基于区块链的联邦学习: 模型、方法与应用

李 程[1, 2] 袁 勇[1] 郑志勇[1] 杨 东[2] 王飞跃[3, 4]

摘 要 近年来, 人类社会快速步入大数据时代, 数据安全与隐私保护已成为发展大数据生态及相关数字经济的关键问题. 联邦学习 (Federated learning) 作为分布式机器学习的一种新范式, 致力于在保护数据隐私的同时从分布式本地数据集中训练全局模型, 因而获得了广泛和深入的研究. 然而, 联邦学习体系面临的中心化架构、激励机制设计和系统安全等技术挑战仍有待进一步研究, 而区块链被认为是应对这些挑战的有效解决方案, 并已成功应用于联邦学习的许多研究和实践场景. 在系统性地梳理现阶段区块链与联邦学习集成研究成果的基础上, 提出基于区块链的联邦学习 (Blockchain-enabled federated learning, BeFL) 概念模型, 阐述其中的若干关键技术、研究问题与当前研究进展, 探讨该领域的应用场景以及有待进一步研究的关键问题, 并讨论未来发展的潜在方向, 致力于为构建去中心化和安全可信的数据生态基础设施、促进数字经济与相关产业的发展提供有益的参考与借鉴.

关键词 区块链, 联邦学习, 智能合约, 机器学习, 隐私保护

引用格式 李程, 袁勇, 郑志勇, 杨东, 王飞跃. 基于区块链的联邦学习: 模型、方法与应用. 自动化学报, 2024, **50**(6): 1059−1085

DOI 10.16383/j.aas.c230336

Blockchain-enabled Federated Learning: Models, Methods and Applications

LI Cheng[1, 2] YUAN Yong[1] ZHENG Zhi-Yong[1] YANG Dong[2] WANG Fei-Yue[3, 4]

Abstract In recent years, human society has been witnessed to evolve fast to the era of big data, rendering the data security and privacy protection a key issue for the development of digital economies. Federated learning, as a novel pattern for distributed machine learning, is aimed to train a centralized model from decentralized datasets while protecting user privacy, and is now intensively studied in literature. However, a variety of technical challenges, e.g., centralized architecture, incentive mechanism design, and system-wide security issues, are still awaiting further research efforts. In this respect, blockchain proves to be an elegant solution for federated learning to overcome these issues, and thus has been applied in federated learning in many scenarios with success. In this paper, we proposed the conceptual model for blockchain-enabled federated learning (BeFL) based on a comprehensive review of related literatures, and discussed the key techniques, research issues, as well as the state-of-the-art research progresses. We also investigated potential application scenarios, several key issues to be addressed and the future trends. Our work is aimed at offering useful reference and guidance for establishing a new infrastructure for decentralized, secured and trusted data ecosystem, and also promoting the development of digital economy industries.

Key words Blockchain, federated learning, smart contract, machine learning, privacy protection

Citation Li Cheng, Yuan Yong, Zheng Zhi-Yong, Yang Dong, Wang Fei-Yue. Blockchain-enabled federated learning: Models, methods and applications. *Acta Automatica Sinica*, 2024, **50**(6): 1059−1085

随着信息与智能技术的高速发展, 互联网与物联网设备产生的数据呈现出爆炸式增长态势. 国际数据公司 (International Data Corporation, IDC) 的全球数据规模预测显示, 到 2025 年, 全球数据可达 175 泽字节 (Zetta byte, ZB), 其中 90 ZB 来自物联网设备, 数据交互用户将从 2018 年的 50 亿增至 60 亿. 数据已经成为一种新的、更为重要和有效的生产要素. 例如, 以深度学习为代表的新一代人工智能技术通常需要大量数据来训练理想模型, 以期提高智能系统的性能与效率.

然而, 数据在发挥重要作用的同时, 其采集与使用也将关系到个人安全与国家安全, 因而国内外

收稿日期 2023-06-07 录用日期 2023-10-21
Manuscript received June 7, 2023; accepted October 21, 2023
国家自然科学基金 (72171230), 澳门科学技术发展基金 (0050/2020/A1), 北京市未来区块链与隐私计算高精尖创新中心项目资助
Supported by National Natural Science Foundation of China (72171230), Science and Technology Development Fund of Macau (0050/2020/A1), and Beijing Future Blockchain and Privacy Computing Advanced Innovation Center
本文责任编委 张向荣
Recommended by Associate Editor ZHANG Xiang-Rong
1. 中国人民大学数学学院 北京 100872 2. 中国人民大学交叉科学研究院 北京 100872 3. 中国科学院自动化研究所复杂系统管理与控制国家重点实验室 北京 100190 4. 澳门科技大学系统工程研究所 澳门 999078
1. School of Mathematics, Renmin University of China, Beijing 100872 2. School of Interdisciplinary Studies, Renmin University of China, Beijing 100872 3. State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing 100190 4. Institute of Systems Engineering, Macau University of Science and Technology, Macao 999078

对于数据隐私保护的法律法规也日趋严格: 2018 年, 欧盟发布《通用数据保护条例》(General data protection regulation, GDPR); 2021 年, 中国相继发布《数据安全法》和《个人信息保护法》. 这些法律法规虽然有助于保护数据安全和隐私, 但同时也在一定程度上限制了数据流通和价值创造, 迫使数据由于安全隐私或地理位置等因素而散落在互不连通的数据孤岛中. 因此, 在保障隐私和安全的前提下, 如何促进数据流通与共享、增进机构间的协同与合作效率, 是目前学术界和产业界普遍关注的问题.

联邦学习 (Federated learning) 是近年来兴起的分布式机器学习新范式, 可以实现各个机构的私有数据不出本地, 在不披露底层原始数据或其加密形态数据的前提下, 通过迭代式交换和更新加密参数的方式共建一个虚拟的全局模型. 由于数据本身不移动, 有效降低了隐私泄露和数据合规风险, 因此联邦学习近年来获得了广泛和深入的研究关注[1−3]. 在理论建构上, 联邦学习的研究可以追溯到 1996 年, Cheung 等[4] 首次在分布式数据库中实现了关联规则挖掘, 为联邦学习奠定了理论和方法基础. 2016 年, 谷歌公司正式提出联邦学习技术, 并用于实现输入法优化[5]. 2017 年, Tan 等[6] 提出远域迁移学习 (Distant domain transfer learning) 理论体系, 并将迁移学习与联邦学习相结合, 于 2020 年提出了联邦迁移学习技术框架, 以解决数据孤岛问题[7].

近年来, 联邦学习在产业实践中已经发展和衍生出 3 种服务形态, 即横向联邦学习 (样本维度) 、纵向联邦学习 (特征维度) 和联邦迁移学习[8−9]. 在应用架构上, 横向联邦学习分为客户端−中心协调器架构和对等网络架构, 纵向联邦学习通常为两方参与且假设存在双方信任的第三方充当协调者来协同双方进行隐私计算. 联邦迁移学习则是在面向隐私保护的分布式机器学习架构上, 结合传统的迁移学习方法实现知识迁移. 在应用场景上, 针对参与方的数据分布特点, 横向联邦学习适用于用户特征部分重叠较多、用户样本部分重叠较少的应用场景; 纵向联邦适用于用户特征部分重叠少、用户样本部分重叠多的应用场景; 联邦迁移学习适用于用户特征和用户样本都重叠较少的应用场景.

现阶段, 联邦学习仍面临诸多挑战[10−11]. 1) 在基础架构层面, 主流的联邦学习的底层网络拓扑结构依赖于中心化服务器来处理各节点上传的参数, 一旦服务器发生单点故障, 则整个系统将陷于瘫痪. 同时, 随着参与训练的节点增多, 中心化服务器的网络负载也将相应增大, 降低系统联合训练的效率; 另一方面, 虽然对等联邦学习网络架构采用点对点 (Peer to peer, P2P) 网络使得各参与节点可以相互传递加密梯度或模型参数, 而无需经过中央服务器来进行聚合, 从而有效缓解了单点故障这一挑战, 然而整个系统却缺乏统一的调度机制来协调多个参与方进行联邦计算. 由此可见, 传统的联邦学习网络拓扑结构制约了整个系统的健壮性和效率. 2) 在据安全层面, 虽然联邦学习采用加密算法可以保护数据在传输过程中不被窃取或篡改, 但是无法防止敌手通过分析模型参数或输出来推断数据的信息. 例如, 敌手可以采取成员推理攻击和特征推理攻击, 通过观察模型参数的变化, 推断出参与者的训练数据是否包含某些特定的样本或属性. 或者, 敌手可以采取重构攻击和模型反演攻击, 通过构造特殊的输入, 观察模型的输出, 反向推导出训练数据的内容; 同时, 联邦学习主要聚焦于数据计算过程, 相比之下关于输入数据筛选以及输出数据或参数检查的有效手段还不多见[12−13], 因此在数据安全和完整性方面尚不完善. 3) 激励机制层面, 参与联合训练的用户需要贡献其计算资源和私有数据, 来训练各方共享的全局模型; 实际应用中, 各用户的计算资源和数据质量往往存在较大差异, 因而具有优势资源和高质量数据的参与方为维护其行业优势, 通常缺乏参与联邦学习的动力. 因此, 联邦学习需要有效的激励机制来激发用户参与的积极性. 4) 节点信任层面, 联邦学习的前提假设是参与训练的节点共同信任中心服务器来做参数处理; 而在一个动态开放的网络环境中, 很难找到一个让所有参与方共同信任的中心节点. 因此, 如何在参与方之间建立信任, 是提高联邦学习有效性的关键.

区块链技术的去中心化基础架构、用户身份安全认证机制、自动化激励分配机制和区块数据的不可篡改性等技术优点有望为应对联邦学习面临的挑战提供解决方案. 区块链系统的基本工作流程是: 分布式的区块链节点通过 P2P 网络共同参与预先设定的共识过程来完成交易或事务数据的验证, 并以链式区块结构封装这些数据, 从而在共识节点间维护相同的数据账本. 共识过程通常是各节点根据预定义的共识机制 (例如, 基于算力或权益的竞争记账、基于特定顺序的轮流记账等) 获得记账权, 获胜节点将当前时间段产生的所有数据打包, 封装到一个新的区块中, 并按照时间顺序链接到主链上. 同时, 区块链系统可能会发行一定数量的代币以奖励获胜节点, 并激励其他节点继续参与数据共识过程[14].

作为一种分布式计算新范式, 区块链可以从如下 4 个方面改进联邦学习. 1) 区块链网络采用完全

去中心化 (或弱中心化) 的 P2P 网络拓扑结构, 为联邦学习的分布式模型聚合提供了合适的架构, 提高了计算弹性、系统完整性和容错能力; 2) 区块链系统的身份认证和权限管理等机制可以提高联邦学习系统的安全性; 3) 区块链可以通过自定义智能合约来自动化地管理不同设备集的多回合联邦学习任务, 同时还可以通过加密货币激励更多用户参与共建生态系统; 4) 在底层分布式共识协议的支持下, 区块链可确保联邦学习过程的公平性和公正性, 帮助参与训练的用户节点之间建立信任.

因此, 近年来, 将区块链技术与联邦学习相结合, 已经成为保障数据安全和隐私、构建数据要素流通新型基础设施的新趋势. 二者互利互补, 在激励联邦学习各参与方进行协同数据训练而又同时确保数据隐私与安全方面, 将形成更为完备的解决方案[15−17].

基于区块链的联邦学习 (Blockchain-enabled federated learning, BeFL) 架构的潜在优势包含以下 3 个方面. 1) 合作模式相似: 区块链是基于分布式系统的、多方协同的网络架构, 而联邦学习需要多个分布式实体的共同参与来协同训练模型, 因此区块链可以作为联邦学习的基础拓扑架构. 2) 二者都具有可信的特征: 联邦学习的可信体现在其数据合作过程可以保护隐私不被泄露, 区块链的可信则体现在记账过程中可以采用共识机制和数据验证机制, 使得数据不可篡改且不可抵赖. 3) 区块链和联邦学习的应用目的是相互补充的: 联邦学习旨在“创造价值”, 利用各个参与方数据的互补性, 通过联合训练来提升模型效果. 而区块链旨在“转移价值”, 真实记录参与各方的贡献, 并进行奖励. 因此, 区块链与联邦学习的融合将成为发展趋势, 也是本文的主要研究动机[18−19].

目前, 基于区块链的联邦学习研究尚处于起步阶段, 现有研究大多是结合边缘计算、物联网和车联网等典型场景研究区块链+联邦学习的应用模式, 缺乏全面总结该领域本身的架构模型、理论体系和技术进展的综述文章[20−28]. 近年来主要国内外综述工作与本文的差异总结如表 1 所示. 总体来说, 本文在对该领域全面调研的基础上, 从利用区块链改进联邦学习的角度出发, 首次提出区块链与联

表 1　BeFL 研究相关综述

Table 1　Overview of BeFL research

文献及作者	主要内容	与本文的差异	应用领域
Nguyen 等[20]	边缘计算中基于区块链的联邦学习概念、应用场景、优势和挑战	文献方法重点讨论边缘计算中基于区块链的联邦学习的通信成本、资源配置、激励学习、安全和隐私保护; 而本文则从通用领域整体归纳了区块链与联邦学习的集成, 及二者进一步研究问题和未来研究方向	边缘计算
Ali 等[21]	物联网中基于区块链的联邦学习发展历程、应用案例、挑战和解决方案	文献方法主要关注物联网中基于区块链的联邦学习的整体研究历程; 而本文从通用领域的角度提供了一个更全面的基于区块链与联邦学习的概览	物联网
Issa 等[22]	物联网中基于区块链的联邦学习的安全性问题	文献方法讨论了在隐私保护、数据共享、攻击防御等方面的优势, 并评估了现有的安全机制和协议; 而本文则关注于通用领域的安全、效率等研究问题和应用领域	物联网
Zhu 等[23]	从多个角度综合考虑了基于区块链的联邦学习所面临的问题和解决方法	文献方法聚焦基于区块链的联邦学习中的安全和奖励等问题及其解决方案, 分析了不同系统架构及未来挑战; 而本文更侧重于以统一的区块链与联邦学习集成的概念模型出发, 更加全面归纳了进一步研究问题	通用领域
Javed 等[24]	车载网络中基于区块链技术和联邦学习技术的优势和挑战	文献方法专注于车联网领域; 而本文则提供了一个针对区块链和联邦学习整合的全面概述, 并适用于众多应用领域	车联网
Qu 等[25]	基于区块链的联邦学习的概念、原理、应用和现有研究工作	文献方法主要从区块链的角度全面介绍了基于区块链的联邦学习; 而本文对比之下则讨论两者的集成概念模型, 并讨论了其架构应用的局限性和现有解决方案	通用领域
李凌霄等[26]	基于区块链的联邦学习技术的发展背景、研究现状和主要挑战	文献方法从架构特点、资源分配、安全机制、激励机制等方面进行了简述; 而本文更为详细和全面地给出了统一的区块链联邦学习概念模型, 并总结了关键研究问题和未来研究方向	通用领域
孙睿等[27]	基于区块链的联邦学习所面临问题、解决方法和应用领域	文献方法主要阐述了体系架构、激励、安全和效率等问题; 而本文更全面归纳了研究现状, 详细讨论了基于区块链的联邦学习在效率、异构、博弈和安全等方面的问题, 并讨论了进一步研究问题和未来方向	通用领域
Saraswat 等[28]	5G 网络中无人机中基于区块链的联邦学习技术	文献方法的研究是关于在 5G 网络的无人机中使用的技术; 而本文则主要关注通用领域, 并以架构模型为基础讨论了基于区块链的联邦学习如何应用在相关领域中	无人机

邦学习集成架构的概念模型, 全面归纳和总结该领域的关键问题、研究方法与当前进展、应用领域以及未来研究方向, 可望为该领域的发展提供借鉴.

本文结构安排如下: 第 1 节给出基于区块链的联邦学习架构的概念模型, 概述其基本工作流程; 第 2 节分别详细阐述该概念模型中的基础架构、共识机制、经济激励、智能合约以及隐私安全五个层面的主要研究问题和当前的进展; 第 3 节介绍基于区块链的联邦学习架构的应用领域; 第 4 节讨论现有的技术瓶颈和解决方案; 第 5 节概述未来发展方向; 第 6 节对本文内容进行总结.

1 基于区块链的联邦学习: 概念模型

为系统和全面地概述区块链与联邦学习集成领域的研究现状与进展, 本文首先提出基于区块链的联邦学习架构模型. 如图 1 所示, BeFL 架构自底向上分别为基础架构层、共识机制层、经济激励层、智能合约层、隐私安全层以及应用领域层. 其中, 基础架构层旨在将区块链这一去中心化 (或弱中心化) 的分布式系统架构作为联邦学习的底层框架, 从而保障系统稳健性和数据可信性; 共识机制层则旨在借鉴现有区块链共识算法并加以改进, 从而避免资源浪费并且保证联邦学习结果可信; 经济激励层主要是设计奖惩机制来实现用户节点利益最大化, 并激励更多节点加入联合学习过程; 智能合约层旨在用智能合约代替中央服务器来对联邦学习作自动化流程管理, 并作为区块链与人工智能技术集成的接口与载体; 隐私安全层则是利用加密和隐私计算技术来保证联邦学习系统的安全和用户隐私.

BeFL 架构的基本运作流程如图 2 所示, 包括参与节点的授权筛选、计算过程的联邦建模以及计算结果的可信存储 3 个主要环节. 在联邦节点授权筛选环节, 每个参与者拥有自己的私有数据, 任务发布者通过在区块链网络上部署智能合约来广播联合学习任务, 并利用区块链身份认证机制来对参与者进行筛选和授权. 经过认证的参与者都将作为“矿工”参与到区块链网络中, 不同的是少部分参与者会在区块链网络共识机制下被选为验证节点参与到联合训练中.

