基于环签名的医疗区块链隐私数据共享模型

王瑞锦*，余苏喆，李　悦，唐榆程，张凤荔

(电子科技大学信息与软件工程学院　成都　610054)

【摘要】随着医疗行业信息化的推进，医疗领域已进入大数据时代，但在数据异构、互操作性和隐私保护等方面仍面临诸多挑战。针对上述问题，该文构建了基于环签名的去中心化医疗大数据共享模型。该模型基于区块链去中心化思想维护一个可靠的医疗数据账本，确保隐私数据的不可篡改。构建了基于环签名的隐私数据存储协议，利用其完全匿名性保障了医疗数据和病人身份隐私的安全性；提出了基于智能合约自动化执行预设指令的医疗信息严密访问控制管理机制，通过明确划分医疗隐私信息访问权限来保障医疗隐私数据的权威性和机密性。经安全性测试结果表明，相比于传统医疗大数据共享模式，该模型具有更好的实时性和鲁棒性。

关　键　词　区块链；　医疗大数据；　环签名；　安全共享；　智能合约

中图分类号　TP309.3　　**文献标志码**　A　　doi:10.3969/j.issn.1001-0548.2019.06.013

Medical Blockchain of Privacy Data Sharing Model Based on Ring Signature

WANG Rui-jin*, YU Su-zhe, LI Yue, TANG Yu-cheng, and ZHANG Feng-li

(School of Information and Software Engineering, University of Electronic Science and Technology of China　Chengdu　610054)

Abstract With the progress of information development of medical industry, the medical field has got into the era of big data. However, it still faces many challenges in data heterogeneity, interoperability, and privacy protection. In response to the above problems, a decentralized medical big data sharing model based on ring signature is constructed. The model maintains a reliable medical ledger database based on the decoupling of blockchain, ensuring that the privacy data cannot be tampered. It constructs a private data storage protocol based on ring signature, which guarantees medical data and patient identity privacy with its full anonymity. We proposed a medical information strict access control management mechanism based on smart contract automation execution of preset instructions. The authority and confidentiality of medical privacy data are guaranteed by clearly dividing the access rights of medical privacy information. The safety test results show that the model has better real-time and robustness than the traditional medical big data sharing model.

Key words　blockchain;　medical big data;　ring signature;　safe sharing;　smart contract

随着医疗行业的信息化发展和数字化医院的建设，医疗数据增长呈井喷之势。经IDC Digital调研，截至2020年医疗服务产生的数据总量将达40万亿GB，是2010年该数据的30倍。在过去几年中，我国医疗数据的生成和共享始终保持着较高的增长速度，由每月43.6亿GB增长到120.6亿GB。医疗信息化高速发展，也给医疗信息共享提出新的挑战。首先，来源广泛、更新迅速的海量医疗数据缺乏统一规划的医疗信息融合管理平台，致使数据标准乱、数据共享难、信息孤岛化严重；其次，患者未参与到医疗信息的访问控制策略当中，信息系统权限划分不明确，无法实现病人可控的个性化隐私保护；同时，医疗大数据时代的来临导致隐私信息公开透明，使得医疗信息去隐私化面临广泛多样的攻击，对数字签名医疗信息的溯源愈加困难[1]。

在医疗信息方面，目前主要采用数据集成和共享技术，如模式映射、数据复制、综合集成和基于语义的数据交换等，通过集成独立数据源中的有效数据来实现医疗信息共享[2]。但实践表明，传统数据集成方法不能有效适应当今环境的复杂性，不但增加维护成本还降低了医疗信息的共享效率。在医疗隐私信息保护方面，文献[3]提出基于安全多方计

收稿日期：2018－04－03；修回日期：2018－06－20

基金项目：国家自然科学基金(61802033, 61472064, 61602096)；四川省科技计划(2018GZ0087, 2019YJ0543)；博士后基金项目(2018M643453)；网络与数据安全四川省重点实验室开放课题(NDSMS201606)；国家互联网应急中心(2019R015)；教育部产学研项目(201802095001, 201801002050, 201801154052, 201702178018)

