基于区块链的工业互联网数据安全存储与共享方案

吴 斌

(哈尔滨工业大学计算学部，黑龙江 哈尔滨 150001)

摘 要：在工业数字化转型的深度推进下，工业互联网已成为连接工业设备、生产流程、产业链上下游的核心载体，其产生的海量工业数据（涵盖生产控制、设备运行、研发设计、经营管理等全流程）已成为工业企业核心资产。然而，工业互联网数据具有多源异构、实时性强、敏感性高、价值密度不均等特点，传统集中式数据存储与共享方案存在单点故障、数据篡改风险高、隐私泄露严重、权限管理混乱等诸多安全隐患，严重制约了工业数据价值的释放和工业互联网的高质量发展。区块链技术凭借其去中心化、不可篡改、可追溯、透明可信、多方协同等核心特性，为解决工业互联网数据安全存储与共享难题提供了全新的技术路径。本文针对工业互联网数据安全存储与共享的核心需求，系统分析了区块链核心技术与工业互联网数据安全的内在关联，设计了一套基于区块链的工业互联网数据安全存储与共享方案。该方案构建了分层化总体架构与混合链结构，实现了数据分片加密存储、链上存证与链下存储协同、数据完整性动态验证等存储机制，提出了基于属性的访问控制、动态权限管理、全流程审计追溯的共享机制，并引入同态加密、差分隐私等技术增强隐私保护能力。通过搭建实验环境，对方案的吞吐量、延迟等性能指标，以及数据完整性、机密性等安全性指标进行了全面验证，结果表明该方案能够有效抵御各类常见攻击，保障数据存储安全与共享合规，同时具备良好的性能适配性，能够满足工业互联网多场景、高并发的数据处理需求。最后，总结了本文的研究成果，并对未来方案的优化方向和技术拓展进行了展望，为工业互联网数据安全管理提供了理论支撑和实践参考。

关键词：区块链；工业互联网；数据安全；存储机制；共享机制；隐私保护；访问控制

中图分类号：TP393 **文献标识码：**A **文章编号：**3106-2709（2025）03-0024-13

DOI：10.62022/NCAR.issn3106-2709.2025.03.003

Blockchain-Based Secure Data Storage and Sharing Scheme for Industrial Internet

Wu Bin

(School of Computing, Harbin Institute of Technology, Harbin Heilongjiang150001)

Abstract: With the in-depth advancement of industrial digital transformation, the industrial Internet has become the core carrier connecting industrial equipment, production processes, and the upper and lower reaches of the industrial chain. The massive industrial data generated by it (covering the entire process of production control, equipment operation, R&D and design, operation and management, etc.) has become the core asset of industrial enterprises. However, industrial Internet data has the characteristics of multi-source heterogeneity, strong real-time performance, high sensitivity, and uneven value density. The traditional centralized data storage and sharing schemes have many security risks such as single point of failure, high risk of data tampering, serious privacy leakage, and chaotic permission management, which seriously restrict the release of industrial data value and the high-quality development of the industrial Internet. Blockchain technology, with its core characteristics of decentralization, immutability, traceability, transparency and trustworthiness, and multi-party collaboration, provides a new technical path for solving the problems of secure data storage and sharing in the industrial Internet. Aiming at the core needs of secure data storage and sharing in the industrial Internet, this paper systematically analyzes the internal connection between core blockchain technologies and industrial Internet data security, and designs a blockchain-based secure data storage and sharing scheme for the industrial Internet. The scheme constructs a hierarchical overall architecture and a hybrid chain structure, realizes storage mechanisms such as sharded encrypted data storage, collaboration between on-chain certificate storage and off-chain storage, and dynamic verification of data integrity, and proposes a sharing mechanism based on attribute-based access control, dynamic permission management, and full-process audit and traceability. In addition, technologies such as homomorphic encryption and differential privacy are introduced to enhance privacy protection capabilities. By building an experimental environment, the performance indicators such as throughput and latency of the scheme, as well as the security indicators such as data integrity and confidentiality, are comprehensively verified. The results show that the scheme can effectively resist various common attacks, ensure the security of data storage and compliance of data sharing, and has good performance adaptability, which can meet the data processing needs of multi-scenario and high concurrency in the industrial Internet. Finally, the research results of this paper are summarized, and the future optimization direction and technical expansion of the scheme are prospected, providing theoretical support and practical reference for industrial Internet data security management.

作者简介：吴斌，博士，副教授，研究方向为区块链技术、工业互联网安全。

Keywords: blockchain; industrial Internet; data security; storage mechanism; sharing mechanism; privacy protection; access control

1 引言

随着新一代信息技术与制造业的深度融合，工业互联网已进入规模化发展阶段，成为推动工业经济高质量发展的重要引擎。工业互联网通过将工业设备、传感器、控制系统、信息系统等进行全面互联，实现了生产要素的智能化配置和生产流程的高效协同，催生了智能制造、柔性生产、远程运维等新型工业模式。在这一过程中，工业互联网产生了海量的多类型数据，这些数据贯穿于工业生产的全生命周期，涵盖设备运行数据、生产工艺数据、产品质量数据、供应链数据、经营管理数据等，是工业企业实现精细化管理、智能化决策、产业链协同的核心基础。然而，随着工业互联网数据规模的不断扩大、应用场景的不断丰富，数据安全问题日益凸显，成为制约工业互联网健康发展的关键瓶颈。传统集中式数据存储与共享方案由于其自身架构的局限性，难以应对工业互联网数据安全的复杂需求，而区块链技术的出现为解决这一难题提供了新的思路和方法。本章将从研究背景与意义出发，分析工业互联网数据安全的重要性、传统方案的局限性以及区块链技术的优势，明确本文的研究目的和研究内容。

1.1 研究背景与意义

当前，全球制造业正处于数字化、网络化、智能化转型的关键时期，工业互联网作为数字经济与实体经济深度融合的重要载体，已被各国提升至国家战略层面。我国也高度重视工业互联网的发展，先后出台了《工业互联网发展行动计划（2021–2023年）》《“十四五”数字经济发展规划》等一系列政策文件，明确提出要加强工业互联网安全保障体系建设，提升数据安全防护能力，推动工业数据安全有序共享。在政策引导和市场需求的双重驱动下，我国工业互联网产业规模持续扩大，截至2025年底，工业互联网平台数量已突破2000个，连接工业设备数量超过10亿台（套），工业数据产量年均增长率超过30%。海量工业数据的产生和应用，不仅为工业企业带来了新的发展机遇，也带来了严峻的数据安全挑战。工业数据中包含大量敏感信息，如核心工艺参数、设备运行机密、产品设计方案、供应链核心数据等，这些数据一旦发生泄露、篡改或丢失，将给企业带来巨大的经济损失，甚至威胁国家工业安全。因此，加强工业互联网数据安全存储与共享研究，具有重要的理论意义和现实价值。

1.1.1 工业互联网数据安全的重要性

工业互联网数据安全是工业互联网健康发展的前提和基础，其重要性主要体现在企业发展、产业升级和国家安全三个层面。

从企业发展层面来看，工业数据是企业的核心战略资产，其安全直接关系到企业的生存和发展。在智能制造场景中，设备运行数据的实时采集和分析的准确性，直接影响生产流程的优化和产品质量的控制；研发设计数据的安全性，决定了企业的核心技术竞争力，一旦泄露，可能导致企业失去市场优势[1]；供应链数据的安全共享，能够实现上下游企业的协同高效运作，降低运营成本，提升市场响应速度。如果工业数据出现安全问题，如数据篡改可能导致生产工艺混乱、产品质量不达标，数据泄露可能导致核心技术被窃取、商业机密泄露，数据丢失可能导致生产中断、业务停滞，这些都会给企业带来巨大的经济损失，甚至影响企业的可持续发展。例如，某大型装备制造企业曾因生产控制数据被篡改，导致生产线停工3天，直接经济损失超过千万元；某汽车制造企业的核心零部件设计数据泄露，被竞争对手抄袭，导致其市场份额大幅下降。

