区块链在医疗行业的应用前景

黄建华 江亚慧 李忠诚 范 丽

（华东理工大学信息科学与工程学院 上海 200237）

〔摘要〕 介绍区块链技术的概念及其对医疗行业发展的影响，基于区块链去中心化、不可篡改和可追溯特性解决医疗数据管理、分享和隐私问题，指出区块链与医疗行业相结合存在的问题、面临的挑战以及可行的解决方案，对未来发展进行展望，以期为更好地支持医学研究和精准医疗提供参考。

〔关键词〕 区块链；医疗保健；电子病历；安全性；隐私

〔中图分类号〕R－056 〔文献标识码〕A 〔DOI〕10.3969/j.issn.1673－6036.2018.02.001

Application Prospect of Blockchain in Medical Industry *HUANG Jian－hua, JIANG Ya－hui, LI Zhong－cheng, FAN Li, School of Information Science and Engineering, East China University of Science and Technology, Shanghai 200237, China*

〔**Abstract**〕 The paper introduces the concept of blockchain and its impact on the development of medical industry, solves problems including medical data management, sharing and privacy based on decentralization, non－tampering and traceability of blockchain, points out problems and challenges confronting the combination of blockchain with medical industry, feasible solutions and outlooks into future development as well as providing reference for better support for medical studies and precision care.

〔**Keywords**〕 Blockchain; Medical care; Electronic Medical Records (EMR); Security; Privacy

1 引言

电子病历（Eletronic Medical Records，EMR）的广泛使用给医疗领域带来非常大的便利，使得数据的存储复制非常简单。但随着社会发展目前的电子病历系统已经无法满足人们的需求。首先现有体系下，患者的个人健康数据是由不同的医院或企业来进行管理的，患者的个人数据是分散的，数据难以交互，互操作性差，难以协调管理；其次，患者个人健康数据是有价值的，本质上归患者所有，但是管理数据的企业往往因为经济利益将这些数据占为己有，患者无法掌控和管理自己的个人医疗数据，无法对自己的数据进行访问控制、权限设定；最后，医疗数据的安全性和有效性完全依赖于企业，一旦企业的数据库遭受破坏，医疗数据就会损失，难以恢复，且企业很可能会为自身利益，泄露医疗数据，对患者隐私造成危害。显然，这种中心化的管理方式和分散的数据存储方式已经不是医疗行业的最佳选择。

区块链技术通过去中心化的方式维护一个可靠数据库[1]，是一个自带信任化、防篡改及能进行多签名复杂权限管理的分布式记录系统，利用区块链可以集成不同数据库中的医疗信息，实现互操作性、数据共享以及安全可靠存储数据，进行权限管理。本文介绍区块链技术在医疗保健领域的应用前景和可行的解决方案，指出区块链与医疗行业相结合面临的挑战以及应对措施，以期为医学研究和医疗行业的发展提供参考。

〔收稿日期〕 2017－07－20

〔作者简介〕 黄建华，副教授，博士，发表论文 40 篇。

2 区块链技术

2.1 区块链

2.1.1 结构 区块链是随着比特币[2]等数字加密货币的出现而逐渐兴起的一种全新的去中心化的分布式数据库。在区块链中，一段时间内生成的交易或数据信息被打包成一个区块，每个区块有自己的哈希标识，引用之前块的哈希，即每个新块按时间顺序连链到前一个块，这样就在区块间建立一种由后一块指向前一块的链式数据结构，见图 1。

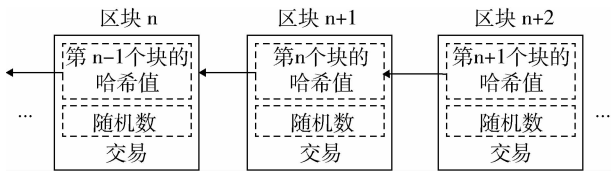

图 1 区块链的链式结构

目前大多数体系均被视为“一个中心”化的智能系统，如银行体系（央行是中心）和交易系统(交易所是中心)。中心化的特点是中心节点掌握分布节点信息，分节点不掌握其他节点信息，其不足是系统安全性取决于中心节点的安全性，分布节点对此没有控制权。而区块链建立的是一种去中心化的分布式共享账本，账本为全网所有结点所共享，通过将交易信息广播给全网节点进行共同验证，区块链排除第 3 方权威机构的必要。节点通过对交易的签名进行检验，就能够验证交易的有效性，且每个节点都存储有之前发生过的所有基于密码学体制建立的交易序列，也能够验证是否存在重复矛盾的交易，如比特币的双重支付。区块链通过分布式存储与全网验证来保证安全性，这种数据共享的机制可确保既使少数结点的崩溃也不会影响总账的完整性[3]。

