Journal of Computer Applications
计算机应用,2020,40(1):157-161
ISSN 1001-9081
CODEN JYIIDU
2020-01-10
http://www.joca.cn

文章编号:1001-9081(2020)01-0157-05
DOI:10.11772/j.issn.1001-9081.2019060994

基于区块链的电子医疗病历共享方案

罗文俊,闻胜莲,程　雨
(重庆邮电大学 计算机科学与技术学院,重庆 400065)
(* 通信作者电子邮箱 906045083@qq.com)

摘　要: 针对当前各医疗相关机构间数据共享困难、数据隐私易泄露等问题,提出了一个基于区块链的电子医疗病历(EHR)共享方案。首先,基于区块链不可篡改、去中心化、分布式存储的特点,设计了基于区块链的EHR数据共享模型,采用区块链网络和分布式数据库共同存储加密的EHR及相关访问控制策略,防止EHR数据被篡改和泄露;其次,将分布式密钥生成(DKG)技术与基于身份的代理重加密(IBPRE)技术相结合,设计了数据安全共享协议,协议使用委托权益证明(DPOS)算法选取代理节点,重加密EHR,实现单对用户间的数据共享。安全性分析表明,所提方案能够抵抗身份伪装和重放攻击。仿真实验与对比分析表明,DPOS算法的效率高于工作量证明(POW)算法,略低于实用拜占庭容错(PBFT)算法,但所提方案去中心化程度更高,耗费算力较小。

关键词: 电子医疗病历;区块链;基于身份的代理重加密;分布式密钥生成;数据共享
中图分类号: TP309.2　　**文献标志码:** A

Blockchain-based electronic health record sharing scheme

LUO Wenjun, WEN Shenglian, CHENG Yu
(*College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: To solve the problems such as data sharing difficulty, data privacy disclosure of data sharing between medical institutions, a blockchain-based Electronic Health Record (EHR) sharing scheme was proposed. Firstly, based on the blockchain characteristics of non-tampering, decentralization and distributed storage, a blockchain-based EHR data sharing model was designed. The blockchain network and distributed database were used to jointly store the encrypted EHR and the related access control policies, preventing the modification and leakage of EHR data. Secondly, the Distributed Key Generation (DKG) and Identity-Based Proxy Re-Encryption (IBPRE) were combined to design a data secure sharing protocol. The Delegated Proof of Stake (DPOS) algorithm was used in this protocol to select the proxy node, which re-encrypted the EHR to achieve the data sharing between single pair of users. The safety analyses show that the proposed scheme can resist the fake identity and the replay attack. Simulation experiments and comparative analyses show that DPOS algorithm has the efficiency higher than Proof of Work (POW) algorithm, and slightly lower than the Practical Byzantine Fault Tolerance (PBFT) algorithm, but the proposed scheme is more decentralized and costs less computing power.

Key words: Electronic Health Record (EHR); blockchain; Identity-Based Proxy Re-Encryption (IBPRE); Distributed Key Generation (DKG); data sharing

0　引言

随着医疗行业的飞速发展、医疗健康数据的急剧增多,许多医院开始使用电子医疗病历(Electronic Health Record,EHR)[1]记录病患的医疗健康数据。使用电子医疗病历的好处也有许多,例如:为医疗数据提供了便利的存储方式、为医生开处方提供了数据来源、为研究机构提供了研究数据等。通常,病人在一个医院就医后就会产生自己的电子医疗病历,当该病人到另一家医院就医时,往往需要该病人之前的一些就诊记录或医疗数据,这时就要在不同的医疗机构间共享电子医疗病历。

由于医疗数据类型繁多,如何对其进行合理的整合存储,以及如何进行有效的共享,始终是一个研究热点;同时,电子医疗病历包含病患的许多隐私信息,在共享时如何防止隐私数据的泄露,这也是一个研究难题。

云计算[2-3]的发展为电子医疗病历的共享提供了一个好的方法。通常医院会将电子医疗病历外包给云服务器,当其他的用户想要获取云上的某些医疗病历时,需要经过云的验证,验证通过后云才会将数据共享给该用户;但是基于云的电子医疗病历共享方案[4-5]也有一个弊端:数据存储中心化。这也就意味着,所有的医疗数据都集中存储在云上,一旦云服务器被恶意攻破,那么云上存储的医疗数据将会泄露,从而造成用户的隐私泄露等一系列问题,由此引发的后果十分严重。