从产业升级层面来看，工业互联网数据的安全共享是推动产业链协同、实现产业升级的关键。工业互联网的核心价值在于通过数据的互联互通，打破企业之间的“数据孤岛”，实现产业链上下游的资源整合和协同发展。例如，在供应链协同场景中，上游原材料供应商、中游生产企业、下游经销商之间的数据分析共享，能够实现生产计划的精准制定、库存的合理调配、物流的高效运转，提升整个产业链的运行效率。然而，数据安全问题是制约数据共享的核心障碍，由于缺乏有效的安全保障机制，企业之间普遍存在“不愿共享、不敢共享”的问题，导致数据资源无法得到充分利用，产业链协同效应难以充分发挥[2]。只有建立完善的数据安全存储与共享机制，才能消除企业的共享顾虑，推动工业数据的有序流动和高效利用，促进产业结构优化升级，提升产业整体竞争力。

从国家安全层面来看，工业互联网数据安全直接关系到国家工业安全和经济安全。工业是国民经济的支柱产业，工业互联网涵盖了能源、制造、化工、航空航天、国防等多个关键领域，这些领域的工业数据涉及国家核心利益和安全。例如，能源领域的电网运行数据、石油化工领域的生产工艺数据、国防工业领域的装备研发数据等，一旦被非法获取或篡改，可能影响国家能源安全、产业安全，甚至威胁国家安全。近年来，全球工业互联网安全事件频发，境外黑客组织针对工业控制系统的攻击日益频繁，试图窃取敏感工业数据、破坏工业生产秩序，给各国工业安全带来了严重威胁。

因此，加强工业互联网数据安全存储与共享研究，构建自主可控的数据安全保障体系，对于维护国家工业安全、保障经济社会稳定发展具有重要的战略意义[3]。

此外，随着《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规的相继出台，工业企业的数据安全责任更加明确，对工业数据的收集、存储、使用、共享等环节提出了严格的合规要求。企业如果未能落实数据安全保护措施，不仅会面临经济处罚，还会影响企业的信誉和市场竞争力。因此，加强工业互联网数据安全存储与共享研究，也是企业落实法律法规要求、实现合规经营的必然选择。根据中华人民共和国国家标准《工业互联网企业网络安全 第4部分：数据防护要求》（征求意见稿），工业互联网数据处理者需对不同级别数据实施分级防护，确保数据全生命周期的安全，这进一步凸显了工业互联网数据安全的重要性和紧迫性。

1.1.2 传统数据存储与共享方案的局限性

目前，工业互联网领域普遍采用传统的集中式数据存储与共享方案，这种方案以中心化服务器为核心，负责数据的集中存储、管理和共享，虽然在一定时期内满足了工业数据处理的基本需求，但随着工业互联网的快速发展，其局限性日益凸显，主要体现在以下几个方面。

第一，单点故障风险突出，数据可用性难以保障。传统集中式存储方案将所有数据集中存储在一台或少数几台中心化服务器中，服务器成为整个系统的核心节点。一旦中心化服务器发生硬件故障、软件漏洞、网络攻击等问题，将导致整个数据存储系统瘫痪，所有数据无法访问，严重影响工业生产的正常运行。例如，某工业互联网平台的中心化存储服务器曾因遭受分布式拒绝服务（DDoS）攻击，导致平台瘫痪长达8小时，涉及数十家企业的生产数据无法访问，造成了巨大的经济损失。此外，中心化服务器的存储容量有限，随着工业数据规模的不断扩大，服务器的存储压力日益增大，容易出现存储瓶颈，进一步影响数据的可用性。

第二，数据篡改风险高，完整性无法保证。在集中式存储方案中，数据的管理权集中在少数管理员手中，管理员可以随意修改、删除数据，且修改痕迹难以追溯。同时，中心化服务器容易成为黑客攻击的目标，黑客通过利用服务器的漏洞，可对数据进行篡改、伪造，导致数据失去真实性和完整性。例如，黑客通过篡改工业生产控制数据，可能导致生产设备异常运行，引发生产安全事故；篡改产品质量检测数据，可能导致不合格产品流入市场，损害企业信誉和消费者利益。此外，传统存储方案缺乏有效的数据完整性验证机制，无法及时发现数据被篡改的情况，进一步加剧了数据安全风险[4]。

第三，隐私泄露问题严重，数据机密性难以保障。工业互联网数据中包含大量敏感信息，传统集中式共享方案中，数据的共享需要通过中心化服务器进行中转，所有数据都需要经过服务器存储和转发，这就导致数据在传输和存储过程中存在被窃取、泄露的风险。同时，中心化服务器的管理员能够直接访问所有数据，存在内部泄露的风险。例如，某工业企业的员工利用职务之便，窃取了企业的核心生产工艺数据，并出售给竞争对手，给企业带来了巨大的经济损失。此外，传统共享方案缺乏完善的访问控制机制，无法对数据访问权限进行精细化管理，导致未授权用户可能非法访问敏感数据，进一步加剧了隐私泄露风险[5]。

第四，权限管理混乱，数据共享缺乏可控性。传统集中式共享方案中，权限管理通常采用简单的角色分配方式，无法根据用户的身份、属性、访问场景等因素进行精细化的权限控制，导致权限分配不合理，出现“权限过高”或“权限不足”的问题。例如，某些普通员工可能拥有访问核心敏感数据的权限，而某些需要访问特定数据的用户却无法获得相应权限。同时，权限的分配和变更需要通过管理员手动操作，效率低下，且缺乏有效的权限审计机制，无法对权限的使用情况进行实时监控和追溯，导致数据共享过程缺乏可控性，容易出现数据滥用、非法访问等问题。

第五，“数据孤岛”现象严重，数据共享效率低下。由于不同企业、不同部门采用的存储系统和数据格式不同，且缺乏统一的数据共享标准和安全保障机制，导致各主体之间的数据无法实现有效互通，形成“数据孤岛”[6]。例如，同一产业链中的上下游企业，由于数据存储格式不兼容、共享机制不健全，无法实现生产数据、供应链数据的实时共享，导致生产计划无法精准对接，库存积压、物流延误等问题频发。此外，传统共享方案中，数据的共享需要经过多环节的审批和中转，流程繁琐，效率低下，无法满足工业互联网实时性数据共享的需求。

第六，缺乏有效的审计追溯机制，责任难以界定。传统集中式方案中，数据的操作记录通常存储在中心化服务器中，容易被篡改或删除，无法实现数据操作的全流程追溯。当发生数据泄露、篡改等安全事件时，无法准确追溯事件的源头和责任主体，导致责任难以界定，无法及时采取应对措施，也无法对相关责任人进行追责。这与工业互联网数据全生命周期防护的要求存在较大差距，难以满足合规管理的需求。

综上所述，传统集中式数据存储与共享方案已无法满足

工业互联网数据安全、高效、可控的存储与共享需求，亟需一种新的技术方案来解决上述问题。

1.1.3 区块链技术的优势

区块链技术是一种基于密码学、分布式系统、共识机制等技术的新型去中心化数据存储与交易技术，最初由中本聪在2008年提出，用于比特币的底层技术支撑。经过多年的发展，区块链技术已从单一的数字货币应用，拓展到金融、物流、医疗、工业等多个领域，其去中心化、不可篡改、可追溯、透明可信、多方协同等核心优势，恰好能够解决传统工业互联网数据存储与共享方案的局限性，为工业互联网数据安全保障提供了全新的技术路径。

第一，去中心化特性，有效规避单点故障风险。区块链技术采用分布式账本存储数据，将数据分散存储在网络中的多个节点上，每个节点都拥有完整的账本副本，不存在中心化的核心节点[7]。这种去中心化架构使得整个系统不再依赖于单一节点，即使部分节点发生故障、被攻击或离线，其他节点依然能够正常运行，确保数据的正常访问和系统的稳定运行，有效规避了传统集中式方案的单点故障风险。例如，当区块链网络中的某个节点遭受DDoS攻击时，其他节点依然能够正常处理数据存储和交易请求，不会导致整个系统瘫痪，从而保障了工业数据的可用性。进入2026年，随着区块链技术的不断成熟，联盟链在工业场景中的应用日益广泛，其在保证去中心化信任的同时，通过准入机制限制参与节点范围，进一步提升了系统稳定性。

