原始数据、链上存储数据索引提升效率,并依赖智能合约实现自动化管理[34]. 然而在数据上链存储的关键阶段,存在三个安全挑战. 在共识验证环节,基于密码学难题保证安全性的共识算法面临量子计算暴力破解的风险,动摇了信任基础;在存储写入环

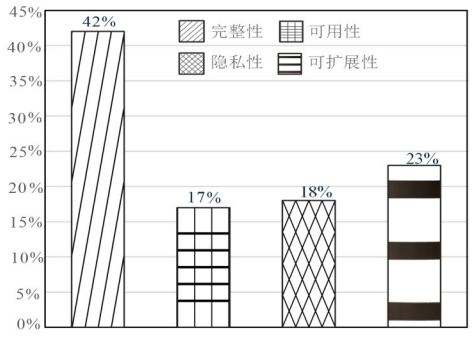

图2 面向存储阶段数据安全服务属性的文献占比分析

节,存储后的编辑行为存在编辑内容和编辑权限的双重风险,加剧了审计复杂度,使得在存储验证阶段难以准确判断数据的真实性和可用性,进一步加剧了隐私与可用性的冲突;在存储验证环节,动态审计需同步处理隐私与可用的互斥需求,效率瓶颈可能使前序环节的安全隐患放大,进而削弱系统对风险的响应能力. 而提升审计效率、优化动态审计流程,则有助于加速安全策略的调整过程. 这不仅能及时应对潜在风险,还反过来进一步强化共识机制的量子安全性,从而在整体上加固了循环链条,提升了系统的鲁棒性. 上述三个问题形成了上链存储过程的循环风险链条,其相互作用机制如图3所示.

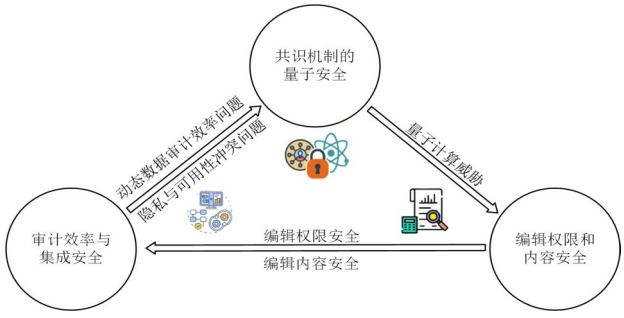

图3 区块链存储完整性中存在的主要安全挑战

3.1 共识机制的量子安全

在区块链赋能的Web3与元宇宙生态体系中,共识机制作为分布式信任基础设施的核心组件,其抗攻击能力直接决定系统数据的完整性. 经典拜占庭容错(Practical Byzantine Fault Tolerance,PBFT)共识机制虽然能够实现1/3容错阈值的理论极限,却面临着量子计算的双重威胁. 一方面,基于数论难题(如大整数分解)的拜占庭协议易受Shor算法[35]攻击,该算法可在多项式时间内破解RSA等非对称加密体系. 另一方面,Grover算法使哈希碰撞搜索复杂度由$O(N)$降至$O(\sqrt{N})$,导致工作量证明(Proof-of-Work,PoW)共识机制面临量子算力主导的51%攻击风险.

为应对量子计算对区块链共识机制的安全威胁,当前研究主要沿着抗量子密码增强与量子区块链架构两条技术路径展开. 在抗量子密码学增强方面,研究者通过格密码、哈希签名等后量子算法重构共识协议. 例如,Behnia等人[36]构建了基于Hermite格最短向量问题的PoW共识机制,其计算复杂度在量子计算模型下仍保持指数级增长特性. 同样,Dolev等人[37]设计了异步拜占庭容错协议,采用后量子加密工具来抵御具备量子计算能力的对手. 在量子区块链方面,研究者通过将量子计算和量子加密技术深度融入区块链架构,提出了新型共识机制和量子区块链. 针对传统共识协议易受量子算力攻击的缺陷,Wang等人[38]提出了基于非对称量子加密的区块链算法,该算法通过结合委托权益证明共识算法和节点行为评分机制,选举出见证节点以负责区块生成,避免了传统PoW共识算法中对算力的竞争,有效抵御了量子计算对传统PoW算法的威胁. 同时,区块内包含经过量子签名验证的交易信息,利用量子态的不可区分性和不可克隆性,确保交易信息的不可伪造性和抗量子攻击能力,为区块链提供了更高的安全性和效率,但是无法完全防止投票信息被窃取或篡改. Li等人[35]提出了基于量子投票的新型共识机制,该机制通过量子投票选举代表节点,利用量子特性和量子纠缠确保投票过程的安全性和公平性,再由代表节点构建量子块,量子块通过量子纠缠链接形成区块链.

3.2 编辑权限与内容安全

区块链的不可篡改性作为其核心特性,是区块链赋能数据安全的主要原因之一. 但其不变性也带来了一定的安全和业务问题. 在数据安全层面上,不法分子可能会利用区块链传播不正当内容,区块链参与者可能会因为无法识别非法或不当信息而无意中助长其传播. 从法律层面看,区块链的不可篡改性与《通用数据保护条例》规定的数据“被遗忘的权利”等法规相矛盾. 在业务需求层面,基于区块链的应用程序也存在弹性数据管理的需要. 因此,为擦除一些数据,Ateniese等人[39]提出可编辑区块链技术,便于以可控的方式打破不可篡改性.

根据可编辑区块链方案的数据修改机制是否主要依赖于密码学技术,将其分为基于密码学的可编辑区块链和非密码学的可编辑区块链. 基于密码学的可编辑区块链又分为基于变色龙哈希的可编辑区块链[39]和基于RSA的可编辑区块链[40],这两种技术都拥有陷门密钥,可以在不改变哈希值的情况下对区块的内容进行修改. 具体来说,基于变色龙哈希的可编辑区块链是通过特殊的哈希函数性质来实现内容变哈希值不变;而基于RSA的可编辑区块链利用模幂运算和大整数分解的困难性来保证安全性. 基于非密码学的可编辑区块链方案通过预定义的规则与共识机制来实现数据编

辑. 这类方案通常通过设计特定的区块链结构(如单链、双链或多链),并采用追加或替换等操作方式,在达成共识后对数据进行修改,以保证数据的一致性和可追溯性[41,42]. 通过分析上述可编辑区块链研究方案,本文将从两个角度针对可编辑区块链存在的问题展开讨论:权限安全问题和内容安全问题.

3.2.1　编辑权限安全

可编辑区块链技术能够容许链上数据的更新,但若编辑权限管理不当,可能会影响链上数据的完整性. 根据编辑权是否依赖个体,研究者们将当前编辑权限的组织架构分为三类:中心化、半中心化和去中心化,并具体讨论其存在的安全问题.

(1)中心化. 在基于变色龙哈希算法的可编辑方案中,陷门密钥由中心化第三方生成[43]. 若第三方宕机或遭受恶意入侵,便无法执行编辑操作.

(2)半中心化. 半中心化的分布式陷门生成机制通过多用户协同工作模式有效解决了中心化架构的单点信任问题. 该机制采用门限秘密共享算法实现密钥份额的分布式管理. 此外,系统设计了动态节点管理协议,使得委员会成员在不触发密钥重构的前提下即可实现身份注册与安全退出,从而保障了编辑操作的高效性和系统可用性[44]. 值得关注的是,这种密码学驱动的架构设计虽然提升了系统安全性,但带来了巨大的加密开销.

(3)去中心化. 在去中心化网络架构中,现有方案采用基于共识投票的编辑权限决策机制. 该机制虽然通过分布式决策有效降低了加密开销,但出现了显著的系统效率瓶颈[45]. 首先,多轮投票协商过程导致的时延累积问题会放大交易确认时间;其次,基于阈值的动态参与机制存在共识失效风险,当活跃节点数量未达到预设的参与度阈值时,系统编辑功能将无法执行. 因此,为了解决系统效率瓶颈问题,研究者们从影响系统效率的投票时间和可信节点入手,通过限制投票时间和保证编辑所有者可信,以此来提高系统效率. Dai 等人[46]提出动态委员会机制限制投票节点数量,基于门限机制提前结束投票,将投票结果嵌入到区块链传播过程,并同步验证区块,进一步提升效率. Li 等人[47]将投票阶段从共识层分离出来,构建动态快速委员会限制投票节点数量,基于门限签名机制和无陷门累加器提前结束投票并加速验证过程.

3.2.2　编辑内容安全

可编辑区块链对链上数据的编辑方式分为追加和替换两种,不同的编辑方式影响着区块链系统的性能和正确性.

(1)存储成本. 部分解决方案采用追加的方法,不断在逻辑上追加新交易来代替旧交易. 这种方法虽然保证了数据的可追溯性,但造成大量空间浪费,极大增加存储成本[38].

(2)交易一致性. 现有研究方案采用替换的方法修改数据,用新数据覆盖旧数据,这种方案虽然节省了存储空间,但当数据存在关联性时,编辑失误也会导致相关数据失效. Li 等人[48]设计“影子”交易机制,将交易分为稳定字段和可修改字段两部分. 使用影子交易替换原交易,同时保留签名链的完整性. 但对数据关联性的可编辑区块链研究较少,更多方案仍局限于审计追溯层面[49,50].

3.3　审计效率与集成安全

云计算作为承载海量数据的便捷平台,提供大数据分析、存储和计算功能[51]. 然而,在数据外包场景下,用户失去对数据的控制权,当不可信云服务器出现如故障、操作失误或为节省存储成本而隐瞒其已删除或篡改数据的行为时,用户的数据将在不知情的情况下丢失或损坏[52]. 因此,确保存储数据的完整性至关重要. 为此,Ateniese 等人[53]首次提出数据持有性证明算法,通过同态验证标签和抽样策略等方法,实现数据完整性审计. 基于云的完整性审计方法相关研究开始发展,该研究主要由用户提出挑战信息,云服务器提供完整性审计证明给可信第三方并告知给用户. 但该方案仍未解决共谋攻击[54~57]、仲裁困难[58~60]、单点故障[61]安全问题.

针对单点故障和共谋攻击问题,Li 等人[62]采取协作式审计减少对外部实体的依赖,但仲裁审计困难仍是一个未解决的问题. 为了弥补基于云的完整性审计方案的缺点,利用区块链进行完整性审计的方案受到关注. 方案采用区块头的 nonce、hash 作为随机挑战种子,元数据存储在区块链上,智能合约执行验证流程,以区块链作为各方通信平台,保证验证过程的公平和可信. 多数基于区块链的完整性审计方案主要集中在对功能的改进. Miao 等人[63]提出了一种区块链辅助的支持故障定位的多副本可证明数据拥有方法,该方法通过在区块链上部署智能合约,并结合二分搜索技术来实现故障数据块的定位. Wang 等人[64]提出基于区块链的数据一致性验证方案,该方案不仅实现了故障定位,还将用户、审计方以及云存储服务器之间的交互记录存储在区块链上,便于事后查证. 然而不同用户可能上传相同数据,导致云上数据量激增,存在存储空间不足和通信成本增加等问题. 为了解决上述问题,在完整性审计之前会对数据进行去重. 数据去重方案与完整性审计相集成的研究仍面临着隐私与可用性冲突以及动态数据审计效率两大问题.

3.3.1　隐私与可用性冲突问题

现有重复数据删除与完整性审计方案通常基于所有权证明机制实施完整性验证,并依赖消息锁定技术

实现相同文件去重,然而当多个用户对云存储中的相同数据检索时,不仅会向云服务器暴露用户间的协作关系,还会因公共审计日志的透明性导致用户隐私泄露[65];同时,由于低熵数据对字典攻击和离线穷举攻击的脆弱性,云服务器可能通过密钥推测伪造有效认证标签,进而篡改审计结果[66],这些安全缺陷使得现有方案在隐私和可用性方面面临挑战.

