计 算 机 研 究 与 发 展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202330286
60(11): 2567−2582, 2023

基于区块链辅助的半中心化联邦学习框架

施宏建[1,2] 马汝辉[1,2] 张卫山[3] 管海兵[1,2]

[1](上海交通大学电子信息与电气工程学院 上海 200240)

[2](上海市可扩展计算与系统重点实验室(上海交通大学) 上海 200240)

[3](中国石油大学(华东)青岛软件学院、计算机科学与技术学院 山东青岛 266580)

(shhjwu5@sjtu.edu.cn)

Blockchain-Assisted Semi-Centralized Federated Learning Framework

Shi Hongjian[1,2], Ma Ruhui[1,2], Zhang Weishan[3], and Guan Haibing[1,2]

[1](*School of Electronic Information and Electrical Engineering*, *Shanghai Jiao Tong University*, *Shanghai* 200240)

[2](*Shanghai Key Laboratory of Scalable Computing and Systems*, *Shanghai* 200240)

[3](*Qingdao Institute of Software*, *College of Computer Science and Technology*, *China University of Petroleum* (*East China*), *Qingdao*, *Shandong* 266580)

Abstract With the development of network technology, building a trusted new-generation information management system is necessary. Blockchain technology provides a decentralized, transparent, and tamper-proof distributed base. On the other hand, with the development of artificial intelligence technology, data islands have been a common issue in the field of network data computing. The distrust among developers has made it difficult to jointly utilize all parties' data for collaborative training. Although federated learning provides data privacy protection, there are still hidden dangers in server-side security. The traditional methods replace the server in the federated learning framework with a blockchain system to provide a tamperproof global model database. However, this approach does not utilize all available network connections in the Internet of things scenario and lacks a block structure design for federated learning tasks. We propose a blockchain-assisted semi-centralized federated learning framework. Starting from the requirements of the Internet of things scenario, our approach constructs a semi-centralized Internet of things structure and utilizes all trusted network connections to support federated learning tasks. At the same time, our approach constructs a tamper-proof model database for untrusted and remote clients through blockchain technology. Compared with traditional blockchain federated learning frameworks, our approach has a smaller communication overhead and better universality. The framework includes two major designs. The semi-centralized federated learning framework reduces the communication overhead brought by aggregation through trusted connections between clients, and stores client models through blockchain for aggregation on remote or untrusted clients to improve the universality and performance of local models. The design of blockchain blocks for federated learning tasks can support the needs of underlying federated learning training. Experiments have shown that this framework has an accuracy improvement at least 8% compared with traditional federated learning algorithms on multiple datasets, and significantly reduces the

收稿日期: 2023-04-03; **修回日期**: 2023-06-13

基金项目: 无锡物联网创新促进中心物联网专项课题(2022SP-T13-C); 中国航天科技集团有限公司第八研究院产学研合作基金资助项目(USCAST2022-17)

This work was supported by Internet of Things Special Subject Program from Wuxi IoT Innovation Promotion Center (2022SP-T13-C) and the Industry-university-research Cooperation Funding Project from the Eighth Research Institute in China Aerospace Science and Technology Corporation (USCAST2022-17).

通信作者: 马汝辉(ruhuima@sjtu.edu.cn)

communication overhead caused by the waiting aggregation process between clients, providing guidance for the deployment of blockchain federated learning systems in practical scenarios.

Key words Internet of things; blockchain system; federated learning; semi-centralized structure; model aggregation

摘 要 随着网络技术的发展,如何构建可信任的新一代信息管理系统成为了必要需求,区块链技术提供了去中心化、透明、不可篡改的可信分布式底座.随着人工智能技术的发展,网络数据计算领域出现了数据孤岛问题,各开发者之间的不信任导致难以联合利用各方数据进行协同训练,联邦学习虽然提供了数据隐私性保障,但是服务器端安全性仍存在隐患.传统方法通过将联邦学习框架中的服务器端替换为区块链系统以提供不可篡改的全局模型数据库,但是这种方式并未利用物联网场景中所有可用网络连接,并缺少了针对联邦学习任务的区块结构设计.提出了基于区块链辅助的半中心化联邦学习框架,从物联网场景需求出发,构建了半中心化的物联网场景,利用了所有可信的网络连接以支撑联邦学习任务,同时通过区块链技术为不可信、距离远的客户端之间构建了不可篡改的模型库,相比传统区块链联邦学习框架有更小的通信开销和更好的普适性.所提框架包含两大设计,半中心化的联邦学习框架通过客户端之间的可信连接减少聚合所带来的通信开销,并通过区块链存储客户端模型以便于距离较远或者相互不可信的客户端进行聚合;设计了针对联邦学习任务的区块链区块,使区块链能够支持底层联邦学习训练的需求.实验证明所提框架在多个数据集上相比传统联邦学习算法有至少8%的准确率提升,并大幅度减少了客户端之间相互等待带来的通信开销,为实际场景下的区块链联邦学习系统部署提供了指导.

关键词 物联网;区块链系统;联邦学习;半中心化架构;模型聚合

中图法分类号 TP39

随着网络技术[1-2]的发展,网络用户之间的交互变得十分普遍和重要.而在社会、经济和工程等各大领域数字化转型的过程中,网络信任问题成为了主要矛盾.构建可信任的新一代信息管理系统[3]成为了迫切的需求.此种信息管理系统可以提高社会运行效率,降低社会协作成本,对经济发展和工程技术开发均有十分重大的意义,也是推动我国技术进步并在国际竞争中形成核心竞争力的关键.而近些年在网络信任领域兴起的区块链技术[4-6]则是现阶段发展的主要方向之一.

区块链(blockchain)系统是集合分布式网络、加密技术、智能合约等多种技术的新型数据存储系统,能够记录和验证交易并保护数据的安全性,是基于信任的数据管理基础设施.在区块链系统中,每个参与者都可以共同验证交易,并且整体交易信息被保存在一个不断增长的链式结构中,称为区块链数据库,每个链上的区块都包含有一定数量的交易信息.区块链的去中心化使其不需要可信第三方控制交易;透明性保证所有参与者都可以共同查看和验证交易;不可篡改性则确保了交易信息不会被修改或删除.区块链系统涉及数据存储、事务处理、智能合约执行、安全隐私保护等核心技术,但现今大部分区块链研究仍集中于经济金融等数据存储领域,并未与目前最急需发展的数据计算领域融合.与数据存储相似,在网络数据计算[7-8]中也需要考虑网络用户之间的信任问题.

另一方面,随着人工智能技术[9]的发展,开发者对数据量和数据多样性的需求逐步增加,但是单一开发者并不能收集到高质量高数量的研究数据,进而导致网络数据计算领域出现了数据孤岛问题.用户需和他人联合训练人工智能算法,这就涉及到了隐私性问题.在这种需求下,联邦学习[10-13]应运而生.

联邦学习(federated learning, FL)是近几年发展起来的新兴机器学习技术,可以在去中心化的数据存储下,让多个设备及用户共同学习和构建机器学习或深度学习模型.在联邦学习中,每个设备或用户都被视作一个客户端,其拥有自己的本地数据集,且并不需要将这些本地数据在网络中进行直接传输或发送到服务器端.联邦学习架构为人工智能算法提供了联合学习的可能,打破了数据孤岛,使得研究人员能够在保障数据隐私性的情况下构建出适用于大部分用户的神经网络模型.

但实际场景下,可信的服务器端极难获取,相对应的,能够提供去中心化、透明、不可篡改的数据存储框架的区块链系统正好能够弥补联邦学习架构这一方面的需求,进而区块链联邦学习[14-17]成为了网络数据计算领域的新型应用.过去几年中,有若干在区块链联邦学习框架领域开展的研究,主要集中于联

邦学习架构的客户端选择[18-19]、聚合权重[20-21]、本地训练调整[20,22]、隐私保护[23-29]、安全防护[24,30-31]、模型压缩[32]设计，以及区块链系统的共识机制[18-19,30]、区块结构[30,33-34]、委员会选取[21,34]、激励机制[23,25-26,29]设计上，另一方面，也有在两方结合的层次化结构[22,32,35]或者异步聚合[19,20,36-37]进行探索的.

但是文献 [18−37] 所述的主要问题在于底层联邦学习架构没有完全发掘区块链系统的潜力，顶层区块链系统也没有为联邦学习架构提供完整的支撑. 具体来说，现有的联邦学习区块链框架并未利用实际物联网场景中所有可用的网络连接，带来了较大的通信开销，在异构资源场景下限制了整体的训练效率；同时缺少在区块链与联邦学习结合的场景下较为完整合理的区块结构设计，不能够保障用户的知识产权和维护需求.

基于上述需求，本文设计了基于区块链辅助的半中心化联邦学习框架，从实际场景出发，通过利用不同种的网络连接辅助训练，并通过区块链系统为联邦学习架构提供完整的分布式训练支持，以减少区块链联邦学习框架的通信开销并提高其普适性. 框架主要包含两大设计，其一为半中心化的联邦学习架构设计，主要通过将聚合任务放到客户端上，并利用客户端之间的可信连接减少聚合所用时间开销，同时通过区块链辅助对不可信客户端的模型进行集中聚合，保障本地模型泛用性和性能；其二为区块链系统中的联邦区块设计，主要通过对上传区块、下载区块、评分区块的设计，使区块链能够支持底层联邦学习训练的需求. 本文的主要贡献有 4 个方面:

1) 提出了基于区块链辅助的半中心化联邦学习架构，能够在物联网场景下对分散的数据提供可信的协同训练环境，提高了人工智能任务的准确率和训练效率，为区块链联邦学习算法设计提供了指导；

2) 对半中心化架构进行了建模和公式化表述，基于物联网场景给出了更加实际、更加全面的分布式架构，并在其基础上设计了联邦学习算法，利用损失函数和延迟轮次进行权重设计，提高算法准确率和效率；

3) 针对联邦学习任务的区块链区块进行了结构设计，包括模型下载对应的下载区块、模型上传对应的上传区块和模型评分对应的评分区块，为联邦学习任务提供了区块链系统支持，便于系统部署；

4) 通过实验证明了所提框架在 2 个数据集上相比传统联邦学习算法提高了至少 8% 的准确率，并大幅度提高了设备计算时间比例，进而提高了训练效率.

1 相关工作

本节主要介绍区块链系统和联邦学习架构的相关工作.

