(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110299195 B
(45)授权公告日 2023.05.30

(21)申请号 201910500453.3
(22)申请日 2019.06.11
(65)同一申请的已公布的文献号
申请公布号 CN 110299195 A
(43)申请公布日 2019.10.01
(73)专利权人 中国矿业大学
地址 221116 江苏省徐州市大学路1号南湖校区
(72)发明人 姜顺荣 王虹 周勇
(74)专利代理机构 南京苏高专利商标事务所(普通合伙) 32204
专利代理师 唐红
(51)Int.Cl.
G16H 10/60(2018.01)
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/30(2006.01)
H04L 67/1097(2022.01)
G06F 21/60(2013.01)
G06Q 20/38(2012.01)
H04L 9/40(2022.01)

审查员 谭碧云

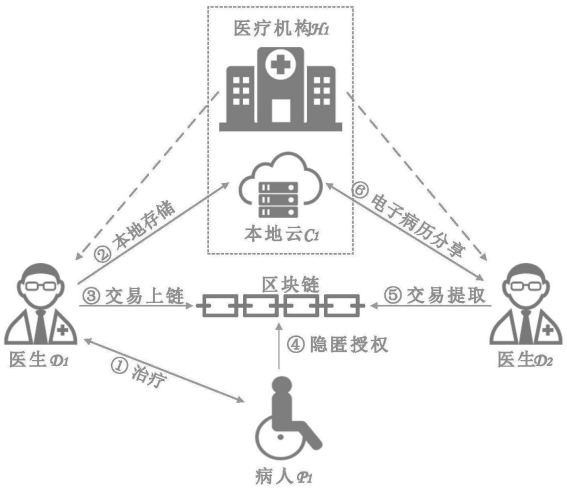
权利要求书6页 说明书13页 附图3页

(54)发明名称

基于联盟链的具有隐私保护的电子病历共享系统及应用方法

(57)摘要

本发明公开一种基于区块链的具有隐私保护的电子病历共享系统及应用方法，包括医疗管理部门、医疗机构和医疗服务接收方，实现系统初始化、注册、电子病历共享、电子病历删除等操作。本发明通过隐匿授权机制，实现电子病历分享过程的隐私保护，并能够实现两种场景下的电子病历共享：在同一医院不同医生之间的电子病历共享以及在不同医院的不同医生之间的电子病历共享，在电子病历分享过程中，病人对其电子病历拥有完全的控制权。另外，在电子病历超出有效期之后，各医疗机构的本地云端和区块链对电子病历进行删除操作。



CN 110299195 B

1.一种基于联盟链的具有隐私保护的电子病历共享系统，其特征在于：包括医疗管理部门$\mathcal{M}$、医疗机构和医疗服务接收方，所述医疗管理部门是系统中的可信机构，根据政府法规管理医疗机构，在医疗服务接收方和医疗机构加入联盟链之前对其进行身份验证和注册；所述医疗机构是指提供医疗服务的医院、诊所和疗养院，医疗机构为病人提供医疗服务，且在通过区块链技术获取病人的授权之后，访问病人的电子病历，并在治疗过程中可以添加新的电子病历，并将其存储于本地云和区块链；所述医疗服务接收方是病人及其家属的统称，病人具有本人电子病例的访问权，必要情况下更新电子病历，在病人没有决策能力的情况下，可向其家属或医疗机构管理人员授予访问权限；

该共享系统的应用方法包括如下步骤：

(1)系统初始化：

(1.1)医疗管理部门$\mathcal{M}$选取有限域GF的椭圆曲线E，其中，GF(p)是有限域q的素数阶，G是椭圆曲线E的基点，l是G对应的素数阶；

(1.2)医疗管理部门$\mathcal{M}$选取两个哈希函数h_1和h_2，其中$h_1: E \to \mathbb{Z}_p^*$，

$h_2: \{0,1\}^* \to \mathbb{Z}_q^*$；

(1.3)$\mathcal{M}$发布系统参数(q,p,E,G,l,h_1,h_2)；

(1.4)系统中每一个参与方需要注册一个以太坊账号/地址$ID_{\mathcal{U}_i}$，其中$\mathcal{U}_i$包含医疗管理部门$\mathcal{M}$，医院$\mathcal{H}_i$，病人$\mathcal{P}_i$；$ID_{\mathcal{U}_i}$的私钥和公钥分别为$SK_{\mathcal{U}_i}$，$PK_{\mathcal{U}_i}$；

(1.5)$\mathcal{M}$设置不同形式的交易格式用于删除操作；

(2)注册，即医生在加入系统之前，在医疗管理机构进行注册另外，身份为$ID_{\mathcal{H}_i}$的医疗机构$\mathcal{H}_i$向医疗管理机构$\mathcal{M}$注册并申请证书$Cer_{\mathcal{M},\mathcal{H}_i} = Sig_{SK_{\mathcal{M}}}(T, ID_{\mathcal{H}_i}, PK_{\mathcal{H}_i})$；然后每一个工作在医院$\mathcal{H}_i$的医生$\mathcal{D}_i$会获取证书$Cer_{\mathcal{H}_i,\mathcal{D}_i} = Sig_{SK_{\mathcal{H}_i}}(T, ID_{\mathcal{D}_i}, PK_{\mathcal{D}_i})$；T是证书验证的周期；

(3)电子病历共享：

(3.1)病人$\mathcal{P}_i$前往医院$\mathcal{H}_1$的医生$\mathcal{D}_1$处接受治疗；在治疗过程中，医生$\mathcal{D}_1$为病人$\mathcal{P}_i$生成一个阶段的治疗记录$EHR_{\mathcal{P}_i}$，并对$EHR_{\mathcal{P}_i}$进行加密$CEHR_{\mathcal{P}_i} = Enc_{K_{\mathcal{P}_i}}(EHR_{\mathcal{P}_i})$，电子病历的加密/解密方式为AES-128，所用密钥为病人$\mathcal{P}_i$的电子病历共享密钥$K_{\mathcal{P}_i}$，由病人$\mathcal{P}_i$选取的128位随机数生成；

(3.2)医生$\mathcal{D}_1$将$CEHR_{\mathcal{P}_i}$存储在医院$\mathcal{H}_1$的本地云$\mathcal{C}_1$中，并计算$CEHR_{\mathcal{P}_i}$的哈希值$eh_1 = h_2(CEHR_{\mathcal{P}_i})$；

(3.3)$\mathcal{D}_1$向$\mathcal{H}_1$发送交易以便在区块链上记录治疗记录：

$\mathcal{D}_1 \to \mathcal{H}_1: T_1, Ty_1, eh_1$，$T_1$是日期，$Ty_1$是交易类型；

(3.4)$\mathcal{P}_i$为$CEHR_{\mathcal{P}_i}$创建索引以实现电子病历共享：

$$\begin{cases}\mathcal{X}_i=h_2(\mathcal{H}_1\|T_1\|0,k_t)\\ \mathcal{Y}_i=h_2(\mathcal{H}_1\|T_1\|1,k_t)\\ \mathcal{Z}_i=txid\oplus\mathcal{Y}_i\\ \mathcal{K}_i=K_{\mathcal{P}_i}\oplus\mathcal{Y}_i\end{cases},$$

其中，k_t是由病人$\mathcal{P}_i$选择的随机密钥，txid是交易ID；

(3.5) $\mathcal{D}_1$将$CEHR_{\mathcal{P}_i}$的索引$\mathcal{X}_i,\mathcal{Y}_i,\mathcal{Z}_i,\mathcal{K}_i$发送到$\mathcal{C}_1$，并由$\mathcal{C}_1$存储索引信息：

