基于区块链的医疗数据安全存储研究

刘志豪,马金刚,李逢天,生　慧*
(山东中医药大学,济南 250355)

[摘要] 目的:构建医疗数据存储共享平台,提升医疗信息存储共享的效率和安全性。方法:结合区块链存储技术和云数据库设计一个安全、高效的分布式医疗数据存储方案。区块链中存储医疗数据的元数据和数据提供者签名,保证医疗数据的隐私性和完整性;云数据库中存储医疗数据的完整记录,利用云数据库特性保证医疗数据的共享便利性和可扩展性。结果:该方案既可以实现医疗数据防篡改和分布式存储的需求,又可以保证患者对医疗数据的权限控制,还可以实现第三方用户对医疗数据的共享使用。结论:将区块链技术应用于医疗数据存储是解决当前医疗数据安全共享问题的可行方案。

[关键词] 区块链;云数据库;数据安全;数据防篡改;分布式存储;隐私保护
[中国图书资料分类号] R318;TP311 [文献标志码] A [文章编号] 1003-8868(2019)03-0031-04
DOI:10.19745/j.1003-8868.2019060

Research on medical data storage based on blockchain

LIU Zhi-hao, MA Jin-gang, LI Feng-tian, SHENG Hui*
(Shandong University of Traditional Chinese Medicine, Jinan 250355, China)

Abstract **Objective** To build a medical data storage sharing platform to improve the efficiency and security of medical information storage and sharing. **Methods** Blockchain and cloud storage technologies were used to design a secure and efficient distributed medical information storage platform. Information such as medical data metadata and signatures of data provider was stored on the blockchain to ensure the privacy and integrity of medical data; the complete records of medical data were stored on the cloud to ensure the convenience and scalability of medical data sharing. **Results** Security analysis demonstrated that the medical data storage system based on blockchain and cloud achieved efficient information storage sharing and security protection. **Conclusion** The application of blockchain technology to medical data storage is a viable solution for blockchain application in the medical field. [Chinese Medical Equipment Journal, 2019, 40(3): 31-33, 37]

Key words blockchain; cloud database; data security; data anti-tampering; distributed storage; privacy protection

0 引言

在目前的医疗机构中,医疗数据主要面临数据泄露和数据篡改两大方面的风险。患者的电子病历中包含着大量的隐私信息,如患者的病情信息、消费记录等,这些信息会集中存储在医院的服务器上,而大多数医院对信息安全的重视程度不高,医院网站漏洞数不胜数,使攻击者可以轻而易举得到医院的数据库、患者的信息,从而造成用户的隐私泄露,即存在数据泄露风险。同时,若攻击者对数据进行蓄意破坏、篡改,会严重阻碍医疗系统的可用性,即存在数据篡改风险。

区块链技术(Blockchain technology)是一种去中心化的分布式存储技术,具有不可篡改、去信任、匿名性等特点,可以实现网络中去中心化信用的数据共享、协调与协作。本文提出的基于区块链技术设计的医疗数据存储平台可有效解决上述问题。

1 区块链技术简介

区块链技术也称为分布式账本技术,其本质上是一种去中心化的数据库技术,特点是去中心化、不可篡改等。

(1)去中心化。区块链是一种分布式数据存储结构,且没有中心节点,所有节点都保存全部的、相同的区块信息,完全实现去中心化,很大程度上保证了分布式数据库开放透明、安全可信、不可篡改的特点。

基金项目:山东省社会科学规划研究项目(17CHLJ09);山东省重点研发计划(重大关键技术)(2016CYJS08A01-1);山东中医药大学科学基金(2018zk23);山东省高校科研计划项目(J18RA226)
作者简介:刘志豪(1998—),男,研究方向为医疗信息安全,E-mail:17862971503@163.com。
通信作者:生　慧,E-mail:shenghui2217@163.com

