基于区块链的医疗数据共享模型研究

薛腾飞 [1,2] 傅群超 [1,2] 王 枞 [1,2] 王新宴 [3]

摘 要 根据医疗行业现状, 不难发现各医疗机构间共享数据困难, 因为医疗数据的校验、保存和同步一直是一个难点. 病人、医生以及研究人员在访问和共享医疗数据时存在严格的限制, 这一过程需要花费大量的资源和时间用于权限审查和数据校验. 本文提出一个基于区块链的医疗数据共享模型, 具有去中心化、安全可信、集体维护、不可篡改等特点, 适用于解决各医疗机构数据共享的难题. 本文详细介绍了模型的组件以及实现原理. 将现有医疗机构进行分类, 配合使用改进的共识机制实现了方便、安全、快捷的数据共享. 此外, 通过对比医疗数据共享存在的问题, 分析了本模型的优势以及带来的影响.

关键词 医疗数据, 区块链, 共识机制, 共享模型

引用格式 薛腾飞, 傅群超, 王枞, 王新宴. 基于区块链的医疗数据共享模型研究. 自动化学报, 2017, **43**(9): 1555−1562

DOI 10.16383/j.aas.2017.c160661

A Medical Data Sharing Model via Blockchain

XUE Teng-Fei[1,2] FU Qun-Chao[1,2] WANG Cong[1,2] WANG Xin-Yan[3]

Abstract According to the status quo of medical industry, verification, storage and synchronization of clinical data are difficult, therefore, clinic data sharing between institutions become a challenging task. There are many restrictions in data access and sharing for patients, doctors and even researchers, which results in a high cost of both resources and time for authority authentication and verification. To solve this problem, we propose a blockchain-based medical data sharing model, with advantages of decentralization, high security, collective maintenance and tamper resistance. We discuss the critical principles and components of this model in detail. Furthermore, we improve the consensus mechanism so as to better match different types of medical institutions for a more convenient, secure and faster data sharing. In addition, the merits and impacts of this model are presented and analyzed by comparisons in terms of existing issues in medical data.

Key words Medical data, blockchain, consensus mechanism, sharing model

Citation Xue Teng-Fei, Fu Qun-Chao, Wang Cong, Wang Xin-Yan. A medical data sharing model via blockchain. *Acta Automatica Sinica*, 2017, **43**(9): 1555−1562

目前全球解决医疗健康信任问题的应用很少, 主要由于医疗记录的校验、保存和同步一直是一个难点. 当病人、医生在访问和共享医疗数据的时候会受到严格的限制, 需要花费大量的资源和时间进行权限审查和数据校验. 这使得用户获得医疗数据十分困难, 每次使用时需要向类似于健康信息交易所 (Health information exchange, HIE) 和全员人口数据库 (APCD) 这样的组织机构提交申请. 整个响应过程存在很多问题, 例如响应缓慢、数据可被篡改、数据传输不安全等. 这些都严重阻碍了智慧医疗和医疗大数据的发展.

截止到 2015 年, 至少有 10% 的医疗记录实现了电子化存储, 较 2008 年有 90% 的增长[1] (图 1). 2011 年全部类别的医院超过 20% 都开始建设基础的电子健康记录系统 (Electronic health record system, EHRS) (图 2). 这说明医疗数据信息化已经相对成熟, 例如类似于 EHRS 的还有医院信息系统 (Hospital information system, HIS)、放射科信息管理系统 (Radio information management system, RIS)、医学数字成像和通信系统 (Digital imaging and communications, DICOM)、影像归档和通信系统 (Picture archiving and communication system, PACS). 这些系统都被设计用来解决医疗信息存储和共享等问题. 然而区块链技术的诞生, 改变了这种医疗数据集中存储, 需通过组织机构完成权限审查和数据校验的结构, 提出了一种可去除中间机构、增加数据安全性、节约时间和成本的全新模式.

收稿日期 2016-09-18 录用日期 2017-04-21
Manuscript received September 18, 2016; accepted April 21, 2017
科技基础性工作专项 (2015FY111700-06) 资助
Supported by Science and Technology Basic Work (2015FY111700-06)
本文责任编委 王飞跃
Recommended by Associate Editor WANG Fei-Yue
1. 北京邮电大学软件学院 北京 100876 2. 可信分布式计算与服务教育部重点实验室 北京 100876 3. 空军总医院 北京 100142
1. School of Software, Beijing University of Posts and Telecommunications, Beijing 100876 2. Key Laboratory of Trustworthy Distributed Computing and Service, Ministry of Education, Beijing 100876 3. Air Force General Hospital, Beijing 100142