(3.6)最后将上述电子病历进行共享，包括两种情况：在同一医院不同医生之间的电子病历共享和在不同医院的不同医生之间的电子病历共享；

(4)电子病历删除；

(4.1)当电子病历超过有效期时，医院的本地云将删除对应的电子病历$CEHR_{\mathcal{P}_i}$；

(4.2)电子病历$CEHR_{\mathcal{P}_i}$对应的哈希值也将从区块链中删除；

(4.3)对于已删除的交易，医疗管理机构$\mathcal{M}$创建一个布隆过滤器BF_i来存储已删除交易的ID，并以交易的形势广播到区块链网络：

$\mathcal{M}\rightarrow *:Deletion,BlockID,Expired,BF_i$

其中，BlockID为删除的区块号，Expired为交易有效期。

2.根据权利要求1所述的基于联盟链的具有隐私保护的电子病历共享系统的应用方法，其特征在于：步骤(1.5)中$\mathcal{M}$设置的交易格式包括：

Ty_1代表治疗记录，有效期为15年；Ty_2代表住院记录，有效期为30年；Ty_3代表电子病历分享记录，有效期为5年；在交易打包阶段，矿工根据不同的交易类型对交易进行打包；在删除阶段，将按照区块的有效期是否到达，对整个区块进行删除。

3.根据权利要求1所述的基于联盟链的具有隐私保护的电子病历共享系统的应用方法，其特征在于：步骤(2)的详细过程如下：

(2.1) $\mathcal{D}_i$选取椭圆曲线私钥a_i，其中$a_i\in\mathbb{Z}_p^*$；

(2.2) $\mathcal{D}_i$计算对应的椭圆曲线公钥A_i，其中$A_i=a_iG$；

(2.3) $\mathcal{D}_i$发送交易$ID_{\mathcal{D}_i}\|PK_{\mathcal{D}_i}\|A_i$到医疗管理机构$\mathcal{M}$，并安全地存储椭圆曲线私钥$a_i$：

$\mathcal{D}_i\rightarrow\mathcal{M}:ID_{\mathcal{D}_i},PK_{\mathcal{D}_i},A_i$；

当医疗管理机构$\mathcal{M}$接收到交易$ID_{\mathcal{D}_i}\|PK_{\mathcal{D}_i}\|A_i$以后，$\mathcal{M}$运行注册合约验证交易的有效性，验证方法如下：

输入： $ID_{\mathcal{D}_i}$

输出： 验证结果

1：**if** 消息发送方不是$\mathcal{M}$ **then**

2： 舍弃该消息

3：**end if**

4：**if** $ID_{\mathcal{D}_i}$在黑名单列表中 **then**

5： 返回 false

6：**else**

7： **if** $ID_{\mathcal{D}_i}$已存在 **then**

8： $Users[ID_{\mathcal{D}_i}] \leftarrow true$

9： 返回 true

10： **end if**

11：**end if**

(2.4)如果交易通过验证操作，$\mathcal{M}$计算证书：

$$Cer_{\mathcal{M},\mathcal{D}_i} = Sig_{SK_{\mathcal{M}}}(T, ID_{\mathcal{D}_i}, PK_{\mathcal{D}_i}, A_i)$$

其中，T是证书验证的周期，签名算法Sig(•)/签名验证算法Ver(•)采用椭圆曲线签名/验证算法；

(2.5) $\mathcal{M}$通过交易向$\mathcal{D}_i$发送证书：$\mathcal{M} \rightarrow \mathcal{D}_i : T, Cer_{\mathcal{M},\mathcal{D}_i}$。

4.根据权利要求1所述的基于联盟链的具有隐私保护的电子病历共享系统的应用方法，其特征在于：步骤(3)中的存储结构为：

令牌	内容 1	内容 2	内容 3
$\mathcal{X}_1$	$\mathcal{Z}_1$	$\mathcal{K}_1$	$CEHR_{\mathcal{P}_1,1}$
$\mathcal{X}_2$	$\mathcal{Z}_2$	$\mathcal{K}_2$	$CEHR_{\mathcal{P}_2,2}$
…	…	…	…
$\mathcal{X}_i$	$\mathcal{Z}_i$	$\mathcal{K}_i$	$CEHR_{\mathcal{P}_i}$

。

5.根据权利要求1所述的基于联盟链的具有隐私保护的电子病历共享系统的应用方法，其特征在于：步骤(3.6)中当病人$\mathcal{P}_i$在同一医院不同医生之间进行电子病历共享时：病

人$\mathcal{P}_i$向医院$\mathcal{H}_1$的医生$\mathcal{D}_2$分享电子病历，并采用隐匿授权来实现访问权限传输过程中的隐私保护；

其中，隐匿交易生成的具体步骤如下：

1)发送方$\mathcal{P}_i$获取接收方$\mathcal{D}_2$的椭圆曲线公钥A_j，并选取随机数$r_\tau \in \mathbb{Z}_p^*$；

2)$\mathcal{P}_i$计算隐匿标签$ST=h_1(r_\tau A_j)G$和隐匿密钥$R_\tau=r_\tau G$；

3)$\mathcal{P}_i$计算授权内容$AutCon=(\mathcal{H}_1,T_1,k_t)$；

4)$\mathcal{P}_i$加密授权内容$c_1=\mathcal{ENC}_{PK_{\mathcal{D}_2}}(AutCon)$，授权内容的加密/解密方式为椭圆曲线加密/解密；

5)$\mathcal{P}_i$计算打包交易$R_\tau||ST||c_1$，并将交易发送到以太坊网络：

$\mathcal{P}_i \rightarrow *:Ty_3,R_\tau,ST,c_1$；

其中，接收方$\mathcal{D}_2$从新生成的区块中的交易中恢复隐匿授权信息，隐匿授权恢复方法为：

输入： R_τ， ST， c_1

输出： 隐匿授权恢复结果

1： **for** $i=1;i\le n_{tr};i++$ **do**

2： 计算$ST'=h_1(a_jR_\tau)G$

3： **if** $ST'=ST$ **then**

4： 计算$\mathcal{DEC}_{SK_{\mathcal{D}_2}}(c_1)$得到$AutCon$

5： 返回$AutCon$

6： **else**

7： 返回$NULL$

8： **end if**

9： **end for**

$\mathcal{D}_2$获取到解密结果后，通过$\mathcal{D}_2$与$\mathcal{H}_1$的从属关系，计算：

$$\begin{cases}\mathcal{X}_i'=h_2(\mathcal{H}_1\|T_1\|0,k_t)\\ \mathcal{Y}_i'=h_2(\mathcal{H}_1\|T_1\|1,k_t)\end{cases}$$

6）$\mathcal{D}_2$设定令牌$token=\mathcal{X}_i'$并计算签名$sig_1=Sig_{SK_{\mathcal{D}_2}}(token)$；最后，$\mathcal{D}_2$向$\mathcal{H}_1$发送$token\|sig_1\|Cer_{\mathcal{H}_1,\mathcal{D}_2}$；

7)当$\mathcal{H}_1$接收到请求以后，$\mathcal{H}_1$执行以下步骤：

A)$\mathcal{H}_1$检查$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_1,\mathcal{D}_2}$；

B)如果$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_1,\mathcal{D}_2}$有效，$\mathcal{H}_1$检查$\mathcal{D}_2$的签名$\mathrm{sig}_1$；

C)如果$\mathcal{D}_2$的签名sig_1有效，$\mathcal{H}_1$根据$\mathcal{D}_2$传输的token返回$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$给$\mathcal{D}_2$；

8)当$\mathcal{D}_2$接收到$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$以后，$\mathcal{D}_2$执行以下步骤：

A)$\mathcal{D}_2$计算$txid'=\mathcal{Z}_i\oplus\mathcal{Y}_i'$，并计算$K_{\mathcal{P}_i}'=\mathcal{K}_i\oplus\mathcal{Y}_i'$；

B)$\mathcal{D}_2$根据txid′获取eh_1'，并验证等式$h_2(CEHR_{\mathcal{P}_i})=eh_1'$是否成立，如果等式成立，执行步骤3)；

C)$\mathcal{D}_2$解密$Dec_{K_{\mathcal{P}_i}'}(CEHR_{\mathcal{P}_i})$获取$EHR_{\mathcal{P}_i}$，并根据治疗记录为病人提供进一步的治疗。

