

融合区块链和联邦学习技术的数据资产流通交易方案研究

莫梓嘉¹, 赵晨²

1. 中国工商银行博士后科研工作站, 北京 100140;

2. 宁波工程学院网络空间安全学院, 浙江 宁波 315211

摘要

作为重要生产要素, 数据资产正逐步演变为推动我国稳增长、促转型的重要引擎。然而, 数据资产的流通交易面临多重挑战, 包括交易前的数据真实性和隐私性、交易中的安全性与可信性, 以及交易后的可靠性与可溯性问题。针对此, 提出了一种融合区块链和联邦学习技术的链上链下数据资产流通交易方案, 旨在通过研究数据可信交互框架、多源敏感数据确权与隐私保护技术、数据全生命周期可信保障技术及异常交易数据溯源机制, 确保数据资产流通交易的高安全性、高隐私性及可追溯性, 构建高效、安全、可信的数据资产流通交易体系, 推动数据要素市场安全有序、平稳持续发展, 为我国数字经济高质量发展提供技术支持。

关键词

数据资产; 数据交易; 区块链; 联邦学习

中图分类号: TP181

文献标志码: A

doi:10.11959/j.issn.2096-0271.2025068

Research on data asset circulation and trading scheme integrating blockchain and federated learning technologies

MO Zijia¹, ZHAO Chen²

1. Postdoctoral Research Center, Industrial and Commercial Bank of China, Beijing 100140, China

2. School of Cyber Science and Engineering, Ningbo University of Technology, Ningbo 315211, China

Abstract

As a key production factor, data assets are gradually evolving into a crucial engine driving China's stable growth and economic transformation. However, the circulation and trading of data assets face multiple challenges, including issues related to data authenticity and privacy before transactions, security and trustworthiness during transactions, and reliability and traceability after transactions. In response to these challenges, the study proposes an on-chain and off-chain data asset circulation and trading scheme that integrates blockchain and federated learning technologies. The study focuses on establishing a trustworthy data interaction framework, technologies for ownership confirmation and privacy protection of multi-source sensitive data, as well as full-lifecycle data trustworthiness assurance and abnormal transaction traceability mechanisms. This approach ensures high security, privacy, and traceability in the circulation and trading of data assets, aiming to build an efficient, secure, and trustworthy data asset trading system that promotes the

safe, orderly, and sustainable development of the data element market, thereby providing technical support for the high-quality development of China's digital economy.

Key words

data asset, data trading, blockchain, federated learning

0 引言

伴随着互联网产业和大数据、人工智能、区块链等新一代信息技术的兴起,全球经济步入了数字经济时代。为了提高数字化建设水平,推动数字经济社会和信息化行业的健康高速发展,2020年4月,中共中央、国务院颁布的《关于构建更加完善的要素市场化配置体制机制的意见》明确将数据纳入生产要素,并提出“加快培育数据要素市场”“加强数据资源整合和安全保护”等要求。数据要素化发展的前提是实现数据的自由流转交易,激发价值转化,实现经济价值变现。2022年,《“十四五”数字经济发展规划》中明确指出,要加快构建数据要素市场规则,规范数据交易管理,提升数据交易效率。当前,数据要素市场化已成为建设数字中国的关键引擎,数据资产时代已然来临^[1]。

数据资产的流通交易环境成为制约数据要素市场建立的重要因素。究其原因,数据资产具有复杂性、动态性、无限性等明显区别于传统要素的特殊属性^[2],在流通交易过程中涉及多方主体,难以形成安全可信的交易环境。为了保障数据资产安全可信、集约高效地流通交易,构建安全、合规、可信的数据资产流通交易技术体系成为学术界和产业界关注的热点问题。

近年来,国内外学者和研究组织尝试利用区块链(blockchain)技术的分布式

存储、极难篡改、匿名性和可追溯性等特性来解决上述问题^[3]。但从数据资产流通交易的全生命周期视角看,当前大部分研究仍存在以下问题。

(1) 交易前的数据真实性和隐私性问题

数据资产交易事前安全风险可归纳为信息不对称风险和隐私泄露风险两方面。一方面,数据资产的流通交易过程缺乏透明性,交易双方存在信息不对称现象,导致数据的真实性难以验证,质量难以评估,进而使数据市场交易秩序无法建立,抑制了数据的共享和流通,无法有效激活数据资产的价值和创新应用,最终限制了数据资产交易的规模。另一方面,数据资产在流通过程中涉及多个交易主体,在不可信环境中容易受到第三方的访问和利用,使隐私数据的泄露风险大大提高。

(2) 交易中的数据安全性和可信性问题

在数据传输过程中,现阶段多数机构和企业依然采用传统的中心化交易方式,这意味着所有的数据流都必须经过一个中心节点。这种集中式的交易方式为恶意攻击者提供了机会,一旦中心节点遭受攻击,整个系统的数据都可能受到威胁。此外,单一的交易环境无法保证数据不被恶意篡改或违规伪造。