为了解决隐私与可用性问题,Song等人[66]提出了一种可审计的安全重复数据删除方案,该方案引入多个密钥服务器来生成加密密钥,从而防止攻击者通过字典攻击推导出密钥.但审计要求用户保持在线状态,给用户带来了高昂的通信成本.Li等人[65]提出了基于区块链的透明完整性审计和加密重复数据删除方案.该方案采用双向所有权证明,用户和云服务提供商可以相互验证对数据的所有权,避免了去重过程中验证信息的丢失,同时保证去重后的数据仍具有完整性审计能力.Miao等人[67]提出基于身份广播加密的无密钥重复删除协议和数据完整性审计协议,该协议利用收敛加密技术,实现云服务提供者端的身份认证重复数据删除,并提高了审计结果的可信度.

3.3.2 动态数据审计效率问题

用户对云服务器上的数据操作具有动态性,在实际应用中,动态数据的审计也更符合现实需要.然而大部分数据审计方案完整性审计效率较低,或缺少对动态操作的支持,影响系统的可用性.针对动态数据审计效率低的问题,现有方案采用批量操作或将相关数据绑定实现动态数据的高效审计.Tian等人[68]提出高效完整性审计的可编辑区块链方案,该方案采用聚合向量绑定区块数据和区块头,实现轻节点对区块数据完整性的快速验证.Zhang等人[69]提出了一种基于区块链的动态数据审计方案,将时间戳封装到同态可验证标签中,利用默克尔哈希树来存储标签,实现了数据完整性和时间戳有效性的同时检测.然而链上开销随着审计请求的增加而线性增加,区块链网络将不可避免地超载.为此,Zhang等人[70]提出了一种高效的多副本数据完整性审计方案,该方案使用多项式承诺技术将批量审计证明大小固定为一个常量值,通过固定的链上存储开销显著减少区块链资源的消耗.

3.4 小结及分析

数据的完整性是存储系统的信任基石,确保数据在链上不被非法篡改.由前述分析的内容可知,现有区块链赋能数据完整性研究仍存在一定的发展空间.

(1)共识机制的量子安全.现有工作从抗量子算法与量子区块链两种思路来解决量子共识机制的安全性威胁.抗量子算法通过引入后量子密码算法实现抗量子功能.量子区块链在共识算法中融入量子特性,提出量子拜占庭共识、量子投票共识等抗量子共识算法.然而,上述两种方案需要高度复杂的量子计算和密码学知识,面临开发部署难度大、能耗高、计算存储资源需求高等挑战.

(2)可编辑区块链技术.可编辑区块链技术围绕“可控编辑”核心目标展开.在操作权限层面,研究者们采用半中心化和去中心化方式授予编辑权限.然而去中心化和半中心化方案对于授权节点的恶意行为仅能在事后发现,不能有效地挽回损失.去中心化方案虽然通过限制投票节点数量或提前结束投票以此来限制投票时间,但限制了应用场景,可扩展性较低.未来可以构建异步投票架构,从不同维度充分利用计算资源.

在编辑内容安全问题上,当前研究通过替换或追加实现数据修正.然而关联性属性的数据编辑功能仍局限于审计追溯层面[49,50],编辑被依赖数据可能引起关联数据的逻辑冲突与状态不一致问题.现有方案对编辑区块链中关联关系的研究并不充分,若在编辑中加入对关联关系的分析,则编辑行为将涉及多方协同的复杂管理问题,这也是实现高质量数据融合与提升数据完整性的前提.此外,目前暂无解决存储空间优化问题的方案.随着追加数据量的攀升,脏数据也会随之增加.对大量脏数据进行清理不仅可以充分利用空间还能够降低区块链系统负载.

(3)基于区块链的完整性审计.区块链审计技术研究集中于解决隐私与可用性权衡和动态效率瓶颈问题.未来研究需聚焦于密码学创新、动态架构设计与跨链协同优化.通过深度融合区块链的可信特性与密码学工具,结合轻量化验证与智能合约自动化管理,有望突破现有技术局限,构建兼顾高效、安全与隐私的新一代审计体系.

4 区块链赋能数据存储可用性

数据存储在日常面临着多种可用性威胁,这些威胁可能来自外部攻击或系统内部功能的异常.根据异常原因,可以将其归为拒绝服务(Denial-of-Service,DoS)攻击和低效率功能威胁.

4.1 DoS攻击

区块链的分布式架构特性提升了系统透明性与抗审查能力,但其开放性设计也进一步扩大了攻击面.根据OWASP Web3安全报告,针对存储层的DoS攻击已成为影响数据可用性的首要威胁.此类攻击通过定向耗尽节点资源,致使合法用户无法访问链上数据并进行交易验证,对Web3生态系统、数字孪生平台等关键基础设施构成风险.基于对近年来DoS攻击研究的调查,本节从计算资源消耗和服务中断两个维度分析其主要安全问题,并对所提出的DoS攻击进行总结,如表3所示.

表3　区块链DoS攻击汇总

文献	攻击类型	具体攻击形式	攻击原理	挑战
文献[71]	共识干扰型	基于自私挖矿的DoS攻击	攻击者通过隐藏自己挖到的区块,试图在私有链上积累更多的区块,从而在分叉竞争中占据优势	攻击方与诚实矿工的博弈演变
文献[72]		基于竞争贪婪的SDoS攻击	当攻击者建立私有链并取得领先时,不广播完整区块以获取即时奖励,而是选择性发布区块头,使网络陷入“伪链头”状态,从而影响诚实矿工的挖矿意愿	区块链真实状态难以判断,干扰诚实矿工决策
		基于跟踪贪婪的SDoS攻击	当对手落后时,攻击者并不会急于接受公共链,而是继续在私有链上挖矿,试图重新创建分叉,以获取区块奖励	分叉情况复杂,影响诚实矿工挖矿策略
		基于混合贪婪的SDoS攻击	通过同时采取延迟区块发布和选择性广播,进一步增加了对其他矿工的干扰	攻击行为难以预测
文献[73]	经济勒索型	经济可持续DoS攻击	通过破坏服务并要求大量额外付款,从而导致重大财务损失	攻击较为隐蔽且资源消耗大
文献[74]	资源耗尽型	基于委员会节点的DoS攻击	通过向委员会节点发送大量无效请求或交易数据,迫使节点消耗大量计算资源或带宽	攻击者动态调整攻击策略,使其难以有效防御
文献[75]		基于状态存储的DoS攻击	通过复制中间节点来增加区块链在维护和验证状态时所消耗的资源,从而削弱区块链的性能	检测困难和修复复杂
文献[76]		分布式DoS攻击	通过控制大量设备向目标系统发送海量的请求或数据包,从而耗尽目标系统的资源,使其无法正常响应合法用户的请求	攻击流量难以区分

4.1.1　计算资源消耗

现有DoS攻击从矿工算力和系统网络两个层面消耗区块链计算资源. 一方面,攻击者通过扭曲激励模型诱发算力停摆;另一方面,攻击者分别从决策层和网络层发动洪泛攻击耗尽节点资源,对区块链系统造成严重影响.

(1)矿工算力停摆. 在针对区块链的DoS攻击中,通过耗尽目标资源迫使其停止服务的攻击方式成本较为低廉. 为缓解此类攻击,研究者提出了多种对策,例如增加区块大小、提高交易费用或限制交易规模[77]. 然而在实践中,由于矿工数量众多且分布广泛,对区块链系统实施传统DoS攻击面临较大挑战. 因此,Wang等人[71]提出了一种新型自私挖矿的拒绝服务攻击(Selfish mining-based Denial-of-Service attack,SDoS). 该攻击巧妙利用区块链自身的奖励机制,诱使矿工自愿停止挖矿. 此举减少了矿工的整体算力投入,导致诚实矿工算力闲置. 攻击者只需控制超过19.6%的总算力,即可从中获利. 基于此,Wang等人[72]进一步提出了三种更为贪婪的SDoS攻击策略,对手通过调整私有链的策略,不仅进一步抑制了诚实矿工的挖矿积极性,还加剧了其算力的浪费.

(2)系统网络阻塞. 分布式拒绝服务(Distributed Denial of Service,DDoS)攻击通过对区块链网络的内存池进行洪泛攻击,严重影响合法用户操作. 为检测DDoS攻击,Kumar等人[74]提出基于雾计算的新型分布式入侵检测系统,该系统对传入流量进行评估,根据评估结果采取相应措施. 但该方案是事后进行处理,无法及时有效预防DoS攻击. 因此,Chen等人[78]提出基于硬件可信执行环境的许可区块链共识协议,该协议通过为每个区块选择一个不同的隐形委员会来防止攻击者锁定特定节点,并利用概率论和重复采样机制以压倒性的概率在所有节点中确认相同的区块,从而解决系统阻塞问题.

4.1.2　服务中断

区块链的数据服务场景依赖海量数据交易处理,却也成为攻击者诱发服务中断的焦点. 攻击者既可以通过存储与验证过载制造交易延迟,又能借第三方计费机制触发巨额支出,造成可用性缺失,本节接下来将从交易确认延迟和服务巨额付费两个方面展开详述.

(1)交易确认延迟. 在DeFi等应用场景下,大量交易被发送到单个分片中,导致区块链节点存储过载,无法支持web应用程序,影响系统可用性. 为了解决存储过载导致的交易延迟问题,Nguyen等人[79]利用可信执行环境,让区块链的验证器安全地执行事务分片算法. 与此同时,Tennakoon等人[73]提出交易验证和传播减少机制,通过改变区块的验证上链过程,防止交易的冗余验证和传播. 随着区块链攻击技术的发展,He等人[80]提出了一种新的攻击面,并基于此提出了一种检测困难且修复复杂的状态存储DoS攻击. 此类攻击通过提高与区块链状态存储交互的时间成本来削弱区块链的性能. 同时为了减轻基于状态存储的DoS攻击带来的影响,采用Verkle树替代MPT结构以减少节点更新和验证数量,同时调整Gas机制抵御状态存储的DoS攻击.

(2)服务巨额付费. 在云服务场景下,攻击者通过

经济可持续拒绝服务攻击(Economic Denial of Sustainability attack,EDoS)发起大量冗余请求,使得第三方云服务器下载次数激增,导致流量付费金额急剧增加,产生了不合理的财务负担. 通过对EDoS的研究,Ta等人[75]提出基于多头注意力网络的EDoS检测方案,该方案通过检查数据包和特征之间的注意力分数变化,帮助分类模块区分攻击流量和正常网络流量. 此外,Zhang等人[81]设计细粒度的访问控制方案,该方案将挑战明文的哈希值和数据所有者生成的相应挑战密文上传到区块链,然后区块链验证数据用户是否有访问数据的权限,避免半信任的云提供商和恶意用户串通发起EDoS攻击.

4.2 低效率功能威胁

区块链的去中心化特性实现了数据的安全性和不可篡改性,但传统区块链在数据读写操作方面存在效率低下的问题. 链式结构导致查询速度较慢,且所有节点需存储完整账本,浪费存储资源. 随着区块链应用和数据量的增长,数据存储的可用性受限和性能瓶颈等问题愈发明显. 因此,优化数据存储结构、提升读写性能成为区块链技术发展的关键.

4.2.1 区块链存储结构

(1)数据查询效率低. 传统区块链采用链式结构将数据存储和区块生成放在同一层级,缺乏跨层数据访问优化,导致查询路径过长,检索效率低下. 针对数据查询效率低的问题,Wang等人[82]提出基于区块链存储系统的跨层直接存储访问策略,该方案从分配策略和存储结构两方面优化当前的链下区块链存储系统,减少链下区块链存储系统的读/写放大并降低访问延迟. 然而,其冷启动优化依赖动态内存表扩容与后期压缩操作,可能引入额外写开销. Guo等人[83]提出基于有向无环图(Directed Acyclic Graph,DAG)的去中心化存储网络,支持存储多版本文件时的文件级重复数据删除. 在更新文件时,采用增量生成方法,仅计算和存储增量,而不是更新整个文件,从根本上规避冷启动问题. 该方案还引入了基于DAG的两层区块链账本,可以直接使用区块链数据库提供灵活且节省存储的文件索引,而不会产生额外存储开销.

(2)存储优化不足. 区块链上所有节点均需存储整个账本数据,浪费大量资源. 特别是在分片区块链中,委员会成员的动态加入和退出使得每次变动后都需要重新同步数据,这显著影响了系统的可用性和效率. 针对存储优化不足导致的数据可用性问题,Qi等人[76]采用一致性哈希划分全局状态数据,使得在网络变化时,只有小部分状态数据需要迁移到其他分片. 其次,结合默克尔树和B+树的特点,提出新的数据存储结构,用于在每个分片内部管理状态数据,优化数据的读取和写入性能. 此外,设计委员会添加和移除协议,允许新分片在迁移期间继续处理交易和提供状态数据的认证查询,从而保证系统服务的连续可用性.