区块链技术[6-8]的发展与应用为解决这一问题带来了新机遇。2008年,中本聪发表了论文"Bitcoin: A peer-to-peer electronic cash system"[9],论文中提到了基于比特币的区块链技术,此项技术一经提出立马引起了广泛关注。区块链技术具有去中心化和分布式存储、不可篡改等优点,可提供更高的安全性。基于该技术的优点,逐渐有研究人员开始使用区块链技术构建电子医疗病历共享系统[10-13]。Xia等[14]提出了

收稿日期:2019-06-12;修回日期:2019-09-01;录用日期:2019-09-12。　基金项目:国家自然科学基金资助项目(61672004,61702067)。
作者简介:罗文俊(1966—),男,重庆合川人,教授,博士,主要研究方向:网络空间安全、密码学;　闻胜莲(1995—),女,重庆荣昌人,硕士研究生,主要研究方向:区块链、密码学;　程雨(1995—),男,山西朔州人,硕士研究生,主要研究方向:区块链。

一个基于区块链的医疗数据共享模型——MeDShare，系统中使用区块链存储医疗数据包，利用智能合约跟踪对数据的所有操作，一旦监测到恶意行为时，可以及时撤销对数据的访问权限；根据访问权限，对数据请求者身份的合法性进行验证，通过验证后再实现数据安全共享，防止数据隐私泄露。Fan 等[15]提出了 MedBlock 方案，方案利用区块链的分布式账本实现有效的电子病历（Electronic Medical Record，EMR）访问和检索，在授权用户之间共享电子病历。方案中使用了加密策略，确保信息的安全性和隐私性，同时降低了成本；由于方案对共识机制进行改进，所以有效地提高了区块共识的效率。此外，Zhang 等[16]提出了一种基于区块链的个人健康记录共享方案；该方案构建了两种不同的区块链来实现医疗数据的安全共享，方案分别构建了私链和联盟链，私链实现个人医疗数据的加密存储，联盟链保存个人医疗数据对应的安全索引，通过验证医生的身份令牌进行数据安全共享，很好地保护了医疗数据隐私；但是利用两种类型的区块链不仅会增加成本，其执行效率也会降低。

在本文中，提出了一个基于区块链的电子医疗病历安全共享方案，本文方案在文献[17]中提出的模型上进行了改进，并设计了数据安全共享协议，协议将分布式密钥生成（Distributed Key Generation，DKG）技术[18-19]和基于身份的代理重加密（Identity-Based Proxy Re-Encryption，IBPRE）方案[20]相结合。与传统的基于身份的加密方案相比，本文方案不用 PKG 生成主密钥，而是采用 DKG 技术，让每个机构用户共同协商生成私钥，不仅防止了 PKG 被恶意攻破时，各机构的私钥泄露的问题，还有效抵抗了用户间的合谋攻击。方案采用 IBPRE 技术，在保证 EHR 的保密性、完整性和隐私性的基础上，实现了单对用户间的加密数据共享。

1 相关知识

1.1 代理重加密

代理重加密是一种可以在密文间使用的转换机制，最初由 Balze 等[21]提出。使用代理重加密的目的是解决用户共享数据时的不便，在减轻用户负担的同时，还可以增强数据的可靠性和安全性。在代理重加密的过程中，每个参与者都无法获取任何明文消息。其具体工作过程涉及到三种角色：数据拥有者、数据用户和代理者。当数据所有者 Alice 想要将已加密的文件共享给数据用户 Bob 时，Alice 为 Bob 生成代理重加密密钥，并将代理密钥通过安全信道传送给第三方的半可信代理者，半可信代理者用代理密钥根据代理重加密算法对加密文件进行重加密，Bob 获取重加密的文件后，可利用自己的私钥对重加密文件解密，解密后可获取明文文件。

