第 62 卷　第 1 期
2026 年 1 月

南京大学学报(自然科学)
JOURNAL OF NANJING UNIVERSITY
(NATURAL SCIENCE)

Vol. 62, No. 1
Jan., 2026

DOI:10.13232/j.cnki.jnju.2026.01.002

基于联盟链和Stackelberg博弈的EMRs分布式共享模型

姜　茸[1,2,3],娄文璐[1,2,4*],张金鹏[1,2,3],张荷娇[1,2,4],王海洋[1,2,3]

(1.云南省服务计算重点实验室,云南财经大学,昆明,650221;2.云南财经大学智能应用研究院,昆明,650224;
3.云南财经大学信息学院,昆明,650600;4.云南财经大学商学院,昆明,650221)

摘　要:电子病历(Electronic Medical Records,EMRs)共享对辅助诊断和提升医疗服务质量具有重大意义,但数据共享过程中的隐私泄露风险和数据安全隐患常使数据持有方拒绝共享.在保障数据安全的基础上激励数据持有方可信共享,打破数据孤岛,成为学术界的重要研究内容.针对该问题,提出基于联盟链和Stackelberg博弈的EMRs分布式共享模型,通过联盟链的去中心化特性与Stackelberg博弈策略优化机制来实现数据的安全高效共享及用户信息的隐私保护.首先搭建联盟链架构,通过多方参与者协作实现EMRs数据可信、安全共享.其次,运用Stackelberg博弈理论分析共享过程中的决策冲突,设计激励机制,保障各方数据共享过程中的合理回报.设计目标函数描述数据提供者利润最大化和消费者效用最大化的激励目标,利用交替方向乘子法(Alternating Direction Multiplier Method,ADMM)的分解特性与快速收敛性分布式求解函数以适应大规模机构间的病历共享需求.最后,模型通过凝聚层次聚类(Agglomerative Hierarchical Clustering,AHC)算法对共识节点聚类,改进传统区块链的PBFT共识算法为AHC-PBFT算法,提升数据共享效率,减少通信开销.实验表明,和传统的区块链共享模型相比,提出的共享模型可以提供安全的EMRs管理与交易服务,降低医疗节点间数据共享的通信开销和时延,提高吞吐量,增进医疗机构及相关部门间的数据可信共享.

关键词:Stackelberg博弈,EMRs共享,联盟链,ADMM,AHC-PBFT

中图分类号:TP305　　**文献标志码**:A

A distributed sharing model for EMRs based on consortium chain and Stackelberg game theory

Jiang Rong[1,2,3], Lou Wenlu[1,2,4*], Zhang Jinpeng[1,2,3], Zhang Hejiao[1,2,4], Wang Haiyang[1,2,3]

(1. Yunnan Key Laboratory of Service Computing, Yunnan University of Finance and Economics, Kunming, 650221, China; 2. Institute of Intelligence Application Research, Yunnan University of Finance and Economics, Kunming, 650224, China; 3. School of Information, Yunnan University of Finance and Economics, Kunming, 650600, China; 4. Business School, Yunnan University of Finance and Economics, Kunming, 650221, China)

Abstract: The sharing of Electronic Medical Records (EMRs) is crucial for supporting diagnosis and improving the quality of medical services. However, the risks of privacy breaches and data security vulnerabilities during the sharing process often deter data holders from participating in data sharing. Incentivizing data holders to share data in a trustworthy manner while ensuring data security, thereby dismantling data silos, has emerged as a significant research topic in academia. To address this challenge, this paper proposes a distributed EMR sharing model based on a consortium chain and Stackelberg game. The model enables secure and efficient data sharing while preserving user privacy by leveraging the consortium chain's distributed

基金项目:国家自然科学基金(72471206,72164037),云南省科技计划(重大科技专项)(202502AD080011),云南财经大学研究生创新基金(2025YUFEYC104)

收稿日期:2025－12－08

*通信联系人,E-mail:wenlu_lou@163.com

architecture and the strategic optimization mechanism of the Stackelberg game. First, the model establishes a consortium chain architecture to enable trusted and secure sharing of EMRs data through collaboration among multiple participants. Second, it utilizes Stackelberg game theory to analyze decision-making conflicts during the sharing process and designs incentive mechanisms to ensure equitable returns for all parties involved. The model formulates objective functions that capture the dual goals of maximizing data providers' profits and consumers' utility. It leverages the decomposition property and rapid convergence of the Alternating Direction Method of Multipliers (ADMM) to solve these optimization problems in a distributed manner, thereby meeting the demands of large-scale EMRs sharing across institutions. Lastly, the model employs the Agglomerative Hierarchical Clustering (AHC) algorithm to cluster consensus nodes and modifies the traditional PBFT consensus algorithm into AHC-PBFT. This enhancement improves data sharing efficiency and reduces communication overhead. Experimental results demonstrate that, compared to traditional chain sharing models, the proposed model can provide secure EMRs management and transaction services, reduce communication overhead and latency in data sharing among medical nodes, increase throughput, and foster trustworthy data sharing among medical institutions and relevant departments.

Keywords: Stackelberg games, EMRs sharing, consortium chain, ADMM, AHC-PBFT

医院信息系统(Hospital Information System, HIS)是为医院的整体运行提供全面的自动化信息管理及服务的集中式系统. 电子病历(Electronic Medical Records, EMRs)是医院信息系统的核心组成部分,它代替了传统的纸质病历,将患者的医疗信息以数字化的形式记录下来[1]. 随着EMRs数据规模的爆炸式增长,人们提出了一些基于物联网技术的新方法来提高EMRs共享系统的鲁棒性和安全性. Fabian et al[2]提出一种基于多云的新型体系结构,可以在半可信的云计算环境中实现协同、安全的EMRs共享. Manoj et al[3]提出一种基于代理的访问控制方案,用于云计算中不同医疗保健提供者之间的选择性EMRs共享. 为了实现医疗用户和EMRs共享系统的身份验证, Ibrahim et al[4]在云上使用公钥基础设施(Public Key Infrastructure, PKI)来确保电子医疗系统的安全标准. 此外, Ying et al[5]在基于属性的加密(CP-ABE)原型系统中使用属性权限为数据消费者授予密钥,以实现云上EMRs共享的细粒度访问控制. 然而,这些基于物联网的HIS是集中式的,无法满足多个医疗机构之间间日益增长的EMRs共享的安全性和效率需求. 同时,出于隐私方面的考虑和竞争压力,不同的医疗机构也不愿共享自己的数据[6],并且来自不同医疗机构的数据规范差异和互操作性障碍也是影响数据共享的重要问题[7-8].

