(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108600227 A
(43)申请公布日 2018.09.28

(21)申请号 201810383020.X

(22)申请日 2018.04.26

(71)申请人 众安信息技术服务有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室(入驻深圳市前海商务秘书有限公司)

(72)发明人 阚海斌 张亮 张新鹏 孙亮 唐正超

(74)专利代理机构 北京市万慧达律师事务所 11111
代理人 赵然

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G06Q 20/38(2012.01)

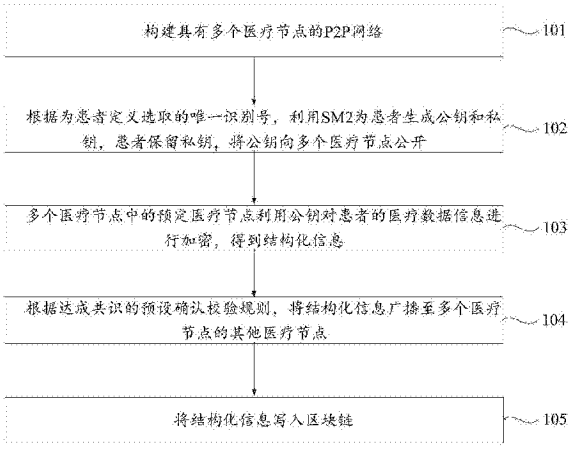
权利要求书2页 说明书10页 附图4页

(54)发明名称

一种基于区块链的医疗数据共享方法及装置

(57)摘要

本发明公开了一种基于区块链的医疗数据共享方法及装置,属于区块链技术领域。所述方法包括:构建具有多个医疗节点的P2P网络;根据为患者定义选取的唯一识别号,利用SM2为所述患者生成公钥和私钥,所述患者保留所述私钥,将所述公钥向所述多个医疗节点公开;所述多个医疗节点中的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密,通过密文构造区块链的结构化信息;根据达成共识的预设确认校验规则,将所述结构化信息广播至所述多个医疗节点的其他医疗节点;将所述结构化信息写入区块链。本发明既能提高医院之间数据共享效率,又能从技术上保证信息的隐私性和安全性,适于在医疗领域进行广泛的推广与应用。



CN 108600227 A

1.一种基于区块链的医疗数据共享方法，其特征在于，所述方法包括：

构建具有多个医疗节点的P2P网络；

根据为患者定义选取的唯一识别号，利用SM2为所述患者生成公钥和私钥，所述患者保留所述私钥，将所述公钥向所述多个医疗节点公开；

所述多个医疗节点中的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，通过密文构造区块链的结构化信息；

根据达成共识的预设确认校验规则，将所述结构化信息广播至所述多个医疗节点的其他医疗节点；

将所述结构化信息写入区块链。

2.根据权利要求1所述的方法，其特征在于，构建具有多个医疗节点的P2P网络，包括：

利用Kademlia协议构建具有多个医疗节点的P2P网络。

3.根据权利要求1所述的方法，其特征在于，根据为患者定义选取的唯一识别号ID，利用SM2为所述患者生成公钥和私钥，所述患者保留所述私钥，将所述公钥向所述多个医疗节点公开，包括：

将患者的身份证号作为患者的唯一识别号，利用国密SM2为所述患者生成公钥和私钥，存储所述私钥，并将所述公钥发送至所述多个医疗点。

4.根据权利要求1所述的方法，其特征在于，所述多个医疗节点的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，通过密文构造区块链的结构化信息，包括：

所述多个医疗节点的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，得到密文，对所述密文进行哈希运算，得到所述密文的摘要信息，所述预定医疗节点通过所述密文和摘要信息构造区块链的结构化信息。

5.根据权利要求1所述的方法，其特征在于，根据达成共识的预设确认校验规则，将所述结构化信息广播至所述多个医疗节点的其他医疗节点，包括：

探测所述多个医疗节点是否在线；

若其回复确认在线信息，将带有校验和的结构化信息发送给对方；

待对方校验通过校验和后，返回带校验和的确认信息。

6.根据权利要求1所述的方法，其特征在于，将所述结构化信息写入区块链，包括：

在预定时间节点，将所述结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

7.根据权利要求1所述的方法，其特征在于，所述方法还包括：

所述其他医疗节点通过所述患者提供的授权查看的私钥获取所述患者的医疗数据信息。

8.根据权利要求1所述的方法，其特征在于，所述方法还包括：

当所述患者丢失所述私钥或公钥，所述区块链内的任一医疗节点根据所述患者的唯一识别号，通过所述区块链内的预设私有算法，获得所述私钥或公钥。

9.一种基于区块链的医疗数据共享装置，其特征在于，包括：

P2P网络构建模块，用于构建具有多个医疗节点的P2P网络；

档案建立模块，用于根据为患者定义选取的唯一识别号，利用SM2为所述患者生成公钥和私钥，所述患者保留所述私钥，将所述公钥向所述多个医疗节点公开；

加密模块，用于使所述多个医疗节点中的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，通过密文构造区块链的结构化信息；

数据共享模块，用于根据达成共识的预设确认校验规则，将所述结构化信息广播至所述多个医疗节点的其他医疗节点；

区块链构建模块，用于将所述结构化信息写入区块链。

10.根据权利要求9所述的装置，其特征在于，所述P2P网络构建模块，用于利用Kademlia协议构建具有多个医疗节点的P2P网络。

11.根据权利要求9所述的装置，其特征在于，所述档案建立模块用于：将患者的身份证号作为患者的唯一识别号，利用国密SM2为所述患者生成公钥和私钥，存储所述私钥，并将所述公钥发送至所述多个医疗点。

12.根据权利要求9所述的装置，其特征在于，所述加密模块用于：使所述多个医疗节点的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，得到密文，对所述密文进行哈希运算，得到所述密文的摘要信息，所述预定医疗节点通过所述密文和摘要信息构造区块链的结构化信息。

