计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400240

基于区块链的患者在线交流模型

陈先来[1,2]　赵晓宇[3]　曾工棉[3]　安　莹[1,2]
1 中南大学大数据研究院　长沙 410083
2 中南大学医疗大数据应用技术国家工程实验室　长沙 410083
3 中南大学生命科学学院　长沙 410083
(chenxianlai@csu.edu.cn)

摘　要　针对目前互联网上虚假信息盛行,患者在互联网上交流时无法保证共享信息真实性的问题,提出了一种基于区块链的患者在线交流模型,患者可以匿名与其他患者共享真实的医疗数据并进行交流。首先,使用患者的数字身份保护隐私,将患者交流所需要的医疗摘要数据上传至区块链,并且公开全部数据以供检索,可以使患者检索到需要的病例而不会定位到具体的患者;其次,为了避免授权人员的恶意上传行为,设定智能合约对数据上传进行多重身份认证,医生和患者相互制约,保证链上数据全部真实可靠;最后,改进的 RAFT 共识算法可以快速识别拜占庭节点从而更好地使区块链达成共识。通过实验对模型性能进行评估,结果表明该模型在保证患者隐私的前提下,可以进行医疗数据的共享,满足患者在线交流需求。

关键词:区块链;医疗数据共享;智能合约;共识机制;患者交流
中图法分类号　TP311.13

Online Patient Communication Model Based on Blockchain

CHEN Xian-lai[1,2],ZHAO Xiao-yu[3],ZENG Gong-mian[3] and AN Ying[1,2]
1 Big Data Institute,Central South University,Changsha 410083,China
2 National Engineering Laboratory for Medical Big Data Application Technology,Central South University,Changsha 410083,China
3 Life Science College,Central South University,Changsha 410083,China

Abstract　At present,false information is prevalent on the Internet,and the authenticity of shared information cannot be guaranteed when patients communicate on the Internet. In order to solve this problem,a blockchain-based online patient communication model is proposed,and patients can anonymously share real medical data and communicate with other patients. Firstly,the patient's digital identity is used to protect privacy,the medical summary data needed for patient communication are uploded to the blockchain and published all the data for retrieval,and it allows patients to retrieve the required cases without locating a specific patient. Secondly,in order to avoid malicious uploading by authorized personnel,smart contracts are used to perform multiple authentication on data upload,and doctors and patients restrict each other to ensure that all the data on the blockchain is true and reliable. Finally,the improved RAFT consensus algorithm can quickly identify Byzantine nodes so as to better achieve consensus on the blockchain. The performance of the model is evaluated through experiments,and the results show that the medical data could be shared,and meet the needs of patients for online communication under the premise of ensuring patient privacy.

Keywords　Blockchain,Medical data sharing,Smart contract,Consensus mechanism,Patient communication

1　引言

近年来,电子信息医疗技术正在加速发展。由于我国人口基数大,医疗资源紧张,医患信息不对称的现象频发[1]。患者的情绪对疾病的治疗有一定的影响,而医患信息的不对称性很有可能加深患者的焦虑情绪,这也是我国医患矛盾愈演愈烈的主要原因[2]。目前,患者对医疗信息的需求日益增加,迫切需要在各种情境下集成和共享医疗信息[3]。

在我国医疗资源匮乏的时代背景下,患者往往无法通过医生获得足够的信息,许多患者在医院就医的同时会选择在互联网上交流获取医疗信息,不少患者有意愿对其医疗数据进行共享[4]。好大夫、丁香园论坛、百度贴吧等平台都能够提供相关的服务,患者之间的交流成为一种获取和共享医疗信息的新方式,患者间交流不仅可以分享各自的疾病治疗信息,还可以交流出院后的饮食、运动等习惯对疾病的影响等。但是,由于缺乏监管,各大平台虚假医疗广告盛行,医托药托等

到稿日期:2021-04-22　返修日期:2021-08-04
基金项目:国家重点研发计划项目(2016YFC0901705)
This work was supported by the National Key R&D Program of China (2016YFC0901705).
通信作者:安莹(anying@csu.edu.cn)

群体趁虚而入，使网络上信息的真实性难以保证。并且，由于医疗数据涉及大量个人信息，一些人利用患者共享的医疗数据进行非法盈利，这也使得患者在互联网上共享医疗信息的意愿大大降低。目前，患者更倾向于在线下面对面交流病情，但是现实中很难发现大量相同或相似疾病的病友，导致部分患者既无法大量获取关于自身疾病的信息，也无法有效地和病友进行沟通。因此，需要一种既能保证医疗数据真实共享，又能使患者之间可以匿名交流的方法来促进患者更便捷地交流医疗信息。

随着比特币的出现，越来越多的人开始了解区块链技术[5-7]，不同区块链应用随之产生[8]。2019 年 10 月 24 日习近平总书记在中央政治局第十八次集体学习时强调，把区块链作为核心技术自主创新重要突破口，再一次掀起了区块链的热潮。区块链技术的不可篡改性、匿名性和可追溯性[9]与医疗数据有着很高的契合度，为医疗数据的共享提供了新的思路[10]。用区块链技术来解决医疗数据共享的问题成为目前医疗行业的研究热点。

本文旨在让患者能够自主获取医疗数据并且能够在患者之间进行医疗数据传播，针对患者在线交流中无法共享真实数据的问题，提出了一种基于区块链的患者在线交流模型。该模型基于区块链技术，利用智能合约机制保证上传数据的真实性，而数据一经上传便无法被篡改。患者在区块链网络中使用数字身份，可以在该网络中检索与自身疾病相同或相似的病例，并与病友进行交流，分享疾病治愈经验，而不会泄漏隐私。

