基于区块链的个人健康记录分布式框架研究*

姚俊明 邢 丹 李庆玲

（济宁医学院医学信息工程学院 日照 276826）

〔摘要〕 利用区块链技术构建个人健康记录分布式框架，分析采用区块链存储医疗大数据存在的问题并提出相应改进措施，包括采取开放式电子健康记录规范（openEHR）标准，在区块链中仅存储主索引和查询位置等。阐述架构设计及安全性，指出其有助于实现可信任的个人健康记录访问。

〔关键词〕 区块链；个人健康记录；分布式；对等网；openEHR

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2019.03.005

Study on Blockchain－based Distributed Framework of Personal Health Records *YAO Junming, XING Dan, LI Qingling, School of Medical Information Engineering of Jining Medical University, Rizhao 276826, China*

〔**Abstract**〕 The distributed framework of Personal Health Records (PHR) has been built by utilizing blockchain technology. The paper analyzes the problems with storing healthcare big data by adopting blockchain technology and comes up with corresponding measures to achieve improvement, including adopting openEHR standard, only storing prime index and location query in the blockchain, etc. It also elaborates on the architecture design and security of the framework, points out that such a framework can facilitate the reliable access to PHR.

〔**Keywords**〕 blockchain; Personal Health Records (PHR); distributed; peer to peer; openEHR

1 引言

以计算机为代表的通信技术促使医院广泛使用电子健康记录（Electronic Health Records，EHR），患者的健康记录可以在医疗机构内部供医护人员使用。随着人口的流动，不同医疗机构之间的信息共享需求日益增强。同时随着生活水平的提高人们对健康信息管理的需求日益突显，希望拥有个人医疗健康数据的访问权。但由于系统的使用依赖于专属数据库，这些数据库很少或根本无法同其他系统互操作。此外现有的医疗健康机构采用不同标准的技术，导致患者医疗数据分散在多个医疗机构内部，

〔收稿日期〕 2018－10－17

〔作者简介〕 姚俊明，硕士，讲师，发表论文18 篇，参编专著2 部；通讯作者：邢丹，硕士，讲师，发表论文20 篇。

〔基金项目〕 济宁医学院青年教师科研扶持基金“移动云环境下具有计算迁移的远程医疗架构研究”（项目编号：JY2017KJ057）；济宁市哲学社会科学规划研究2018 年度课题“大物移云时代济宁市医养结合养老模式研究”（项目编号：18JSGX011）。

无法以统一的视图查看患者医疗健康档案。尽管目前国际卫生组织制定很多规范，但出于安全性的考虑，医疗机构并不共享患者数据。同 EHR 相比，个人健康记录（Personal Health Records，PHR）可以接收患者输入数据，查询如体重或血压等健康相关信息。而现有的医疗健康数据大多分散在各个区域医疗系统内部，信息呈碎片化，无法有效地服务于个人健康管理。传统医疗数据共享高度依赖于第3 方机构（如健康信息交易所、人口数据库），存在因第 3 方机构发生欺诈或受攻击而产生个人医疗隐私数据泄漏的问题。目前国内外医疗健康领域呼吁以患者为中心，让患者成为其健康记录的所有者，授予访问权限，与第 3 方机构共同管理个人健康数据。基于此，本研究目标是提供个人健康记录的分布式框架。为 PHR 提供分布式、可互操作的体系结构模型，为患者和医疗保健服务人员提供统一视角，患者可以从统一视图中维护其健康历史记录，无论在哪里接受治疗，医疗服务提供者拥有这些最新数据。

区块链使用一系列技术组合完成去中心化的数据存储，具有分布式、去中心化、信息安全保密和可追溯性等特点，可用于医疗领域实现电子健康病历、DNA 钱包、药品防伪等方面的应用，实现对患者隐私的保护及维护信息的完整性[1]。