在计算过程的联邦建模环节, 根据数据的分布特点可分为横向联邦训练、纵向联邦训练和联邦迁移训练三类场景. 横向联邦训练中, 被选为训练节

图 1 基于区块链的联邦学习概念模型

Fig. 1 Conceptual model of blockchain-based federated learning

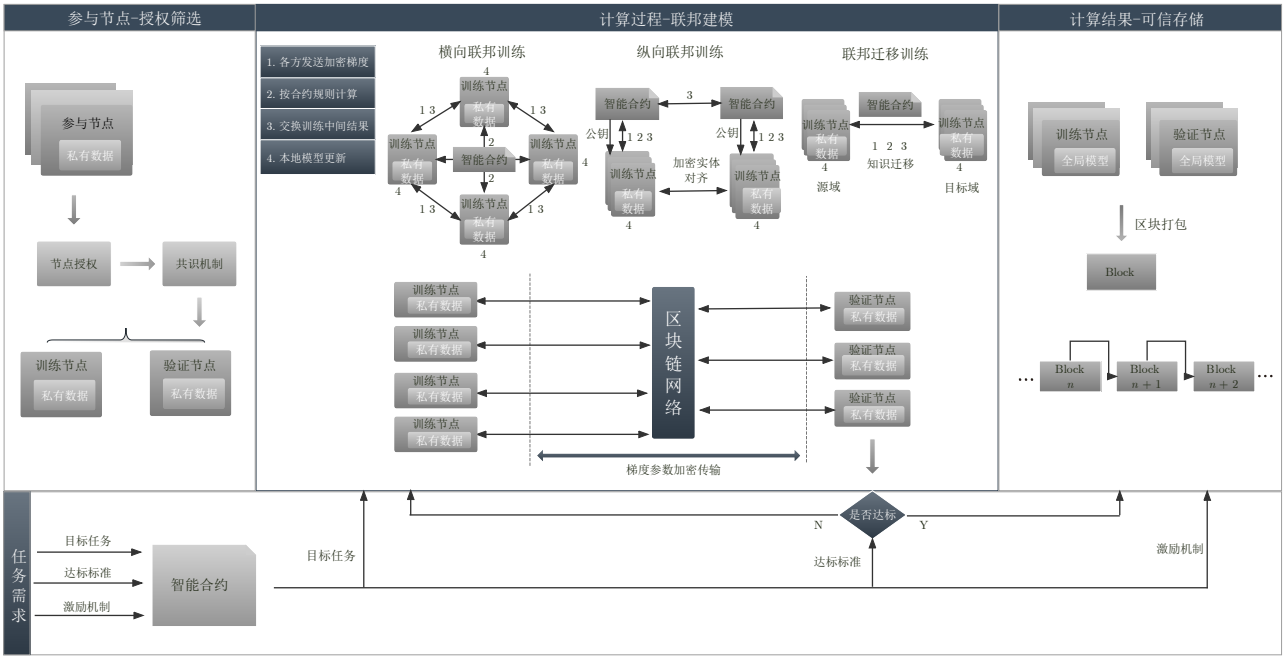

图 2　BeFL 架构的基本运作流程

Fig. 2　The basic operational process of the BeFL architecture

点的参与者使用自己的本地私有数据样本、参照智能合约广播的训练任务进行本地模型训练, 训练完成后对模型参数进行加密, 并在 P2P 网络广播其本地加密参数更新状况和相应的处理信息. 与横向联邦训练相比, 纵向联邦训练需要在训练前做加密实体对齐, 对齐算法和规则按照事先定义在智能合约中的代码执行, 并在训练开始时由系统分发公钥. 联邦迁移训练中, 训练节点被分为源域、目标域双方, 按照智能合约中的秘密共享协议来共同计算损失函数. 随后, 每个参与节点都会在预设时间戳之前从训练节点接收到其本地训练的加密模型参数, 并根据智能合约中定义的聚合规则实现局部模型参数聚合.

智能合约接收参与节点上传的聚合模型后, 将其在区块链网络中进行广播. 与此同时, 被选择作为验证节点的参与者从区块链网络中获取聚合模型后, 根据智能合约中预定义的验证方式对该模型进行验证, 得到全局模型, 并量化训练节点的贡献值, 同时在下一轮联合学习之前通过 P2P 网络使得每个参与者都更新全局模型.

在计算结果的可信存储环节, 联邦学习结果存储在区块中, 每个矿工 (参与者) 按照区块链共识协议挖掘区块, 直到找到符合要求的随机数或收到其他矿工生成的区块为止. 当一个矿工生成新区块时, 其他矿工会验证该区块的内容 (例如随机数、智能合约更改的状态、交易和汇总模型等) . 如果一个区块被大多数矿工验证通过, 该区块将被添加到区块链中并被整个网络接受, 同时根据智能合约中预定义的奖励机制来对参与者进行奖励, 并再次对参与者进行授权和筛选, 开始下一轮的训练.

2　关键技术与研究进展

本节将阐述 BeFL 概念模型的关键技术及其研究进展 (如表 2 所示), 包括基础架构、共识机制设计、经济激励机制设计、智能合约集成以及安全与隐私保护.

2.1　BeFL 的基础架构

传统联邦学习模式通常采用星型网络拓扑结构, 由一个中央服务器协调通信回合、以迭代方式向参与者广播当前模型、收集本地计算的梯度更新, 并通过聚合生成下一代模型. 这种中心化网络拓扑可能存在单点故障和信任缺失等问题. 首先, 中央服务器一旦发生故障, 将导致整个网络瘫痪, 并且当有大量的参与者进行联合训练时, 中央服务器会构成性能和通信瓶颈. 其次, 中心化网络拓扑结构设计的前提假设是参与者愿意信任这个中央服务器. 然而, 即使这个中央服务器可以保证模型参数更新的安全性和隐私, 参与者也可能会因缺乏对于中央服务器的信任而更愿意彼此直接共享参数. 最后, 多方参与的联邦学习任务的优势在于可以将存储在各方私有服务器上的数据进行中心化聚合, 从

表 2 BeFL 研究现状
Table 2 Current status of BeFL research

架构	研究要点	研究内容	代表性文献
基础架构	去中心化架构	采用区块链的去中心化 P2P 网络替代传统联邦学习的星型网络	[29−34]
	参数/身份校验	对参与节点身份和上传参数进行验证、筛选和授权	[29−30, 33−34]
	链上−链下架构	结合分布式存储系统, 链上传输参数, 链下训练模型	[31]
共识机制	选举类联邦共识	基于预置的投票和选举规则对训练节点进行选择	[35−38]
	证明类联邦共识	参与节点竞争解决联合学习任务	[20, 39−41]
	联盟类联邦共识	选举委员会节点来评估全局模型	[42−43]
	联邦学习改进共识算法	利用联邦学习来分析和预测节点间进行共识过程时的网络状况	[44−45]
经济激励	面向数据的激励	衡量用户贡献数据的质量	[31, 46−48]
	面向行为的激励	激励用户选择正确的参与训练的方式	[49−54]
	面向信誉的激励	多维度对参与节点进行信誉评分	[55−58]
智能合约	基于智能合约的调度	利用智能合约代替中央协调器来调度整个联邦学习流程	[43, 59−61]
	集成 AI 算法的智能组件	将人工智能算法集成到智能合约中, 形成基于 BeFL 的智能组件	[62−69]
	多智能体与 DAO	基于多智能体技术和 DAO 的自组织联邦生态	[70−73]
隐私安全	加密机制	与同态加密、安全多方计算、差分隐私等加密技术相集成	[74−83]
	推理攻击	抵御 BeFL 的成员推理攻击、特征推理攻击和模型反演攻击等	[79, 84−85]
	投毒攻击	缓解 BeFL 的数据投毒攻击和模型投毒攻击等	[86−88]
应用领域	联邦云计算	实现云计算节点、雾计算节点、边缘计算节点之间互联互通	[89−96]
	医疗健康	实现医疗数据共享同时保证医疗数据安全	[97−108]
	车联网	保证车联网安全有效的同时促进车辆间的数据共享	[109−112]
	智慧城市	打通城市“数据孤岛”, 构建城市数据安全共享机制	[113−117]
	移动网络	在移动网络中, 保护数据隐私的同时提供可靠、高效的网络服务	[118−119]

而提高联邦学习模型的性能. 然而, 随着参与计算的数据所有方增加, 参与方可能会出现恶意攻击系统的情景. 在如今数据已成为一种价值资源的情况下, 迫切需要引入新的技术解决方案来审核参与方的可信度并激励其贡献数据.

区块链技术近年来在数据确权、身份认证以及自动化执行激励机制方面的技术特点可以为数据联邦的构建提供有效的技术支撑. 区块链系统通常基于 P2P 网络, 每个节点都地位对等且以扁平式拓扑结构相互连通和交互, 不存在任何中心化的特殊节点和层级结构, 每个节点均会承担网络路由、验证和传播区块数据、发现新节点等功能. P2P 节点将其部分资源能力 (如处理能力、存储能力或网络带宽) 直接提供给其他网络参与者, 而不需要中央服务器进行集中协调.

联邦学习模型与 BeFL 架构的网络拓扑结构图对比如图 3 所示. 与联邦学习模型相比, BeFL 架构的网络拓扑结构是去中心化 (或弱中心化) 的, 每个用户节点的地位是对等的, 可以自由地加入和退出, 因而整体网络具有更强的可扩展性、服务能力和负载均衡能力; 同时, 用户节点既使用本地数据训练局部模型, 又接受其他节点的梯度参数更新来对全局模型进行聚合, 因此单点故障不会影响整体系统, 具有更高的网络健壮性和可用性; 最后, 所有节点都具备中继转发功能, 可以大幅提高通信的匿名性、保护个人数据的隐私性[28].

BeFL 架构在现有文献中有两种分类方式. 一种是以节点是否同时承担联邦模型训练任务和区块共识任务为标准, 可将 BeFL 架构分为紧耦合架构和松耦合架构. 前者的特点是节点既承担联邦模型训练任务又承担区块共识验证任务, 即联邦学习网络本身是区块链网络[50, 63, 67]; 而后者的共识节点和联邦模型训练节点是逻辑上独立的两组节点, 分别承担各自任务[30, 37, 117−118]. 另一种可根据集成的区块链平台不同分为公有链 BeFL 架构和许可链 BeFL 架构[29, 31, 62]. 前者主要以激励机制设计为主来构建整个系统, 而后者则包括联盟链和私有链, 主要以设计共识机制对参与者进行分类、选择, 从而提高整个系统的安全性和效率[32, 34, 67].

传统联邦学习架构中, 难以保证上传参数的质量也是目前面临的主要挑战之一. 不同参与方持有的数据集规模和质量不同, 会导致它们训练出的参数存在显著的质量差异. 即使没有恶意参与方故意上传低质量参数, 这种质量不均也会严重拖累联邦

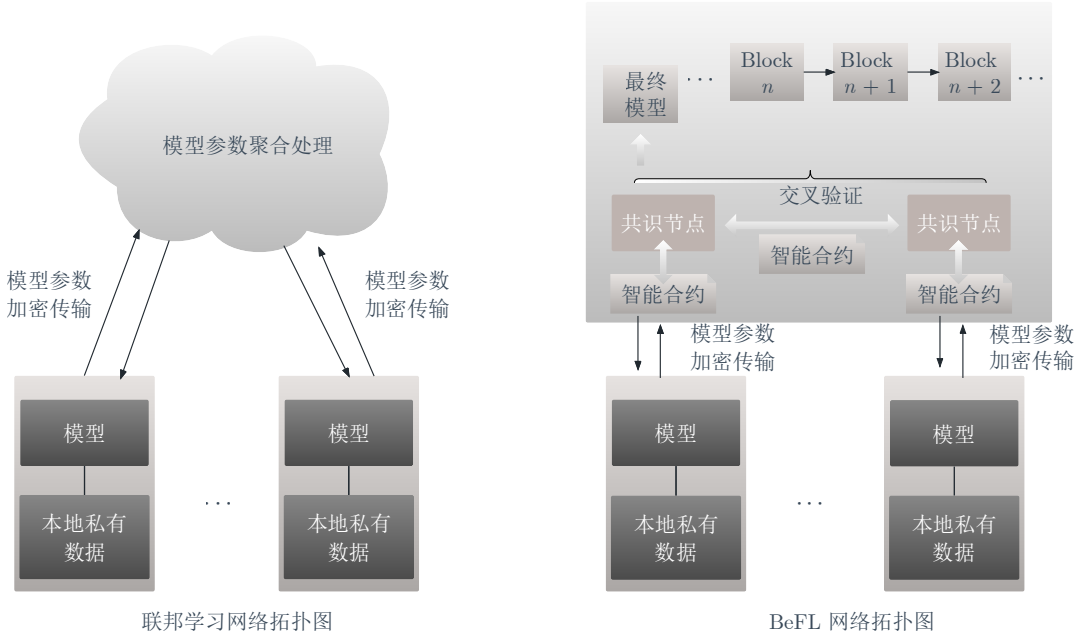

图 3　联邦学习架构与 BeFL 架构的网络拓扑结构

Fig. 3　The network topology of federated learning architecture and BeFL architecture

学习的训练进度和准确率. 低质量的参数可能会降低系统性能, 导致无法承受的收敛时间. 对此, 引入区块链技术虽然无法影响参与方本身的数据质量, 但可以影响其上传数据的行为和策略: 通过集成区块链后的 BeFL 架构、利用区块链的数据验证机制, 可以对参与方的身份信息及其上传参数进行验证, 从而对参与方进行筛选和奖惩, 促使参与方贡献质量高的数据.

现有文献采用的验证过程从如下两个阶段实现安全身份认证机制: 首先, 训练节点在参与联合训练前将会抵押部分存款到智能合约中. 接着, 参与联合训练的节点完成联合训练任务后, 训练节点将在区块链上广播其公钥, 并在具有合法签名 (由其私钥生成) 的区块链上以交易的形式发送更新后的模型参数. 如果其签名有效, 矿工确认上传的模型来自合法参与者, 就将收到的模型放入本地模型库. 矿工将执行模型汇总和区块挖掘等工作, 将汇总后的模型结果反馈给训练节点, 并报告其验证结果. 如果其签名无效, 则将这些节点标记为不可信节点, 并将其公钥更新为无效状态, 系统将扣缴其在智能合约中的存款[30].

考虑到区块链上存储空间和通信带宽的限制, 尽管将模型和模型更新数据存储在链上具有安全优势, 但同时也会造成区块链节点存储容量的巨大负担. 因此, 通常采用星际文件系统 (Inter-planetary file system, IPFS) 等去中心化存储协议来存储模型的参数, 在链上仅传输和存储哈希值, 而不是整个模型参数或模型梯度; 模型训练过程则在链下执行, 这种链上+链下协同的架构设计有助于提高 BeFL 框架的效率和适用性[31].

现有文献中, 研究者已经针对去中心化架构、身份认证和链上+链下架构三个方面提出许多新的 BeFL 架构. 例如, 2021 年 Warnat-Herresthal 等[32] 提出的群体学习 (Swarm learning, SL) 就是集成联邦学习和区块链的 BeFL 计算架构, 其底层网络架构采用了私有许可链技术, 每个参与者只有在预先授权的情况下才能执行交易, 新加入的节点需要经过智能合约审核才能加入到联合训练中来. 经过授权后, 每个参与节点都使用本地私有数据来进行模型训练, 通过区块链网络来传递模型参数, 独立地构建模型. SL 在采用区块链作为基础架构的情况下, 与传统联邦学习架构相比, 省去了中央协调器, 每个节点都有同等的权力来对模型参数做聚合操作, 可确保学习结果的可信性; Kim 等[33] 提出 BlockFL (Blockchained federated learning), 其中用户节点在本地进行模型训练后, 可将本地模型更新的参数通过区块链网络发送给与之关联的节点. 节点之间交叉验证所有的本地更新, 获得记账权的节点负责将所有更新打包至区块中, 并广播给其他节点进行验证; 只有验证通过, 区块才会被添加到区块链中. 这种架构设计可以有效地防止联邦学习过程中模型参数数据被篡改, 提高系统安全性. BlockFL 通过区块链的分布式账本机制, 可以验证每个参与方上传的参数是否匹配其声称的本地数据集规模,

从而避免参与方上传故意篡改或是低质量的模型参数. 然而, BlockFL 无法访问或验证参与方的原始本地数据集, 参与方仍可通过修改数据集来影响模型参数. 因此, BlockFL 只能防止模型参数被直接篡改, 但无法防止参与方通过修改数据集来间接影响模型参数. 这一问题可以通过其他技术手段来配合解决, 如引入信誉机制, 或让参与方只使用可验证的数据集如对数据集添加数字签名或水印等; Lu 等[34] 设计的 BeFL 架构通过区块链网络在所有终端物联网设备之间建立安全链接, 其底层区块链架构仅检索相关数据和管理数据的可访问性, 而不是记录原始数据. 每个用户节点之间执行检索交易和数据共享交易, 并在区块链中广播. 所有的记录都被收集成区块, 由收集节点加密和签名. 这样由区块链来记录所有数据共享事件, 跟踪数据的使用情况, 确保了系统的可审计性.

2.2 共识机制设计

区块链共识算法的核心是通过选举、证明、联盟、随机或者混合等方式从全体共识节点集中选出一个 (或多个) 记账节点的过程. 现有区块链共识算法的优点是任何已经完成的请求都不会 (或极难) 被更改, 可以在存在拜占庭恶意节点的环境中可信地执行客户请求, 因而具有很高的安全性[35]. 在联邦学习系统中, 如何对参与节点做到可信筛选并自动化地执行奖惩来维护系统的安全性并提高系统性能, 一直是亟待解决的问题. 因此, 利用区块链技术来设计联邦共识机制以缓解联邦学习系统中所面临的安全与系统性能挑战, 是 BeFL 架构重要的设计目的之一, 主要体现为以下方面.

首先, BeFL 底层区块链网络架构中, 每个节点都是对等的主体, 中央协调器的聚合功能也由每个训练节点承担; 因此, 区块链共识机制确保了分布式账本的一致性, 这一设计理念也保证了 BeFL 节点在参数更新时的一致性, 并使其获得共同的全局模型. 其次, 区块链的共识机制可以激励诚实节点、惩罚恶意节点. 对于 BeFL 的参与节点来说, 同样存在敌手节点采用恶意行为来攻击系统, 这就需要共识机制来惩罚敌手节点, 并且让诚实节点获得更多的权力. 这对于传统的联邦学习防御机制是一个很好的补充, 可以由整个系统的机制设计来保障系统的健壮性.

现有文献中, 研究者借鉴主流的区块链共识算法, 设计了多种适合 BeFL 的联邦共识机制. 本节从基于选举、证明和联盟机制三种共识类型的角度, 概述 BeFL 联邦共识机制的研究现状与进展.

1) 选举类共识 (例如 Paxos 和 Raft) 中, 矿工节点在每一轮共识过程中通过投票选举的方式选出当前轮次的记账节点. BeFL 可以利用选举类共识算法来对参与训练的节点进行选择, 通过选择诚实节点以维护系统健壮性, 并且由于对节点进行筛选而减少了通信轮次, 从而进一步提高了各方进行协同学习的效率[36]. 在联合训练过程中, 需要考虑到节点的数据质量、计算资源数量、当前功率和网络条件等因素, 并且根据一定的权重来对节点进行选择[37]. 依据权重递减的候选者选择算法, 将使得 BeFL 网络在每个联合训练回合中选择合适的设备加入训练. 即使某些参与节点退出, BeFL 框架仍可以有效地帮助其余节点继续训练以获得更好的模型[38].

