華中科技大學

本科生毕业设计[论文]

面向智慧医疗的区块链底层数据交换系统设计和实现

院　　系　电子信息与通信学院

专业班级　电信（种子）1601 班

姓　　名　李泽霖

学　　号　U201617159

指导教师　黑晓军

2020 年 5 月 20 日

学位论文原创性声明

（黑体小 2 号加粗居中）

本人郑重声明：所呈交的论文是本人在导师的指导下独立进行研究所取得的研究成果。除了文中特别加以标注引用的内容外，本论文不包括任何其他个人或集体已经发表或撰写的成果作品。本人完全意识到本声明的法律后果由本人承担。

（宋体小 4 号）

作者签名：　　年　　月　　日

学位论文版权使用授权书

（黑体小 2 号加粗居中）

本学位论文作者完全了解学校有关保障、使用学位论文的规定，同意学校保留并向有关学位论文管理部门或机构送交论文的复印件和电子版，允许论文被查阅和借阅。本人授权省级优秀学士论文评选机构将本学位论文的全部或部分内容编入有关数据进行检索，可以采用影印、缩印或扫描等复制手段保存和汇编本学位论文。

本学位论文属于 1、保密□，在　　年解密后适用本授权书

2、不保密□　。

（请在以上相应方框内打“√”）

（宋体小 4 号）

作者签名：　　年　　月　　日

导师签名：　　年　　月　　日

（注：此页内容装订在论文扉页）

摘 要

区块链是用分布式数据库识别、传播和记载信息的智能化对等网络，而智慧医疗是未来医疗发展大方向。如今随着新基建概念提出，智慧医疗也是一个重点研究方向。本文提出了一个系统模型，将区块链技术应用于智慧医疗应用，推动个人医疗数据的分享和应用，并明确了在智慧医疗的物联网场景中，如何使用区块链系统增强穿戴式通信设备的安全性。

本文应用自主设计的智慧医疗-区块链系统，从网络通信到共识算法,从共识算法到上层应用,均是自主设计和实现。该系统能满足智慧医疗场景下应用功能；同时结合物联网边缘计算特性，保证了穿戴式设备数据的存储、交换和隐私保护。本文也对该系统进行了性能测试、稳定运行测试和资源占用评估，保证系统真实可用。

关键词：区块链；智慧医疗；系统设计，系统模型；性能测试；边缘计算

Abstract

Blockchain is an intelligent peer-to-peer network that uses distributed databases to identify, disseminate and record information; smart healthcare is the future of medical development. Nowadays, with the new concept of infrastructure, smart healthcare is also a key research direction.

This article proposes a system model that applies blockchain technology to smart medical applications, design and implementation of the underlying data exchange system of blockchain for intelligent medical care promotes. The system provides the sharing and application of personal medical data, and clarifies how to use the blockchain system to enhance wearable communication devices in the smart medical IoT scenario Security. In this paper, the self-designed smart medical-blockchain system can be used to meet the application functions in the smart medical scene; at the same time, combined with the edge computing characteristics of the Internet of Things, it ensures the storage, exchange and privacy protection of wearable device data. This article also conducted performance tests, stable operation tests, and resource occupancy evaluations of the system to ensure that the system is truly usable.

Key Words： Blockchain; Smart healthcare; System design, system model; performance testing; edge computing

目 录

1 绪论

1.1 研究背景与意义

区块链（英语： blockchain 或 block chain）是分布式数据库的一个分支, 也称为价值互联网。现在，区块链技术发展迅速，并已应用于许多领域，例如智能驾驶，电力资源管理（绿色网格），计算分配和智慧医疗等。众所周知，与传统的集中式系统相比，区块链和分布式系统可以提供更安全，更私有的服务，具有更好的容错能力。这就是为什么我选择区块链系统作为我的研究主题的原因。同时，区块链技术已经成为许多领域的新技术应用典范。智慧医疗在 5G 时代能发挥巨大的作用，所以我们想要建立一个面向智慧医疗的区块链底层系统。区块链作为技术基础和基础平台，能在智慧医疗的数据管理上解决集中式数据管理策带来的问题。通过这项研究，我们可以开展其他基于区块链技术的重要研究。

在智慧医疗的场景下，物联网需要处理私有和敏感数据。例如，许多家庭选择在他们的房屋中部署监控器，以在小偷闯入或年长者摔倒时引起注意。但是同时我们也需要知道，这些监控数据和图像非常私密且敏感，没有人希望这些图像泄漏出去。此外，我们需要针对这些情况构建一个安全且受信任的数据共享网络。区块链技术正好能提供这样安全的特性。建立在区块链架构之上的应用不用担心自己的数据被数据提供商盗窃和获取，因为在区块链架构中不会有一个中心化的数据管理服务商。不过，可惜的是，许多区块链项目或系统运行速度不太尽如人意。而且因为区块链上的数据是公开的，不允许存储私人和个人数据。与此同时，智慧医疗会产生很多数据，大部分的数据不必存储下来，但是也有部分数据需要存储：诊疗的结果、诊断的片子和处方药单等等。除了智慧医疗应用的部分信息，还有区块链网络的维护信息也需要存储下来。比如智慧治疗设备的行为、网络接入许可和数字货币的使用记录等等。现有的区块链架构比如比特币、以太坊是公有链，速度比较慢而且节点接入不需要许可（permissionless）。同时现有的区块链架构的数据存储是公开的，所有节点只需要同步区块即可获取合约信息，而智慧医疗的数据需要加密，所以需要改进。

本论文研究区块链技术如何应用于智慧医疗应用，推动个人医疗数据在链上的持久化。我们也需要研究以下问题：在智慧医疗的物联网场景中，如何使用区块链系统增强穿戴式通信设备的安全性、如何增强数据传输时的私密性是我们的

重点问题。区块链系统是一个安全可信的分布式计算系统，比传统的中心化系统更稳定更安全。随着区块链新的技术和边缘计算的新算法的提出，区块链系统的响应速度有很大的提升。我们的系统设计使用联盟链的架构设计，通过应用自主设计的区块链智慧医疗系统，能满足智慧医疗场景下，穿戴式设备数据的存储、交换和隐私保护。

1.2 区块链技术发展现状

区块链是一项技术，综合了计算机网络，密码学，物联网，社会经济学，金融学等多学科。区块链不等同于数字货币，更加不等同于比特币；区块链可以为非常多的应用提供技术支持，它的应用可以衍生到数字金融、智能制造、供应链管理、数字资产交易等多个领域。目前，全球的主要国家都在加快布局区块链技术发展。比如就有美国众议院议员就大力支持 FaceBook 的 libra 数字货币，并对标中国在该领域的发展进度。中国理应抓住机会，利用我国区块链技术的良好基础，继续巩固区块链技术在全球发展的前列位置。习近平主席在中央政治局第十八次集体学习中指出，要探索“区块链+”在民生领域的运用，积极推动区块链技术在各个领域的应用。其中重点提到了医疗健康和社会救助两个领域，可见区块链+智慧医疗是未来“区块链+”的一个重要研究领域。

随着计算机科学的发展，区块链技术也发展迅速，并已实际应用于许多领域，例如智能驾驶，电力资源管理（绿色网格），计算分配和智慧医疗等。众所周知，与传统的集中式系统相比，区块链和分布式系统可以提供更安全，更私有的服务，具有更好的容错能力。日前，除了比特币的 POW 共识算法，其他更优的算法层出不穷。比如以太坊的 POW+POS 共识算法，EOS 的 DPOS+PBFT 共识算法，还有 Libra 的 LibraBFT 共识算法等等。这些新算法的提出大大提升了区块链技术的多样性，也大大提升了区块链应用的使用范围。因为区块链技术是分布式系统的一个分支，而分布式系统中有一个不可能三角（即这三个特性无法同时满足）--CAP 原则。CAP 原则分别是强一致性（consistency），可用性（availability），分区容忍性（partition tolerance）。而对于一个大规模分布式数据系统来说，CAP 三要素是不可兼得的，同一系统至多只能实现其中的两个，而必须放宽第 3 个要素来保证其他两个要素被满足。一般在网络环境下，运行环境出现网络分区是不可避免的，所以系统必须具备分区容忍性(P)特性，所以在一般在这种场景下设计大规模

分布式系统时，往往在 A 或者 C 中选择一个进行舍弃。不同的共识算法正是在 CAP 三个选项中进行了平衡和取舍，比如 POW 的强一致性和分区容忍性比较出色，但是这个导致了可用性会有一定降低，表现在 TPS（性能速度）的降低；而 EOS 的 DPOS+PBFT 舍弃了强一致性，将出块的权力进行了一部分的集中，但是这个做法也大大提升了共识算法的性能，是 POW 共识算法的性能上千倍的提升。正是因为区块链技术发展和各种新型共识算法的提出，才让我们的系统有了更加合适的选择。

除了区块链底层技术的发展，区块链在各个地方的应用也发展迅速。区块链在数字货币和货币国际化有着推动作用。中国银行推出了中国的数字货币，收到中国银行的监管，但是可以在全世界范围内进行结算而不用计算人民币的国际汇率。这是推动中国金融走向世界的一个缩影。所以，区块链底层技术的发展必须结合其他实际的应用场景，才能发挥它更大的作用。