(3) 交易后的数据可靠性和可溯性问题

尽管国家已经出台《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等数据管理法规和政策,但是数据

保护的精细化程度和可操作性尚存不足,各种监管机构及其监管手段并没有充分融通^[1]。数据交付后的使用权限难以控制,难以从大量冗余信息中获知异常行为之间的内在关联,数据泄露、违规操作、异常交易等问题难以发现。

上述问题使数据流通交易确权难、互信难、入场难、监管难。因此,迫切需要寻求一种方法,实现数据资产流通交易的高安全性、高隐私性以及可追溯性,促进数据市场安全有序、平稳持续发展。

联邦学习(federated learning, FL)作为一种新兴的分布式机器学习框架,可以在保护数据隐私的前提下进行模型训练与数据共享,从而避免原始数据上传与数据泄露问题^[4]。具体来说,联邦学习通过一个中央服务器协调各个参与方(客户端)来实现模型协同训练,客户端基于本地数据集进行模型训练,并根据服务器的参数聚合结果进行模型更新,所有更新操作都是针对模型而非数据的。各个参与方通过交换加密模型参数来达到知识共享的效果,实现了敏感数据不出本地的目的,极大降低了数据采集带来的隐私泄露风险。另外,由于不需要提供原始数据,联邦学习为多方数据交易提供了一种高效且安全的方法,尤其是规避了数据跨境交易的复杂性和安全风险,有效解决了“数据孤岛”问题。不同于传统的分布式训练技术,联邦学习考虑到了数据隐私、数据分布、传输瓶颈等问题,有望打破各领域、各行业的数据壁垒。基于此,研究融合区块链和联邦学习技术的数据资产交易可信保障技术,能够优化数据交易治理体系,稳步推进数据价值化和资产化,对增强我国科技自主创新能力、加快形成数据要素市场体系、推动高质量发展具有重要意义。

本文将紧密围绕数据资产流通交易中

的3个关键问题,结合与多元主体、多源数据、多层业务等进行交互的实际应用情况,从保障数据来源真实性、传输可靠性、隐私安全性等角度出发,构建融合区块链和联邦学习技术的链上链下数据资产流通交易保障技术体系,以实现数据资产流通交易的高安全性、高隐私性以及可追溯性,促进数据市场安全有序、平稳持续发展。

1 现有工作

在交易事前的敏感数据确权方面,Shafagh等人^[5]较早地讨论了区块链系统访问权限控制的3个关键问题:实体授权、基于访问控制规则的策略执行和去中心化访问权限评估。基于此,Zhang等人^[6]研发了面向数据访问控制的认证数据馈送系统Town Crier,通过跨链可信组件混合计算方法为智能合约提供源数据认证服务,但是该方案并未考虑用户信息隐私问题。针对这个问题,Liu等人^[7]将超级账本技术和基于属性的加密方案相结合来实现去中心化环境下隐私数据共享的细粒度访问控制,然而该方法在大规模节点访问的情况下难以保证权限执行的灵活性。

在交易事中的安全可信交互方面,Xiong等人^[8]通过融合联盟链和智能合约技术,提出基于声誉的数据共享机制确保高质量数据共享,但是该机制将数据存储在云端,对于边缘节点需求的响应不足。蔡亮等人^[9]提出了一种结合粗粒度和细粒度双层协同的联盟链数据交互方法,但是该方法尚未结合隐私保护机制,存在信息泄露的风险。周炜等人^[10]提出基于区块链的隐私保护去中心化联邦学习模型,该方案使用同态加密技术防止模型中间参数的泄

露，并通过选举得出的联邦学习委员会进行模型聚合和协同解密，然而该模型难以实现不同业务的跨链交互。

在交易事后的监管权限控制方面，目前国内外尚未开展大规模面向区块链交易事后的异常溯源研究。陈纯院士在2019年总结了目前区块链监管发展的4种思路^[11]：区块链节点的追踪与可视化、联盟链的穿透式监管技术、公有链的主动发现与探测技术、以链治链的体系结构及标准。进一步地，经普杰等人^[12]提出一种分层跨链的监管架构，设计了监管链-业务链跨链协作的以链治链的监管模式，但上述方案仅为理论分析，尚未实现落地应用。

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的同时确保数据隐私与安全。目前，基于区块链的联邦学习研究尚处于起步阶段，现有研究缺乏面向数据资产流通交易的架构模型、理论体系的相关文章。总体来说，本文在对数据资产流通交易全面调研的基础上，从利用区块链赋能联邦学习的角度出发，首次提出区块链与联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、关键技术以及未来研究方向，旨在为该领域的发展提供借鉴。