2) 证明类共识算法 (例如 Proof of work/PoW 和 Proof of stake/PoS) 中, 矿工节点每一轮必须证明自己具有某种特定的能力, 证明方式通常是竞争性地完成某项难以解决但易于验证的任务, 在竞争中胜出的矿工节点将获得记账权. 受此启发, 现有 BeFL 研究中也设计了类似的共识算法来保障系统运行的健壮性. 例如, Chen 等[39] 设计了一种专用的权益证明 PoS 共识机制. 这种机制通过更频繁地向诚实设备奖励股权, 从而增加诚实节点对区块进行支配的机会, 来保护正确合法的本地模型更新. 这种设计促进了诚实设备更频繁地参与联合训练, 从而得到更好的全局模型. 仿真实验结果显示, 若使用 MNIST 手写数据集进行联合训练, 则在存在 15%的恶意设备的环境中可达到 87%的准确性. 类似地, Kang 等[40] 提出 PoV (Proof of verifying) 共识算法, 以分散且安全的方式删除低质量的模型更新并管理合格的模型更新, 可以防御投毒攻击并确保可靠的联合边缘学习. 进一步, 朱建明等[20] 设计的 PoC (Proof of contribution) 共识算法, 从节点在线时间、本地模型质量与数据贡献度三个方面来综合考量节点对于整个 BeFL 的贡献. 与区块链系统传统的证明类共识算法相比, 节约了求解无意义密码难题的计算资源, 防止了节点自私利己的行为, 有效保证了整个 BeFL 奖励分配的公平性. 此外, 联邦学习中一个重要问题是随着数据量的激增, 需要从众多不相关的数据中筛选出相关数据. 为解决这类问题, Doku 等[41] 利用区块链技术, 设计提出 PoCI (Proof of common interest) 共识机制来解决相关数据稀缺的问题. 在该共识机制的设计中, 整个网络由不同的利益群体组成. 每个利益群体目标是训练己方的全局模型, 想加入利益群体的潜在节点将执行一个计算任务, 利益群体将判断计算任务结果与己方利益是否一致, 从而决定是否将该潜在

节点吸纳到己方群体中来. 由此, 通过这种机制对训练节点的数据作出筛选, 有助于缓解数据稀缺问题.

3) 联盟类共识 (例如 Delegated proof of stake/DPoS) 中, 共识节点基于某种特定方式确定一组代表节点, 而后由代表节点以轮流或者选举的方式依次取得记账权. BeFL 网络架构中, 随着中央服务器的消失, 计算和网络传输的压力都将转移至训练节点, 特别是当所有节点都必须处理共识任务时, 每轮的计算开销都非常大. 因此, 受联盟类共识思想启发, 设计一种基于委员会的共识机制, 不仅可以提高训练效率, 还可以对机器学习的训练流程进行优化[42−43]. 其具体方式为: 由共识机制确定一组诚实节点, 形成一个负责验证局部梯度的委员会并生成区块, 其余节点执行本地训练, 并将本地更新发送给委员会. 然后, 委员会的本地数据将作为验证集对更新进行验证, 并对它们给出一个分数, 只有合格的更新才会打包到区块链上. 在下一轮开始时, 系统将根据上一轮的分数来选出新的委员会. 利用组织者已发布的数据集和评估功能, 用户就可以竞争出第一个或最佳的训练模型, 从而最大程度地发挥评估功能. 由此可见, BeFL 通过区块链选择了一个委员会来汇总模型并在区块链中记录可验证的证明, 从而提高了可验证性.

与上述三种方式利用区块链设计联邦共识机制、旨在改进联邦学习性能不同的是, 研究者同时也致力于设计新型 BeFL 架构、利用联邦学习来改进区块链系统的共识算法. 例如, 常用的 Raft 共识协议是一种简单的、基于领导者的共识算法, 其中只有领导者才能处理所有客户端请求、复制日志并将其传输到节点. 因此, 许多私有区块链都使用 Raft 作为其基础共识算法. 然而, 如果领导者存在诸如包丢失之类的网络不稳定问题, 则使用 Raft 算法会增加网络分裂的可能性, 并且超过一半的节点将失去当前领导者的控制. 当发生网络分裂时, Raft 将开始一个领导者选举期. 在此期间, 网络将停止处理来自客户端的请求. 这会导致事务延迟增加, 每秒交易数 (Transaction per second, TPS) 吞吐量降低. 因此, 结合联邦学习来分析预测各个节点的网络日志数据, 不仅可以识别影响网络稳定性的因素、选择新的领导者以最大程度上减少网络分裂, 同时也可以通过缩短区块决策时间并根据网络环境的状态灵活地选择一个可产生更好性能的节点来提高 Raft 算法的性能[44]. 再如, 比特币采用的 PoW 共识算法通过节点 (矿工) 之间的竞争来确定记账权力和报酬, 以通过密集计算来解决硬密码难题, 这是一个非常耗费计算资源的过程. PoW 的能源浪费问题偏离了当前技术发展的可持续性和环境友好型趋势, 从而稀释了其价值并阻碍了其进一步应用. BeFL 可以把 PoW 中的密码难题替换为联邦学习任务, 将无意义的哈希计算工作证明转化为完成联邦学习模型训练过程的实际任务, 因而扩大了区块链的应用范围[45].

2.3 经济激励机制设计

联邦学习的效果取决于节点本地模型更新的质量. 但是, 节点可能不愿意在没有足够激励的情况下参加联合训练和共享其模型更新. 与基于云的分布式机器学习不同, BeFL 架构中的参与节点是独立的, 数据所有者可以确定何时、何地以及如何参与联合学习. 再者, 参与联邦学习将导致计算资源和网络带宽消耗, 只有足够的奖励才可以激励用户忍受这些成本. 因此, 奖励可以用来以某种方式影响用户的决定. 通过不同的激励机制, 用户将执行不同的训练策略, 从而影响最终的机器学习模型性能.

区块链是典型的经济系统, 其参与者可以通过贡献算力来获得经济激励. 因此, BeFL 激励机制设计的关键在于合理地评估每个节点所做出的贡献, 并且吸引和留住更多的用户来参与联合训练. 本节所述的算法假设参与节点拥有不同质量的数据集, 以此来考察不同的激励机制能否对参与训练的节点进行公平公正的奖励, 并吸引更多的节点加入到联合训练中来. 现有文献中, 许多研究者致力于根据用户的贡献来设计 BeFL 激励机制, 具体可以从用户数据质量、用户行为和用户信誉三方面来设计激励机制.

2.3.1 基于用户数据质量的激励机制

在参与方数据质量验证方面, 可以通过在联邦学习中执行专门的算法来实现, 使用区块链会增加一定的复杂性, 并可能带来一些性能和资源开销. 然而结合区块链和联邦学习进行数据质量验证的主要原因在于数据共享和模型聚合过程中的可信度和安全性需求. 联邦学习涉及多个参与方合作训练模型, 而这些参与方通常分布在不同的地理位置或组织中, 存在信任和数据安全方面的挑战. 区块链的去中心化、不可篡改和透明性特性可以增强数据交换和模型聚合过程的可信度和安全性. 在数据质量验证方面, 区块链可以确保数据交换的历史记录被公开验证, 防止数据篡改或恶意行为. 同时, 区块链可以提供激励机制, 鼓励参与方提供高质量的模型更新, 增加了参与方的积极性和动力.

SV (Shapley value) 是评估数据质量和价值的

典型方法. SV 方法起源于博弈论, 并广泛应用于经济活动中利益合理分配等问题. SV 的计算需要考虑数据点在不同子集中的平均边际效用, 即数据点加入或移除对模型性能的影响. SV 越高, 说明数据点对模型的价值越大[47]. Liu 等[46] 提出称为 FedCoin 的 BeFL 框架, 其中用户节点计算 SV、基于 PoSap (Proof of shapley) 共识协议创建新区块. 基于用户节点计算出的 SV, FedCoin 将执行具有抵赖和防篡改特性的激励收益分配方案. 实验表明, FedCoin 能够正确确定联邦学习用户对训练全局模型的贡献, 并达到完成 PoSap 共识所需的计算资源上限. 类似地, Ma 等[47] 基于区块链, 以可配置的分辨率来测量数据所有者基于 SV 的贡献, 而不会牺牲其隐私性, 解决了在跨数据孤岛联邦学习环境下, 不同数据所有者进行透明贡献评估的挑战. 然而, SV 同样存在一些缺陷, 其在计算不同节点的贡献指数时, 需要对具有不同训练数据集组合的机器学习模型进行训练和评估, 这将消耗更多的时间和资源. 在节点产生对抗行为时, SV 也无法准确衡量数据质量.

此外, 还可以对训练模型设定评估标准. 例如, Mendis 等[31] 研究了以太坊区块链奖励的分布式机器学习和联邦学习机制. 参与者使用本地数据训练全局模型, 并通过 IPFS 上传模型参数; 如果上传模型评估值超过预定义的最低可接受适用率阈值, 则将在以太坊中奖励参与者. Martinez 等[48] 提出基于智能合约仅对有价值的上传更新进行验证和奖励的类抽样验证错误方案, 并检查和评估了错误趋势与错误阈两个验证标准, 以确定用于训练模型的本地数据的质量或有用性.

2.3.2 基于用户行为的激励机制

分析用户行为动机并激励其选择正确的行为, 也是目前研究者关注的重要课题. 例如, BeFL 架构中, 训练节点可能不会执行本地学习, 而是直接从其他客户端复制上传的模型参数以节省其计算资源, 从而造成懒惰节点可以投入更多的计算资源来挖掘区块, 以此获得更多的区块奖励[49]. 这种行为对于其他使用计算资源来进行模型训练的节点来说是不公平的. 为此, BeFL 通常依据博弈论中竞争理论的激励相容性, 通过对参与训练的节点数量、奖励分配方式以及节点贡献制订严格的奖励政策, 以使任何理性的参与节点都能遵循协议并且实现自身利益最大化[50].

传统联邦学习一般采用众包模式来设计奖励机制. 例如 Pandey 等[51] 设计的联邦学习框架中, 在考虑计算和通信成本效益的情况下, 依据众包模式以促使多个设备能够参与到联邦学习中来. 该文献依据 Stackelberg 博弈理论来研究参与的客户端和应用程序平台之间交互模式, 以使参与用户的利益最大化, 并且构建高质量的学习模型. 这种方法可以很好地与区块链结合来设计去中心化的自组织激励机制[52−53]. 如 Cai 等[54] 设计的 BeFL 框架 2CP (Crowdsource protocol and consortium protocol) , 在众包模式的支持下, 用户节点提出模型进行训练, 并使用自己的数据评估其做出的贡献. 系统将根据用户的相对贡献来奖励用户, 拥有更大或更高质量数据集的用户在最终模型中获得更高份额的奖励.

2.3.3 基于用户信誉的激励机制

信誉是联邦学习过程中选择用户节点的重要指标. 具有较高信誉的用户更有可能为联邦学习任务带来高质量和可靠的训练. 在每个训练任务结束时, 将根据用户的行为更新用户的信誉, 然后在下一次训练中选择用户时会考虑信誉记录. 当用户贡献正确和有用的模型参数时, 其声誉会增加, 而在上传恶意模型参数时, 其声誉会下降. 这样做有许多好处, 比如在区块链节点进行投票时, 信誉高的节点可以避免进行复杂的多数表决以进行验证, 从而减少了时间成本. 在处理分叉时, 如果一个节点同时从不同的节点那里收到两个或多个满意的模型, 一个自然的解决方案是选择信誉最高的节点.

在设计 BeFL 信誉评分机制时, 需要确保信誉分数的真实性和客观性. 具体来说, 参与联邦学习的边缘节点、雾节点和云端服务器之间可以依据各自的数据质量、参与程度等进行分级, 并且互相评分; 然后通过智能合约记录每个参与者在联邦学习中的信誉[55]. 为了使信誉分数更加客观, 需要从多个维度来对每个参与者进行评分. Kang 等[56] 设计的 BeFL 架构中, 任务发布者使用针对独立同分布方案的 RONI (Reject on negative influence) 方案和针对非独立同分布方案的 FoolsGold 方案来检测攻击者和不可靠的客户端, 依据检测结果来更新用户信誉分数. 每个用户的信誉分数将结合所有任务发布者给出的不同分数并综合权重来生成[57]. 由此, 依靠信誉评分机制, 用户的诚实行为和高质量数据将使自身受益, 并促进整个系统健康发展. Qi 等[58] 提出的 BFL 框架设计了一种基于模型质量的声誉评估机制和一种基于声誉加权贡献的奖励分配算法, 以激励数据拥有者提供高质量的数据. 该算法考虑了数据拥有者的数据量、声誉值和单位资源消耗, 求解了最优的数据贡献策略. 为了分析数据拥有者的行为策略, 其建立了一个非合作博弈模型, 证明了该博弈模型存在唯一的纳什均衡, 即每个数

据拥有者都没有动机偏离其最优策略, 并通过模拟实验和理论分析验证了 BFL 的有效性、安全性和可靠性.

2.4 BeFL 的智能合约集成

智能合约是区块链上以去中心化自治方式运行的计算机程序, 可以发送、接收和存储信息, 并根据预定义的执行逻辑对输入信息做出响应. 一旦部署上链, 智能合约就不可否认和篡改. 智能合约通常由专用编程语言编写 (如以太坊上的 Solidity 语言), 并通过基于区块链的虚拟化环境执行. 这种虚拟化环境为创建、测试和部署智能合约驱动的去中心化应用程序 (Decentralized applications, DApp) 提供了通用平台. 基于智能合约来设计联邦学习任务发布、局部参数验证、全局模型聚合、全局模型发布、节点贡献评估、激励机制实施等多样化调度规则, 有助于实现去中心化联邦学习过程的高效自适应优化调度[59−60].

智能合约与联邦学习的集成研究通常沿用现阶段主流的智能合约编程语言 (如以太坊的 Solidity 语言). 例如, Li 等[43] 采用传统的 Solidity 智能合约管理联邦学习流程, 用预编译的智能合约设计相应的功能函数模块 (在本地进行联邦学习训练时需要对从链上传来的合约字节码数据做数据转换), 分别监听模型参数、预设模型聚合规则、广播全局模型参数等. 总的来说, 在 BeFL 架构中, 中央服务器的功能改为由去中心化执行的智能合约来实施, 以自动化地协调分布式节点的工作流程. 这些功能大致可分为参与方管理、联邦建模流程管理和激励机制管理三个主要部分.

1) 在参与方管理部分, 对于参与联邦训练的每个参与方, 都有相同预置算法的智能合约与之对应, 并在每个参与方计算环境中单独隔离执行. 智能合约通过去中心化数字身份管理系统初步对参与节点做筛选. 经过身份认证的节点发起建模任务, 智能合约根据相应事件 (例如输入数据的属性、任务的预期输出以及激励措施) 的详细信息来启动数据驱动的学习任务.

2) 在联邦建模流程管理部分, 参与节点在链下使用本地私有数据, 针对发布的任务来训练模型, 并使用分布式存储系统 (例如 IPFS) 来存储模型的参数. 训练节点通过将返回的哈希值导入到 DApp 中, 可以广播实现的计算模型. 收到计算模型后, 验证节点开始进行评估, 并报告其评估结果. 智能合约通过获取各个验证节点的评估结果, 然后对照由任务发布者在智能合约中预先设定的验证标准进行检查. 如果符合标准的评估结果数量超过特定阈值, 系统将会自动分发经济激励到相关训练节点的账户, 同时所有验证节点将获得经济激励.

3) 在激励机制管理部分, 由于训练过程中可能出现不正确甚至是恶意的节点行为, 因此通常要求训练和验证节点在每轮训练开始时将一定数量的代币质押给智能合约. 如果节点正确地参与联合训练过程, 则在训练结束后, 训练和验证节点将根据智能合约中约定的承诺, 获得相应的服务报酬以及质押的代币. 如果检测到恶意或异常行为, 则节点将不会获得报酬, 同时其质押代币将被分配给所有其他参与节点. 结合底层区块链的数据不可篡改性, 智能合约可以监督、规范和溯源参与各方的行为, 并自动化地实施奖惩激励机制.

由此可见, 利用智能合约来管理联邦学习过程有诸多优势: 首先, 智能合约中维护全局模型副本和相关计算状态, 模型选择和聚合以去中心化的方式进行, 参与节点可以自行确定自己的选择, 有助于建立节点之间的信任. 参与节点可以使用全局模型副本在每个回合中自主执行聚合步骤, 并且独立更新全局模型, 从而推动全局计算的发展. 在底层共识协议的支持下, 智能合约有助于确保联邦学习流程的自主性、公平性和公正性. 其次, 智能合约可以同时协调来自不同用户设备集的多个联邦学习的任务回合设定以及模型参数聚集等要素. 与基于中央服务器的联邦学习模式相比, 基于智能合约的联邦学习可以显著降低设置和运营成本, 从而降低了联邦学习训练的门槛、有助于吸引更多的用户加入到联合训练中来. 最后, 智能合约可以监督和规范化参与各方的行为, 并自动化地实施奖惩激励机制[61].

此外, 运行在区块链上的各类智能合约可以视为用户的智能代理 (Intelligent agents). 现阶段, 智能合约只能按照预置规则来执行预定义的触发动作, 尚不具有智能性. 区块链与联邦学习的集成, 将有助于机器学习、深度学习、强化学习等人工智能技术以智能合约的形式集成到 BeFL 架构中来, 形成针对不同任务和场景的智能组件, 从而促使智能合约从具备任务选择、优先级排序和目标导向行为等基础能力, 逐步发展为具有感知、推理、学习和自主决策等高层能力的智能代理, 并通过彼此间的交互通信、协调合作、冲突消解等具备一定的社交能力, 进而形成去中心化自治组织 (Decentralized autonomous organizations, DAO), 其集成与演进过程如图 4 所示.

在智能合约与人工智能的集成方面, 研究者们已经提出利用机器学习算法 XGBoost 来检测区块链上的庞氏骗局[62], 利用嵌入支持向量机算法的智

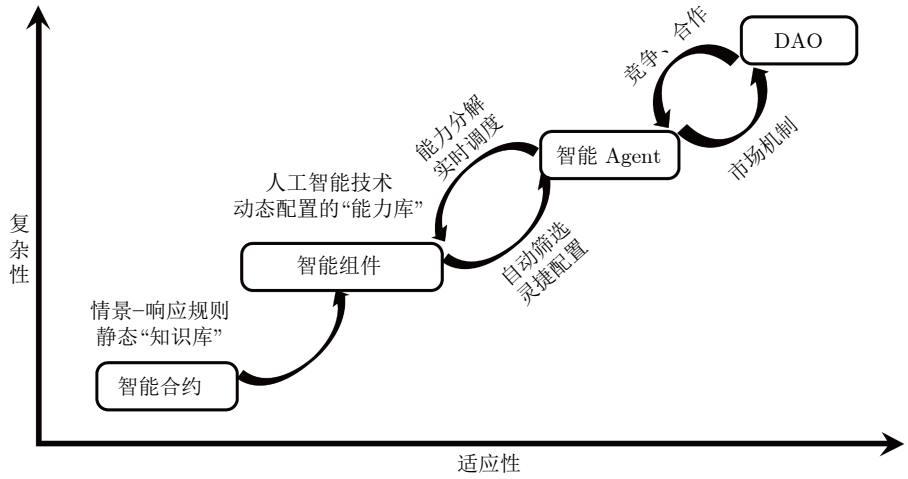

图 4 智能合约与人工智能的集成与演进

Fig. 4 The integration and evolution of smart contracts and artificial intelligence

能合约来处理列车运行时产生的非均衡牵引和制动数据[63], 以及利用基于集成学习模型的智能合约来优化无线电中自动调制的分类任务等[64]; 此外, 深度学习算法也可以与智能合约集成, 利用自动编码器来对网络入侵做异常检测[65−66], 但是对于较深的参数模型的集成仍然需要做进一步研究; 结合强化学习则可以用于筛选计算能力和通信良好的 BeFL 参与节点, 并且能优化系统所占用的计算和通信资源, 提升系统的运行效率[67−69].