⑵ 不可篡改性。区块链中存储的交易信息每一条都有相对应的哈希值，若想篡改区块链中的一条记录，不仅要修改此区块的哈希值，还要修改后续所有区块的哈希值。除非能同时修改系统中超过51%的区块，否则对单个区块上数据库的修改是无效的。

⑶ 去信任。因为数据库和整个系统的运作是完全公开透明的，且系统中所有节点之间无需信任也可以进行交易，所以在系统的规则和时间范围内，节点之间无法彼此欺骗，即节点之间去信任。

⑷ 匿名性。由于节点间的交换遵循固定的算法，其数据的交互是无需信任的，因此交易双方无须公开身份就可以让双方产生信任，即区块链技术具有匿名性。

2 基于区块链技术的医疗数据存储现状

近几年里，各医疗机构都经历过黑客攻击或数据泄露，患者因此遭受经济威胁、精神痛苦和社会舆论等，利用区块链技术去中心化和不可篡改性的特点不仅可以避免类似事件的发生，还可以大大提高医疗服务效率。

区块链包含 n 个随时间排序的区块，每个区块都有一个指向前一区块的指针，所有区块通过这个指针形成一个链，因此称为区块链。而第一个区块则称为创世块，其后每个想要参与进来的节点都要下载并更新一份从创世块延续下来的数据包。随着医疗数据的积累，基于区块链的医疗数据存储，其数据量会迅速上升，区块承载的数据会越来越多，这便对区块链数据库的存储空间有了更高的要求。如果每一个节点的数据都完全同步，区块链数据的存储空间容量要求就势必会成为一个限制其发展的关键问题，会直接影响医疗部门更新数据信息和医患对数据获取实时性的需求[1]。基于上述问题，本文设计了一个结合区块链和云存储技术的医疗数据存储平台。

2.1 医疗数据存储平台设计

由于区块链的存储容量有限，无法存储患者的全部医疗数据，因此，本设计中区块链只保存医疗数据的元数据和摘要、数据提供者公钥、数据提供者签名以及该医疗记录在云数据库中的引用，而具体的医疗记录保存在云数据库中。基于区块链存储技术和云数据库的医疗数据存储平台体系结构，如图 1 所示。

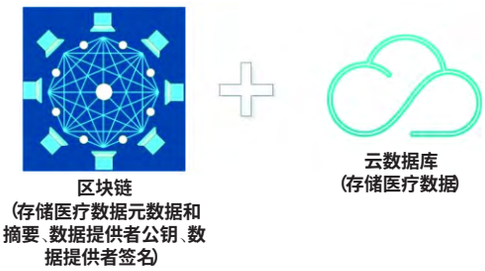

图 1 医疗数据存储平台体系结构图

将区块链技术应用于医疗健康数据平台后，基于区块链的安全特性，医疗健康平台可以确保安全、高效地存储患者数据。以公钥加密为基础的共享访问方式是医疗健康数据平台的重要设计方案。医院及权威机构保管患者公钥，并利用公钥将患者的医疗健康数据进行加密，患者通过私钥访问个人医疗健康数据[2]。同时，由于区块链具有高安全性、隐私保护、高冗余存储、去中心化等特点，因此能够防止遭受攻击或权限管理不当导致的数据丢失，使数据更加安全可靠[3]。

对医疗大数据的分析处理需要强大的数据存储和计算能力。针对不同用户，医疗数据云存储具有不同的意义[4]。患者可以在云数据库中存储医疗健康数据并实现随时随地的访问；研究人员可以使用云数据库中汇集的医疗数据进行分析和计算；医疗存储机构采用区块链加云储存方式是一种安全、经济、便利且可以随意改善管理的方式[5]。

2.2 医疗数据存储

虽然区块链技术采用了密码学等相关技术，但整个区块链网络在安全方面仍然存在薄弱环节。尤其是数据隐私方面，现阶段还没有健全的医疗隐私法律保护制度，民众对个人数据也没有较强的自我保护意识，区块链的安全性仍令人担忧[6]。