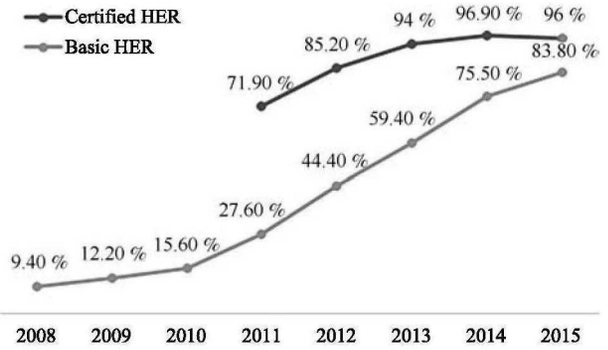

图 1 2008～2015 年护理医院采用基础版 EHR 与采用标准版 EHR 的占比情况[1]

Fig. 1 Percent of non-federal acute hospitals with adoption of at least a basic EHR with notes system and possession of a certified EHR: 2008～2015[1]

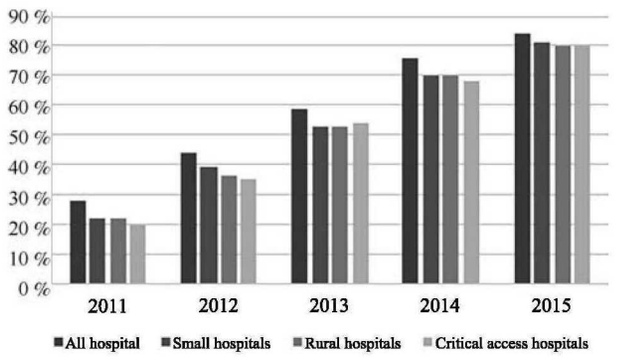

图 2 不同类型医院采用基础版 HER 的百分比情况[1]

Fig. 2 Percent of non-federal acute care hospitals with adoption of at least a basic EHR system by hospital type[1]

区块链技术[2] 可以帮助医生、病人和研究人员快速安全地认证权限, 实现自由的数据访问和分享. 因此, 目前区块链在医疗领域的应用和研究备受关注, 世界上许多公司和研究机构均参与其中. 位于瑞士的 Healthbank 公司是全球数字健康的创新者, 通过区块链采用透明化的方式处理健康系统的事务, 保证了健康数据存储的绝对安全[3]. Gem Health 联手飞利浦区块链实验室构建了一个包含区块链的健康生态系统, 推动全球医疗一体化, 使得医疗健康更加个性化和平民化[4]. 飞利浦医疗与 Tierion 公司成立新的科研项目, 研究区块链技术是否可以增加医疗健康产业中数据交换的价值. Bithealth 机构研究如何采用区块链记录和认证全球的医疗健康数据.

本文介绍和设计了一个基于区块链的医疗数据分享模型 (Medical data share model, MDSM), 帮助解决医疗数据存储集中、安全共享难、数据可信度过度依赖组织机构等问题. 实现去中心化、安全、不可篡改的医疗数据分享. 该模型的主要特点有:

1) 医疗机构联盟服务器群 (Medical institution federate servers, MIFS) 和审计联盟服务器群 (Auditing federate servers, AFS): 根据医疗资源分布的现状可以发现, 主要的医疗信息服务和主要的数据存储节点都部署在大医院或者核心医疗机构. 因此可以将医疗机构划分等级, 高等级的机构节点加入 MIFS 成为代理, 第二等级的机构加入 AFS 作为审计校验的节点. 模型中采用改进的股份授权证明机制 (Delegate proof of stake, DPOS) 实现节点之间的共识.

2) 医疗记录存储结构: 自定义一套层级存储结构, 可以高效方便地传播. 最后将所有数据的 Merkle 根锚定到比特币区块链, 实现真正的不可篡改和不可抵赖.

3) 分布式数据库系统 (Distributed database system, DDBS): 医疗数据文件将加密存储在数据库中, 解决了数据集中存储在各个医疗机构的数据服务器上的问题, 同时也减轻了区块链上的数据存储和高频访问的压力.

本文内容安排如下: 第 1 节介绍基于区块链的医疗领域的研究情况以及相关技术介绍; 第 2 节详细阐述医疗数据共享模型的各环节; 第 3 节通过与现有问题的对照以及其他模型的比较进行模型评估. 第 4 节对本文工作的总结和展望.

1 相关工作

目前, 关于区块链的研究很多, 但结合医疗领域的研究相对较少, 方向主要有医疗信息保护、医疗支付、医疗数据应用、医疗数据存储分享、医疗信息交易、预测分析等. 区块链技术的快速发展引起了政府部门、金融机构、企业和资本市场的广泛关注. 为推动区块链技术和产业发展, 国务院工业和信息化部信息化和软件服务业司指导中国电子技术标准化研究院, 联合蚂蚁金融云、万向控股、微众银行等骨干企业, 开展区块链技术和应用发展趋势专题研究, 发布了《中国区块链技术和应用发展白皮书 (2016)》[5]. Lvan 等提出了一个基于区块链安全存储病人医疗记录的方法[6]. Shrier 等提出采用美国麻省理工学院的 OPAL/Enigma 加密平台, 配合区块链技术可以创建一个用于存储和分析医疗数据的安全环境[7]. Kuo 等采用区块链私链网络技术, 创建了一个跨机构的医疗健康预测模型[8]. Ekblaw 等提出一个新颖的去中心化电子病历管理系统[9]. 还有一些研究对使用区块链存储电子病例[9−10] 和健康相关事务[11] 进行了评估. 对比发现国内区块链结合

医疗领域的研究刚刚起步, 国外的研究相对更多. 我们创新地提出并设计了基于区块链的医疗数据共享模型.

