基于区块链的联邦学习技术综述*

李凌霄[1a,1b]，袁 莎[2†]，金银玉[2]
(1. 北京外国语大学 a. 网络教育学院；b. 人工智能与人类语言重点实验室，北京 100089；2. 北京智源人工智能研究院，北京 100084)

摘 要：联邦学习与区块链在应用领域、架构特点、隐私保护机制等方面具有很强的共性、互补性和契合度，近年来，一些研究与应用将两种技术结合起来，在数据隐私保护强度、数据共享激励机制、计算性能等方面取得了不少进展。为了帮助研究者掌握联邦学习结合区块链的最新研究成果与发展方向，对基于区块链的联邦学习进行了综述。首先，介绍了联邦学习技术的相关研究和存在的不足；其次，详细讨论了当前基于区块链的联邦学习的相关研究，重点从架构特点、资源分配、安全机制、激励机制等方面进行了分析；最后，总结了基于区块链的联邦学习应用在人工智能领域的未来发展趋势和需要关注的问题。

关键词：联邦学习；区块链；人工智能；数据安全；数据隐私
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2021)11-003-3222-09
doi:10.19734/j.issn.1001-3695.2021.04.0094

Review of blockchain-based federated learning

Li Lingxiao[1a,1b], Yuan Sha[2†], Jin Yinyu[2]
(1. *a. Institute of Online Education, b. Artificial Intelligence & Human Languages Laboratory, Beijing Foreign Studies University, Beijing* 100089, *China*; 2. *Beijing Academy of Artificial Intelligence, Beijing* 100084, *China*)

Abstract: Federated learning and blockchain have a strong commonality, complementarity and compatibility in application fields, architectural features and privacy protection mechanisms. In recent years, some research and applications combined the two technologies and made a lot of progress in terms of data privacy protection, data sharing and computational performance. To help researchers grasp the latest research achievements and development directions, this paper presented a review of blockchain-based federated learning. Firstly, this paper presented the relevant research and the shortcomings of federated learning. Then, it discussed the current research related to blockchain-based federated learning, mainly focused on the architectural features, resources allocation, security mechanism and incentive mechanism. Finally, this paper concluded the future trends and issues of blockchain-based federated learning.

Key words: federated learning; blockchain; artificial intelligence; data security; data privacy

0 引言

当前，人工智能技术发展迅猛，已经从几年前的发明期逐渐转入了落地应用期，在越来越多的应用场景中，人工智能技术得到了应用。然而在算法、算力都大幅跃升，对数据规模需求更大和数据隐私保护更为重视的情况下，如何满足人工智能模型对数据的需求，成为当下人工智能技术发展亟待解决的问题。

如今的机器学习算法越来越依赖于大量数据，然而实际情况却是，在隐私保护的限制下，数据分散在不同的组织中，因此当前人工智能的发展面临着数据孤岛问题和数据安全、隐私保护问题两个挑战。首先，数据孤岛问题极大地制约了大数据的可用性。互联网虽然每天产生数以亿计的数据，然而其中缺乏有用的高维度、高质量的数据。其次，各国都在加强对数据安全和隐私的保护，对用户数据隐私和安全管理的日趋严格将是世界趋势。若没有让用户放心的隐私保护方法，数据不足问题将会严重限制人工智能的发展。

由于这些因素，新兴的机器学习技术——联邦学习(federated learning，FL)[1,2]已成为机器学习中的热门研究主题。例如，不同医院的数据是孤立的，成为“数据孤岛”。由于每个数据孤岛在大小和逼近实际分布方面都有局限性，所以一家医院可能无法训练对特定任务具有良好预测准确性的高质量模型。理想情况下，如果多家医院可以结合多方数据共同训练机器学习模型，则可以实现更准确的模型训练结果。然而，由于各种政策和法规，数据不能简单地在医院之间共享。同样地，“数据孤岛”现象在金融、政府和供应链等许多领域也很普遍。另外，类似通用数据保护条例(GDPR)[3]等政策规定了不同组织之间的数据共享规则，因此，开发一种具有良好的预测准确性，同时能遵守政策和法规以保护隐私的联邦学习系统是一项非常有挑战性的工作。

联邦学习在安全和隐私保护方面仍面临很多问题，目前联邦学习加密算法的执行速度不足以支撑大规模深度学习应用。如何激励人工智能数据共享，提高联邦学习训练性能和效率，加强安全隐私保护机制也是联邦学习亟待突破的研究方向。与联邦学习技术的发展脉络相似，区块链的去中心化、不可窜改以及隐私保护等特性，使得区块链技术得到了广泛的关注与研究。但随着深度学习引领人工智能第三次热潮，人工智能应用场景复杂性的增加，原有的区块链架构也不足以支撑大规模深度学习应用。

收稿日期：2021-04-08；**修回日期**：2021-06-07 **基金项目**：国家重点研发计划资助项目(2020AAA0105200)；国家自然科学基金资助项目(61806111)

作者简介：李凌霄(1986-)，男，讲师，博士，主要研究方向为数据处理、信息挖掘；袁莎(1989-)，女(通信作者)，副研究员，博士，主要研究方向为数据智能、知识工程、大规模预训练模型(yuansha@baai.ac.cn)；金银玉(1986-)，硕士，主要研究方向为信息安全、区块链.

通过这些年联邦学习和区块链的技术积累,以及各相关领域对这两项技术的应用与探索,区块链 + 联邦学习(BlockFL, BFL)已具备在高度隐私敏感的行业中应用的能力与前景。区块链作为一种去中心化的分布式存储架构,以密码学方式保证其不可窜改性和不可伪造性。由于区块链在身份认证、去中心化、可追溯、可审计等方面的优势,已有很多研究工作将区块链作为联邦学习的底层基础架构,通过在区块链上层设计协议来实现分布式模型聚合的任务。虽然区块链是替换联邦学习中心服务器的一种有效方式,区块链对于联邦学习模型存储和更新过程中的安全性也有很大提升,但是在联邦学习应用场景下,区块链也面临着很多新的问题。

在已有文献中,研究人员对联邦学习和区块链技术分别进行了综述,不过对于联邦学习与区块链相结合的研究与应用而言,到目前为止还没有总结与综述的工作。因此,本文从联邦学习技术的架构出发,概述了联邦学习的相关研究成果,结合人工智能和联邦学习的发展,介绍了当前联邦学习技术面临的问题和发展需求,分析并讨论了联邦学习与区块链技术相结合的需求及其发展方向,总结出区块链技术在联邦学习技术方向上的应用优势和探索方向。

1　联邦学习概述

1.1　起源

早在 20 世纪 90 年代,就有相关的工作[4]对联邦数据库系统(federated database system,FDBS)进行了研究。联邦数据库是合作互利的自治数据库的集合。研究[4]指出,联邦数据库的三个重要组成部分是自治性、异构性和分布性。其后,随着云计算的发展,又有许多科研人员对联邦云(federated cloud)进行了研究[5]。联邦云是对多个外部和内部云计算服务的部署和管理。联邦云的概念可以将成本通过外包给更具效益的一方而进一步降低。资源迁移和资源冗余是联邦云的两个基本特征[5]。首先,资源可以从一个云提供商转移到另一个云提供商,迁移可以重新分配资源。其次,冗余允许在不同域中并发使用相似的服务功能。例如,可以按照相同的计算逻辑在不同的提供者处对数据进行分区和处理。总体而言,不同资源的调度是联邦云系统设计中的关键因素。

联邦学习与传统的联邦系统之间存在一些异同。一方面,联邦的概念仍然适用,共同的基本思想是多个独立部署的协作。因此,考虑不同部署之间的异质性和自治性的观点仍然可以应用于联邦学习系统。此外,分布式系统设计中的某些因素对于联邦学习仍然很重要,例如各部署间共享数据的方式会影响系统的效率。另一方面,以上三种联邦系统类型在协作和约束方面有不同的侧重。联邦数据库专注于分布式数据的管理,联邦云专注于资源的调度,而联邦学习则更关注多方之间的安全计算。联邦学习的兴起带来了许多新的挑战,例如分布式训练的算法设计和隐私限制下的数据保护。如今,“数据独岛”现象在人工智能技术的应用中十分普遍,并且越来越成为机器学习中的重要问题,因此,联邦学习研究与普及的必要性和紧迫性日益突显。

