Computer Science and Application 计算机科学与应用, 2022, 12(7), 1814-1821
Published Online July 2022 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2022.127182

Hans汉斯

基于联盟链的电子病历数据上链系统

陈　涛[1]，莫晶亮[2]，邱　钊[1*]，张开锋[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20日；录用日期：2022年7月19日；发布日期：2022年7月26日

摘　要

随着电子病历的不断发展，其安全性和真实性越来越受到人们的重视。对于电子病历进行数据的上链，将电子病历放在区块链中可以为医院和患者带来极大的便利，实现电子病历去中心化和防篡改。本文基于联盟链的电子病历，采用区块链的相关技术来对电子病历的数据进行存储，并加入了去中心化的IPFS系统进行对电子病历的上链，可以实现无第三方机构的情况下对电子病历进行访问和电子病历的可追溯性，来保证了医院的电子病历的安全。

关键词

电子病历，联盟链，区块链，IPFS

Electronic Medical Record Data On-Chain System Based on Alliance Chain

Tao Chen[1], Jingliang Mo[2], Zhao Qiu[1*], Kaifeng Zhang[1]

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

Received: Jun. 20th, 2022; accepted: Jul. 19th, 2022; published: Jul. 26th, 2022

Abstract

With the continuous development of electronic medical records, more and more attention has been paid to its security and authenticity. For the data upload of electronic medical records, placing electronic medical records in the blockchain can bring great convenience to hospitals and patients, and realize the decentralization and tamper-proof of electronic medical records. The paper

*通讯作者。

文章引用: 陈涛, 莫晶亮, 邱钊, 张开锋. 基于联盟链的电子病历数据上链系统[J]. 计算机科学与应用, 2022, 12(7): 1814-1821. DOI: 10.12677/csa.2022.127182

is based on the electronic medical record of the alliance chain, adopts the relevant technology of blockchain to store the data of the electronic medical record, and joins the decentralized IPFS system to upload the electronic medical record to the chain. It can realize the access and traceability of electronic medical record without third-party institutions, so as to ensure the safety of the electronic medical record of the hospital.

Keywords

Electronic Medical Record, Alliance Chain, Blockchain, IPFS

1. 引言

近几年以来，区块链技术一直都是国家推动并且研究人员十分关注的研究课题，而区块链技术的不可篡改性和去中心化正好可以为医院的电子病历保护提供了新的思路，所以也一直受到研究者的密切关注，有着巨大的研究和应用价值。因此，我们可以在原有电子病历和区块链的基础上，将电子病历和区块链进行改进和结合，这样既保证了电子病历的存储可靠性，也保证了其的安全性和不可篡改性，确保了医生和患者的权益。

区块链技术分为区块链 1.0 阶段、区块链 2.0 阶段和区块链 3.0 阶段三大时期[1]。其中区块链 1.0 阶段是区块链技术的初级阶段。该阶段主要是以中本聪提供的比特币概念为主，实现了去核心化的虚拟币种。让货币的交易过程达到去中心的效果。区块链的第二阶段是区块链技术的进阶阶段，在这一阶段主要是以太坊的智能合约为主，通过智能合约的使用来对金融领域的相关应用进行开放和实现。区块链的第三阶段是区块链技术的现在的最高级阶段，在这一阶段中区块链技术可以应用到社会中任何需要它的领域当中去，这个领域不再限于金融领域，可以是政府、医疗和文化等方方面面，包含了整个社会。目前，我们正处于区块链 2.0 向区块链 3.0 的过渡阶段，这个阶段实现核心是区块链相关技术的应用的落地。为了更好地对数据进行存储，一些使用区块链的方案被提出来。Tian [2]等提出了一种轻量级、可扩展的区块链框架，该框架采用松耦合设计来为证据提供完整性和有效性验证。Liang [3]等提出了一种能够解决数据存储和恢复方法的区块链技术方案，该方案可以对网络数据存储进行编码和修复。

