

基于区块链的航天数据安全共享机制

戴旭鹏

航天科技控股集团股份有限公司，北京，100071；

摘要：本文围绕航天数据安全共享展开深入研究，详细阐述其在科学研究、地球观测及航天工程领域的重要价值，同时指出共享过程中面临的数据安全风险、权属界定模糊、数据质量不一以及传统共享方式局限等突出问题。区块链技术凭借去中心化、不可篡改、可追溯等独特特性，在保障数据安全、明晰权益归属、实现全流程溯源等方面优势显著，与航天数据多源、异构、海量、高价值的特性高度适配。文中构建了包含数据层、网络层、共识层、合约层和应用层的完整机制框架，深入探讨数据加密、智能合约、共识算法优化及数据溯源等关键技术，并提出建立数据共享联盟、加强安全管理等应用策略。研究表明，区块链为航天数据安全共享提供了全新路径，虽在技术融合方面仍需深化，但未来通过优化算法等可完善解决方案。

关键词：区块链；航天数据；安全共享；机制构建

DOI：10.64216/3080-1508.25.05.041

航天数据是人类探索宇宙的重要成果，在科学研究中助力科学家深入了解宇宙演化规律、天体物理特性，推动天文学、物理学等基础学科持续突破；在地球观测领域为气象预报、资源勘探、环境监测等提供高精度信息，是人类科学管理和保护地球家园的关键支撑；在航天工程中，不同部门和机构通过共享航天器设计、测试、运行数据，能显著提升项目协同效率，降低研发成本，加速航天技术迭代升级。然而，其共享存在诸多阻碍：数据包含航天器关键参数、军事侦察信息等敏感内容，泄露将严重威胁国家安全；权属涉及多参与方，界定不清易引发权益纠纷；不同来源数据格式不统一、精度有差异，增加整合分析难度；传统集中式共享模式易受攻击，且灵活性不足。区块链技术的出现为破解这些难题带来新希望，研究其在航天数据安全共享中的应用具有重要意义。

1 航天数据共享现状与问题分析

1.1 航天数据共享的重要性

航天数据是探索宇宙、认识自然的重要成果，应用价值广泛。科学研究中，共享数据能助科学家全面了解宇宙演化、天体物理特性，推动相关学科发展。地球观测领域，遥感数据为气象预报、资源勘探等提供准确信息，助力地球管理保护。航天工程中，共享航天器相关数据可提高协同效率，降低研发成本，提升技术水平。

1.2 航天数据共享面临的问题

航天数据共享存在安全和管理问题。数据安全是首要的，其含大量敏感信息，泄露会严重威胁国家安全与航天事业。数据所有权和使用权界定不清，因涉及多参与方，易引发纠纷。此外，数据质量和一致性影响共享

效果，不同来源数据格式、精度可能不一，增加整合分析难度。

1.3 传统数据共享方式的局限性

传统航天数据共享基于集中式数据库和服务器，有明显局限。集中式系统易成攻击目标，中心服务器被攻破则数据面临安全风险。集中式管理下，数据共享流通受中心机构严格控制，缺乏灵活性和自主性，难满足多主体、多层次需求。且数据溯源和审计困难，无法有效跟踪流向和使用，不利于监管。

2 区块链技术在航天数据安全共享中的应用原理

2.1 区块链技术概述

区块链是分布式账本技术，由多节点网络共同维护不可篡改的数据库。数据以区块存储，含一定交易记录，通过哈希算法与前一区块相连成链式结构。其具有去中心化（无中心节点，节点平等参与存储验证）、不可篡改（数据记录后难修改，保证完整可靠）、可追溯（能追踪数据来源和历史记录）、共识机制（确保节点对数据一致认可）等特点。

2.2 区块链技术在航天数据安全共享中的优势

区块链为航天数据安全共享带来显著优势。数据安全上，加密算法和分布式存储让数据难被窃取篡改，部分节点受攻击不影响整体。数据权属管理上，可通过智能合约精细控制，依预设规则管理访问使用，明确各方权责。数据溯源审计上，可追溯性让数据流转清晰，便于监管审计，提升共享透明度和可信度。

2.3 区块链与航天数据的适配性分析

航天数据多源、异构、海量、高价值，与区块链特性适配性好。多源异构数据可借分布式存储和格式标准化整合共享；海量数据需可靠存储管理，分布式账本提供高可用、容错的方案；高价值数据对安全可信度要求高，区块链不可篡改、可追溯能满足；多方参与共享时，去中心化和共识机制可促进信任协作，提高效率。

