

DOI:10.19344/j.cnki.issn1671-5276.2025.04.026

高端装备分布式生产过程数据可信管理方法研究

朱浩杰¹, 张浩², 朱海华¹, 张毅¹

(1. 南京航空航天大学 机电学院, 江苏 南京 210016;

2. 中国电子科技集团公司第二十八研究所, 江苏 南京 210016)

摘 要:针对高端装备分布式协同生产过程中存在的数据存储效率低、安全性不强、缺乏一致性等问题,提出基于区块链技术的分布式数据可信管理方法。通过分析高端装备数据管理流程,提出基于区块链的高端装备生产数据管理架构,阐述基于 IPFS 的数据存储共享与基于信用模型的 Raft 共识技术,以此实现生产数据真实可信和高效存储共享,并通过实验验证其可行性。

关键词:区块链; 高端装备; 数据管理; Raft 共识

中图分类号: TP274 **文献标志码:** A **文章编号:** 1671-5276(2025)04-0144-06

Research on Trusted Management Method of Distributed Production Process Data for High-end Equipment

ZHU Haojie¹, ZHANG Hao², ZHU Haihua¹, ZHANG Yi¹

(1. College of Mechanical and Electrical Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China;

2. The 28th Research Institute of China Electronics Technology Group Company, Nanjing 210016, China)

Abstract: A distributed data trusted management method based on blockchain technology is put forward regarding low data storage efficiency, weak security, and lack of consistency ect. in the distributed collaborative production process of high-end equipme. By analyzing the data management process of high-end equipment, a blockchain-based production data management architecture is proposed, and the IPFS-based data sharing method and the credit-based Raft consensus technology are elaborated to achieve authentic, credible and efficient storage and sharing of production data with the verification of its feasibility through experiments.

Keywords: blockchain; high-end equipment; data management; Raft consensus

0 引言

高端装备是制造产业链中关键基础装备,广泛应用于卫星、航空、船舶等领域^[1]。高端装备具有零部件结构多且复杂、配套产业涉及的企业多等特点,通常由多家企业共同承担完成其生产任务^[2-6]。

目前,高端装备生产数据的管理方式主要采用集中式架构^[7]。在此架构下,参与协同生产的配套企业需要将制造资源信息及运行数据上传至中心管理平台。在数据共享过程中,企业担心敏感数据信息存在泄密风险,从而倾向于将数据保存在本地数据库。因此,集中式数据管理模式缺乏陌生企业间数据共享的可信保障机制^[8-14]。

针对分布式制造中数据共享缺乏可信机制的问题,学者展开深入研究。孙淑文^[15]提出重定向

代理重加密方法抵御对数据发起的攻击,保证制造数据安全和高效存储。刘思彤等^[16]将区块链技术运用于航天侦察领域,实现航天侦察资源高效运用。徐杨杨等^[17]提出基于区块链的去中心化云制造交易平台框架,设计了制造资源校验合约和制造资源交易合约以实现资源匹配与配置,为协同制造过程提供了可追溯和安全性交易数据。SINGH 等^[18]针对跨领域数据共享存在的隐私安全问题,采用临时椭圆曲线签名算法完成数据签名验证,提出使用智能合约的惩罚机制从而避免数据提供商的不当行为,实现数据安全可信共享。通过对互联开放式协同制造领域相关文献进行的总结与分析,说明了区块链技术在分布式制造资源互信协作方面的可行性与必要性。

综上所述,已有研究采用去中心化联盟链框架、改进智能合约和共识机制等方法去解决隐私

基金项目:国家重点研发计划项目(2021YFB1716300)

第一作者简介:朱浩杰(1999—),男,江西九江人,硕士研究生,研究方向为分布式协同制造,17855519381@163.com。

• 145 •

术相结合,构建分布式 CA 数字身份认证联合体,解决配套生产企业身份与资源认证问题,如图 3 所示。设备层包括配套企业中的生产设备,用于提供各种生产过程数据;网关层包括网络服务基站和注册企业服务器(R_A)等,该层的网络设备接收企业设备发送的数据请求并转发给 R_A 。 R_A 是 CA 服务器与身份验证设备之间的接口,用于收集用户信息,确认用户身份,接受用户注册申请。区块链层用于认证 CA。CA 作为公钥基础设施系统的核心,负责颁发和管理证书,以及对各企业与用户的身份认证。