6.根据权利要求1所述的基于联盟链的具有隐私保护的电子病历共享系统的应用方法，其特征在于：步骤(3.6)中，当病人$\mathcal{P}_i$在不同医院的不同医生之间电子病历共享时：病人$\mathcal{P}_i$从医院$\mathcal{H}_1$转向医院$\mathcal{H}_2$，并向医院$\mathcal{H}_2$的医生$\mathcal{D}_2$分享电子病历；然后进行电子病历的隐匿授权及匿名恢复；经过隐匿授权之后，执行以下操作：

（A）、假定$\mathcal{D}_2$从以太坊交易中恢复隐匿交易并获取到隐匿授权内容$AutCon=(\mathcal{H}_1,T_1,k_t)$；

（B）、由于$\mathcal{D}_2$和$\mathcal{H}_1$不具有从属关系，$\mathcal{D}_2$计算$\mathcal{X}_i'=h_2(\mathcal{H}_1\|T_1\|0,k_t)$以及$\mathcal{Y}_i'=h_2(\mathcal{H}_1\|T_1\|1,k_t)$；

（C）、$\mathcal{D}_2$设定$token=\mathcal{X}_i'$并计算签名$sig_1=Sig_{SK_{\mathcal{D}_2}}(token\|\mathcal{H}_1)$；最后，$\mathcal{D}_2$向$\mathcal{H}_2$发送$token\|\mathcal{H}_1\|sig_1\|Cer_{\mathcal{H}_2,\mathcal{D}_2}$；

(D)、当$\mathcal{H}_2$接收到请求信息，$\mathcal{H}_2$执行以下步骤：

1)$\mathcal{H}_2$验证$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_2,\mathcal{D}_2}$的有效性；

2)如果$\mathcal{D}_2$的证书有效，进一步地，$\mathcal{H}_2$验证$\mathcal{D}_2$签名sig_1的有效性；

3)如果$\mathcal{D}_2$签名有效，进一步地，$\mathcal{H}_2$计算$sig_2=Sig_{SK_{\mathcal{H}_2}}(token)$并向$\mathcal{H}_1$发送交易：

$\mathcal{H}_2\rightarrow\mathcal{H}_1:Ty_3,token,sig_2,Cer_{\mathcal{M},\mathcal{H}_2}$；

(E)、当$\mathcal{H}_1$接收到$\mathcal{H}_2$的电子病历分享请求交易，$\mathcal{H}_1$执行以下步骤：

1)$\mathcal{H}_1$检查$\mathcal{H}_2$的证书$Cer_{\mathcal{M},\mathcal{H}_2}$的有效性；

2)如果$\mathcal{H}_2$的证书有效，$\mathcal{H}_1$验证$\mathcal{H}_2$的签名sig_2；

3)如果$\mathcal{H}_2$的签名有效，$\mathcal{H}_1$根据$\mathcal{H}_2$传输的token返回$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$给$\mathcal{H}_2$；

(F)、当$\mathcal{H}_2$接收到$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$之后，$\mathcal{H}_2$将其转发给$\mathcal{D}_2$；$\mathcal{D}_2$执行以下步骤：

1)$\mathcal{D}_2$计算$txid'=\mathcal{Z}_i\oplus\mathcal{Y}_i'$，并计算$K_{\mathcal{P}_i}'=\mathcal{K}_i\oplus\mathcal{Y}_i'$；

2)$\mathcal{D}_2$根据txid′获取eh_1'，并验证等式$h_2(CEHR_{\mathcal{P}_i})=eh_1'$是否成立，如果等式成立，执行步骤3)；

3) $\mathcal{D}_2$解密$Dec_{K_{P_i}'}(CEHR_{P_i})$获取$EHR_{P_i}$，并根据治疗记录为病人提供进一步的治疗。

基于联盟链的具有隐私保护的电子病历共享系统及应用方法

技术领域

[0001] 本发明属于电子病历共享技术，具体涉及一种基于联盟链的具有隐私保护的电子病历共享系统及应用方法。

背景技术

[0002] 电子病历(EHR)是病人健康状况相关的数据集，包含医疗状况(疾病等)、药物处方、医学影像以及个人信息(姓名、年龄、性别、体重、票据信息等)。然而，在不同医院之间，病人的医疗信息并不被视为有效的。例如，假定病人从医院$\mathcal{H}_1$转到另一个医院$\mathcal{H}_2$，医院$\mathcal{H}_2$可能无法获取病人在医院$\mathcal{H}_1$的检查结果，医院$\mathcal{H}_2$也可能认为医院$\mathcal{H}_1$的检查结果没有参考价值，因此对于该病人而言，需要在医院$\mathcal{H}_2$重新进行相关检查。在很大程度上，两个医院的检查结果可能是相同的，这将给病人带来巨大的经济负担。因此，允许电子病历在不同医疗机构和不同医生之间以去中心化的方式进行共享，对于增强医疗便利性和灵活性有很大的帮助。考虑到病人的医疗记录涉及病人隐私，因此在电子病历共享过程中应该保护病人的隐私并增强访问控制。另外，为防止恶意参与方破坏系统运行、窥探用户隐私，因此需要考虑数据的可追溯性和可审计性。

[0003] 为实现安全的电子病历共享，最常用的方法是为病人的电子病历建立索引，并在上传到公有云/社区云之前对电子病历进行加密。然而，这种共享方式的弊端是很明显的：不同医院在创建索引和加密电子病历的方式可能不尽相同，因而会产生不同的处理结果，这将阻碍不同机构和个人间的电子病历共享过程。另外，这一共享方式是中心化的架构，需要依赖完全可信的云来实现，因此，数据所有者(病人)将失去其电子病历的控制权。

[0004] 随着区块链技术的发展，为去中心化系统的实现提供了很好的解决方式。区块链技术具有去中心化、不可篡改、可审计等特点，可以满足电子病历共享的安全需求。作为区块链节点，医疗机构可以很方便地使用区块链来存储和验证病人的电子病历。区块链的共识机制也为整个治疗过程提供分布式决策和审计。另外，通过使用智能合约，这些操作可以自动、高效、可信地执行，使得数据共享更加便利。

[0005] 目前已有一些基于区块链的电子病历共享方案，保证了数据完整性、机密性和访问控制，但是这些方案存在一些不足：首先，攻击者可能会获取病人的隐私信息，比如攻击者可能通过区块链上公开的交易信息和数据，推测用户对于医生的偏好情况。为消除这一风险，需要保护电子病历访问权传输过程中病人的隐私。另外，由于医院的云存储空间有限，医院在保存电子病历时通常会为其设置一个有效期，当电子病历达到有效期时，医院会在云端将其删除。然而，虽然云端将数据删除了，区块链上依然存储了该电子病历的信息(散列值)。因此，如何设计针对区块链的删除方案，是一个亟需解决的问题。

发明内容

[0006] 发明目的：本发明的目的在于解决现有技术中存在的不足，提供一种基于联盟链的具有隐私保护的电子病历共享系统及应用方法。

[0007] 技术方案：本发明的一种基于联盟链的具有隐私保护的电子病历共享系统，包括医疗管理部门$\mathcal{M}$、医疗机构和医疗服务接收方，所述医疗管理部门是系统中的可信机构，根据政府法规管理医疗机构，在医疗服务接收方和医疗机构加入联盟链之前对其进行身份验证和注册；所述医疗机构是指提供医疗服务的医院、诊所和疗养院，医疗机构为病人提供医疗服务，且在获取病人的授权之后，访问病人的电子病历，并在治疗过程中可以添加新的电子病历；所述医疗服务接收方是病人及其家属的统称，病人具有本人电子病例的访问权，必要情况下更新电子病历，在病人没有决策能力的情况下，向其家属或医疗机构管理人员授予访问权限。

