项目介绍

1. 项目概述

项目名称

《星联》——基于区块链的联邦学习系统。

项目背景

随着人工智能（AI）在医疗领域的应用逐渐增多，尤其是在医学影像分析（如 X 光片、CT 扫描等）中的应用，AI 在疾病检测和诊断方面取得了显著的成果。然而，医学数据尤其是患者的隐私数据极其敏感，传统的数据共享方式容易面临隐私泄露的风险。为了解决这一问题，联邦学习（Federated Learning, FL）应运而生，它允许不同的医疗机构在不交换数据的情况下进行联合训练，从而保护患者隐私。

然而，联邦学习的一个重要挑战在于如何保证数据的透明性、模型更新的可信性和参与方的公平性。针对这一问题，区块链技术为联邦学习提供了有效的解决方案，尤其是在确保数据溯源、模型更新的透明性和信任机制方面。本项目旨在通过结合 面向活跃账户的区块链和联邦学习，实现不同规模的医疗机构之间共享数据并共同训练模型，以提高 X 光片识别不同疾病的智能化水平。

项目目标

开发基于区块链的联邦学习系统架构，确保多个医疗机构在进行 X 光片数据训练时的隐私保护和数据安全。

设计面向活跃账户的区块链系统，通过智能合约和区块链技术确保医疗数据和模型更新的透明性、可追溯性。

设计一种支持自适应联邦学习任务的可信公平区块链架构，使用 PoTF（proof of trust and fair）机制，过将算力使用在联邦任务上，避免 了传统 PoW 的算力过度耗费问题。

实现一个公平、公正的模型训练过程，确保各医疗机构的贡献得到合理的评估和奖励。

提高 X 光片模型训练的效率与准确性，通过大规模数据共享来优化疾病检测能力。

2. 目标受众

各个医疗机构

3. 项目创新

面向活跃账户的区块链
基于自适应联邦学习任务的可信公平区块链框架
联邦学习与区块链的结合
活跃账户表

4. 框架设计

联邦学习任务与节点角色

设计了两个主要类型的节点：

1. 服务节点：
服务节点是上一轮训练中贡献度最高的节点，负责收集上传的模型参数，进行聚合操作，并计算节点的贡献度。
服务节点的职责是确保整个训练过程的高效性，同时计算并记录贡献度。
2. 普通节点：
普通节点从事本地训练，并将训练结果（模型更新的参数）上传给服务节点。
普通节点的贡献度根据其上传的模型质量和训练参与度进行评估。

通过将算力使用专注于联邦学习任务，避免了传统 PoW 机制中的算力过度消耗问题，确保区块链的高效性和节能性。

新的共识机制：PoTF

使用了全新的 PoTF 共识机制，该机制结合了 PoW（工作量证明）和 PoTF（信任与公平证明）。每个联邦学习任务开始时，系统会选择贡献度最高的节点作为服务节点。具体流程如下：

任务启动时：上次训练任务贡献度最高的节点会被指定为服务节点，负责收集并聚合各普通节点上传的模型更新参数。
贡献度计算：服务节点会对上传的模型进行评估，并计算普通节点的贡献度。贡献度可以基于上传的模型质量、参与训练的频率等因素进行评定。
共识切换：服务节点和普通节点通过贡献度来决定是否使用 PoW 或 PoTF 进行共识切换。通过这一方式，节省了计算资源，同时确保了区块链系统的安全性和效率。

这种共识机制的优势在于，它减少了不必要的算力消耗，并能够根据节点的贡献动态切换共识机制，确保整个联邦学习系统的效率和公平性。

联邦学习奖励分配机制

设计了一种基于区块链和贡献度计算的联邦学习奖励分配机制，用于保证各节点的奖励分配

公平，并鼓励节点积极参与到联邦学习任务中。具体机制如下：

奖励分配：
奖励基于节点的贡献度进行分配。贡献度较高的节点（如服务节点）会获得更多的奖励，而参与较少的节点（贡献度较低）会获得较少的奖励。

服务节点流动性：
为了避免服务节点被垄断，TFchain 引入了服务节点的流动性机制。每轮联邦任务结束后，贡献度最高的普通节点将有机会成为下一轮的服务节点。

作恶检测与惩罚：
通过投票机制，系统能够有效检测并排除作恶的服务节点。例如，上传恶意或不符合要求的模型会导致该节点被排除。
同时，系统会通过评估普通节点的贡献度，排除贡献度异常的节点，进一步提高奖励分配的公平性。