1.3 智慧医疗产业生态发展现状

智慧医疗的说法在 2017 年就已经被提出来了，并和新基建一起，是国家重点发展的计划之一，邬贺铨（2017）和潘峰（2019）都提出了智慧医疗未来的应用场景。在过去的半年里，中国和世界经历了新型冠状病毒的袭击。在这次疫情中，大数据和人工智能在“抗疫”战役中表现出了自己的特色和作用。丁香医生的数据及时发布，让广大民众能及时获取最新的疫情信息。还有健康码和各类互联网消息平台的建立，也助力了

疫情常态化防控的政策部署。除此之外，因为疫情严峻，为了防止人员聚集，医院现在大力推广线上挂号、错峰就诊、电子病历等等的先进服务，将医疗和就诊真正的“智慧化”。

除了在这次疫情智慧医疗体现出来的作用，智慧医疗在很多领域也表现出自己的强大作用。比如在现在的远程医疗、重点城市的专家远程指导农村医生进行诊断等方面都有良好的应用。同时，随着 5G 和物联网的发展，智慧医疗产业生长地更加完善和茁壮；在农村地区、经济不发达的地区，智慧医疗能产生巨大的能量，大大提升村民和农民的健康水平。在国家的《健康 2030》计划中，提出了这么一个口号“医疗健康大数据‘开放共享、深度挖掘和广泛应用’”。这其中在大数据方面，可以应用区块链来保护数据的安全、降低运营成本和增强对数据的监管。

在智慧医疗发展程度还不够完善，一切都是一片蓝海的情况下，本文的区块链+智慧医疗系统将是一个有用且有前景的尝试。

1.4 智慧医疗+区块链的主要研究内容

本论文是建立基于安全，高效的面向智慧医疗的基础区块链架构：使用高速的共识算法优化现有的私有和敏感的数据传输系统。本文同时也研究区块链中的挖矿机制的方案和接入的安全验证方法。如今，数据传送系统存在许多问题。最严重的问题是如何保护私有数据。所有用户数据（例如聊天记录，电子邮件，图片）上传到中心架构并存储在中心架构中，可能会带来不可预测的风险。比如美国政府就曾多次要求苹果公司将客户信息透露，协助美国政府进行调查。这样的风险是不可控的，如果被别有用心的人非法利用，后果不堪设想。

本论文将设计一个基本智慧医疗-区块链系统，以支持具有私有和敏感数据的智慧医疗应用 - 病人的状态监测、医生的诊断和物联网设备的隐私数据上传等。使用该系统，这些应用可以拥有安全性和分布式双重特征。而且本论文提出的智慧医疗-区块链系统可以支持我们的智慧医疗上层应用，提供可支持实际应用的交易速度、可控的。为此，该联盟链系统被设计为实用工具，有科学的运行速度、稳定的性能和足够的拓展性。本论文提出的架构主要解决如下几个问题：

首先是中心化服务商泄露隐私的问题。区块链的数据是分布式的，关键的账户信息、监测图像和节点行为是公开透明的，不会有被某一小部分怀揣恶意的人利用。而且，节点是不能随意从链上获取信息的。我们设计的智慧医疗区块链系统是具有访问权限控制的，用户的个人信息是会被通过公钥加密，所以私人信息能持久化地安全地存储在链上。

其次是对物联网设备的行为约束功能。在我们提出智慧医疗区块链系统中，物联网设备的计算能力和存储是不足以承载所有的区块信息的，所以它们的主要算力和存储空间是由边缘服务器群提供的。边缘服务器我们称为本地区块链系统，相当于边缘计算中的靠近物联网设备的服务器群。如果物联网设备恶意泄露用户信息，本地区块链系统会向全局区块链系统警告，限制甚至禁用该设备的算力和储存空间支持。

对本论文来说，区块链-智慧医疗系统支持具有私有和敏感数据的某些应用程序。使用此区块链-智慧医疗系统，上层的智慧医疗可以拥有安全性和分布式双重特征。同时，我们提出区块链-区块链系统被设计为实用工具，换句话而言，它是切实可用的，能在生产环境中部署的模型；它能有实用的运行速度、稳定的性能和足够的拓展性。

1.5 论文结构

本文下面将从文献综述、系统设计、功能和性能测试和实验结论四个章节进行。

文献综述会结合现有的文献研究，提出本文的创新点和研究点。第三章系统设计会详细阐述本系统的设计，包括概念和框架图都会进行说明。第四章会对系统的实现功能进行测试，同时监控系统运行时的 TPS（出块速度）、CPU 占用率、内存占用率等性能指标。第五章会结合实验结果得出实验结论。

2 文献综述

区块链技术在很早就被提出了，Satoshi Nakamoto（2008）提出的《比特币：一种点对点的电子现金系统》白皮书，讲述了 P2P 网络技术、加密技术、时间戳技术、区块链技术等的电子现金系统构架理念。后来随着比特币的快速发展，市值快速攀升，这个领域的研究也越来越深入。后来，区块链在纯粹技术上的研究文献也越来越全面，有在比特币之上进行完善的研究：F.Tschorsch and B. Scheuermann（2016），从比较宏观的角度对比特币和其继续发展做出了一定贡献；也有囊括了底层的共识算法，比如 Thuat Do, Thao Nguyen,Hung Pham（2019）和王冠,张文月（2020）提出了有一定改进的共识算法，令区块链底层发展更加的稳固。除了共识算法这个比较基础性的研究，区块链的一大特色就是与实际应用结合，在这方面也有很多出色的研究，比如 Zehui Xiong， Yang Zhang， Dusit Niyato，Ping Wang 和 Zhu Han 在（2018,2019） 提了一个结合区块链和边缘计算的模型。他们的主要思想是物联网设备从边缘网络购买计算能力，行为规范的设备会被奖励，从而维持整个物联网的生态健康。除了模型，他们也仔细分析了激励出块的问题，在经济学层面和数学层面研究了共识机制的，使用了非常多公式来进行证明。这项研究阐述清楚了区块链技术在实际应用场景是如何部署和使用的，是一个非常实用的研究成果。

同时，Xiong（2018,2019）、CCF（2020）和刘洋（2020）等人和组织提出区块链结合物联网的实际部署框架；同时也有学者提出了实际应用场景中一些通用的改进方法，并进行了可用性的评估。如 Liehuang Zhu（2018）提出了一个利用改进的共识流程出块的区块链数据共享网络，它是建立在云网络上的。这个改进的共识算法是实用的，它给予了部分可信任节点否决权。因此，即使这个系统的百分之五十一被恶意节点控制，恶意节点也不能完全获取链上的出块权。这个改进使得区块链技术更加地安全，因为传统 POW 算法中，如果有超过 51%的节点被控制，该区块链就会被敌方控制。所以该系统改进后，可以容许超过 51%节点被控制，毫无疑问这个非常有价值的。

上述文献提出了区块链技术在实际场景中的一些部署方法，现在细化到智慧医疗领域，有一定的研究文献提供支持，但是数量不多。结合了区块链和智慧医疗两者的研究，有部分是聚焦在接入控制和数据获取等方面。比如 Raifa 的

EdgeMediChain 是一篇结合和区块链和智慧医疗的文献。该论文提出了一个基于以太坊的智慧医疗数据交换系统，同时结合了边缘计算的思想。该论文提出的架构是将挖矿节点分布到本地和全局两部分，大大减轻区块链网络中通信压力。该论文也提出了边缘计算的思想，将整个区块链网络分成几个层，数据不需要全部进行全网同步。同时结合账户的等级和获取数据时候的分级，高效地利用了区块链密码学的特性，使智慧医疗中的数据和账户能安全平稳地掌握在医生和病人手中。关于智慧医疗网络中的接入控制，李志斌 (2019) 在“基于以太坊私有链的医疗安全网络接入控制研究”论文中主要研究了区块链网络的接入控制，从而防止区块链网络受到 DoS 的攻击。文中核心贡献是设计和实现了区块链与 NAC 结合的方式进行接入控制系统。此论文和上述的论文测试方法一样，是在自己搭建的以太坊私有链上进行测试，在以太坊基础上加了一层设备认证模块，进行区块链的部分开发。

总的来说，上述研究提出了比较可靠的区块链 + 物联网的实际应用网络架构，也提出了智慧医疗场景中如何控制身份验证和识别的风险的方法。但现有研究并没有从头搭建面向智慧医疗应用的区块链底层系统，也没有对交易内容数据的进行部分加密，所以这部分是缺失的。而且，在智慧医疗的应用环境下，将上述的私密性和安全性进行区块链上的技术创新是有必要的，这也是本文的创新之处。我们希望综合上述的研究成果，将智慧医疗区块链底层系统进行实现，并评测它的实际性能（包括出块时间，每秒处理事务数，CPU 内存占用）。

值得一提的是，在我们这个项目中，特别是在智慧医疗的应用场景下，每个帐户访问私人的内容时候，需要被授权，这可以防止私人数据公开，防止恶意获取私人的数据。这是公钥、私钥和数字签名在区块链中特殊的研究意义，而本论文希望将这个特殊意义应用到智慧医疗中来，使得区块链-智慧医疗更加安全、实用。