进一步, 在结合人工智能技术之后, BeFL 可以视为由许多智能代理组成的分布式智能系统, 因而可以将复杂的任务自上而下地划分为相互关联的子任务, 利用智能代理采用分治法解决这些子任务, 并通过高层涌现自下而上地解决实际系统的业务[70]. 例如, Zhang 等[71] 设计了基于智能代理的 BeFL 框架 (SABlockFL), 其中智能代理同时充当区块链网络的共识节点和联邦学习任务的参与节点, 并使用机器学习任务数据集 (如 MNIST 和 CIFAR) 进行联合训练, 实验结果证明了该框架的有效性.

从社会智能或群体智能的角度来看, 基于智能合约的联邦学习将对以社区为中心的组织形态产生深远影响. 同一社区的微型组织可以使用区块链上的智能合约实现自组织地联合训练[72]. 这样, 社区中的每个组织都可以在保护数据隐私的前提下, 通过协作来训练公共任务, 以帮助解决整个社区共同面临的挑战. 进一步, 通过将核心的法律条文、商业逻辑和意向协定编码到智能合约中, 可实现针对特定业务场景和监管需求的“以法入链”, 构建合规可信、数据共享和监管友好的 BeFL 多代理系统, 进而逐步演化为各类 DAO 形成的联邦生态[73]. 这将促进分布式人工智能技术的发展, 推动传统商业模式和社会生产关系的变革.

2.5 安全与隐私保护

联邦学习的主要优点是每一轮模型训练在本地完成, 并且保留全局模型的副本; 在每轮训练过程中, 数据存储在终端设备而非云端服务器上, 因而可以极大地提高隐私性, 并有助于满足 GDPR 等法规的要求. 然而, 在联邦学习的训练过程中也面临着安全和隐私方面的挑战. 在联邦学习安全方面面临的攻击方式主要有投毒攻击、后门攻击、拜占庭攻击、搭便车攻击和女巫攻击等, 在隐私方面遇到的攻击方式主要有推理攻击和对抗攻击等[74−76].

BeFL 架构将联邦学习部署在区块链网络上, 利用区块链的加密、不可篡改、去中心化等特性, 可以更好地保护数据隐私和安全. 例如数据和模型参数更新时以加密方式写入区块链, 降低被中间第三方窃取的风险; 通过将联邦学习的模型参数或更新存储在区块链上, 可以确保模型的训练历史是可追溯和透明的. 这有助于检测和防止恶意攻击, 因为所有的操作都被记录下来, 任何未经授权的访问或篡改都会立即被发现; 此外, 区块链技术还可以用于身份验证和访问控制, 以进一步提高联邦学习系统的安全性[81−82].

在结合区块链技术后, BeFL 架构虽然利用区块链技术来对联邦学习参与节点进行筛选、自动化执行激励机制以及采用可信区块存储等方式, 在一定程度上帮助联邦学习系统缓解安全与隐私方面的问题, 但仍然无法做到彻底解决. 相关研究主要思路是在构建 BeFL 架构基础上, 假设在参与节点中选取不超过一半的节点作为非诚实节点来对系统实行模拟攻击, 以此来考察 BeFL 架构的健壮性. 本

节将首先讨论 BeFL 架构的隐私保护机制, 然后介绍 BeFL 架构研究中目前重点解决的推理攻击和投毒攻击等挑战.

2.5.1 隐私保护机制

现有文献中提出了对应不同业务场景的多种隐私保护机制. 例如, 同态加密、安全多方计算和差分隐私是运用最广泛的隐私保护技术: 同态加密旨在对密文进行计算操作并得到加密结果, 加密结果经解密后, 与对明文进行该计算操作的结果相同; 安全多方计算旨在实现多个参与方协同计算某个函数, 而不用暴露己方的隐私输入数据; 差分隐私旨在通过添加少量噪声来隐藏客户端模型更新中的个人信息. 基于这些隐私保护技术, 研究者们已经提出许多 BeFL 设计框架 [77−81].

值得注意的是, 在 BeFL 框架的设计中, 需要考虑减少繁重的计算与通信开销, 例如使用差分隐私时, 更高的私密性要求意味着需要在查询结果中添加更多的噪声, 如果用户使用差分隐私来保护自己的参数, 那么他们需要发送更多的比特来保证聚合结果的准确性, 并且不同参与方需要相互通信来协调添加噪声的过程, 因此更高的私密性要求意味着更高的通信成本[82]. 安全多方计算协议要求所有各方生成其私有数据的秘密份额并与其他各方交换, 因而需要多次数据传输, 不可避免地导致更高的通信开销. 同态加密的计算与传输过程均在密文状态下进行, 因此计算时间更长并且传输较慢. 由此可见, 通信开销、计算耗时、部署环境等是 BeFL 在设计隐私保护机制时必须考虑的问题. 为了在使用差分隐私的情况下不降低预测精度, Lyu 等[83] 提出的 FPPDL (Fair and privacy-preserving deep learning) 在开始训练时会预留一部分不敏感的数据来进行全局共享, 通过使用生成对抗网络 (Generativeadversarial network, GAN) 来生成训练数据, 并基于合成后的数据样本实现深度学习. FPPDL 在第一阶段利用差分隐私 GAN (Differentially private GAN) 来发布差分隐私本地样本, 以便在初始基准测试阶段进行相互评估. 在第二阶段参数上传时, 借助流密码思想对同态加密算法加以改进, 以降低通信开销. FPPDL 的加密方案使其对于高维数据加密变得有效, 部分解决了联邦学习中高维度参数向量的大型模型容易受到隐私和安全攻击这一问题.

2.5.2 推理攻击

联邦学习训练期间, 梯度交换可能会将与参与者训练数据有关的信息泄漏给对抗性参与者, 这种情形称为推理攻击. 因此, 对模型更新的观察可用于推理私人信息. 现阶段的研究重点包括针对成员资格、属性和模型等要素的推理攻击.

成员推理攻击是指给定确切的数据点, 攻击者旨在确定是否用于训练模型. 例如, 攻击者可以推理是否使用特定的患者资料来训练与疾病相关的分类器. Liu 等[79] 设计的 BeFL 框架中提出在参与者上传的模型更新中添加高斯噪声. 数值结果表明: 该框架可以有效阻止成员推理攻击, 从而提高联邦学习在 5G 网络中的安全性.

特征推理攻击是指攻击者推理其他参与者的训练数据的属性. 攻击者可以使用多任务学习来欺骗联邦学习模型, 以学习对具有和不具有属性的数据进行更好的分离, 从而提取更多信息. 例如, 当参与者的模型更新存在属性泄漏时, 敌手将能够识别具有特定属性的一组参与者. 针对这种情况, Shen 等[84] 基于区块链技术设计了 BeFL 框架, 实验结果表明, 该框架可以保持联邦学习中主要任务不受影响.

模型反演攻击旨在从模型中抽取训练数据或训练数据的特征向量, 攻击者通过“查询−回应”数据来模拟出一个与原始模型相似的模型. Fang 等[85] 证明了在面临模型反演攻击时, 区块链技术可以为联邦学习提供可靠的解决方案.

2.5.3 投毒攻击

投毒攻击是联邦学习中另一种常见的安全攻击. 按照攻击方式, 可以分为数据投毒攻击和模型投毒攻击. 前者是指攻击者通过直接将投毒数据注入目标设备或通过其他设备注入投毒数据来使数据中毒, 从而降低整体模型的准确性; 后者则指攻击者尝试对本地模型而不是本地数据进行毒化, 例如攻击者将本地模型更新发送到服务器之前将其毒化, 或者将隐藏的后门插入全局模型中来引入错误, 从而影响全局模型的准确性.

区块链技术可以有效缓解投毒攻击. 在联邦学习开始前, 参与者验证机制可以筛选出外部攻击者; 在每轮训练时, 针对节点和上传参数的审核将使得系统拒绝对全局模型产生错误影响的数据和模型, 并且底层的共识协议保证了整个系统即使在少部分错误影响下依然能正确运行; 另外, 激励机制使得每个节点基于自身利益最大化的假设下选择正确的参与方式, 而智能合约的公开透明使得每个节点的错误行为都将被追溯责任. 这些措施都有助于保障 BeFL 架构在投毒攻击时的健壮性[86].

现有文献中, Shayan 等[87] 提出的 BeFL 框架 Biscotti 通过使用差分隐私噪声和 Shamir 秘密分享方案提供数据隐私性和安全性, 可以在高度分布式的环境中提供安全的私有多方机器学习. 实验证

明, Biscotti 可以抵抗数据投毒攻击, 当 30% 的敌手试图毒害该模型时, Biscotti 可以大规模地保护训练节点参数更新的隐私和全局模型的性能. BlockFlow 则是一种用于联邦学习的隐私保护解决方案, 该方案考虑利用拉普拉斯噪声来保护差分隐私, 以避免将客户端信息泄漏给其他客户端. 在模型投毒攻击中, BlockFlow 可以在确保不共享个人隐私信息的情况下, 检测出提供不良模型的代理, 并抵制不超过 50% 的恶意代理的攻击[88].

3 BeFL 的应用场景

现阶段, BeFL 架构已在许多领域得到研究和应用, 致力于解决数据共享和多方协作场景中的安全和隐私保护等关键问题、提高数据要素在共享和流通中的价值. 本节将概述 BeFL 在联邦云计算、医疗健康、车联网、智慧城市和移动网络等典型领域的应用现状与进展. 这些领域面临的共性问题是弱信任环境下基于不完备数据的多方共享与协作及其隐私保护问题. 一方面, 机构之间可能由于信任缺失而难以充分共享必要的数据; 另一方面, 市场竞争或行业隐私约束也可能使得各机构间不愿共享数据. 因此, 突围数据孤岛困境、在保护数据隐私的同时促进各机构之间的数据共享与跨链流通, 是 BeFL 架构与相关技术在这些领域的广泛应用需求与重要应用目标.

需要考虑的是, 在常见的 cross-device 场景中, 参与方规模非常庞大, 可能达到几百万甚至上千万. 这种情况通常会面临信息交互的巨大开销: 每一轮共识过程中通过投票选举记账节点, 且节点同时承担共识任务和联邦聚合任务, 可能会导致性能瓶颈和可扩展性问题 (这对于紧耦合架构尤为明显, 而对共识节点和联邦节点相互独立的松耦合架构则不常见). 因此, 为了提高网络带宽、计算资源和共识算法的效率, 现有研究一方面是使用基于选举类的共识机制来对参与节点进行选择, 另一方面使用基于梯度压缩或差分隐私的技术来减少上传数据量和保护数据隐私. 对于参与方规模相对有限的 cross-silo 场景, 同样需要在弱信任的环境中 (如跨地域和跨境的应用场景) 使用区块链来增加参与方之间的信任程度, 并结合区块链实行公开追溯和激励机制来维护系统的可靠性和公平性.

图 5 描述了 BeFL 架构在应用场景中的通用模式: 首先, 在数据接入和预处理阶段, 各方需要将接入数据加载到可信计算环境中, 并对来自不同用户终端的多源数据 (如联邦云计算的云端, 雾节点以及边缘端上传的数据) 做异构数据融合等预处理操作, 并为后续不同联邦建模场景提供如 PSI (Private set intersection) 隐私样本对齐、差分隐私、同态加密、安全多方计算以及联邦学习模型等的算法模块库.

其次, 数据预处理完成后, 将触发智能合约状态变更, 由智能合约来调度各方进行联邦计算, 在联邦计算完成后由获胜节点打包数据区块至区块链中, 并自动化执行奖励分配, 详细工作流程和智能合约功能模块设计参照图 2 及第 2.4 节.

需要说明的是, BeFL 存在松耦合与紧耦合两种主要架构. 松耦合架构的特点是联邦计算节点与区块链共识节点是相互独立的, 联邦学习系统的节点完成训练后, 将触发智能合约状态变更, 由智能合约调度区块链系统, 接受从联邦学习节点广播的统一格式的模型参数. 松耦合架构适用于车联网及移动网络等动态变化场景, 其优点是可以做到不影响双方系统已有的内部计算逻辑和底层代码, 只需事先制定双方都能执行的数据交互形式并约定执行顺序以达到二者计算流程同步即可; 而缺点则是计算和通信的开销较大, 并且由于计算环境影响将导致通信传输不稳定进而影响系统稳定性. 与松耦合架构不同的是, 紧耦合架构中参与节点既作为联邦学习系统的训练节点同时又作为区块链系统中的共识节点来对本地模型进行交叉验证. 这种架构设计的优点是数据在节点内部处理, 所传输的数据均可保证是脱敏后的数据, 能有效缓解数据在联邦学习系统和区块链系统之间转换时所产生的额外计算资源和通信开销以及数据在系统之间传输时的泄露风险, 适用于联邦云计算场景中对数据有容灾备份需求以及医疗健康场景中对数据隐私有强敏感的应用场景. 同样, 紧耦合架构较难兼容其他联邦学习系统或区块链系统, 技术升级成本大, 容易形成单一的 BeFL 生态闭环.

最后, BeFL 架构的 API (Application program interface) 服务直接服务于各类应用场景, 以 DApp 的形式直接和参与方节点进行交互. BeFL 通常提供的服务包括联邦建模任务提交、任务审批、计算结果查询、状态分析和数据统计等, 通过这些 API 服务在不同应用场景中构建起一个公平可信的联邦计算环境. 后文将具体阐述 BeFL 架构是如何缓解不同应用场景中所面临的数据共享与隐私保护挑战.

3.1 联邦云计算

联邦云是云计算的重要发展趋势, 其基本思路是通过边缘计算、雾计算和终端云计算之间的连接和交互, 来增强云设备. 对于企业来说, 联邦云这种

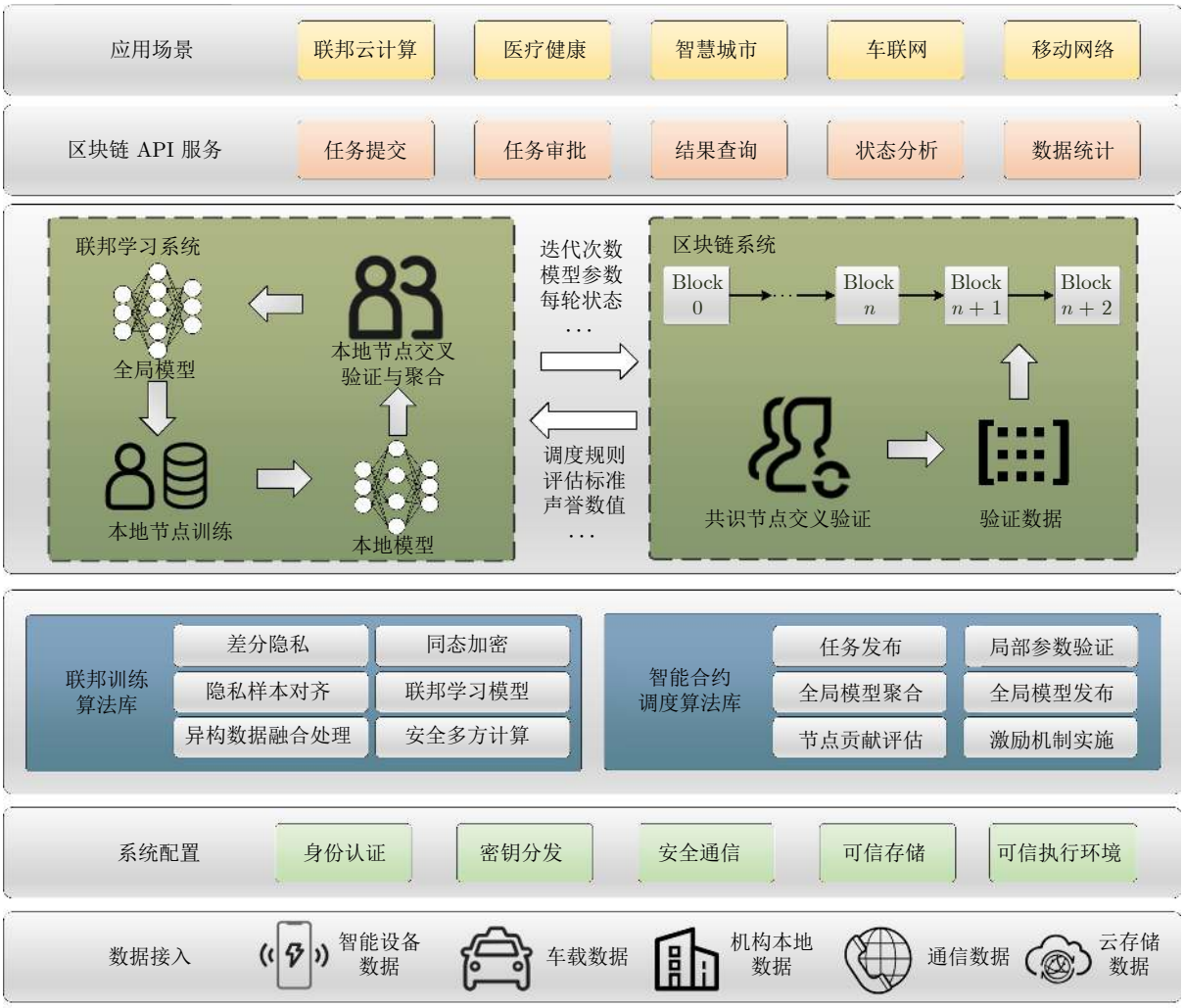

图 5　BeFL 架构的应用场景

Fig. 5　Application scenarios of the BeFL architecture

无需同步的异地数据存储模式将会极大提高企业的数据容灾处理能力、保护非现场的数据资产, 并且雾计算和边缘计算可以用来缓解数据从终端设备上传到云服务器时由于计算资源限制和网络信号等因素而造成的延迟. 然而, 对于雾计算和边缘计算来说, 仍然需要将本地数据上传到雾计算和边缘计算平台, 由此必然存在数据隐私和数据安全问题. 因此, 在越来越严格的数据隐私政策下, 区块链技术与联邦云计算模式的集成需求日趋明显, 二者的结合可有效支持数字资产的异地安全存储, 必将获得更加广泛的应用[89–94].

首先, 雾节点作为云计算和物联网的基础设施, 可以解决网络拥塞和延迟, 实现本地自治, 但同时依然面临着隐私问题、投毒攻击和随之而来的低效率. Qu 等[95] 提出的 BeFL 框架使用具有分布式隐私协议的区块链来代替中央机构, 仅将全局模型更新的指针保存在区块链上, 而将相关原始数据保存在链下分布式哈希表中, 从而达到保护隐私、减少投毒攻击和提高模型运行效率的目的.