5. 项目优势

增强数据隐私与安全性

数据不离开本地：
传统的机器学习方法需要将数据上传到中央服务器进行处理，而联邦学习则使得数据始终保留在本地，仅上传模型参数（如梯度或权重）。这使得敏感数据如个人隐私数据、医疗数据等不需要共享，大大降低了数据泄露的风险。

区块链的加密性：
区块链提供了不可篡改的加密记录，通过加密技术确保每次上传的模型更新和数据使用记录都是安全的。这为参与方提供了额外的保障，避免了数据被恶意篡改或泄露。

提高系统的可信性和透明性

不可篡改的记录：
区块链能够记录每次模型更新的源头和历史记录，这使得每个参与方的贡献都可以追溯。参与者的行为被透明地记录下来，有助于防止不诚实的行为或作弊。

验证与信任：
区块链通过其去中心化的特性，消除了对单一信任方的依赖。所有的模型更新和数据使用都可以通过区块链验证，这增加了系统的可信度。

激励机制与公平性

贡献度计算与奖励机制：

在传统的联邦学习中，参与者往往没有足够的激励去积极参与训练过程，特别是在多方参与的情况下。区块链结合智能合约可以实现基于贡献度的奖励分配，确保每个参与方根据其模型贡献获得合理的回报。

去中心化的奖励分配：
区块链的智能合约可以自动化处理奖励分配、参与者信誉管理等问题，确保奖励和惩罚机制的公正性，从而提升参与者的积极性和公平性。

防止恶意行为与数据篡改

防止数据篡改：
区块链的不可篡改性使得每次模型的更新和数据使用都在区块链上有记录，任何篡改行为都能被追踪和发现。恶意的模型更新或篡改行为会被识别，并且可以在区块链上被公开审计。

作恶节点检测：
通过区块链的共识机制和投票机制，可以有效检测并剔除参与训练过程中的恶意节点或数据污染源，确保联邦学习的训练结果不被恶意干扰。

提高系统效率与去中心化

去中心化架构：
区块链的去中心化特点使得没有单一控制点的中央服务器，减少了对中央服务器的依赖，提高了系统的可靠性和抗攻击性。

智能合约的自动化执行：
区块链的智能合约可以自动执行合约条款，如奖励分配、作恶检测等操作，从而减少人工干预，提升系统效率。

可扩展性与跨域协助

可扩展的模型训练：区块链技术能够轻松扩展，允许大量的参与者加入联邦学习系统。在医疗、金融、智能制造等多个领域，参与方的数据分布可能不同，但区块链能提供一个透明的环境来促进跨域协作和数据共享。
跨机构协作：不同机构或不同国家的数据隐私和安全标准可能不同，通过区块链技术，联邦学习系统可以在保证隐私的前提下，促进跨机构甚至跨国的数据共享与联合训练。

动态调整与自适应机制

动态选择参与者：区块链和智能合约结合可以动态调整参与方的权重、贡献度，并根据需要选择参与训练的节点。通过自适应学习任务，系统能够自动评估各节点的性能和贡献，动态调整其在模型训练中的角色和权重，确保整体系统的高效性。

解决数据异质性问题

多方数据整合：在联邦学习中，各个参与方的数据分布可能不同（即数据是非独立同分布的，Non-IID）。区块链系统可以通过智能合约控制各方的数据使用和模型更新，从而在保证数据隐私的前提下，实现不同来源的数据有效整合，提升模型的泛化能力。

6. 评估标准

成功标准

用户注册人数超过 1000 人。

用户满意度调查平均分超过 4.5 分（满分 5 分）。

反馈机制

设置用户反馈通道，定期进行用户满意度调查。