基于区块链的电子病历安全共享方案*

姚　尧　袁骏毅　岑星星

（上海市胸科医院/上海交通大学医学院附属胸科医院　上海 200030）

〔摘要〕　**目的/意义** 针对传统医疗信息系统中医疗数据共享困难的问题，提出基于区块链的电子病历安全共享方案。**方法/过程** 利用区块链去中心化、防篡改、可追溯的特性，搭建数据安全共享平台，建立用户鉴权、病历加密、隐私保护、全程追溯等安全机制，实现电子病历的安全共享。**结果/结论** 该方案能够防御潜在的网络攻击且满足患者隐私保护与机密性要求，实验验证了方案的可行性与运行效率。

〔关键词〕　电子病历；区块链；数据安全；数据共享

〔中图分类号〕R－058　　〔文献标识码〕A　　〔DOI〕10.3969/j.issn.1673－6036.2023.11.015

An Electronic Medical Record Security Sharing Scheme Based on Blockchain

YAO Yao, *YUAN Junyi*, *CEN Xingxing*

Shanghai Chest Hospital/Shanghai Chest Hospital, *Shanghai Jiao Tong University School of Medicine*, *Shanghai 200030*, *China*

〔**Abstract**〕　**Purpose/Significance** Aiming at the difficulty of medical data sharing in traditional medical information systems, an electronic medical record (EMR) security sharing scheme based on blockchain is proposed. **Method/Process** The blockchain features of decentralization, tamper－proof and traceability are utilized to build a data security sharing platform and establish security mechanisms such as user authentication, medical record encryption, privacy protection and full traceability to realize the safe sharing of EMR. **Result/Conclusion** The proposed scheme can resist the potential network attack and meet the needs of patients' privacy protection and confidentiality. The feasibility and operation efficiency of the scheme are verified by experiments.

〔**Keywords**〕　electronic medical record; blockchain; data security; data sharing

1　引言

电子病历（electronic medical records, EMR）的建设对于就医流程服务质量、效率、用户体验的提升以及医院智能化水平的促进等有重要作用[1－2]，近年来越来越多的研究者致力于挖掘 EMR 的潜力，涉及公共卫生管理[3]、患者医疗数据共享[4]等方面。由于 EMR 包含患者大量的隐私信息，传统的医疗信息系统将其存储在就诊医院，导致不同医疗机构间共享困难，容易造成“数据孤岛”。

为实现医疗数据的安全共享，有研究[5]提出将区块链技术引入 EMR 系统建设中。区块链本质上是一个授权的账本，具有去中心化、时序数据、集体维护、可编程性、安全性和可靠性等特点[6]。基于区块链的 EMR 系统也面临数据存储、安全分享、访问控制等难点[7－8]。Zheng X 等[9]和 Lin C 等[10]

〔修回日期〕　2023－10－24

〔作者简介〕　姚尧，硕士，助理工程师，发表论文 1 篇；通信作者：岑星星。

〔基金项目〕　上海交通大学医院发展研究院医疗服务管理研究所 2022 年医院管理建设项目（项目编号：YJGL－2022－05）。

提出使用链下的分布式数据库存储医疗数据，解决了医疗数据过于庞大以至于无法存储在链上的难题，但是增加了数据保护难度。Huang H 等[11]使用群签名技术实现病历共享的匿名性与安全性，但是系统的运算开销过大。Nguyen D 等[12]使用对称加密技术保证共享数据的机密性，并通过访问控制手段保证安全性，但是攻击者可能会在挖取节点过程中获取私人信息。Patel P 等[13]和 Lee J 等[14]都提出将智能合约与访问控制结合，对访问区块链的用户进行权限管理，但使后期追溯变得困难。现有研究表明，将区块链和 EMR 数据共享相结合具有以下优势。一是去中心化，防止病历数据的未经授权访问和篡改。二是数据隐私与匿名性，确保只有授权的用户可以访问和查看特定的病历数据。三是可追溯性，意味着 EMR 的共享可以被准确地追踪和审计。四是易共享性，使不同的医疗机构系统可以无缝共享和交换数据。本文提出一种基于区块链的 EMR 共享方案，主要工作包括结合区块链技术与传统数据存储方式，建立区块链安全共享平台，通过智能合约与外部服务交互，实现第三方用户的鉴权与访问控制；探讨医疗数据全生命周期各环节的保护方案，针对不同数据运用不同的加密方式，针对机构间信息交互做到数据存证与操作审计，保障系统的安全性。

