基于区块链的医疗信息安全存储模型

王 辉 周明明
(南京工业大学计算机科学与技术学院 南京 211816)

摘 要 我国医疗信息化的现状显示,传统的电子数据模式在医疗信息存储方面存在以下两个问题:1)电子数据规范性较差,流通慢;2)电子数据安全性和隐私性易受到威胁。针对各个医疗信息系统之间存在的信息存储安全问题和信息间的共享问题,结合区块链的共识机制、加密机制、点对点网络等技术,提出了一种基于区块链的信息管理方案来实现医疗信息的存储和共享,该方案具有不可篡改、去中心化等特点。通过改进的拜占庭协议实现网络节点的共识,通过访问控制机制达成医疗信息的共享,通过区块链来保存医疗信息的公共信息,而就诊的真实数据被加密保存在数据库或者云中,方便且有效地实现了敏感医疗数据的存储和系统之间的信息共享。在联盟链的环境下选取若干网络节点进行性能测试,实验结果表明,所提方案在防篡改、隐私保护等安全保护方面和吞吐量等性能方面具有较好的表现。此外,所提方案提出的索引机制能够实现快速检索,提高检索效率。通过搭建测试网络,证明了所提方案在医疗信息存储方面的可行性。所提方案利用区块链技术进行去中心化和不可篡改的管理,能够极大地提高医疗服务效率,提升医疗服务质量,为进一步研究区块链底层技术和探索区块链技术在医疗信息领域的应用奠定了良好的基础。

关键词 医疗区块链,共识机制,信息安全,信息共享
中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/jsjkx.181102034

Medical Information Security Storage Model Based on Blockchain Technology

WANG Hui ZHOU Ming-ming
(School of Computer Science and Technology, Nanjing Tech University, Nanjing 211816, China)

Abstract According to the status quo of medical informationization in China, the traditional electronic data model has the following problems in information storage. Firstly, electronic data have poor standardization and slow circulation. Secondly, electronic data security and privacy are threatened. Aiming at the security problem of information storage and the sharing of information between medical information systems, combined with the consensus mechanism of blockchain, encryption mechanism and peer-to-peer network, a blockchain-based information management scheme was proposed to realize the storage and sharing of medical information, which is non-tamperable and decentralized. The consensus of the network nodes is realized through the improved Byzantine protocol, the medical information is shared through the access control mechanism, the public information of the medical information is saved through the blockchain, and the real data of the medical treatment is encrypted and stored in the database or the cloud, which conveniently and effectively implements the storage of sensitive medical data and the sharing of information between systems. In the environment of the alliance chain, several network nodes are selected for security and performance testing. The experimental analysis shows that the proposed scheme has better performance in terms of security protection such as tamper resistance, privacy protection and throughput. In addition, the indexing mechanism proposed in this scheme can achieve fast retrieval and improve retrieval efficiency. By establishing a test network, the feasibility of this program in medical information storage is proved. The decentralized and non-tamperable management of the program using the blockchain can greatly improve the efficiency and the quality of medical services. It lays a good foundation for further research on the bottom technology of block chain and for exploring the application of block chain technology in the field of medical information.

Keywords Medical blockchain, Consensus mechanism, Information security, Information sharing

1 引言

医疗信息孤岛问题和医疗数据安全问题一直是我国医疗信息化的两大难题。随着数字化和云存储等技术的发展,各个医疗信息系统均采用了数字化存储技术,医疗数据信息化已经基本成熟。但是,病人基本信息和就诊记录等医疗大数据的巨大价值,以及医疗设备提供商之间的竞争关系,使得医疗数据信息在不同医院或者不同的医疗系统之间的传输壁垒

到稿日期:2018-11-04 返修日期:2019-03-31
王 辉(1962—),女,博士,教授,主要研究方向为有光传输理论与系统、信号处理与控制技术,E-mail:2049319291@qq.com(通信作者);周明明(1993—),女,硕士,主要研究方向为信息安全。

较高。此外，医疗机构存储的医疗数据结构不统一、工具不兼容，无法真正意义上实现跨机构的安全信息共享。目前，大多数医疗系统都依靠单点登录来实现各个系统之间的登录和数据访问，但是当一个单点发生故障或者受到网络攻击时则容易导致所有人的信息泄露，因此医疗记录的安全和隐私问题是亟待解决的。