2 国内外研究现状

2.1 国内

中国工信部 2016 年发布《中国区块链技术和应用发展白皮书》，制定区块链标准。国内将区块链与医疗健康领域结合的研究相对较少，目前仅限于在行业内对应用场景的设想。梅颖[2]针对医疗信息系统中存在的医疗信息记录存储安全和隐私保护问题，结合区块链和云存储技术，提出医疗记录安全存储方案，但未考虑医疗记录在各机构间的数据兼容性和互操作性等问题。薛腾飞[3]等提出基于区块链的医疗数据共享模型，适用于解决各医疗机构数据共享难题，但这一设计在具体实施中会遇到问题和挑战。阿里健康与常州市医联体合作“医联体+区块链”试点项目，在项目中设置多层安全屏障，设计数字资产协议和数据分级体系，通过协议和证书明确规定各级医院和卫生行政部门的访问和操作权限。

2.2 国外

世界上许多公司和研究机构均参与到区块链在医疗领域的应用。瑞士 Healthbank 为保证健康数据存储安全，通过区块链处理事务；Gem Health 联合飞利浦区块链实验室构建区块链健康生态系统。在医疗健康领域的分布式体系框架问题研究中开展以下相关工作。层次化分布式 EHR 集成模型（Hierarchical Distributed EHR，HDEHR）的目标是在卫生组织中维护患者数据，同时为保证容错能力将其复制到所在地区的其他医院[4]；在 m-Health 的泛在云健康服务（Ubiquitous healthcare services in cloud）模型中，提出一种基于分发事件的体系结构，其互操作性服务遵循 CCR 标准，但未提及隐私问题[5]。泛在的个人健康记录框架（Ubiquitous PHR framework）模型是一种基于事件的分布式模型[6]。以上模型均未涉及安全性和隐私性问题。概念框架（Conceptual Framework）[7]模型是可穿戴医疗系统的一个框架，采用基于对象的分布式机制——云服务器分布，采取安全和隐私保护，但没有关注互操作性；HealthVault[8]是遵循护理连续性记录（Continuity of Care Record，CCR）和卫生信息交换标准（Health Level，HL7）的专有解决方案，是基于 Web 的 PHR 维护健康和体重的记录，但由客户组成服务器平台，所有健康数据均存储在公司服务器；HealthTicket[9]模型是 PHR 的设计与实现案例，该体系结构是移动和医疗服务提供商通过 Web 应用程序访问患者数据，遵循 CCR 和 HL7 标准，使用客户机-服务器模型，利用密码文本策略属性加密方案的安全机制来保护隐私；分布式电子记录（Distributed Electronic Patient Records）模型[10]是一种基于 OpenEMR 系统的分布式组件方案，符合多种标准，但未注重安全性和隐私性；OminiPHR[11]整合 PHR 支持分布式 PHR 的体系模型，使患者和健康机构能

够从任何设备统一维护其健康历史记录，同时使健康组织之间信息共享成为可能，但未详细说明区块链的设计问题。目前患者健康数据集中在一个或多个服务器上，采用客户机－服务器体系结构。其他模型只是提出将来进一步进行分布式体系结构研究，OminiPHR 尽管采用分布式体系架构，但未深入探讨区块链在该架构中的应用细节。

2.3 研究目标

本研究旨在利用区块链实现安全可信的个人健康记录分布式框架。国外医疗保健组织已采用区块链技术，在临床试验记录、监管合规性和医疗/健康监控记录以及健康管理、医疗设备数据记录、药物治疗、计费和理赔、不良事件安全性、医疗资产管理、医疗合同管理等方面发挥重要作用，IBM 公司推测未来全球 56% 的医疗机构将在两年之内投资区块链。全球互联网机构和创业公司也积极探索区块链在医疗领域的应用。目前医疗数据共享仅限于医院内部医疗信息系统之间，研究热点集中在区域医疗内部实现数据互相访问。而真正意义上的数据共享应该是院内、院际、第 3 方机构的全面互联互通。笔者尝试将区块链应用于解决 PHR 的安全性和医疗机构之间的互操作问题，期望通过采用区块链构建云环境下的去中心化、安全且可信任的个人健康记录访问模型。