2.1.2 共识机制 是区块链得以实现去中心化的核心，目前区块链主要使用工作量证明[4]（PoW）共识机制。区块链工作时每个节点都收集新的交易数据并试图根据这些交易生成新的区块，但只有一个节点生成的新区块为全网所接纳，以形成全网一致的区块链。PoW 解决这个问题的基本思路是寻找随机数（Nonce），该随机数要使得该给定区块的哈希值出现所需的多个 0，而找到这个解所需要的工作量与 0 的数目呈指数增长。每个节点都尝试找到这个具有足够难度的工作量证明，这个过程称为挖矿(Mining)。当一个节点找到一个工作量证明，它就向全网广播，其他节点验证成功后就接受该区块，然后跟随在该区块的末尾制造新的区块。想要更改该区块的信息，代价是需要重新完成之后所有区块的全部工作量。这样的设计使得区块链中的交易一旦被记录就难以篡改，且每笔交易信息都可追溯。

2.1.3 特点 与传统的中心化记账技术相比，区块链技术有以下特点：（1）不可篡改。数据一旦被添加到区块链上，就会形成永久记录，不可删除和篡改，保证数据的完整性，也保证交易双方对交易的不可抵赖。（2）去中心化。区块链使用分布式计算和存储，没有中心化的管理机构，数据的安全性和完整性由加入区块链网络的所有节点共同维护。（3）可追溯。区块链是一种带有时间戳的链式数据存储结构，链上的记录永久存在且不可篡改，这就使得链上的每笔交易信息都可追溯。（4）可靠性。区块链本质上是分布式数据库，当部分节点被攻击，数据遭受损坏，存储在其他节点的数据副本仍然完好无损，整体不受影响。（5）去信任。区块链中的节点是匿名的，节点之间无需相互信任，节点之间的数据交换遵循固定算法，运作公开透明。

2.2 智能合约

2.2.1 内涵 智能合约[5]可以追溯到 1994 年，由跨领域法律学者 Nick Szabo 提出。定义是：“一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议”。智能合约的工作理论迟迟没有实现的一个重要原因是缺乏能够支持可编程合约的数字系统和技术。区块链技术的出现解决该问题，区块链的去信任机制推动智能合约的发展。传统合约是指双方或者多方协议做或不做某事来换取某些东西，每一方必须信任彼此会履行义务；而智能合约无须彼此信任，因为智能合约不仅是由代码进行定义的，也是由代码强制执行的，完全自动且无法干预。

2.2.2 本质 智能合约的本质是编写在区块链上的一段代码，它可以实现一定的功能。比特币内置的脚本程序可以在一定的程度上实现“智能合约”，但是这套脚本语言有非常大的局限性，缺少图灵完备性，无法实现复杂的多阶段合约。为克服比特币脚本语言的局限性，支持更强大多功能的智能合约，出现一种全新开放的区块链平台——以太坊[6-7]，它提供图灵完备的编程语言以及编写平台，开发者可以在上面实现任意复杂的智能合约。

2.2.3 类型 在以太坊中，包括两种类型的账户，外部账户和合约账户。外部账户由用户控制，即由用户私钥控制，里面不含代码；合约账户包含智能合约代码，由代码控制，不能被用户控制，除非合约里指定可以由某个用户私钥控制，这样就保证智能合约照着既定的规则运行。一份智能合约被参与者签署后，会由一个外部账户将其发送到区块链中，经过网络中的节点验证之后永久保存在区块链中。智能合约由从其他合约账户或外部账户接收到的消息或交易触发，一旦触发，它会自动执行特定的代码片段，代码可以读写自己的内部存储，发送和接收存储消息和价值。智能合约也被称为第 2 代区块链技术，将区块链技术与智能合约技术结合，将在金融、保险、医疗保健、电子商务、物联网和社交通讯领域展示广阔的应用前景。

