

# 区块链在糖尿病医疗数据管理和访问控制中的应用探索

李明

何娟

(武汉大学人民医院信息中心 武汉 430065) (武汉大学人民医院计财处 武汉 430065)

〔摘要〕 介绍基于糖尿病的慢病管理系统研究现状、区块链内涵、智能区块链平台发展情况,提出构建基于区块链的平台以管理和共享医疗数据,阐述平台构建方法、应用探索,分析平台优势及局限性。

〔关键词〕 区块链;糖尿病;医疗保健;访问管理

〔中图分类号〕 R-058 [文献标识码] A [DOI] 10.3969/j.issn.1673-6036.2022.09.011

**Application and Exploration of Blockchain in Diabetes Medical Data Management and Access Control** LI Ming, Department of Information Center, Renmin Hospital of Wuhan University, Wuhan 430065, China; HE Juan, Department of Accounting and Finance, Renmin Hospital of Wuhan University, Wuhan 430065, China

〔Abstract〕 The paper introduces the research status of chronic disease management system based on diabetes, the connotation of blockchain, and the development of intelligent blockchain platform, proposes the construction of blockchain-based platform to manage and share medical data, expounds the platform construction method, application and exploration, and analyzes the advantages and limitations of the platform.

〔Keywords〕 blockchain; diabetes; health care; access management

## 1 引言

糖尿病是一种慢性疾病,治疗过程漫长而复杂。糖尿病患者在治疗过程中会产生大量与疾病相关的数据及健康状况数据,例如健康记录、体育活动、自测血糖、自测尿液中葡萄糖、连续葡萄糖监测、血压等数据<sup>[1-3]</sup>。目前尚未实现在不同医疗保健机构的数据平台共享这些患者健康数据,而解决这一问题将会改善临床疗效和提高临床研究效率<sup>[4-6]</sup>。医疗保健机构出于隐私保护及竞争等原因

一般不愿意共享数据,且共享数据存在较大技术障碍<sup>[7]</sup>。此外患者并未实际掌控自身数据,无法决定哪些实体有权访问其个人数据<sup>[8]</sup>,如果患者能够拥有控制数据的主动权,将有可能更多地参与治疗。随着科技进步,居家监测已成为现实,许多患者已能够测量自身健康指标数据,如生命体征(血压、血糖值等)、用药情况、锻炼情况、睡眠质量、身体机能状况和生活质量。然而由于在数据共享及保护方面存在技术困难,这些数据无法获得医疗保健机构认可<sup>[9]</sup>。

## 2 研究现状及相关概念

### 2.1 国内外研究现状

2.1.1 国外 近年来随着远程医疗及慢病管理系

〔修回日期〕 2021-10-09

〔作者简介〕 李明,工程师,发表论文2篇;通信作者:何娟,会计师。

统的日趋成熟, 针对糖尿病的慢病管理系统在国内 外逐步得到应用。这类系统通过指导患者测量糖尿病 相关数据、上传数据实现系统评估、风险预警及 在线问诊等功能, 帮助患者实现自我管理。数据管理 问题日益凸显, 随着区块链技术的发展及广泛应用, 利用区块链技术解决糖尿病等慢性疾病数据管理 问题逐渐成为可能。Azbeq K、Ouchetto O 和 Andalousi S J 等<sup>[10]</sup> 提出一个基于物联网和区块链的平台架构, 结合物联网和区块链技术以便收集患者数据, 从而实现对糖尿病患者状态的实时监测并帮助 其实现自我管理, 同时也保证了患者隐私。有学者<sup>[11]</sup> 运用区块链技术和远程医疗技术解决了疫情期间 糖尿病患者的家庭护理难题, 从而保证糖尿病患者 护理的连续性。Shynu P G、Menon V G 和 Kumar R L 等<sup>[12]</sup> 利用雾节点搜集患者体征采集设备信息并 存储在区块链上, 并将基于规则的聚类算法应用到 患者健康记录中, 最后使用基于特征选择的自适应 神经模糊推理系统预测糖尿病和心脏病等慢性 疾病。

