基于联盟链的医联体应用研究

Application Research of Medical Alliance Based on Consortium Chain

冯霄鹏[1]，夏俊杰[2]，章　峰[1]，孙　晔[1]（1. 北京电信规划设计院有限公司，北京 100044；2. 中国联通智能城市研究院，北京 100044）

Feng Xiaopeng[1]，Xia Junjie[2]，Zhang Feng[1]，Sun Ye[1]（1. Beijing Telecom Planning&Designing Institute Co.，Ltd.，Beijing 100044，China；2. China Unicom Smart City Research Institute，Beijing 100044，China）

摘　要：

针对医联体存在的数据共享慢、信息安全风险高、运维成本高等问题，提出基于联盟链的医联体架构。将各个参与方作为参与节点，为不同的节点设置不同的数据通道，为不同的组织结构和业务部门设置不同的权限等级，使用SM2对信息和人员进行加密验证，并对联盟链平台进行了测试，测试结果表明平台可以稳定地运行，联盟链的TPS可以稳定在2 235左右。基于联盟链的医联体应用进一步完善了医联体的分级诊疗、医疗服务、可信管理等功能。

关键词：

医联体；联盟链；权限控制；数据交易

doi：10.12045/j.issn.1007-3043.2020.11.001

文章编号：1007-3043（2020）11-0001-06

中图分类号：TP391

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Aiming at the problems of slow data sharing，high information security risks，and high maintenance costs of the medical alliance，the medical alliance architecture based on the consortium chain is proposed. Each participant is regarded as the participating node，different data channels are set for different nodes，different authority levels are set for different organizations and departments，and SM2 is used to encrypt and verify information and personnel. Finally，the implemented consortium chain platform is tested，and it is found that it can work stably，and the TPS of the consortium chain can be stabilized at around 2 235. The medical alliance application based on the consortium chain further improves the medical alliance's hierarchical diagnosis and treatment，medical services，credible management and etc.

Keywords：

Medical alliance；Consortium chain；Access control；Data transaction

引用格式：冯霄鹏，夏俊杰，章峰，等. 基于联盟链的医联体应用研究[J]. 邮电设计技术，2020（11）：1-6.

0 引言

2013年9月，信息化和工业部在《信息化发展规划》中，提出创立全面的电子病案和居民健康档案，通过开展卫生信息化区域试点，最终实现医疗服务、公共卫生服务等的数据共享和互通有无。在当下，随着信息化建设的快速发展，北上广深等一线城市信息化的不断展开，信息化工具已经融入了医院管理的各个方面，其中包括医院的信息系统、远程诊疗系统、药品管理系统以及办公自动化系统。但是，很多地方的中小医院的信息化建设还是相当落后，甚至有不少的二级医院仍旧处在传统的信息化状态，没有实现信息化管理，工作效率极其低下。我国提出了医疗联合体的医改方案，来合理配置区域医疗资源，提高区域内的医疗服务效率。但是，目前国内主流的医疗机构都是公立医疗资源，所以大部分医联体都是由政府出面强行进行整合，存在着各种问题亟待解决。

a）医联体中的各个医院数据没有及时同步，存在明显的信息不对称和较高的数据冗余。病人的信息无法及时同步，容易造成人力物力的浪费，使得医疗卫生服务碎片化。

收稿日期：2020-10-09

b)国内的医疗一般都是由相关机构进行监管,缺乏来自患者的真实意见。并且,监管中存在灰色地带,部分环节无法得到直接的监管。

c)随着越来越多的设备接入到互联网中,信息安全问题日益突出,医疗行业的数据维护成本开始增加。

针对现有的医联体存在的问题,本文提出基于联盟链的可信医联体应用,通过联盟链技术带来的去中心化、数据一致性、不可篡改、可追溯、共同维护等特性,对医联体中的数据进行加密,实现可信高效的数据共享,提高数据安全性,保证操作的可追溯、可审计,医联体中的设备共同维护全部的医疗数据,提高数据的透明度,减少医患纠纷。