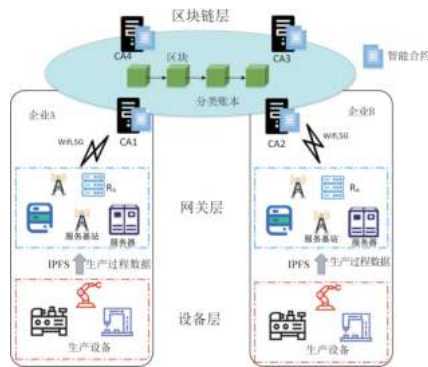


图3 身份认证架构图

当企业间某两台设备需要对进度数据等进行交互验证时,企业 A 中的设备 D_1 向企业 B 的设备 D_2 发送连接请求, D_2 向服务器 R_B 查询 D_1 的认证信息。 R_B 生成随机数 N 并发送给 D_1 , D_1 使用其私钥 SK_1 对数字 N 进行签名以获得 $\text{sign}(N, SK_1)$ 。同时,它对证书 Cert_1 执行哈希操作,并将 Cert_1 的哈希值 $\text{Hash}(\text{Cert}_1)$ 和 $\text{sign}(N, SK_1)$ 发送给 R_B , R_B 收到上述参数后开始进行身份验证。

R_B 解析证书 Cert_1 得到设备 D_1 的公钥 PK_1 和身份信息,用 PK_1 验证签名得到随机数 N' ,然后将 N' 与之前生成的 N 进行数值校对。如果校对结果为不同,则拒绝认证请求;如果相同的话, R_B 向区块链发起新一轮证书信息查询交易,通过此次交易过程获取证书的哈希值和状态,并验证证书的状态是否有效。如果无效,则表示认证失败;如果有效,将证书哈希值与请求参数中的哈希值进行比较。若比较结果不同,则拒绝认证请求;否则, R_B 保存设备 D_1 的证书,用 D_1 的公钥对设备 D_2 的证书 Cert_2 进行加密,并将认证同意结果反馈给 D_1 ,从而允许 D_1 访问 D_2 。其流程如图 4 所示,通过上述流程完成企业 A 中的设备 D_1 到企业 B 的设备 D_2 的数据交互请求。

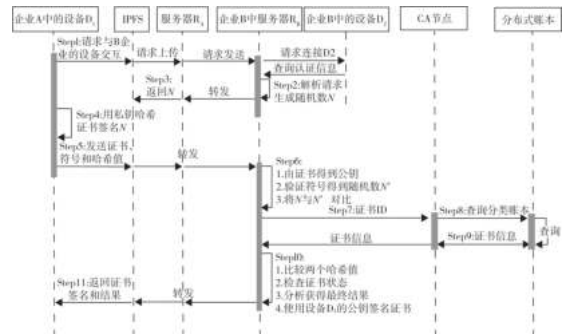


图4 企业间身份验证图

2.2 基于 IPFS 的数据共享与管理技术

高端装备生产数据结构关系复杂、数据量庞大,会大幅提升链上存储压力。采用传统数据库存储不利于数据共享,且数据访问效率低。本文将 IPFS 协议与区块链结合,实现对海量生产数据的分布式安全存储,利用 IPFS 的分布式存储特性来提高数据共享效率、缓解数据存储压力。图 5 展示了 IPFS 与 FISCO BCOS 相结合的体系结构。

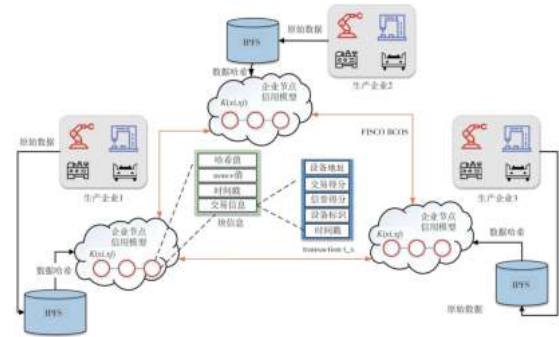


图5 基于 IPFS 的 FISCO BCOS 数据共享架构图

在该架构中,生产企业是 IPFS 的节点,区块链负责管理文件系统的数据哈希、分类账本存储与数据交易相关的信息。数据哈希会上传至 IPFS 网络,同时触发智能合约添加到分类账本中。对于大型文件数据,企业通过“ipfs add filename”将数据文件上传至 IPFS 网络,采用 SHA256 哈希算法对数据进行加密,从而生成唯一的文件内容标识(content identifier, CID),依此确保数据安全性和防篡改性。同时,因为链上只需保存数据相应的加密散列值,大大缓解了链上存储压力。

当企业需要对数据进行共享时,企业通过“ipfs cat ipfs/CID”命令读取 CID 值对应的数据信息,如果需要下载该文件内容,则可以通过“ipfs get ipfs/CID”下载文件到本地。通过 IPFS 协议,企业可以通过访问数据 CID 值直接对内容进行寻