其次, 对于联邦云中的边缘节点, Majeed 等[96] 设计了面向边缘网络的 BeFL 框架, 使联邦学习适用于支持 5G 的智能物联网应用. 在该框架中, 由边缘设备组成的区块链网络以区块的形式, 将来自用户设备的本地模型更新, 存储在单独特定渠道的区块中, 全局模型更新则存储在特定通道的分类账上的默克尔帕特里夏树 (Merkle Patricia tree) 中.

3.2　医疗健康

在医疗健康领域, 机器学习等新一代人工智能技术持续推动医疗机构中诸如智能影像辅助诊断等应用的落地, 而当用机器学习来训练数据时, 医疗机构关注的首要问题是训练数据需要保留在本地, 并且避免从经过训练的模型中推理出敏感信息, 这导致各医疗机构间难以共享这些敏感数据. 同时,

数据源不足和标签不足将导致机器学习模型的性能不能令人满意, 这已成为当前智慧医疗与健康领域发展的瓶颈问题. 对此, 利用区块链和联邦学习, 可以在实现医疗健康数据共享的同时, 运用隐私保护技术来保证数据安全[97−106]. 同时, 引入区块链技术将会使得不受信任的医疗数据联邦能够有效构建起可追溯和可问责的完整安全流程. 例如, El 等[107] 提出基于智能合约实现协调服务器的联邦学习算法, 以确保医疗数据共享时的透明度和使用许可, 并应用于糖尿病的预测与决策支持. Qayyum 等[108] 提出的 BeFL 框架, 可以从不同来源协作收集数据, 同时保护患者的数据隐私, 在此架构上使用深度学习模型从肺部影像扫描中检测新冠肺炎图像, 提高了医院智能诊疗水平.

3.3 车联网

车联网具有协作式环境数据感知, 实时数据计算和处理的特征. 车联网环境下智能车数据是指智能网联汽车在运行过程中产生的各种数据, 包括车辆状态、行驶轨迹、车内外环境、驾驶行为、用户偏好等. 这些数据可以用于提供车辆控制、信息娱乐、安全防护、远程诊断等服务, 也可以用于优化交通管理、路况监测、出行规划等应用. 大数据和人工智能技术使得智能车之间的数据共享成为发展趋势. 然而, 涉及到个人身份、位置、习惯等信息的数据, 以及影响到车辆功能、安全性能的数据, 都需要进行隐私保护和安全加密[109]. 因此, 在数据共享过程中如何保证数据的安全性和隐私性是当下具有挑战性的问题. 随着车辆数量的增加, 传统的基于人工智能的算法越来越难以应对大规模、分布式的车辆网络; 主要原因在于传统人工智能解决方案需要系统对于车辆等候时间进行精准预测, 而由于通信和隐私上的局限, 车主们可能不愿直接共享个人数据. 联邦学习作为新兴的计算范式, 在保护数据隐私的同时为车辆之间的数据共享提供了可行的解决方案. 但是通过分析从数据提供者上传的本地模型更新的参数, 仍然可以泄露私人信息, 并且当部分车辆节点执行恶意行为时, 将影响整个车联网系统的性能. 为此, Wang 等[110] 将区块链、差分隐私和移动边缘计算技术集成到联邦学习框架中, 在确保车联网安全有效的同时促进车辆间的数据共享. 具体来说, 其所设计的系统采用智能合约来对联合训练过程进行调度: 首先智能合约对参与节点进行身份认证, 并对所传模型参数进行筛选以确保模型的可靠性; 随后, 智能合约按预置评估标准, 将参与节点上传的模型参数量化为总权重, 并以此作为联邦任务利润分配的标准. Posner 等[111] 基于区块链来优化联邦学习系统, 用于分析处理车辆通信网络, 其以去中心化方式在每个车辆间更新验证车载机器学习模型参数, 通过利用区块链的共识机制, 无需任何数据中心来协调即可实现车载机器学习. Chai 等[112] 提出利用层次化区块链框架和层次化联邦学习算法来进行机器学习模型参数共享, 这种分层 BeFL 架构可以使车辆获得更多的环境数据, 特别适用于大规模车载网络.

3.4 智慧城市

数据是智慧城市建设的重要因素. 在应用人工智能技术建设智慧城市的过程中, 存在数据利用率低、模型精确度低等问题, 其原因在于城市数据由许多数据孤岛组成, 例如交通数据、产业数据和居民数据等. 如何解决数据孤岛间的数据共享问题, 提供更安全可信的数据服务是智慧城市建设必须面对的问题. 联邦学习允许不同参与方共同训练模型, 而无需共享原始数据. 这解决了敏感数据隐私问题. 然而, 有些场景下需要跨组织或跨城市的数据共享, 而区块链可以提供一种安全且可信任的方式来实现跨组织之间的数据交换. 区块链技术可以记录数据交换的历史, 确保数据来源和使用透明, 从而促进更多组织之间的数据合作. 联邦学习在模型更新的过程中涉及多个参与方, 但在这个过程中, 有可能出现某些恶意参与方试图篡改模型或提供错误的更新. 在这种情况下, 区块链可以用来记录模型的更新历史, 保证参与方的行为被公开验证, 从而增加整个过程的信任度. 它们结合在智慧城市中可以为跨组织数据合作提供更安全、透明和可信的框架. 因此, 基于 BeFL 可以有效地构建智慧城市数据安全共享机制, 并且有助于解决智慧城市数据复杂性不断增加、环境不断变化以及传统安全攻击等问题[113−116]. 例如, 可以基于 BeFL, 通过人工智能算法来对工业物联网系统中的网络流量进行智能分类, 以识别敌手攻击引起的网络异常[117].

3.5 移动网络

数字孪生和第六代网络 (6G) 等新兴技术已经加速了工业物联网中边缘智能的实现. 数字孪生和 6G 的集成在物理系统和数字空间之间架起了桥梁, 并实现了强大的即时无线连接. 随着对数据隐私的日益关注, 联邦学习已被视为在无线网络中部署分布式数据处理和学习的重要解决方案. 但是, 不可靠的通信渠道、有限的资源以及用户之间缺乏信任, 阻碍了联邦学习在移动网络中的有效应用. 结合区块链来改进联邦学习框架, 可以提高系统的可靠性和安全性、增强数据隐私性. 同时, 随着网络规模的

扩大, 如何优化网络并分配有限的资源来提供高效率、高质量的服务, 是需要重点解决的关键问题. BeFL 可以结合经济激励机制来综合考虑数字孪生与边际服务器关联数量、训练数据批量大小和带宽分配等各方面因素, 并在联合训练中利用共识机制对参与节点进行选择以提高系统的效率. 现有的 BeFL 研究已经提出采用强化学习和异步聚合等方案来提高运行效率, 但仍需要作进一步研究[118−119].

4 进一步研究的问题

区块链与联邦学习的融合虽然可以有效缓解后者所面临的部分挑战, 然而却并未完全解决联邦学习系统固有的效率、异构、博弈和安全问题. 通过对 BeFL 架构常用的模型、区块链平台、数据集和评估标准的归纳整理 (如表 3 所示), 本节将概述这些有待进一步研究的问题 (如表 4 所示), 并给出现有文献中的解决方案.

4.1 BeFL 架构的效率问题

与传统的联邦学习相比, BeFL 需要考虑区块链共识过程引起的性能损失和时间延迟, 这将导致严重的效率问题. 首先, 当训练节点是需要高度动态实时性的设备 (例如智能车或无人机) 时, 其高效共识必然面临着更大的计算和通信资源挑战; 其次, 虽然一些深度学习模型可以融合到 BeFL 架构中来, 但是较深的深度学习模型需要存储更多可学习的参数来进行模型融合. 因此, 与集中式联邦学习方法相比, BeFL 的计算开销仍将受到限制. 最后, 机器学习不需要强共识或一致性即可收敛, 因此常用的实用拜占庭容错 (Practical Byzantine fault-tolerance, PBFT) 等强共识协议对于机器学习工作负载而言就显得过于严格. 现有研究中常用的模型有 NN/CNN/MLP, 但是模型层数浅、大模型部署难、训练收敛速度慢; 采用的区块链平台大多是 Hyperledger Fabric 和 Ethereum; 效率评估标准则通常包括模型准确率、区块生成时间和运行时间等. 本节将概述现有研究中提升效率的三种主要方法, 其主要目的是提升模型训练精度、减少通信和计算开销、优化系统运行和模型训练效率.

4.1.1 调整区块生成率

实际运行中, 数据区块的生成率会受到诸多因素的影响, 需要综合考虑通信、算力和共识延迟等因素来构建和优化端到端的模型[92]. 在优化方法方面, 可以结合系统动力学来对端到端的延迟作量化分析, 并通过考虑 BeFL 架构中系统延迟与优化目标值之间的偏差, 实现在实际网络条件下动态调整区块生成率[120−121]. 此外, 与深度强化学习等人工智能技术相结合来确定区块生成率, 也可以减少能耗、提高系统运行效率[68].

4.1.2 压缩梯度和模型

梯度压缩是分布式机器学习中常用的减少通信负载的方法. 除了能提高运行效率外, 梯度压缩还可以保护隐私. BeFL 架构中可以采用梯度压缩方案来生成稀疏但重要的梯度, 压缩边缘节点上传的梯度来减少通信所需的时间, 可以在不影响准确性的情况下减少通信开销, 从而加快联邦学习的训练过程, 并进一步加强训练数据的隐私保护[122−123]. 模型压缩是深度学习的另一个研究要点, 旨在降低模型的复杂度, 使算法运行更稳定高效. 为了提高 BeFL 架构中的建模效率问题, 可采用知识蒸馏等模型压缩技术, 并结合联邦学习的聚合算法, 在区块链网络进行参数广播之前实施模型压缩, 从而减少整个区块链网络的负载, 提高系统建模的效率[124].

4.1.3 采用双链架构

一方面, 在公有链上采用智能合约实施模型汇总和奖惩机制将会极大地减慢联邦学习进程, 并且在以太坊等公有链上发送模型会导致客户端和服务器双方产生昂贵的成本; 另一方面, 采用联盟链 (或私有链) 的通信效率很高, 并且仅允许一组经过授权的参与者查看敏感数据, 因而有助于解决数据隐私问题. 因此, 采用公有链+联盟链混合架构, 在联盟链上执行聚合并在公有链上执行奖惩机制, 既保持了算法的通信效率, 同时也降低了运行成本[69, 125−126].

4.2 BeFL 架构的异构问题

与运行在云端的分布式机器学习不同, BeFL 面临着严峻的异构性挑战. 由于在区块链中允许参与节点自由地加入和退出训练过程, 而参与者类型是多样的, 可以是传感器、雾节点、云服务提供商等, 并且在参与训练时所拥有的数据特征维度也各不相同, 这种异构性导致训练节点提供和接收的更新模型会非常多样化, 算法的收敛性能也会较差. 现有研究常用的数据集有 MNIST/CIFAR-10, 而较少使用可划分为非独立同分布的复杂异构数据集如 Federated-MINST\Shakespeare; 在真实场景中, 因不同的本地数据类型和参与者的复杂性将会引发数据、模型和网络资源层面的异构问题.

4.2.1 数据异构

训练模型的数据通常是非独立同分布的, 这既是联邦学习的特征也是其面临的挑战. 在联邦学习中有许多数据异构方面的研究, 例如通过在所有边缘设备之间全局共享一小部分数据来改进对非独立

表 3 BeFL 架构实验设计

Table 3 Experimental design of the BeFL architecture

文献	训练模型	区块链平台	数据集	评估标准
[20]	CNN/MLP	区块链仿真平台	MNIST/CIFAR-10	模型准确率
[29]	CNN	Ethereum	MNIST/CIFAR-10	模型准确率
[31]	NN/CNN	Ethereum	私有数据集	任务分类准确率
[32]	NN	许可链	私有数据集	AUC/准确率/灵敏度/特异性/F1 得分
[34]	GCN	许可链	路透社数据集/新闻组数据集	AUC/安全性分析/模型准确率/运行时间
[37]	MLP	区块链仿真平台	MNIST	模型准确率
[38]	NN	Hyperledger Fabric	MNIST	模型准确率
[39]	CNN	区块链仿真平台	MNIST	模型准确率
[40]	CNN	EOSIO 区块链	MNIST/CIFAR-10	运行时间/模型准确率
[41]	LDA	区块链仿真平台	单词数据集	网络中延迟的节点数
[42]	CNN	Corda V3.0	MNIST	密码大小/吞吐量/训练精度/总时间成本
[43]	AlexNet	FISCO BCOS	FEMNIST	模型准确率
[46]	/	区块链仿真平台	MNIST	搬土距离/区块生成时间/准确率
[47]	LR	区块链仿真平台	手写体数字光学识别数据集	余弦相似度/运行时间
[48]	/	Hyperledger Fabric	MNIST	模型准确率
[49]	MLP/VGG11	区块链仿真平台	MNIST/Fashion-MNIST	损失函数/准确率
[52]	NN	Truffle	威斯康星州乳腺癌数据集 (BCWD)/心脏病数据集 (HDD)	测试精度/时间开销/通信开销
[53]	CNN	联盟链	MNIST	测试准确率/训练时间
[57]	/	联盟链	MNIST	搬土距离/准确率
[61]	ResNet50/GhostNet	联盟链	X 激光图片数据集	损失函数/准确率
[62]	XGBoost	Ethereum	交易和源代码数据集	精准度/召回率/F1 得分
[67]	DNN	Ethereum	出租车运行数据	效益分析/燃气费/运行时间
[69]	CNN	许可链/DAG	MNIST	损失函数/模型准确率/累计消耗时间/标准化即时奖励
[70]	CNN	区块链仿真平台	MNIST	平均作用时间/训练时间/模型准确率
[71]	NN	Ethereum	私有数据	损失函数/模型准确率
[77]	NN	区块链仿真平台	MNIST	模型准确率
[78]	NN	私有链	私有采集数据集	分类交叉熵损失/模型准确率
[79]	AlexNet	Ethereum	MNIST/CIFAR-10	模型准确率/搬土距离
[82]	CNN/MLP	私有链	MNIST	测试准确率
[83]	CNN	区块链仿真平台	公有数据集/MNIST	模型准确率/迭代次数
[84]	LR	区块链仿真平台	合成数据/眼状态数据集	模型推理运行时间
[86]	LR	区块链仿真平台	信用卡数据集/MNIST/CIFAR-10 人脸数据集	测试误差/每次迭代的平均时间/攻击率
[87]	LR	Ethereum	成人人口普查收入数据	F1 得分

注: NN: 神经网络, CNN: 卷积神经网络, DNN: 深度神经网络, MLP: 多层感知机, LR: 逻辑回归, GCN: 图卷积神经网络, LDA: 文档主题生成模型, XGBoost: 分布式梯度增强库, AUC: 曲线下面积, ResNet50: 一种残差神经网络, GhostNet: 一种端侧神经网络架构.

同分布数据的训练, 设计一些优化算法来保证模型在使用异构数据训练时稳定收敛等. BeFL 研究中, Zhang 等[127] 为了解决工业物联网故障检测中的数据异构问题, 基于区块链和联邦学习设计了一个平台体系结构, 提出了一种质心距离加权联合平均算法; 为了生成无偏全局模型, 在权重计算中考虑了每个客户端数据集的正类与负类之间的距离, 一定程度上解决了 BeFL 的数据异构问题.

4.2.2 模型异构

联邦学习和 BeFL 模型均需要根据各方提供的数据源来训练主模型或全局模型, 并要求局部模型是同构的. 但是, 实际中每一方都基于自己的本地数据来训练模型, 因而异构模型以及基于异构模型的联邦学习在实际应用中可能更普遍. 为此, Wang

表 4　关键问题与未来方向

Table 4　Key issues and future directions

		研究要点	研究内容	代表文献
关键问题	效率	调整区块生成率	在通信、算力和共识延迟之间权衡	[68, 93, 120−121]
		压缩梯度和模型	压缩梯度和模型以减少通信开销	[122−124]
		采用双链架构	联盟链上执行聚合, 公链上实施奖惩	[69, 125−126]
	异构	数据异构	设计优化算法处理非独立同分布的联合训练数据	[127]
		模型异构	使 BeFL 架构满足参与节点, 依据需求选取不同的模型来参与联合训练	[128]
		网络资源异构	处理各参与节点网络环境和网络资源不同而引发的可靠交互问题	[129]
	博弈	共识与激励机制设计	依据博弈论来设计共识算法, 经济激励机制等	[45−47, 50]
		系统性能分析	依据博弈论对 BeFL 在计算开销、通信成本、系统效率之间做权衡	[95]
		参与节点竞合分析	在信息不对等时, 利用博弈论来对参与节点进行竞合分析	[130−133]
	安全	节点可信	利用身份认证和敌手节点阈值分析来确保节点可信	[134−135]
		数据安全	对智能合约数据、参与方本地模型数据和存储设备上的数据进行安全保护	[136−138]
		系统安全	对计算环境、通信环境和智能合约运行环境进行安全保护	[139−140]
未来方向	数据要素市场	参与对象	对于数据要素市场的参与对象进行划分	[126, 141]
		交易机制	数据竞价定价机制, 确保成交价最优	[142]
		供需情况	考虑算力、模型、数据三者之间的供需情况来构建市场模型	[143]
	与新一代人工智能技术集成	推荐模型	利用 BeFL 架构隐私保护和去中心化特点增强推荐模型	[144−146]
		搜索模型	集成 BeFL 增强搜索模型对于去中心化存储和加密数据查询分析需求	[52, 147]
		AIGC 模型	结合 BeFL 架构激励用户参与并贡献数据来提升 AIGC 模型	[148−149]
	隐私与监管	隐私与监管的权衡	在多方参与弱信任环境中利用区块链监管计算流程	[150]
	量子计算带来的机遇与挑战	量子数据安全共享	利用区块链和联邦学习可以使量子数据留在本地, 有效防止中心节点故障, 并实现量子数据的安全共享	[151−153]
	未来数字空间元宇宙中的应用	数据协作和价值共享	利用区块链的去中心化信任机制与联邦学习的隐私保护属性, 在元宇宙不同平台、应用、空间之间实现数据协作和价值交换	[154−161]

等[128] 提出了基于区块链的去中心化安全多方学习 (Blockchain-empowered decentralized secure multiparty learning, BEMA) 系统, 该系统将分布式多方学习扩展到去中心化结构之中, 允许每个参与节点都持有异构的本地模型并进行训练, 增强了 BeFL 架构的有效性和可靠性.