1 区块链技术

自2008年起,比特币开始出现并蓬勃发展,区块链技术开始进入人们的视野,引起了极大的关注。现在各国都纷纷进行区块链的投资研发,区块链已经进入区块链3.0时代。狭义的区块链是一种时序数据区块,相互连接组成一种链式结构,用密码学方式来确保分布式账本的不可篡改和不可伪造。广义的区块链技术是利用块链式数据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,利用密码学的方式保证数据传输和访问的安全,利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。区块链技术具有去中心化、追踪溯源、不可篡改、可编程和集体维护等特性。有5种应用模式,即公有链(Public blockchain)、联盟链(Consortium blockchain)、私有链(Private blockchain)、混合链(Hybrid blockchain)和许可链(Permissioned blockchain)。

一般来说,区块链系统由数据层、网络层、共识层、合约层和应用层5部分组成。区块链架构如图1所示。

在区块链系统中,最底层的原始数据需要进一步加工才能存储到区块之中。底层数据最根本的是信息记录,其他的数据只是为了对信息记录进行封装。该过程涉及哈希算法、Merkle树和时间戳等技术。

网络层封装了区块链的组网模式、消息传播协议、数据验证机制等要素。在设定的消息传播协议与数据验证机制下,能够让区块链中的所有节点或者是大部分节点都能够参与到区块数据的验证与记账过

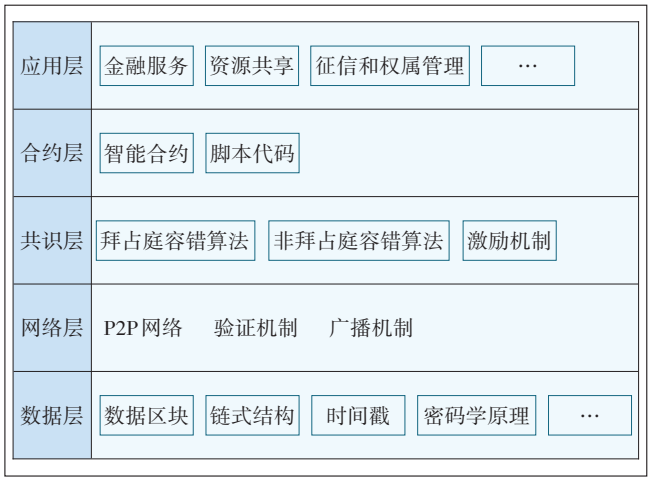

图1　区块链架构

程中,当大部分节点对区块数据校验成功后,区块数据才能记入区块中。

共识机制是为了保证分布式账本的所有节点所存储信息的准确性与一致性而设计的一套机制,就像社会系统中"民主"和"集中"的对立关系,决策权越分散的系统达成共识的效率就越低,但是系统的满意度和稳定性会越高;反之,决策权越集中的系统越容易达成共识,但是整个系统的满意度和稳定性也就会降低。共识机制的设计主要是由业务与性能的需求决定的,从PoW到PoS再到DPoS和Paxos以及各种拜占庭容错算法,共识机制不断创新,区块链平台性能也得到大幅提升。

合约层主要封装了区块链系统运行中需要的各类脚本代码、算法以及由此生成的更为复杂的智能合约。数据、网络和共识这三层可作为区块链底层,分别承担数据表示、数据传播和数据验证,合约层是建立在区块链底层之上的逻辑、算法或者说是规则策略,从而实现区块链系统灵活编程和操作数据等功能。

合约层的一个相关概念就是智能合约。智能合约是20世纪90年代由Nick Szabo提出的,几乎与互联网同龄。那个年代由于缺少可信的执行环境,智能合约并没有被应用到实际产业中,自比特币诞生后,人们认识到比特币的底层技术区块链可以为智能合约提供可信的执行环境。一个成功的案例就是,以太坊看到了区块链和智能合约的契合点,发布以太币,打造以太坊平台。智能合约的运行机制如图2所示。