3 区块链与医疗行业

3.1 医疗保健存在的问题及区块链技术的应用

3.1.1 概述 在医疗系统中存在多个利益相关者，他们之间的关系错综复杂且相互作用比较敏感，整个系统的运营效率低下，当医疗数据为多方所用时，其安全性和隐私性难以保障。可信的数据管理和安全访问控制是至关重要的，如何高效简单低成本地完成上述目标是目前的一大挑战。利用区块链分布式总账的特性及自身固有的安全属性，可以为医疗领域的数据互操作性、安全性和隐私性提供解决方案，除此之外，区块链和智能合约的结合可以减少医疗行业的争议并加强监管，提高医疗行业运行效率，推动医疗服务的创新[8]。

3.1.2 互操作性、可访问性 当前体制下供应商不对信息互用性负责，数据孤岛和数据复杂性限制了数据的互操作和共享。利用区块链可聚合来自不同数据库的 EMR 数据，消除数据孤岛，推动医疗系统间的互操作，更好地支持医学研究和精准医疗。

3.1.3 隐私和安全 医疗数据可能会遭受黑客攻击，其机密性、完整性、可用性和不可否认性无法保障，对数据的访问控制缺乏有效的机制。区块链支持数据加密，可以强行执行权限设置，区块链本质是分布式数据库，数据冗余存储，可以提高完整性，促进可信数据之间的交换和去中心化。

3.1.4 医疗保健交付模型和费用 目前的医疗系统存在服务费与价值费不平衡、管理精算风险以及维护现有 EMR 开销过大等问题。利用区块链可以在整体上实现更好的风险管理，通过物联网实现价值费。

3.1.5 欺诈和滥用 目前医疗诈骗、代位求偿、药物滥用和虚报费用的问题比较突出，这也反映当前医疗行业问责制的不健全，对于医疗行为难以追溯。通过在区块链上编写智能合约可以减轻代位求偿，除此之外区块链的时间戳协议及其内容的不可篡改性使得医疗行为可追溯，促进问责制的健全，从而减少滥用和欺诈。

3.1.6 患者参与 目前医疗数据中心化的管理方式剥夺患者对数据具有拥有权，使得患者无法参与自身数据的管理。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。

3.1.7 采购和承包 医疗供应链存在太多中介机构，合同处理复杂，谈判效率低下。通过在区块链中编写智能合约可以减少中介机构并使得供应链合理化。

3.1.8 管理 医疗行业需要维护敏感数据隐私，满足安全的监管要求，服从当前法案规定。区块链允许数据供应商在不危及数据隐私、安全和完整性的情况下共享网络，可以管理患者记录生命周期和使医疗账单生命周期合理化。

3.2 区块链具体解决方案

3.2.1 使用区块链实现医疗数据的访问控制和权限许可 在医疗行业比较突出的问题是数据的互操作性和权限管理问题，为解决上述问题，麻省理工学院媒体实验室提出基于区块链的 MedRec 系统[9]。为实现数据权限管理，MedRec 提出 3 类智能合约，分别是登记合约（Registrar Contract，RC），患者 - 提供商关系合约（Patient - provider Relationship Contact，PPR），总结合约（Summary Contract，SC）。合约的结构和其相互关系，见图 2。