为保证医疗数据的安全存储，基于区块链的医疗数据存储系统的数据存储过程设计如下：

⑴ 医疗机构生成医疗记录，并将医疗记录元数据和摘要上传至区块链。医疗记录元数据包括医疗数据 ID 及其在云数据库中的 URL 等信息。

⑵ 医疗记录安全传输至患者。医疗机构将医疗数据以对称加密算法加密后传输给患者，对称密钥的分发采用公钥加密算法进行。患者首先利用个人的私钥解密医疗机构发送过来的会话密钥，然后再用该会话密钥解密医疗记录。该过程可保证密钥的安全分发及医疗记录安全、快速传递。

⑶ 患者对医疗记录加密并上传至医疗云数据库。患者生成新的会话密钥并用该密钥加密医疗记录后上传至云数据库中存储。医疗数据的所有权限归患者所有，其他用户的使用权限也需患者分配以

控制不同用户对数据的访问。

上述存储过程中医疗元数据和医疗数据分别存储在区块链和云数据库中，可实现医疗数据的分布式存储；患者作为医疗数据的所有者，利用自己的私钥可保证医疗数据的隐私安全性，并具有对医疗数据权限的分配权，这为医疗数据的安全共享奠定了基础。

2.3　医疗数据共享

在医院中，如果使用区块链技术对医疗数据进行保护，当患者、医生在对医疗数据进行访问或者多科室协调工作时，需要对医疗数据进行访问和共享。传统的数据访问机制需要花费大量的时间及硬件资源进行审查和数据校验，因此需要考虑对医疗数据进行访问和共享的需求。

调查表明医疗数据中心往往建立在大型重点医疗机构，并提供接口给下属医疗机构使用，而医生和患者是小型在线客户端直接与数据中心进行信息交互[7]。在调查和分析后，本研究采用了自底向上的方式，依次研究了在线客户端、二级医疗机构和顶级数据中心的数据共享与访问机制，在此基础上建立一个完整的医疗卫生信息化系统数据共享与访问模型。大型医疗机构即顶级数据中心的职责是存储数据，并向下属的二级医疗机构提供数据共享接口；二级医疗机构作为区块链模型中的一个节点，对顶级数据中心提供的接口进行解析，接收来自顶级数据中心的医疗数据；在二级医疗机构的基础上再次建立二级区块链模型，以在线客户端作为节点，保障与顶级数据中心交互过程中的数据共享与访问[8]。

3　医疗数据的存储安全性分析

本设计的医疗数据存储平台的安全机制是由3个维度共同保证的，如图2所示。

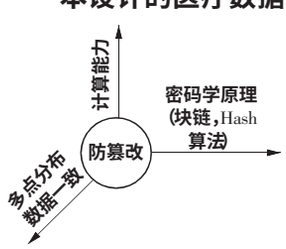

图2　医疗存储平台防篡改机制结构示意图

第一个维度是分布式账本技术。基于区块链技术实现的医疗数据平台网络具有大量节点，它创建了一个多点分布，网络成员之间共享、复制和同步的数据库。攻击者若要实施攻击、更改医疗记录，必须要在短时间内改动超过51%的节点，其技术难度巨大，计算上几乎不可能实现。

第二个维度是巨大的计算力成本。区块链从创世块开始，后续每一个区块中的交易记录都包含前一个区块中的内容，因此区块链中的数据采用链式结构存储。攻击者若想更改医疗交易记录，那么首先需要根据当前交易内容追溯上一个区块的位置，然后更改之前每一个区块中的相应信息，直至完成所有节点中的备份交易记录，而完成这些工作的前提要求其他节点必须都处于静止状态。由第一维度可见，更改一个区块中的记录于计算上是不可行的，而更改多个区块，其难度必然更大。