1.1 传统联邦学习

传统联邦学习的研究有很多[38-52]. FedAvg[38] 算法是所有联邦学习架构中最基础也是最早的算法，其利用服务器端的模型聚合方法在含有不同数据分布的客户端之间进行参数交互，同时通过提高本地训练轮次数来减少通信开销提高收敛性. FedProx[39] 算法在 FedAvg 算法基础上，往损失函数中加入了近端项（proximal term）来应对联邦环境中的系统异构性问题. MOON[40] 算法则是利用全局模型中区分度更高的特征表征来指导本地训练，通过在损失函数中加入对比学习项来减少 2 个特征表征之间的区别，以此来进一步提高联邦学习算法的效果. FedDyn[41] 从损失函数的收敛性入手，通过在损失函数上添加一个一阶泰勒展开项，使其从理论上可以证明本地损失函数收敛性和全局损失函数收敛性是可以统一的，保证了聚合操作的合理性和有效性.

很多区块链联邦学习算法都是基于传统联邦学习架构的，主要将原本的服务器替换为区块链，负责聚合等任务，然后对应在通信效率、安全性等方面进行了优化. 文献 [35] 采用了层次化的区块链联邦学习框架，上层负责管理全局模型，下层负责调度底层资源更新本地模型，以使本地训练去中心化，可以有效地减少通信延时和提高通信效率. Biscotti[24] 重点关注了中心化区块链联邦学习框架中的安全隐私性，其在传统框架中加入了 Multi-Krum, VRF, PoF, Shamir 秘密共享和差分隐私等多个安全防护技术. 文献 [22] 在传统区块链联邦学习中通过 A2C 算法确定各节点本地训练参数. 文献 [27] 和 FedTwin[23] 类似地运用了基于 GAN 的差分隐私防护机制，其定性地分析了区块链联邦学习框架在延迟和解决数据孤岛问题上的有效性. 文献 [28] 则是运用差分隐私保护了客户端数据隐私，但还利用了零知识证明对客户端上传模型的有效性和安全性进行了验证. BFCL[32] 在中心化区块链联邦学习框架中引入了 Top K 的模型压缩机制，从理论和实验上证明了其性能的提升. SAGIN[31] 在空天地架构中利用区块链联邦强化学习优化了任务卸载问题，对空天地架构的拓扑优化问题进行建

模优化，并提供了基于准确度的拜占庭防御机制.

但是传统联邦学习中出现的一大问题是其并不适用于物联网或边缘计算中. 在这 2 种场景下，数据中的统计异构性较强，也就是说各个客户端上的标签分布数量、分布比例不同，导致用同一个全局模型无法在所有客户上都有较高的准确度，使得模型泛用性和有效性降低.

1.2 个性化联邦学习

为了解决统计异构性所带来的特征偏移的问题，个性化联邦学习成为了一大研究方向. 个性化联邦学习会在不同客户端上维护不同模型以在各数据集上得到更高的准确率，主要包含部分聚合、个性化训练和独立聚合 3 种模式.

部分聚合只聚合模型中的全局层，而不聚合个性化层，以此满足个性化要求. FedBN[42] 与 FedAvg 类似，只是将批次化归一层(batch normalization)留在本地，不参与聚合，以此来应对特征偏移问题. FedPer[43] 则是将模型分成了数据端的全局层和标签端的个性化层，并只对全局层进行聚合，这样可以得到更高的训练准确度. FedRep[44] 则是在 FedPer 的目的和算法的基础上，进一步分析了本地训练阶段的效果和合理性，进而提出了将全局层和个性化层分开训练的算法来提升效果. FedBABU[45] 也使用了类似 FedPer 和 FedRep 的神经网络切分方式，并且在训练中只聚合全局层，但是与 FedPer 和 FedRep 两种算法不同的是，FedBABU 在训练阶段并不会训练个性化层，而是在训练结束后会对个性化层进行微调.

个性化训练通过运用全局模型和本地模型信息辅助本地训练，而并不直接用全局模型或上一轮本地模型进行训练，主要以调整损失函数及聚合权重为主. FedPHP[47] 的关注点在于聚合后的全局模型在本地数据集上的表现其实不一定比上一轮本地模型要好，于是其在全局模型本地训练的基础上，将上一轮次的本地模型信息，也用于监督本轮次的本地模型训练. Ditto[48] 则关注的是联邦学习算法的公平性和鲁棒性，更是提出了统一的性能指标来表征这 2 个特性，并且运用求解器优化这 2 个指标. APPLE[51] 则是在上述相关性聚合的基础上，适应性地调整了全局损失函数和本地损失函数之间的比例，使算法能够更好地收敛到一个较高的准确度. APFL[46] 提出了混合权重的概念，即将上一轮全局模型也纳入考量之后生成的聚合权重. 其在分析了本地模型和全局模型的泛化能力的基础上对混合权重进行了优化，这个混合权重最终被用于混合本地模型参数和全局模型参数以得到效果更好的模型.

独立模型并不通过聚合的方式维护全局模型，而是直接维护各个客户端的模型来达到个性化的目的. FedFomo[49] 对每一个客户端都维护了单独的服务端模型，每个客户端会根据其他服务端模型计算相关性权重矩阵，然后根据相关性权重矩阵聚合相关的服务端模型，这种方法提高了模型的个性化能力和本地模型效果. FedAMP[50] 则采用了类似 FedFomo 的方式，进一步给出了凸优化和非凸优化下的理论证明.

部分聚合和个性化训练的问题在于虽然它们在部分任务上能够适当增加各个客户端在本地数据集上的模型准确率，但是其泛用性较差，面对新类型数据无法有效判断其所属类别；独立模型的问题在于由于维护对象的变更，网络中需要传输的数据量变大，导致通信开销大幅度提升. 故而现有个性化模型较难在实际场景中进行部署运行.

1.3 异步联邦学习

物联网及边缘计算中的联邦学习还存在系统异构性的问题，由于不同设备计算能力和网络连接情况的不同，会导致其单次训练时长不同，而传统联邦学习采用同步聚合的方式，客户端之间相互等待会带来极大的通信开销，解决此问题最常用的方法是异步聚合. FedAsync[52] 提出了异步联邦学习架构，传统联邦学习架构会对上传的模型进行同步聚合，而 FedAsync 则是在每一个本地模型传到服务器端时都会单独地将此模型和当前全局模型进行聚合以减少通信开销.

也有部分文献尝试运用区块链优化异步联邦学习. BAFL[20] 从理论层面求解了最优聚合权重，提高了算法的收敛性和最终的准确率；另一方面 BAFL 对本地训练过程进行了适应性调整，进一步提高了训练效率. 文献 [19] 类似文献 [18]，利用深度强化学习做客户端选择. BLADE-FL[36] 利用了去中心化网络，会在网络中进行广播操作，通信开销较大，但给出了较为详尽的理论分析和实验证明其方法的收敛性.

但是异步联邦学习的问题在于其中传输的模型参数或模型更新实时性不强，低实时性模型会破坏全局模型或各客户端模型的效果.

1.4 区块链联邦学习

关于区块链联邦学习框架的研究在近几年发展较快[18-28,30-36]. 在共识机制上，文献 [18] 利用容器技术为联邦学习提供后端支撑，同时利用 A3C 算法做了客户端选择，提高了算法的收敛性和效果. 而其在区块链端共识机制的设计也提高了区块链系统的效率.

文献 [33] 对 Proof of Work 进行了理论上的优化，降低了区块链联邦学习算法的延迟. 同时其对区块的生成过程和过程性能都做了分析和优化，提高了区块生成过程的效率.

在委员会机制和区块结构设计上，BFLC[34] 使用了基础的中心化区块链联邦学习框架，设计了委员会机制和区块结构来辅助模型存储和模型下载. BytoChain[30] 给出了针对联邦学习训练系统的区块设计，并定性地分析了各种联邦学习中的攻击方式，为后续防御方式的设计给出了指导方向. FGFL[21] 在区块链委员会利用计算的客户端可信度进行选取，在模型聚合的时候利用计算的客户端贡献度确定聚合权重，通过 2 个客户端指标的结合提升系统收敛性和效果.

在奖励机制上，FedTwin[23] 在原有的中心化区块链联邦学习框架的基础上，用对抗生成网络（generative adversarial network, GAN）进行了隐私保护，同时根据各个模型的效果提供了奖励机制. 另一方面其引入了全局模型回滚机制，防止因服务器错误导致的训练失效. PF-PoFL[25] 从任务层面对区块链进行了设计，在区块链中加入了任务队列，通过下发任务接受模型参数，然后通过验证者（validator）对上传的模型参数进行评分，并用此评分设计激励机制，还附带着提供了差分隐私方案. 文献 [26] 特别考虑了区块链联邦学习框架对多模态 Transformer 任务的训练效果，同时加入了激励机制和差分隐私技术.

当前区块链联邦学习框架的相关工作重点关注联邦学习或者区块链本身的优化和改进. 本文将重点放在了区块链系统和联邦学习架构的协同设计上，从区块链系统设计上支持联邦学习全流程训练，从联邦学习架构设计上合理利用区块链透明和不可篡改的特性. 同时针对系统异构性和通信效率进行了优化，以提高整体框架的训练效率，并能够适应不同的运行场景.

2 系统模型

本节主要介绍联邦学习架构及其公式化表达，并且将区块链的概念引入联邦学习中.

