Journal of Computer Applications 计算机应用 | ISSN 1001-9081 CODEN JYIIDU | 2019-01-17 http://www.joca.cn

文章编号:1001-9081(****)**-0000-00 doi:10.11772/j.issn.1001-9081.2018102241

基于区块链网络的医疗记录安全储存访问方案

徐健[1,2*]，陈志德[1,2]，龚平[1]，王可可[1,2]

(1.福建师范大学 数学与信息学院，福州 350007； 2.福建省网络安全与密码技术重点实验室(福建师范大学)，福州 350007)

(*通信作者电子邮箱 zhidechen@fjnu.edu.cn)

摘 要: 针对在当前医疗系统中，医疗记录授权流程繁琐、记录分享效率低下和身份验证困难问题，提出一种结合区块链技术与密码学的非对称加密技术的方法，将非对称加密技术的安全性高、多方协作简单等特性应用到区块链技术构成的点对点网络中，使得医疗记录跨域分享可追踪、数据不可篡改和身份验证简化。首先，基于区块链技术的不可篡改性结合非对称加密技术，设计了文件同步合约和授权合约，其分布式储存优势保证了用户医疗信息隐私。其次，跨域获取合约的设计能够有效验证数据分享双方身份与传输效率，使得不需要第三方公证机构便可安全过滤非合法用户。仿真实验结果显示，本文提出的方案相比传统使用云计算方法解决医疗记录分享问题，在数据防盗窃、多方身份验证和节约系统开销方面有明显优势。对于利用区块链的去中心化可审计等优点解决数据分享过程中的安全问题提供参考，为解决数据跨域分享、跨域身份验证问题上提供借鉴思路。

关键词: 区块链；医疗记录；去中心化；隐私保护；智能合约

中图分类号:TP399 **文献标志码：A**

Security medical record storage and access scheme based on blockchain

XU Jian[1,2*], CHEN Zhide[1,2], Gong Ping[1], WANG Keke[1,2]

(*1.College of Mathematics and Informatics, Fujian Normal University, Fuzhou Fujian 350007, China;*

2.Fujian Provincial Key Laboratory of Network Security and Cryptology (Fujian Normal University), Fuzhou Fujian 350007, China)

Abstract: To solve the problem of the cumbersome process in medical record authorization, the low efficiency in record sharing and the difficulty in identity verification. An asymmetric encryption technology method combining blockchain technology are proposed to makes medical records cross-domain sharing traceable, anti-tamper of data and identity verification simplified. Based on the irreparable modification and traceability of blockchain technology combined with asymmetric encryption technology, the file synchronization contract and authorization contract are designed, features such as decentralized and distributed storage advantages secure the privacy of user's medical information. The cross-domain acquisition contract which proposed blow can effectively verify the identity and transmission efficiency of the data sharing parties, so that without third-party notary agencies can be used to securely filter non-legitimate users. The experimental and analysis results show that the proposed method compared with the traditional use of cloud computing methods to solve medical record sharing problems has obvious advantages in data theft prevention, multi-party authentication and data access control. Methods mentioned above provides a good application demonstration for solving the security problems in the data sharing process across medical institutions and a reference for cross-domain identity verification in the process of sharing data used blockchain.

Keywords: Blockchain; electronic medical records; decentralization; privacy protection; smart contracts

0 引言

医疗记录信息，传统来说包括病人的基本资料、检查症状、医嘱信息、以及非文本检查信息（包括超声图像、核磁

收稿日期: 2018-11-08； 修回日期:2018-12-19； 录用日期: 2018-12-26。

基金项目:国家自然科学基金资助项目(61841701)、福建省自然科学基金资助项目(2016J01287，2018J01781)

作者简介: 徐健(1995—)，男，湖北荆州人，硕士研究生，主要研究方向：网络与信息安全；陈志德(1976—)，男，福建泉州人，教授，博士，主要研究方向：网络安全与密码学、分布式计算；龚平(1982—)，男，福建福州人，副教授，博士，主要研究方向：形式化建模与分析，业务过程管理与监控；王可可(1992—)，男，河南汝州人，硕士研究生，主要研究方向：网络与信息安全。

图像等），这些都是患者宝贵的生命体数据，不仅仅为当前医生对病情做出判断提供依据，还为其他医护人员对患者情况做出正确评估，理解历史治疗方案，进一步制定个性化治疗方案提供依据和参考[1]。在医生对患者的综合性复杂疾病及各种慢性疾病方面，一份可靠、安全、易访问的电子病历档案无疑在提高医疗文件搜索速度和对患者综合情况评估制定合理方案提供更好效果。

对于一个病人来说，在检查过程中一个病症可能伴随这多种特征，在医生诊断病症的时候，通常做法是询问病人一些历史病症、身体状况等。这样的做法有两个缺点:1) 很难保证病人能够精确记得历史病症的量化值，例如血压历史记录等。2) 病人在描述病症的时候往往夹杂非专业医学词语，这将影响医生对病人历史病症的理解。因此一份精准精确的医疗记录文件对一个医生来说无疑提供更加可靠的参考。