4.2.2 区块链数据服务

在信用调查、供应链管理、健康分析等应用场景中,区块链难以提供高效的在线分析处理服务,限制其在实际场景中的应用. 针对区块链搜索结果的及时性与更新速度问题,Liu等人[84]提出区块链数据库上富查询的新鲜度认证框架,该框架保证用户以可验证的方式高效地从区块链数据库中检索最新的数据. 而在提升区块链分析能力方面,Wang等人[85]提出SQL支持的区块链框架,其通过关系化重组链上数据以支持完整的SQL操作,并设计了关系版本控制方案来保障事务的原子性与一致性. 上述研究分别从查询结果的可验证性与分析能力的完备性两个关键维度,共同推动区块链作为实用数据库的发展.

4.3 小结及分析

存储可用性确保数据可被授权访问,是服务连续性的保障中枢. 本节从计算资源消耗和服务中断角度分析DoS攻击和低效率功能威胁,优化系统的安全性和数据的可用性.

(1)DoS攻击. 区块链的分布式架构提升了可用性,但其开放式设计使DoS攻击成为核心威胁,攻击者通过耗尽资源破坏系统可用性. 现有研究提出分片优化、可信执行环境、访问控制等方案解决资源消耗和服务中断问题. 然而可信硬件可能存在单点故障风险,动态共识调整机制在超大规模网络中也存在效率瓶颈. 未来可探索轻量级零信任架构的DoS防御模型,结合智能合约和边缘计算技术实现攻击预测和资源弹性分配.

(2)低效率功能威胁. 区块链的低效率功能主要源于数据存储和查询效率的问题,传统链式结构.

存储资源浪费、可扩展性受限和查询速度慢,影响其在高效数据处理场景中的应用. 尽管研究人员提出了诸如跨层存储访问、DAG存储网络及新型数据结构与协议等优化方案,并努力提升查询分析能力以改善效率和拓展实际应用,但由于区块链自身的性能瓶颈,现有优化方案难以彻底解决高并发、大数据查询复杂等问题. 未来,区块链的低效问题有望借助多技术融合实现突破. 一方面,通过引入人工智能和物联网技术,优化数据处理与分析流程,提升系统智能化水平;另一方面,进行区块链自身架构的创新,如分片机制、共识协议优化等,增强其性能. 同时,随着研究的深入,更高效的数据存储与查询方案或将涌现,有望在高并发、大数据量场景下突破现有瓶颈,使复杂SQL查询等操作更加高效.

5　区块链赋能数据存储隐私性

为保障共享数据存储的隐私性,通常情况下需采用加密算法将数据存储到区块链上,通过身份验证管理用户,根据用户身份管理访问权限实现存储过程的隐私.

5.1　身份管理

身份管理技术作为隐私保护的关键环节,能够确保用户身份信息的安全存储、传输和使用,防止身份信息泄露和滥用. 然而,传统的身份管理依赖中心化系统,其固有的单点故障风险制约系统可靠性,成为发展的关键瓶颈. 区块链的去中心化特性弥补了传统身份管理遇到的问题,表4为在解决身份管理安全问题上,区块链技术方案与传统方案对比分析.

表4　面向身份管理安全问题的区块链技术方案与传统方案对比分析

安全问题	传统身份管理	区块链身份管理
信息篡改问题	易遭受篡改	数据不可更改
身份管理和安全问题	更新系统,打补丁方式	经济奖惩机制
恶意用户问题	多采用冻结或关闭用户账户的单一模式,无法实施对用户的适度惩戒	全网公开所有的交易记录,并利用共识机制对交易进行背书和验证,恶意用户无法作恶

为实现分布式管理目标,需将验证后的交易数据广播至全网节点,并通过共识机制使所有参与节点对账本状态达成一致,最终保障数据的全局一致性. 然而现有数字身份方案存在以下安全问题.

(1)跨域身份管理问题. 现有跨域身份管理方案主要分为集中式解决方案和基于区块链的身份验证两种. 集中式身份验证方案依赖于可信第三方管理认证或更新假名,存在单点故障问题. 基于区块链的身份管理技术弥补了集中式身份验证方案的缺点. 根据对跨域身份论文的整理,分析比较了基于区块链的不同身份标识技术,如表5所示. 基于区块链的跨域身份验证方案多为静态的,没有考虑域间的交互与变化,这种局限性导致实际应用中通信延迟、计算复杂、存储开销大、密钥管理困难等问题. 针对上述问题,现有研究采用优化身份认证算法和批量认证请求等方式解决. Zhang等人[86]提出基于区块链的边缘计算跨域认证方案,该方案基于数字证书和签名的跨域双向身份认证算法,利用区块链在不同域之间共享信息,以减少计算开销. 然而,随着身份数量的指数级增长,节点存储空间需求也随之呈指数级上升. 为了解决存储开销,Cui等人[87]提出基于区块链的跨域认证协议,该协议基于假名的隐私保护方法将可信第三方生成假名的任务转移到边缘服务器上,以保证设备的条件匿名性,同时该设备通过批量请求假名减少交易数量,从而降低区块链上的存储开销. 同年,Zhang等人[88]提出基于无状态区块链的轻量级身份管理架构,该架构结合基于RSA的累加器,使身份集成为常数身份承诺,并将其添加到区块头 中,使得存储空间不会随着数据量的增加而呈指数级增长. 但无状态区块链需要节点之间频繁地同步累加值和证明,这在网络条件不佳的情况下可能会导致延迟增加,影响系统的整体性能. Meng等人[89]基于区块链的车载边缘计算网络提出轻量级的多实体认证组密钥协商协议,该协议通过划分计算任务并将其分配给多个路侧单元以减少延迟,实现了车辆、路侧单元和可信机构之间的轻量级匿名认证,允许车辆在保证安全的前提下动态地加入或离开边缘网络. 为了解决密钥管理困难问题,Liu等人[90]提出基于区块链的分布式密钥生成和认证方法,该方法基于区块链的轻量级跨域认证架构,引入分布式密钥生成方法,改变了密钥基础设施.

表5　基于区块链的身份标识技术现状比较分析

身份标识技术	实现原理	实现方式	中心化程度
公钥转换	公钥密码算法	公私钥对	去中心化
数字证书	PKI/CA	数字证书	中心化
分布式数字身份	分布式数字身份技术	规范和可验证凭证	去中心化

(2)身份隐私泄露问题. 在数字化应用场景中,用户的身份信息面临着被过度收集滥用和隐私暴露风险. 针对身份信息泄露的问题,研究者们提出了身份隐藏技术方案. Yu等人[91]通过基于身份的加密技术,确保用户身份在数据存储和查询过程中的匿名性. Bao等人[92]采用匿名凭证和不可链接性技术,确保身份在跨域认证中的隐私保护. Zhu等人[93]采用无证书签名技术和预认证机制,避免中心化依赖,在降低计算与通信开销的同时保障隐私和身份安全. Zhang等人[94]提出基于区块链和去中心化身份技术,用户通过域注册生成凭证即可进行跨域认证,无需重复注册,从而提升效率并保护隐私. 综上,现有身份认证分为实名认证、匿名认证、可控匿名认证,其中可控匿名认证介于实名认证和匿名认证之间,用户可以自由选择是否公开身份,采用分布式数字身份(Decentralized Identifier,DID)、群签名技术实现身份标识. 具体身份认证方式比较如表6所示.

(3)数据非法访问问题. 传统的身份验证方法容易受到安全威胁,如密码泄露、暴力破解、钓鱼攻击等. 这些攻击手段可以轻易地盗用用户身份,导致用户账户被非法访问和操作. 为了提高安全性,通常需要更有效

表6 基于区块链的身份认证方式比较分析

身份认证方式	身份标识	应用场景
匿名身份认证	公钥、公钥+零知识证明	比特币、以太坊
实名身份认证	数字证书、DID	Fabric
可控匿名身份认证	DID、群签名、隐蔽身份	Fabric、FiscoBcos

的身份验证机制,单一的密码验证已经不足以应对复杂的攻击环境.针对用户非法访问问题,多数方案采用基于区块链的多因素认证技术,减少身份被盗用风险.Popa等人[95]采用区块链技术分布式存储用户标识和身份验证,利用数字签名和哈希技术保护隐私.Xu等人[96]引入模糊提取器和生物特征数据,结合密码学方法构成多因素认证机制.

5.2 密文存储

基于区块链的加密算法保护了数据完整性和隐私性.然而,量子算法能够以多项式时间高效破解基于整数分解和离散对数问题的加密方法,对这类隐私保护方案带来了威胁,直接影响区块链的安全性,导致交易数据和存储信息存在被篡改和泄露的可能.

基于格的加密算法对量子计算展现出的抗性,使其成为区块链存储抵御量子计算的核心技术,并被多个研究团队应用于保护数据隐私、实现匿名性、可追溯性及动态密钥管理.Sezer等人[97]使用格加密和零知识证明保护工业物联网数据隐私,结合智能合约降低通信开销并支持分层隐私管理.同样,Chen等人[98]设计基于格加密的环签名,结合区块链分布式存储机制,确保数据不可篡改、匿名性和可追溯性,同时防止量子攻击.Shekhawat等人[99]基于格加密技术设计无证书数据认证和密钥交换方案,结合区块链存储身份信息和加密数据,支持动态密钥更新和条件匿名.此外,曹博雅等人[100]提出基于格的可监管区块链隐私保护方案,该方案利用格上R-LWE困难问题与R-BGV加密方案设计用户身份公钥证明,实现用户的匿名与身份可监管.

5.3 小结与分析

存储隐私性是合规与伦理的守护边界,同时加密机制反向促进完整性保护.本节从身份管理和密文存储两方面介绍区块链赋能隐私性的相关威胁,并归纳总结不同技术特性.现有区块链赋能隐私性上仍存在不足,具体表现如下:

(1)身份管理.现有论文集中研究资源受限情况下的跨域身份管理方案来防止数据隐私泄露,面临着存储开销大、计算成本高、动态密钥管理困难等问题.研究者们采用边缘计算、智能合约等技术保证跨域节点间可信.但方案只是单一解决了其中一个问题,导致当前缺乏能在异构网络环境中同时满足低时延、轻量级存储与强隐私保障的协同优化方案.

(2)密文管理.基于格的加密算法能够抵抗量子算法攻击,为区块链存储提供了长期的安全保障.然而,该算法计算复杂度较高,可能会导致存储和处理开销增加,对于资源受限设备不友好.其次,在具体应用方面,从传统的加密算法到后量子加密算法迁移,需要考虑其现实系统的兼容性和过渡成本.

6 区块链赋能数据存储可扩展性

随着用户数量和访问需求的增加,现有区块链体系结构可扩展性不足导致的性能瓶颈问题制约了区块链技术的应用和推广.共识机制和区块链结构很大程度上影响了区块链系统的性能.共识机制在运行过程中产生的系统吞吐量、共识时延和运行成本等核心指标,直接决定了区块链网络的扩展维度.在区块链架构层面,分片机制是对区块链系统进行扩容的最直接且最有潜力的方案,它将网络参与者按特定算法动态划分为若干个共识单元,每个分片独立处理交易子集,从而在共识层实现横向扩展,显著提升网络的整体并发处理能力.

6.1 共识协议

共识机制作为确保链中各节点对数据达成一致的重要算法直接影响数据的安全性、可靠性和可扩展性.与传统的集中式系统不同,区块链通过去中心化的方式维护一个共享账本,这要求所有节点在没有信任基础的情况下协作,并对交易或区块的有效性达成一致,这也是共识协议广泛应用的核心原因之一.当区块链技术赋能物联网等场景时,底层系统必须具备高效处理高并发业务的能力.然而,这种能力的提升面临着诸多制约因素,其中单节点性能瓶颈以及网络通信开销较大问题尤为突出.基于以上背景,本文将深入探讨现有共识协议所存在的成本开销大、边缘设备适配性低和大数据处理局限等问题.