3 采用区块链存储医疗大数据分析

3.1 传统医疗数据存储存在问题

传统的大量医疗数据存储在医院信息中心或区域卫生数据中心，使得中心负载增加，存在被攻击的安全隐患。同时医疗保健机构系统相互独立，产生的数据仅限于系统内部使用，导致个人健康记录分散在各个医疗健康系统内部，缺乏统一共享的模型。目前国内医疗是在医联体内采取分级诊疗的策略，如何在各个医联体系统基础上构建整合的分布式系统，使个人拥有健康记录的访问权限，是当前亟待解决的问题。

3.2 区块链存储健康大数据的挑战

目前区块链应用在医疗健康领域的目标是使个人拥有自身医疗大数据，构建中心化的分布式存储，个人拥有更多的控制权。通过访问权限的控制有选择地和医生或第 3 方医疗机构共享医疗数据。而区块链最先应用在比特币上，解决因金融机构发生欺诈或倒闭导致交易存在风险的问题，实现去中心化、不依赖第 3 方金融机构电子货币的发行交易。如果通过区块链底层技术实现医疗健康数据的存储，连接医生、患者以及医疗机构，需要着重理清其区别于比特币应用的特点。在比特币等数字化货币中，数字即是货币，数据量小，流程简单，交易方明确，数据链反复多重叠加成为可能。而医疗健康数据来自人体，与数字货币、合约文本不同，数据量大，单个数据大小是数字货币、合约文本的千万倍，相对于数字货币是巨块数据。同时不同于比特币的数字型数据，医疗健康数据类型复杂多样（包括字符型、布尔型、数值型、日期型、日期时间型、时间型、二进制），使其加密数据等措施更加复杂。区块链具有保护数据及提供数据可追溯性的特征，因此需要明确医疗健康领域数据操作的种类。如果将医疗健康数据索引和内容均列为区块链保护对象时，海量医疗数据内容在数据链反复多重叠加，将导致数据链过于庞大，储存容量和速度激增而难以实现。个人健康记录是以满足居民自身需要和健康管理为重点，内容不仅涉及疾病的诊断治疗过程，而且关注机体、心理、社会因素对健康的影响。其信息主要来源于居民生命过程中，与各类卫生服务机构发生接触所产生的所有卫生服务活动（或干预措施）的客观记录。因此必须着重解决何种数据存储到区块链中的问题。

4 个人健康记录分布式模型设计

4.1 采取 openEHR 标准

考虑到各个医疗健康机构内部标准不同，在应用层采取开放式电子健康记录（openEHR）标准进

行数据结构设计。openEHR 是由国际 openEHR 组织于 1999 年提出的开放式电子健康档案规范，将医疗领域知识从具体的临床信息中分离出来，从而保证信息模型的高可扩展性。openEHR 在欧洲、澳洲和日本等国家地区得到广泛应用，于 2008 年被国际标准组织接受，发展为 ISO 13606 – 2 标准。迄今很多国家的电子健康档案数据中心均采用该标准。为能够满足不同系统的访问需求，在应用层构建对等覆盖网络，对分布于各个医疗健康机构的 PHR 在区块链中采取 openEHR 标准进行存储。