作者简介：王瑞锦(1980－)，男，博士，主要从事区块链、信息系统与内容安全、量子通信安全等方面的研究. Email: wrj8882003@163.com

算的隐私保护决策树方案，来解决垂直分布数据集中的医疗隐私问题。文献[4]提出利用矩阵奇异值分解(SVD)、独立成分分析(ICA)和旋转数据扰动3种不同技术来隐藏敏感的数值属性。文献[5]采用粒子群算法(PSO)降低医疗隐私信息中的敏感项频率，从而提高隐私信息的安全性。文献[6]将基因算法引入到规则隐藏中，并基于可信第三方模式将该算法实现在OLAP数据立方体中来保护医疗数据信息。

上述解决方案均是基于中心化架构和关系型数据库来实现医疗数据共享和病人隐私保护。但中心式存储容易遭受数据丢失、更改和攻击，不能保证医疗信息的安全可信。同时，信息系统对医疗隐私信息的访问控制管理不严密，权限划分不明确，无法切实保障患者隐私的安全性。此前提出的技术具有一定的局限性，并不适用于大数据时代复杂的医疗信息融合环境，且实现成本较高。

区块链去中心化、不可篡改的特性更契合当今分布式安全存储数据的趋势[7]，数据块无法篡改、无法撤销，链上的每一次动作都会被记录让医疗数据的正确性与唯一性得到保证。本文提出区块链架构下基于环签名的医疗大数据安全共享模型，为大数据时代的医疗信息提供数据共享、信息同步、隐私保护等全方位一体化管控服务。设计基于区块链的端到端体系架构，利用其不可篡改、可溯源的特性确保医疗信息的权威性和病人隐私的机密性。构建基于环签名的医疗隐私存储协议，利用环签名的完全匿名性在区块链公开透明的环境下保障医疗信息和病人隐私的安全性。区块链、智能合约及环签名将共同打造一个可信、智能和高效的医疗大数据安全共享平台，从根本上解决现行医疗信息共享平台存在的一系列问题。

1　模型技术基础

本模型实现的核心技术包括区块链技术、密环签名技术和智能合约技术。

1.1　区块链技术

区块链是以比特币为例的各类新型加密数据货币的技术基础[8-9]，通过区块链构建去中心化的架构，不需要传统的服务器和数据库，区块链网络中的各个节点可以收集一段时间内的交易数据，利用工作量证明机制等算法将交易确认并封装在区块中。将新区块进行全网广播，利用上一个区块的哈希值形成链式结构，保证记录的不可删除、不可篡改。区块按照时间链接，时间的不可逆转性致使任何试图篡改历史区块的行为很容易被追溯并被其他节点排斥[10]。

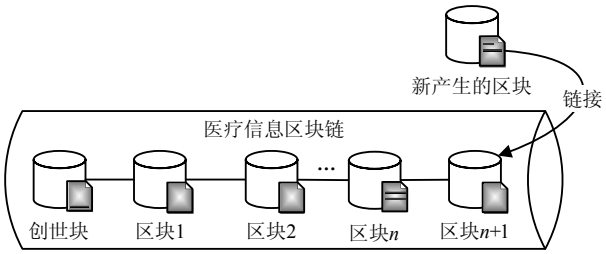


图1　医疗数据区块链

本文模型利用区块链技术搭建去中心化的医疗数据安全共享架构区块链，如图1所示，为当下医疗数据孤岛化、数据质量问题提供解决方案。区块链的存储方式确保医疗数据的来源透明化，从技术上保障数据留痕、数据汇集、数据关联、数据分析、数据智能等，从而实现数据来源可追溯、去向可追踪、责任可追究，进而保证医疗数据的权威性。

1.2　环签名技术

环签名是一种类群签名，用公钥集代替特定的公钥进行签名的有效性验证[11-13]。在如图2的环签名方案中，签名由一定的规则组成了一个环，签名者可以使用自己的私钥和环中其他成员的公钥进行签名，不需要征得环中其他成员的同意，验证者通过特定的方式检查签名，验证者只知道签名来自于这个环，但是不知道确定的签名者，保证了签名者的匿名性，而用户手中的私钥，确保了区块链整体中只有私钥持有者有资格查看数据的安全性。