1.1　区块链和股份授权证明机制 (DPOS)

目前尚未形成一个公认的区块链定义. 狭义地讲, 区块链是一种按照时间顺序将有效数据区块以链式形式组合而成的数据结构, 并通过密码学方式保证不可篡改和不可抵赖的、可附加的去中心化共享总账 (Decentralized shared ledger). 广义的区块链技术则是利用加密链式区块结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用自动化脚本代码 (智能合约) 来编程和操作数据的一种全新的去中心化基础架构与分布式计算范式[12]. 区块链的基本原理简单易懂, 包括三个主要组件:

1) 电子交易: 记录账本的变化. 任何类型的有效交易信息都会通过数字化或加密方式来确保准确性和真实性.

2) 区块: 一个存储所有交易信息的数据结构, 包括区块头和区块体.

3) 链: 包含按时间顺序生成的区块, 记录状态的改变.

DPOS 被称为是更有效、更去中心化、更灵活的共识机制[12]. 它允许所有的股东节点都具有投票权, 通过公平民主的方式票选出 101 个权益代表. 并可以在后续过程中根据代表的表现自由重投选票. 有效地降低了参与记账节点的数量, 实现快速共识验证. DPOS 的基本工作思路是:

1) 每一个股东节点都需要把票投给信任的代表. 得票数最高的且愿意成为代表的前 101 个节点将轮流记账生成新的区块.

2) 如果授权代表生产了错误的区块或者错过了签署新区块, 那么将由下一个代表代替完成. 并有可能被股东节点投出代表席.

3) 想成为代表, 需要在网上使用公钥注册一个 32 位的唯一编码, 每一条记录的头部会引用这个标识数字.

4) 每一个股东都有一个表现指示器来记录代表的行为. 如果错过很多个区块的签署或者签署过错误区块, 指示器会建议选取别的代表.

1.2　哈希算法与 Merkle 树

哈希算法是一项在通信领域很基本也很重要的技术. 通过数学算法将大小不一致的数据映射成固定大小的字符串. 从另一个角度看, 加密的哈希算法是一个单项函数, 即可以很容易地计算出数据的哈希值, 但反过来根据哈希值很难推算出原数据, 这一特性对于区块链非常重要. Merkle 树是一个基于哈希算法的数据结构, 它的特点是每一个非叶子节点都是其叶子节点的哈希值[13]. 在点对点的网络中, 可以使用 Merkle 树来验证数据是否被篡改或接收到的数据是否损坏. 在区块链中生成的所有记录通过 Merkle 树的哈希过程生成唯一的 Merkle 根, 存储在区块链的头部.

2　医疗数据共享模型

医疗数据共享模型包括许多重要的组件, 如图 3 所示.

根据医疗行业现状, 我们设定用户分为不同的类型: 完备级、轻量级和普通用户. 其中轻量级的用户将使用网站或者移动应用查看他们的医疗数据并且可以授权或撤销数据的访问权限. 我们将用户使用的客户端分为 3 个类型:

1) 完备级客户端: 存储所有记录 (医疗机构可以提供接口对外服务);

2) 轻量级客户端: 不保存记录, 需要向其他节点或者 MIFS 查询 (医疗机构可以提供查询接口, 个人用户可以完成授权等操作);

3) 在线客户端: 网页模式浏览, 例如, 用户在医疗机构就诊结束时申请数据记录上传, 医院会通过完备级的客户端对 MIFS 申报. 当用户再次就诊时可以通过轻量级客户端授权查询获得自己的历史记录. 在线客户端则是为用户提供简单自查阅的服务.

行业背景研究发现, 医疗大数据中心基本都建设在重点医疗机构. 小规模的医疗机构一方面流量小, 产生的医疗数据少; 另一方面数据中心建设也不够完善, 没有很强的数据处理能力. 因此我们设计了 MIFS 和 AFS 两套联盟服务器群, 配合使用改进的 DPOS 共识机制, 可以有效地利用当前医疗机构现状实现去中心化、安全、快捷可追溯的医疗数据共享. 此外, 很多医疗数据文件体积较大, 例如病人的住院记录文档、处方、医疗视频和图片等, 这类数据将使用所有者的公钥加密存储在分布式数据库中. 为了保证记录内容可信、未篡改, 模型记录所有医疗数据的摘要并采用分层机构存储. 将数据哈希值存放在 Item 结构中, 再计算出每个 Item 的哈希值放入 Item 块结构中, 这样做可以有效减少搜索空间, 加快用户对记录的校验速度.