3 基于区块链的航天数据安全共享机制框架构建

3.1 机制框架总体设计

基于区块链的航天数据安全共享机制框架含数据层、网络层、共识层、合约层和应用层^[1]。数据层用分布式存储技术，将航天数据分散存于多节点，提升安全性与可靠性；网络层为节点通信网络，借 P2P 协议实现信息传输交互；共识层采用 PoW、PoS 等合适算法，确保节点对数据一致认可；合约层含智能合约，定义共享规则流程以实现自动化管理；应用层为用户提供共享接口和服务，满足不同需求。

3.2 数据层设计

在数据层，首先需要对航天数据进行分类和标准化处理。根据数据的类型、来源和用途，将航天数据分为不同的类别，如科学探测数据、地球观测数据、工程实验数据等，并制定统一的数据格式和标准，以便于数据的存储和共享。然后，采用分布式文件系统（如 IPFS）将数据存储在多个节点上，每个节点只存储部分数据，通过哈希指针将数据块链接起来，保证数据的完整性和可追溯性^[2]。同时，对数据进行加密处理，采用对称加密和非对称加密相结合的方式，确保数据在存储和传输过程中的安全性^[3]。

3.3 网络层设计

网络层是区块链节点之间进行通信和数据交换的基础。采用 P2P 网络架构，每个节点都可以与其他节点直接通信，形成一个去中心化的网络。为了提高网络的可靠性和性能，需要优化节点的选择和连接策略。例如，可以采用基于地理位置、网络带宽等因素的节点选择算法，选择合适的节点进行连接。同时，为了保证网络的安全性，需要对节点之间的通信进行加密和认证，防止中间人攻击和数据泄露。

3.4 共识层设计

共识层是区块链核心，确保网络节点对数据一致认可。航天数据安全共享需选合适共识算法：安全性要求高、节点少的场景，可用权益证明（PoS）算法，依节点权益比例选记账节点，避免工作量证明（PoW）高能耗，且保证一定安全性；需快速共识、节点多的场景，

可采用实用拜占庭容错（PBFT）算法，能在保障安全的同时快速达成共识，提升数据共享效率。

3.5 合约层设计

合约层的智能合约是实现航天数据安全共享规则和流程自动化的关键。智能合约可以定义数据的所有权、使用权、访问权限、共享费用等规则。例如，通过智能合约可以规定只有经过授权的用户才能访问特定的数据，并且在数据使用过程中，根据使用的次数或时长收取相应的费用。智能合约还可以实现数据的自动分发和更新，当数据发生变化时，智能合约可以自动通知相关用户，并更新他们的数据副本。同时，智能合约的执行过程是公开透明的，可以接受所有节点的监督，保证了数据共享过程的公正性和可信度。

3.6 应用层设计

应用层为用户提供了便捷的数据共享接口和服务。开发专门的航天数据共享平台，用户可以通过该平台上传、下载、查询和分析航天数据。平台提供友好的用户界面，方便用户操作。同时，平台还提供数据安全审计和监管功能，对数据的共享行为进行实时监控和记录，生成审计报告，以便于对数据共享过程进行管理和监督。此外，应用层还可以与其他相关系统进行集成，如航天项目管理系统、科学研究平台等，实现数据的无缝对接和协同工作。

4 基于区块链的航天数据安全共享机制的关键技术

4.1 数据加密技术

数据加密是保障航天数据安全的重要手段。在区块链环境下，采用对称加密和非对称加密相结合的方式。对称加密算法如 AES，具有加密速度快、效率高的特点，用于对大量的数据进行加密^[4]。非对称加密算法如 RSA，用于对对称加密密钥进行加密和数字签名。在数据存储时，首先使用对称加密算法对数据进行加密，然后使用接收方的公钥对对称加密密钥进行加密，将加密后的密钥和数据一起存储在区块链上。在数据传输过程中，同样采用加密技术，确保数据在网络中传输的安全性。

4.2 智能合约技术

智能合约是区块链技术的重要应用之一，在航天数据安全共享中发挥着关键作用。智能合约可以用编程语言（如 Solidity）编写，部署在区块链上^[5]。通过智能合约，可以实现数据共享的自动化管理，包括数据的授权、访问控制、费用结算等。例如，当用户请求访问数据时，智能合约会根据预设的规则进行验证，如果用户满足条件，则自动授予访问权限，并记录数据的使用情