(1)成本开销大.传统的区块链共识协议多适用于资源消耗密集型环境,往往存在成本开销大的问题.其不仅体现在带宽资源消耗上,更涵盖了巨大的计算、存储及高昂的运维成本,极大地限制了系统在高吞吐量场景下的可扩展性.为应对共识机制高能耗导致的效率低下问题,Hao等人[101]提出了一种结合抽签与投票机制优势的高效区块链共识协议,提供了可持续高性能的解决方案,但其研究未能量化评估在网络拥堵条件下的延迟表现.与此同时,Li等人[102]提出基于区块链架构的分布式两层信任管理框架,该框架采用轻量级Q学习改进的共识算法,有效破解了区块链共识机制中的高能耗问题,并通过设计云边端分层结构,成功解决了资源受限难题,进一步提升了物联网应用的安全性.但在基于Q学习的投票优化算法中,由于初始状态转移具有随机性,可能导致部分节点获得不公平的

利益分配. Zhao等人[103]提出基于轻量级模型的进化共识协议,通过机器学习方法解决区块链即服务中物联网系统的共识问题. 该协议利用监督学习算法训练模型来选择矿工,将共识过程封装在一个“黑箱”中,使得外部或内部攻击者难以准确预测下一个矿工,从而提升安全性. 它通过预训练模型实现高效共识,降低了计算和通信开销,并设计了动态机制以应对节点的动态加入和退出,提高了系统的适用性和可扩展性. 尽管进行了广泛的实验和模拟,但其性能测试主要是在原型系统和模拟环境中进行的,缺乏在真实物联网环境中的长时间运行和大规模验证.

(2)边缘适配性低. 在资源受限的场景下,共识机制需要动态调整以适应环境变化. 然而现有共识机制多为有线网络设计,依赖于网络的稳定性. 通信链路不稳定导致的数据包丢失,不仅会制约共识机制的成功率,同时也会造成边缘计算场景适应性不足的问题. 为了应对共识算法难以动态调整的问题,Cheng等人[104]提出了基于模块化区块链的自适应共识协议. 该协议利用机器学习模型,综合考量网络规模、错误节点比例、网络延迟等特征因素,以各类共识算法为标签,经过对不同模型的训练与测试,挑选出准确率最高的模型接入区块链系统. 在实际运行过程中,协议会定期获取当前网络状态,并将正在使用的共识算法与模型预测出的最优共识算法进行对比. 倘若两者不一致,协议将广播交易提案,进而触发共识算法的替换流程,由此实现了在区块链运行时动态更换共识算法. 然而,共识算法切换需要投票,影响实时性,且切换依赖离线训练的模型,动态环境数据不足也可能影响其准确性. Wang等人[105]提出基于Raft协议的飞行自组织网络共识方案,该方案在领导者选举阶段,集成了多标准决策和链路预测算法,设计了一种高效的稳定领导者选举方法. 在共识阶段,提出了一种基于历史验证信息的动态区块验证算法,以实现高效的区块共识. 但该协议基于Raft协议改进,仅适用于许可链,不支持拜占庭容错,且在无线通信环境中仍存在通信开销较大和资源消耗高的问题. 而无线通信环境本身的特性,恰恰为解决这些高开销问题提供了潜在思路. Xie等人[106]提出了一种用于无线用户设备的拜占庭容错共识协议,该协议利用无线信道的固有特性,在接收来自用户设备数据的同时自动在物理层达成共识,减少了传统共识协议所带来的通信和计算成本. 上述研究正积极应对边缘适配性低的挑战. 未来研究方向应聚焦于提升共识机制在动态、资源受限环境中的适应性和效率,融合多种创新方案,以期在边缘计算场景下实现高效、可靠的共识机制.

(3)大数据处理局限. 大数据处理的核心挑战在于高效、可靠地存储、管理和分析海量数据,区块链技术作为分布式数据存储和处理的重要工具,其性能和扩展性直接关系到大数据应用场景中的效率和可靠性. 为了解决区块链技术赋能大数据领域的瓶颈,研究者们对共识算法进行了改进,通过整合不同共识算法优势设计可扩展性更强的共识算法. Tang等人[107]提出混合区块链共识算法,该算法采用茎叶链结构,茎链作为选举和信标链,通过容量证明算法提供系统的基本安全性和选举公平性;叶链作为交易链,通过许可的异步拜占庭容错共识算法实现系统的高吞吐量. 虽然容量证明算法相比其融合的两个算法有一定的优势,但安全性在一定程度上依赖于存储资源的投入,可能存在存储资源被恶意利用的风险. 针对这一问题,Shen等人[108]提出了一种基于保证树的节点可靠分片模型,该模型通过创建担保机制来表示节点间的信任关系,并设计可靠节点选择策略评估节点行为确定信任状态,识别恶意节点和选择可信领导者,从而在去中心化的基础上增强安全性. 同时,该模型还引入了双领导者监督机制,能够快速识别并切换异常领导者,减少对共识过程的影响. 此外,该模型采用基于担保机制和可靠节点选择策略的网络分片方法,实现了多个分片的高并发共识. 这不仅保证了分片的可靠性,还有效提升了区块链的可扩展性. 与上述方案不同,Gai等人[109]提出一种共享内存池协议,该机制将事务分配与共识机制解耦,仅保留共识机制负责事务ID排序. 通过共享内存池架构,每个副本节点都能接收并转发客户端事务,使主节点仅需处理事务ID排序任务,缩小提案规模并提高了吞吐量. 大数据处理的核心局限在于现有技术的性能扩展存在瓶颈,使得无法满足海量数据的实时、高效处理需求. 上述研究分别从算法融合、信任建模与负载优化角度切入,有效提升了区块链的性能、安全性和可扩展性,为克服大数据处理瓶颈提供了重要思路. 这些进展显著增强了区块链支撑大数据应用的能力,未来有望在边缘计算等场景发挥更关键作用.

6.2　分片机制

分片技术通过将整个区块链网络划分为多个相互独立的分片,每个分片由其对应的节点负责本地事务的处理与状态的存储. 由于各分片能够并行地验证和处理事务,从而使得整个区块链系统的吞吐量几乎能够线性增长. 此外,随着网络中节点数量的增加,可支持的分片数也相应提升,从而进一步增强全网的事务处理能力与系统可扩展性. 分片机制主要分为网络分片、交易分片和状态分片三种,能够在提高性能的同时保证交易原子性. 网络分片将区块链网络中的节点分为多个小分片,每个分片包含一定数量的节点,这些节点共同负责处理该分片内的交易和区块生成. 然后采

用基于密码学哈希的随机分配算法将用户账户分配到相应的分片中,确保每个账户被分配到各个分片的概率相等,从而避免人为干预带来的偏差. 当发生跨分片交易时,通常需要通过特定的协调协议,来保证所有相关分片上的操作要么全部成功,要么全部失败,从而确保交易的原子性,但仍存在负载不均和并发性弱的问题.

6.2.1 面向解决跨分片负载不均衡问题

在区块链发展过程中,不平衡的交易负载和跨分片交易是区块链性能下降的主要原因[102],也是可扩展性发展的关键瓶颈. 为此,研究者们从交易分配优化、跨分片交易处理以及状态分片动态调整等多个维度入手,提升系统的整体效能.

(1)交易分配的随机性. 现有的分片系统通常采用随机分配算法将交易分配到不同的分片中,这种随机性可能导致某些分片接收到的交易量远高于其他分片,从而造成负载不均. 为了解决上述问题,Li等人[3]提出一种新颖的分片系统,该系统基于长短期记忆网络的机器学习模型,收集历史交易统计数据,以预测下一个时间段内各账户的交易数量. 该系统再依据交易预测结果以及当前各分片的负载状况,精准决策账户的迁移目的地,以此动态平衡不同分片上的交易负载. 然而当账户在不同分片之间迁移时,目标账户的状态及其相关交易都需要被锁定,导致了相关交易的处理时间较长. 为了解决该问题,Huang等人[110]提出微调锁定协议,通过修改区块链的账本状态和区块的数据结构,使账户迁移期间仅锁定迁出账户的付款方交易,而收款方交易能在源分片继续处理,以此降低关联交易的完成时间,解决跨分片负载不均衡问题.

(2)状态分片的动态调整不足. 状态分片中账户状态划分策略不合理将导致各个分片的交易负载不均衡以及跨分片交易比例过高. 此外,现有的分片系统在按既定规则将交易映射到分片时,并未考虑分片内各节点的能力差异,节点仅依靠随机分配,可能会出现某个分片负载大但节点性能差的情况. 针对状态分片动态调整不足的问题,Jia等人[111]通过引入多级状态模型、灵活的状态分割与聚合机制,有效降低了跨分片交易的比例,缓解了分片工作负载的不均衡,大幅提升了区块链系统的吞吐量和可扩展性. 这一机制虽然有效,但在面对活跃账户频繁发起交易导致的热分片问题时,可能无法实现完全的工作负载均衡,从而影响交易确认的及时性. 针对这一问题,Huang等人[112]提出了基于账户余额的跨分片区块链协议,利用细粒度的状态分区和账户分段,使得良好分区的账户状态可以由多个分片分摊,以实现所有分片之间的工作负载均衡. 上述方案将状态与节点的静态绑定解耦,通过动态拓扑重组提升吞吐量并降低跨片交易频率,但仍面临高频交易响应与跨分片原子性挑战.

(3)跨分片交易的复杂性. 在分片数量较多的情况下,跨分片交易比例升高,这不仅导致热分片的交易确认延迟增加,还使得跨分片通信开销激增,进而加重了额外交易负载. 与此同时,冷分片区块的交易填充率不高,造成资源浪费. 此外,跨分片交易需要中继链协调各个分片上的交易,以确保交易的原子性和一致性. 然而,中继链的协调机制可能会增加通信开销和处理时间,进一步影响跨分片交易的效率. 针对中继链的性能瓶颈,Wang等人[113]提出了一个多中继架构,通过对中继链本身进行分片来提高中继链的可扩展性. 此外,还提出中继分片算法来动态调整中继数量或优化中继和分片之间的拓扑,以自适应地扩展中继链的性能. 针对跨分片交易处理延迟高的问题,Liu等人[114]提出灵活的跨分片拜占庭容错协议,该协议通过减少投票轮次和引入多签名聚合技术,降低了跨分片交易的确认延迟. 同时,Xu等人[115]通过基于历史交易模式的账户分配减少跨分片交易,同时引入乐观策略,将跨分片交易分解为多个子交易并行处理,仅在提交时验证有效性,显著提升跨分片交易的效率. 上述方案均通过空间和时间的角度降低跨分片协调成本.

6.2.2 面向解决并发性弱问题

分片机制通过将节点划分为多个小组,实现并行处理交易. 然而分片的大小以及分片间的协作设计都是影响并发性的重要因素.

(1)分片大小问题. 区块链系统通过配置大量小型分片提高交易并发性和吞吐量. 然而,简单地增加分片数量往往会导致部分分片损坏,这会威胁系统的安全性. 因此,现有的解决方案通常会配置较大的分片,以确保每个分片几乎不会被破坏. 但这种大分片配置不仅减慢了分片内部的共识速度,还减少了整个网络中的分片数量,从而显著降低了现有大规模区块链系统的交易并发性. 为了解决这个问题,Li等人[116]提出一种区块链分片系统,该系统配置较小的分片,允许部分分片出现故障或损坏,同时确保每个分片都受到多个其他分片的实时监控,在保护系统安全的同时允许存在更多恶意节点的分片,从而安全地减小分片大小. 同样,为了保证每个分片的安全和活性,David等人[117]提出基于安全-活性二分法的动态优化方案,该方法将分片共识中的活性和安全性分离,允许动态调整分片参数以实现最优效率. 上述方案通过打破安全性与效率的强耦合约束,实现分片规模与性能的协同优化.

(2)分片间节点性能差异. 节点之间的计算能力、存储能力和网络带宽存在差异,若高性能节点和低性能节点被分配到同一个分片,也可能会导致分片内的处理能力不均衡. Cai等人[118]设计了基于协作的分片

扩展方案,该方案采用双链架构分离交易记录与共识执行功能,实现跨分片合作,增强并发性. 此外,该方案采用基于投票的共识协议使每个分片的交易由所有分片同时投票确认,提高容错性并降低确认延迟.

