网络出版时间：2018-12-21 17:32:59
网络出版地址：http://kns.cnki.net/kcms/detail/61.1450.TP.20181221.1524.034.html

基于区块链的电子医疗记录共享研究

董黛莹[1]，汪学明[2]

（1.贵州大学 计算机科学与技术学院，贵州 贵阳 550025；
2.贵州大学 计算机科学与技术学院，贵州 贵阳 550025）

摘 要：电子医疗记录（EMR）是高度敏感且非常重要的信息记录，医疗记录的共享对患者的准确调治、医疗的发展等方面具有重大意义。为改善由于各医疗机构的电子医疗记录系统出现的数据安全得不到保证、权限验证周期长等现象，而造成电子医疗记录不能在安全高效率的环境下共享的问题。对区块链主要原理和关键技术进行了研究，并基于区块链去中心化、不可篡改、开源透明、可编程等特点，设计了加入改进的拜占庭容错系统共识机制的电子医疗记录（EMR）共享模型，能够为数据安全和隐私存储提供保障。文中对电子医疗记录模型进行分析评价，保证安全的同时可以减少医学数据共享的周转时间，从而提高效率。最后探讨了基于区块链技术的医疗共享系统目前有待解决的问题和局限性。

关键词： 区块链；安全；分布式；数据共享；去中心化

Design of Electronic Medical Record Sharing Model based on Blockchain

DONG Dai-ying[1], WANG Xue-ming[2]

(1. Guizhou University, Guiyang, Guizhou 550025, China;
2. Department of Computer Science and Technology, Guizhou University, Guiyang, Guizhou 550025, China)

Abstract: The electronic medical record (EMR) is a highly sensitive and very important information. The sharing of EMR have great significance to the accurate regulation of patients and the development of medical treatment. In the fact, Electronic medical records can not be shared because of the incompatibility of electronic medical record system, the lack of guarantee of data security and the long cycle of authorization verification. The main principle and key technology of block chain, based on block chaining, centering, can not change, open source, transparent, programmable and so on. The electronic medical record (EMR) sharing model based on the improved consensus mechanism of Byzantine fault tolerant system is designed to provide data security and privacy storage, and reduce the turnaround time of medical data sharing Next, analysis and evaluation of electronic medical record model. And this paper discusses the problems and limitations of the shared medical system using Blockchain.

Key words: Blockchain;security;distributed;data sharing;decentralization

0 引 言

在医疗行业中，数据共享对智慧医疗的发展、医疗机构之间学术讨论等方面都有着突破性的重大意义[1]。如阿里健康将区块链应用到医疗架构体系中，与常州市合作将同区域医疗资源整合到一起，实现部分医疗机构的数据共享。Healthnautica 使用区块链技术制作了可指定化的客户驱动的云软件系统，供医生操作和病人办理手续，让医院、医生、病人三者之间沟通无阻碍。BitHealth 将区块链运用到医疗健康数据存储保护[2]，采用 BitTorrent[3]的点对点文件传播形式，有利于网络延迟恢复数据，减少各方面的支出、解决医疗记录的重复和分散问题。Gem[4]用区块链技术构建一个医疗保健全球一体化的平台，更加贴合人们的需求，提供更好的更有意义的服务。电子医疗记录共享难以实现，主要原因有：第一，电子医疗记录系统不统一。各医疗机构使用的电子医疗记录系统模式存在较大差异，医疗记录数据格式没有统一，各系统不能协同工作，数据共享困难。第二，访问数据周期长。用户在访问时需要借助医疗信息系统（HIS），期间需要进行身份核实、访问权限审核等环节，访问量较大还可能造成网络拥塞，数据访问周期相对较长。第三，用户电子医疗记录安全得不到保证。电子医疗记录信息量大且重要，患者担心自己的电子记录用在何处会被谁查看，泄露个人隐私，而且电子医疗记录存储在特定医疗机构，若有针对性攻击，系统很容易出现信息泄露、数据被篡改的情况。同时，纸质

项目基金：国家自然科学基金项目([2011]61163049)； 贵州省自然科学基金项目(黔科合 J 字[2014]7641)
作者简介：董黛莹(1993-)，女，辽宁鞍山人，硕士研究生，研究方向：密码学与信息安全,CCF 会员号：72439G；汪学明(1965-)，男，安徽绩溪人，教授、博士，研究方向：密码学与信息安全。CCF 会员号：E200036215M；