如图 4 所示, 数据块由多个 Item 块构成, 层层计算哈希值会得到这一数据块的 Merkle 根, 每 1 分钟进行一次. 由于比特币区块链采用工作量证明机制 (Proof of work, PoW), 稳定在每 10 分钟生成一

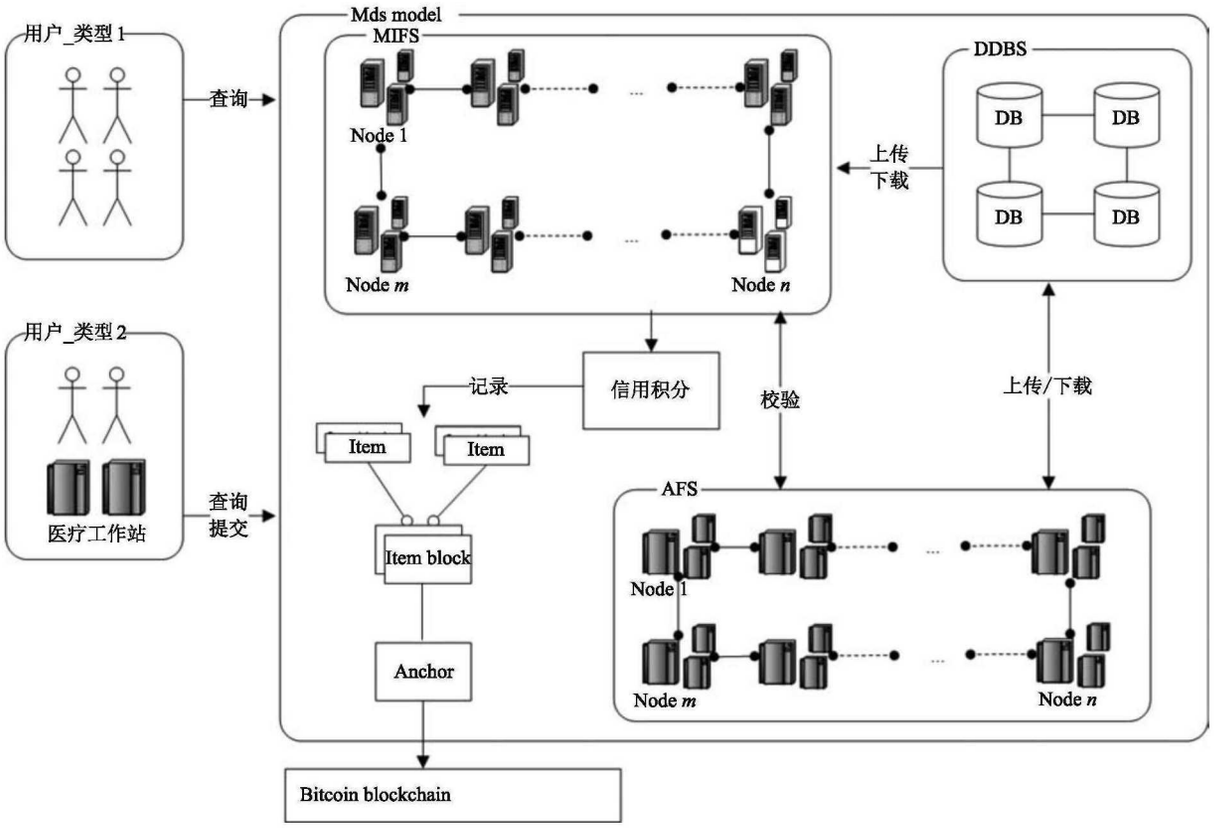

图 3 医疗数据共享模型结构

Fig. 3 The framework of the medical data sharing model

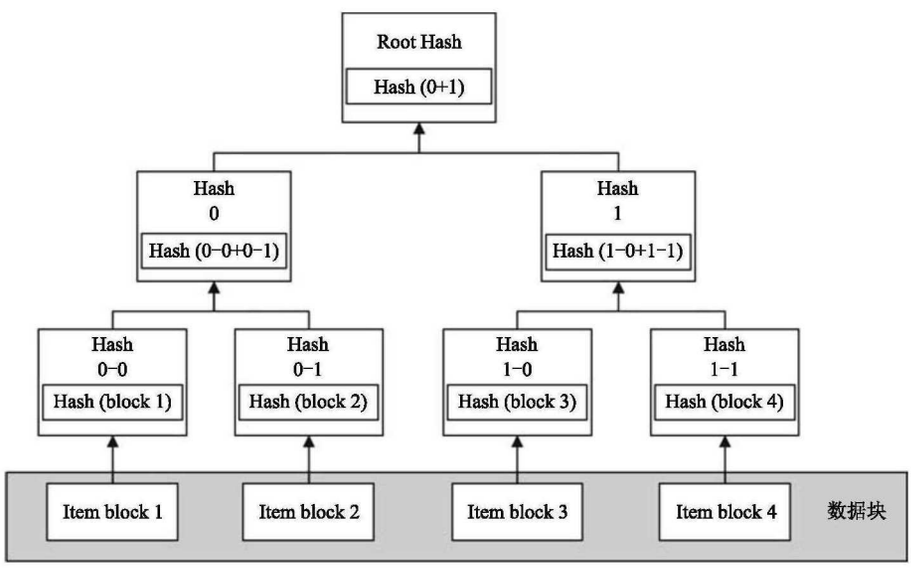

图 4 存储记录信息的 Merkle 树

Fig. 4 Merkle tree of the storage structure

个区块, 所以在模型中每 10 分钟冻结数据, 由 MIFS 中的当值代表提交生成的 Merkle 根到比特币区块链中, 形式类似于提交一笔比特币交易. 这样可以实现真正意义上的不可篡改, 因为比特币区块链相对于我们的模型更具公信力. 每个 Item 块都只存储 Item 的哈希值以及一个头部信息 (如图 5), 这样不仅利于每个块在点对点网络的传播, 也减少了数据校验的成本. 每个 Item 中可存储 10 条医疗数据, 每条都包含三个信息: 数据所有者公钥、元数据、数据摘要.