针对这个问题，传统的方案是在就医的机构保留一份医疗记录，当患者下次继续就医，就可以向医生查询相关的病例历史记录。然而，一旦病人在不同科室就医，需要从原来的科室医疗记录库或者医疗机构的数据库里调用这份医疗记录，这样的解决方案不仅效率十分低下，而且针对患者在不同的医疗机构或者不同的地域就医来说，这些解决方案就不可用。

为解决这个问题，随着云计算云存储等互联网技术的流行，不少学者把医疗数据的储存和管理放到云端执行，即在医院形成一份电子医疗记录文件(Electronic Medical Record，EMR)，由第三方云服务机构托管。这样的方案解决了不同机构就医，不同地区就医共享医疗记录的难题[2-5]。Berman F[6]提出了一种基于大规模相关性的数据库网络存储隐私信息和医疗记录信息，这些数据库之间通过主机与服务器之间的通信保证数据传输，但是在方案布置上具有较高成本，服务布置具有很高复杂度。Shen M[7]提出一种能够验证数据完整性与安全性的数据存储方案，该方案能够在下载数据之前及时发现数据是否被篡改。在医疗大数据储存方面，Cheng H[8]提出一种将大数据切成一些列有序数据列，然后在多种云储存服务器上放置这些数据，这样保证了数据的安全性。然而，一份完整的 EMR 文件通常包含患者的个人隐私信息，这样的一份 EMR 文件转交给第三方云服务机构管理保存，在隐私保护与安全性上没有保证。第三方云服务提供机构在云服务研究中通常被认为是半可信的，因为一旦云服务管理不当就会造成数据被篡改，泄露甚至丢失。因此，中心化结构的云服务器，在数据的隐私与安全性方面存在诸多问题。

目前，利用区块链技术解决这一难题的学者也有很多。Hao W [9]提出了一种结合了属性加密(attribute-based encryption, ABE)和身份加密(identity-based encryption, IBE)加密方案加密医疗数据，并且利用基于身份的签名(identity-based signature, IBS)来实现数字签名，方便系统的管理，而不需要引入不同的系统，使用区块链技术来确保完整性和医疗数据的可追溯性。但在此方案中，并未针对数据存储位置做出明显改变，依然存在云端，这将极大降低数据安全性。Xia Q[10]提出了一种基于区块链技术的医疗数据分享框架，这个方案设立了一些访问规则保证了储存在云端数据的安全性，为了实现数据的溯源性，该方案设置了一些智能合约去实现数据审计功能，这些智能合约能够帮助快速识别数据修改、数据删除等不利于保护数据完整性的行为，并且定位其地址。但是，此方案中数据的访问控制也是只针对云端数据，数据源头安全性并未解决。Hussein A F [11] 提出了基于离散小波变换与遗传算法技术优化访问队列，增强整体安全性。此外还加入了密钥生成器增强系统鲁棒性与访问控制，最后利用区块链记录访问日志。虽然在安全性上采用诸多技术加持，但频繁访问区块链将导致交易费用急增，系统耗费过大，在一般实用性上欠佳。Liu J [12]提出了一种基于区块链的EMR隐私保护数据共享方案(Based privacy-preserving data sharing, BPDS)，在 BPDS 中，原始 EMR 安全地存储在云中，索引保留在防篡改联盟区块链中。通过这种方式，可以大大降低医疗数据泄漏的风险，同时，区块链中的索引确保 EMR 不能被任意修改。但缺点也很明显，基于联盟链的区块链系统中，其半去中心化的特征使得操作数据权力容易集中，这也会导致数据泄露问题。

在本研究中，利用区块链技术的安全性与隐私性，能够很好解决上述问题。区块链技术能够分布式在各个计算机节点形成一个账本，并且这个账本是分布式的，并且不能够被修改。在 EMR 储存与管理领域中，把 EMR 数据的储存于管理放在区块链这个分布式帐本中，能够很好解决两个问题：1) 是数据储存安全问题，2) 数据跨域共享问题。尽管能够解决传统云计算对 EMR 文件储存于管理的关键问题，但是对于利用区块链这一分布式账本技术解决 EMR 文件储存与管理任然面临着几个问题：1) 面对昂贵的区块链数据交易费用，如何解决大文件储存的问题？2) 如何保证用户的 EMR 文件隐私不被泄露？3) 如何保证用户或医生查询 EMR 信息的方便快捷？

为解决这几个问题，本文提出了一个基于区块链技术的实时安全的医疗记录解决方案(Realtime-Security Medical Record，RSMR)。本方案在数据储存过程中利用一个星际文件系统(InterPlanetary File System, IPFS)[13]，该系统是一个面向全球的、点对点的分布式版本文件系统，该系统能够将所有具有相同文件系统的计算设备连接在一起，寻找文件时不需要验证发送者的身份，而只需要验证内容的哈希。在数据分享管理过程中，本文采用基于以太坊(Ethereum)[14]的智能合约(SmartContract)技术，该技术能够保证在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