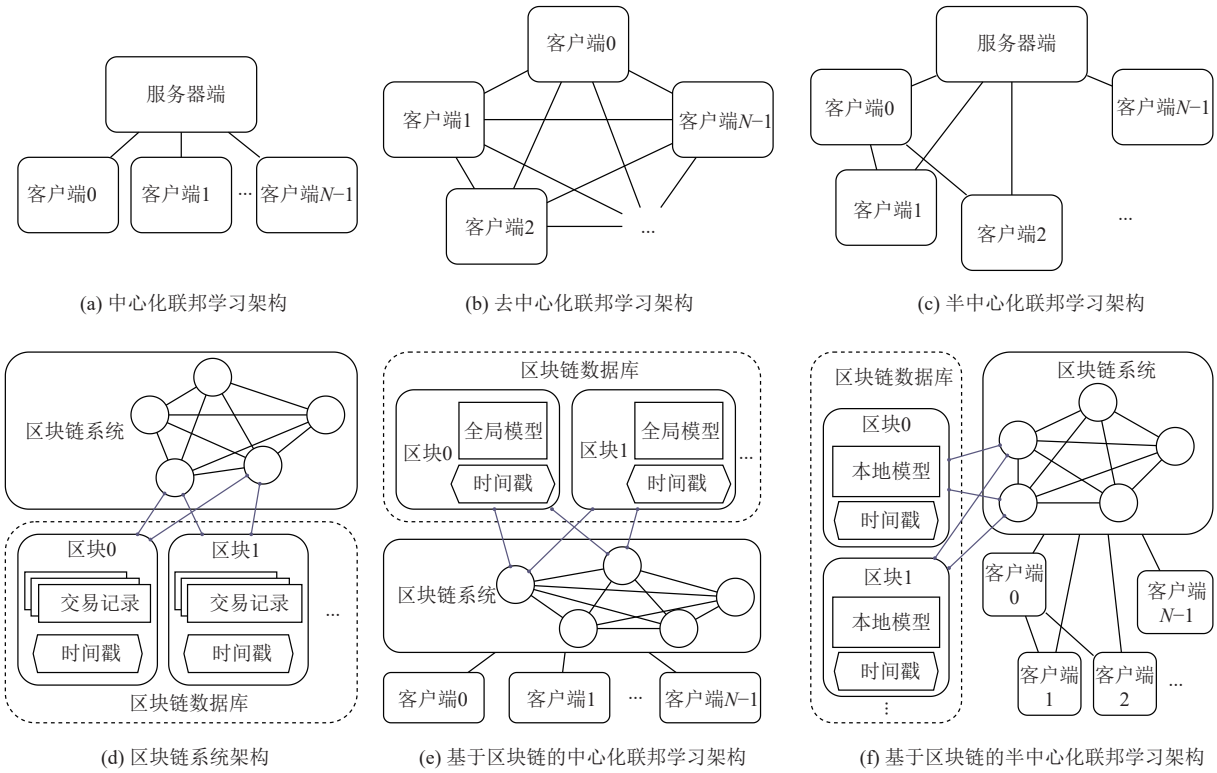
2.1 基本框架

联邦学习的核心框架是将机器学习算法推送到数据源头，即客户端上，并在客户端本地对算法进行训练. 传统中心化联邦学习架构遵循服务器-客户模型，如图 1(a)所示，客户端负责在本地数据集上训练各自的本地模型，最终目的是通过聚合各本地模型，在服务器端上得到适用于大部分本地数据集的全局模型. 而去中心化联邦学习架构则抛弃了传统的服务器-客户模型，而是转用纯分布式客户端架构，如图 1(b)所示，客户端既负责在本地数据集上训练各自的本地模型，又需要根据接收到的其他客户端的模型进行聚合得到新一轮的本地模型. 更加贴合实际的则是半中心化的联邦学习架构，如图 1(c)所示，这种架构在服务器-客户模型的基础上也考虑了客户与客户之间的连接，在去中心化架构的基础上引入服务器对不可信或者距离较远的客户端之间进行模型交互，使得架构既能保持一个较少的通信开销，又能解决客户端之间的数据孤岛问题.

区块链的核心架构是一个去中心化的区块链系统和链状的数据库，如图 1(d)所示. 链状的数据库用于存储实际的区块信息，每个数据库包含一些数据、1 个时间戳和前一个区块的哈希值. 每个区块的数据可以是任何形式的信息，例如交易记录、合约代码等；时间戳记录了该区块被创建的时间；而前一个区块的哈希值则将当前区块与之前的所有区块链连接在一起，形成一个不可篡改的链式结构. 而区块链系统中的每个节点都可以维护一个副本，任何修改都需要得到网络中多数节点的确认才能生效，这使得区块链具有高安全性和可靠性，因为攻击者需要修改网络上大多数节点的数据才能破坏整个系统.

在图 1(a)~(d)的基础上，衍生出了中心化的区块链联邦学习框架，如图 1(e)所示. 该学习框架遵循了中心化联邦学习的架构，但是将联邦学习中原有的服务器端替换成了一个区块链系统，使其能够拥有去中心化、透明和不可篡改的特性. 区块链的功能和原有的服务器相似，负责收集本地模型，并负责聚合、存储、下发全局模型.

本文考虑了实际场景中，尤其基于 5G/6G 技术的物联网场景下，客户端之间是相互联通的，所以本质上是一个纯分布式的架构. 但是另一方面，基于可信度和网络延迟的考虑，并不是所有连接都是可用的，客户端会因为不信任对方或者对方在直连范围之外导致双方不能实现点对点的数据传输. 在这种场景下，本文提出了半中心化的区块链联邦学习框架，如图 1(f)所示. 将去中心化架构和中心化架构结合，利用去中心化架构提升中心化架构的传输效率，减少区块链端的计算量；利用中心化架构的高可信度和连通性，提高客户端准确度，更好地解决数据孤岛问题.



(a) 中心化联邦学习架构 (b) 去中心化联邦学习架构 (c) 半中心化联邦学习架构

(d) 区块链系统架构 (e) 基于区块链的中心化联邦学习架构 (f) 基于区块链的半中心化联邦学习架构

Fig. 1 Federated learning structures, blockchain structures, and blockchain-based federated learning frameworks

图 1 联邦学习架构、区块链架构及区块链联邦学习框架

2.2 区块链联邦学习问题表述

传统区块链联邦学习框架基本遵循传统联邦学习的训练流程，唯一的区别是将服务器端的全局模型存储和聚合过程放在了区块链上进行，其基本流程有 4 个：1)在第t个全局训练轮次中，区块链会下发全局模型θ^{t-1}至各个客户端$C_0, C_1, \cdots, C_{N-1}$以初始化客户端本地模型$\theta_0^{t-1}, \theta_1^{t-1}, \cdots, \theta_{N-1}^{t-1}$. 2)如式(1)所示，各个客户端运用其本地数据集$D_0, D_1, \cdots, D_{N-1}$对各本地模型进行训练得到新的本地模型$\tilde{\theta}_0^{t-1}, \tilde{\theta}_1^{t-1}, \cdots, \tilde{\theta}_{N-1}^{t-1}$.

$$\tilde{\theta}_i^{t-1} = \theta_i^{t-1} - \alpha \nabla L(\theta_i^{t-1} | D_i). \tag{1}$$

3)各客户端将其新的本地模型上传至区块链. 4)区块链通过式(2)对上传的本地模型进行聚合得到下一轮的全局模型θ^t. 联邦学习会重复上述步骤直至轮次达到一定数量或是全局模型收敛，其中N_i表示客户端C_i上本地数据集D_i的样本数，w_i^t表示第t轮中C_i对应的聚合权重.

$$\theta^t = \sum_{i=0}^{N-1} w_i^t \tilde{\theta}_i^{t-1}. \tag{2}$$

其中最常用的聚合权重是根据各客户端上的样本量决定的，如式(3)所示.

$$w_i^t = \frac{N_i}{\sum_{i=0}^{N-1} N_i}. \tag{3}$$

而针对半中心化的区块链联邦学习框架，由于其聚合步骤并不在区块链系统中进行，而是各个客户端各自进行聚合，在客户端C_i的聚合过程中包含 3 种模型：第一种模型是本地模型$\tilde{\theta}_i^{t-1}$，第二种模型来源于C_i的可信邻居客户端集C_i^{neigh}中，第三种模型来源于区块链系统中存储的剩余客户端的模型. 在这种半中心化区块链联邦学习框架下，各客户端的聚合公式就变成了式(4).

$$\theta_i^t = w_i^t \tilde{\theta}_i^{t-1} + \sum_{C_j \in C_i^{\text{neigh}}} w_j^t \tilde{\theta}_j^{t_j} + \sum_{C_k \notin C_i^{\text{neigh}}} w_k^t \tilde{\theta}_k^{t_k}. \tag{4}$$

2.3 符号及其表述

为了方便理解和引用，本文将文中所用的符号及其表述解释整合在表 1 中.

3 基于区块链辅助的半中心化联邦学习框架

本节详细介绍本文所设计的基于区块链辅助的半中心化联邦学习框架及其模块设计. 本文提出了半中心化的区块链联邦学习框架，通过去中心化的高效点对点连接和中心化的区块链可信机制，统一实现了可信高效的联邦学习架构. 整体模块设计如图 2 所示，分别在联邦学习部分和区块链系统部分进行了设计和构造.

Table 1 The Used Notations and Their Descriptions in Our Paper

表 1 本文所用符号及其表述

符号	符号表述	符号	符号表述	符号	符号表述
N	客户端数量	C_i	第 i 个客户端	T	最大训练轮次
D_i	C_i上的本地数据集	N_i	D_i中的样本数	α	本地学习率
θ^t	第t轮中的全局模型	θ_i^t	第t轮中C_i上的本地模型	$\tilde{\theta}_i^t$	第t轮中C_i上训练后的本地模型
$L(\theta_i^t \mid D_i)$	θ_i^t在D_i上的损失函数	w_i^t	第t轮中θ_i^t的聚合权重	C_i^{neigh}	C_i的邻居可信客户端集合
t_i	客户端C_i当前所处的轮次	$w_{1,i}^t$	本地第t轮时，从C_i接收到的模型的准确率所决定的聚合权重	$w_{2,i}^t$	本地第t轮时，从C_i接收到的模型的延迟轮次所决定的聚合权重
τ_i^t	C_i在第t轮的总用时	$\tau_{i,\text{cal}}^t$	C_i在第t轮的计算用时	$\tau_{i,\text{wait}}^t$	C_i在第t轮的等待用时

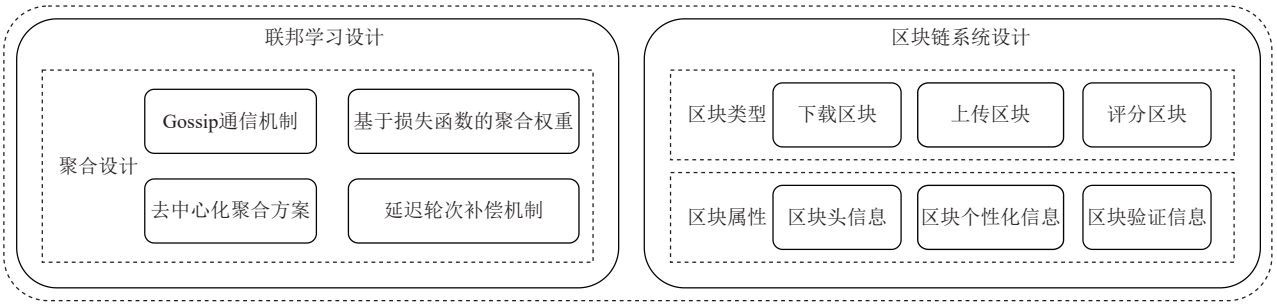


Fig. 2 Our proposed blockchain-assisted semi-centralized federated learning framework

图 2 本文提出的基于区块链辅助的半中心化联邦学习框架

在联邦学习设计部分，主要包含聚合流程的设计. 聚合组件中基于 Gossip 的通信机制可以在去中心化的网络中利用 P2P 的连接提高模型传输和聚合效率；基于去中心化的聚合模式使得聚合操作可以在各个客户端上单独进行，使得区块链上的计算量大大减小，提高了整体的训练效率；基于损失函数的聚合权重计算方案可以通过模型效果决定聚合比例，进而提高模型的准确率；基于延迟的聚合权重补偿方案则根据不同本地模型所在轮次调整模型聚合时的权重，防止过时参数影响聚合后模型的准确度.