医疗记录保存管理不易，并且医务人员可能由于不能确信病人病历而发生误用药物。

电子医疗记录要实现共享，首要就是保证数据的安全可靠，针对该问题研究者们做了大量工作，设计出了很多防止医疗记录泄露的系统，如基于医学数字成像和通信(DICOM)的相关系统，但这并没有真正实现电子医疗记录共享。而区块链的出现可以解决电子医疗共享上存在的很多问题。

本文基于区块链技术公开透明、不易篡改、去中心、非对称加密等特性，设计了电子医疗记录共享模型，保证电子医疗记录的真实有效，为数据安全和隐私存储提供保障，还可以大大降低成本，提高医疗效率，减少医疗过失。并让患者可以定制个性化访问控制，实现患者真正参与到电子记录共享中。

1 相关技术

区块链概念于 2008 年中本聪在一次密码小组讨论中发表的论文《比特币：一种点对点的电子现金系统》[5]中首次提出，2015 年下半年梅兰妮.斯万[6]对区块链的应用前景及区块链的局限性进行了系统阐述。同年，《The promise of the blockchain：The trust machine》发表之后，区块链正式引起人们的关注，IT 巨头、研究学者纷纷投入到区块链的研究中。近几年各国纷纷投入到区块链研发当中，成立区块链研发公司、开发区块链平台来研究其潜在应用场景。

区块链技术可以理解为是分布式的数据库[7]，有别于当前主流的关系型数据库的不可转移信息与安全化。区块链技术方案主要是将数据区块（Block）使用数学方法，通过安全可靠的加密算法相互关联。区块链技术方案主要是将数据区块（Block）使用数学方法，通过安全可靠的加密算法相互关联。用区块记录一定时间内的交易信息，并通过密码学方法验证信息是否真实有效，并用指针链接到上一个区块形成一条主链（Chain）[8]。

1.1 哈希函数和 Merkle 树

在区块链系统中，节点将一段时间的交易信息进行打包，通过各节点用特定哈希算法将交易分别压缩成一段 64 位代码（哈希值），两两哈希值继续压缩生成唯一的哈希值称为 Merkle 树根[9]。使用哈希加密的好处在于哈希函数具有抗碰撞性，且哈希计算时间相同输出长度固定。此外，无论文件有多大，哈希对应过程是无法通过计算反推的。每一个区块头中的哈希值指向前一个区块，形成链式结构。在本文中哈希指针起到验证信息是否发生改变的作用。

1.2 智能合约

智能合约是区块链的核心要素[10]，智能合约是使区块链可编程的一段脚本代码，由事件触发。本文将其应用在以太坊区块链上，一旦符合规定的条件即自动执行代码的内容。在以太坊中，智能合约能够帮助系统实现复杂的访问控制策略，有助于数据的维护、存储。智能合约模型如图 1 所示。

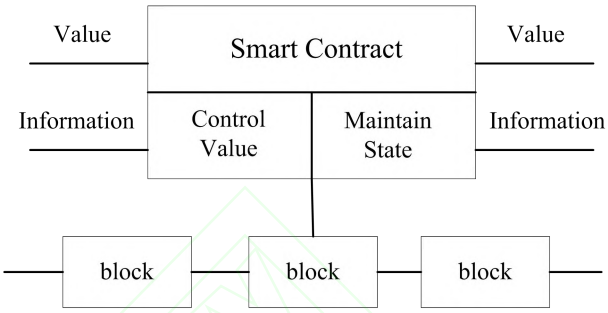

图 1 区块链上的智能合约模型结构

Fig.1 The smart contract model structure of Blockchain

2.3 以太坊区块链

比特币区块链中的每笔交易可写入的信息量是 40 字节，随着交易量的增加，累积的数据量就会增大，交易确认需要花费的时间就会很长。为了加快交易速度、缩短交易时间，以太坊区块链[11]应运而生。以太坊区块链可以解决区块链中因累积数据过多而处理效率下降这一问题。另外，可以灵活使用智能合约，并具有图灵完备性[12]。可以通过 solidity 语言编写所需要的应用场景，依靠 EVM 自动执行，并以 P2P 网络为基础，真正实现无中心化的管理。使用简单，易储存合约数据。以太坊与区块链交互时需要区块链地址 Add=SHA3（pk-‘04’）和密码 password[13]。

2 医疗数据共享模型

2.1 电子病历共享模型设计

医疗机构联盟服务群组：根据医疗机构评审，由国家医疗卫生政策管理机构选出满足硬件设施、流量大、数据多等条件的医疗机构，根据标准将所有医疗机构综合评估进行排名取前 200 家医疗机构为高级联盟服务群。

本模型加入 Hash 算法，将上传的数据信息进行 hash 算法生成特定的摘要值存入区块，这样不仅节省空间还可以通过摘要与原文 hash 的对比来验证上传数据的真实性。查看时通过摘要来检索。