13.根据权利要求9所述的方法，其特征在于，所述数据共享模块用于：探测所述多个医疗节点是否在线；若其回复确认在线信息，将带有校验和的结构化信息发送给对方；待对方校验通过校验和后，返回带校验和的确认信息。

14.根据权利要求9所述的方法，其特征在于，所述区块链构建模块用于：在预定时间节点，将所述结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

15.根据权利要求9所述的方法，其特征在于，所述装置还包括获取模块，用于：使所述其他医疗节点通过所述患者提供的授权查看的私钥获取所述患者的医疗数据信息。

16.根据权利要求9所述的方法，其特征在于，所述装置还包括丢失信息获取模块，用于：当所述患者丢失所述私钥或公钥，使所述区块链内的任一医疗节点根据所述患者的唯一识别号，通过所述区块链内的预设私有算法，获得所述私钥或公钥。

一种基于区块链的医疗数据共享方法及装置

技术领域

[0001] 本发明涉及区块链技术领域，特别涉及一种基于区块链的医疗数据共享方法及装置。

背景技术

[0002] 随着医疗卫生事业的发展，国内医疗信息化建设已经取得显著性成果，绝大部分三级医院和部分先进的二级医院信息化程度已经非常高。主要的医疗业务信息化系统包括：医院信息系统、电子病历系统、医学影像存档与通信系统、检验信息系统、超声信息系统、心电网络系统、体检管理信息系统等。

[0003] 上述信息化系统的建设，完成了医疗信息化的第一个步骤，逐步实现医疗业务数据的采集和存储。医疗信息系统不断深入应用，使得医院对医疗数据信息化的需求，从简单的采集、存储和“一院所有”到医疗数据共享和交换，以提高医疗数据对患者对人类的贡献。然而，如果仅仅将医疗信息简单粗暴的罗列在一起，存放在一个系统或者一台服务器中，医疗数据的共享将面临很大的社会隐私泄露问题。

[0004] 区块链是最近比较时兴的一项技术，它采用分布式的存储，利用块链式数据结构来验证与存储数据，利用分布式节点共识算法来生成和更新数据，利用密码学的方式保证数据传输和访问的安全，利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新分布式基础架构与计算范式。将区块链技术存储和传播加密后的医疗信息，将使得医疗信息既能全网共享，又能充分保证数据安全，从而保证隐私不被泄露。

[0005] 非对称加密算法需要两个密钥：公开密钥(publickey)和私有密钥(privatekey)。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。非对称加密算法实现机密信息交换的基本过程是：甲方生成一对密钥并将其中的一把作为公用密钥向其它方公开；得到该公用密钥的乙方使用该密钥对机密信息进行加密后再发送给甲方；甲方再用自己保存的另一把专用密钥对加密后的信息进行解密。我国国家秘密管理局在2010年发布了SM2椭圆曲线(ECC)公钥秘密算法，SM2主要包括4部分，第1部分为总则，主要介绍了ECC基本的算法描述，包括素数域和二元扩域两种算法描述，第2部分为数字签名算法，第3部分为密钥交换协议，第4部分为公钥加密算法，使用ECC公钥进行加密和ECC私钥进行解密算法。SM2在计算上比国际上公布的ECC算法复杂，相对来说算法速度可能慢，但可能是更安全一点。

[0006] 对等网络(P2P网络)，即对等计算机网络，是一种在对等者(Peer)之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式。网络的参与者共享他们所拥有的一部分硬件资源，这些共享资源通过网络提供服务和内容，能被其它对等节点(Peer)直接访问而无需经过中间实体。在此网络中的参与者既是资源、服务和内容的提供者，又是资源、服务和内容的获取者。P2P网络提供了对等者间合作的桥梁，

但并一定不能提供数据传输的可靠性。

[0007] 区块链格式首先用于比特币，作为解决数据库安全和不需要信任的管理员问题的解决方案。第一块区块链由中本聪在2008年概念化，并在次年实施作为数字货币比特币的核心组成部分，通过使用对等网络和分布式时间戳服务器，区块链数据库被自主地管理。比特币区块链的发明使它成为第一个解决双重支出问题的数字货币，比特币设计一直是其他区块链应用的灵感。区块链被分为三类：公有链(public blockchain)、联盟链(consortium blockchain)、私有链(private blockchain)。其中，比特币等加密货币属于公有链的范畴，联盟链常常用于企业之间，一方面保证数据的共享，另一方面保证链上数据的准入资格，这样既有助于协作，又有利于降低风险。

[0008] 加上区块链作为一项分布式、不可篡改、可追溯等特性的新技术，对于保存患者病人的就医历史信息具有极好的作用，因此本申请结合非对称加密和区块链技术，提出一种基于区块链的医疗数据共享方案设计，既提高医院之间数据共享效率，又能从技术上保证信息的隐私性和安全性。

发明内容

[0009] 为了解决现有技术的问题，本发明实施例提供了一种基于区块链的医疗数据共享方法及装置。所述技术方案如下：

[0010] 第一方面，提供了一种基于区块链的医疗数据共享方法，所述方法包括：

[0011] 构建具有多个医疗节点的P2P网络；

[0012] 根据为患者定义选取的唯一识别号，利用SM2为所述患者生成公钥和私钥，所述患者保留所述私钥，将所述公钥向所述多个医疗节点公开；

[0013] 所述多个医疗节点中的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，通过密文构造区块链的结构化信息；

[0014] 根据达成共识的预设确认校验规则，将所述结构化信息广播至所述多个医疗节点的其他医疗节点；

[0015] 将所述结构化信息写入区块链。

[0016] 结合第一方面，在第一种可能的实现方式中，构建具有多个医疗节点的P2P网络，包括：

[0017] 利用Kademlia协议构建具有多个医疗节点的P2P网络。

[0018] 结合第一方面，在第二种可能的实现方式中，根据为患者定义选取的唯一识别号ID，利用SM2为所述患者生成公钥和私钥，所述患者保留所述私钥，将所述公钥向所述多个医疗节点公开，包括：