在区块链系统设计部分，主要集中于支持半中心化联邦学习训练的区块设计部分. 从区块类型来看，主要包含上传区块、下载区块和评分区块；从区块属性来看，主要包含了区块头信息、区块个性化信息和区块验证信息的设计.

3.1 半中心化联邦学习组件设计

本文提出了半中心化的联邦学习架构，其采用去中心化的点对点通信模式提高整体训练效率，同时采用中心化的区块链辅助解决数据孤岛问题，防止模型收敛到局部最优. 在联邦学习聚合算法方面，本文主要对聚合通信模式和聚合权重计算两方面进行了设计研究. 在传统中心化联邦学习的场景下，往往采用的是同步聚合的方式，这种方式会使得计算快的客户端需要等待计算慢的客户端计算完成之后才能进行聚合，导致通信开销较大；另一方面，为了保障可信性而将服务器端替换成区块链系统之后，会导致聚合操作所花费的时间变长，这就降低了整体训练效率. 而在去中心化联邦学习的场景下，纯分布式的通信模式会导致距离较远的客户端模型参数会在很长时间之后才能够传输到当前客户端，降低了客户端模型泛化能力和准确度；另一方面，由于可信度考量，并非所有客户端之间都是连通的，这就导致了如果采用完全去中心化通信模式，部分客户端所聚合的模型无法表征所有数据信息，限制了模型的准确度和泛化能力. 因此我们将中心化和去中心化联邦学习架构组合，提出了更加符合现实场景的半中心化联邦学习架构.

在聚合通信模式下，本文主要采取了去中心化的聚合方案和基于 Gossip 的通信机制. 去中心化的聚合方案将聚合过程放在了客户端上，每个客户端都独自对其本地模型、从邻居可信客户端接收到的本地模型和从区块链系统中获取的其他客户端的可信模型 3 组模型进行聚合，得到新的本地模型. 同时，为了减少模型参数传输时数据交换请求带来的传输延时，模型采用 Gossip 通信机制在去中心化架构中进行传输. Gossip 机制在模型本地训练完后会向邻居可信客户端广播新的本地模型参数，而邻居客户端会重复这一操作直到所有连通客户端均接收到此模

型,这种机制可以有效减少通信等待时长,提高通信效率.

特别地,本文考虑了客户端之间数据分布的不一致性,又称统计异构性.统计异构性是由于客户端所处环境不同,故其所能获取到的数据种类和数据分布不同,如果将所有模型直接根据样本数量进行加权平均,并不能很好地在本地客户端上得到一个适用于本地数据集的模型.故而需要根据各个客户端之间的模型表现进行加权,提高聚合后新一轮本地模型在对应数据集上的表现.基于此,本文设计了基于损失函数的聚合权重调整方案,根据接收和下载到的模型对在本地数据集上推理所得到的损失函数进行加权,对应权重如式(5)所示.需要说明的是,考虑到在整个客户端训练集上进行推理耗时较长,本文所提出的方法采用单次推理的方式,即从客户端数据集中随机采样一个批次的数据进行推理,此次推理得到的损失函数被近似作为整个数据集上的损失函数进行评价.

$$w_{1,j}^t=\frac{1}{L(\theta_j^{t_j}|D_i)},w_{1,k}^t=\frac{1}{L(\theta_k^{t_k}|D_i)}. \tag{5}$$

同时本文也考虑到了客户端之间设备计算能力的不一致性,又称系统异构性.系统异构性是由于客户端计算硬件及计算环境不同,故其本地训练所用时长均不相同,虽然通过去中心化的聚合方案和基于 Gossip 的通信机制将客户端之间的等待时间降到了最低,但是由于各客户端训练速度不同,在聚合的时候会出现模型所处训练轮次不同,也就是在式(4)中会出现式(6)的情况.

$$t-1\neq t_j,t-1\neq t_k,t_k\neq t_j. \tag{6}$$

这种情况下,如果直接聚合会导致过时的模型参数影响本地模型的准确度,故而需要对过时的模型参数进行一定程度上的补偿和调整以提高聚合后新一轮本地模型的准确度.基于此,本文设计了基于延迟轮次的过时模型补偿方案,根据接收和下载到的模型和当前模型所处轮次的差值对权重进行调整,对应权重如式(7)所示.

$$w_{2,j}^t=\begin{cases}e^{(t_j-t)}, & t_j<t\\ 1, & t_j\geqslant t\end{cases},w_{2,k}^t=\begin{cases}e^{(t_k-t)}, & t_k<t\\ 1, & t_k\geqslant t\end{cases}. \tag{7}$$

基于上述聚合权重的调整和补偿措施设计,本文所提出的区块链辅助的半中心化联邦学习框架中聚合阶段的总体聚合公式如式(8)所示.

$$\theta_i^t=\frac{w_i^tw_{1,i}^t}{w^t}\tilde{\theta}_i^{t-1}+\sum_{C_j\in C_i^{\text{neigh}}}\frac{w_j^tw_{1,j}^tw_{2,j}^t}{w^t}\tilde{\theta}_j^{t_j}+\sum_{C_k\notin C_i^{\text{neigh}}}\frac{w_k^tw_{1,k}^tw_{2,k}^t}{w^t}\tilde{\theta}_k^{t_k}. \tag{8}$$

式(8)中聚合权重包含了归一化流程,其中归一化参数w^t满足式(9).

$$w^t=w_i^tw_{1,i}^t+\sum_{C_j\in C_i^{\text{neigh}}}w_j^tw_{1,j}^tw_{2,j}^t+\sum_{C_k\notin C_i^{\text{neigh}}}w_k^tw_{1,k}^tw_{2,k}^t. \tag{9}$$

在上述组件设计动机和设计方案下,本文所提出的基于区块链辅助的半中心化联邦学习框架整体训练流程如算法 1 所示.需要说明的是,所有客户端本地模型都是由初始模型θ^0进行初始化的,而所有客户端训练过程都是并行进行的.

算法 1. 基于区块链辅助的半中心化联邦学习框架中客户端C_i在第t轮的训练过程.

输入:本地模型θ_i^{t-1}、本地数据集D_i和邻居可信客户端C_i^{neigh},学习率α,损失函数$L(\theta|D)$;

输出:客户端新一轮本地模型θ_i^t.

① 通过式(1)更新本地模型θ_i^{t-1}得到$\tilde{\theta}_i^{t-1}$;

② 通过 Gossip 将$\tilde{\theta}_i^{t-1}$广播至C_i^{neigh}中的客户端;

③ 对$\forall C_j\in C_i^{\text{neigh}}$,接收其本地模型$\theta_j^{t_j}$;对$\forall C_k\notin(C_i^{\text{neigh}}\cup\{C_i\})$,从区块链系统中下载其最新上传的模型$\theta_k^{t_k}$;

④ 区块链系统根据③构造下载区块并上链;

⑤ C_i对每个接收和下载的模型均进行评估,确认或计算各相关客户端样本量N_j(或N_k)、模型损失值L_j(或L_k),以及所在轮次t_j(或t_k);

⑥ 将计算出的下载模型的损失值L_k和对应模型编号上传至区块链系统;

⑦ 区块链系统根据⑥构造评分区块并上链;

⑧ 通过式(8)聚合本地模型θ_i^{t-1}、接收到的模型$\theta_j^{t_j}$和下载到的模型$\theta_k^{t_k}$,以得到新一轮本地模型θ_i^t;

⑨ 将聚合得到的新一轮本地模型θ_i^t上传至区块链系统;

⑩ 区块链系统根据⑨构造上传区块并上链.

3.2 区块链辅助组件设计

3.1 节介绍了基于区块链辅助的半中心化联邦学习框架的训练流程,其中一共存在着 3 个上链步骤,算法 1 中的④⑦⑩三个步骤分别对应客户端从区块链系统下载模型所生成的下载区块、客户端对下载模型进行评估所生成的评分区块以及客户端上传聚合后的本地模型所生成的上传区块.这 3 种区块设计要能够支持半中心化联邦学习的训练流程,提供联邦学习训练所需的必要信息.总体区块结构设计如图 4 所示,下面会详细描述这 3 种区块的组成结构.