采用改进的实用拜占庭容错系统（Practical Byzantine Fault Tolerance，PBFT）共识机制[14]，为避免某些节点不符合条件或者没有记账和查询的能力，因此选取高级联盟服务群作为主节点的选取范围，并选

排在首位的医疗机构为主节点。这样不仅可以降低主节点出错的可能概率，还可以在提高效率的同时降低危险系数，并提高达成共识的速度。设计模型如图 2 所示。

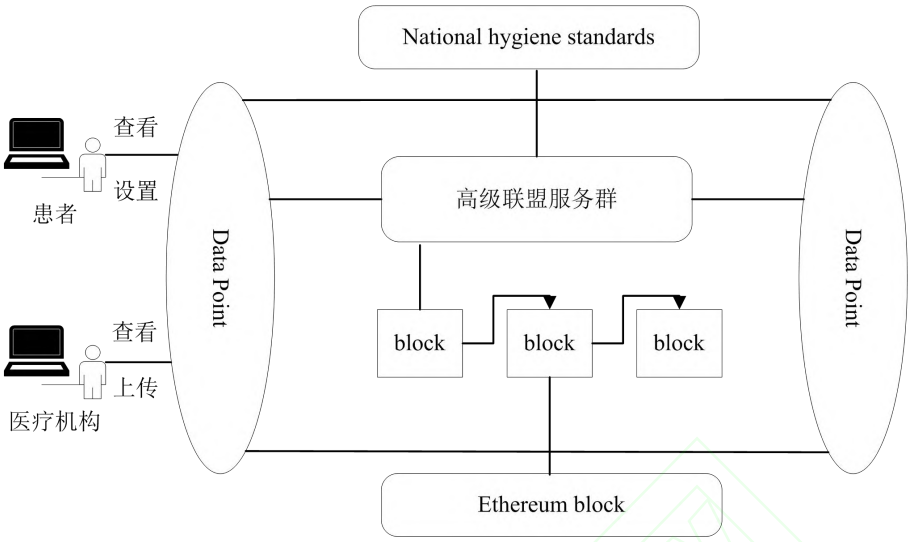

图 2 电子病历记录共享模型（EMRM）

Fig.2 Design of electronic medical record sharing mode

模型工作步骤如下：

(1)高级联盟服务群中的节点需要在网络上注册一个公钥，得到一个特定的 32 位标识符。然后该标识符会被每笔交易数据的“头部”引用。

(2)医疗机构通过客户端将数据用公钥加密并上传到链外的可信数据库中。

(3)客户端通过 P2P 网络向主节点发送请求，主节点收到请求将其排序后广播之后达成共识。

(4)将达成共识后的数据上传到区块链分布式数据库。

(5)节点将区块形成区块链，用 web3 提供的 API 与 Geth 节点相交互，并用 password 对用户的私钥加密。

(6)患者可通过身份认证查询数据，医生可上传数据或通过访问控制对数据进行查询。

医疗机构通过身份认证后将患者的电子病历数据进行封装并使用患者的私钥对数据加密,上传送到脱链的可信存储库，向请求端 C 发送<REQUEST,O,T,C>到主节点，主节点收到请求后除自己以外的所有节点广播，Commit 阶段，节点们收到主节点广播的数据后备份再次广播，这时为节省空间和通信费用，将区块的唯一标识符封装进行广播，直到所有节点都广播为止。若收到超过一定数量的相同请求，则对 C 进行反馈，确保数据的真实可靠后由节点将数据生成区块加入区块链。改进后的 PBFT 机制比原以太坊 PoW 共识机制的 CPU 占用率低，可以节省算力，提高效率。

2.2 访问控制模型描述

本文设计的区块链电子医疗记录共享模型，通过访问控制，实现用户自定义个性化访问控制策略，是为解决数据共享在隐私保护方面存在几个问题[15]：首先患者敏感数据可能会被非法窃取，容易被泄露，其次大多数情况下医生在没有通过患者的同意就查看患者的历史医疗记录。另外，患者没有参与到自己的健康数据共享中，不知自己的数据会用在何种用途。因此设置访问控制能够更好的保护患者个人隐私的同时也帮助医疗机构更高效准确的诊治患者。

定义 访问控制模型基本元素

用户集：$U=\{user_1, user_2...user_n\}$，所有用户的集合。

角色集：$R=\{role_1, role_2...role_3\}$，用户在一个系统中的身份的集合，有角色来决定对资源操作的权利。

会话：SESSION，表示用户与角色之间相互对应的关系。

权限：Permission，表示访问数据可以进行的操作。

目的集：Purpose=$\{pu_1, pu_2...pu_n\}$,分为访问目的（AP）和使用目的（UP）。AP 是指医疗相关人员想要将访问的数据用在何处，UP 是指患者希望自己的医疗数据用在何处。