2　系统架构（图 1）

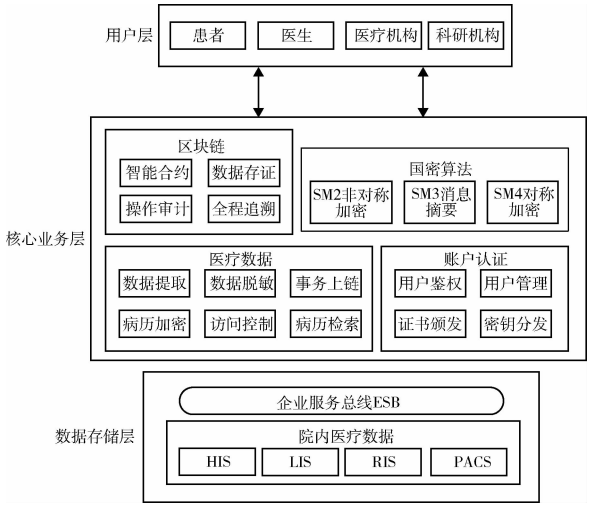

图 1　总体架构

2.1　用户层

用户层共包含 4 个实体。患者：患者到医院就诊后会生成相应的医疗数据，是数据的拥有者，对病历是否共享拥有决定权。患者通过区块链平台进行身份注册并获得统一的身份标识符与密钥。医生：可以在平台查看患者的历史病历，授权后可在院外远程查看病历数据。医疗机构：若患者需要在不同的医疗机构查看历史病历，授权后可通过共享平台实现跨机构的病历检索与查阅。科研机构：可以向多个医疗机构请求医疗数据共享，用于科研，需要得到相应患者和医院的授权。

2.2　核心业务层

核心业务层通过区块链服务、医疗数据处理、国密算法和账户认证 4 个模块实现 EMR 的安全共享。区块链是保障系统安全性的核心部件，其基本结构，见图 2。由于区块链去中心化特点，系统不需要可信的第三方或者中心节点统一处理事务，各节点都拥有一个区块链副本，并随时同步和维护链上内容。由于每一个区块同时包含自身的哈希值与前一个区块的哈希值，如果其中某一个区块的信息被篡改，将会导致自身哈希值的变化，使区块链断链，保证了系统的防篡改。

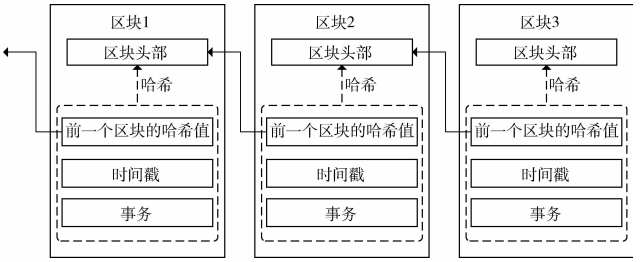

图 2　区块链基本结构

区块链系统采用多节点共识的存证服务，经证书签证机关（certification authority，CA）授权的多个医疗机构组成联盟，各自作为系统的节点，负责将信息交互事务记入共享账本。按照 T/CESA 1048—2018、T/CESA 1049—2018 相关标准，对用户注册、病历提交、获取、检索、调阅等业务服务交互进行信息安全审计。智能合约是集成在区块链