1.2　联邦学习的研究方向

考虑到不同联邦学习系统构建中的要素,本文从以下几个方面对联邦学习进行讨论:通信体系结构、隐私机制以及采用联邦学习技术的动机与激励机制。这些方面是在设计联邦学习系统整体框架和具体内容中需要考虑的关键因素,也是当前联邦学习的发展中亟需突破的主要方向。

1.2.1　通信体系架构

在通信体系架构方面,最初的联邦学习系统一般为中心式的,但后来出现了一些去中心化的设计,所以联邦学习系统中有两种主要的通信方式,即中心式和去中心式。在中心式的通信体系架构设计中,数据流通常是不对称的,这意味着中心服务器从其他参与方收集信息(如梯度或模型参数)并发送回训练结果[6]。全局模型上的参数更新始终在此中心服务器中完成。中心服务器与本地参与方之间的通信可以是同步[7]或异步[8,9]。在去中心式设计中,通信在各方之间进行[10,11],并且每一方都能够直接更新全局参数。

中心式架构通常是简单有效的,其可扩展性和稳定性是联邦学习系统设计中的两个重要因素。尽管中心式设计在现有研究中已广泛使用,但在一些情况下,更适合采用去中心式设计,因为将信息集中在一台服务器上可能会带来潜在的风险或不公平性。

1.2.2　隐私机制

尽管本地数据在联邦学习中是非公开且受到保护的,但由于交换了模型参数,其安全性可能会受到影响,威胁模型在不同隐私级别的联邦学习系统中也有所不同[12]。攻击可以来自联邦学习过程的任何阶段。在输入阶段的攻击:恶意方可以在联邦学习上进行数据投毒攻击[13~15]。例如,当事方可以在学习之前修改特定类别的样本标签,导致所学习的模型在该类别上表现不佳。在学习过程中的攻击:各方可以执行模型投毒攻击[16,17]以上传经过恶意设计的模型参数。与数据投毒攻击相似,由于本地更新被投毒,导致全局模型的准确性可能非常低。除了模型投毒攻击之外,拜占庭式故障[18~21]也是分布式学习中的常见的问题,在这种情况下,各方模型的学习效果可能会表现得很差,并且还会随机上载更新。在学习的模型中的攻击:如果将学习的模型公开,则可以对其进行推理攻击[22~25],服务器可以从交换的模型参数中推断出有关训练数据的敏感信息。例如,成员推断攻击[23,25]可以推断在训练中是否使用了特定的数据记录。另外,值得注意的是联邦学习管理方也可以在学习过程中访问各方的本地更新从而进行推理攻击。

目前有许多隐私机制提供了不同的隐私保证,例如差分隐私[26]和 k-匿名[27,28],也有研究调查总结了现有隐私机制的特征[29]。在这里,本文仅总结当前联邦学习系统中用于数据保护的两种主要方法:加密方法和差分隐私。

加密方法(例如同态加密[1,30~38]和多方安全计算[39~50])目前被广泛应用于保护隐私的联邦学习算法中。通过这些方法,一般情况下可以很好地保护联邦学习系统中的用户隐私[51~55]。比如,在多方安全计算中[56]除了输出之外,所有各方都不能学习其他任何东西。但是,这种方法容易受到推理攻击,而且由于附加的加密和解密操作,将使系统承担极高的计算开销。

差分隐私[26,57]可以保证单个记录不会对函数的输出产生太大影响,换句话说,就是保证任意个体在数据集中或者不在数据集中时,对最终发布的查询结果几乎没有影响。许多研究采用差分隐私[11,58~64]来保护数据隐私,其中各参与方并不知道其他参与方是否参与了学习过程。通过将随机噪声添加到数据或模型参数[60,63,65],差分隐私可为单个记录提供统计隐私保证,并防止对模型的推理攻击,且与加密方法相比,不产生额外的计算开销[66],但由于学习过程中的噪声,此类系统倾向于生成精度较低的模型。

上述方法彼此独立,并且联邦学习系统可以采用多种方法来增强隐私保证[67,68]。尽管大多数现有的联邦学习系统采用加密技术或差分隐私可以实现良好的隐私保证,但是这些方法的一些局限性目前很难克服。现有的一些尝试性工作主要是以最小化这些方法带来的副作用,同时继续寻找一种兼顾数据隐私保护和灵活隐私要求的新方法,比如不久前的研究中[69]

采用稍弱的安全模型[70]以求实现更加实用的系统。

1.2.3 联邦学习动机与激励机制

在联邦学习的实际应用中,各方可能需要一定的动机来激励他们参与联邦学习系统,这些动机可以是规则约束或是激励措施。公司间或组织内部的联邦学习通常受规则约束的激励。但是在许多合作中,不能强制各方根据约束规则提供其数据。以较早就开始应用联邦学习技术的谷歌键盘为例[71],虽然不提供共享数据的用户也可以使用谷歌键盘,但是同意上传输入共享数据的用户则能享受更高的单词预测准确度。这种激励措施可以鼓励每个提供数据的用户改善整体模型的性能。但是,如何设计这样一个合理的协议仍然非常具有挑战性。

通过以上对现阶段联邦学习现状的整理、总结可以看出,目前联邦学习面临的挑战主要集中在安全性、隐私性、性能以及激励机制等方面。当前加密算法的执行速度不足以支撑大规模深度学习的应用,且如何激励数据共享意愿,提高联邦学习训练性能和效率,加强安全隐私保护机制都是当前联邦学习亟待突破的研究方向。而在这几方面,区块链技术有着天然的优势,最近几年,一些研究把联邦学习技术与区块链技术相结合来克服上述联邦学习应用中的问题。

2 基于区块链的联邦学习技术

在传统的联邦学习架构中,中心服务器负责收集、聚合和广播新的全局模型,因此可能导致如下问题:a)中央服务器的稳定性可能受到云服务提供商的影响;b)中央服务器可能会偏袒某些客户端;c)恶意的中央服务器可能会对模型进行投毒或者收集客户端的隐私信息。针对这些问题,最直接的办法就是去掉中央服务器,交由客户端节点来处理对应的任务,而这一需求恰恰符合区块链技术本身的特点。最近的一些研究以区块链分布式存储架构作为联邦学习的基础架构,通过在区块链上层设计协议来实现在客户端上运行模型聚合的任务;同时,区块链中合理的激励机制也为提高各参与方合作参与联邦学习模型训练的积极性提供了技术上的解决方案。

对于去中心式联邦学习系统,客户端设备之间相互通信,而无须中央服务器的协调。移除的中央服务器主要由区块链代替,作为模型和信息来源的组件[72~79]。区块链还负责提供激励和差异化的私人多方数据模型共享。在没有中央服务器的情况下,初始模型可以由每个客户端设备使用本地数据集在本地创建,并使用基于共识的方法来更新模型,该方法使设备能够发送模型更新并从邻居节点接收梯度[80~82]。客户端设备之间的通信是通过对等网络[83~85]实现的。每个设备都具有所有客户端设备的模型更新副本,通过目前主流的共识机制[86],如工作量证明机制(PoW)、权益证明机制(PoS)[87]、股份授权证明机制(DPoS)[88]、拜占庭容错机制(PBFT)等进行处理,当达成共识后,所有客户端设备都使用新的梯度进行模型训练。目前基于区块链的联邦学习技术研究主要集中在去中心化的通信体系架构、安全性能和激励机制等方面。在表 1 中,列举总结了目前结合了联邦学习技术与区块链技术的最新研究,下面将重点从上述几个重点研究方向进行总结。

2.1 去中心化的通信体系架构

利用区块链为联邦学习设计一个去中心化的系统是非常具有挑战性的任务。在联邦学习系统的学习过程中,各方几乎都受到同等对待,并且不需要设置信任服务器。而在去中心化式设计中,主要难点在于很难设计出一种协议,以合理的通信开销近乎公平地对待每个参与方。并且由于区块链分类帐取代了中央服务器,并且训练在各方本地进行,所以每个参与方可能必须与所有其他方交换模型参数信息,这样尽管减少了与中央服务器通信所引起的如延迟等情况的网络成本,但增加了与区块链挖掘相关的新的成本。因此,在设计 BFL 通信体系时,需要考虑到本地训练延迟、更新通信延迟和区块挖掘延迟等问题,同时还要兼顾到训练的准确性。