医院数据库中的就诊记录和基本信息涉及隐私和安全问题，而数据匿名性可以保护个人医疗数据的安全。在这方面，研究者提出了很多关于数据安全性和隐私保护的技术，例如同态加密、基于属性的加密方案。近年来，随着云存储技术的发展，研究人员提出了一种基于云技术的存储服务，其通过对访问权限的控制来达到共享医疗数据的目的。Esposito 等[1]阐述了一种在医疗信息方面使用云存储技术的数据共享模型，并列举了在医疗数据共享中使用区块链技术可能存在的挑战。但是，这些医疗网络依赖交易双方共同相信的角色，即利用一个可信赖的第三方(Trusted Third Party，TTP)来保障交易的正常进行，它是一个中心化的模式。这需要第三方绝对可信并且不会受到网络攻击，然而，这样理想的网络环境几乎是不可能实现的。因此，传统的医疗信息解决方案不是一个很好的选择。

随着比特币在国内的不断发展，区块链技术逐渐走向成熟。国内关于区块链技术的研究很多，但是基于区块链的医疗信息存储方案并不多。Zyskind 等提出了将区块链技术用于访问控制管理和安全数据存储的方案[2]。该方案将加密数据存储在受信任的第三方托管服务中，并在区块链上记录事件日志，但其依旧存在数据泄露的风险，且没有实现去中心化。Azaria 等[3]提出了一种基于区块链的数据共享系统，该系统通过分散记录管理系统来处理电子病历。该系统为矿工提供了汇总的权限，并将数据奖励给簿记员[4]，但是数据使用效率并不令人满意。因此，基于现有的思路，本文结合区块链的去中心化、分布式、匿名性等特点，提出了一种医疗记录存储和共享的方案，该方案以所有人可以理解的数据结构和方式安全地分享、存储数据。首先，通过改进的拜占庭协议等关键技术来达成节点的共识，通过访问控制来合理地共享和访问医疗信息；其次，在安全性、容错率等方面，将现有的一些基于区块链的医疗存储方案与本方案进行比较，结果表明，本方案在安全性、容错性、检索效率等方面有较大的优越性。

本文第 2 节简单介绍了比特币挖矿过程和共识机制等基础概念；第 3 节提出了医疗存储区块链的方案；第 4 节给出了实验结果，并且系统地分析了所提方案在安全性方面的优势；最后总结全文。

2　区块链技术

区块链技术属于一种去中心化的记录技术。区块链上的数据可以由参与到系统的所有节点共同维护，每个参与维护的节点可以隶属于不同组织，并且不需要节点之间相互信任，但是每个节点都能获得一份完整记录[5]。从狭义上来讲，区块链是一种按时间顺序连接数据区块的链式数据结构，并利用密码学方面的技术实现了数据安全传输与访问的分布式账本[6]。

2.1　工作原理

区块链中的每一个数据块都包含着交易和前一数据块的哈希值(除了创世块)[6]。任何一个网络节点都能访问这个链式数据结构，读取交易数据，并通过数学算法计算出所有交易的状态[7]。具体步骤如下：

步骤 1　用户通过一个公私密钥对与区块链网络交互，公钥作为网络地址；每生成一笔交易，用私钥对交易进行数字签名，并向它的下一跳节点进行广播。

步骤 2　周围的节点在收到交易消息后，验证消息是否有效，若无效则丢弃，否则向其下一跳节点转发。最后，将有效的交易消息传播到整个区块链网络。

步骤 3　在一定的时间间隔(一般为 10 min)内，交易会被网络收集和验证，按照时间顺序对其进行排序并打包成一个候选块。根据工作量证明机制，最先获胜的节点在网络中广播候选块。