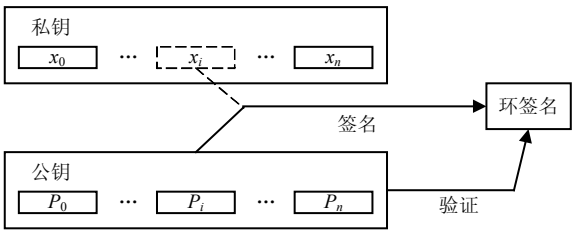


图2　环签名实现机制

区块链作为公共透明的记录账本，同时也开发了用户的医疗问题隐私保护的新途径。本模型采用环签名的交易签名方案保证用户的绝对匿名，从而保护用户的隐私。

1.3　智能合约

智能合约是能够自动执行合约条款的计算机指令，1995年由文献[14]提出，其认为智能合约就是执行合约条款的可计算交易协议。虽然智能合约的概念和互联网同时期诞生，但是却一直缺乏应用平台。

新兴的区块链技术为智能合约提供了契合的执行平台。区块链将智能合约的代码和状态作为一种交易保存到区块中，实时监测已部署的智能合约动

态，当其满足执行规则时，触发预设指令[15]。通过一份智能合约可以设置对单项信息数据分配多把私钥，并通过执行规则来对该数据进行每一次访问，同时此操作必须获得用户私钥授权才能进行。区块链的这一特性确保了个人敏感资料数据在全网络使用中的规范化和合法化，同时保证了智能合约从创建到执行整个过程透明、高效、不受干预。

本模型采用智能合约处理医疗数据共享体系业务逻辑，智能合约自动化执行预设指令的机制保证了模型的高效、透明、权威、智能。

2 基于环签名的医疗隐私数据存储

本节主要介绍在区块链的架构下使用环签名设计完全匿名的用户医疗数据存放协议，进而保证区块链中医疗信息的隐私性。

2.1 隐私交易创建

在医疗信息区块链网络中，对于没有交易记录存在的用户，将自动发起部署合约的操作，进而产生交易。已经部署好的医疗智能合约实时监测网络中的动态，当满足预设的条件时，触发预设指令执行，交易T的序列化表示如下：

$$T=\begin{cases}\mathrm{RLP}(T_n,T_t,T_s,T_c)\\ \mathrm{RLP}(T_n,T_t,T_d,T_s)\end{cases}$$

式中，T_n表示账户产生交易的数量；T_t为消息调用的接受地址；T_c是医疗合约的代码。上述通过RLP运算序列化链接，部署合约的交易方的address即T_t为空，T_d表示调用合约接口的数据，T_s代表交易信息的签名。

本模型采用EdDSA设计一次一密的交易环签名方案[16]，交易发起方m随机选取私钥$\mathrm{sk}_m\in z_n^*$，通过$\mathrm{pk}_m=\mathrm{sk}_m G$计算得到相应的公钥$\mathrm{pk}_m$，其中$G$为椭圆曲线的一个基准点。交易发起方选取一个公钥集$R=\{\mathrm{pk}_1,\mathrm{pk}_2,\cdots,\mathrm{pk}_n\}$，其中不包括$\mathrm{pk}_m$，对于每一个公钥设定相应的$v_t$和$w_t$，两者均为随机设定。$L_i$和$R_i$为公钥$\mathrm{pk}_i$属性值。

当$i=m$时，即公钥属于签名方m的相应公钥属性值的计算如下：

$$L_m=v_m*G$$
$$R_m=v_m*\mathrm{H}(\mathrm{pk}_m)$$

当$i\neq m$时，相应的公钥属性值计算如下：

$$L_i=v_i*G+w_i*\mathrm{pk}_i$$
$$R_i=v_i*\mathrm{H}(\mathrm{pk}_i)+w_i*l_m$$

式中，$I_m=\mathrm{sk}_m*\mathrm{H}(\mathrm{pk}_m)$，为该消息的签名镜像，用于防止双花攻击；$\mathrm{H}(\mathrm{pk}_i)$将$\mathrm{pk}_i$映射到有限域椭圆曲线的一个点。

设定签名内容包括签名消息S、每个公钥对应的c_i和e_i这3大类。其中设定非签名者公钥满足$c_i=w_i$，$e_i=v_i$。对于签名者m计算方式如下：

$$c_m=\mathrm{H}_2(S,L_1,L_2,\cdots,L_n,R_1,R_2,\cdots,R_n)-\sum_{i=1}^{n}c_i$$
$$e_m=v_m-c_m*\mathrm{sk}_m$$

