基于区块链技术的电子病历系统研究*

孙成浩 刘 芬 赵 峰

（皖南医学院弋矶山医院 芜湖 241001）

〔摘要〕 分析目前医院电子病历系统应用存在的问题，阐述基于区块链技术的电子病历系统构建与应用，介绍区块链数字签名技术架构及其在电子病历系统中的应用与实践。

〔关键词〕 区块链；电子病历；资源共享；数字签名

〔中图分类号〕R－058 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2021.05.014

Study on the Electronic Medical Record System Based on Block Chain Technology *SUN Chenghao, LIU Fen, ZHAO Feng, Yijishan Hospital of Wannan Medical College, Wuhu 241001, China*

〔**Abstract**〕 The paper analyzes the problems existing in the application of Electronic Medical Record System (EMRS) in hospitals, expounds the building and application of EMRS based on block chain technology, and introduces the framework of digital signature of block chain technology and its application and practice in EMRS.

〔**Keywords**〕 block chain; Electronic Medical Records (EMR); resource sharing; digital signature

1 引言

目前医院电子病历系统存在书写规范性、真实性、法律约束力较差以及数据不便于管理、无法实现智能化、病历书写和医学相关信息支持不能相互结合、系统管理复杂等缺点。应用区块链能够将不同的电子健康档案（Electronic Health Records, EHR）中包含的离散患者记录（或数据“块”）包含到一个内容链中[1]。虽然电子病历给医院及患者带来便利，但是其潜在的安全漏洞也为患者带来隐私泄露等风险，必须要从技术及管理层面做好电子病历安全保障工作。区块链中的数字签名技术可为提高电子病历安全性提供有力保障[2]。利用区块链对医疗数据进行去中心化管理，使患者可以控制数据分享，提升隐私保护力度[3]。基于区块链的电子病历是用电子设备以 P2P 方式保存、管理、重现、共享、加密的数字化患者医疗记录。数字签名通过非对称加密技术加密患者信息并确认发送者身份，因诊疗产生的图形、图像、视频等多媒体签名具有相同法律效力。通过区块链技术可记录患者全生命周期健康数据，使区块链上的机构保有统一数据，保证患者数据不可篡改并交给患者本人，为医疗、科研、辅助诊断等提供稳固平台。

〔收稿日期〕 2020－07－26

〔作者简介〕 孙成浩，本科；通讯作者：刘芬，硕士。

〔基金项目〕 安徽省高等学校省级质量工程项目“基于智慧医院科研兴趣小组的医学信息人才培养模式研究与实践”（项目编号：2018jyxm1266）。

2 基于区块链技术的电子病历系统

2.1 技术分析

基于数字签名的可信电子病历系统提供数字签名服务并对结果进行真实性、有效性验证，保证数据真

实、完整、合法[4]。应用 P2P 通讯技术可实现各医院点对点信息传输；区块链内医院通过约定的决策机制自动达成共识，共享同一份可信、标准统一的就诊记录账本；通过非对称加密算法、哈希算法等密码学工具确保共有信息安全及各患者身份准确。数字签名应用非对称加密方法产生与电子病历内容关联的签名，已签名的数据无法被破解、篡改和抵赖。此技术符合《电子签名法》要求，具有法律效力。按照目前技术水平，在管理、经济、技术上都具备可行性。签名的电子病历增加到区块链中，数据不会更改和丢失，使区块链上的电子病历更加安全，生成的唯一密钥交由患者管理[5]。通过访问 RESTful 架构下的应用程序接口（Application Programming Interface，API）可以查看患者所有电子病历。

2.2 技术架构

2.2.1 区块链类型架构 区块链技术可分为公共链、联盟链和私有链 3 种模式[6]，见图 1。根据实际应用场景和需求，最适合医院的区块链类型是联盟链，其节点可以一直增加。联盟链不需要集中的服务器，区块链共识机制的存在让节点不需要互相信任就可以互相传输信息。为了获得更好的性能，联盟链对于共识或验证节点的配置和网络环境有一定要求。设置准入机制可以对参与者进行限制和筛选，有助于提高交易性能。