第二，不可篡改特性，保障数据完整性。区块链技术通过密码学算法（如哈希算法、数字签名等）对数据进行加密处理，每一笔数据交易都会被记录在区块中，区块与区块之间通过哈希值相互关联，形成一条不可篡改的链式结构。一旦数据被记录到区块链中，就无法被随意修改或删除，即使有少数节点试图篡改数据，也需要修改网络中超过51%的节点的账本副本，这在技术上具有极高的难度和成本，几乎不可能实现[8]。这种不可篡改特性能够有效保障工业数据的完整性，防止数据被篡改、伪造，确保数据的真实性和可靠性。例如，工业生产控制数据、产品质量检测数据等被记录到区块链后，能够确保数据的不可篡改，为生产决策、质量追溯提供可靠的数据支撑。同时，这种特性也符合工业互联网数据全生命周期防护中对数据不可篡改的核心要求。

第三，可追溯特性，实现数据操作全流程追踪。区块链技术对每一笔数据交易都进行详细记录，包括交易时间、交易主体、交易内容等信息，这些信息被永久存储在区块链中，且可通过区块链的链式结构进行追溯。无论数据经过多少次传输和操作，都能够追溯到数据的源头和所有操作记录，实现数据操作的全流程追踪。这种可追溯特性能够有效解决传统方案中数据操作无法追溯、责任难以界定的问题，当发生数据安全事件时，能够快速定位事件源头，明确责任主体，及时采取应对措施。例如，当工业数据出现泄露时，通过区块链的追溯功能，能够快速查明数据泄露的环节和责任人，为追责提供有力依据。在产品全生命周期追溯场景中，区块链的可追溯特性能够实现从原材料采购到最终消费的完整追溯，极大提升了产品质量管控水平。

第四，透明可信特性，提升数据共享信任度。区块链网络中的所有节点都拥有完整的账本副本，数据交易信息对所有节点公开透明，任何节点都可以查看数据交易记录，且数据的生成和验证过程由所有节点共同参与，确保数据的真实性和可信度。这种透明可信特性能够消除企业之间的信任壁垒，解决传统数据共享中“不愿共享、不敢共享”的问题，提升数据共享的信任度。例如，在产业链协同场景中，上下游企业通过区块链网络共享数据，所有企业都能够查看数据的来源和操作记录，确保数据的真实性，从而实现高效的协同合作。同时，透明可信特性也有助于企业落实数据合规要求，接受监管部门的监督检查。

第五，多方协同特性，实现高效的数据共享。区块链技术采用共识机制，使得网络中的多个节点能够在无需中心化中介的情况下，实现数据的协同验证和交易确认，提高了数据共享的效率。同时，区块链技术支持智能合约的部署和执行，能够实现数据共享的自动化、智能化，减少人工干预，进一步提升数据共享的效率和便捷性。例如，通过智能合约，可以自动实现数据访问权限的分配、数据交易的结算等功能，无需人工手动操作，提高了数据共享的效率。此外，区块链与IPFS等技术的结合，能够有效解决传统区块链存储效率低的问题，为工业互联网海量数据的存储和共享提供了支撑。

第六，加密保护特性，保障数据机密性。区块链技术采用多种密码学算法对数据进行加密处理，包括对称加密、非对称加密、哈希加密等，确保数据在传输和存储过程中的安全性。数据被加密后，只有拥有相应密钥的用户才能解密和访问数据，有效防止数据被窃取、泄露。这种加密保护特性能够保障工业敏感数据的机密性，解决传统方案中隐私泄露严重的问题。例如，工业企业的核心工艺参数、研发设计数据等敏感信息，通过区块链加密存储和传输，能够有效防止被非法获取和泄露。同时，零知识证明、同态加密等隐私计算技术与区块链的结合，进一步提升了数据隐私保护能力，实现了数据“可用不可见”。

综上所述，区块链技术的核心优势与工业互联网数据安全存储与共享的需求高度契合，能够有效解决传统方案的局限性，为工业互联网数据安全保障提供了可靠的技术支撑。因此，研究基于区块链的工业互联网数据安全存储与共享方案，具有重要的理论价值和实践意义。

2 区块链与工业互联网数据安全关键技术

要实现基于区块链的工业互联网数据安全存储与共享，需要深入掌握区块链核心技术和工业互联网数据安全需求，明确两者之间的内在关联，为方案设计提供技术支撑。本章将系统介绍区块链核心技术的原理和应用，分析工业互联网数据安全的核心需求，为后续方案设计奠定基础。

2.1 区块链核心技术

区块链技术是一个融合了密码学、分布式系统、共识机制、智能合约等多种技术的综合体，其核心技术体系包括分布式账本、密码学技术、共识机制、智能合约等，这些技术相互协同，共同实现了区块链的去中心化、不可篡改、可追溯等核心特性。

2.1.1 分布式账本

分布式账本是区块链技术的核心基础，是指将数据分散存储在网络中的多个节点上，每个节点都拥有完整的账本副本，节点之间通过点对点（P2P）网络进行数据同步和交互，实现数据的分布式存储和管理。与传统集中式账本不同，分布式账本不存在中心化的管理节点，所有节点都拥有平等的权利和义务，共同参与账本的维护和更新。

分布式账本的核心特点主要包括以下几个方面：一是去中心化，账本数据分散存储在多个节点上，没有中心化的存储节点，避免了单点故障风险；二是一致性，网络中的所有节点通过共识机制，确保账本数据的一致性，即所有节点的账本副本保持同步，不存在数据差异；三是透明性，账本数据对所有节点公开透明，任何节点都可以查看账本中的数据交易记录，确保数据的可信性；四是不可篡改，账本数据通过密码学算法进行加密处理，一旦数据被记录到账本中，就无法被随意修改或删除，确保数据的完整性[9]。

在工业互联网场景中，分布式账本的应用具有重要意义。工业互联网涉及多个参与主体，包括工业企业、设备制造商、供应商、经销商、监管部门等，这些主体之间需要进行大量的数据交互和共享。通过分布式账本，能够将各主体的数据分散存储在各自的节点上，同时实现数据的同步和共享，避免了数据集中存储带来的单点故障和隐私泄露风险。例如，在供应链协同场景中，上下游企业通过分布式账本共享供应链数据，每个企业都拥有完整的供应链账本副本，能够实时查看供应链的运行状态，实现供应链的协同高效运作。同时，分布式账本的不可篡改和可追溯特性，能够确保供应链数据的真实性和完整性，防止数据被篡改、伪造，为供应链管理提供可靠的数据支撑。

分布式账本的实现方式主要有两种：一是全节点账本，即网络中的每个节点都存储完整的账本数据，能够参与账本的验证和更新，这种方式具有较高的安全性和一致性，但存储成本较高，适合节点数量较少的场景；二是轻节点账本，即节点只存储账本的部分数据（如区块头信息），不参与账本的验证和更新，需要通过全节点获取完整的账本数据，这种方式存储成本较低，适合节点数量较多、资源有限的场景。在工业互联网场景中，可根据不同的应用需求，选择合适的分布式账本实现方式。例如，对于核心数据的存储和管理，可采用全节点账本，确保数据的安全性和一致性；对于普通数据的存储和共享，可采用轻节点账本，降低存储成本，提高系统的扩展性。

此外，分布式账本的同步机制也是其核心技术之一。节点之间通过P2P网络进行数据同步，当某个节点产生新的交易数据时，会将交易数据广播到整个网络，其他节点收到交易数据后，通过共识机制进行验证，验证通过后将交易数据记录到自己的账本中，实现账本数据的同步[10]。常用的同步机制包括推送式同步和拉取式同步，推送式同步是指产生交易数据的节点主动将数据推送给其他节点，拉取式同步是指其他节点主动向产生交易数据的节点请求获取数据。在工业互联网场景中，由于数据实时性要求较高，通常采用推送式同步机制，确保数据能够及时同步到所有节点，满足工业生产的实时性需求。