4.2 PHR 主索引数据存储

个人健康档案的内容是从日常卫生服务记录中适当抽取的、与居民个人和健康管理、健康决策密切相关的重要信息，详细的卫生服务过程记录仍保留在卫生服务机构中，需要时可通过一定机制进行调阅查询。健康档案的基本内容主要由个人基本信息和主要卫生服务记录两部分组成。根据健康档案的基本概念和系统架构，如果将海量的个人健康记录信息都存储在区块链上势必会造成存储量增大。实际应用中县外就诊人群将控制在 10% 以内，医疗数据并无共享需求。以全覆盖的区块链应对少量跨域医疗需求，经济投入与需求应用不对称；区块链仅覆盖医疗数据索引可降低建设与运维压力，但医疗数据内容将脱离区块链保护。针对医疗健康记录数据量大、类型复杂的特点，为减轻存储运算负担，本研究创新地将 PHR 主索引数据存储在健康链上。区块链只是保护医疗数据索引和相对应内容的哈希值，医疗健康数据内容仍然采用原有方式存储，通过索引即可找出 PHR 存储位置。在应用层构建覆盖网络，采取对等网（Peer – to – peer，P2P）云架构存储。将 PHR 主索引数据存储在区块链上，其他数据以移动 P2P Cloud[12] 云的形式存储在医联体内。

4.3 系统架构

该方案利用区块链技术和链下对等云存储技术实现个人健康记录的安全存储和共享，称之为健康链，为保证个人数据安全，健康链采用私有链方式。个人通过授权在健康链上建立健康记录的主索引和存储位置。患者或用户能够向医疗机构申请查看医疗信息，包括电子病历、处方、最新医院和药店分布等。实现共享医疗信息功能，根据需求将医疗数据共享给医疗机构、医疗健康服务提供商、商业保险等机构。此外如果用户向医院提供权限，医生将能够获得该用户精确病史，通过医疗设备了解患者可能患有的疾病及用药等信息。经过授权后还可以访问分散在不同医疗机构的医疗数据，在药效分析、疾病防控等方面节约不必要的重复检查时间，政府可以进行更有序高效的监管。基于区块链接分布式架构，见图 1。

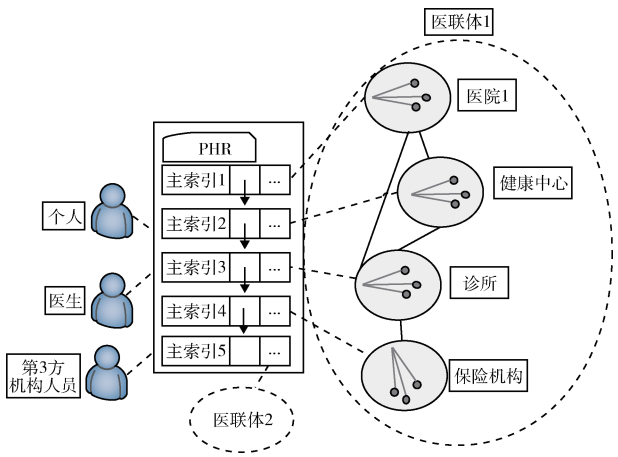

图 1 基于区块链的分布式体系架构

从数据管理角度，区块链的本质是构建在对等网络上、提供可信数据管理功能的数据库系统。体系架构中自下而上通常是数据层、网络层、安全层。（1）数据层。存储患者医疗健康记录的主索引、信息摘要和数据细节，在医联体的对等云存储中，结构相同的区块通过链式结构形成数据链。在健康链中利用时间戳来保证各区块按照时序链接，哈希函数保证数据不被篡改，公钥加密实现身份认证，这些技术共用保证健康链的安全。同时为实现新技术与现有技术的平稳升级，对医联体内医疗健康数据的存储保持原有方式。在区块链的主索引采用 openEHR 中的 openID 代码，保证个人编码的唯一性。（2）网络层。通过 P2P 协议完成分布式存储，利用 P2P 协议进行数据传输：将需要存储的数据分布到所有节点上进行存储；查询整个网络集群

中所有节点的最新数据，如果自身节点数据与大部分节点数据不一致，则更新自身数据与其一致。（3）安全层。对个人健康记录使用 hash 运算后用密钥签名，附带个人公钥，系统利用签名和公钥验证实现数据的不可篡改。

