区块链技术及其在医疗领域的价值研究

倪培昆

（青岛大学商学院 青岛 266061）

〔摘要〕 阐述区块链技术概念、原理及特点，介绍区块链 + 医疗模式及其应用，包括建立个人健康数据库、打造智能化医疗救助平台，以及构建开放的医疗健康资源互助共享中心，分析区块链技术在医疗领域应用面临的挑战。

〔关键词〕 区块链；应用模式；现实挑战；医疗数据库

〔中图分类号〕R - 056 〔文献标识码〕A 〔DOI〕10. 3969/j. issn. 1673 - 6036. 2018. 02. 002

Study on Value of Blockchain Technology in Medical Field *NI Pei - kun, Scool of Business, Qingdao University, Qingdao 266061, China*

〔**Abstract**〕 The paper expatiates on the concept, principle and characteristics of the blockchain technology, introduces the blockchain + medical treatment mode and its application, including the building of personal health database, the shaping of intelligent medical assistance platform, and the structuring of an open mutual - aid and sharing center of medical health resources, and analyzes challenges confronting application of the blockchain technology in the medical treatment field.

〔**Keywords**〕 Blockchain; Application mode; Current challenges; Medical database

1 引言

区块链（Blockchain）技术已被视为继云计算、物联网、大数据之后的又一项颠覆世界的技术，国际上对区块链的研究发展迅速，国内政策也释放出积极信号，如国务院印发的《“十三五”国家信息化规划》就将区块链技术列入其中[1]。2016 年英国、美国、新西兰、韩国等发达国家相继将区块链技术上升到国家战略层面，其中爱沙尼亚、英国、以色列、韩国、新西兰成立数字化 D5 项目[2]。2017 年 7 月 11 日在青岛市区块链产业发展意见发布会上，发布了《青岛市市北区人民政府关于加快区块链产业发展的意见》，提出加快区块链在政府管理、跨境贸易、大健康产业等 10 大应用场景的开发落地，力争到 2020 年创建中国第 1 条“链湾”[3]。

区块链技术在金融、互联网等领域得到广泛的应用，显示出广阔的前景。随着区块链技术的逐步完善，在医疗领域应用也取得飞快发展，许多人认为医疗健康领域是除金融领域外的第 2 大研究领域。通过 IBM 发布的商业价值研究院区块链调研报告可知，对于区块链技术，人们希望不仅仅止于试用阶段，而是大规模采用商用区块链解决方案。从整体来看虽然当前区块链技术在医疗领域的应用有一定的发展，但相当有限，Gem、飞利浦医疗等医疗企业目前也还在逐步摸索实践中。基于此，本研究将对区块链的基础理论知识进行简单介绍，结合当前医疗部门存在的问题对区块链在医疗领域的应

〔修回日期〕 2017 - 10 - 07

〔作者简介〕 倪培昆，本科生。

用思路及体系进行探讨，以期推动区块链技术更好地服务于医疗部门。

2 区块链技术

2.1 概念

区块链技术是伴随着比特币的出现而出现的，最早于 2008 年出现在论文"Bitcoin：A Peer - to - Peer Electronic Cash System" 中[4]，起初区块链被分开使用为“区块”和“链”，直到被广泛使用时才合称为“区块链”。区块链是指彼此相连的含有时间戳的信息形成的信息块链条。区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。从数据的观点来看，区块链是一个几乎不可能改变的分布式数据库。这里的“分布式”包括分布式数据存储和分布式数据记录。从技术的角度来看，区块链接并不是一种或几种技术组成，而是多种技术集成的结果。这些技术以新的结构组合在一起，形成一种新的数据记录、存储和表达的方式。

2.2 技术原理

2.2.1 *分布式记账* 区块链设计者并没有预留一个特定的位置为专业的会计记录，而是希望建立人人都可参与的分布式记账系统，通过自愿记录的原则，分散会计责任，由所有网络参与者共同记录。区块链中的每笔新交易按对等（P2P）网络层协议分布，通过单个节点直接发送到整个网络的每个节点。区块链技术使数据库中的所有数据均存储于系统所有的电脑节点中，实时更新。

2.2.2 *非对称加密算法* 在区块链系统中，非对称加密算法是所有权验证机制的基础，非对称加密算法主要包括 ELGAMAL、RSA、D - H、ECC 等。在区块链系统的交易中，非对称加密算法中密钥的应用情形有两种：一是公钥对信息进行加密，私钥对收到的信息进行解密；二是私钥对信息签名，公钥验证签名。