[0008] 本发明还公开了一种基于联盟链的具有隐私保护的电子病历共享系统的应用方法，包括以下步骤：

[0009] (1)系统初始化；

[0010] (1.1)医疗管理部门$\mathcal{M}$选取有限域GF的椭圆曲线E，其中，GF(p)是有限域q的素数阶，G是椭圆曲线E的基点，1是G对应的素数阶；

[0011] (1.2)医疗管理部门$\mathcal{M}$选取两个哈希函数h_1和h_2，其中$h_1:E\rightarrow\mathbb{Z}_p^*$，$h_2:\{0,1\}^*\rightarrow\mathbb{Z}_q^*$；

[0012] (1.3)$\mathcal{M}$发布系统参数(q,p,E,G,1,h_1,h_2)；

[0013] (1.4)系统中每一个参与方需要注册一个以太坊账号/地址$ID_{\mathcal{U}_i}$，其中$\mathcal{U}_i$包含医疗管理部门$\mathcal{M}$，医院$\mathcal{H}_i$，病人$\mathcal{P}_i$；$ID_{\mathcal{U}_i}$的私钥和公钥分别为$SK_{\mathcal{U}_i}$，$PK_{\mathcal{U}_i}$；

[0014] (1.5)$\mathcal{M}$设置不同形式的交易格式用于删除操作；

[0015] (2)注册，即医生在加入系统之前，在医疗管理机构进行注册

[0016] 另外，身份为$ID_{\mathcal{H}_i}$的医疗机构$\mathcal{H}_i$向医疗管理机构$\mathcal{M}$注册并申请证书$Cer_{\mathcal{M},\mathcal{H}_i}=Sig_{SK_{\mathcal{M}}}(T,ID_{\mathcal{H}_i},PK_{\mathcal{H}_i})$；然后每一个工作在医院$\mathcal{H}_i$的医生$\mathcal{D}_i$会获取证书$Cer_{\mathcal{H}_i,\mathcal{D}_i}=Sig_{SK_{\mathcal{H}_i}}(T,ID_{\mathcal{D}_i},PK_{\mathcal{D}_i})$；T是证书验证的周期；

[0017] (3)电子病历共享：

[0018] (3.1)病人$\mathcal{P}_i$前往医院$\mathcal{H}_1$的医生$\mathcal{D}_1$处接受治疗；在治疗过程中，医生$\mathcal{D}_1$为病人$\mathcal{P}_i$生成一个阶段的治疗记录$EHR_{\mathcal{P}_i}$，并对$EHR_{\mathcal{P}_i}$进行加密$CEHR_{\mathcal{P}_i}=Enc_{K_{\mathcal{P}_i}}(EHR_{\mathcal{P}_i})$，电子病历的加密/解密方式为AES-128，所用密钥为病人$\mathcal{P}_i$的电子病历共享密钥$K_{\mathcal{P}_i}$，由病人$\mathcal{P}_i$选取的128位随机数生成；

[0019] (3.2)医生$\mathcal{D}_1$将$CEHR_{\mathcal{P}_i}$存储在医院$\mathcal{H}_1$的本地云$\mathcal{C}_1$中，并计算$CEHR_{\mathcal{P}_i}$的哈希值$eh_1=h_2(CEHR_{\mathcal{P}_i})$；

[0020] (3.3)$\mathcal{D}_1$向$\mathcal{H}_1$发送交易以便在区块链上记录治疗记录：

[0021] $\mathcal{D}_1\rightarrow\mathcal{H}_1:T_1,Ty_1,eh_1$，$T_1$是日期，$Ty_1$是交易类型；

[0022] (3.4)$\mathcal{P}_i$为$CEHR_{\mathcal{P}_i}$创建索引以实现电子病历共享：

[0023] $$\begin{cases}\mathcal{X}_i=h_2(\mathcal{H}_1\|T_1\|0,k_t)\\ \mathcal{Y}_i=h_2(\mathcal{H}_1\|T_1\|1,k_t)\\ \mathcal{Z}_i=txid\oplus\mathcal{Y}_i\\ \mathcal{K}_i=K_{\mathcal{P}_i}\oplus\mathcal{Y}_i\end{cases},$$

[0024] 其中，k_t是由病人$\mathcal{P}_i$选择的随机密钥，txid是交易ID；

[0025] (3.5) $\mathcal{D}_1$将$CEHR_{\mathcal{P}_i}$的索引$\mathcal{X}_i,\mathcal{Y}_i,\mathcal{Z}_i,\mathcal{K}_i$发送到$\mathcal{C}_1$，并由$\mathcal{C}_1$存储索引信息：

[0026] (3.6)最后将上述电子病历进行共享，包括两种情况：在同一医院不同医生之间的电子病历共享和在不同医院的不同医生之间的电子病历共享；

[0027] (4)电子病历删除；

[0028] (4.1)当电子病历超过有效期时，医院的本地云将删除对应的电子病历

[0029] $CEHR_{\mathcal{P}_i}$；

[0030] (4.2)电子病历$CEHR_{\mathcal{P}_i}$对应的哈希值也将从区块链中删除；

[0031] (4.3)对于已删除的交易，医疗管理机构$\mathcal{M}$创建一个布隆过滤器BF_i来存储已删除交易的ID，并以交易的形势广播到区块链网络：

[0032] $\mathcal{M}\rightarrow *:Deletion,BlockID,Expired,BF_i$

[0033] 其中，BlockID为删除的区块号，Expired为交易有效期。

[0034] 进一步的，步骤(1.5)中$\mathcal{M}$设置的交易格式包括：

[0035] Ty_1代表治疗记录，有效期为15年；Ty_2代表住院记录，有效期为30年；Ty_3代表电子病历分享记录，有效期为5年；在交易打包阶段，矿工根据不同的交易类型对交易进行打包；在删除阶段，将按照区块的有效期是否到达，对整个区块进行删除，如表1所示。

[0036] 表1不同交易类型

[0037]

操作	交易类型	有效期
治疗	Ty_1	15年
住院	Ty_2	30年
分享	Ty_3	5年
……	……	……

[0038] 进一步的，步骤(2)的详细过程如下：

[0039] (2.1) $\mathcal{D}_i$选取椭圆曲线私钥a_i，其中$a_i\in\mathbb{Z}_p^*$；

[0040] (2.2) $\mathcal{D}_i$计算对应的椭圆曲线公钥A_i，其中$A_i=a_iG$；

[0041] (2.3) $\mathcal{D}_i$发送交易$ID_{\mathcal{D}_i}\|PK_{\mathcal{D}_i}\|A_i$到医疗管理机构$\mathcal{M}$，并安全地存储椭圆曲线私钥$a_i$：

[0042] $\mathcal{D}_i\rightarrow\mathcal{M}:ID_{\mathcal{D}_i},PK_{\mathcal{D}_i},A_i$；

[0043] 当医疗管理机构$\mathcal{M}$接收到交易$ID_{\mathcal{D}_i}\|PK_{\mathcal{D}_i}\|A_i$以后，$\mathcal{M}$运行注册合约验证交易的有效性，验证方法如下：

输入： $ID_{\mathcal{D}_i}$

输出： 验证结果

1：**if** 消息发送方不是$\mathcal{M}$ **then**

2： 舍弃该消息

3：**end if**

4：**if** $ID_{\mathcal{D}_i}$在黑名单列表中 **then**

[0044] 5： 返回 false

6：**else**

7： **if** $ID_{\mathcal{D}_i}$已存在 **then**

8： $Users[ID_{\mathcal{D}_i}] \leftarrow true$

9： 返回 true

10： **end if**

11：**end if**

[0045] (2.4)如果交易通过验证操作，$\mathcal{M}$计算证书：

[0046] $Cer_{\mathcal{M},\mathcal{D}_i} = Sig_{SK_{\mathcal{M}}}(T, ID_{\mathcal{D}_i}, PK_{\mathcal{D}_i}, A_i)$