址,实现数据快速便捷的访问共享。

2.3 基于 Raft 共识的数据一致性存储方案

为提升区块链安全性和节点性能,提出了节点信用评估标准,如表 1 所示。区块链生产网络节点根据此标准自动生成节点状态列表。考虑到生产联盟链中区块链网络规模较大,节点数量较多,故障节点的数量远小于诚实节点。本文使用一类支持向量机作为异常节点检测算法来解决故障节点与诚实节点之间的样本不均衡问题。

表 1 节点信用评判标准

索引	标准	权重
节点账户 交易	加入网络后产生的交易总数	0.1
	单位时间内产生的交易数量	0.1
	提交了无效事务	0.2
节点的性能	网络延时时间	0.1
	节点离线次数	0.1
	节点离线时间	0.1
节点积分 动态反馈	节点加入网络的时间	0.1
	在上一轮的 ANB(Array of non-Byzantine nodes, ANB)中	0.2

一类支持向量机问题可以被表示为如下的二次规划问题^[19]:

$$\begin{cases} \min \frac{1}{2} \|\mathbf{w}\|^2 + \frac{1}{vN} \sum_{i=1}^N \xi_i - \rho \\ \mathbf{w}^T \phi(x_i) \geq \rho - \xi_i, \xi_i \geq 0 \end{cases} \quad (1)$$

式中: x_i 表示一组训练样本, $i=1,2,\dots,N$; $\phi(x_i)$ 是一个特征投影函数,将 x_i 投影到更高维度的投影空间, $\mathbf{w}$ 是学习的权重向量; ρ 是偏移量,并且预定义参数 $v(0,1]$ 表示位于超平面的异常值侧的数据上限。引入松弛变量 ξ 以允许一些数据点位于裕度内。通过使用 Lagrange 变换并利用用于点积计算的核函数,将决策函数变为:

$$f(x) = \text{sign}((\mathbf{w}^T \phi(x_i)) - \rho) = \text{sign}\left[\sum_{i=1}^N \alpha_i K(x, x_i) - \rho\right] \quad (2)$$

$$\rho = (\mathbf{w}^T \phi(x_i)) = \sum_{i=1}^N \alpha_i K(x_i, x_j) \quad \sum_{i=1}^N \alpha_i = 1 \quad (3)$$

使用高斯径向基函数变换后:

$$K(x_i, x_j) = \exp \frac{-\|x_i - x_j\|^2}{2\sigma^2} \quad \sigma > 0 \quad (4)$$

式中: $\mathbf{w}^T$ 为训练集 T 中的权重; α_i 为任意非零乘数; σ 是核参数。基于来自每个节点的节点状态

列表,使用核函数 $K(x_i, x_j)$ 来确定节点是否属于学习区域。如果属于学习区,则是诚信节点;否则为拜占庭节点。

此阶段,随机选择主节点对网络中的全部节点进行信用评估。首先,主节点向生产网络中的所有节点发起信用评估请求,获取节点状态列表。在指定时间窗口内,主节点不断接收来自其他节点的状态记录列表,并结合自身状态列表作为输入。其次,使用节点信用评估模型确定节点是否为拜占庭节点,将由非拜占庭节点编号所构成的 ANB 作为输出。如果生产网络中的拜占庭节点数量为 f 时,需要为该节点选择并使用信用评估模型进行 $f+1$ 轮过滤和重复操作,同时每轮选中的主信用评估节点保持一致。每个回合,主节点将会生成 ANB_t ,其 t 为主节点被选中的次数。为了解决信用评估阶段可能出现的拜占庭问题,提出如下算法。

算法 1 ANB 生成算法

输入:n 个节点号和节点状态记录列表

输出:ANB,所有非拜占庭节点号组成的数组

ANB 是一个 ANB_t数组,每轮都要确认

H_t 为第 t 次的主节点

for 1 to (f+1) do

a. 执行节点信用评估模型

b. 生成 ANB

c. 广播 ANB_t

d. 如果 H_t 接收到超过 f 个节点的确认

ANB = ANB_t;

t++;

e. 否则:t++;

end for

节点信用评估模型能够在拜占庭节点数量远小于诚实节点数量的情况下,过滤出性能良好、可信度高的诚实节点,从而满足网络规模大、拜占庭节点数量一定的联盟链环境。使用 ANB 生成算法,确保了在第 $f+1$ 个节点过滤操作之后,所得到的 ANB 不被拜占庭节点篡改,确保了 Raft 共识阶段的非拜占庭网络环境。所有共识节点维护当前 ANB,并且仅与 ANB 中的节点通信,共识节点向公共节点发起同步块请求,从而更新整个网络的区块链。