3 区块链-智慧医疗系统设计

3.1 系统共识算法

本文构建了一个面向智慧医疗应用的底层区块链应用系统，使用 DPOS+PBFT 这个速度比较高的共识算法。区块链系统的核心是共识算法和网络模型，网络模型一般都是使用 P2P 网络，广播方式常使用洪泛的机制；共识算法现在常用的是 POW、POS、DPOS 这三种基础的共识算法。共识算法就是其字面意思：多个节点之间通过怎样一种机制达成一致的共识。本文经过调研和尝试，将 DPOS+PBFT 共识算法定为本系统的共识算法。

3.1.1 DPOS 算法

DPOS 共识算法和比特币的 POW 共识算法不同，并不是所有的节点参与出块过程。POW 的共识过程是用计算量来衡量节点的对链的出块权，即每一轮的共识中，区块链系统都会产生一个数学难题，哪个节点最优先解决该数学难题，就获得此轮的出块权；POS 是通过权益来决定出块的节点，那段时间内拥有最多数字货币或者份额的那部分节点拥有该段时间的出块权。而本文使用的 DPOS 则是通过数字货币权益的拥有权选出一个委员会，该委员会之间进行协商和讨论完成出块。下图是 DPOS 的网络拓扑图，蓝色节点代表的普通节点（不参与出块流程，不维护公共池），黑色节点代表出块节点（本轮出块委员会，承担出块任务，维护公共池，执行 PBFT 算法机制）。

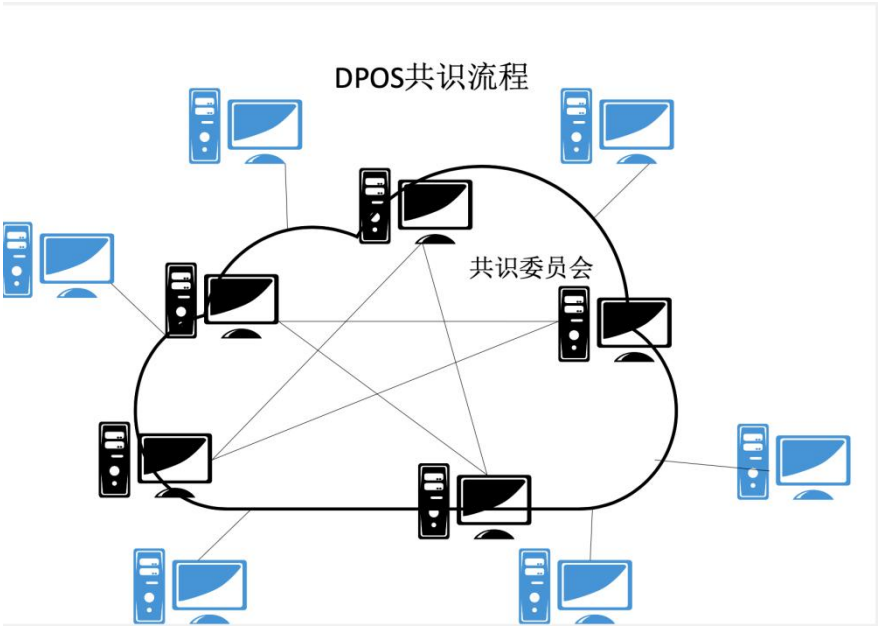


图 3-1 DPOS 共识算法拓扑图

关于委员会的选举：整个网络节点每一轮都需要抵押自己的数字货币，换取相应的票数，投出出块节点。每一轮结束的时候，各个节点会在本地统计票数，票数最高的 4 个节点成为出块节点，并且按照得票数从高到低确定出块顺序，每个出块节点出块一次后结束出块，轮到下一个出块节点出块。新产生的块由当前轮次中所有出块节点进行确认（确认过程执行 PBFT 算法）。关于交易池：每一个出块节点（参与竞选的节点，有能力进行出块的节点）都存在交易池，记录自己收到的每一笔交易。并且在确认区块有效时，将交易池中的记录在有效区块里的交易执行后移除。当节点成为出块节点后，根据自己的交易池打包交易出块。

3.1.2 PBFT 算法

PBFT 算法也是本文使用的共识算法的重点，在此需要进行详尽说明。PBFT 是多个节点之间通过一个协议的算法。它解决的是拜占庭将军问题，所以它本质是一种拜占庭容错算法。拜占庭将军问题就是多个将军需要进行协商同时进军的时间，但是他们之中有可能有叛徒或者奸细；在不能面对面协商（消息同时达到且保证对面不是叛徒）时候，如何能够达成一致，得出一个大部分将军（节点）都同意的共识结果？PBFT 算法就是解决这个问题。

PBFT 算法通过下图（图 3-2）的五个阶段来进行消息传播完成最后的共识过程：请求阶段，预准备阶段，准备阶段，提交阶段，答复阶段。其中中间设置三个反复的沟通阶段是为了防止有节点伪造其他节点的消息、散播虚假的通过信息或者提前结束此轮进行下一轮的共识的恶意行为。我们可以在图中看到，开始时由一个主节点发出主导的共识消息，广播给出块委员会的其他节点。接下来的部分就是 PBFT 的主要流程。

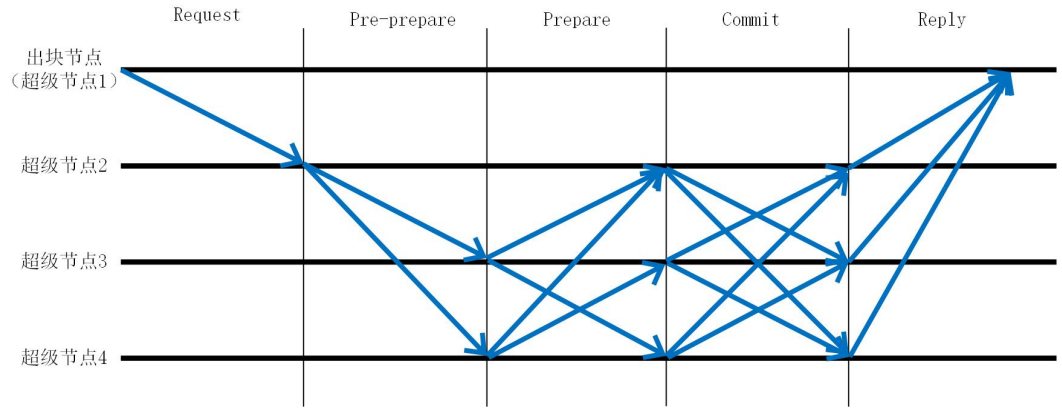


图 3-2 PBFT 算法消息传播图

在 PBFT 部分中，区块从产生到被验证有效需要经过广播，完成 4 次状态转换。每一个被确认有效的区块都需要经过上述五个阶段。每一个有效区块都已至少被 2/3 的节点（对于 4 个节点来说最少为 3 个节点）验证有效，并且得到主导节点的最后确认且在其他节点有超过 2/3 阶段的预准备阶段和准备阶段的记录，该区块在出块委员会中才算是通过。这个是没有办法伪造的，因为这一轮伪造了，下一轮的出块的时候诚实节点总归是超过 2/3（PBFT 共识算法前提：超过 2/3 节点是诚实节点），此轮伪造的块会被丢弃，视作无效。下面是 PBFT 算法流程图，结合上述的消息传播图，更易于理解。完成上述 DPOS+PBFT 流程后，出块即完成，会广播给所有节点，完成同步和持久化。

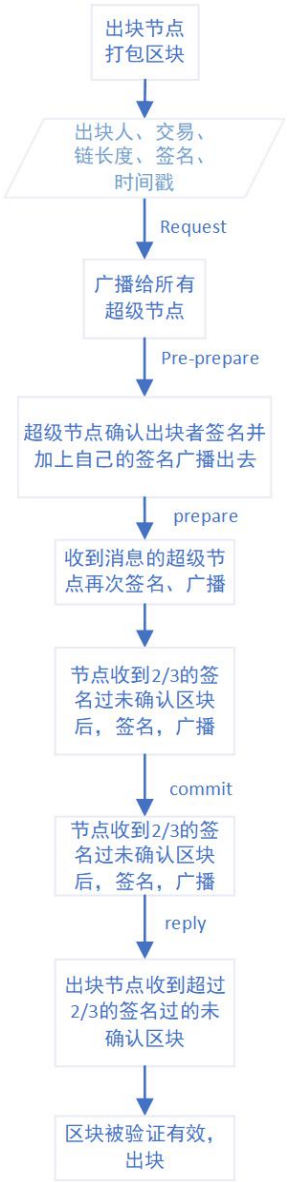


图 3-3 PBFT 算法流程图

3.2 公私钥模型（ECC 椭圆加密算法）

区块链系统中，在共识算法之后，其次需要确定本系统的账户模型--即公私钥的生成算法和加密方式。比如很多区块链系统使用的是 RSA 公私钥，是美国军方在上世纪 60 年代提出的一个非对称算法（能用私钥推出公钥，却无法用公钥反推私钥）；我们 linux 系统中的远程登录算法中也使用了 RSA 的加密算法，方便常用的 ip 和主机快速登录服务器（不需要对称的密码）。我们日常使用的密码是对称密码，即只有一个，掌握了密码就有登录的能力。但是这个密码是明文的，在网络中传播被证明了是不安全的，所以便产生了非对称加密的加密算法。