1.2 区块链技术

区块链技术是一种特定的数据结构，这种数据结构按照时间顺序将数据区块组合成链条，当前区块通常由前一个区块的哈希值、有效负载、贡献签名和时间戳等组成，以此来保证其不可篡改性和不可伪造性；区块链也是一种去中心化的分布式数据库，传统的分布式数据库只有一个中心服务器维护数据，而区块链不一样，它由区块链网络中的所有节点共同维护数据，每一个节点都会对数据进行备份。如果单个节点上的数据被篡改或破坏，也不会对区块链存储的数据产生影响，除非有 51% 的节点都被篡改，那么区块链上存储的数据才会被篡改成功。区块链网络包含两种重要实体，分别是矿工和验证者。矿工指为区块链生成新区块的节点，不同的应用场景中可以定义不同的节点为矿工。在比特币区块链中，只有提供工作证明的矿工节点能够保存交易记录，而验证者则会在验证矿工提交的区块后，生成新区块。

2 本文方案

2.1 基于区块链的电子医疗病历共享模型

本文方案的模型对文献[17]进行了改进，如图 1 所示，该模型主要由 4 种角色组成，分别是 N 个权威中心、数据拥有者、数据用户、代理者。其中，N 个权威中心是本文新增加的角色，其余角色是原模型中本就包含的。区块链节点由一个联盟组织内的医院、银行、保险公司、研究所等构成，每一个节点可以至少扮演一种角色。模型采用分布式数据库和区块链共同存储医疗数据：数据库存储加密的 EHR，区块链存储 EHR 的对应访问控制策略、其在数据库上的存储地址和 EHR 的数据哈希。采用这种存储模式既解决了数据集中存储在各医疗机构的数据库中的问题，同时也减轻了区块链上的数据存储和高频访问的压力。

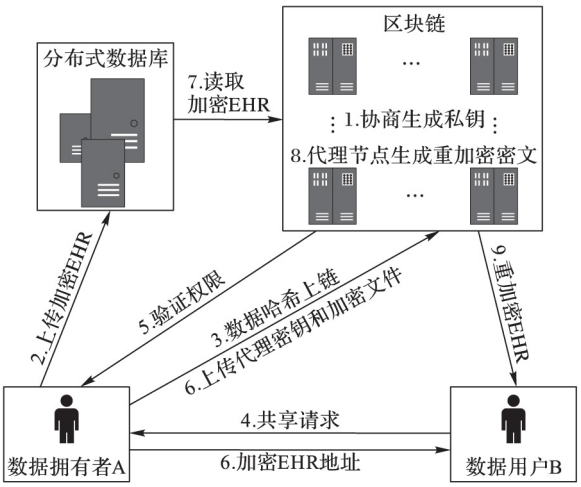

图 1 基于区块链的电子医疗病历共享模型

Fig. 1 Blockchain-based electronic health record sharing model

1) N 个权威中心。N 个权威中心分别代表联盟链内不同的医疗相关机构，例如：医院、研究所、银行、保险公司等。各权威中心可自己生成一部分秘密，然后根据各自的身份信息协商出每个机构的私钥。

2) 数据拥有者。数据拥有者拥有自己的 EHR，可以将 EHR 分享给其他机构。数据拥有者将原始的医疗数据加密存储在分布式数据库中并且将该医疗记录的 hash 值、存储地址、访问控制策略存储到区块链，以防止数据被恶意篡改。在数据共享的过程中，数据拥有者需生成代理重加密密钥并将该密钥分发给代理节点。

3) 数据用户。数据用户可从数据所有者处获取 EHR，授权数据用户可通过发送验证请求来获取重新加密的 EHR，也可使用自己的私钥来解密重加密后的 EHR。

4) 代理者。根据委托权益证明（Delegated Proof Of Stake，DPOS）共识算法[23]所推举出来的矿工节点作为代理节点。该代理执行重加密算法重新加密 EHR。具体而言，代理节点根据来自数据所有者的重加密密钥来重新加密 EHR。

2.2 基于区块链的电子医疗病历共享协议

根据本文方案的模型，本文采用一种多中心的基于身份

的代理重加密方案作为数据共享协议。协议根据 Matthew Green 提出的 IBPRE 方案进行改进。在 Matthew Green 的方案中,用户私钥是由 PKG(Private Key Generation) 产生的主密钥生成,但是这里存在一个问题: 如果 PKG 的真实性无法信任或 PKG 被恶意攻击,那么主密钥就有可能泄露,从而泄露用户的私钥。为了提高用户密钥生成的安全性,本文方案对 IBPRE 方案的密钥生成部分采用 DKG 技术进行优化,用 DKG 以后,每一个用户的私钥都根据其余用户的秘密值协商生成,即使单个用户被恶意攻击也能保证密钥的安全性。具体的数据共享协议由以下 5 个步骤组成: 系统初始化,密钥生成,数据存储,数据共享,数据恢复。

