基于区块链和 IPFS 技术的医疗档案管理系统的研究

李哲

（湖北商贸学院　湖北省武汉洪山区　430079）

摘要:本文研究了区块链技术、IPFS 星际云存储技术在医疗档案系统中的应用。首先分析了传统医疗档案的不足和用户的期待的改进需求，包括传统医疗档案中患者的隐私保护缺失、档案数据的安全性低下、档案共享的不便性等。讨论了区块链技术和 IPFS 技术在医疗档案管理中的研究现状和市场应用。介绍了区块链技术和 IPFS 技术的基本原理和特点，分析了它们用于医疗档案系统的作用和优势。基于以上提出了基于区块链和 IPFS 技术的医疗档案管理系统的设计与实现，它详细分析了系统架构和智能合约设计，并通过实验设计来验证区块链技术存储的有效性和 IPFS 系统存储相对于传统存储的优势。实验结果显示，基于区块链和 IPFS 技术的病历管理系统具有更高的安全性、可靠性、便捷性。

关键词：〈医疗档案管理〉;〈区块链技术〉;〈IPFS 技术〉;

中图分类号：T　　文献标识码：J

Abstract: This paper investigates the application of blockchain technology, IPFS star cloud storage technology in medical file system. The study first analyses the shortcomings of traditional medical records and the improvement needs expected by users, including the lack of privacy protection of patients in traditional medical records, the low security of record data, and the inconvenience of record sharing. The research status and market application of blockchain technology and IPFS technology in medical records management are discussed. The basic principles and characteristics of blockchain technology and IPFS technology are introduced, and their roles and advantages for medical file system are analysed. Based on the above, the design and implementation of a medical file management system based on blockchain and IPFS technologies is proposed, which analyses the system architecture and smart contract design in detail, and verifies the effectiveness of blockchain technology storage and the advantages of IPFS system storage over traditional storage through experimental design. The experimental results show that the medical record management system based on blockchain and IPFS technology has higher security, reliability, and convenience.

Keywords: 〈medical record management system〉, 〈blockchain technology〉, 〈IPFS technology〉

0　引言

传统的医疗档案一般使用文件的方式存储在医院等医疗机构的个人电脑上。这些档案既没有进行加密来保护患者的隐私，也容易出现病毒感染、计算机宕机导致档案丢失的情况，患者的医疗数据得不到较好的保存。另一方面，患者在一个医院的诊疗记录不能在多个医疗机构之间实现方便的共享。这样患者在不同的医院看病就需要医生进行重新诊断和建立档案，不仅提高了患者的治疗成本，而且消耗了更多的医疗资源。研究机构和医学学者在调用患者的医疗档案进行研究和讨论的时候，由于档案不能在医院之间共享，这些资料的调用就会变得极不方便。同一个患者在不同的医院有多个医疗诊断档案，使得数据的冗余性增大，而且不同的医生诊断的结果也有可能不一样。如果同一个患者的档案能在不同的医疗机构之间共享，那么下一个医生诊断疾病会考虑上一个医生诊断的结果，减少了疾病的误诊率。

区块链是一种分布式的存储网络，而联盟链对于新用户的加入会进行严格的证书的验证和身份检验，确保安全的用户才能接入联盟链中。新的区块加入区块链需要大多数节点进行验证才能添加到链上，保护了数据的安全性，区块链上的数据是永远存在的不会丢失。所有的区块链网络节点可以看到每一个交易和更新，使其对于用户具有很高的透明度。我们在区块链上部署智能合约可以在满足条件的情况下自动完成功能和交易，实现了系统的自动化，提高了系统的效率。IPFS 技术使用云存储的方式减轻了本地存储的负担，是一个网络的分布式存储系统。它把数据分块和分散到多个服务器上进行存储，而且进行了数据的备份和复制，这使得它比一般的数据存储要可靠很多。IPFS 技术可以自动从多个服务器中选择一个最近的服务器或者从多个下载路线中选择一个网络状况最好的服务器进行下载。这就意味着它具有较快的下载速度，并且能够处理较大的负载流量。这非常适合应用于庞大的医疗数据的存储、传输和共享。

针对以上这些传统医疗档案系统的不足，利用区块链和 IPFS 技术的优势，本文将提出包括整体架构、设计合约设计及实现在内的基于区块链和 IPFS 技术的医疗档

案管理系统设计和实现方案。通过本文的研究，将为医疗档案管理系统的改进和优化提供一种创新的解决方案，从而提高医疗档案的安全性、隐秘性和共享便捷性，为医疗信息化建设提供有力支撑。