近些年也有越来越多的区块链存储平台开始出现，这些平台都是分布式的，例如 IPFS [4]，Storj，Sia [5]，Swarm [6]。其中的星际文件系统 IPFS 是一种点对点分布式文档系统，是指通过内容寻址的方式，给所有已保存的文档分配唯一的哈希值，是使用最为广泛的存储平台之一。解决了中心化存储不足、网络数据保存和数据分发的问题，能够安全且速度更快地保存数据，对区块链建设起到重大的作用。所以现在很多基于区块链的方案都是用 IPFS 来作为的存储层进行去中心化存储。Sun J [7]提供了一个基于属性电子病历的加密方法，该方案通过把个人数据保存到 IPFS 中，来确保在电子病历中的安全。Zheng [8]等人提出通过使用 IPFS 网络来减少区块链当中的数据存储大小，该方案在存储空间和安全性等方面有着很好的效果。Chen [9]等人提出了一种用区块链将 IPFS 存储于锯齿形存储模型结合起来的方案，该方案解决了 IPFS 中个人用户的高吞吐量的问题。

本文在区块链的基础上，采用了现有的联盟链，利用 IPFS 来对电子病历中的数据进行上链操作，实现了联盟链中对电子病历的数据上链系统。

2. 相关研究

存储和共享作为电子病历中的热点问题，基于区块链的电子病历的研究也成为了当下研究的重点之一，特别是在疫情严重的情况下，各地电子病历如何共享和存储的问题更是成为急需解决的重点。

2.1. 区块链框架

区块链的体系架构如图 1 所示，它是由数据层、网络层、共识层、激励层、合约层和应用层六层所组成的，每个层次结构虽然功能不同却能相互支持实现一个去中心化的信任机制。