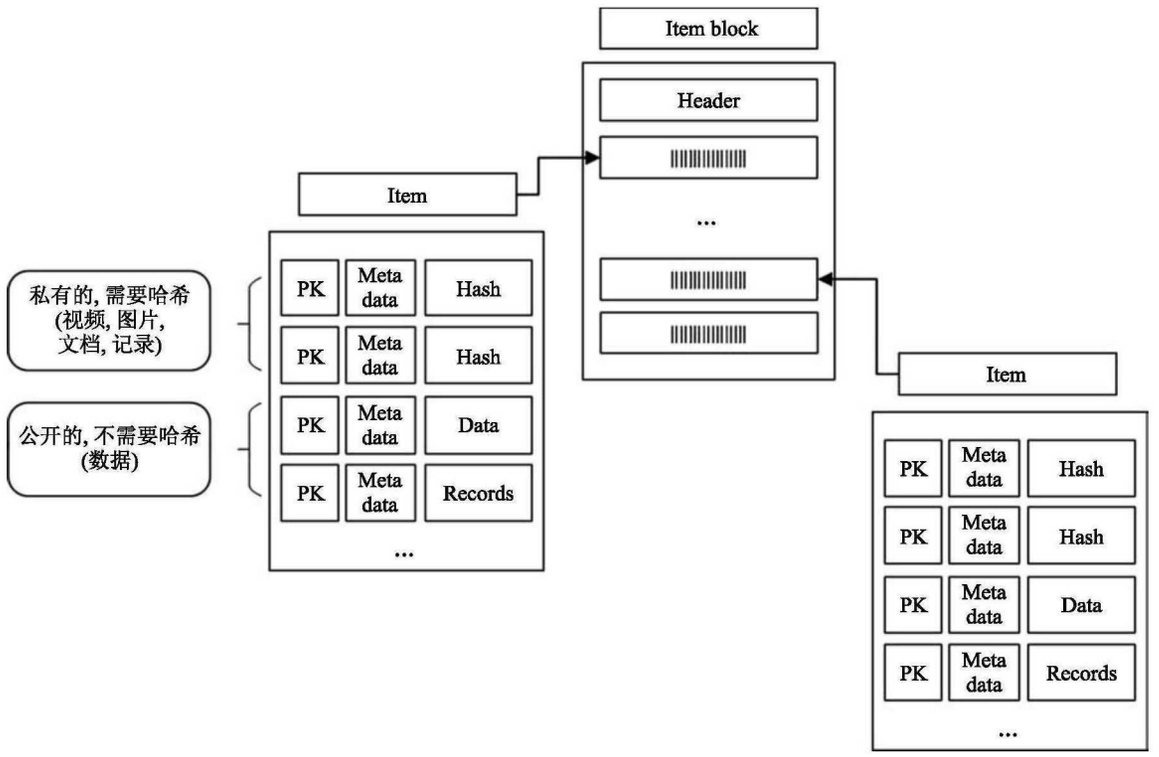

图 5　医疗数据存储层级结构

Fig. 5　Medical data storage hierarchy structure and details

2.1　医疗数据存储机构 Item 和 Item 块

与比特币类似, 在 Item 中存储的每条医疗数据不得大于 100 KB, 因此在用户不愿对数据加密且数据量很小的情况下, 数据摘要部分可以存储医疗数据原文. 数据类型可能是一个链接、一段文本、一个小图片或者一小段检验视频等. 另外当用户希望数据加密或医疗数据文件很大时, 解决方案是一边计算数据摘要并将其存储在 Item 中, 一边将文件加密存储在分布式数据库系统中. 这样做使得 Item 中的数据摘要不仅可以对数据进行完整性校验, 同时可以作为在数据库中查找数据的索引. 作为绑定用户的唯一标识, 公钥字段则可以很方便地查到某用户发布的数据记录以及是否拥有访问权限. 元数据部分存放数据的电子资源, 例如生成时间戳等信息.