随着区块链技术的发展,其去中心化、可追溯性、匿名性等特点受到了广泛关注[9]. 区块链由众多节点(可以是计算机、服务器等设备)共同维护,数据并非存储在单一的中心化服务器上,而是分散在各个节点中. 每个节点都拥有完整或部分账本的副本,当有新的数据产生时,经过一定的验证机制,各个节点会同步更新账本内容,确保所有节点账本的一致性. 区块链使用如实用拜占庭容错算法(PBFT)[7]、工作量证明[10]、权益证明[11]、委托PoS[12]等共识算法实现不信任的用户之间数据的分布式管理. 同时,区块链使用签名算法[13]验证用户合法性,保护用户和交易的隐私安全. 在数字货币领域,区块链可用于解决金融诚信问题[14];在智能合约领域,区块链解决了跨境支付难题[15];在人工智能领域,区块链广泛应用于身份认证[16]、投票选举[17]、医疗保险[18]等服务应用,推动了政府公共服务创新. 目前,许多学者都在关注基于区块链技术的EMRs共享问题. Zheng et al[19]提出一种基于区块链技术的个人持续动态健康数据共享的概念设计,并辅以云存储,以安全透明的方式共享个人健康信息. Cao et al[20]提出一种云辅助的安全电子健康系统,使用区块链技术保护云中的外包EMRs不被非法修改. 该系统的关键思想是EMRs只能由经过认证的参与者外包,外包EMRs的每个操作都作为交易集成到公共区块链中. Liu et al[21]提出一种基于区块链的隐私保护

数据共享方案BPDS,在BPDS中,云被用来安全地存储原始EMRs,还设计了一个防篡改的联盟区块链来共享EMRs索引. Niu et al[22]提出一种基于区块链的可搜索加密方案用于EMRs共享,以提高数据的可搜索性. 为了进一步提高EMRs共享的安全性,Chen et al[23]提出一种基于区块链和云的医疗数据存储、共享和使用的存储方案和服务框架. 在该方案中,基于区块链的个人医疗数据应用可以在不侵犯隐私的情况下提供患者EMRs共享服务.

以上工作从不同方面提出了各种EMRs共享方案,但没有针对促进医疗机构参与数据共享提供现实解决方案. 特别地,在EMRs跨域共享的过程中,保证不同场景下各个机构之间的互信和数据的安全共享是亟待解决的问题. 另外,大规模的用户访问会给区块链网络造成巨大的压力,影响系统的运行效率.

联盟链是由多个特定机构或组织联合组成节点共同维护、有准入门槛、兼具部分去中心化与隐私性等特点,适用于企业间合作场景且常用PBFT等共识方法的区块链类型. 因此,本文基于联盟链构建EMRs共享模型,使用Stackelberg博弈理论对普通节点与当值节点之间的交互进行建模,并使用AHC (Agglomerative Hierarchical Clustering)思想对共识节点进行分组以提高共识效率,以促进EMRs的高效共享.

1　基于联盟链和Stackelberg博弈的EMRs分布式共享模型

本文将区块链中的共识节点分为普通节点和当值节点,当值节点是从普通节点中根据一定规则选取出来承担特定时期主要记账或共识等关键任务的节点,普通节点是区块链网络中数量较多、具有一般性功能和角色的节点群体. Stackelberg博弈中存在两类参与者,分别是领导者和追随者. 博弈分两个阶段,第一阶段,领导者先行动,作出决策并对外公布;而第二阶段,追随者在观察到领导者的决策后,据此作出自己的决策. 区块链中的当值节点和普通节点与Stackelberg博弈中的领导者和追随者存在角色逻辑相似性,因此,本文将区块链网络中的普通节点作为Stackelberg博弈模型中的追随者,将当值节点作为领导者,通过Stackelberg博弈模型中领导者与追随者之间EMRs资源的交易,促进EMRs在整个区块链网络中的共享和医疗系统及相关机构的互操作性,提高信息流通效率,缓解信息孤岛问题.

1.1　参数及定义　如图1所示,当值节点(Duty Node,DN)被定义为领导者角色. 作为单一网络中的节点管理器,当值节点受到网络中节点的信任,负责异构网络间通信,处理内部和外部的访问请求. 数据用户(Data Users,DU)被定义为追随者角色,主要包括医生、健身教练和其他数据访问者. 数据用户的每一次访问记录都会存储在区块链中,其中,网络内部访问记录在日志本地联盟链中存储共享,跨域访问记录在医疗健康公共联盟链中存储共享.

整个医疗健康公共联盟链网络中共有N个数据用户(DU)作为普通节点,$i\in N=\{1,2,\cdots,N\}$,将普通节点分为M组. 每个本地联盟链网络中有一个当值节点(DN)负责异构网络间通信,整个网络中共有M个DN,$N>M$,其中,$\mathrm{DN}_j, j\in M=\{1,2,\cdots,M\}$. 数据用户既是本地区块链网络的EMRs数据的创建者,又是异构区块链网络中EMRs数据的使用者. 但是每个数据用户只能共享访问其所属区块链网络内部的局部电子病历(L-EMRs),要想跨域访问异构区块链网络中的EMRs,当值节点会向普通节点收取一定价格的费用才会将其所在的医疗健康公共联盟链中的EMRs共享给相应的数据用户. 特别地,当数据用户和当值节点属于同一个局域网时,当值节点即使拥有整个医疗健康公共联盟链网络中的全局电子病历(G-EMRs),也不能将G-EMRs免费共享给数据用户,只能免费共享局域网中的L-EMRs.