5 安全性分析

5.1 防篡改

系统每个时间戳生成一张表格，新的交易记录都记录在新表中，创建新表采用的方法是用当前表的顺序号、上一个表记录的 hash 值、系统时间戳，再找一个随机值、几个数据加在一起，hash 值满足一定条件，系统就接收这个新表，形成表的链式结构。新表的产生依赖于上一个表的数据和当前系统的时间戳，一旦新表产生，历史表的数据就无法被篡改。为防止上个表的数据被篡改，产生的新表需要依赖上一个表中所有记录的 hash 值，为提高对表中所有记录计算 hash 值的效率，采用 merkle 树对表中的所有记录进行 hash 计算。按照 P2P 网络结构自动更新网络集群中大部分节点维护的相同表。

5.2 有利于隐私保护和安全存储

健康链中不包含用户身份信息，只包含个人记录的编码和存储位置，而且是加密的，没有本人的加密密钥无法解密出明文，所以不能从健康链的公开信息中获取任何有关个人健康记录的真实数据。在区块链中的数据需通过授权并具有区块链安全措施的保证，真正数据的存取并不在区块链中，需要进一步根据地址再次查询，因此相当于两层保护。个人健康记录都加密存放在链下的云存储中，对记录的权限和粒度都只属于本人，可以将某个数据对象授权给某个实体，也可随时撤销其访问权限。医疗机构作为医疗记录的生产者可能保留本机构生产记录的原始数据，这对于患者来说只是其个人记录的部分信息。此外需要相关法律和机制防止医疗机构泄露用户医疗记录，以保护其隐私[2]。

6 结语

我国医疗信息共享机制不健全，医疗健康数据由各个标准不同的机构持有，对此本研究构建安全可信的个人健康记录分布式框架，使个人拥有对数据的访问权，实现医疗健康机构对 PHR 的互操作和安全访问。通过分析医疗健康领域应用区块链的特点，提出在应用层通过覆盖网络实现与原有数据库的集成。为减少区块链分布式冗余存储带来的空间开销，未来还需进一步设计合理、高效的区块链数据结构[13]，实现在区块链上进行数据存储和查询机制。同时还需针对医疗健康行业背景，采取提高系统吞吐率的共识机制[14-15]。区块链技术有助于实现医疗健康数据存储中建立信任网络、降低交易成本、统一数据标准、健康数据智能合约和安全访问。构建安全、互操作的 PHR 数据的分布式共享访问框架有助于医疗卫生体制改革和推进健康中国 2030 建设。

参考文献

1 祝烈煌，高峰，沈蒙，等. 区块链隐私保护研究综述[J] 计算机研究与发展，2017，54（10）：2170-2186.

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 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）：1555-1562.

4 Xia C，Song S. Resource Allocation in Hierarchical Distributed EHR System Based on Improved Poly-particle Swarm[C]. Hangzhou，China：International Conference on Biomedical Engineering & Informatics，2013：51-65.

5 He C，Fan X，Li Y. Toward Ubiquitous Healthcare Services With a Novel Efficient Cloud Platform[J]. IEEE Transactions on Bio-medical Engineering，2013，60（1）：230.

6 Sternly K S，Anbananthen K，Seldon L. A Ubiquitous Personal Health Record（uPHR）Framework[J]. International Conference on Advanced Computer Science and Electronics Information，2013（41）：423-427.

7 Safavi S，Shukur Z. Conceptual Privacy Framework for Health Information on Wearable Device[J]. Plos One，2014，9（12）：e114306.