2.2　医疗机构联盟服务器、校验联盟服务器和改进的 DPOS

现阶段我国对医疗机构的评级采用卫生部 1994 年印发的《医疗机构基本标准》和 1989 年印发的《医院分级管理办法》, 从硬件条件、社会效益、服务质量等多个维度进行评估, 百分制评分. 本模型采用这套评分体系作为评价医疗机构的依据. DPOS 共识机制采用投票的方式选出 101 个权益代表, 但这种方式应用于医疗数据共享模型有明显的问题. 这样的初始化不能保证选出的权益代表是具有影响力的医疗机构, 不具备提供记账、查询等服务的能力. 模型改进了 DPOS 的初始化方法, 根据现阶段国家对医疗机构的评级和信息中心的配置规模将医疗机构进行初始排名, 排在前 101 位的信息中心被指定为 MIFS 中的一员, 轮流负责把提交上来的请求记录到 Item 中并用自己的私钥签名. 这类医疗机构包括高级别医院 (三甲)、妇幼保健院、急救中心、高级别临床检测中心等. 排在第 101 位之后的 20 位被指定为 AFS, 轮流校验每个被签署的区块是否真实有效. 其余的医疗中心使用完备的客户端向用户提供服务. 这样有效地解决了医疗数据共享模型初始化无效的问题. 医疗机构排名的依据被称为信用积分, 积分的高低代表了医疗机构积的综合实力, 可以为负数但不能转赠和退还. MIFS 和 AFS 中的节点对外提供服务可以增加信用积分. 如果 MIFS 中的节点签署无效区块或者作假会丢失信用积分, 积分低于阈值将被踢出 MIFS, 由 AFS 中积分较高的节点填补. 同样地, AFS 中的节点错误审计、作弊等也将扣除信用积分. 信用积分的加入充分调动了医疗机构主动参与评审的积极性, 也将成为评估医疗机构的重要依据. 因为各大医疗机构本身具备很强的公信力和政府背书, 同时可以方便直接地将授权的医疗数据进行处理, 所以将其初始设定成 101 个权

益代表节点是十分合理的. 下面是 MIFS 具体工作过程:

步骤 1. 用户提记录请求, 并提交公钥作为标识.

步骤 2. 某代表节点接受请求.

步骤 3. 某代表节点广播已接受请求.

步骤 4. 用户提交记录, 如果不希望公开数据, 使用公钥对数据进行加密.

步骤 5. 当值的代表节点根据用户公钥将记录添加入 Item.

步骤 6. 当值的代表节点广播 Item 确认信息, 并将需要上传的大文件存入分布式数据库.

步骤 7. 校验代表节点对记录进行校验, 其他节点更新数据.

步骤 8. 每隔 1 分钟检查一下 Item block 的数量, 达到 10 个则组成一个数据块, 并计算该数据块的 mertle 根.

步骤 9. 每隔 10 分钟将所有新生成的数据块的 merkle 根锚定到比特币区块链.

步骤 10. 返回步骤 1.

2.3 数据共享与访问控制

数据所有者将医疗数据加密存储在分布式数据库中, 模型采用密码学中代理重加密 (Proxy re-encryption)[14−15] 机制来实现对医疗数据的访问控制和共享. 因为模型基于区块链技术是一个去中心化的应用场景, 没有可信的第三方也就不存在传统重加密场景中的唯一的代理角色. AFS 和 MIFS 中的任何节点都可以充当代理完成重加密的操作, 作为报酬可以获得相应的信用积分. 例如, 当医生对病人数据有访问需求时, 病人将对应于医生查询的部分医疗数据做正常的加密操作, 并且产生对应于自己到该医生的代理重加密密钥; AFS 和 MIFS 中的节点竞争代理重加密权利, 病人选取竞争列表中的一个服务节点, 并将对应的重加密密钥发送给该节点, 代理重加密节点根据密文和重加密密钥如实完成重加密操作, 最后将密文存入数据库, 索引标识是医生的公钥. 此时医生就可以访问数据库并用自己的私钥解密获取医疗数据. 通过代理重加密可以方便地实现医疗数据的共享与控制, 达到对于数据所有者的权利委托. 本模型采用文献 [15] 中的格基算法设计协议.

1) 生成随机矩阵 $A \in Z_q^{n*n}$, 选择安全整数 q, n.