在Stackelberg博弈的第一阶段,当值节点以利润最大化为目标,作为领导者设定整个医疗健康公共联盟链网络中的G-EMRs的单位价格p_j. 在Stackelberg博弈的第二阶段,数据用户基于EMRs数据资源价格的基础,作为追随者确定其数据资源的需求量d_{ij},当$d_{ij}=0$时,$p_{ij}=0$. 因此,

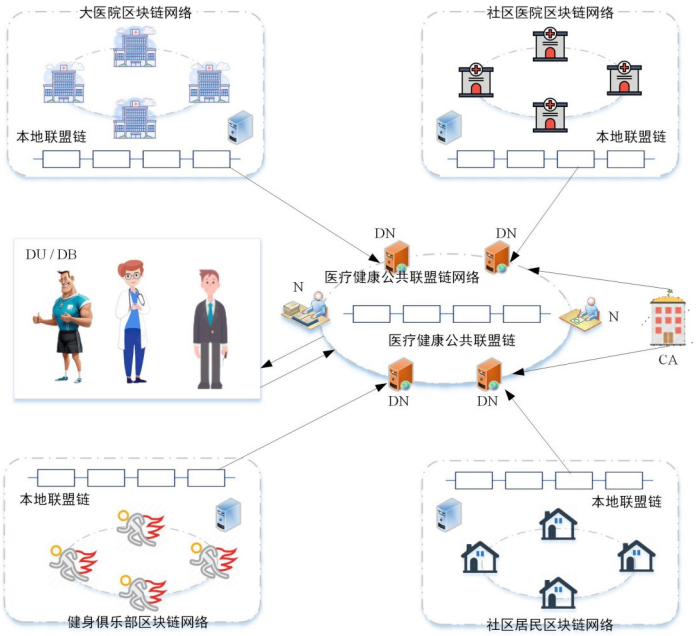

图 1　基于联盟链的医疗健康数据管理场景

Fig. 1　Healthcare data management scenario based on hybrid consortium chain

所有数据用户的需求矩阵为：

$$D=\begin{bmatrix} d_{11} & d_{12} & d_{13} & \cdots & d_{1M} \\ d_{21} & d_{22} & d_{23} & \cdots & d_{2M} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ d_{N1} & d_{N2} & d_{N3} & \cdots & d_{NM} \end{bmatrix}$$

所有普通节点/数据用户对应的支付矩阵为：

$$P=\begin{bmatrix} p_{11} & p_{12} & p_{13} & \cdots & p_{1M} \\ p_{21} & p_{22} & p_{23} & \cdots & p_{2M} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{N1} & p_{N2} & p_{N3} & \cdots & p_{NM} \end{bmatrix}$$

由于所有当值节点拥有的数据是一样的，都是医疗健康公共联盟链上经过PBFT共识的真实可信的G-EMRs数据，因此普通节点/数据用户无论向哪一个当值节点提出EMRs共享请求，都可以实现对全局区块链网络中G-EMRs的数据共享．即普通节点/数据用户只会对一个当值节点提出G-EMRs数据共享请求，普通节点/数据用户与当值节点之间的共享请求矩阵为：

$$X=\begin{bmatrix} x_{11} & x_{12} & x_{13} & \cdots & x_{1M} \\ x_{21} & x_{22} & x_{23} & \cdots & x_{2M} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{N1} & x_{N2} & x_{N3} & \cdots & x_{NM} \end{bmatrix}$$

其中，$\sum_{k\in M} x_{ik}=1$，当$x_{ij}=1$时，普通节点DU_i向当值节点DN_j提出共享请求d_{ij}，支付价格为p_{ij}；当$x_{ij}=0$时，$d_{ij}=0$，相应地，$p_{ij}=0$.

1.2　Stackelberg博弈模型　在Stackelberg博弈模型中，当值节点为领导者，普通节点/数据用户为追随者．为了提高医疗健康公共联盟链网络中EMRs共享流通的效率，参考文献[24]对当值节点与普通节点之间的相互作用进行建模，该模型为每一个普通节点DU_i选择DN_j的情况设置了概率ω_{ij}：

$$\omega_{ij}=\frac{b_{ij}x_{ij}}{\sum_{k\in M} b_{ik}} \tag{1}$$

其中，b_{ij}是当值节点DN_j的最高单位价格$\hat{p}$与普通节点DU_i的单位支付价格p_{ij}之间的差．同理，b_{ik}是当值节点为普通节点提供G-EMRs数据共享时的降价动力，如式(2)所示：

$$b_{ik}=\hat{p}-p_{ik}, i\in N, k\in M \tag{2}$$

命题　根据式(1)和式(2)，当其他当值节点固定EMRs数据的定价时，ω_{ij}的值与普通节点DU_i支付给当值节点DN_j的价格p_{ij}负相关，即普通节点选择当值节点的概率与支付给该当值节点的价格负相关．

证明　首先,根据式(1)和式(2)可将ω_{ij}转换为如下形式:

$$\omega_{ij}(p_{ij})=\frac{\hat{p}-p_{ij}}{\sum_{k\in M}(\hat{p}-p_{ik})}x_{ij}=\frac{\hat{p}-p_{ij}}{\left[\hat{p}+\sum_{k\in M,k\neq j}(\hat{p}-p_{ik})\right]-p_{ij}}x_{ij}=\frac{A-p_{ij}}{B-p_{ij}}x_{ij} \tag{3}$$

当$x_{ij}=1$时,基于式(3)求$\omega_{ij}(p_{ij})$的一阶导数和二阶导数:

$$\frac{\partial\omega_{ij}}{\partial p_{ij}}=\frac{A-B}{(B-p_{ij})^2}<0 \tag{4}$$

$$\frac{\partial^2\omega_{ij}}{\partial p_{ij}^2}=\frac{2(A-B)}{(B-p_{ij})^2}<0 \tag{5}$$