[0047] 其中，T是证书验证的周期，签名算法Sig(•)/签名验证算法Ver(•)采用椭圆曲线签名/验证算法；

[0048] (2.5) $\mathcal{M}$通过交易向$\mathcal{D}_i$发送证书：$\mathcal{M} \rightarrow \mathcal{D}_i : T, Cer_{\mathcal{M},\mathcal{D}_i}$。

[0049] 进一步的，步骤(3)中的存储结构如表2所示：

[0050] 表2本地云$\mathcal{C}_1$中的存储结构

[0051]

令牌	内容 1	内容 2	内容 3

[0052]

$\mathcal{X}_1$	$\mathcal{Z}_1$	$\mathcal{K}_1$	$CEHR_{\mathcal{P}_1,1}$
$\mathcal{X}_2$	$\mathcal{Z}_2$	$\mathcal{K}_2$	$CEHR_{\mathcal{P}_2,2}$
…	…	…	…
$\mathcal{X}_i$	$\mathcal{Z}_i$	$\mathcal{K}_i$	$CEHR_{\mathcal{P}_i}$

[0053] 进一步的，步骤(3.6)中当同一医院不同医生之间的电子病历共享时：病人$\mathcal{P}_i$向医院$\mathcal{H}_1$的医生$\mathcal{D}_2$分享电子病历，并采用隐匿授权来实现访问权限传输过程中的隐私保护；

[0054] 其中，隐匿交易生成的具体步骤如下：

[0055] 1)发送方$\mathcal{P}_i$获取接收方$\mathcal{D}_2$的椭圆曲线公钥A_j,并选取随机数$r_\tau \in \mathbb{Z}_p^*$;

[0056] 2) $\mathcal{P}_i$计算隐匿标签$ST=h_1(r_\tau A_j)G$和隐匿密钥$R_\tau=r_\tau G$;

[0057] 3) $\mathcal{P}_i$计算授权内容$AutCon=(\mathcal{H}_1,T_1,k_t)$;

[0058] 4) $\mathcal{P}_i$加密授权内容$c_1=\mathcal{ENC}_{PK_{\mathcal{D}_2}}(AutCon)$,授权内容的加密/解密方式为椭圆曲线加密/解密;

[0059] 5) $\mathcal{P}_i$计算打包交易$R_\tau||ST||c_1$,并将交易发送到以太坊网络:

[0060] $\mathcal{P}_i \rightarrow *: Ty_3, R_\tau, ST, c_1$;

[0061] 其中,接收方$\mathcal{D}_2$从新生成的区块中的交易中(假定数量是n_{tr})恢复隐匿授权信息,隐匿授权恢复方法为:

[0062]

输入: R_τ, ST, c_1

输出: 隐匿授权恢复结果

1: **for** $i=1; i \le n_{tr}; i++$ **do**

2: 计算$ST' = h_1(a_j R_\tau)G$

3: **if** $ST' = ST$ **then**

4: 计算$\mathcal{DEC}_{SK_{\mathcal{D}_2}}(c_1)$得到$AutCon$

5: 返回$AutCon$

6: **else**

[0063] 7: 返回$NULL$

8: **end if**

9: **end for**

[0064] $\mathcal{D}_2$获取到解密结果后,通过$\mathcal{D}_2$与$\mathcal{H}_1$的从属关系,计算:

[0065]
$$\begin{cases} \mathcal{X}_i' = h_2(\mathcal{H}_1 \| T_1 \| 0, k_t) \\ \mathcal{Y}_i' = h_2(\mathcal{H}_1 \| T_1 \| 1, k_t) \end{cases}$$

[0066] 6) $\mathcal{D}_2$设定令牌$token=\mathcal{X}_i'$并计算签名$sig_1=Sig_{SK_{\mathcal{D}_2}}(token)$;最后,$\mathcal{D}_2$向$\mathcal{H}_1$发送$token \| sig_1 \| Cer_{\mathcal{H}_1,\mathcal{D}_2}$;

[0067] 7)当$\mathcal{H}_1$接收到请求以后,$\mathcal{H}_1$执行以下步骤:

[0068] A) $\mathcal{H}_1$检查$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_1,\mathcal{D}_2}$;

[0069] B)如果$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_1,\mathcal{D}_2}$有效，$\mathcal{H}_1$检查$\mathcal{D}_2$的签名$\mathrm{sig}_1$；

[0070] C)如果$\mathcal{D}_2$的签名sig_1有效，$\mathcal{H}_1$根据$\mathcal{D}_2$传输的token返回$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$给$\mathcal{D}_2$；

[0071] 8)当$\mathcal{D}_2$接收到$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$以后，$\mathcal{D}_2$执行以下步骤：

[0072] A)$\mathcal{D}_2$计算$txid'=\mathcal{Z}_i\oplus\mathcal{Y}_i'$，并计算$K_{\mathcal{P}_i}'=\mathcal{K}_i\oplus\mathcal{Y}_i'$；

[0073] B)$\mathcal{D}_2$根据txid′获取eh_1'，并验证等式$h_2(CEHR_{\mathcal{P}_i})=eh_1'$是否成立，如果等式成立，执行步骤3)；

[0074] C)$\mathcal{D}_2$解密$Dec_{K_{\mathcal{P}_i}'}(CEHR_{\mathcal{P}_i})$获取$EHR_{\mathcal{P}_i}$，并根据治疗记录为病人提供进一步的治疗。

[0075] 进一步的，步骤(3.6)中，当不同医院的不同医生之间电子病历共享时：病人$\mathcal{P}_i$从医院$\mathcal{H}_1$转向医院$\mathcal{H}_2$，并向医院$\mathcal{H}_2$的医生$\mathcal{D}_2$分享电子病历；然后进行电子病历的隐匿授权及匿名恢复；经过隐匿授权之后，执行以下操作：

[0076] (A)、假定$\mathcal{D}_2$从以太坊交易中恢复隐匿交易并获取到隐匿授权内容$AutCon=(\mathcal{H}_1,T_1,k_t)$；

[0077] (B)、由于$\mathcal{D}_2$和$\mathcal{H}_1$不具有从属关系，$\mathcal{D}_2$计算$\mathcal{X}_i'=h_2(\mathcal{H}_1\|T_1\|0,k_t)$以及$\mathcal{Y}_i'=h_2(\mathcal{H}_1\|T_1\|1,k_t)$；

[0078] (C)、$\mathcal{D}_2$设定$token=\mathcal{X}_i'$并计算签名$sig_1=Sig_{SK_{\mathcal{D}_2}}(token\|\mathcal{H}_1)$；最后，$\mathcal{D}_2$向$\mathcal{H}_2$发送$token\|\mathcal{H}_1\|sig_1\|Cer_{\mathcal{H}_2,\mathcal{D}_2}$；

[0079] (D)、当$\mathcal{H}_2$接收到请求信息，$\mathcal{H}_2$执行以下步骤：

[0080] 1)$\mathcal{H}_2$验证$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_2,\mathcal{D}_2}$的有效性；

[0081] 2)如果$\mathcal{D}_2$的证书有效，进一步地，$\mathcal{H}_2$验证$\mathcal{D}_2$签名sig_1的有效性；

[0082] 3)如果$\mathcal{D}_2$签名有效，进一步地，$\mathcal{H}_2$计算$sig_2=Sig_{SK_{\mathcal{H}_2}}(token)$并向$\mathcal{H}_1$发送交易：

[0083] $\mathcal{H}_2\rightarrow\mathcal{H}_1:Ty_3,token,sig_2,Cer_{\mathcal{M},\mathcal{H}_2}$；

[0084] (E)、当$\mathcal{H}_1$接收到$\mathcal{H}_2$的电子病历分享请求交易，$\mathcal{H}_1$执行以下步骤：

[0085] 1)$\mathcal{H}_1$检查$\mathcal{H}_2$的证书$Cer_{\mathcal{M},\mathcal{H}_2}$的有效性；