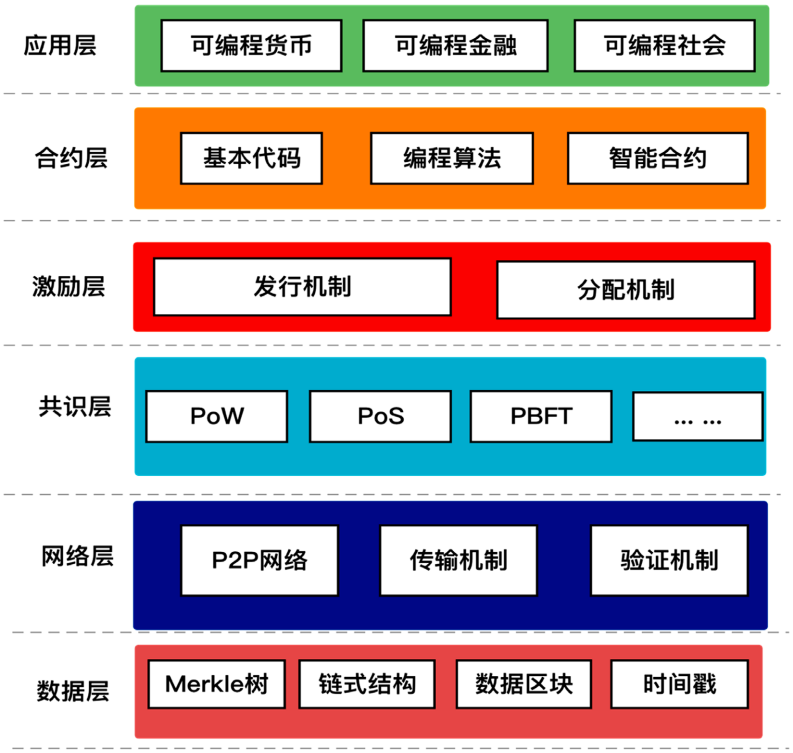

Figure 1. Blockchain architecture diagram
图 1. 区块链体系架构图

其中数据层是定义区块链技术的最基本的、最重要的物理形态，包括 Merkle 树、块的存储和时间戳等，是区块链架构的基础层。网络层是一个分布式的网络，同时它也不会被第三方的中心组织检测，实质上它是一个 P2P 网络，每个节点既接收信号，也产生信号。共识层是使高度离散的节点在去中心化的体系中有效地面对区块数据信息后来达成一个共识，这也是来保证整个区块链网络状态良好的重点。在这里面，较为普遍的共识机制大致有工作证明(Proof of Work)、权益证明(Proof of Stake)和实用拜占庭(Practical Byzantine Fault Tolerance)。激励层一般是用相应的奖励制度，来激发区块中的各个结点和交易的积极性，而目前人们最熟悉的比特币的奖励因素，一是产生新区块的系统奖励，二是我们在进行交易时产生的手续费。合约层一般是由基本代码、编程算法以及智能合约等组成的，是实现区块链可编程的关键层，区块链中的相关智能合约也可以根据自己的实际要求部署到区块链当中，并且是由平台自动执行的。应用层是区块链及其衍生应用层序的层次，在这里封装了区块链的多个应用场合和案例。在这些基础的模型当中，每个层次都有自己的作用和实现方法，能够让区块链灵活的使用于不同的应用场合之中。

2.2. 区块链分类

从分布式网络的大规模的发展和数据读写严格管控的角度，人们把区块链分为公有链、私有链和联盟链[10]。

1) 私有链

私有链，顾名思义，是一种完全私有的区块链[11]，它的任何写入权完全掌握在一个体或公司手中，区块链会严格监管任何要加入这些区块链中的节点。私有链具有如下特点：a) 去中心化，不可篡改性。b) 安全性强，无需可信第三方来维护整个系统，只有合法授权的节点才能够访问这个区块。c) 可管理性强。d) 在有些情况下，机构可以改变关于私有链的具体规则，例如恢复交易流程服务。同时，私有链的交易成本远远低于公有链和联盟链，而且不需要每个网络节点都进行审查，只需要几个高计算节点进行审查，因此私有链的交易速度非常快。但是在使用的时候，必须保证整个系统是安全的。由于读取权限的限制，任何一个用户都不可能将自己所有的隐私资料泄信息泄漏出去。因此信息安全保护得到了相对较好的保护。它的信任机制是一种完全的自我背书。

2) 联盟链

联盟链是指由众多组织或机构共同参加管理的区块链[12]，由所有的组织者或机构共同发展管理的单一或众多节点，其数据信息只可以在整个系统内不同的组织机构负责读取和传输。首先要保证各主体间具有明确的权利义务关系，其次还要制定统一的技术标准，最后是加强监管。其中最重要的就是一批机构和组织将形成利益关系共同体，来共同确保区块链的健康运行。

3) 公有链

公有区块链从字面上理解就是“公有”的[13]。它是指全世界任何人都能进行查看和加入的、所有人都能进行交易并且交易的过程和结果都能得到有效证实的、所有人都能加入其中的共识与认证过程的区块链。公有链中最出名就是比特币和以太坊，这两者都是使用的公有链，没有任何的限制，所有人都可以参加。正是因为这样，公有链才具备了较低使用门槛、链上的数据能被所有人查看且无法修改、匿名性强以及难以受到开放者影响等优势。

Table 1. Blockchain feature comparison table
表 1. 区块链特点对比表

	私有链	联盟链	公有链
参与者	个体或公司内部	特定人群	任何人随意进出
信任机制	自行背书	集体背书	POW/POS/POA
记账人	自定	参与者协商决定	所有参与者
激励机制	不需要	可选	需要
中心化程度	中心化	多中心化	去中心化
突出优势	透明和可追溯	效率和成本优化	信用的自建立
典型应用场景	审计、发行	结算	token
典型代表	Overstock	Fabric	BTC、ETH
承载能力	1000~10 万笔/秒	1000~1 万笔/秒	3~10 笔/秒

综上所述，这三类区块链的各有各个的特点、缺点和优势，它们是为了适用于区块链中的各种场景和应用而设计出来的，这三类区块链特点对比如表 1 所示。尽管私有链交易速度快，交易成本相对低廉，

但是私有链仍面临着很多问题，例如权限往往被少数节点所掌控，无法完全处理作弊问题，从而背离了去中心化的初始目标；另外，私有链上的各种数据信息是可以被人操纵处理的，代码也可能被更改。同时，因为在联盟链是由众多组织参与的，这些组织包括医院、政府、医生和第三方医疗机构等等，可以让电子病历的共享成为现实的同时还保护了电子病历的安全。所以在本系统中，我们将会使用联盟链让电子病历实现去中心化，解决了电子病历中心化太强的弊端。