2 相关工作

2.1 患者交流平台现状

目前，患者在线交流主要集中在开放型社交平台、在线医疗平台和患者社区这三大类平台。

(1)开放型社交平台

开放型社交平台是患者交流中使用最多的一类平台，这些交流主要集中在微信群、QQ 群、百度疾病贴吧等。在这类平台中，患者除了分享自身疾病信息和治疗经验外，还会对多种情感进行表达交流[11]。

这类平台的用户量庞大，并且有即时通讯的特点，满足用户日常使用。但是这类平台的门槛极低，通常只需要手机号即可加入，导致医托药托和各种无用信息涌入，无法保障数据的真实性。

(2)在线医疗平台

我国的在线医疗平台主要包括丁香园社区、好大夫等[12]。这类平台多与医院合作，有医生参与，提供类似患者社区的功能，可以实现患者与患者之间、医生与患者之间的交流以及医生之间的相互学习。

这类平台注册成本依然不高，患者间交流仍然存在数据真实性问题。虽然平台有医生参与，但医生的建议经常是主观且重复的，患者难以获取额外的有价值的信息。

(3)患者社区

患者社区如 PatientsLikeMe，是一个旨在帮助患者交互和共享信息的平台[13]。不同于微信、QQ、医疗 APP 等企业开发的平台，PatientsLikeMe 是一个由患者自发组织的病友互助社区，该平台可以帮助患者找到相似的病友。用户可以在论坛中以私信的方式提问，交流和分享医疗数据，从他人的治疗经验中学习并更好地应对自身的疾病[14]。

目前，PatientsLikeMe 已经成为美国最大的患者社区，以罕见病患者居多。患者自发地在平台分享自身疾病的治疗经验，以帮助其他患者渡过难关。虽然该平台拥有大量用户并且趋于成熟，但是仍然不能杜绝“假病友”的信息。

2.2 区块链在医疗领域的尝试

区块链作为一种新兴技术，被认为可以满足医疗领域的应用需求[15]。在现有研究中，许多学者尝试将区块链技术与医疗领域相结合，最常见的就是利用区块链技术实现电子病历的共享。Niu 等[16]基于可搜索加密方案提出了一个电子病历共享方案，私有链存储密文哈希值，联盟链存储关键字索引，以实现电子病历的共享。Su 等[17]设计并实现了一套基于区块链的区域板式电子病历管理系统，实现了电子病历的长期保存和共享。Qin 等[18]针对卒中病历共享问题，以 BFT-RAFT 为共识机制设计了私有链和联盟链结合的区块链系统，提出了基于区块链的卒中病历共享方案。Azaria 等[19]提出了一种基于区块链的医疗数据共享系统，通过发行代币奖励给矿工从而使矿工将数据存储在本地数据库中。还有一些学者提出了云链协同的模型，Zhang 等[20]通过对比现有方案，提出了一种基于区块链的病人可控的云链协同模型，将电子病历的摘要存储在区块链上，将完整的电子病历存储在云端，改进 PBFT 算法并通过属性加密与多关键词加密实现数据可控共享。Dubovitskaya 等[21]提出了一种云链协同模型 ACTION-EHR，将元数据存储在区块链上，将完整病历信息存储在云中，患者通过设定访问权限来制定医护人员的访问，实现病历的安全共享。Zhou 等[22]提出了一种基于联盟链的医疗数据共享方案，使用 PBFT 共识机制，通过智能合约和 CP-ABE 相结合的方式保证了医疗数据的安全共享。

诸多研究表明，区块链可以用于存储医疗数据，通过将医疗数据上传至区块链，形成匿名且不可篡改的数据库，从而实现医疗数据安全的共享。目前的研究多为将区块链用于医疗机构间电子病历的共享，很少有学者提及在患者之间共享医疗数据；同时，由于区块链本身的缺陷，授权用户的恶意上传行为会使区块链系统的性能下降，少有学者提出对数据上传的过程进行认证。因此，本文基于现有研究，提出了一种将区块链技术用于患者在线交流的模型。通过设定智能合约机制，在数据上传过程中加入了多重身份认证，医生和患者相互制约，保证所有链上的数据真实可靠。在该模型中患者可以看到其他患者客观、真实且不可篡改的医疗数据，并且能够与感兴趣的患者进行在线交流，分享自身疾病治疗的经验。

3 模型设计

3.1 患者交流模型的整体框架

本文提出一种基于区块链的患者交流模型。根据医疗数据存储的特点，本文选择构建一个由多家医院组成的联盟链，所有联盟链成员共同维护联盟链状态。考虑到区块链本身性能的瓶颈，该模型旨在用最少的有价值的信息定位到有需求的患者，实现患者间的交流。模型的整体框架如图 1 所示。