[0086] 2)如果$\mathcal{H}_2$的证书有效，$\mathcal{H}_1$验证$\mathcal{H}_2$的签名sig_2；

[0087] 3)如果$\mathcal{H}_2$的签名有效，$\mathcal{H}_1$根据$\mathcal{H}_2$传输的token返回$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$给$\mathcal{H}_2$；(F)、当$\mathcal{H}_2$接收到$(\mathcal{Z}_i,\mathcal{K}_i,CEHR_{\mathcal{P}_i})$之后，$\mathcal{H}_2$将其转发给$\mathcal{D}_2$。$\mathcal{D}_2$执行以下步骤：

[0088] 1)$\mathcal{D}_2$计算$txid'=\mathcal{Z}_i\oplus\mathcal{Y}_i'$，并计算$K_{\mathcal{P}_i}'=\mathcal{K}_i\oplus\mathcal{Y}_i'$；

[0089] 2)$\mathcal{D}_2$根据txid′获取eh_1'，并验证等式$h_2(CEHR_{\mathcal{P}_i})=eh_1'$是否成立，如果等式成立，执行步骤3)；

[0090] 3) $\mathcal{D}_2$ 解密 $Dec_{K_{\mathcal{P}_i}'}(CEHR_{\mathcal{P}_i})$ 获取 $EHR_{\mathcal{P}_i}$，并根据治疗记录为病人提供进一步的治。

[0091] 有益效果：本发明通过隐匿授权机制，实现电子病历分享过程的隐私保护；并且能够实现两种场景下的电子病历共享：在同一医院不同医生之间的电子病历共享以及在不同医院的不同医生之间的电子病历共享，在电子病历分享过程中，病人对其电子病历拥有完全的控制权，在电子病历超出有效期之后，各医疗机构的本地云端和区块链对电子病历进行删除操作。

[0092] 总之，本发明具有以下优点：病人对其电子病历拥有完全的控制权，没有病人的授权，医疗机构无法获取电子病历的任何信息；并且在电子病历达到有效期后，在云端删除电子病历，并且删除区块链上存储的文件元数据；同时通过区块链交易实现电子病历所有权的传输，并且采用隐匿授权机制，实现电子病历共享过程中的隐私保护。

附图说明

[0093] 图1是本发明中场景一的系统结构图；

[0094] 图2是本发明中场景二的系统结构图；

[0095] 图3是本发明中隐匿授权的生成过程示意图；

[0096] 图4是本发明中隐匿授权的恢复过程示意图；

[0097] 图5是本发明实施例中不同大小电子病历情况下不同操作的时间开销对比图。

具体实施方式

[0098] 下面对本发明技术方案进行详细说明，但是本发明的保护范围不局限于所述实施例。

[0099] 如图1所示，本发明的基于联盟链的具有隐私保护的电子病历共享系统，包括三个实体：医疗管理部门、医疗机构、医疗服务接收方。其中，医疗管理部门是系统中的可信机构，根据政府法规管理医疗机构，在医疗服务接收方和医疗机构加入联盟链之前对其进行身份验证；医疗机构和医疗服务接收方之间的交互是在医疗管理部门的监管之下进行。当医生或者医疗服务接收方存在恶意行为时，医疗管理部门将作为仲裁机构来解决医生和医疗服务接收方之间的纠纷。医疗机构是指提供医疗服务的医院、诊所、疗养院等，主要包含两类员工：医疗人员和管理人员。其中，医疗人员为病人提供医疗服务的员工，比如医生、护士等。医疗人员在获取医疗服务接收方的授权之后，可以访问病人的电子病历，并且在治疗过程中可以添加新的电子病历。管理人员负责医疗机构日常事宜，保证医疗机构正常运转的员工。医疗服务接收方是病人及其家属的统称。病人具有本人电子病例的访问权，必要情况下可更新电子病历。另外，在病人没有决策能力的情况下，可向其家属或医疗机构管理人员授予访问权限。

[0100] 总体来说，本发明的电子病历共享过程中，病人对其电子病历拥有完全的控制权，没有病人的授权，医疗机构无法获取电子病历的任何信息。在电子病历达到有效期后，在云端删除电子病历，并且删除区块链上存储的文件元数据。并且在电子病历共享过程中，通过区块链交易实现电子病历所有权的传输，并且采用隐匿授权机制，实现电子病历共享过程中的隐私保护。

[0101] 上述基于联盟链的具有隐私保护的电子病历共享系统的应用方法，具体过程为：

[0102] 步骤(1)系统初始化：

[0103] 系统初始化操作由医疗管理部门$\mathcal{M}$完成。采用椭圆曲线算法(ECC)来实现隐匿授权。首先，$\mathcal{M}$选取有限域GF的椭圆曲线E，GF(p)是有限域q的素数阶，G是椭圆曲线E的基点，l是G对应的素数阶；选取两个哈希函数h_1和h_2，其中$h_1: E \to \mathbb{Z}_p^*$， $h_2: \{0,1\}^* \to \mathbb{Z}_q^*$。最后，$\mathcal{M}$发布系统参数(q,p,E,G,l,$h_1$,$h_2$)。

[0104] 另外，每一个参与方需要注册一个以太坊账号/地址$ID_{\mathcal{U}_i}$，其中$\mathcal{U}_i$包含医疗管理部门$\mathcal{M}$，医院$\mathcal{H}_i$，病人$\mathcal{P}_i$。$ID_{\mathcal{U}_i}$的私钥和公钥分别为$SK_{\mathcal{U}_i}$， $PK_{\mathcal{U}_i}$。

[0105] 为实现删除操作，$\mathcal{M}$设置几种不同形式的交易格式，其中Ty_1代表治疗记录，有效期为15年；Ty_2代表住院记录，有效期为30年；Ty_3代表电子病历分享记录，有效期为5年。在交易打包阶段，矿工根据不同的交易类型对交易进行打包。在删除阶段，将按照区块的有效期是否到达，对整个区块进行删除。

[0106] (2)注册：

[0107] 即医疗机构以及医生在加入系统之前，在医疗管理机构进行注册。具体地，根据系统参数(q,p,E,G,l,h_1,h_2)，身份为$ID_{\mathcal{D}_i}$医生$\mathcal{D}_i$执行以下操作：

[0108] (2.1) $\mathcal{D}_i$选取椭圆曲线私钥a_i，其中$a_i \in \mathbb{Z}_p^*$；

[0109] (2.2) $\mathcal{D}_i$计算对应的椭圆曲线公钥A_i，其中$A_i = a_i G$；

[0110] (2.3) $\mathcal{D}_i$发送交易$ID_{\mathcal{D}_i} \| PK_{\mathcal{D}_i} \| A_i$到医疗管理机构$\mathcal{M}$，并安全地存储椭圆曲线私钥$a_i$：

[0111] $\mathcal{D}_i \to \mathcal{M}: ID_{\mathcal{D}_i}, PK_{\mathcal{D}_i}, A_i$

[0112] 当医疗管理机构$\mathcal{M}$接收到交易$ID_{\mathcal{D}_i} \| PK_{\mathcal{D}_i} \| A_i$以后，$\mathcal{M}$运行注册合约验证交易的有效性，注册合约的交易验证方式如算法1所示。如果交易通过验证操作，$\mathcal{M}$计算证书$Cer_{\mathcal{M},\mathcal{D}_i} = Sig_{SK_{\mathcal{M}}}(T, ID_{\mathcal{D}_i}, PK_{\mathcal{D}_i}, A_i)$，其中，T是证书验证的周期，签名算法Sig(•)/签名验证算法Ver(•)采用椭圆曲线签名/验证算法。$\mathcal{M}$通过交易向$\mathcal{D}_i$发送证书：