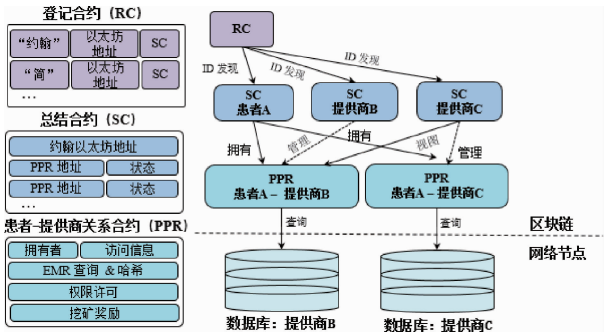

图 2 MedRec 在区块链上的智能合约

（1）登记合约。用于管理账户身份。区块链账户的身份信息都是由用户私钥生成的公钥作为身份，这可能与现有的 ID 形式不相符合，RC 就将用户真实身份和其以太坊账号做映射，合约中的编码可以允许新身份的注册及现有映射的改变。此外，RC 也将用户身份与相应的 SC 做映射。（2）患者 - 提供商关系合约。用于实现访问控制。患者的医疗记录可能会由不同的提供商进行管理，每个提供商也会管理不同患者的医疗数据，PPR 就是对提供商和患者一对一关系进行说明的合约，里面定义一系列数据指针和相关访问权限。通过数据指针可以访问到数据库中的数据，数据的访问权限主要通过数据库检索指令来约束，不同权限的人可使用的数据检索指令不相同。具体实现时会为患者设计一个简单的图形界面工具，由患者在此界面上对自身数据进行权限管理。（3）总结合约。用于管理用户和其所有 PPR 的映射。一个患者其所有的提供商都会为其制定 PPR，SC 拥有一张列表，里面存有 PPR 地址，只要访问患者的 SC，就可以链接到患者的 PPR，除此之外，SC 中还存有 PPR 的状态，用来表示该 PPR 中的权限是否被患者确认。MedRec 系统的工作流程，见图 3。

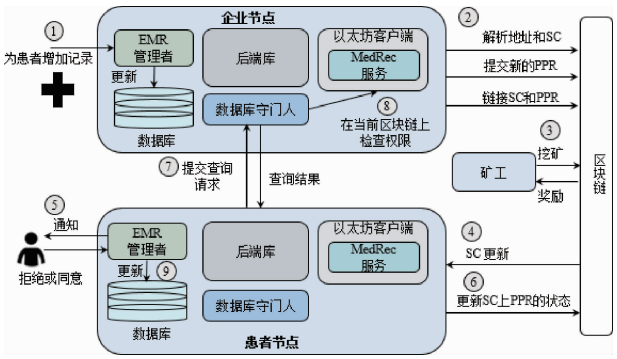

图 3 MedRec 系统的工作流程

MedRec 为一个新患者增添记录的步骤为：（1）提供商为一个新患者添加医疗记录到本地数据库。（2）MedRec 以太坊客户端使用 RC 识别患者身份信息，无法识别则为患者制定新的 RC 并链接到 SC，提供商为患者制定新的 PPR，将该 PPR 加入 SC 中，其状态处于待确认状态。这一步中 3 个合约都可能得到更新，提交到区块链等待验证。（3）矿工挖矿，对合约进行验证。（4）验证成功之后，SC 得到更新。（5）患者得到其医疗记录元数据已被写入区块链的通知后，对其数据权限进行管理，选择数据共享，更新相应的 PPR 与第 3 方地址和查询字符串。（6）更新 SC 中 PPR 的状态，表示权限已被患者确认。（7）、（8）、（9）是 MedRec 系统根据用户的身份来判断其是否有权访问患者数据。MedRec 系统在区块链上存储患者记录的索引，通过索引将不同数据库的数据集成，实现医疗数据的互操作性，同时通过在以太坊区块链上为用户编写智能合约，使得用户可以对自己的数据进行权限管理并在一定程度上保护用户数据隐私。

3.2.2 基于区块链的病历安全存储方法 在 MedRec 系统中，患者数据存在供应商自己的数据库中，区块链上并没有存储数据，而是通过智能合约中数据指针与供应商数据库相链接，所以它并不能保证供应商数据库的安全性。如果将数据存储在区块链上，将没有任何实体会掌握这些数据，各方需

协作负责维护数据的安全性和完整性，这为医疗提供了唯一的真实性来源，除此之外区块链通过对之前发生的任何变化创造永久的记录来保护在线健康档案，区块链上患者的历史医疗记录会形成永久的日志。要用区块链存储患者病历，相关文献[10]给出 3 种思路。第 1 种是 EMR 提供商在他们的 EMR 软件中实现一个区块链客户端，这样可以直接自动与区块链上的个人健康记录（Personal Health Records，PHR）通信，这是首选方案，但该方案需要 EMR 提供商的合作，需要监管或激励。第 2 种是 EMR 提供商通过现有的协议如 REST，SOAP 协议向 PHR 发送健康信息，PHR 根据标准来接收数据。这就意味着 PHR 将要兼容这些通信协议并进行配置以接收来自不同来源的文件，对于区块链系统这将是重量级的。第 3 种是患者通过现存的患者门户网站来接收他们的信息，然后转发或上传文件到区块链上的 PHR 中。但是如果患者不及时上传数据，可能会导致不完整的记录。基于区块链存储医疗数据为医疗数据安全存储提供了新的方向，但是短时间内由现有的 EMR 技术向区块链存储方式过渡的可行性比较低，因为庞大的医疗数据对于区块链来说是个巨大的存储负担。