步骤 4　节点验证如步骤 3 所述的网络中广播的候选块，对块中的有效交易进行检测，如果验证失败则丢弃，否则将其加入到区块链中。

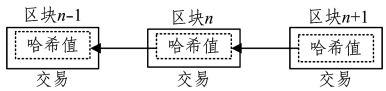

图 1　区块链的链式结构

Fig. 1　Chain structure of blockchain

上述步骤在规定的时间间隔内会重复执行。由此可见，区块链是一个已经通过验证的标记时间的网络活动记录[8-12]。

2.2　共识算法

目前常见的共识机制有应用在比特币上的工作量证明机制(Proof of Work，PoW)、权益证明机制(Proof of Stake，PoS)、股份授权证明机制(Delegated Proof of Stake，DPoS)、实用拜占庭容错机制(Practical Byzantine Fault Tolerance，PBFT)和改进的拜占庭容错算法(Delegated Byzantine Fault Tolerant，DBFT)[13-19]。DBFT 是一种代理拜占庭容错算法，它与股份授权证明机制类似，有投票权的节点投票选出代理记账人来验证和生成区块，这样可以有效地减少参与记账或者验证过程中节点的数量，解决了拜占庭算法固有的扩容性问题[20-21]。该算法中存在两种节点：普通节点和专业记账节点。不参与记账的节点称为普通节点，它们可以看到共识过程，并且需要同步信息。参与记账的节点称为超级节点，负责记账，它们由普通节点按照持有权益比例通过投票方式决定。假设在网络中存在 n 个超级节点，包括 1 个主节点和 $n-1$ 个记账节点，主节点由超级节点轮流当选。每次记账时，主节点首先发起对区块内容的提案，一旦有大于 $(2n+1)/3$ 个记账节点通过并同意这个主节点的提案，则最终发布的区块内容就是该提案；并且由于这个过程是不可逆的，区块不会出现分叉问题，区块中的一切交易可以完全确认。

3　医疗区块链方案

该方案利用区块链的共识机制、点对点网络传输技术、加密算法等相关技术来完成医疗数据网络中的共享和安全的存

储。医疗区块链的体系结构如图 2 所示。

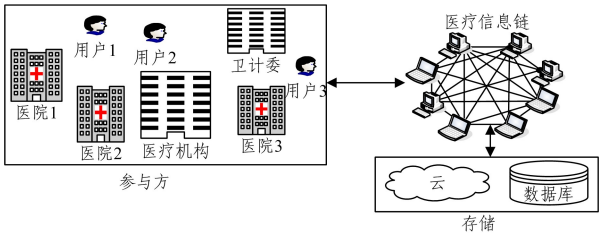

图 2 医疗区块链的体系

Fig. 2 Medical blockchain system

在该方案的医疗信息链中有多方交易主体，例如监管机构、病人、医院。病人对自己的医疗记录拥有绝对的所有权和控制权，病人查询医疗记录时，能够得到存储在链上的历史医疗记录摘要，并根据私钥查阅或者下载详细的电子病历。医生或者医院为病人进行诊断并且提供此次诊断的相关医疗记录，医院的服务器会在一定的时间内完成一次添加块的处理。

图 3 给出了按照医疗区块链的模型给出的医疗信息链中各层的设计。系统自下向上可分为数据层、点对点网络层、管理层、应用层。

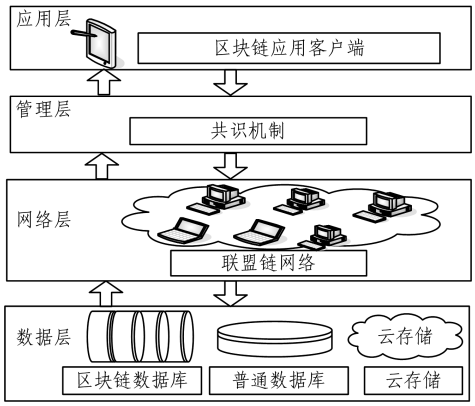

图 3 医疗区块链的分层结构图

Fig. 3 Hierarchical structure diagram of medical blockchain

3.1 数据层

数据层是系统的最底层，可以存储区块的数据等。区块链中一般存储了存储节点提交的交易数据，它可以是区块链数据、普通数据库或者医院云存储。区块链上的第一个块(创世块)由系统自动创建，它的区块高度为零；其他的区块需要通过节点生成，并且需要验证，符合要求的区块才会被加到主链上，区块高度依次增加 1。本方案的信息链的数据块结构如图 4 所示，版本号指当前最新版本的区块链；时间戳标志生成一个新的区块的时间；签名集合是此块中所有交易的签名的集合；Merkle 根是指区块中的一系列交易通过层层哈希计算得到，即每两个相邻的哈希摘要通过合并形成新的字符串并进行哈希计算，依次递进，最终得到哈希值；系统中的交易都是通过 Merkle 树进行组织的，本方案的每个区块的交易数目是 10。本方案通过时间戳来决定区块链接的顺序，采用单向性的哈希函数确保数据无法被篡改，利用公钥加密实现身份的识别和认证。此外，将区块头哈希值和区块的高度存储在索引数据库中，以加快检索速度。