由此可见,$\omega_{ij}(p_{ij})$为凸函数,$\omega_{ij}(p_{ij})\in[0,1]$,当$x_{ij}=0$时,$\omega_{ij}(p_{ij})=0$. 其中,

$$B=\hat{p}+\sum_{k\in M,k\neq j}(\hat{p}-p_{ik})$$

$$A=\hat{p}$$

$$B\geqslant A\geqslant p_{ij}\geqslant 0$$

$\omega_{ij}(p_{ij})$为凸函数,说明普通节点选择数据共享的当值节点的解空间存在最优解,选择过程可以被建模成一个优化问题. 因此,为了鼓励更多的普通节点/数据用户参与整个联盟区块链网络中的G-EMRs共享,促进医疗系统和相关机构的互操作性,提高数据流通效率,缓解信息孤岛问题. 基于Stackelberg博弈模型的每个当值节点倾向于向普通节点/数据用户提供较低的价格p_{ij},其原因是当ω_{ij}增加时,普通节点DU_i更有可能向当值节点DN_j提出数据共享请求,这就导致当值节点之间的价格竞争.

普通节点/数据用户对当值节点的EMRs数据资源请求被视为普通节点/数据用户的数据共享访问能力. 当普通节点/数据用户向当值节点提出数据共享请求之前,普通节点DU_i拥有初始的数据共享访问能力l_i. 因此,普通节点DU_i向当值节点DN_j购买EMRs数据资源d_{ij}后总的共享访问能力为:

$$l_i^{\text{total}}=l_i+\sum_{j\in M}\omega_{ij}d_{ij} \tag{6}$$

普通节点DU_i的数据共享与访问能力可以影响其在购买当值节点DN_j的EMRs数据资源过程中的决策和行为,从而对普通节点DU_i的满意度S_i^{sat}产生影响:

$$S_i^{\text{sat}}=\lambda_i\ln l_i^{\text{total}} \tag{7}$$

由于满意度通常是一种正反馈过程,设定普通节点DU_i的共享访问能力的影响因子$\lambda_i>0$,并使用影响因子λ_i和普通节点DU_i的总共享访问能力共同描述普通节点DU_i的满意度S_i^{sat}. 对于每一个普通节点DU_i,$i\in N$,它根据当值节点设定的价格p_j来决定EMRs请求策略为$d_i=\{d_{i1},d_{i2},\cdots,d_{iM}\}$,从而实现效用最大化,如式(8)所示:

$$u_i=\sum_{j\in M}(S_i^{\text{sat}}-p_{ij}\omega_{ij}d_{ij})=\sum_{j\in M}\left[\lambda_i\ln\left(l_i+\sum_{j\in M}\omega_{ij}d_{ij}\right)-p_{ij}\omega_{ij}d_{ij}\right] \tag{8}$$

对于每一个作为领导者的当值节点DN_j,$j\in M$,除了向作为追随者的普通节点DU_i,$i\in N$收取共享服务的收入外,还有运营和维护的服务成本. 当值节点的成本与电力消耗或硬件损耗有关,用cd_{ij}表示,其中,c表示成本系数,$0<c<p_{ij}$. 因此,每一个当值节点j在策略空间$\left\{p_j=[p_{ij}]_{i\in N}:0\leqslant p_{ij}\leqslant\hat{p}\right\}$内确定EMRs数据资源的价格以实现利润最大化,如式(9)所示:

$$\Pi_j=\sum_{i\in N}\left[\omega_{ij}\left(\sum_{i\in N}p_{ij}d_{ij}-\sum_{i\in N}cd_{ij}\right)\right]=\sum_{i\in N}\left[\frac{(\hat{p}-p_{ij})x_{ij}}{\sum_{k\in M}(\hat{p}-p_{ik})}\left(\sum_{i\in N}p_{ij}d_{ij}-\sum_{i\in N}cd_{ij}\right)\right] \tag{9}$$

为了提高医疗健康公共联盟链网络中EMRs数据共享流通的效率,促进医疗系统和相关机构的互操作性,模型引入了多领导者多追随者Stackelberg博弈理论来对普通节点/数据用户和当值节点之间的EMRs数据资源交易进行建模. 在Stackelberg博弈的第一阶段,当值节点以利润Π_j最大化为目标设定EMRs数据资源的价格p_{ij};在Stackelberg博弈的第二阶段,普通节点DU_i在当值节点DN_j设定价格p_{ij}的基础上,以效用u_i最大化为目标,确定EMRs数据资源的需求量d_{ij}.

在Stackelberg博弈的第二阶段,由于外部节点的作用,普通节点的EMRs数据资源需求d_{ij}会受到当值节点DN_j的价格$P=\{p_1,p_2,\cdots,p_M\}$和除了节点DU_i以外其他数据用户需求DU_{-i}的影响.并且,每一个普通节点DU_i通过求解以下效用最大化问题来确定自己的EMRs数据资源需求d_{ij}:

$$u_i(d_i,D_{-i},P)=\sum_{j\in M}\left(S_i^{\text{sat}}-p_{ij}\omega_{ij}d_{ij}\right)=\sum_{j\in M}\left[\lambda_i\ln\left(l_i+\sum_{j\in M}\omega_{ij}d_{ij}\right)-p_{ij}\omega_{ij}d_{ij}\right] \tag{10}$$

普通节点(追随者)DU_i的子博弈问题可以被写为以下的数学规划问题,如式(11)所示:

$$\begin{aligned}&\underset{d_i}{\text{maximize}}\ u_i(d_i,D_{-i},P)\\&\text{subject to:}\quad\begin{aligned}&d_{ij}\geqslant 0\\&\sum_{j\in M}d_{ij}\leqslant D_{\max}\\&\sum_{j\in M}x_{ij}=1\end{aligned}\end{aligned} \tag{11}$$

由于其财务负担,每个普通节点DU_i都没有动力无限制地增加其服务需求,因此第二个约束条件表示由于普通节点DU_i的总预算有限,每个普通节点DU_i的最大EMRs数据资源需求不超过$D_{\max}$.

