# 基于联盟链的区域医疗健康数据安全共享研究*

王甜宇 张柯欣

（辽宁中医药大学信息工程学院 沈阳 110847）

〔摘要〕 介绍国内外区域医疗健康数据共享研究进展以及区块链相关技术，提出基于联盟链的区域医疗健康数据安全共享模型、技术架构及共享过程，为区域医疗健康数据安全共享提供参考和借鉴。

〔关键词〕 联盟链；区域医疗健康数据；安全；共享

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2022.02.011

**Study on Secure Sharing of Regional Medical and Health Data Based on Alliance Chain** *WANG Tianyu, ZHANG Kexin, School of Information Engineering, Liaoning University of Traditional Chinese Medicine, Shenyang 110847, China*

〔**Abstract**〕 The paper introduces the research progress of regional medical and health data sharing at home and abroad and blockchain related technologies, proposes a regional medical and health data security sharing model, technical framework and sharing process based on alliance chain, which provides references for regional medical and health data security sharing.

〔**Keywords**〕 alliance chain; regional medical and health data; security; sharing

## 1 引言

近年来随着我国医疗信息化发展的不断深入以及人工智能、物联网、云计算、可穿戴设备的广泛应用，医疗健康数据呈指数级增长。医疗健康数据是医学研究的宝贵资源，对于疾病预测、诊断、治疗与康复具有重要价值，目前分别存储于各级医疗机构医院信息系统、电子病历系统、影像存储与传输系统、通信系统及实验室信息管理系统中[1]，分散在不同医疗机构的中心式数据库，没有实现区域内医疗机构之间、医疗机构与养老机构之间、医疗机构与政府监管部门之间、医疗机构与保险公司之间、医疗机构与患者之间、医疗机构与第 3 方科研机构之间数据流通与共享[2]，造成信息孤岛。区域医疗健康数据共享能够有效改善医疗机构服务质

〔收稿日期〕 2021－02－24

〔作者简介〕 王甜宇，讲师，发表论文 5 篇。

〔基金项目〕 国家重点研发计划项目“‘肾阳虚证’核心病机、辨证要素与证候辨识标准研究”（项目编号：2018YFC1704301）；辽宁省教育厅科学研究项目“家庭健康管理中医机器人的研究”（项目编号：L202059）；辽宁中医药大学自然科学研究项目“基于区块链技术的中医药大数据安全共享研究”（项目编号：X202010162039）；2021 年辽宁中医药大学一流本科课程培育项目“Oracle 数据库应用”（项目编号：LNZYBK202117）。

量、减少医疗差错、降低患者医疗成本、提高患者满意度[3]，也可以使保险公司获得真实可靠的医疗健康数据。但是医疗健康数据中含有的患者隐私数据高度敏感，容易遭到倒卖和篡改，因此安全共享区域内医疗健康数据已成为亟待解决的问题。

## 2 相关研究

### 2.1 国外

Vazirani A A，O'Donoghue O 和 Brindley D 等[4]通过区块链技术创建高效和可互操作的基础架构管理电子病历中的医疗记录，以改善医疗结果，保持患者数据所有权及敏感数据隐私性、安全性；Kaur H，Alam M A 和 Jameel R 等[5]提出在云环境中搭建基于区块链的异构医疗数据平台，用于存储和管理电子病历；Kim M H，Yu S J 和 Lee J Y 等[6]设计了基于区块链的云辅助电子病历系统安全协议，以防止遭受攻击；Zhang Y L，Wen L 和 Zhang Y J 等[7]提出基于区块链技术的医学图像数据共享加密方案，确保图像数据不可篡改。

### 2.2 国内

梅颖[8]基于区块链技术提出个人医疗记录的分布式安全存储和共享方案，使得个人对医疗记录共享具有使用权和控制权；张超、李强和陈子豪等[9]设计多节点共同维护和共享的联盟即医疗区块链系统，用来防止数据泄露和篡改；杨明、丁龙和许艳[10]提出基于区块链技术的医疗云数据共享方案，使用公开审计确保医疗数据完整性；成丽娟、祁正华和史俊成[3]提出基于联盟链的电子健康记录安全存储共享方案，以实现数据安全存储，提高下载效率；生慧、周扬和马金刚[11]基于联盟区块链和非结构化数据库 MongoDB 设计中医药海量异构数据存储共享方案；宋波、刘铮和冯云霞等[12]基于区块链技术提出医联体系统架构，以解决医联体医院间数据安全问题；黄敬英和蒋勤勤[13]介绍区块链在医联体中的具体应用并提出面临的挑战及应对措施。本文基于联盟链提出区域医疗健康数据安全共享模型、技术框架以及共享过程，为实现区域医疗健康数据安全共享提供参考和借鉴。