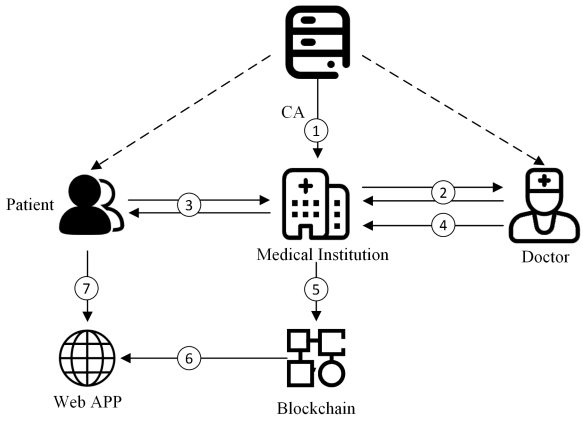

图 1 患者交流模型的运行框架

Fig. 1 Operating framework of patient communication model

该模型主要包括 6 个实体，分别为：证书机构、医疗机构、患者、医生、联盟链网络和应用程序。

(1)证书机构：主要负责为加入联盟链的医疗机构以及医生、患者颁发证书，并且起到全局监管的作用。本文假设证书机构完全可信。

(2) 医疗机构：医疗机构包括所有加入联盟链的医院，患者和医生的行为均在医疗机构中进行。

(3)患者：医疗数据的拥有者。在该模型中，只有加入联盟链网络的患者才有权限访问该网络。

(4)医生：医疗数据的生成者。患者就医后医生负责生成医疗数据，并上传至医疗机构进行验证。

(5)联盟链网络：由加入联盟链网络的所有医院共同组成，负责存储上传的医疗数据，以达到医疗数据不可被篡改的目的。

(6)应用程序：应用程序是患者对医疗数据访问的途径，提供患者的登录、搜索以及在线交流功能。

该模型采用链上存储医疗数据，患者在链下交流的形式，系统流程主要包括 7 个步骤。

步骤 1 身份分发。证书机构 CA 审查医疗机构资质，为加入区块链网络的医疗机构颁发数字证书及私钥。

步骤 2 医生注册。医生实名制向自身所在医疗机构发送注册请求，医疗机构审查医生资质后由 CA 为医生颁发证书。

步骤 3 患者注册。患者在就医时提交用户名和密码发送注册请求，医疗机构负责认证患者身份，CA 为验证后的患者颁发证书。

步骤 4 数据生成及身份验证。患者就医后，由医生生成患者的医疗数据，并将患者的医疗数据上传至医疗机构进行验证。具体过程如图 2 所示。

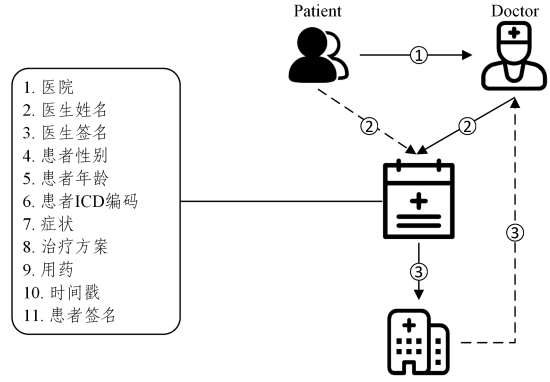

图 2 医疗数据内容及验证过程

Fig. 2 Content and verification process of medical data

(1)患者就医。

(2)数据生成。患者就医后，由医生负责医疗数据的生成。由于电子病历中包含大量信息，考虑到区块链本身性能的瓶颈，该模型中的医疗数据主要是基于患者角度，将患者想要对比自身疾病情况所需的如医院、疾病类型、主治医师、症状、治疗手段、用药、疾病治愈周期等信息上传至区块链网络中。其中，医疗数据中还包括医患双方的数字签名 Sig_{doc} 和 Sig_{id}，用于医疗数据的验证和追溯。

(3)身份验证。医生将医疗数据发送至医疗机构进行验证。首先，医疗机构调用智能合约对医生身份进行验证，验证通过则接收医疗数据，验证失败则将数据返回医生。随后，医疗机构调用智能合约对患者身份进行验证，验证通过则将该医疗数据视为有效数据，存储并等待上传，验证失败则删除该数据。

步骤 5 数据存储。医疗机构将验证后的有效医疗数据存储并等待上传至区块链网络中。

步骤 6 数据上传。医疗机构将有效医疗数据归属于指定患者并上传至区块链及应用程序中，为该患者打开在该 ICD 编码下交流的权限。

步骤 7 患者访问。患者使用步骤 3 中注册的用户名和密码登录系统，检索 ICD 编码获得有该 ICD 编码的病友数据。新加入网络的患者只有检索数据的权限，有医疗数据的患者会获得自身疾病对应 ICD 编码下的交流权限，患者可以在已获得交流权限的 ICD 编码下选择感兴趣的病友进行在线交流。如图 3 所示，患者 YC 只能和患有 A15.001 疾病的患者进行交流。