6.3 小结与分析

存储可扩展性作为分布式系统的核心能力,为系统更新迭代提供弹性框架. 本节从共识机制和分片协议介绍可扩展性面临的威胁,并归纳总结针对不同威胁的可扩展性方案.

(1)共识协议. 现有共识协议的可扩展性受制于成本高、边缘适配性不足以及大数据处理局限三个挑战. 虽有轻量化改进、动态调整尝试及架构创新,但仍普遍存在普适性不够以及安全效率与去中心化难以平衡的问题. 未来可以聚焦于深度融合轻量化技术以降低成本、发展自适应机制,进而提升边缘动态环境适应力,通过优化负载均衡与探索高效混合架构来克服大数据瓶颈.

(2)分片机制. 分片机制通过将网络节点划分为多个子分片并行处理交易,显著提升区块链性能,但存在跨分片负载不均衡和并发性弱两大挑战. 在负载均衡方面,随机账户分配导致分片间交易量存在差异,引发了通信开销大与延迟高的问题. 研究者通过动态账户迁移、优化中继链架构以及细粒度状态分片等方案缓解负载不均,但仍需权衡状态锁定开销与系统复杂性. 在并发性方面,分片规模矛盾突出,同时节点性能差异进一步削弱并行效率. 其解决方案依赖动态分片调整和跨分片协作机制,以平衡安全性与吞吐量. 当前研究集中在动态自适应分片和轻量化跨片协议,但安全与效率的平衡仍是关键瓶颈. 未来需研究流量适应性、去中心化与性能的三角矛盾,并深化网络、共识、状态三层的协同优化,以实现分片机制在可扩展性与去中心化的统一.

7 区块链赋能大语言模型

上述数据存储安全服务属性为评估系统提供了基础框架. 与此同时,随着数据要素市场的发展及其价值体系的重构,数据质量也逐渐引起人们重视. 数据质量作为大语言模型(Large Language Model,LLM)训练的核心要素,贯穿模型开发的整个周期. 然而,当前LLM提供服务的核心矛盾在于其技术复杂程度与现有安全防护能力不匹配. 在模型能力提升的同时,数据安全不足、模型可信度不够以及模型部署成本高等关键挑战也日益凸显. 区块链凭借其去中心化特性,为破解LLM困局提供新的路径. 本章从区块链技术赋能视角出发,系统梳理LLM的解决方案,构建涵盖数据安全治理、模型可信增强与部署优化的多维分析框架,如图4所示. 区块链为数据采集、管理、隐私保护与溯源提供了关键技术支撑;同时,通过抵御攻击与量化评估机制提升了模型训练及输出的可靠性;并借助其分布式特性优化部署模式,有效缓解了集中式部署的延迟与成本压力.

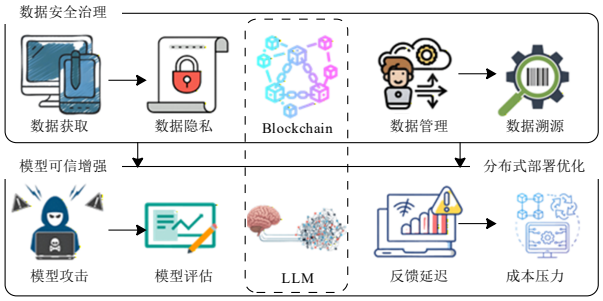

图4　区块链赋能LLM的主要研究方向

7.1 数据安全治理

数据安全治理流程包含数据的采集、管理、隐私和溯源四个阶段. 在数据采集层面,LLM面临数据时效性不足与隐私泄露的双重挑战. 现有方案主要通过跨链机制实现域间数据传输,并采用差异化隐私技术应对隐私风险. Su等人[119]提出基于混合检索增强生成的医疗框架,该框架利用层次交叉链设计实现安全的数据训练,并构建合同理论模型激励医疗机构以低信息年龄贡献高质量数据,从而提升医疗LLM的推理性能. 然而,该合同模型将医疗机构简化为二元分类,未能涵盖资源分配和政策变动等动态因素影响的更新频率差异;同时仅依赖数据新鲜度作为质量指标,忽视了临床关键数据的准确性与完整性. 尽管跨链机制支持域间传输,但通信过程仍存在隐私泄露隐患. 为进一步强化隐私保护,Kang等人[120]提出跨元宇宙赋能的双重假名管理框架,通过分层架构设计,结合零知识证明技术共同构建车联网可信交互机制. 该机制采用多个本地元宇宙协作形成全球元宇宙,实现双重假名管理,并利用公正机制的跨链技术完成虚拟终端迁移时的去中心化假名分发与撤销. 该机制提出的隐私熵模型虽能量化假名更换后的隐私水平,但仅基于位置信息的指数衰减假设,未验证对多源关联攻击的防御能力,导致隐私度量维度不足. 在数据全生命周期管理方面,Wang等人[121]提出分布式LLM框架,创新性地将模型输出验证与区块链存证相结合,确保数据完整性与可审计性. 该框架基于椭圆曲线密码算法的抗恶意敌手门限签名协议,通过融合离散对数证明与可验证秘密共享,在摒弃乘法三元组协议的前提下,实现分布式LLM中的高效数据认证. 但该协议计算复杂度随门限值增长呈二次方上升,限制了协议在大规模分布式系统中的应用潜力. 上述安全治理方案通常与特定场景绑定,主要关注安全交易协议和隐私法规,这些模型在处理数据流的动态性方面存在不足,未能全面覆盖整个数据供应链的需求. Liu等人[122]提出基于区块链的数据物料清单

方案,通过结构化元数据建模、分层式智能合约设计及细粒度访问控制机制,实现数据供应链的端到端治理.该框架将碎片化的数据治理转化为可证明安全的链上流程,为跨组织数据协作提供可审计、可验证且权责明晰的基础.区块链通过跨链机制融合密码学技术,在数据采集阶段保障域间传输的隐私性,并在数据管理阶段借助智能合约实现链上存证,为数据溯源提供不可篡改的完整性验证,从而将碎片化治理转化为可验证安全的动态流程,赋能端到端数据供应链治理.综上所述,通过区块链技术保障数据全生命周期的安全与可信,是构建可信LLM的基石与前提.在此基础上,研究者们进一步聚焦于模型训练与推理过程本身的安全威胁,提出了更深层的可信增强机制.

7.2 模型可信增强机制

确保数据安全仅为构建可信大语言模型的第一道防线.在此基础上,本节将重点探讨如何在后继的模型训练与推理阶段筑牢第二道可信防线,保障训练过程免受对抗性攻击与拜占庭故障等安全威胁,并对模型输出进行有效审计与评估.现有研究主要从这两个方面来提升模型的可信度.对抗性攻击通常由未经授权的恶意实体发起,它们利用模型漏洞窃取隐私信息、注入虚假数据,导致模型训练结果出现偏差.针对这些威胁,研究者们提出多种可信增强方案.Salim等人[123]提出基于区块链和联邦学习的大语言模型,该模型通过多特征编码设计了本地差分隐私协议,在数据源处添加噪声来平衡数据隐私性与实用性.在本地模型与区块链网络聚合前进行加密,有效抵御联邦学习过程中的对抗性投毒攻击.通过将秘密共享技术与区块链相结合,保障模型聚合和验证的安全性,同时在联邦学习模型训练过程中保护了用户数据的隐私性和完整性.随着多智能体系统规模的扩大,部分智能体的恶意操作风险上升,易引发决策失误.而基于大语言模型的多智能体系统面临的拜占庭问题更为复杂.一方面,LLM智能体可能继承了底层模型的偏见,表现出欺骗行为;另一方面,智能体数量的增加使得智能体与环境交互变得复杂且不可控,增加智能体间合谋的可能性.对此,Chen等人[124]通过区块链赋能的协作流程解决拜占庭攻击问题.首先基于历史贡献值筛选高信誉节点担任矿工角色,隔离潜在恶意节点;在评估阶段,矿工采用多维度提示词模板检测毒化内容,并启动多轮辩论式投票,每轮需超半数矿工达成共识,恶意评估会被实时修正或否决,且攻击者因低评分丧失贡献值而永久失去关键角色资格;最终所有操作记录于不可篡改的区块链上,实现恶意行为溯源与经济抑制的双重防御闭环.尽管存在上述解决方案,相关威胁仍削弱用户对LLM的信任,导致用户对人工智能生成的内容持谨慎态度.因此,对LLM行为进行追溯评估与量化衡量是保障模型可靠的关键环节.Sachan等人[125]提出链上审计方案,通过默克尔树指纹比对技术实现决策生成的全链路追溯.同样,Amine等人[126]研发声誉评估系统,该系统引入动态加权信誉模型,为LLM服务提供量化评估标准.通过区块链共识机制、分布式架构与链上追溯能力等技术支撑,为LLM的训练、推理与行为审计构建可信基座.

7.3 分布式部署优化方案

分布式部署优化对于计算密集型和资源需求高的LLM至关重要.传统集中式部署因其高度依赖云计算资源常面临响应时间长和带宽成本高的问题.这种高延迟和高成本严重阻碍了机器人控制、导航等实时应用的快速响应能力,降低模型的实用效能.为应对这些挑战,研究者们从边缘计算和激励机制入手增加LLM所需资源.Zhang等人[127]提出面向边缘计算环境的通用LLM推理框架,该框架利用动态规划算法,将计算密集型LLM拆分为可负担的分片,部署在分布式设备上,并在设备异构环境下优化推理延迟与吞吐量.在此基础上,Arshad等人[128]提出基于区块链的LLM集成框架,该框架将工作量证明与服务质量评估相结合,利用智能合约自动化执行激励机制,有效协调分布式节点的贡献度与收益分配.同时,通过分片技术的横向扩展和并行处理机制,显著提升资源受限环境下的计算效率.由此,区块链技术通过优化资源分配和强化安全保障两个维度,为提升应用场景下的系统性能和可靠性提供支撑.

7.4 小结与分析

本章主要介绍区块链赋能LLM的相关研究现状.在模型训练阶段,区块链的不可篡改性和智能合约执行机制为模型训练透明度与输出可解释性提供了技术保障.同时,区块链的分布式特性为LLM提供分布式部署方案,通过共识协议、智能合约等技术实现节点间资源的高效协作和合理分配,提高模型多场景适配度和生成内容可靠度.但是在模型可信、分布式优化等方面仍然可进一步改进.

(1)数据安全治理.尽管现有方案在隐私保护与管理上有所突破,其设计仍需进一步贴合现实场景,如增强隐私模型对多源关联攻击的鲁棒性、降低密码协议计算开销等,提升实际部署价值.

(2)模型可信增强机制.现有研究大多从模型训练过程的安全威胁和模型结果两方面来提升模型可信度.然而,在模型训练阶段,目前的应用策略只能缓解而不能彻底解决这些问题.对抗性攻击的检测和防御机制会影响模型训练效果,而拜占庭故障的处理机制需要额外的计算和通信开销,影响了实时检测的效率和适用性.在模型结果评估方面,为了优化多模态LLM

服务的安全评估,需要更全面的基准和更合理的指标.因此未来研究应侧重开发更加轻量化的动态防御机制和客观的安全评估机制.

(3)分布式部署优化.分布式部署优化方案多采用边缘设备提供计算资源,然而由于边缘设备的移动性和地理位置多样性等特性,边缘计算相较于云计算更容易受到安全威胁.此外,虽然边缘设备在一定程度上缓解了资源紧张问题,但边缘计算节点所提供的资源在短期内仍然有限.因此,为从根源上解决资源供需不平衡的矛盾,迫切需要开发轻量化的模型训练和服务方案,以实现对现有资源的高效利用,并更好地满足实际应用需求.

8　总结与展望

8.1　调研问题答案

区块链是密码学、共识机制、智能合约等技术的综合体,在工业物联网、智慧城市、元宇宙、LLM等行业有着广泛的应用.人们默认区块链可以赋能数据安全,但并未深入探究如何赋能以及赋能程度.本文从数据服务特性出发,选择研究者最关注的四个数据安全服务特性,在数据存储阶段展开讨论.下面将回答本文研究的三个问题.