2.3. IPFS

IPFS 是能够进行内容寻址的、具有分布式存储特点的传输协议，可以共享文件。也更为适合作为电子病历的存储中心。IPFS 目的是为了使我们的网络更快、更安全、更开放。正是因为 IPFS 是通过分布式保存文件才使得各种计算设备连接到同一个文件系统，这样就能让全球文件进行统一保存成为了可能，它的结构图如图 2 所示。

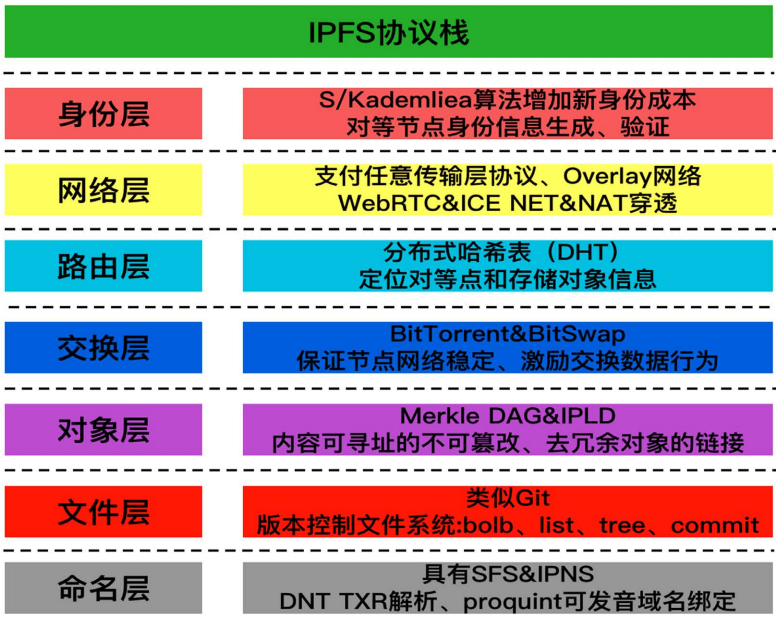

Figure 2. IPFS structure diagram
图 2. IPFS 结构图

IPFS 与联盟链协同工作，能弥补区块链中存储效能低下、成本昂贵和跨链各个链之间无法协作这两大不足。针对第一个不足，我们可以将文件的数据保存在 IPFS 中，这样就没有必要将大量数据信息置于区块链中，而是在区块链中保存唯一永久可用的 IPFS 地址。而面对第二个不足，IPFS 也可以允许所有类型的区块链网络进行传送信息和相关文件。

3. 论基于联盟链的电子病历的数据上链系统架构

本文提出的联盟链下的电子病历上链系统主要是含如图 3 所示的几个部分。

1) 实体层

实体层由政府、各个医院和患者等机构组成。当各个医院在开具电子病历以后都会上传到区块链层中，在区块链中产生电子病历的信息。在以后需要验证该患者的电子病历时，只需要发送一个核验请求，对上传到区块链的电子病历进行验证。当验证成功时，服务器就会回馈一个电子病历的信息；当验证失败时，就会反馈该用户不符合访问电子病历的信息。

2) 区块链层

在区块链中的区块结构是一个分布式账本。区块是由两个部分组成的，分别是区块头和区块头两部分。区块头存储了区块的原信息，用了对区块内容进行一下标识，校验和说明等等。区块体中是对这个区块中的所有交易进行打包整合在一起将区块组织成链能够有效地降低已有区块数据被更改或删减的可能性，这也是区块链本身的一大特点。

3) 存储层

存储层中存储的电子病历信息和电子病历的影像是存储在链外的 IPFS 中。当实体层发送验证请求时，就需要存储 IPFS 中的信息。为了保护电子病历信息不被恶意修改，以及节约区块链中的空间，存放在 IPFS 中的所有文件会被哈希化，哈希值也会被写在到区块链中。因此，实体层会通过区块中的 hash 值获得存储在 IPFS 的对应的唯一水印信息，然后和核验请求中的图像产生的零水印进行比较，这样就很容易验证电子病历数据的真实性。