随着区块链技术的发展，分布式账本技术也在不断优化和升级，出现了联盟链账本、私有链账本等多种类型，能够适应不同场景的需求。例如，联盟链账本主要用于多个企业之间的协同场景，通过准入机制限制节点的加入，确保账本数据的安全性和隐私性；私有链账本主要用于企业内部的数据管理，节点的加入和退出由企业自行控制，具有较高的安全性和可控性。在工业互联网数据安全存储与共享方案中，可结合工业场景的特点，选择合适的分布式账本类型，实现数据的安全存储和高效共享。

2.1.2 密码学技术

密码学技术是区块链技术的安全基础，贯穿于区块链的整个生命周期，用于保障数据的机密性、完整性、真实性和不可否认性。区块链技术中采用的密码学技术主要包括哈希

算法、对称加密算法、非对称加密算法、数字签名、数字证书等，这些技术相互配合，构建了区块链的安全体系。

哈希算法是区块链技术中最基础的密码学算法，用于将任意长度的输入数据转换为固定长度的输出数据（哈希值），具有不可逆性、唯一性、抗碰撞性等特点。不可逆性是指无法通过哈希值反推原始输入数据；唯一性是指不同的输入数据会产生不同的哈希值；抗碰撞性是指无法找到两个不同的输入数据，使其产生相同的哈希值。在区块链中，哈希算法主要用于数据的加密处理、区块的关联和数据完整性验证。例如，每个区块都包含前一个区块的哈希值，通过哈希值将区块相互关联，形成链式结构，确保区块数据的不可篡改；同时，对交易数据进行哈希处理，生成交易哈希值，用于验证交易数据的完整性，一旦交易数据被篡改，其哈希值会发生变化，从而能够及时发现数据篡改行为。常用的哈希算法包括SHA-256、SHA-3、MD5等，其中SHA-256算法由于其较高的安全性和抗碰撞性，被广泛应用于区块链技术中，如比特币、以太坊等区块链平台都采用SHA-256算法进行数据加密处理。

对称加密算法是指使用相同的密钥对数据进行加密和解密，具有加密和解密速度快、效率高的特点，适合对大量数据进行加密处理。在区块链中，对称加密算法主要用于数据的存储加密，将敏感数据加密后存储在区块链节点中，确保数据的机密性。常用的对称加密算法包括AES、DES、3DES等，其中AES算法由于其较高的安全性和效率，被广泛应用于区块链数据加密中。例如，工业企业的核心工艺参数、研发设计数据等敏感信息，通过AES算法加密后存储在区块链节点中，只有拥有相应密钥的用户才能解密和访问数据，有效防止数据被窃取、泄露。但对称加密算法也存在一定的局限性，即密钥的分发和管理难度较大，一旦密钥泄露，将导致数据安全受到威胁。因此，在区块链中，通常将对称加密算法与非对称加密算法结合使用，提高数据加密的安全性。

非对称加密算法是指使用一对密钥（公钥和私钥）对数据进行加密和解密，公钥可以公开，私钥由用户自行保管，具有较高的安全性。加密时使用公钥对数据进行加密，解密时使用私钥对数据进行解密，只有拥有私钥的用户才能解密数据。在区块链中，非对称加密算法主要用于数字签名、密钥分发等场景。例如，用户通过私钥对交易数据进行签名，其他用户通过用户的公钥对签名进行验证，确保交易数据的真实性和不可否认性；同时，通过非对称加密算法实现密钥的安全分发，避免密钥在分发过程中被窃取。常用的非对称加密算法包括RSA、ECC、DSA等，其中ECC算法由于其密钥长度短、加密效率高、安全性高的特点，被广泛应用于区块链技术中，尤其适合资源有限的工业设备节点。

数字签名是基于非对称加密算法的一种安全技术，用于验证数据的真实性和不可否认性。数字签名的过程如下：用户使用私钥对交易数据进行加密处理，生成数字签名；将交易数据和数字签名一起广播到区块链网络中；其他用户收到交易数据和数字签名后，使用用户的公钥对数字签名进行解密验证，如果验证通过，说明交易数据是真实的，且来自该用户，用户无法否认该交易。在区块链中，数字签名是保障交易安全的核心技术，能够有效防止交易数据被篡改、伪造，确保交易的真实性和不可否认性。例如，在工业数据共享场景中，数据提供方通过数字签名对共享数据进行签名，数据接收方通过数字签名验证数据的真实性，确保共享数据未被篡改，且来自合法的数据提供方。

数字证书是用于验证用户身份和公钥合法性的一种电子凭证，由权威的证书颁发机构（CA）颁发。数字证书中包含用户的身份信息、公钥信息、证书颁发机构的签名等内容，能够确保公钥的合法性和用户身份的真实性。在区块链中，数字证书主要用于节点身份认证和公钥验证，确保网络中的节点都是合法的，避免非法节点加入网络，保障网络的安全性。例如，在工业互联网区块链网络中，每个参与节点都需要向CA机构申请数字证书，通过数字证书验证节点的身份，只有合法的节点才能加入网络，参与数据的存储和共享。同时，数字证书也能够解决非对称加密算法中公钥认证的问题，确保用户使用的公钥是合法的，避免公钥被篡改或伪造。

在工业互联网场景中，密码学技术的应用尤为重要。工业互联网数据中包含大量敏感信息，通过密码学技术对数据进行加密处理，能够确保数据在传输和存储过程中的安全性；通过数字签名和数字证书，能够确保数据的真实性、不可否认性和节点身份的合法性，防止数据被篡改、伪造和非法访问。例如，工业设备运行数据在传输过程中，通过AES算法进行加密，通过数字签名进行签名，确保数据的机密性和真实性；节点之间进行数据交互时，通过数字证书验证节点身份，确保交互的安全性。同时，随着工业互联网的发展，密码学技术也在不断升级，出现了同态加密、零知识证明等新型密码学技术，这些技术能够进一步提升数据的隐私保护能力，为工业互联网数据安全提供更有力的保障。

2.1.3 共识机制

共识机制是区块链技术的核心机制之一，用于解决分布式网络中多个节点之间的信任问题，确保所有节点能够对账

本数据达成一致，实现数据的同步和一致性。在区块链网络中，多个节点相互独立，没有中心化的管理节点，节点之间通过共识机制，对交易数据的有效性进行验证和确认，共同维护账本的一致性。共识机制的核心目标是在存在恶意节点的情况下，确保账本数据的一致性和安全性，同时提高系统的效率和 scalability。

共识机制的设计需要考虑多个因素，包括安全性、效率、scalability、容错性等。安全性是指共识机制能够抵御恶意节点的攻击，确保账本数据的不可篡改和一致性；效率是指共识机制能够快速完成交易验证和确认，满足数据实时性需求； scalability是指共识机制能够适应节点数量的增加和数据规模的扩大，确保系统的性能稳定；容错性是指共识机制能够在部分节点发生故障或被攻击的情况下，依然能够正常运行，确保数据的一致性。

目前，区块链领域存在多种共识机制，不同的共识机制具有不同的特点和适用场景，常用的共识机制主要包括工作量证明（PoW）、权益证明（PoS）、委托权益证明（DPoS）、实用拜占庭容错（PBFT）等。