ECC 椭圆加密算法是对 RSA 算法的一个改进，其实本质是一样的：RSA 是利用质数分解的数学难题来构建秘钥对的安全性，而 ECC 使用了椭圆曲线在图中的唯一性和随机性来保证秘钥对的不可攻破性。同时，ECC 也是比特币的公私钥生成算法，比特币采用 secp256k1 曲线来生成随机的密钥对。本文构建的系统也是参考比特币的密钥对生成曲线，使用 golang 的 elliptic 包中的 P256()函数来生成随机密钥对，生成公私钥对之后，我们对其进行如下处理：

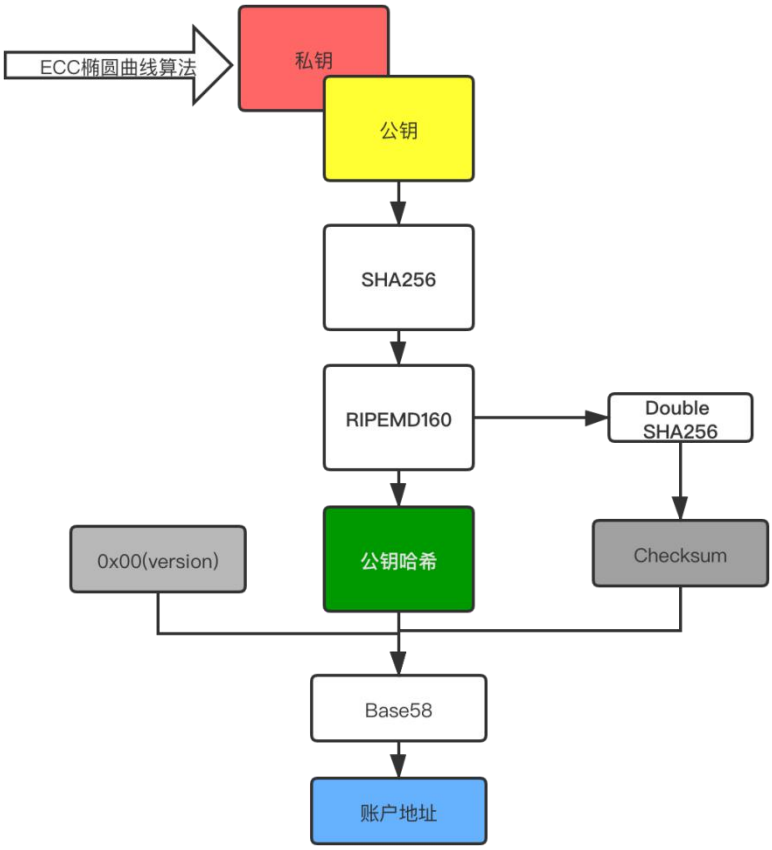


图 3-4 账户生成算法流程图

一个希望加入链上的节点（或者起始的创世节点）经过上述流程，即顺利生成了自己的私钥、公钥和地址。私钥将是该节点在区块链上唯一的身份证明，这相当于自然人的 DNA，是唯一的、不可篡改的。而公钥是公布给其他节点，作为一个身份辨识。用户地址的作用与公钥相似，不同的是 ECC 椭圆加密算法中公钥是一系列坐标点，是向量，而账户地址是可读的字符串，利于存储和传输；所以在本文的区块链系统中均使用账户地址作为节点的“门牌号”--在节点数据库和网络间的 JSON 数据均使用账户地址作为节点标识。

完成公私钥的构建之后，每个节点就有自己的“锁”和“钥匙”，区块上的私人和敏感信息可以获得充分的保护了。

3.3 数据加密模型（AES 加密算法）

公私钥本身是可以对信息进行加密的，流程是这样：生成私人信息的节点会将敏感的信息使用公钥进行加密，而能够查看的节点使用和这个公钥配对的私钥就能解开敏感信息，获得真实的未加密的敏感信息。但是 ECC 密钥对对应的加密和解密过程对于长的字符串或者信息而言是非常慢的。ECC 无论是加密还是解密，一般都是比同长度的 AES 慢许多。在选定特定参数的情况下，经过比较，非对称的解密速度和 AES 对称加密算法不是一个数量级的。所以本文构建的系统中，为了能加快长字符串和大信息量的加密解密，决定采用 ECC+AES 的加密方法。

AES 是密码学中的高级加密标准（Advanced Encryption Standard, AES）又称为 Rijindael 加密法，是美国联邦政府使用的一种区块加密标准。AES 是与 ECC 和 RSA 的非对称加密不相同的对称加密方式。即加密解密都是使用一个钥匙，即上锁的钥匙和开锁的钥匙是一样的。这样的加密解密都使用一个 AES KEY 即可完成。AES 加密过程是非常严密的，在一个 4x4 的字节矩阵上运作，这个矩阵被称为“体（state）”，其初值是一个明文区块，各轮 AES 加密循环四轮，每轮 4 个步骤。因为篇幅原因，且不是本文创新点，在此不进行赘述。本文的系统对下述问题提出了解决（结合 AES+ECC）：这个可读的明文“钥匙”在网络中传播是不安全的，而且是明文，极易被截获和不法利用。

那么此时，ECC 的非对称加密的公私钥就体现出作用来了。在使用 ECC 公私钥对长文本、大信息量数据进行加密解密非常耗费资源和时间，但是我们可以先使用 AES 对长字符串（JSON 数据）进行加密，然后在使用 ECC 对 AES“钥匙”进行加密，如此进行同时兼顾了安全性和速度的双重考虑。结合下述流程图进行理解

会更加易于理解（如图 3-5）。

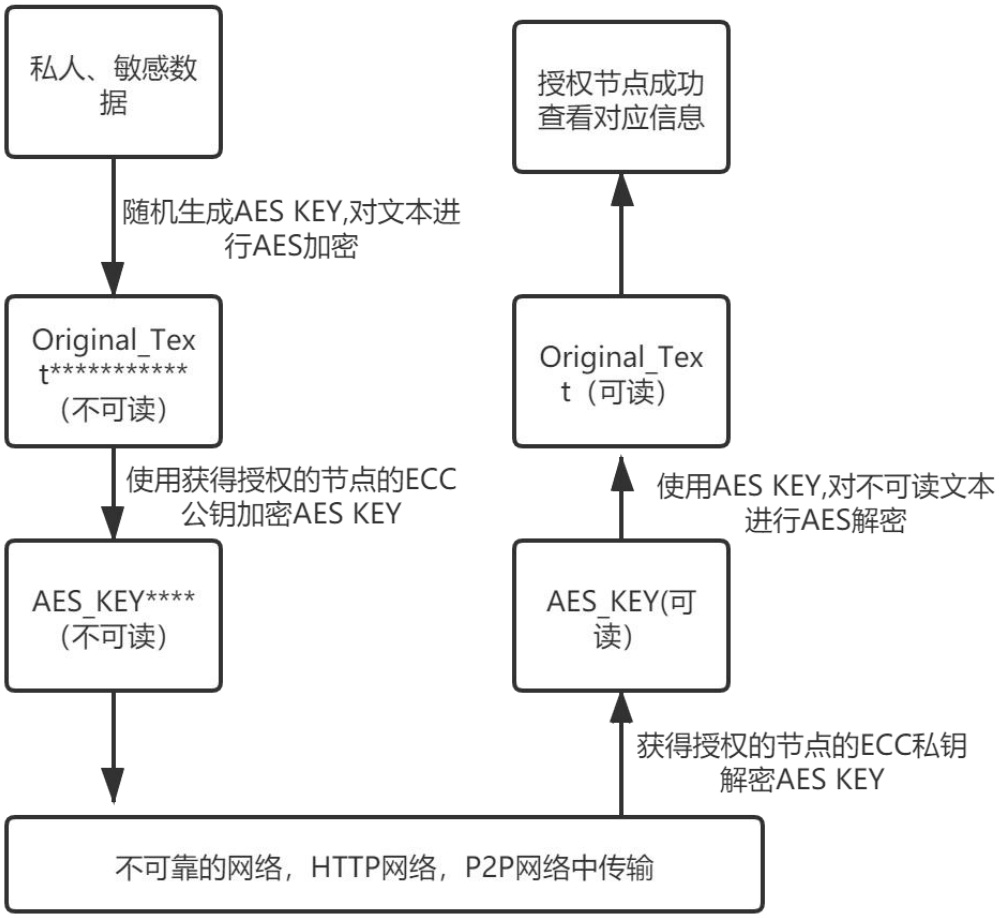


图 3-5 敏感数据加密流程图

3.4 系统整体和局部模型

在上述的基本概念阐述完成之后，本文将要提出最重要的方法创新：设计一个面向智慧医疗应用的区块链系统。该区块链系统从共识算法到网络连接，从账户模型到交易模型，从 P2P 的方式到 HTTP 接口的设计均是自主设计和实现。该系统的面向的用户是智慧医疗场景中的家庭、监听监护人、医生、医疗机构四个方面。在智慧医疗场景中，老人和高位截瘫的病人是最需要利用新技术进行辅助治疗和医护的。所以，本文提出的智慧医疗-区块链系统是一个雏形，面向容易摔倒的老人，帮助其家人和医生通过系统获得更多关于老人的信息，防止其摔倒，改进其治疗方案。在我们的系统模型中，我们提出的场景是老人身上需要佩戴各类传感器，实时监测和上传老人的数据；这些数据会上传到附近的边缘服务器中（此处