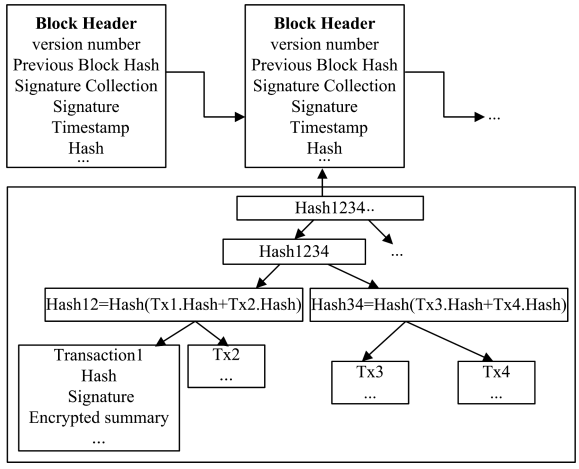

图 4 医疗信息链的数据块结构

Fig. 4 Data block structure of medical information chain

3.2 网络层

数据层之上是网络层，它是一个点对点网络，能够实现联盟链网络中节点之间的相互通信。为了保持通信的一致性，网络中的各个节点需要维护一个共同的账本。目前，现阶段的网络由医院的服务器构成的，而网络中的超级节点一般是由大城市的三甲医院的服务器构成，普通节点则由小型医院的服务器构成。因此，在本方案的网络中，共识节点负责产生每个新的区块，随后超级节点将新区块广播到整个网络。验证节点负责验证广播接收的区块信息，验证通过后将继续在网络中广播。一般根据系统采用的共识机制进行验证，当前新区块得到多于 2/3 的共识节点认可后，即可增加到链上。

3.3 管理层

管理层提供一种数学算法，使医院、医疗产品供应服务商、患者、政府部门等各个分布式节点之间验证行为、建立信任和获取权益[10]，即共识机制。本方案采用改进的拜占庭协议的共识机制，该协议的共识节点需要具有记账、验证等功能。而节点的选取是由权益持有者投票选举产生的代理记账人，这种方式不适合我国的医疗行业。鉴于我国的医疗现状，即医疗信息大数据或者资源一般集中在重点医院，例如三甲医院或者级别较高的医院、组织机构等，本方案选择本省中的所有三甲医院、妇幼保健院、急救中心等医疗机构的服务器作为超级节点，并按照现阶段国家对医院的评级标准，选择排名第一的三甲医院作为初始的记账节点，设其编号为 0，其他的三甲医院作为议员，按照排名将其依次编号为 $1,2,\cdots,n-1$，超级节点的个数通常在 50 至 100 之间。根据拜占庭容错算法的要求，系统可容忍的最大恶意节点数 f 为 $f=(n-1)/3$；参与共识的验证节点会记录当前的共识的状态，并将其维护成一个状态表。一次共识从开始到结束所用的数据集合称为视图，用符号 V 表示。视图的编号也是从 0 开始，逐渐增加。如果当前视图内不能达成共识，则需要更换共识。共识机制的步骤如下：

步骤 1 发送签名后的交易请求，验证节点向全网广播该交易，并附上发送者的签名；

步骤 2 所有共识节点均独立监听全网的交易消息，并进入初始视图；

步骤 3 主节点 $p=(h-v)\bmod n$，其中 h 表示区块的高

度，经过一段时间后，发送区块消息、当前视图编号、区块高度、主节点编号等，即〈PrepareRequest，h，v，p，$block$，〈$block$〉σp〉；

步骤 4　任意节点 i 在收到 PrepareRequest 消息后，若同意，则发送 PrepareResponese 消息，其中包括当前区块高度、节点编号、所在视图编号等，即〈PrepareResponese，h，v，i，〈$block$〉σi〉；

步骤 5　若任意节点收到至少 $2n/3$ 个 PrepareRequest 消息，则说明达成共识，发布完整的区块并将其保存在本地的分布式账本中，如果少于 $2n/3$ 个 PrepareRequest 消息，则没有达成共识，发送视图更换请求；

步骤 6　节点在一定时间内收到的更换视图请求多于 $n-f$ 时，说明验证节点之间没有达成共识，需要判断自身是否为新一轮视图的主节点，由新的主节点向网络中广播视图，进行视图更换，返回步骤 3。

如果验证的节点或者主节点在一定时间内无法达成共识，网络会更换视图进行新一轮的共识。假设共识时间是 t，当节点 i 经过 $2^{(v_k+1)}\cdot t$ 之后还没达成共识，则进入视图更换流程。视图更换的步骤如下：