2.1.2 国内 在区块链上升到国家战略的背景 下, 区块链技术逐步融入到各行业中。2016 年湖南 省科技厅设立和启动重大专项“心脑血管疾病防治 协同创新工程”, 2018 年该工程发布重要成果, 我国 首个具有自主知识产权的“区域慢病智能管理与 药品配送平台”正式上线, 糖尿病等慢病患者复 诊无需到医院挂号、排队, 在家不仅可以通过手机 向大医院医师进行线上复诊, 处方药物还能直接配 送到家中。该平台的建设首次引入区块链技术, 使 处方流转及药物配送可追溯, 确保相关医疗数据和 运营安全。2020 年 11 月浙江大学推出基于区块链 等技术的慢病管理 APP“浙里管”。该应用是面向 浙江全省的创新慢病管理产品, 通过打造医保医疗 一体化的慢病管理平台, 实现慢病“医防融合”创 新式管理。

## 2.2 区块链内涵

2.2.1 定义 区块链是由块组成的分布式分类 账本, 每个块表示链接到前一个块的数据(按时间 顺序加密哈希数据层)。区块链通常由对等网络协作

管理, 该网络遵守用于对区块链中的新块进行身份 验证<sup>[13]</sup>的某种协议。

2.2.2 特点 区块链具有几个显著特点, 例如区 块链中块是不可变的, 因为每个块包含前一个块内 容的散列值, 这意味着整个区块链有效地链接在一 起, 更改历史链中的一个块也会更改链中所有其他 块的内容<sup>[14]</sup>。网络中节点之间的区块链一致性机制 确保数据的不可变性。新兴的区块链平台也使用了一 些不同机制, 如权益证明或重要性证明, 这些机制 已被证明更有效<sup>[15]</sup>。区块链的特性使数据具有较 高的有效性和安全性。

## 2.3 智能区块链平台

新一代智能区块链平台, 如 Ethereum、NEO 和 NEM<sup>[16]</sup>等为开发基于区块链的医疗数据管理平台 提供了一些实用功能。智能区块链平台有资产管理 功能, 这意味着其可以在网络中创建新的令牌(资 产), 这些资产可以分配给不同的场景和目的。智 能区块链平台的另一个特征是支持多账户交互的多 签名契约, 即在区块链上授权事务时需要多个密 钥, 一个多签名契约可以用来控制实体有权访问帐 户并对帐户进行更改。通过简单的 Web 调用可以与 NEM 区块链进行交互, 简化了客户端应用程序的创 建过程。同时可以使用任何编程语言访问和修改区 块链, 使不同系统能够向区块链添加和读取患者数 据。Ethereum 等其他区块链平台则较为复杂, 交互 规则需要使用专门的编程语言编写并上传到区块链 平台。

## 3 数据管理的实现

本文提出的方法涉及智能区块链平台使用, 利 用 NEM 公共或私有区块链对存储在链上和链外的 以患者为中心的健康数据进行管理。该方法包括使 用多重签名契约获得控制数据管理和数据加密权 限, 从而达到保密和管控医疗保健数据的目的<sup>[17]</sup>。 患者具有完全访问个人数据的权限, 并控制与哪些 实体共享这些数据。患者可以设置访问权限, 并指 定谁可以读取和写入医疗保健数据到该帐户。这种

访问控制管理可以用于链下应用程序，应用程序将允许患者查看哪些实体有权访问个人数据，并允许患者分配新的许可证及撤销访问权限，权限可以根据时间范围和数据类型灵活设置。链下管理应用程序将确保契约按时间执行，并为区块链提供直观的接口。这将提高管理透明度，并允许患者就收集的医疗保健数据以及相关实体之间如何共享数据等问题做出决策<sup>[18]</sup>。

## 4 实施

### 4.1 架构

4.1.1 体系构建 该体系结构是围绕加密、马赛克（区块链上的一个令牌）和平台上可用的多签名契约构建的。多签名契约允许多个实体管理帐户活动、控制来自一个帐户的资产（如马赛克）或创建其他契约<sup>[19]</sup>，NEM 的多重签名特性使得一个可编辑的契约可以将某个特定帐户的权利和权力分配给其他帐户。创建多重签名的契约以便任意数量的签名签署到同一个事务上，这称为  $m/n$  多重签名，其中  $m$  可以是  $\leq n$  的任意数字。在医疗区块链的体系结构中，应用  $2/n$  多重签名契约。患者将控制合同中的两个密钥，与患者账户相关的合同中包含的每个医疗保健机构将持有 1 个密钥。这意味着通过拥有编辑契约所需的密钥数量患者将保持对账户的控制。医疗保健机构能够查看账户信息（如一般消息、治疗措施等）并发起交易，患者仍然需要联合签署由其他机构发起的事务，但是可以将其设置为自动完成，或者在离线应用程序层的规则中完成，见图 1。