[0113] $\mathcal{M} \to \mathcal{D}_i: T, Cer_{\mathcal{M},\mathcal{D}_i}$。

[0114] 另外，身份为$ID_{\mathcal{H}_i}$的医疗机构$\mathcal{H}_i$也向医疗管理机构$\mathcal{M}$注册并申请证书$Cer_{\mathcal{M},\mathcal{H}_i} = Sig_{SK_{\mathcal{M}}}(T, ID_{\mathcal{H}_i}, PK_{\mathcal{H}_i})$。最后，每一个工作在$\mathcal{H}_i$的医生$\mathcal{D}_i$会获取证书$Cer_{\mathcal{H}_i,\mathcal{D}_i} = Sig_{SK_{\mathcal{H}_i}}(T, ID_{\mathcal{D}_i}, PK_{\mathcal{D}_i})$。

算法 1 注册合约

输入： $ID_{\mathcal{D}_i}$

输出： 验证结果

1：**if** 消息发送方不是$\mathcal{M}$ **then**

2： 舍弃该消息

3：**end if**

4：**if** $ID_{\mathcal{D}_i}$在黑名单列表中 **then**

5： 返回 false

6：**else**

7： **if** $ID_{\mathcal{D}_i}$已存在 **then**

8： $Users[ID_{\mathcal{D}_i}] \leftarrow true$

9： 返回 true

10： **end if**

11：**end if**

[0115]

[0116]

[0117] 步骤(3)电子病历共享

[0118] 如图1所示，病人$\mathcal{P}_i$前往医院$\mathcal{H}_1$的医生$\mathcal{D}_1$处接受治疗。在治疗过程中，医生$\mathcal{D}_1$为病人$\mathcal{P}_i$生成一个阶段的治疗记录$EHR_{\mathcal{P}_i}$，并对$EHR_{\mathcal{P}_i}$进行加密$CEHR_{\mathcal{P}_i} = Enc_{K_{\mathcal{P}_i}}(EHR_{\mathcal{P}_i})$，其中，电子病历的加密/解密方式为AES-128，所用密钥为病人$\mathcal{P}_i$的电子病历共享密钥$K_{\mathcal{P}_i}$，由病人$\mathcal{P}_i$选取的128位随机数生成。进一步地，医生$\mathcal{D}_1$将$CEHR_{\mathcal{P}_i}$存储在医院$\mathcal{H}_1$的本地云$\mathcal{C}_1$中，并计算$CEHR_{\mathcal{P}_i}$的哈希值$eh_1 = h_2(CEHR_{\mathcal{P}_i})$。为了在区块链上记录治疗记录，$\mathcal{D}_1$向$\mathcal{H}_1$发送交易：

[0119] $\mathcal{D}_1 \rightarrow \mathcal{H}_1 : T_1, Ty_1, eh_1$，

[0120] 其中，T_1是日期，Ty_1是交易类型。

[0121] 为实现电子病历共享，$\mathcal{P}_i$为$CEHR_{\mathcal{P}_i}$创建索引：

[0122]
$$\begin{cases} \mathcal{X}_i = h_2(\mathcal{H}_1 \| T_1 \| 0, k_t) \\ \mathcal{Y}_i = h_2(\mathcal{H}_1 \| T_1 \| 1, k_t) \\ \mathcal{Z}_i = txid \oplus \mathcal{Y}_i \\ \mathcal{K}_i = K_{\mathcal{P}_i} \oplus \mathcal{Y}_i \end{cases},$$

[0123] 其中，k_t是病人$\mathcal{P}_i$选择的随机密钥，txid是交易ID。

[0124] $\mathcal{D}_1$将$CEHR_{P_i}$的索引$\mathcal{X}_i,\mathcal{Y}_i,\mathcal{Z}_i,\mathcal{K}_i$发送到$\mathcal{C}_1$，并由$\mathcal{C}_1$存储索引信息。

[0125] 如图1和图2所示，本发明考虑两种情形下的电子病历共享：1)在同一医院不同医生之间的电子病历共享2)在不同医院的不同医生之间的电子病历共享。

[0126] (3.1)场景一：同一医院不同医生之间的电子病历共享：如图2所示，病人$\mathcal{P}_i$向医院$\mathcal{H}_1$的医生$\mathcal{D}_2$分享电子病历。在这种情形下，我们采用隐匿授权来实现访问权限传输过程中的隐私保护。如图3所示，交易生成的具体步骤如下：

[0127] 1)发送方$\mathcal{P}_i$获取接收方$\mathcal{D}_2$的椭圆曲线公钥A_j，并生成随机数$r_\tau \in \mathbb{Z}_p^*$；

[0128] 2) $\mathcal{P}_i$计算隐匿标签$ST=h_1(r_\tau A_j)G$和隐匿密钥$R_\tau=r_\tau G$；

[0129] 3) $\mathcal{P}_i$计算授权内容$AutCon=(\mathcal{H}_1,T_1,k_t)$；

[0130] 4) $\mathcal{P}_i$加密授权内容$c_1=\mathcal{ENC}_{PK_{\mathcal{D}_2}}(AutCon)$，授权内容的加密/解密方式为椭圆曲线加密/解密；

[0131] 5) $\mathcal{P}_i$计算打包交易$R_\tau||ST||c_1$，并将交易发送到以太坊网络：

[0132] $\mathcal{P}_i \rightarrow *: Ty_3, R_\tau, ST, c_1$。

[0133] 如图4所示，接收方$\mathcal{D}_2$按照算法2所示步骤从新生成的区块中的交易中(假定数量是n_{tr})提取隐匿授权信息。

算法 2 隐匿授权恢复

输入： R_τ， ST， c_1

输出： 隐匿授权恢复结果

1： **for** $i=1;i\le n_{tr};i++$ **do**

2： 计算$ST'=h_1(a_jR_\tau)G$

[0134] 3： **if** $ST'=ST$ **then**

4： 计算$\mathcal{DEC}_{SK_{\mathcal{D}_2}}(c_1)$得到$AutCon$

5： 返回$AutCon$

6： **else**

7： 返回$NULL$

8： **end if**

9： **end for**

[0135] $\mathcal{D}_2$获取到解密结果后，可以通过$\mathcal{D}_2$与$\mathcal{H}_1$的从属关系，计算：

[0136] $$\begin{cases}\mathcal{X}_i' = h_2(\mathcal{H}_1 \| T_1 \| 0, k_t) \\ \mathcal{Y}_i' = h_2(\mathcal{H}_1 \| T_1 \| 1, k_t)\end{cases}$$

[0137] $\mathcal{D}_2$ 设定 $token = \mathcal{X}_i'$ 并计算签名 $sig_1 = Sig_{SK_{\mathcal{D}_2}}(token)$。最后，$\mathcal{D}_2$ 向 $\mathcal{H}_1$ 发送 $token \| sig_1 \| Cer_{\mathcal{H}_1,\mathcal{D}_2}$。

[0138] 当$\mathcal{H}_1$接收到请求以后，$\mathcal{H}_1$执行以下步骤：

[0139] 1) $\mathcal{H}_1$检查$\mathcal{D}_2$的证书$Cer_{\mathcal{H}_1,\mathcal{D}_2}$；

[0140] 2)如果$\mathcal{D}_2$的证书有效，$\mathcal{H}_1$检查$\mathcal{D}_2$的签名；

[0141] 3)如果$\mathcal{D}_2$的签名有效，$\mathcal{H}_1$根据$\mathcal{D}_2$传输的token返回$(\mathcal{Z}_i, \mathcal{K}_i, CEHR_{\mathcal{P}_i})$给$\mathcal{D}_2$。

[0142] 当$\mathcal{D}_2$接收到$(\mathcal{Z}_i, \mathcal{K}_i, CEHR_{\mathcal{P}_i})$以后，$\mathcal{D}_2$执行以下步骤：

[0143] 1) $\mathcal{D}_2$计算$txid' = \mathcal{Z}_i \oplus \mathcal{Y}_i'$，并计算$K_{\mathcal{P}_i}' = \mathcal{K}_i \oplus \mathcal{Y}_i'$；

[0144] 2) $\mathcal{D}_2$根据txid′获取eh_1'，并验证等式$h_2(CEHR_{\mathcal{P}_i}) = eh_1'$是否成立，如果等式成立，执行步骤3)；