式中，H_2是哈希函数，运算输出结果大小接近l阶的曲线，交易发起方m对消息的环签名T_s为：

$$T_s=(s,c_1,c_2,\cdots,c_m,\cdots,c_n,c_1,c_2,\cdots,c_m,\cdots,c_n)$$

本模型内部对交易发起方的交易T进行有效性检查，首先检查其是否为规定的RLP结构，然后检测交易签名T_s，过程如下：

$$\begin{cases}\alpha_i=e_iG+c_i*\mathrm{pk}_i\\ \beta_i=e_i\mathrm{H}(\mathrm{pk}_i)+c_i*l_m\end{cases}$$

判断上述公式是否满足，若相等表示签名合法，否则拒绝该签名。

2.2 新区块的产生与链接

医疗数据网络中的矿工节点B通过对一段时间内网络中交易$T=\{T_1,T_2,\cdots,T_n\}$进行收集，然后通过不断尝试随机数来构造符合预设条件的区块M确认交易。区块分为区块头和区块体两部分，区块头的序列化构造如下：

$$\mathrm{H}=\mathrm{RLP}(H_p,H_o,H_{\mathrm{tr}},H_b,H_s,H_d,H_n,H_t,H_{\mathrm{no}},H_m)$$

式中，H_p代表前一个区块的哈希值；H_o代表叔块的哈希值，通过哈希值将区块链接起来；H_{tr}为确认交易内容的哈希根；H_b为产生区块的矿工的哈希值；H_s为状态根的哈希值；H_d代表区块的难度等级系数；H_n表示区块号，创始块为零；H_t表示时间戳；H_{no}与H_m分别代表随机数和混合哈希，两者共同作为矿工的工作量证明。

矿工在规定时间内成功构造出区块B后，在医疗数据区块链网络中广播新区块B，节点将按照区块的构造机制对区块B进行合法性验证，如果新区块有效就将其添加到区块链上，区块链网络中的其他节点需同步区块B以获得下一次的记账权，详细过程描述如图3所示。

通过哈希值和时间戳进行新区块的链接和区块链的同步，医疗信息区块链的状态变化形式化描述如下：

$$\alpha_{t+1}=\lambda(\alpha_t,B)$$

式中，α_t表示t时刻的医疗信息区块链状态；B为通过验证的新区块；α_{t+1}表示添加新区块B后的医疗信息区块链状态：

$$B=(T_0,T_1,\cdots,T_n)$$

式中，区块B是一段时间内交易T_i的确认记录。所以，可以将α_{t+1}状态描述如下：

$$\alpha_{t+1}=\gamma(\cdots\lambda(\lambda(\alpha_t,T_0),T_1)\cdots)$$

式中，γ为状态转变函数，α_{t+1}的区块链包含网络中交易的所有信息。

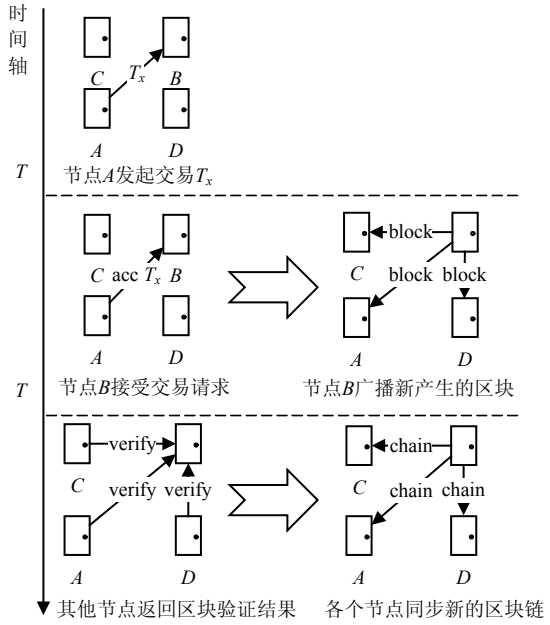


图3　医疗交易数据区块存储

3　基于智能合约的医疗数据安全共享

本节介绍了如何设计智能合约进行医疗数据的访问授权管理。

1) 注册合约(register contract, RC)：注册合约RC对应记录用户的个人身份信息，每位用户拥有唯一一份RC合约，与个人账户的公钥地址address绑定。