[0019] 将患者的身份证号作为患者的唯一识别号，利用国密SM2为所述患者生成公钥和私钥，存储所述私钥，并将所述公钥发送至所述多个医疗点。

[0020] 结合第一方面，在第三种可能的实现方式中，所述多个医疗节点的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，通过密文构造区块链的结构化信息，包括：

[0021] 所述多个医疗节点的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，得到密文，对所述密文进行哈希运算，得到所述密文的摘要信息，所述预定医疗节

点通过所述密文和摘要信息构造区块链的结构化信息。

[0022] 结合第一方面，在第四种可能的实现方式中，根据达成共识的预设确认校验规则，将所述结构化信息广播至所述多个医疗节点的其他医疗节点，包括：

[0023] 探测所述多个医疗节点是否在线；

[0024] 若其回复确认在线信息，将带有校验和的结构化信息发送给对方；

[0025] 待对方校验通过校验和后，返回带校验和的确认信息。

[0026] 结合第一方面，在第五种可能的实现方式中，将所述结构化信息写入区块链，包括：

[0027] 在预定时间节点，将所述结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

[0028] 结合第一方面，在第六种可能的实现方式中，所述方法还包括：

[0029] 所述其他医疗节点通过所述患者提供的授权查看的私钥获取所述患者的医疗数据信息。

[0030] 结合第一方面，在第七种可能的实现方式中，所述方法还包括：

[0031] 当所述患者丢失所述私钥或公钥，所述区块链内的任一医疗节点根据所述患者的唯一识别号，通过所述区块链内的预设私有算法，获得所述私钥或公钥。

[0032] 第二方面，提供了一种基于区块链的医疗数据共享装置，包括：

[0033] P2P网络构建模块，用于构建具有多个医疗节点的P2P网络；

[0034] 档案建立模块，用于根据为患者定义选取的唯一识别号，利用SM2为所述患者生成公钥和私钥，所述患者保留所述私钥，将所述公钥向所述多个医疗节点公开；

[0035] 加密模块，用于使所述多个医疗节点中的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，通过密文构造区块链的结构化信息；

[0036] 数据共享模块，用于根据达成共识的预设确认校验规则，将所述结构化信息广播至所述多个医疗节点的其他医疗节点；

[0037] 区块链构建模块，用于将所述结构化信息写入区块链。

[0038] 结合第二方面，在第一种可能的实现方式中，所述P2P网络构建模块，用于利用Kademlia协议构建具有多个医疗节点的P2P网络。

[0039] 结合第二方面，在第二种可能的实现方式中，所述档案建立模块用于：将患者的身份证号作为患者的唯一识别号，利用国密SM2为所述患者生成公钥和私钥，存储所述私钥，并将所述公钥发送至所述多个医疗点。

[0040] 结合第二方面，在第三种可能的实现方式中，所述加密模块用于：使所述多个医疗节点的预定医疗节点利用所述公钥对所述患者的医疗数据信息进行加密，得到密文，对所述密文进行哈希运算，得到所述密文的摘要信息，所述预定医疗节点通过所述密文和摘要信息构造区块链的结构化信息。

[0041] 结合第二方面，在第四种可能的实现方式中，所述数据共享模块用于：探测所述多个医疗节点是否在线；若其回复确认在线信息，将带有校验和的结构化信息发送给对方；待对方校验通过校验和后，返回带校验和的确认信息。

[0042] 结合第二方面，在第五种可能的实现方式中，所述区块链构建模块用于：在预定时间节点，将所述结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部

写入区块链，使得区块链在各节点一致。

[0043] 结合第二方面，在第六种可能的实现方式中，所述装置还包括获取模块，用于：使所述其他医疗节点通过所述患者提供的授权查看的私钥获取所述患者的医疗数据信息。

[0044] 结合第二方面，在第七种可能的实现方式中，所述装置还包括丢失信息获取模块，用于：当所述患者丢失所述私钥或公钥，使所述区块链内的任一医疗节点根据所述患者的唯一识别号，通过所述区块链内的预设私有算法，获得所述私钥或公钥。

[0045] 本发明实施例提供的技术方案带来的有益效果是：

[0046] 通过借助已有的高效点对点(P2P)网络，在可信的众多医疗节点中，结合区块链与非对称加密技术，将患者医疗数据信息加密，并写入区块链，在医疗节点间传播数据时，通过多次握手确认数据在各方均有备份，只需按合适的排序方式即可达到数据在区块链上的一致性。任何需要共享的医疗数据均可通过某一个节点生成、广播、达成共识，然后写入区块链，并支持在其他医院发出请求时提供授权查询。当每个节点拥有了同样的医疗数据项目，可以按照数据项目的生成时间排序，使得每个节点得到完全一样的区块。因此，本发明实施例提供的基于区块链的医疗数据共享方法及装置既能提高医院之间数据共享效率，又能从技术上保证信息的隐私性和安全性，适于在医疗领域进行广泛的推广与应用。

附图说明

[0047] 为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0048] 图1是本发明实施例1提供的基于区块链的医疗数据共享方法流程图；

[0049] 图2是本发明实施例2提供的基于区块链的医疗数据共享方法流程图；

[0050] 图3是本发明实施例3提供的基于区块链的医疗数据共享装置结构示意图；

[0051] 图4是本发明实施例提供的基于区块链的数据共享方法及装置的应用实例中的操作流程示意图。

具体实施方式

[0052] 为使本发明的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0053] 需要说明的是，在本发明的描述中，“多个”的含义是两个以上，除非另有明确具体的限定。

[0054] 本发明实施例提供的基于区块链的医疗数据共享方法及装置，在参与节点可信的多个医疗节点范围内，借助已有的高效点对点(P2P)网络，结合区块链与非对称加密技术，将患者医疗数据信息加密，并写入区块链，在医疗节点间传播数据时，通过多次握手确认数据在各方均有备份，只需按合适的排序方式即可达到数据在区块链上的一致性。本发明实施例提供的基于区块链的数据共享方法及装置，既能提高医院之间数据共享效率，又能从

