Computer Science and Application 计算机科学与应用, 2022, 12(7), 1855-1861
Published Online July 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.127185

Hans汉斯

基于区块链的电子病历系统模型的研究

卢本本[1]，莫晶亮[2]，邱　钊[1*]，杨子睿[1]，杨　磊[1]，廉应生[1]

[1]海南大学计算机科学与技术学院，海南　海口
[2]海口市妇幼保健院，海南　海口

收稿日期：2022年6月22日；录用日期：2022年7月20日；发布日期：2022年7月27日

摘　要

本文针对区块链技术的特点研究安全高效的电子病历系统模型以及相关的智能合约。为了保护患者的隐私安全，首先对这些患者的诊疗数据进行脱敏处理，同时针对不同类型的医疗数据采取不同的处理方式，支持多种类型的数据安全存储。为适应P2P网络，引入PBFT共识算法，最后引入MetaMask钱包插件，使用IPFS星际文件系统应用于系统设计之中。本文在模型中将各个医疗机构视为联盟成员，不同医疗机构之间可以相互联系，都需遵循智能合约，通过授权后可共享患者的诊疗数据信息。本文创新性地将患者敏感数据进行脱敏后部署到区块链上，然后针对性设计智能合约，保证患者隐私数据在各机构之间安全存储与共享。

关键词

电子病历，区块链，智能合约，数据脱敏

Research on Electronic Medical Record System Model Based on Blockchain

Benben Lu[1], Jingliang Mo[2], Zhao Qiu[1*], Zirui Yang[1], Lei Yang[1], Yingsheng Lian[1]

[1]School of Computer Science and Technology, Hainan University, Haikou Hainan
[2]Haikou Maternal and Child Health Hospital, Haikou Hainan

Received: Jun. 22nd, 2022; accepted: Jul. 20th, 2022; published: Jul. 27th, 2022

Abstract

According to the characteristics of blockchain technology, this paper studies a safe and efficient electronic medical record system model and related smart contracts. In order to protect the pri-

*通讯作者。

文章引用: 卢本本, 莫晶亮, 邱钊, 杨子睿, 杨磊, 廉应生. 基于区块链的电子病历系统模型的研究[J]. 计算机科学与应用, 2022, 12(7): 1855-1861. DOI: 10.12677/csa.2022.127185

vacy and safety of patients, first desensitize the diagnosis and treatment data of these patients, and adopt different processing methods for different types of medical data to support the safe storage of various types of data. In order to adapt to P2P network, PBFT Consensus algorithm is introduced. Finally, MetaMask wallet plug-in is introduced, and IPFS interstellar file system is used in system design. In this model, each medical institution is regarded as a member of the alliance. Different medical institutions can contact each other, and they all need to follow the smart contract. After authorization, they can share the diagnosis and treatment data information of patients. This paper innovatively desensitizes patient sensitive data and deploys it on the blockchain, and then designs smart contracts to ensure the safe sharing of patient privacy data among institutions.

Keywords

Electronic Medical Record, Blockchain, Smart Contract, Data Desensitization

1. 引言

随着社会的不断发展，电子病历对于医疗的重要性也越来越被重视。电子病历中包含了非常多医疗信息数据[1]，对于当前的医疗服务行业的作用也是不言而喻的。但是当前的电子病历还是有着非常多的问题，因为电子病历中包含着大量的患者的隐私信息[2]，所以对于这些医疗数据的存储以及在各个医疗机构之间的共享是一个非常重要的问题。所以如何设计一个可以数据存储效率高、数据共享更加安全便捷的电子病历系统是关键也是难点。区块链存储数据的方式与传统方法不同的是，主要是通过分布式数据库来完成存储过程。为了实现共享数据的一致性，会采用自信任共识机制用以实现。同时未来保证数据的安全性，最好的方式是将对称和非对称加密技术加以结合。引入智能合约用以规范化处理数据，目的是完成不同个之间的价值交换，而且不需要其他机构或者个体的加入，这在解决信任问题方面有着很大的意义。区块链网络中存储的数据由全网所有节点共同产生，也由所有节点共同维护，节点间相互独立，可以实现在无信任或者低信任的团体组织间的价值传递。所以为了解决患者敏感数据问题，我们可以采用区块链技术在各个需共享的医疗机构之间建立联盟区块链，对于各个授权进来的节点采用一样的结构来进行存储和访问数据。