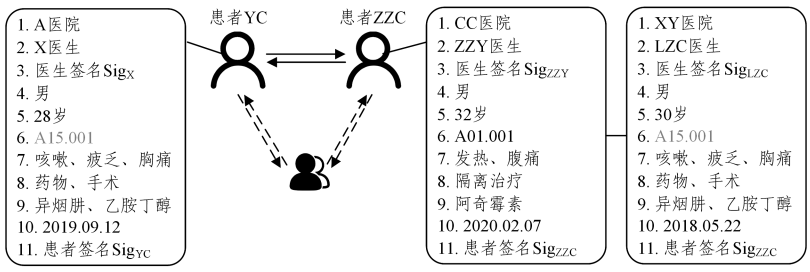

图 3 患者交流示例

Fig. 3 Example of patient communication

3.2 流程设计

3.2.1 用户注册与登记

证书机构 CA 设置全局参数，使用非对称加密算法生成主私钥 MK 和系统公钥 PK。证书机构负责审查医疗机构的资质，只有经过审查且被授权的医疗机构才可以加入联盟链网络。加入联盟链的医疗机构作为管理员用户，向证书机构 CA 提交用户名 admin 和密码 adminpw 进行用户登记。证书机构 CA 使用非对称加密算法为医疗机构生成公私钥对 A_{pk} 和 A_{sk}，将 A_{pk} 进行 SHA256 运算得到哈希值 h_1 并使用主私钥 MK 对 h_1 进行签名得到 h_1'，随后使用 h_1'、用户公钥 A_{pk} 和用户名 admin 以及医疗机构标识 A 生成数字证书 $C_{\text{admin}}\{h_1', A_{pk}, \text{admin}, A\}$，并存储在医疗机构证书库中，最后采用安全协议将证书 $C_{\text{admin}}\{h_1', A_{pk}, \text{admin}, A\}$ 和私钥 A_{sk} 返回医疗机构。其中，证书的签发及验证过程如图 4 所示。证书验证时，医疗机构首先对自身公钥 A_{pk} 进行 SHA256 运算得到哈希值 h_1，随后使用系统公钥 PK 解密证书中的 h_1' 得到 h_2，如果 $h_1=h_2$ 则验证成功，说明用户属于该系统。

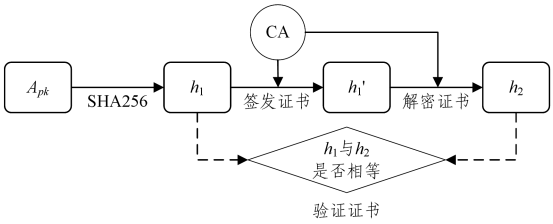

图 4 证书签发及验证

Fig. 4 Certificate issuance and verification

医生和患者的注册需要通过医疗机构来实现，医疗机构首先审查医生和患者资质，帮助本医疗机构的医生和就诊患者完成注册，具体过程如下：经医疗机构审查资质后的医生和患者向医疗机构提供注册用户名，由医疗机构向证书机构 CA 提交该用户名发送注册请求，如果该用户名存在则返回请求，不存在则使用安全协议返回该用户名以及唯一标识符，唯一标识符用于用户直接向 CA 发起登记请求从而避免医疗机构截获用户私钥。用户收到用户名和唯一标识符后，将用户名和密码连同唯一标识符一起发送给证书机构 CA 进行登记，CA 审核标识符后为用户生成公私钥对以及证书。医生在该过程中采用实名制注册，医疗机构向 CA 发起请求时会标记医生用户名为医生用户，医生用户的证书中额外包含医生标识 D。患者则自行设置用户名以保证隐私。最终证书机构 CA 为医生和患者颁发证书 $C_{\text{doc}}\{h_d', D_{pk}, \text{name}, D\}$ 以及 $C_{\text{user}}\{h_u', U_{pk}, id\}$ 并返回私钥 D_{sk} 和 U_{sk}，随后将证书分别存储在医生证书库和患者证书库中。医疗机构为新的注册患者创建医疗数据列表 id_list 并上传至应用程序，用于存储患者未来的医疗数据。新加入网络的患者只有数据检索的权限，没有交流权限。

3.2.2 数据生成

患者就医后，由医生撰写患者的医疗数据 T，完整的医疗数据需要患者和医生双方的数字签名。医疗数据 T 包含医生签名 Sig_{doc}、患者签名 Sig_{id}、医生姓名 name、就诊医院 H、患者疾病编码 ICD、时间戳 t 以及患者诊断产生的元数据 mdata。最终，医疗数据可以表示为：$T\{Sig_{id}, Sig_{\text{doc}}, \text{name}, H, \text{ICD}, t, \text{mdata}\}$。

3.2.3 身份验证

医疗数据生成后，医生使用证书 $C_{\text{doc}}\{h_d', D_{pk}, \text{name}, D\}$ 和医疗数据 T 向医疗机构发起数据验证请求，医疗机构调用智能合约对医生身份进行验证，具体算法如算法 1 所示。首先，医疗机构验证医生证书，如果验证成功则证明该医生是系统认证医生；随后使用医生公钥解密医疗数据中的医生签名，如果解密成功则证明是医生本人签名；最后将医生证书中的姓名与医疗数据 T 中的医生姓名进行对比，相匹配则接收医疗数据 T，否则将医疗数据返回医生。

算法 1 医生身份验证算法

```
输入：医生证书 Cdoc=C_doc，医疗数据 T
输出：ture，接收医疗数据；false，将医疗数据返回医生
1. /* Sigdoc=Sig_doc，Dpk=D_pk */
2. if VerifyTheCert (C_doc，PK){
3.     if decrypt (T. Sig_doc，D_pk){
4.       if C_doc. name==T. name {
5.         Receive(T)
6.         return true
7.       }else{
8.         Print("没有匹配的医生")
9.         return false
10.      }
11.    }else {
12.      print ("医生签名认证失败")
13.      return false
14.    }
15. } else {
16.    print ("医生身份认证失败")
17.    return false
18. }
```

医疗机构接收到医疗数据 T 之后，调用智能合约对其中的患者身份进行验证以确保该病例归属到具体患者，具体算法如算法 2 所示。首先，医疗机构遍历患者证书库，尝试使用患者证书中的患者公钥 U_{pk} 对患者签名 Sig_{id} 解密。如果解密成功则将该医疗数据 T 视为有效数据，提取患者证书中的用户名，存储医疗数据 T 并等待上传。