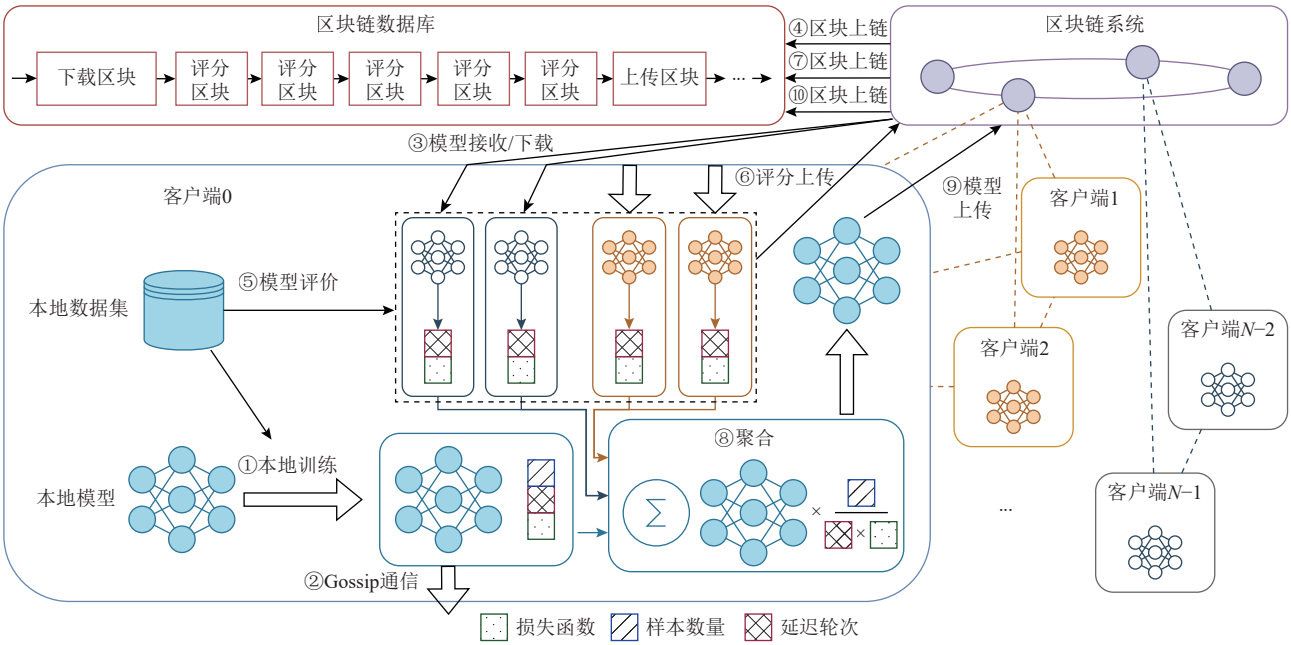


Fig. 3 The training procedure of the semi-centralized federated learning framework

图 3 半中心化联邦学习框架的训练流程

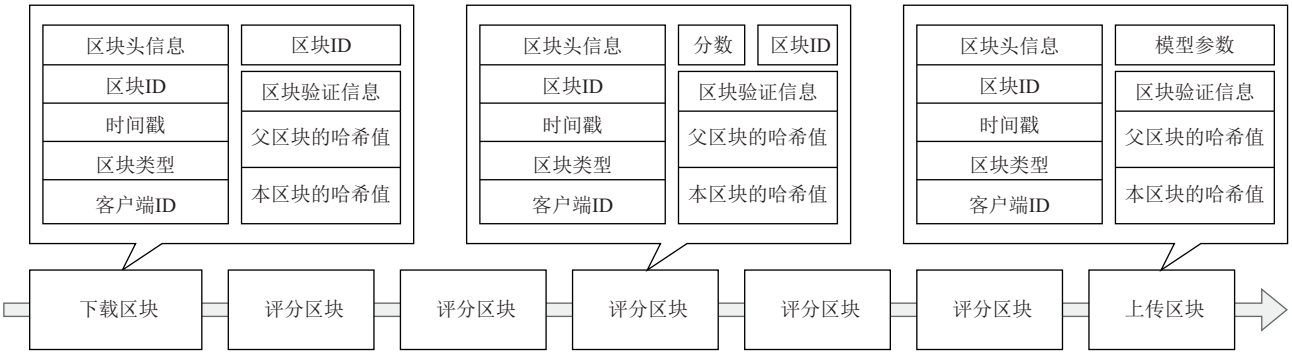


Fig. 4 The design of the block structures in the blockchain system

图 4 区块链系统中的区块结构设计

所有区块设计都包含主要三大部分内容：区块头信息、区块个性化信息和区块验证信息.

1)区块头信息. 区块头主要记录了区块本身的一些用于区块链的历史记录和追溯所需要的信息. 区块头中统一的信息有 3 个：区块 ID 赋予了当前区块一个唯一的标识，使得其他区块能够对当前区块进行区分和引用；区块时间戳记录了当前区块上链的时间，方便后续对于异常情况的追溯和时间线构建；区块类型则是记录了当前区块是下载区块、评分区块和上传区块的哪一种，便于后续对区块个性化信息的处理. 客户端 ID 记录了当前区块所包含的操作涉及的客户端识别信息，便于追溯操作者.

2)区块个性化信息. 主要包含了用于联邦学习训练过程所需的信息和属性. 此部分和区块类型强相关，后续会根据区块类型做详细介绍.

3)区块验证信息. 主要是区块链本身用于其内容准确性验证的信息，通过记录父区块的哈希值和本区块的哈希值，可以保障攻击者没有办法通过修改单一区块破坏整个区块链，保障了区块链的不可篡改性.

在上述区块设计的基础上，针对不同功能的区块进行了一定的个性化设计以支撑区块的指定功能.

下载区块负责记录某客户端从区块链系统中下载的某一个模型，以此可以对此模型上传者的贡献度进行更新，或者根据其知识产权提供奖励. 另一方面如果系统中某客户端本地模型出现了不安全或是错误，可以通过追溯下载记录确定是否是区块链系统中存储的模型导致的，这样可以保障系统的可追溯性. 在区块头信息中，下载区块的客户端 ID 会记录是哪一个客户端进行的下载操作，便于追溯；而在

区块个性化信息中，会记录此次下载操作是下载的哪一个上传区块中的模型参数，记录的内容是模型参数所在的区块 ID. 通过记录区块 ID 而非模型参数可以有效减少此区块占用的存储空间.

评分区块负责记录某客户端对区块链系统中某个模型参数的评价，主要是记录对用模型在此客户端上推理所得的损失函数值，使得系统能够对某一模型参数的质量和可信度进行跟踪和记录. 这样可以根据其质量给予对应模型参数上传的客户端以激励，以推动客户端进行高质量训练. 在区块头信息中，评分区块的客户端 ID 会记录是哪一个客户端进行的评分操作，便于追溯；而在区块个性化信息中，会记录此次评分操作是评价的哪一个上传区块中的模型参数，记录的内容是模型参数所在的区块 ID 和对应的评分. 本文主要对评分区块进行了设计，暂未对评分区块的后续利用进行展开.

上传区块负责存储某客户端进行本地聚合后得到的新一轮本地模型，主要是用于为其他客户端提供可信的模型参数用于聚合，以提高各客户端本地模型的准确性和泛化性. 在区块头信息中，上传区块的客户端 ID 会记录是哪一个客户端上传的模型参数，便于追溯；而在区块个性化信息中，会记录此次上传的全部模型参数.

4 实验与结果

在本节中，我们在 4.1 节提供了实验设置，4.2 节对本文提出的基于区块链辅助的半中心化联邦学习框架进行了测试.

4.1 实验设置

本节提供了本文中后续实验部分的硬件设备、数据集介绍、数据分布、神经网络模型选取、超参数设定、基准算法和测试指标等.

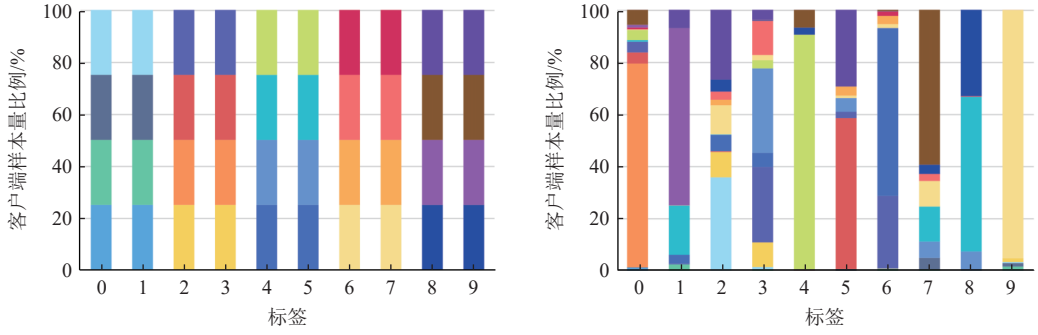
1）硬件设备. 实验是在 Intel® Xeon® Gold 6140 CPU 和一个 8 节点 GeForce RTX 2080 Ti GPU 的硬件环境下进行的.

2）数据集介绍. 实验在 FMNIST[53] 和 CIFAR10[54] 数据集上均进行了测试. FMNIST 数据集涵盖了来自 10 个类别的 7 万个不同商品的正面图片，其训练集包含 6 万个商品，测试集包含 1 万个商品，每个商品为 28×28 的灰度图像. CIFAR10 数据集涵盖了来自 10 个类别的 6 万张普适物体的图像，其训练集包含 5 万个物体，测试集包含 1 万个物体，每个物体为 32×32 的彩色 RGB 图像.

3）数据分布. 实验在病态独立同分布（Pathelogical, PAT）和基于 Dirichlet 的非独立同分布（DIR）上均进行了对比，如图 5 所示. PAT 中每个客户端只包含 2 种标签，并且在拥有同样标签的客户端中随机分配数据；而 DIR 则根据数据标签，基于 Dirichlet 分布对数据进行了分配. 图 5 中不同颜色代表了不同客户端的数据集上含有对应标签的比例.

4）神经网络模型选取. 实验在 FMNIST 数据集和 CIFAR10 数据集上均采用了双层卷积神经网络，如图 6 所示. 2 个数据集上的模型结构相同，因输入输出不同，故模型中参数数量略有不同.

5）超参数设定. 实验中对于场景设定有若干超参数设置. 其中客户端数量设置为 20；除非特殊说明，50% 的客户端计算速度相比另外的 50% 慢了一倍，即存在系统异构性；每个实验结果均经过 5 次评估并取统计学结果. 对于联邦学习训练过程也有若干超参数设置. 其中批次大小设置为 10，即同一个批次内包含 10 条数据；设置本地学习率 α=0.005；本地训练次数设置为 1，即客户端只在本地数据集上进行 1 次遍历并进行梯度下降操作；最大训练轮次被设置



(a) FMNIST数据集下的PAT分布　(b) FMNIST数据集下的DIR分布

Fig. 5 The PAT and DIR distribution of FMNIST dataset for different clients

图 5 不同客户端在 FMNIST 数据集的 PAT 分布和 DIR 分布

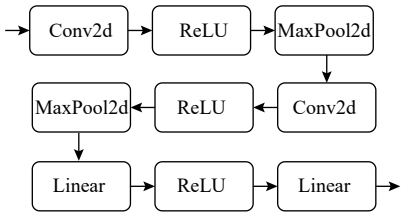


Fig. 6 Structure of the neural network model used in the experiment

图 6 实验中运用的神经网络模型结构

为 100, 即所有客户端在聚合 100 次后停止训练; 聚合比例为 100%, 即在中心化联邦学习算法中所有客户端均参与每一轮聚合. 其他未提及的超参数均按各算法在原论文中的设置.