本文主要是针对区块链技术在电子病历领域的应用，在医疗机构间建立联盟区块链，并构建提供可进行电子病历共享的数据共享平台[3]，采用智能合约来表示区块链上患者、医院、病历信息指针和患者－医院之间的就诊关系、信息如何存储和查询。同时为了保护患者的隐私信息，对患者的医疗数据信息进行脱敏处理，为了存储多种类型的电子病历，引入了与区块链原理相同的 IPFS 文件系统，并将返回的文件 Hash 值上传到区块链存储，设计理念就是既可以更好地保护患者的隐私又可以进行高效便捷的信息共享。结合医疗健康信息集成规范对医院间电子病历互访机制建模，区块链储存着患者关键医疗数据和交易记录。医院机构作为联盟的成员可以相互联系，自动执行智能合约，在经过授权后可以共享所需的全部患者医疗数据信息。区块链的作用就是为数据记录和身份管理提供一个标准，椭圆曲线加密算法进行数字签名，在进行数据共享的同时又能最大程度上保护隐私数据不受危害。这个模型的设计可便于患者跨域诊疗，让医疗服务系统更加高效便捷，对于当前医疗大环境下的数据资源共享，整合挖掘医疗数据有现实意义[4]。

2. 电子病历系统模型的分析

2.1. 数据存储要求

电子病历数据存储系统应符合我国数据库管理系统安全技术要求规范并通过信息安全等级保护测评[5]：一是对于存储容量要求要足够大，可以满足需求；二是对于患者信息的保留要具备很好的完整性；三是要求系统的数据存储要快速便捷，具有更高的效率。需优化查询语句，避免过多的表关联，先过滤有索引的，尽量缩小数据范围[6]。在数据库中创建表时，将表中字段的宽度设的尽可能小，执行的查询速度就越快。建立数据表索引，它在检索行中的速度比没有索引快得多。此外，还需要记录注册信息：就诊类型、医生 ID、就诊时间、病史、病程记录等信息，其中包括患者的部分隐私(如身份证、健康信息等)的安全加密建设应视为重点。

2.2. 数据处理

患者的医疗数隐私保护据保护是一个不可避免的问题。但是，并不不是每一条患者的电子病历数据都会侵犯到患者的隐私，比如说性别、姓氏、医生治疗方法等数据并不会危害到患者隐私。对于此类数据我们成为非隐私数据，尽管对与患者来说，这些数据依然会涉及到他们的隐私，但是其他人并不能利用这些信息进行整合而确定到个人，所以这些数据也可以称为非隐私数据。对于非隐私数据我们是不会太过担心数据泄露的，只需要对此类数据进行标准化处理就可以满足我们的使用需求。

与非隐私数据不同的是，一些患者的隐私数据是不容许泄露出去的，这容易被非法分子加以利用，所以我们有必要将这些隐私数据进行脱敏处理然后再进行存储上传。针对文本类隐私数据，可以使用传统的数据脱敏技术来处理此类信息。一方面可以患者的隐私数据不能被别人准确的识别出来，另一方面还可以使得这些隐私数据仍然具有可用性。在一般情况下，我们有很多种方法来实现数据脱敏，比如说：加密、遮挡、泛化、替代、截断、数值变化、空值插入、删除等等。因为我们在不同的条件下会用到不同的数据类型，所以必须综合使用上述的脱敏技术来针对不同需求的隐私数据才能够满足我们的现实需求。

对于病历信息中的图片数据，因为当前区块链并不支持超文本传输，所以无法之间将患者的医疗图片数据直接存储到区块链上，我们只能寻找一些替代方案来完成图片数据的存储使用。面对这个问题，研究人员已经开发了 IPFS 星际文件系统、MaidSafe 等解决这个问题。所以我们可以先将患者图片数据存储至 IPFS 星际文件系统中，并且设置节点权限来构建联盟链，设计分布式流媒体节点，通过一致性哈希重新设计了数据并行和模型分片方案，使系统能够适应数据流环境和集群计算能力的动态变化，如此便可简便地搭建一个受监管的寻址储存网络[7]。将患者图片数据发送到 IPFS 星际文件后会返还对应该文件的唯一 Hash 值，这个 Hash 值可进行十六进制转码，然后我们再将其发送至区块链上，因为患者的图片数据可能会侵犯到患者的隐私，我们将已经发布到链的上 Hash 值再加密处理，这会使得数据的匿名性有很大的提高。