2 面向数据资产流通交易的安全可信技术方案

本文以数据资产的流通交易为研究对象，从保障交易前的数据真实性和隐私性、交易中的数据安全性和可信性、交易后的数据可靠性和可溯性角度出发，从构建融

合区块链和联邦学习的链上链下数据可信交互框架入手，针对数据交易过程中存在的数据确权难、可信交互差、溯源监管效率低问题，提出多源敏感数据确权、数据全生命周期可信交互、异常交易数据溯源监管等技术方案，如图1所示。

具体来说，针对系统结构可扩展和数据一致性保障等问题，本文提出链上链下数据可信交互框架，为数据资产的流通交易提供基础理论技术框架支撑：针对链下数据真实性和隐私性问题，探讨面向链下多源敏感数据的可信确权与隐私保护技术，包括可信数据确权与标记、敏感数据访问控制与分布式离链存储相关内容；针对链上数据有效性和可信性问题，探讨面向链上数据交易全生命周期可信保障机制，包括提出数据安全上链保障机制、数据链上通信机制以解决链上通信与安全交互问题；针对数据交易的可靠性和可追溯性问题，探讨链上异常交易数据的溯源机制，包括基于图神经网络的异常交易识别和溯源方法，通过受控回滚技术实现数据资产溯源。

2.1 融合区块链与联邦学习的链上链下数据可信交互框架

将区块链与联邦学习用于数据管理可有效防止数据被篡改，并且能够在弱信任环境下实现多主体的数据安全流通和协作。联邦学习能够保障用户隐私数据不出本地，交易双方只能确定运算结果而无法获知实际的数据，从根本上杜绝了隐私泄露的情况。同时，区块链的去中心化特点可保障数据资产提供方的合法权益不受侵犯，保证数据交易执行的公平公正性和极难篡改性，能够降低数据交易的信任成本。最后，融合联邦学习和区块链的数据流通交易机制可在保证交易可靠性的同时维护交易双方利益。一方面，可以通过分析区块链链

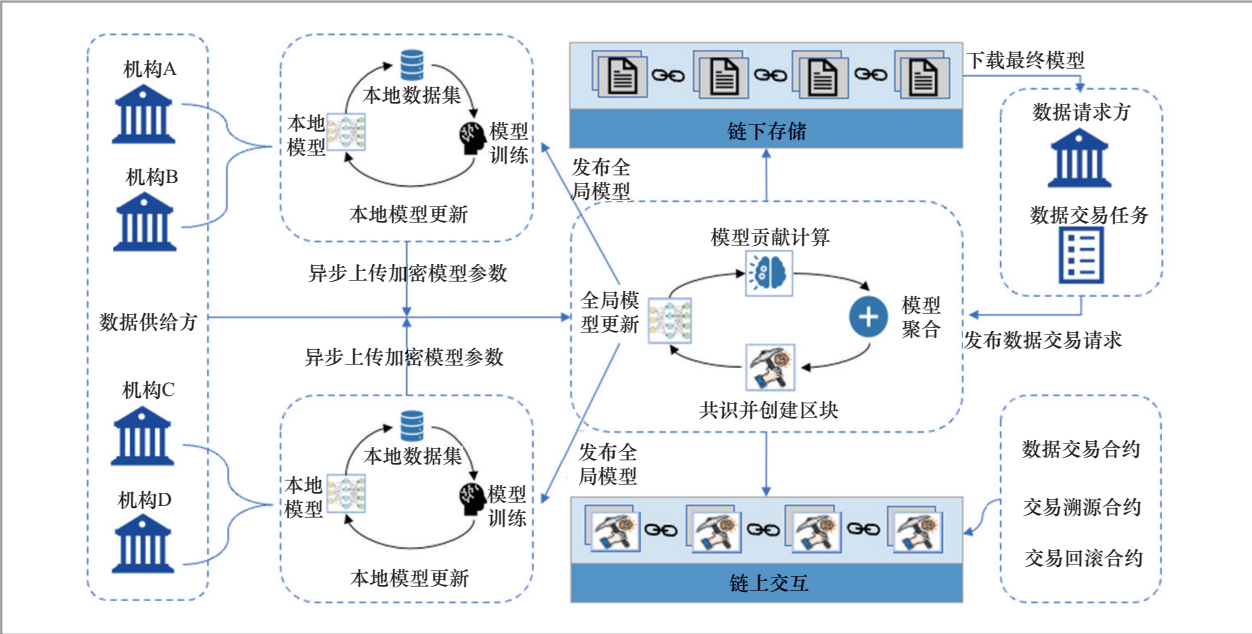


图1 面向数据资产流通交易的安全可信技术方案

上节点行为来捕捉可疑交易行为；另一方面，基于联邦学习的交易模型可以基于历史数据交易信息来识别可疑数据交易序列，并将该序列信息与历史恶意交易序列进行比较，从而提前识别数据攻击类型，及时防范恶意攻击等安全风险。除此之外，区块链可以通过自定义智能合约来自动化地管理不同供应方的多轮交易任务，同时还可以通过激励机制激励更多用户参与交易生态系统共建，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^[13]。