4.2.3　网络资源异构

由于网络环境的时变性和网络资源的异构性, 边缘设备与边缘服务器之间很难实现稳定、可靠和实时的交互, 这在 5G 超密集网络环境中尤为明显. 为此, Yu 等[129] 提出智能超密集边缘计算框架, 将区块链和联邦学习技术集成到 5G 超密集边缘计算网络中, 并且制定了超密集边缘计算的异构网络资源和混合计算分流模式. 该框架为了最大程度地减少任务执行时间和网络资源使用, 在两个不同的时间范围内优化了应用程序分区、资源分配和服务缓存配置机制, 实验结果证实了该计算框架的有效性.

4.3　BeFL 架构的博弈问题

博弈论是设计 BeFL 架构和机制的重要工具. 首先, 博弈论可用于改进 BeFL 的共识机制. BeFL 可依据节点数据质量以及节点参与联合训练的贡献度和积极性等参数, 基于博弈和机制设计理论来设计共识算法. 例如, 根据合作博弈理论来衡量每个节点在联合训练中所作的贡献[46−47]; 基于拍卖模型的激励相容博弈分析, 促使理性节点都能遵循协议并最大限度地提高它们的利润[50]; 依据机制设计理论, 将联邦学习的实际任务求解过程集成到区块链的共识算法 (如 PoW) 中[45].

其次, 博弈论可以使得 BeFL 架构在各方面限制条件下达到某种均衡状态. 例如, 当需要部署防御机制以检查敌手是否攻击 BeFL 架构时, 服务器将产生联合训练之外的额外计算成本. 通常来说, 不同的防御机制对于各种攻击具有不同的效力和成本, 这就需要结合博弈论来优化部署防御机制. 博弈论还可以用来模拟设备与服务器之间的交互, 以在计算开销、通信成本之间确定最佳条件, 并据此来提高区块生成率[95]. 此外, 在隐私保护和效率之间也存在着类似的情况, 比如采用差分隐私时, 更高的私密性要求需要向数据添加更多的噪声, 与此同时通信成本也随之增加, 可以运用博弈论在私密

性和效率之间来做权衡优化.

最后, 由于 BeFL 架构降低了联合训练的准入门槛, 可以吸引更多的用户加入联合学习过程, 运用博弈论可以分析用户节点在联合训练时的竞合情况[130−133].

4.4 BeFL 架构的安全问题

引入区块链技术虽然一定程度上缓解了联邦学习所面临的安全威胁, 然而 BeFL 本身仍然存在诸多安全挑战. 现有文献主要探讨的 BeFL 架构安全问题包括节点可信、数据安全和系统安全等.

节点可信对于 BeFL 安全构建是十分重要的. 例如, 敌手节点可以采用投毒攻击、推理攻击等手段来破坏全局模型并侵犯其余节点隐私, 而诚实节点可以贡献自己的高质量数据并维护系统健康稳定运行. BeFL 架构研究主要采用两种方法确保节点可信: 一是利用身份认证来确保参与者身份的真实性, 常用身份认证方法主要有基于对称密码学的、使用票据认证的 Kerberos 协议和基于公钥密码学的公钥基础设施 (Public key infrastructure, PKI) 系统, 以期在多重验证的机制下保证用户秘钥身份的唯一性, 从而缓解敌手攻击和保证节点共享数据的可信性[134]; 二是对于敌手节点占多少比例的阈值进行分析, 并由此来设计相应的共识激励机制算法以确保整个系统的安全性[135].

除联邦计算过程中需要采用同态加密、差分隐私等方式进行隐私保护外, 数据安全还体现在参与方将数据上传至智能合约后的数据安全、参与方本地的模型数据安全以及数据在计算设备上的存储安全. 在智能合约的数据安全研究中, Kosba 等[136] 提出了一个隐私保护智能合约开发框架 Hawk. 在 Hawk 中, 智能合约分为私密合约和公共合约, 私人数据和相关财务信息写入私密合约后只有合约拥有者可见. 此外, Zhang 等[137] 提出了一种可信数据输入系统 Town Crier, 合约在发送请求之前用 Town Crier 的公钥加密请求, Town Crier 收到请求后利用私钥解密, 从而保证区块链中其他用户无法查看请求内容. 参与方本地的模型数据安全主要是保护联邦模型的所有权, 对此, Li 等[138] 提出的 FedIPR 提出了一种基于特征和基于后门的水印嵌入和验证方案, 旨在不泄露多方私有训练数据或水印信息的情况下, 嵌入和验证私有水印. FedIPR 是在安全联邦学习环境中保护联邦模型所有权的技术解决方案, 通过理论分析和实验结果证明了水印的有效性、可靠性和鲁棒性, 并且有助于检测和排除联邦学习中的搭便车者. 数据存储安全通常以加密存储的方式实现, 采用基于属性的加密 (Attribute based encryption, ABE) 和代理重加密 (Proxy re-encryption, PRE) 来存储加密密钥和对关键数据进行访问控制, 从而确保数据存储安全.

系统安全主要体现在计算环境安全、智能合约运行安全以及通信安全. 计算环境安全包括执行环境的隔离、应用的完整性以及数据的机密性等, 通常采用英特尔的 SGX (Software guard extentions) 等底层硬件可信执行环境来维护计算环境安全[139]. 智能合约运行安全在于已部署上链的智能合约是不可逆转的, 其潜在的安全问题一旦引发就难以被修复. 为此, Chen 等[140] 提出了一个名为 Gasper 的智能合约高耗燃操作检测工具, 可自动发现死代码、无用描述和昂贵的循环操作等. BeFL 架构的通信安全在于不论是采用同态加密或是不经意传输, 都应在传输中保证通信机密性和传输数据完整性, 常用的方式为使用洋葱路由 (Onion router) 来保护通信双方的通信关系和 IP 地址等用户身份信息、使用 TLS (Transport layer security) 协议和 DTLS (Datagram transport layer security) 协议来确保网络传输安全和上传数据安全.

5 未来研究方向

区块链与联邦学习的深度融合必将催生或赋能一些新模式和新业态, 并衍生出新的研究机遇和方向. 本节将简要探讨基于 BeFL 的数据要素市场、博弈分析与机制设计、隐私与监管的权衡、量子计算以及新一代元宇宙数字空间对 BeFL 的潜在影响等目前已初现端倪的潜在方向.

5.1 基于 BeFL 的数据要素市场

无论是对于企业或政府来说, 数据都是非常有价值的数字资产, 尤其是在互联网行业中, 机器学习模型的训练依赖于大量的数据. 然而, 随着数据隐私保护法规的推进和人们对于数据隐私保护的重视程度越来越高, 数据将会保留在机构和个人本地设备上而不是共享在云端. 在此情况下, 数据要素市场将是促进数据要素共享和价值流通的有效方案.

BeFL 有望解决数据要素市场所面临的一些技术挑战. 首先, 数据不同于其他资产, 当数据所有者交易数据后, 数据所有者将失去其资产所有权, 并且无法以可持续的方式从其资产中获取价值. 其次, 集中式的数据市场依赖于一个信任中央实体来维护数据共享, 这可能造成数据垄断并侵犯用户隐私. 基于 BeFL 架构的数据要素市场可以在去中心化的数据市场中保留数据资产的隐私和所有权, 并且满足买卖双方对拟交易的数据资产的信息透明度以及信任需求[141].

现阶段, 数据要素市场面临的主要问题是: 哪些要素 (数据、模型或算力等) 会参与市场交易; 买卖双方的供需匹配会在什么样的情况下产生; 数据要素交易过程中如何有效定价; 采用何种机制来保障市场公平有序运行等. 现有文献在这些方面做了初步的研究.

Fan 等[126] 基于 BeFL 设计的数据要素市场结合了公有区块链和联盟区块链的优势, 提出了一种基于混合区块链的资源交易系统, 可以在基础架构上减少系统延迟; 同时, 该系统采用反向拍卖机制, 用支付渠道技术来实现请求者和边缘节点之间的可信、快速、低成本和高频支付交易. Somy 等[142] 在 BeFL 构建的市场中考虑了三类市场参与者: 数据所有者、模型开发者和云所有者, 并在区块链系统中提供可验证的数据来解决纠纷. 对于数据要素市场的供需关系, Ouyang 等[143] 考虑交易可能发生在多个算力所有者需要访问同一组数据的情况, 基于以太坊智能合约来协调多个算力所有者, 并自动化实施模型调度和奖惩激励.

5.2 与新一代人工智能模型集成

基于 BeFL 架构来集成大规模智能模型和算法, 将会成为新一代人工智能落地应用的重要发展趋势, 并为近年来快速发展的 Web3 生态奠定坚实的数据和信任基础[144]. 现阶段的主要结合点包括基于 BeFL 的智能推荐模型、基于 BeFL 的新一代搜索模型以及基于 BeFL 的人工智能生成内容 (Artificial intelligence generated content, AIGC) 模型等.

基于 BeFL 的智能推荐模型旨在解决目前推荐系统的中心化架构带来的弱隐私保护问题, 利用 BeFL 架构来认证参与用户的身份并对推荐客户端进行选择以确保推荐项目的可信性[145−146]. 根据 BeFL 隐私保护机制, 客户端收集本地用户行为数据 (如网页点击数据和收藏数据等) 并在数据不出本地的限制下协同进行模型训练, 从而构建联合推荐模型, 以解决在保护数据隐私情况下推荐效果差的技术问题.

基于 BeFL 架构的搜索模型亦有广泛需求: 一方面, 针对用户数据分布式存储在本地服务器的场景, 需构建去中心化和强安全隐私的联合搜索模型; 另一方面, 随着区块链技术的广泛应用, 不同用户以及区块链之间也同样存在着数据查询和统计分析等业务需求. 因此, 基于 BeFL 架构集成搜索模型, 可以利用区块链基础存储文件的密文和搜索的索引, 对参与节点进行筛选验证、利用智能合约进行搜索服务以对加密数据实现安全可信搜索, 同时利用联邦学习技术来处理异质数据并对搜索结果进行分析, 以适应用户对于搜索服务的个性化需求[52, 147].

AIGC 是继专业生产内容、用户生产内容之后的新型内容创作方式, 其发展离不开用户高质量的数据贡献和积极参与. 基于 BeFL 架构的 AIGC 模型中, 可利用区块链技术将网络数据所有权及控制权交还给用户, 产生高度附着于用户的数字身份和数据资产, 并设计经济激励机制吸引用户参与和贡献数据; 同时, 利用联邦学习技术处理用户数据并适配 AIGC 模型训练, 以提升模型效果, 将是 AIGC 模型发展的趋势之一[148−149].

5.3 隐私与监管的权衡

数据隐私保护对于企业和个人至关重要. 欧盟颁布的 GDPR 坚持以强数据保护为前提, 但因此存在数据使用的监管盲区和随之而来的安全挑战. 因此, 必须在数据隐私保护与业务流程监管之间找到更合适的平衡点, 在保证数据安全的同时, 实现数据最大限度的合规利用.

实际中, 互联网企业及大数据企业在数据计算能力方面强于政府机构, 因此数据监管和治理通常需要一个多方参与且协同互信的环境. 如何在这种多方参与的协同监管环境中实现各方数据的隐私保护, 并在此基础上面向多方弱信任环境实现监管数据的主动共享与激励、跨部门监管业务的可信集成与冲突协商以及跨链监管协同与监管服务, 进而实现多方主动协同监管与隐私保护的高效平衡, 是亟待解决的关键技术问题.

因此, 需要结合区块链和以联邦学习为代表的隐私计算技术来针对多监管主体、弱信任环境中的协同监管与数据共享需求[150], 设计跨行业、跨部门多方监管规范和冲突协商技术, 研究监管数据的主动共享与激励机制设计方法, 设计监管数据的隐私保护机制, 支撑主动、可信的监管协同与数据共享.

5.4 量子计算带来的机遇与挑战

量子计算是遵循量子力学规律调控量子信息单元进行计算的新型计算模式. 现有的量子计算机在计算效率上要优于传统的计算机, 用量子的训练方法代替经典的机器学习算法在计算效率和安全等方面取得了良好的效果. 同时, 量子数据隐私和传输效率是进行大规模量子机器学习时所应考量的问题. 结合联邦学习这一新型计算范式, 可以有效解决量子数据隐私和传输效率等问题[151−153]. 但不可避免地, 量子联邦学习同样面临着中心节点故障等传统问题.

因此, 随着量子计算的发展, 结合区块链与联邦学习技术, 设计一个基于区块链的量子联邦学习计算框架, 不仅可以使得量子机器学习模型在量子

客户端之间进行分布式量子学习, 并且无需传输量子数据本身, 还可以有效抵御中心节点故障、提高分布式量子计算资源的协作效率、加速量子计算机的应用进程.

与此同时, 量子计算是区块链底层加密体系的潜在威胁. 随着通用容错量子计算机研发进程的加速, 基于数学困难问题的传统哈希算法和非对称加密算法面临着攻击难度减半或完全攻破的风险. 因此, 研究者相继提出基于编码问题、格问题等抗量子密码算法的抗量子区块链模式, 以及基于量子密钥分发和一次一密等量子密码体系的量子区块链模式, 来应对量子计算的潜在威胁. 通常来说, 抗量子区块链模式更适用并已逐渐融入现有的公有链体系, 而量子区块链模式则更适用于具有量子能力和固定节点的联盟链体系.

5.5 未来数字空间–元宇宙中的应用

随着元宇宙概念的兴起, 作为其重要技术基础的区块链和联邦学习受到广泛关注. 区块链的去中心化信任机制与联邦学习的隐私保护特性, 可有效解决数字世界的身份割裂、数据隔离、权益流失等问题, 是构建开放、公平、可信元宇宙的基石. 因此, BeFL 架构有助于实现不同元宇宙平台、应用、空间的数据协作和价值交换, 并解决元宇宙愿景中的若干关键问题[154].

首先, BeFL 架构可以赋能用户数字身份和资产的自主管理. 用户在元宇宙中需要一个可以跨平台、应用、空间的统一数字身份, 以及可以创造、确权和流通的数字资产, 如虚拟土地、游戏装备、艺术品等. 传统互联网中的身份识别与管理机制存在中心化和碎片化问题, 用户难以真正拥有与控制自己的数字身份. BeFL 架构可以利用区块链为用户提供一个去中心化的账本系统, 支持用户使用隐私计算技术建立和验证自己的数字身份, 并以非同质化代币 (Non-fungible token, NFT) 的形式记录和交易自己的数字资产[155].

其次, BeFL 架构可以实现元宇宙中用户数据协作和交互时的隐私保护和信任保障. 用户在元宇宙中需要提供大量个人数据, 如位置、偏好、行为等, 以实现更真实和沉浸式的体验. 直接共享这些敏感数据会暴露用户隐私. BeFL 架构可以为用户提供一个保护隐私的数据协作和交互系统, 允许用户在本地节点上训练机器学习模型, 并只交换模型参数, 而不是原始数据. 此外 BeFL 架构可以为用户提供一个去中心化的信任机制, 支持用户使用密码学机制验证和记录模型参数的交换过程, 防止篡改和欺诈[156−157].

最后, BeFL 架构可以构建元宇宙中的新型经济体系与社区治理结构. 用户在元宇宙中需要一个可以衡量自己贡献的经济体系, 以及一个可以参与和影响元宇宙发展方向的社区治理结构. 区块链可以为用户提供一个价值交换系统, 支持用户使用加密数字货币进行支付和奖励, 并以智能合约的形式定义和执行各种规则和协议. 联邦学习可以为用户提供一个数据协作系统, 支持用户使用机器学习模型进行知识共享和创新, 并以 DAO 的形式实现民主化治理[158−161].

6 结束语

区块链与联邦学习的集成创新是新一代信息技术发展的重要趋势之一. 本文提出了 BeFL 的概念模型, 阐述了 BeFL 的基本工作流程, 并从基础架构、共识机制、经济激励、智能合约、隐私保护和应用领域 6 个维度论述了该领域的关键研究问题和现有研究进展. 本文同时探讨了 BeFL 的开放研究问题和应用场景. 需要指出的是, 区块链与联邦学习的结合还处于起步阶段, 面临着崭新的发展机遇和严峻的研究挑战, 需要结合更多的研究领域和应用场景来加以探讨. 期待本文可为未来的研究提供有益的参考与借鉴.

References

1 Antunes R S, André da Costa C, Küderle A, Yari I A, Eskofier B. Federated learning for healthcare: Systematic review and architecture proposal. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2022, **13**(4): 1–23

2 Ghimire B, Rawat D B. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for internet of things. *IEEE Internet of Things Journal*, 2022, **9**(11): 8229–8249

3 Nguyen D C, Pham Q V, Pathirana P N, Ding M, Seneviratne A, Lin Z H, et al. Federated learning for smart healthcare: A survey. *ACM Computing Surveys (CSUR)*, 2023, **55**(3): 1–37

4 Cheung D W, Ng V T, Fu A W, Fu Y J. Efficient mining of association rules in distributed databases. *IEEE Transactions on Knowledge and Data Engineering*, 1996, **8**(6): 911–922

5 Konečný J, McMahan H B, Yu F X, Richtárik P, Suresh A T, Bacon D. Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv: 1610.05492, 2016.