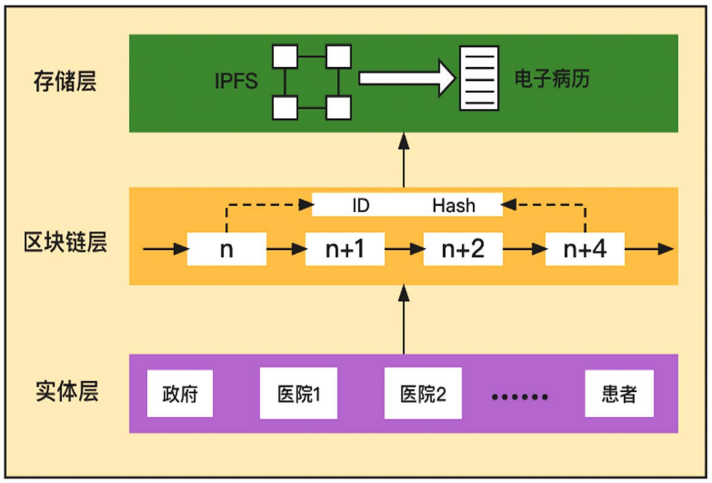

Figure 3. System architecture diagram
图 3. 系统架构图

4. 系统功能模块说明

本文提出了一种基于联盟链的电子病历的数据上链系统设计方案，通过区块链中的联盟链来对电子病历进行存储和查询，然后再将电子病历的相关信息存放到去中心的 IPFS 上，根据各个组织的权限来决定能否让该组织对电子病历进行查看，得到在链上的电子病历。本系统的各个功能模块如图 4 所示：

1) 注册/登录模块

在注册模块中，重点是对于医生和患者的用户的身份信息和系统账号密码的进行绑定。每个用户必须在经过身份认证以后才能进入到系统的各自页面当中去，进行各自用户的相应操作。

2) 患者病历管路模块

患者病历管理模块主要是患者自身的个人信息、病历信息、挂号审核和权限审核。是为了方便患者能对自己的病历信息进行审核个管理的一个模块，在该模块中，患者有权利查看自己的信息，审核自己的病历信息有没有进行被人修改。