第一章 医疗档案管理系统的现状与问题

1.1 传统医疗档案管理系统的局限性

传统的医疗档案管理系统在保护隐私和数据安全方面存在一些局限性，这些问题严重影响了医疗档案的可靠性和完整性。

1.1.1 隐私保护不足的问题

在传统医疗档案管理系统中，患者的个人隐私往往无法得到充分保护。病人担心个人隐私外泄的风险是因为医疗数据的敏感性和私密性。医院和其他相关机构也面临着难以确保患者隐私安全的挑战。现行医疗档案管理制度缺乏有效的隐私保护机制容易造成非法获取、篡改或滥用患者信息的情况发生。

1.1.2 档案数据易于篡改的风险

传统医疗档案管理系统中存在着档案数据易于篡改的风险。由于传统系统中的数据存储和访问机制相对集中，一旦恶意攻击者入侵系统或内部人员进行数据篡改，档案数据的完整性将受到严重破坏。由于缺乏有效的数据溯源机制，很难追溯和发现数据篡改行为，导致档案数据的可信度降低。

1.2 医疗档案管理中区块链技术的应用前景

区块链技术为解决传统医疗档案管理系统所面临的问题提供了新的解决方案作为一种分布式、去中心化的数据存储和管理技术技术具有诸多优势。

1.2.1 区块链技术的特点及优势

区块链技术采用去中心化的存储方式以及多节点确认的工作模式保证了存放数据的可靠性。去中心化地减少了传统中心网络存储系统面临的单点故障和数据篡改的风险，这有利于降低区块链系统的维护成本和使用成本。一方面确保了区块链数据对于用户是透明的共享的，另一方面使得存放的数据在整个系统没有完全崩溃的情况下仍然能被获得。这就要比一般的存储方式可靠很多。区块链技术通过利用多重加密手段和电子签名技术来封装患者的档案，实现对患者隐私的深层保护。使用不同的加密算法可以实现不同的保密效果，而多重加密使得恶意用户想要窃取患者隐私变得很困难，极大的增强了对外界恶意用户的防御效果。根据用户需求，通过在区块链上部署不同的智能合约，我们可以实现不同的用户功能，自动完成交易和存储。这使得区块链的功能从原本的单一功能获得了极大的扩展空间。厂商和用户可以自定义智能合约的功能，满足市场需求的智能合约产品能够广泛应用于商业领域。

1.2.2 医疗档案管理问题的可行性分析区块链技术的解决方法

在医疗存档管理系统的实践中，区块链技术的应用显示出了高度的可行性。利用区块链技术，医疗档案的去集中存储和管理能力能够提升数据的共享与存储效率。利用加密策略和签名验证，以及智能合约策略，能够保证医疗档案信息的必要的隐秘性和较高的安全性。区块链技术的本质是一种网络技术，它将不同的用户连接起来，实现了用户数据的便捷共享。

第二章 系统的技术介绍

2.1 IPFS 技术的基本原理和特点

IPFS(InterplanetaryFileSystem)是一种具有去中心化、高效可靠、数据完整性验证等特点的分布式文件存储和传输协议。

2.1.1 分布式存储与访问机制

IPFS 实施了分布式的存储与访问策略，把文件拆分成若干数据模块，并采用哈希方法对每一数据模块实施唯一的识别。为了实现分布式文件存储，这些数据块可被存储在各种节点之间。借助于内容寻址以及数据路径技术，IPFS 技术能够达到对文件的高效访问和传送。

2.1.2 数据完整性验证与去重机制

IPFS 技术会使用不用的数据检验算法来计算每一个数据的检验值，常见的数据检验算法有 MD5 算法、base64 算法等，并把数据的校验值作为该数据的标记。一旦数据感染病毒或者发生了变化，计算出来的检验值就和原来的检验值不一样，实现了数据的完整性验证。IPFS 存储还会自动去除存储服务器中相同的数据来减少数据的冗余性，提高整个系统的存储利用率。

2.2IPFS 技术在医学档案管理中的作用与优势

IPFS 技术除了以上优势，还具有智能目录功能。这样可以方便的在一个单独的文件中存储和管理多个文件或目录。这对于庞大医疗档案的维护是极其便捷的，降低了档案维护人员的维护成本和难度。作为分布式文件存储与传输协议的 IPFS 技术，在医疗资料档案管理方面具有巨大的应用潜力。它能够让医学档案去中心化地存储和共享，从而增强数据的可获取性和分享的效率。IPFS 不仅可以加强医疗记录在传输和存储时的保障，还可以增强对个人隐私的保护力，确保信息的完整性和安全性。