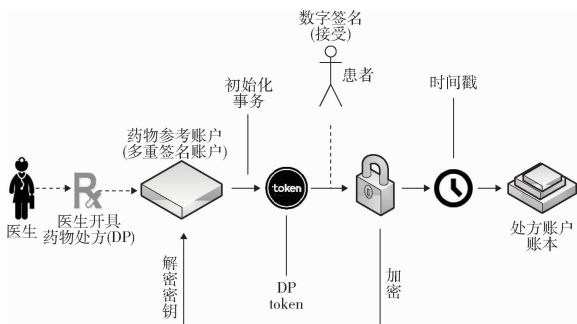


图 1 医疗实体给患者开处方过程

4.1.2 数据存储 新数据将以以下方式存储在区块链上：患者或医疗保健实体（至少有 1 个密钥与患者的多签名账户关联）将启动事务，发送包含数据的马赛克作为消息。同时消息将被加密，解密密钥将在单独的事务中发送到多签名账户，当手动或自动对数据马赛克事务进行联合签名时，事务被发送到与该特定数据类型相关的账户。这确保了只有能够访问多重签名账户的实体才能使用解密密钥读取患者数据。在实践中患者将控制多个多重签名账户，即给每个账户分配特定类型的数据，这种体系结构将允许在医疗实体之间对不同类型的数据进行分区访问。

### 4.2 可信方

区块链要在现实世界中实现还应考虑当患者无法获得必要的访问许可时如何实现自我管理，例如患者急危重症病发、无自主意识或丢失个人密钥等情况。本文给出的解决方案是可信方在紧急情况下持有额外密钥对。可信方可以是患者近亲，也可以是与医疗保健机构无关的特殊政府机构。在紧急情况下医务人员可以执行该方案，允许其使用可信方访问医疗数据，监管和立法将确保程序的合法、有效实施并防止滥用，见图 2。

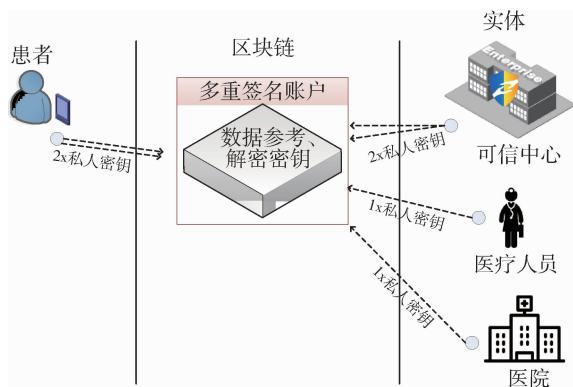


图 2 可信方紧急情况授权访问

### 4.3 数据湖

原始心电图和医学影像文件等大数据文件不适合直接存储在区块链上。此类患者数据在医疗机构较常见，可在区块链中建立一个具有引用地

址的存储库进行数据及其解决方案的存储。所有大型医疗数据集合都可以存储在数据湖中，即区块链之外的仓库。数据湖是一种高度可扩展、可存储各类数据（如图像和时间序列数据）的存储方法。数据湖将对所有医疗保健服务提供者开放，并且仅用于存储加密数据。在数据湖的设定中，患者可以控制谁有权访问个人数据，如果没有存储在患者区块链账户上的解密密钥数据将无法读取，见图3。

## 5 应用探索

### 5.1 应用

基于区块链的糖尿病等慢性疾病医疗数据管理和访问控制应用探索主要有以下几个方面：一是医疗机构患者医疗数据的上传与访问；二是患者就诊的医疗机构访问其他医疗机构医疗数据及患者自测数据；三是其他用户访问患者就诊医疗机构医疗数据及患者自测数据，见图4。患者在各医疗机构就诊过程中会产生大量医疗数据，医疗机构将数据加密并经过签名后存储到数据湖中，同时医疗机构会将数据索引地址及签名信息传入区块链平台中，这种数据存储方式可以减轻区块链平台反复高频进行数据存储和访问的压力。患者如果需要查询个人医疗数据只需提供私人密钥即可获得数据访问地址。当患者前往医疗机构就诊时，医疗机构或医生可提交私人密钥配合患者提供的密钥发送至区块链平台后获得数据访问权限及存储地址，以访问数据湖中存储的患者在其他医疗机构就诊的医疗数据。当药房药师或健康管理师等其他用户需要获得患者数据时，只需提供数据用户和患者密钥即可获得数据访问权限及存储地址，从而访问数据湖中的患者医疗数据。