技术上保证信息的隐私性和安全性，适于在医疗领域进行广泛的推广与应用。

[0055] 下面结合实施例，对本发明实施例提供的基于区块链的医疗数据共享方法与装置作具体说明。

[0056] 实施例1

[0057] 图1是本发明实施例的基于区块链的医疗数据共享方法流程图，如图1所示，本发明实施例提供的基于区块链的医疗数据共享方法，包括以下步骤：

[0058] 101、构建具有多个医疗节点的P2P网络。

[0059] 由于公私钥仅限于可信的联盟成员之中，如果构建了高效安全的P2P网络，即可达到该医疗数据共享节点的共识。因此首先在该步骤中，要构建可靠的具有多个医疗节点的P2P网络。这里的医疗节点包括医院或其他涉及到需要医疗数据共享的医疗结构，并且这里的医疗节点可以选择的尽量多、尽量全面，也就是说，有关医疗节点的数量和种类，本发明实施例不对其加以特别限制。

[0060] 具体的，利用Kademlia(简称Kad)协议构建具有多个医疗节点的P2P网络。Kademlia是一种结构化的P2P覆盖网络，属于一种分布式哈希表(DHT)技术，它以独特的异或算法(XOR)为距离量度基础，来建立一种DHT网络拓扑结构，拥有极高的路由查询速度。

[0061] 102、根据为患者定义选取的唯一识别号，利用SM2为患者生成公钥和私钥，患者保留私钥，将公钥向多个医疗节点公开。

[0062] 医疗节点通过患者身份证号或其他唯一识别号ID作为种子(以在特殊情况下可辅助用于恢复患者的私钥，由于在联盟链内，因此可以认为节点不会泄露私钥恢复算法)，为每一个患者均采用SM2生成公钥和私钥，私钥在个人手中保存并做好备份和保护措施，公钥可对外公布。本发明实施例不对患者唯一识别号的选取加以特限制。

[0063] 具体的，在患者在某一医疗节点首次就医或就医次数较频繁的场景下，将患者的身份证号作为患者的唯一识别号，利用国密SM2为患者生成公钥和私钥，存储私钥，并将公钥发送至多个医疗点。由于患者的身份证号基本上在所有的医疗节点进行就医或其他医疗服务登记的必备信息，因此可以较便利地使用其作为唯一标识患者的唯一识别号，另外利用国密SM2加密，安全性更高。需要注意的是，本发明实施例不对上述应用场景加以特别限制。

[0064] 103、多个医疗节点中的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到结构化信息。

[0065] 具体的，多个医疗节点的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到密文，对密文进行哈希运算，得到密文的摘要信息，通过密文构造区块链的结构化信息。因为哈希运算是不可逆的，并且是一一对应的，所以，哈希运算得到的摘要信息可以作为校验手段来校验消息是否遭到篡改。举例说明，医院节点使用密文以及摘要信息来构造区块链的结构信息，其中包括当前的时间戳。

[0066] 104、根据达成共识的预设确认校验规则，将结构化信息广播至多个医疗节点的其他医疗节点。

[0067] 具体的，达成共识的预设确认校验规则为：

[0068] 探测所述多个医疗节点是否在线；

[0069] 若其回复确认在线信息，将带有校验和的结构化信息发送给对方；

[0070] 待对方校验通过校验和后，返回带校验和的确认信息。

[0071] 示例性地，为实现P2P网络的可靠性，可先探测对等方是否在线，待其回复yes后再发送带有校验和的结构化信息，在对等方校验通过校验和后，返回带校验和的确认，确保数据在区块链节点中完全共享。

[0072] P2P网络中的节点和其它节点通信的方式是通过广播的方式来进行的，医疗节点使用P2P网络将该结构化信息广播至其他节点。

[0073] 示例性地，P2P网络中每个节点在本地都有一个缓冲池，用来存放从其它节点广播而来的加密信息，当节点收到其它节点广播而来的加密信息，它会先把密文进行哈希运算，把哈希运算得到的摘要和本消息中的摘要进行比对，如果不匹配，则丢弃该消息。如果匹配，则把该消息放到本地的消息缓冲池，同时把该消息广播到临近的其它节点，以此类推，从而把一条消息扩散到整个网络中。

[0074] 105、将结构化信息写入区块链。

[0075] 在预定时间节点，将结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

[0076] 示例性地，每隔一段时间，P2P网络中的节点对消息缓冲池的消息按时间戳递增排序，通过merkle tree组织起来，并添加时间、序号等头部写入区块链，使得区块链在各节点一致。

[0077] 在另一优选实施方式中，除了上述步骤，上述基于区块链的医疗数据共享方法还包括以下步骤：

[0078] 其他医疗节点通过患者提供的授权查看的私钥获取所述患者的医疗数据信息。示例性地，当患者在一家新的医疗节点就医，根据非对称加密算法特点，要查看通过公钥加密的密文需要公钥对应的私钥来解密，患者提供私钥来授权该医疗节点查看患者在其他医院的详细病史等医疗信息。医疗节点获取到患者的病史信息，根据病史信息对患者进行诊断。

[0079] 在另一优选实施方式中，上述基于区块链的医疗数据共享方法还包括以下步骤：

[0080] 当患者丢失私钥或公钥，区块链内的任一医疗节点根据患者的唯一识别号，通过区块链内的预设私有算法，获得私钥或公钥。在为患者注册加密后，会存在患者丢失私钥或公钥的情况，由于患者的医疗数据信息在区块链内的所有医疗节点均有备份，因此通过区块链内的任一医疗节点，根据患者的唯一识别号，通过区块链内的预设私有算法，处理获取患者的私钥或公钥。这里，区块链内的预设私有算法可以采用现有技术中任何可能的找寻丢失私钥或公钥的算法，本发明实施例不对其加以特别限制。