基于此，本文提出了链上链下数据可信交互层次体系模型，明确了不同层次之间的关系和功能定位。具体框架如图2所示。

数据资产的买方、卖方、管理者作为参与节点具有区块链和联邦学习的双重身份。买方和卖方仅对自己参与的数据资产有访问权限，可以通过信息加密对访问权

限进行控制。为了保证系统的稳定性和安全性，所有参与节点在交易开始前均具有基础信誉值，并参与信誉值评估体系。信誉值在参与联邦学习训练以及区块链共识过程时动态改变，低于系统设定的阈值时，节点将无法参与数据资产的流通交易过程。

在数据层，针对数据交易环境中数据来源广泛且敏感信息丰富的问题，建立标准化适配模块，同时使用加密算法来保证安全与隐私性；在模型层，通过联邦学习技术上传模型训练参数，并设置模型贡献度激励机制以鼓励节点积极参与数据共享，同时引入模型水印以防止公开模型被盗用；在合约层，通过建立智能合约实现数据交易自动化管理，基于联盟链进行数据确权上链，实现对数据的快速完整性校验；在溯源层，通过构建基于图神经网络的节点关系度量机制，计算异常交易源头的概率，并通过聚类的中心性排名排除无关干扰项。

本文所提节点模型的联邦学习训练主

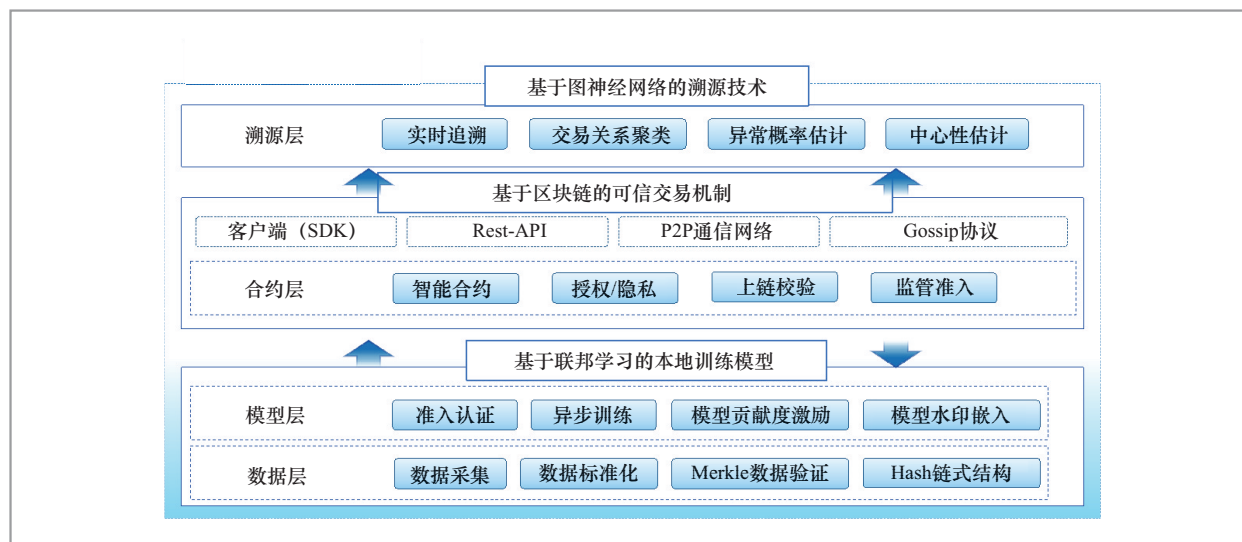


图2 融合区块链与联邦学习的链上链下数据可信交互框架示意图

要包括两个阶段，分别是每个参与节点维护的本地模型更新阶段和使用聚合算法生成的全局模型更新阶段。其中，节点的本地模型训练损失函数定义为：

$$\arg \min_{\theta_i} F_i(\theta_i) := \sum_{(x_i, y_i) \in D_i} L_i(f(x_i; \theta_i), y_i) \quad (1)$$

其中，节点 i 的本地数据被定义为 $(x_i, y_i) \in D_i$ ，该节点拥有本地模型参数 θ_i ，模型参数会在本地独立多次更新，并在更新后将参数发送给虚拟中心节点进行加权平均。所有参与节点的训练目标是在不泄露隐私数据的前提下进行本地模型训练，从而获得全局最优模型。

传统的联邦学习方法存在一个中心服务器以聚合多节点上传的模型参数，一旦中心服务器被攻击，可能会造成模型输出不可用以及节点参数数据泄露的情况^[3]。鉴于此，本文所提方案使用区块链技术代替中心服务器，以点对点通信网络构建去中心化协议，规避系统性安全风险。在参与节点完成本地训练后，将模型参数、模型性能提升率作为凭证打包为区块，并向