（下转第43 页）

况，医务人员能快速调阅及掌握患者信息，根据手术麻醉需求迅速展开医疗操作。而操作过程中系统自动记录相应操作并生成医疗电子文书，医务人员可根据需要快速准确地查阅患者所有信息。

5 结语

重庆市中医院手术麻醉系统在实施期间，还经历前期准备项目计划书、手术室网络布线、设备安装调试、需求调研修改、接口调试、医护人员培训、测试运行、持续改进等过程[10]。系统实施过程中，医院设备处、信息科作为协调部门，多次召集医务部、麻醉科、手术室、多方系统研发公司等相关部门进行研讨、论证，相关使用科室提出问题、明确问题归属和解决问题的时间，以提高系统的实施效率。设备处、信息科作为院方代表，积极协调不同研发公司各类系统之间的接口制作。在专业需求方面医院麻醉科积极配合，特别是麻醉科主任从专业角度对麻醉单的信息展现直观性、录入方式方便性、麻醉相关表单内容丰富性提出详尽要求，从而构建既具有很强专业性又有医院特色的手术麻醉信息系统。为完善手术申请信息，规范医生填写及提交手术申请的行为，医务部应发文对医生提交手术申请提出更加规范的要求，保障工作流程顺利进行。各部门通力合作才能确保手术麻醉系统可以在较短时间上线。

参考文献

1 董继红，孙新宇，金冉，等. 手麻系统在手术室压疮防护与监管中的应用［J］. 国际护理学杂志，2018，37（5）：623－625.

2 李爱清，邵伟. 我院感染监测系统的实施［J］. 中国医疗设备，2014，29（4）：84－85.

3 何伟，王涛，马艳凯，等. 手术麻醉信息系统对麻醉文书质量的影响［J］. 中国病案，2018，19（1）：37－39.

4 金杨君，应争先，徐星娥，等. 手术室麻醉药品闭环管理系统的设计与应用［J］. 现代医院管理，2018，16（2）：7－9.

5 孟凡星，周霞，赵琨浩. 浅谈手术室麻醉废气排放系统［J］. 中国医院建筑与装备，2018，4（2）：88－89.

6 刘蓓，谭军. 手术麻醉信息系统在医学临床中的应用［J］. 数字化用户，2017，47（1）：144－145.

7 张歆婷. 医院 docare 手术麻醉临床信息系统的组成与应用——以宜兴市人民医院为例［J］. 今日科技，2017，10（5）：60－61.

8 李苏敏，费惠. 手术麻醉信息系统提高首台手术准时率效果观察［J］. 现代实用医学，2016，28（5）：687－688.

9 李立，周鑫. 手术麻醉信息系统应用［J］. 现代仪器与医疗，2015，21（3）：25－26.

10 刘月辉，曹秀堂，姚远，等. 医疗质量指标信息化过程监测与绩效考核［J］. 中国卫生质量管理，2017，24（6）：23－25.

（上接第 35 页）

8 Spil T, Klein R. Personal Health Records Success: why google health failed and what does that mean for microsoft healthvault? ［C］. USA: Hawaii International Conference on System Sciences. IEEE Computer Society, 2013: 2818－2827.

9 Kyazze M, Wesson J, Naude K. The Design and Implementation of a Ubiquitous Personal Health Record System for South Africa ［J］. Studies in Health Technology & Informatics, 2014, 206 (206): 29－41.

10 Kemkar O S, Kalode P. Formulation of Distributed Electronic Patient Record (DEPR) System Using Openemr Concept ［J］. International Journal of Engineering Innovation & Research, 2015, 4 (1): 85－89.

11 Roehrs A, Da C C, Rosa Righi R D. OmniPHR: a distributed architecture model to integrate personal health records ［J］. Journal of Biomedical Informatics, 2017 (71): 70.

12 邢丹，姚俊明. P2P Cloud 混合网络基础上的远程医疗架构［J］. 医学信息学杂志，2017，38（4）：32－35.

13 王继业，高灵超，董爱强，等. 基于区块链的数据安全共享网络体系研究［J］. 计算机研究与发展，2017，54（4）：742－749.

14 邵奇峰，金澈清，张召，等. 区块链技术：架构及进展［J］. 计算机学报，2018（5）：1－21.

15 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.