国际教育论坛
Journal of International Education Forum
第 6 卷◆第 11 期◆版本 1.0◆2024 年
文章类型：论文|刊号 ISSN: 2705-120X（O） EISSN: 2705-1196（P）

理论研究

区块链的工业物联网隐私保护协作学习系统探讨

刘璐
重庆工贸职业技术学院 408000

DOI:10.12238/jief.v6i11.11147

[摘 要] 随着信息技术的不断发展，现代社会当中人们最关注的问题就是信息的隐私与保护。区块链技术最早的提出是被用于比特币的交易当中，由于其独特的特性导致其具有较强的数据保护性以及透明性，因此被用于各个领域当中。区块链的工业物联网隐私保护协作学习系统就是采用了区块链技术的优势来确保工业物联网当中数据的隐私性和安全性，并加强了工业物联网的隐私保护协作学习系统的可行性。

[关键词] 区块链；工业物联网；隐私保护；协作学习系统

Discussion on the collaborative learning system of industrial Internet of Things privacy protection of blockchain

Liu Lu
Chongqing Vocational and Technical College of Industry and Trade 408000

[Abstract] With the continuous development of information technology, people's most concerned issue in modern society is the privacy and protection of information.Blockchain technology was first proposed to be used in bitcoin transactions.Due to its unique characteristics, it has strong data protection and transparency, so it is used in various fields.The industrial Internet of Things privacy protection collaborative learning system of blockchain adopts the advantages of blockchain technology to ensure the privacy and security of data in the industrial Internet of Things, and strengthens the feasibility of the privacy protection collaborative learning system of the industrial Internet of Things.

[Key words] Blockchain; Industrial Internet of Things; Privacy protection; collaborative learning system

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文|刊号 ISSN: 2705-120X（O） EISSN: 2705-1196（P）

由于现代工业物联网技术的不断发展，许多设备的数据信息正在被收集分析，因此数据隐私的保护问题成为了大众讨论的热点话题。因此如何在保护数据隐私的前提下进行高效的协作学习成为了现阶段工业物联网发展的重要难题。本文将分析讨论基于区块链的工业物联网隐私保护协作学习系统的设计，通过结合区块链技术为工业物联网隐私保护协作学习提供安全性进行分析讨论，希望可以为相关工作人员提供有效的思路。

一、区块链技术概述

区块链技术是一种常见的分布式账本技术，区块链技术最初被应用在比特币的交易当中，由于其可以通过数据块链的不断增长来记录交易信息，可以有效的确保数据的安全性以及透明性。由于区块链根据作用和特点可以分为三个部分：（1）公有链（2）联盟链（3）私有链。公有链顾名思义就是公共的、开放的区块，这部分区块是完全对外开放的，所有感兴趣的人都可以随时的参与进来。联盟链的主要作用就是管理，联盟链是由当前项目或行业的多个领头组织以及实体经营者共同管理的一个管理层。私有链就是针对个人单个团队和实体开放的控制管理层面。整个区块链技术包含了数据层、网络层、共识层和合约层等多个层级，每个层级具有自身的意义和作用，区块链技术通过采用共识机制来保障这些网络节点的所有数据都具有同步性和一致性，确保数据的安全可信性。在 2008 年区块链由一个神秘人中本聪提出，并在 2009 年的比特币市场交易中应用。随着时代的进步与发展，区块链由于其本身的独特特性：去中心化、不可篡改、透明开放、安全可信等特点[1]。常被人们应用到金融、供应链、物联网等多个商业领域当中，发挥着重要的作用。

二、区块链在工业物联网隐私保护中的作用

2.1 确保数据安全性与隐私性

由于区块链技术的特性，它能够有效的确保工业物联网设备之间相互传输的数据的安全性以及不可篡改性。实现这一特征的技术就是区块链技术当中的分布式存储以及密码学加密技术。这类技术可以有效的确保信息的安全性以及可靠性，由于工业物联网常被应用在无线接入训练数据集、大数据和 AI 计算等场景，因此对传输的数据信息的安全性以及可靠性要求较高，而在工业物联网设备上应用区块链技术就可以使得工业物联网产生的所有数据都存储在区块链当中，有效的避免了数据的丢失和数据被恶意修改泄漏等问题的发生，有效的确保了信息的完整性、安全性以及可靠性，进而保护用户的隐私安全。

2.2 提高设备与设备之间的信任协作

区块链当中还有一个重要的特性就是去中心化，去中心化是指去除中心机构或第三方信任，完全依靠分布式账本以及密码学算法来确保信息的安全性、不可篡改和透明性。将区块链技术应用在工业物联网当中可以使得物联网设备去除中心控制节点，使设备与设备之间建立信任，通过区块链设备与设备之间可以自动建立智能合约，并自动执行合约条件，实现真正意义上的设备之间智能化协作。由于设备之间可以自动执行信任合约，降低了人工的使用，这样可以有效的提高工业物联网的系统响应效率。

2.3 加强供应链管理

区块链技术不仅可以确保数据的完整性以及可靠性，同时区块链技术与供应链技术相结合还可以确保数据的透明性以及可追溯性。由于区块链技术的分布式存储可以记录大量数据，因此将区块链技术与供应链技术相结合，区块链技术可以记录所有的交易信息，同时还可以对交易进行实时的监控管理，提高了供应链信息的透明性。并且由于区块链的加密密码算法导致信息不可以被篡改，有效的解决了供应链数据当中可能会出现的虚假信息问题，进而确保供应链当中产品的质量以及真实性，并且由于区块链技术记录了所有的交易信息，还可以使得供应链信息具有可追溯性，从而加强了供应链管理。

三、基于区块链的工业物联网隐私保护协作学习系统设计

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.