6) 基准算法. 本文主要构建了基于区块链辅助的半中心化联邦学习框架, 在训练准确率和效率上进行了优化, 故将其主要和传统联邦学习算法[38-39, 42, 45, 47]、个性化联邦学习算法[43-44, 46, 48−51]和异步联邦学习算法[52]做了对比.

7) 测试指标. 本文主要考虑所提出的基于区块链辅助的半中心化联邦学习框架的准确率和效率, 故采用了测试集准确率和测试集 AUC 作为准确率指标, 这两者值越高代表模型准确率越高; 采用了平均训练时间和设备计算时长比例作为效率指标, 其中平均训练时间越低代表计算效率越高, 设备计算时长比例越高, 代表设备之间训练时间差距越小, 设备利用率越高. 设备计算时长比例由式(10)计算得出.

$$UtilRatio=\frac{\sum_{i=0}^{N-1}\sum_{t=0}^{T}\tau_{i,\mathrm{cal}}^{t}}{\sum_{i=0}^{N-1}\sum_{t=0}^{T}\tau_{i}^{t}}\times 100\%. \tag{10}$$

其中 $\tau_{i,\mathrm{cal}}^{t}$ 是 C_i 在第 t 轮的计算时长, τ_i^t 是 C_i 在第 t 轮的总用时, 由于通信开销主要来源于客户端之间的相互等待时间而非模型传输时间, 故而 $\tau_i^t=\tau_{i,\mathrm{cal}}^t+\tau_{i,\mathrm{wait}}^t$, 其中 $\tau_{i,\mathrm{wait}}^t$ 是客户端等待聚合的用时.

4.2 实验和结果

在本节中, 我们对比了基于区块链辅助的半中心化联邦学习框架与传统联邦学习算法的准确率和效率, 在 FMNIST 数据集的 DIR 分布下的结果如表 2 所示, 在 CIFAR10 数据集的 DIR 分布下的结果如表 3 所示. 从表 2 和表 3 可以看出, 本文所提出的方案在准确率和效率上存在着若干特性. 从测试准确率和测试 AUC 上可以看出, 本文所提出的方法比传统联邦学习算法和异步联邦学习算法效果要好得多, 主要是由于在非独立同分布的数据分布下, 采用统一的全局模型作为最终的模型是不合适的. 对各个客户端本地模型进行加权得到统一的全局模型会破坏在各个客户端上学习到的个性化信息, 这也是个性化联邦学习算法拟解决的问题. 故而在准确率上, 个性化联邦学习算法均得到了较好的效果, 而我们算法的准确率比个性化联邦学习的算法准确率低了 8%~13%, 这主要是由于本文所提出的框架并未在算法层面进行个性化设计. 但是本文框架可用性较好, 后续会在本文框架基础上对个性化算法的嵌入进行进一步研究以提高框架准确率.

从平均训练时间和设备计算时长比例可以看出, 本文所提框架所用平均训练时间和传统联邦学习算法相当, 主要是因为并未引入大量额外计算, 所以本地训练和传统联邦学习算法计算量相似. 唯一引入的额外计算是对接收和下载到的模型进行评价, 但是由于本文的评价方式是采用随机采样的一个批次数据的损失函数作为对应模型的评价指标, 并未对整个数据集进行遍历, 故而相比本地训练, 本文评价过程并未引入过多的计算开销. 同时可以看出大部分个性化联邦学习算法由于在客户端进行了额外的计算, 其平均训练时间均相比传统联邦学习算法长. 另一方面, 从设备计算时长比例可以看出, 在 50% 的客户端训练时间较长时, 传统联邦学习算法和个性化联邦学习算法的比例均不到 50%, 而本文框架算法和异步联邦学习算法 FedAsync 均有 100% 的设备计算时长比例. FedAsync 有此等效果主要是因为其并没有聚合过程, 而只是在每一个本地模型上传到服务器后单独进行聚合, 并没有客户端之间相互等待的时间; 而本文所提框架的聚合过程是分布式的, 虽然依旧是在各个客户端上进行同步聚合, 但是由于不限制只对当前轮次的模型进行聚合, 故而不需要等待其他客户端训练完成来进行聚合, 所以也不存在等待时间.

特别地, 本文对框架设计的聚合权重进行了消融实验, 主要针对基于损失函数的聚合权重设计(loss)和基于延迟轮次的过时参数补偿方案(delay)这 2 种权重. Ours−delay 表示从我们的方法中删除基于损失函数的聚合权重设计. 可以看出, 基于损失函数的聚合权重设计在任何情况下均能提高框架的最终准确率, 这是因为这种方法可以有效避免统计异构性带来的最优模型参数的区别, 使得各个客户端可以去选取更适合本地数据集的模型参数进行聚合; 而在存在系统异构性的情况下, 基于延迟轮次的过时参数补偿方案可以进一步提升最终准确率, 这是

Table 2 Results of Our Framework and Other Federated Learning Frameworks Under FMNIST-DIR

表 2 本文框架与其他联邦学习框架在 FMNIST-DIR 下的结果

算法框架	测试准确率	测试 AUC	平均训练时间/s	设备计算时长比例/%
FedAvg	0.799 5±0.002 4	0.966 6±0.024 5	1.388 7±0.060 0	35.64±3.77
FedAvg + loss	0.805 1±0.005 4	0.969 9±0.021 2	1.740 6±0.079 5	30.93±3.22
FedProx	0.799 3±0.002 2	0.966 6±0.024 6	1.598 9±0.075 2	36.27 ±3.39
FedBN	0.799 4±0.002 3	0.966 6±0.024 5	1.616 3±0.039 5	33.21±1.74
FedPer	0.973 5±0.000 1	0.996 7±0.005 7	1.458 4±0.086 4	26.43±1.84
FedRep	0.974 3±0.000 5	0.997 4±0.006 1	2.232 5±0.102 6	38.73±4.17
FedBABU	0.768 5±0.007 0	0.995 0±0.009 0	1.431 3±0.073 3	35.48±3.38
APFL	0.972 0±0.000 2	0.997 6±0.007 7	3.685 5±0.162 1	29.11±1.21
FedPHP	0.091 9±0.018 5	0.507 2±0.231 3	3.922 1±0.346 2	36.44±1.55
Ditto	0.971 4±0.000 5	0.998 6±0.010 3	3.545 0±0.287 0	30.81±1.29
FedFomo	0.971 9±0.000 4	0.997 1±0.017 9	2.013 9±0.278 8	38.14±1.94
FedAMP	0.972 0±0.000 6	0.997 1±0.011 4	1.682 6±0.054 6	29.34±2.52
APPLE	0.963 8±0.000 6	0.990 7±0.020 6	30.172 1±13.138 5	36.25±4.49
FedAsync	0.835 2±0.037 2	0.948 2±0.187 0	1.426 0±0.074 9	100.00±0.00
Ours	0.890 1±0.009 2	0.976 0±0.130 3	1.839 6±0.021 3	100.00±0.00
Ours − delay	0.874 9±0.007 0	0.971 4±0.129 1	1.646 0±0.051 7	100.00±0.00
Ours − delay −loss	0.659 5±0.077 2	0.899 4±0.215 3	1.476 6±0.041 7	100.00±0.00

Table 3 Results of Our Framework and Other Federated Learning Frameworks Under CIFAR10-DIR

表 3 本文框架与其他联邦学习框架在 CIFAR10-DIR 下的结果

算法框架	测试准确率	测试 AUC	平均训练时间/s	设备计算时长比例/%
FedAvg	0.430 1±0.002 1	0.856 1±0.054 9	1.265 9±0.047 4	38.91±2.24
FedAvg + loss	0.459 5±0.007 6	0.861 0±0.056 3	1.130 5±0.067 2	40.96±5.34
FedProx	0.430 2±0.002 0	0.856 2±0.054 9	1.466 1±0.064 5	38.39±3.94
FedBN	0.430 2±0.002 0	0.856 3±0.054 8	1.228 1±0.055 1	35.13±2.84
FedPer	0.892 5±0.002 0	0.983 3±0.020 5	1.136 0±0.029 5	40.44±3.78
FedRep	0.899 7±0.001 9	0.984 6±0.019 5	1.797 7±0.086 3	36.00±3.34
FedBABU	0.875 7±0.001 4	0.983 8±0.020 9	1.193 3±0.037 5	40.64±4.58
APFL	0.888 4±0.001 9	0.983 7±0.023 0	2.846 3±0.086 9	46.31±3.31
FedPHP	0.107 5±0.012 4	0.507 9±0.199 1	3.447 4±0.191 9	37.39±2.10
Ditto	0.885 7±0.001 2	0.987 8±0.020 9	2.753 9±0.170 7	38.90±1.99
FedFomo	0.881 8±0.001 0	0.982 4±0.023 6	1.467 5±0.186 9	46.03±3.48
FedAMP	0.887 9±0.002 0	0.983 4±0.023 0	1.276 0±0.072 9	37.19±3.04
APPLE	0.880 7±0.108 1	0.980 3±0.024 1	25.164 6±5.619 9	38.39±1.33
FedAsync	0.466 8±0.133 8	0.835 4±0.242 2	1.540 2±0.070 4	100.00±0.00
Ours	0.766 0±0.008 7	0.945 3±0.135 6	1.273 2±0.027 0	100.00±0.00
Ours − delay	0.758 1±0.013 9	0.932 8±0.154 9	1.222 4±0.075 5	100.00±0.00
Ours − delay −loss	0.488 6±0.070 8	0.812 0±0.230 9	1.417 1±0.032 5	100.00±0.00

因为这种设计可以有效避免过时参数影响聚合模型.