3 系统实现与验证

3.1 实验环境

为了验证所提出高端装备生产数据管理方法的可行性,以某型号航空飞机生产过程为例,由分布在南京、苏州、泰州的 4 家制造商(A、B、C、D)

分别负责其机翼、尾翼、起落架以及动力装置的生产环节,如图6所示,对其供应链生产过程数据进行管理分析。

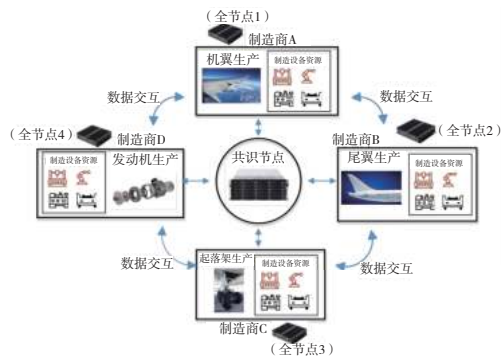


图6 某飞机协同生产参与方

本文基于 FISCO BCOS 来构建多节点数据管理联盟链网络。实验环境使用 5 台主机,每台主机为云端服务器。联盟链生产网络包括 4 个全节点和 1 个共识节点,对应 4 家制造商和总装企业。智能合约使用 Solidity 进行开发,服务端采用 Golang + Gin 框架实现。

3.2 实验验证

参与生产的企业首先需要生成身份证书,作为加入联盟链的凭证。然后,部署联盟链,启动区块链节点并安装链码,部署完成后在 web 端可以看到参与联盟链中企业的账号名称、所承担的角色等基本信息;同时总装企业可以对企业相关信息进行删除或修改等操作。生产任务管理界面如图7所示。



图7 生产任务的管理界面

生产数据由 IPFS 存储后,由智能合约将数据哈希上传至区块链,子任务信息则由总装企业在管理端创建并发布到联盟链,配套企业可看到所有任务信息。以尾翼生产任务为例,首先总装企业创建任务(图7(a)),并对任务进行分配(图7(b))。然后,可以查看尾翼生产子任务的详细信息(图7

(c)),同时对尾翼生产数据进行监控(图7(d))。

在制造企业实际生产过程中,总装企业可以通过质量数据管理页面看到实时生产质量数据信息。生产质量数据监控界面如图8所示。



图8 生产质量数据监控

在联盟链环境下,部分关键数据(如:飞机尾翼)需要由共识机制完成认证和区块写入,实现对关键数据的一致性存储。最后在联盟链管理界面如图9所示可以对尾翼生产时上链信息进行总体概览。通过点击左上角界面可以跳转到对应页面进而查看到参与企业节点、部署合约数量、产生区块数量和发起交易数量等详细信息。



图9 联盟链管理界面

4 结语

本文使用区块链技术及 IPFS 实现面向高端装备供应链的生产数据管理方法,通过数字身份验证方法支持制造企业灵活加入联盟链生产网络,然后采用 IPFS 协议实现关键、复杂数据的分流存储与共享,最后基于信用模型的 Raft 共识机制实现数据上链,提高系统安全性和数据可信性。实验证明:文中方法可保证企业数据交互时重要数据安全性和可信性。然而,目前提出的共识机制效率还不够高,多企业部署环境下系统性能不够强,这些都将在后续研究中进行进一步探索。

参考文献:

- [1] 丁文锋,万年,赵彪,等. 航空航天先进制造理论与技术研究现状及趋势[J]. 航空学报, 2025, 46(6):

- 收稿日期: 2023-11-10

- [4] 何琦. 红外制冷型探测器驱动及信息获取技术研究[D]. 上海:中国科学院大学(中国科学院上海技术物理研究所),2019.
- [5] 程起森. 轻小型非制冷短波红外相机信息获取关键技术研究[D]. 上海:中国科学院大学(中国科学院上海技术物理研究所),2018.
- [6] 陈晓屏. 微型低温制冷技术的现状和发展趋势[J]. 红外与激光工程,2008,37(1):45-49,92.
- [7] 孙闻. 制冷型红外探测器组件低温热特性研究[D]. 上海:中国科学院大学(中国科学院上海技术物理研究所),2017.
- [8] 孙辉艺,戴焕云. 某动车转向架构架静强度分析[J]. 机械制造与自动化,2023,52(5):96-99,103.
- [9] 陈俊林,王小坤,曾智江,等. 低温光学用杜瓦柔性外

- 收稿日期:2023-10-16