2.2.3 *智能合约（脚本）* 每个智能合约本质是许多指令的集合，这些指令记录需要满足哪些条件才可以执行每次交易活动的数字化合约。智能合约的特性在于：（1）可以动态地改变条件来花费掉留存价值。（2）可以动态设置转移条件在发送价值时增加额外一些价值，如智能合约系统可利用条件来说明某笔价值只能用作特定的用途。

2.3 技术特点

2.3.1 *去中心化* 区块链以对等网络协议和纯数学方法原理为基础，利用去中心化结构或部分中心化结构，形成网络节点与分布式系统结构之间的信任关联。去中心化或部分中心化的结构设置，使数据并不是只有 1 个人记录，而是全网络中每个节点通过共识机制来完成记录，保证数据在参与数据存储的网络节点实时更新，其他网络节点进行数据同步记录，很大程度上保证分布式数据库开放透明、安全可信、不可篡改的特性。

2.3.2 *开放透明* 分布式系统的每笔交易数据是开放透明的，但并不是绝对的，而是相对的。网络中每个节点具有相同的权利和义务，可以访问得到授权的信息，允许同一网络中的其他人访问信息。网络系统中所有代码都是开源的，每个人都可以学习其代码及分析其逻辑关系。

2.3.3 *安全可信* 区块链的数据交换全部依靠机器的自制完成，依靠每个节点形成强大的“算力”来抵御外部攻击，无需人为的干预，交易双方利用对机器的信任在完全匿名的条件下完成交易，既可以保护交易双方的隐私，也可以增加交易的安全性及可信性。另外区块链上的每个节点都存储整个系统总账，只要不是网络中全部的节点都被黑客占用，系统就是安全的、可以被信任的。

3 区块链 + 医疗

3.1 概述

区块链 + 医疗代表着一种新形式的、更科学的运作模式，必须使二者融合在一起、相互借鉴，才能使区块链技术更好地应用于医疗领域。我国医疗信息化自 2007 年提出至今已有 10 多年，虽然在某些方面取得很大的进展，但目前医疗机构的电子数

据设立与使用仍然存在很多问题：（1）电子数据规范性较差、流通慢。由于业务数据量大、种类繁多，工作人员处理效率低下导致电子病历填写不规范、信息不真实、复制粘贴现象严重。据统计在医疗数据结构化问题中，有 30% ~50% 的信息是不真实的。另外电子数据内部信息流通不及时，造成部门之间的摩擦，进而推卸责任造成医患关系紧张。（2）电子数据安全性和隐私性受到威胁。在过去 10 年中，医疗卫生行业经历很多黑客攻击和数据泄露事件，使患者暴露于经济威胁、精神痛苦和可能的社会耻辱环境下。传统的电子数据模式极大地限制医疗企业更好、更快地发展，利用区块链进行去中心化和不可篡改的管理可以大大提高医疗服务效率，提升医疗服务质量。区块链技术有望在区块链 + 医疗数据库的构建上发挥重要作用。医疗区块链的应用价值与思路主要体现在 3 个方面：建立个人医疗健康数据库、打造智能化的医疗救助平台和构建开放的医疗健康资源共享互助中心。区块链技术在医疗领域的应用价值，见图 1。其有助于推动医疗信息化体系变革，加快医疗机构提升服务质量和提高服务效率。