另外，本文对系统异构性的存在与否也进行了测试，如表 4 所示. 从表 4 可以看出，针对测试准确度和测试 AUC，系统异构性不影响传统联邦学习算法和个性化联邦学习算法，也不影响其训练准确度，故最终的结果均没有太大变化. 但对于异步联邦学习和本文提出的算法而言，系统异构性会造成一定的负面影响，但本文方法可以有效减少此影响. 在平均

Table 4 Results of Our Framework and Other Federated Learning Frameworks Under CIFAR10-DIR Without Straggler

表 4 本文框架与其他联邦学习框架在没有系统异构性时 CIFAR10-DIR 下的结果

算法框架	测试准确率	测试 AUC	平均训练时间/s	设备计算时长比例/%
FedAvg	0.430 1±0.002 1	0.856 1±0.054 8	0.614 6±0.031 3	49.09±3.27
FedAvg + loss	0.459 9±0.007 9	0.861 0±0.056 3	0.890 5±0.064 0	47.46±7.65
FedProx	0.430 2±0.002 1	0.856 2±0.054 8	0.635 8±0.034 0	50.02±5.27
FedBN	0.426 8±0.002 0	0.853 1±0.056 1	0.603 3±0.035 5	47.07±4.87
FedPer	0.892 6±0.002 0	0.983 3±0.020 5	0.588 1±0.033 1	47.00±3.10
FedRep	0.900 0±0.002 0	0.985 0±0.019 1	0.661 6±0.075 4	45.42±2.78
FedBABU	0.882 0±0.001 5	0.983 0±0.021 5	0.591 1±0.051 4	47.98±5.39
APFL	0.891 3±0.001 9	0.984 5±0.021 4	1.176 4±0.045 4	51.42±3.74
FedPHP	0.093 7±0.000 0	0.494 0±0.218 2	1.500 1±0.117 5	49.82±3.76
Ditto	0.886 8±0.001 3	0.987 9±0.019 7	1.225 4±0.107 9	49.81±4.40
FedFomo	0.881 7±0.001 3	0.982 4±0.023 7	0.688 5±0.079 6	50.95±4.06
FedAMP	0.888 0±0.002 1	0.983 4±0.023 2	0.615 7±0.028 6	49.27±3.35
APPLE	0.880 6±0.108 0	0.980 3±0.024 0	5.457 1±3.278 4	51.05±1.32
FedAsync	0.486 0±0.113 3	0.869 8±0.205 5	1.033 9±0.016 6	100.00 ±0.00
Ours	0.764 5±0.004 1	0.945 4±0.110 3	0.920 8±0.025 6	100.00±0.00
Ours − delay	0.763 4±0.007 3	0.937 6±0.142 3	0.908 4±0.032 4	100.00±0.00
Ours − delay − loss	0.491 5±0.068 6	0.769 8±0.259 5	0.853 0±0.009 5	100.00±0.00

训练时间和设备计算时长比例方面，平均训练时间本身就是系统异构性的指标体现，故而有系统异构性时，会表现为平均训练时间变长；随着系统异构性的减小，虽然设备计算时长比例均有所提升，但是仍旧不超过 55%，说明在系统中，尤其本文的训练任务和网络模型下，设备本身的波动就会带来极大的通信开销，导致系统训练效率降低，设备利用率低，进而证明了采用本文所提出的半中心化的联邦学习架构的必要性和有效性.

另外，本文对 PAT 分布下的实验效果也进行了测试，如表 5 所示. 从表 5 可以看出，在 PAT 分布下，测试准确率、测试 AUC、平均训练时间和设备计算时长比例这 4 项指标的变化趋势均与 DIR 分布下的指标变化趋势相同，说明我们提出的基于区块链辅助的半中心化联邦学习框架能够在不同的非独立同分布数据下均有相同的效果和表现.

Table 5 Results of Our Framework and Other Federated Learning Frameworks Under CIFAR10-PAT

表 5 本文框架与其他联邦学习框架在 CIFAR10-PAT 下的结果

算法框架	测试准确率	测试 AUC	平均训练时间/s	设备计算时长比例/%
FedAvg	0.476 8±0.006 1	0.861 2±0.002 6	1.476 8±0.087 1	46.85±6.29
FedAvg + loss	0.477 6±0.006 2	0.847 5±0.003 2	1.496 9±0.063 3	49.41±6.30
FedProx	0.475 7±0.005 7	0.861 0±0.002 6	1.838 3±0.068 8	48.47±8.44
FedBN	0.475 7±0.005 6	0.861 1±0.002 6	1.564 8±0.079 6	49.13±5.27
FedPer	0.890 2±0.002 1	0.985 2±0.000 4	1.613 8±0.129 8	49.99±6.19
FedRep	0.899 1±0.001 1	0.986 3±0.000 4	2.691 2±0.177 7	52.31±5.64
FedBABU	0.459 2±0.005 1	0.848 6±0.003 4	1.555 6±0.056 1	51.59±4.13
APFL	0.880 0±0.000 5	0.990 4±0.000 1	4.332 2±0.256 2	55.91±4.95
FedPHP	0.093 4±0.000 0	0.489 9±0.000 0	4.934 2±0.164 1	57.63±4.52
Ditto	0.476 6±0.005 9	0.861 3±0.002 6	3.889 1±0.134 3	59.30±4.16
FedFomo	0.897 3±0.001 0	0.990 7±0.000 3	2.637 7±0.147 3	54.42±4.84
FedAMP	0.880 4±0.000 5	0.990 4±0.000 1	1.669 9±0.079 0	45.50±6.23

表 5（续）

算法框架	测试准确率	测试 AUC	平均训练时间/s	设备计算时长比例/%
APPLE	0.851 0±0.003 0	0.978 7±0.000 5	6.159 6±0.138 1	65.08±2.53
FedAsync	0.458 8±0.006 2	0.878 1±0.042 3	1.507 1±0.031 7	100.00±0.00
Ours	0.584 8±0.075 5	0.927 1±0.051 3	1.553 6±0.054 4	100.00±0.00
Ours − delay	0.553 3±0.068 4	0.924 6±0.070 2	1.488 6±0.029 7	100.00±0.00
Ours − delay − loss	0.276 1±0.031 4	0.775 2±0.040 9	1.452 6±0.037 3	100.00±0.00

5 总　　结

本文提出了一种基于区块链辅助的半中心化联邦学习框架，可以在适配物联网场景的前提下，提高联邦学习算法的准确率和效率，其设计能够知道实际环境中的框架部署. 半中心化的联邦学习框架可以有效利用物联网中的网络连接以辅助联邦学习任务的完成，同时可以分散聚合操作至各个客户端以减少通信开销. 而针对联邦学习的区块链区块设计则基于联邦学习训练过程，设计了下载区块、上传区块和评分区块以指导区块链联邦学习系统部署. 实验结果表明，本文提出的基于区块链辅助的半中心化联邦学习框架在准确度方面相较于传统联邦学习算法至少提高了 8%，在效率方面则大幅度降低了因客户端相互等待带来的通信开销. 因此，本文的方法是可行且高效的. 但本文也有部分限制：1）虽然实验可以证明方法有效性，但是算法收敛性缺乏一定的理论证明，相关研究对于异步联邦学习和同步联邦学习均有理论依据，故本文后续会从理论角度对半中心化联邦学习框架进行分析；2）算法中对区块链中的共识算法等内容并未进行对应联邦学习任务的设计，且评分区块虽有设计，但并未加以利用，故本文后续会从区块链中的算法设计和联邦学习任务进一步适配展开；3）本文框架准确率相较个性化联邦学习仍有优化空间，故而本文后续会研究个性化联邦学习算法的嵌入.

作者贡献声明：施宏建负责实验方法设计、实验数据整理与分析、论文初稿撰写；马汝辉负责实验设计验证与核实、论文审阅与修订；张卫山负责论文审阅与修订；管海兵负责论文审阅与修订.

参　考　文　献

[1] Yang Yang, Ma Mulei, Wu Hequan, et al. 6G network AI architecture for everyone-centric customized services[J/OL]. IEEE Network, 2022: 1−10. [2023-05-28].https://ieeexplore.ieee.org/document/9839652

[2] Zhang Rui, Chu Xuesen, Ma Ruhui, et al. OSTTD: Offloading of splittable tasks with topological dependence in multi-tier computing networks[J]. IEEE Journal on Selected Areas in Communications, 2023, 41(2): 555−568

[3] Akabane A T, Immich R, Pazzi R W, et al. TRUSTed: A distributed system for information management and knowledge distribution in VANETs[C] //Proc of 2018 IEEE Symp on Computers and Communications. Piscataway, NJ: IEEE, 2018: 1−6

[4] Yuan Shijing, Li Jie, Wu Chentao. JORA: Blockchain-based efficient joint computing offloading and resource allocation for edge video streaming systems[J]. Journal of Systems Architecture, 2022, 133: 102740

[5] Lin Yangfei, Li Jie, Kimura S, et al. Consortium blockchain-based public integrity verification in cloud storage for IoT[J]. IEEE Internet of Things Journal, 2021, 9(5): 3978−3987

[6] Zhang Weishan, Sun Gang, Xu Liang, et al. A trustworthy safety inspection framework using performance-security balanced blockchain[J]. IEEE Internet of Things Journal, 2022, 9(11): 8178−8190

[7] Shi Hongjian, Wang Hao, Ma Ruhui, et al. Robust searching-based gradient collaborative management in intelligent transportation system[J/OL]. ACM Transactions on Multimedia Computing, Communications, and Applications, 2022[2023-05-28].https://dl.acm.org/doi/10.1145/3549939

[8] Zheng Lianmin, Li Zhuohan, Zhang Hao, et al. Alpa: Automating inter- and intra-operator parallelism for distributed deep learning[C] //Proc of the 16th USENIX Symp on Operating Systems Design and Implementation. Berkeley, CA: USENIX Association, 2022: 559−578

[9] Zhang Jiaru, Hua Yang, Song Tao, et al. Improving Bayesian neural networks by adversarial sampling[C] //Proc of the AAAI Conf on Artificial Intelligence. Palo Alto, CA: AAAI, 2022, 36(9): 10110−10117

[10] Du Zhaoyang, Wu C, Yoshinaga T, et al. Federated learning for vehicular Internet of things: Recent advances and open issues[J]. IEEE Open Journal of the Computer Society, 2020, 1: 45−61

[11] Zhang Jianqing, Hua Yang, Wang Hao, et al. FedALA: Adaptive local aggregation for personalized federated learning[C]//Proc of the AAAI Conf on Artificial Intelligence. Palo Alto, CA: AAAI, 2023, 37(9):11237−11244

[12] Guo Hanxi, Wang Hao, Song Tao, et al. Siren: Byzantine-robust federated learning via proactive alarming[C]//Proc of ACM Symp on Cloud Computing. New York: ACM, 2021: 47−60

[13] Zhang Weishan, Zhou Tao, Lu Qinghua, et al. Dynamic-fusion-based federated learning for COVID-19 detection[J]. IEEE Internet of Things Journal, 2021, 8(21): 15884−15891