2018 年,研究人员对分布式机器学习中的非线性学习模型的隐私和安全问题进行了分析并基于区块链技术提出了支持隐私保护的分布式安全机器学习系统 LearningChain[89]。他们提出了没有中央服务器的通用学习模型并通过区块链私有链进行搭建,通过引入差分隐私技术实现了数据隐私保护并提出了新的聚合算法来抵御拜占庭攻击。文献[90]提出了基于区块链的联邦学习环境 BAFFLE,通过公有链或私有链的区块链来存储和分享全局模型并通过智能合约来进行模型聚合任务。BAFFLE 利用智能合约来管理全局模型以及用户的相关计算状态,用户可以并行地对全局模型进行更新。通过评估每个用户本地训练对模型更新起到的作用大小来决定用户的收益,从而保证训练过程对于每个用户的公平性。文献[91]提出了一个基于区块链分片的 5G 分布式计算环境下拜占庭回弹的分布式学习框架 PIRATE。PIRATE 以 5G 场景下足够短的通信时延以及足够大的带宽为前提,主要解决分布式学习中的模型参数更新以及梯度聚合过程中存在的拜占庭攻击问题。PIRATE 中引入了区块链分片协议以及梯度异常检测技术[92],其架构中同样没有中央服务器的存在。

小结:在部署基于区块链的联邦学习系统时,通信成本是需要关注的关键问题之一。当前大多数的 BFL 系统方案是通过结合训练延迟、矿工通信延迟与挖矿延迟来分析通信成本,但如果具体到某些特定应用时,通信成本可能会有不同的侧重,如在边缘计算的应用当中,通信成本集中在边缘计算延迟和参数传输通信延迟上。当前,多数基于区块链的联邦学习系统都依赖于 PoW 共识机制,但这样的共识机制通常需要消耗较大的带宽和计算开销来实施区块链的挖矿过程,因此,研究开发较为轻量级的区块链应用于联邦学习系统可以很大程度上地解决通信成本问题,实现系统成本的大幅降低。

2.2 资源分配与数据管理

在 BFL 系统中,资源分配与数据管理非常重要。每个联邦学习参与方的客户端中,设备需要共享其计算与存储资源以训练模型和参与区块链。

2020 年,文献[93]针对移动设备的计算、存储资源限制以及区块链交易过程带来的训练时延增加问题提出了基于深度强化学习(DRL)的解决方案。要解决上述问题,联邦学习训练的发起者需要确定适当的资源分配以及区块链中区块生成的频率,然而对于复杂的 IoT 环境来说,这是非常困难的。因此提出了一套基于深度强化学习的方案,使得训练的发起者可以在没有 IoT 网络先验知识的情况下进行有效的资源分配。

2020 年,文献[94]针对移动边缘计算网络提出了一套基于区块链的联邦学习框架。在移动边缘计算网络中,传统的联邦学习存在如下的局限性:a)设备和服务器的异构性;b)数据和模型更新的高维;c)数据、算法、数据源、数据预处理以及模型训练带来的误差;d)中心化的模型训练;e)单点失败问题。针对上述问题提出了一个更细粒度的联邦学习框架,将数据集进行了垂直分割,从而实现了多层次的数据管理。

小结:资源分配是 BFL 系统中非常关键的任务,用以确保用于数据训练的最优资源使用。目前,比较流行使用深度强化学习的方法,在计算开销和通信带宽都得到满足的情况下,为基于区块链的联邦学习系统实现资源分配策略。另一方面的研究从减轻联邦学习训练的消耗入手,解决资源分配问题,如基于 DPoS 共识的轻量级区块链平台已经得到了比较多的使

用,以支持基于区块链的联邦学习中的模型更新和区块挖掘。此外,综合考虑整个基于区块链的联邦学习系统中的本地设备学习率、模型到达率以及区块生成等问题,是未来进一步改善资源分配问题的有效途径,从而实现系统网络中矿工和本地设备的合作资源分配方案。

2.3　安全性、可靠性、鲁棒性、可审计性

为了确保基于区块链的联邦学习系统的鲁棒性和安全性等问题,建立安全和隐私保护机制至关重要,这也是联邦学习系统中引入区块链技术的关键原因。利用区块链技术来控制节点之间数据信息交互的数据出处机制对于解决单点故障和对抗攻击非常有效,尤其是对于去中心式的联邦学习系统。区块链记录所有共享事件而不是记录原始数据,以进行审核和数据跟踪,并且仅允许拥有权限的参与方访问信息[77,95]。

为了解决去中心式系统中存在的性能问题,尤其是安全性问题,2020 年,中山大学的研究人员基于区块链系统提出了一个分布式、自治的联邦学习框架 BFLC(blockchain-based federated learning framework with committee consensus)[96],BFLC 重新定义了模型的存储模式、训练过程以及委员会共识机制,对共识效率以及存储消耗两方面进行了优化,同时也对恶意节点攻击的场景进行了模拟来证明框架的安全性。

2020 年,文献[97]针对 5G 网络下联邦学习中存在的投毒攻击以及成员推理攻击两种威胁,提出了联邦学习的安全框架[97],利用区块链智能合约的能力来抵御投毒攻击,并引入本地化差分隐私技术来抵御成员推理攻击。类似的研究还有应用于众包物联网的 BFL 中,文献[98]采用差异性隐私技术来抵御恶意方在进行联邦学习时使用区块链记录众包活动来推断敏感的个人信息的攻击。

文献[99]提出了针对雾计算的基于区块链的联邦学习。他们使用分布式哈希表对区块链上数据的存储进行优化,从而提升了区块产生的效率,借助区块链去中心化的特点实现了分布式隐私保护并解决了雾计算场景下的单点失败问题。此外,通过去掉中央服务器,解决了联邦学习中的投毒攻击问题。

2018 年,文献[100]针对异常检测模型提出了一个基于许可链的联邦学习方法,通过分布式账本来记录对模型的增量更新,从而实现了在不收集训练数据的情况下对机器学习模型的审计。文献[101]针对移动设备上的本地模型更新的场景提出了一套基于区块链的联邦学习框架 BlockFL,通过矿工把移动设备联系起来,用户可以通过交易自己的本地模型获取报酬,矿工对所有的本地模型进行交换和验证,进而执行工作量证明来获取报酬。同时,单一矿工或设备的故障不会影响全局模型的更新,这也增强了系统的鲁棒性。

2019 年,文献[102]针对车联网的场景,引入了许可链以及有向无环图(DAG)技术,提出了一个新的联邦学习架构来提高数据共享的效率和安全性。同时,还应用了深度强化学习来进行节点选择以提升性能,从而提出了一个异步联邦学习方案。文献[78]提出的 FLchain 引入了区块链中 channel 的概念来学习多个全局模型,通过共识的过程得到最终的全局模型,并把本地模型参数作为一个区块存储在特定的账本中。作者提出了全局模型状态树的概念,通过对状态树的共识来求解模型的全局参数,相比于传统的联邦学习模型,该模型具有更强的鲁棒性。

小结:通过总结以上研究可以发现,在 BFL 系统中,攻击者可以尝试使用伪造数据来训练局部模型以替换全局模型,并在模型传输期间修改参数值,从而操纵训练输出。现有的很多工作都集中在建立用于模型训练和更新基于区块链的联邦学习系统传输时的攻击检测机制。除此之外,还可以通过调整采矿难度而不降低训练性能来降低如中毒攻击等的可能性。在整个基于区块链的联邦学习系统中,攻击模型在区块链挖矿和本地数据训练的过程中都应被综合考虑到。例如,有恶意的矿工可能会利用整个基于区块链的联邦学习系统来增强其采矿能力来对矿工组进行控制,从而达到修改数据块的目的;恶意方也可使用如女巫攻击的方式进行双重交易,使得挖矿效率大幅降低。