步骤 1　令 $k=1$，$v_k=v+k$；

步骤 2　节点 i 发出视图更换请求，其中包括区块的高度、视图编号等，即〈changeView，h，v，v_k〉；

步骤 3　任意节点收到大于 $n-f$ 个不同 i 节点的相同 v_k 值后，更换视图，令 $v=v_k$，开始新的视图内共识；

步骤 4　若经过 $2^{(v_k+1)}\cdot t$ 时长后，视图更换没有成功，则 k 递增，返回步骤 2。

共识机制的具体流程如图 5 所示。

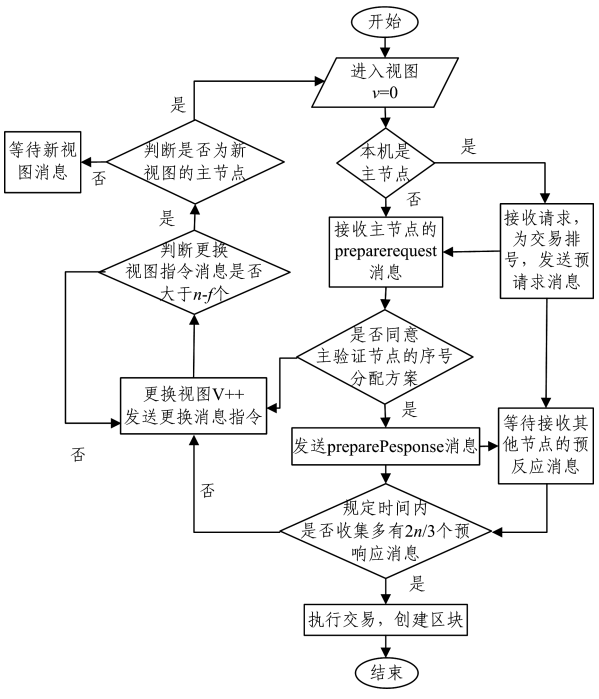

图 5　DBFT 算法的流程图

Fig. 5　Flow chart of DBFT algorithm

3.4　应用层

3.4.1　数据发布与存储

医院对医疗信息进行哈希，并且用发行方的私钥进行签名，然后将其发布到网络中，用对称密钥对医疗记录进行加密，并用病人的公钥加密对称密钥，之后将加密的密文发送给病人。用户接收到医疗数据后，先验签并且用私钥解密，在得到医疗信息数据和签名后再对其加密并将其放到数据库或者云中。

3.4.2　数据共享与访问控制

制定合适的访问控制协议能够避免未经授权的用户获取敏感信息，并且能够实现数据的共享。当医生想要获得病人的诊断记录时，需要病人授予权限。访问者提供签名作为身份属性的唯一标识。系统遍历所有的块，通过比较链上的签名集合找到正确的块。访问者是否可以在上面看到加密内容块取决于比较的结果。如果访问者被授权，系统允许其查看隐私信息，并且可以使用他们的私钥来解密数据。

3.4.3　快速检索

本方案对用户的病历建立一个简单的索引目录，根据不同的部门对患者过去的加密摘要进行分类并记录数据的位置，即根据医院部门分类记录患者相关块的哈希值。如果患者未访问某些部门，则相关的哈希值记录为空。之后，患者只需要更新相关的哈希值记录即可，这为数据查询带来了极大的便利。

4　安全性和性能分析

4.1　安全性分析

本文采用访问控制、区块链技术确保数据的安全性，从防篡改、隐私保护、抗网络攻击这 3 个方面进行安全性分析。

4.1.1　防篡改

区块链上的记录通过 Merkle 树哈希生成 Merkle 根，并将其存储在区块链的区块头部。它是一个基于哈希算法的数据结构，由于哈希算法具有单项性，因此可以验证链上信息是否被篡改。当攻击者成功地得到某个区块的信息时，对数据做任何的修改都会导致整个区块上哈希值的变化，这可以保证医疗记录的不可篡改性。

4.1.2　隐私保护

交易都是通过发起者进行签名并通过校验存储到区块上，因此私钥的私密性能够保证交易的安全性，每次交易都是以匿名的方式参加的。访问控制协议使得病人对医疗记录拥有绝对的控制权，只有有权限的用户才能查看真实的医疗记录数据，因此访问控制协议和私钥很好地保障了医疗记录的隐私。

