文章编号：2096-1472(2020)-09-56-03
DOI:10.19644/j.cnki.issn2096-1472.2020.09.016

基于区块链的电子病历存证系统设计与实现

韦智勇[1]，周立广[2]

(1.南宁职业技术学院财经学院，广西 南宁 530008；
2.南宁市第二人民医院五象医院，广西 南宁 530219)
✉122570724@qq.com; 1960480023@qq.com

摘 要：目前许多医院使用电子信息系统进行医疗管理，数据存储一般都以中心化的方式进行，这种方式存在数据安全的隐患。本文研究在原有系统的基础上用区块链技术进行改进，使新的电子病历系统能防止信息泄露或篡改，同时可实现数据的共享，系统服务端开发主要使用Go语言，同时使用加密方法对电子病历存证数据进行加密，从而解决系统的安全性和共享性。

关键词：区块链技术；存证系统；信息安全；数据共享
中图分类号：TP311.5 **文献标识码**：A

Design and Implementation of Electronic Medical Record System based on Blockchain

WEI Zhiyong[1], ZHOU Liguang[2]

(1.*School of Finance and Economics*, *Nanning College for Vocational Technology*, *Nanning* 530008, *China*;
2.*Wuxiang Hospital of Nanning Second Peoples Hospital*, *Nanning* 530219, *China*)
✉122570724@qq.com; 1960480023@qq.com

Abstract: Hospitals using electronic information systems for medical management with data recorded in a centralized way, risk with data security problems. This paper aims to improve the hospital information systems with blockchain technology, so to prevent medical information from leakage and being tampered with, and to realize data sharing at the same time. This new system server is developed with Go programming language and the electronic medical record data is encrypted, which ensures the security and sharing of this system.

Keywords: blockchain technology; record system; information security; data sharing

1 引言(Introduction)

病人的医疗存证作为一种数据资产，电子病历存证系统的出现给医疗患者带来很大便利，同时也给医疗领域的研究人员研究各种病例提供了极大的帮助，病人的医疗存证属于个人私有数据，医疗数据安全是受到法律保护的，其他机构获得数据必须获得个人授权允许。在现有的电子病历存证系统采用中心化的数据存储模式，病人的医疗存证往往由不同的医疗机构来存储控制，导致存在数据隐私泄漏等安全问题。同时，病人无法有效管控本人的医疗数据，对数据无法进行权限设置和访问控制，传统的由医疗机构进行中心化数据存储模式已经不适合作为存储病人医疗记录的最佳方式。

近年来，随着云计算技术的发展，电子病历存证系统也逐步迁移到云端，Zhang等[1]首先提出了保障云环境下医疗数据安全的方案。Yang等[2]利用基于属性的加密技术来保护云中的数据。但是，基于云端存储的方案依赖于云服务提供商，在数据存储方式上还是属于传统中心存储模式的改进，医疗记录数据的隐私与安全保护上仍然存在很大隐患。

区块链概念是由中本聪在比特币中提出的一种数字货币加密存储技术[3]，它独特的去中心化数据存储方式，以及数据抗篡改性和非对称加密的等特点。区块链的智能合约发展在医疗行业的应用已得到关注[4]。

2 相关技术(Related technology)

2.1 区块链技术

区块链是由一系列区块组成的数据集合，区块与区块之间形成数据相互关联并形成逻辑上的链式结构，区块由事务发起方通过广播方式发送到所有节点，在区块链中有51%节点达成共识确认后，将新生成的有效地区块加入区块链，每个区块都有一个Timestamp和前一个区块的Hash，当修改了一个区块的数据之后，它后面所有的区块Hash值都不能通过校验，可以防止篡改区块链中的数据，形成一种存储在对等网络节点间共同维护且不能被篡改的分布式账本数据库，因为区块链中每个节点都保留了相同的交易记录，所有对单个节点的攻击不影响数

据的安全性[5]，对数据的攻击具有很强的鲁棒性。

2.2 Fabric技术

Fabric是由linux基金会主办的区块链项目，是区块链的基础核心平台，其主要提供区块链成员服务、构建分布式账本、链码服务和事务流服务等区块链的基础服务。在Fabric中，每一个运行的区块链网络中的节点都是平等的，主要由Peer节点、Order节点和Client节点组成，peer节点，同时每个节点有着不同的作用，Peer节点主要是验证交易并进行签名，Order节点主要是接收交易信息，并将其排序后打包成区块，Client节点主要是将终端用户的请求发送到区块链中。