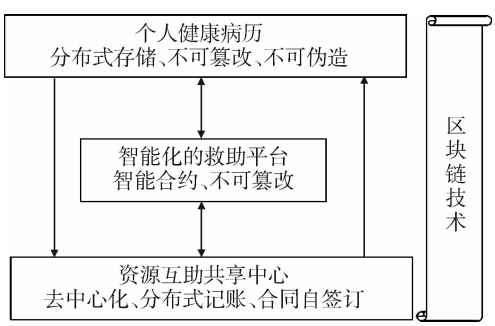

图 1 区块链在医疗领域的应用价值

3.2 建立个人健康数据库

基于区块链的分布式记录与储存、不可篡改、不可伪造等特性，建立结构化电子健康数据库。电子健康数据是患者数字化的记录，主要包括基本信息、病史记录、检查结果、疗程记录、用药说明、诊断效果等。区块链允许医疗机构、患者等跨平台、跨系统记录电子健康数据，区块链的去中心化结构能使医疗数据在每一个参与数据存储的网络节点进行实时更新，安全采集存储数据并在云服务器上永久保存，降低医疗数据及敏感信息的丢失风险，增加医疗数据的安全性及可信性。基于区块链技术的个人健康数据内容，见图 2。个人基本信息利用区块链技术的非对称加密算法使其进行加密隐藏，防止信息的泄露、丢失。健康信息应根据个人的意愿决定是否分享在某一网络中。对于个人而言，利用健康数据、体检信息查询个人的健康状况，系统会自动根据其医疗数据对其健康状况进行评分，得出个人健康状况等级评价。通过用药信息来查询药品的价格、数量等，查看药品价格是否与国家在某一地区标准的价格有差异，查看药品数量是否与治疗周期相符等。还可对医生的服务态度及治疗结果等进行评价。对于医生而言，利用健康数据库能更快了解患者的禁忌信息，获得仪器诊断结果。利用获得的数据，进行临床科研和案例分析提高医疗服务水平。对于医院及医疗研究机构而言，通过医疗数据库进行大数据分析挖掘，对医嘱、药物等进行合理监测。利用个人评价对医师进行绩效考评以及职称评定等。

个人健康数据

个人基本信息			
ID号	姓名	性别	出生日期
民族	籍贯	住址	…
健康信息			
历史信息		本次信息	
就诊信息	体检信息	禁忌信息	疗程记录
手术信息	禁忌信息	病况自述	用药信息
住院信息	…	病况描述	患者评价
恢复信息		检查结果	…

图 2 个人健康数据内容

3.3 打造智能化医疗救助平台

利用区块链的嵌入式智能合约可以自动形成医疗救助契约和凭证，构建智能化的医疗救助系统。系统中的每个人可以在医疗救助平台上注册并获得唯一的 ID 号，通过 ID 号登录系统来确认自动形成医疗救助契约后，允许医生访问医疗记录并实施救助。智能化的医疗救助系统过程，见图 3。当患者昏迷或无主观能动性时，医生可通过个人 ID 号来检索患者的 ID 号，然后医生在健康链数据网络中发布广播，广播会自动选择患者的紧急联系人并向其发送请求，

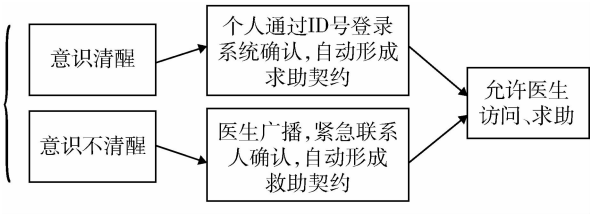

图 3 医疗救助系统过程

要求尽快确认允许医生访问患者的医疗记录。两名及以上紧急联系人确认并自动形成医疗救助契约后，医生可访问患者的医疗记录并实施紧急救助。当个人在医院外突发紧急情况时，可在医疗救助平台上发起医疗求助，平台根据定位自动向最近的医院发送救助信息，医院接受信息并自动形成救助契约后，对发起求助者进行最快、最有效的救助。

3.4 构建开放的医疗资源互助共享中心

通过区块链的去中心化的分布式账本技术，将医疗健康数据分布存放在不同的区块中，建立结构化电子病历数据，利用点对点的传播方式，将所有节点通过达成共识的、标准的软件协议共享医疗健康数据等资源。当患者被实施救助并且审查后，医生会询问患者是否愿意将医疗记录信息等相关资料匿名分享到公共研究库中，如果患者同意分享，将会获得一定金额的虚拟币，医生将根据患者患病类型、年龄、工作类型等特征进行标准匹配，将其加入到私人网络的共享中心。患者可以通过共享网络查看某类病症是否有良好的解决方案；当病症得到很好的治疗时，加入到健康资源共享中心可以与康复的病友对康复后的注意事项、药品以及生活保健方面等进行沟通交流；可以查阅在同一私人网络中已授权的其他人的个人健康信息等。否则可以通过“众筹”的方式进行捐款集资，使医疗研究组织可以并愿意研究此类病症。当有研究团队正在研究此病症，患者对研究团队进行“众筹”捐款时，网络就会自动签订合同并保存在第 3 方。合同签订后，治疗团队则根据患者的病症特点设计定制化的治疗方案，包括药物治疗以及其他的辅助治疗，研究团队（包括医生和保险公司）可以收集治疗者的活动手环、可检测的药物及治疗效果数据，保险公司根据患者完成治疗方案的情况进行奖励，所有账单自动支付，无需纸质通知。在同一家医院中不同科室的医生，可以通过个人 ID 号并进行同种类型医疗信息纵向查看和不同时间医疗信息横向查看，了解患者的病史记录、用药信息等。

