

中国人民大学

硕士学位论文

(中文题目) 基于区块链的医养结合数据共享模型研究
Research on the Data Sharing Model of
Integrated Medical Care and Senior Care Based
(英文题目) on Blockchain

学 号：2018104171

作者姓名：郭鑫鑫

所在学院：信息学院

专业名称：软件工程

导师姓名：左美云 王杰

论文主题词：
(3-5个) 医养结合；区块链；数据共享

论文提交日期：2021年5月27日

独创性声明

本人郑重声明：所呈交的论文是我个人在导师指导下进行的研究工作及取得的研究成果。尽我所知，除了文中特别加以标注和致谢的地方外，论文中不包含其他人已经发表或撰写过的研究成果，也不包含为获得中国人民大学或其他教育机构的学位或证书所使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示了谢意。

论文作者（签名）：郭毅毅 日期：2021.5.8

关于论文使用授权的说明

本人完全了解中国人民大学有关保留、使用学位论文的规定，即：学校有权保留送交论文的复印件，允许论文被查阅和借阅；学校可以公布论文的全部或部分内容，可以采用影印、缩印或其他复制手段保存论文。

论文作者（签名）：郭毅毅 日期：2021.5.8

指导教师（签名）：胡景 日期：2021.5.8

摘要

当前，我国已经正式迈入老龄社会，且具有基数大、增速快的特点。为老年人提供医养结合服务是当前研究的热点，然而，医养结合数据共享程度仍十分有限。医养结合数据分散存储于医疗卫生和养老服务等机构中，且在采集过程中缺乏统一标准导致医养结合数据无法实现共享，医疗卫生机构、养老服务机构等形成了一个数据孤岛；另外，医养结合数据具有私密性、特殊性等特点，数据共享过程中存在泄漏风险，且数据泄露后果严重，出于对数据安全的担忧，导致各涉老主体的数据共享意愿不强。

基于以上背景，本文的研究主题是医养结合模式中数据共享模型的构建及其关键机制设计。首先，从数据流动的角度系统地梳理了医养结合模式中的角色和数据，基于区块链技术构建了医养结合数据共享模型，具体包括数据收集层、数据存储层、智能合约层和数据共享层；然后，针对数据共享模型中的关键机制包括激励机制和监管机制进行了详细分析，设计了一种虚拟货币 ShareCoin；最后，结合模拟的医养结合情境，基于 Hyperledger Fabric 对本文构建的数据共享模型仿真实现，并分析验证了模型的可用性和安全性。

基于上述研究内容，本文的理论贡献主要包括：（1）丰富了医养结合领域中对于数据共享的研究；（2）本文提出的数据共享激励机制丰富了区块链研究中对于激励机制的研究。本文的实践贡献主要包括：（1）对于医养结合领域的研究者来说，一方面，ShareCoin 数量可以为“智慧医养发展指数”等评测工作提供参考，另一方面，本文设计的监管机制提供了一种医养结合数据监管途径；（2）对于医养结合相关机构来说，可将本文设计的医养结合数据共享模型应用于实际场景中；（3）对于老年人来说，老年人可以享受更多高质量、针对性的服务；（4）对于整个养老行业来说，本文构建的模型为连通医疗和养老数据孤岛、发挥数据价值提供了解决方案。

关键词：医养结合；区块链；数据共享

Abstract

At present, China has formally entered the aging society, and has the characteristics of a large base and fast growth. Providing integrated medical care and senior care services for the elderly is a hot topic of current research. However, the degree of data sharing of integrated medical care and senior care is still very limited. The integrated medical care and senior care data are scattered in medical care and senior care service institutions, and the lack of unified standards in the collection process leads to the inability to share the Integrated medical and senior care data. Medical and health institutions and senior care service institutions form data islands one by one. In addition, the integrated medical care and senior care data has the characteristics of privacy and particularity, and there is a risk of leakage in the process of data sharing, and the consequences of data leakage are serious. Due to the concern for data security, the old subjects involved are not strong in the willingness to share data.

Based on the above background, the research topic of this paper is the construction of the data sharing model and the design of the key mechanism in the integrated medical care and senior care mode. First of all, the roles and data in integrated medical care and senior care were systematically analyzed from the perspective of data flow. A data sharing model of integrated medical care and senior care was built based on blockchain technology, including data collection layer, data storage layer, smart contract layer, and data sharing layer. Then, the key mechanisms in the data sharing model, including incentive mechanism and supervision mechanism, are analyzed in detail, and a virtual currency ShareCoin is designed. Finally, combined with the simulated medical and senior integration situation, the data sharing model constructed in this paper is simulated and realized based on Hyperledger Fabric, and the availability and security of the model are analyzed and verified.

Based on the above research contents, the theoretical contributions of this paper

mainly include :(1) enriching the research on data sharing in the field of medical and senior integration; (2) The data sharing incentive mechanism proposed in this paper enriches the research on incentive mechanism in blockchain research. The practical contributions of this paper mainly include :(1) For researchers in the field of integration of medical and senior care, on the one hand, the number of ShareCoin can provide a reference for the evaluation of the "development index of smart medical and senior care"; on the other hand, the regulatory mechanism designed in this paper provides a regulatory approach for the integration of medical and senior care data; (2) For institutions related to the integrated medical care and senior care, the data sharing model designed in this paper can be applied to the actual scene; (3) For the elderly, they can enjoy more high-quality and targeted services; (4) For the whole pension industry, the model constructed in this paper provides a solution for connecting the isolated islands of medical care and senior care data and giving full play to the data value.

Key words: Integrated Medical Care and Senior Care; Blockchain; Data Sharing

目录

第 1 章 绪论.....	1
1.1 研究背景.....	1
1.2 研究意义.....	2
1.3 本文研究内容与方法.....	3
1.3.1 本文研究内容.....	3
1.3.2 主要研究方法.....	3
1.4 难点与创新点.....	4
1.4.1 研究中的难点.....	4
1.4.2 研究中的创新点.....	5
1.5 论文结构.....	5
第 2 章 国内外研究现状及理论基础.....	7
2.1 国内外研究现状.....	7
2.1.1 关于医养结合的研究.....	7
2.1.2 关于数据共享的研究.....	11
2.1.3 数据共享中关于激励机制的研究.....	12
2.1.4 数据共享中关于监管机制的研究.....	14
2.2 理论基础.....	14
2.2.1 区块链.....	14
2.2.2 Hyperledger Fabric.....	20
2.3 本章小结.....	20
第 3 章 医养结合数据共享模型的构建.....	22
3.1 医养结合模式角色和数据分析.....	22
3.1.1 医养结合模式角色分析.....	22
3.1.2 医养结合模式数据分析.....	24
3.2 基于区块链的医养结合数据共享模型.....	25
3.3 基于区块链的医养结合数据共享模型分层架构.....	27

3.3.1 数据收集层.....	27
3.3.2 数据存储层.....	28
3.3.3 智能合约层.....	30
3.3.4 数据共享层.....	32
3.4 本章小结.....	32
第 4 章 医养结合数据共享机制研究.....	34
4.1 医养结合数据共享模型中的激励机制.....	34
4.2 医养结合数据共享模型中的监管机制.....	37
4.3 本章小结.....	38
第 5 章 医养结合数据共享平台的设计与实现.....	40
5.1 医养结合场景.....	40
5.2 医养结合数据共享平台框架介绍.....	41
5.3 医养结合数据共享平台实现.....	43
5.3.1 开发环境准备.....	43
5.3.2 智能合约实现.....	43
5.3.3 平台可视化界面实现.....	46
5.4 模型分析.....	48
5.4.1 安全分析.....	48
5.4.2 性能分析.....	48
5.5 本章小结.....	49
第 6 章 总结与展望.....	50
6.1 研究总结.....	50
(1) 理论成果.....	50
(2) 实践成果.....	50
6.2 研究局限.....	51
6.3 研究展望.....	51
参考文献.....	53
致谢.....	60

图目录

图 1-1	研究技术路线图.....	4
图 2-1	2005 年至 2020 年国内“医养结合”研究文献柱状图.....	7
图 2-2	2010-2020 年医疗数据泄露事件数量.....	10
图 2-3	区块链网络的示例图.....	15
图 2-4	区块链网络的层次模型.....	16
图 2-5	Merkle 树示意图.....	17
图 3-1	医养结合模式表现形式一.....	23
图 3-2	医养结合模式表现形式二.....	23
图 3-3	基于区块链的医养结合数据共享模型.....	26
图 3-4	基于区块链的医养结合平台数据共享架构.....	27
图 3-5	医养结合数据共享模型的数据存储机制.....	30
图 3-6	以老年人为中心的权限管理机制.....	31
图 3-7	数据操作流程.....	32
图 4-1	数字社区货币的构建原则.....	35
图 5-1	A 先生的医养结合场景.....	40
图 5-2	医养结合数据共享平台框架.....	41
图 5-3	区块链网络.....	42
图 5-4	医养结合数据共享中的交易流程.....	44
图 5-5	用户登录界面.....	46
图 5-6	数据共享平台可视化界面截屏.....	47
图 5-7	权限管理功能.....	47
图 5-8	新建授权.....	48
图 5-9	性能测试结果.....	49
图 5-10	资源使用情况.....	49

表目录

表 2-1	不同养老方式中的医养结合载体.....	9
表 2-2	数据共享中关于激励机制的研究内容.....	13
表 2-3	数据共享中关于监管机制的研究.....	14
表 3-1	医养结合模式中的角色.....	24
表 3-2	医养结合模式中的服务及相关数据.....	25
表 3-3	非关系型数据库分类.....	29
表 4-1	医养数据共享模型激励方案样例.....	36
表 4-2	监管智能合约.....	38
表 5-1	数据共享状态.....	44
表 5-2	数据操作智能合约的伪代码实现.....	45

第 1 章 绪论

1.1 研究背景

最新人口普查结果显示，我国老龄人口有 26402 万人。我国人口老龄化这一基本国情的形势越来越严峻，具有基数大、增长迅速的特征。世界银行预测，到 2030 年的时候，人口老龄化这一基本现状将使我国的慢性病负担增长 40%。但需要注意的情况是，我国医疗和养老的资源很有限。为了积极应对人口老龄化，我国逐步建立了以居家养老为根本，并且把社区养老作为依托，把机构养老作为一种增补方式，医养相结合的多主体、多形式的养老服务体系。当前关注和研究重点是医养结合，该类型服务将医疗保健资源与养老服务资源结合起来。

医养结合是指整合医疗保健资源和养老资源，一方面提供生活照护、家政服务、文化娱乐等基本生活服务，另一方面提供预防、治疗、护理、临终关怀等医疗服务。医养结合这种养老服务模式不仅可以为老年人提供定制化、精准化、持续的医疗保健和养老服务，高质量、高效率地使老年人的健康养老服务需求得到满足，而且能够发挥数据价值、释放出医疗和养老资源，从而减少社会对养老的支出成本。

近年来，我国发布了一系列与医养结合相关的政策来促进其蓬勃发展，如《关于深入推进医养结合发展的若干意见》。该文件要求促进医养结合的智慧化，借助新兴技术整合现有的健康服务和智慧养老等信息系统，搭建一个智能型的健康养老服务网络，紧密连接起涉老主体包括家庭、社区和机构等。尽管利用信息技术构建医养结合平台进行数据共享已成为国内学者的研究重点之一，但是我国当前的医疗卫生和养老服务数据共享程度仍十分有限。医养结合数据分散存储于医疗卫生和养老服务等机构中，由于在采集过程中缺乏统一标准导致医养结合数据无法实现数据交流、共享，医疗、养老机构等形成了一个数据孤岛；另外，医养结合数据具有私密性、特殊性等特点，数据共享过程中存在泄漏风险，且数据泄露后果严重，出于对数据安全的担忧，导致各涉老主体的数据共享意愿不强；医养结合这一模式使得医疗卫生资源和养老服务资

源得到连接和整合，从而可用信息化手段使医养结合数据实现在各涉老主体之间的同享，但当前存在的医养结合平台多采用集中式存储，易出现“监守自盗”、单点故障等问题使用户数据泄露。因此，当前医养结合这一模式中的数据共享程度十分有限且有数据泄露的风险。

随着区块链技术的不断发展，随着我国相关政策文件的不断完善，区块链已经成为我国数字经济发展中的一项极其重要的推动力。区块链利用密码学方法和分布式架构来实现，具备透明可信、不可以被更改、可以溯源、安全等特点，因此基于区块链技术的以上优点，可实现医养结合数据流转过程的透明，从而保证数据的安全性。同时，可在区块链架构的激励层里设置一定的数据共享激励机制来促进数据共享。

针对以上背景和问题，本文拟利用区块链技术，研究医养结合模式中的数据共享。首先梳理现有数据共享研究；然后借助文献研究等方法系统地分析了医养结合模式中的角色和数据；之后按照数据收集、存储、智能合约和共享四层结构对医养结合数据共享模型完成详细设计，包括数据存储、访问控制、共享激励、数据监管等四类利用智能合约来实现的机制；最后设置模拟医养结合场景，采用 Hyperledger Fabric 对数据共享模型仿真，同时分析验证模型的可用性及安全性。

本文通过研究医养结合数据共享模型，以期连通医疗卫生和养老服务数据，发挥数据价值，帮助智慧养老行业实现可持续发展。本文丰富了医养结合领域对于数据共享的研究，本文提出的数据共享模型可应用于实际场景中，具有一定的实践意义。

1.2 研究意义

本研究的理论贡献有两点：

- (1) 丰富了医养结合领域中对于数据共享的研究；
- (2) 本文提出的数据共享激励策略丰富了区块链研究中对于激励机制的研究。

本研究的实践意义有以下四点：

- (1) 对于政府和医养结合领域的研究者来说

- 1) 一个区域中的 ShareCoin 数量可用于“智慧医养发展指数”、“智慧助老指数”等指标体系中,对于评测工作具有一定的参考价值
 - 2) 为医养结合相关政策的制定提供参考,如可制定使用 ShareCoin 来抵扣税款等,吸引和鼓励机构开展医养结合服务
 - 3) 本文中提出的监管机制为政府提供了一种医养结合数据监管途径
- (2) 对于医养结合相关的机构来说,一方面,本文设计的医养结合数据共享模型可应用于实际场景中,有利于挖掘养老行业的商业模式,机构之间通过共享医养结合数据来获取更大的经济利益;另一方面,可通过展示拥有的 ShareCoin 数量来表征自身的信用等级,对于提高机构的信誉具有正向促进作用。
- (3) 对于老年人来讲,可获得更多高质量、针对性的服务。
- (4) 对于整个养老行业来说,本文提出的医养结合数据共享模型可以为相关主体之间提供数据共享途径,一定程度上解决医养资源整合难题。

1.3 本文研究内容与方法

1.3.1 本文研究内容

本文重点构建医养结合数据共享模型,通过构建并应用医养结合数据共享模型,可以进一步整合医疗和养老资源,促进我国智慧医养的发展。本文主要内容包括:

- (1) 通过文献回顾,了解了“医养结合”和“数据共享”的研究现状,分析总结了医养结合的两种表现形式及其角色和数据。
- (2) 基于区块链技术构建了医养结合数据共享模型,具体包含四层。
- (3) 设计了共享模型中的关键机制——激励机制和监管机制,基于激励相容理论和社会资本理论设计了激励机制,基于文献回顾设计了监管机制。
- (4) 通过设置医养结合应用情景,基于仿真实验法利用 Hyperledger Fabric 对本文构建的模型进行仿真实现。

1.3.2 主要研究方法

本文主要使用的研究方法有文献研究法、案例调研法、软件工程法、规范分

析法和仿真实验法。其中：

- (1) 文献研究法和案例调研法用于对医养结合及数据共享研究的梳理与分析；
- (2) 软件工程法主要用于医养结合数据共享模型的构建阶段；
- (3) 规范分析法主要用于医养结合数据共享模型中两种关键机制包括激励机制和监管机制的设计阶段；
- (4) 仿真实验法主要用于医养结合数据共享模型的应用阶段。

本研究的技术路线图如图 1-1 所示，其中靠左一侧包含了具体研究内容，右侧为各阶段使用的科学方法。

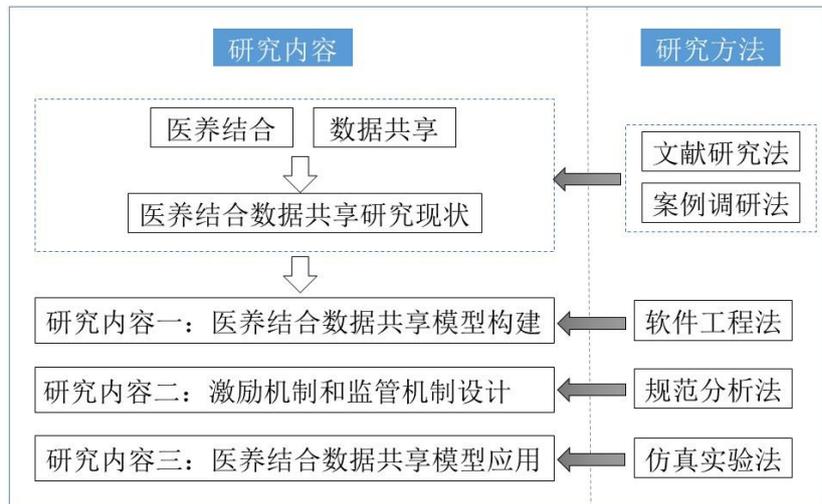


图 1-1 研究技术路线图

1.4 难点与创新点

1.4.1 研究中的难点

本研究将构建并应用基于区块链的医养结合数据共享模型，结合研究技术路线图，可以看到，本研究中的难点包括以下两点：

- (1) 医养结合模式涉及到的角色和数据较多，目前尚无统一而全面的研究，所以需要细致梳理医养结合里的角色及数据，做到不重不漏。

- (2) 本文拟通过发布虚拟代币的方式来实现共享激励机制，但是由于涉及的角色及区块链中的节点较多、平台间流通的数据种类较多，故较难公平、全面地设计出代币激励方案。

1.4.2 研究中的创新点

本研究包含三部分内容，分别为医养结合数据共享模型构建、激励机制和监管机制设计、医养结合数据共享模型应用。本文的创新点主要有三个，具体展开如下：

- (1) 领域创新：针对养老领域，本文提出了一个基于区块链的医养结合数据共享模型，丰富了医养结合领域中对于数据共享的研究。
- (2) 理论创新：本文提出的医养结合数据共享激励机制丰富了区块链研究中的激励机制研究。
- (3) 应用创新：本文提出的医养结合数据共享模型可以扩展至实际的场景中，因此具有较大的实用性。

1.5 论文结构

本研究包含六章内容，具体如下：

第一章为绪论部分。展开介绍了人口老龄化趋势越来越严峻，并且医养结合深入推进困难重重的研究背景，介绍了研究意义，之后介绍了研究内容包括构建医养结合数据共享模型、提出数据存储机制、激励机制和共享机制、对数据共享模型进行仿真实现；以及所采用的研究方法。最后对本文的整体框架做了安排。

第二章为国内外现状及理论基础部分。回顾国内外学者在医养结合、数据共享等方面已有研究及不足，介绍了本文的理论基础包含有区块链、Hyperledger Fabric 框架等内容。

第三章为医养结合数据共享模型构建研究。首先借助文献研究等方法系统地分析了医养结合模式中的角色和数据，然后基于区块链技术，按照四层模型架构进行详细设计。

第四章设计了医养结合数据共享模型中的关键机制，包括激励机制和监管机制。

第五章是医养结合数据共享模型的应用研究。主要是根据前两章的设计的医养结合数据共享模型和机制，利用 Hyperledger Fabric 技术实现了一个医养结合数据共享平台。

第六章为总结与展望。总结本文工作和成果，基于此，提出本文的研究共享和尚不完善的地方，并给出之后的研究计划。

第 2 章 国内外研究现状及理论基础

为了借鉴已有研究的经验，并总结研究不足之处，本章将查阅文献和图书专著，梳理医养结合、数据共享以及数据共享中的激励机制和监管机制等方面的国内外研究现状，还梳理了相关的技术理论。

2.1 国内外研究现状

2.1.1 关于医养结合的研究

“医养结合”是我国老龄事业发展过程中创造的一个词汇，最早是由郭东等（2005）学者提出的，他们提出“医养结合、持续照顾”构念，认为医疗和养老机构之间可以实现多类型结合，可以使“资源共享”，有助于处理由人口老龄化带来的多项难题。此后学者们开始关注医养结合相关的研究，并从 2013 年起，相关研究文献呈现井喷态势。图 2-1 展示了从 2005 年 1 月至 2020 年 12 月，以“医养结合”为检索主题词，在中国知网上检索到的相关研究文献数量。



图 2-1 2005 年至 2020 年国内“医养结合”研究文献柱状图

资料来源：本文根据参考文献整理

在国家支持层面，国务院于 2013 年 9 月首次发布了含“医养结合理念”的

政策，即《国务院关于加快发展养老服务业的若干意见》，指出要推动医和养的融合发展；2015年11月首次发布了含有“医养结合”一词的政策文件，即《关于推进医疗卫生与养老服务相结合的指导意见》，此后相关的研究文献便有了大量增长。2016年10月，国务院发布《“健康中国2030”规划纲要》，要求建立健全医养结合相关机构之间的合作方案，推动医养结合，为老人提供涵盖全生命周期类型的医养紧密连接服务。此后陆续出台了医养结合试点单位、机构审批登记、服务指南等多项相关制度，深入促进医养结合发展。

（1）医养结合模式

医养结合指整合了医疗卫生和养老服务资源，一方面为老年人提供看管照顾、家政、文化娱乐等基本生活服务，另一方面提供预防保健、康复护理、临终关怀等医疗护理服务的一种服务模式（左美云，2016）。在健康中国战略实施的大背景下，医养结合是通过整合资源、衔接服务，将医、养在制度上深度融合，是一种养老模式创新和社会治理创新（朱庆，2020）。

学者们基于不同视角研究了医养结合类型。从资源配置的角度出发，陈俊峰等（2016）把区域个案作为基本，按照医养等资源的不同配置方案，分别把医和养按照“七三”、“五五”等进行组合，将医养结合分为“医养一体”、“养医一体”、“联合运行”、“支撑辐射”以及“护养一体”五大类。

从资源整合的角度出发，左美云等学者（2016）认为医养结合具体表现为四种模式类型，包括医中加养、养中加医、医养相邻及上门服务。穆光宗（2018）则把它分成了四种模式，其中三种为居家养老加上家庭医生或社区医疗或医院医护，还有一种模式为医院医护+机构养老。杨一帆等学者（2020）则认为服务模式分别为“以医疗结合养老”、“以养老结合医疗”及“医养同步”。朱庆（2020）认为我国包含四种相对成熟的服务模式，分别为“医养签约合作”、“养老组织内部设立医疗部门”、“医疗卫生服务延伸到社区和家庭”以及“医疗组织开展养老服务”。

综合文献回顾和本文观点，将医养结合模式分为医中加养、养中加医及医养合作三类。“医中加养”是指医疗卫生机构内设或设立养老机构，“养中加医”是指养老服务机构中内设或设立医疗机构，“医养合作”是指医疗卫生机构和养老服务机构进行签约合作。同时，在表2-1中总结了当前主要养老方式中医

养结合模式的实现载体。

表 2-1 不同养老方式中的医养结合载体

医养结合模式 实现医养结合的载体	医中加养	养中加医	医养合作
居家养老			家庭病床 未来的家庭医生体系
社区养老			社区卫生服务中心 养老服务驿站等
机构养老	康复中心 护理医院 安宁疗护中心等	敬老院 养老院 老年公寓等	医养结合机构 (可和周边综合医院等实现转诊)

资料来源：本文根据参考文献整理

(2) 医养结合数据共享现状

医养结合中关乎多个群体及部门、组织。医养结合数据含医疗保健数据、养老数据等，较一般数据来说具有隐私性和特殊性。张丽等（2019）分析了智慧养老平台中所涉及到的政府层次，服务提供方包含各类企业和养老机构等，涉老数据在跨行业、跨部门、跨地域的共享和整合尚未实现，造成数据孤立等问题。我国的医疗数据目前还都分散在各个部门、单位，没有打通成一体，形成了“数据孤岛”（马红丽，2016）。当前我国医院间存在严重的“信息孤岛”，医院参与医疗信息共享意愿不高，患者的诊疗信息被静态碎片化储存而无法充分地利用。

同时，根据 HIPAA Journal 报告显示，过去十年来医疗保健数据泄露事件持续增多，图 2-2 展示了从 2010 年至 2020 年的医疗数据泄露事件数量。泄露原因包括处置不当、盗窃、未授权访问以及黑客攻击。未授权访问是指内部人员

故意外泄患者的医疗数据；黑客事件主要为利用漏洞实施网络钓鱼、恶意和勒索软件攻击。医疗隐私数据中包含了大量的个人数据及隐私信息，它一旦发生泄漏会使个人从个人信息到生理数据都将变成“透明”（王强芬，2016）。同时，医疗隐私泄露也会给患者带来一系列困扰，如骚扰、歧视、不公平对待等，给当事人造成了身心伤害（刘海琴等，2019），甚至被威胁、勒索，造成严重的财产损失。

500条及以上医疗数据泄露事件

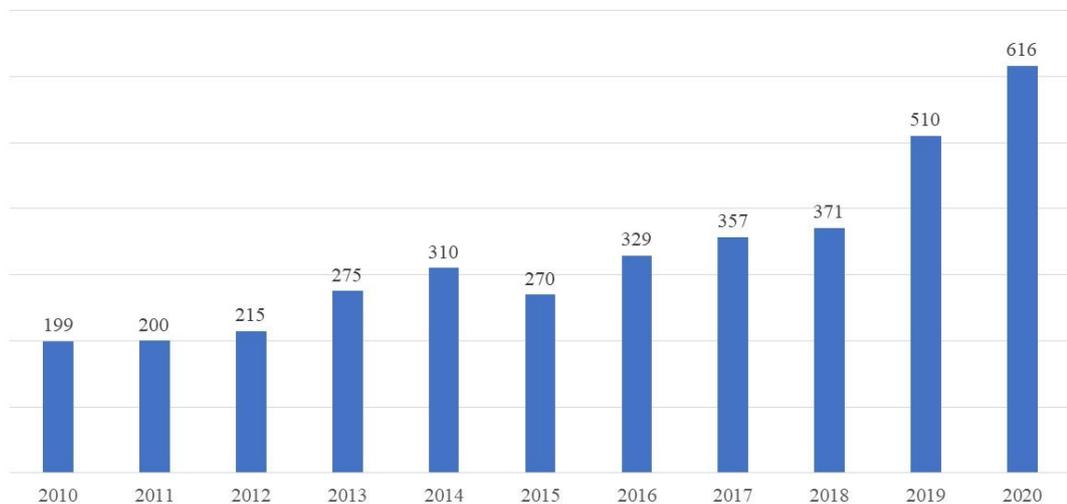


图 2-2 2010-2020 年医疗数据泄露事件数量

资料来源：HIPPA Journal

较多学者利用信息化手段构建出医养结合平台，以此来实现医养结合数据的共享。彭荣等学者（2017）通过分析医养结合养老服务系统中的主体及之间的相互联系，通过借助 MAS 建模技术，把老年人放在系统设计的中心位置，构建了一个医养结合智慧化模型。侯玉梅等（2020）使用新型的物联网技术和信息处理技术，设计出了包含居家长者、营养餐饮商家、医疗服务机构、监管部门等在内的 8 种角色，构建出一个医养结合类型的居家服务平台，整合了医、养和家政三方面资源。黄娜娜等（2019）基于信息安全技术，提出了一种数据共享方案，该方案特点是可撤销，实现了在医疗云中安全高效的数据共享。Mateo et al.（2020）通过集中定义和存储数据改善了医疗专业人员之间的信息共享。

从以上研究可以看到，目前存在的医养结合平台，均采用集中存储的方式来构建系统进行数据共享，致使隐私数据极其容易泄露，且后果较为严重且不可逆；同时缺乏相应的隐私保护和共享激励等机制来保证数据的私密性和完整性，因此，当前医养结合数据共享情况较为薄弱。

2.1.2 关于数据共享的研究

数据共享是国内外的热点研究课题，发挥数据价值的一个重要前提即为数据共享，目前已经探索了包括云计算、联邦学习、区块链等多种技术来实现数据共享。

(1) 基于云计算的数据共享

有学者基于云计算来研究数据共享。Li et al. (2012) 提出了一种属性加密的共享方案，该方案通过判断参与方特征来配置不同权限；Chow et al. (2013) 提出了聚合密钥加密算法，对数据文件进行分类，然后对组成的文件集提取出一个聚合密钥，系统里的用户可利用该密钥来打开里面的任意文件。Lu et al. (2020) 设计了基于代数签名的完整性机制，对数据请求者进行访问授权控制，保证了数据共享过程中的隐私安全。

基于云计算的数据共享虽然已经在气象、政务、数字化校园等多领域的信息平台中得到应用，但是由于数据在存储上相对来说呈现中心化的特点，因此存在云内里和云外部的威胁。在云内里，超级管理员可能会泄露数据如错误操作等；在云外部，破坏分子可能会恶意攻破云服务器，那么其中保存的大量隐私数据将会被泄漏。

(2) 基于联邦学习的数据共享

联邦学习是一种数据不脱离本地，在保证符合相关法律法规前提下，在多参与主体或者多个计算结点间开展机器学习的一种技术。该方式仅共享模型参数，不共享原始数据。2016年，谷歌公司提出联邦学习的概念，在用户隐私不被泄露的前提下，完成在不同安卓手机终端的机器学习模型训练。有学者将联邦学习应用于词汇联想 (McMahan, 2017)、医学成像 (Lundervold, 2019) 等多个领域。关于联邦学习的研究聚焦于解决精度损失和提高安全性方面，主要应用于面向用户的个性化服务场景。何雯等 (2020) 基于联邦学习技术，利用支