借助了边缘计算的概念），在边缘计算中进行处理和计算之后，和全局网络（全国或者全世界的区块链系统节点）进行共识和沟通，将检测数据隐私话、持久化和固定化（存储在区块中，不可篡改）。如图 3-6 所示。

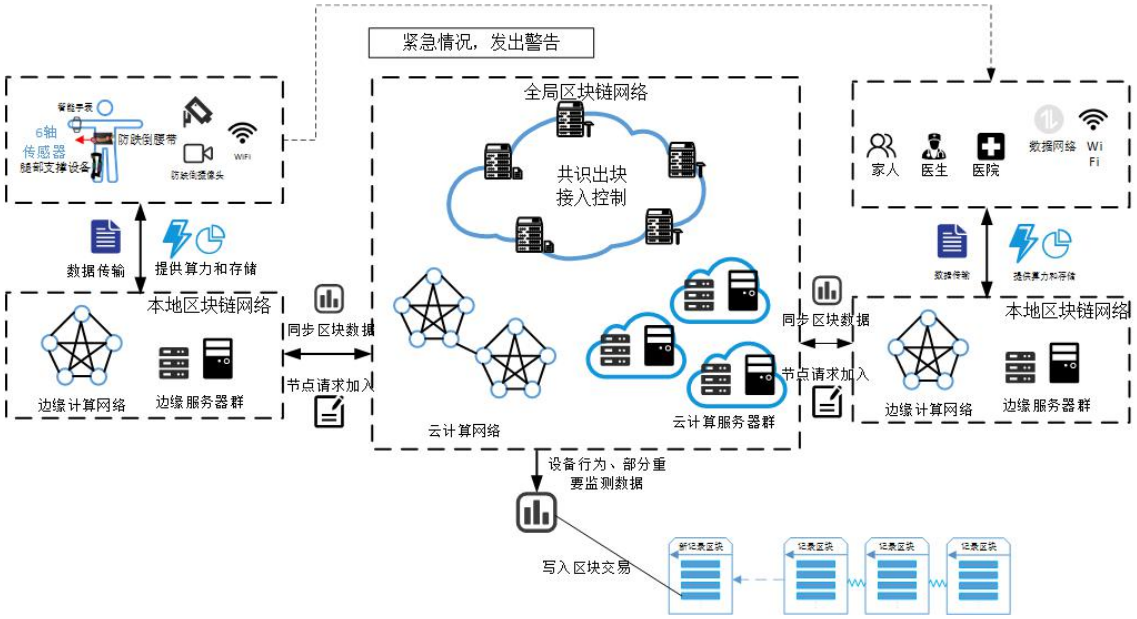


图 3-6 智慧医疗-区块链系统示意图

从上图中很清晰可以看出，每个节点（一个节点对应一个账户，对应一个家庭或个人）都会从边缘计算网络中获取算力和存储空间，反过来边缘计算网络也会通过算力和存储空间来对物联网节点行为进行约束，对其不当行为进行控制和惩罚。如果节点正常上报老人状态和数据，及时得反馈设备信息，该节点对应的账户就会得到合理的信誉分，这些信誉分可以用来换取数字货币，从而在链上能请求更多的资源，获得更频繁的数据上传次数。在检测节点上传之后，通过共识的数据固定化和持久化在链上就会完成。随后这个区块会和前面的区块链连接，形成最新的区块链向全网广播。从上图的右边可以看出，处于诊断端和观察端的医生和家人也能通过边缘计算网络获取最新的链上信息，即病人（老人）最新的健康状态和数据。

根据上述讲解的 AES+ECC 加密流程，其在系统中的表现如下图 3-7 所示：

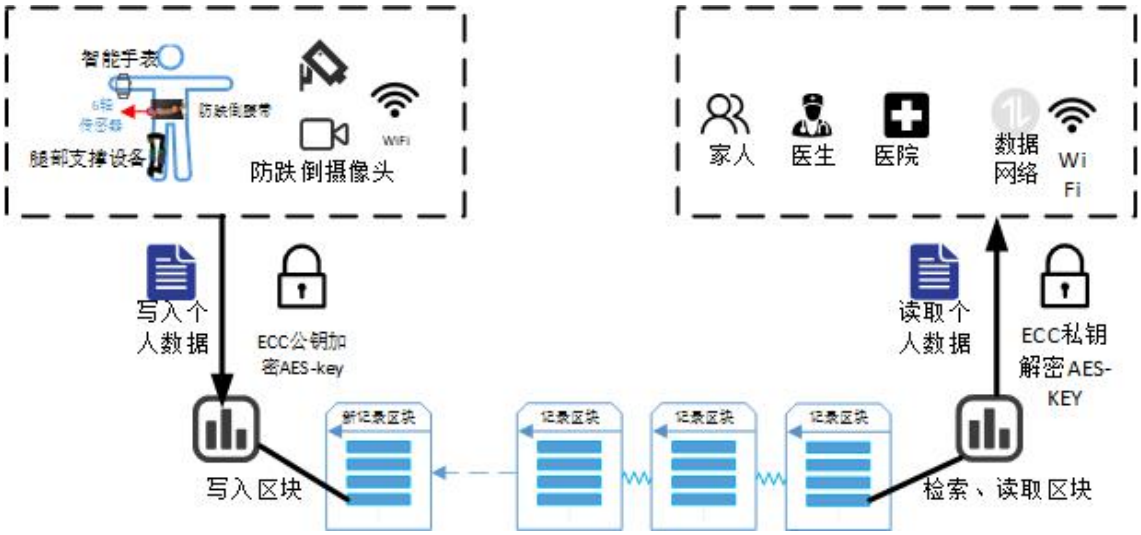


图 3-7 敏感数据写入读取示意图

整体系统架构就如上文所述，整个系统基于 DPOS+PBFT 共识算法和 P2P 全连接实现，同时采用 ECC 公私钥加密和 AES 对称加密对私人数据进行加密。同时系统对外开放 HTTP 接口，数据上传的时候通过上传接口，向系统发起请求。同时也提供包括转账、查询等区块链基本的用户接口，保证系统的日常可用，正常运行。本文创新是应对特定应用的方法创新。在智慧医疗场景下，区块链架构的应用研究还不是很充分，去中心架构的实用性还有待进一步的研究了加强。已有的智慧医疗+区块 链架构基本是基于比特币、以太坊的传统平台，能耗高，速度慢，不适合实际应用场景，也不易于部署。智慧医疗场景下是需要一定的网络速度的，而 DPOS 的代理类共识算法，正是 牺牲了一定的去中心化特性，换来了应用速度的大幅提升。POW 共识需要全网共识，DPOS 只需要出块节点共识通过就可以完成出块。在成熟可用的、现有的区块链平台中，POW 区块链系统的 TPS 普通处于 5-30 之间，而我们的系统的 TPS 达到 500-1000。因此，我们的工作在智慧医疗领域应用不一样的共识算法，是具有创新性的；同时也是可以解决实际问题的。

4 系统的部署和实验

智慧医疗-区块链系统是一个系统模型的构建和实现。既然是一个系统，我们必须对其进行功能测试和性能评估。第三节提出的系统模型是一个概念图，具体的实现中我们建立了一个雏形。上述的功能均可以进行模拟和测试，下面将进行功能测试和性能评测。

表 4-1 系统测试环境

SN	Parameters	Values
1	处理器	2.7GHz 四核 Intel Core i7
2	内存	16 GB 2133 MHz LPDDR3
3	启动磁盘	Macintosh HD
4	操作系统	macOS Catalina 10.15.3
5	网络参数	100Mbps

在上述环境中，模拟程序将启动十个节点，每个节点对应一个进程，一个节点生成一个账户，对应实际环境中 5 个物联网设备（普通节点）和 5 台服务器（出块节点）。

4.1 系统功能展示

本小节功能展示主要通过 Postman 发送请求进行功能测试。

4.1.1 上传监测数据

该接口展示了节点在监测数据的时候，将数据上传到边缘计算网络中，并获得了确认的信息，得到了该合约在链上持久化对应的合约 ID（如图 4-1 所示）。通过这个合约 ID，我们可以在智慧医疗-区块链系统的任何一个节点中查询到这个合约，这个合约 ID 是根据上传数据的时间、地址、类型生成的独一无二的标识。在区块链正常运行的时候，进行共识的时候，出块节点会检验区块上的信息，并执行智能合约，对系统的资源进行分配；同时也会结合区块中的信息，作为考察区块节点的行为的参考—长期表现出恶意节点模样（比如不断上传数据、上传不合规范数据）会被惩罚甚至清除上链的资格。