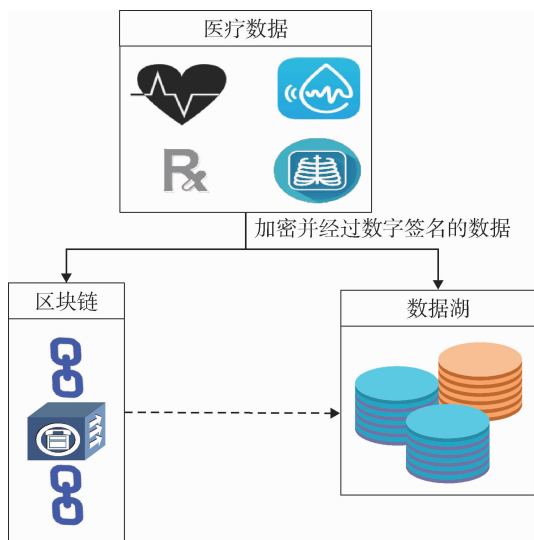


图3 数据湖概念

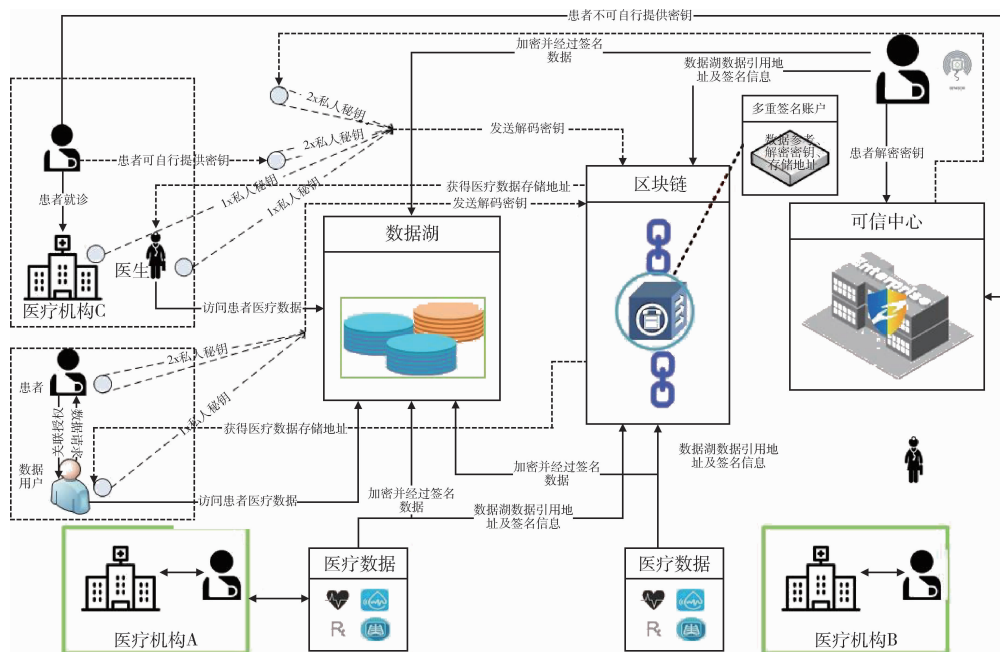


图4 数据管理及访问控制方案

## 5.2 优势及局限性

5.2.1 优势 区块链的使用可能会促进医疗保健机构做出改进,从患者角度来看其具有两项优势:一是患者可拥有个人数据的控制权;二是实现更直观的健康数据共享,符合患者利益,随着区块链应用的推进也将有可能轻松地共享来自家庭医疗设备的数据。

5.2.2 局限性 医疗保健机构在区块链技术应用领域仍面临挑战。例如在对患者进行急性治疗期间需要快速获取个人数据,可以通过可信的第 3 方来解决,而具体如何实现还存在较多问题。又如哪些数据应该存储在区块链中尚待探讨,从技术角度来看在区块链上存储大量时间序列数据是不切实际的,本文提出只使用区块链进行访问管理,并将数据存储和数据湖中来解决这一问题。上述做法虽然符合《信息安全技术公共及商用服务信息系统个人信息保护指南》,但是如果医疗保健数据直接存储在区块链上不可变,这可能会对执行个人信息保护国家标准规则造成困扰。