服务内的一个自动执行的程序，作为外部服务和区块链交互的接口，用于约定事务上传的格式以过滤节点非法请求，提供服务封装。通过配置访问控制列表功能，判断请求者是否有获取相应数据的权限，实现用户识别。各节点将事务打包上传，经实用拜占庭容错[15]共识算法认定成功后，上传至区块链。医疗数据处理涵盖 EMR 脱敏、加密与事务上链等功能，保证数据的安全共享。共享的 EMR 经国密 SM2 非对称加密算法与 SM4 对称加密算法处理，即使发生泄漏，攻击者也无法获得有用信息。

2.3 数据存储层

基于等级保护 2.0 的要求，院内医疗数据保存在内网，区块链安全共享平台部署在外网单独的安全隔离区，内外网通过防毒墙与网闸隔离，保证数据的安全交换[16]。互联网应用通过区块链前置机访问共享平台，接口设计基于企业服务总线，提供符合标准规则的封装服务。共享数据平台均按照《WS/T 447—2014 基于电子病历的医院信息平台技术规范》与《医院信息互联互通标准化指标》建设。

3 EMR 安全共享

对 EMR 共享全生命周期进行推导，其符号，见表 1。共享模型，见图 3。

表 1 符号及其解释

符号	解释
P	患者
PI_p	患者的身份信息
No_p	患者的医保卡号
Sig_p	患者的唯一身份标识符号
SK_x/ PK_x	x 的私钥/公钥
K_x	x 的对称密钥
EMR	明文电子病历
EMRen	密文电子病历
E_{SK}（m）/ E_{PK}（m）/ E_K（m）	用私钥、公钥、对称密钥加密消息
T_R	注册事务
T_M	病历事务
h（）	消息摘要计算
||	拼接操作

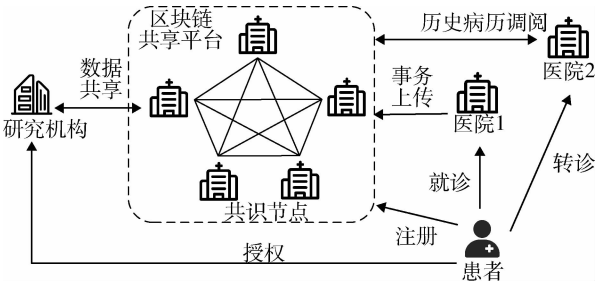

图 3 共享模型

3.1 系统初始化

医院在 CA 注册后，生成医院节点公、私钥对（SK_{hos}，PK_{hos}），经 CA 签发数字证书后返回医院进行本地保存。

3.2 患者注册

患者首次来院需要在平台注册，医院生成相应的区块链注册事务 T_R =（register，h（PI_p || No_p，sig_p），其中 register 表明此事务功能为患者注册，h（PI_p || No_p 为患者注册信息（医保卡号、身份信息）的摘要，sig_p 为该患者的唯一身份标识符。系统收集注册事务后进行共识上链，最后随机生成该患者的对称密钥 K_p。

3.3 患者就诊

患者经医生诊断后，医院首先生成患者的明文 EMR，并使用国密 SM3 算法计算得到摘要 h（EMR）。然后使用医院本地私钥 SK_{hos} 并采用国密 SM2 算法对摘要进行数字签名得到 $E_{Sk_{hos}}$（h（EMR））。最后，将明文 EMR 与数字签名拼接，使用患者密钥 K_p 进行基于国密 SM4 的分组对称加密，得到加密后的病历数据 $EMR_{en} = E_{K_p}$（EMR || $E_{Sk_{hos}}$（h（EMR））），存入医院本地数据库。区块链平台通过企业服务总线的接口与医院本地数据库交互，自动生成病历上传事务 T_M =（medical，h（EMR_{en}），sig_p，pointer），其中 medical 表明此事务功能为病历信息，h（EMR_{en}）为密文 EMR 的消息摘要，sig_p 为患者唯一身份标识符，pointer 为病历在本地数据库的索引信息，事务经共识后上链。