在Stackelberg博弈的第一阶段,同样由于外部节点的作用,当值节点DN_j的EMRs数据资源定价p_{ij}会受到其他当值节点DN_j的价格P_{-j}和普通节点/数据用户需求的影响,并且每一个当值节点DN_j通过解决以下利润最大化问题确定自己的EMRs数据资源价格p_{ij}:

$$\Pi_j(p_j,P_{-j},D)=\sum_{i\in N}\left[\omega_{ij}\left(\sum_{i\in N}p_{ij}d_{ij}-\sum_{i\in N}cd_{ij}\right)\right]=\sum_{i\in N}\left[\frac{(\hat{p}-p_{ij})x_{ij}}{\sum_{k\in M}(\hat{p}-p_{ik})}\left(\sum_{i\in N}p_{ij}d_{ij}-\sum_{i\in N}cd_{ij}\right)\right] \tag{12}$$

当值节点(领导者)DN_j的子博弈问题可以被写为以下数学规划问题,如式(13)所示:

$$\begin{aligned}&\underset{p_j}{\text{maximize}}\ \Pi_j(p_j,P_{-j},D)\\&\text{subject to:}\quad 0\leqslant p_j\leqslant\hat{p}\end{aligned} \tag{13}$$

传统的Stackelberg博弈问题只存在一个领导者和多个追随者.本文提出的多领导者多追随者博弈模型的关键挑战在于每个普通节点(追随者)的策略空间的高度多维性,使模型无法使用传统的逆向归纳法得到纳什均衡解.因此,本文采用ADMM算法来实现EMRs共享模型最优策略的求解.

1.3 基于ADMM的Stackelberg博弈模型 为了促进EMRs共享流程的执行,引入定价机制对共享流程收费,构建普通节点和当值节点之间的分布式EMRs共享模型,使用多领导者多追随者Stackelberg博弈理论来平衡EMRs数据的供需关系,实现EMRs资源的优化共享.

本文提出的基于联盟链的多领导者多追随者EMRs分布式共享模型中,普通节点DU_i和当值节点DN_j都被假设为理性的代理人,其目标是分别使它们的效用和利润最大化.根据文献[25—26],将价格p_{ij}视为当值节点DN_j向普通节点DU_i提供的激励因素,因此,可以将基于联盟链的EMRs分布式共享模型作为一种激励机制设计,使式(13)中当值节点DN_j的利润达到最优,同时考虑式(11)中普通节点DU_i的效用.通过调整激励因子p_{ij},当值节点DN_j可以间接地使普通节点DU_i确定EMRs数据资源的需求量d_{ij},使数据提供者的利润$\Pi_j(p_j,P_{-j},D)$最大化.

具体地,激励机制问题可以表述为如式(14)的目标函数:

$$\begin{aligned}&\Pi_j(p_j,P_{-j},D)=\sum_{i\in N}\left[\omega_{ij}\left(\sum_{i\in N}p_{ij}d_{ij}-\sum_{i\in N}cd_{ij}\right)\right]\\&\text{subject to:}\quad 0\leqslant p_j\leqslant\hat{p}\\&\qquad\quad d_i=\operatorname{argmax}u_i(d_i,D_{-i},P)\\&\qquad\quad\text{subject to:}\quad\begin{aligned}&d_{ij}\geqslant 0\\&\sum_{j\in M}d_{ij}\leqslant D_{\max}\\&\sum_{j\in M}x_{ij}=1\end{aligned}\end{aligned} \tag{14}$$

基于联盟链的多领导者多追随者EMRs分布式共享模型分层优化问题(式(14))中包含了两个阶段的均衡问题,是一个标准的均衡约束问题.在该问题下协调多个相互冲突角色的利益,即普通节点的效用和当值节点的利润,不可避免地需要更复杂的解决方案.为了获得能够在考虑普通节点效用的同时优化当值节点利润的解决方案,本文采用ADMM算法,这是一种具有分解和快

速收敛特性的并行优化工具,特别适用于大规模优化问题.ADMM算法先将原始优化问题重构为如式(14)的拉格朗日函数,再交替固定拉格朗日乘子去求解各变量子问题并更新乘子,按收敛准则判断迭代是否停止以得到最优解.

2　实验结果与分析

为了评估提出的EMRs分布式共享模型的性能和效果,基于Hyperledger Fabric和Docker容器搭建区块链平台,并利用Caliper测试工具获取模型性能的相关数据.参考文献[27－28]设置区块大小为32 MB,出块时间为2 s,采用PBFT共识算法.同时,假设普通节点的初始计算能力l_i服从正态分布$N=\left(\mu_l,\sigma_l^2\right)$,$\mu_l=10$,$\sigma_l=5$.实验中节点随机分布,不具有移动性.测试总节点数为160,M为1,4,8,10时,AHC-PBFT和PBFT算法的时延和吞吐量.每组实验重复50次,取指标的平均值进行分析,使实验结果具有客观性.

基于Python 3.7实现了ADMM竞争算法、ADMM合作算法、AHC-PBFT和PBFT算法.实验平台的硬件配置:处理器为Intel(R) Core(TM) i5-9400 CPU,内存16 GB,硬盘1200 GB.

通过以下三部分实验验证共享模型的性能:第一,分析EMRs共享情景下,竞争博弈与合作博弈这两种博弈方式的总利润和总效用差异;第二,探究AHC算法对传统的PBFT共识算法进行共识改进的有效性;第三,研究共享模型较传统区块链算法的通信开销、时延和吞吐量的优化效果.