4.1.3　协议攻击

以黑客常用的攻击方式之一——重放攻击为例，假设系统中存在一个普通的用户 U、一台服务器 S 和一个攻击者 T。$E_{(K_u^{-1})}(M)$ 指签名消息，$E_{(K_u)}(M)$ 是被 K_u 加密的消息，$T(U)$ 表示 T 伪装成 U 发送消息。

假设一次攻击中联盟链网络需要 T 有一定的访问权限，一旦 T 没有身份权限访问网络，它将不能看见链上的签名和加密的摘要信息。

$$T\rightarrow S:E_{(K_t^{-1})}(E_{K_s}(N_u,C)) \tag{1}$$

如果 T 可以顺利拦截 U 发送的信息，如式(2)所示，那么 T 也可以伪装成服务器 S，并且执行重放攻击，即 T 可以伪装成 U 向服务器 S 发送消息，如式(3)所示，T 也可以伪装成 U

接收服务器的消息；最终 T 只能得到加密的摘要，而不能得到其他信息。

$$U\rightarrow T(S):E_{(K_u^{-1})}(E_{K_s}(N_u,A)) \tag{2}$$

$$T(U)\rightarrow S:E_{(K_u^{-1})}(E_{K_s}(N_u,A)) \tag{3}$$

$$S\rightarrow T(U):E_{(K_s^{-1})}(E_{K_u}(M)) \tag{4}$$

如果 T 能够发送虚假信息，如式(5)所示，那么 T 也可以伪装成服务器向用户发送信息；但是它缺少 S 的认证信息，并且发送的消息中含有攻击者 T 的身份信息，因此 U 还是能够识别出虚假信息 M'。

$$T\rightarrow S:E_{(K_u^{-1})}(E_{K_s}(N_u,A)) \tag{5}$$

$$T(S)\rightarrow U:E_{(K_t^{-1})}(E_{K_u}(M')) \tag{6}$$

4.2 安全性证明

本方案采用文献[12]中的攻击模型来分析区块链潜在的被攻击风险。假设在网络中诚实节点生成区块链的概率是 r，攻击者节点伪造区块链的概率是 w，则攻击者节点控制全网 n 个节点的概率是 w_n：

$$w_n=\begin{cases}1, & r\leqslant w\\ \left(\dfrac{w}{r}\right)^2, & r>w\end{cases} \tag{7}$$

从攻击者节点与正常节点相差区块数量的规律来看，它满足泊松分布的概率密度，期望值为：

$$\lambda=n\frac{w}{r} \tag{8}$$

攻击者节点攻击成功的概率 P 为：

$$P=\lim_{\lambda\rightarrow\infty}\sum_{\alpha<k<\beta}\frac{\lambda^k e^{-\lambda}}{k!}\left(\frac{r}{w}\right)^n,k=0,1,2,\cdots \tag{9}$$

设定 w 的值为 0.1，0.2 和 0.3 进行测试，攻击者节点攻击成功的概率结果如图 6 所示。可以看出，随着伪造节点与正常节点数值的不断增大，攻击者攻击成功的概率 P 呈现指数下降趋势。

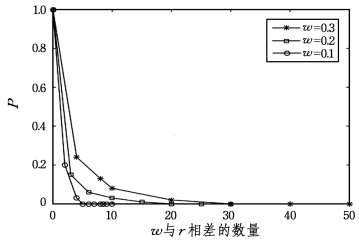

图 6 攻击者节点攻击成功的概率图

Fig. 6 Probability map of attacker attacking nodes successfully

在真实的医疗信息网络中，诚实节点和非诚实节点数之差远远超过 20 个，因此攻击者成功攻击的概率几乎为零。

4.3 医疗区块链中的性能分析

4.3.1 理论分析

本方案采用的改进拜占庭容错协议的容错能力为全网节点的 33%左右，并且在容错范围内系统无法出现分叉的情况。假设全网节点被分割成 3 个部分：

$$R=R_1\cup R_2\cup F \tag{10}$$

并且满足：

$$R_1\cap R_2=\varnothing,R_1\cap F=\varnothing,R_2\cap F=\varnothing \tag{11}$$

其中，R_1 和 R_2 是诚实节点，且已经形成网络孤岛；F 是非诚实节点，它们行动一致，同时 F 中所有节点可以和全网中任意节点进行消息传播。F 如果想要分叉，则需要和 R_1 达成共识并发布区块，并且在不通知 R_2 的情况下达成第二次共识，“撤销”与 R_1 的共识，需要满足：