[14] Qu Youyang, Uddin M P, Gan Chenquan, et al. Blockchain-enabled federated learning: A survey[J]. ACM Computing Surveys, 2023, 55(4): 70: 1−70: 35

[15] Issa W, Moustafa N, Turnbull B P, et al. Blockchain-based federated learning for securing Internet of things: A comprehensive survey[J]. ACM Computing Surveys, 2023, 55(9): 191: 1−191: 43

[16] Singh S K, Yang L T, Park J H. FusionFedBlock: Fusion of blockchain and federated learning to preserve privacy in industry 5.0[J]. Information Fusion, 2023, 90: 233−240

[17] Zhang Weishan, Lu Qinghua, Yu Qiuyu, et al. Blockchain-based federated learning for device failure detection in industrial IoT[J], IEEE Internet of Things Journal, 2021, 8(7): 5926−5937

[18] Guo Shaoyong, Zhang Keqin, Gong Bei, et al. Sandbox computing: A data privacy trusted sharing paradigm via blockchain and federated learning[J]. IEEE Transactions on Computers, 2023, 72(3): 800−810

[19] Lu Yunlong, Huang Xiaohong, Zhang Ke, et al. Blockchain and federated learning for 5G beyond[J]. IEEE Network, 2021, 35(1): 219−225

[20] Feng Lei, Zhao Yiqi, Guo Shaoyong, et al. BAFL: A blockchain-based asynchronous federated learning framework[J]. IEEE Transactions on Computers, 2022, 71(5): 1092−1103

[21] Gao Liang, Li Li, Chen Yingwen, et al. FGFL: A blockchain-based fair incentive governor for federated learning[J]. Journal of Parallel and Distributed Computing, 2022, 163: 283−299

[22] Nguyen D C, Hosseinalipour S, Love D J, et al. Latency optimization for blockchain-empowered federated learning in multi-server edge computing[J]. IEEE Journal of Selected Areas in Communications, 2022, 40(12): 3373−3390

[23] Qu Youyang, Gao Longxiang, Xiang Yong, et al. FedTwin: Blockchain-enabled adaptive asynchronous federated learning for Digital Twin networks[J]. IEEE Network, 2022, 36(6): 183−190

[24] Shayan M, Fung C, Yoon C J M, et al. Biscotti: A blockchain system for private and secure federated learning[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(7): 1513−1525

[25] Wang Yuntao, Peng Haixia, Su Zhou, et al. A platform-free proof of federated learning consensus mechanism for sustainable blockchains[J]. IEEE Journal of Selected Areas in Communications, 2022, 40(12): 3305−3324

[26] Wang Weilong, Wang Yingjie, Huang Yan, et al. Privacy protection federated learning system based on blockchain and edge computing in mobile crowdsourcing[J]. Computer Networks, 2022, 215: 109206

[27] Wan Yichen, Qu Youyang, Gao Longxiang, et al. Privacy-preserving blockchain-enabled federated learning for B5G-Driven edge computing[J]. Computer Networks, 2022, 204: 108671

[28] Ruckel T, Sedlmeir J, Hofmann P. Fairness, integrity, and privacy in a scalable blockchain-based federated learning system[J]. Computer Networks, 2022, 202: 108621

[29] Zhou Wei, Wang Chao, Xu Jian, et al. Privacy-preserving and decentralized federated learning model based on the blockchain[J]. Journal of Computer Research and Development, 2022, 59(11): 2423−2436 (in Chinese)
(周炜, 王超, 徐剑, 等. 基于区块链的隐私保护去中心化联邦学习模型[J]. 计算机研究与发展, 2022, 59(11): 2423−2436)

[30] Li Zonghang, Yu Hongfang, Zhou Tianyao, et al. Byzantine resistant secure blockchained federated learning at the edge[J]. IEEE Network, 2021, 35(4): 295−301

[31] Tang Fengxiao, Wen Cong, Luo Linfeng, et al. Blockchain-based trusted traffic offloading in space-air-ground integrated networks (SAGIN): A federated reinforcement learning approach[J]. IEEE Journal of Selected Areas in Communications, 2022, 40(12): 3501−3516

[32] Cui Laizhong, Su Xiaoxin, Zhou Yipeng. A fast blockchain-based federated learning framework with compressed communications[J]. IEEE Journal of Selected Areas in Communications, 2022, 40(12): 3358−3372

[33] Pokhrel S R, Choi J. Federated learning with blockchain for autonomous vehicles: Analysis and design challenges[J]. IEEE Transactions on Computers, 2020, 68(8): 4734−4746

[34] Li Yuzheng, Chen Chuan, Liu Nan, et al. A blockchain-based decentralized federated learning framework with committee consensus[J]. IEEE Network, 2021, 35(1): 234−241

[35] Feng Lei, Yang Zhixiang, Guo Shaoyong, et al. Two-layered blockchain architecture for federated learning over the mobile edge network[J]. IEEE Network, 2022, 36(1): 45−51

[36] Li Jun, Shao Yumeng, Wei Kang, et al. Blockchain assisted decentralized federated learning (BLADE-FL): Performance analysis and resource allocation[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(10): 2401−2415

[37] Zhang Weishan, Yu Fa, Wang Xiao, et al. R2Fed: Resilient reinforcement federated learning for industrial applications[J/OL]. IEEE Transactions on Industrial Informatics, 2022[2023-05-28]. https://ieeexplore.ieee.org/document/9950718

[38] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data[C] //Proc of the 20th Int Conf on Artificial Intelligence and Statistics. New York: PMLR, 2017, 54: 1273−1282

[39] Li Tian, Sahu A K, Zaheer M, et al. Federated optimization in heterogeneous networks[C] //Proc of Machine Learning and Systems. Indio, CA: Systems and Machine Learning Foundation, 2020: 429−450

[40] Li Qinbin, He Bingsheng, Song D. Model-contrastive federated learning[C] //Proc of IEEE Conf on Computer Vision and Pattern Recognition. Piscataway, NJ: IEEE, 2021: 10713−10722

[41] Acar D A E, Zhao Yue, Navarro R M, et al. Federated learning based on dynamic regularization[C/OL] //Proc of the 9th Int Conf on Learning Representations. OpenReview. net, 2021[2023-05-28].https://openreview.net/forum?id=B7v4QMR6Z9w

[42] Li Xiaoxiao, Jiang Meirui, Zhang Xiaofei, et al. FedBN: Federated learning on non-IID features via local batch normalization[C/OL] //Proc of the 9th Int Conf on Learning Representations. OpenReview. net, 2021[2023-05-28].https://openreview.net/forum?id=6YEQUn0-QICG

[43] Arivazhagan M G, Aggarwal V, Singh A K, et al. Federated learning

with personalization layers[J/OL]. arXiv preprint, arXiv: 1912.00818, 2019[2023-05-28].https://arxiv.org/abs/1912.00818

[44] Collins L, Hassani H, Mokhtari A, et al. Exploiting shared representations for personalized federated learning[C] //Proc of the 38th Int Conf on Machine Learning. New York: PMLR, 2021, 139: 2089−2099

[45] Oh J, Kim S, Yun S Y. FedBABU: Towards enhanced representation for federated image classification[J/OL]. arXiv preprint, arXiv: 2106.06042, 2021[2023-05-28].https://arxiv.org/abs/2106.06042

[46] Deng Yuyang, Kamani M M, Mahdavi M. Adaptive personalized federated learning[J/OL]. arXiv preprint, arXiv: 2003.13461, 2020 [2023-05-28].https://arxiv.org/abs/2003.13461

[47] Li Xinchun, Zhan Dechuan, Shao Yunfeng, et al. FedPHP: Federated personalization with inherited private models[C] //Proc of Machine Learning and Knowledge Discovery in Databases. Berlin: Springer, 2021, 12975: 587−602

[48] Li Tian, Hu Shengyuan, Beirami A, et al. Ditto: Fair and robust federated learning through personalization[C] //Proc of the 38th Int Conf on Machine Learning. New York: PMLR, 2021, 139: 6357−6368

[49] Zhang M, Sapra K, Fidler S, et al. Personalized federated learning with first order model optimization[C/OL] //Proc of the 9th Int Conf on Learning Representations. OpenReview. net, 2021[2023-05-28]. https://openreview.net/forum?id=ehJqJQk9cw

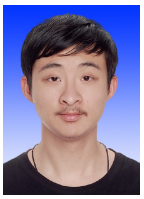
[50] Huang Yutao, Chu Lingyang, Zhou Zirui, et al. Personalized cross-silo federated learning on non-IID data[C] //Proc of the 35th AAAI Conf on Artificial Intelligence. Palo Alto, CA: AAAI, 2021: 7865−7873

[51] Luo Jun, Wu Shandong. Adapt to adaptation: Learning personalization for cross-silo federated learning[C] //Proc of the 31st Int Joint Conf on Artificial Intelligence. California: ijcai. org, 2022: 2166−2173

[52] Fraboni Y, Vidal R, Kameni L, et al. A general theory for federated optimization with asynchronous and heterogeneous clients updates[J/OL]. arXiv preprint, arXiv: 2206.10189, 2022[2023-05-28].https://arxiv.org/abs/2206.10189

[53] Zalando. Fashion-MNIST[DB/OL]. [2023-04-01].https://github.com/zalandoresearch/fashion-mnist

[54] Krizhevsky A, Nair V, Hinton G. The CIFAR-10 dataset[DB/OL]. [2023-04-01].https://www.cs.toronto.edu/~kriz/cifar.html



Shi Hongjian, born in 1998. PhD candidate. His main research interests include distributed machine learning and AI systems.

施宏建, 1998 年生. 博士研究生. 主要研究方向为分布式机器学习和人工智能系统.

Ma Ruhui, born in 1984. PhD, associate professor, PhD supervisor. His main research interests include cloud computing systems, AI systems, and machine learning.

马汝辉, 1984 年生. 博士, 副研究员, 博士生导师. 主要研究方向为云计算系统、人工智能系统和机器学习.

Zhang Weishan, born in 1970. PhD, professor, PhD supervisor. His main research interests include big data processing, AI, and middleware for Internet of things.

张卫山, 1970 年生. 博士, 教授, 博士生导师. 主要研究方向为大数据处理、人工智能和物联网中间件.

Guan Haibing, born in 1971. PhD, professor, PhD supervisor. His main research interests include cloud/distributed computing and machine learning.

管海兵, 1971 年生. 博士, 教授, 博士生导师. 主要研究方向为云/分布式计算和机器学习.