3.2.3 大数据隐私问题 医疗行业对于数据隐私非常敏感，对于隐私保护有一套独特的法规要求，如美国的医疗服务行业必须遵守该国政府 1996 年颁布的《健康保险隐私及责任法案》（HIPAA）[11]，所以将区块链应用于医疗行业需要克服隐私保护方面的挑战。区块链是基于数学派生的假名进行分布式账本验证，HIPAA 规则禁止使用数学派生的假名，因为存在对去标识的受保护的健康信息重新识别的危险[12-13]。对使用数学派生的假名作为去身份信息的重新识别码这一限制使得区块链和 HIPAA 不兼容。Anonos 公司提出一种动态数据匿名方法，将区块链和动态匿名结合在一起来支持非数学派生的动态匿名标识符以解决 HIPAA 合规性问题，克服马赛克效应，实现细粒度的隐私控制。传统的静态匿名方法试图用单一的、不变的标识符来隐藏数据和数据主体之间的关联，但存在一定的安全隐患，攻击者只要收集到足够多的固定的数据，将其组合起来就会产生新的意义。这些数据单看都是安全不会暴露隐私的，攻击者将这些数据重新组合就可能发现数据主体及其对应的敏感信息。这就是马赛克效应。Anonos 提出动态匿名标识符[14]的概念，它是一个在一定时间内有效的假名，可以用来替换数据主体身份和其他一些可能会暴露数据主体的相关属性值，以掩盖数据主体身份和其数据之间的对应关系，达到隐私保护的目的。当区块链提供一个公开透明的交易记录时，如何保护用户隐私是个值得研究的问题，使用动态匿名方案可以在不同时间和不同地方，根据不同的目的向不同的人展示不同的数据信息，满足 HIPAA 的隐私要求。

3.3 展望

最新的 IBM 商业价值研究院区块链调研项目对 200 位医疗保健高管开展了调查，除此之外来自不同国家和地区的医疗支付者和提供者也参与其中。调研结果[15]表明，对于区块链技术，16% 的受访者不仅仅止于试用阶段，他们想成为区块链应用于医疗行业的开拓者，希望在 2017 年大规模采用商用区块链解决医疗行业现存的一些问题。预计在 2018－2020 年，56% 的医疗保健组织会成为区块链技术的大规模采用者，剩下的将会成为追随者，在 2020 年之后应用区块链技术。早期的合作者更有机会抓住新的合作伙伴，进而获得互补优势。如医疗保健巨头飞利浦公司（Philips）在 2015 年 10 月与区块链初创公司特瑞思达成合作[16]，于 2016 年 3 月宣布建立飞利浦区块链实验室；区块链技术提供商杰姆公司（Gem）正与医疗保健的多家公司展开合作，向医疗保健服务商提供网络基础设施，致力于构建一个全球化医疗保健综合体并为人们提供更加私人化以及更低费用的服务；还有区块链技术公司比特医疗（BitHealth）将区块链技术运用于医疗健康数据存储和保护，致力于存储和安全地在全球范围内传送医疗健康数据。这些开拓者无疑是非常有远见的，他们紧紧抓住机遇，积极推动区块链与医疗行业的结合。

4 挑战与应对措施

4.1 行业惯性

大的老牌公司拥有数据，但不和其他人（特别是患者和用户）共享[17]，能否将区块链充分应用到医疗行业很大一部分取决于提供商的意愿。患者的数据是有价值的，显然很多提供商是不愿意放弃对患者数据的掌握权。要让提供商积极参与区块链的使用，需要有某种激励机制鼓励提供商完成角色转换，由医疗数据管理者转换为区块链服务提供者，为医疗行业构建区块链公共基础设施或为患者编写智能合约等。为实现高比率的 EMR 采用，相关国家机构已经花费大量的财力物力构建 EMR 基础设施。以美国为例，美国医疗保险和医疗补助中心自 2011 年以来已经在 EMR 上花费 300 多亿美元，显然完全摒弃现有的医疗数据管理模式是不现实的[11]。目前各医疗机构都在持续改造原有的系统以及投资现有 EMR，区块链不需要医疗机构放弃当前的数据库，而是对当前数据库进行集成。