$$|R_1|+|F|\geqslant n-f \tag{12}$$

$$|R_2|+|F|\geqslant n-f \tag{13}$$

而全网中恶意节点的最大值为：

$$|F|_{\max}=f \tag{14}$$

综合式(12)－式(14)可以得到：

$$|R_1|+|R_2|\geqslant 2n-4f \tag{15}$$

根据式(9)，化简式(15)得：

$$n\leqslant 3f \tag{16}$$

而全网中：

$$f=(n-1)/3 \tag{17}$$

与式(16)矛盾。

4.3.2 实验分析

本方案的仿真平台为：Inter(R) Core (TM) i7-4770 CPU，内存为 16 GB，操作系统为 Windows10 64 位。在联盟链的网络中取 150 个节点，对算法性能进行分析。

(1)本方案提供了一种快速检索的方法。如图 7 所示，当用户的数量较少时，本方案与其他的基于区块链的医疗方案相比，检索信息的时间没有优势；随着用户数量的逐渐增多，本方案的延迟时间明显缩短，这主要是因为本方案采用的方式可以直接引导用户查找相应的区块。因此，采用本方案进行检索能够高效率地得到信息并实现数据之间的共享。

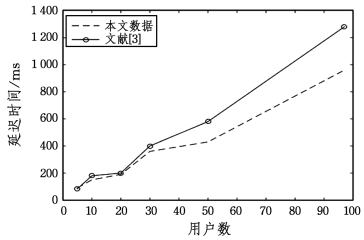

图 7 检索性能

Fig. 7 Retrieval performance

(2)本方案采用的是 DBFT 算法，它最多容忍的不诚实节点如式(17)所示，大概是全网节点数的 1/3。由图 8 可知，错误节点在 0～50 之间时，算法延迟呈下降趋势，说明该算法的容错机制能保证节点数满足医疗信息场景中生成区块的节点数；当错误节点数超过 50 时，延迟明显上升，且在半数节点为错误节点时，共识网络宕机。信息交易区块的高度如表 1 所列，随着诚实节点数量的逐渐减少，生成的区块链数目也逐渐减少，并且生成区块的速度也变慢。

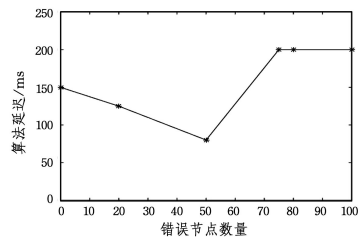

图 8 DBFT 算法的延迟

Fig. 8 Delay time of DBFT algorithm

表 1　高度对比

Table 1　Height comparison

诚实节点数	非诚实节点数	区块高度
150	0	5000
130	20	2912
100	50	2875
75	75	860
80	70	859
50	100	858

(3)将本文方案与文献[9]所采用的共识机制 PBFT 进行吞吐量的比较。

在节点数量为 50，100，150 时，DBFT 和 PBFT 的吞吐量比较如表 2 所列。从表中可以看出，在相同网络环境条件下，DBFT 算法的性能均优于 PBFT 算法，平均吞吐量提升了 8%左右。

表 2　吞吐量对比

Table 2　Throughput comparison

节点数量	DBFT/TPS	PBFT/TPS
50	158.2	135.3
100	148.5	135.9
150	146.3	135.6

4.3　医疗信息链和健康链的综合比较

健康链[6]是一个新近提出的基于区块链的数据存储共享方案，该系统中的医疗记录由病人存储在云上，以实现数据的加密和共享。健康链和信息链在安全性和性能方面的综合比较如表 3 所列。通过比较可知，本文提出的方案在容错率、检索效率等方面有较好的优势。

表 3　性能对比

Table 3　Performance comparison

方案名称	吞吐量	可扩展性	防篡改	安全存储	检索效率
健康链	低	弱	高	安全	较低
信息链	高	高	高	安全	较高

结束语　我国医疗信息化发展已有 10 年，但是电子数据易受到黑客的攻击，而区块链技术在医疗互联网上的使用能保证数据的安全性，并能在方便监管的同时提高了资源的利用率。本文结合现代医疗＋互联网的实际需求，在医疗信息存储方面，提出了一种基于区块链技术的安全存储。改进的拜占庭协议保证了医疗信息系统中网络节点的共识，并将数据存放在链下的数据库中，通过访问控制协议实现了医疗数据的共享。仿真实验表明，该模型在安全性、稳定性、吞吐量等方面都有较好的表现。

区块链上的信息是具有不可篡改性的，这是以私钥安全为前提的。如果私钥丢失，安全存储将不存在，下一步将重点围绕该问题展开研究。

参 考 文 献

[1] ESPOSITO C，SANTIS A D，TORTORA G，et al. Blockchain：A Panacea for Healthcare Cloud-Based Data Security and Privacy?[J]. IEEE Cloud Computing，2018，5(1)：31-37.