8.1.1　区块链在存储阶段具备哪些安全能力?

本节将从数据安全服务属性的四个角度回答该问题.在数据完整性上,区块链结合共识机制、可编辑区块链以及完整性审计技术为存储阶段的全生命周期赋予数据完整性.具体来讲,构建量子区块链保证共识机制的量子安全,采用半中心化或去中心化可编辑区块链保证链上数据的一致性,研究智能合约与去重协议的协同方法实现隐私与多副本审计间的平衡,结合批量审计技术减少链上开销.在系统可用性上,通过调整区块链共识机制的内部结构和改进存储结构,解决可能遇到的DoS攻击和低效率功能威胁,从而提升系统透明性与抗审查能力,实现数据的安全性和不可篡改性.在系统可扩展性上,区块链集合共识协议和分片技术,从机制和区块结构上增强可扩展性.通过整合各类共识协议结合机器学习、聚类分析等技术实现轻量化,并动态调整交易实现工作负载均衡,提高并发性.在数据隐私性上,区块链利用其自身具有的加密机制保证存储数据的机密性,同时结合身份管理、访问控制、量子计算等技术增强数据隐私性.

8.1.2　当前存储安全体系存在哪些薄弱环节?

(1)可编辑区块链的权限与存储缺陷.去中心化方案对恶意编辑行为的检测依赖事后审计,无法实时阻断攻击.现有编辑技术仅支持单点数据修改,未解决关联数据的协同编辑问题,可能引发数据逻辑不一致.此外,若采用追加式编辑将导致“脏数据”累积,这种方式缺乏自动化清理机制,长期运行后存储负担激增.

(2)异步量子区块链共识协议研究不足.目前量子区块链研究方向多集中在同步拜占庭共识协议上,在实际应用中应允许任意长延迟,因此异步拜占庭共识算法更为实用,同步拜占庭算法研究缺乏在实际应用中的考虑.

(3)共识机制及分片负载适用性不足.改进的共识算法多针对特定场景优化,缺乏通用性,难以适配异构网络环境.此外,现有分片方案未解决跨分片交易的随机分配问题,导致分片间资源利用率差异显著,缺乏动态分片模式切换机制.

(4)性能、隐私、空间之间的平衡.现有防御机制多数依赖于可信执行环境,若可信执行环境被攻破,可能导致分片策略泄露或验证失效.而针对具体攻击所提出的解决方案,在高负载场景下,会加剧交易拥堵造成新的可用性瓶颈.此外,优化后的存储结构由于区块链本身限制仍难以支持大规模数据的实时复杂查询,从而制约区块链在分析型场景的应用.因此,在设计方案时,需要在性能、隐私、空间三者之间寻找平衡,实现资源利用最大化.

8.1.3　在大语言模型通用智能场景下区块链如何赋能数据安全?

区块链技术凭借其数据完整性、隐私性、可扩展性与服务可用性为构建面向LLM的数据安全存储平台提供了底层支撑.它通过链式存证与默克尔树校验机制确保训练数据与参数的不可篡改性,并利用模型输出的链上哈希指纹实现生成内容的全程审计.在隐私保护方面,结合身份认证与密文存储,确保车联网等场景中的敏感数据共享保持“可用不可见”,同时减少针对模型参数逆向攻击的可能性.在可扩展性与服务可用性方面,区块链通过分片技术与边缘计算架构优化LLM部署方式.其“思考证明”共识机制将模型推理逻辑量化为节点贡献权重,使得区块链不仅能验证数据真实性,还能直接参与模型训练过程监管,既防止模型被投毒,又保障了训练效率.此外,智能合约为高并发场景提供了弹性扩展能力,而链上声誉系统则基于历史行为数据为节点建立可信画像,支撑复杂环境下的服务择优与故障追责.最终,区块链通过去中心化架构、不可篡改存证和智能合约自动化,为LLM构建了覆盖数据安全、模型可信、高效部署的全流程赋能框架.

8.2　发展趋势展望

(1)量子密码增强.量子计算与区块链的研究主要体现在量子共识机制、量子密钥分发算法及量子通信资源态三个方面.目前的共识算法研究多集中在量子拜占庭共识协议方面,异步量子拜占庭协议被认为是

实际应用的必经之路. 此外,现有的共识算法依赖随机数来确保节点选举的公平性,但这些随机数通常基于经典物理噪声的随机数发生器生成,本质上属于伪随机数. 相比之下,量子随机数基于量子力学原理,具备信息理论安全性. 将量子随机数与共识机制结合,可以实现真正的随机性,从而为节点选举提供更高的公平性和安全性. 在量子密钥分发方面,研究重点在于选择适合区块链设备的量子密码算法,以降低能耗并提升效率. 量子密钥分发技术能够为区块链提供更高的通信安全性,尽管已经有多种解决方案,但其大规模商用仍需解决与现有区块链的适配问题. 在量子通信资源态方面,需探索纠缠态的高效生成、存储与分发机制,优化区块链节点的量子通信开销.

(2)区块链性能. 区块链可扩展性是实现大规模应用的关键,跨链、分片、共识机制等技术在解决区块链可扩展性方面具有重要作用. 利用跨链技术解决不同区块链域之间的信息孤岛问题,然而需要考虑跨链技术中安全性、效率以及兼容度三种属性的平衡. 在分片方面,现有分片方案没有考虑分片之间的分片信任差异、通信时延差异和节点数差异. 扩展共识机制的挑战在于需要提高吞吐量的同时保证安全和去中心化. 针对上述存在的问题,未来需进一步探究优化增强区块链可扩展性方案.

(3)区块链赋能大语言模型. 区块链与大语言模型融合研究的核心目标在于构建安全合规的非毒性模型,即在保障高性能输出的同时满足伦理、法律与社会责任的综合要求. 当前区块链虽通过透明审计机制为模型安全提供基础支撑,但仍存在针对性治理缺失和资源协同瓶颈问题. 现有链上审计主要依赖底层协议实现基础安全,缺乏面向LLM的自动化有害内容过滤与抑制机制;区块链与LLM的融合系统需应对显著资源挑战,简单融合将加剧能耗,导致资源分配失衡,亟需开发轻量化框架与节能共识协议以提升可持续性. 因此,未来可以进一步研究可控遗忘机制,研究“遗忘”概念[129]在LLM和区块链中的应用. 通过可编辑区块链实现有害数据或模型的合规删除,从源头消除毒性内容再生产风险. 同时探索轻量化架构与资源动态优化方案,结合模型压缩与边缘分片调度策略,构建高能效的资源协同基础设施,最终实现安全治理与计算效率的协同演进.

8.3 结语

本文深入研究了区块链技术在数据安全领域的应用,以数据安全服务属性为基础,对近期基于区块链的数据安全研究成果进行系统地梳理与总结,详细阐述了区块链如何从数据治理、可信增强以及部署优化这三个方面来增强大语言模型质量. 此外,本文对引言部分提出的三个关键问题进行了针对性地回答,并深入探讨了未来的研究方向. 具体而言,量子密码算法与量子区块链在实际应用过程中,仍需进一步研究能效优化机制;区块链的性能优化方案仍处于持续研究阶段,亟待进一步完善;区块链与大语言模型结合方面需要研究一种能耗低、可扩展性强、可信数据要素驱动的大语言模型方案,为后续相关研究工作提供具有价值的参考,推动该领域的持续发展与创新.

参考文献

[1] BI Y R, WU Y H, LIU J F, et al. When data pricing meets non-cooperative game theory[C]//2024 IEEE 40th International Conference on Data Engineering. Piscataway: IEEE, 2024: 5548-5559.

[2] SHEN W T, QIN J, YU J, et al. Enabling identity-based integrity auditing and data sharing with sensitive information hiding for secure cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2019, 14(2): 331-346.

[3] LI M Z, WANG W, ZHANG J. LB-chain: Load-balanced and low-latency blockchain sharding via account migration[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(10): 2797-2810.

[4] HEO J W, RAMACHANDRAN G S, DORRI A, et al. Blockchain data storage optimisations: A comprehensive survey[J]. ACM Computing Surveys, 2024, 56(7): 1-27.

[5] ISLAM M M, ISLAM M K, SHAHJALAL M, et al. A low-cost cross-border payment system based on auditable cryptocurrency with consortium blockchain: Joint digital currency[J]. IEEE Transactions on Services Computing, 2023, 16(3): 1616-1629.

[6] GUPTA A, RATHOD J, PATEL D, et al. Tokenization of real estate using blockchain technology[C]//Applied Cryptography and Network Security Workshops. Cham: Springer International Publishing, 2020: 77-90.

[7] LAKSHMANAN M, ANANDHA MALA G S. Merkle tree-blockchain-assisted privacy preservation of electronic medical records on offering medical data protection through hybrid heuristic algorithm[J]. Knowledge and Information Systems, 2024, 66(1): 481-509.

[8] LACSON R, YU Y F, KUO T T, et al. Biomedical blockchain with practical implementations and quantitative evaluations: A systematic review[J]. Journal of the American Medical Informatics Association, 2024, 31(6): 1423-1435.

[9] SHARMA S K, DWIVEDI Y K, MISRA S K, et al. Conjoint analysis of blockchain adoption challenges in government[J]. Journal of Computer Information Systems, 2024,

64(2): 173-186.

[10] ZHANG C, ZHOU G, Li H, et al. Manufacturing blockchain of things for the configuration of a data-and knowledge-driven digital twin manufacturing cell[J]. IEEE Internet of Things Journal, 2020, 7(12): 11884-11894.

[11] 陆琪鹏, 刘亚丽, 刘长庚, 等. 基于区块链的RFID供应链产品所有权转移方案[J]. 电子学报, 2025, 53(2): 451-459.
LU Q P, LIU Y L, LIU C G, et al. Product ownership transfer scheme of RFID-enabled supply chain based on blockchain[J]. Acta Electronica Sinica, 2025, 53(2): 451-459. (in Chinese)

[12] ZEKIYE A, BOUACHIR O, ÖZKASAP Ö, et al. Blockchain-enabled energy trading and battery-based sharing in microgrids[C]//ICC 2024 - IEEE International Conference on Communications. Piscataway: IEEE, 2024: 4674-4679.

[13] HOU W G, GUO L, NING Z L. Local electricity storage for blockchain-based energy trading in industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6): 3610-3619.

[14] YE T, LUO M, YANG Y, et al. A survey on redactable blockchain: Challenges and opportunities[J]. IEEE Transactions on Network Science and Engineering, 2023, 10(3): 1669-1683.

[15] BAO Q H, LI B X, HU T Y, et al. A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work[J]. Journal of Systems and Software, 2023, 196: 111555.

[16] WU H Q, DÜDDER B, WANG L M, et al. Survey on secure keyword search over outsourced data: From cloud to blockchain-assisted architecture[J]. ACM Computing Surveys, 2023, 56(3): 1-40.

[17] WU G F, WANG H P, LAI X, et al. A comprehensive survey of smart contract security: State of the art and research directions[J]. Journal of Network and Computer Applications, 2024, 226: 103882.

[18] ZHOU L, DIRO A, SAINI A, et al. Leveraging zero knowledge proofs for blockchain-based identity sharing: A survey of advancements, challenges and opportunities[J]. Journal of Information Security and Applications, 2024, 80: 103678.

[19] JAIN A K, GUPTA N, GUPTA B B. A survey on scalable consensus algorithms for blockchain technology[J]. Cyber Security and Applications, 2025, 3: 100065.

[20] HUO R, ZENG S Q, WANG Z H, et al. A comprehensive survey on blockchain in industrial Internet of Things: Motivations, research progresses, and future challenges[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 88-122.

[21] LENG J W, YE S D, ZHOU M, et al. Blockchain-secured smart manufacturing in industry 4.0: A survey[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2021, 51(1): 237-252.

[22] XU H S, WU J, PAN Q Q, et al. A survey on digital twin for industrial Internet of Things: Applications, technologies and tools[J]. IEEE Communications Surveys & Tutorials, 2023, 25(4): 2569-2598.

[23] FU Y C, LI C L, YU F R, et al. A survey of blockchain and intelligent networking for the metaverse[J]. IEEE Internet of Things Journal, 2023, 10(4): 3587-3610.