工作量证明（PoW）是最早出现的共识机制，也是比特币采用的核心共识机制。其核心原理是：节点通过完成一定量的计算工作（即“挖矿”），来竞争交易验证和区块生成的权利，计算工作的难度由系统动态调整，确保区块生成的速度保持在一定范围内。节点完成计算工作后，将生成的区块广播到网络中，其他节点对区块进行验证，验证通过后将区块添加到自己的账本中，实现账本数据的同步。PoW共识机制具有较高的安全性和容错性，能够抵御恶意节点的攻击，但其也存在明显的局限性，即计算工作量巨大，能源消耗高，效率低下，不适合实时性要求较高的场景。例如，比特币网络的区块生成时间约为10分钟，每秒只能处理几笔交易，无法满足工业互联网高并发、实时性的数据处理需求。因此，PoW共识机制主要适用于对实时性要求不高、安全性要求较高的场景，如数字货币交易。

权益证明（PoS）是为了解决PoW共识机制能源消耗高、效率低下的问题而提出的一种共识机制。其核心原理是：节点的投票权和区块生成权取决于节点持有的代币数量和持有时间，持有代币数量越多、持有时间越长，节点获得区块生成权的概率越大。节点不需要进行大量的计算工作，只需通过质押一定数量的代币，即可参与共识过程。PoS共识机制的能源消耗低、效率高，区块生成速度快，适合对实时性要求较高的场景。但PoS共识机制也存在一定的局限性，即存在“富人更富”的问题，持有大量代币的节点能够获得更多的区块生成权，可能导致网络中心化；同时，代币质押的方式可能导致节点的积极性不足，影响系统的稳定性。常用的PoS共识机制包括以太坊2.0采用的Casper共识机制、Cardano采用的Ouroboros共识机制等。

委托权益证明（DPoS）是在PoS共识机制的基础上进行优化和改进的一种共识机制。其核心原理是：节点通过投票选举出一定数量的代表节点（通常为21–101个），由代表节点负责交易验证和区块生成，其他节点不参与共识过程，只需监督代表节点的行为。代表节点的选举周期固定，节点可以根据代表节点的表现进行重新投票，更换代表节点。DPoS共识机制的效率极高，区块生成速度快，每秒能够处理数千笔交易，适合高并发、实时性要求较高的场景。同时，DPoS共识机制通过选举代表节点，减少了参与共识的节点数量，降低了系统的计算压力，提高了系统的 scalability。但DPoS共识机制也存在一定的局限性，即代表节点的数量较少，可能导致网络中心化，且代表节点的安全性直接影响整个系统的安全性。常用的DPoS共识机制包括EOS采用的DPoS共识机制、TRON采用的DPoS共识机制等。

实用拜占庭容错（PBFT）是一种基于拜占庭容错算法的共识机制，主要适用于联盟链和私有链场景。其核心原理是：网络中的节点分为诚实节点和恶意节点，诚实节点按照协议进行数据交互和验证，恶意节点试图破坏系统的一致性。PBFT共识机制通过多轮投票和验证，确保在存在一定数量恶意节点（不超过总节点数的1/3）的情况下，依然能够实现账本数据的一致性。PBFT共识机制的效率高、延迟低，能够快速完成交易验证和确认，适合对实时性和安全性要求较高的场景。同时，PBFT共识机制不需要代币质押，节点的参与门槛较低，适合企业之间的协同场景。但PBFT共识机制也存在一定的局限性，即节点数量较多时，共识效率会下降，系统的 scalability较差。常用的PBFT共识机制包括Hyperledger Fabric采用的PBFT共识机制、Stellar采用的SCP共识机制等。

在工业互联网场景中，共识机制的选择需要结合工业场景的特点，综合考虑安全性、效率、实时性、 scalability等因素。工业互联网具有数据量大、实时性强、参与主体多、敏感数据多等特点，因此，需要选择效率高、延迟低、安全性高、能够适应高并发场景的共识机制。例如，在工业企业内部的数据存储和管理场景中，可采用PBFT共识机制，确保数据的安全性和实时性；在产业链协同场景中，可采用DPoS共识机制，提高数据共享的效率和 scalability；在对安全性要求极高的场景中，可采用PoS共识机制，兼顾安全性

和效率。此外，随着区块链技术的发展，越来越多的新型共识机制不断涌现，如混合共识机制、分片共识机制等，这些共识机制能够结合不同共识机制的优势，进一步提升系统的性能和安全性，为工业互联网数据安全存储与共享提供更有力的支撑。例如，在私有以太坊区块链网络中，Clique权威证明（PoA）共识算法比默认的Ethash工作量证明（PoW）算法具有更低的延迟，更适合工业互联网实时性需求，实验表明，使用1秒块周期时，平均延迟可降低至约6秒。

2.1.4 智能合约

智能合约是区块链技术的重要组成部分，是一种基于区块链的、能够自动执行预设规则的计算机程序，其核心思想是将合同的条款和条件编码到计算机程序中，当满足预设的触发条件时，程序自动执行相应的操作，无需人工干预。智能合约具有自动化、透明化、不可篡改、可追溯等特点，能够实现交易的自动化和智能化，减少人工干预，提高交易效率，降低交易成本。

智能合约的运行机制主要包括以下几个步骤：一是合约编写，开发人员根据业务需求，将合同的条款和条件编码到智能合约中，明确合约的触发条件、执行逻辑和操作内容；二是合约部署，将编写好的智能合约部署到区块链网络中，合约一旦部署，就无法被随意修改或删除，确保合约的不可篡改；三是合约触发，当区块链网络中发生满足合约触发条件的事件时，智能合约自动执行相应的操作；四是合约执行，智能合约执行过程中，所有操作都会被记录到区块链中，实现操作的可追溯。

智能合约的核心特点主要包括以下几个方面：一是自动化，智能合约能够自动执行预设的规则，无需人工干预，提高交易效率，减少人为错误；二是透明化，智能合约的代码和执行过程对所有节点公开透明，任何节点都可以查看合约的代码和执行记录，确保合约的公平性和可信性；三是不可篡改，智能合约一旦部署到区块链中，就无法被随意修改或删除，确保合约的稳定性和安全性；四是可追溯，智能合约的所有执行操作都会被记录到区块链中，能够实现操作的全流程追溯，便于监督和审计。

在工业互联网场景中，智能合约具有广泛的应用前景，能够解决传统工业场景中流程繁琐、效率低下、人为干预多等问题，实现工业流程的自动化和智能化。例如，在工业设备运维场景中，可部署智能合约，预设设备维护的触发条件（如设备运行时间达到预设值、设备运行参数异常等），当满足触发条件时，智能合约自动触发维护指令，通知维护人员进行设备维护，同时记录维护过程和结果，实现设备运维的自动化和可追溯；在供应链协同场景中，可部署智能合约，预设供应链交易的条款和条件（如货物交付时间、付款金额、质量标准等），当货物交付完成且质量合格时，智能合约自动触发付款操作，实现供应链交易的自动化结算，提高交易效率，减少交易纠纷；在数据共享场景中，可部署智能合约，预设数据访问权限的分配规则和数据共享的收益分配规则，当用户申请访问数据时，智能合约自动验证用户的权限，符合权限要求的用户才能访问数据，同时根据数据共享的情况，自动分配共享收益，实现数据共享的自动化和智能化。

智能合约的开发语言主要有Solidity、Vyper、Go等，其中Solidity是最常用的智能合约开发语言，被广泛应用于以太坊等区块链平台。Solidity语言具有语法简洁、功能强大、兼容性好等特点，能够满足不同场景的智能合约开发需求。在工业互联网场景中，开发智能合约时，需要结合工业业务的特点，确保合约的安全性、可靠性和实用性。例如，智能合约的代码需要经过严格的安全审计，避免出现代码漏洞，防止被黑客攻击；合约的执行逻辑需要符合工业业务的规则，确保合约能够正确执行相应的操作；合约的触发条件需要明确、具体，确保合约能够在合适的时机被触发。

然而，智能合约也存在一定的局限性，主要包括以下几个方面：一是代码漏洞风险，智能合约的代码一旦存在漏洞，可能被黑客利用，导致合约被攻击，造成经济损失；二是灵活性不足，智能合约一旦部署，就无法被随意修改，当业务需求发生变化时，无法及时调整合约的规则；三是算力限制，智能合约的执行需要消耗区块链网络的算力，复杂的智能合约可能会消耗大量的算力，影响系统的性能。为了解决这些问题，需要加强智能合约的安全审计和测试，采用代码审计工具和漏洞检测工具，及时发现和修复代码漏洞；同时，研究可升级的智能合约技术，实现智能合约的灵活调整；此外，优化区块链网络的算力分配，提高智能合约的执行效率。