3.4 病历共享

共享场景一：患者去医院 2 就诊并有查看医院 1 历史病历的需求，通过身份验证登录平台。由该医院前置机启动区块链智能合约，根据sig_p查询区块链记录，随后发起病历调阅请求。待节点共识存证后，平台自动根据 pointer 检索患者历史病历，并使用PK_{hos2}加密相应患者的对称密钥E_{K_p}，与密文EMR_{en}经安全网络通道传输至医院 2。医院 2 使用SK_{hos2}解密得到E_{K_p}，再使用E_{K_p}解密得到具有数字签名的明文 EMR ‖ $E_{Sk_{hos1}}$(h(EMR))。拆分出后 32 字节之后使用PK_{hos1}解密，得到 EMR 的摘要 h(EMR)。同时根据 SM3 算法计算出 h’(EMR)。若二者比对一致，则表示 EMR 是完整有效的。

共享场景二：科研机构向平台申请 EMR 的共享，注册并获得相应患者的授权。由于科研机构并不具备直接访问链上数据的权限，需要以共识节点中某一医疗机构为代理，发起病历共享申请。与医疗机构间共享过程的区别在于科研机构获得的 EMR 会经平台脱敏处理，避免泄露患者敏感信息。

4 安全性分析

4.1 数据安全

患者病历数据经对称加密后保存在医院本地安全区域，不直接暴露在互联网环境，保证数据存储安全。在病历共享过程中，密文只有拥有 K_p 的授权用户才能解密。此外，区块链的去中心化、透明性、信息不可篡改性特点，对病历共享交互全程数据存证，确保可信安全。

4.2 防重放攻击

假设攻击者有能力在区块上链过程中拦截，并意图重放该区块到区块链服务器以修改事务数据，则该攻击者必须要面临时间戳过期的问题。由于区块链的特性，元数据中的时间戳是不容易被篡改的，一旦某个发送到区块链的请求被重放，时间戳一定会发生变化，影响整个链的哈希验证，以此抵御重放攻击。

4.3 患者隐私保护

首先，患者在区块链上的身份信息均经过了国密 SM3 摘要算法处理，避免了敏感信息的直接暴露。其次，与科研机构共享的病历数据均进行了脱敏处理，去除了患者身份信息，科研机构不能从共享的医疗数据中获取患者隐私。

4.4 监管与追溯

基于区块链的 EMR 共享平台构建了一套完整的用户授权、事务存证、数据交换鉴权、操作审计的监管方案。数据访问记录全流程上链，确保数据访问路径的全程可回溯。当发生数据泄露时，能快速定位问题源并处理。

5 可行性分析

5.1 实验环境

为验证本文方案的可行性，对整个系统流程进行了仿真实验，实验平台为 Windows Server 2019，处理器为 Intel Xeon Silver 4210R，内存为 64 GB，基于 Hyperledger Fabric[17] 框架搭建区块链系统与云服务器，采用 go 语言开发智能合约应用程序接口，实现功能主要包括：用户节点管理、区块链的生成与维护、区块查询、事务上传等功能。借助 Hyperledger Explorer 实现区块链系统的后台管理。

5.2 数据准备

选用上海市胸科医院医院信息系统存储的真实患者 EMR 作为测试数据，涵盖门诊病历、住院病历、药品处方、检查检验报告等，EMR 文件的平均大小为 32 KB。调取其中 500 000 份用于测试不同 EMR 文件数量下区块链消耗的存储空间，例如，若要通过区块链系统分享 250 000 份 EMR，则包含相应事务的区块链共占用 119 MB 的空间，见图 4。