2.3 共识机制

对于一个系统而言，如果设有一个统一的决策层，会造成共享识性差，造成系统的效率低下，采用区块链技术的系统，不仅可以达成高效共享，而且可以提高系统的效率，同时也提高系统的容错性，同时也保证了数据的安全性和有效性。典型的算法有POW、POS和PBFT算法。例如POW算法，主要通过各节点的算力达成数据的共识，而POS在POW的基础上进行必要的改进，用权益证明取代了工作量证明，这种机制可节约成本。PBFT算法仅需要系统出现错误时才达成共识，一般情况下不需要各节点达成共识。

2.4 存储结构

在区块链存储中一般包含几个数据存储单元，主要有区块数据、链式结构、时间戳等，区块数据一般分成区块体和区块头，区块头主要包含有前一块头的地址和版本信息，区块体包括交易的数据信息；链式结构主要根据区块的生成顺序生成一条数据链，每个结点包括数据信息，这些信息可用于追溯来源。时间戳主要记录了数据的存储时间，它具有区块数据的存在证明，确保了数据的真实有效性。

3 系统设计分析(System design analysis)

3.1 系统需求分析

目前，病人的医疗存证往往由不同的医疗机构来存储控制，电子病历存证系统在应用过程中还存在诸多问题：(1)病人的医疗记录存证数据是分散的在不同的医疗机构中，对数据的管理和共享造成困难；(2)传统的由医疗机构进行中心化数据存储模式，病人无法有效管控本人的医疗数据，对数据无法进行权限设置和访问控制；(3)对病人医疗记录存证数据隐私与安全保护不够重视。为解决这些问题，本文提出了基于区块链的电子病历存证系统，在系统中主要有管理员、病人和医疗机构等三种类型用户，主要功能如图1所示，病人只能管控本人的数据，医疗机构用户可以获取某类病人病症的医疗信息。

根据传统的电子病历系统所存在的问题，结合新系统的构建设想，本系统功能需要分为三大模块，即前置客户端模块、系统管理模块和后台数据存储模块。前置客户端模块主要是就诊病人或医务人员使用本系统时，必须通过帐号进行登录使用，对于医务人员而言，可对患者的电子病历进行建档，并对其进行就诊信息录入、修改和查阅等，对于患者而言，可以查询到就诊的信息、检查结果、就诊进度、费用等信息。系统管理模块主要是对系统的使用者进行权限管理，为用户分配密钥，对数据进行加密和解密等，后台数据存储模块主要是对产生的数据通过相应的算法加密后进行后台的存储，确保数据在存储后不能被修改和窃取，以保证数据的安全性，从而保证了患者的个人隐私得到保密。

另外，对于系统的非功能需求，主要包括系统的可操作性和兼容性，主要是在确保数据信息安全的基础上，操作应该简单明了，可通过人机对话窗口和提示窗口进行操作，同时，系统在各种环境下均可以运行，不能局限于某个版本的操作系统，此外，系统的各个功能模块都有相对独立性，不能因某个功能缺失影响到别的系统的正常使用，系统功也要易于扩展。

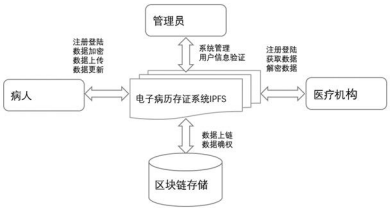

图1 系统基本流程

Fig.1 Basic process of the system

3.2 系统架构设计

基于区块链的电子病历存证系统主要由病人、医疗机构、区块链集群、IPFS集群和加密技术模块组成，通过区块链技术和IPFS分布式存储系统实现病人医疗记录存证数据的去中心化存储，使用加密技术实现对数据的细粒度访问控制，实现病人控制个人自身医疗记录存证数据，并设置加密访问策略，只有符合访问策略的医疗机构才能够用密匙来解密病人的医疗记录存证数据，如图2所示。