[2] ZYSKIND G，NATHAN O，ALEX P. Decentralizing Privacy：Using Blockchain to Protect Personal Data[C]// 2015 IEEE Security and Privacy Workshops (SPW). IEEE Computer Society，2015.

[3] AZARIA A，EKBLAW A，VIEIRA T，et al. MedRec：Using Blockchain for Medical Data Access and Permission Management[C]// 2016 2nd International Conference on Open and Big Data (OBD). IEEE，2016.

[4] YUE X，WANG H，JIN D，et al. Healthcare Data Gateways：Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control[J]. Journal of Medical Systems，2016，40(10)：218.

[5] METTLER M. Blockchain technology in healthcare：The revolution starts here[C]// 2016 IEEE 18th International Conference on e-Health Networking，Applications and Services (Healthcom). IEEE，2016.

[6] MEI Y. Research on Blockchain Method of Secure Storage Medical Record[J]. Journal of Jiangxi Normal University (Natural Science)，2017，41(5)：481-487.

[7] XIA Q，SIFAH E B，ASAMOAH K O，et al. MeDShare：Trustless Medical Data Sharing Among Cloud Service Providers Via Blockchain[J]. IEEE Access，2017，PP(99)：1-1.

[8] DUBOVITSKAYA A，XU Z，RYU S，et al. Secure and Trustable Electronic Medical Records Sharing using Blockchain[C]// Annual Symposium Proceedings/AMIA Symposium. AMIA，2017.

[9] HOY M B. An Introduction to the Blockchain and Its Implications for Libraries and Medicine[J]. Medical Reference Services Quarterly，2017，36(3)：273-279.

[10] SHAE Z，TSAI J J P. On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine[C]// IEEE International Conference on Distributed Computing Systems. IEEE，2017：1972-1980.

[11] HOY M B. An Introduction to the Blockchain and Its Implications for Libraries and Medicine[J]. Medical Reference Services Quarterly，2017，36(3)：273-279.

[12] XUE T F，FU Q C，WANG W，et al. Research on medical data sharing model based on blockchain[J]. Acta Automatica Sinica，2017(9)：73-80.

[13] CHA H J，YANG H K，SONG Y J. A Study on Access Structure Management of CP-ABTD Based Blockchain for Medical Information Monitoring System[J]. Advanced Science Letters，2018，24(3)：2026-2030.

[14] ANTONOPOULOS A M. Mastering Bitcoin：unlocking digital cryptocurrencies [M]. Sebastopol O' Reilly Media，Inc，2014.

[15] CHRISTIDIS K，DEVETSIKIOTIS M M. Blockchains and Smart Contracts for the Internet of Things[J]. IEEE Access，2016，4：2292-2303.

[16] WANG H，SONG Y. Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain[J]. Journal of Medical Systems，2018，42(8)：152.

[17] ANDROULAKI E，BARGER A，BORTNIKOV V，et al. Hyperledger Fabric：A Distributed Operating System for Permissioned Blockchains[C]// Proceedings of the Thirteenth Eurosys Conference. ACM，2018.

[18] PEI-KUN N I，BUSINESS S O，UNIVERSITY Q. Study on Value of Blockchain Technology in Medical Field[J]. Journal of Medical Informatics，2018，39(2)：9-13.

[19] WANG H L，RHEUMATOLOGY D O，HOSPITAL G. Application Prospect of Blockchain Technology in Traditional Chinese Medicine[J]. Journal of Guiyang University of Chinese Medicine，2017，39(3)：1-4.

[20] FUNK E，RIDDELL J，ANKEL F，et al. Blockchain Technology：，A Data Framework to Improve Validity，Trust，and Accountability of Information Exchange in Health Professions Education[J]. Academic Medicine，2018，93(12)：1.

[21] MA X F，DU M X，YU W B，et al. A Supply Chain Financial Service Platform Based on Blockchain[J]. Big Data，2018，4(1)：2018002.