在工业互联网数据安全存储与共享方案中，智能合约将发挥重要作用，通过部署智能合约，能够实现数据访问权限的自动分配、数据共享的自动审计、数据交易的自动结算等功能，提高数据存储与共享的效率和安全性。例如，通过智能合约实现基于属性的访问控制，自动验证用户的属性和权限，确保只有授权用户才能访问相应的数据；通过智能合约实现数据共享的审计追溯，自动记录数据的访问和操作记录，便于监督和审计；通过智能合约实现数据交易的自动化结算，确保数据共享的收益能够公平分配给数据提供方。同

时，结合工业互联网的业务特点，开发专用的智能合约，满足不同场景的数据安全存储与共享需求。例如，在工业数据共享场景中，智能合约可以定义数据查询的事件关键字，将交易元数据记录在区块链中，确保数据共享的不可抵赖性。

2.2 工业互联网数据安全需求

工业互联网数据涵盖工业生产全生命周期的各类数据，具有多源异构、实时性强、敏感性高、价值密度不均等特点，其安全需求与传统互联网数据安全需求存在显著差异，主要体现在数据完整性、数据机密性、数据可用性、细粒度访问控制等方面。明确工业互联网数据安全需求，是设计基于区块链的工业互联网数据安全存储与共享方案的前提和基础，能够确保方案的针对性和实用性。

2.2.1 数据完整性

数据完整性是工业互联网数据安全的核心需求之一，指工业数据在采集、传输、存储、使用、共享等全生命周期过程中，保持数据的真实性、准确性和一致性，不被篡改、伪造、丢失或损坏。工业互联网数据是工业企业生产决策、质量控制、设备运维等工作的重要依据，一旦数据完整性受到破坏，将导致企业决策失误、生产工艺混乱、产品质量不达标、设备故障等严重问题，给企业带来巨大的经济损失。

工业互联网数据完整性的需求主要体现在以下几个方面：一是数据采集阶段的完整性，工业数据主要通过工业设备、传感器、控制系统等进行采集，需要确保采集的数据真实、准确、完整，避免因采集设备故障、网络中断、人为操作失误等原因导致数据缺失、错误或失真；二是数据传输阶段的完整性，工业数据在网络中传输时，需要确保数据不被篡改、伪造或丢失，避免因网络攻击、传输链路故障等原因导致数据完整性受到破坏；三是数据存储阶段的完整性，工业数据存储在存储设备或系统中时，需要确保数据不被篡改、删除或损坏，避免因存储设备故障、软件漏洞、黑客攻击等原因导致数据丢失或完整性破坏；四是数据使用和共享阶段的完整性，工业数据在使用和共享过程中，需要确保数据的一致性，避免因数据复制、修改等操作导致数据出现差异，影响数据的使用价值。

例如，在工业生产控制场景中，设备运行数据的完整性直接影响生产工艺的优化和产品质量的控制。如果设备运行数据被篡改，可能导致生产设备异常运行，生产出不合格产品；如果设备运行数据丢失，可能导致生产流程中断，无法正常生产。在产品质量追溯场景中，产品质量数据的完整性直接影响追溯的准确性和有效性。如果产品质量数据被伪造，可能导致不合格产品流入市场，损害企业信誉和消费者利益；如果产品质量数据缺失，可能无法准确追溯产品的质量问题源头，无法及时采取召回措施。

为了满足工业互联网数据完整性需求，需要采取有效的技术措施，确保数据在全生命周期过程中的完整性。传统的技术措施主要包括数据校验、数据备份、访问控制等，但这些措施存在一定的局限性，无法有效抵御黑客攻击、数据篡改等安全威胁。区块链技术的不可篡改、可追溯特性，能够为工业互联网数据完整性提供可靠的保障。通过将工业数据记录到区块链中，利用哈希算法、数字签名等技术对数据进行加密处理，确保数据一旦被记录，就无法被随意修改或删除；同时，通过分布式账本实现数据的多副本存储，确保数据不会因单点故障而丢失，从而保障数据的完整性。根据中华人民共和国国家标准《工业互联网企业网络安全 第4部分：数据防护要求》（征求意见稿），工业互联网数据处理者需对重要和核心数据的完整性进行重点保护，做好数据分类分级管理，确保数据全生命周期的完整性。

此外，还需要建立数据完整性验证机制，定期对工业数据进行完整性检测，及时发现数据篡改、丢失等问题，并采取相应的恢复措施。例如，通过区块链的哈希值验证机制，定期计算数据的哈希值，并与区块链中存储的哈希值进行对比，如果两者不一致，说明数据完整性受到破坏，需要及时进行数据恢复。同时，加强数据采集、传输、存储、使用、共享等环节的管理，规范操作流程，避免人为操作失误导致数据完整性破坏。

2.2.2 数据机密性

数据机密性是工业互联网数据安全的重要需求，指工业数据中包含的敏感信息（如核心工艺参数、设备运行机密、研发设计方案、供应链核心数据、个人信息等）不被未授权的用户获取、窃取或泄露，确保数据的隐私和安全。工业互联网数据中包含大量的敏感信息，这些信息关系到企业的核心竞争力和国家工业安全，一旦发生泄露，将给企业带来巨大的经济损失，甚至威胁国家安全。

工业互联网数据机密性的需求主要体现在以下几个方面：一是数据存储的机密性，工业敏感数据存储在存储设备或系统中时，需要确保数据不被未授权的用户访问、窃取或泄露，避免因存储设备漏洞、黑客攻击、内部人员泄露等原因导致数据机密性受到破坏；二是数据传输的机密性，工业敏感数据在网络中传输时，需要确保数据不被窃听、截取或篡改，避免因网络攻击、传输链路不安全等原因导致数据泄露；三是数据使用和共享的机密性，工业敏感数据在使用和共享过程中，需要确保数据只被授权的用户访问和使用，避

免未授权用户获取敏感数据，确保数据的隐私和安全。

例如，某航空航天企业的核心装备研发数据，包含装备的设计方案、工艺参数、性能指标等敏感信息，这些数据一旦泄露，可能被竞争对手窃取，导致企业失去市场优势，甚至威胁国家国防安全；某化工企业的生产工艺数据，包含化学反应方程式、原料配比、生产流程等敏感信息，这些数据一旦泄露，可能导致生产工艺被复制，企业的核心竞争力下降，同时可能引发安全事故。此外，工业互联网数据中还可能包含员工个人信息、客户信息等，这些信息的泄露也会违反相关法律法规，给企业带来法律风险。

为了满足工业互联网数据机密性需求，需要采取有效的加密保护措施，对工业敏感数据进行加密处理，确保数据在存储和传输过程中的安全性。传统的加密技术主要包括对称加密、非对称加密等，但这些技术在工业互联网场景中存在一定的局限性，如密钥管理难度大、加密效率低等。区块链技术结合密码学技术，能够为工业互联网数据机密性提供更有力的保障。通过采用对称加密算法对敏感数据进行加密存储，采用非对称加密算法对数据传输进行加密，结合数字签名、数字证书等技术，确保数据的机密性和真实性；同时，通过区块链的去中心化架构，避免数据集中存储带来的隐私泄露风险，确保敏感数据只有授权用户才能访问和使用。

此外，还需要建立完善的访问控制机制，对用户的访问权限进行精细化管理，确保只有授权用户才能访问相应的敏感数据；加强内部人员管理，规范内部人员的操作行为，防止内部人员泄露敏感数据；建立数据泄露检测机制，及时发现数据泄露事件，并采取相应的应对措施，减少数据泄露带来的损失。例如，通过基于属性的访问控制机制，根据用户的身份、属性、访问场景等因素，分配不同的访问权限，确保敏感数据不被未授权用户访问；通过数据泄露检测工具，实时监控数据的传输和使用情况，及时发现异常访问行为，防止数据泄露。同时，结合同态加密、差分隐私等新型隐私保护技术，进一步提升数据机密性保护水平，实现数据“可用不可见”。