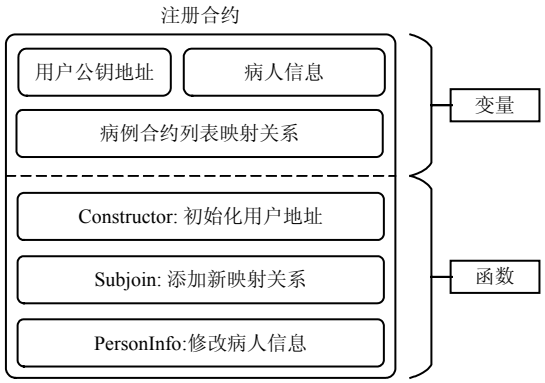


图4　注册合约详细结构设计

该合约在用户注册时根据注册信息使其被部署在区块链上，使用构造函数将信息写入区块链，完成注册合约的绑定。RC合约中除了存储用户个人基本信息之外，还维护该用户的病历合约列表，管理该用户的病历历史。由于合约是硬编码并且由以太坊虚拟机自动执行，因而能够严格保证注册流程的透明度[17-18]。

从图4可以看到，RC合约结构分为变量区和函数区，其中owner address是保存用户公钥地址，数据类型为bytes32，在合约被部署的时候通过调用构造函数constructor绑定拥有者，不可修改。Patient information为结构体变量，存放用户的个人基本信息，如姓名、性别、年龄等属性，可通过调用PersonInfo函数修改个人信息。MRC List是一个数组类型的变量，与用户的病历合约建立一对多的映射关系，用户通过检索该列表查询自己的病历信息，可通过调用Subjoin函数添加新的病历合约，但不提供删除或修改接口。RC合约实现如下所示：

Protocol 1: RC合约实体

Variables: bytes32 Addr, struct Pinfo,mapping Mlist

```
    procedure constructor()
        Addr = msg.sender
    end procedure
Input: bytes32 MRCAddr
    procedure subjoin(MRCAddr)
        if msg.sender == Addr is True then
            Mlist.push(MRCAddr)
        end if
    end procedure
Input: struct Pinfo
    procedure personInfo(Pinfo)
        if msg.sender == Addr is True then
            update(Pinfo)
        end if
    end procedure
```

2) 病历合约(medical records contract, MRC)：用户拥有零至多份病历合约MRC，一次病历对应一份MRC合约，通过RC合约维护的病历合约列表形成一对多的映射关系。MRC合约中的owner字段在合约部署时，通过构造函数赋值自动绑定合约拥有者的公钥address，并且不可进行二次修改。同时，MRC合约还用于存放此病历信息，以及其被允许访问的授权列表。用户可以对其特定的MRC合约共享给特定的机构，也可以随时收回或者授予访问权限，保证对个人医疗隐私信息的完全掌控。

MRC合约的详细结构设计如图5所示。

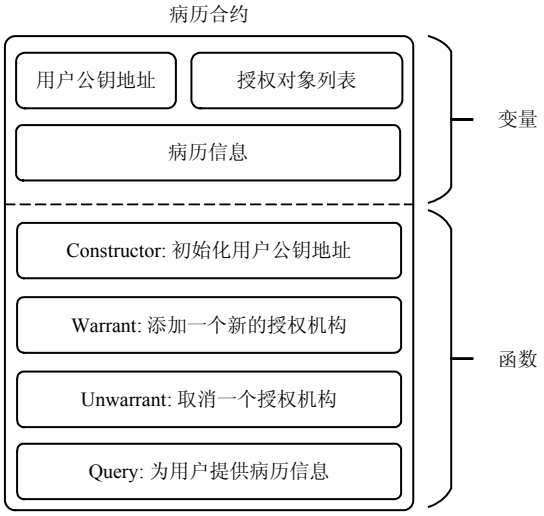


图5 病历合约详细结构设计

MRC合约也可以将owner变量绑定拥有者公钥地址，通过构造函数赋予初值。MR Information结构化存储此病历信息，包含具体的医疗数据以及时间戳等，用户可通过Query函数获取此次病历信息，此函数仅为用户开放调用权限。

Authorization List存放该份MRC合约的授权对象列表，只有在授权列表中的机构才有获取合约医疗数据的权限。用户可以通过调用Warrant或Unwarrant函数随时添加或者取消对部分机构的授权，具有较强的灵活性。

