《星联》项目概述：基于面向活跃账户的区块链的自适应联邦学习系统架构

---

1. 项目背景与目标

1.1 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。

1.2 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。

1.3 关于作品名称

联邦学习的将各个机构串联起来，其中活跃账户会每隔一段时间进行更新，体现在活跃账户表中就像星星一样明灭闪动，起名《星联》

---

2. 系统架构

2.1 系统概述

本系统架构将采用 **基于面向活跃账户的区块链** 技术来支撑医疗机构之间的协作，使用 **自适应的联邦学习** 对模型进行分布式训练。系统由以下几个主要组成部分构成：

- **客户端（医疗机构）**：每个医疗机构作为客户端，本地训练模型并上传更新。
- **区块链网络**：通过区块链记录数据的溯源信息、模型更新和信誉管理。
- **聚合服务器（可选）**：对来自各医疗机构的模型更新进行聚合，生成全局模型。预期采用PoTF机制，每次通过历史贡献度选择PoTF共识机制的服务节点。
- **智能合约**：管理各客户端的模型上传、验证、奖励与惩罚机制，确保训练过程的公平性。

2.2 系统流程

1. **本地数据训练**：
    - 各医疗机构（如医院、诊所）基于本地的 X 光片数据进行模型训练。
    - 模型训练过程中，数据保持本地，只有模型参数（如梯度、权重等）被上传。
2. **模型更新上传**：
    - 每个客户端将本地模型更新（如权重或梯度）上传到区块链，区块链负责记录上传信息的哈希值。
    - 上传时，客户端通过智能合约进行验证，确保模型更新符合要求并且没有恶意。

3. **区块链数据验证与记录**：

    - 区块链通过智能合约验证上传的模型更新是否有效，并确保更新的来源是可信的。
    - 区块链将每次模型更新的哈希值、时间戳及相关信息记录下来，保证其不可篡改。

4. **选择聚合服务器**

    - 在每次训练任务开始时, 根据历史贡 献度选择 PoTF 共识机制的服务节点. 服务节点负责 收集训练后的参数并进行聚合，然后打包包含每个 普通节点训练参数和普通交易的区块，在完成每次 的训练任务后，服务节点会在本地计算每个普通节点的贡献度，在本次训练周期 Epoch 的最后一个区块 中，服务节点会上传计算的所有参与方本次学习任 务的最终贡献度并且分配奖励. 普通节点会作为联邦学习的参与方，使用私有数据集 训练本地模型并上传训练后的模型参数，并根据贡献领取相应的奖励。

5. **全局模型聚合**：

    - 通过去中心化的方式，聚合各医疗机构上传的模型更新，生成全局模型。
    - 聚合方法（如加权平均、FedAvg）基于各客户端的贡献权重进行处理。

6. **奖励与惩罚机制**：

    - 智能合约根据每个医疗机构的贡献和信誉评分，对诚实贡献的医疗机构进行奖励，对恶意更新的机构进行惩罚。

7. **活跃账户的更新**

    - 根据每个医疗机构的贡献度与活跃程度，更新活跃账户表。

8. **回馈与再训练**：

    - 聚合后的全局模型反馈给各客户端，客户端继续在本地进行训练和更新，形成一个闭环。

创新点总结

3.面向活跃账户的区块链

面向活跃账户的区块链是一个基于区块链的账户管理模型，旨在通过集中关注系统中“活跃”账户的行为和状态来提高系统效率、降低存储成本，并增强系统的安全性和可扩展性。在这个设计中，**活跃账户**是指在某一时间段内有频繁操作、贡献或参与的账户。与传统区块链系统中所有账户都被平等对待不同，面向活跃账户的区块链系统会根据账户的活跃度（例如交易频率、贡献度、行为模式等）进行优先处理。

这种设计特别适用于像 **联邦学习**、**医疗数据共享**、**IoT 设备管理** 等场景，其中账户的活动频率差异较大，且需要针对活跃账户提供更高效的查询、更新和管理策略。

3.1 面向活跃账户区块链的特点与优势

3.1.1 高效的账户管理

- **活跃账户表**：区块链系统维护一个“活跃账户表”，用于快速访问当前活跃账户的信息。活跃账户通过定义的标准（如交易频率、参与度、行为）来确定。只有活跃账户才能进行某些特定的操作，如上传模型、参与数据共享、进行交易等。
- **存储优化**：避免在每次操作时都需要扫描整个账户池，只有活跃账户会被记录和查询，从而优化存储空间和查询速度。

3.1.2 动态调整活跃账户状态

- **账户活跃性管理**：系统根据账户的活动情况动态调整其状态。长期没有活动的账户会被标记为“非活跃”账户，并从活跃账户表中移除。反之，如果某账户恢复活跃，系统会重新将其加入到活跃账户表中。
- **灵活的活动标准**：活跃账户的标准可以根据业务需求动态调整。例如，联邦学习系统中，只有参与过一定次数模型训练并上传模型的账户才能被视为活跃。