2.1　基于ADMM的竞争博弈与合作博弈　在合作场景中,当值节点之间的合作是为了使它们的总利润最大化,如图2所示.显然,合作情景下当值节点的总利润高于竞争情景,此时,当值节点共同优化它们的总利润,不会竞争性地提供较低的价格来吸引普通节点.相反,当值节点可以合作鼓励普通节点要求更多的EMRs数据共享服务.当值节点可以进一步从普通节点那里提取更多的盈余,因此当值节点合作时普通节点的总效用低于当值节点竞争时普通节点的总效用.另外,由于当值节点基于EMRs数据定价和普通节点对EMRs数据的需求具有一定的随机性,因此当值节点的利润和普通节点的效用具有一定的浮动性.

2.2　数据聚类　在AHC算法的仿真实验中,人工随机生成一部分网络共识节点,每个共识节点拥有EMRs交易请求信息,如血压、血糖、心跳等身体指标.若使用AHC算法将网络共识节点划分为四类,可以得到如图3的结果,其中颜色相同的网络共识节点属于同一个类簇.由图可见,每个子集群中的共识节点均服从正态分布.其中,灰点为恶意节点,使用PBFT共识算法可以容忍部分恶意节点,因此,在使用AHC算法对传统的PBFT共识算法进行改进时,AHC算法的分类效果不受区块链网络中恶意节点的影响,说明AHC算法可以对区块链中的节点数据进行有效共识判定.

2.3　通信开销

2.3.1　传统的PBFT共识算法通信开销　在医疗健康公共联盟链网络中有N个共识节点,如果不将医疗健康公共联盟链网络划分为四个异构网络,则医疗健康公共联盟链网络中只有一个领导者节点/当值节点,此时$M=1$.

当客户端发送请求给领导者节点/当值节点,

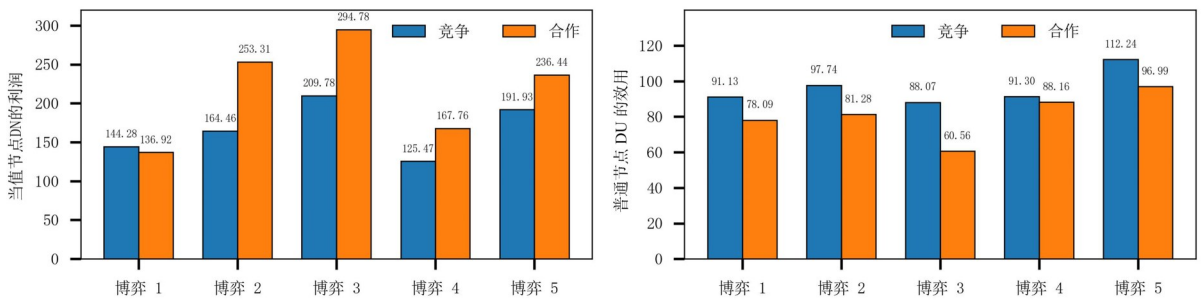

图2　基于ADMM的竞争与合作场景下的性能对比

Fig.2　Performance comparison in competitive and cooperative scenarios based on ADMM