MRC合约实现如Protocol 2所示：

Protocol 2: MRC合约实体

```
Variables: bytes32 Addr, struct MRInfo,mapping Alist
        procedure constructor()
            Addr = msg.sender
        end procedure
    Input: bytes32 InstAddr
        procedure warrant(InstAddr)
            if msg.sender == Addr is True then
                Alist.push(InstAddr)
            end if
        end procedure
    Input: bytes32 InstAddr
        procedure unwarrant(InstAddr)
            if msg.sender == Addr is True then
                Alist.pop(InstAddr)
            end if
        end procedure
    Output: struct MRInfo
        procedure query()
            if msg.sender == Addr is True then
                return MRInfo;
            end if
        end procedure
```

3) 访问列表合约(access list contract, ALC)：医疗机构或大数据产业通过认证拥有一份访问列表合约ALC，通过机构的公钥address与该合约绑定。该合约维护一个具有访问权限的用户列表，机构可通过自己的ALC合约获取到已获得授权的用户匿名医疗数据集合，用于科学研究。当用户收回对该机构的授权时，该机构的ALC合约也会自动从可访问列表中删除这位用户。

ALC合约中的变量区拥有两个变量，其中Institution Address用于存放机构的公钥地址，通过构造函数进行初始化。另一个Authorized List是合约维护的可访问列表，机构可以通过GetData函数获取到被授权访问的匿名病历数据集，仅有读权限，可用于科学研究。如果用户在他的一份MRC合约中取消对该机构的授权，则该机构的ALC合约中的授权列表会自动删除用户的这份病历合约，这一机制完全由计算机自动执行，具有较强的即时性。ALC合约实现如Protocol3所示：

Protocol 3: ALC合约实体

```
Variables: bytes32 InstAddr, mapping Alist
        procedure constructor()
            InstAddr = msg.sender
        end procedure
    Output: mapping(uint=>struct) Data Alist
        procedure get Data()
            if msg.sender == InstAddr is True then
                return Data Alist;
            end if
        end procedure
```

上述3种类型合约关系的映射如图6所示。

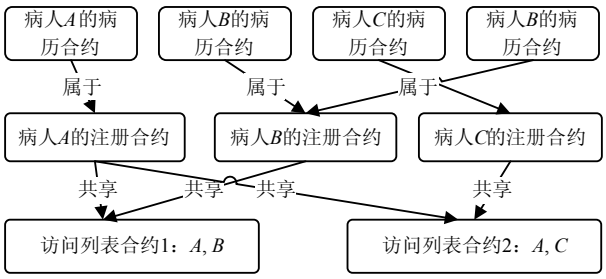


图6 3种类型合约关系映射图

4 安全性分析

本节从环签名的安全性和区块存储的安全性对

模型整体的安全性进行分析。

4.1　环签名安全性分析

一个安全的环签名方案应满足正确性、无条件匿名性和不可伪造性3个方面。

1) 正确性

验证签名方按照公式验证交易签名T_s，如果成立，验证通过。

$$\sum_{i=0}^{n} c_i = \mathrm{H}_2(S,\alpha_0,\alpha_1,\cdots,\alpha_n,\beta_0,\beta_1,\cdots,\beta_n)$$

式中，$i \neq m$时，α_i和β_i的转化如下：

$$\alpha_i = e_i * G + ic_i * \mathrm{pk}_i = v_i G + w_i * \mathrm{pk}_i = L_i$$

$$\beta_i = e_i \mathrm{H}(\mathrm{pk}_i) + c_i * I_m = v_i \mathrm{H}(\mathrm{pk}_i) + w_i * I_m = R_i$$

式中，$i = m$时，α_i和β_i的转化如下：

$$\alpha_m = e_m * G + c_m * \mathrm{pk}_m =$$
$$(v_m - c_m * \mathrm{sk}_m)G + c_m * \mathrm{pk}_m =$$
$$v_m * G = L_m$$
$$\beta_m = e_m \mathrm{H}(\mathrm{pk}_m) + c_m * I_m =$$
$$(v_m - w_m * \mathrm{sk}_m)\mathrm{H}(\mathrm{pk}_m) + w_m * \mathrm{sk}_m \mathrm{H}(\mathrm{pk}_m) =$$
$$v_m \mathrm{H}(\mathrm{pk}_m) = R_m$$