智能合约发起交易，智能合约经过共识验证后记录在区块链上，并根据该区块对全局模型性能贡献程度给予节点信誉值奖励，为训练过程提供防篡改和激励机制。

2.2 面向链下多源敏感数据的可信确权与隐私保护技术

传统的区块链区块之间使用链表结构将所有区块首尾相连，并在区块内部使用默克尔树（Merkle tree）结构存储数据，这种方式虽然能够有效防篡改，但查询方式过于简单，使得链上数据查询效率较低。然而在数据资产的流通交易场景中，数据频繁交互的需求使得链上数据查询效率变高。因此，本文所提框架基于 MPT（Merkle Patricia tree）和链式存储相结合的关键技术，对海量异构多源数据特征进行标准化处理，为后续数据可信共享提供数据规范；同时通过数据交互和计算交互实现高性能分布式实时区块模型多级协同优化，确保数据资产流通交易安全可信。该方法结合了默克尔树和前缀树两种数据结构，能够用最少

的哈希计算完成数据校验，同时实现节点
的快速插入和删除，保证数据可验证^[14]。

2.3 面向链上数据交易全生命周期的可信保障技术

基于区块链的数据资产流通交易模式与传统的公有链应用场景不同^[15]，由于数据资产交易场景丰富多样，单链的性能越来越难以满足实际应用需求。因此，区块链跨链交互通信技术成为研究热点。目前主流的跨链技术中公证人机制、侧链中继和哈希锁定技术方案都存在一定缺陷^[16]，而预言机作为链接链上智能合约和链下真实数据的可信中间件，能够保证多链数据交互的一致性与可靠性^[17]。因此，本文所提框架中区块链的通信机制为基于椭圆曲线算法的跨链安全传输通信协议，保证跨链数据传输过程中的安全性。在发起跨链请求之前，参与节点向预言机服务器A申请注册，并获取基于椭圆曲线的加密密钥，之后在分布式账本上发起跨链数据请求，预言机服务器B使用对称密钥解密并验证签名，验签成功后读取数据并返回。基于预言机的跨链数据安全传输方案能够兼容多链数据交互，同时抵御重放攻击、假冒攻击、中间人攻击等攻击方式，满足安全通信需求。

2.4 面向链上异常交易数据的溯源机制

目前关于区块链链上链下的异常交易识别与溯源缺少相关研究，大多研究聚焦于交易数据分析。因此，本文所提框架的交易溯源机制为基于图神经网络的异常交易识别和溯源方法，通过对区块链交易拓扑建立节点特征矩阵的方法建立特征相似度矩阵，得到未知交易属性的标签值矩阵，并将构建区块链交易拓扑图进行区块链异常交易识别。进

一步地，向图神经网络模型输入区块链拓扑图的邻接矩阵和初始特征矩阵，以模拟得到异常交易的异常传播过程，实现对可疑交易有害数据的快速检测和有效监管，保证数据的可追溯和受控回滚。

3 融合区块链和联邦学习的链上链下数据可信交互框架原理验证

为了验证本文所提框架的有效性，笔者在MNIST数据集和FMNIST数据集上对所提框架进行了初步评估。MNIST数据集、FMNIST数据集均为来自真实世界的数据集，可代表数据资产流通交易应用中数据供给方拥有的复杂度中等的的数据，也被大量区块链和联邦学习算法研究作为实验数据集使用。数据集被平均分为 N 个子集分配给 N 个用户，实验使用轻量级卷积神经网络作为本地模型（该网络由2个 5×5 卷积层、一个全连接层和一个Softmax输出层构成）。实验中本地模型训练的迭代周期为5个训练轮次。为了公平测试所提方法性能，本文采用传统实用拜占庭容错（practical Byzantine fault tolerance, PBFT）共识算法作为区块链共识算法，以达到高吞吐量和低共识时延的目的。

图3和图4给出了在不同参与数据分享的用户数量情况下，本文所提框架在MNIST数据集和FMNIST数据集上的准确率。为了更加贴近实际应用中的真实场景，实验将随机选取3个通信和计算能力较差的用户作为低质量参与者，并通过随机噪声干扰原始参数为模型聚合过程提供较低的模型质量。实验结果表明，本文所提框架具有良好的精确度和稳定的收敛速度，由于数据集本身结构更加复杂，本文所提算法在FMNIST数据集上的全局准确率结果略低于MNIST数据集，但是同样能够达到较高的