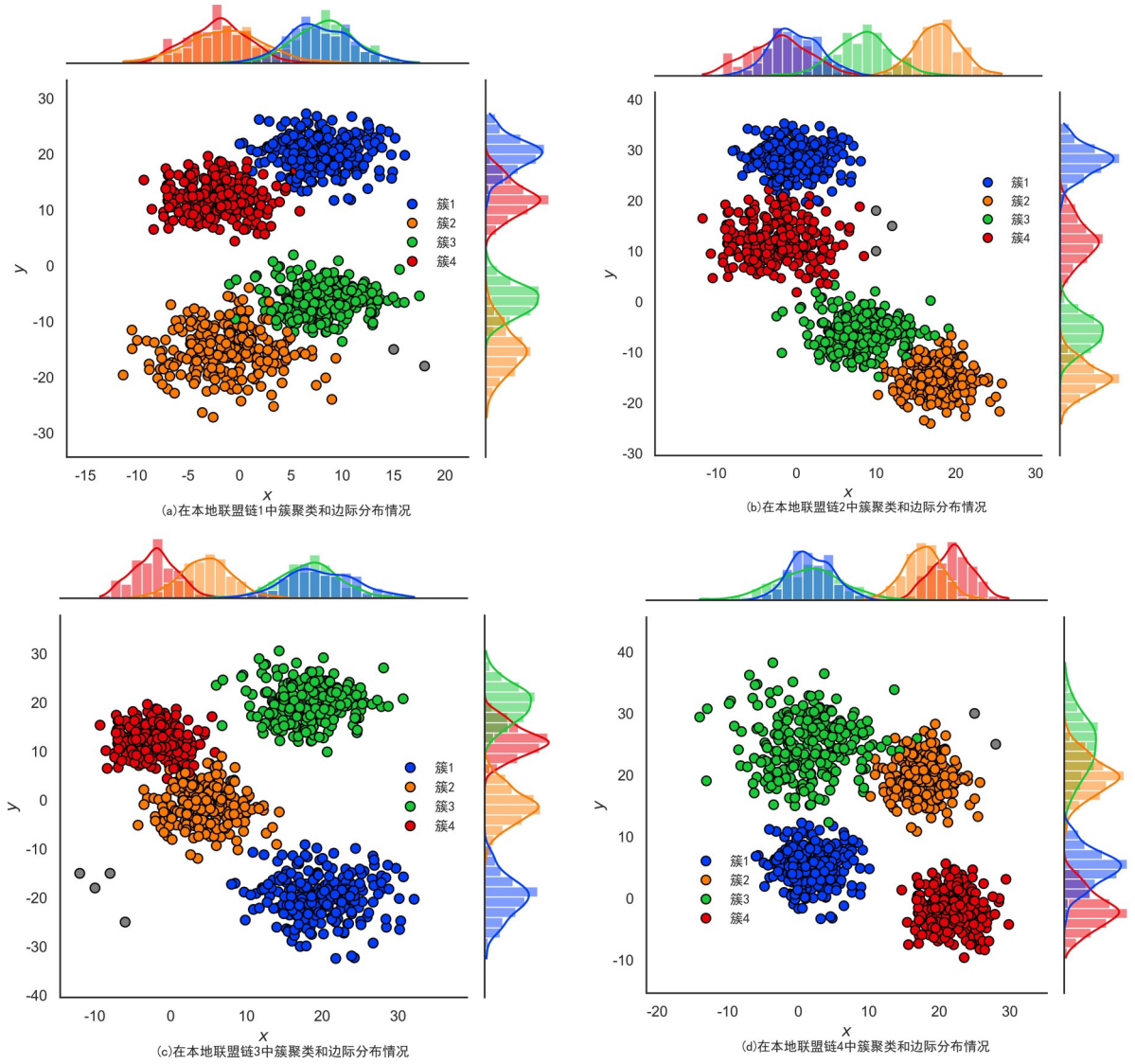

图 3　不同本地联盟链网络中的聚类结果

Fig.3　Cluster results in different local consortium chain networks

领导者节点/当值节点将广播请求给其他节点，节点执行传统 PBFT 算法的预准备阶段、准备阶段、确认阶段三阶段共识流程. 在预准备阶段，领导者节点/当值节点向所有的普通节点广播请求消息. 这一步的通信次数是$(N-1)$，通信复杂度为$O(N)$. 在准备阶段，每个节点都会将预准备阶段接收到的信息再次广播给所有其他节点，每个节点都将接收到$(N-1)$个消息，因此通信次数为$(N-1)^2$，通信复杂度为$O(N^2)$. 确认阶段与准备阶段类似，每个节点收到准备消息后会向所有节点广播确认消息，通信次数为$N(N-1)$，通信复杂度为$O(N^2)$. 因此，传统的 PBFT 算法的共识过程的通信次数主要集中在准备和确认两个阶段，通信次数为$2N(N-1)$，通信复杂度为$O(N^2)$.

2.3.2　AHC-PBFT 共识算法通信开销　若将N个共识节点分为M个子集群，则每个子集群中的节点个数为$\frac{N}{M}$. 运行 AHC-PBFT 共识算法所需的通信次数分析如下. 在集群内共识阶段，每个子集群中的当值节点向普通节点发送预准备消息，此过程的通信次数为$(N-M)$. 每个子集群

中普通节点收到预准备消息并验证,验证结果为真之后向集群内除自己外的所有节点发送准备消息,此过程的通信次数为$M\left(\frac{N}{M}-1\right)^2$. 每个子集群中普通节点收到预准备消息并验证,验证结果为真之后会向所有节点广播确认消息,此过程的通信次数为$N\left(\frac{N}{M}-1\right)$. 由此可见,在集群内共识阶段,节点执行AHC-PBFT算法的预准备阶段、准备阶段、确认阶段时的通信次数为$2N\left(\frac{N}{M}-1\right)$. 显然,在集群间共识阶段,节点的通信次数为$2M(M-1)$.

2.4　时延与吞吐量　如图4a和图4b所示,传统PBFT共识算法的时延随着医疗健康公共联盟链网络中节点数的增加而急剧增长,这是$O(N^2)$的复杂度决定的. 与传统PBFT不同,AHC-PBFT共识算法将全网范围内的共识节点划分为M个子集群,减少了节点的通信次数,通信复杂度为$O(\zeta^2)$,其中,$\zeta=\max\left\{\frac{N}{\sqrt{M}},M\right\}$. 因此,AHC-PBFT共识算法的通信复杂度$O(\zeta^2)$远小于PBFT共识算法的通信复杂度$O(N^2)$.

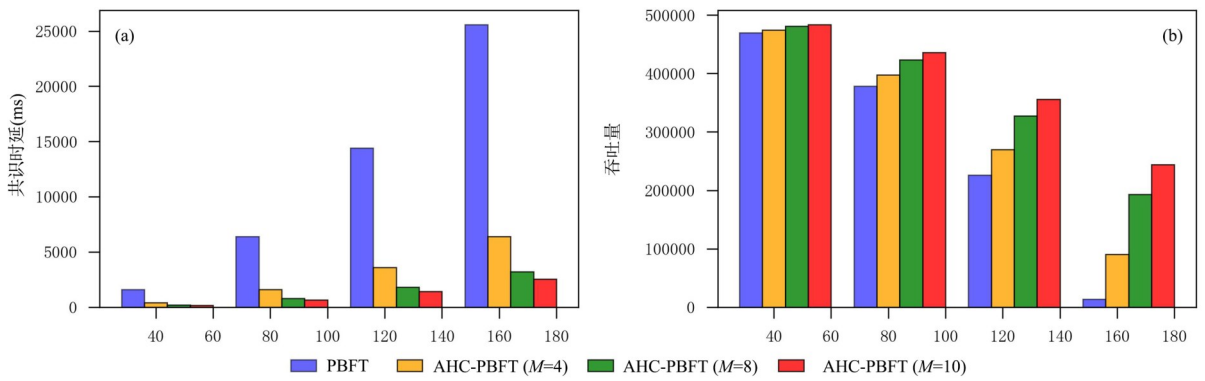

图4　时延与吞吐量对比

Fig.4　Comparison of delay and throughput

由图可见,AHC-PBFT共识算法的时延随共识节点数的增加而缓慢增长,其增长幅度远小于传统的PBFT共识算法. AHC-PBFT共识算法首先在各个子集群内小范围共识后,再在相对少量的当值节点之间共识,这极大地降低了通信开销,使得系统在面对大量网络节点的情况下也能较快地处理交易事务,保持较高的吞吐量.