## 3 区块链相关技术

### 3.1 区块链

3.1.1 *定义及特征* 区块链是一个分布式、去中心化的共享账本或数据库。其使用加密链式区块结构存储数据，应用共识算法产生、验证和更新数据，利用智能合约操作数据，在去信任的条件下通过分布式系统实现点对点交易和协作，有效解决互联网上信任与价值可靠性传递难题[14]。区块链网络上的节点都是平等的，没有中心服务器；区块链中的数据公开透明，交易数据通过加密技术进行验证和记录，无需第 3 方信任机构参与；区块链由全网节点共同参与维护，某一节点数据更新需要全网其他节点验证，不受少数节点控制；区块链中每个节点都保存全网数据，单个节点故障不会影响整个系统；在区块链上用一串唯一数字代表一个身份，使用数字签名进行身份认证，具有匿名特点，能够更好地保护个人隐私[15]。根据区块链开放程度不同，可以分为私有链、联盟链和公有链。本文基于联盟链实现区域医疗健康数据安全共享。

3.1.2 *私有链* 对单独组织机构开放，如医院、养老院、保险公司内部等使用，私有链上的读写权限以及记账权限由私有组织决定。私有链除增强数据安全性与网络运行可靠性外，与传统中心化技术相比并没有明显优势。

3.1.3 *联盟链* 仅限联盟成员使用，如已被授权的各级医疗机构、养老院等，可以对成员开放链中功能，联盟链读写权限和记账规则由联盟制定。联盟链使参与主体的共识边界由原来的主体私有范围扩展至整个联盟范围。

3.1.4 *公有链* 对外公开，任何个体或组织机构都可以参与、完全去中心化。通过加密技术能够保证交易及链上数据不可被篡改，在不可信的网络环境下建立共识，形成去中心化的信用机制[16]。

### 3.2 安全技术

3.2.1 *非对称加密* 由 1 对唯一的公开密钥（公

钥）和私有密钥（私钥）组成，任何持有公钥的用户都可以使用公钥对信息进行加密，以实现安全交互。只有持有该公钥对应私钥的用户才能正常解密该信息，任何不持有公钥对应私钥的用户都无法将信息解密。

3.2.2 哈希算法 也称数据摘要或散列算法，是将 1 段信息映射成 1 个固定长度的二进制值（哈希值），给定 1 个输入，能够很容易计算对应哈希值，但是对于给定的哈希值，很难计算其对应的输入；对于同一个输入，无论计算多少次都会得到相同哈希值；输入值的微小变化会引起输出哈希值巨大变化[17]。典型的哈希算法有 MD5、SH1、SH256 和 SM3。本文采用中国国家密码管理局发布的 SM3，符合国家安全和监管要求。

## 4 基于联盟链的区域医疗健康数据安全共享

### 4.1 模型

云计算的存储可用性、可伸缩性和按需服务等特性为区域医疗健康数据存储、共享和管理提供便利，但是需要选择值得信任的第 3 方才能确保数据安全性和完整性。医疗健康数据包含较多隐私数据，较易受到非法用户攻击而导致数据泄露。区块链技术以去中心化、透明性、开放性、自治性、不易篡改性和匿名性等特征保证了云服务器中医疗健康数据安全性、完整性和可追溯性。基于联盟链和云计算建立区域医疗健康数据安全共享模型，见图 1。该模型中共有 7 个实体，即患者、医生、医院、保险公司、养老院、第 3 方科研机构和政府监管部门。将联盟链和分布式数据库分别部署在云平台上，对于联盟链来说，患者医疗健康数据需要加密后存储到区块中，包括关键医疗记录、治疗结论、核心账单、存储信息哈希值及云存储链接地址等。将患者在医院诊疗的完整记录信息加密后存储到云平台中的数据库上，同时还存储个人穿戴设备提供的传感器数据、患者在养老院采集的健康数据。医疗健康数据结构复杂，包括患者基本资料（姓名、年龄、性别、身份证号、手机号）、检验和影像数据、电子病历、账单以及个人传感器数据，不适合将所有数据存储在联盟链中，在链下适合使用分布式数据库进行存储，本文采用 MongoDB 在云服务器上存储完整的患者健康数据。

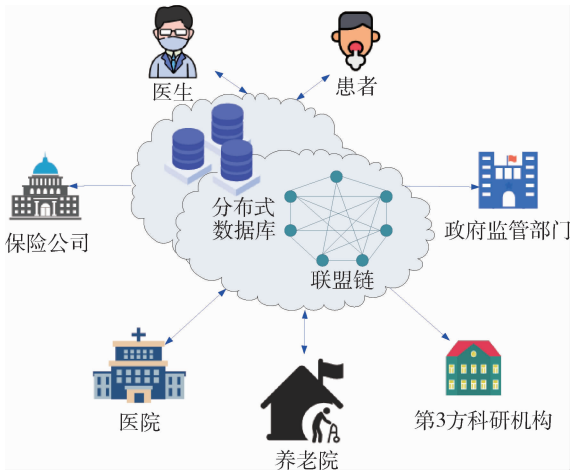


图 1 基于联盟链的区域医疗健康数据共享模型

### 4.2 架构

4.2.1 概述 区块链基础架构分为数据层、网络层、共识层、激励层、合约层和应用层[8]。在区块链基础架构基础上结合现有医联体区块链分层架构[12]设计基于联盟链的区域医疗健康数据共享架构，见图 2。