## 6 结语

使用区块链技术将使糖尿病患者、医疗保健机构和研究人员能够从持续更新的泛数据池中访问患者数据。在研究方面,使发现患者特定特征和诊断之间的联系成为可能,也将促进公众更好地理解和治疗疾病。区块链数据和访问管理结合数据湖的使用可以支持广泛的医疗保健数据,包括不同医疗机构生成的数据,如血样、生命体征、医学图像、诊断等。此外还将纳入患者生成的数据,如可穿戴传感器和患者上报的测量结果数据,这些数据可以使治疗者加深对患者的了解并且提升治疗效果。将区块链用于医疗数据和访问管理具有潜在的综合优势,但相关研究数量较少,未来应在现有的小规模糖尿病医疗保健系统中实施这项技术,进行进一步研究。

## 参考文献

- 1 王娅,孙娟,邓楠,等.久坐行为干预在 2 型糖尿病患者及其高危人群中的研究进展 [J]. 中国全科医学, 2018, 21 (34): 4283 - 4288.
- 2 唐晓梅,徐大才.餐后不同时间点运动对 2 型糖尿病患者血糖的影响 [J]. 护理学杂志, 2019, 34 (15): 32 - 34.

- 3 Cichosz S L, Johansen M D, Hejlesen O. Toward Big Data Analytics: Review of Predictive Models in Management of Diabetes and Its Complications [J]. Diabetes Science Technology, 2016, 10 (1): 27 - 34.
- 4 徐健,陈志德,龚平,等.基于区块链网络的医疗记录安全储存访问方案 [J]. 计算机应用, 2019, 39 (5): 1500 - 1506.
- 5 Ge Y, Ahn D K, Unde B, et al. Patient - controlled Sharing of Medical Imaging Data Across Unaffiliated Healthcare Organizations [J]. Journal of the American Medical Association, 2013 (20): 157 - 163.
- 6 Walker J, Pan E, Johnston D, et al. The Value of Health Care Information Exchange and Interoperability [J]. Health Affairs, 2005 (1): 1 - 3.
- 7 杨朝晖,王心,徐香兰.医疗健康大数据分类及问题探讨 [J]. 卫生经济研究, 2019, 36 (3): 29 - 31.
- 8 冯云霞,魏昂,韩正亮,等.基于区块链技术的全民健康信息平台的研究 [J]. 中国数字医学, 2019, 14 (6): 24 - 26.
- 9 Goldwater J C. The Use of a Blockchain to Foster the Development of Patient - reported Outcome Measures [C]. Gaithersburg: ONC/NIST Use of Blockchain for Healthcare and Research Workshop, 2016.
- 10 Azbeg K, Ouchetto O, Andaloussi S J, et al. Blockchain and IoT for Security and Privacy: A Platform for Diabetes Self - management [C]. Brussels: 2018 4th International Conference on Cloud Computing Technologies and Applications (Cloudtech), 2018.
- 11 Alsalamah H A, Alsuwailem G, Rajeh F B, et al. eHome-Caregiving: A Diabetes Patient - Centered Blockchain Ecosystem for COVID - 19 Caregiving [J]. Frontiers in Blockchain, 2021 (4): 477012.
- 12 Shynu P G, Menon V G, Kumar R L, et al. Blockchain - based Secure Healthcare Application for Diabetic - Cardio Disease Prediction in Fog Computing [J]. IEEE Access, 2021 (99): 1.
- 13 Nakamoto S. Bitcoin: A Peer - to - Peer Electronic Cash System [EB/OL]. [2021 - 08 - 10]. <http://bitcoin.org/bitcoin.pdf>.
- 14 Swan M. Blockchain: Blueprint for a New Economy [M]. Sebastopol: O' Reilly Media, 2015.
- 15 NEM Foundation. NEM Technical Report [EB/OL]. [2021 - 08 - 10]. [https://nem.io/wp-content/themes/nem/files/NEM\\_techRef.pdf](https://nem.io/wp-content/themes/nem/files/NEM_techRef.pdf).
- 16 Wood G. Ethereum: A Secure Decentralised Generalised Transaction Ledger [EB/OL]. [2021 - 08 - 10]. <http://gavwood.com/Paper.pdf>.
- 17 王震,周颖,黄赅东,等.面向大数据应用的区块链解决方案综述 [J]. 计算机科学, 2019, 46 (z1): 6 - 10.
- 18 Peterson K, Deeduvanu R, Kanjamala P, et al. A Blockchain - based Approach to Health Information Exchange Networks [J]. NIST Workshop Blockchain Healthcare, 2016 (11): 1 - 10.
- 19 高东平,王士泉,李伟,等.基于区块链技术的医疗大数据平台架构研究 [J]. 中国数字医学, 2019, 14 (1): 29 - 32.