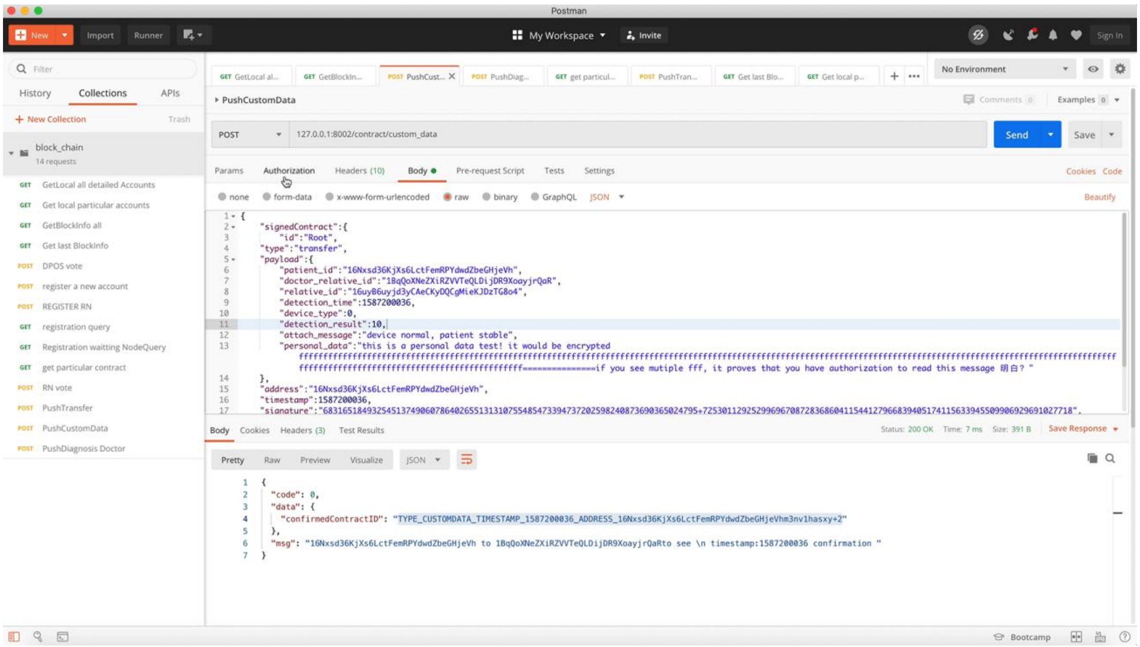
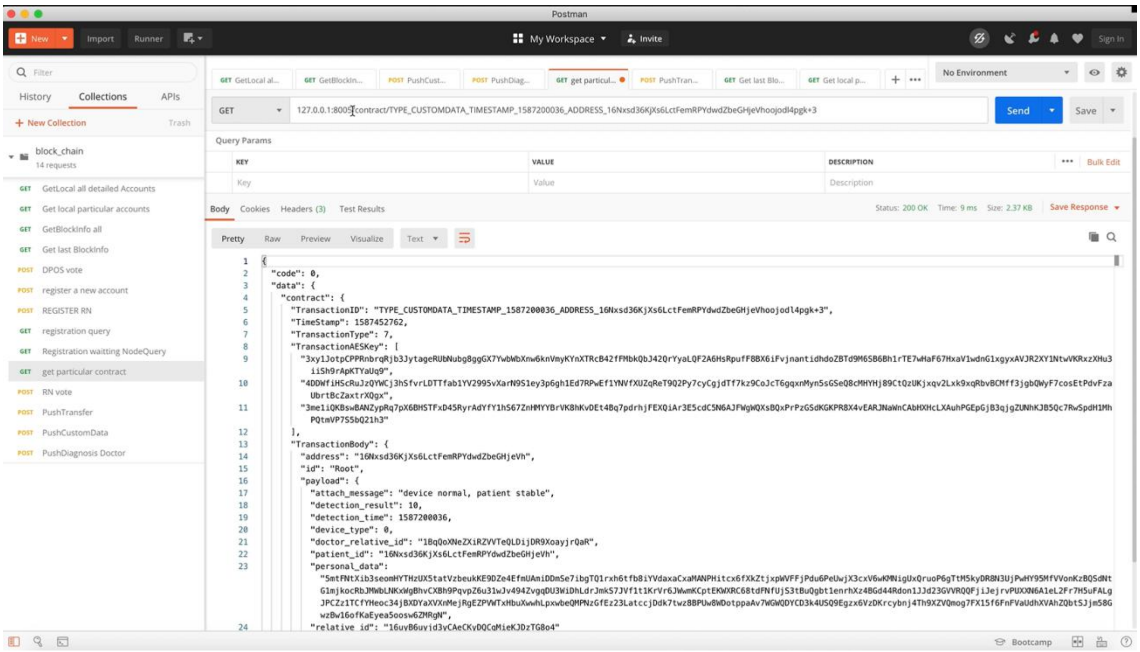


图 4-1 敏感数据写入读取示意图

物联网节点（摄像头、防摔倒装置）在将监测数据上传的时候，会对其中的私人数据进行 ECC+AES 加密，再在区块链系统上进行信息持久化。同时，AES“钥匙”被使用授权节点的公钥进行加密，写入合约之中。在查询的时候，节点使用自己的私钥解密 AES，再使用 AES 解密敏感数据，如果是被授权节点，就可以成功解密，得到原始信息；如果是非授权节点，就是解密失败，只能看到加密之后的信息（如图 4-2 所示）。



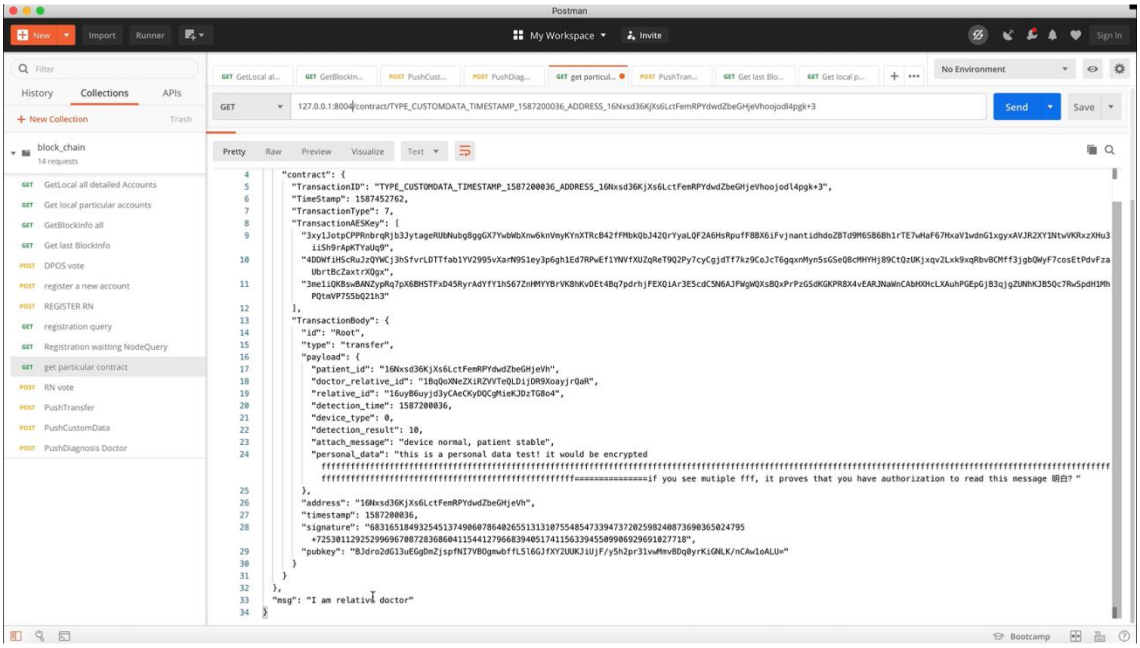


图 4-2 非授权与授权节点节点读取结果对比图

上述功能展示可以看到，物联网设备的上传数据是成功的。同时，节点的数据也会被记录在区块链中，并且可以被查询；其中公共的信息是均可以直接获取，但是敏感的个人数据是只有授权节点才可以查看。这也表明，物联网定时上传监测数据功能是没有问题的。

4.1.2 上传诊断数据

上传诊断数据的数据结构和上传监测信息的非常相似，也是以一个合约的形式将信息上传到边缘计算网络，随后在边缘计算网络（边缘区块链）进行共识和计算，将医生的诊断数据上传到区块链系统中进行持久化。

诊断数据也包含私人数据，所以也会像上一小节所说的，上传的医生会使用 ECC+AES 对私人数据敏感信息进行加密，授权部分账户进行查看。展示过程于上一小节大同小异，在此不进行赘述。

4.2 系统 TPS 评测

本文建立的智慧医疗区块链系统希望构建一个完整的服务体系，从第三节的整体系统设计框图也可以看出，该系统是一个实用的大型系统：涵盖病人、医生、家属和医疗机构。虽然系统的使用的是现有的网络架构，但是在现有的网络架构之上，网络应用之下，设计了一个底层系统。既然这个系统是面向现实生活中使用的，它的可用性是非常重要的。所以本节会对我们完成的系统做一个 TPS（transaction per second 每秒处理事务数）的评估和测试。