2.3. PBFT 的共识算法

拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)是在异步网络环境下使用状态机的副本复制算法[8]，通常在一些分布式系统中有着广泛的运用，它的特点包含吞吐量大、延时低、容错性强等。其共识过程为：在整个网络中选择主节点，经过共识过程后像其他节点发布消息，其他节点接收消息后需进行验证，如果验证协议消息通过则完成共识。本文引入 PBFT 算法对电子病历系统进行设计，用以保证系统的交易确认速度，同时其吞吐量大的特性也可以满足系统的大规模数据交易，同时面对患者医疗数据丢失、损坏等问题时候也可以很好的解决。引入 PBFT 共识算法还有个优点就是可以确保所有患者病

历数据的一致性，因为它可以使用系统中存在的好的节点替换某些恶意节点所发的信息，具有非常强的容错力。

3. 电子病历系统模型设计

3.1. 区块链模型构建

区块链的构建模型主要分为应用层、合约层、共识层、网络层和数据层，通过各个结构的相辅相成，可以实现动态管理电子病历。其中应用层的主要作用是为了方便数据共享与查询所设计的模块。合约层是封装各类脚本代码、算法以及更为复杂的智能合约，是区块链系统实现灵活编程和操作数据的基础[9]。共识层包括 POW、DPOS 和 PBFT 等一些共识算法，目的是让各个节点在高度去中心化的区块链网络中高效的针对区块链数据有效达成共识。网络层其最重要的功能是让区块链中的各个节点能够顺利的进行信息共享，一般通过 P2P 技术来实现分布式网络的机制。数据层是最基本的，包含了底层数据区块、基础数据以及基本算法等等[10]。区块链模型图如下图 1 所示。

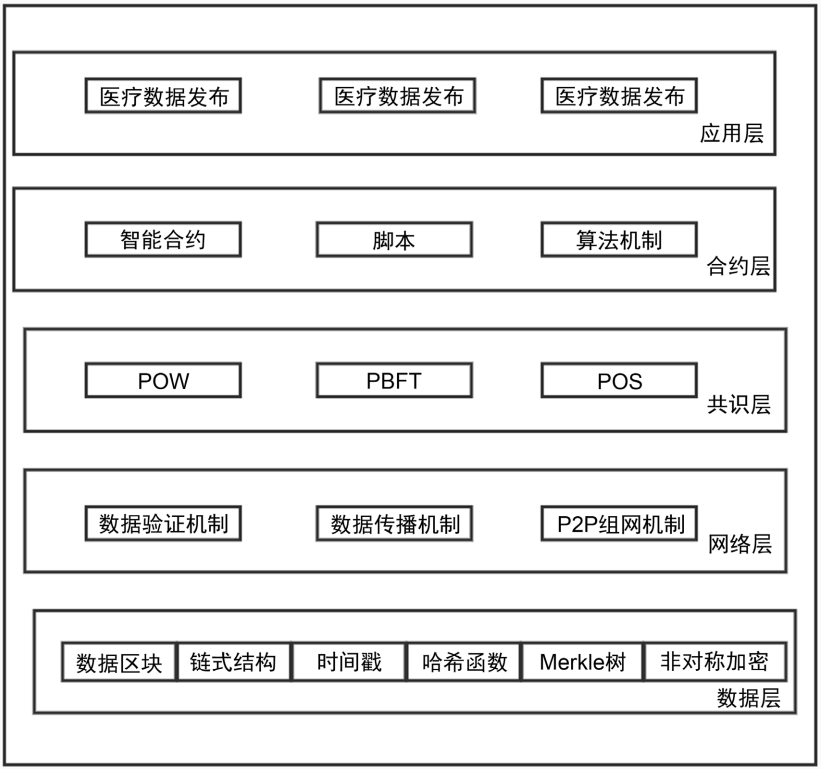

Figure 1. Blockchain model diagram
图 1. 区块链模型图

3.2. 构建电子病历系统模型

本文基于联盟链的基础，搭建电子病历系统，该系统包含了 n 个节点，各个节点都是用 P2P 网来相连。区块链整体结构是用 Hash 值将创世区块和一些其他区块相连，创世区块是区块链的重要部分，区块链的 ID、智能合约、主节点和 IPBTF 都在其中。一般主节点具有写数据的权限，对与新加入联盟链的实例的新节点来说，需要判断有没有读取电子病历的信息数据的权限，有没有写电子病历数据的权限。电子病历系统模型的整体架构图如下图 2 所示。