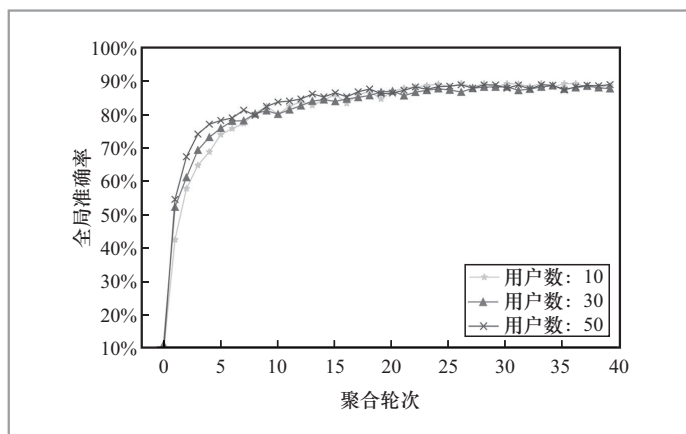


图3 MNIST数据集上不同用户数量的全局准确率

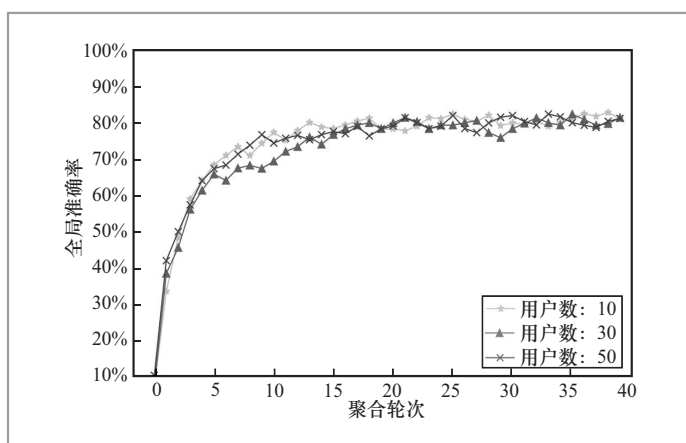


图4 FMNIST数据集上不同用户数量的全局准确率

精度,证明了本文所提方案对不同数据集的通用性。当参与训练的用户数量变化时,随着训练迭代次数的增加,全局准确率结果有小幅的降低,但整体差异不大。实验结果变化的幅度较小,说明本文所提框架具有良好的可扩展性,并且能够有效减少低质量用户对整体系统精准度的影响。

以上实验可以证明,参与数据共享的用户数量的增加对本文所提方案的准确性影响不大,初步证明了所提方案在数据交易应用中的可行性。

4 进一步研究的问题

现阶段,融合区块链与联邦学习的计算架构已在医疗、车联网、智慧城市等许多数据共享和多方协作场景中得到研究和应用。与上述弱信任场景类似,数据交易场景同样面临基于不完备数据的多方共享与协作及其隐私保护问题^[13]。尽管本文提出的融合区块链与联邦学习的链上链下数据可信交互框架能够有效解决部分挑战,但对于区块链与联邦学习系统的固有通信、异构和共识问题仍存在缺陷。因此,本文总结了需要进一步探索的问题,以支撑所提技术方案。

4.1 通信问题

与传统的区块链方法相比,融合区块链与联邦学习的链上链下数据可信交互框架需要考虑联邦学习系统中不同节点的通信引起的性能损失和时间延迟。一方面,参与数据交易的节点数量增加会给系统通信资源带来更大的压力;另一方面,复杂的深度学习模型使联邦学习每次训练迭代都需要传输大量参数数据。这些固有问题将大大增加所提框架在问题建模、理论分析以及实际部署方面的复杂度,并对系统性能产生极大影响。

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^[13]。本文所提架构可以通过压缩模型梯度方案来减少通信所需的时间,从而在通信资源受限的数据交易环境中提供最优的模型训练策略,同时最小化模型的性能损失。除此之外,对本地模型进行压缩是另一种常见的降低模型复杂度的方法,可采用量化、剪枝、知识

蒸馏等模型压缩方法，在保证模型精确度的情况下尽可能压缩模型参数量，从而实现模型复杂度和精确度之间的平衡，减少通信网络负载，提高系统整体建模效率。

4.2 异构问题

与传统分布式机器学习不同，基于区块链与联邦学习的数据交易方案面临着严峻的异构性挑战。在真实场景中，参与数据共享的数据供给方类型是多样的，并且在参与交易时拥有的数据分布也各不相同。这种客户端数据异构性导致本地模型训练存在“数据漂移”现象，进而导致模型训练缓慢和不稳定地收敛。

对于非独立同分布数据已有多方面的研究，例如对数据集进行重采样以减小数据样本之间的相关性，模型参数自适应调整以适应节点的数据分布情况，特征相关性选择以减少非独立同分布数据中的噪声和不相关信息等。对数据及模型训练方法进行优化可改进异构环境下的模型性能，同时使训练能够快速稳定收敛。

4.3 共识问题

与传统的联邦学习相比，本文所提框架需要考虑区块链共识过程的性能损失与时间延迟导致的系统效率问题。传统共识算法，如工作量证明（proof of work, PoW）算法采用哈希难题来确定候选区块的发布者，其中能够最快解出难题的获得记账权，但是这种方法有吞吐量较低、确认时延较高。作为平衡，代理权益证明（delegated proof of stake, DPoS）算法采用选举部分特殊节点代理网络中其余节点的方式，减少参与区块生产和验证的节点数量。然而，DPoS仍存在部分缺陷：一方面，其选举出的代理人节点存在错误的可能性，可能会对整个系统的安全性造