[0081] 实施例2

[0082] 图2是本发明实施例2提供的基于区块链的医疗数据共享方法流程图，如图2所示，本发明实施例提供的基于区块链的医疗数据共享方法，包括以下步骤：

[0083] 201、利用Kademlia协议构建具有多个医疗节点的P2P网络。

[0084] Kademlia是一种结构化的P2P覆盖网络，属于一种分布式哈希表(DHT)技术，它以独特的异或算法(XOR)为距离量度基础，来建立一种DHT网络拓扑结构，拥有极高的路由查询速度。

[0085] 值得注意的是，步骤201除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0086] 202、将患者的身份证号作为患者的唯一识别号，利用国密SM2为患者生成公钥和私钥，存储私钥，并将公钥发送至多个医疗点。

[0087] 在患者在某一医疗节点首次就医或就医次数较频繁的场景下，将患者的身份证号作为患者的唯一识别号，利用国密SM2为患者生成公钥和私钥，存储私钥，并将公钥发送至多个医疗点。由于患者的身份证号基本上在所有的医疗节点进行就医或其他医疗服务登记的必备信息，因此可以较便利地使用其作为唯一标识患者的唯一识别号，另外利用国密SM2加密，安全性更高。需要注意的是，本发明实施例不对上述应用场景加以特别限制。

[0088] 值得注意的是，步骤202除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0089] 203、多个医疗节点的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到密文，对密文进行哈希运算，得到密文的摘要信息，预定医疗节点通过密文和摘要信息构造区块链的结构化信息。

[0090] 因为哈希运算是不可逆的，并且是一一对应的，所以，哈希运算得到的摘要信息可以作为校验手段来校验消息是否遭到篡改。举例说明，医院节点使用密文以及摘要信息来构造区块链的结构信息，其中包括当前的时间戳。

[0091] 值得注意的是，步骤203除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0092] 204、探测多个医疗节点是否在线；若其回复确认在线信息，将带有校验和的结构化信息发送给对方；待对方校验通过校验和后，返回带校验和的确认信息。

[0093] 示例性地，为实现P2P网络的可靠性，可先探测对等方是否在线，待其回复yes后再发送带有校验和的结构化信息，在对等方校验通过校验和后，返回带校验和的确认，确保数据在区块链节点中完全共享。

[0094] P2P网络中的节点和其它节点通信的方式是通过广播的方式来进行的，医疗节点使用P2P网络将该结构化信息广播至其他节点。

[0095] 示例性地，P2P网络中每个节点在本地都有一个缓冲池，用来存放从其它节点广播而来的加密信息，当节点收到其它节点广播而来的加密信息，它会先把密文进行哈希运算，把哈希运算得到的摘要和本消息中的摘要进行比对，如果不匹配，则丢弃该消息。如果匹配，则把该消息放到本地的消息缓冲池，同时把该消息广播到临近的其它节点，以此类推，从而把一条消息扩散到整个网络中。

[0096] 值得注意的是，步骤204除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0097] 205、在预定时间节点，将结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

[0098] 示例性地，每隔一段时间，P2P网络中的节点对消息缓冲池的消息按时间戳递增排序，通过merkle tree组织起来，并添加时间、序号等头部写入区块链，使得区块链在各节点一致。

[0099] 值得注意的是，步骤205除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0100] 206、其他医疗节点通过患者提供的授权查看的私钥获取患者的医疗数据信息。

[0101] 示例性地，当患者在一家新的医疗节点就医，根据非对称加密算法特点，要查看通过公钥加密的密文需要公钥对应的私钥来解密，患者提供私钥来授权该医疗节点查看患者在其他医院的详细病史等医疗信息。医疗节点获取到患者的病史信息，根据病史信息对患者进行诊断。

[0102] 值得注意的是，步骤206除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0103] 207、当患者丢失私钥或公钥，区块链内的任一医疗节点根据患者的唯一识别号，通过区块链内的预设私有算法，获得私钥或公钥。

[0104] 在为患者注册加密后，会存在患者丢失私钥或公钥的情况，由于患者的医疗数据信息在区块链内的所有医疗节点均有备份，因此通过区块链内的任一医疗节点，根据患者的唯一识别号，通过区块链内的预设私有算法，处理获取患者的私钥或公钥。这里，区块链内的预设私有算法可以采用现有技术中任何可能的找寻丢失私钥或公钥的算法，本发明实施例不对其加以特别限制。

[0105] 值得注意的是，步骤207除了上述步骤所述的方式之外，还可以通过其他方式实现该过程，本发明实施例对具体的方式不加以限定。

[0106] 实施例3

[0107] 图3是本发明实施例提供的基于区块链的医疗数据共享装置结构示意图，如图3所示，本发明实施例提供的基于区块链的医疗数据共享装置，包括P2P网络构建模块31、档案建立模块32、加密模块33、数据共享模块34和区块链构建模块35。

[0108] P2P网络构建模块31，用于构建具有多个医疗节点的P2P网络。具体的，P2P网络构建模块31用于利用Kademlia协议构建具有多个医疗节点的P2P网络。

[0109] 档案建立模块32，用于根据为患者定义选取的唯一识别号，利用SM2为患者生成公钥和私钥，患者保留私钥，将公钥向多个医疗节点公开。具体的，档案建立模块用于：将患者的身份证号作为患者的唯一识别号，利用国密SM2为患者生成公钥和私钥，存储私钥，并将公钥发送至多个医疗点。

[0110] 加密模块33，用于使多个医疗节点中的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到结构化信息。具体的，加密模块33用于：将多个医疗节点的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到密文，对密文进行哈希运算，得到密文的摘要信息，预定医疗节点通过密文及摘要信息构造区块链的结构化信息。

[0111] 数据共享模块34，用于根据达成共识的预设确认校验规则，将结构化信息广播至多个医疗节点的其他医疗节点。具体的，数据共享模块34用于：探测多个医疗节点是否在线；若其回复确认在线信息，将带有校验和的结构化信息发送给对方；待对方校验通过校验和后，返回带校验和的确认信息。

[0112] 区块链构建模块35，用于将结构化信息写入区块链。具体的，区块链构建模块35用于：在预定时间节点，将结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