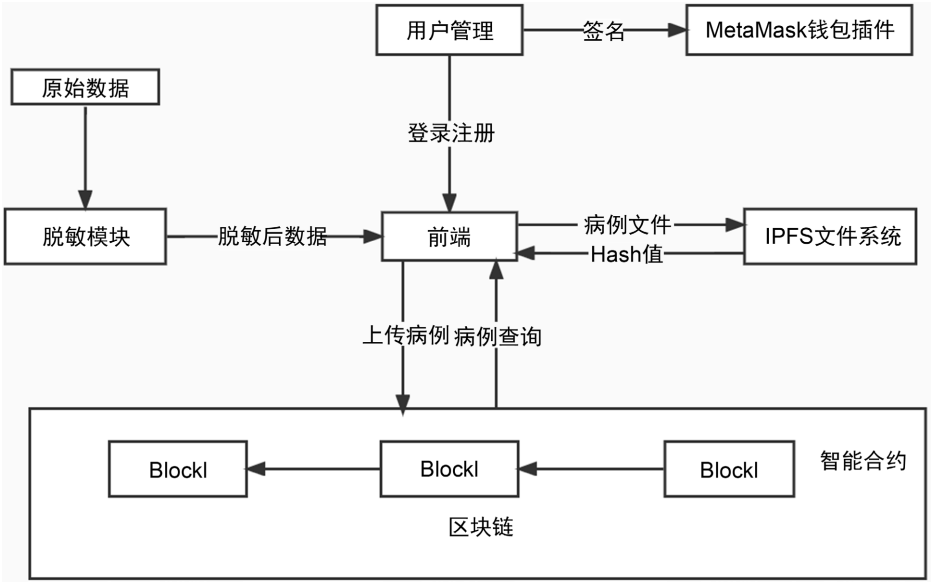

Figure 2. Model diagram of electronic medical record system
图 2. 电子病历系统模型图

如图 2 所示，MeatMask 钱包可以解决业务系统账户问题，同时具有很高的安全性，可以规避钱包数据被不法分子侵入。脱敏模块是保证患者隐私的重要保障，因为区块链上所存储的数据是透明的[11]，所以必须保证所有患者隐私数据在上链前都经过严格的脱敏处理。区块链上所存储的信息都是单一的文本数据，因为患者的医疗数据还包含很多其他数据格式的数据，比如医疗影响、DICOM 文件等，所以本文引入了 IPFS 星际文件系统来解决这个问题，该系统原理与区块链相同，可以将文件返回的 Hash 值上传到链上。同时采用区块链的 DAPP 开发组件可以很好地支持智能合约。

3.3. 电子病历系统功能模块设计

电子病历系统的功能分为五个部分：登录模块、病历管理模块、病历权限管理模块、加密模块、区块链客户端模块。功能模块图如下图 3 所示。

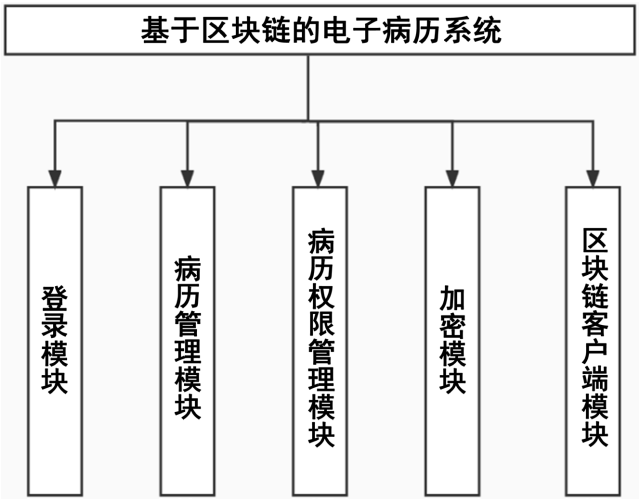

Figure 3. EMR function module diagram
图 3. 电子病历功能模块图

其中登录模块可以对所有用户的身份信息进行管理，包含了各个节点用户的注册、登录和注销，对于新加入的用户节点需要发送申请，需系统审核完成之后，被允许通过才可加入。病历管理模块可以查阅所有患者的诊疗数据信息，还可以新增或者修改这些数据，包括非文本类数据也可上传。病历权限管理模块可被用来患者进行挂号，查阅病历权限和注销。加密模块用以对交易的管理。区块链客户端模块对于整个区块链网络进行严格管理。