在本章开头，已经给出了测试环境的详细参数。本小节的测试环境也是在如此环境中得出的。我们的智慧医疗-底层系统是一个系统，既然是系统，所得到的性能测试就应该是一个比较长时间的。本文进行 TPS 测试的时候经过调研，决定在系统运行之后，每 10 秒采集一个数据点，共采集 500 个数据点，时间跨度 5000 秒，一个多小时，可以作为系统的一个稳定状态下的性能参考值。

在进行性能评测的时候，我们编写了测试用例，对系统发起 POST 的转账请求（区块链的最基本功能），具体的请求参数：每 1.5 秒测试程序向节点 1（出块节点）建立 5 条 tcp 连接，每条连接发送 80-150 个合约请求，即每秒发起 600 个左右的转账请求。我们得到如下的性能评测结果（如图 4-3 所示）：

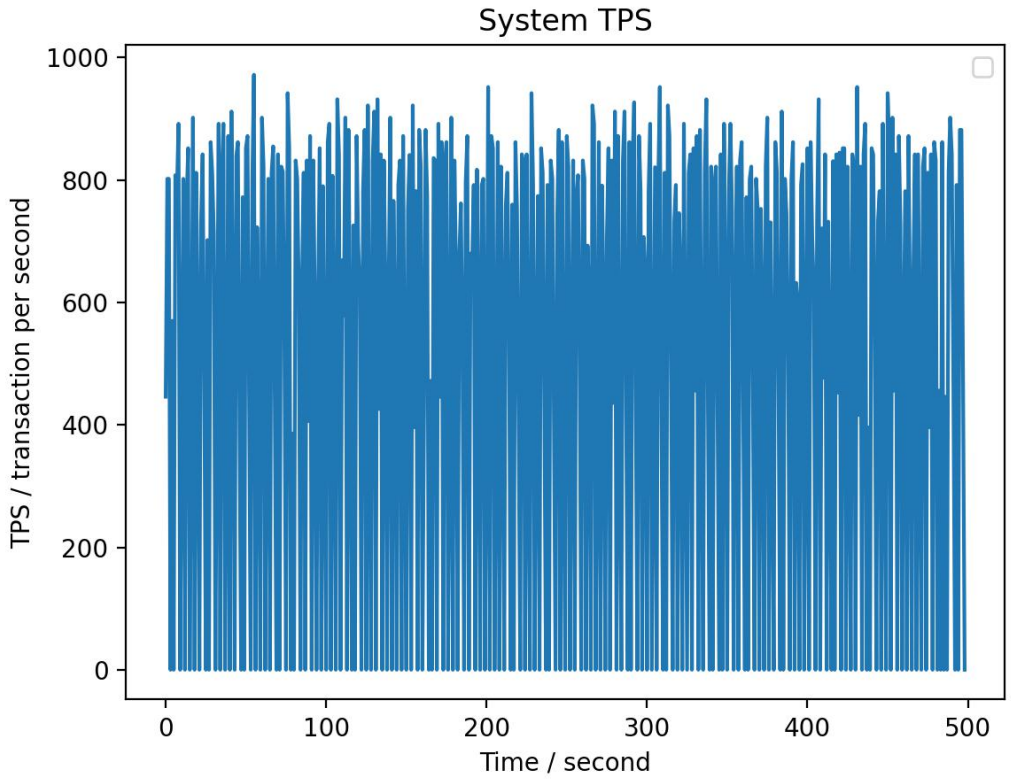


图 4-3 系统 TPS 测试结果示意图

上述结果可以看出我们系统的平均速度可以稳定在 800 左右。在进行测试的时候我们尝试加大测试用例的时候，发现系统变得不那么稳定，网络会出现阻塞。所以我们得出的性能测试就是比较保守的本系统稳定在 1000tps，这是一个不错的速度—相对于以太坊和比特币，和 EOS（企业级分布式区块链系统）也有媲美的能力。在保证系统稳定的情况下是 TPS（transaction per second)可以保持在 600 以上。这个速度是可以满足使用的。我们假设一栋楼有 20 层，每层四户，一个小

区十栋楼，一户人家 5 台设备，每分钟刷新一次检测数据，只需要达到 100TPS 就可以满足日常使用，可用性达标。

4.3 系统资源占用评测

上一小节对系统的 TPS 进行了评测，本小节将对系统在运行时占用的资源进行一个评测。并与参考文献中的 Jianli Pan（2018）提出的物联网-区块链原型系统进行对比。

4.3.1 CPU 占用率

CPU 占用率是区块链系统一个比较常见的指标，因为区块链系统是一个需要花费大量计算量的系统，在保证性能不变的情况下，如果能将 CPU 占用率降下来，或者说采用计算量更低的共识算法而不损害安全性的情况下，这对区块链系统是非常有益的。

我们同样沿用了第四章开头给出的测试环境，在外部给予高并发的测试用例，同测试 TPS 时候一致：每 1.5 秒测试程序向节点 1（出块节点）建立 5 条 tcp 连接，每条连接发送 80-150 个合约请求，即每秒发起 600 个左右的转账请求。在此期间，我们每一分钟采集一个数据点，共 200 个数据点，时间跨度 3 个小时，这个数据点是过去一分钟该节点（进程）CPU 平均占用率。结果如下图 4-4 所示：

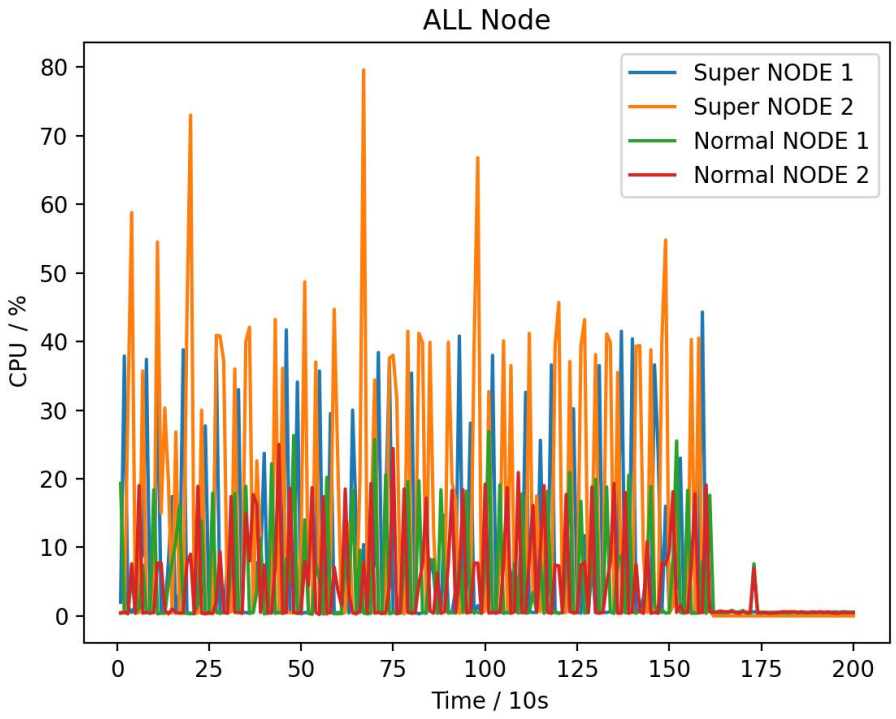


图 4-4 系统 CPU 占用测试结果图

在上图中可以看出，两个出块节点的计算量（CPU 占用率）是明显高于普通节点的，而且普通节点的 CPU 占用更加稳定，说明了共识过程的通信和检查都是非常花费计算量的。为了更加客观的比较出块节点和普通节点占用资源的差别，我们在评测的时候将 5 个出块节点和 5 个普通节点的 CPU 占用率做了平均，这样可以更明显看出两者的差距（如图 4-5 所示）：

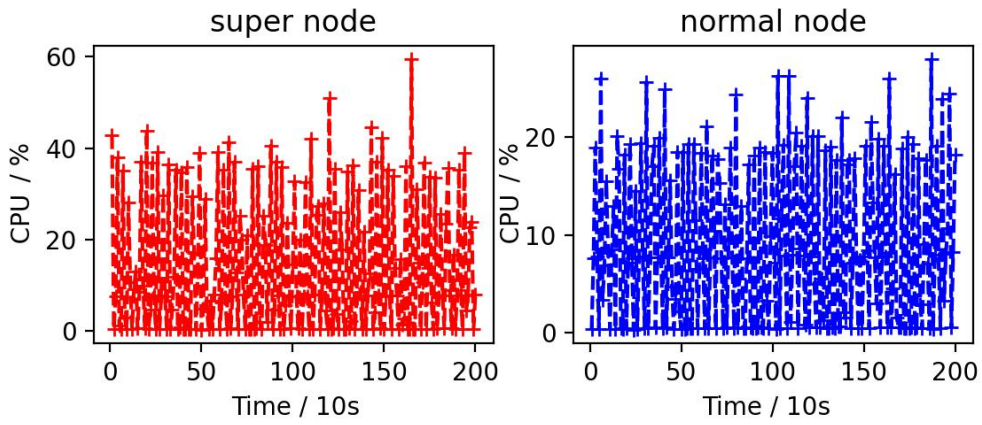


图 4-5 超级节点与普通节点内存占用对比图

图 4-5 表现的 CPU 占用率，出块节点（左）大约是普通节点的 2 倍。与 Jianli Pan（2018）的结果类似。包括出块阶段和静止阶段也是类似的（出块：50%，静止：2%）这也说明这个结果是合理的，本系统是有效可用的。