第三个维度是密码学的应用。基于区块链技术的医疗信息平台采用了大量的密码学技术，如Hash算法、椭圆曲线、RSA加密算法等。其中Hash算法的应用最为关键，该算法对区块进行SHA-256加密。SHA-256加密算法的输入长度为256位，输出长度是32字节的随机散列数据。区块链中用Hash算法对一个交易区块中的交易信息进行加密，并压缩为一串由数字和字母构成的散列字符串，该串字符串便是这个区块的Hash值，如图3所示。而按现有的计算机技术，很难找到高效率的解密算法[9]。

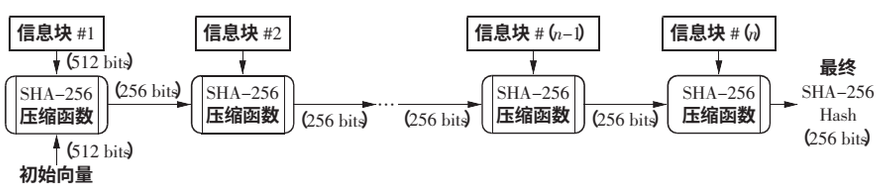

图3　SHA-256加密算法加密流程图

4　结语

区块链和云数据库存储为医疗大数据的安全存储和共享提供了技术基础，本文设计的医疗数据平台既可以实现医疗数据的分布式存储，又保证了患者对医疗数据的权限控制，还可以实现第三方用户对医疗数据的共享应用。患者、医疗机构和科研机构之间可在该平台分享医疗数据，例如共享疾病诊疗、遗传、饮食、环境和生活方式等医疗健康数据，并以此为基础挖掘、开发新的养生和疾病防治方式。

随着医疗大数据的发展，区块链作为系统存储技术，将对医疗信息化的发展带来更多的机遇和挑战。现阶段对政策、标准等环节的探索和实践，是行业发展的首要任务，针对这一颠覆性的变革，采取谨慎、循序渐进的方法也是医疗领域中区块链应用的可取途径。

[参考文献]

[1]　王文明，刘云，周钰，等. 医院诊疗健康信息数据的分类

(►►下转第37页►►)

波刀临床治疗中，对于肿瘤直径小于 15 mm 的患者，不建议选择肺部跟踪技术。

根据表 2、3 统计数据分析，在肿瘤直径 10 mm≤d<15 mm 的 3 例患者中，通过优化措施后，治疗过程中 Synchrony 模型重建频率降低了 2.0，优化效果最为明显；肿瘤直径 15 mm≤d<20 mm 的 24 例患者中，通过优化措施重建频率也下降了0.77，表明肺追踪优化措施对于降低治疗过程中 Synchrony 模型重建频率是有效的。本研究中肿瘤直径 10 mm≤d<15 mm 的病例数偏少，可以进一步进行统计研究以获得更多的数据支持，但在 15 mm≤d<20 mm 和 d≥20 mm 病灶治疗中依然可以看到优化措施对于 Synchrony 模型重建频率有下降趋势，综上，肺追踪优化对模型重建是有积极作用的。此结论的前提是同一例患者在不同分次治疗过程中的呼吸习惯和规律一致，因为呼吸规律对 Synchrony 模型重建也有影响[8-10]。但是本研究中，射波刀治疗分次少，因此在短时间内同一个患者呼吸习惯变化较小，建议可以进一步探讨呼吸习惯和规律对 Synchrony 模型重建的影响。

X-sight lung 肺部跟踪技术是射波刀唯一一种可直接对患者呼吸运动进行追踪而不需要穿刺植入金属标志物[11]、放疗前的准备和医疗付出较少的同步运动追踪技术。在 Synchrony 建模前正确的目测判断和采用肺追踪优化措施可使建模的成功率最大提高 44.6%（肿瘤直径 15 mm≤d<20 mm），且综合采用二次脊柱追踪辅助定位和启用建议影像/主要参考影像可以提高射波刀肺追踪治疗旋转偏差的修正，降低治疗风险。因此，放射治疗师应综合利用各种优化手段，在提高射波刀治疗精度的同时规避治疗的意外和风险。

[参考文献]