1) 系统初始化。系统服务器选择安全参数 λ,输入系统安全参数后,输出系统公共参数。首先,选取双线性映射 $e: G_1 \times G_1 \rightarrow G_T$,其中,$G_1$ 的生成元是 g,G_T 的阶为 q。令哈希函数 $H_1: \{0,1\}^* \rightarrow G_1$,$H_2: G_T \rightarrow G_1$。令 N 代表系统中所有权威的个数,所以系统公共参数为 $params = (G_1, G_T, e, g, H_1, H_2, N)$。公布系统公共参数后,每个权威中心需要设置自己的多项式算法并且输入该算法,然后利用 DKG 生成主密钥。其具体步骤如下: 首先,每个权威中心 $A_i(i = 1,2,\cdots,N)$ 在 Z_q^* 上随机选择一个多项式 $f_i(x) = a_{i0} + a_{i1}x + \cdots + a_{i(N-1)}x^{N-1}$,$a_i = f_i(0)$。接着,每一个中心 A_i 计算并广播 $B_{ik} = g^{a_{ik}} \pmod q$ $(k = 0,1,\cdots,N-1)$,同时,每一个 A_i 向系统中的其余权威 A_j 发送秘密值 $s_{ij} = f_i(j)$。然后,每一个权威中心 A_i 收到 s_{ji} 后检查等式 $g^{s_{ji}} \stackrel{?}{=} \prod_{k=0}^{N-1} (B_{jk})^{ik} \pmod q$ 是否成立,如果等式成立,则代表从发过来的秘密值是有效的; 反之,则秘密无效,那么 A_i 返回给 A_j 一个错误提示。如果权威 A_j 是错误的,那么它需要广播新 s_{ij} 的满足等式,如果等式仍然不满足,则重新发送 s_{ij} 直到满足等式。最后,N 个权威建立其主密钥 $s = \sum_{i=1}^{N} a_{i0} \pmod q$,主公钥为 $y = \prod_{i=1}^{N} g^{a_{i0}} = g^{\sum_{i=1}^{N} a_{i0}} = g^s$。

2) 密钥生成。每个权威根据输入的参数和身份标志 id_i,返回其私钥 $sk_{id_i} = H_1(id_i)^s$。

3) 数据存储。当患者在医院治疗后,医院会生成该患者的 EHR。对于 EHR,医院首先用自己的公钥 sk_{id_i} 加密该 EHR,根据其身份 id_i 和明文 EHR,在 Z_q^* 上随机选取 r,得到加密后的 EHR 密文 $c_{id_i} = (g^r, m \cdot e(g^s, H_1(id_i))^r)$ (这里也将称为第一层密文) ,再将 c_{id_i} 存储在分布式数据库上。然后,医院作为数据拥有者对原始的 EHR 签名,并将签名的 EHR、EHR 的 hash、存储位置和访问控制策略等作为文件写入交易,然后将交易进行广播。经由矿工验证交易且验证通过后将该交易写入区块链。

4) 数据共享。当某一用户想读取某医院的某一份 EHR 时,该用户首先需要发送签名请求给医院,医院首先通过该请求消息验证用户的身份是否合法,其次检查该文件的访问控制策略,如果用户身份合法且拥有读取权限,那么医院将会利用用户的身份 id_j 及自己的私钥 sk_{id_i} 生成代理重加密密钥 $rk_{id_i \rightarrow id_j} = \langle g^r, X \cdot e(g^s, H_1(id_j))^r, sk_{id_i}^{-1} \cdot H_2(X) \rangle$(其中 s 是在 G_T 上随机选取的值) 。此后,医院会将代理密钥、EHR 的存储地址传送给代理节点,代理节点根据存储地址读取分布式数据库上存储的加密 EHR 文件。接着,代理节点利用代理重加密密钥 $rk_{id_i \rightarrow id_j}$ 对加密的 EHR 进行重加密计算,得到重加密密文 $c_{id_j} = \langle c_1, (c_2 \cdot e(c_1, R_3)), R_1, R_2 \rangle$(重加密密文也叫第二层密文) 。最后,代理节点将重加密后的 EHR 密文 c_{id_j} 发送给用户。