Rpu⊆Roles×purpose,表示角色与目的的绑定。

Rpe⊆Roles×Permission 表示角色与权限的绑定，不同角色由不同的权限设置。

PR⊆Purpose×Permission 表示目的在特定权限上

的操作。

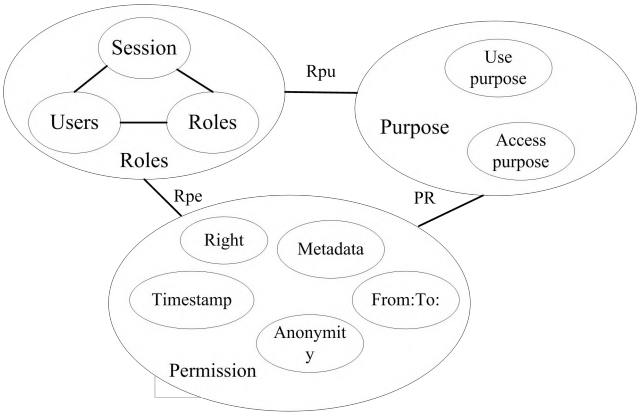

图 3 访问控制模型结构

Fig.3 The model of access control

访问控制模型结构如图 3 所示。用户根据自己的偏好对自己的健康数据设置允许数据使用的意图，并对自己的数据设置权限，其中 Right（read/share）规定数据可以进行哪些操作，患者设置 From：To:，只有在这个过程中有权访问，患者也可以使用匿名标签指定数据是否需要匿名。Timestamp 的目的是为了确保一个权限值设置了一次。

访问控制步骤：

(1)生成系统参数 K_P 和主私钥 K_M

(2)用户申请注册，将获取的身份 ID 和用户属性集 Att_u 发送给认证中心 CA，验证正确后进行步骤(3)，否则终止。在区块链中注册后，只能用户本身访问数据或者由通过权限的代理可以访问数据。

(3)认证中心 CA 通过量子密钥分配方式下发私钥 Ks 给用户。

(4)患者制定访问控制策略，输入要加密的数据信息 m，生成密文后上传。

(5)用户要访问数据时，首先进行身份认证，之后用户提出访问请求。其次检测该角色是否拥有指定的访问目的，若通过则根据患者设置的可访问时间段，使 UP 与 AP 相核对，AP 与 UP 不符，请求被拒绝。访问控制步骤如图 4 所示。

3 对模型的评价分析

3.1 安全分析

本模型特点是采用 P2P 结构，避免了单点攻击，通过所有节点共同维护，可以很好的保证系统稳定性。

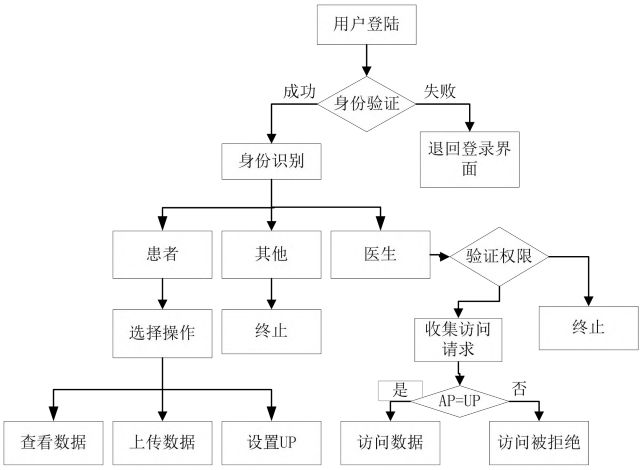

图 4 访问控制流程图

Fig.4 The flow of access control

在分发密钥过程中，若私钥被窃听或截取，根据采用的量子密钥分配的特性，会被通信双方所察觉，认证中心会将此密钥作废另发新密钥，直到安全为止。

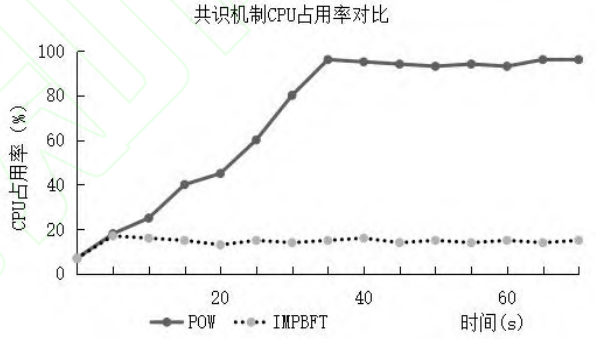

图 5 CPU 占用率对比

Fig.5 CPU utility compare

3.2 效率分析

全网采用改进的 PBFT 共识机制，保证数据的真实有效。通过实验收集的数据得出，改进的 PBFT 共识机制比原以太坊使用的 PoW 共识机制更适用于本模型如图 5 所示。从图中数据线性趋势对比可以看出，改进后的 PBFT（IMPBFT）比原来的 POW 共识机制占用的时间明显要少很多，对请求可作出快速响应。