算法 2 患者身份验证算法

```
输入：医疗数据 T
输出：true，存储医疗数据；false，删除医疗数据
1. /* 患者证书库=Cp_list Sigid=Sig_id Upk=U_pk */
2. Vertify=false
3. for Cert in Cp_list {
4.     if decrypt (T. Sig_id，Cert. U_pk){
5.       Verify=true
6.       id=Cert. id
7.       T_val=T
8.       return true
9.     }
10. }
11. if Verify=false{
```

```
12.  print ("用户身份认证失败")
13.  return false
14. }
```

3.2.4 数据存储及上传

医疗机构准备好存储的有效医疗数据 T_val 以及医疗机构证书 C_{admin} 向矿工节点发送数据上传请求，如算法 3 所示。矿工节点验证医疗机构证书，验证通过则将医疗数据 T 上传至区块链网络。随后，医疗机构在应用程序中将该医疗数据 T 添加至指定患者的 id_list 中，并为患者打开该 ICD 编码下的疾病交流权限。

算法 3 医疗数据的存储及上传算法

```
输入：有效医疗数据 T_val，医疗机构证书 C_admin=C_admin
输出：true，医疗数据上传并为患者打开交流权限；false，返回医疗数据
1. if VerifyTheCert (C_admin, PK){
2.  Uploadtoblockchain (T_val)
3.  Id_list. append (T_val)
4.  Communication (T_val. ICD)=true
5.  Return true
6. } else {
7.  print ("管理员认证失败")
8.  return false
9. }
```

3.2.5 患者访问

患者使用注册的用户名及密码登录应用程序，可以对与自身相同或自身感兴趣的 ICD 编码进行搜索，获取所有患该疾病的医疗数据，获取检索结果后，患者还可以对年龄、医院、主治医生等信息进行进一步搜索。患者可以和已获取交流权限的 ICD 编码下的医疗数据归属者进行在线交流。应用程序中还提供区块链查询接口，患者可以通过向区块链发送查询请求来获取链上的医疗数据，与应用程序中的数据进行对比查看数据是否被篡改。

3.3 模型的共识机制

本文模型改进了 Huang 等[23]提出的 RBFT 共识机制，该共识机制基于实用拜占庭容错算法[24](Practical Byzantine Fault Tolerance，PBFT)和 RAFT[25]算法。在本文中，由全国 n 家医院作为节点组成联盟链，根据地区经济、医院医疗水平等因素将各家医院均分为 k 组，保证每组综合水平相当。系统每隔一段时间进行一次重新分组。

3.3.1 Leader 节点的选举

本文采用 RAFT 算法选举 Leader 节点。在 RAFT 算法中，所有节点包括 3 个状态：Follower，Candidate 以及 Leader。初始状态下所有节点均为 Follower 状态，每个节点上都有一个倒计时器（Election Timeout）。当 Follower 节点倒计时结束时，如果当前网络存在 Leader 节点则保持 Follower 状态，否则节点变为 Candidate 状态，对其他节点发送选举请求，由其余 Follower 节点对其进行投票，具体过程如图 5 所示。当 Candidate 节点收到超过一半的同意票则成为 Leader 节点，否则继续倒计时等待下一个 Candidate 节点。Leader 节点每隔一段时间向各节点发送 Heartbeat 以保持所有节点状态。每隔一段时间重新选取 Leader 节点。

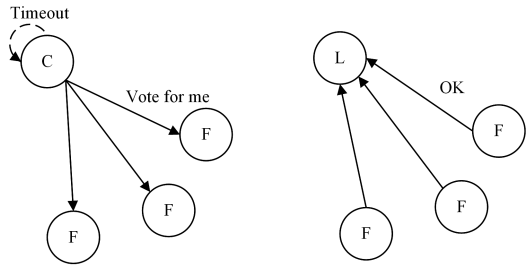

图 5 RAFT 算法中 Leader 节点的选举过程

Fig. 5 Leader node election process in RAFT

3.3.2 模型的共识过程

模型的共识过程主要分为两个阶段。

阶段 1 各组间的共识。各组间的 Leader 节点执行 PBFT 算法达成组间的共识，如图 6 所示。在阶段 1 产生的所有 Leader 节点中随机选取一个节点作为主节点，由客户端向主节点发送请求。Leader 节点间执行 PBFT 算法的预准备(pre-prepare)、准备(prepare)以及确认(commit)阶段，当各节点收到超过三分之二节点的确认消息后进行组内共识。

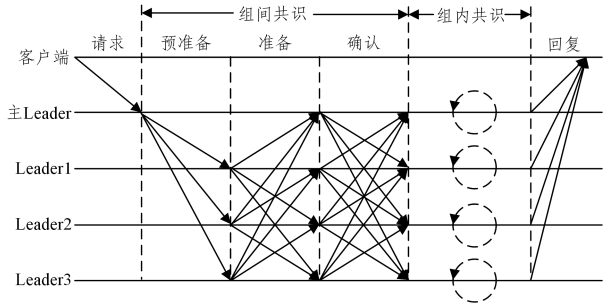

图 6 改进的 RAFT 共识机制

Fig. 6 Improved RAFT consensus mechanism

阶段 2 组内共识。组内共识由各组执行 RAFT 算法，Leader 节点在 Heartbeat 中发送日志，其余节点收到消息后复制日志并存储，随后向 Leader 节点发送确认消息达成组内共识，各组 Leader 节点向客户端回复，完成共识算法。在本文的共识算法中，在 RAFT 共识中加入了签名验证环节，并且在分组前选取一个监督节点，监督节点在分组时会被分配至每个组。被选中的监督节点上没有倒计时器，无法进行 Leader 节点的选举，但会参与所有组内的共识，如图 7 所示。当监督节点收到不同组的 Leader 消息后对签名进行验证并鉴别消息内容，如果发现消息不同则说明存在恶意节点。