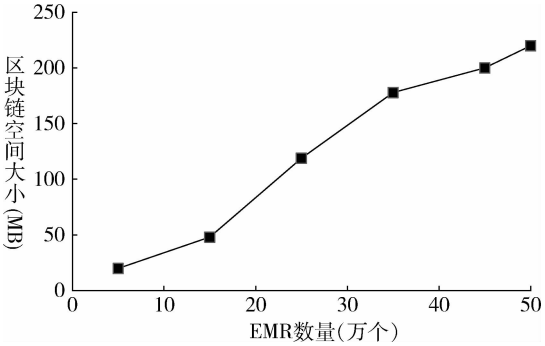

图 4　不同 EMR 数量下区块链占用空间

5.3　吞吐量分析

定义每秒处理的事务量为系统吞吐量（transaction per second，TPS），通过仿真实验测试事务提交上链的吞吐量，运行初始节点数量为 4，依次新增 2 个节点，见图 5。当区块大小固定为 4 MB 时，系统的吞吐量最高。由于增加节点数量会增加共识过程消耗的时间，当区块大小固定时，随着节点数量的增加，吞吐量逐渐减少。当区块大小为 4 MB 时，吞吐量从 17 TPS 减少为 12 TPS。

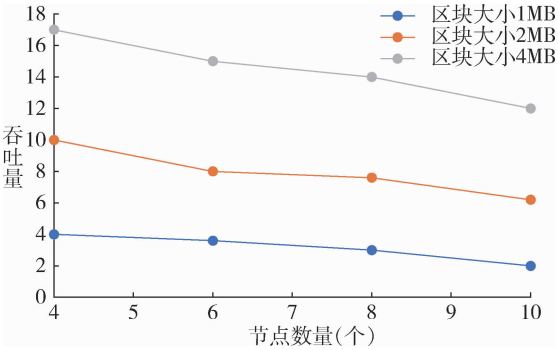

图 5　不同节点数量下系统吞吐量

5.4　耗时分析

本文运用的各种加解密运算消耗时间，见表 2。非对称加密方式的运算消耗远大于对称加密，因此采用前者加密重要信息与数字签名，采用后者加密数据量较大的 EMR 文件。

表 2　运算时间消耗(毫秒)

T_{XOR}	T_h	T_E	T_D	T_K
0.002 0	0.002 5	0.024 5	46.735 1	0.003 8

注：T_{XOR} 为异或运算消耗的时间，T_h 为哈希运算消耗的时间，T_E、T_D、T_K 为非对称加密、解密、对称加密消耗的时间。

为了评估区块链系统的运行效率，测试不同区块数量（1 ~ 10 000）下系统的平均响应时间，涵盖上传时间与验证时间，见图 6。测试结果表明，本文的区块链系统在面对大量请求的同时能够达到较低的延迟，满足实际场景使用要求。

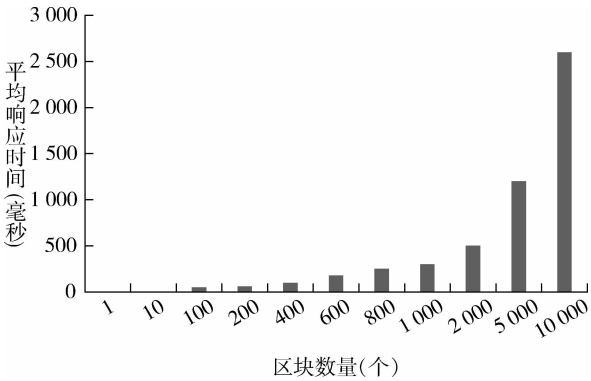

图 6　不同区块数量下区块链平均响应时间

6　结语

本文提出一种基于区块链的 EMR 安全共享方案，利用区块链去中心化、透明性、信息不可篡改性等特点，实现医疗数据的安全共享。阐述了方案整体架构，论证了区块链系统和国密算法在 EMR 共享全流程的安全保护作用。通过安全性分析评估了方案在数据安全、防御攻击、隐私保护等安全指标的表现。通过实验分析了方案的吞吐量、响应时间等综合性能水平。区块链分布式的特性使系统具有可扩展性，可以根据需求增加或减少节点数量。当用户数量或数据量增大时，可添加更多节点来水平扩展分担负载，提高系统的性能。以下问题待进