[0113] 另外，在一优选实施方式中，本发明实施例提供的基于区块链的医疗数据共享装置还包括获取模块36，获取模块36用于：使其他医疗节点通过患者提供的授权查看的私钥获取患者的医疗数据信息。

[0114] 在一优选实施方式中，本发明实施例提供的基于区块链的医疗数据共享装置还包括丢失信息获取模块37，用于：当患者丢失私钥或公钥，使区块链内的任一医疗节点根据患者的唯一识别号，通过区块链内的预设私有算法，获得私钥或公钥。

[0115] 应用实例

[0116] 图4是本发明实施例提供的基于区块链的数据共享方法及装置的应用实例中的操作流程示意图，如图4所示，该应用实例中的基于区块链的数据共享方法及装置的操作流程，包括以下步骤：

[0117] 1、构建可靠的P2P网络。利用Kademlia(简称Kad)协议构建具有多家医院节点(其中包含医院节点A)的P2P网络。

[0118] Kad网络中每个节点都有一个160bit的ID值作为标志符，Key也是一个160bit的标志符，每一个加入Kad网络的计算机都会在160bit的key空间被分配一个节点ID(node ID)值(可以认为ID是随机产生的)。

[0119] 对每一个0≤i≤160，每个节点都保存有一些和自己距离范围在区间[2^i,2^(i+1))内的一些节点信息，这些信息由一些(IP address,UDP port,Node ID)数据列表构成(Kad网络是靠UDP协议交换信息的)，每一个这样的列表都称之为一个K桶。因为是用指数方式划分区间，经过证明，对于一个有N个节点的Kad网络，最多只需要经过logN步查询，就可以准确定位到目标节点。

[0120] 2、每个节点使用SM2为患者生成一组公私钥，私钥由患者保留。每个节点以患者的身份证号或者其他唯一的标识为参数，采用SM2算法为患者生成一组公私钥，因为SM2算法是一种更安全先进的加密算法，因此可以保证较高的安全性。

[0121] 3、当某患者a在医院节点A就医，A使用a的公钥对a的信息加密，得到CT。当某患者a在医院节点A就医，A使用上一步中生成的a的公钥和加密算法对a的病历信息进行加密，得到密文CT，然后对密文进行哈希运算，得到摘要信息。因为哈希运算是不可逆的，并且是一一对应的，所以，哈希运算得到的摘要信息可以作为校验手段来校验消息是否遭到篡改。

[0122] 4、医院节点A使用CT构造区块链的结构信息M，使用P2P网络将该结构化信息广播至其他节点。医院节点A使用密文CT以及摘要信息来构造区块链的结构信息M，其中包括当前的时间戳，P2P网络中的节点和其它节点通信的方式是通过广播的方式来进行的，医院节点A使用P2P网络将该结构化信息广播至其他节点。

[0123] 5、其他节点将M放入本地的消息缓冲池。P2P网络中每个节点在本地都有一个缓冲池，用来存放从其它节点广播而来的加密信息，当节点收到其它节点广播而来的加密信息，它会先把密文CT进行哈希运算，把哈希运算得到的摘要和本消息中的摘要进行比对，如果不匹配，则丢弃该消息。如果匹配，则把该消息放到本地的消息缓冲池，同时把该消息广播到临近的其它节点，以此类推，从而把一条消息扩散到整个网络中。

[0124] 6、在规定的时间节点，所有节点对消息缓冲池的消息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。每隔一段时间，P2P网络中的节点对消息缓冲池的消息按时间戳递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致。

[0125] 7、当患者a在一家新的医院B就医，a提供其私钥，授权B查看a在其他医院的详细病史信息。当患者a在一家新的医院B就医，根据非对称加密算法特点，要查看通过公钥加密的

密文需要公钥对应的私钥来解密，a提供私钥来授权B查看a在其他医院的详细病史信息。

[0126] 8、B获取到a的历史信息，根据历史信息对a进行诊断，步骤同3-6。医院B获取到患者a的病史信息，根据病史信息对a进行诊断。

[0127] 上述所有可选技术方案，可以采用任意结合形成本发明的可选实施例，在此不再一一赘述。

[0128] 综上所述，本发明实施例提供的基于区块链的医疗数据共享方法及装置，相对于现有技术具有以下有益效果：

[0129] 通过借助已有的高效点对点(P2P)网络，在可信的众多医疗节点中，结合区块链与非对称加密技术，将患者医疗数据信息加密，并写入区块链，在医疗节点间传播数据时，通过多次握手确认数据在各方均有备份，只需按合适的排序方式即可达到数据在区块链上的一致性。任何需要共享的医疗数据均可通过某一个节点生成、广播、达成共识，然后写入区块链，并支持在其他医院发出请求时提供授权查询。当每个节点拥有了同样的医疗数据项目，可以按照数据项目的生成时间排序，使得每个节点得到完全一样的区块。因此，本发明实施例提供的基于区块链的医疗数据共享方法及装置既能提高医院之间数据共享效率，又能从技术上保证信息的隐私性和安全性，适于在医疗领域进行广泛的推广与应用。

[0130] 需要说明的是：上述实施例提供的基于区块链的医疗数据共享装置在触发基于区块链的医疗数据共享业务时，仅以上述各功能模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能模块完成，即将装置的内部结构划分成不同的功能模块，以完成以上描述的全部或者部分功能。另外，上述实施例提供的基于区块链的医疗数据共享装置与基于区块链的医疗数据共享方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

[0131] 本领域普通技术人员可以理解实现上述实施例的全部或部分步骤可以通过硬件来完成，也可以通过程序来指令相关的硬件完成，所述的程序可以存储于一种计算机可读存储介质中，上述提到的存储介质可以是只读存储器，磁盘或光盘等。

[0132] 以上所述仅为本发明的较佳实施例，并不用以限制本发明，凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