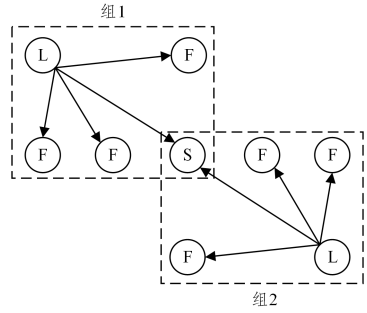

图 7 带有监督节点的 RAFT 共识机制

Fig. 7 RAFT consensus mechanism with supervisory nodes

4 安全性分析

本文选择构建一条由多家医院组成的联盟链。不同于公有链的随意加入，联盟链本质上是一条私有链，需要对资质进行认证且达成共识后才能将其加入。在本文模型中，每个节点都由一家医院组成，且医院之间不存在利益冲突，所有医院共同维护该区块链网络。该模型采用 RAFT 算法和 PBFT 算法相结合的共识机制。原始的 RAFT 算法只能容错故障节点，改进的共识算法可以识别拜占庭节点，当发现恶意节点时可以根据实际情况使其退出联盟链或进行处罚，从而有效避免了系统恶意节点的异常行为。

在该模型中，只有经过认证并注册的用户才可以访问该区块链网络，且患者就医后获取医疗数据中的 ICD 编码后才可以与对应病历的病友进行交流，每条医疗数据都需要医生和患者的签名，医生与患者相互制约，保证了所有检索到的病例都是真实的，诈骗者如果想直接与对应病友进行交流就必须要患有相同疾病，从而极大地降低了患者在线交流过程中不确定对方是否为假病友的风险。所有患者在该模型中使用 id 作为用户名，实现了医疗数据的匿名共享。在患者交流过程中可以利用医疗数据定位到具体的患者而无需获取患者本人的个人信息，有效保护了患者的隐私。

在具体流程的实施过程中，本文选择遍历患者证书库的形式来取代患者自己提供证书。虽然患者自己提供证书可以使医疗机构直接对自身身份进行验证，避免了医疗机构服务器对证书库的搜寻，可以提高系统的整体性能，但是在患者提供证书的过程中也暴露了患者的数字身份，在患者就医的同时可能会使数字身份定位到具体的个人。因此，本文选择牺牲部分系统性能来保证患者隐私的安全。

5 方案评估

5.1 共识机制分析

本文采用改进的 RAFT 共识机制，对模型共识机制的通信次数进行分析。假设各个节点通信正常，联盟链由 n 家医院组成，根据其地区经济、医院医疗水平等因素将各家医院均分为 k 组，保证各组综合医疗水平相当。阶段 1 执行 PBFT 算法，请求和预准备阶段总通信次数为 k，准备阶段和确认阶段的通信次数分别为 $(k-1)\cdot(k-1)$ 和 $k\cdot(k-1)$，回复阶段的通信次数为 k，阶段 1 的总通信次数为 $2k^2-k+1$。阶段 2 进行组内共识，改进共识机制中监督节点的加入会导致分组人数的变化。假设监督节点所在的组内人数为 n/k，由主节点向各个节点发送数据并接收数据的通信次数为 $2(n/k-1)$。其余 $k-1$ 组加入该监督节点后组内人数变为 $n/k+1$，组内通信次数为 $2(n/k)\cdot(k-1)$。改进的 RAFT 共识的总通信次数为 $2k^2-k+2n-1(k\geqslant 4, n>k)$。

在 PBFT 算法中，算法通信的复杂度为 $O(n^2)$，在 RAFT 算法中，算法通信的复杂度为 $O(n)$，本文采用的共识机制算法的通信复杂度为 $O(n/k)+O(k^2)$。表 1 对 3 种共识机制进行了对比。PBFT 算法的节点数一般控制在 100 以内，当系统节点 $n=1\,000$ 时 PBFT 算法的通信次数达到 1 999 001，极大地影响了系统的整体性能。RAFT 算法的通信次数虽然较少，但 RAFT 算法不能识别拜占庭节点，当系统存在拜占庭节点时很难有效达成共识。本文共识机制取 k 分别为 10，20，30，40 和 50 时的通信次数为 2 189，2 779，3 769，5 159 和 6 949。可以发现随着分组的增加，通信次数也有所增加，其通信次数仅略微高于 RAFT 算法，但是整体远小于 PBFT 算法。本文共识机制能够识别拜占庭节点，当监督节点发现恶意节点时可以采取将恶意节点踢出联盟链或进行处罚等手段，从而保证系统能够更好地达成共识。

表 1 3 种共识机制的对比

Table 1 Comparison of three consensus mechanisms

共识机制	算法通信复杂度	共识通信次数	$n=1\,000$ 时的通信次数
PBFT	$O(n^2)$	$2n^2-n+1$	1 999 001
RAFT	$O(n)$	$2n$	2 000
本文机制	$O(n/k)+O(k^2)$	$2k^2-k+2n-1$	$2k^2-k+1\,999$

5.2 智能合约性能评估

为了更准确地评估本文模型，探究其实际可操作性，对智能合约的性能进行测试。实验环境为 Intel（R）Core（TM）i5-5250U CPU @1.60 GHz×4，RAM 8 GB。系统模拟由 10 000 名患者组成，所有代码均以 GO 语言实现。医疗数据的生成阶段需要医生和患者对医疗数据进行签名，智能合约中的验证阶段需要医疗机构对医生身份进行验证。本文对该过程进行模拟，结果如图 8 所示，其中医疗数据属性的数目设置为 10，20，30，40 和 50。