付数据实现数据共享，完成了风险商户识别模型的训练。

联邦学习技术仍然处于发展阶段，存在通信效率低、系统异构、数据异构等难题（Li, 2020）。此外，在联邦学习场景中，服务器和参与者可成为被动和主动攻击者，从而造成用户隐私泄露（陈冰等, 2020）。

（3）基于区块链的数据共享

区块链作为一种新兴信息技术，通过分布式架构、密码学算法以及共识策略在各个参与方之间建立起信任关系，其账本可溯源且不可被篡改，而且可设置一定的激励策略来促进共享。目前在金融、供应链及医疗保健等领域得到了广泛的研究实践。

Wang et al. (2019) 构建了一个基于区块链的金融贷款管理系统来实现数据溯源和隐私保护。Zhang et al. (2018) 分析了临床数据共享的重要性和存在的困难，设计了一个基于区块链的架构 FHIRChain，并基于 FHIRChain 架构实现了一个可以为患者提供协作治疗的分布式应用程序；Khatoun (2020) 设计出一个实现多种智能合约算法的医疗管理平台，在患者授权的前提下促进患者信息在患者、医疗机构、实验室、保险公司、药品公司等地方进行共享，可实现定制化的医疗服务、削减管理费用支出并提高效率。Kaaniche et al. (2017) 提出了一个基于区块链的数据使用审核架构，可以向数据控制者提供用户同意的不可伪造的证据，并且在区块链网络中使用基于 ID 的分层加密方法来防止数据泄露。Gordon et al. (2018) 使用区块链共享状态一致性的数据，并且对涉及用户健康数据的读写权限进行严格的访问控制。

目前基于区块链的数据共享研究中，鲜有学者在养老服务领域进行探索；并且在医疗健康等领域中提出的解决方案中大多仅限于某一种数据如电子病历，鲜少将研究对象的不同数据进行整合研究。

2.1.3 数据共享中关于激励机制的研究

激励是指在管理或经济活动中，使用一定手段和方法如奖励或惩罚措施激发参与者的主动性，使参与方为了实现自己的利益按照预期目标行动，从而促成管理效用最大化。激励机制是针对不同情景设置的适合用来充分调动参与方积极性的策略或方法。

数据共享中关于激励机制的文献的主要观点如表 2-2 所示，主要包括金钱式

激励和非金钱式激励。

表 2-2 数据共享中关于激励机制的研究内容

研究内容	主要观点	文献来源
金钱式激励	平台为参与者支付一定的金钱, 或者通过发行电子货币来跟踪平台中的各种交易并进行计费	移动群智感知网 (Zhang et al,2017; Jia et al.2018; Xuan et al.,2020) ; 科学研究数据 (Shresth et al.,2019) ; 医学数据 (Zhu et al.,2019)
非金钱式激励	社交关系激励: 构建平台中的社交圈、发布好友排名、选拔等	视频内容共享 (Wu et al.,2017) ; 车辆群智感知 (Zhao et.al.,2020) ; P2P 网络中的文件服务 (Du et al.,2020)
	区分服务: 基于参与者的信誉分数来提供有差别的服务	
	虚拟积分: 可兑换一定的实物或者服务	
	娱乐礼包: 基于游戏属性来向参与者发放有吸引力的实物或虚拟的礼包	

资料来源: 本文根据参考文献整理

为了使各个主体主动加入共享账本中, 实现从数据共享到价值共享, 胡元聪 (2021) 将区块链技术激励机制划分为三种类型, 分别为权力赋予型、收益增加型和声誉提高型。

Xuan 等学者 (2020) 借助区块链和进化博弈论设计出一个共享激励模型。该模型通过用户量划分用户参与阶段, 根据用户共享的成本和收益之间的关系, 对于不同阶段采取不同的激励方法, 在初始阶段用户量较小时, 使用奖励而非收取费用; 当用户量越过某一阈值时, 将收取特定费用。在该模型中的智能合约机制可以动态控制激励参数, 并不断鼓励用户参与数据共享, 但该模型未考虑数据质量问题。

Shresth 等学者 (2019) 针对科学研究数据的共享探索出了一个基于区块链的共享框架, 在该框架中创建了一种智能合约来激励用户共享数据, 数据消费者和数据拥有者通过预付保证金的形式来确保所有参与者诚实地共享数据; Zhu 等学者 (2019) 提出了一种区块链共享医学数据的合作模型, 推导了数据所有

者、矿工和第三方等参与者之间的拓扑关系以及价值分配过程，利用 Shapley 价值理论，将为患者提供诊断服务获得的收入分配给参与医学数据共享过程的合作者。

由以上分析可知，数据共享中激励机制可利用区块链实现，具体来说，可以通过发布数字货币、创建智能合约等形式来激励参与者共享数据，另外可以看到，养老领域或者医养结合领域中对于共享数据的激励机制研究有限，因此本文将对医养结合数据的数据共享激励机制进行详细探究。

2.1.4 数据共享中关于监管机制的研究

数据共享的监管是指在数据共享的整个过程中包括权限控制、数据访问等，通过采取一定的措施或策略来对参与者的行为进行监控的过程，从而减少由数据共享带来的潜在后果和影响。

表 2-3 展示了数据共享中关于监管机制的研究的主要观点。针对数据共享的监管机制研究包含实证分析和技术两大视角，在实证分析中，以制定规则制度来体现监管；在技术视角中，学者们大多利用区块链的智能合约技术来实现监管的自动化操作包括记录、拦截、撤销权限等。

表 2-3 数据共享中关于监管机制的研究

研究内容	主要观点	文献来源
制定规则制度	如规范、操作、绩效等方面的管理制度	郝世博等，2018； 杨帆，2019
利用区块链的智能合约	采用区块链存储操作日志，记载参与者读写行为；使用智能合约检测访问控制活动，违规操作时拦截访问请求、撤销该参与者的所有权限	Xia et al., 2017； Ferdous et al., 2017； Taha et al., 2020

资料来源：本文根据参考文献整理

2.2 理论基础

2.2.1 区块链

区块链的最初提出者是中本聪，它是一系列区块，它保存着像传统公共账本

这样的完整交易记录列表。图 2-3 为区块链示例图。按照节点间初始信任度及参与度等，区块链网络包括公有、私有和联盟三种形式。公有链有比特币网络等，联盟链有 Hyperledger Fabric 等。



图 2-3 区块链网络的示例图

资料来源：本文根据参考文献整理

(1) 区块链网络层次模型

区块链网络的逻辑结构是一种层次模型，按照自底向上方向，具体包括数据层、网络层、共识层、激励层、合约层和应用层。根据实际业务场景构建的区块链网络中，模型中的下面三层是必须考虑的，上面三层则是可选的。如图 2-4 所示。

1) 数据层

数据层在层次模型中位于最底层，主要描述了区块的数据结构。区块里面记录实际要存储数据，除了创世块以外，其他的每个区块头均含有前一个哈希值，该值指向了前置区块，从而使区块在逻辑上呈现链式结构，并一一相连。在数据层里面，主要包含的密码学技术有哈希函数、非对称加密等。

哈希函数是一种可以在有限时间里输出一个固定长度数字的函数，函数传入参数大小没有限制。在区块链网络中通常使用 SHA-256 这一哈希函数，即将任何大小的树转换成相对唯一的固定 256 位的值。这个值叫做哈希值。该值经常

被用来检验数据是否被更改过，即检验数据完整性。哈希函数可用以下公式表示。

$$\text{hash}(x) = \text{digest}, \quad x \text{ 表示输入, digest 表示输出} \quad (2-1)$$

非对称加密是指使用两个密钥来对数据进行保密的技术,这对密钥分别被叫做公钥 (Public Key, PK) 和私钥 (Private Key, SK)。用来实现对数据的签名和加密。在数据签名算法中,可以使用 SK 给数据签名,之后利用对应的 PK 来验证该数据是否被人更改过,以此确保数据完整性。在数据加密算法中,可以使用对应用户的 PK 给数据加密,之后该用户需要查看数据的时候,用自己的 SK 解开数据,以此实现机密性。即公钥加密,私钥解密;私钥签名,公钥验证。



图 2-4 区块链网络的层次模型

资料来源：张增骏等，2018

如图 2-3 所示,在一个 Blockchain 网络中有许多区块。每个块包括一个头部和块体。块的头部包含数据,例如版本号、时间戳、任意数字、Merkle 树根的哈希值和先前一个块的哈希等。版本是指区块要遵循的一些验证规则或策略的集合;时间戳用来表示区块的生成时间;随机数是一个任意值,每次计算都不

同；Merkle 树根的哈希值是对块里面所有交易实现一个哈希函数而得到。

区块体包括交易（Transaction, TX）数据，使用 Merkle 树来把块内交易整合在一起。一个交易代表双方之间的相互作用即传输数据，以加密货币为例，交易代表区块链网络用户之间加密货币的转移。区块链使用非对称加密技术来验证交易者的身份。该技术可以在不可信的环境中使用。在交易中，发送信息的一方使用自己的私钥进行数字签名，接收信息的一方可以用发送方的公钥来验证签名，看数据的完整性是否被破坏。

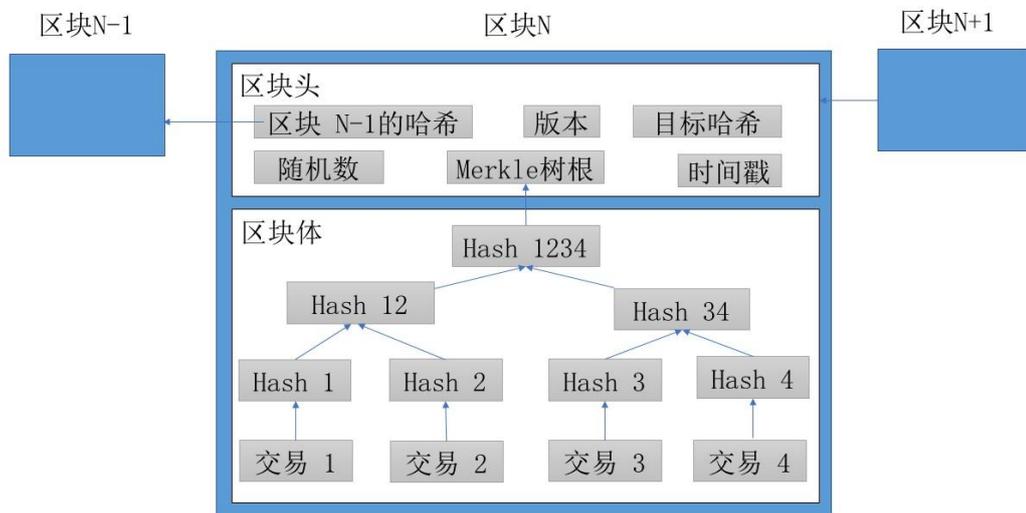


图 2-5 Merkle 树示意图

文献来源：郭上铜等，2021

Merkle 树是被 Ralph Merkle 提出的，这是一种基于数据哈希来构建出来的树形结构，在区块链网络中包含有 Merkle 树如图 2-5 所示，它的数据结构为一棵树，一般是二叉树；叶子节点对应了当前区块内一笔交易数据的哈希值，叶子节点两两连接经过哈希形成父节点，非叶子节点的哈希值是使用其子节点来计算出来的，通过反复执行哈希函数，最后就生成了交易 Merkle 树的根哈希。Merkle 树可以快速归纳和校验当前区块里的交易，因此块内任何数据的更改包括删除、添加、修改等都会被检测到，从而保证了交易的完整性。

2) 网络层

网络层提供可靠地数据传输服务，在这一层里面采用 P2P 协议来实现参与者之间的对等通信。根据实际产品或业务场景中的不同要求，区块链网络可以设计专属的传播策略和数据验证策略。传播协议可以确定区块链网络中数据的传播形式，并且按照数据验证机制来保证数据的有效性，区块链网络中的每个参与者都可以对区块进行校验和记账，只有被大部分参与方验证有效以后，才能被加入到区块链网络中。

3) 共识层

共识是指在一个区块链网络中，互不信任的节点通过某一机制在短时间内排除恶意节点的干扰，并对正确结果达成一致的观点。共识层非常重要，其中包含了共识算法，保证数据的正确性和完整性。为了保持账本的一致性，需要通过竞争记账的方式选出记账节点，由记账节点广播新的记账区块。共识算法确定由哪个用户发布下一个区块。

在公有链如比特币网络中，通常有多个节点同时竞争发布下一个区块，在获取记账权后，可获得加密货币——比特币奖励，由于公有链中各节点之间信任程度很低，因此共识机制须要耗费大量的资源比如挖矿需要耗费很多的算力和电力。在联盟链或私有链中，各参与方之间的初始信任度比较高，所以达成共识所需资源较少。当前已有多种共识机制，且每种共识机制仅适用于某类场景，常见的共识机制有工作量证明（Proof of Work, PoW）、权益证明（Proof of Stake, PoS）、股份授权证明（Delegated Proof of Stake, DPoS）和拜占庭将军容错共识（Practical Byzantine Fault Tolerance, PBFT）。

4) 激励层

为了实现区块链网络的持续发展，保证各节点积极参与记账，可在区块链网络中设置一定的激励手段来调动节点的积极性。激励层里包含分配和发行机制。在比特币网络中，获得记账权的节点将获得系统提供的比特币虚拟货币这一奖励，同时可获得交易流通过程中的手续费。在实际场景中，一些算力小的节点选择合作“挖矿”，以此提高获得记账权概率，并根据系统设计的分配机制获

取相应比例的奖励。

5) 合约层

各种脚本,算法和智能合约封装在区块链网络的合约层中,因此区块链具有可编程功能。智能合同一词是在1994年,由Nick Szabo界定为“自动执行合同条款的交易协议”。区块链网络中使用了智能合约,是一种可以自动执行的程序代码,在智能合约里可以实现约定好的合同条款。区块链使用智能合约来查询账本里面的数据。

区块链网络通过调用智能合约及触发事件来完成数字资产的自动化处置,智能合约的生命周期包括协商、开发、部署、运行和销毁5个阶段,是一段可以执行的代码。

6) 应用层

区块链网络的应用层封装了区块链的应用场景,目前的应用场景主要集中在数字货币、物流、金融等领域,包括比特币、以太坊、Hyperledger Fabric等。

(2) 区块链主要特征

1) 去中心化

区块链中的所有操作都可以由任何参与节点来完成。在传统的集中式交易系统中,每笔交易都需要通过中央信任机构如央行进行验证,导致中央服务器的成本高且性能低。与集中式相比,区块链不需要可信的第三方,而是使得权利下放,使用共识机制保证了账本中数据的一致性。

2) 不可篡改

一旦交易数据保存在区块链中,几乎不可能将其篡改,如果有恶意节点要篡改数据,则需要控制网络中至少51%的节点来对此次篡改达成共识,否则完全无效。因此在区块链中所保存的数据具有较高的可靠性。