区块链技术的出现,为可信医联体的架构提供了技术基础,可以更加高效地促进医联体的发展与合

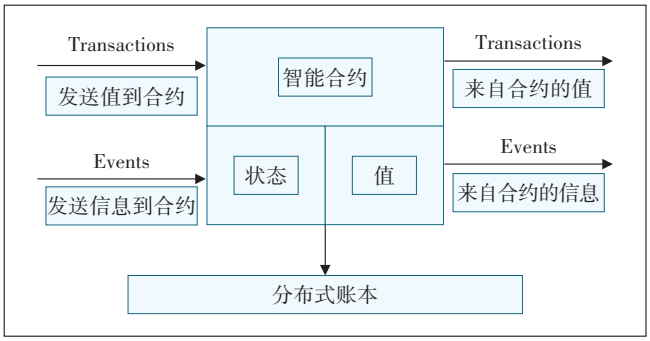

图2　智能合约的运行机制

作。

2 可信医联体

2.1 整体架构

为了更好地整合医疗资源，提高服务效率，实现分级诊疗。医联体中涉及到大型医院、基层医疗卫生机构、药品企业、监管部门等多个部门，且各部门之间是相互平等的，不应存在中心化节点。因此，本文将医联体中涉及到的多个部门设置称为联盟链中的各个节点，参与到联盟链中，构成一条医联体联盟链，具体架构如图3所示。

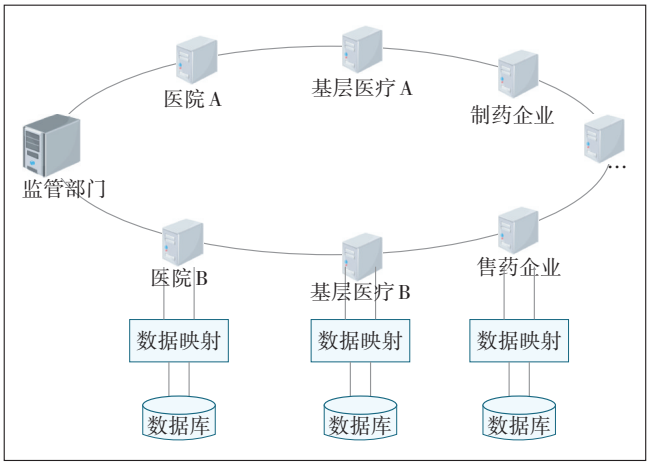

图3　可信医联体架构

图3中的数据映射功能主要是将已有的数据库中的内容，映射上传到联盟链中，同时也负责将联盟链中的数据通过数据映射存储到数据库中。

基于联盟链的可信医联体应用的整体功能架构如图4所示，底层的运行环境是通过云上的容器服务实现快速部署，结合本地服务器的现有计算资源，最大程度降低整个医联体联盟链的建设成本，更加快速地构建可信医联体，更快地投入应用。

2.2 功能设计

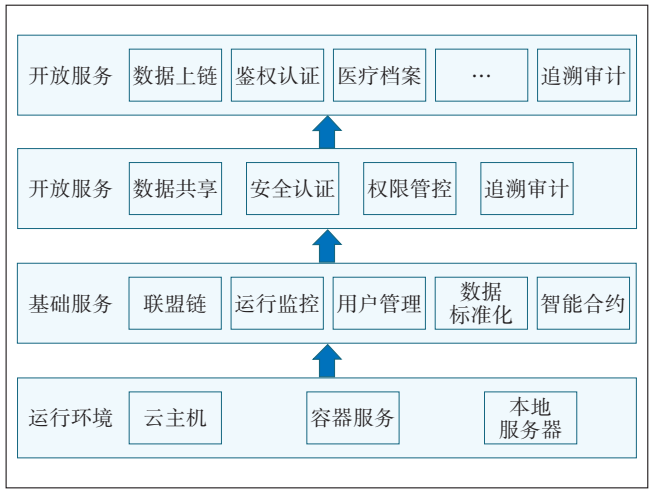

图4　功能架构

为了更好地统筹管理整个可信医联体联盟链，每一个联盟链中的用户都将在注册信息后，获取到一个全局唯一的层次化的ID，比如北京A医院的B部门的C员工，身份编号为0123，系统将自动为其生成一个唯一的ID：CN.A.B.C.0123。每一位注册的新员工都将由联盟链生成的唯一的公私钥来进行用户身份的认证，确保联盟链中记录的对应操作、相关数据都是真实有效的。