5) 数据恢复。当用户接收到重加密后的 EHR 时,可使用自己的私钥 sk_{id_j} 对重加密密文进行解密,解密后就可获取 EHR 明文文件 M。其第一层密文解密过程如下: 首先用户计算 $X_j = Decrypt(sk_{id_j}, (c_3, c_4)) = c_4 / e(c_3, sk_{id_j})$,然后计算 $X_i = c_2 / e(c_1, H_2(X_j))$,计算所得的 X_i 即为 EHR 明文文件 M。

3　分析与评估

3.1　正确性分析

3.1.1　用户私钥的正确性

本文提出的方案和其他的基于身份的加密方案[23-24]类似,都是先产生主密钥,再根据主密钥生成用户私钥。在这些方案中,需要一个可信第三方权威(例如 PKG) 来保护主密钥并生成用户私钥; 但是在本文方案的模型中没有可信第三方,所以采用文献[8-19]中的 DKG 技术来实现没有可信第三方时的密钥生成,用户私钥生成的正确性可以由 DKG 技术来保证。

3.1.2　密文的正确性

在本文方案中,需要验证两层密文的正确性,即加密密文的正确性和重加密密文的正确性。首先,第一层密文 m 经过用户 id_i 加密后得到密文 $c_{id_i} = (g^r, m \cdot e(g^s, H_1(id_i))^r)$,其用户私钥为 $sk_{id_i} = (H_1(id_i)^s)$,通过如下等式来验证其正确性: $(m \cdot e(g^s, H_1(id_i))^r) / e(g^r, H_1(id_i)^s) = m$。

在重加密过程中,重加密密文 $c_{id_j} = \langle c_1, (c_2 \cdot e(c_1, R_3)), R_1, R_2 \rangle$,重加密密文是由重加密密钥对第一层密文 c_{id_i} 计算得到的。经计算后,可得 $c_{id_j} = (g^r, m \cdot e(g, H_2(X))^r, R_1, R_2)$,给出解密密钥 $sk_{id_j} = H_1(id_j)^s$,可以解密第二层密文 c_{id_j}。

将此解密过程分为两部分,首先将重加密密文的后两部分 $c_{id_j}' = \langle R_1, R_2 \rangle$ 看作用户在私钥 sk_{id_j} 下加密的单层密文,然后根据单层密文解密过程对其进行解密,计算可得到 $X = Decrypt(params, sk_{id_j}, c_{id_j}') = R_2 / e(R_1, sk_{id_j})$,再使用得到的 X 对重加密密文的前两部分继续进行解密,计算 $m \cdot e(g, H_2(X))^r / e(g^r, H_2(X))$ 可获取明文。

综上所述,本文提出的协议是正确的。

3.2　安全性分析

本文的模型和协议共同保证了数据的安全性和隐私性。

首先,从方案所提出的模型上来讲: 模型使用分布式数据库保存加密的 EHR,这保证了即使加密数据泄露,在没有数据拥有者的私钥的情况下,加密数据也无法被攻击者解密从而获取明文内容。此外,模型使用区块链存储数据的 hash、存储地址和访问控制策略,根据区块链自身可防篡改的特性,极大地提高了数据的安全性和隐私性。具体而言,由于区块链本身包含许多个节点,一旦数据被写入区块链,那么每个节点都会备份该数据,所以除非发生 51% 攻击,否则区块链上的数据是无法被篡改的; 即便最后发生了 51% 攻击,由于区块链上并未存储原始的 EHR,这种篡改对 EHR 的元数据也并不会产生影响。

其次,从方案所提出的协议上来讲: 本文采用的基于身份的代理重加密协议由于经过了优化改进,其用户私钥生成部

分不再依靠 PKG 来生成，而是每一个机构用户自己选择多项式生成秘密值，再由秘密值来生成自己的私钥，相比 PKG 这种密钥集中生成的办法，分布式密钥生成法可以有效地防止私钥泄露的问题，其安全性在于：即使单个用户遭受到恶意攻击，攻击者也无法获取该用户的秘密值，更无法获取其私钥，那么利用用户公钥加密存储在分布式数据库的 EHR 也无法被攻击者利用其私钥解获。如果遭受恶意攻击的是多个用户，或者多个用户进行合谋攻击，也无法获取私钥，因为协议中会对每一个用户发过来的秘密值进行检验，检验不成功是无法生成私钥的。由此得出，用户的私钥是安全的，且不易被恶意攻击造成私钥泄露。