3.4. 电子病历系统的智能合约设计

智能合约其实就是一种用计算机编程语言取代了法律语言记录条款并由程序自动执行的条约[12]。它提供了非常多的 API 接口，是开源区块链的底层系统。本文针对所设计的基于区块链的电子病历系统设计了一些智能合约，包括：病历管理合约、权限管理合约、注册管理合约、机构联盟合约和索引合约。其中病历管理合约主要针对医生对于患者病历管理这一应用场景，医生像系统发送申请会返回一个患者数据信息。权限管理合约针对用户对患者病历操作的权限进行控制，用户包含医生和患者本人。注册管理合约是定义了用户的身份字符串作为唯一标识符，确保唯一性。机构联盟合约是将每个医疗机构的身份字符存储到链上，作为节点形成一个联盟。索引合约的主要功能是让患者可以快捷的查询自己的电子病历数据以及该病历的历史记录，患者可以用个人或者医院作为自己的搜索条件。

4. 结束语

本文主要是对电子病历系统模型进行设计，目的是为了保障患者的隐私数据在存储和共享过程中更加的安全高效。创新之处在于针对患者的隐私数据采用脱敏方法进行处理，然后部署到区块链上，同时为了保证各个类型的医疗数据都能够存储，引入 IPFS 星际文件系统。针对患者病历信息可以在各个医疗机构之间进行高效安全的互通，采用联盟技术进行设计，确保这些患者数据不会单独存储在私人领域，是真正意义上的共享，由所有参与者共同维护，确保这些信息的安全。同时患者也可以对自己的信息进行查询，也可对信息交易进行授权，对于历史记录也有查询权力。每次交易都会保留记录，这就确保了不会有人对系统信息进行恶意篡改，使得这些数据更加安全。最后针对该模型的实际应用场景，针对性地设计适合该模型的智能合约，保证患者电子病历数据在共享过程中的安全性。

当今社会，无论是区块链技术还是电子病历系统的研究都还处于初级阶段，电子病历中涉及了患者的诊疗数据，这对于电子系统的研究和设计是十分重要的。所以，如何保证这些数据能够安全快速高效地存储，如何让这些数据在各个机构之间安全高效地共享，如何确定这些数据在交易时候的安全性，这些问题仍是我们之后的研究重点。这些问题对于今后医疗服务行业的未来有着极其重要的意义，解决这些问题还是任重而道远。

基金项目

1) 海口市科技计划项目“基于区块链技术建立安全可信的电子病历研究”(编号 2020-049)；
2) 海南省重点科技计划项目“基于区块链的联盟业务协同关键技术研究与应用”(编号 2020018)；
3) 海南省教育厅项目资助(编号 Hnjg2021ZD-10)。

参考文献

[1] 袁勇, 王飞跃. 区块链技术发展现状与展望[J]. 自动化学报, 2016, 42(4): 481-494.

[2] Heart, T., Ben-Assuli, O. and Shabtal, I. (2017) A Review of PHR, EMR and EHR Integration: A More Personalized Healthcare and Public Health Policy. *Health Policy and Technology*, **6**, 20-25. https://doi.org/10.1016/j.hlpt.2016.08.002

[3] Sanz-Ortega, L., Rojas, J.M., Marcos, A., *et al.* (2019) T Cells Loaded with Magnetic Nanoparticles Are Retained in Peripheral Lymph Nodes by the Application of a Magnetic Field. *Journal of Nanobiotechnology*, **17**, Article No. 14. https://doi.org/10.1186/s12951-019-0440-z

[4] 宋华刚. 医院电子病历管理系统研究[J]. 电子元器件与信息技术, 2020, 4(8): 130-131.

[5] 秦虎, 时艳博, 王帅. 同基于结构化电子病历的医疗质量管理系统应用研究[J]. 中国数字医学, 2020(2): 13-14.

[6] 琚春华, 邹江波, 傅小康. 融入区块链技术的大数据征信平台的设计与应用研究[J]. 计算机科学, 2018, 45(S2): 522-526, 552.

[7] 李丹, 曹小佳. 电子病历信息管理系统的设计与实现[J]. 微型机与应用, 2013(1): 11-13.

[8] 王子鹏, 李璐璐. 基于区块链技术的电子文件管理模式研究[J]. 浙江档案, 2018(2): 18-20.

[9] Si, H., Sun, C., Li, Y., *et al.* (2019) IoT Information Sharing Security Mechanism Based on Blockchain Technology. *Future Generation Computer Systems*, **101**, 1028-1040. https://doi.org/10.1016/j.future.2019.07.036

[10] 阎虹. 智慧医院信息系统的关键技术研究与应用[J]. 电子技术与软件工程, 2020(23): 139-140.

[11] 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): 260-266.

[12] Xu, M., Chen, X. and Kou, G. (2019) A Systematic Review of Blockchain. *Financial Innovation*, **5**, Article No. 27. https://doi.org/10.1186/s40854-019-0147-z