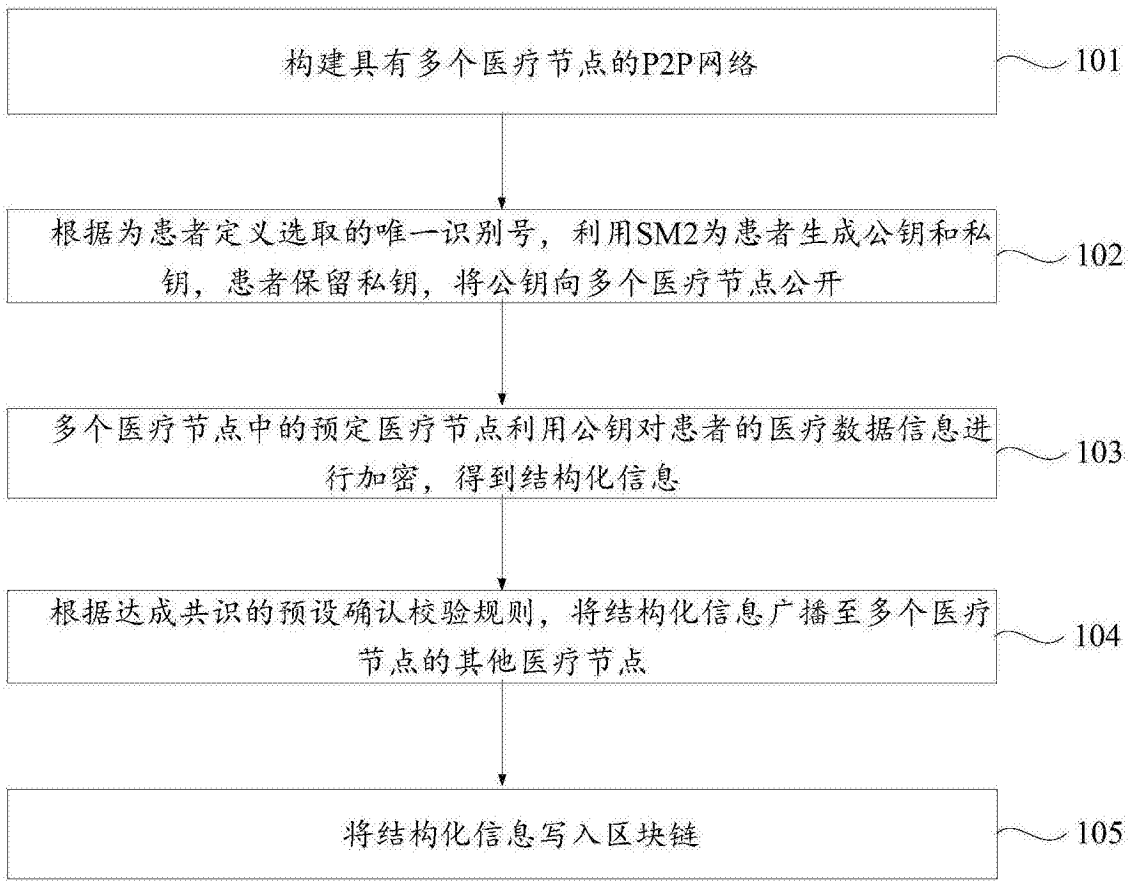

构建具有多个医疗节点的P2P网络
101
根据为患者定义选取的唯一识别号，利用SM2为患者生成公钥和私钥，患者保留私钥，将公钥向多个医疗节点公开
102
多个医疗节点中的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到结构化信息
103
根据达成共识的预设确认校验规则，将结构化信息广播至多个医疗节点的其他医疗节点
104
将结构化信息写入区块链
105