2.2.1 数据共享

医联体中的人员利用自己的私钥信息登录到医联体联盟链后，通过联盟链数据上传合约上传患者的信息，在联盟链中构建患者的健康档案。上传数据的时候，需要人员的私钥信息对上传的数据进行签名，同时联盟链还将根据操作人员的ID自动生成该档案信息的来源组织，确保整个患者健康档案的真实可信。

因为医联体中存在的不同的机构组织，不同的机构组织负责不同的业务数据，所以医联体联盟链为不同的机构组织设置不同的数据通道，避免机构组织、不同职责的负责人访问不属于自身业务范围的数据，增加医联体联盟链中的安全性与数据隐私性。

医联体中医院的专家需要获取患者的病例或者健康档案的时候，需要使用自身的私钥进行合约验证，验证通过后才可以向医联体联盟链发起数据请求。联盟链将获取到的患者档案通过申请者的公钥信息加密，然后进行传输，申请者通过使用自身的私钥对加密信息进行解密，获取到相关的信息。具体流程如图5所示。

2.2.2 权限控制

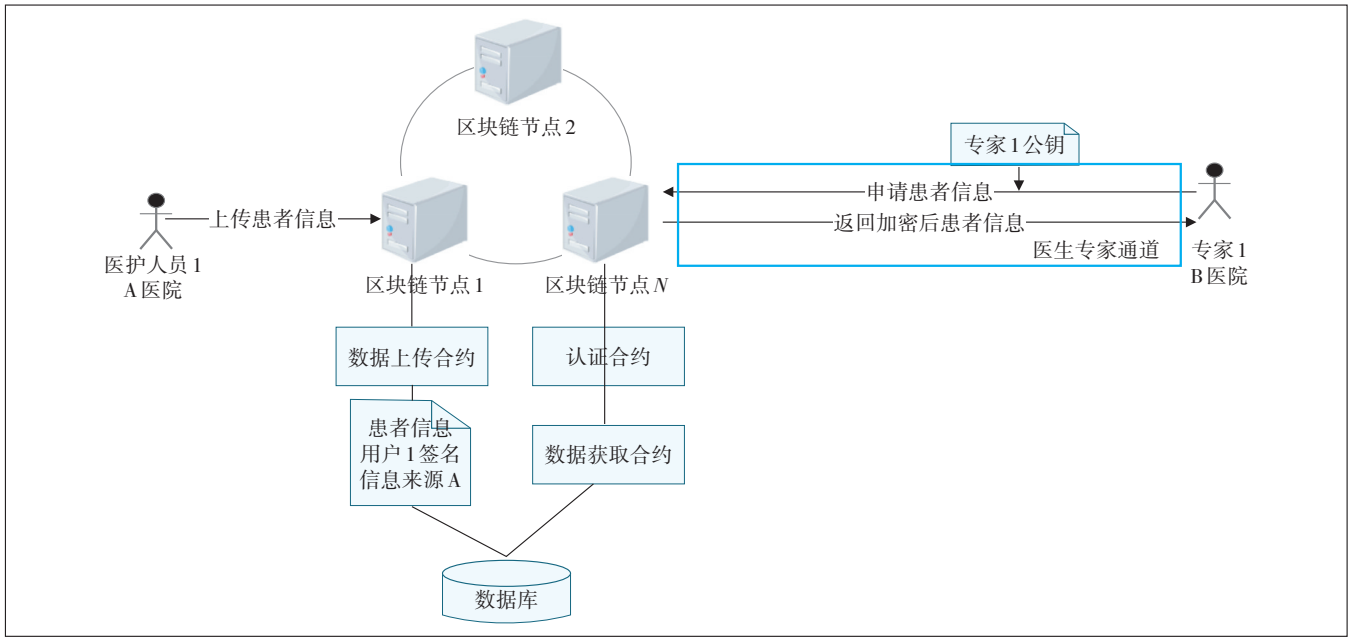

图5　数据上链与获取

为了进一步加强医联体中不同部门的信息安全等级,本文设计了不同的权限等级控制机制。不同科室的医生和不同级别的专家具备不同的浏览权限,不同的机构之间也有着不同的浏览权限,不同机构组织的人员权限,由机构组织根据职位、部门分发权限等级。本文设立了三级权限分级,具体分级如图6所示。