在数据隐私保护机制方面,差分隐私、同态加密等技术依然是对于基于区块链的联邦学习训练时最有效的手段。例如,通过将拉普拉斯噪声添加到私有树的每个中间节点中随机选择的叶子节点上,极大地消除了噪声被去除的可能性并满足 ε-差分隐私;同态加密对于联邦学习训练中加强外包存储和计算的隐私保护非常有效,在区块链上共享联邦学习模型聚合之前,可以对数据进行有效加密,在对个人信息和隐私数据极其敏感的任务中有着非常重要的作用。

2.4　激励机制与共识协议

基于区块链的联邦学习技术的研究,一方面的研究重点是通过去中心化解决安全、性能等问题,另一方面的研究重点是建立合理的激励机制。尽管联邦学习技术本身在保护用户隐私的同时促进了协作学习训练,但仍然面临着如何更合理地激励各方参与联邦学习过程并贡献其数据和计算资源的挑战。如果没有适当的激励机制,各参与方可能不愿意参加数据训练,这将降低所设计的联邦学习系统的可扩展性。通过从区块链中引入适当的激励机制,实行透明且经济有效的激励机制设计,将能很好地提高联邦学习系统中各方参与训练的积极性。

通常情况下,激励机制可以由中央服务器[103,104]或区块链[75,77]托管,区块链中激励机制是一种提高联邦学习合作训练积极性的很好的解决方案。例如,文献[105]针对无人驾驶场景提出了基于区块链的新的联邦学习框架,该框架主要针对 Google 的联邦学习框架[106]应用到无人驾驶场景时存在的两个问题:a)中心化问题,如果中央服务器出现故障,会造成较大的风险;b)缺少激励机制,本地的驾驶数据对无人驾驶来说非常重要,需要一定的激励机制鼓励用户提供数据进行模型训练。通过区块链来解决去中心化的问题,并设计了一套激励机制从而使得数据提供者可以从中获取回报。

训练过程中的参与者越多,全局模型的性能就越好。但是,如果数据所有者或设备所有者没有贡献数据和资源的利益,则没有义务参加训练过程。因此,一些研究人员引入了激励机制来吸引数据和设备所有者加入模型训练。例如,基于提供的计算量、通信量和能源量[76,107],本地模型精度和性能[108],提供的数据质量[109],客户端设备的诚实行为[100],客户端节点的丢失率[110]等。

激励机制设计对于联邦学习系统的成功非常重要,而在区块链中已经有很多非常成功的激励机制设计案例[111,112]。系统内部的各方可以是合作者,也可以是处于竞争中的参与者。文献[74,103]提出了独特的激励机制设计,以吸引具有联邦学习高质量数据的参与者。因此,在联邦学习系统下应重新审视不同的博弈机制模型[113~115]及其均衡设计。

在当前大数据时代,每天有大量的数据产生,这些数据往往是互不相关的,同时绝大多数数据都掌握在少数大型科技公司手中,为了解决这一问题,文献[116]将区块链与联邦学习结合,借助权益证明的共识算法以及 IPFS 分布式存储,提出了一套新的联邦学习框架,从而可以借助激励机制来鼓励用户参与联邦学习的训练来提取数据之间的关联性。

文献[74]针对联邦学习的激励机制问题,利用多权重主

看着一段

观逻辑模型来评估用户的信用,设计了一套高效的激励机制。文献[117]以 EOS 区块链以及 IPFS 为基础提出了基于区块链的联邦学习框架,以可扩展的方式存储用户上传的参数更新,并通过 EOS 使上传更新的用户获得收益。

Kim 等人[101]将区块链架构与联邦学习相结合,在联邦平均(FedAvg)算法的基础上,使用区块链网络交换设备的本地模型更新,该更新比在中央服务器中进行时更稳定,并且可以为设备提供奖励。Kang 等人[74]设计了一种基于信誉的矿工选择方案,通过使用多权重主观逻辑模型来实现可靠的联邦学习。他们还利用区块链以分散的方式为具有抗抵赖和防窜改特性的矿工实现安全的声誉管理。Bao 等人[73]设计了一种基于信任和激励的 FLChain 框架,可以保存矿工的信息和可验证的训练细节以供公众审核,其激励机制会激励诚实守信的矿工,反之会进行惩罚,以此维护健康可靠的公共平台。

为了解决在梯度收集和模型参数更新过程中存在的不诚实用户的威胁以及激励机制缺乏的问题,文献[79]提出了支持可审计以及隐私保护的联邦学习框架 DeepChain,它给不信任的各方提供激励,使其参与保护隐私的学习,共享梯度和正确更新参数,并最终实现迭代的深度学习,从而获得双赢的结果。DeepChain 基于区块链的激励机制建立了一套完整的模型交易体系,从而鼓励用户参与模型的训练,并借助区块链交易来记录模型训练的过程,实现了隐私保护以及训练过程的可审计。DeepChain 保密性优良[100],考虑了梯度交互的安全性问题,但是 DeepChain 在工作中使用的阈值 Paillier 算法具有较高的计算开销,并且实验无法完全解释该算法导致的吞吐量变化。在激励机制方面,他们提出的基于 Deepcoin 的激励机制并未在实验中显示出来。类似的工作还包括 Chen 等人[89]提出的 LearningChain 。DeepChain 与 LearningChian 的不同之处在于,LearningChain 采用差分隐私机制来保护数据持有人在本地培训过程中的数据隐私,并设计了 l-nearest 聚合算法在全局梯度聚合过程中防御拜占庭式攻击。

小结:本节涉及研究提出的激励机制中,大多数的共同目标都是为了在模型训练中吸引更多的参与方或数据量,从而提高整个基于区块链的联邦学习系统的鲁棒性。其次,区块链的加入也为联邦学习训练中实现安全的激励机制提供了一些独特的功能,比如模型更新由区块链进行验证和审计,而梯度收集和参数更新则由所有参与方通过分类账网络进行监控,从而确保联邦学习过程的公平性。不过,在激励过程中,梯度更新的验证成本在已有的研究中还没有得到全面的考量,在未来的工作中,权衡从激励机制中获得的收益和系统成本将变得更为重要,从而使模型所有者和各区块链客户端共同获益。

表 1 基于区块链技术的联邦学习系统

Tab. 1 Blockchain-based federated learning systems

研究工作	应用领域	隐私保护机制	区块链结构	激励机制	共识协议
BC-based PPFL[72]	通用/理论研究	同态加密	-	基于贡献	-
LearningChain[89]	通用/理论研究	差分隐私	私有链	-	PoW
BAFFLE[90]	通用/理论研究	-	公有链/私有链	-	PoA
PIRATE[91]	5G	-	-	-	-
基于 DRL 的资源分配[93]	物联网	-	-	基于贡献	PoW
细粒度 BFL[94]	物联网	-	-	信誉感知	-
基于许可链的 BFL[77]	工业物联网	差分隐私	许可链	-	PoW
BFLC[96]	通用/理论研究	-	-	基于贡献	PBFT
5G 网络中的安全 BFL[97]	5G	智能合约/差分隐私	-	-	-
用于雾计算的安全 BFL[99]	雾计算	差分隐私	-	-	PoW
针对异常检测的 BFL[100]	通用/理论研究	模型增量审计	许可链	-	-
BlockFL[101]	通用/理论研究	-	-	基于数据量的大小	PoW
异步 BFL[102]	车联网	-	许可链	-	DPoS
多访问 FLchain[78]	通用/理论研究	-	-	-	PBFT,PoW
On-device BFL[75]	通用/理论研究	-	-	-	PoW,PoS,BFT
用于无人驾驶的 BFL[105]	oVML	-	-	-	PoW
BFL 的端子集的选择[76]	通用/理论研究	-	-	-	-
TCLearn[108]	通用/理论研究	同态加密	联盟链	-	custom FBA
利用 EOS 的 BFL[117]	通用/理论研究	同态加密	公有链	-	-
DeepChain[79]	通用/理论研究	-	-	-	Blockwise-BA
信任和激励的 FLchain[73]	通用/理论研究	-	-	基于信誉	-
众包物联网 BFL[98]	物联网	差分隐私	联盟链	基于信誉	Algorand