总的来说，本研究贡献如下：

1) 提出一种基于区块链技术的电子医疗记录 ERM 存储与管理框架，该框架能够很好解决用户数据的隐私与安全问题。

2) 设计了一种基于 IPFS 数据储存与基于 Ethereum 的智能合约管理数据的数据安全分享方案。

3) 提出了一个基于 Ethereum 智能合约的多方协商方案。段。

1 系统模型

1.1 应用场景

传统的医疗记录解决方案在储存和实时查看医疗记录方面受限于授权和公务部门效率影响，例如：Patient 在某地的医院 Hospital_A 检查后，由于医疗设备限制不得不转院到 Hospital_B，在拿到自己的医疗记录过程中需要找医生签字盖章授权，由于我国较好医院就医人口常年处于饱和水平需要提前预约，拿到自己的医疗记录往往需要排队等候等等复杂过程。对于 Patient 来说，这将是极大的时间开销，病情严重甚至威胁到生命安全。另外，一旦 Patient 遗失这份纸质记录，在患者后续就医过程中无法提供完整的医疗记录，这样在跨域就医方面可无法提供可信记录。由于医疗技术日益发达，对患者评估需要多方面的检查，有时检查项目甚至超过 10 项，有效完整保存这份 EMR 至关重要。对于 Patient 的医疗记录 EMR 来说，EMR 中往往储存这患者的隐私信息，如何保证存放在医院数据库中的 EMR 信息不被不法分子获取。

为解决上述问题，本方案针对目前在医疗记录 EMR 领域的四大核心问题:1) 如何安全有效储存患者的 EMR，2) 如何实时上传 EMR，3) 如何设置访问控制过滤非法者。4) 如何方便跨域下载 EMR。设计了三个基于 Ethereum 的以太坊智能合约：文件同步合约、授权合约和跨域获取合约。

1.2 智能合约算法

1.2.1 文件同步合约

为保证上传到 RSMR 上的文件不被盗窃，本文中在加密层中用一种非对称加密算法 ECC[15]用于给患者的 EMR 加密。在本方案中，用户在医院注册会给患者本方案中患者需要保存的三个数字密码：一个是经过哈希算法 SHA-256 加密过后唯一 ID 以及用 ECC 算法加密的公私密钥对 PK (Public Key)、SK (Secret Key)，另外就是经过 IPNS 协议经过哈希加密后的医疗记录文件夹地址 FolderAddress。整个初始用户数据用公式(1) 表示

$$Patient\{ID, PK, SK, FolderAddress, Permission\} \quad (1)$$

患者经过哈希算法 SHA-256 加密过后唯一 ID 用于唯一识别患者身份，ECC 算法加密的公私密钥对 PK 用于对患者的 EMR 加密，加密后得到一个唯一文件 ID（HashID）,加密可用公式(2)表示:

$$SHA256(PK, EMR) = HashID \quad (2)$$

加密及同步过程如图 1 所示：

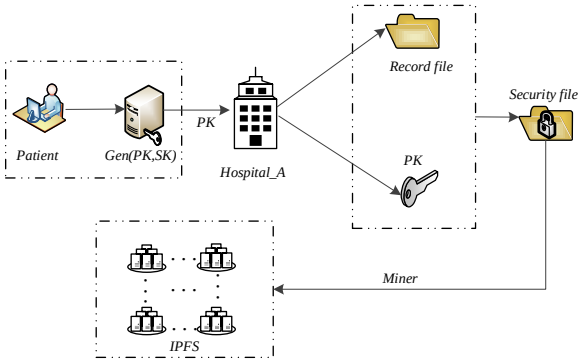

图 1：RSMR 文件同步过程

Fig. 1 Upload to IPFS network

患者自身持有一个公私钥对(PK,SK)，在医院就医完成后，把公钥 PK 给医院 A，医院利用公式(2)对患者的医疗记录文件 EMR 加密，得到加密后的文件 SecurityFile，加密后的记录文件储存在医疗记录文件夹地址 FileAddress 下以便上传到 IPFS 服务。整个加密过程可用算法 1 表示：

算法 1：文件同步合约

1. **Input**：PK, RecordFile
2. **Output**：SecurityFile
3. **begin**
4. **while**(用户第一次使用 RSMR 系统)
5. **if**(患者符合使用条件)
6. {为患者创建结构体数据：
7. $Patient\{ID, PK, SK, FolderAddress\}$ }
8. **if**(创建 FoldAddress 成功&&得到医疗记录文件 EMR)
9. {用公式 $SHA256(PK, EHR) = HashID$ 加密得 SecurityFile }
10. reture SecurityFile;
11. **if**(SecurityFile 的哈希值重复性检查通过)
12. {上传 SecurityFile 到 IPFS 网络上，并且副本同时同步在私有网络的不同网络位置}
13. **else**
14. {文件已经上传过，不需要重复上传，节约带宽}
15. **else**
16. 医院分配具有 IPFS 服务的虚拟机供患者使用
17. **end**

1.2.2 授权合约

本节描述一个 EMR 文件经过一个自动执行的智能合约在以太坊区块链网络上的传输过程。首先，经过加密层输出的唯一文件 ID（HashID）与 EMR 密文文件 SecurityFile。合约收到传输过来的 SecurityFile 后自动将文件传输到医疗私有 IPFS 协议网络 MPN（Medical Private Network）上。在上传之前，IPFS 会自动检验 SecurityFile 是否重复以节约带宽。检验成功后，经过公式(3)加密得到该文件个唯一文件 ID（$HashID_1$）。然而，一份完整的 EMR 文件中常常包括不同