3) 可溯源性

创建区块时,区块链中的每个区块均包含唯一的时间戳,并且每个区块均包

含前一个区块的哈希值，因此区块链网络中的区块按时间顺序排序，其中的任何交易数据可以快速验证和跟踪。

2.2.2 Hyperledger Fabric

Hyperledger(超级账本)项目是由Linux基金会于2015年创建的。Hyperledger Fabric 构建了一个联盟链，使用智能合约，采用可插拔式的模块化共识（崩溃容错或拜占庭容错），是一个参与者管理交易的系统。其关键概念有身份管理、通道和智能合约。

(1) 身份管理

Hyperledger Fabric 是联盟链，在该区块链网络中的各个成员都需要有一定的身份，成员身份由成员服务商模块（Membership Service Provider, MSP）注册验证，且该模块是可信赖的。通过身份管理，确定了区块链网络中的参与者对资源的确切权限。如果参与者需要其他权限则需要特定授权。

(2) 通道

Hyperledger Fabric 提供了创建通道的功能，通道是用于数据隔离和保密的一个私有区块链即网络的网络。在一个通达里面可以有多个参与者，有一个仅属于该通道的账本，并且每个参与者都有这个账本的副本，通道外面的其他参与者没有该副本。各个交易方需要被通道授权，之后才可以和账本交互。

通道的出现有利于一个大的区块链网络中间继续实现小范围的数据共享，其中的数据不会对交易方的竞争对手所看到，保证了数据的隐私性及访问控制。

(3) 智能合约

智能合约是被区块链网络外部的客户端应用程序调用的代码，用于管理世界状态中的键值对的访问和修改。

2.3 本章小结

首先，本章回顾了医养结合、数据共享以及数据共享中关于激励机制和监管机制的研究等国内外研究现状。可以看到，当前医养结合数据的共享仍依赖于集中式的系统，隐私风险较高；区块链技术相较于云计算和联邦学习可以更好

地解决数据共享过程中存在的隐私安全问题，并且已经取得了一些成果，但大多数解决方案局限于某一种数据如电子病历，鲜少将研究对象的不同数据进行整合研究；在数据共享中关于激励和监管机制的研究中，鲜有学者在养老服务领域进行研究。因此，目前来看，在养老服务领域，关于医养结合模式中的数据共享问题，尚未得到充分关注。

然后，本章详细阐述了区块链层次结构和去中心化、不可篡改、可溯源性三个主要特征，另外还介绍了 Hyperledger Fabric 的身份管理、通道和链码三个关键概念，为后面几章提供了研究基础。

第3章 医养结合数据共享模型的构建

尽管我国的医养结合已经推进了一定程度的发展，但仍存在数据孤岛、易于泄露、共享情况相对薄弱等问题。为了科学厘清医养结合数据共享的现状，明确当前实践模式中涉及的主体和数据项，本章将借助文献研究法、案例调研法以及软件工程法分析医养结合模式中的角色和数据，构建医养结合数据共享模型及分层架构，共包括四层，并对每一层进行详细阐述。

3.1 医养结合模式角色和数据分析

3.1.1 医养结合模式角色分析

根据我国在2019年发布的《医养结合机构服务指南》，指南中定义了新一类型的机构，被称为“医养结合机构”。它是一个既具备医疗卫生资质又具有养老服务能力的机构。主要包括两种表现形式，分别是养老机构内部开设一个医疗相关的部门以及医疗机构在内部设立一个养老相关的部门或开展一些养老相关的服务。因此，根据该机构是否同时具备医疗和养老服务能力，将当前的医养结合模式区分为两种表现形式，分别为图3-1和图3-2所示。

在医养结合模式中，主要包括家庭、医疗卫生机构、养老服务机构、医养结合机构、社区及政府部门等多个主体。其中，家庭是整个医养服务的需求方，具体包括家庭里的老年人及其家人；服务的供给方主要包含医疗卫生、养老、医养结合机构。医疗卫生机构包括各种类型的综合医院、社区卫生服务站、乡镇卫生院、康复或护理相关的医院、安宁疗护机构等；养老服务机构包括养老机构如敬老院、老年公寓等，以及提供养老服务的公司如一号护工、金牌护士等，还包括提供智能养老硬件的公司如可穿戴式、便携式或自助式健康监测或管理设备、服务机器人等；医养结合机构是指提供医养整合服务的组织；社区在整个模型里是支持方，为供需双方提供一定支持如提供驿站、筛选机构等；政府部门是服务的监管方，包含卫健委、民政部、公安、市场监管局、街道/乡镇等。

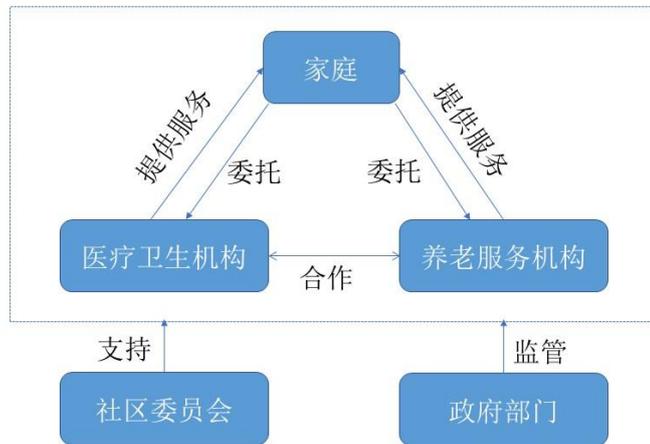


图 3-1 医养结合模式表现形式一
资料来源：本文根据参考文献整理

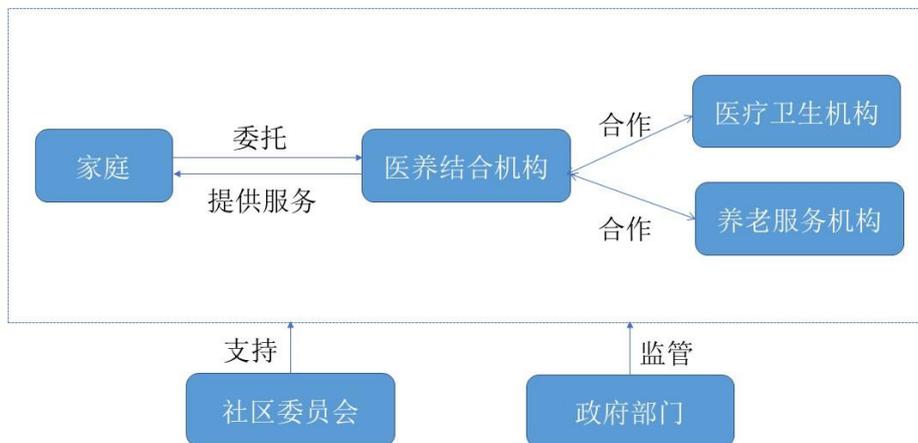


图 3-2 医养结合模式表现形式二
资料来源：本文根据参考文献整理

在表现形式一中，家庭请求并委托医疗卫生和养老机构提供服务。在整个过程中，医疗机构和相应养老机构可以签约合作。同时，社区起一定的支持作用，

政府部门在其中起一定的监管作用。表现形式二里面，同样地，家庭请求或者委托医养结合机构供应服务，医养结合机构可以和周边医疗机构如综合医院、中医医院建立签约合作关系，例如可以开启转诊的绿色通道，或者为老人提供远程医疗等服务；并且可以和养老服务机构如智慧养老监护设备厂商等合作，同样的，社区起支持作用，政府部门起监管作用。

基于以上分析，表 3-1 展示了医养结合模式中的角色。

表 3-1 医养结合模式中的角色

一级角色	二级角色
服务需求方	老年人及其家属
服务供给方	医疗卫生、养老服务及医养结合机构
服务支持方	社区
服务监管方	政府部门

资料来源：本文根据参考文献整理

3.1.2 医养结合模式数据分析

在现有的医养结合模式中，各主体之间依然处于一种独立的、非共享的状态，各主体通过各自的平台独立运行，甚至没有信息化平台仅通过线下运行，缺少信息交互和资源整合即缺少医养数据共享模型。医养数据共享模型借助区块链等信息技术，为各主体之间数据的流动提供路径，通过数据流动实现医养数据的共享，老人可获得连续、全流程、定制化的医养服务，进而实现主动及被动的健康管理。

从医养结合含有的服务类型出发，从而厘清其中涉及的医养数据。医养结合模式以健康管理为目的，协助改善老年人健康水平。医疗服务内容包括医疗保健、疾病诊治等，相关数据有电子健康档案和电子病历等；养老服务内容包括生活照料、精神慰藉等，相关数据有服务档案、物联网设备数据等。如表 3-2 所示。

表 3-2 医养结合模式中的服务及相关数据

服务类型	服务内容	相关数据
医疗服务	预防保健	电子健康档案
	疾病诊治	电子病历
	医疗护理	
	医疗康复	
	安宁疗护	
养老服务	生活照料	服务档案 物联网设备数据
	精神慰藉	
	文化娱乐	
	家政服务	
	康复训练	
	慢病护理	

资料来源：本文根据参考文献整理

电子健康档案是指按照相关规范建立的资料，其中包含基础信息、体检表、健康管理表以及就诊、转诊等诊疗记录。个人信息表里面包含有姓名、疾病历史等字段；健康体检包括健康状况、用药等字段；健康管理表中有老年人生活和健康评估、检查、指导等字段；就诊、会诊、转诊等接受医疗服务的记录包括时间、医生姓名等，医师巡诊记录包括时间、医师姓名、老年人血压、心率等身体状况。

电子病历是指老年人就医病历，包括诊断科室、诊断结果、药物名称、服用剂量等数据项。

服务档案资料包括老年人护理需求评估数据，养老服务记录如护理类型、服务项目、下单时间等数据项。

物联网设备数据包括心电监测、血压监测、血糖检测、血氧检测、体温检测、手环手表类、智能照护、智能康复等物联网设备数据。

3.2 基于区块链的医养结合数据共享模型

从宏观角度出发，基于区块链的医养结合数据共享模型包括数据、数据共享

平台、权限管理方、数据供给方、数据需求方五部分内容，如图 3-3 所示。数据是指与老人密切相关的医养结合数据，具体为上一小节得出的四类数据。数据共享平台是指底层应用了区块链网络、实现了医养结合数据共享功能的管理信息系统。权限管理方是指对医养结合数据拥有管理权限的角色，拥有授权和除权功能，从而控制哪些人能看哪些人不能看。数据供给方是指医养数据的拥有者，存储有老人的医养隐私数据。比如医疗卫生机构存有老人的电子健康档案和电子病历，养老服务机构拥有老年人曾经获取服务的档案、物联网设备数据等数据。数据需求方是指需要处理医养结合数据的访问者。

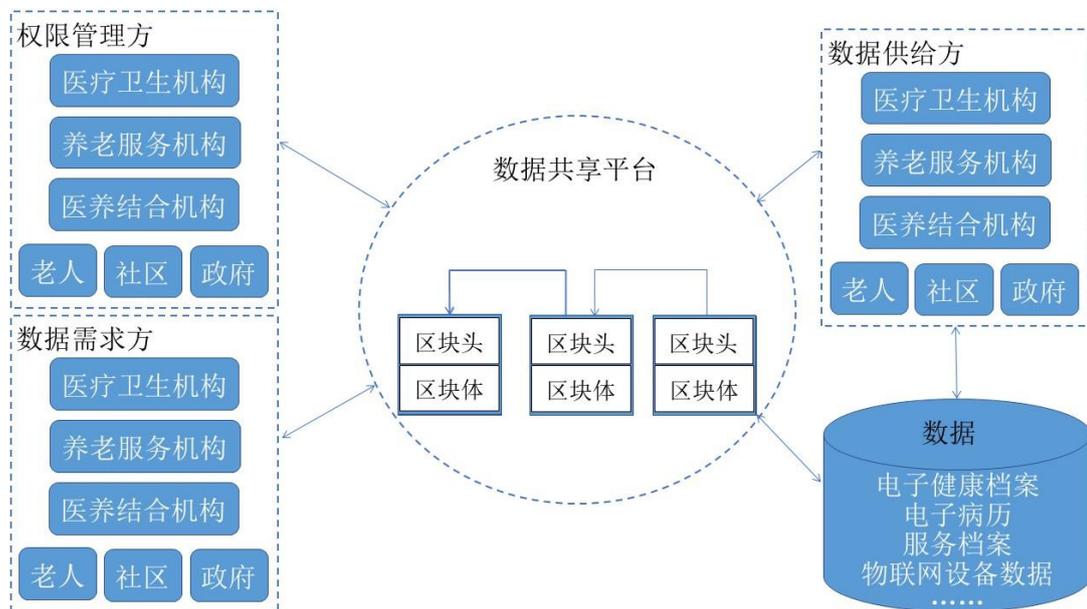


图 3-3 基于区块链的医养结合数据共享模型

可以看到，在该模型中，各角色之间可以相互依赖和转换，如医养结合机构既是模型中的数据供给方，又是数据需求方，同时也可以作为权限管理方。整体模型中的数据流动规则是，首先由权限管理方将数据授权给相应的数据供给和需求双方，之后数据供给方通过医养结合数据共享平台发布数据、分享数据，随后，被授权的数据需求方可检索、查看数据，最终达到整个数据流过程的透明及可信。通过区块链的虚拟代币的激励机制可以促进整个共享模型的可持续发展，同时区块链具有的时序不可改变、可溯源等特点确保了数据的隐私和完整性。

3.3 基于区块链的医养结合数据共享模型分层架构

在孟小峰等学者（2020）的研究中把基于区块链实现数据获取和共享的框架分为数据获取、存储、区块链和共享四层，因此我们延续该思路，将基于区块链的医养结合数据共享模型的结构分成四层，如图 3-4 所示，自下向上包括数据收集层、数据存储层、智能合约层和数据共享层，接下来我们将详细描述每一层。

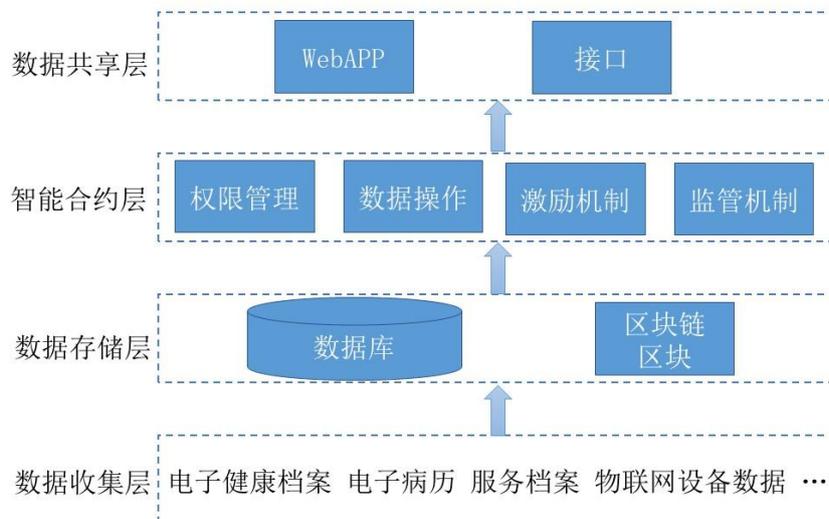


图 3-4 基于区块链的医养结合平台数据共享架构

3.3.1 数据收集层

医养数据是在医养结合里面，各个涉老角色或者主体产生的各种类型的数据。医养结合数据共享模型的逻辑结构之数据收集层是指医养结合数据由角色或主体产生之后，被获取并保存到相应的存储设备中形成数据源。该角色或主体被称为数据所有者。在此过程中，数据所有者有权了解被收集数据的内容、形式、目的及相应的分析、处理过程，并且有权设置第三方对某些或全部数据的访问权限。