3 基于区块链的工业互联网数据安全存储与共享方案设计

针对工业互联网数据安全的四大核心需求，结合区块链核心技术特性，本文设计一套分层化、混合链架构的工业互联网数据安全存储与共享方案，融合密码学、隐私计算、分布式存储等技术，实现数据全生命周期的安全存储、合规共享与隐私保护，兼顾系统性能与工业场景的高并发、实时性要求。

3.1 总体架构设计

3.1.1 分层架构

方案采用五层分层架构，从下到上依次为物理层、数据采集层、区块链基础层、安全服务层、应用层，各层相互独立又协同联动，实现数据从采集到应用的全流程安全管控，同时便于系统的扩展与维护。

1.物理层：由工业设备、传感器、服务器、网络设备等硬件组成，是工业数据产生和传输的物理载体，通过硬件级加密、节点身份认证实现底层安全防护；

2.数据采集层：负责工业全流程数据的采集、清洗、标准化处理，解决工业数据多源异构问题，同时对采集数据进行初步哈希校验，确保原始数据的完整性；

3.区块链基础层：是方案的核心技术层，包含分布式账本、密码学模块、共识机制、智能合约引擎等，实现数据的链上存证、分布式同步、智能规则执行，采用PBFT+DPoS混合共识机制，兼顾安全性与高并发处理能力；

4.安全服务层：提供数据加密、访问控制、权限管理、审计追溯、隐私保护等核心安全服务，是连接区块链基础层与应用层的桥梁，适配工业互联网的细粒度安全需求；

5.应用层：面向工业生产控制、设备运维、供应链协同、研发设计等具体场景，提供可视化的数据存储、共享、查询界面，满足不同工业主体的实际业务需求。

3.1.2 混合链结构

结合工业互联网参与主体多元、数据敏感程度差异大的特点，方案采用联盟链+私有链的混合链结构，对不同类型数据进行分级存储与共享，兼顾数据安全性、共享效率与管理可控性。

1.私有链：部署于企业内部，用于存储企业核心敏感数据，如研发设计方案、核心工艺参数、经营管理机密等，节点加入与退出由企业自主管控，仅对企业内部授权人员开放，采用PBFT共识机制，确保数据的高安全性和低延迟访问；

2.联盟链：由产业链上下游企业、监管部门等多方共同参与搭建，用于存储企业间需共享的非核心数据，如供应链交易数据、设备运维协同数据、行业监管数据等，通过准入机制限制节点范围，采用DPoS共识机制，提高数据共享的效率和扩展性；

3.跨链交互：通过跨链技术实现私有链与联盟链的安全数据交互，企业可将需共享的非核心数据从私有链同步至联盟链，核心数据仅在私有链内流转，同时通过智能合约

实现跨链数据的访问权限管控，防止数据越权访问。

3.2 数据安全存储机制

3.2.1 数据分片与加密存储

针对工业互联网海量数据存储需求和敏感数据保护需求，采用数据分片+混合加密的存储方式，既降低单节点存储压力，又提升数据加密等级。

1.对采集的工业数据按数据类型、密级、业务场景进行分片处理，将大文件数据拆分为多个小数据分片，分散存储在区块链网络的不同节点上，避免单节点存储过载；

2.采用“对称加密+非对称加密”混合加密策略：对数据分片采用AES-256对称加密算法进行加密存储，提高加密效率；对对称加密的密钥采用ECC非对称加密算法进行加密，密钥仅由数据拥有方和授权访问方持有，确保密钥安全。

3.2.2 链上存证与链下存储结合

为解决区块链本身存储容量有限、海量数据存储效率低的问题，采用链上存证+链下分布式存储的协同模式，实现数据高效存储与可追溯性的兼顾。

1.链上存证：将工业数据的哈希值、数据元信息（数据名称、类型、密级、采集时间、拥有方）、访问权限规则等关键信息记录在区块链上，利用区块链的不可篡改、可追溯特性，确保数据关键信息的真实性和完整性；

2.链下存储：将数据本体存储在IPFS分布式存储系统中，IPFS为每个数据文件生成唯一的内容标识（CID），并与区块链上的哈希值关联，实现数据本体与链上信息的一一对应；

3.数据访问时，用户先通过区块链验证数据元信息和访问权限，验证通过后根据CID从IPFS中获取数据本体，既保证了数据的可追溯性，又突破了区块链的存储瓶颈。

3.2.3 数据完整性动态验证

建立全生命周期数据完整性动态验证机制，实时检测数据在采集、传输、存储、使用过程中的完整性，及时发现数据篡改、丢失问题。

1.采集阶段：对采集的原始数据进行哈希计算，将哈希值与数据同步上传至区块链，实现原始数据的哈希存证；

2.传输阶段：采用哈希链技术，对传输过程中的数据分片依次生成哈希值，形成哈希链，接收方通过验证哈希链的连续性验证数据传输完整性；

3.存储与使用阶段：智能合约定时对链下存储的数据进行哈希重计算，将计算结果与区块链上存储的原始哈希值进行对比，若两者不一致，立即触发安全预警，同时通过区块链追溯数据修改节点和操作记录，实现数据完整性的动态监控和问题溯源。

3.3 数据安全共享机制

3.3.1 基于属性的访问控制

结合工业互联网细粒度访问控制需求，设计基于属性的访问控制（ABAC）模型，并将访问控制规则编码到智能合约中，实现权限的自动化、精细化管控。

1.定义多维度属性集，包括用户属性（身份、岗位、所属企业、操作权限）、数据属性（数据密级、类型、所属业务场景）、环境属性（访问时间、访问地点、网络环境）；

2.智能合约根据预设的访问控制策略，对用户的访问请求进行多维度属性匹配，只有当用户属性、环境属性与数据属性的匹配度满足预设条件时，才授予用户相应的访问权限，实现“按需授权、最小权限”。

3.3.2 动态权限管理

针对工业互联网业务场景动态变化的特点，实现权限的全生命周期动态管理，通过智能合约实现权限的自动分配、更新与回收，减少人工干预，提高权限管理效率。

1.权限分配：数据拥有方通过智能合约预设权限分配规则，根据用户属性自动为新加入节点分配相应的访问权限；

2.权限更新：当用户属性、数据属性或业务场景发生变化时，智能合约自动触发权限更新，实时调整用户的访问权限；

3.权限回收：当合作关系终止、用户岗位调整或访问期限到期时，智能合约自动回收用户的相关访问权限，防止权限滥用。

3.3.3 数据共享审计与追溯

利用区块链的不可篡改、可追溯特性，建立全流程数据共享审计追溯机制，对所有数据共享操作进行实时记录和永久存储，实现操作行为的可审计、可溯源、可追责。

1.数据的每一次访问、查询、修改、共享操作都会被记录在区块链上，记录内容包括操作主体、操作时间、操作内容、数据状态等关键信息，且记录无法被篡改或删除；

2.系统提供审计查询界面，企业和监管部门可随时查询数据共享操作记录，对异常操作进行实时监控；

3.当发生数据安全事件时，通过区块链的链式结构追溯数据的全流程操作记录，快速定位事件源头和责任主体，及时采取应对措施。

3.4 隐私保护增强技术

为进一步提升工业互联网敏感数据的隐私保护能力，引入同态加密和差分隐私等隐私计算技术，与区块链技术

融合，实现数据“可用不可见”，兼顾数据共享价值与隐私保护。

3.4.1 同态加密

在数据共享计算场景中，采用部分同态加密算法对敏感数据进行加密处理，使得数据在加密状态下可直接进行计算，无需解密，计算结果解密后与原始数据计算结果一致。

例如，在供应链协同场景中，上下游企业需要对销售数据、库存数据进行联合统计分析，采用同态加密技术对各自的敏感数据进行加密后上传至联盟链，在加密状态下完成数据统计计算，既实现了数据的协同分析，又避免了原始数据的泄露，保障了企业数据隐私。