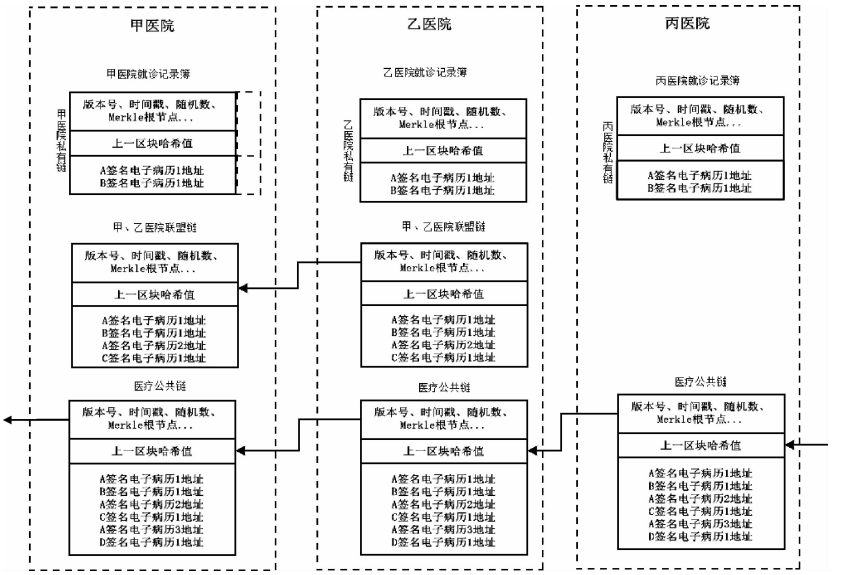

图 1 区块链类型架构

2.2.2 实现电子病历共享 区块链协议是通用的，在医疗保健领域的应用程序彼此兼容。底层区块链技术可以确保信息安全。区块链加电子病历技术可以使加入联盟链的医院共享患者电子病历，电子病历经过非对称加密存储在医院服务器上，由区块链生成 Web 服务的 API 保存在院内就诊记录账本中。在节点上的医院遵循同一标准电子病历格式，每次数字签名结束后只能在之前电子病历后新加电子病历，不能更改已经签名的病历，通过区块链中的工作量证明（Proof of Work，POW）机制让新产生的电子病历 API 通过区块链上其他节点的就诊记录账本进行共享。在患者允许的情况下，医生可以查看患者完整诊疗记录、遗传病史、过往病史等数据作为诊断参考，大幅降低误诊机率，有助于预测可能发生的疾病，以便提前预防。

2.3 实践与应用

2.3.1 数字签名技术应用 加入区块链的每家医院都相当于 1 个节点，患者在医院使用电子健康卡就诊结束时，医生通过专用私钥对共享电子病历执行数字签名。数字签名技术首先会在患者电子病历信息扣上时间戳，然后对电子病历进行哈希算法加密生成摘要，医生使用私钥对摘要进行非对称加密，在使用私钥进行签名时还需要输入个人识别码

以确认签名人身份。当该患者诊疗结束时医院电子病历系统会验证所有数字签名是否有效。如有效则电子病历系统执行数字签名并加盖时间戳。医生使用数字签名结束后不可再对电子病历进行修改。数字签名特点是其代表电子病历特征，电子病历如果发生改变其摘要内容也会变化。

2.3.2 发送方医院流程 医院作为联盟链上的节点会对电子病历信息再次进行非对称加密，通过随机数生成器生成256位随机数作为私钥。将256位二进制形式的电子病历私钥通过SHA256哈希算法和Base58转换，形成固定长度密钥，即为患者电子健康卡号。医院将加密后的电子病历信息保存到院内服务器上，生成Web服务API并上传至医院就诊记账簿中，将此条信息经过时间戳服务器盖上时间戳，然后广播给此联盟链上的其他医院节点，见图2。

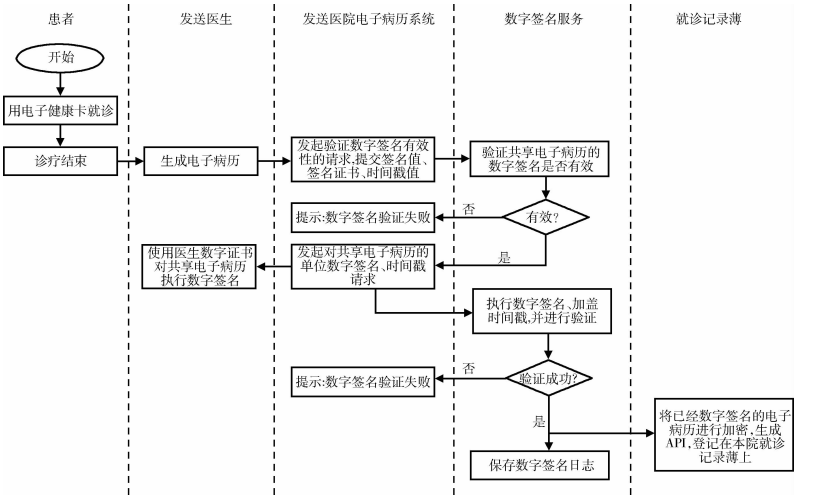

图2 发送方医院流程

2.3.3 接受方医院流程 其他医院节点收到此广播后，通过区块链共识机制验证其是否符合预定规则，若符合则将此API保存至医院节点就诊记账簿中，此时在联盟链上的所有医院节点都有相同记录。访问此API需要储存在患者电子健康卡上的姓名和健康卡号信息。患者用电子健康卡到联盟链上其他医院就诊时，医生可以查看此患者所有经数字签名技术加密的电子病历信息。医院电子病历系统会根据公钥验证数字签名数据有效性，若有效则可以直接查看病历，所有已经进行数字签名的电子病历都不可被修改、不可抵赖，见图3。