老人接受相应的医或养老服务后，相应的医疗组织和养老机构即获取到老人相应信息。基于物联网设备的养老服务已经被广泛应用，老年人可使用手表式安全健康检测仪等物联网设备，同时设备数据将上传至服务商，从而实现多方面

危险监测与分析。具体的监测内容包括：（1）体征监测，检测老年人的体温、血压等生命体征；（2）环境监测，测量老年人所处环境中的位置、温度、烟雾等内容；（3）运动监测，通过物联网设备中的传感器来检测老年人是否摔倒、是否从床上等地方掉落等；（4）服务过程监测，通过采集图片、语音、视频等内容来对服务过程的意外情况及服务质量等进行监测。以上数据经医疗服务机构、养老服务机构等主体储存后形成一个个孤立的数据源，存储方式大部分为集中式存储。

3.3.2 数据存储层

数据存储层是指医养数据的存储方式。这里包含两种方式，**方式一**是数据供给方将数据传输并存储在共享平台的数据库；**方式二**是数据供给方因各种原因希望保持自身数据的所有权，因此可以仅提供一个数据访问地址（URI）来共享数据。

首先我们针对方式一的情况进行详细讨论。医养结合模式中的医养结合数据具有私密性、特殊性等特点，并且数据量大、数据类型多，因此，在设计数据存储机制的过程中，需考虑隐私保护和安全存储方面的问题。

大数据可按照其类型分为结构化、半结构化以及非结构化。主要通过数据库来存储，其中关系型数据库主要用来存储数据间耦合度高、对扩展性要求不高的数据，有易于维护、使用方便、支持复杂操作等优点，同时具有海量数据读写性能较差、灵活度不高等缺点；非关系型数据库适用于存储数据量大、对可扩展性要求高等类型的数据，它具备格式灵活、速度快、扩展性高等优点，但同时也有数据结构相对复杂、复杂查询功能较差、无事务处理等缺点。

结构化数据通常用关系型数据库存储，方便查询和修改。常用的关系型数据库有 MySQL、SQL Server、Oracle 等。

半结构化数据没有严格的结构和关系，但包含一些标记，被称为自描述的结构，常用于网站日志。在存储上，可以转换为结构化数据，如拆分为多个表结构，但其扩展性不高；此外，半结构化数据还可以采用 XML 或 JSON 格式处理并存储，可以实现灵活扩展，但是其检索速度相对较慢。

非结构化数据包含图片、语音、视频、报表、文本等类型，缺少完整结构或者不规范，可以采用非关系型数据库存储。表 3-3 展示了常用的非关系型数据

库。

表 3-3 非关系型数据库分类

类型	数据库举例	数据模型	优点	缺点	应用场景
键值型 (Key-Value)	Redis、Risk、 LevelDB	Key-Value 键值 对	扩展性高， 性能高	不支持复杂 的数据结构	内容缓存等
列存储型 (Column)	HBase、 Cassandra	同一列数据存储 在一起	扩展性高， 检索高效	功能局限	分布式数据 存储
文档型 (Document)	MongoDB、 CouchDB	Key-Value 形式	结构灵活	缺少统一的 查询语法， 检索速度慢	Web 应用等
图形(Graph)	Neo4j、InfoGrid	图结构	支持图形 算法	复杂性高	知识图谱、 社交网络、 推荐系统等

资料来源：本文根据参考文献整理

医养结合数据主要包含四类。电子健康档案中基础表、体检表可以为结构化数据，健康管理表是一些结构化或半结构化数据；电子病历里有如科室、处方等的结构数据，也有例如脑电图等图像信息；服务档案中多为结构化数据，但也存在语音、视频等用来记录服务过程及结果的非结构化数据；物联网设备数据多为半结构化或非结构化的。因此其中的结构化数据较多，针对方式一，当数据供给方同意将数据收集、传输并存储在数据共享平台的数据库中时，本文采用数据库与区块链结合的形式存储医养数据。

为了保护数据隐私，本文使用加密算法对数据进行加密，之后存储至数据库中，并用一个元数据指针（Reference Point, RP）指向该数据存储的地址，也被称为数据访问地址 URI，该 URI 是唯一的且不可改变。同时在智能合约层的发布交易中存储 URI，即区块链中仅存储 URI，从而使区块链上的数据保持轻量化。当需要对区块链网络中的其他角色授权时，则在访问控制交易中写入 URI，共享相应的 URI，数据需求方可以访问 URI 来获取到真实的数据，因此，可以通过共享 URI 即可实现对特定数据的共享。

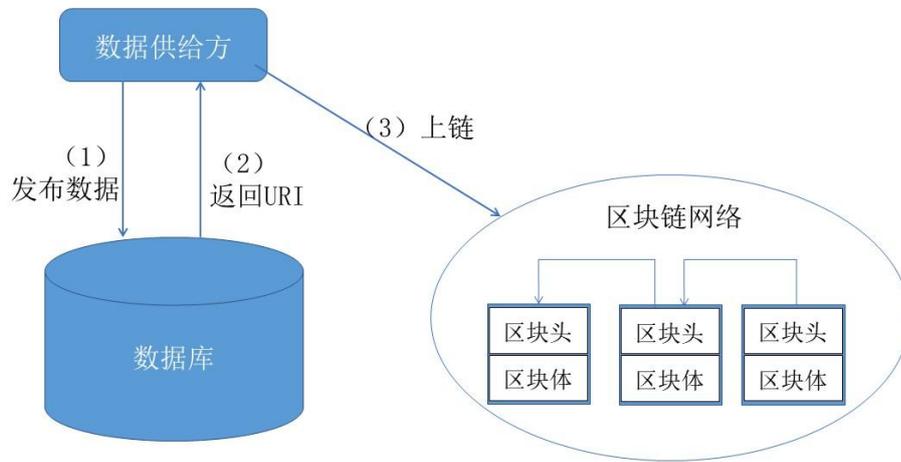


图 3-5 医养结合数据共享模型的数据存储机制

图 3-5 展示了基于方式一的模型中的数据存储机制。首先，数据供给方发布数据，供给方使用个人私钥加密数据后存储至数据库中，同时获取到唯一的数据访问地址 URI；然后会在网络中发布上链交易，即调用上链智能合约把 URI 保存到区块链网络中。需要说明的是，只有数据所有者才可以是数据供给方，被分享数据后拥有查询权限的用户不是数据供给方，也就不能向其他用户分享数据。

接下来我们针对方式二的情况进行详细讨论，当数据供给方选择将数据存储于自己的设备中，可以仅提供针对不同数据提供唯一且不变的 URI，数据需求方可以通过该 URI 获取到相应数据。在该方式中，数据供给方提供数据访问地址 URI 并将 URI 发布到区块链网络中。

可以看到区块链中仅保存数据的 URI，经加密后的数据实际存储地址仍在传统数据库中，以此实现区块链网络的高效运行。在区块链网络中，我们使用智能合约来上传、访问数据，用户在区块链网络中处理的任何操作都会被记录在区块链中，并且不会被篡改，以此保证数据共享过程的透明性，实现医养结合数据的共享。

3.3.3 智能合约层

这一层包含有各种智能合约。智能合约提供一种可编程业务逻辑，且能够自

自动化执行。在医养数据共享模型中使用智能合约来实现权限控制和数据操作，任何数据的授权和访问情况都通过区块链的交易记录在区块链中，为了减小链上数据存储、提高区块链的效率，我们仅操作和存储 URI。区块链网络中的角色可以先获取到 URI，再通过 URI 获取到相应的完整数据。在本小节将定义权限管理和数据操作两类智能合约。在智能合约层还包含有两种关键机制——激励机制和监管机制，这两种机制将在本文的第四章进行详细分析。

在权限控制部分，本文实现以老年人为中心的权限管理机制，该机制实际是一类智能合约，权限管理方以老年人为主，社区和政府部门为辅，提供以资源为单位的访问控制策略。在该机制中，权限管理方可以实现授权和除权操作。如图 3-6 所示，老年人作为权限管理方，可以向数据供给方和数据需求方发起授权和除权操作，当老年人发起授权操作后，数据供给方可以发布数据，并且和相应的被授权的数据需求方分享该类型的数据；当老年人发起除权操作后，数据共享方相应取消与数据需求方的数据共享。

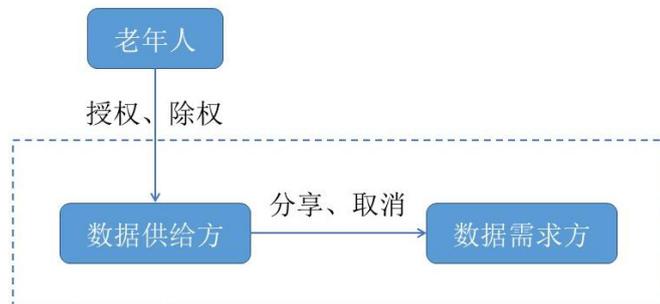


图 3-6 以老年人为中心的权限管理机制

合约模块的另一部分是数据操作机制，顾名思义，数据操作主要是提供医养结合数据的发布、共享、取消以及查询等功能的一类智能合约，是实现共享过程中最为关键的部分。在数据操作机制中，数据按 3.1.2 节分析可分为电子健康档案、电子病历、有服务档案、物联网设备数据四种类型。

数据操作流程如图 3-7 所示，当权限管理方发起授权操作时，数据供给方首先在区块链网络中执行发布操作从而发布数据，然后向相应的被授权的数据需求方分享数据；当权限管理方发起除权操作时，数据供给方取消与数据需求方的数据共享。数据需求方在获取相应的数据权限后，通过“查询”操作利用自

己的相应密钥获取到数据访问地址 URI，再通过页面访问获取到真正的数据。可以看到，权限管理智能合约和数据操作智能合约联系紧密，并且以上所有操作包括授权、发布、分享、除权、取消以及查询都将记录在区块链的账本中，并且记录不会被改变。

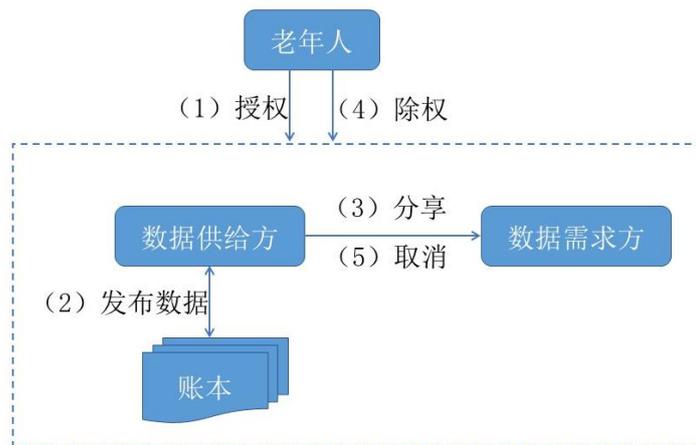


图 3-7 数据操作流程

3.3.4 数据共享层

数据共享层位于医养结合数据共享模型逻辑结构的顶层，是指通过调用相关接口，以可视化的形式如 WebApp 界面，实现医养结合数据发布和访问，从而实现数据共享。

3.4 本章小结

为了破解医养结合模式里面的“数据孤岛”难题，增强医养结合数据在流通过程中透明性，本章首先从刻画了医养结合的两种表现形式，并在此基础上，基于数据流动角度，探究了医养结合模式中的角色和数据；然后从宏观角度构建了基于区块链的医养结合数据共享模型，包括数据共享平台、数据供给方、数据需求方、数据四部分内容；紧接着分析并构建了医养结合数据共享模型。详细描述了数据共享模型中的数据存储机制以及智能合约模块中的权限管理和数据操作两类智能合约。基于区块链的医养结合数据共享模型的智能合约层中

还包含有两类关键机制，分别为激励机制以及监管机制，本文将在下一章详细描述。

第 4 章 医养结合数据共享机制研究

在上一章中我们分析了医养结合模式中的角色和数据,并构建了基于区块链的医养结合数据共享模型,其中在智能合约层还包括有两种关键机制,分别为激励机制和监管机制,在本章中,本文将借助规范分析法来构建医养结合数据共享中的激励和监管机制,两种机制并非独立存在,而是相互联系和作用的,这两种机制均利用智能合约技术来实现。

4.1 医养结合数据共享模型中的激励机制

激励相容 (Incentive Compatibility) 理论是一种基础理论。它指的是对于一定的经济环境和社会目标,如果能有一种策略使人们自主采取相应的行动,正好使预定目的得以实现,我们就称这个策略是激励相容的 (Myerson, 1979)。该策略设计的目的是让一个人的社会选择函数实现最优化,这个函数是确定的 (胡元聪, 2021)。

在医养结合数据共享模型中,激励机制是指在医养结合模式中,通过设置一定的激励方法来促进各角色用户对于数据共享这一行为的参与,同时促进用户之间的信任。在信息系统领域用户参与的研究中,社会资本理论作为一种社会学经典理论常被引入用户参与行为、用户参与的信任等研究中。因此我们结合激励相容理论和社会资本理论来探究医养结合数据共享中的激励机制。

医养结合数据共享模型中的各个角色之间存在一定的信任基础,即有信任这一关系型社会资本。本文将通过发布数字货币的形式来增强用户的社会资本,从而激励用户参与共享,下面将详细描述。

在数字货币的研究中,Chasin 等 (2020) 通过对 16 种数字社区货币 (Digital Community Currencies, DCCs) 进行文献回顾,构建了数字社区货币的六项设计原则,分别是竞争性 (Competitiveness)、透明性与自治 (Transparency and Self-government)、流通性 (Circulation Velocity)、不可转让性 (Non-transferability)、合法性 (Legitimacy)、无边界性 (Self-organizing Locality)。

竞争性是指建立强有力的市场机制,鼓励社区成员赚取和使用数字社区货币;**透明性与自治**是指数字社区货币应该由各自的社区拥有,并且货币治理组

织结构应完全透明；**流通性**是指建立鼓励会员使用其电子货币而不是堆积的激励机制，提高货币循环或流通速度；**不可转让性**是指禁止将数字社区货币兑换为其他货币，从而保持社区财富和价值，防止任何人从中获取不当利益；**合法性**是指获得政府的官方支持，以此取得社区成员对数字社区货币的信任，并一定程度上减少法律或行政障碍；**无边界性**是指数字社区货币不应限制货币使用的地理位置。