在用户私钥生成以后，假设某一个数据用户想要获取 EHR 的明文内容，首先需要满足访问控制策略，其次需要解密 EHR 密文。将协议剩下的步骤分为两个阶段，如下所示。

阶段一　数据用户 B 首先发送含有自己签名的请求给数据拥有者 A，数据拥有者查看该用户对应的访问策略，确认有读取权限后再生成代理密钥并发给代理者 S，同时也将加密数据存储的地址发给代理者。在此阶段，假设数据拥有者是可信的，且数据用户从未将自己的身份凭证暴露给其他人，攻击者 C 无法恢复密钥，可以设想攻击者的不同攻击情况：

1）情况一。C 发送给 A 一个请求，试图获取加密数据，由于 C 没有用户的身份凭证，那么 A 接收到 C 的请求后，查看不到对应 C 的访问控制策略，那么就不会执行接下来的协议步骤，C 攻击不成功。

2）情况二。允许攻击者 C 拦截用户 B 发送给 A 的请求消息并执行重放攻击。假设 C 可以成功欺骗 A，这导致 A 将 C 视为 B，那么 A 可以查询到 B 的相应访问控制策略，如果 B 有读取权限，A 会生成针对 B 的代理密钥，然后发送代理密钥和请求数据的地址给代理者，代理者正常执行余下步骤后，再将重加密的密文发送给 C，但这段密文对 C 来说仍是无法解密的，因为该密文是用针对 B 的代理密钥加密生成的。

总之，协议的第一阶段能有效抵抗身份伪装和重放攻击。

阶段二　代理者接收到数据拥有者发送的重加密密文和加密数据的存储地址后，代理者再根据协议下载加密数据并重加密该数据密文，然后将重加密密文发送给用户。在重加密过程中，仍然假设数据拥有者是可信的，同时数据用户的身份凭证从未暴露给其他人，代理者是半可信的，即代理者对存储的 EHR 文件感兴趣，并且尝试获取文件内容从而获得好处，但是会按照协议规定执行协议的每一步，不会中途退出协议也不会提供虚假数据，那么代理者尝试获取 EHR 明文的方式有两种：方法一，根据数据拥有者的私钥直接对第一层密文解密；方法二，对加密文件进行重加密，重加密后利用数据用户的私钥解密密文。对于方法一，由于数据拥有者可信，其身份凭证也未暴露，根据分布式密钥生成的数据拥有者的私钥无法被代理者获取，那么代理者在获取到第一层密文文件时无法使用私钥解密文件，即代理者不能通过此方法获取 EHR 明文。对于方法二，假设代理者通过代理密钥将密文重加密，然后得到重加密密文，那么此时要获取 EHR 明文，代理者需要获得数据用户的私钥才能解密第二层密文。与方法一同理，由于数据用户的身份凭证未暴露，且其私钥是根据分布式密钥生成法生成的，代理者无法获取数据用户的私钥，那么代理者也无法解密第二层密文来获取 EHR 明文。总之，虽然代理者是半可信的，但是这也不会影响方案的安全性，也不会影响数据用户获取 EHR 的真实性。

3.3　评估

由于目前医疗信息化存在一些问题，现列举这些问题，并分析了本文方案中针对这些问题所提出的解决措施：

1）隐私和安全问题。本文方案采用非对称加密技术加密数据，可以保证隐私数据不会受到威胁。将医疗相关数据的 hash 存储在区块链，保证医疗数据的不可篡改性，也保证其不可抵赖性。

2）数据可访问性、操作性和完整性问题。本文方案采用分布式数据库存储加密数据，并将原始数据哈希、访问权限存入区块链，方便检测各机构的不同权限，实现各机构间的数据共享，保证数据可访问性和操作性。由于区块链具有分布式数据库的特性，数据在每一个节点上都有备份，可有效防止数据丢失，以保证其完整性。