3 面临挑战与未来研究方向

在前面章节中重点介绍并讨论了将联邦学习和区块链技术相结合的研究与应用的最新进展。本章中就这两种技术相组合的未来发展前景和面临的挑战进行简要讨论。

3.1 隐私保护

公开的区块链分类账可实现安全可靠的数据处理,但是收集的联邦学习训练数据可公开访问,并供所有参与方使用,这可能导致规避隐私保护机制的问题产生。此外,物联网中无处不在的传感系统不断收集消费者的个人和敏感数据,将这些数据放在开放的分类账中可能会导致隐私问题。使用私有区块链分类账可以通过启用加密和允许对分类账的受控访问来确保数据隐私,但是,此类私有区块链平台将限制联邦学习系统处理和执行的准确性,从而影响决策和分析所需的大量数据的访问和公开。

3.2 计算速度、性能问题、可扩展性

当在联邦学习系统中应用一些隐私加密算法时将导致整个系统的处理速度大幅下降,这也使得当前对于联邦学习系统的高强度隐私保护机制难以实际应用。而对于区块链系统,对于加密货币区块链平台,比特币区块链平均每秒可执行 4 笔交易,而以太坊则平均每秒可执行 12 笔交易,与 VISA 每秒处理数百万笔交易相比,这种表现实在令人无法接受。比较新的研究中,利用侧链(也称为侧通道)提高区块链的性能,其中交易在主链之外以快速方式在各方之间进行结算,并且每天仅在主链上结算一次[118]。许多新兴的区块链类型显著改善了挖掘节点的共识算法,例如像 Algorand 和 IoTA 这样的平台可以提供比以太坊和 Hyperledger 区块链[119,120]更好的性能。但是,仍需要做更多的工作来提高可扩展性,解决现存的性能问题,从而提升与联邦学习系统结合的整体系统性能。

另外,区块链的加/解密流程以及工作量证明机制,这些过程的复杂性会很大程度上降低模型训练的效率。对于较为复杂的模型,模型参数的加密以及传输都需要较长的时间,区块链中存储的迭代过程中的模型规模过大也会导致需要较大的存储成本。未来的区块链联邦学习系统还需要进一步加强其实用性,提高其在应用中的实际价值。

3.3　安全问题

以区块链以基础的联邦学习系统可能会发生去中心化权力遭到滥用的问题。尽管区块链提供了可靠的方案来保护联邦学习系统各方以及预测分析过程中的参数交换,但整个区块链系统仍然容易受到像 51% 攻击等形式的网络攻击[121]。另外,取决于矿工哈希能力的共识机制同样可能会受到损害,导致原本去中心化的平台最终集中在一些控制共识和结算的矿场周围。这种安全性问题在以太坊和比特币等公共区块链中更为明显,私有区块链平台则受此问题影响较小,因为各方之间已预定义了共识协议。

另外,当前智能合约的执行结果都是确定性的,不可能是概率性的,这可能给去中心化联邦学习系统带来关键性的问题。在这种去中心化联邦学习系统中,基于联邦学习的机器学习的决策算法由挖掘节点作为智能合约执行,其中执行结果通常是不确定的、随机的、不可预测的且通常是近似的,这需要一种创新性的解决方案来处理近似计算,并为采矿节点设计共识协议。

4　结束语

本文对联邦学习技术进行了回顾,重点对当前联邦学习技术的最新发展动向,尤其是与区块链技术相结合的新形态架构进行了梳理与总结,介绍了区块链技术如何增强和解决与联邦学习相关的关键问题。具体就去中心化的联邦学习系统、共识协议设计、隐私安全等问题进行了讨论,并对目前这方面的一些研究工作进行了比较与讨论。以上的文献综述表明,将区块链用于联邦学习的基本架构仍处于起步阶段,并且在与隐私保护,安全性与智能合约,可扩展性与性能问题,共识协议与激励机制设计等相关的领域中存在许多需要解决的挑战亟待研究。

参考文献:

[1] Bourse F, Minelli M, Minihold M, *et al*. Fast homomorphic evaluation of deep discretized neural networks[C]//Proc of Annual International Cryptology Conference. Cham: Springer, 2018: 483-512.

[2] Shi E, Chan T H H, Rieffel E, *et al*. Distributed private data analysis: lower bounds and practical constructions[J]. ACM Trans on Algorithms, 2017, 13(4): 1-38.

[3] Albrecht J P. How the GDPR will change the world[J]. European Data Protection Law Review, 2016, 2: 287.

[4] Sheth A P, Larson J A. Federated database systems for managing distributed, heterogeneous, and autonomous databases[J]. ACM Computing Surveys (CSUR), 1990, 22(3): 183-236.

[5] Kurze T, Klems M, Bermbach D, *et al*. Cloud federation[C]//Proc of the 2nd International Conference on Cloud Computing, GRIDs, and Virtualization. 2011.

[6] Bonawitz K, Eichner H, Grieskamp W, *et al*. Towards federated learning at scale: system design[EB/OL]. (2019-03-22). https://arxiv.org/abs/1902.01046.

[7] Mcmahan B, Moore E, Ramage D, *et al*. Communication-efficient learning of deep networks from decentralized data[C]//Proc of International Conference on Artificial Intelligence and Statistics. 2017: 1273-1282.

[8] Sprague M R, Jalalirad A, Scavuzzo M, *et al*. Asynchronous federated learning for geospatial applications[C]//Proc of Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Cham: Springer, 2018: 21-28.

[9] Xie Cong, Koyejo S, Gupta I. Asynchronous federated optimization[EB/OL]. (2020-12-05). https://arxiv.org/abs/1903.03934.

[10] Li Qinbin, Wen Zeyi, He Bingsheng. Practical federated gradient boosting decision trees[C]//Proc of AAAI. 2020: 4642-4649.

[11] Zhao Lingchen, Ni Lihao, Hu Shengshan, *et al*. Inprivate digging: enabling tree-based distributed data mining with differential privacy[C]//Proc of IEEE Conference on Computer Communications. Piscataway, NJ: IEEE Press, 2018: 2087-2095.

[12] Lyu Lingjuan, Yu Han, Yang Qiang. Threats to federated learning: a survey[EB/OL]. (2020-03-04). https://arxiv.org/abs/2003.02133.

[13] Chen Xinyun, Liu Chang, Li Bo, *et al*. Targeted backdoor attacks on deep learning systems using data poisoning[EB/OL]. (2017-12-15). https://arxiv.org/abs/1712.05526.

[14] Li Bo, Wang Yining, Singh A, *et al*. Data poisoning attacks on factorization-based collaborative filtering[C]//Proc of the 30th International Conference on Neural Information Processing Systems. Red Hook, NY: Curran Associates Inc., 2016: 1893-1901.

[15] Alfeld S, Zhu Xiaojin, Barford P. Data poisoning attacks against autoregressive models[C]//Proc of the 30th AAAI Conference on Artificial Intelligence. Palo Alto, CA: AAAI Press, 2016: 1452-1458.

[16] Bagdasaryan E, Veit A, Hua Y, *et al*. How to backdoor federated learning[C]//Proc of International Conference on Artificial Intelligence and Statistics. 2020: 2938-2948.

[17] Xie Chulin, Huang Keli, Chen Pinyu, *et al*. DBA: distributed backdoor attacks against federated learning[C]//Proc of International Conference on Learning Representations. 2019.

[18] Castro M, Liskov B. Practical Byzantine fault tolerance[C]//Proc of the 3rd Symposium on Operating Systems Design and Implementation. 1999: 173-186.

[19] Blanchard P, Guerraoui R, Stainer J. Machine learning with adversaries: Byzantine tolerant gradient descent[C]//Advances in Neural Information Processing Systems. 2017: 119-129.

[20] Chen Yudong, Su Lili, Xu Jiaming. Distributed statistical machine learning in adversarial settings: Byzantine gradient descent[J]. Proceedings of the ACM on Measurement and Analysis of Computing Systems, 2017, 1(2): 1-25.

[21] Su Lili, Xu Jiaming. Securing distributed machine learning in high dimensions[EB/OL]. (2018-04-26). https://arxiv.org/abs/1804.10140.

[22] Fredrikson M, Jha S, Ristenpart T. Model inversion attacks that exploit confidence information and basic countermeasures[C]//Proc of the 22nd ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2015: 1322-1333.

[23] Shokri R, Stronati M, Song Congzheng, *et al*. Membership inference attacks against machine learning models[C]//Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2017: 3-18.