图 4-1 数字社区货币的构建原则

资料来源：Chasin et al. 2020

本文参考以上设计原则中透明性、合法性以及无边界性等特点，提供一种持续性的数字货币激励方案，称之为“共享币 ShareCoin”。

在共享币的发行环节，可以通过众筹或政府如卫健委拨发助老经费的方式来启动项目；在运行和分配环节，老年人通过付款来获取医疗卫生和养老服务机构的的服务，这里的机构为数据需求方；老年人向数据供给方和数据需求方授权，来使自身的医养结合数据可以在机构之间共享，同时机构可获得一定比例的酬劳以及系统自动发放的共享币。

在运行环节，老年人向数据需求方付款来获取相应的医疗或养老服务，之后数据需求方向数据供给方预付共享币，该预付的共享币存储在预付账户（Pay Address）中，数据供给方分享了相应的数据后即可获取预付账户中的共享币，同时还可获得系统自动发放的共享币。

一切激励的基础是数据共享活动，即在权限管理和数据操作中，基于不同的交易活动由系统自动发放货币奖励，可参考表 4-1 给出的一种激励方案样例。

表 4-1 医养数据共享模型激励方案样例

交易活动类型	ShareCoin 奖励数量	被奖励方
授权	5	权限管理方
除权	1	权限管理方
发布	5	数据供给方
分享	5	数据供给方
取消	1	数据供给方
查询	0.01	数据需求方

基于不同类型的交易活动为不同角色用户奖励相应数量的 ShareCoin，其中“授权、发布和分享”操作是数据共享模型中的关键流程，因此给予较多 ShareCoin 奖励；同时为了保证数据的隐私性，确保用户及时除权，为“除权、取消”操作奖励 1 个 ShareCoin；在数据共享模型中，对数据的查询是最基础的操作，因此获得的 ShareCoin 奖励也将最少。在整个数据共享模型中，所有 ShareCoin 奖励的发放均是由系统即智能合约自动完成，保证了透明性。ShareCoin 的合法性指严格遵守所有法律、法规，并且获取政府部门支持，ShareCoin 的无边界性是指没有地理位置上的限制，任何通过该模型系统操作的用户均可以获得相应数量的 ShareCoin，同时增强了 ShareCoin 的开放性和可持续性。

该数据共享激励机制的研究意义有：

1) 对政府而言，一个区域内的 ShareCoin 总量这一数据可用于“智慧医养发展指数”、“智慧助老指数”等指标体系中，作为评测工作的重要参考。以城市为例，当一座城市中的共享币 ShareCoin 的数量越多，说明该城市中医养结

合数据的共享活动越频繁，共享程度越高，从而表示发挥出了更大的数据价值，老年人需求得到了更多满足。

2) 对于机构而言，当一个机构拥有的 ShareCoin 越多，可表征机构适老化指数、信用评级等方面，促进机构可持续良好发展；此外，可在政策指导下，向政府申请使用 ShareCoin 抵扣税款等，减轻机构运营压力。

3) 对老年人来讲，老年人可以从中获得更多持续性、针对性的服务。

4.2 医养结合数据共享模型中的监管机制

基于区块链的医养结合数据共享模型中的监管机制是指政府部门对医养结合数据流动的全过程进行监控，通过审计、监督等功能，从而对医疗机构、养老组织和医养结合机构等医养结合涉老主体起到监管作用。在这一节中，我们可以发现在医养结合数据共享模型中，权限管理方除了老年人这一主要角色外，还包括政府部门，这是因为，在数据共享过程中，可能会出现老年人已经离世等情况，因此就需要政府部门依据老年人户籍信息来相应撤销医养结合数据的共享权限。由于政府这一监管方角色属于医养结合数据共享模型中的角色之一，因此我们假定监管者的动力也是由上一小节中的激励机制提供的。

在监管机制中，本文主要通过系统自动监管和设置监管节点两种方式来实现。

系统自动监管方式，是指利用智能合约技术，当用户对数据执行读、写等操作时，系统会检查用户权限，如果用户无权限时则表明用户违规操作，将自动拦截请求并扣除一定的 ShareCoin，并把用户的所有行为记录在系统日志中，然后存在链上。表 4-2 展示了一种利用智能合约技术伪代码形式实现的监管机制。

设置监管节点是指引入政府部门这一类监管节点，检查系统中的权限管理和数据操作等交易，对系统中的数据流转过程进行监控。监管机制的实现主要是使用智能合约来实现，监管节点可以通过查看系统日志中的用户违规操作来对用户所属机构进行信用评级和安全风险评估，对于风险较高的机构采取线下监督整改等措施，从而实现事前监督。

另外，监管节点可以查看区块链账本中的所有数据被发布或访问的情况，定期审计共享模型中的交易，检查区块链网络中数据已授权但未分享、已除权但

未取消分享等应该或不应该共享的异常情况，对于涉及的机构进行线上线下的提醒。

表 4-2 监管智能合约

监管智能合约
前置条件：用户在平台成功注册 传入参数：共享数据的类型 dataType、userID 算法： for func(发布数据) do // Check publish authority; if authority == false then Revoke(拦截方法, prompt error message); //拦截请求 Log(违规发布, userID, dataType); //记入日志 end for for func(分享数据) do // Check share authority; if authority == false then Revoke(拦截分享, prompt error message); //拦截请求 Revoke(access authority); //撤销访问权限 Log(违规分享, userID, dataType); //记入日志 end for

4.3 本章小结

为了促进医养数据的共享，激励各个涉老主体或者角色主动参与，监控整体流程。在本章中利用规范分析法，探究并设计了医养结合数据共享模型中的关键机制包括激励机制和监管机制。两种机制的完成均依赖于智能合约。

在激励机制设计中，我们设计了一种持续性的数字货币激励方案，讨论了“共享币”的发行和分配机制，在医养结合数据共享模型中，用户参与程度越高，经授权分享的医养结合数据越多，即可以获得更多的共享币。通过共享币的形

式促进了医养结合数据在相应主体之间的共享，在一定程度上解决了医养结合模式中的数据孤岛问题。

在医养数据共享过程中，数据首先由老年人授权，同时，数据供给方发布、共享数据以及数据需求方访问数据时均利用了非对称加密技术来实现。在监管机制的设计中，通过系统自动监管和设置监管节点两种方式对系统中的医养结合数据的流动过程来实现事前监督和实时监管。因此，在医养结合数据共享模型中，数据安全性可以得到保障。

在下一章中，将基于第三章和本章设计的医养结合数据共享模型和机制探究在实际中的应用，并用 Hyperledger Fabric 进行仿真。

第 5 章 医养结合数据共享平台的设计与实现

医养结合数据共享模型的构建，对于共享平台或系统研发具有重要作用。本章将基于已构建好的医养结合数据共享模型来探究如何应用至实际中。本文将通过设置医养结合场景，借助 Hyperledger Fabric 技术，来对前两章提出的医养结合数据共享模型及关键机制进行仿真实现。

5.1 医养结合场景

我们假设 A 先生今年 65 岁，患有糖尿病、高血压等慢性病，养老方式为居家养老。当有医疗服务需求时会去签约医院看病或者电话咨询签约的家庭医生、请求提供上门诊疗服务等。另外，经常会使用养老服务机构的线上平台来预约日常照料、慢病护理等。医院存有 A 先生的电子病历和电子健康档案，机构存有 A 先生的养老服务数据和物联网设备数据。

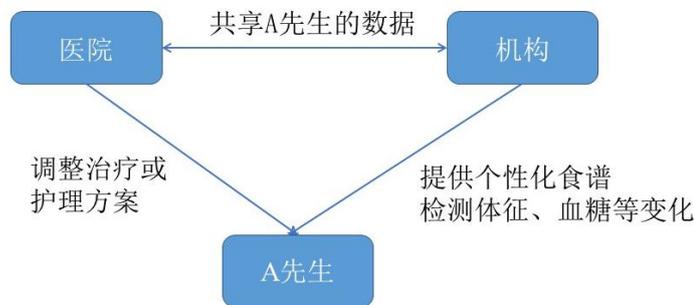


图 5-1 A 先生的医养结合场景

如图 5-1 所示，在 A 先生的授权下，医院会和机构互相共享 A 先生的数据，比如当 A 先生预约生活照护服务时，养老机构可查看电子病历得知 A 先生患有慢性病，因此派遣具备相关慢病管理知识的护理员为 A 先生提供个性化服务，如在饮食上提供富含膳食纤维的食物；根据治疗方案提醒 A 先生按时服药、监测血糖和体征变化。同时，医院也可以根据 A 先生的体征状况去相应调整治疗或护理方案等。即整合医和养的资源为 A 先生提供针对性服务。

本文将基于以上场景来仿真医养结合数据共享模型。

5.2 医养结合数据共享平台框架介绍

以上述构建的医养结合场景为例，本文使用 Hyperledger Fabric 框架来模拟实现。与其他区块链网络相比，Fabric 作为一种联盟链，对于数据安全性和隐私保密性方面拥有优异表现。Fabric 中的账本分为两类，分别是区块链和世界状态，链上保存更新世界状态的交易，且记录不可改变；世界状态描述在某个时间点的数据，使用 CouchDB 或者 LevelDB 存。

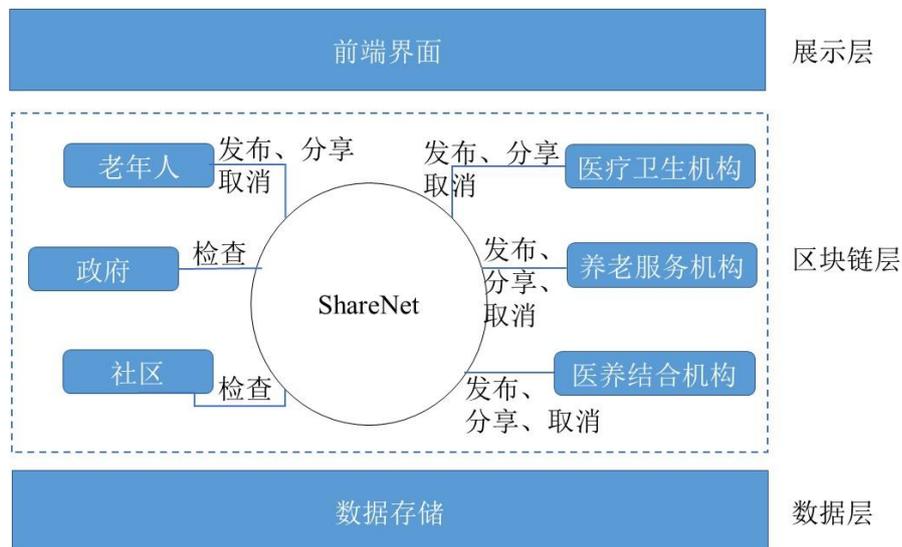


图 5-2 医养结合数据共享平台框架

从图 5-2 可以看出，本文设计的医养结合数据共享平台为三层结构。

(1) 展示层：利用 HTML、Less、JavaScript、React、Ant design 等语言实现前端界面，直观展示平台功能，保证易用性。

(2) 区块链层：使用 Fabric 技术构建区块链网络，并提供前端与区块链的 API，提供授权、发布、分享接口。

(3) 数据层：是指把加密后的数据存在传统数据库里，仅提供一个访问地址 URI 存储在链上，以此实现轻量化区块链。

在区块链层，包含了医养结合模式中的各个角色，以及角色在区块链网络中

所能执行的智能合约类型。

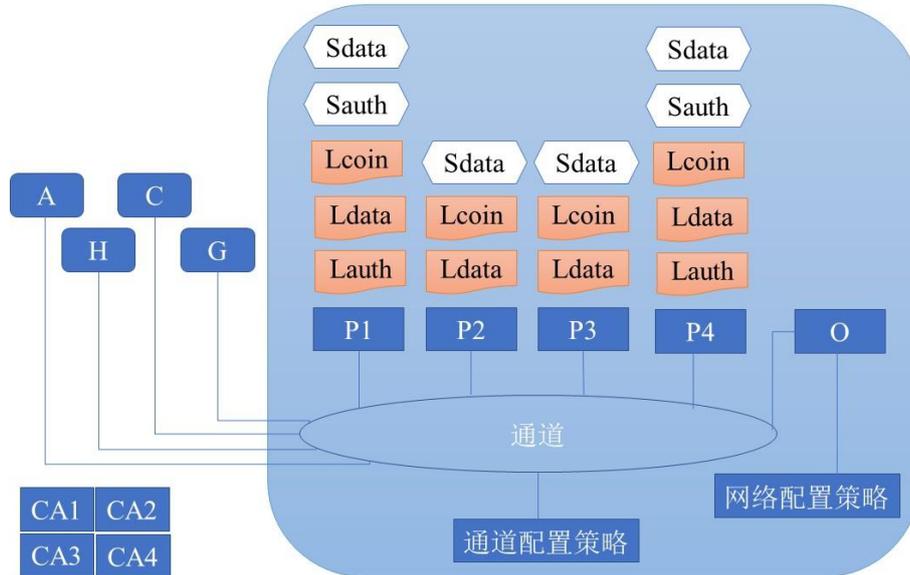


图 5-3 区块链网络

在区块链层中详细的网络细节如图 5-3 所示，在该网络中包含了 4 个组织，每个组织中均包含有 1 个用户。整个区块链网络中包含有 4 个 Peer 节点和 1 个排序节点，此外，还包含 4 个 CA（证书认证机构），分别为 4 个组织中的节点和用户颁发证书；包含权限控制状态、数据共享状态、数字资产状态三种状态。O 表示排序节点，所有节点均在同一个通道中。网络根据网络配置 NC 中指定的策略规则进行管理，通道由 CC1 中制定的策略规则进行管理，由 O1 和 O4 控制。

在区块链网络中包含三个账本 Lauth、Ldata 和 Lcoin，分别表示权限管理状态、数据共享状态和数字资产状态；分别由三类智能合约控制 Sauth、Sdata 及 Scoin，分别为权限管理、数据操作和数字资产智能合约。节点 P1 和 P4 上部署有所有账本和权限管理、数据操作智能合约；节点 P2 和 P3 上部署有数据共享状态和数字资产状态，以及数据操作智能合约。在应用程序上分别有 A、H、C 和 G 分别代表具体的用户，依次为老年人 A 先生、医院的系统管理员、养老服务机构的护理员以及政府工作人员。