类型的病历文件，例如：X 光图片，症状视频，治疗结果文字 ：

$$SHA256\{PK, RecordFile(Pic_1 \cdots Pic_n, Video_1 \cdots Video_n, Text_1 \cdots Text_n)\} = HashID_1 \quad (3)$$

加密得到的一个文件夹哈希值 内包含多个文件，本文用下列符号表示：

$$Pic_{11} \cdots Pic_{1n}$$
$$Video_{11} \cdots Video_{1n}$$
$$Text_{11} \cdots \in Text_{1n}$$

一个患者若是综合症患者或者是身患多种疾病，在一个 IPFS 协议下，用同样的密钥对可以对应多个文件夹，本文用 $Hospital_A(HashID_1 \cdots HashID_n)$ 表示在医院 A 就诊过程中，综合性疾病包含的文件夹。

校验与上传过程完成后，这份文件被分成序列 $sequence_1, sequence_2 \cdots\cdots sequence_n$ 储存在与患者计算机相连的机器上，即使某个主机关机或者不可预知性错误发生，也不会影响患者拿到储存在其他地方的副本文件，如图 2 所示。

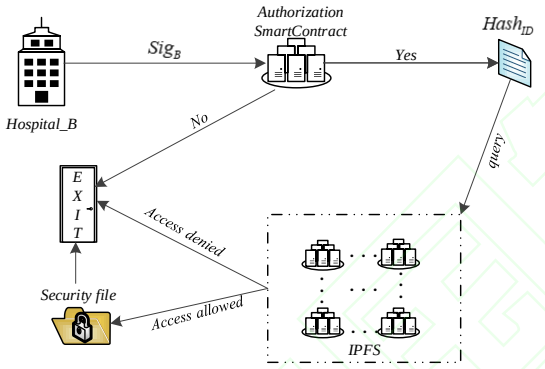

图 2：授权合约执行过程

Fig. 2 The process of authorized smart contract

当 $Hospital_B$ 需要检索 EMR 时，首先需要验证 $Hospital_B$ 的签名 Sig_B，以确定为合法机构。通过检验后，机构便可以得到 $Hospital_A(HashID_1 \cdots HashID_n)$，利用 $Hospital_A(HashID_1 \cdots HashID_n)$，找到副本的文件地址。也就是说，合成储存在不同机器上的副本文件哈希值序列 $(sequence_1, sequence_2 \cdots\cdots sequence_n)$。通过这些哈希值，患者可以方便在自己的机器上下载得到自己先前传输的 EMR 文件。下载完成后，用户还需执行本文 2.2.2 解密文件过程得到解密后的明文文件。合约执行过程如算法 2：

算法 2：授权合约

1. **Input**:PK,SK, SecurityFile
2. **Output**: SecurityFile, RecordFile
3. **Initialization**: getHashvalue, VerificationSig, Download
4. **Ensure**:用户的 EMR 文件在本地计算机同步完成
5. func(**getHashvalue**)
6. func(**VerificationSig**)
7. func(**Download**)
8. **AccessControl**:用户在 Hospital_B 需要 EMR 文件
9. **do** VerificationSig(Sig_B)验证 Hospital_B 签名
10. **if**(验证通过){
11. Allow acess
12. **do** getHashvalue()
13. 得到文件哈希 $Hospital_A(HashID_1 \cdots HashID_n)$ }
14. **do** download($Hospital_A(HashID_1 \cdots HashID_n)$)
15. 下载得到密文文件 SecurityFile
16. Hospital_B 查看完成，合约结束
17. **else** {Access denied}
18. **end**

1.2.3 跨域获取合约

针对本文中的场景，在跨域就医过程中，到达 *Hospital_B* 后，针对某些慢性病（例如癌症等），医生需要获取到公式 (1) 中的文件夹的地址哈希 *FolderAddress* 与权限 $Permis$。医生可以在方案服务上从文件夹 *FolderAddress* 下载得到患者的历史患病记录 *EMR* 与各项检查多媒体资料（例如图片、症状视频、治疗结果文字等辅助治疗病历）。但是下载后的文件医生没有办法解密，出于医疗病历隐私性与安全性考虑，运用非对称加密的文件，只允许患者通过注册后的 SK 解密。解密公式为公式(4)：

$$Unlock(SK, SecutyFile, Sig_B) = RecordFile \quad (4)$$

获取文件过程如图 3 所示，

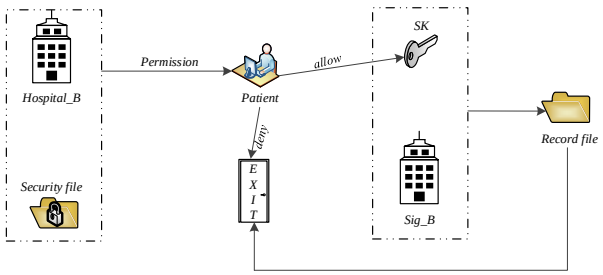

图 3：跨域获取合约

Fig. 3 Cross-domain get EMR contract

用户得到 Security file 后，需要询问用户的允许。若用户允许访问，则能够通过合于得到用于加密此文件的私钥 SK。此时，在解密前，为防止文件泄露，需要验证 *Hospital_B* 的签名 Sig_B，验证通过后方可得到原文件 Record file，同时，合约执行结束。跨域获取合约如算法 3：