4.2 区块链本身存在一些待改进的地方

任何基于区块链的解决方案，性能是一个主要要考虑的技术性问题。具体实现中在区块链上处理大量的交易，时间和计算上的花费是非常昂贵的，这意味着性能和可扩展性需要从一开始就考虑进去。区块链技术目前使用的 PoW 共识机制存在固有的性能局限，性能可拓展性差，一致性确认有较长延迟[18]，无法满足高吞吐量的要求，也不能进行实时交易[19]，安全性也同样难以保证[20]。针对区块链吞吐量扩展性的不足，有文献[21]提出一种节点分区的方法，先通过 PoW 机制对参与一致性达成的节点进行过滤，防止恶意节点实行 Sybil 攻击[22]，根据节点算出的 nonce 值对节点进行分区划分，所形成的多个分区可以并行操作，各自对交易进行验证，这样就使得总的交易吞吐量与分区数规模近似呈线性比例增长。

4.3 医疗数据的隐私问题

隐私级别低的数据会存在 3 个缺陷。首先，对于数据所有者来说，没有隐私权可能会使其遭受潜在的歧视和伤害。以基因研究为例，通过收集研究基因数据，科学家可以推断出患者潜在的疾病从而能够为其量身定制治疗方法[23]。然而由滥用基因数据产生的危害是无法挽回的，基因信息的泄露对个人及其家庭特别是直系亲属会带来非常大的影响，这些影响包括心理障碍、就业歧视和拒绝提供人寿保险等。其次就大数据分析而言，数据没有隐私保护，其价值实际上会降低，因为没有过滤掉数据集中的任何信息，进行实际数据分析时会有太多干扰项。事实上经过隐私保护处理的一些数据往往不是分析者所需要的，如在分析研究患者医疗数据时，不需要知道患者的真实身份。最后根据相关信息安全规定和数据保护要求，数据处理者对数据有着潜在的责任，数据处理者可能会承担为数据泄露负责的风险。虽然数据匿名、数据库安全技术以及相关保护性法规能为数据提供基础性的安全保护，但是多种因素，包括形成的庞大数据库，数据不可避免的共享以及大量的访问量等都对数据隐私保护形成挑战。医疗数据需要共享以促进医学发展，但是对隐私问题极其敏感，数据发布时需要采用匿名技术来隐藏数据主体与数据之间的关系。除此之外，对于医疗数据的处理可以使用安全多方计算[24]，即在数据请求者看不见源数据的情况下，得到需要的结果数据。

5 结语

区块链可以显著地促进医疗信息的共享，创造安全、可信和便捷的医疗记录，具有高度的完整性和可信性。在医疗行业区块链技术将会创造一个连接医疗健康产业的新框架，将所有医疗平台的重要数据连接到一起，从而解决数据互操作性问题。此外，区块链保证了数据的有效性和安全性，使得医院、保险公司和实验室能够实现连接并且及时无缝分享信息，而无需担心信息被泄露或者被篡改。通过在区块链上编写智能合约，可以对患者数据进行访问控制，保证患者对自己数据的所有权，在一定程度上保护患者隐私。从区块链采用角度来看，医疗保健组织发展速度较快，其势头甚至有超过金融行业的迹象。大多数的医疗保健组织都认为区块链

可以显著降低运营相关时间、成本和风险。未来，区块链可以为医疗行业临床试验记录、监管合规性、医疗/健康记录等 9 个核心业务带来令人信服的收益[15]。将区块链应用于医疗行业，需要拓展新的业务和制定技术标准，除此之外医疗数据的安全和隐私需要相关法律法规的保护，监管机构可以和医疗保健机构合作，利用区块链执行监管法规。区块链可为医疗行业带来的另一大变革是促进医疗服务向以患者为中心转变，在物联网及认知分析等技术的协同作用下，全新的远程医疗护理、按需服务和精准医疗将成为可能。

参考文献

1 张亚娇，王枞. 区块链技术在医疗数据安全存储中的应用［EB/OL］.［2016 - 12 - 27］. http://www.paper.edu.cn/releasepaper/content/201612 - 553.