2) 生成公私钥对: 公钥 $pk = P$, $P = R - A$, $S \in Z_q^{n*1}$, 其中 R, S 是高斯参数, 则私钥 $sk = S$.

3) 加密算法:

$$c = (c_1, c_2) = \left(e_1 A + e_2, e_1 P + e_3 + m \cdot \left\lfloor \frac{q}{2} \right\rfloor\right)$$

其中, e_1, e_2, e_3 是误差参数.

4) 解密算法:

$$m = c_1 S + c_2$$

根据与 0 的距离远近判断为 0 还是为 1.

5) 重加密密钥生成算法:

$$rk_{a\to b} = (P_B, Q)$$

$$Q = \begin{bmatrix} X & -XS_B + E + S_A \\ 0 & I \end{bmatrix}$$

其中, X 是随机矩阵, E 是噪声.

6) 重加密算法:

$$(c_1', c_2') = h_1(A, P_B) + (h_2, h_3) + (c_1, c_2) \cdot Q$$

其中, h_1, h_2, h_3 是选自误差分布.

3 评估

采用对照分析的方法来评估提出的医疗数据共享模型, 一方面, 通过与现有研究成果中的其他解决方案的对比, 分析我们模型的优缺点 (如表 1); 另一方面, 通过与现存医疗数据问题的对比, 分析模型的优势以及影响 (如表 2)[10, 16].

表 1 从五个角度将模型与几种研究成果进行对比, 可以看出本模型整体上具有一定优势. 这五个角度均是五者描述中共同提到的特性. 但模型与其他研

表 1 模型与现有解决方案对比

Table 1 The model is compared to existing solutions

	基于区块链	共识机制	专为医疗问题设计	减轻主链压力	私有链
Factom[17]	否	无	否	是	否
MedRec[9]	是	POW	是	否	否
ModelChain[8]	是	POI	是	否	是
MDSM	是	改进 DPOS	是	是	是

表 2　当前面临的问题以及模型应对的方法

Table 2　The problems faced and the coping methods of the model

类型	面临问题	模型应对方法及分析
隐私和安全	信任和访问控制	提倡医疗数据电子化, 医疗数据由可信的代理负责记录
	黑客攻击和医疗数据保护	采用非对称加密技术加密数据
	不可抵赖性	周期性将信息锚定到比特币公链, 借助公链实现不可篡改
医疗数据滥用和诈骗	被滥用, 追责困难	模型是轮流责任制, 采用区块链技术方便追责
	记录难以辨识	数字化电子病历即时存储, 机器可识别易辨认
	不正当收费, 虚假声明等	每种类型客户端均可快捷查询, 获得统一且可信的结果
用户参与度	用户无法管理自身的健康数据	完全由用户管理自己的医疗数据, 代理重加密实现权利委托
	公共卫生相关研究与用户无直接关联	开放自己的医疗数据, 做为研究素材推动相关研究
互操作性, 可访问性, 数据完整性	数据分别存储在不同的数据中心, 形成数据孤岛共享困难	模型打通各医疗机构之间的数据孤岛, 实现方便的数据互操作
	各机构权限不明确, 数据所属权不明确	医疗联合服务器负责代理记账, 审计服务器负责校验记账. 客户端分不同类型, 支持不同的访问限制. 另外, 明确各个医疗机构的职责, 方便外部审计.
	数据容易丢失, 造成数据不完整	分布式的存储节点, 保证数据的多重备份
规则	不同的数据标准和共享规则	统一的数据查询接口, 统一的数据标准, 可以实时数据共享

究成果相比同样有许多弱点和需要改进的地方. 例如不具备预测模块、不具备机器学习算法的能力以及不具备更广泛的数据存储能力.

4　总结和展望

随着区块链技术的快速发展, 这一新兴技术会逐步成为热点研究课题. 医疗领域区块链的研究已经备受关注, 本文提出的医疗数据共享模型可以帮助现有医疗机构的数据中心进行转型, 以满足越来越多的医疗数据安全存储、共享等需求. MIFS 和 AFS 的设计可以与改进的 DPOS 机制有效配合, 为实现智慧医疗和医疗大数据构建基础平台. 但这一设计在具体实施中会遇到问题和挑战, 需要随着区块链技术的发展不断完善. 本文希望可以对未来的研究提供有益的启发. 文中涉及到的分布式存储数据库, 实现主要采用 LevelDB 技术, 设计细节还有待进一步完善.