算法 3：跨域获取合约

1. **Input**:SK, SecurityFile
2. **Output**: RecordFile
3. **while**(用户到达 Hospital_B 满足使用条件)
4. **if**（Hospital_B 得到下载权限）
5. {利用 FolderAddress 哈希下载 EMR 记录文件 SecurityFile}

6. **while**(用户输入 PrivateKey 与初始分配一致)
7. {执行算法 $Unlock(SK, SecutyFile, \mathrm{Sig}_B) = RecordFile$ 得到历史病历 RecordFile}
8. **else**
9. 患者需授权 Hospital_B；continue;
10. 合约结束
11. **end**

1.3 安全性分析

文件储存地址安全：假设攻击者能够通过某种手段得到患者保存在 *RSMR* 的数据，但是保存在 *RSMR* 中的数据并不会被查看，也不会被删除或者被修改，因此数据是安全的。

区块链的特性作为一种时间戳系列的账本，一旦共识机制确认，便不发修改内容。如果攻击者想要修改在区块链系统中储存的数据，必须仿造一个跟源链一样的主链，而这需要极大算力，这几乎是不可能的。另外在 RSMR 中储存的数据 *SecurityFile* 被分成序列（$sequence_1, sequence_2 \cdots\cdots sequence_n$）储存在与患者计算机相连的机器上，得到这些数据并按照一定序列顺序拼接才能形成源文件，其概率为 $1/\prod_{i=1}^{n} i$，想要按照顺序合成这些文件，这也是困难的。

数据防篡改：假设攻击者能够通过某种手段得到被分成碎片的文件并且按照一定顺序拼接起来，得到跟源文件一样的文件。攻击者想要查看得到文件内容，需要通过患者的 SK 才能解密文件。而通过非对称加密的文件 SecurityFile，想要在不得到 SK 情况下解密是困难的。

在“跨域获取合约”算法中，经过加密的文件被储存在区块链中。因此，在得不到患者的私钥情况下，即使文件与源文件一样，也无法解密文件，即攻击者并不能查看患者的 EMR 真实内容，从而保证患者隐私安全。

数据防盗窃：攻击者通过某种手段试图使用一个虚假文件替换储存在 RSMR 中的真实文件，在源文件存在情况下，这是困难的。

在本文“授权合约”描述中，对执行智能合约的文件需要进行 SecurityFile 的哈希值重复性检查，当攻击者驶入使用一个虚假文件 M' 执行智能合约，通过哈希算法得到的哈希为 $hash_{M'}$，源文件 M 执行智能合约，通过哈希算法得到的哈希为 $hash_M$。根据哈希规则，两个内容不是完全相同的文件经过哈希得到的 hash 值是不同的，即 $hash_{M'} \neq hash_M$。这样，虚假文件 M' 不能够通过 *REMR* 智能合约层的哈希重复性检验，合约不能执行。因此，这个机制能够保证用户的源文件不能够被攻击者使用的虚假文件所替换，从而保证了用户 *EMR* 文件溯源安全性。

1.4 预期目标

1) 隐私保护

本方案中，基于区块链的特性，患者的个人信息将会被唯一哈希值标识，而不像传统医疗机构中使用用户姓名或者 ID 标识。用户的医疗记录文件访问权掌握在自己手中，基于密码学的非对称加密技术使得用户可以在每次上传中重新生成公私钥对，这样实现了用户对每个文件的访问权限限定。而医疗机构 A，则在加入到区块链网络中时，身份信息已被唯一哈希标识，使其同步的文件具有权威性。本方案中区块链网络本质上时保存文件唯一标识的哈希值，因此即得到了文件哈希，没有用户的私钥也无法解开任何在区块链网络中的任何密文信息。

2) 不可修改性

基于区块链的设计，使得上传到到私有网络中的文件带有时间戳，任何操作记录都被同步到所有节点，保证了文件使用透明性。基于区块链特性，每个文件的区块中保存有上一个所存文件的哈希，要想改变当前文件哈希必须保证私有网络中超过 50%的节点同意，在一个较大规模的区块链网络中，这几乎是一件不可能事件。所以，对初始文件的任何改变都会实时显示在区块链网络中，保证了本方案私有区块链网络中文件的不可修改性。

3) 存取流程简化

在本文方案中，基于私有区块链的数据在以上分析中保证了其不可篡改性，在储存过程中，只需要一次储存便可随时随地访问。基于哈希算法的重复文件检查机制，使得在重复文件上传到私有区块链网络中时，具有相同的文件哈希，真正实现“一次上传，永久保存”。在用户授权医院机构得到访问 EMR 文件权限后，医院机构只需根据哈希值便可唯一获取到指定文件，节约了传统医疗记录保存方案中的时间成本，彻底实现“精准定位”。故在本文实验方案中，存取过程都是一次性操作，大大节约了人力成本、时间成本，提高检索文件精确度。