[24] Melis L, Song Congzheng, De Cristofaro E, *et al*. Exploiting unintended feature leakage in collaborative learning[C]//Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2019: 691-706.

[25] Nasr M, Shokri R, Houmansadr A. Comprehensive privacy analysis of deep learning: passive and active white-box inference attacks against centralized and federated learning[C]//Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2019: 739-753.

[26] Dwork C, Mcsherry F, Nissim K, *et al*. Calibrating noise to sensitivity in private data analysis[C]//Proc of the 3rd Theory of Cryptography Conference. 2006: 265-284.

[27] El Emam K, Dankar F K. Protecting privacy using *k*-anonymity[J].

Journal of the American Medical Informatics Association, 2008, 15(5): 627-637.
[28] 刘海, 李兴华, 雒彬, 等. 基于区块链的分布式 K 匿名位置隐私保护方案[J]. 计算机学报, 2019, 42(5): 942-960. (Liu Hai, Li Xinghua, Luo Bin, *et al*. Distributed K anonymous location privacy protection scheme based on blockchain [J]. Chinese Journal of Computers, 2019, 42(5): 942-960.)
[29] Wagner I, Eckhoff D. Technical privacy metrics: a systematic survey [J]. ACM Computing Surveys (CSUR), 2018, 51(3): 1-38.
[30] Aono Y, Hayashi T, Wang Lihua, *et al*. Privacy-preserving deep learning via additively homomorphic encryption [J]. IEEE Trans on Information Forensics and Security, 2018, 13(5): 1333-1345.
[31] Hardy S, Henecka W, Ivey-Law H, *et al*. Private federated learning on vertically partitioned data via entity resolution and additively homomorphic encryption [EB/OL]. (2017-11-29). https://arxiv.org/abs/1711.10677.
[32] Chabanne H, De Wargny A, Milgram J, *et al*. Privacy-preserving classification on deep neural network [C]//Proc of the 14th Annual Conference on Privacy, Security and Trust. 2017: 35.
[33] Hall R, Fienberg S E, Nardi Y. Secure multiple linear regression based on homomorphic encryption [J]. Journal of Official Statistics, 2011, 27(4): 669.
[34] Riazi M S, Weinert C, Tkachenko O, *et al*. Chameleon: a hybrid secure computation framework for machine learning applications [C]//Proc of Asia Conference on Computer and Communications Security. New York: ACM Press, 2018: 707-721.
[35] Rouhani B D, Riazi M S, Koushanfar F. DeepSecure: scalable provably-secure deep learning [C]//Proc of the 55th Annual Design Automation Conference. New York: ACM Press, 2018: 1-6.
[36] Yuan Jiawei, Yu Shucheng. Privacy preserving back-propagation neural network learning made practical with cloud computing [J]. IEEE Trans on Parallel and Distributed Systems, 2013, 25(1): 212-221.
[37] Zhang Qingchen, Yang L T, Chen Zhikui. Privacy preserving deep computation model on cloud for big data feature learning [J]. IEEE Trans on Computers, 2015, 65(5): 1351-1362.
[38] Liu Jian, Juuti M, Lu Yao, *et al*. Oblivious neural network predictions via miniONN transformations [C]//Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 619-631.
[39] Shamir A. How to share a secret [J]. Communications of the ACM, 1979, 22(11): 612-613.
[40] Chaum D. The dining cryptographers problem: unconditional sender and recipient untraceability [J]. Journal of Cryptology, 1988, 1(1): 65-75.
[41] Bonawitz K, Ivanov V, Kreuter B, *et al*. Practical secure aggregation for federated learning on user-held data [EB/OL]. (2016-11-14). https://arxiv.org/abs/1611.04482.
[42] Du Wenliang, Zhan Zhijun. Building decision tree classifier on private data [C]//Proc of IEEE International Conference on Privacy, Security and Data Mining. 2002: 1-8.
[43] Bonawitz K, Ivanov V, Kreuter B, *et al*. Practical secure aggregation for privacy-preserving machine learning [C]//Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2017: 1175-1191.
[44] Li Ping, Li Jin, Huang Zhengan, *et al*. Multi-key privacy-preserving deep learning in cloud computing [J]. Future Generation Computer Systems, 2017, 74: 76-85.
[45] Bahmani R, Barbosa M, Brasser F, *et al*. Secure multiparty computation from SGX [C]//Proc of International Conference on Financial Cryptography and Data Security. Cham: Springer, 2017: 477-497.
[46] Gascón A, Schoppmann P, Balle B, *et al*. Secure linear regression on vertically partitioned datasets [J]. Cryptology ePrint Archive, 2016, 2016: 892.
[47] Kilbertus N, Gascón A, Kusner M J, *et al*. Blind justice: fairness with encrypted sensitive attributes [EB/OL]. (2018-06-08). https://arxiv.org/abs/1806.03281.
[48] Wan Li, Ng W K, Han Shuguo, *et al*. Privacy-preservation for gradient descent methods [C]//Proc of the 13th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM Press, 2007: 775-783.
[49] Chen V, Pastro V, Raykova M. Secure computation for machine learning with SPDZ [EB/OL]. (2019-01-02). https://arxiv.org/abs/1901.00329.
[50] Ghazi B, Pagh R, Velingker A. Scalable and differentially private distributed aggregation in the shuffled model [EB/OL]. (2019-12-02). https://arxiv.org/abs/1906.08320.
[51] Kantarcioglu M, Clifton C. Privacy-preserving distributed mining of association rules on horizontally partitioned data [J]. IEEE Trans on Knowledge and Data Engineering, 2004, 16(9): 1026-1037.
[52] Yu H, Jiang Xiaoqian, Vaidya J. Privacy-preserving SVM using nonlinear kernels on horizontally partitioned data [C]//Proc of ACM Symposium on Applied Computing. New York: ACM Press, 2006: 603-610.
[53] Karr A F, Lin Xiaodong, Sanil A P, *et al*. Privacy-preserving analysis of vertically partitioned data using secure matrix products [J]. Journal of Official Statistics, 2009, 25(1): 125.
[54] Nock R, Hardy S, Henecka W, *et al*. Entity resolution and federated learning get a federated resolution [EB/OL]. (2018-03-11). https://arxiv.org/abs/1803.04035.
[55] Yu H, Vaidya J, Jiang Xiaoqian. Privacy-preserving SVM classification on vertically partitioned data [C]//Proc of Pacific-Asia Conference on Knowledge Discovery and Data Mining. Berlin: Springer, 2006: 647-656.
[56] Goldreich O. Secure multi-party computation [EB/OL]. (2002-10-27). https://www.wisdom.weizmann.ac.il/~oded/psx/prot.pdf.
[57] Dwork C, Roth A. The algorithmic foundations of differential privacy [J]. Foundations and Trends in Theoretical Computer Science, 2014, 9(3-4): 211-407.
[58] Chaudhuri K, Monteleoni C, Sarwate A D. Differentially private empirical risk minimization [J]. Journal of Machine Learning Research, 2011, 12(3): 1069-1109.
[59] Bassily R, Smith A, Thakurta A. Private empirical risk minimization: efficient algorithms and tight error bounds [C]//Proc of the 55th IEEE Annual Symposium on Foundations of Computer Science. Piscataway, NJ: IEEE Press, 2014: 464-473.
[60] Abadi M, Chu A, Goodfellow I, *et al*. Deep learning with differential privacy [C]//Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2016: 308-318.
[61] Wu Xi, Li Fengan, Kumar A, *et al*. Bolt-on differential privacy for scalable stochastic gradient descent-based analytics [C]//Proc of ACM International Conference on Management of Data. New York: ACM Press, 2017: 1307-1322.
[62] Iyengar R, Near J P, Song D, *et al*. Towards practical differentially private convex optimization [C]//Proc of IEEE Symposium on Security and Privacy. Piscataway, NJ: IEEE Press, 2019: 299-316.
[63] Li Qinbin, Wu Zhaomin, Wen Zeyi, *et al*. Privacy-preserving gradient boosting decision trees [C]//Proc of AAAI Conference on Artificial Intelligence. 2020: 784-791.
[64] Andrew G, Thakkar O, Mcmahan H B, *et al*. Differentially private learning with adaptive clipping [EB/OL]. (2021-03-12). https://arxiv.org/abs/1905.03871.
[65] Song Shuang, Chaudhuri K, Sarwate A D. Stochastic gradient descent

with differentially private updates[C]//Proc of IEEE Global Conference on Signal and Information Processing. Piscataway, NJ: IEEE Press,2013:245-248.