成影响；另一方面，代理人节点生产的区块需要得到三分之二的其他代理人节点验证通过后才允许加入区块链，这种验证方式使区块验证时延大大提高。

为了解决共识算法的性能限制，部分学者通过引入并行计算、优化网络通信和改进区块确认机制等手段，提升共识算法的整体性能。除此之外，筛选交易节点以减少共识节点数量、简化共识投票流程从而节省通信开销的方法，同样能够提高区块链系统的交易率和吞吐量。针对数据资产流通交易的共识算法需要评估实际需求，并综合考虑可扩展性、效率和安全性等多方面因素，以缩短交易时间、优化系统运行效率。

5 关于推进数据资产流通交易体系建设的建议

5.1 加快制定政策法规，强化应用顶层设计

一方面，政府应当出台数据流通和交易等一系列配套法规、条例和相关指引，通过建立数据资产的分类分级授权应用规范，积极推动数据基础设施建设，推动匿名化、联邦学习、多方安全计算等隐私计算和区块链技术应用，增强数据利用可信、可控、可计量能力，形成公平、安全、开放的数据资产市场；另一方面，完善数据资产交易的全流程合规与监管规则体系，落实产权分置制度，明确数据交易主体的责任义务和行为边界，防控数据交易风险。

5.2 推动产业标准制定，夯实基础设施建设

截至目前，学术界与工业界尚未就数

据资产交易达成统一的标准化共识，亦未形成广泛认可的技术路径。数据来源的多样性及其结构的异构性，加之不同应用链之间的通信交互难题，严重制约了数据资产服务生态体系的兼容性与可扩展性。鉴于此，亟须深化对联邦学习、区块链等核心技术的研究，从技术架构、算法规范、评价机制、安全准则等多个维度，推进标准化进程，以明确数据流通中的隐私保护和安全要求。各相关行业应基于实际应用需求，与行业监管机构协同制定并推广行业通用标准；针对联邦学习与区块链技术可能产生的技术和伦理问题，制定详细的合规框架，以确保数据交易安全合法，避免数据滥用和隐私泄露。

5.3 鼓励各方积极参与,共建数据资产交易生态

数据资产流通交易涵盖了从数据采集、加工、存储、流通、交付、认证、合规到监管等多个环节，涉及众多参与主体，多方共同构成了一个复杂的服务生态体系。为促进该生态体系的健康发展，首先，政府应倡导并支持各行业积极发展联邦学习与区块链技术，激励企业在数据资产交易中扮演服务提供者和连接者的角色，以提高市场活跃度和生态协同效应。其次，鼓励行业领军企业为中小企业提供技术支持，构建“政府-领军企业-中小企业”的互动机制，促进企业间的协同发展；同时，激励企业将创新技术应用于数据资产交易的实践中，为技术创新提供适宜的环境，并提升自主创新能力。针对行业发展痛点堵点，形成一批服务经济社会发展的典型应用场景，加速数据资产交易相关技术在实际交易场景中的落地应用。最后，加强产学研合作，成立专注于数据资产交易的产业联盟，促进学术界、企业界及政府间的

积极互动，通过自主研发和合作创新，推动“联邦学习+区块链”技术在数据资产交易中的应用，促进技术的持续创新及其在实际应用中的有效实施，从而构建一个协同发展的生态体系。

6 结束语

随着国家数据基础制度体系出台，数据资产作为一种新型资产形态，已成为重要资产和核心竞争力。以数据为驱动的高度智能化、精细化、多元化、场景化业务形态将成为必然发展方向。本文针对数据资产流通交易中事前、事中、事后的确权难、互信难、入场难、监管难问题，提出基于区块链和联邦学习技术的链上链下数据资产流通交易方案，包括基础系统架构、链下数据确权、链上数据交互、链中数据监管四方面研究内容；同时，提出融合联邦学习和区块链技术在数据资产交易中的应用建议。本文研究旨在提升数据资产流通交易的高安全性、高隐私性以及可追溯性，促进数据市场安全有序、平稳持续发展。

参考文献：

- [1] 季良玉. 数据资产的交易困境及其治理[J]. 会计之友, 2023 (13): 27-31.
JI L Y. The transaction dilemma and governance of data assets[J]. Friends of Accounting, 2023 (13): 27-31.
- [2] 陆岷峰, 欧阳文杰. 商业银行数据资产的价值评估与交易定价研究[J]. 会计之友, 2022 (19): 30-37.
LU M F, OUYANG W J. Research on the value evaluation and transaction pricing of data assets in commercial banks[J]. Friends of Accounting, 2022(19): 30-37.