2 实验和表现评估

2.1 方案部署

本方案实验过程中，采用 5 个第三代 B 型树莓派(ARM Cortex-A53 1.2GHz,1G RAM,Ubuntu OS)做硬件载体模拟节点 A、B、C、D、E 的功能，软件方案使用本文前文所述协议分布在每一个硬件载体。为解决拓扑结构中拜占庭问题，本文模拟实验部分选择节点管理工具 IPFS-Cluster 解决，分为服务端与管理端。管理端一般配置在医院服务器，本文拟在 A 节点部署管理端，用于管理 EMR 文件在多节点执行相同操作，例如管理上传文件、更新文件、下载文件。在 B、C、D、E 硬件上部署服务端用于执行 EMR 文件传输。

节点对象：医疗机构所有参与对象，包括医生电脑，患者在家的电脑，或者是医疗记录患者在任何地方的一台个人PC。

模型节点：五个节点，节点 A，B，C，D，E。

节点 A：医生要同步医疗记录信息的计算机。

节点 B：患者要保留个人医疗记录信息的计算机。

节点 C：跟患者有关系的亲邻的个人计算机。

节点 D、E ：医院服务器上虚拟机镜像。

智能合约部分，本方案使用 Remix-IDE 作为以太坊智能合约开发工具，以 Solidity 语言编写，部署在以太坊测试网 Ropsten Test Network 上运行。实验硬件与软件如表 1 所示：

表 1：实验硬件与软件参数

Table1: Hardware and software parameters

硬件/软件	版本
RospberryPi	3B
CPU	Broadcom CortexA53@1.4GHz
内存	1GB LPDDR2
系统	Ubuntu 16.04 LTS
IDE	Remix
编写语言	Silidity 0.4.7
编译环境	JavaScript VM
以太坊钱包	Metamask
测试网络	Ropsten Test Network

2.2 实验流程

本文实验按照如下步骤执行：

1. 密钥生成与同步：所有节点共享一个公钥，当 A 节点生成公私密钥对后，合约执行把 PK 同步到 B、C、D、E 节点。只有树莓派 A 节点所分配的初始私钥 SK 可以解密 EMR 文件。

2. 启动节点：本研究中默认配置有集群管理端的 A 节点作为默认启动节点，负责分配 EMR 执行的任务，主要包括 EMR 文件公钥加密与上传同步形成区块链系统，智能合约执行使默认节点地址自动拷贝到其余 4 个节点。启动完成后，会给当前机器分配一个唯一哈希 ID(QmbQy…mG9bP)作为计算机地址唯一识别，另外包含与本节点相连的四个主机地址。

3. 上传 EMR 文件：如图 3 所示上传加密后的 EMR 文件会得到文件唯一哈希(QmY…Dz4TM)地址与上传时间，这个地址是 EMR 文件在区块链网络中的唯一识别标志，得到这个哈希便可以得到这份加密后的 EMR 文件。

4. 确认交易：节点 A 上传到私有集群网络中的一份加密文档 SecurityFile，得到的哈希值 Hashtext 与时间戳 Timestamp 等，根据 Ethereum 的工作量证明(Proof of Work, POW)共识机制确认交易，同步到其余 4 个私有节点。根据区块链特性，若有节点想要改变文件，需要得到 50%以上节点同意，但这个过程算力成本巨大，一般来说概率极小，保证了 EMR 文件的防篡改性，医疗隐私得以保护。

5. 文件溯源：在本文模型场景中，跨域医院 Hospital_B 想要获取到初始医院 Hospital_A 的文件，必须得到患者的允许下载并提供私钥解密文件，文件更新通过管理端 A 节点下文件目录的哈希值，基于区块链特性，文件会在 B、C、D、E 节点同步一份副本哈希，实现文件可溯源性，如图 6 所示，输入文件哈希值便可以下载 EMR 文件到本地然后触发智能合约中的算法，输入私钥 SK 便可解密得到 EMR 源文件。

2.3 实验分析

2.3.1 储存效率

通常来说，一份 EMR 文件大小在 1~5M 之间，在本方案中上传与下载一份 EMR 文件在小于 100ms 级别。但实际应用场景来说，一个医院通常可能同时存取成百上千分 EMR 文件，在如此高并发文件存取条件下，本实验模拟了从 1~300 份 EMR 文件并行。同时考虑到实际情况，有一部分 EMR 文件是多媒体文件，有一部分是纯电子文档文件，两种不同类型文件的实验表现如图 4 所示：