3) 医生病历管理模块

医生病历管理模块主要是医生的个人信息、挂号管理和患者管理。是让医生对患者的病历进行修改的，同时也是让患者能够让患者看到自己实时看到自己的病历情况。

4) 后台模块

后台模块主要是医生管理和身份审核两个模块，是对实体层中的医院对于医生信息和资质的审核以及对于患者身份的审核。

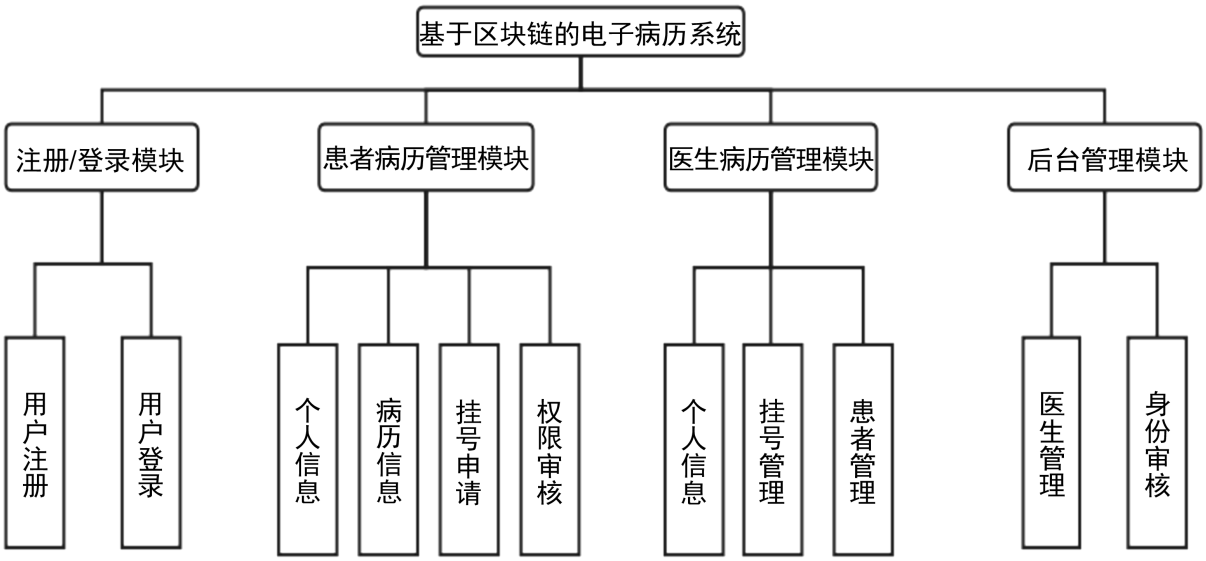

Figure 4. System function module diagram
图 4. 系统功能模块图

5. 结束语

电子病历是当前医院中十分重要的一环，这个重要性不止是对于患者，同是对于医生和医院也是一样的，正是有了电子病历才会在以后的看病过程中有所依据，才能在一定程度上改变医患矛盾的问题。本文提出的基于联盟链的电子病历，能够有效解决在无第三方机构时对医院电子病历进行访问，同时对电子病历能够进行追溯，来保证了患者手中的电子病历安全。

致　谢

本文的撰写要十分感谢我的导师邱钊教授的耐心指导，也感谢课题组的科研项目让我能够加入到区块链技术和电子病历的研究中去。本文提出的系统架构和模块都是我们实验室共同努力下完成的，在此，十分感谢我们团队中的每一位小伙伴。

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] 代闯闯, 栾海晶, 杨雪莹, 过晓冰, 陆忠华, 牛北方. 区块链技术研究综述[J]. 计算机科学, 2021, 48(S2): 500-508.

[2] Tian, Z., Li, M., Qiu, M., *et al.* (2019) Block-DEF: A Secure Digital Evidence Framework Using Blockchain. *Information Sciences*, **491**, 151-165. https://doi.org/10.1016/j.ins.2019.04.011

[3] Liang, W., Fan, Y., Li, K.C., *et al.* (2020) Secure Data Storage and Recovery in Industrial Blockchain Network Envi-

ronments. *IEEE Transactions on Industrial Informatics*, **16**, 6543-6552.

[4] Benet, J. (2014) IPFS-Content Addressed, Versioned, P2P File System. arXiv preprint arXiv:1407.3561.

[5] Vorick, D. and Champine, L. (2018) Sia: Simple Decentralized Storage.

[6] Acampora, L. (2012) Swarm. *The Missouri Review*, **35**, 64-80. https://doi.org/10.1353/mis.2012.0080

[7] Sun, J., Yao, X., Wang, S., *et al.* (2020) Blockchain-Based Secure Storage and Access Scheme for Electronic Medical Records in IPFS. *IEEE Access*, **8**, 59389-59401. https://doi.org/10.1109/ACCESS.2020.2982964

[8] Zheng, Q., Yi, L., Ping, C., *et al.* (2018) An Innovative IPFS-Based Storage Model for Blockchain. 2018 *IEEE*/*WIC*/*ACM International Conference on Web Intelligence* (*WI*), Santiago, 3-6 December 2018, 704-708. https://doi.org/10.1109/WI.2018.000-8

[9] Chen, Y., Hui, L., Li, K., *et al.* (2017) An Improved P2P File System Scheme Based on IPFS and Blockchain. 2017 *IEEE International Conference on Big Data* (*Big Data*), Boston, 11-14 December 2017, 2652-2657. https://doi.org/10.1109/BigData.2017.8258226

[10] 史锦山, 李茹. 物联网下的区块链访问控制综述[J]. 软件学报, 2019, 30(6): 1632-1648. https://doi.org/10.13328/j.cnki.jos.005740

[11] 王新宇. 基于故障注入的以太坊私有链性能测试系统的设计与实现[D]: [硕士学位论文]. 南京: 南京大学, 2020.

[12] 刁一晴, 叶阿勇, 张娇美, 等. 基于群签名和同态加密的联盟链双重隐私保护方法[J]. 计算机研究与发展, 2022, 59(1): 172.

[13] 韦安垒. 公有链技术及其应用价值[J]. 互联网经济, 2018(7): 26-31. https://doi.org/10.19609/j.cnki.cn10-1255/f.2018.07.005