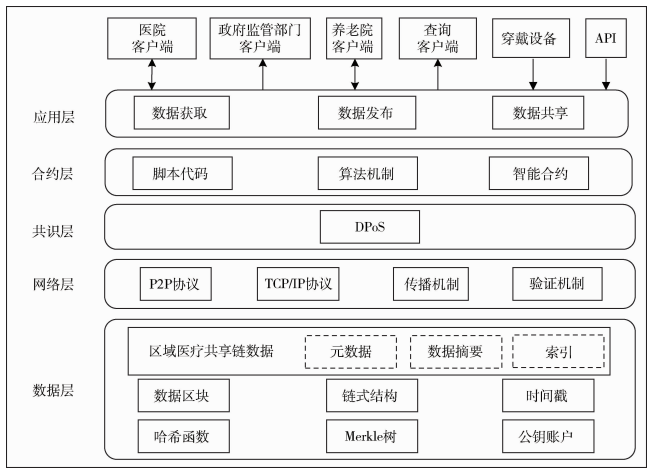


图 2 基于联盟链的区域医疗健康数据安全共享分层架构

4.2.2 数据层 用来存储区域医疗共享链中的区块信息，包括区块头和区块体。利用“区块 + 链”数据结构存储医疗记录，通过 Merkle 存储状态数据，链上每个节点均保存一份数据的完整备份，在

区块链中的数据不易被篡改并能回溯到任意时刻医疗记录。区域医疗共享链是联盟链，其中每个节点都保存前 1 个区块的哈希值，按照时间顺序加入链中，对于被授权用户来说链上数据是公开的，但只保存患者元数据、对应医疗记录数据摘要和该条记录在云平台中的索引。

4.2.3 网络层 联盟链基于点对点（Peer to Peer，P2P）网络协议实现节点间的数据交换与同步，无中心节点，不受单一节点或少数节点控制，保证网络开放性、安全性和稳定性。网络层主要完成节点和节点之间通信，包括 P2P 协议、TCP/IP 协议、传播机制和验证机制。联盟链中的节点分为产生数据的节点、验证节点和审计节点，其中三级甲等医院作为产生数据的节点、二级乙等医院和养老机构作为验证节点，政府监管部门作为审计节点。

4.2.4 共识层 共识机制是区块链技术的核心技术之一，决定了区块链中区块的生成规则。常见共识机制主要有算力证明（Proof－of－Work，PoW）共识机制，权益证明（Proof of Stake，PoS）共识机制，委托权益证明（Delegate Proof of Stake，DPoS）共识机制，实用拜占庭容错算法（Practical Byzantine Fault Tolerance，PBFT）等。本文采用改进的 DPoS 共识机制，由区域内三级甲等医院作为产生数据的节点，为医疗机构、养老机构、保险公司、第 3 方科研机构设置信用积分，存在违规操作会扣除相应积分，按照规定正常操作会获得积分奖励，根据积分变化对产生数据的节点和验证节点进行调整。

4.2.5 合约层 又称扩展层，通过 2 次开发或编程提供扩展性功能，包括脚本代码、算法机制和智能合约。区块链中的智能合约可视为一段部署在区块链上、由事件驱动、具有状态且获得多方承认、可自动运行、无需人工干预、能够根据预设条件自动执行的程序[14]。由系统管理员设置智能合约执行条件，包括向联盟链中上传医疗记录、下载医疗记录、访问对应云平台中的完整医疗记录的条件。当满足执行条件时智能合约被触发执行，完成相应操作。

4.2.6 应用层 在该层医疗机构可以实现医疗记录上传、共享；患者可实现个人医疗记录查看与授权；政府监管部门可实现医疗记录监管；保险公司和第 3 方科研机构通过查询客户端查看共享的医疗健康数据。

### 4.3 过程

4.3.1 数据发布 首先，医疗机构提出医疗健康数据发布请求，将发布的数据用私钥进行签名，请求内容包括发布的数据、签名和公钥；即将存储在联盟链中的数据请求广播到联盟链中，联盟链中的其他节点均收到数据发布请求。其次，由具有确认权限的其他机构进行确认，验证要发布的数据、地址、签名和公钥计算是否匹配，发布数据请求得到确认后将医疗健康数据添加到区块中。最后，将区块添加到联盟链中完成数据发布，见图 3。