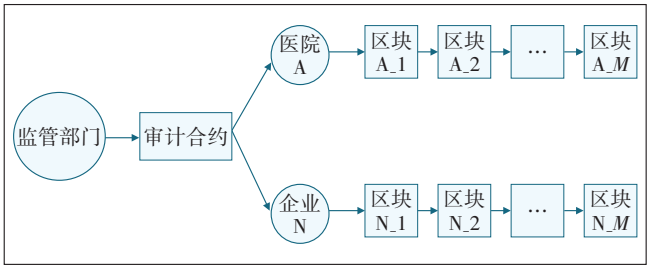

图6　权限分级

由于整套医联体联盟链中存在监管部门,且监管部门处于最高的三级权限,负责审计医联体联盟链中的全部数据。所以,本文在设计不同机构部门在联盟链中的数据通道、监管部门最终的审计时,也将按照不同的机构部门进行分类,分别记录不同的操作、信息、数据,交由监管组织进行审计,如图7所示。

3 实验分析

本文在Hyperledger的Fabric的基础上,实现了医联体联盟链底层平台。本节针对实现的联盟链平台进行实验测试。测试环境如表1所示。

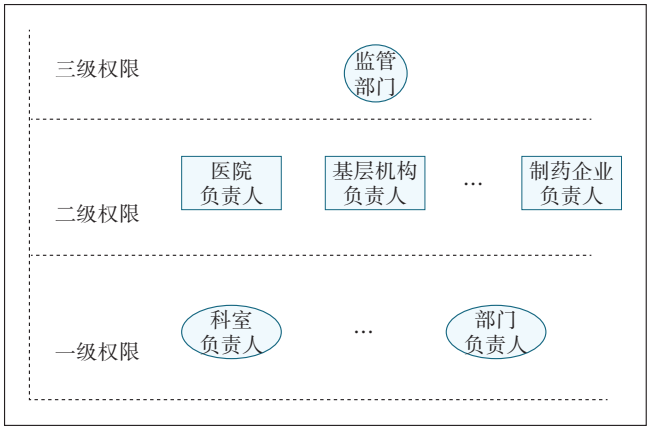

图7　监管审计

表1　测试环境

节点数	节点配置	网络带宽	共识机制	密码学算法
22台	24C128G	万兆	Kafka	SM2

3.1 高并发测试

在联盟链平台测试环境下,1 s内发送5万笔交易请求,交易包括不同的类型:身份认证、档案查询、信息提交等。在高并发的情况下,吞吐量达到2 235 tps。Orderer节点和Peer节点的内存占比如图8和图9所示,从图8和图9中可以发现,整体的运行情况较为平稳。