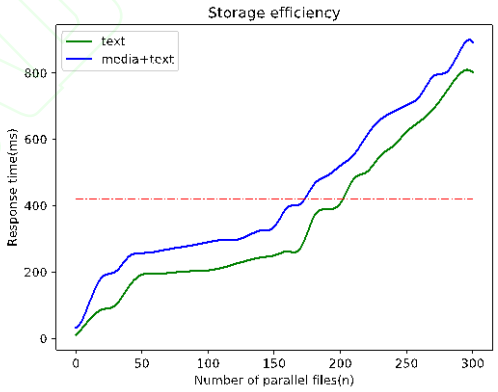

图 4：储存效率图

Fig.4 Comparison of storage efficiency

从图 4 中可以看出，纯文本文件与多媒体融合文件增长趋势基本一致，随着文件增多，节点确认压力变大，响应时间变缓。可以看出，在同时上传 EMR 文件在 180 个文件以下响应速度呈平缓趋势，响应时间大约在 400ms 以下。但是在文件数量在 180 个以上是，响应时间急速增加，其中的原因可能原因是实验中基于 POW 共识机制中，打包合约节点(挖矿节点)过少，导致交易缓慢，理论上将实验布置到公网中效率会进一步优化。但是 180 个文件情况下，完全能够满足模型中的要求，用户不会感到明显迟延现象。总体来说系统表现良好，未出现明显堵塞现象，符合研究初始期望值。

2.3.2 方案时间对比

本方案采取非对称加密方式加密 EMR 文件，当用户需要访问加密后上传到区块链网络的文件，就需要执行授权合

约查看用户是否有权访问。对比了利用云储存方案的(Data Access Control for Multi-Authority Cloud Storage, DAC-MACS)[16]数据访问控制策略方案与基于移动设备的属性加密方案(attribute-based encryption, ABE)[17]，对比结果如表 2：

表 2：安全性与下载效率对比

Table2: Comparison of Security and download efficiency

方案	中心化	加密时间	解密时间	访问控制	下载密文大小
DAC-MACS	Yes	lT_e	lT_c	Yes	$(3l+1)M$
ABE	Yes	T_e	T_c	No	l^2+lM+M
本方案	No	T_e	T_c	Yes	M

其中 M 为密文数据大小，l 为密文属性数量，T_c 为解密 1byte 数据所花时间，T_e 为加密 1byte 数据所花时间。从表中可以看出，在储存方式中，本方案采用的基于区块链技术的非中心化储存，这种去中心化储存方式能够有效解决 DAC-MACS 和 ABE 中半可信第三方可能造成的数据泄露和窃取问题。另外，由于本方案密文下载不依赖于数据属性个数，故在加密阶段时，相同文件条件下需要时间为 T_e，相对于依赖与属性个数的方案 DAC-MACS 的加密时间 lT_e 来说，加密时间开销降低，解密阶段也是如此。在多节点并行时，综合时间大大降低。访问控制方面，DAC-MACS 中未设立数据访问控制策略，本方案中的访问控制策略能够帮助用户与其他医疗机构迅速识别合法访问人，并且给出 EMR 文件。节约带宽方面，DAC-MACS 与 ABE 方案想要获得密文需要依赖于属性的数量，其大小分别为 $(3l+1)M$ 和 l^2+lM+M，本方案在通过访问控制后下载密文，在医院获取多个患者 EMR 时能够节约带宽。综上，本方案相对于 DAC-MACS 与 ABE 方案，能够明显提升数据安全性，节约用户或医院时间，能够有效识别合法访问者，节约下载带宽。

2.3.3 交易储存开销

为了防止无意义交易产生，例如一个空交易，浪费矿工打包交易资源，现有的共有链都采用了交易收费的手段防止无意义交易。简单来说，每执行一笔交易，都需要一定的交易费用，根据一笔交易合约的计算步骤能够计算出对应交易所需费用。以太坊中用 Gas 计算交易费用[18]，具体每个计算步骤与交易费用如表 3 所示：

表 3：常见计算步骤消耗

Table3: Common calculation steps consume

执行语句	Gas/wei	描述
Step	1	执行一个周期默认费用
Sha3	20	一个散列算法费用
Sload	20	从储存器获取
Sstore	100	输入到储存器中
Balance	20	调用账户余额费用
Create	100	合约创建
Call	20	初始化一个只读调用
Memory	1	扩充内存一个额外字符
Txdata	5	交易或编码一个字节
Transaction	500	基础交易费用
Create Contract	53000	合约创建同步区块

假设医疗记录文件文件 EMR 的大小为 ，对比文献[19]中的方案(简称方案 A)中的合约开销，得到如下表 4：

表 4：合约开销对比

Table4: Comparison of contract cost

	储存开销	交易开销	执行开销	总开销
方案 A	5N	$53641+6N$	$640+N$	$54281+12N$
本方案	无	53601	640	54241

从表中可以看出，由于本方案中，医疗数据文件 EMR 储存在 IPFS 网络中，储存在 IPFS 网络中的数据不许要支付代币，只需等待验证即可，因此不需要花销。而方案 A 当中需要把数据存储到以太坊网络中，文件储存开销为 $5N$ wei，在节点较多时，储存开销较大。在合约交易开销方面，同上利用到 IPFS 网络中不需要代币储存，因此比方案 A 节约开销大约为 $40+6N$ wei，执行合约过程中节约的开销为 N wei。计算所有流程后，总开销大约节约了 $40+12N$ wei。综上，本方案在储存开销方面能够大大降低储存医疗记录文件 EMR 的开销。