3.1.3 高效的智能合约执行

- **智能合约优化**：针对活跃账户，区块链可以执行更复杂、更多样化的智能合约，确保只有经过验证的活跃账户能够执行重要的操作，如数据上传、模型更新、奖励分配等。
- **自动化审核与验证**：系统可以通过智能合约自动审核活跃账户的贡献度并奖励高贡献的账户，确保系统透明和公正。

3.2. 系统设计与架构

3.2.1 活跃账户表与区块链集成

- 活跃账户表（Active Account Table）

  ：

  - 用于存储当前活跃账户的索引和基本信息。账户状态、贡献度、参与度等指标将决定其是否被视为“活跃账户”。
  - 活跃账户表通过哈希表或数据库索引优化查询时间，确保能够在 **O(1)** 的时间复杂度下访问和更新活跃账户。

- 区块链的角色

  ：

  - **区块链存储**：区块链仍然负责记录所有账户的基本信息、交易历史以及重要的模型更新和数据共享行为。每个活跃账户的操作都会在区块链中生成不可篡改的记录。
  - **智能合约**：智能合约负责根据活跃账户的活动情况进行自动化管理、奖励分配和行为验证。智能合约还可以在活跃账户变更状态时，自动更新活跃账户表。

3.2.2 活跃账户的生命周期管理

- **账户注册**：每个新账户注册时，区块链会将其信息存储到链上，并在初期为账户分配一个临时状态（如“待验证”）。只有通过验证的账户才会被加入到活跃账户表。
- **活动监控与状态更新**：
  - 系统根据账户的行为（如数据上传、模型更新、参与训练次数等）对其活跃性进行评分。
  - 如果账户的行为超过了预定阈值，该账户将被视为“活跃”并加入活跃账户表。
- **非活跃账户的处理**：
  - **时间阈值**：长期未参与活动的账户将被标记为“非活跃”。
  - **强制清除**：非活跃账户的历史数据可以从活跃账户表中删除，但仍可通过区块链查询其基本信息。

3.3. 活跃账户管理示例

假设我们有几个医疗机构参与 X 光片数据的联邦学习训练：

1. **账户注册**：
   - 医疗机构 A 注册账户，并提交基本信息到区块链。此时账户处于“待验证”状态。
2. **账户活跃性评估**：
   - 医疗机构 A 开始上传数据并训练本地模型，系统根据上传频率、模型质量等评估其活跃度。
   - 如果医疗机构 A 上传的模型质量高，并且参与了多次模型训练，它将被标记为“活跃账户”，并加入活跃账户表。
3. **奖励机制**：
   - 智能合约会根据医疗机构 A 的贡献度分配奖励（如代币、积分等）。
4. **非活跃账户**：
   - 如果医疗机构 B 长时间没有参与训练，系统会根据预设的时间阈值将其标记为“非活跃”账户，并将其从活跃账户表中移除。

4.基于自适应联邦学习任务的可信公平区块链框架

在本项目中，我们将引入一种 **支持自适应联邦学习任务的可信公平区块链框架**，来解决 **算力过度耗费问题** 和 **联邦学习缺乏有效公平激励** 的问题。通过引入新的 **共识机制 PoTF**（Proof of Trust and Fairness），优化了传统的区块链系统，并设计了合理的贡献度评估与激励机制，有效提升了整个系统的效率和安全性。

4.1. 支持自适应联邦学习任务的可信公平区块链框架

通过将 **服务节点** 和 **普通节点** 组成一个联邦系统，来完成所有联邦学习任务的训练与验证。解决了传统 **Proof of Work (PoW)** 机制中算力过度消耗的问题，同时采用 **PoTF** 机制动态切换共识方式，根据参与者的贡献度来调节共识方式，从而提高区块链系统的效率和安全性。

4.2. 框架设计

4.2.1 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。

4.2.2 新的共识机制：PoTF（Proof of Trust and Fairness）

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。

4.2.3 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。

4.3. 优势

4.3.1 提高算力效率

通过 **PoTF** 共识机制， 能够减少区块链系统的算力消耗，避免传统 PoW 中的无效算力浪费。系统根据每个节点的贡献动态调整共识机制，节省了大量的计算资源。

4.3.2 提供公平的激励机制

引入了基于 **贡献度计算** 的奖励分配机制，确保了联邦学习任务中各节点的贡献得到公平的回报。这不仅鼓励更多的参与，还能够有效减少恶意行为。

5.联邦学习与区块链的结合

基于区块链的联邦学习框架，通过结合区块链的去中心化、透明性、不可篡改性等优势，能够有效解决传统联邦学习面临的数据隐私、安全性、信任和激励机制等问题。区块链技术不仅为参与方提供了一个可信的训练环境，还能够通过智能合约确保公平的激励机制，提升系统的透明性与安全性。随着技术的进一步发展，基于区块链的联邦学习将在医疗、金融、智能制造等多个领域得到广泛应用，推动跨领域、跨机构的数据共享与智能协作。

5.1. 基于区块链的联邦学习的优势

结合区块链技术后，联邦学习可以享受到以下几个重要的优势：

5.1.1 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。

5.1.2 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。

5.1.3 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。

5.1.4 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。

5.1.5 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。

5.1.6 可扩展性与跨域协作

- **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。

5.1.7 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。

5.1.8 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。