由此，可以使用上述关系按照以上方法来验证此环签名方案的的正确性：

$$\mathrm{H}_2(S,\alpha_0,\alpha_1,\cdots,\alpha_m,\cdots,\alpha_n,\beta_0,\beta_1,\cdots,\beta_m,\cdots,\beta_n) =$$
$$\mathrm{H}_2(S,L_0,L_1,\cdots,L_m,\cdots,L_n,R_0,R_1,\cdots,R_m,\cdots,R_n) =$$
$$c_m + \sum_{i=1,i\neq m}^{n} c_i = \sum_{i=0}^{n} c_i$$

2) 无条件匿名性分析

在环签名T_s中，计算c_i，e_i所需的L_i，R_i值是签名者通过随机选取相应的v_i，m_i计算得出的，所以签名T_s的结果在G中呈均匀分布状态。环签名成员之外能够猜出实际签名人的概率不超过$1/(n+1)$，而环内的城管猜出实际签名者的概率不超过$1/n$，所以签名方案满足无条件匿名性。

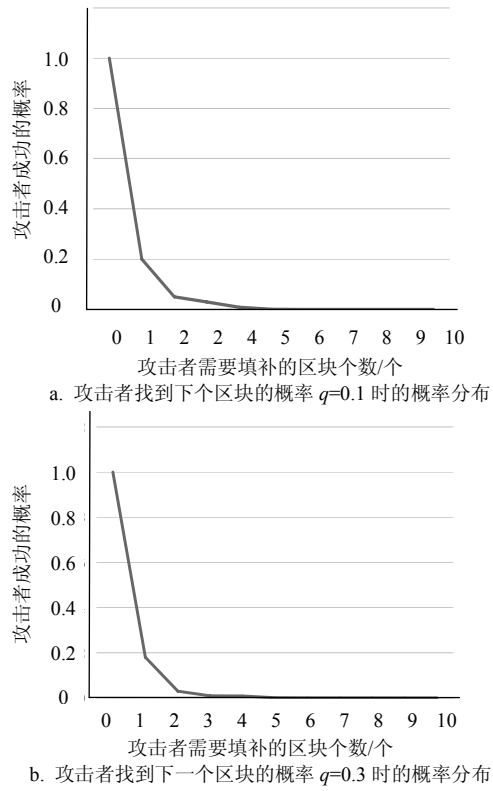
3) 不可伪造性分析

攻击者从$\mathrm{pk}_m=\mathrm{sk}_m G$中计算出$\mathrm{sk}_m$是一个椭圆曲线上的离散对数非常困难，可以认为私钥是安全的。

在未知密钥的条件下计算出密钥镜像$\mathrm{sk}_m * \mathrm{H}(\mathrm{pk}_m)$也是不可能的，即使攻击者随机选取$v_i$，$m_i$伪造$L_m$，$L_i$，$R_m$，$R_i$和$e_m$，计算中都需要得到签名者的私钥，所以攻击者伪造签名T_s是不可能的。

4.2　区块伪造攻击控制

要想成功发起一次区块伪造攻击，攻击者必须比诚实节点更快的产生出新的区块。本节从概率角度将攻击事件模型化，分析攻击者伪造区块并成功替代诚实节点的可能性。



a. 攻击者找到下个区块的概率 q=0.1 时的概率分布

b. 攻击者找到下一个区块的概率 q=0.3 时的概率分布

图7　攻击者伪造区块的成功概率

根据文献[19]所述，攻击者成功填补某一既定差距的可能性，可以近似看作赌徒破产问题。假定一个赌徒拥有无限的透支信用，然后开始进行潜在次数为无穷的赌博，试图填补上自己的亏空。那么可以计算出他填补上亏空的概率，也就是该攻击者赶上诚实链条的概率，计算如下：

$$P_z = 1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!}\left[1 - \frac{q^{z-k}}{p}\right] \qquad \lambda = z\frac{q}{p}$$

式中，变量p为诚实节点制造出下一个节点的概率，变量q为攻击者制造出下一个节点的概率。如图7所示，通过对q=0.1与q=0.3两种情况下进行P_z的大小进行计算统计，可以发现概率对z值呈指数下降。而且医疗数据区块链网络中拥有大量的节点和算力，这样攻击者成功制造出区块并修改网络中所有的节点区块记录的概率接近于零。