4 存在的问题

4.1 对区块链存在质疑，推广运行存在阻力

目前区块链技术的研究主要聚焦在金融领域，在医疗领域该技术仍处于试点阶段。首先，在医疗领域的实践经验较少，很多医疗专家持观望态度。其次，医疗领域的特殊性以及去中心化属性对传统的医疗管理机构造成强烈冲击，在利益分配上对传统医疗管理部门造成巨大损失，导致相关部门和机构持谨慎态度。最后，医疗区块链中数据库领域的法律不健全，导致人们对其安全性、隐私性以及处理大数据时的抗压能力和可监管性存在质疑。以上种种原因严重阻碍了区块链在医疗领域的应用推广。

4.2 系统网络容量小，数据存储空间遇瓶颈

虽然区块链技术是互联网信息技术的一种创新，但其许多技术尤其是系统网络容量和数据存储空间目前还处于发展的初级阶段。区块链数据库记录每项事务的所有数据信息，任何进行数据存储的用户都需要下载并存储承载所有资源信息的创世块（Creation Block）。随着区块链技术在医疗领域的应用，个人、医生、医疗研究部门产生的数据量将会呈指数式增长，导致区块链中的区块所需存储空间呈现井喷式增长趋势。另外区块链数据库对网速的要求较高，数据保存在网络上较其保存在本地上慢。由于数据量越来越大，一方面导致数据存储空间受限，影响患者、医生以及医疗研究机构存储数据信息；另一方面将会降低数据传播效率，影响医生、患者对数据获取实时性的需求。

4.3 匿名技术尚未成熟，个人健康隐私保护有风险

区块链技术的隐私保护仅仅是通过隔绝交易 IP

地址的持有人和网络 IP 地址之间的关联，防止因交易信息公开而导致用户隐私泄露，但这样的保护并非完全匿名。随着各类反匿名技术的发展，实现部分重点交易持有人的真实信息可见性极为可能。医疗区块链技术将面临患者健康隐私泄露的风险，从两个方面可以看出：一是共享信息的透明度，任何共享的信息都可以跟踪查询，或对个人的状态、行为进行预测，不利于个人隐私的保护；二是区块链的安全性通过算法保障，理论上只有超过 51% 的节点用户同时被黑客攻破后数据信息才会被泄漏或篡改，但安全威胁仍然存在。

5 结语

目前区块链在医疗领域的应用还处于起步阶段，有专家预测称至少还需要 5 ~ 10 年区块链才能在医疗领域较为成熟地应用。虽然现在区块链技术的理论相对较为成熟，但技术方面还存在诸多缺陷。尽管区块链创新发展之路并非一帆风顺，但其创新的力量将会打破医疗卫生领域原有的格局，颠覆式的创新将会给医疗卫生领域带来跨越式的发展。

参考文献

1 比特币中文网（2017）. 苏州同济金融科技研究院首期区块链技术开发人才培训项目招生［EB/OL］.［2017 - 07 - 12］. http://www.bitecoin.com/online/2017/07/24283.html.

2 杨现民，李新，吴焕庆，等. 区块链技术在教育领域的应用模式与现实挑战［J］. 现代远程教育研究，2017，(2)：34 - 45.

3 比特币中文网（2017）. 青岛市北区区块链产业打造中国首条“链湾”［EB/OL］.［2017 - 07 - 12］. http://www.bitecoin.com/online/2017/07/24274.html.

4 Nakamoto S. Bitcoin: a peer - to - peer electronic cash system［EB/OL］.［2017 - 10 - 31］. http://akamotoinstiute.org/bitcoin/.

（上接第 8 页）

20 Natoli C, Gramoli V. The Blockchain Anomaly［C］//Pellegrini A, Gkoulalas - Divanis A, Di Sanzo P, et al. International Symposium on Network Computing and Applications. Piscataway: IEEE, 2016: 310 - 317.

21 Luu L, Narayanan V, Baweja K, et al. SCP: A Computationally - Scalable Byzantine Consensus Protocol For Blockchains［J］. IACR Cryptology ePrint Archive, 2015, 2015 (1): 1168.

22 Thaddeus Dryja Joseph Poon. The Bitcoin Lightning Network: Scalable off - chain Instant Payments［EB/OL］.［2016 - 11 - 20］. http://lightning.network/lightning - network - paper.pdf.

23 Malin B, Sweeney L. Sweeney, L. How (not) to Protect Genomic Data Privacy in a Distributed Network: using trail re - identification to evaluate and design anonymity protection systems［J］. Journal of Biomedical Informatics, 2004, 37 (3): 179 - 192.

24 Yue X, Wang H, Jin D, et al. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control［J］. Journal of Medical Systems, 2016, 40 (10): 1 - 8.