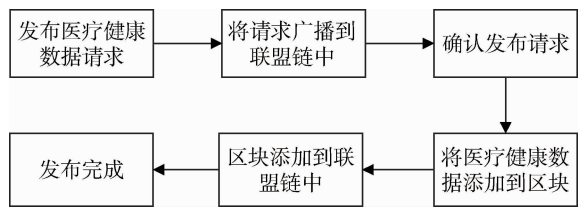


**图 3 联盟链上数据发布过程**

4.3.2 数据共享 在联盟链中已注册机构均可共享联盟链中的数据，如果联盟链中的数据不能满足其需求，提出共享云平台中的数据请求，触发智能合约自动执行，检查请求者签名及请求者查看的该条医疗记录对应在云平台中的链接地址，找到该条记录，通过公钥加密后返回给数据请求者，见图 4。

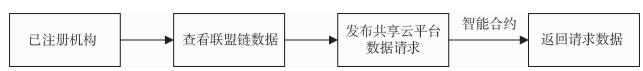


**图 4 医疗数据共享过程**

## 5 结语

医疗健康是人民群众最根本的需求之一，实现区域内医疗健康数据安全共享对于改善医疗资源供需不平衡、缓解医患紧张关系、优化区域内相关机构业务流程、提高医疗健康服务能力具有重要意义[18]。区块链是一种全网串行计算机制，是一种完全去中心化、分布式的结构，将区块链应用在区域

医疗健康数据共享中能够有效解决数据隐私保护、共享、安全管理以及数据可信度等问题。但是区域医疗健康数据发布频率高，区块链中每次交易都需要得到各个节点认可，处理效率有限，同时还会受到网络限制导致拥堵和延迟，降低交易效率，如何提高处理效率是亟待解决的问题。

## 参考文献


1 卫荣，钱步月，兰欣，等. 基于区块链技术的区域医疗数据安全共享问题研究［J］. 中国卫生信息管理杂志，2020，17（2）：136－140，150.

2 王甜宇，孙艳秋，燕燕. 大数据时代云计算在区域医疗信息化中的应用［J］. 中国医疗设备，2015，30（6）：72－74，17.

3 成丽娟，祁正华，史俊成. 基于区块链的 HER 数据安全存储共享方案［J］. 南京邮电大学学报（自然科学版），2020，40（4）：96－102.

4 Vazirani A A，O’Donoghue O，Brindley D，et al. Blockchain Vehicles for Efficient Medical Record Management［J］. NPJ Digital Medicine，2020，3（1）：k4832－5690.

5 Kaur H，Alam M A，Jameel R，et al. A Proposed Solution and Future Direction for Blockchain－Based Heterogeneous Medicare Data in Cloud Environment［J］. Journal of Medical Systems，2018，42（8）：1－11.

6 Kim M H，Yu S J，Lee J Y，et al. Design of Secure Protocol for Cloud－Assisted Electronic Health Record System Using Blockchain［J］. Sensors，2020，20（10）：2913.

7 Zhang Y L，Wen L，Zhang Y J，et al. Deniably Authenticated Searchable Encryption Scheme Based on Blockchain for Medical Image Data Sharing［J］. Multimedia Tools and Applications，2020，79（37－38）：27075－27090.

8 梅颖. 安全存储医疗记录的区块链方法研究［J］. 江西师范大学学报（自然科学版），2017，41（5）：484－490.

9 张超，李强，陈子豪，等. Medical Chain：联盟式医疗区块链系统［J］. 自动化学报，2019，45（8）：1495－1510.

10 杨明，丁龙，许艳. 基于区块链的医疗数据云存储共享方案［J］. 南京信息工程大学学报（自然科学版），2019，11（5）：590－595.

11 生慧，周扬，马金刚. 一种基于联盟链的中医药海量异构数据安全共享解决方案［J］. 世界科学技术－中医药现代化，2019，21（8）：1662－1669.

12 宋波，刘铮，冯云霞，等. 基于区块链技术的医联体系统架构研究［J］. 计算机测量与控制，2020，28（9）：196－201.

13 黄敬英，蒋勤勤. 区块链技术在医联体建设中的应用探讨［J］. 医学信息学杂志，2019，40（10）：30－34.

14 马小峰. 区块链技术原来与实践［M］. 北京：机械工业出版社，2020.

15 范凌杰. 自学区块链原理、技术及应用［M］. 北京：机械工业出版社，2019.

16 陈迪，邱菡，朱俊虎，等. 区块链技术在域间路由安全领域的应用研究［J］. 软件学报，2020，31（1）：208－227.

17 赵其刚，王红军，李天瑞，等. 区块链原理与技术应用［M］. 北京：人民邮电出版社，2020.

18 闵栋. AI＋医疗健康［M］. 北京：机械工业出版社，2018.