5　结 束 语

本文提出了基于区块链技术的去中心化医疗大数据共享模型。集成环签名技术，在区块链共享透明的环境下也能确保用户数据的隐私。采用智能合约设计医疗数据的安全共享机制，让用户能对自己的医疗信息实现自主可控。同时，区块链与智能合约相结合，保证了医疗数据的权威性和可信性，为

医疗科研提供更加优质的数据。本模型为解决现行医疗数据共享存在的一系列问题提供了解决方案。

参 考 文 献

[1] DENNIS R, OWENSON G, AZIZ B. A temporal blockchain: A formal analysis[C]//2016 International Conference on Collaboration Technologies and Systems (CTS). Orlando, FL, USA：IEEE，2016: 430-437.

[2] DIMITROV D V. Medical internet of things and big data in healthcare[J]. Healthcare Informatics Research, 2016, 22(3): 156-163.

[3] SHEELA M A, VIJAYALAKSHMI K. A novel privacy preserving decision tree induction[C]//2013 IEEE Conference on Information & Communication Technologies. Thuckalay, Tamil Nadu, India: IEEE, 2013: 1075-1079.

[4] LAKSHMI M N, RANI K S. SVD based data transformation methods for privacy preserving clustering[J]. International Journal of Computer Applications, 2013, 78(3): 39-43.

[5] BONAM J, REDDY A R, KALYANI G. Privacy preserving in association rule mining by data distortion using PSO[C]// Advances in Intelligent Systems and Computing. [S.l.]: Springer, 2014: 551-558.

[6] DEHKORDI M N. A novel association rule hiding approach in OLAP data cubes[J]. Indian Journal of Science and Technology, 2013, 6(2): 4063-4075.

[7] VUKOLI M. Rethinking permissioned blockchains[C]// Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts. Abu Dhabi, United Arab Emirates: ACM, 2017: 3-7.

[8] KIYOMOTO S, RAHMAN M S, BASU A. On Blockchain-based anonymized dataset distribution platform[C]//2017 IEEE 15th International Conference on Software Engineering Research, Management and Applications (SERA). London, UK: IEEE, 2017: 85-92.

[9] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized anonymous payments from bitcoin[C]//2014 IEEE Symposium on Security and Privacy. San Jose, CA, USA: IEEE, 2014: 459-474.

[10] WOOD G. Ethereum: A secure decentralised generalised transaction ledger[J]. Ethereum Project Yellow Paper, 2014, 151:1-32

[11] PETERS G W, PANAYI E. Banking beyond banks and money[M]. Berlin: Springer, 2016.

[12] DHILLON V, METCALF D, HOOPER M. Blockchain Enabled Applications[M]. Berlin: Springer, 2017.

[13] ZHANG Y H, HU Y, XIE J, et al. Efficient ring signature schemes over NTRU Lattices[J]. Security and Communication Networks, 2016, 9: 5252-5261.

[14] WU L, MENG K, XU S, et al. Democratic centralism: A hybrid blockchain architecture and its applications in energy internet[C]//2017 IEEE International Conference on Energy Internet (ICEI). Beijing, China: IEEE, 2017: 176-181.

[15] LIND J, NAOR O, EYAL I, et al. Teechain: Reducing storage costs on the blockchain with offline payment channels[C]//11th ACM International Systems and Storage Conference. Haifa, Israel: ACM, 2018: 125.

[16] DAI M, ZHANG S, WANG H, et al. A low storage room requirement framework for distributed ledger in blockchain[J]. IEEE Access, 2018, 6: 22970-22975.

[17] KOSBA A, MILLER A, SHI E, et al. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts[C]//2016 IEEE Symposium on Security and Privacy (SP). San Jose, CA, USA: IEEE, 2016: 839-858.

[18] HALPIN H, PIEKARSKA M. Introduction to security and privacy on the blockchain[C]//2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). Paris, France: IEEE, 2017: 1-3.

[19] XU C, WANG K, XU G, et al. Making big data open in collaborative edges: A blockchain-based framework with reduced resource requirements[C]//2018 IEEE International Conference on Communications (ICC). Kansas City, MO, USA: IEEE, 2018: 1-6.

编 辑 刘飞阳