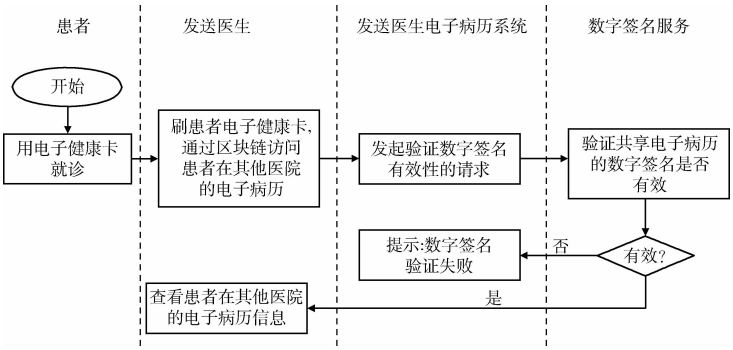

图3 接收方医院流程

2.3.4 电子病历查询 患者到联盟链上的任何一家医院都可以查看之前所有就诊记录，而且每家医院诊疗记录都会盖上时间戳进行加密处理，已经进行数字签名的电子病历信息不可更改。查阅区块链上某患

者电子病历信息必须使用患者本人电子健康卡，即只有获得患者允许才可以访问其病史，见图 4。

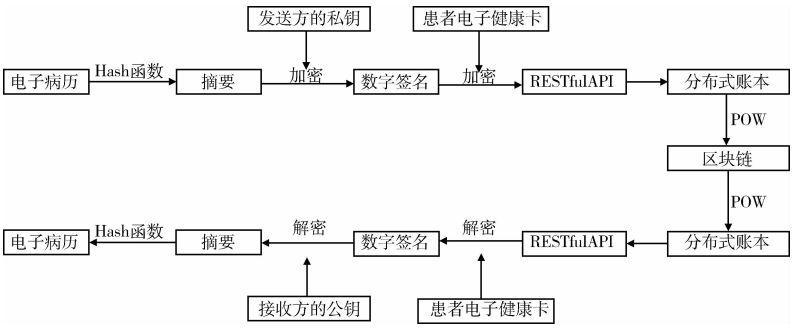

图 4　区块链数字签名电子病历架构

3　结语

区块链与数字签名技术在电子病历系统中的应用，使电子病历具有和手工签名一样的法律效力且不可篡改、抵赖。患者电子病历信息经过哈希算法、非对称加密和椭圆曲线加密后存储在医院服务器中，保证隐私安全。将患者电子病历信息以 API 方式登记在就诊记录账本中，每家医院的就诊记录账本都会有相同记录。只有在患者允许的情况下医生才可以访问其所有电子健康记录，有助于准确了解病情；医院管理制度更规范、更严谨；实现无纸化，减少资源浪费；区块链 POW 机制可有效防止黑客攻击。电子病历具有统一格式，可以方便地进行大数据分析处理与深度学习，以辅助诊断并为医疗信息化发展提供优质平台。

参考文献

1　陈隆轩，马俊秋，倪若宇，等．区块链技术在电子病历上的应用研究［J］．大数据时代，2018（5）：11－13.
2　田国栋，符晓婷，宗文红，等．数字签名技术在电子病历中的应用及发展趋势［J］．中国卫生信息管理杂志，2011，8（6）：58－61.
3　黄建华，江亚慧，李忠诚，等．区块链在医疗行业的应用前景［J］．医学信息学杂志，2018，39（2）：2－8.
4　王文翠，李志强，秦芳，等．基于数字签名的可信电子病历系统［J］．中国数字医学，2016，11（3）：19－21.
5　Jorwekar GJ，Dandekar KN，Baviskar PK，et al. Picture Archiving and Communication System（PACS）：clinician perspective about filmless imaging［J］. The Indian Journal of Surgery，2015，77（3）：774－777.
6　熊志强，周吴．基于区块链技术的电子病历研究［J］．中国数字医学，2019，14（1）：64－66.

（上接第 60 页）

交互支持等要素，实现多源异构数据整合、治理和共享。智慧医院的智慧应用涉及临床治疗、患者服务和医院管理运营，具有丰富应用场景和广阔发展空间。因此伴随着数字化转型的智慧医院将秉承场景开放的创新思路，充分调动医院、企业等各方力量，吸引多元主体共同参与智慧应用建设。在国家推动新基建战略机遇下，智慧医院作为医疗健康新基建的重要组成部分将持续推动大数据、云计算、人工智能、区块链等技术与医疗健康业务深度融合与应用，以先进技术能力推动医疗健康产业转型升级与高速发展。

参考文献

1　张建忠，李永奎，曹玲燕，等．国内外智慧医院建设研究［J］．中国医院管理，2018，38（12）：64－66.
2　崔文彬，唐燕，刘永斌，等．智慧医院建设理论与实践探索［J］．中国医院，2017，21（8）：1－4.
3　张红伟，翟鹏程，冯思度，等．数字化医院多源异构数据集成平台研究与设计［J］．医学信息学杂志，2019，40（1）：23－25.
4　刘艳亭，李健，郭敬鹏．智慧医院规划建设与应用研究进展［J］．中国医学装备，2019，16（6）：177－181.
5　徐安琪，范春．智慧医院建设及应用场景的研究与实践［J］．中国数字医学，2018，13（7）：90－92.
6　周红林，曾春生，常欢欢．基于领域驱动的企业中台设计研究［J］．现代信息科技，2019（20）：79－81.