[66] 张啸剑,孟小峰. 面向数据发布和分析的差分隐私保护[J]. 计算机学报,2014,37(4):927-949. (Zhang Xiaojian, Meng Xiaofeng. Differential privacy in data publication and analysis[J]. Chinese Journal of Computers,2014,37(4):927-949.)

[67] Goryczka S, Xiong Li. A comprehensive comparison of multiparty secure additions with differential privacy[J]. IEEE Trans on Dependable and Secure Computing,2017,14(5):463-477.

[68] Xu Runhua, Baracaldo N, Zhou Yi, *et al*. Hybridalpha: an efficient approach for privacy-preserving federated learning[C]//Proc of the 12th ACM Workshop on Artificial Intelligence and Security. New York: ACM Press,2019:13-23.

[69] Liu Yang, Chen Tianjian, Yang Qiang. Secure federated transfer learning[EB/OL]. (2020-06-24). https://arxiv.org/abs/1812.03337.

[70] Du Wenliang, Han Y S, Chen Shigang. Privacy-preserving multivariate statistical analysis: linear regression and classification[C]//Proc of SIAM International Conference on Data Mining. 2004:222-233.

[71] Yang T, Andrew G, Eichner H, *et al*. Applied federated learning: improving google keyboard query suggestions[EB/OL]. (2018-12-07). https://arxiv.org/abs/1812.02903.

[72] Awan S, Li Fengjun, Luo Bo, *et al*. Poster: a reliable and accountable privacy-preserving federated learning framework using the blockchain[C]//Proc of ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press,2019:2561-2563.

[73] Bao Xianglin, Su Cheng, Xiong Yan, *et al*. FLChain: a blockchain for auditable federated learning with trust and incentive[C]//Proc of the 5th International Conference on Big Data Computing and Communications. 2019:151-159.

[74] Kang Jiawen, Xiong Zehui, Niyato D, *et al*. Incentive mechanism for reliable federated learning: a joint optimization approach to combining reputation and contract theory[J]. IEEE Internet of Things Journal,2019,6(6):10700-10714.

[75] Kim H, Park J, Bennis M, *et al*. Blockchained on-device federated learning[J]. IEEE Communications Letters,2019,24(6):1279-1283.

[76] Kim Y J, Hong C S. Blockchain-based node-aware dynamic weighting methods for improving federated learning performance[C]//Proc of the 20th Asia-Pacific Network Operations and Management Symposium. 2019:1-4.

[77] Lu Yunlong, Huang Xiaohong, Dai Yueyue, *et al*. Blockchain and federated learning for privacy-preserved data sharing in industrial IoT[J]. IEEE Trans on Industrial Informatics,2019,16(6):4177-4186.

[78] Majeed U, Hong C S. FLChain: federated learning via MEC-enabled blockchain network[C]//Proc of the 20th Asia-Pacific Network Operations and Management Symposium. 2019:1-4.

[79] Weng Jiasi, Weng Jian, Zhang Jilian, *et al*. DeepChain: auditable and privacy-preserving deep learning with blockchain-based incentive[J]. IEEE Trans on Dependable and Secure Computing,2021,18(5):2438-2455.

[80] Lalitha A, Kilinc O C, Javidi T, *et al*. Peer-to-peer federated learning on graphs[EB/OL]. (2019-01-31). https://arxiv.org/abs/1901.11173.

[81] Lalitha A, Wang Xinghan, Kilinc O, *et al*. Decentralized Bayesian learning over graphs[EB/OL]. (2019-05-24). https://arxiv.org/abs/1905.10466.

[82] Savazzi S, Nicoli M, Rampa V. Federated learning with cooperating devices: a consensus approach for massive IoT networks[J]. IEEE Internet of Things Journal,2020,7(5):4641-4654.

[83] Hu Chenghao, Jiang Jingyan, Wang Zhi. Decentralized federated learning: a segmented gossip approach[EB/OL]. (2019-08-21). https://arxiv.org/abs/1908.07782.

[84] Roy A G, Siddiqui S, Pölsterl S, *et al*. Braintorrent: a peer-to-peer environment for decentralized federated learning[EB/OL]. (2019-05-16). https://arxiv.org/abs/1905.06731.

[85] Shayan M, Fung C, Yoon C J, *et al*. Biscotti: a ledger for private and secure peer-to-peer machine learning[EB/OL]. (2019-12-12). https://arxiv.org/abs/1811.09904.

[86] 袁勇,倪晓春,曾帅,等. 区块链共识算法的发展现状与展望[J]. 自动化学报,2018,44(11):2011-2022. (Yuan Yong, Ni Xiaochun, Zeng Shuai, *et al*. Blockchain consensus algorithms: the state of the art and future trends[J]. Acta Automatica Sinica,2018,44(11):2011-2022.)

[87] 刘怡然,柯俊明,蒋瀚,等. 基于沙普利值计算的区块链中 PoS 共识机制的改进[J]. 计算机研究与发展,2018,55(10):2208-2218. (Liu Yiran, Ke Junming, Jiang Han, *et al*. Improvement of the PoS consensus mechanism in blockchain based on Shapley value[J]. Journal of Computer Research and Development,2018,55(10):2208-2218.)

[88] 谈森鹏,杨超. 区块链 DPoS 共识机制的研究与改进[J]. 现代计算机:专业版,2019(6):11-14. (Tan Senpeng, Yang Chao, Research and improvement of block chain DPoS consensus mechanism[J]. Mo-dern Computer: Professional,2019(6):11-14.)

[89] Chen Xuhui, Ji Jinlong, Luo Changqing, *et al*. When machine learning meets blockchain: a decentralized, privacy-preserving and secure design[C]//Proc of IEEE International Conference on Big Data. Piscataway, NJ: IEEE Press,2018:1178-1187.

[90] Ramanan P, Nakayama K. BAFFLE: blockchain based aggregator free federated learning[EB/OL]. (2020-10-18). https://arxiv.org/abs/1909.07452.

[91] Zhou Sicong, Huang Huawei, Chen Wuhui, *et al*. PIRATE: a blockchain-based secure framework of distributed machine learning in 5G networks[EB/OL]. (2019-12-17). https://arxiv.org/abs/1912.07860.

[92] Li Suyi, Cheng Yong, Liu Yang, *et al*. Abnormal client behavior detection in federated learning[EB/OL]. (2019-12-06). https://arxiv.org/abs/1910.09933.

[93] Hieu N Q, Anh T T, Luong N C, *et al*. Resource management for blockchain-enabled federated learning: a deep reinforcement learning approach[EB/OL]. (2020-05-01). https://arxiv.org/abs/2004.04104.

[94] Ur Rehman M H, Salah K, Damiani E, *et al*. Towards blockchain-based reputation-aware federated learning[C]//Proc of International Symposium on Edge Computing Security and Blockchain. 2020.

[95] Yin Bo, Yin Hao, Wu Yulei, *et al*. FDC: a secure federated deep learning mechanism for data collaborations in the Internet of Things[J]. IEEE Internet of Things Journal,2020,7(7):6348-6359.

[96] Li Yuzheng, Chen Chuan, Liu Nan, *et al*. A blockchain-based decentralized federated learning framework with committee consensus[EB/OL]. (2020-04-02). https://arxiv.org/abs/2004.00773.

[97] Liu Yi, Peng Jialiang, Kang Jiawen, *et al*. A secure federated learning framework for 5G networks[EB/OL]. (2020-05-12). https://arxiv.org/abs/2005.05752.

[98] Zhao Yang, Zhao Jun, Jiang Linshan, *et al*. Privacy-preserving blockchain-based federated learning for IoT devices[EB/OL]. (2021-02-01). https://arxiv.org/abs/1906.10893.

[99] Qu Youyang, Gao Longxiang, Luan T H, *et al*. Decentralized privacy using blockchain-enabled federated learning in fog computing[J]. IEEE Internet of Things Journal,2020,7(6):5171-5183.