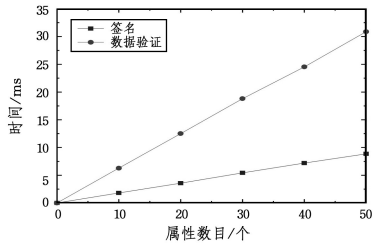

图 8 签名及数据验证性能

Fig. 8 Signature and data verification performance

对患者身份认证进行性能测试，测试医疗数据属性数目分别为 10，20，30，40 和 50，计算单次患者身份认证的平均耗时，结果如图 9 所示。结果显示，随着属性数目的增加，患者身份认证的时间呈上升趋势。结合数据签名和数据验证的结果，智能合约执行单个患者数据上传操作的时间在 1.5 s 之内，可以满足患者交流模型的数据快速上传需求。

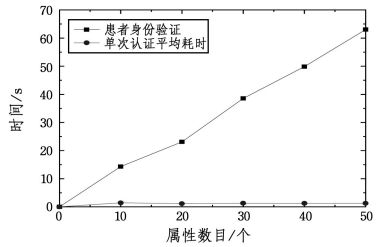

图 9 患者身份认证性能

Fig. 9 Patient authentication performance

5.3 对比分析

本文采用对比分析的方法，将本文方案与现有的基于区块链的医疗数据共享方案进行对比，结果如表 2 所列。

表 2 本文方案与现有方案的比较

Table 2 Comparison between different schemes

方案	共识机制	共识通信次数	智能合约	多重身份认证
文献[18]	BFT-RAFT	$2n$	否	否
文献[20]	改进 PBFT	$2n^2/k^2+k^2+k$	否	否
文献[22]	PBFT	$2n^2-n+1$	是	否
本文方案	改进 RAFT	$2k^2-k+2n-1$	是	是

由于区块链本身的特性会使链上数据不断增加，引起服务器存储的压力，而授权用户的恶意上传行为会导致区块链性能的下降，且该过程不可逆，因此，对数据上传的审查是有必要的。文献[18,20,22]选择数据拥有者对文件上传且未设置上传数据的校验。本文的智能合约中定义了数据上传的多重身份认证算法，由医生将医疗数据 T 上传至医疗机构，随后医疗机构需要先对医生身份进行验证，验证成功后再对患者身份进行验证，确认双方身份之后再进行数据上传。由于医疗数据中包含医患双方签名，医生在上传数据时也是医患相互监督的过程。

本文采取摘要电子病历的方案，将数据全部存储在区块链中，相比于文献[20,22]使用云链协同存储电子病历的方案，本文模型只需上传患者交流需要的医疗摘要数据，最大化地利用了区块链不可篡改的特性，同时也避免了因云上数据受攻击导致链上数据无用的情况。

下面对 4 种不同方案共识机制的通信次数进行对比分析。其中节点数量由 200 增加至 1 000，每次增加 200。节点数量变化的同时分组数量 k 值也随之变化，保持每组人数为 50。图 10 给出了具体通信次数的结果(为了使结果更清晰，纵坐标取对数运算)。可以发现本文方案相比于文献[20,22]有着更少的通信次数。本文采用的改进 RAFT 共识机制能够有效地识别拜占庭节点，当系统存在拜占庭节点时，相比于文献[18]选择切换为 BFT 共识算法应对的方案，本文方案有更好的共识效率。

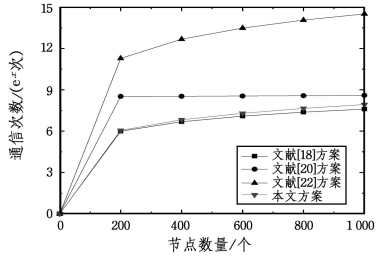

图 10 不同方案共识通信次数的对比

Fig. 10 Comparison of communication time between different schemes

结束语 为了使患者在互联网中交流时可以共享真实的医疗数据，本文基于区块链技术提出了一种患者在线交流模型。通过多重身份认证将医疗数据存储在区块链上并设置访问机制，实现了只有进行医疗数据共享的患者才能访问该医疗数据网络，在患者间建立起一个只有真实患者的交流模型。患者可以在该模型中检索与自身相同的病例并与病友进行在线交流，分享疾病治愈的经验。随后，通过实验测试了本文模型，结果表明该模型的性能满足正常数据上传共享的需求。

同时，本研究存在一定的局限性。首先，本文模型中的患者认证算法基于患者的证书库，系统用户量增多时会引起系统性能的下降，当系统用户量达到某一阈值时可能会导致数据上传时间过长，未来考虑采用将患者证书库分组的方案缓解系统压力；其次，在共识机制阶段，如果监督节点同时也是拜占庭节点将会导致其他拜占庭节点的作恶成功，未来考虑加入多个匿名监督节点或加入对监督节点的审查，从而更好地提高共识效率。

参 考 文 献

[1] HE M M, CUI Y M. The influence of information asymmetry on the doctor-patient relationship in contemporary China and its countermeasures[J]. Journal of Suzhou University of Science and Technology(Social Science), 2020, 37(6): 39-45.

[2] CHEN W J, ZANG Y S, ZHOU G R. The new changes in the doctor-patient relationship under the background of "Internet+" and development suggestions[J]. Chinese Hospital Management, 2019, 39(12): 68-69.