3.4.2 差分隐私

在数据公开与批量共享场景中，采用差分隐私技术，通过向原始数据中添加适量的噪声数据，对数据进行扰动处理，使得攻击者无法从扰动后的数据中推导出单个数据主体的敏感信息，同时保证数据的整体统计特征不变。

例如，企业向行业监管部门上报生产统计数据时，通过差分隐私技术对数据进行扰动处理，监管部门可利用扰动后的数据进行行业整体分析，而无法推导出企业的具体生产数据，既满足了监管需求，又保护了企业的商业隐私。

4 方案实施与验证

4.1 实验环境搭建

4.1.1 区块链平台选择

基于方案的混合链结构和工业场景需求，选择Hyperledger Fabric作为联盟链开发平台，该平台支持模块化设计、细粒度访问控制和智能合约开发，适配企业间的协同场景；采用私有以太坊作为企业私有链平台，通过定制化共识机制（PoA）降低访问延迟，满足企业内部高实时性数据处理需求。

实验环境基于Docker容器化部署，搭建由10个节点组成的区块链网络，其中6个联盟链节点（涵盖生产企业、供应商、监管部门），4个私有链节点（企业内部各部门），节点配置为CPU 4核、内存8G、硬盘512G，网络带宽为1000Mbps。

4.1.2 工业互联网模拟场景构建

模拟装备制造行业供应链协同场景构建实验环境，搭建工业数据采集模拟系统，模拟设备运行数据、生产工艺数据、供应链交易数据、库存数据等多类型工业数据的采集与传输，数据采集频率为1秒/次，模拟生成海量异构工业数据；同时搭建数据共享模拟平台，实现上下游企业、监管部门之间的数据共享与交互，模拟工业互联网多主体、高并发的业务场景。

4.2 性能与安全性分析

4.2.1 吞吐量与延迟测试

对方案的吞吐量和访问延迟两个核心性能指标进行测试，并与传统集中式存储方案进行对比，测试结果表明：

1.方案的吞吐量可达3200 TPS（每秒交易数），远高于传统集中式方案的1800 TPS，能够满足工业互联网高并发的数据处理需求；

2.数据访问平均延迟为8.2ms，联盟链跨节点数据共享延迟为15.6ms，均控制在工业场景可接受的延迟范围内，优于纯区块链存储方案的延迟表现，主要得益于链上存证与链下存储的协同模式。

4.2.2 安全性验证

通过模拟常见的网络攻击手段（DDoS攻击、数据篡改攻击、越权访问攻击）对方案进行安全性验证，验证结果表明：

1.面对DDoS攻击，由于区块链的去中心化架构，单个节点遭受攻击后，其他节点仍能正常运行，系统无服务中断现象，数据可用性不受影响；

2.尝试对链下存储数据进行篡改，系统通过哈希值对比快速检测到数据篡改，并触发安全预警，同时通过区块链追溯到篡改节点，数据完整性得到有效保障；

3.未授权用户尝试越权访问核心敏感数据，由于基于属性的访问控制机制的拦截，访问请求均被拒绝，数据机密性得到有效保护。

4.2.3 隐私保护效果评估

对同态加密和差分隐私技术的隐私保护效果进行评估，结果表明：

1.采用同态加密技术后，数据在加密状态下的计算误差率低于0.5%，既保证了数据计算的准确性，又实现了原始数据的隐私保护；

2.采用差分隐私技术后，数据的整体统计特征保持不变，单个数据主体的敏感信息泄露风险低于0.1%，满足工业互联网数据隐私保护的要求。

5 结论与展望

5.1 研究成果总结

本文针对工业互联网传统集中式数据存储与共享方案的安全隐患，结合区块链技术的核心特性，设计了一套基于区块链的工业互联网数据安全存储与共享方案，主要研

究成果如下：

1.系统分析了工业互联网数据安全的核心需求（完整性、机密性、可用性、细粒度访问控制），明确了区块链技术与工业互联网数据安全的内在关联，为方案设计奠定了理论基础；

2.构建了五层分层架构与联盟链+私有链的混合链结构，实现了不同密级数据的分级存储与管控，兼顾了系统的安全性、扩展性与工业场景适配性；

3.设计了数据分片加密存储、链上存证与链下存储协同、数据完整性动态验证的存储机制，解决了工业海量数据存储与数据完整性保障问题；

4.提出了基于属性的访问控制、动态权限管理、全流程审计追溯的共享机制，实现了工业数据的合规共享与细粒度权限管控；

5.引入同态加密、差分隐私等隐私计算技术，增强了方案的隐私保护能力，实现了数据“可用不可见”；

6.通过搭建装备制造行业供应链协同模拟场景，对方案的性能和安全性进行了全面验证，结果表明方案能够有效抵御各类常见网络攻击，保障数据存储安全与共享合规，同时具备良好的吞吐量和低延迟特性，能够满足工业互联网多场景、高并发的数据处理需求。

本文的研究成果为工业互联网数据安全管理提供了新的技术路径和实践参考，对推动工业互联网的高质量发展具有重要的理论和现实意义。

5.2 未来研究方向

虽然本文设计的方案在性能和安全性方面取得了较好的验证效果，但仍存在一些不足，未来将从以下几个方面进行优化和拓展：

1.共识机制优化：进一步研究适用于工业互联网的轻量化、自适应共识机制，结合工业场景的实时性、高并发需求，实现共识机制的动态调整，兼顾系统安全性和处理效率；

2.跨链技术升级：目前的跨链交互仍存在一定的延迟和复杂度，未来将研究高性能的跨链技术，实现私有链、联盟链与公有链的高效、安全交互，打破不同区块链网络之间的“数据孤岛”；

3.边缘区块链融合：将区块链技术与边缘计算结合，构建边缘区块链网络，将工业数据的采集、存储、计算下沉至边缘节点，降低数据传输延迟，满足工业互联网设备端的实时性数据处理需求；

4.智能合约安全增强：针对智能合约的代码漏洞风险，研究智能合约的自动化安全审计和漏洞修复技术，开发适用于工业场景的专用智能合约框架，提升智能合约的安全性和可靠性；

5.多技术融合应用：进一步融合人工智能、大数据、数字孪生等技术，实现工业互联网数据安全的智能化管控，例如利用人工智能算法对异常数据操作进行实时检测和预警，提升系统的安全防护能力。

未来，随着区块链技术的不断成熟和工业互联网的深入发展，将持续优化方案的技术架构和功能模块，推动方案在更多工业场景的落地应用，为工业互联网数据安全保障体系建设提供更有力的支撑。

参考文献：

[1]区块链技术与应用编写组.区块链技术与应用[M].北京：人民邮电出版社，2021.

[2]谢希仁.计算机网络（第8版）[M].北京：电子工业出版社，2021.

[3]王健，张艳霞，李琦.区块链在工业互联网数据安全中的应用研究[J].计算机工程与应用，2023，59（12）：1-10.

[4]张楠，刘军，王颖.基于联盟链的工业数据共享模型设计与实现[J].计算机应用研究，2024，41（03）：892-896.

[5]陈俊宇，李红娟，杨明.混合加密技术在工业互联网数据存储中的应用[J].微电子学与计算机，2023，40（08）：78-85.

[6]孟小峰，杜治娟.大数据隐私保护技术研究综述[J].计算机学报，2019，42（01）：1-31.

[7]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（04）：481-494.

[8]高胜，李丽香，张伟.基于Hyperledger Fabric的工业供应链数据共享系统[J].计算机工程，2024，50（02）：201-208.

[9]黄瑞章.工业互联网细粒度访问控制模型研究[D].杭州：浙江大学，2023.

[10]刘鹏，王健.同态加密与区块链融合的工业数据隐私保护方案[J].通信学报，2023，44（09）：123-132.