3.2 压力测试

在设置4个共识节点的情形下,我们设计了压力测试,不停地发送交易,使压力维持在较高的水平(未

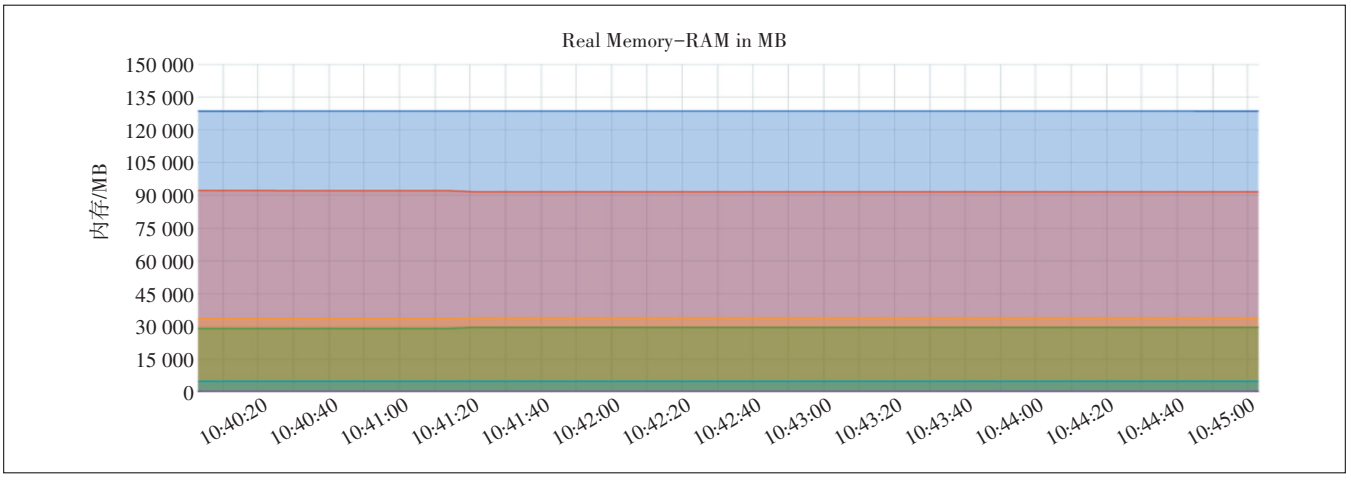

图8　Orderer节点内存运行

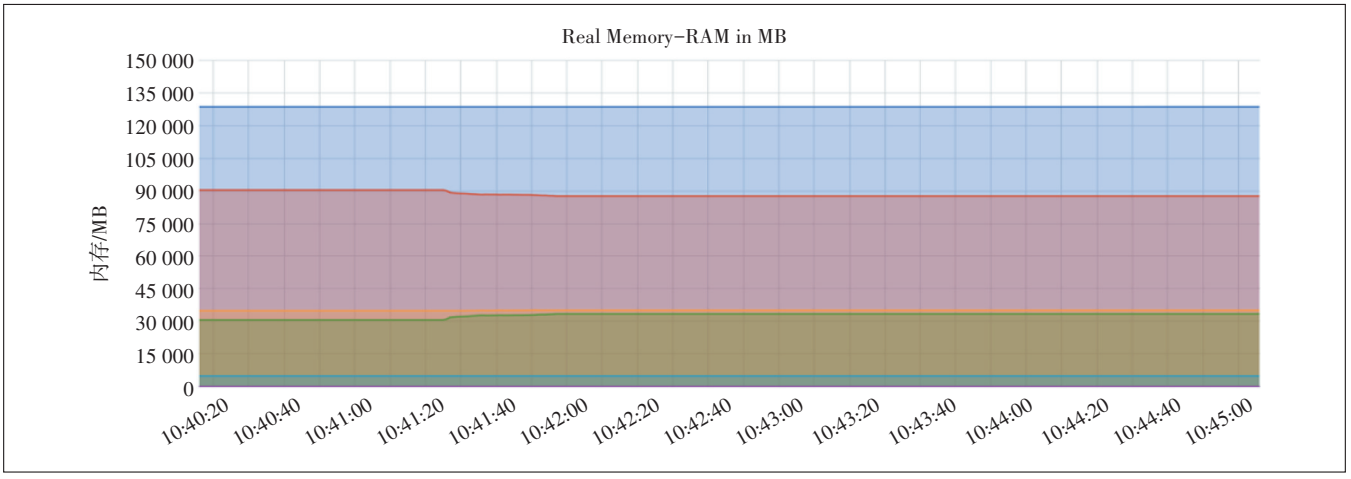

图9　Peer节点内存运行

处理交易保持在1 000以上),且持续运行1 h。Orderer与Peer节点网络消耗如图10和图11所示,从图10和图11可以发现,平台在压力测试的情况下仍然可以保证平稳的效率。