一步研究：一是系统的可推广性，由于本文方案包含患者自行注册与身份验证环节，有待进一步减轻患者使用区块链平台的难度；二是数据的共享标准问题，拟通过人工智能信息提取技术，采用结构化的病历共享标准，促进数据的无缝交互。

参考文献

1 国家卫生健康委员会. 关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知［EB/OL］.［2023－08－22］. https：//www. gov. cn/zhengce/zhengceku/2018－12/31/content_5435418. htm.

2 国家卫生健康委员会. 2018 年我国卫生健康事业发展统计公报［EB/OL］.［2023－08－22］. https：//www. gov. cn/guoqing/2020－04/29/content_5507528. htm.

3 CRAMERI K, MAHER L, VAN D, et al. Personal electronic healthcare records：what influences consumers to engage with their clinical data online? A literature review［J］. Health information management journal, 2022, 51（1）：3－12.

4 HO S, GUO X, VOGEL D. Opportunities and challenges in healthcare information systems research：caring for patients with chronic conditions［J］. Communications of the association for information systems, 2019, 44（1）：852－873.

5 SHI S, HE D, LI L, et al. Applications of blockchain in ensuring the security and privacy of electronic health record systems：a survey［J］. Computers & security, 2020, 97（1）：101966.

6 LI H, ZHU L, SHEN M, et al. Blockchain－based data preservation system for medical data［J］. Journal of medical systems, 2018, 42（8）：1－13.

7 DAI W, DAI C, CHOO K, et al. SDTE：a secure blockchain－based data trading ecosystem［J］. IEEE transactions on information forensics and security, 2019, 15（1）：725－737.

8 KIM M, LEE A, KWON H, et al. Sharing medical questionnaries based on blockchain［C］. Madrid：IEEE International Conference on Bioinformatics and Biomedicine, 2018.

9 ZHENG X, MUKKAMALA R, VATRAPU R, et al. Blockchain－based personal health data sharing system using cloud storage［C］. Ostrava：IEEE 20th Internation Conference on E－health Networking, Applications and Servvices, 2018.

10 LIN C, HE D, HUANG X, et al. DCAP：a secure and efficient decentralized conditional anonymous payment system based on blockchain［J］. IEEE transactions on information forensics and securiy, 2020, 15（1）：2440－2452.

11 HUANG H, CHEN X, WANG J. Blockchain－based multiple groups data sharing with anonymity and traceability［J］. Science China information sciences, 2020, 63（3）：1－13.

12 NGUYEN D, PATHIRANA P, DING M, et al. Blockchain for secure EHRs sharing of mobile cloud based e－health systems［J］. IEEE access, 2019, 7（1）：66792－66806.

13 PATEL P, MAJUMDER S, SHEVKAR S, et al. EMRs with blockchain：a distributed democratised electronic medical record sharing platform［C］. Hawaii：International Conference on Blockchain, 2021.

14 LEE J, CHEW C, LIU J, et al. Medical blockchain：data sharing and privacy preserving of EHR based on smart contract［J］. Journal of information security and applications, 2022, 65（1）：103117.

15 XIONG H, CHEN M, WU C, et al. Research on progress of blockchain consensus algorithm［J］. Future internet, 2022, 14（2）：47.

16 袁骏毅，潘常青，宓林晖. 基于等级保护 2.0 标准体系的医院信息化安全建设与研究［J］. 中国医院，2021，25（1）：72－73.

17 ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric：a distributed operating system for permissioned blockchains［C］. Porto：The Thirteenth EuroSys Conference, 2018.