6 Tan B, Zhang Y, Pan S, Yang Q. Distant domain transfer learning. In: Proceedings of the 31st AAAI Conference on Artificial Intelligence. San Francisco, USA: AAAI, 2017. 2604–2610

7 Liu Y, Kang Y, Xing C P, Chen T J, Yang Q. A secure federated transfer learning framework. *IEEE Intelligent Systems*, 2020, **35**(4): 70–82

8 Yang Q, Liu Y, Chen T J, Tong Y X. Federated machine learning: Concept and applications. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 2019, **10**(2): Article No. 20

9 Kairouz P, McMahan H B, Avent B, Bellet A, Bennis M, Bhagoji A N, et al. Advances and open problems in federated learning. *Foundations and Trends® in Machine Learning*, 2019, **11**(1–2): 1–210

10 Mothukuri V, Parizi R M, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G. A survey on security and privacy of federated learning. *Future Generation Computer Systems*, 2021, **115**: 619–640

11 Li T, Sahu A K, Talwalkar A, Smith V. Federated learning:

Challenges, methods, and future directions. *IEEE Signal Processing Magazine*, 2020, **37**(3): 50−60

12 Zhao Y, Chen J J, Zhang J L, Wu D, Blumenstein M, Yu S. Detecting and mitigating poisoning attacks in federated learning using generative adversarial networks. *Concurrency and Computation: Practice and Experience*, 2022, **34**(7): Article No. e5906

13 Wang L P, Wang W, Li B. CMFL: Mitigating communication overhead for federated learning. In: Proceedings of the 39th International Conference on Distributed Computing Systems (ICDCS). Dallas, USA: IEEE, 2019. 954−964

14 Yuan Yong, Wang Fei-Yue. Blockchain: The state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

15 Whig P, Velu A, Sharma P. Demystifying federated learning for blockchain: A case study. *Demystifying Federated Learning for Blockchain and Industrial Internet of Things*. IGI Global Press, 2022. 143−165

16 Singh S, Rathore S, Alfarraj O, Tolba A, Yoon B. A framework for privacy-preservation of IoT healthcare data using federated learning and blockchain technology. *Future Generation Computer Systems*, 2022, **129**: 380−388

17 Miao Y B, Liu Z T, Li H W, Choo K K R, Deng R H. Privacy-preserving Byzantine-robust federated learning via blockchain systems. *IEEE Transactions on Information Forensics and Security*, 2022, **17**: 2848−2861

18 Shao Jun, Lin Jing-Ru. Research on the application of federated learning based on blockchain. *China New Telecommunications*, 2021, **23**(5): 124−125
(邵俊, 蔺静茹. 基于区块链的联邦学习应用研究. 中国新通信, 2021, **23**(5): 124−125)

19 Gao Sheng, Yuan Li-Ping, Zhu Jian-Ming, Ma Xin-Di, Zhang Rui, Ma Jian-Feng. A blockchain-based privacy-preserving asynchronous federated learning. *SCIENTIA SINICA Informationis*, 2021, **51**(10): 1755−1774
(高胜, 袁丽萍, 朱建明, 马鑫迪, 章睿, 马建峰. 一种基于区块链的隐私保护异步联邦学习. 中国科学: 信息科学, 2021, **51**(10): 1755−1774)

20 Nguyen D C, Ding M, Pham Q V, Pathirana P N, Le L B, Seneviratne A, et al. Federated learning meets blockchain in edge computing: Opportunities and challenges. *IEEE Internet of Things Journal*, 2021, **8**(16): 12806−12825

21 Ali M, Karimipour H, Tariq M. Integration of blockchain and federated learning for internet of things: Recent advances and future challenges. *Computers & Security*, 2021, **108**: Article No. 102355

22 Issa W, Moustafa N, Turnbull B, Sohrabi N, Tari Z. Blockchain-based federated learning for securing internet of things: A comprehensive survey. *ACM Computing Surveys*, 2023, **55**(9): Article No. 191

23 Zhu J C, Cao J N, Saxena D, Jiang S, Ferradi H. Blockchain-empowered federated learning: Challenges, solutions, and future directions. *ACM Computing Surveys*, 2023, **55**(11): Article No. 240

24 Javed A R, Hassan M A, Shahzad F, Ahmed W, Singh S, Baker T, et al. Integration of blockchain technology and federated learning in vehicular (IoT) networks: A comprehensive survey. *Sensors*, 2022, **22**(12): Article No. 4394

25 Qu Y Y, Uddin M P, Gan C Q, Xiang Y, Gao L X, Yearwood J. Blockchain-enabled federated learning: A survey. *ACM Computing Surveys*, 2023, **55**(4): Article No. 70

26 Li Ling-Xiao, Yuan Sha, Jin Yin-Yu. Review of blockchain-based federated learning. *Application Research of Computers*, 2021, **38**(11): 3222−3230
(李凌霄, 袁莎, 金银玉. 基于区块链的联邦学习技术综述. 计算机应用研究, 2021, **38**(11): 3222−3230)

27 Sun Rui, Li Chao, Wang Wei, Tong En-Dong, Wang Jian, Liu Ji-Qiang. Research progress of blockchain-based federated learning. *Journal of Computer Applications*, 2022, **42**(11): 3413−3420
(孙睿, 李超, 王伟, 童恩栋, 王健, 刘吉强. 基于区块链的联邦学习研究进展. 计算机应用, 2022, **42**(11): 3413−3420)

28 Saraswat D, Verma A, Bhattacharya P, Tanwar S, Sharma G, Bokoro P N, et al. Blockchain-based federated learning in UAVs beyond 5G networks: A solution taxonomy and future directions. *IEEE Access*, 2022, **10**: 33154−33182

29 Hu Y F, Zhou Y H, Xiao J, Wu C. GFL: A decentralized federated learning framework based on blockchain. arXiv preprint arXiv: 2010.10996, 2020.

30 Ma C, Li J, Shi L, Ding M, Wang T T, Han Z, et al. When federated learning meets blockchain: A new distributed learning paradigm. *IEEE Computational Intelligence Magazine*, 2022, **17**(3): 26−33

31 Mendis G J, Sabounchi M, Wei J, Roche′ R. Blockchain as a service: An autonomous, privacy preserving, decentralized architecture for deep learning. arXiv preprint arXiv: 1807.02515, 2018.

32 Warnat-Herresthal S, Schultze H, Shastry K L, Manamohan S, Mukherjee S, Garg V, et al. Swarm learning for decentralized and confidential clinical machine learning. *Nature*, 2021, **594**(7862): 265−270

33 Kim H, Park J, Bennis M, Kim S L. Blockchained on-device federated learning. *IEEE Communications Letters*, 2020, **24**(6): 1279−1283

34 Lu Y L, Huang X H, Dai Y Y, Maharjan S, Zhang Y. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. *IEEE Transactions on Industrial Informatics*, 2020, **16**(6): 4177−4186

35 Yuan Yong, Ni Xiao-Chun, Zeng Shuai, Wang Fei-Yue. Blockchain consensus algorithms: The state of the art and future trends. *Acta Automatica Sinica*, 2018, **44**(11): 2011−2022
(袁勇, 倪晓春, 曾帅, 王飞跃. 区块链共识算法的发展现状与展望. 自动化学报, 2018, **44**(11): 2011−2022)

36 Zhang K S, Huang H W, Guo S, Zhou X C. Blockchain-based participant selection for federated learning. In: Proceedings of the 2nd International Conference on Blockchain and Trustworthy Systems. Dali, China: Springer, 2020. 112−125

37 Kim Y J, Hong C S. Blockchain-based node-aware dynamic weighting methods for improving federated learning performance. In: Proceedings of the 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). Matsue, Japan: IEEE, 2019. 1−4

38 Wu X, Wang Z, Zhao J, Zhang Y, Wu Y. FedBC: Blockchain-based decentralized federated learning. In: Proceedings of the IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA). Dalian, China: IEEE, 2020. 217−221

39 Chen H, Asif S A, Park J, Shen C C, Bennis M. Robust blockchained federated learning with model validation and proof-of-stake inspired consensus. arXiv preprint arXiv: 2101.03300, 2021.

40 Kang J W, Xiong Z H, Jiang C X, Liu Y, Guo S, Zhang Y, et al. Scalable and communication-efficient decentralized federated edge learning with multi-blockchain framework. In: Proceedings of the 2nd International Conference on Blockchain and Trustworthy Systems. Dali, China: Springer, 2020. 152−165

41 Doku R, Rawat D B. IFLBC: On the edge intelligence using federated learning blockchain network. In: Proceedings of the 6th International Conference on Big Data Security on Cloud (BigDataSecurity). Baltimore, USA: IEEE, 2020. 221−226

42 Weng J S, Weng J, Zhang J L, Li M, Zhang Y, Luo W Q. DeepChain: Auditable and privacy-preserving deep learning with blockchain-based incentive. *IEEE Transactions on Dependable and Secure Computing*, 2021, **18**(5): 2438−2455

43 Li Y Z, Chen C, Liu N, Huang H W, Zheng Z B, Yan Q. A blockchain-based decentralized federated learning framework with committee consensus. *IEEE Network*, 2021, **35**(1): 234−241

44 Kim D, Doh I, Chae K. Improved raft algorithm exploiting federated learning for private blockchain performance enhancement. In: Proceedings of the International Conference on Information Networking (ICOIN). Jeju Island, South Korea:

IEEE, 2021. 828−832

45 Qu X D, Wang S L, Hu Q, Cheng X Z. Proof of federated learning: A novel energy-recycling consensus algorithm. *IEEE Transactions on Parallel and Distributed Systems*, 2021, **32**(8): 2074−2085

46 Liu Y, Ai Z P, Sun S, Zhang S F, Liu Z L, Yu H. FedCoin: A peer-to-peer payment system for federated learning. *Federated Learning: Privacy and Incentive*. Cham: Springer, 2020. 125−138

47 Ma S C, Cao Y, Xiong L. Transparent contribution evaluation for secure federated learning on blockchain. In: Proceedings of the 37th International Conference on Data Engineering Workshops (ICDEW). Chania, Greece: IEEE, 2021. 88−91

48 Martinez I, Francis S, Hafid A S. Record and reward federated learning contributions with blockchain. In: Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). Guilin, China: IEEE, 2019. 50−57

49 Li J, Shao Y M, Wei K, Ding M, Ma C, Shi L, et al. Blockchain assisted decentralized federated learning (BLADE-FL): Performance analysis and resource allocation. *IEEE Transactions on Parallel and Distributed Systems*, 2022, **33**(10): 2401−2415

50 Toyoda K, Zhang A N. Mechanism design for an incentive-aware blockchain-enabled federated learning platform. In: Proceedings of the IEEE International Conference on Big Data (Big Data). Los Angeles, USA: IEEE, 2019. 395−403

51 Pandey S R, Tran N H, Bennis M, Tun Y K, Manzoor A, Hong C S. A crowdsourcing framework for on-device federated learning. *IEEE Transactions on Wireless Communications*, 2020, **19**(5): 3241−3256

52 Li Z Y, Liu J, Hao J L, Wang H M, Xian M. CrowdSFL: A secure crowd computing framework based on blockchain and federated learning. *Electronics*, 2020, **9**(5): Article No. 773

53 Zhao Y, Zhao J, Jiang L S, Tan R, Niyato D, Li Z X, et al. Privacy-preserving blockchain-based federated learning for IoT devices. *IEEE Internet of Things Journal*, 2021, **8**(3): 1817−1829

54 Cai H, Rueckert D, Passerat-Palmbach J. 2CP: Decentralized protocols to transparently evaluate contributivity in blockchain federated learning environments. arXiv preprint arXiv: 2011.07516, 2020.

55 ur Rehman M H, Salah K, Damiani E, Svetinovic D. Towards blockchain-based reputation-aware federated learning. In: Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Toronto, Canada: IEEE, 2020. 183−188

56 Kang J W, Xiong Z H, Niyato D, Zou Y Z, Zhang Y, Guizani M. Reliable federated learning for mobile networks. *IEEE Wireless Communications*, 2020, **27**(2): 72−80

57 Kang J W, Xiong Z H, Niyato D, Xie S L, Zhang J S. Incentive mechanism for reliable federated learning: A joint optimization approach to combining reputation and contract theory. *IEEE Internet of Things Journal*, 2019, **6**(6): 10700−10714

58 Qi J H, Lin F L, Chen Z Y, Tang C B, Jia R H, Li M L. High-quality model aggregation for blockchain-based federated learning via reputation-motivated task participation. *IEEE Internet of Things Journal*, 2022, **9**(19): 18378−18391

59 Short A R, Leligou H C, Theocharis E. Execution of a federated learning process within a smart contract. In: Proceedings of the IEEE International Conference on Consumer Electronics (ICCE). Las Vegas, USA: IEEE, 2021. 1−4

60 Behera M R, Upadhyay S, Shetty S. Federated learning using smart contracts on blockchains, based on reward driven approach. arXiv preprint arXiv: 2107.10243, 2021.

61 Lo S K, Liu Y, Lu Q H, Wang C, Xu X W, Paik H Y, et al. Toward trustworthy AI: Blockchain-based architecture design for accountability and fairness of federated learning systems. *IEEE Internet of Things Journal*, 2023, **10**(4): 3276−3284

62 Chen W L, Zheng Z B, Cui J H, Ngai E, Zheng P L, Zhou Y R. Detecting ponzi schemes on ethereum: Towards healthier blockchain technology. In: Proceedings of the World Wide Web Conference. Lyon, France: ACM, 2018. 1409−1418

63 Hua G F, Zhu L, Wu J S, Shen C Z, Zhou L Y, Lin Q Q. Blockchain-based federated learning for intelligent control in heavy haul railway. *IEEE Access*, 2020, **8**: 176830−176839

64 Majeed U, Hong C S. Blockchain-assisted ensemble federated learning for automatic modulation classification in wireless networks. In: Proceedings of the Korean Network Operations and Management (KNOM). Daejeon, South Korea: 2020. 111−113

65 Preuveneers D, Rimmer V, Tsingenopoulos I, Spooren J, Joosen W, Ilie-Zudor E. Chained anomaly detection models for federated learning: An intrusion detection case study. *Applied Sciences*, 2018, **8**(12): Article No. 2663

66 Ren Tao, Jin Ruo-Chen, Luo Yong-Mei. Network intrusion detection algorithm integrating blockchain and federated learning. *Netinfo Security*, 2021, **21**(7): 27−34
(任涛, 金若辰, 罗咏梅. 融合区块链与联邦学习的网络入侵检测算法. 信息网络安全, 2021, **21**(7): 27−34)

67 Ramanan P, Nakayama K. BAFFLE: Blockchain based aggregator free federated learning. In: Proceedings of the IEEE International Conference on Blockchain (Blockchain). Rhodes, Greece: IEEE, 2020. 72−81

68 Hieu N Q, Anh T T, Luong N C, Niyato D, Kim D I, Elmroth E. Resource management for blockchain-enabled federated learning: A deep reinforcement learning approach. arXiv preprint arXiv: 2004.04104, 2020.

69 Lu Y L, Huang X H, Zhang K, Maharjan S, Zhang Y. Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles. *IEEE Transactions on Vehicular Technology*, 2020, **69**(4): 4298−4311

70 Połap D, Srivastava G, Yu K P. Agent architecture of an intelligent medical system based on federated learning and blockchain technology. *Journal of Information Security and Applications*, 2021, **58**: Article No. 102748

71 Zhang Z Z, Yang T Z, Liu Y. SABlockFL: A blockchain-based smart agent system architecture and its application in federated learning. *International Journal of Crowd Science*, 2020, **4**(2): 133−147

72 Liang J C, Li S Z, Jiang W S, Cao B C, He C Y. OmniLytics: A blockchain-based secure data market for decentralized machine learning. arXiv preprint arXiv: 2107.05252, 2021.

73 Wang Fei-Yue, Wang Yan-Fen, Chen Yi-Zhu, Tian Yong-Lin, Qi Hong-Wei, Wang Xiao, et al. Federated ecology: From federated data to federated intelligence. *Chinese Journal of Intelligent Science and Technology*, 2020, **2**(4): 305−311
(王飞跃, 王艳芬, 陈薏竹, 田永林, 齐红威, 王晓, 等. 联邦生态: 从联邦数据到联邦智能. 智能科学与技术学报, 2020, **2**(4): 305−311)

74 Lyu L J, Yu H, Yang Q. Threats to federated learning: A survey. arXiv preprint arXiv: 2003.02133, 2020.

75 Li Q B, Wen Z Y, Wu Z M, Hu S X, Wang N B, Li Y, et al. A survey on federated learning systems: Vision, hype and reality for data privacy and protection. *IEEE Transactions on Knowledge and Data Engineering*, 2023, **35**(4): 3347−3366

76 Zhou Jun, Fang Guo-Ying, Wu Nan. Survey on security and privacy-preserving in federated learning. *Journal of Xihua University (Natural Science Edition)*, 2020, **39**(4): 9−17
(周俊, 方国英, 吴楠. 联邦学习安全与隐私保护研究综述. 西华大学学报 (自然科学版), 2020, **39**(4): 9−17)

77 Short A R, Leligou H C, Papoutsidakis M, Theocharis E. Using blockchain technologies to improve security in federated learning systems. In: Proceedings of the 44th Annual Computers, Software, and Applications Conference (COMPSAC). Madrid, Spain: IEEE, 2020. 1183−1188

78 Yin B, Yin H, Wu Y L, Jiang Z X. FDC: A secure federated deep learning mechanism for data collaborations in the internet of things. *IEEE Internet of Things Journal*, 2020, **7**(7): 6348−6359

79 Liu Y, Peng J L, Kang J W, Iliyasu A M, Niyato D, El-Latif A A A. A secure federated learning framework for 5G networks. *IEEE Wireless Communications*, 2020, **27**(4): 24−31

80 Zhao Dong-Ming, Liu Jing, Xu Chen-Xing, Yang Ai-Dong, Kong Ling-Lu. Research on the "federated learning + blockchain" multi-party secure computation engine system. *Electronic Technology and Software Engineering*, 2020, (21): 184−186
(赵东明, 刘静, 徐晨兴, 杨爱东, 孔令鲁. "联邦学习+区块链"多方安全计算引擎系统研究. 电子技术与软件工程, 2020, (21): 184−186)

81 Zhu Jian-Ming, Zhang Qin-Nan, Gao Sheng, Ding Qing-Yang, Yuan Li-Ping. Privacy preserving and trustworthy federated learning model based on blockchain. *Chinese Journal of Computers*, 2021, **44**(12): 2464−2484
(朱建明, 张沁楠, 高胜, 丁庆洋, 袁丽萍. 基于区块链的隐私保护可信联邦学习模型. 计算机学报, 2021, **44**(12): 2464−2484)

82 Wei K, Li J, Ding M, Ma C, Yang H H, Farokhi F, et al. Federated learning with differential privacy: Algorithms and performance analysis. *IEEE Transactions on Information Forensics and Security*, 2020, **15**: 3454−3469

83 Lyu L, Yu J S, Nandakumar K, Li Y T, Ma X J, Jin J, et al. Towards fair and privacy-preserving federated deep models. *IEEE Transactions on Parallel and Distributed Systems*, 2020, **31**(11): 2524−2541

84 Shen M, Wang H, Zhang B, Zhu L H, Xu K, Li Q, et al. Exploiting unintended property leakage in blockchain-assisted federated learning for intelligent edge computing. *IEEE Internet of Things Journal*, 2021, **8**(4): 2265−2275

85 Fang C, Guo Y B, Ma J L, Xie H D, Wang Y F. A privacy-preserving and verifiable federated learning method based on blockchain. *Computer Communications*, 2022, **186**: 1−11

86 Kebande V R, Alawadi S, Bugeja J, Persson J A, Olsson C M. Leveraging federated learning & blockchain to counter adversarial attacks in incremental learning. In: Proceedings of the 10th International Conference on the Internet of Things. Malmö, Sweden: ACM, 2020. Article No. 2

87 Shayan M, Fung C, Yoon C J M, Beschastnikh I. Biscotti: A ledger for private and secure peer-to-peer machine learning. arXiv preprint arXiv: 1811.09904, 2018.

88 Mugunthan V, Rahman R, Kagal L. BlockFLow: An accountable and privacy-preserving solution for federated learning. arXiv preprint arXiv: 2007.03856, 2020.