况。智能合约还可以实现数据的版本控制和更新,确保用户使用的是最新的数据。

4.3 共识算法优化技术

在航天数据安全共享中,需要根据不同的应用场景优化共识算法。对于对安全性要求较高的场景,可以采用混合共识算法,结合多种共识算法的优点,提高共识的可靠性和效率。例如,可以将 PoS 和 PBFT 算法相结合,先通过 PoS 算法选择出一组候选记账节点,然后在这些节点中采用 PBFT 算法达成共识。同时,为了提高共识算法的性能,需要对算法进行优化,如减少共识过程中的通信开销、降低算法的复杂度等。

4.4 数据溯源技术

数据溯源是区块链技术的重要特性之一,在航天数据安全共享中具有重要意义。通过区块链的链式结构和哈希算法,可以实现对数据的全生命周期追溯。从数据的产生、存储、传输到使用,每一个环节都被记录在区块链上,形成一个完整的溯源链条。当出现数据安全问题或纠纷时,可以通过溯源链条快速定位问题的源头,查明数据的流向和使用情况,为数据安全管理和责任追究提供有力的证据。

5 基于区块链的航天数据安全共享机制的应用策略

5.1 建立数据共享联盟

为了推动航天数据的安全共享,需要建立数据共享联盟。联盟成员包括航天科研机构、高校、企业等相关参与方。联盟制定统一的数据共享规则和标准,明确各方的权利和义务。通过区块链技术,实现联盟内数据的安全共享和管理。联盟成员可以根据自身的需求上传和下载数据,同时按照规则对数据的使用进行付费和监管。建立数据共享联盟可以促进航天领域的协同创新,提高数据资源的利用效率。

5.2 加强安全管理

加强航天数据安全共享的管理是保障数据安全的关键。制定严格的安全管理制度,包括数据访问控制、用户认证、数据备份等。对参与数据共享的人员进行安全培训,提高他们的安全意识和防范能力。同时,建立安全审计机制,对数据共享过程进行实时监控和审计,及时发现和处理安全隐患。采用多重安全防护技术,如防火墙、入侵检测系统等,保障区块链网络的安全。

5.3 促进技术创新和人才培养

为了推动基于区块链的航天数据安全共享机制的发展,需要加强技术创新和人才培养。鼓励科研机构和

企业开展区块链技术在航天领域的应用研究,探索新的技术解决方案。同时,加强高校和职业院校的相关专业建设,培养既懂航天技术又懂区块链技术的复合型人才。通过技术创新和人才培养,不断提升航天数据安全共享的技术水平和应用能力。

6 结论与展望

6.1 研究成果总结

本文深入研究了基于区块链的航天数据安全共享机制,通过分析航天数据共享的现状与问题,阐述了区块链技术在航天数据安全共享中的应用原理,构建了基于区块链的航天数据安全共享机制框架,并对其关键技术和应用策略进行了探讨。研究表明,区块链技术能够有效解决航天数据共享中的安全、管理等问题,提高数据共享的安全性和效率,为航天领域的数据资源有效利用提供了新的途径。

6.2 研究的不足与展望

虽然本文在基于区块链的航天数据安全共享机制方面取得了一定的研究成果,但仍存在一些不足之处。例如,在区块链技术与航天数据的深度融合方面还需要进一步探索,如何更好地适应航天数据的特殊需求和应用场景,还需要开展更多的研究工作。未来的研究方向可以包括:进一步优化区块链的共识算法和智能合约,提高系统的性能和可靠性;加强区块链技术与其他新兴技术(如人工智能、大数据等)的融合,提升航天数据的分析和处理能力;拓展航天数据安全共享的应用范围,推动航天数据在国际间的共享与合作等。通过不断的研究和创新,有望为航天事业的发展提供更加完善的数据安全共享解决方案。

参考文献

- [1]王小畅. 基于区块链的分布式数据安全共享技术研究及应用[D]. 北京邮电大学,2021.
- [2]陈嘉熈. 基于区块链的跨域数据共享技术研究[D]. 电子科技大学,2021.
- [3]岑志鹏. 基于 React 的布控报警系统的设计与实现[D]. 武汉邮电科学研究院,2020.
- [4]刘博文. AES-RSA 混合加密算法的研究及其在军队后勤管理系统中的应用[D]. 浙江大学,2022.
- [5]兰田. 基于深度卷积神经网络的区块链异常行为检测方法研究[D]. 齐鲁工业大学,2023.

作者简介:戴旭鹏,(1989.10—),男,汉族,辽宁丹东人,工程师,本科,研究方向:物联网、油料能源、航天仪器仪表等。