此外，本文采用对照分析的方法来评估所提出的电子医疗病历共享方案。由于本文方案是基于区块链的，且是为了解决医疗数据共享问题所提出的，与文献[12]、文献[17]、文献[25]所提出的方案属于同类型的医疗区块链方案，所以将本文方案与以上三种方案对比，从各方案所采用的共识机制、区块链类型、算力需求等几方面着手，能够有效对比出本文方案的优缺点，结果如表1所示。

表1　不同方案的优缺点对比

Tab. 1　Comparison of advantages and disadvantages of different schemes

方案	共识机制	单链	算力需求	链类型
文献[12]方案	PBFT	否	小	私链、联盟链
文献[17]方案	POW	是	大	联盟链
文献[25]方案	POW	是	大	联盟链
本文方案	DPOS	是	小	联盟链

由表1的对比可知，本文方案使用 DPOS 算法作为共识机制，相对于文献[17]和文献[25]使用的 POW 算法，本文方案所需要启动的节点数相对更少，且不需要花费大量的算力去维护区块链；虽然文献[12]需要耗费的算力也较小，但是该方案方案涉及到两种类型的区块链，分别是联盟链和私有链，两种类型的区块链要进行维护肯定耗费的成本更高，同时，私链的去中心化程度不如联盟链。

为了比较三种共识算法的效率，将三种共识算法进行仿真，通过对实验数据的仿真测试得出各共识算法运行时的 CPU 占用率，其结果如图2所示。仿真结果表明，DPOS 虽然不如 PBFT 响应快速，但是相对于 POW，DPOS 对 CPU 的占用率明显小很多。

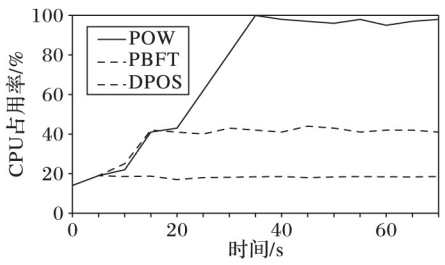

图2　3种共识机制对 CPU 占用率的对比

Fig. 2　Comparison of CPU utility by three consensus mechanisms

综上所述，相对于其他三种方案，本文方案的效率虽比不上文献[12]方案，但是远高于文献[25]和文献[17]方案，不

仅保证了更高程度的去中心化,同时也不需要花费太高的算力和成本。本文方案明显具有一定优势。

4　结语

由于当前在各医疗相关机构间进行医疗数据共享始终是一个热门研究问题,因此保证医疗数据隐私性、实现基于区块链的电子医疗病历共享具有重要意义。本文基于区块链的去中心化和不可篡改性等特点,提出了基于区块链的电子医疗病历共享方案。本文方案改进了文献[17]的模型,并提出了数据共享协议,实现了单对授权用户间的医疗数据安全共享功能;但方案只能实现单对用户间的数据共享,且方案中的 DPOS 算法效率还有待提高。

如何改进共识算法,提高共识效率,实现一个用户到多个用户的数据共享是下一步研究的主要工作。

参考文献 (References)

[1] HEART T, BEN-ASSULI O, SHABTAI I. A review of PHR, EMR and EHR integration: a more personalized healthcare and public health policy[J]. Health Policy and Technology, 2017, 6(1): 20 – 25.

[2] DUDIN E B, SMETANIN Y G. A review of cloud computing[J]. Scientific and Technical Information Processing, 2011, 38(4): 280 – 284.

[3] 侯佳音,史淳樵. 云计算技术在医院的信息化建设中的应用研究[J]. 电子设计工程,2016,24(5): 35 – 39. (HOU J Y, SHI C Q. Application of cloud computing technologies in information technology of hospitals [J]. Electronic Design Engineering, 2016, 24(5): 35 – 39.)

[4] ZHANG H, YU J, TIAN C, et al. Cloud storage for electronic health records based on secret sharing with verifiable reconstruction outsourcing[J]. IEEE Access, 2016: 40713 – 40722.

[5] LIU Y, ZHANG Y, LING J, et al. Secure and fine-grained access control on e-healthcare records in mobile cloud computing[J]. Future Generation Computer Systems, 2018, 78: 1020 – 1026.

[6] UNDERWOOD S. Blockchain beyond bitcoin[J]. Communications of the ACM, 2016, 59(11): 15 – 17.