89 Malomo O O. Cybersecurity Through a Blockchain Enabled Federated Cloud Framework. Howard University, USA, 2018.

90 Wang S F. BlockFedML: Blockchained federated machine learning systems. In: Proceedings of the International Conference on Intelligent Computing, Automation and Systems (ICICAS). Chongqing, China: IEEE, 2019. 751−756

91 Malomo O, Rawat D, Garuba M. Security through block vault in a blockchain enabled federated cloud framework. *Applied Network Science*, 2020, **5**(1): Article No. 16

92 Malomo O O, Rawat D B, Garuba M. Next-generation cybersecurity through a blockchain-enabled federated cloud framework. *The Journal of Supercomputing*, 2018, **74**(10): 5099−5126

93 Sharma P K, Park J H, Cho K. Blockchain and federated learning-based distributed computing defence framework for sustainable society. *Sustainable Cities and Society*, 2020, **59**: Article No. 102220

94 Fang Chen, Guo Yuan-Bo, Wang Yi-Feng, Hu Yong-Jin, Ma Jia-Li, Zhang Han, et al. Edge computing privacy protection method based on blockchain and federated learning. *Journal on Communications*, 2021, **42**(11): 28−40
(方晨, 郭渊博, 王一丰, 胡永进, 马佳利, 张晗, 等. 基于区块链和联邦学习的边缘计算隐私保护方法. 通信学报, 2021, **42**(11): 28−40)

95 Qu Y Y, Gao L X, Luan T H, Xiang Y, Yu S, Li B, et al. Decentralized privacy using blockchain-enabled federated learning in fog computing. *IEEE Internet of Things Journal*, 2020, **7**(6): 5171−5183

96 Majeed U, Hong C S. FLchain: Federated learning via MEC-enabled blockchain network. In: Proceedings of the 20th Asia-Pacific Network Operations and Management Symposium (APNOMS). Matsue, Japan: IEEE, 2019. 1−4

97 Połap D, Srivastava G, Jolfaei A, Parizi R M. Blockchain technology and neural networks for the internet of medical things. In: Proceedings of the IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). Toronto, Canada: IEEE, 2020. 508−513

98 Passerat-Palmbach J, Farnan T, McCoy M, Harris J D, Manion S T, Flannery H L, et al. Blockchain-orchestrated machine learning for privacy preserving federated learning in electronic health data. In: Proceedings of the IEEE International Conference on Blockchain (Blockchain). Rhodes, Greece: IEEE, 2020. 550−555

99 Aich S, Sinai N K, Kumar S, Ali M, Choi Y R, Joo M I, et al. Protecting personal healthcare record using blockchain & federated learning technologies. In: Proceedings of the 23rd International Conference on Advanced Communication Technology (ICACT). PyeongChang, South Korea: IEEE, 2021. 109−112

100 Vaid A, Jaladanki S K, Xu J, Teng S, Kumar A, Lee S, et al. Federated learning of electronic health records to improve mortality prediction in hospitalized patients with COVID-19: Machine learning approach. *JMIR Medical Informatics*, 2021, **9**(1): Article No. e24207

101 Rahman M A, Hossain M S, Islam M S, Alrajeh N A, Muhammad G. Secure and provenance enhanced Internet of health things framework: A blockchain managed federated learning approach. *IEEE Access*, 2020, **8**: 205071−205087

102 Alzubi J A, Alzubi O A, Singh A, Ramachandran M. Cloud-IIoT-based electronic health record privacy-preserving by CNN and blockchain-enabled federated learning. *IEEE Transactions on Industrial Informatics*, 2023, **19**(1): 1080−1087

103 Abou El Houda Z, Hafid A S, Khoukhi L, Brik B. When collaborative federated learning meets blockchain to preserve privacy in healthcare. *IEEE Transactions on Network Science and Engineering*, 2023, **10**(5): 2455−2465

104 Passerat-Palmbach J, Farnan T, Miller R, Gross M S, Flannery H L, Gleim B. A blockchain-orchestrated federated learning architecture for healthcare consortia. arXiv preprint arXiv: 1910.12603, 2019.

105 Wang Sheng-Sheng, Chen Jing-Yu, Lu Yi-Nan. COVID-19 chest CT image segmentation based on federated learning and blockchain. *Journal of Jilin University (Engineering and Technology Edition)*, 2021, **51**(6): 2164−2173
(王生生, 陈境宇, 卢奕南. 基于联邦学习和区块链的新冠肺炎胸部 CT 图像分割. 吉林大学学报 (工学版), 2021, **51**(6): 2164−2173)

106 Xing Dan, Xu Qi, Yao Jun-Ming. Medical and health data sharing model based on blockchain and federated learning in the edge computing environment. *Journal of Medical Informatics*, 2021, **42**(2): 33−37
(邢丹, 徐琦, 姚俊明. 边缘计算环境下基于区块链和联邦学习的医疗健康数据共享模型. 医学信息学杂志, 2021, **42**(2): 33−37)

107 El Rifai O, Biotteau M, de Boissezon X, Megdiche I, Ravat F, Teste O. Blockchain-based federated learning in medicine. In: Proceedings of the 18th International Conference on Artificial Intelligence in Medicine. Minneapolis, USA: Springer, 2020. 214−224

108 Qayyum A, Ahmad K, Ahsan M A, Al-Fuqaha A, Qadir J. Collaborative federated learning for healthcare: Multi-modal covid-19 diagnosis at the edge. *IEEE Open Journal of the Computer Society*, 2022, **3**: 172−184

109 Mo Zi-Jia, Gao Zhi-Peng, Yang Yang, Lin Yi-Jing, Sun Shan, Zhao Chen. Efficient distributed model sharing strategy for data privacy protection in internet of vehicles. *Journal on Communications*, 2022, **43**(4): 83−94
(莫梓嘉, 高志鹏, 杨杨, 林怡静, 孙山, 赵晨. 面向车联网数据隐私保护的高效分布式模型共享策略. 通信学报, 2022, **43**(4): 83−94)

110 Wang R, Li H J, Liu E W. Blockchain-based federated learning in mobile edge networks with application in internet of vehicles. arXiv preprint arXiv: 2103.01116, 2021.

111 Posner J, Tseng L, Aloqaily M, Jararweh Y. Federated learning in vehicular networks: Opportunities and solutions. *IEEE Network*, 2021, **35**(2): 152−159

112 Chai H Y, Leng S P, Chen Y J, Zhang K. A hierarchical blockchain-enabled federated learning algorithm for knowledge shar-

ing in internet of vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 2021, **22**(7): 3975−3986

113 Guo S Y, Xiang B Y, Xia X W, Yan Z H, Li Y L. Blockchain and federated learning based data security sharing mechanism over smart city. *Research Square*, DOI: 10.21203/rs.3.rs-104012/v1

114 Yang F, Qiao Y N, Abedin M Z, Huang C. Privacy-preserved credit data sharing integrating blockchain and federated learning for industrial 4.0. *IEEE Transactions on Industrial Informatics*, 2022, **18**(12): 8755−8764

115 Kang J W, Li X D, Nie J T, Liu Y, Xu M R, Xiong Z H, et al. Communication-efficient and cross-chain empowered federated learning for artificial intelligence of things. *IEEE Transactions on Network Science and Engineering*, 2022, **9**(5): 2966−2977

116 Yu Qiu-Yu, Lu Qing-Hua, Zhang Wei-Shan. Federated learning system architecture in industrail IoT based on blockchain. *Computer Systems & Applications*, 2021, **30**(9): 69−76
(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. 计算机系统应用, 2021, **30**(9): 69−76)

117 Demertzis K. Blockchained federated learning for threat defense. arXiv preprint arXiv: 2102.12746, 2021.

118 Lu Y L, Huang X H, Zhang K, Maharjan S, Zhang Y. Communication-efficient federated learning and permissioned blockchain for digital twin edge networks. *IEEE Internet of Things Journal*, 2021, **8**(4): 2276−2288

119 Lu Y L, Huang X H, Zhang K, Maharjan S, Zhang Y. Low-latency federated learning and blockchain for edge association in digital twin empowered 6G networks. *IEEE Transactions on Industrial Informatics*, 2021, **17**(7): 5098−5107

120 Pokhrel S R, Choi J. A decentralized federated learning approach for connected autonomous vehicles. In: Proceedings of the IEEE Wireless Communications and Networking Conference Workshops (WCNCW). Seoul, South Korea: IEEE, 2020. 1−6

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

122 Cui L Z, Su X X, Ming Z X, Chen Z T, Yang S, Zhou Y P, et al. CREAT: Blockchain-assisted compression algorithm of federated learning for content caching in edge computing. *IEEE Internet of Things Journal*, 2022, **9**(16): 14151−14161

123 Qin Z, Yan X Q, Zhou M C, Deng S G. BlockDFL: A blockchain-based fully decentralized peer-to-peer federated learning framework. In: Proceedings of the ACM on Web Conference. ACM, 2024. 2914−2925

124 Chen Y T, Chen Q, Xie Y X. A methodology for high-efficient federated-learning with consortium blockchain. In: Proceedings of the 4th Conference on Energy Internet and Energy System Integration (EI2). Wuhan, China: IEEE, 2020. 3090−3095

125 Desai H B, Ozdayi M S, Kantarcioglu M. BlockFLA: Accountable federated learning via hybrid blockchain architecture. In: Proceedings of the 11th ACM Conference on Data and Application Security and Privacy. ACM, 2021. 101−112

126 Fan S Z, Zhang H B, Zeng Y C, Cai W. Hybrid blockchain-based resource trading system for federated learning in edge computing. *IEEE Internet of Things Journal*, 2021, **8**(4): 2252−2264

127 Zhang W S, Lu Q H, Yu Q Y, Li Z T, Liu Y, Lo S K, et al. Blockchain-based federated learning for device failure detection in industrial IoT. *IEEE Internet of Things Journal*, 2021, **8**(7): 5926−5937

128 Wang Q L, Guo Y F, Wang X F, Ji T X, Yu L X, Li P. AI at the edge: Blockchain-empowered secure multiparty learning with heterogeneous models. *IEEE Internet of Things Journal*, 2020, **7**(10): 9600−9610

129 Yu S, Chen X, Zhou Z, Gong X W, Wu D. When deep reinforcement learning meets federated learning: Intelligent multitimescale resource management for multiaccess edge computing in 5G ultradense network. *IEEE Internet of Things Journal*, 2021, **8**(4): 2238−2251

130 Zhang Qin-Nan, Zhu Jian-Ming, Gao Sheng, Xiong Ze-Hui, Ding Qing-Yang, Piao Gui-Rong. Incentive mechanism for federated learning based on blockchain and bayesian game. *Scientia Sinica Informationis*, 2022, **52**(6): 971−991
(张沁楠, 朱建明, 高胜, 熊泽辉, 丁庆洋, 朴桂荣. 基于区块链和贝叶斯博弈的联邦学习激励机制. 中国科学: 信息科学, 2022, **52**(6): 971−991)

131 Wang Z L, Hu Q, Li R N, Xu M H, Xiong Z H. Incentive mechanism design for joint resource allocation in blockchain-based federated learning. *IEEE Transactions on Parallel and Distributed Systems*, 2023, **34**(5): 1536−1547

132 He Y H, Luo M S, Wu B, Sun L M, Wu Y D, Liu Z Q, et al. A game theory-based incentive mechanism for collaborative security of federated learning in energy blockchain environment. *IEEE Internet of Things Journal*, 2023, **10**(24): 21294−21308

133 Ding N N, Fang Z X, Huang J W. Optimal contract design for efficient federated learning with multi-dimensional private information. *IEEE Journal on Selected Areas in Communications*, 2021, **39**(1): 186−200

134 Feng C S, Liu B, Yu K P, Goudos S K, Wan S H. Blockchain-empowered decentralized horizontal federated learning for 5G-enabled UAVs. *IEEE Transactions on Industrial Informatics*, 2022, **18**(5): 3582−3592

135 Bonawitz K, Ivanov V, Kreuter B, Marcedone A, McMahan H B, Patel S, et al. Practical secure aggregation for federated learning on user-held data. arXiv preprint arXiv: 1611.04482, 2016.

136 Kosba A, Miller A, Shi E, Wen Z K, Papamanthou C. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: Proceedings of the IEEE Symposium on Security and Privacy (SP). San Jose, USA: IEEE, 2016. 839−858

137 Zhang F, Cecchetti E, Croman K, Juels A, Shi E L N. Town crier: An authenticated data feed for smart contracts. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Vienna, Austria: ACM, 2016. 270−282

138 Li B W, Fan L X, Gu H L, Li J, Yang Q. FedIPR: Ownership verification for federated deep neural network models. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2023, **45**(4): 4521−4536

139 Zhang X L, Li F T, Zhang Z Y, Li Q, Wang C, Wu J P. Enabling execution assurance of federated learning at untrusted participants. In: Proceedings of the IEEE Conference on Computer Communications. Toronto, Canada: IEEE, 2020. 1877−1886

140 Chen T, Li X Q, Luo X P, Zhang X S. Under-optimized smart contracts devour your money. In: Proceedings of the 24th International Conference on Software Analysis, Evolution and Reengineering (SANER). Klagenfurt, Austria: IEEE, 2017. 442−446

141 Wang P F, Zhao Y A, Obaidat M S, Wei Z Z, Qi H, Lin C, et al. Blockchain-enhanced federated learning market with social internet of things. *IEEE Journal on Selected Areas in Communications*, 2022, **40**(12): 3405−3421

142 Somy N B, Kannan K, Arya V, Hans S, Singh A, Lohia P, et al. Ownership preserving ai market places using blockchain. In: Proceedings of the IEEE International Conference on Blockchain (Blockchain). Atlanta, USA: IEEE, 2019. 156−165

143 Ouyang L W, Yuan Y, Wang F Y. Learning markets: An ai collaboration framework based on blockchain and smart contracts. *IEEE Internet of Things Journal*, 2022, **9**(16): 14273−14286

144 Wang F Y. New control paradigm for industry 5.0: From big models to foundation control and management. *IEEE/CAA Journal of Automatica Sinica*, 2023, **10**(8): 1643−1646

145 Wang Y C, Tian Y Y, Yin X Y, Hei X. A trusted recommendation scheme for privacy protection based on federated learning. *CCF Transactions on Networking*, 2020, **3**(3): 218−228

146 Hai T, Zhou J C, Srividhya S R, Jain S K, Young P, Agrawal S. BVFLEMR: An integrated federated learning and blockchain technology for cloud-based medical records recommendation system. *Journal of Cloud Computing*, 2022, **11**(1): Article

No. 22

147 Peng Z, Xu J L, Chu X W, Gao S, Yao Y, Gu R, et al. VFChain: Enabling verifiable and auditable federated learning via blockchain systems. *IEEE Transactions on Network Science and Engineering*, 2022, **9**(1): 173−186

148 Xu M R, Ng W C, Lim W Y B, Kang J W, Xiong Z H, Niyato D, et al. A full dive into realizing the edge-enabled metaverse: Visions, enabling technologies, and challenges. *IEEE Communications Surveys & Tutorials*, 2023, **25**(1): 656−700

149 Huang H W, Zhang Q N, Li T T, Yang Q L, Yin Z K, Wu J H, et al. Economic systems in the metaverse: Basics, state of the art, and challenges. *ACM Computing Surveys*, 2023, **56**(4): Article No. 99

150 Truong N B, Sun K, Lee G M, Guo Y K. Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Transactions on Information Forensics and Security*, 2020, **15**: 1746−1761

151 Chehimi M, Saad W. Quantum federated learning with quantum data. In: Proceedings of the IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). Singapore: IEEE, 2022. 8617−8621

152 Xia Q, Li Q. QuantumFed: A federated learning framework for collaborative quantum training. In: Proceedings of the IEEE Global Communications Conference (GLOBECOM). Madrid, Spain: IEEE, 2021. 1−6

153 Pujahari R M, Tanwar A. Quantum federated learning for wireless communications. *Federated Learning for IoT Applications*. Cham: Springer, 2022. 215−230

154 Wang F Y. Parallel intelligence in metaverses: Welcome to Hanoi! *IEEE Intelligent Systems*, 2022, **37**(1): 16−20

155 Kang J W, Ye D D, Nie J T, Xiao J, Deng X J, Wang S M, et al. Blockchain-based federated learning for industrial metaverses: Incentive scheme with optimal AoI. In: Proceedings of the IEEE International Conference on Blockchain (Blockchain). Espoo, Finland: IEEE, 2022. 71−78

156 Moudoud H, Cherkaoui S. Federated learning meets blockchain to secure the metaverse. In: Proceedings of the International Wireless Communications and Mobile Computing (IWCMC). Marrakesh, Morocco: IEEE, 2023. 339−344

157 Chatterjee P, Das D, Rawat D B. Next generation financial services: Role of blockchain enabled federated learning and metaverse. In: Proceedings of the 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW). Bangalore, India: IEEE, 2023. 69−74

158 Cao L B. Decentralized AI: Edge intelligence and smart blockchain, metaverse, Web3, and DeSci. *IEEE Intelligent Systems*, 2022, **37**(3): 6−19

159 Fu Y C, Li C L, Yu F R, Luan T H, Zhao P C, Liu S. A survey of blockchain and intelligent networking for the metaverse. *IEEE Internet of Things Journal*, 2023, **10**(4): 3587−3610

160 Wang X X, Yang J, Wang Y T, Miao Q H, Wang F Y, Zhao A J, et al. Steps toward industry 5.0: Building "6S" parallel industries with cyber-physical-social intelligence. *IEEE/CAA Journal of Automatica Sinica*, 2023, **10**(8): 1692−1703

161 Wang F Y, Qin R, Wang X, Hu B. Metasocieties in metaverse: Metaeconomics and metamanagement for metaenterprises and metacities. *IEEE Transactions on Computational Social Systems*, 2022, **9**(1): 2−7

李 程 中国人民大学数学学院、交叉科学研究院博士研究生. 主要研究方向为区块链, 联邦学习与机制设计.
E-mail: cheng.li@ruc.edu.cn
(**LI Cheng** Ph.D. candidate at the School of Mathematics and the School of Interdisciplinary Studies, Renmin University of China. His research interest covers blockchain, federated learning, and mechanism design.)

袁 勇 博士, 中国人民大学数学学院教授. 主要研究方向为区块链, 计算经济学与分布式人工智能. 本文通信作者.
E-mail: yong.yuan@ruc.edu.cn
(**YUAN Yong** Ph.D., professor at the School of Mathematics, Renmin University of China. His research interest covers blockchain, computational economics, and distributed artificial intelligence. Corresponding author of this paper.)

郑志勇 中国人民大学数学学院教授. 主要研究方向为解析数论与代数数论. 在指数和与特征和的几何理论以及函数域的解析理论等领域上有突破性贡献.
E-mail: zhengzy@ruc.edu.cn
(**ZHENG Zhi-Yong** Professor at the School of Mathematics, Renmin University of China. His research interest covers analytic number theory and algebraic number theory. He has made breakthrough contributions in the geometric theory of exponents and characteristic sums and analytic theory of functional domains.)

杨 东 中国人民大学交叉科学研究院教授. 主要研究方向为金融科技, 区块链, 数字货币.
E-mail: yangdongbeijing@163.com
(**YANG Dong** Professor at the School of Interdisciplinary Studies, Renmin University of China. His research interest covers financial technology, blockchain, and digital currency.)

王飞跃 中国科学院自动化研究所复杂系统管理与控制国家重点实验室研究员. 主要研究方向为智能系统和复杂系统的建模, 分析与控制.
E-mail: feiyue.wang@ia.ac.cn
(**WANG Fei-Yue** Professor at the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences. His research interest covers modeling, analysis, and control of intelligent systems and complex systems.)