3.3 性能分析

采用对照分析法，从是否基于区块链、能否减轻主链压力、网络容错性这三个方面的性能，对主流医疗模型进行分析，其中 BitHealth 可以称作是近年来最可靠的医疗平台，几乎不会出现瘫痪的情况，但是在资源利用方面存在一定的缺陷，MedRec 的主要特点是隐私保护，但在资源占用和网络容错方面没有 EMRM 有优势，还有最近薛腾飞等人提出的 MDSM 使用改进

的 DPOS 共识机制，能够减轻主链压力，但在网络的稳定性方面有一定劣势。本文提出的 EMRM 通过改进的 PBFT 增强网络的稳定性，降低了资源利用率，与具有代表性的模型进行对比的具体情况如表 1 所示。

表 1 模型对比

Table1 Model contrast

模型	基于区块链	减轻主链压力	网络健壮
Factom	否	是	否
MedRec	是	否	否
BitHealth	是	否	是
MDSM	是	是	否
EMRM	是	是	是

4 结论

本文研究了区块链的主要技术和发展现状，介绍了电子医疗记录共享的重大意义以及现实电子医疗记录共享存在的问题，根据存在的问题，设计了基于区块链的电子医疗记录共享模型，解决了当前电子医疗记录共享中存在的信息安全性弱的问题。但也存在很多不足，接下来会对细节进一步完善，对共识算法进一步改进，实施的过程进一步探究。

参考文献

[1] Charles D,Gabriel M,Furukawa M F.Adoption of electro nic health record systems amongUS non-federal acute c are hosp-itals:2008-2012[J].ONC data brief,2013,9:1-9.

[2] Baxendale G. Can Blockchain Revolutionise EPRs[J]. It now, 2016, 58(1):38-39.

[3] Brad Rougeau,Mea Wang.Uncover the Peer Distribution in BitTorrent[J].Tsinghua Science and Technology,2012, 17(01):17-28.

[4] Tong Zhang. The Business Model of Health Websites [A]. Wuhan Zhicheng Times Cultural Development Co., Ltd.Proceedings of 2017 International Conference on Sp orts,Arts,Education and Management Engineering(SAEM E 2017)[C].Wuhan Zhicheng Times Cultural Developme nt Co., Ltd:,2017:5.

[5] 秦波,陈李昌豪,伍前红,张一锋,钟林,郑海彬.比特币与法定数字货币[J].密码学报,2017,4(02):176-186.

[6] SWAN M. Blockchain: blueprint for a new economy [M].USA: O'Reilly Media Inc,2015.

[7] 蔡维德,郁莲,王荣,刘娜,邓恩艳.基于区块链的应用系统开发方法研究[J].软件学报,2017,28(06):1474-1487.

[8] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494.

[9] 钱卫宁,邵奇峰,朱燕超,金澈清,周傲英.区块链与可信数据管理:问题与方法[J].软件学报,2018,29(01):150-159.

[10] 杨德昌,赵肖余,徐梓潇,李勇,李强.区块链在能源互联网中应用现状分析和前景展望[J].中国电机工程学报,2017,37(13):3664-3671.

[11] 黄秋波,安庆文,苏厚勤.一种改进 PBFT 算法作为以太坊共识机制的研究与实现[J].计算机应用与软件,2017,34(10):288-293+297.

[12] 刘肖飞.基于动态授权的拜占庭容错共识算法的区块链性能改进研究[D].浙江大学,2017.

[13] 安瑞,何德彪,张韵茹,李莉.基于区块链技术的防伪系统的设计与实现[J].密码学报,2017,4(02):199-208.

[14] 刘庆云,沙泓州,李世明,杨嵘. 一种基于量化用户和服务的大规模网络访问控制方法[J]. 计算机学报,2014,37(05):1195-1205. [2017-10-10].

[15] 田海博,何杰杰,付利青.基于公开区块链的隐私保护公平合同签署协议[J].密码学报,2017,4(02):187-198.