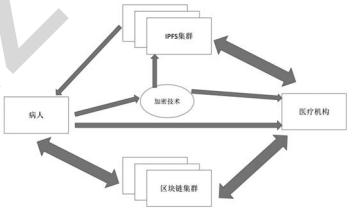

图2 系统核心架构

Fig.2 System core architecture diagram

本系统设计主体框架为B/S模式，把医疗行业的业务基础上，把系统设计为三层架构，即客户端、服务端和数据库端三层。

(1)客户端。客户端主要是用户通过浏览器进行系统操作和信息查询，客户端功能又称为展示层，该功能主要用Java语言开发，这样可提高系统的性能和效率，同时可以使系统达到负载均衡的效果，提高系统的稳定性。

(2)服务端。服务端主要是根据用户的请求进行后台数据服务，该功能采用Web应用框架，使用python语言编写程序代码，这样可提高系统的兼容性和扩展性，对第三方的插件提供可靠的接口。另外，服务端框架分为三层，即模型、模板和视图。

(3)数据库端。数据库端主要是把用户和系统的数据存储在后台数据库中，该功能主要使用MYSQL数据库的管理病患者的个人信息，为系统的数据存储提供了高效、安全的环境。区块链数据的存储使用CouchDB存储超级帐本Hyperledger Fabric状态数据信息，超级帐本设计采用拜占庭容错算法，确保所有节点数据的一致性。

3.3 系统功能模块

基于区块链的电子病历系统功能模块一般分成用户模块、数据存储模块、病例查询模块三大功能。

(1)用户模块。主要为医生提供系统帐户，使医生能正常登录并使用电子病历系统，进行患者病历书写，同时修改个人密码，创建患者帐户等功能。数据一般都通过DES算法进行加密

后，再存储到数据库中。

(2)数据存储模块。主要是医生为患者建立病历档案，录入患者就诊数据信息，提高后台进行数据存储，在这些数据中，医生个人信息、患者公钥信息具有数据量大、冗余性高、操作次数较多等特点，这些数据仅储存在传统数据库系统即可，这样可提高系统的效率。对于患者的个人隐私信息则必须通过区块链存储功能来进行数据存储，因为这些数据存储次数较少，但要求较高的安全性，同时，这些数据在存储前必须进行对称加密操作。

(3)病例查询。主要是为患者提供自助服务功能，同时也为医生就诊提供方便。患者就诊时，可以通过个人身份证或就诊卡，查看自己的就诊信息，可打印出来拿给医生作参考，同样对于医生而言，也可在系统中查看到患者的数据信息，为患者下一步的诊疗方案作参考。

4 系统的实现(Implementation of the system)

4.1 系统的运行环境

本系统的运行环境是使用Linux Ubuntu操作系统，并使用Docker容器，版本选择17.06，数据库使用CouchDB，开发语言选择Go和JAVA，Hyperledger Fabric选择V1.1版本，IPFS选择V0.4版本，并配置NodeJs等环境。

4.2 系统的功能实现

4.2.1 合约设计

合约设计采用先进行系统开发，然后再进行部署，因为合约之前必须使用节点许可后才能进入到部署环节，即必须获得相应的权限后才能部署到区块链系统中[6]。为了加快开发进度，本文使用Go语言作为合约设计的开发语言。

4.2.2 加密功能实现

为了保护电子存证病历数据的安全性，必须对数据进行加密处理，在数据上传前通过加密算法加密技术对数据加密。在为患者建档时，系统会自动分配一把密钥给该用户，对用户的文件通过该密钥进行数据加密，当用户访问该数据时必须通过该密钥进行解密，如果解密无效则无法访问该用户电子病历数据。由于区块链存储容量比较小，所以使用IPFS来扩充存储系统的容量，病患者将电子存证病历加密后将密文上传到IPFS系统中，系统会返回一个Hash地址。