3 结语

在本研究中，提出了区块链技术在特定医疗环境中应用的情景：跨域记录分享与溯源。并系统讨论了本文所提出的方案在隐私保护、存取效率、安全性、部署复杂性、易用性等方面的优缺点。实验结果表明，在上述方面性能指标方面，本研究所提出的方案具有高效储存文件、低交易开销、可溯源和低延迟特点。

但是，区块链作为一种多方参与、多方监管技术，虽然能够保证交易记录随时追溯，但是也可能会受到诸如密钥在传播中遭到人为泄露等安全问题。本研究未来将采用密码学中诸如属性加密、同态加密和代理加密技术，结合区块链技术中多方参与、不可篡改等特点，保护用户隐私信息。

参考文献

[1] Okura Y, Urban L H, Mahoney D W, et al. Agreement between self-report questionnaires and medical record data was substantial for diabetes, hypertension, myocardial infarction and stroke but not for heart failure[J]. Journal of Clinical Epidemiology, 2004, 57(10):1096-1103.

[2] Collier D S, Grant R W, Estey G, et al. Physician ability to assess rheumatoid arthritis disease activity using an electronic medical record-based disease activity calculator.[J]. Arthritis Care & Research, 2010, 61(4):495-500.

[3] Li Z R, Chang E C, Huang K H, et al. A secure electronic medical record sharing mechanism in the cloud computing platform[C]// IEEE, International Symposium on Consumer Electronics. IEEE, 2011:98-103.

[4] Haskew J, Rø G, Saito K, et al. Implementation of a cloud-based electronic medical record for maternal and child health in rural Kenya[J]. International Journal of Medical Informatics, 2015, 84(5):349-354.

[5] Biswas S, Anisuzzaman, Akhter T, et al. Cloud based healthcare application architecture and electronic medical record mining: An integrated approach to improve healthcare system[C]// International Conference on Computer and Information Technology. IEEE, 2015:286-291.

[6] Berman F. Got Data:A Guide to Data Preservation in the Information Age[J]. Communications of the Acm, 2008, 51(12):50-56.

[7] Shen M, Ma B, Zhu L, et al. Cloud-Based Approximate Constrained Shortest Distance Queries Over Encrypted Graphs With Privacy Protection[J]. IEEE Transactions on Information Forensics & Security, 2018, 13(4):940-953.

[8] Cheng H , Rong C , Hwang K , et al. Secure big data storage and sharing scheme for cloud tenants[J]. China Communications, 2015, 12(6):106-115..

[9] Hao W , Yujiao S . Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain[J]. Journal of Medical Systems, 2018, 42(8):152-.

[10] Xia Q, Sifah E B, Asamoah K O, et al. MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers Via Blockchain[J]. IEEE Access, 2017, PP(99):1-1.

[11] Hussein A F , Arunkumar N , Gustavo R G , et al. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform[J]. Cognitive Systems Research, 2018, 52:1-11.

[12] Liu J , Li X , Ye L , et al. BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records[J]. 2018.

[13] Benet J. IPFS - Content Addressed, Versioned, P2P File System[J]. Eprint Arxiv, 2014.

[14] Luu L, Chu D H, Olickel H, et al. Making Smart Contracts Smarter[C]// ACM Sigsac Conference on Computer and Communications Security. ACM, 2016:254-269..

[15] Wang J, Zeng X, Chen J. A VLSI implementation of ECC combined with AES[C]// International Conference on Solid-State and Integrated Circuit Technology. IEEE, 2006:1899-1904.

[16] Yang K, Jia X, Ren K, et al. DAC-MACS: Effective data access control for multi-authority cloud storage systems[C]// IEEE INFOCOM. IEEE, 2013:1790-1801.

[17] Akinyele J A, Pagano M W, Green M D, et al. Securing electronic medical records using attribute-based encryption on mobile devices[C]// ACM Workshop on Security and Privacy in Smartphones and Mobile Devices. ACM, 2011:75-86.

[18] 闫莺, 郑凯, 郭众鑫. 以太坊技术详解与实战[M]. 机械工业出版社:闫莺, 2018:40-43.(Yan Y, Zheng K, Guo Z X. Technical Details and Practical Warfare of Ethereum [M]. China Machine Press, 2018:40-43)

[19] KN Griggs, O Ossipova, CP Kohlios, AN Baccarini, EA Howson, et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring[J]. Journal of Medical Systems, 2018, 42(7):130.

This work is partially supported by the National Natural Science Foundation of China (61841701)

This work is partially supported by the National Natural Science Foundation of Fujian Province (2016J01287)

This work is partially supported by the National Natural Science Foundation of Fujian Province (2018J01781)

XU Jian, born in 1995, M. S. candidate. His research interests include network and information security.

CHEN Zhide, born in 1976, Ph.D., professor. His research interests include network security and cryptography, distributed computing.

GONG Ping, born in 1982, Ph.D., associate professor. His research interests include formal modelling and analysis , BPM and monitoring.

WANG Keke, born in 1992, M. S. candidate. His research interests include network and information security.