[100] Preuveneers D, Rimmer V, Tsingenopoulos I, *et al*. Chained anomaly detection models for federated learning: an intrusion detection case study[J]. Applied Sciences,2018,8(12):2663.

[101] Kim H, Park J, Bennis M, *et al*. Blockchained on-device federated learning[EB/OL]. (2018-08-12). https://arxiv.org/abs/1808.03949.

[102] Lu Yunlong, Huang Xiaohong, Zhang Ke, *et al*. Blockchain empowered asynchronous federated learning for secure data sharing in Internet of Vehicles[J]. IEEE Trans on Vehicular Technology, 2020, 69(4): 4298-4311.

[103] Kang Jiawen, Xiong Zehui, Niyato D, *et al*. Incentive design for efficient federated learning in mobile networks: a contract theory approach[C]//Proc of IEEE VTS Asia Pacific Wireless Communications Symposium. Piscataway, NJ: IEEE Press, 2019: 1-5.

[104] Zhan Yufeng, Li Peng, Qu Zhihao, *et al*. A learning-based incentive mechanism for federated learning[J]. IEEE Internet of Things Journal, 2020, 7(7): 6360-6368.

[105] Pokhrel S R, Choi J. Federated learning with blockchain for autonomous vehicles: analysis and design challenges[J]. IEEE Trans on Communications, 2020, 68(8): 4734-4746.

[106] Konečný J, Mcmahan H B, Ramage D, *et al*. Federated optimization: distributed machine learning for on-device intelligence[EB/OL]. (2016-10-08). https://arxiv.org/abs/1610.02527.

[107] Wang Guan, Dang C X, Zhou Ziye. Measure contribution of participants in federated learning[C]//Proc of IEEE International Conference on Big Data. Piscataway, NJ: IEEE Press, 2019: 2597-2604.

[108] Lugan S, Desbordes P, Brion E, *et al*. Secure architectures implementing trusted coalitions for blockchained distributed learning (TCLearn)[J]. IEEE Access, 2019, 7: 181789-181799.

[109] Yurochkin M, Agarwal M, Ghosh S, *et al*. Bayesian nonparametric federated learning of neural networks[EB/OL]. (2019-05-28). https://arxiv.org/abs/1905.12022.

[110] Pandey S R, Tran N H, Bennis M, *et al*. Incentivize to build: a crowdsourcing framework for federated learning[C]//Proc of IEEE Global Communications Conference. Piscataway, NJ: IEEE Press, 2019: 1-6.

[111] Zyskind G, Nathan O. Decentralizing privacy: using blockchain to protect personal data[C]//Proc of IEEE Security and Privacy Workshops. Piscataway, NJ: IEEE Press, 2015: 180-184.

[112] Eyal I, Gencer A E, Sirer E G, *et al*. Bitcoin-NG: a scalable blockchain protocol[C]//Proc of the 13th USENIX Symposium on Networked Systems Design and Implementation. 2016: 45-59.

[113] Samek W, Wiegand T, Müller K-R. Explainable artificial intelligence: understanding, visualizing and interpreting deep learning models[EB/OL]. (2017-08-28). https://arxiv.org/abs/1708.08296.

[114] Jurca R, Faltings B. An incentive compatible reputation mechanism[C]//Proc of IEEE International Conference on E-Commerce. Piscataway, NJ: IEEE Press, 2003: 285-292.

[115] Naor M, Pinkas B, Sumner R. Privacy preserving auctions and mechanism design[C]//Proc of the 1st ACM Conference on Electronic Commerce. New York: ACM Press, 1999: 129-139.

[116] Doku R, Rawat D B, Liu Chunmei. Towards federated learning approach to determine data relevance in big data[C]//Proc of the 20th IEEE International Conference on Information Reuse and Integration for Data Science. Piscataway, NJ: IEEE Press, 2019: 184-192.

[117] Martinez I, Francis S, Hafid A S. Record and reward federated learning contributions with blockchain[C]//Proc of International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery. 2019: 50-57.

[118] Hwang G H, Chen P H, Lu C H, *et al*. InfiniteChain: a multi-chain architecture with distributed auditing of sidechains for public blockchains[C]//Proc of International Conference on Blockchain. Cham Springer, 2018: 47-60.

[119] Boyen X, Carr C, Haines T. Graphchain: a blockchain-free scalable decentralised ledger[C]//Proc of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts. New York: ACM Press, 2018: 21-33.

[120] Gilad Y, Hemo R, Micali S, *et al*. Algorand: scaling Byzantine agreements for cryptocurrencies[C]//Proc of the 26th Symposium on Operating Systems Principles. New York: ACM Press, 2017: 51-68.

[121] Li Xiaoqi, Jiang Peng, Chen Ting, *et al*. A survey on the security of blockchain systems[J]. Future Generation Computer Systems, 2020, 107: 841-853.

(上接第 3221 页)

[54] Bengio Y, Courville A, Vincent P. Representation learning: a review and new perspectives[J]. IEEE Trans on Pattern Analysis & Machine Intelligence, 2013, 35(8): 1798-1828.

[55] Hochreiter S, Schmidhuber J. Long short-term memory[J]. Neural Computation, 1997, 9(8): 1735-1780.

[56] 周风顺, 王林章, 李宣东. C/C++程序缺陷自动修复与确认方法[J]. 软件学报, 2019, 30(5): 1243-1255. (Zhou Fengshun, Wang Linzhang, Li Xuandong. Automatic defect repair and validation approach for C/C++ programs[J]. Journal of Software, 2019, 30(5): 1243-1255.)

[57] Gong Qucheng, Tian Yuandong, Zitnick C L. Unsupervised program induction with hierarchical generative convolutional neural networks[C]//Proc of the 5th International Conference on Learning Representations. 2017.

[58] Cochran R A, D'Antoni L, Livshits B, *et al*. Program boosting: program synthesis via crowd-sourcing[J]. ACM SIGPLAN Notices, 2015, 50(1): 677-688.

[59] Zhai Juan, Huang Jianjun, Ma Shiqing, *et al*. Automatic model generation from documentation for Java API functions[C]//Proc of the 38th International Conference on Software Engineering. New York: ACM Press, 2016: 380-391.

[60] 胡星, 李戈, 刘芳, 等. 基于深度学习的程序生成与补全技术研究进展[J]. 软件学报, 2019, 30(5): 1206-1223. (Hu Xing, Li Ge, Liu Fang, *et al*. Program generation and code completion techniques based on deep learning: literature review[J]. Journal of Software, 2019, 30(5): 1206-1223.)

[61] Hindle A, Barr E T, Su Zhendong, *et al*. On the naturalness of software[C]//Proc of the 34th International Conference on Software Engineering. Piscataway, NJ: IEEE Press, 2012: 837-847.

[62] Jian Jian, Wang Yue, Lyu M R, *et al*. Code completion with neural attention and pointer networks[C]//Proc of the 27th International Joint Conference on Artificial Intelligence. Palo Alto, CA: AAAI Press, 2018: 4159-4225.

[63] Raychev V, Vechev M, Yahav E. Code completion with statistical language models[J]. ACM SIGPLAN Notices, 2014, 49(6): 419-428.

[64] Deisenbock F, Pizka M. Concise and consistent naming[C]//Proc of the 13th International Workshop on Program Comprehension. Piscataway, NJ: IEEE Press, 2005: 97-106.

[65] 高原, 刘辉, 樊孝忠, 等. 基于代码库和特征匹配的函数名称推荐方法[J]. 软件学报, 2015, 26(12): 3062-3074. (Gao Yuan, Liu Hui, Fan Xiaozhong, *et al*. Method name recommendation based on source code depository and feature matching[J]. Journal of Software, 2015, 26(12): 3062-3074.)

[66] Allamanis M, Barr E T, Bird C, *et al*. Learning natural coding conventions[EB/OL]. (2014-04-07). http://doi.org/10.1145/2635868.2635883.

[67] Allamanis M, Barr E, Bird C A, *et al*. Suggesting accurate method and class names[C]//Proc of the 10th Joint Meeting on Foundations of Software Engineering. New York: ACM Press, 2015: 38-49.

[68] Biggerstaff T J, Mitbander B G, Webster D E. Program under-standing and the concept assignment problem[J]. Communications of the ACM, 1994, 37(5): 72-82.