文章类型：论文|刊号 ISSN: 2705-120X（O） EISSN: 2705-1196（P）

3.1 联邦学习系统架构概述

基于区块链的工业物联网隐私保护协作学习系统架构设计，该技术是通过区块链技术的特性确保数据信息的安全性，并提高工业物联网设备之间的协作学习能力。

本系统结构是由分组联邦学习（如图 1）、分割学习及差分隐私技术组成。联邦学习系统架构（如图 1）是基于区块链的工业物联网隐私保护协作学习系统基础系统框架。图 1 当中的分组联邦学习系统架构中客户组织具有多个传感器设备以及一个区块链全节点，中心处理是由中心服务器以及区块链全节点组成。确保数据的安全性的同时，由于区块链的分布式账本可以有效的对模型训练数据进行存储和溯源，因此确保了模型数据的一致性和安全[2]。同时智能合约与访问控制机制可以进一步的增强系统的可信度，为工业物联网的隐私保护与协作学习提供基础。

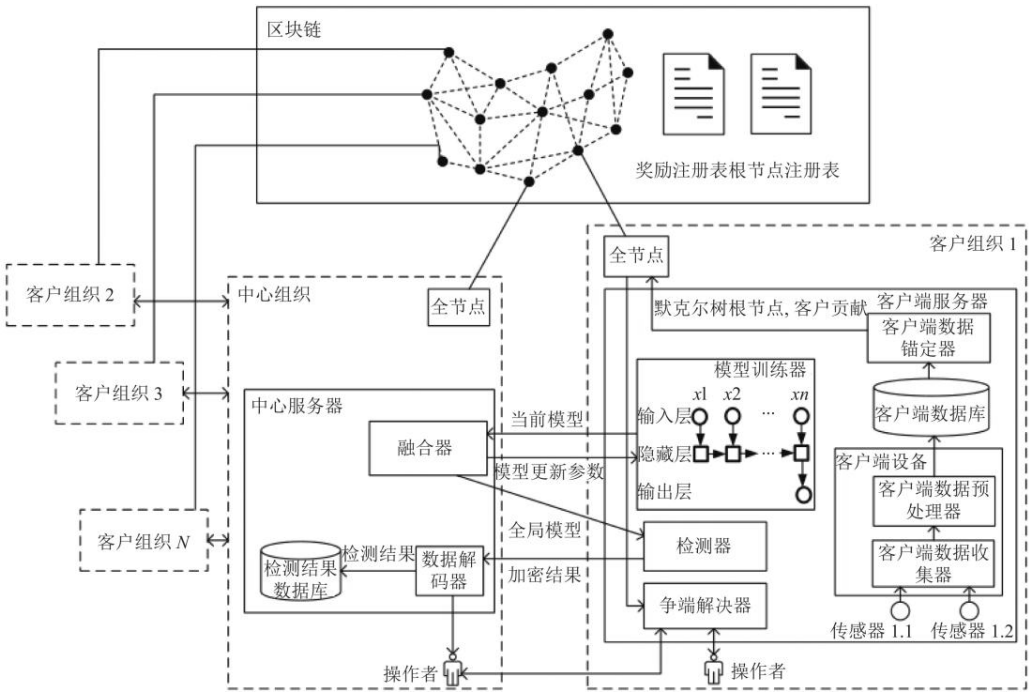

图 1　联邦学习系统架构

3.2 协作学习流程设计

协作学习流程设计是基于区块链的工业物联网隐私保护协作学习系统的重要环节。流程主要包含：数据预处理、模型训练、结果验证与模型更新等步骤。物联网设备通过对数据的采集之后，进行处理加密上传到云端，利用分组联邦学习与分割学习技术对所加密的数据进行模型训练训练完成之后的结果通过区块链网络进行验证和存储，最后将所验证的结果对模型进行更新来提高模型的准确性以及可行性。

结束语：

综上所述，本文通过对区块链技术的优势和特点进行分析与讨论，为研究基于区块链的工业物联网隐私保护协作学习系统设计。区块链技术在工业物联网隐私保护协作学习当中可以有效的为数据提供保护，通过分布式账本存储功能以及密码加密算法可以有效的确保数据的安全性以及透明性，为工业物联网隐私保护协作学习提供坚实的基础。

[参考文献]

[1]林峰斌 王灿 吴秋新 李涵 秦宇 龚钢军.基于区块链的工业物联网隐私保护协作学习系统[J].计算机应用研究，2024（2）.

[2]于秋雨，卢清华，张卫山.基于区块链的工业物联网联邦学习系统架构[J].计算机系统应用，2021，30（9）：69-76.

Copyright © This work is licensed under a Commons Attibution-Non Commercial 4.0 International License.