4.3.2 内存占用率

除了 CPU 占用，内存占用也是区块链系统必须考虑的系统性能指标。对内存占用的评测采用了 CPU 评测一样的评测方法：我们每 5 秒采集一个数据点，共 2000 个数据点，时间跨度 3 个小时，这个数据点是过去一分钟该节点（进程）CPU 平均占用率。

而测试请求（压力测试）的强度也是与 TPS、CPU 评测的强度一致。下面给出结果图。

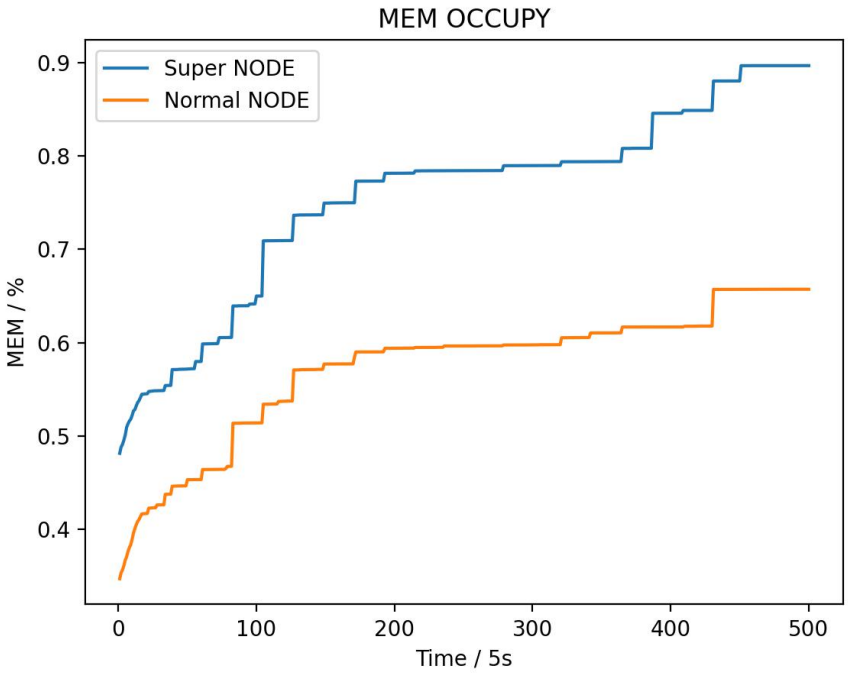


图 4-5 超级节点与普通节点内存占用对比图

上述图表现可以看出出块节点（超级节点）占用的内存是要比普通节点高的，这是因为出块节点直接需要进行共识，而共识过程的 PBFT 算法需要储存大量的信息，以免有恶意节点进行攻击（在第三章出块机制中有阐述）。与 Jianli Pan（2018）结果也是相似的，即出块节点内存占用比普通节点要低，但是没有达到多一倍的水平。说明这个结果是可靠的。

其次我们看到内存逐步上升，这是因为系统选用的数据库存在一定的内存泄露问题，目前正在积极解决中：需要更新数据库版本或者更改使用的数据库。

5 结论

经过第 2、3、4 章的详尽论述，本文构建的智慧医疗-区块链系统解决了智慧医疗+区块链的底层应用系统的空白，是一个不错的方法创新。同时经过详细的概念阐述和框架图绘制，我们理清了区块链系统在面向智慧医疗时的作用和方向。

本文提出的智慧医疗-区块链系统经过部署，完成了功能测试和测试用例，对节点监测信息的模拟上传是没有问题的，系统真实可用。HTTP 接口的上传数据、发起转账、合约查询、区块获取的接口都经过了正确性检验，功能正常。

同时，本文也对系统的性能进行了测试。在绪论中我们说到，希望本系统能支持智慧医疗的应用，在能保证速度的同时，不会大量消耗性能。在测试中，性能达到了模拟场景下的性能要求，我们的智慧医疗-区块链是满足实际应用需求的。再其次，该系统的 CPU 占用率和内存占用率经过评测，与现有的文献与研究作对比，是有进步的；在资源占用情况一样的前提下，本系统的出块速度提升到 600-1000TPS，这是 DPOS+PBFT 共识算法选择的正确，也是该类系统设计中的一个良好的突破点，能给该领域的研究者一个启发。

致谢

在论文撰写期间，在此我首先感谢家里人：母亲、父亲、姐姐和弟弟。毕设时间一直在家中，家人的陪伴和照顾让我有能力有精力完成自己的实验和模型构建。父母、兄弟姐妹都在一定程度帮助了我完成该本科毕业论文，期间也有巨大压力，甚至生病了。但是家里人的照顾和关心让我挺了过来，完成论文撰写。也感谢家人包容我的忙碌，谢谢！

其次感谢黑晓军老师在毕设期间的悉心指导，每周一次的汇报中都尽心尽力给出实质的建议；在开题报告和中期检查期间也多次帮助我修改 PPT，非常感谢！同时也要感谢团队其他老师：刘玉老师、刘勃老师、钟国辉老师、高雅玥老师、张成伟老师对团队和队员的尽心头；同时还有项目组的其他同学：泥俊沛、周宇轩、唐彬、张新驿、唐若飞，他们和我一起奋斗，完成区块链这个项目，这也是本文的基础架构来源，更是我知识的来源！

最后，感谢女朋友和挚友的陪伴！

最后最后，还想感谢我家的猫猫！在我写论文写不下去的时候去看一下它们，就有了力量！

谢谢大家！

参考文献

[1] Raifa Akkaoui，Xiaojun Hei，Wenqing Cheng，“EdgeMediChain: A Hybrid Edge-Blockchain Authentication and Authorization Framework for Health Data Exchange”，submitted to IEEE Access.

[2] Pan J, Wang J, Hester A, et al. EdgeChain: An edge-IoT framework and prototype based on blockchain and smart contracts[J]. IEEE Internet of Things Journal, 2018, 6(3): 4719-4732.

[3] Zhu H, Huang C, Zhou J. EdgeChain: Blockchain-based multi-vendor mobile edge application placement[C]//2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft). IEEE, 2018: 222-226.

[4] Tschorsch F, Scheuermann B. Bitcoin and beyond: A technical survey on decentralized digital currencies[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 2084-2123.

[5] Xiong Z, Zhang Y, Niyato D, et al. When mobile blockchain meets edge computing[J]. IEEE Communications Magazine, 2018, 56(8): 33-39.

[6] Xiong Z, Feng S, Wang W, et al. Cloud/fog computing resource management and pricing for blockchain networks[J]. IEEE Internet of Things Journal, 2018, 6(3): 4585-4600.

[7] Zhu L, Wu Y, Gai K, et al. Controllable and trustworthy blockchain-based cloud data management[J]. Future Generation Computer Systems, 2019, 91: 527-535.

[8] Do T, Nguyen T, Pham H. Delegated Proof of Reputation: a novel Blockchain consensus[C]//Proceedings of the 2019 International Electronics Communication Conference. 2019: 90-98.

[9] Wang W, Hoang D T, Hu P, et al. A survey on consensus mechanisms and mining strategy management in blockchain networks[J]. IEEE Access, 2019, 7: 22328-22370.

[10] Zhou Z, Wang B, Dong M, et al. Secure and efficient vehicle-to-grid energy trading in cyber physical systems: Integration of blockchain and

edge computing[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2019, 50(1): 43-57.

[11] Gervais A, Karame G O, Wüst K, et al. On the security and performance of proof of work blockchains[C]//Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016: 3-16.

[12] 李志斌. 基于以太坊私有链的医疗安全网络接入控制研究 [J/OL]. 华中科技大学, 2019.

[13] 杨伟杰. 基于区块链的分布式文件存储系统的设计和实现[D].华中科技大学,2019.

[14] 邬贺铨. 智慧医疗　这些场景并不遥远[N]. 健康报,2017-05-13(003).

[15] 中国计算机协会. 区块链前沿技术：性能、安全、应用. 中国计算机协会通讯,2020 年 2 月第 2 期（第十六卷，总第 168 期).https://www.ccf.org.cn.

[16] 王冠,张文月.基于可信性评估的区块链共识机制的研究[J/OL].郑州大学学报(理学版):1-7[2020-04-29].

https://doi.org/10.13705/j.issn.1671-6841.2019428.

[17]吕长顺.从区块链金融、政务、医疗三个细分领域抓住未来的投资机遇[J].财富时代,2019(11):3-5.

[18]潘锋.医疗卫生是信息技术发挥重要作用的领域——访中国工程院院士邬贺铨院士[J].中国医药导报,2019,16(03):1-3.

[19].区块链技术应用与发展[J].高科技与产业化,2017(07):82-85.

[20]刘洋,贾斌.区块链技术与泛在电力物联网的融合发展[J].中国科技信息,2020(09):65-66.