[24] HASAN K M BIN, SAJID M, LAPINA M A, et al. Blockchain technology meets 6G wireless networks: A systematic survey[J]. Alexandria Engineering Journal, 2024, 92: 199-220.

[25] FARAH M BEN, AHMED Y, MAHMOUD H, et al. A survey on blockchain technology in the maritime industry: Challenges and future perspectives[J]. Future Generation Computer Systems, 2024, 157: 618-637.

[26] SALMAN T, ZOLANVARI M, ERBAD A, et al. Security services using blockchains: A state of the art survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(1): 858-880.

[27] LENG J W, ZHOU M, ZHAO J L, et al. Blockchain security: A survey of techniques and research directions[J]. IEEE Transactions on Services Computing, 2022, 15(4): 2490-2510.

[28] XU Y Q, XU G X, LIU Y, et al. A survey of the fusion of traditional data security technology and blockchain[J]. Expert Systems with Applications, 2024, 252: 124151.

[29] KITCHENHAM B, PEARL BRERETON O, BUDGEN D, et al. Systematic literature reviews in software engineering: A systematic literature review[J]. Information and Software Technology, 2009, 51(1): 7-15.

[30] LIU B, YU X L, CHEN S P, et al. Blockchain based data integrity service framework for IoT data[C]//2017 IEEE International Conference on Web Services. Piscataway: IEEE, 2017: 468-475.

[31] DORRI A, KANHERE S S, JURDAK R, et al. LSB: A lightweight scalable blockchain for IoT security and anonymity[J]. Journal of Parallel and Distributed Computing, 2019, 134: 180-197.

[32] TIAN J, TIAN J F, DU R Z. MSLTChain: A trust model

based on the multi-dimensional subjective logic for tree sharding blockchain system[J]. IEEE Transactions on Network and Service Management, 2024, 21(5): 5566-5581.

[33] ZHANG Y X, YANG J C, LEI H, et al. PACTA: An IoT data privacy regulation compliance scheme using TEE and blockchain[J]. IEEE Internet of Things Journal, 2024, 11(5): 8882-8893.

[34] WANG Y C, FAN R, YIN X Y, et al. Trusted storage architecture for machine reasoning based on blockchain[C]// IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops. Piscataway: IEEE, 2022: 1-6.

[35] LI Q, WU J J, QUAN J Y, et al. Efficient quantum blockchain with a consensus mechanism QDPoS[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3264-3276.

[36] BEHNIA R, POSTLETHWAITE E W, OZMEN M O, et al. Lattice-based proof-of-work for post-quantum blockchains[M]//Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham: Springer International Publishing, 2022: 310-318.

[37] DOLEV S, GUO B Y, NIU J Y, et al. SodsBC: A post-quantum by design asynchronous blockchain framework[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(1): 47-62

[38] WANG W S, YU Y, DU L J. Quantum blockchain based on asymmetric quantum encryption and a stake vote consensus algorithm[J]. Scientific Reports, 2022, 12: 8606.

[39] ATENIESE G, MAGRI B, VENTURI D, et al. Redactable blockchain-or-rewriting history in Bitcoin and friends[C]//2017 IEEE European Symposium on Security and Privacy. Piscataway: IEEE, 2017: 111-126.

[40] GRIGORIEV D, SHPILRAIN V. RSA and redactable blockchains[J]. International Journal of Computer Mathematics: Computer Systems Theory, 2021, 6(1): 1-6.

[41] DEUBER D, MAGRI B, THYAGARAJAN S A K. Redactable blockchain in the permissionless setting[C]// 2019 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2019: 124-138.

[42] 张驰骋, 李雷孝, 杜金泽, 等. 可编辑区块链研究综述[J]. 计算机工程与应用, 2024, 60(18): 32-49.
ZHANG C C, LI L X, DU J Z, et al. Redactable blockchain research reviews[J]. Computer Engineering and Applications, 2024, 60(18): 32-49. (in Chinese)

[43] 袁勇, 王飞跃. 可编辑区块链: 模型、技术与方法[J]. 自动化学报, 2020, 46(5): 831-846.
YUAN Y, WANG F Y. Editable blockchain: Models, techniques and methods[J]. Acta Automatica Sinica, 2020, 46(5): 831-846. (in Chinese)

[44] ZHANG D, LE J Q, LEI X Y, et al. Secure redactable blockchain with dynamic support[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(2): 717-731.

[45] XU S M, NING J T, LI X G, et al. A privacy-preserving and redactable healthcare blockchain system[J]. IEEE Transactions on Services Computing, 2024, 17(2): 364-377.

[46] DAI W Q, LIU J K, ZHOU Y, et al. PRBFPT: A practical redactable blockchain framework with a public trapdoor[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 2425-2437.

[47] LI X Y, XU J, YIN L Y, et al. Escaping from consensus: Instantly redactable blockchain protocols in permissionless setting[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(5): 3699-3715

[48] LI J H, MA H, WANG J B, et al. Wolverine: A scalable and transaction-consistent redactable permissionless blockchain[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1653-1666.

[49] ZHANG Y Q, MA Z F, LUO S S, et al. Dynamic trust-based redactable blockchain supporting update and traceability[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 821-834.

[50] DUAN J K, WANG W, WANG L C, et al. Controlled redactable blockchain based on T-times chameleon hash and signature[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 7560-7572.

[51] ZHOU L, FU A M, YU S, et al. Data integrity verification of the outsourced big data in the cloud environment: A survey[J]. Journal of Network and Computer Applications, 2018, 122: 1-15.

[52] LI A T, CHEN Y, YAN Z, et al. A survey on integrity auditing for data storage in the cloud: From single copy to multiple replicas[J]. IEEE Transactions on Big Data, 2022, 8(5): 1428-1442.

[53] ATENIESE G, BURNS R, CURTMOLA R, et al. Provable data possession at untrusted stores[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York: ACM, 2007: 598-609.

[54] ZOU X, DENG X, WU T Y, et al. A collusion attack on identity-based public auditing scheme via blockchain[C]// Advances in Intelligent Information Hiding and Multimedia Signal Processing. Singapore: Springer, 2019: 97-105.

[55] BYEON H, KAUR H, AGAL S, et al. IoT-enabled cloud-based fair provable data possession scheme based on blockchain[C]//2023 Second International Conference on Smart Technologies For Smart Nation. Piscataway: IEEE, 2023: 276-282.

[56] QI X X, FU X D, DAI F, et al. Collusion attack analysis and detection of DPoS consensus mechanism[C]//Blockchain and Trustworthy Systems. Singapore: Springer, 2022: 194-206.

[57] CHEN L X, FU Q X, MU Y, et al. Blockchain-based random auditor committee for integrity verification[J]. Future Generation Computer Systems, 2022, 131: 183-193.

[58] WANG C X, SUN Y F, LIU B Y, et al. Blockchain-based dynamic cloud data integrity auditing via non-leaf node sampling of rank-based merkle hash tree[J]. IEEE Transactions on Network Science and Engineering, 2024, 11(5): 3931-3942.

[59] GU K, WANG Y, QIU J, et al. Blockchain-based data deduplication and distributed audit for shared data in cloud-fog computing-based VANETs[J]. IEEE Transactions on Network and Service Management, 2024, 21(5): 5548-5565.

[60] XU Y, ZHANG C, WANG G J, et al. A blockchain-enabled deduplicatable data auditing mechanism for network storage services[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(3): 1421-1432.

[61] ANKIT K C, PANDEY R, BHANDARI D, et al. Minimizing certificate verification time in blockchain technology[C]//2024 IEEE International Conference on Information Technology, Electronics and Intelligent Communication Systems. Piscataway: IEEE, 2024: 1-6.

[62] LI T F, CHU J F, HU L. CIA: A collaborative integrity auditing scheme for cloud data with multi-replica on multi-cloud storage providers[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(1): 154-162.

[63] MIAO Y, HUANG Q, XIAO M Y, et al. Blockchain assisted multi-copy provable data possession with faults localization in multi-cloud storage[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3663-3676.

[64] WANG F Y, ZHOU J T, WANG H, et al. A blockchain-based multi-cloud storage data consistency verification scheme[C]//2022 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking. Piscataway: IEEE, 2023: 371-377.

[65] LI S S, XU C X, ZHANG Y, et al. Blockchain-based transparent integrity auditing and encrypted deduplication for cloud storage[J]. IEEE Transactions on Services Computing, 2023, 16(1): 134-146.

[66] SONG M Y, HUA Z Y, ZHENG Y F, et al. Blockchain-based deduplication and integrity auditing over encrypted cloud storage[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 4928-4945.

[67] MIAO Y, GAI K K, ZHU L H, et al. Blockchain-based shared data integrity auditing and deduplication[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(4): 3688-3703.

[68] TIAN G H, WEI J H, KUTYŁOWSKI M, et al. VRBC: A verifiable redactable blockchain with efficient query and integrity auditing[J]. IEEE Transactions on Computers, 2023, 72(7): 1928-1942.

[69] ZHANG C, XUAN H J, WU T, et al. Blockchain-based dynamic time-encapsulated data auditing for outsourcing storage[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 1979-1993.

[70] ZHANG Q Y, ZHANG Z M, CUI J, et al. Efficient blockchain-based data integrity auditing for multi-copy in decentralized storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(12): 3162-3173.

[71] WANG Q H, XIA T Y, WANG D, et al. SDoS: Selfish mining-based denial-of-service attack[J]. IEEE Transactions on Information Forensics and Security, 2022, 17: 3335-3349.

[72] WANG Q H, LI C Y, XIA T Y, et al. Optimal selfish mining-based denial-of-service attack[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 835-850.

[73] TENNAKOON D, HUA Y D, GRAMOLI V. Smart redbelly blockchain: Reducing congestion for Web3[C]// 2023 IEEE International Parallel and Distributed Processing Symposium. Piscataway: IEEE, 2023: 940-950.

[74] KUMAR R, KUMAR P, TRIPATHI R, et al. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network[J]. Journal of Parallel and Distributed Computing, 2022, 164: 55-68.

[75] TA V Q, PARK M. MAN-EDoS: A multihead attention network for the detection of economic denial of sustainability attacks[J]. Electronics, 2021, 10(20): 2500.

[76] QI X D. S-store: A scalable data store towards permissioned blockchain sharding[C]//IEEE INFOCOM 2022 - IEEE Conference on Computer Communications. New York: ACM, 2022: 1978-1987.

[77] RAIKWAR M, GLIGOROSKI D. DoS attacks on Blockchain ecosystem[C]//European Conference on Parallel Processing. Cham: Springer International Publishing, 2021: 230-242.

[78] CHEN X S, ZHAO S X, QI J, et al. Efficient and DoS-resistant consensus for permissioned blockchains[J]. ACM SIGMETRICS Performance Evaluation Review, 2022, 49(3): 61-62.

[79] NGUYEN T, THAI M T. Denial-of-service vulnerability of hash-based transaction sharding: Attack and countermeasure[J]. IEEE Transactions on Computers, 2023, 72(3): 641-652.

[80] HE Z Y, LI Z H, QIAO A, et al. Nurgle: Exacerbating resource consumption in blockchain state storage via MPT manipulation[C]//2024 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2024: 2180-2197.

[81] ZHANG Q Y, XU C, ZHONG H, et al. Revocable and efficient blockchain-based fine-grained access control against EDoS attacks in cloud storage[J]. IEEE Transactions on Computers, 2024, 73(8): 2012-2024.

[82] WANG Y, LIAO J, YANG J, et al. Meta-block: Exploiting cross-layer and direct storage access for decentralized blockchain storage systems[J]. IEEE Transactions on Computers, 2023, 72(7): 2052-2064.

[83] GUO H C, XU M H, ZHANG J H, et al. FileDAG: A multi-version decentralized storage network built on DAG-based blockchain[J]. IEEE Transactions on Computers, 2023, 72(11): 3191-3202.

[84] LIU Q, PENG Y, TANG Z Y, et al. veffChain: Enabling freshness authentication of rich queries over blockchain databases[J]. IEEE Transactions on Knowledge and Data Engineering, 2024, 36(5): 2285-2300.

[85] WANG Y C, PENG Y G, LIU X M, et al. aChain: A SQL-empowered analytical blockchain as a database[J]. IEEE Transactions on Computers, 2023, 72(11): 3099-3112.