3　结论

针对EMRs数据分布式共享问题,本文创新性地融合Stackelberg博弈理论、区块链等技术实现低通信开销下的EMRs安全高效共享. 基于联盟链和Stackelberg博弈的EMRs共享模型通过引入ADMM算法实现供需方利益最大化并验证收敛性,基于AHC改进PBFT共识算法提升共享效率,促进医疗系统互操作、缓解数据孤岛. Stackelberg博弈中参与者类型与区块链中的节点类型具有角色逻辑相似性,两者有机结合可以有效解决EMRs数据分布式共享问题. 区块链进行分布式数据记录时,对计算资源需求庞大;而市场化的区块链应用,需要大量用户参与以形成共识,保障区块链网络的稳定性. 博弈理论恰恰能在资源配置方面发挥效用,调动用户积极性,弥补区块链技术的短板. 进一步,再基于AHC思想改进传统区块链中PBFT算法共识效率低、通信开销大的缺陷,以适应大规模医疗机构间EMRs的共享需求.

未来将探索模型在其他领域如跨境数字商务、多部门城市管理等数据共享场景中的应用.

参考文献

[1]　范勇,张政波,王晶. 基于深度学习的电子病历多模态数据融合研究进展. 生物医学工程学杂志,2024,41(5):1062－1071.

[2]　Fabian B, Ermakova T, Junghanns P. Collaborative

and secure sharing of healthcare data in multi-clouds. Information Systems, 2015, 48: 132－150.

[3] Manoj R, Alsadoon A, Prasad P W C, et al. Hybrid secure and scalable electronic health record sharing in hybrid cloud//2017 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering. Piscataway, NJ, USA: IEEE, 2017: 185－190.

[4] Ibrahim A, Mahmood B, Singhal M. A secure framework for sharing electronic health records over clouds//2016 IEEE International Conference on Serious Games and Applications for Health. Piscataway, NJ, USA: IEEE, 2016: 1－8.

[5] Ying Z B, Wei L, Li Q, et al. A lightweight policy preserving EHR sharing scheme in the cloud. IEEE Access, 2018(6): 53698－53708.

[6] Ge Y R, Ahn D K, Unde B, et al. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. Journal of the American Medical Informatics Association, 2013, 20(1): 157－163.

[7] Gordon W J, Catalini C. Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal, 2018, 16: 224－230.

[8] 谷占新, 马利民, 王佳慧, 等. 基于区块链的电子病历安全高效共享方法. 信息安全研究, 2025, 11(1): 74－80.

[9] 杨鑫禹, 牟冬梅, 王萍, 等. 电子病历数据如何驱动临床决策?——驱动过程与影响因素研究. 现代情报, 2025, 45(2): 160－177.

[10] Baza M, Nabil M, Mahmoud M M E A, et al. Detecting sybil attacks using proofs of work and location in VANETs. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 39－53.

[11] Saleh F. Blockchain without waste: Proof-of-stake. The Review of Financial Studies, 2021, 34(3): 1156－1190.

[12] Kiayias A, Russell A, David B, et al. Ouroboros: A provably secure proof-of-stake blockchain protocol// Katz J, Shacham H. Advances in Cryptology. Cham: Springer, 2017: 357－388.

[13] Genç Y, Afacan E. Design and implementation of an efficient elliptic curve digital signature algorithm // 2021 IEEE International IOT, Electronics and Mechatronics Conference. Piscataway, NJ, USA: IEEE, 2021: 1－6.

[14] Chiu W Y, Meng W Z, Ge C P. NoSneaky: A blockchain-based execution integrity protection scheme in industry 4.0. IEEE Transactions on Industrial Informatics, 2023, 19(7): 7957－7965.

[15] Monrat A A, Schelén O, Andersson K. A survey of blockchain from the perspectives of applications, challenges, and opportunities. IEEE Access, 2019(7): 117134－117151.

[16] Cui Z H, XUE F, Zhang S Q, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN. IEEE Transactions on Services Computing, 2020, 13(2): 241－251.

[17] Zaghloul E, Li T T, Ren J. *d*-BAME: Distributed blockchain-based anonymous mobile electronic voting. IEEE Internet of Things Journal, 2021, 8(22): 16585－16597.

[18] Elhence A, Goyal A, Chamola V, et al. A blockchain and ML-based framework for fast and cost-effective health insurance industry operations. IEEE Transactions on Computational Social Systems, 2023, 10(4): 1642－1653.

[19] Zheng X C, Mukkamala R R, Vatrapu R, et al. Blockchain-based personal health data sharing system using cloud storage//2018 IEEE 20th International Conference on E-Health Networking, Applications and Services. Piscataway, NJ, USA: IEEE, 2018: 1－6.

[20] Cao S, Zhang G X, Liu P F, et al. Cloud-assisted secure eHealth systems for tamper-proofing EHR via blockchain. Information Sciences, 2019, 485: 427－440.

[21] Liu J W, Li X L, Ye L, et al. BPDS: A blockchain based privacy-preserving data sharing for electronic medical records//2018 IEEE Global Communications Conference. Piscataway, NJ, USA: IEEE, 2018: 1－6.

[22] Niu S F, Chen L X, Wang J F, et al. Electronic health record sharing scheme with searchable attribute-based encryption on blockchain. IEEE Access, 2020 (8): 7195－7204.

[23] Chen Y, Ding S, Xu Z, et al. Blockchain-based medical records secure storage and medical service

framework. Journal of Medical Systems, 2018, 43(1):5.

[24] Zhang H Q, Xiao Y, Bu S R, et al. Distributed resource allocation for data center networks: A hierarchical game approach. IEEE Transactions on Cloud Computing, 2020, 8(3):778－789.

[25] Zheng Z J, Song L Y, Han Z, et al. Game theoretic approaches to massive data processing in wireless networks. IEEE Wireless Communications, 2018, 25(1):98－104.

[26] Raveendran N, Zhang H Q, Niyato D, et al. VLC and D2D heterogeneous network optimization: A reinforcement learning approach based on equilibrium problems with equilibrium constraints. IEEE Transactions on Wireless Communications, 2019, 18(2):1115－1127.

[27] Jiao Y T, Wang P, Niyato D, et al. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(9):1975－1989.

[28] Xiong Z H, Zhang Y, Niyato D, et al. When mobile blockchain meets edge computing. IEEE Communications Magazine, 2018, 56(8):33－39.

（责任编辑　杨可盛）