本文针对医联体联盟链中使用的SM2算法进行了测试,测试结果如表2所示。

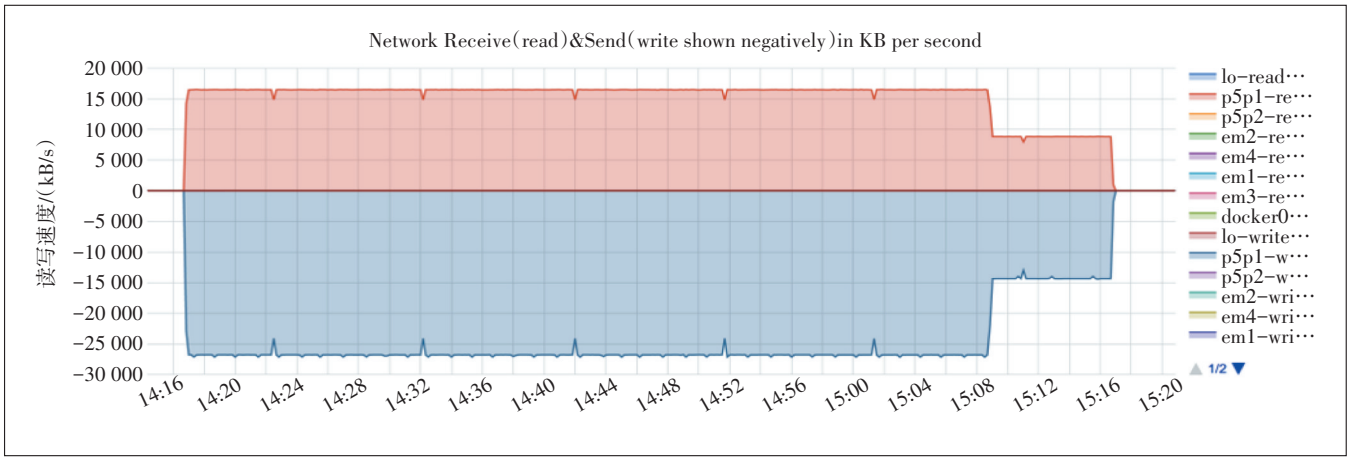

图10　Orderer节点网络消耗

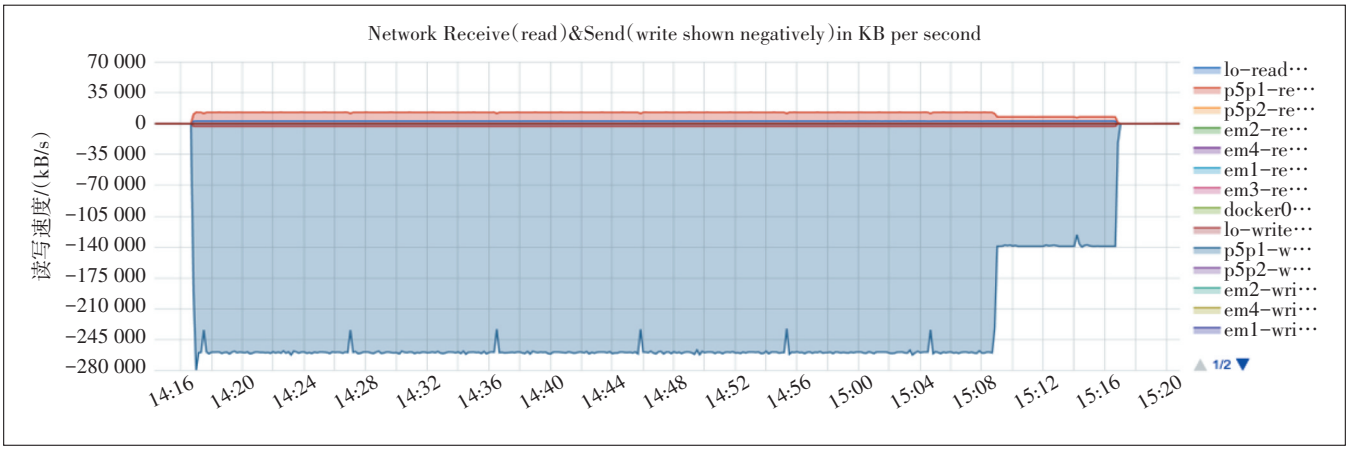

图11　Peer节点网络消耗

表2　SM2性能测试

SM2	次数	总耗时/s	平均耗时/(ms/op)
签名	1 000	1.218 104	1.218
验证签名	1 000	8.580 483	8.580
加密	1 000	9.812 299	9.812
解密	1 000	5.597 929	5.597