第三章医疗档案管理系统的设计与实现方案

3.1 整体架构设计

我们根据用户的功能需求设计了整个系统的大致框架，分析和整理了项目系统的功能和结构。系统包括了以下几个功能：医患档案功能、区块链网络功能、IPFS

星际云存储功能、本地存储功能，这些基本完成了医疗档案的加密、共享、存储、隐私保护等要求。系统整体结构和框架如下图 1 所示。

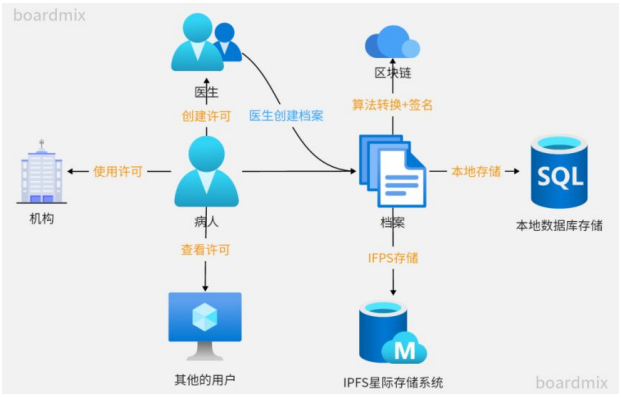

图 1　医疗档案系统整体结构图

3.1.1 IPFS 星际云存储的数据存储与管理模块

该模块负责通过 IPFS 技术将医疗档案资料分割成数据块分散存储和管理。我们搭建 IPFS 接入环境，并使用 python 来接入 IPFS 存储系统，把需要存储的数据存储到 IPFS 系统中。IPFS 系统和浏览器相结合的特点，用户可以通过可读的链接访问 IPFS/IPNS 内容，这就不需要专门 APP 程序来获取数据。用户可以在多个不同的平台和系统上获得存储的数据，实现了数据存取的跨平台特性。而且，IPFS 文件可以变成特殊的 IPFS 目录，这样就可以通过文件的目录索引来快速的找到存放的文件。

3.1.2 医患档案功能模块

在系统的医患功能设计部分，我们把医院和医生自己专属的签名和存取钥匙建立在这个体系结构里。医院和医生根据密钥和签名来访问患者的电子医疗档案。而没有密钥和签名的用户就不能访问该患者的档案。患者的档案也会通过非对称 AES 加密算法进行加密，确保档案在没有经过本人的密钥解密就不能被查看，患者拥有对档案的隐私。医生需要自己的签名和密钥以及病人的签名和密钥才能进行创建患者档案、更新患者档案、删除患者档案的操作，保证了档案的完整性和安全性。研究机构和医疗机构需要得到病人档案的解密密钥才能获得档案的内容用于查看和研究。

3.1.3 区块链网络功能模块

在区块链网络功能部分，通过区块链技术可以有效防止病人档案被随意涂改。区块链存储了患者、医生、医疗机构的各种信息用于验证。只有经过了验证的用户才能够通过区块链网络使用查看、更新、删除等功能。而且存放在区块链上的用户信息是不可能被外界所攻击的，保证了该系统的用户信息的安全性。

3.1.4 本地的数据库存储功能模块

在本地的数据库存储部分，该系统使用了 mysql 和 redis 数据库技术来存储和备份数据。我们把待存储的数据一份保存在 mysql 数据库中，另一份数据副本备份在离线的服务器数据库中，数据库记录了各个用户的信息和档案本身。实验条件有限，我们仅使用了两台普通的 PC 服务器来进行实验。在实际的应用中，使用 RAIDS 磁盘阵列存储技术能够更好的加强数据存储的安全性能，加快数据库存储的速度，增大数据库存储的吞吐量。在数据存储的方面确保数据存储的可行性、便捷性和安全性。

3.2 智能合约设计及实现

3.2.1 合约的功能需求分析

智能合约是一种利用区块链技术能够自动在医疗档案管理系统中提供多种功能需求的合约形式。针对医疗档案管理的真实需求，我们可以构建如下功能要求：数据访问的权限监管、定义数据分享的规则、进行数据变更审核和数据检索等。

3.2.2 合约的设计与实现细节

为了满足上述的功能需求，我们可以开发并创建相应的智慧型合同。合同应确保明确各个用户访问医疗记录数据的权限，并详细记录这些访问的时间以及运行日志。合约应该明确规定数据共享的准则，以便特定医疗记录资料可以在各个医院、医生以及患者之间进行有效的共享。合同还必须包含一个数据更改审计功能，负责记录和验证医疗档案数据的更改情况。合约需要提供数据查询接口，方便用户查询和获取医疗档案数据。智能合约部分代码如下图 2 所示:

智能合约使用了 solidity 语言来进行编程，版本是 0.8.18.编译器采用 remix-ide，并部署在 ganache 区块链模拟器上，设置区块链的 id 号为 5777，接入端口为 8545，gas 价格是 100w WEI，每个用户拥有 100 枚虚拟币用于实验。具体实验步骤如下：

我们使用 RSA 算法生成两组加密和解密的密钥，并使用 python 接入该区块链进行实验。

我们从 remix-ide 中获得智能合约的 abi 结构和 bytecode 代码，将智能合约部署在区块链的 block 1 上。

创建测试的患者档案之后，使用 RSA 加密并在区块链上进行签名交易，将档案信息记录在区块链上。

调用智能合约下载档案并验证档案的签名和真伪。如果得到的档案是假档案，那么就在区块链系统中查不到该档案。如果档案是真档案，那么就可以查到档案的交易签名和交易散列。

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.18;
contract HelloWorld {
    uint CODE_SUCCESS = 1;
    uint CODE_SUCCESS_USE = 15;
    uint DATA_FAIL= 10;
    //创建用户的结构体变量
        struct USE{
        string username;
        bytes user_h;
        string pwd;
        string usersign;
    }
    mapping(bytes => USE) userap;

    //创建数据部分的结构体变量
    struct Data{
        string fileData;    //文件 JSON
        bytes fileHash;//文件 HASH
        string uuid;
        string userAddress;
        string userSign;/*  */
    }
    mapping(bytes => Data) datamap;
    mapping(bytes => tranData) stores_data;
```

```
//使用function完成档案的创建功能
 function upload(string calldata fileData ,bytes
    Data storage data = datamap[fileHash];
       if(data.fileHash.length != 0){
        return DATA_FAIL;
    }
    data.fileHash = fileHash;
    data.fileData = fileData;
    data.uuid = uuid;
    data.userAddress = userAddress;
    data.userSign= userSign;
    return CODE_SUCCESS;}
//使用function完成档案的下载和查看功能
function download(bytes calldata fileHash) public
      Data storage data = datamap[fileHash];
      return(data.fileData,data.fileHash,data.uui
    }
//把创建档案的交易记录在区块中
function tran_upload(string calldata tranHash ,by
        tranData storage trandata = stores_data[f
        trandata.fileHash = fileHash;
        trandata.tranHash = tranHash;
        return CODE_SUCCESS;
}
//下载和查看区块中的交易
```

图 2　智能合约的设计代码

实验结果图 3 所示，通过区块链存储的档案可以验证它的签名和真伪，智能合约完成了医疗链系统的基本功能。在合约部署的区块上查到了档案的名称、具体内容、档案创建的交易记录、档案加密之后的散列值。

图 3　区块链和智能合约的实验结果图

通过区块链与IPFS的技术手段搭建的医疗档案管理系统，结合前面提到的总体构架和智能合约的搭建与执行，有潜力使医疗档案数据实现去中心化的存储和共享，并同时提供了有效且稳定的数据接入及权限控制手段。采取这种措施将极大提升医疗档案的保护、可靠及追溯能力，从而为医疗数字化建设提供更为坚实的支撑。

第四章 讨论和总结

本文了解传统医疗档案管理系统中存在的难题，并研究区块链与 IPFS 在医疗档案管理中的潜在应用。通过分布式的数据存储与管理模块实现医疗档案数据的去中心化存储和共享，并提供高效可靠的数据访问、数据检验、数据共享功能。运用加密算法和电子签名技术，实现了用户隐私的高效保护。智能合约的设计与部署满足了医疗档案管理系统面向市场和商业的各种功能需求，展示了其强大的实用性。基于区块链和 IPFS 技术的医疗档案管理系统具备着非常广泛的应用潜力。

参考文献：

[1] 胡雪峰，范佳佳. 基于区块链和 IPFS 的医疗档案管理系统研究[J]. 中国电信学报, 2019, 26(2):124−130.

[2] 陆琦，陈晓红. 基于区块链技术的医疗档案安全存储研究[J]. 计算机应用与软件, 2020, 37(3):180−184.

[3] 田艳红，马明亮，刘颖. 基于 IPFS 的医疗档案分布式存储研究与实现[J]. 现代电子技术，2018, 41(18):191−194.

[4] 温宇达，陈军. 基于区块链和 IPFS 的隐私保护医疗档案管理系统设计与实现[J]. 电子技术与软件工程, 2021, 38(4):101−108.

[5] 周秋华，李霞，蔡国栋. 基于区块链与 IPFS 的医疗档案安全共享系统研究[J]. 计算机工程与应用，2019, 55(8):184−190.

作者简介：李哲（1991.10.24—），性别男，籍贯湖北，硕士，工程师，研究方向：区块链人工智能。