[3] DURNEVA P, COUSINS K, CHEN M. The Current State of Research, Challenges, and Future Research Directions of Blockchain Technology in Patient Care: Systematic Review[J]. J. Med. Internet Res., 2020, 22(7): e18619.

[4] LEE K, LIM K, JUNG S, et al. Perspectives of Patients, Health Care Professionals, and Developers Toward Blockchain-Based Health Information Exchange: Qualitative Study[J]. J. Med. Internet Res., 2020, 22(11): e18582.

[5] MCGHIN T, CHOO K, LIU C, et al. Blockchain in healthcare applications: research challenges and opportunities[J]. J. Netw. Comput. App., 2019, 135: 62-75.

[6] GAYNOR M, TUTTLE-NEWHALL J, PARKER J, et al. Adoption of Blockchain in Health Care[J]. J. Med. Internet Res., 2020, 22(9): e17423.

[7] YLI-HUUMO J, KO D, CHOI S, et al. Where Is Current Research on Blockchain Technology? —A Systematic Review[J]. PLoS One, 2016, 11(10): e0163477.

[8] DENG K. The essence, carrying out conditions and application prospects of blockchain technology[J]. Journal of Shenzhen University (Humanities and Social Sciences), 2018, 35(4): 53-61.

[9] ASTE T, TASCA P, MATTEO T D. Blockchain Technologies: The Foreseeable Impact on Society and Industry[J]. Computer, 2017, 50(9): 18-28.

[10] AZOGU I, NORTA A, PAPPER I, et al. A Framework for the Adoption of Blockchain Technology in Healthcare Information Management Systems: A Case Study of Nigeria[M]. New York: Assoc Computing Machinery, 2019: 310-316.

[11] LI X G, LI S S, LIU Y F, et al. Research on the relationship between knowledge interaction and emotion interaction in online medical health community on comprehensive social platform[J/OL]. Information studies: Theory & Application: 1-13[2021-06-09]. http://kns.cnki.net/kcms/detail/11.1762.G3.20210312.1117.004.html.

[12] CHEN X. Current status and future prospects of internet medical research[J]. Renming Luntan · Xueshu Qianyan, 2017(24):

40-47,95.

[13] NYMAN E,VAUGHAN T,DESTA B,et al. Characteristics and Symptom Severity of Patients Reporting Systemic Lupus Erythematosus in the PatientsLikeMe Online Health Community:A Retrospective Observational Study[J]. Rheumatology and Therapy,2020,7(1):201-213.

[14] WICKS P,MASSAGLI M,FROST J,et al. Sharing Health Data for Better Outcomes on PatientsLikeMe[J]. J. Med. Internet Res.,2010,12(2):e19.

[15] KUO T T,ROJAS H Z,OHNO-MACHADO L. Comparison of blockchain platforms:a systematic review and healthcare examples[J]. Journal of the American Medical Informatics Association,2019,26(5):462-478.

[16] NIU S F,LIU W K,CHEN L X,et al. Searchable and encrypted electronic medical record data sharing scheme based on alliance chain[J]. Journal on Communications,2020,41(8):204-214.

[17] SU Y F,YIN W D,CHEN P,et al. Regional layout electronic medical record management system based on alliance chain[J]. China Digital Medicine,2020,15(6):42-44,65.

[18] QIN Q L,CAO H,LI M Y,et al. Application of Blockchain in the Sharing of Electronic Medical Records for Stroke[J]. Chinese Journal of Stroke,2020,15(6):606-610.

[19] AZARIA A,LIPPMAN A,VIEIRA T,et al. MedRec:using blockchain for medical data access and permission management [C]// 2016 International Conference on Open and Big Data. Vienna:IEEE Press,2016:25-30.

[20] ZHANG L,ZHENG Z Y,YUAN Y. Controllable sharing model of electronic medical records based on blockchain[J/OL]. Acta Automatica Sinica: 1-14 [2020-12-08]. https://doi. org/10.16383/j. aas. c200359.

[21] DUBOVITSKAYA A,BAIG F,XU Z,et al. ACTION-EHR:Patient-Centric Blockchain-Based Electronic Health Record Data Management for Cancer Care[J]. J. Med. Internet Res.,2020,22(8):e13598.

[22] ZHOU Z Q,CHEN Y L,LI T,et al. Medical data security sharing scheme based on alliance chain[J]. Journal of Applied Sciences,2021,39(1):123-134.

[23] HUANG D Y,LI L,CHEN B,et al. RBFT:Byzantine fault-tolerant consensus mechanism based on Raft cluster[J/OL]. Journal on Communications: 1-11[2021-04-01]. http://kns. cnki.net/kcms/detail/11. 2102. tn. 20210315. 0835. 002. html.

[24] KIM Y,PARK J. Hybrid decentralized PBFT Blockchain Framework for OpenStack message queue[J]. Human-Centric Computing and Information Sciences,2020,10(1):12.

[25] HUANG D Y,MA X L,ZHANG S L. Performance Analysis of the Raft Consensus Algorithm for Private Blockchains[J]. IEEE Transactions on Systems Man Cybernetics-Systems, 2020,50(1):172-181.

CHEN Xian-lai, born in 1970, Ph. D, professor, Ph. D supervisor. His main research interests include medical data mining and decision support system, and medical big data.

AN Ying, born in 1980, Ph.D, associate professor, master instructor. His main research interests include medical big data analysis, machine learning and its applications.