[86] ZHANG S W, YAN Z W, LIANG W, et al. BCAE: A blockchain-based cross domain authentication scheme for edge computing[J]. IEEE Internet of Things Journal, 2024, 11(13): 24035-24048.

[87] CUI J, ZHU Y H, ZHONG H, et al. Efficient blockchain-based mutual authentication and session key agreement for cross-domain IIoT[J]. IEEE Internet of Things Journal, 2024, 11(9): 16325-16338.

[88] ZHANG K N, LEE C K M, TSANG Y P. Stateless blockchain-based lightweight identity management architecture for industrial IoT applications[J]. IEEE Transactions on Industrial Informatics, 2024, 20(6): 8394-8405.

[89] MENG X W, LIU B B, MENG X Y, et al. A lightweight group authentication protocol for blockchain-based vehicular edge computing networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(8): 8556-8567.

[90] LIU K X, GUAN J F, YAO S, et al. DKGAuth: Blockchain-assisted distributed key generation and authentication for cross-domain intelligent IoT[J]. IEEE Internet of Things Journal, 2024, 11(15): 25663-25673.

[91] YU H F, BAI X P. Identity-based searchable attribute signcryption in lattice for a blockchain-based medical system[J]. Frontiers of Information Technology & Electronic Engineering, 2024, 25(3): 461-471.

[92] BAO Z J, HE D B, KHAN M K, et al. PBidm: Privacy-preserving blockchain-based identity management system for industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 1524-1534.

[93] ZHU Y S, ZHOU Y W, WANG J, et al. A lightweight cross-domain direct identity authentication protocol for VANETs[J]. IEEE Internet of Things Journal, 2024, 11(23): 37741-37757.

[94] ZHANG Z N, XIONG R T, DI X Y, et al. CroAuth: A cross-domain authentication scheme based on blockchain and decentralized identity[C]//2024 27th International Conference on Computer Supported Cooperative Work in Design. Piscataway: IEEE, 2024: 2016-2021.

[95] POPA M, STOKLOSSA S M, MAZUMDAR S. Chain-discipline - towards a blockchain-IoT-based self-sovereign identity management framework[J]. IEEE Transactions on Services Computing, 2023, 16(5): 3238-3251.

[96] XU X B, GUO Y J, GUO Y M. Fog-enabled private blockchain-based identity authentication scheme for smart home[J]. Computer Communications, 2023, 205: 58-68.

[97] SEZER B B, AKLEYLEK S. PPLBB: A novel privacy-preserving lattice-based blockchain platform in IoMT[J]. The Journal of Supercomputing, 2024, 81(1): 219.

[98] CHEN X, XU S Y, CAO Y B, et al. AQRS: Anti-quantum ring signature scheme for secure epidemic control with blockchain[J]. Computer Networks, 2023, 224: 109595.

[99] SHEKHAWAT H, GUPTA D S. Quantum-resistance blockchain-assisted certificateless data authentication and key exchange scheme for the smart grid metering infrastructure[J]. Pervasive and Mobile Computing, 2024, 100: 101919.

[100] 曹博雅, 高军涛, 李雪莲. 区块链上基于格的可监管隐私保护方案[J]. 密码学报(中英文), 2025, 12(1): 69-83.

CAO B Y, GAO J T, LI X L. Lattice-based regulatory privacy protection scheme on blockchain[J]. Journal of Cryptologic Research, 2025, 12(1): 69-83. (in Chinese)

[101] HAO R, DAI X H, DAI W Q. BitFT: An understandable, performant and resource-efficient blockchain consensus[J]. IEEE Transactions on Sustainable Computing, 2024, 9(3): 522-534.

[102] LI W J, ZHANG Q F, DENG S G, et al. Q-learning improved lightweight consensus algorithm for blockchain-structured Internet of Things[J]. IEEE Internet of Things Journal, 2024, 11(2): 2855-2869.

[103] ZHAO Y, QU Y Y, XIANG Y, et al. A lightweight model-based evolutionary consensus protocol in blockchain as a service for IoT[J]. IEEE Transactions on Services Computing, 2023, 16(4): 2343-2358.

[104] CHENG Y, GUO Y H, XU M H, et al. An adaptive and modular blockchain enabled architecture for a decentralized metaverse[J]. IEEE Journal on Selected Areas in Communications, 2024, 42(4): 893-904.

[105] WANG Z H, WANG H, LI Z W, et al. Robust permissioned blockchain consensus for unstable communication in FANET[J]. IEEE/ACM Transactions on Networking, 2023, 32(1): 699-712.

[106] XIE X, HUA C Q, HONG J N, et al. AirCon: Over-the-air consensus for wireless blockchain networks[J]. IEEE Transactions on Mobile Computing, 2024, 23(5): 4566-4582.

[107] TANG Y, YAN J W, CHAKRABORTY C, et al. Hedera: A permissionless and scalable hybrid blockchain consensus algorithm in multiaccess edge computing for IoT[J]. IEEE Internet of Things Journal, 2023, 10(24): 21187-21202.

[108] SHEN T, LI T Y, YU Z, et al. GT-NRSM: Efficient and scalable sharding consensus mechanism for consortium blockchain[J]. The Journal of Supercomputing, 2023, 79(17): 20041-20075.

[109] GAI F Y, NIU J Y, BESCHASTNIKH I, et al. Scaling blockchain consensus via a robust shared mempool[C]// 2023 IEEE 39th International Conference on Data Engineering. Piscataway: IEEE, 2023: 530-543.

[110] HUANG H, LIN Y, ZHENG Z. Account migration across blockchain shards using fine-tuned lock mechanism[C]//IEEE INFOCOM 2024 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2024: 271-280.

[111] JIA L P, LIU Y X, WANG K Y, et al. Estuary: A low cross-shard blockchain sharding protocol based on state splitting[J]. IEEE Transactions on Parallel and Distributed Systems, 2024, 35(3): 405-420.

[112] HUANG H W, PENG X W, ZHAN J Z, et al. Brokerchain: A cross-shard blockchain protocol for account/balance-based state sharding[C]//IEEE INFOCOM 2022-IEEE Conference on Computer Communications. Piscataway: IEEE, 2022: 1968-1977.

[113] WANG K Y, JIA L P, SONG Z X, et al. Mitosis: A scalable sharding system featuring multiple dynamic relay chains[J]. IEEE Transactions on Parallel and Distributed Systems, 2024, 35(12): 2497-2512.

[114] LIU Y Z, XING X X, CHENG H S, et al. A flexible sharding blockchain protocol based on cross-shard Byzantine fault tolerance[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 2276-2291.

[115] XU J, MING Y L, WU Z H, et al. X-shard: Optimistic cross-shard transaction processing for sharding-based blockchains[J]. IEEE Transactions on Parallel and Distributed Systems, 2024, 35(4): 548-559.

[116] LI M Z, LIN Y, ZHANG J, et al. CoChain: High concurrency blockchain sharding via consensus on consensus[C]// IEEE INFOCOM 2023 - IEEE Conference on Computer Communications. Piscataway: IEEE, 2023: 1-10.

[117] DAVID B, MAGRI B, MATT C, et al. GearBox: Optimal-size shard committees by leveraging the safety-liveness dichotomy[C]//Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2022: 683-696.

[118] CAI Z T, LIANG J Y, CHEN W H, et al. Benzene: Scaling blockchain with cooperation-based sharding[J]. IEEE Transactions on Parallel and Distributed Systems, 2023, 34(2): 639-654.

[119] SU C, WEN J, KANG J, et al. Hybrid RAG-empowered multi-modal LLM for secure data management in Internet of medical things: A diffusion-based contract approach[J]. IEEE Internet of Things Journal, 2024, 12(10): 13428-13440.

[120] KANG J W, LUO X F, NIE J T, et al. Blockchain-based pseudonym management for vehicle twin migrations in vehicular edge metaverse[J]. IEEE Internet of Things Journal, 2024, 11(21): 34254-34269.

[121] WANG J, YUAN X, XU Y J, et al. An efficient multi-party threshold ECDSA protocol against malicious adversaries for blockchain-based LLMs[J]. IET Information Security, 2024, 2024(1): 2252865.

[122] LIU Y, ZHANG D, XIA B, et al. Blockchain-enabled ac-

countability in data supply chain: A data bill of materials approach[C]//2024 IEEE International Conference on Blockchain. Piscataway: IEEE, 2024: 557-562.
[123] SALIM M M, DENG X, PARK J H. A privacy-preserving local differential privacy-based federated learning model to secure LLM from adversarial attacks[J]. Human-centric Computing and Information Sciences, 2024, 14: 57.
[124] CHEN B, LI G L, LIN X, et al. BlockAgents: Towards Byzantine-robust LLM-based multi-agent coordination via blockchain[C]//Proceedings of the ACM Turing Award Celebration Conference - China 2024. New York: ACM, 2024: 187-192.
[125] SACHAN S, LIU X. Blockchain-based auditing of legal decisions supported by explainable AI and generative AI tools[J]. Engineering Applications of Artificial Intelligence, 2024, 129: 107666.
[126] AMINE B A, TELNOFF Q, BAKKALI S, et al. LLM-chain: Blockchain-based reputation system for sharing and evaluating large language models[C]//2024 IEEE 48th Annual Computers, Software, and Applications Conference. Piscataway: IEEE, 2024: 439-448.
[127] ZHANG M J, SHEN X M, CAO J N, et al. EdgeShard: Efficient LLM inference via collaborative edge computing[J]. IEEE Internet of Things Journal, 2025, 12(10): 13119-13131.
[128] ARSHAD U, HALIM Z. BlockLLM: A futuristic LLM-based decentralized vehicular network architecture for secure communications[J]. Computers and Electrical Engineering, 2025, 123: 110027.
[129] WANG Z Y, YANG E N, SHEN L, et al. A comprehensive survey of forgetting in deep learning beyond continual learning[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2025, 47(3): 1464-1483.

作者简介

张瑶瑶 女,1998年10月出生于河南省郑州市. 现为广州大学网络空间安全学院博士研究生. 主要研究方向为区块链与数据交易.
E-mail: yaoaoz@e.gzhu.edu.cn

陈 凯 男,1997年9月出生于江苏省南通市. 现为广州大学网络空间安全学院在读硕士研究生. 主要研究方向为区块链安全、联邦学习.
E-mail: kaichen@e.gzhu.edu.cn

周 圆 女,1994年3月出生于河南省信阳市. 现为广州大学网络空间安全学院博士研究生. 主要研究方向为网络威胁情报共享机制.
E-mail: wendribs@e.gzhu.edu.cn

李 意 男,2000年2月出生于广东省广州市. 现为广州大学网络空间安全学院在读硕士研究生. 主要研究方向为IPv6空间探测、IPv6应用、区块链应用.
E-mail: yuegeyu@e.gzhu.edu.cn

杨青林 男,1989年4月出生于河南省项城市. 现为广州大学网络空间安全学院特聘讲师. 主要研究方向为区块链、联邦学习. 在国外相关领域主流期刊和会议上发表论文40余篇,主持广州市高校科研面上项目1项,横向课题1项,主持国家重点研发计划青年项目子任务.
E-mail: yangqinglin@gzhu.edu.cn

刘 园 女,1986年10月出生于吉林省长春市. 现为广州大学网络空间安全学院教授、博士生导师. 主要研究方向为网络安全、数据安全、区块链安全. 国家自然科学基金获得者、国家重点研发计划项目项目负责人. 发表学术论文100余篇,专著1部.
E-mail: yuanliu@gzhu.edu.cn

颛孙晨露 女,1990年9月出生于安徽省宿州市. 现为广州大学网络空间安全学院特聘讲师. 主要研究方向为主动防御、欺骗防御及信誉系统等.
E-mail: chenluzhuansun@gzhu.edu.cn

田志宏 男,1978年9月出生于黑龙江省哈尔滨市. 现为广州大学副校长,网络空间安全学院教授、博士生导师,国家级人才项目特聘教授. 主要研究方向为网络攻防对抗,网络靶场、主动实时防护等. 获得省部级奖励4次,发表论文200余篇,专著3部.
E-mail: tianzhihong@gzhu.edu.cn