图1

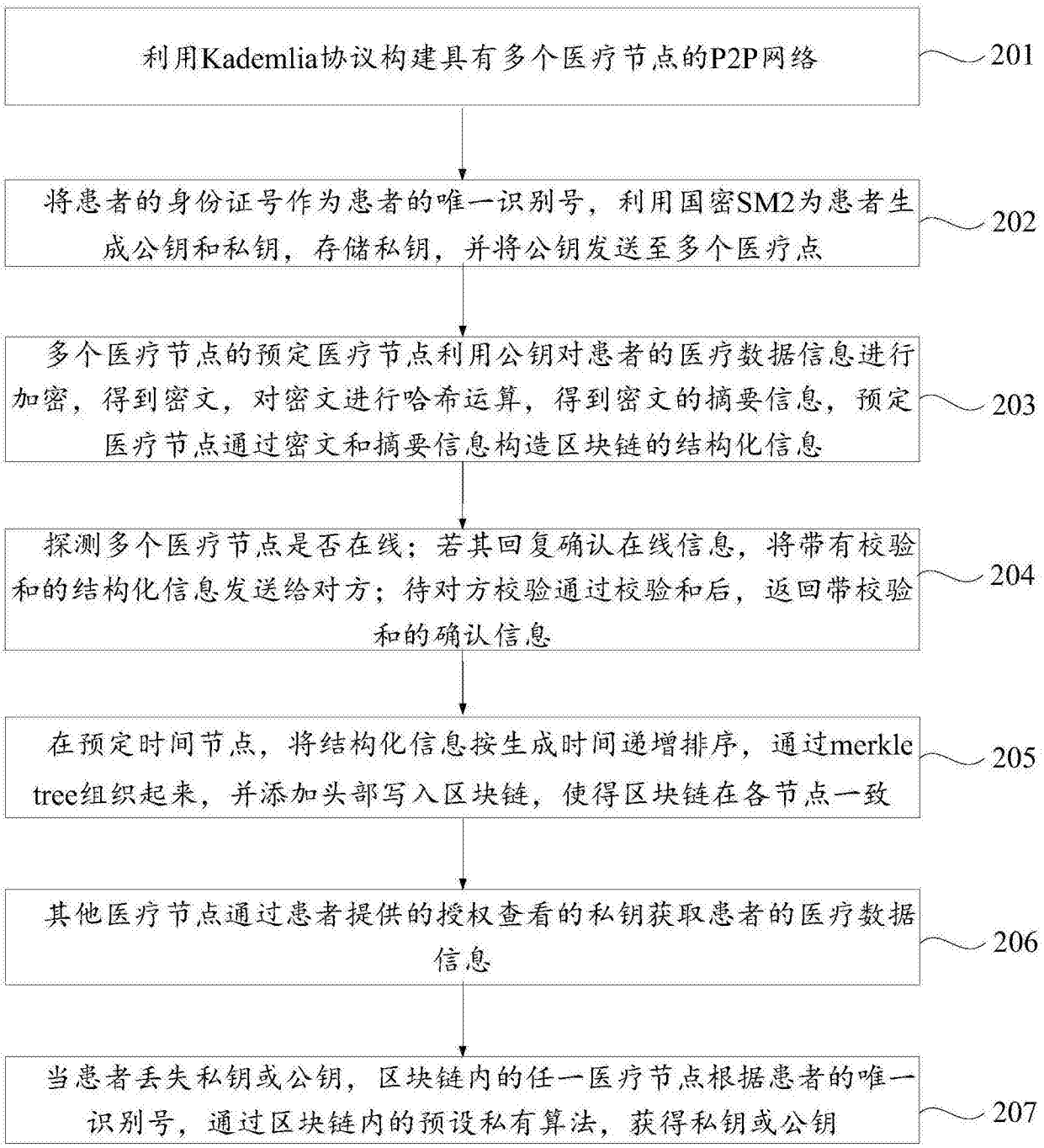

利用Kademlia协议构建具有多个医疗节点的P2P网络
201
将患者的身份证号作为患者的唯一识别号，利用国密SM2为患者生成公钥和私钥，存储私钥，并将公钥发送至多个医疗点
202
多个医疗节点的预定医疗节点利用公钥对患者的医疗数据信息进行加密，得到密文，对密文进行哈希运算，得到密文的摘要信息，预定医疗节点通过密文和摘要信息构造区块链的结构化信息
203
探测多个医疗节点是否在线；若其回复确认在线信息，将带有校验和的结构化信息发送给对方；待对方校验通过校验和后，返回带校验和的确认信息
204
在预定时间节点，将结构化信息按生成时间递增排序，通过merkle tree组织起来，并添加头部写入区块链，使得区块链在各节点一致
205
其他医疗节点通过患者提供的授权查看的私钥获取患者的医疗数据信息
206
当患者丢失私钥或公钥，区块链内的任一医疗节点根据患者的唯一识别号，通过区块链内的预设私有算法，获得私钥或公钥
207

图2


P2P网络构建模块31
档案建立模块32
加密模块33
数据共享模块34
区块链构建模块35
获取模块36
丢失信息获取模块37

图3

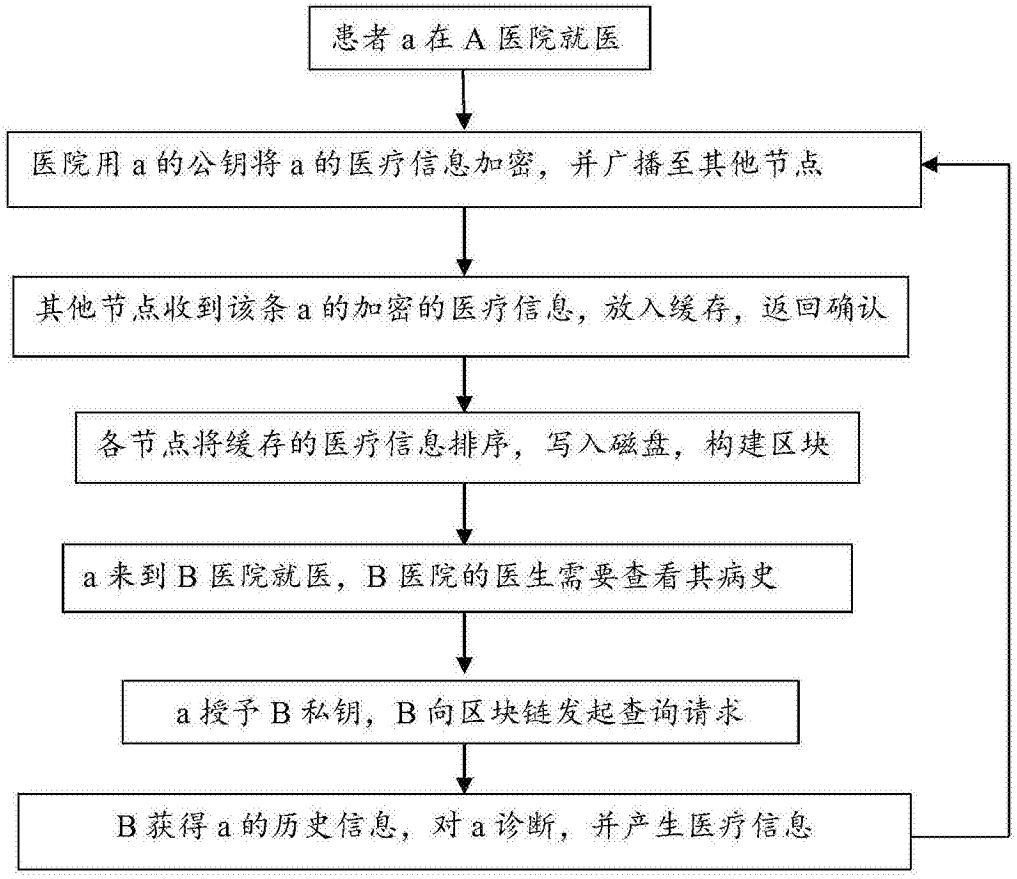

患者a在A医院就医
医院用a的公钥将a的医疗信息加密，并广播至其他节点
其他节点收到该条a的加密的医疗信息，放入缓存，返回确认
各节点将缓存的医疗信息排序，写入磁盘，构建区块
a来到B医院就医，B医院的医生需要查看其病史
a授予B私钥，B向区块链发起查询请求
B获得a的历史信息，对a诊断，并产生医疗信息

图4