References

1 Charles D, Gabriel M, Furukawa M F. Adoption of electronic health record systems among U.S. non-federal acute care hospitals: 2008-2012. *ONC data brief*, 2013, **9**: 1−9

2 Nakamoto S. Bitcoin: a peer-to-peer electronic cash system [Online], available: http://bitcoin.org/bitcoin.pdf, June 12, 2016

3 Healthbank [Online], available: http://www.healthbank.coop, August 18, 2016

4 Health [Online], available: https://gem.co/health, January 22, 2016

5 China Blockchain Development Forum. China Blockchain Technology and Application Development White Paper (2016) [Online], available: http://chainb.com/download/工信部−中国区块链技术和应用发展白皮书 1014.pdf, October 18, 2016
(中国区块链技术和产业发展论坛. 中国区块链技术和应用发展白皮书 (2016) [Online], available: http://chainb.com/download/工信部−中国区块链技术和应用发展白皮书 1014.pdf, October 18, 2016)

6 Lvan D. Moving toward a blockchain-based method for the secure storage of patient records [Online], available: http://www.healthit.gov/sites/default/files/9-16-drew_ivan_20160804_blockchain_for_healthcare_final.pdf, August 4, 2016

7 Shrier A A, Chang A, Diakun-thibault N, Forni L, Landa F, Mayo J, van Riezen R. Blockchain and Health IT: Algorithms, Privacy, and Data. [Online], available: http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/1-78-blockchainandhealthitalgorithmsprivacydata_whitepaper.pdf, September 18, 2016

8 Kuo T T, Hsu C N, Ohno-Machado L. ModelChain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks [Online], available: https://www.healthit.gov/sites/default/files/10-30-ucsd-dbmi-onc-blockchain-challenge.pdf, January 22, 2016.

9 Ekblaw A, Azaria A, Halamka J D, Lippman A. A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data. In: Proceedings of the 2016 IEEE of International Conference on Open and Big Data, 2016. 25−30

10 Yuan B, Lin W, McDonnell C. Blockchains and electronic health records [Online], available: http://mcdonnell.mit.edu/blockchain_ehr.pdf, May 4, 2016

11 Witchey N J. Healthcare Transaction Validation Via Blockchain Proof-of-Work, Systems and Methods: U.S. Patent 2015/0332283, November 2015.

12 Yuan Yong, Wang Fei-Yue. Blockchain: the state of the art and future trends. *Acta Automatica Sinica*, 2016, **42**(4): 481−494
(袁勇, 王飞跃. 区块链技术发展现状与展望. 自动化学报, 2016, **42**(4): 481−494)

13 Merkle R C. A digital signature based on a conventional encryption function. In: Proceedings of the 1987 Conference on the Theory and Applications of Cryptographic Techniques. Berlin Heidelberg, Germany: Springer, 1987. 369−378

14 Blaze M, Bleumer G, Strauss M. Divertible protocols and atomic proxy cryptography. In: Proceedings of the 1998 International Conference on the Theory and Applications of Cryptographic Techniques. Berlin Heidelberg, Germany: Springer, 1998. 127−144

15 Aono Y, Boyen X, Phong L T, Wang L. Key-private proxy re-encryption under LWE. In: Proceedings of the 2013 International Conference on Cryptology in India. Cham, Germany: Springer International Publishing, 2013. 1−18

16 Blockchain: the chain of trust and its potential to transform healthcare-our point of view [Online], available: http://www.healthit.gov/sites/default/files/8-31-blockchain-ibm_ideation-challenge_aug8.pdf, August 8, 2016.

17 Snow P, Deery B, Lu J, Johnston D, Kirby P. Factom: business processes secured by immutable audit trails on the blockchain [Online], available: http://bravenewcoin.com/assets/Whitepapers/Factom-Whitepaper.pdf, November 17, 2014.

薛腾飞 北京邮电大学软件学院博士研究生. 主要研究方向为区块链应用和共识机制. 本文通信作者.
E-mail: tffeiba@126.com
(**XUE Teng-Fei** Ph. D. candidate at the School of Software, Beijing University of Posts and Telecommunications. His research interest covers blockchain application and consensus mechanism. Corresponding author of this paper.)

傅群超 北京邮电大学软件学院博士研究生. 主要研究方向为医学文本处理.
E-mail: fu92811@163.com
(**FU Qun-Chao** Ph. D. candidate at the School of Software, Beijing University of Posts and Telecommunications. His main research interest is medical text processing.)

王 枞 北京邮电大学软件学院教授. 主要研究方向为医疗大数据分析, 智能控制与网络信息安全.
E-mail: huhx@sina.com
(**WANG Cong** Professor at the School of Software, Beijing University of Posts and Telecommunications. His research interest covers medical data analysis, intelligent control, and network information security.)

王新宴 国家科技基础条件平台人口与健康空军总医院平台中心主任, 空军总医院特诊科主任. 主要研究方向为高血压的精准诊断, 健康溯源大队列研究.
E-mail: wangxinyan@china.com
(**WANG Xin-Yan** Director of the Center for National Science and Technology Basic Condition Platform Population and Health Air Force General Hospital Platform and director of the Air Force General Hospital Special Clinic Department. Her research interest covers accurate diagnosis and treatment of hypertension and study of large queues on the health traceability.)