上述测试表明，基于联盟链的医联体应用可以良好稳定地运行，具备良好的安全控制，能够满足医联体的交易需求、安全需求，提高数据共享效率，减少运维成本，增加安全与透明程度。

4 总结

本文提出了基于联盟链的可信医联体构建方式，并且基础平台的测试数据较为理想，基本可以满足医联体的日常事务处理效率，大大的提高了不同机构之间的数据交换效率，提出的权限控制机制，则可以大大的提高不同业务部门的数据安全性以及透明程度，方便监管部门的监督、审计。

参考文献：

[1] 章峰，史博轩，蒋文保．区块链关键技术及应用研究综述[J]．网络与信息安全学报，2018，4(4)：22-29.

[2] ZHANG F，JIANG W，SHI B. TAC：A unified trust anchor framework based on consortium blockchain[C]//Journal of Physics：Conference Series. IOP Publishing，2020，1544(1)：012181.

[3] 史博轩，章峰，蒋文保．基于Zookeeper的全网统一信任锚模型研究[J/OL]．计算机应用研究：1-5[2020-08-10]．https://doi.org/10.19734/j.issn.1001-3695.2019.08.0568.

[4] 夏俊杰，孙晔，杨海涛，等．基于区块链的数据资产保护与交易平台研究及应用[J]．邮电设计技术，2019(9)：5-9.

[5] 黄敬英，范勤勤．区块链技术在医联体建设中的应用探讨[J]．医学信息学杂志，2019，40(10)：30-34.

[6] CACHIN C. Architecture of the hyperledger blockchain fabric[C]//Workshop on distributed cryptocurrencies and consensus ledgers，2016：310.

[7] Decentralized Identifiers (DIDs)：Data Model and Syntaxes for Decentralized Identifiers [EB/OL]．[2020-03-29]．https://w3c-ccg.github.io/did-spec/.

[8] NAKAMOTO S. Bitcoin：A peer-to-peer electronic cash system[EB/OL]．[2020-07-08]．https://blog.csdn.net/yingkee/article/details/53888910.

[9] KALODNER H A，CARLSTEN M，ELLENBOGEN P，et al. An Empirical Study of Namecoin and Lessons for Decentralized Namespace Design[C]//WEIS. 2015.

[10] WILCOX-O'HEARN Z. Names：Distributed，secure，human-readable：Choose two[J]．2001.

[11] ALI M，NELSON J，SHEA R，et al. Blockstack：A global naming and storage system secured by blockchains[C]//2016 {USENIX} Annual Technical Conference ({USENIX}{ATC} 16)．2016：181-194.

[12] BENET J. Ipfs-content addressed，versioned，p2p file system [J]．arXiv preprint arXiv：1407.3561，2014.

[13] BENSHOOF B，ROSEN A，BOURGEOIS A G，et al. Distributed decentralized domain name service[C]//2016 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)．IEEE，2016：1279-1287.

[14] LAMPORT L. Paxos made simple[J]．ACM Sigact News，2001，32(4)：18-25.

作者简介：

冯霄鹏，北京电信规划设计院有限公司总工程师，高级工程师，主要从事数据通信网络、互联网、数据中心、区块链、行业信息化及政企ICT领域相关规划和咨询设计工作；夏俊杰，中国联通智能城市研究院副院长，教授级高级工程师，主要从事智慧城市和网络安全领域的规划和咨询工作；章峰，工程师，硕士，主要从事区块链技术与智慧城市应用场景结合工作；孙晔，北京电信规划设计院有限公司，智慧城市设计院创新业务总监，硕士，主要从事区块链解决方案的设计与其在智慧城市、智慧园区等场景的落地应用工作。