[1] BLANCK O，MASI L，DAMME M C，*et al*. Film-based delivery quality assurance for robotic radiosurgery：commissioning and validation[J]. Phys Med，2015，31(5)：476-483.
[2] 胡斌，程军平，彭振军，等. 全身肿瘤立体定向放射外科系统——第 5 代射波刀[J]. 医疗装备，2016，29(3)：50-51.
[3] 蔡陈枫，朱六玲，徐胜，等. 射波刀治疗系统的精确度评价[J]. 医疗卫生装备，2017，38(6)：121-123.
[4] 景生华，李兵，周正东，等. 射波刀 Synchrony 同步追踪系统三维方向质量保证分析[J]. 医疗卫生装备，2018，39(1)：58-61.
[5] 胡斌，彭振军. 射波刀追踪系技术研究进展[J]. 中国医疗设备，2017，32(2)：100-103.
[6] LIN Y W，LIN K H，HO H W，*et al*. Treatment plan comparison between stereotactic body radiation therapy techniques for prostate cancer：non-isocentric CyberKnife versus isocentric RapidArc[J]. Phys Med，2014，30(6)：654-661.
[7] MONGEON M，THIBAULT F，CHARTRAND-LEFEBVRE C，*et al*. Safety and efficacy of endovascular fiducial marker insertion for CyberKnife stereotactic radiation therapy planning in early-stage lung cancer[J]. J Vasc Interv Radiol，2017，28(8)：1 090-1 097.
[8] BALACHANDRAN R，FRITZ M A，DIETRICH M S，*et al*. Clinical testing of an alternate method of inserting bone-implanted fiducial markers[J]. Int J Comput Assist Radiol Surg，2014，9(5)：913-920.
[9] JUNG J，SONG S Y，YOON S M，*et al*. Verification of accuracy of CyberKnife tumor-tracking radiation therapy using patient-specific lung phantoms[J]. Int J Radiat Oncol Biol Phys，2015，92(4)：745-753.
[10] 朴俊杰，徐寿平，巩汉顺，等. CyberKnife 系统技术评估和临床应用评价[J]. 医疗卫生装备，2016，37(3)：114-117.
[11] TRUMM C G，HÄUSSLER S M，MUACEVIC A，*et al*. CT fluoroscopy-guided percutaneous fiducial marker placement for CyberKnife stereotactic radiosurgery：technical results and complications in 222 consecutive procedures[J]. J Vasc Interv Radiol，2014，25(5)：760-768.

（收稿：2018-04-22 修回：2018-11-20）

（◀◀上接第 33 页◀◀）

分层存储技术研究[J]. 医疗卫生装备，2018，39(2)：51-55.
[2] 梅颖. 安全存储医疗记录的区块链方法研究[J]. 江西师范大学学报(自然科学版)，2017，41(5)：484-490.
[3] 黄永刚. 基于区块链技术的电子健康档案安全建设[J]. 中华医学图书情报杂志，2016，25(10)：38-40，46.
[4] 倪培昆. 区块链技术及其在医疗领域的价值研究[J]. 医学信息学杂志，2018，39(2)：9-13.
[5] 王海隆. 区块链技术在中医药领域中的应用展望[J]. 贵阳中医学院学报，2017，39(3)：1-4.
[6] 钱卫宁，邵奇峰，朱燕超，等. 区块链与可信数据管理：问题与方法[J]. 软件学报，2018，29(1)：150-159.
[7] 薛腾飞，傅群超，王枞，等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报，2017，43(9)：1 555-1 562.
[8] 武岳，李军祥. 区块链 P2P 网络协议演进过程[J/OL]. 计算机应用研究，2019，36(10). [2018-09-17]. http://www.orocmag.com/article102-2019-10-068.html. DOI：10.39691 j.issn.1001-3695.2018.07.0365.
[9] 余伟，姜晓红，薛亮. 区块链行业应用现状综述和发展前景分析[J]. 电子商务，2018(9)：49-50.

（收稿：2018-05-07 修回：2018-11-29）