4.2.3 数据存储功能实现

数据存储主要包括两个部分，即IPFS数据存储和区块链数据存储，一般用户信息主要通过IPFS分布式的存储模式进行数据存储，主要把患者数据加密后，系统会返回一个加密后的地址，通过这个地址可访问到加密后的数据，这种方式可提高存储效率，降低运行成本；对于区块链的存储功能实现，主要是根据用户注册时的地址，找到该用户对应的数据存在地址，系统先通过用户ID找到该用户的地址，然后可猎取用户的数据存储地址，找出该地址后可对数据进行更新，即可实现数据存储。

4.2.4 数据库设计

基于区块链的电子病历存证系统后台使用MYSQL数据库和区块链状态存储数据库CouchDB，CouchDB主要存储历史数据、区块链索引数据和当前数据状态。MYSQL该数据库系统具有占用空间小、运行快、存储效率高等特点，数据库中，主要通过用户ID索引数据，同时也作为主键进行数据检索，通过检索判断用户是否存在，若存在，系统会返回1，否则返回0，此外，使用Navicat作为管理的开发工具，这样可以降低系统的管理成本，数据库系统中的数据表主要包括用户信息表、患者密钥表、医院部门表、医务人员表、药品项目表、检查项目表、就诊信息表等。

4.2.5 系统测试

系统开发完成后，必须进行系统的测试，主要目的是检测系统的功能是否满足用户的需求，同时检测系统在运行过程中存在的错误和缺陷，这样可为后续的维护提供依据，使系统不断的加以完善，提高系统质量和效率[7]。系统测试主要分两种方式，即静态和动态，静态测试方式一般通过源程序代码进行分析结果判断是否存在错误，无须运行该系统，而动态测试方式必须通过运行该系统，从中发现存在的错误，在目前实际运用中，一般采用动态测试方式进行，动态测试又分两种方式，即白盒与黑盒两种，如果在墨盒测试中发现问题，说明程序代码有错误，必须再进行白盒测试。

本系统通过电脑中运行客户端，进行各功能测试，运行环境是Windows 10操作平台，测试分单元功能测试和系统整体测试两个阶段进行，通过单元功能测试发现功能都能达到预期效果，而且操作简单快捷；在系统整体测试，在医生操作界面是都查看到患者的个人信息和就诊信息，界面交互友好，统计数据无差错，整个系统的测试没有发现明显的错误，存在的一些漏洞也已修复，系统运行处于正常状态。

5 结论(Conclusion)

区块链技术具有分布式存储、防止篡改、中心化的特点，基于这些特征，本文把区块链技术融入电子病历系统中，不仅提高的系统的效率，还提高了系统数据的安全性，同时解决了数据的共享性问题，此外，利用区块链技术还可防止数据不被篡改；通过运用对称加密算法把系统的数据进行加密操作，防止了数据的外泄和盗取；在数据存储方面，对于患者的个人信息采用IPFS技术进行分布式存储，对于就诊信息，则采用区块链技术进行存储，由于在患者的就诊信息中，不包括患者个人信息，所有既可对外提供数据共享，又保护了患者的个人隐私，同时也提高了整个系统的工作效率。

参考文献(References)

[1] ZHANG Y, QIU M, TSAI C, et al. Health-CPS: Healthcare Cyber Physical System Assisted by Cloud and Big Data[J]. IEEE SystemsJournal, 2017, 11(1): 88-95.

[2] YANG K, ZHANG K, JIA X, et al. Privacy-preserving attribute-keyword based data publish-subscribe service on cloud platforms[J]. Information Sciences, 2017: 116-131.

[3] NAKAMOTO S. Bitcoin:A peer-to-peer electronic cash system[J]. Consulted, 2009 ,75(8): 1042-1048.

[4] 欧阳丽炜,王帅,袁勇,等.智能合约:架构及进展[J].自动化学报,2019,45(03): 445-457.

[5] 张亮,刘百祥,张如意,等.区块链技术综述[J].计算机工程,2019,45(05):1-12.

[6] 胡逸阳.基于区块链的共享电子病历系统设计与实现[D].浙江工商大学,2019.

[7] 张圣垚.基于区块链的电子病历系统的设计与实现[D].哈尔滨工业大学,2019.

作者简介：

韦智勇(1983-)，男，硕士，信息系统项目管理师.研究领域：区块链应用，大数据技术.

周立广(1974-)，男，硕士，高级工程师.研究领域：云计算，大数据分析.