2 Zohar A. Bitcoin: under the hood［J］. Communications of the ACM, 2015, 58 (9): 104 - 113.

3 Kumar A, Tandon R, Clancy T. On the Latency and Energy Efficiency of Distributed Storage Systems［J］. IEEE Transactions on Cloud Computing, 2017, 5 (2): 221 - 233.

4 Kraft D. Difficulty Control for Blockchain - based Consensus Systems［J］. Peer - to - Peer Networking and Applications, 2015, 9 (2): 397 - 413.

5 Delmolino K, Arnett M, Kosba A, et al. Step by Step Towards Creating a Safe Smart Contract: Lessons and Insights from a Cryptocurrency Lab［M］. Berlin: Springer, 2016: 79 - 94.

6 Vitalik Butterin. A Next - generation Smart Contract and Decentralized Application Platform［EB/OL］.［2014 - 07 - 23］. http://blog.lavoiedubitcoin.info/public/Bibliotheque/EthereumWhitePaper.pdf.

7 Delmolino K, Arnett M, Kosba A, et al. A Programmer's Guide to Ethereum and Serpent［EB/OL］.［2016 - 05 - 06］. https://mc2 - umd.github.io/ethereumlab/docs/serpent_tutorial.pdf.

8 IBM Global Business Services Public Sector Team. Blockchain: The Chain of Trust and its Potential to Transform Healthcare - Our Point ofView［EB/OL］.［2016 - 08 - 08］. https://www.healthit.gov/sites/default/files/8 - 31 - blockchain - ibm_ideation - challenge_aug8.pdf.

9 Azaria A, Ekblaw A, Vieira T, et al. MedRec: Using Blockchain for Medical Data Access and Permission Management［C］// Irfan Awan Muhammad Younas. International Conference on Open and Big Data. Piscataway: IEEE, 2016: 25 - 30.

10 Drew Ivan. Moving Toward a Blockchain - based Method for the Secure Storage of Patient Records［EB/OL］.［2016 - 08 - 02］. https://www.healthit.gov/sites/default/files/9 - 16 - drew_ivan_20160804_blockchain_for_healthcare_final.pdf.

11 United States Department of Health and Human Services. Health Insurance Portability and Accountability Act of 1996［S/OL］.［2016 - 07 - 28］. https://aspe.hhs.gov/report/health - insurance - portability - and - accountability - act - 1996.

12 Kimberly Shutters. Protected Health Information - What is it?［EB/OL］.［2016 - 08 - 11］. https://www.linkedin.com/pulse/protected - health - information - what - kimberly - shutters - bcs - cmrs.

13 Gary LaFever. Blockchain and Big Data Privacy in Healthcare［EB/OL］.［2016 - 05 - 02］. https://iapp.org/news/a/blockchain - and - big - data - privacy - in - healthcare/.

14 Ted Myerson, et al. Dynamic Data Obscurity Supported by Anonos Dynamic Anonymity［EB/OL］.［2016 - 10 - 15］. https://www.slideshare.net/TedMyerson/anonos - dynamic - data - obscurity - october - 2014.

15 IBM Institute for Business Value. Healthcare rallies for blockchains: Keeping patients at the center［EB/OL］.［2016 - 12 - 09］. https://www - 01.ibm.com/common/ssi/cgi - bin/ssialias? htmlfid = GBE03790USEN.

16 Sambuaj Das. Philips Looks to Bring Blockchain Technology to Healthcare［EB/OL］.［2016 - 10 - 27］. https://www.cryptocoinsnews.com/philips - looks - to - bring - blockchain - technology - to - healthcare - 2/.

17 Mike Miliard. Blockkchain's Potential Use Cases for Healthcare: hype or reality［EB/OL］.［2017 - 02 - 22］. http://www.healthcareitnews.com/news/blockchains - potential - use - cases - healthcare - hype - or - reality.

18 Vukolic M. The Quest for Scalable Blockchain Fabric: Proof - of - Work vs. BFT Replication［M］. Berlin: Springer, 2015: 112 - 125.

19 Mccorry P, Möser M, Shahandasti S F, et al. Towards Bitcoin Payment Networks［M］. Berlin: Springer, 2016: 57 - 76.

（下转第 13 页）

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.