5.3 医养结合数据共享平台实现

5.3.1 开发环境准备

用户使用终端或者 WebApp 发起请求，WebApp 调用 Fabric 支持的 SDK 中的 API，然后会生成一个交易提案（Proposal），发到指定的区块链网络的通道中；然后由策略表中的节点参与背书并返回交易提案响应（Response），应用程序收集到足够数量的 Response 后形成完整的已背书的交易，向排序节点发送该交易；接着排序节点（Orderer）将一个个交易加到区块里并且分发给 Peer 节点；随后所有节点验证交易，确保已背书；最后将区块更新进自己维护的账本中。以上即为区块链网络中的交易流程。为了支持不同的编程语言来开发应用程序，Fabric 提供了许多 SDK。稳定版的有 Node.js SDK 和 Java SDK，此外还有 Python SDK 和 Go SDK 可供下载和测试。本研究将采用 Node.js SDK，该版本最为稳定且应用最广泛。

本文使用虚拟机，其操作系统为 Ubuntu 16.04。软件环境包括 cUrl、Node.js、npm package、Docker、Docker Compose、Git、Hyperledger Fabric1.4 等，软件开发工具有 Visual Studio Code，软件开发语言使用 JavaScript。我们根据以上基础实现链码即智能合约和前端可视化界面。

在前端程序中，调用链码来实现各类交易。一种交易流程示例如图 5-4 所示，老年人、医院、养老服务机构以及政府部门这四个组织（Organization）中分别包含一个用户，分别为 A、H、C、G。可以看到，当 A 或 G 执行授权操作，请求 H 向 C 分享数据；然后 H 执行发布交易和分享交易，C 可以查询到被分享的交易信息；当 A 或 G 除权后，H 执行取消交易，C 的权限被取消，从而 C 无法查询到被分享的信息。

基于上述环境，本文将开发医养结合数据共享平台。

5.3.2 智能合约实现

在 Fabric 框架中，智能合约也叫做链码，它实质上是一个程序文件，使用 Go、Node.js 或者 Java 编写，来实现一些预定义接口，接口中定义了交易逻辑。链码是在一个 Docker 容器里运行的，可以和账本实现交互，确切地说，和账本世界状态进行交互，智能合约可以实现对世界状态的读写和删除，还可以查询交易记录，该记录是不可篡改的。而链码初始化及账本状态的管理均是通过

WebApp 提交交易实现的。WebApp 调用智能合约接口来生成交易并且被记录到链上。本文中所实现的为用户链码，主要包括三类：权限管理、数据操作和数字资产，分别和三个账本中的世界状态实现交互。

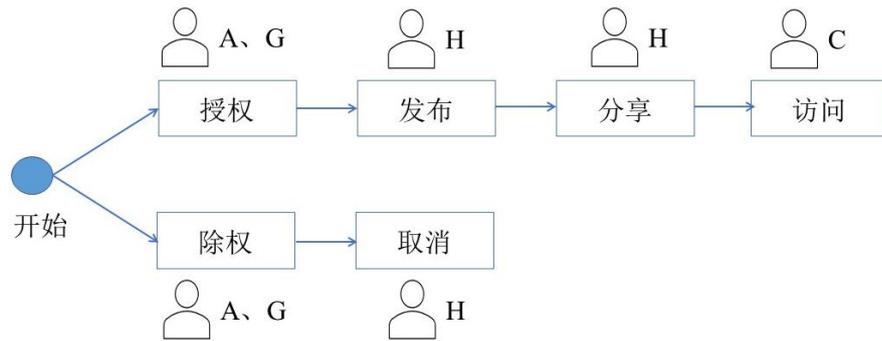


图 5-4 医养结合数据共享中的交易流程

在该系统中包含三类世界状态，即权限控制状态、数据共享状态和数字资产状态，它们存储于 LevelDB 数据库中。下面将以数据操作智能合约为例给出相应的世界状态字段以及使用伪代码形式表示的部分算法。表 5-1 展示了数据共享状态中包含的数据及其意义。

表 5-1 数据共享状态

字段名	含义
theAgedId	老年人 ID
dataType	共享数据的类型，包含电子病历、电子健康档案、服务档案、物联网设备数据
Publisher	数据的发布方
ShareFrom	数据供给方，一般和发布角色一致
ShareTo	数据需求方
Uri	数据访问地址
Date	日期
currentState	数据共享的当前状态，包括已发布 <code>published</code> 、已分享 <code>shared</code> 、已取消 <code>canceled</code>

数据操作智能合约可操作数据共享状态,接下来将以伪代码的形式实现数据操作智能合约的实现过程,如表 5-2 所示。

表 5-2 数据操作智能合约的伪代码实现

数据操作智能合约
<p>前置条件: 用户在平台成功注册且已被授权或除权</p> <p>传入参数: 老年人 ID、共享数据的类型 <code>dataType</code>、发布方 <code>publisher</code>、<code>from</code> 数据来源、<code>to</code> 去处、数据访问地址 <code>uri</code></p> <p>算法:</p> <pre> // 发布 Function publish(theAgedId, dataType, publisher, uri){ const userId = ctx.clientIdentity.getID(); let shareKey = ctx.stub.createCompositeKey(auth, [userId, dataType, publisher, from]); // 获取当前数据的发布状态 const shareKey = ctx.stub.getState(shareKey); if(已存在){throw new Error('数据已被发布过')} // 如果不存在 const shareData = { theAgedId: userId, dataType, publisher, Sharefrom: publisher, uri, currentState: 'published', } // 存储到数据共享账本中 await ctx.stub.putState(shareKey, shareData); invoke.reward(5);// 同时获得 5 个 ShareCoin } // 分享 Function share(theAgedId, dataType, from, to){ const userId = ctx.clientIdentity.getID(); let shareKey = ctx.stub.createCompositeKey(auth, [userId, dataType, from, to]); // 获取当前数据的共享状态 const shareKey = ctx.stub.getState(shareKey); </pre>

```
if(已存在){throw new Error('数据已共享')}  
// 如果不存在  
await ctx.stub.putState(shareKey, {currentState: 'shared'});  
// 同时获得 5 个 ShareCoin  
invoke.reward(5);  
}
```

5.3.3 平台可视化界面实现

本文实现的医养结合数据共享平台可视化界面的用户登录页面截屏如图 5-5 所示，用户登录成功后可实现相应操作。



图 5-5 用户登录界面

用户 A 的功能界面截屏如图 5-6 所示，左侧为功能导航，主要包括流程监管、权限管理、数据管理和个人中心，其中数据管理功能中包含有发布、分享和查看数据；个人中心包含基础信息和我的钱包。整个前端界面为两栏布局，一边是菜单目录部分，另一边是不同类型数据的展示部分。



图 5-6 数据共享平台可视化界面截屏

以权限管理功能为例，其原型界面如图 5-7 所示，为用户 A 的权限管理列表，可以查看授权或者除权情况，并且可以新建授权。



图 5-7 权限管理功能

点击新建按钮，可以增加一条授权信息即构建交易提案，之后经过区块链网络中 Peer 节点的交易背书、Orderer 节点的排序，然后经过所有 Peer 节点的验证，最后提交到账本中，即完成上链，其前端页面如图 5-8 所示。相应的，授权完成后，分享者可以发布、分享数据给被分享者，被分享者可以查询到相应

的数据集访问地址。

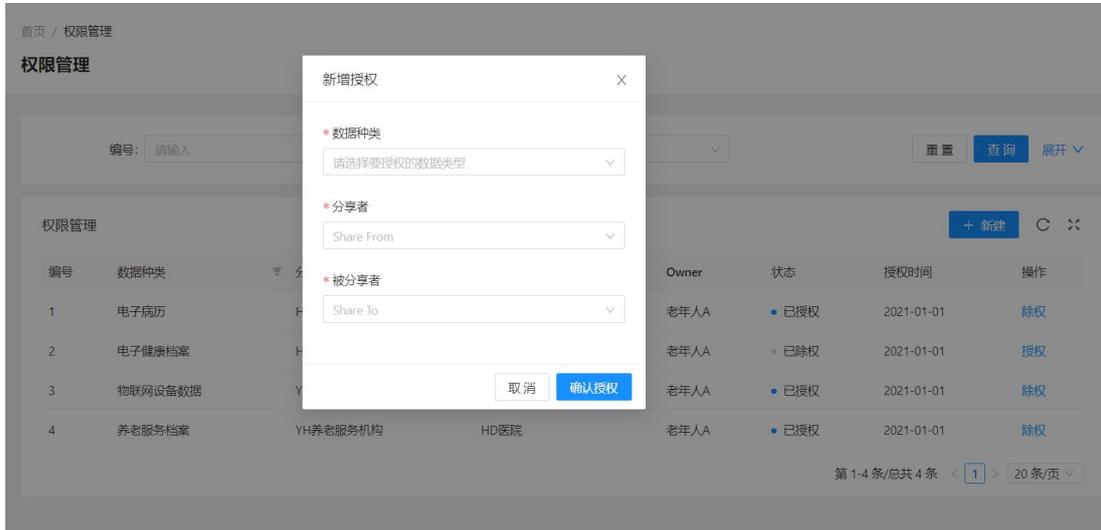


图 5-8 新建授权

5.4 模型分析

5.4.1 安全分析

本文提出的医养结合数据共享模型，以老年人中心，作为权限控制的实际节点。在数据保护上，一方面共享的医养数据经过加密之后才存储于传统的数据库中；另一方面，区块链上存的是加密后的访问地址。在整个共享过程中，任何参与者的访问操作均记录在区块中，实现了数据的防篡改、可溯源。同时利用智能合约实现的监管机制，可以最大程度促进各个参与主体的自律，限制非法行为。因此，本研究设计的医养结合数据共享模型具备了一定的安全性。

5.4.2 性能分析

区块链的性能可以通过交易吞吐量、延时、成功率和资源情况等方面来评价。本文使用 Caliper 工具对本文仿真实现的 Hyperledger Fabric 联盟链进行压力测试。本文采用测试脚本，分别向区块链网络中提交读或者写类型的交易。如图 5-9 所示，在读类型性能测试中，吞吐量最高可达 118.2tps，平均交易延时为 0.05s；在写类型性能测试中，吞吐量最高可达 56.8tps，平均交易延时为 0.49s，两种类型的交易成功率均达到 100%。需要说明的是，图片中展示的是某次性能测试的结果。

```
2021-03-31-03:10:01.033 INFO [Caliper] [ReportController]
```

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
open	1000	0	57.9	0.93	0.19	0.49	56.8
query	1000	0	118.6	0.15	0.01	0.05	118.2

图 5-9 性能测试结果

通过查看资源使用情况，如图 5-10 所示，可以看到，两个 peer 节点作为主节点，内存消耗量最大，分别为 181MB 和 209MB。

```
2021-03-31-00:24:20.273 INFO [Caliper] [ReportController]
```

Name	CPU%(max)	CPU%(avg)	Memory(max) [MB]	Memory(avg) [MB]	Traffic In [MB]	Traffic Out [MB]
peer0.org2.example.com	22.74	14.18	181	179	2.62	1.37
peer0.org1.example.com	22.59	13.86	209	208	2.63	1.39
ca.org2.example.com	0.00	0.00	15.1	15.1	0.00	0.00
orderer.example.com	6.40	3.69	34.4	33.2	1.72	3.46
ca.org1.example.com	0.00	0.00	7.50	7.50	0.00	0.00

图 5-10 资源使用情况

5.5 本章小结

为了探究本文提出的医养结合数据共享模型如何应用于实践中，本章设置了一个以老年人“A 先生”为中心的医养结合场景，以 Fabric 框架作为底层，设计了医养结合数据共享平台。在系统实现中，本文首先分析了医养结合数据共享系统的总体架构，具体包括底层存储层、区块链层及展示层，然后分别实现了智能合约以及前端可视化界面。最后结合仿真实现的医养结合数据共享平台来对本文中提出的医养结合数据共享模型进行安全和性能方面的分析。

第 6 章 总结与展望

在前面六个章节中，我们得出了医养结合模式中的数据和角色，基于区块链技术构建了医养结合数据共享模型，同时，也通过设置虚拟的医养结合场景，借助 Hyperledger Fabric 技术设计了医养结合数据共享平台。在本章中，我们将系统回顾本文所取得的研究成果，思考总结当前的局限性，并且探讨未来的研究展望。

6.1 研究总结

在我国养老事业发展过程中，“医养结合”变为了一种特殊且具有中国特色的服务模式。当前，我国已经陆续发布了多项政策来推进医养结合模式的深入发展。但在当前研究和实践中，医养结合数据的共享始终困难重重，医疗卫生和养老服务资源分散存储于各处，形成了数据孤岛；再加上医养结合数据的私密性、特殊性等特点，医养结合数据在共享的过程中存在泄漏风险，且数据泄露后果严重，出于对数据安全的担忧，导致各涉老主体的数据共享意愿不强；现有的医养结合平台多采用集中式存储，易出现“监守自盗”、单点故障等问题使用户数据泄露。因此，当前医养结合领域中的数据共享程度十分有限。

此外，目前基于区块链的数据共享研究中，鲜有学者在养老服务领域进行探索；并且在医疗健康等领域中提出的解决方案中大多仅限于某一种数据如电子病历，鲜少将研究对象的不同数据进行整合研究。

因此，在以上背景下本文展开了研究，取得了一定成果：

（1）理论成果

首先，本文通过文献回顾总结了医养结合模式的两种表现形式，分析了其中的角色和数据，并且基于区块链技术构建了医养结合数据共享模型，丰富了医养结合领域中对于数据共享的研究。

其次，本文基于激励相容理论和社会资本理论构建了一种可持续的医养结合数据共享激励机制，通过发布数字货币的形式来增强用户的社会资本，从而激励用户参与共享。因此，丰富了区块链中对于激励机制的研究。

（2）实践成果

- 1) 对于政府和医养结合领域的研究者来说，一方面，一个区域中的 ShareCoin 数量可用于“智慧医养发展指数”、“智慧助老指数”等指标体系中，对于评测工作具有一定的参考价值；另一方面，为医养结合相关政策的制定提供参考，如可制定使用 ShareCoin 来抵扣税款等，吸引和鼓励机构开展医养结合服务。
- 2) 对于医养结合相关的机构来说，一方面，本文设计的医养结合数据共享模型可应用于实际场景中，有利于挖掘养老行业的商业模式，机构之间通过共享医养数据来取得更大的经济利益；另一方面，可通过展示拥有的 ShareCoin 数量来表征自身的信用等级，对于提高机构的信誉具有正向促进作用。
- 3) 对于老年人来讲，可获得更多高质量、针对性的服务。
- 4) 对于整个养老行业来说，本文提出的医养结合数据共享模型可以为相关主体之间提供数据共享途径，一定程度上解决医养资源整合难题。

6.2 研究局限

尽管本文获得了一些理论及实践成果，但仍存在一定局限性：

(1) 医养结合模式已经在广大城市实践，受制于本人水平和工作量限制，仅通过文献回顾分析其中的角色和数据，可能还包含有其他特殊类型的涉老主体和数据。

(2) 目前，该模型的实现仍处于概念性验证阶段，本文仅实现了医养结合场景中的部分功能；且实际的医养结合场景中，各主体之间的联系更为复杂，比如在机构之间存在竞争性等，但在本文的实现中未能完全概括。