[3] 王恺祺,洪睿琦,毛云龙,等. 基于区块链构建安全去中心化的联邦学习方案[J]. 中国科学:信息科学, 2024, 54(2): 316-334.
WANG K Q, HONG R Q, MAO Y L, et al. Secure solution for decentralized federated learning with blockchain[J]. Scientia Sinica (Informationis), 2024, 54(2): 316-334.

[4] MCMAHAN H B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Cambridge: PMLR, 2017: 1273-1282.

[5] SHAFAGH H, BURKHALTER L, HITHNAWI A, et al. Towards blockchain-based auditable storage and sharing of IoT data[C]//Proceedings of the 2017 on Cloud Computing Security Workshop. New York: ACM, 2017: 45-50.

[6] ZHANG F, CECCHETTI E, CROMAN K, et al. Town crier: an authenticated data feed for smart contracts[C]//Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2016: 270-282.

[7] LIU X, ZHENG Y G, LI X Z. A revocable attribute-based access control system using blockchain[J]. Journal of Physics: Conference Series, 2021, 1971(1): 012058.

[8] XIONG W, XIONG L. Data trading certification based on consortium blockchain and smart contracts[J]. IEEE Access, 2020, 9: 3482-3496.

[9] 蔡亮,端豪,鄢萌,等. 基于双层协同的联盟区块链隐私数据保护方法[J]. 软件学报, 2020, 31(8): 2557-2573.
CAI L, DUAN H, YAN M, et al. Private data protection scheme for consortium blockchain based on two-layer cooperation[J]. Journal of Software, 2020, 31(8): 2557-2573.

[10] 周炜,王超,徐剑,等. 基于区块链的隐私保护去中心化联邦学习模型[J]. 计算机研究与发展, 2022, 59(11): 2423-2436.
ZHOU W, WANG C, XU J, et al. Privacy-preserving and decentralized federated learning model based on the blockchain[J]. Journal of Computer Research and Development, 2022, 59(11): 2423-2436.

[11] 陈纯. 联盟区块链关键技术与区块链的监管挑战[J]. 中国工业和信息化, 2020(11): 54-58.
CHEN C. Key technologies of consortium blockchain and regulatory challenges of blockchain[J]. China Industry and Information Technology, 2020(11): 54-58.

[12] 经普杰,王良民,董学文,等. 分层跨链结构: 一种面向区块链系统监管的可行架构[J]. 通信学报, 2023, 44(3): 93-104.
JING P J, WANG L M, DONG X W, et al. CHA: cross-chain based hierarchical architecture for practicable blockchain regulatory[J]. Journal on Communications, 2023, 44(3): 93-104.

[13] 李程,袁勇,郑志勇,等. 基于区块链的联邦学习: 模型、方法与应用[J]. 自动化学报, 2024, 50(6): 1059-1085.
LI C, YUAN Y, ZHENG Z Y, et al. Blockchain-enabled federated learning: models, methods and applications[J]. Acta Automatica Sinica, 2024, 50(6): 1059-1085.

[14] 孙一萌,范洪博,彭慢煜,等. 一种面向联盟链的链下数据可验证查询方法[J]. 现代电子技术, 2023, 46(19): 70-74.
SUN Y M, FAN H B, PENG M Y, et al. A method of off-chain data verifiable query for consortium blockchain[J]. Modern Electronics Technique, 2023, 46(19): 70-74.

[15] 赵明,董大治. 基于区块链技术的数据资产管

理机制[J]. 大数据, 2021, 7(4): 49-60.

ZHAO M, DONG D Z. Data asset management mechanism based on blockchain technology[J]. Big Data Research, 2021, 7(4): 49-60.

[16] 孙浩, 毛瀚宇, 张岩峰, 等. 区块链跨链技术发展及应用[J]. 计算机科学, 2022, 49(5): 287-295.

SUN H, MAO H Y, ZHANG Y F, et al. Development and application of block-chain cross-chain technology[J]. Computer Science, 2022, 49(5): 287-295.

[17] 高婷婷, 姚中原, 贾淼, 等. 链上链下一致性保护技术综述[J]. 计算机应用, 2024, 44(12): 3658-3668.

GAO T T, YAO Z, JIA M, et al. Overview of on-chain and off-chain consistency protection technologies[J]. Journal of Computer Applications, 2024, 44(12): 3658-3668.

作者简介



莫梓嘉 (1996-), 女, 博士, 中国工商银行博士后科研工作站博士后研究员, 主要研究方向为边缘智能、联邦学习、区块链。



赵晨 (1992-), 男, 博士, 宁波工程学院网络空间安全学院副研究员, 主要研究方向为联邦学习、隐私计算、人工智能、数据治理。

收稿日期: 2024-10-17

通信作者: 莫梓嘉, mozijia@outlook.com

基金项目: 浙江省自然科学基金项目(No.LQN25F020026)

Foundation Item: The Natural Science Foundation of Zhejiang Province (No. LQN25F020026)