[7] 何蒲,于戈,张岩峰,等. 区块链技术与应用前瞻综述[J]. 计算机科学,2017,44(4): 1 – 7,15. (HE P, YU G, ZHANG Y F, et al. Survey on blockchain technology and its application prospect[J]. Computer Science, 2017, 44(4): 1 – 7, 15.)

[8] VUJICIC D, JAGODIC D, RANDIC S. Blockchain technology, bitcoin, and Ethereum: a brief overview[C]// Proceedings of the 17th International Symposium INFOTEH-JAHORINA. Piscataway: IEEE, 2018: 1 – 6

[9] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[J]. Consulted, 2009, 75(8): 1042 – 1048.

[10] DAGHER G G, MOHLER J, MILOJKOVIC M, et al. Ancile: privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology[J]. Sustainable Cities and Society, 2018, 39: 283 – 297.

[11] 薛腾飞,傅群超,王枞,等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报,2017,43(9): 1555 – 1562. (XUE T F, FU Q C, WANG C, et al. A medical data sharing model via blockchain [J]. Acta Automatica Sinica, 2017, 43(9): 1555 – 1562.)

[12] LIU J, LI X, YE L, et al. BPDS: a blockchain based privacy-preserving data sharing for electronic medical records[C]// Proceedings of the 2018 IEEE Global Communications Conference. Piscataway: IEEE, 2018: 1 – 6.

[13] KOSBA A, MILLER A, SHI E, et al. Hawk: the blockchain model of cryptography and privacy-preserving smart contracts[C]// Proceedings of the 2016 IEEE Symposium on Security and Privacy. Piscataway: IEEE, 2016: 839 – 858.

[14] XIA Q, SIFAH E B, ASAMOAH K O, et al. MeDShare: trust-less medical data sharing among cloud service providers via blockchain[J]. IEEE Access, 2017, 5: 14757 – 14767.

[15] FAN K, WANG S, REN Y, et al. MedBlock: efficient and secure medical data sharing via blockchain[J]. Journal of Medical Systems, 2018, 42(8): No. 136.

[16] ZHANG A, LIN X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain[J]. Journal of Medical Systems, 2018, 42(8): No. 140.

[17] CUI S, ASGHAR M R, RUSSELLO G. Towards blockchain-based scalable and trustworthy file sharing[C]// Proceedings of the 27th International Conference on Computer Communications and Networks. Piscataway: IEEE, 2018: 1 – 2

[18] GENNARO R, JARECKIB S, KRAWCZYK H, et al. Robust threshold DSS signatures[J]. Information and Computation, 2001, 164(1): 54 – 84.

[19] GENNARO R, JARECKI S, KRAWCZYK H, et al. Secure distributed key generation for discrete-log based cryptosystems[J]. Journal of Cryptology, 2007, 20(1): 51 – 83.

[20] GREEN M, ATENIESE G. Identity-based proxy re-encryption [C]// Proceedings of the 2007 International Conference on Applied Cryptography and Network Security, LNCS 4521. Berlin: Springer, 2007: 288 – 306.

[21] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C]// Proceedings of the 1998 International Conference on the Theory and Applications of Cryptographic Techniques, LNCS 140. Berlin: Springer, 1998: 127 – 144.

[22] LUO Y, CHEN Y, CHEN Q, et al. A new election algorithm for DPoS consensus mechanism in blockchain[C]// Proceedings of the 7th International Conference on Digital Home. Piscataway: IEEE, 2018: 116 – 120.

[23] JIA X, HE D, ZEADALLY S, et al. Efficient revocable ID-based signature with cloud revocation server[J]. IEEE Access, 2017, 5: 2945 – 2954.

[24] LIN Q, YAN H, HUANG Z, et al. An ID-based linearly homomorphic signature scheme and its application in blockchain[J]. IEEE Access, 2018, 6: 20632 – 20640.

[25] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission management [C]// Proceedings of the 2nd International Conference on Open and Big Data. Piscataway: IEEE, 2016: 25 – 30.

This work is partially supported by the National Natural Science Foundation of China (61672004, 61702067).

LUO Wenjun, born in 1966, Ph. D., professor. His research interests include cyber security, cryptography.

WEN Shenglian, born in 1995, M. S. candidate. Her research interests include blockchain, cryptography.

CHENG Yu, born in 1995, M. S. candidate. His research interests include blockchain.