(3) 医养结合数据共享过程中的隐私性和安全性仍然是一个重点问题，本研究仅利用 Hyperledger Fabric 中的数据隐私策略，对于数据保护如线下加密存储的论述不足。

6.3 研究展望

基于本文的研究成果和研究不足，总结了几点未来可开展的工作：

- (1) 在医养结合数据共享的研究中，可以通过问卷调查等方法来分析医养结合

数据共享的难点，以及涉老角色和数据。

(2) 通过调研设置符合实际的医养结合场景，考虑各主体之间的合作性和竞争性关系，可使用 **Hyperledger Fabric** 的通道和隐私数据加密技术来实现。

(3) 本文考虑的是将所有的涉老主体都集中在一个联盟链中，但实际中可能存在有多个联盟链，因此可研究多条链间的数据共享。

(4) 未来可以验证本文中设计的关键机制包括激励和监管机制的有效性。

参考文献

- [1] Aledhari M, Razzak R, Parizi R M, et al. Federated learning: A survey on enabling technologies, protocols, and applications[J]. IEEE Access, 2020, 8: 140699-140725.
- [2] Ali B, Maheswaran M. A game theoretic analysis of blacklisting in online data storage systems[C]//GLOBECOM 2009-2009 IEEE Global Telecommunications Conference. IEEE, 2009: 1-7.
- [3] Bonawitz K, Eichner H, Grieskamp W, et al. Towards federated learning at scale: System design[J]. arXiv preprint arXiv:1902.01046, 2019.
- [4] Chang H H, Chuang S S. Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator[J]. Information & management, 2011, 48(1): 9-18.
- [5] Chang H H, Hung C J, Huang C Y, et al. Social capital and transaction cost on co-creating IT value towards inter-organizational EMR exchange[J]. International Journal of Medical Informatics, 2017, 97: 247-260.
- [6] Chasin F, Schmolke F, Becker J. Design Principles for Digital Community Currencies[C]//Proceedings of the 53rd Hawaii International Conference on System Sciences. 2020.
- [7] Chen H S, Jarrell J T, Carpenter K A, et al. Blockchain in healthcare: a patient-centered model[J]. Biomedical journal of scientific & technical research, 2019, 20(3): 15017.
- [8] Cheng X, Chen F, Xie D, et al. Design of a secure medical data sharing scheme based on blockchain[J]. Journal of Medical Systems, 2020, 44(2): 52.
- [9] Chu C K, Chow S S M, Tzeng W G, et al. Key-aggregate cryptosystem for scalable data sharing in cloud storage[J]. IEEE transactions on parallel and distributed systems, 2013, 25(2): 468-477.
- [10] Dorri A, Kanhere S S, Jurdak R. Blockchain in internet of things: challenges and

- solutions[J]. arXiv preprint arXiv:1608.05187, 2016.
- [11]Eltayieb N, Elhabob R, Hassan A, et al. A blockchain-based attribute-based signcryption scheme to secure data sharing in the cloud[J]. *Journal of Systems Architecture*, 2020, 102: 101653.
- [12]Fan K, Wang S, Ren Y, et al. Medblock: Efficient and secure medical data sharing via blockchain[J]. *Journal of medical systems*, 2018, 42(8): 136.
- [13]Gordon, W.J. , Catalini, C. , 2018. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput. Struct. Biotechnol. J.* 16, 224–230 .
- [14]Jiang X, Yu F R, Song T, et al. Blockchain-enabled cross-domain object detection for autonomous driving: A model sharing approach[J]. *IEEE Internet of Things Journal*, 2020, 7(5): 3681-3692.
- [15]Kaaniche, N. , Laurent, M. , 2017. A blockchain-based data usage auditing architecture with enhanced privacy and availability. In: *Proceedings of the 16 th International Symposium on Network Computing and Applications (NCA)*. IEEE, pp. 1–5 .
- [16]Kairouz P, McMahan H B, Avent B, et al. Advances and open problems in federated learning[J]. arXiv preprint arXiv:1912.04977, 2019.
- [17]Khatoun A. A Blockchain-Based Smart Contract System for Healthcare Management[J]. *Electronics*, 2020, 9(1): 94.
- [18]Li M, Yu S, Zheng Y, et al. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption[J]. *IEEE transactions on parallel and distributed systems*, 2012, 24(1): 131-143.
- [19]Lim W Y B, Luong N C, Hoang D T, et al. Federated learning in mobile edge networks: A comprehensive survey[J]. *IEEE Communications Surveys & Tutorials*, 2020.
- [20]Li J, Zhang Y, Chen X, et al. Secure attribute-based data sharing for resource-limited users in cloud computing[J]. *Computers & Security*, 2018, 72: 1-12.
- [21]Li T, Sahu A K, Talwalkar A, et al. Federated learning: Challenges, methods, and future directions[J]. *IEEE Signal Processing Magazine*, 2020, 37(3): 50-60.

- [22]Li N, Guo X, Chen G, et al. Reading behavior on intra-organizational blogging systems: A group-level analysis through the lens of social capital theory[J]. *Information & Management*, 2015, 52(7): 870-881.
- [23]Liang X, Zhao J, Shetty S, et al. Integrating blockchain for data sharing and collaboration in mobile healthcare applications[C]//2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). IEEE, 2017: 1-5.
- [24]Lu X, Pan Z, Xian H. An efficient and secure data sharing scheme for mobile devices in cloud computing[J]. *Journal of Cloud Computing*, 2020, 9(1): 1-13.
- [25]Lundervold A S, Lundervold A. An overview of deep learning in medical imaging focusing on MRI[J]. *Zeitschrift für Medizinische Physik*, 2019, 29(2): 102-127.
- [26]Makhdoom I, Zhou I, Abolhasan M, et al. PrivySharing: A blockchain-based framework for privacy-preserving and secure data sharing in smart cities[J]. *Computers & Security*, 2020, 88: 101653.
- [27]Mateo-Abad M, Fullaondo A, Merino M, et al. Impact Assessment of an Innovative Integrated Care Model for Older Complex Patients with Multimorbidity: The CareWell Project[J]. *International Journal of Integrated Care*, 2020, 20(2).
- [28]Merkle R C. Protocols for public key cryptosystems[C]//1980 IEEE Symposium on Security and Privacy. IEEE, 1980: 122-122.
- [29]Merkle R C. A digital signature based on a conventional encryption function[C]//Conference on the theory and application of cryptographic techniques. Springer, Berlin, Heidelberg, 1987: 369-378.
- [30]M. S. Ferdous, A. Margheri, F. Paci, M. Yang and V. Sassone, "Decentralised Runtime Monitoring for Access Control Systems in Cloud Federations," 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 2632-2633, doi: 10.1109/ICDCS.2017.178.
- [31]Myerson R B. Incentive compatibility and the bargaining problem[J]. *Econometrica: journal of the Econometric Society*, 1979: 61-73.
- [32]Niknam S, Dhillon H S, Reed J H. Federated learning for wireless

- communications: Motivation, opportunities, and challenges[J]. IEEE Communications Magazine, 2020, 58(6): 46-51.
- [33] Shafagh H, Burkhalter L, Hithnawi A, et al. Towards blockchain-based auditable storage and sharing of iot data[C]//Proceedings of the 2017 on Cloud Computing Security Workshop. 2017: 45-50.
- [34] Sultana T, Almogren A, Akbar M, et al. Data sharing system integrating access control mechanism using blockchain-based smart contracts for IoT devices[J]. Applied Sciences, 2020, 10(2): 488.
- [35] Shen J, Zhou T, Chen X, et al. Anonymous and traceable group data sharing in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2017, 13(4): 912-925.
- [36] Sheller M J, Edwards B, Reina G A, et al. Federated learning in medicine: facilitating multi-institutional collaborations without sharing patient data[J]. Scientific reports, 2020, 10(1): 1-12.
- [37] Shrestha A K, Vassileva J. User Data Sharing Frameworks: A Blockchain-Based Incentive Solution[C]//2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON). IEEE, 2019: 0360-0366.
- [38] Taha A, Zakaria A, Kim D, et al. Decentralized Runtime Monitoring Approach Relying on the Ethereum Blockchain Infrastructure[C]//2020 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2020: 134-143.
- [39] Uphoff N, Wijayarathna C M. Demonstrated benefits from social capital: the productivity of farmer organizations in Gal Oya, Sri Lanka[J]. World development, 2000, 28(11): 1875-1890.
- [40] Wang H, Guo C, Cheng S. Loc—a new financial loan management system based on smart contracts[J]. Future Generation Computer Systems, 2019, 100: 648-655.
- [41] Xia Q I, Sifah E B, Asamoah K O, et al. MeDShare: Trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5: 14757-14767.
- [42] Xuan S, Zheng L, Chung I, et al. An incentive mechanism for data sharing based on blockchain with smart contracts[J]. Computers & Electrical Engineering, 2020, 83:

106587.

[43]Yang Q, Liu Y, Chen T, et al. Federated machine learning: Concept and applications[J]. ACM Transactions on Intelligent Systems and Technology (TIST), 2019, 10(2): 1-19.

[44]Zhang P, White J, Schmidt D C, et al. FHIRChain: applying blockchain to securely and scalably share clinical data[J]. Computational and structural biotechnology journal, 2018, 16: 267-278.

[45]Zhang X, Gao L, Cao B, et al. A double auction mechanism for mobile crowd sensing with data reuse[C]//GLOBECOM 2017-2017 IEEE Global Communications Conference. IEEE, 2017: 1-6.

[46]Zhu L, Dong H, Shen M, et al. An incentive mechanism using shapley value for blockchain-based medical data sharing[C]//2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS). IEEE, 2019: 113-118.

[47]郭东,李惠优,李绪贤,官计彬.医养结合服务老年人的可行性探讨[J].国际医药卫生导报,2005(21):45-46.

[48]郭上铜,王瑞锦,张凤荔.区块链技术原理与应用综述[J].计算机科学,2021,48(02):271-281.

[49]郭鑫鑫,左美云.基于区块链的医养结合平台数据共享设计研究[C]//中国老年学和老年医学学会.新时代积极应对人口老龄化研究文集.2020.北京:华龄出版社,2020:10-17

[50]何雯,白翰茹,李超.基于联邦学习的企业数据共享探讨[J].信息与电脑(理论版),2020,32(08):173-176.

[51]郝世博,邓雨亭.融合数据监管与数据溯源的科学数据共享管理研究[J].情报理论与实践,2018,41(03):23-28.

[52]何云华,黄伟,王伟忠,等.基于区块链的分布式激励架构研究.工程科学与技术, 2021, 53(1): 178-187. DOI:10.15961/j.jsuese.202000780

[53]黄娜娜,沈亮,杨元原.医疗云中高效安全的数据共享方案研究[J].计算机工程与应用,2020,56(01):92-97.

- [54]侯玉梅,傅勘,高秋焯,崔研,徐日,梁萧.医养结合型智慧居家养老服务平台设计[J].包装工程,2020,41(06):94-103.
- [55]刘海琴,罗靖,杨敏娟,等.健康大数据背景下患者隐私暴露的伦理思考[J].中国医学伦理学,2019(10):1284-1286.
- [56]孟小峰,刘立新.区块链与数据治理[J].中国科学基金,2020,34(01):12-17.
- [57]穆光宗.“医养”该如何“结合”[J].中国卫生,2018(7):20-21.
- [58]欧阳婷,杨银凤,束建华,张蕾,王丹.健康大数据背景下患者隐私保护意识调查及伦理思考[J].巢湖学院学报,2020,22(06):91-97+136.
- [59]彭荣.基于MAS的医养结合养老服务系统模型构建研究[J].卫生经济研究,2017(03):50-53.
- [60]王辉,周明明.基于区块链的医疗信息安全存储模型[J].计算机科学,2019,46(12):174-179.
- [61]王强芬.大数据时代背景下医疗隐私保护的伦理困境及实现途径[J].中国医学伦理学,2016(4):685-689.
- [62]王秀丽,江晓舟,李洋.应用区块链的数据访问控制与共享模型[J].软件学报,2019,30(06):1661-1669.
- [63]苏雄业.基于区块链的大数据共享模型与关键机制研究与实现[J].北京:北京工业大学,2018.
- [64]杨莉.医养结合的运营模式探究——以武汉市“互联网+居家养老”为例[J].学习与实践,2019(11):101-108.
- [65]袁勤俭,朱哲慧,张一涵.信息系统实证研究的20种重要理论与应用[R].北京:机械工业出版社,2020:56-76
- [66]杨帆.金融监管中的数据共享机制研究[J].金融监管研究,2019(10):53-68.
- [67]杨一帆,张劲松等.积极应对人口老龄化研究报告.2020:聚焦医养结合(中国老年学和老年医学学会主编)[R].北京:社会科学文献出版社,2020:3-4.
- [68]张增骏,董宁,朱轩彤,等.深度探索区块链:Hyperledger技术与应用[J].2018.
- [69]张丽,严晓萍.智慧养老服务供给与实现路径[J].河北大学学报(哲学社会科学版),2019,44(04):96-102.
- [70]左美云,王芳,尚进.“医养结合”面临的问题及对策[J].中国信息

界,2016(02):81-84.

[71]左美云.智慧养老的内涵,模式与机遇[J].中国公共安全,2014,(10):48-50

致谢

时光匆匆，我的研究生阶段的学习就要结束了。

我首先要感谢中国人民大学，为我们提供了良好的学习环境，也让我结识了很多良师益友。

然后，我要感谢我的导师左美云教授。无论是学术研究，还是生活实践上，左老师都给予了热切地指导。在学术研究上，每周一次的例会上左老师点评每一位学生的汇报，鼓励我们大胆交流，教导我们不仅要“会写”，更要“会说、会讲一个好故事”，每周例会上思想的碰撞都让我受益匪浅；在生活实践中，左老师教导我们“功不唐捐”，让我们学会做好时间、精力的管理。同时，本文从选题到定稿离不开左老师的指导，给予了我许多意见和建议。在此郑重感谢我的导师。

我还要感谢其他老师。感谢王杰老师。王杰老师非常认真，会从企业角度给出指导。同时还要感谢团队里的其他老师如余艳老师、许洁萍老师、杜玮老师、周季蕾老师等，还要感谢学院里的其他老师，感谢你们孜孜不倦传道授业解惑以及做各项保障性工作。

此外，我还要感谢实验室的小伙伴们，包括王涛师兄、熊捷师姐、商丽丽师姐、马丹师姐、王配配师姐、藏润强师兄和其他小伙伴们，感谢你们给我各种学术建议，让我的论文不断完善。

我还要感谢我的朋友们，包括邵红琳、银旭、裴佳楠、王雨婷、邓雅茹等，我们一起玩耍、一起进步，感谢你们给予我很多精神上的支持。

我还要感谢我的家人，总是无条件支持我，给我最温暖的家。

最后，在这特殊的新冠肺炎疫情期间，我还要感谢所有抗击疫情的一线人员，感谢所有中国人民的积极努力，才让疫情很快被遏制。我将谨记人民大学“实事求是”的校训，怀着满满的期待，争做国民表率、社会栋梁！