[0145] 3) $\mathcal{D}_2$解密$Dec_{K_{\mathcal{P}_i}'}(CEHR_{\mathcal{P}_i})$获取$EHR_{\mathcal{P}_i}$，并根据治疗记录为病人提供进一步地治疗。

[0146] (3.2)场景二：不同医院的不同医生之间电子病历共享：在这种场景下，如图2所示，病人$\mathcal{P}_i$向医院$\mathcal{H}_2$的医生$\mathcal{D}_2$分享电子病历。与图1相比，前五个步骤的操作是一样的。经过前五个步骤的操作，假定$\mathcal{D}_2$从以太坊交易中获取到隐匿授权内容$AutCon = (\mathcal{H}_1, T_1, k_t)$，由于$\mathcal{D}_2$和$\mathcal{H}_1$不具有从属关系，$\mathcal{D}_2$计算$\mathcal{X}_i' = h_2(\mathcal{H}_1 \| T_1 \| 0, k_t)$以及$\mathcal{Y}_i' = h_2(\mathcal{H}_1 \| T_1 \| 1, k_t)$，$\mathcal{D}_2$设定$token = \mathcal{X}_i'$并计算签名$sig_1 = Sig_{SK_{\mathcal{D}_2}}(token \| \mathcal{H}_1)$；最后$\mathcal{D}_2$向$\mathcal{H}_2$发送 $token \| \mathcal{H}_1 \| sig_1 \| Cer_{\mathcal{H}_2,\mathcal{D}_2}$。

[0147] 当$\mathcal{H}_2$接收到请求信息，$\mathcal{H}_2$执行以下步骤：

[0148] 1) $\mathcal{H}_2$验证$\mathcal{D}_2$证书$Cer_{\mathcal{H}_2,\mathcal{D}_2}$的有效性；

[0149] 2)如果$\mathcal{D}_2$证书有效，$\mathcal{H}_2$验证$\mathcal{D}_2$签名sig_1的有效性；

[0150] 3)如果$\mathcal{D}_2$签名有效，$\mathcal{H}_2$计算$sig_2 = Sig_{SK_{\mathcal{H}_2}}(token)$并向$\mathcal{H}_1$发送交易：

[0151] $\mathcal{H}_2 \rightarrow \mathcal{H}_1 : Ty_3, token, sig_2, Cer_{\mathcal{M},\mathcal{H}_2}$

[0152] 当$\mathcal{H}_1$接收到$\mathcal{H}_2$的电子病历分享请求交易，$\mathcal{H}_1$执行以下步骤：

[0153] 1) $\mathcal{H}_1$检查$\mathcal{H}_2$的证书$Cer_{\mathcal{M},\mathcal{H}_2}$的有效性；

[0154] 2)如果$\mathcal{H}_2$的证书有效，$\mathcal{H}_1$验证$\mathcal{H}_2$的签名sig_2；

[0155] 3)如果$\mathcal{H}_2$的签名有效，$\mathcal{H}_1$根据$\mathcal{H}_2$传输的token返回$(\mathcal{Z}_i, \mathcal{K}_i, CEHR_{\mathcal{P}_i})$给$\mathcal{H}_2$。

[0156] 当$\mathcal{H}_2$接收到$(\mathcal{Z}_i, \mathcal{K}_i, CEHR_{\mathcal{P}_i})$之后，$\mathcal{H}_2$将其转发给$\mathcal{D}_2$。$\mathcal{D}_2$执行以下步骤：

[0157] 1) $\mathcal{D}_2$计算$txid' = \mathcal{Z}_i \oplus \mathcal{Y}_i'$，并计算$K_{\mathcal{P}_i}' = \mathcal{K}_i \oplus \mathcal{Y}_i'$；

[0158] 2) $\mathcal{D}_2$根据txid′获取eh_1'，并验证等式$h_2(CEHR_{\mathcal{P}_i}) = eh_1'$是否成立，如果等式成立，执行步骤3)；

[0159] 3) $\mathcal{D}_2$解密$Dec_{K_{\mathcal{P}_i}'}(CEHR_{\mathcal{P}_i})$获取$EHR_{\mathcal{P}_i}$，并根据治疗记录为病人提供进一步的治疗。

[0160] 步骤(4)电子病历删除

[0161] 当电子病历超过有效期时，医院的本地云将删除对应的电子病历$CEHR_{\mathcal{P}_i}$。另外，电子病历$CEHR_{\mathcal{P}_i}$对应的哈希值也将从区块链中删除。在本发明所涉及方案中，我们将交易打包成不同的类型，同一区块中的交易有相同的有效期，因此很容易实现删除操作。对于已删除的交易，医疗管理机构$\mathcal{M}$创建一个布隆过滤器BF_i来存储已删除交易的ID，并以交易的形势广播到区块链网络：

[0162] $\mathcal{M} \rightarrow *: Deletion, BlockID, Expired, BF_i$

[0163] 其中，BlockID为删除的区块号，Expired为交易有效期。

[0164] 实施例

[0165] 为评估本发明的性能表现，本实施例在本地部署以太坊测试网络(Ganache)，并在测试网络中执行本发明技术方案。

[0166] 在Ganache中，区块链出块时间设为0。因此在评估系统性能表现时，无需考虑以太坊中复杂网络的影响和挖矿耗时。在本实施例中，Ganache运行在配置为AMD Althlon M320(2.1GHz)处理器，4GB RAM，Manjaro操作系统，千兆以太网卡的电脑上。其中，以太坊地址$ID_{\mathcal{U}_i}$的大小设置为20字节；$h_2(\cdot)$算法采用SHA-256，$h_3(\cdot)$算法采用SHA-3；以太坊的私钥$SK_{\mathcal{U}_i}$和公钥$PK_{\mathcal{U}_i}$分别为32字节和66字节；$K_{\mathcal{P}_i}$和k_t设为128位；$\mathcal{ENC}_K(\cdot)/\mathcal{DEC}_K(\cdot)$算法和$Sig_K(\cdot)/Ver_K(\cdot)$算法都是基于sec p256k1算法实现。

[0167] 实施例性能评估如下：

[0168] 在注册阶段，如表3所示，主要开销包括交易生成和证书计算。

[0169] 表3注册阶段性能表现

[0170]

交易方向	交易大小（字节）	Gas 开销	计算开销（ms）
$\mathcal{D}_i \rightarrow \mathcal{M}$	93	111497	NULL
$\mathcal{M} \rightarrow \mathcal{D}_i$	69	109961	46.026
$\mathcal{H}_i \rightarrow \mathcal{M}$	53	88733	NULL
$\mathcal{M} \rightarrow \mathcal{H}_i$	69	109961	45.726
$\mathcal{D}_i \rightarrow \mathcal{H}_i$	53	88733	NULL
$\mathcal{H}_i \rightarrow \mathcal{D}_i$	69	109961	45.347

[0171] 在电子病历存储阶段，病人$\mathcal{P}_i$需要计算CEHR和$\mathcal{D}_1$并生成eh_1。本实施例测量了不同大小电子病历EHR情况下不同操作的计算开销。计算开销主要由一次盘读写操作产生，并随着电子病历文件体积的增加而增加。为记录治疗过程，$\mathcal{D}_1$向$\mathcal{H}_1$发送交易，交易大小为37字节，gas开销为88709。

[0172] 在隐匿授权阶段，病人$\mathcal{P}_i$首先计算交易$R_\tau||ST||c_1$，交易大小为180字节，时间开销为74.803ms，gas开销为164181.62。为恢复隐匿授权信息，接收方$\mathcal{D}_2$根据交易中的R_τ检查隐匿标签ST。在本实施例中，采用160位ECC算法，每一次隐匿标签匹配时间为35.735ms。

[0173] 获取到授权内容后，对于场景一，$\mathcal{D}_2$需要计算签名Sig_1，时间开销为12.263ms。如图5所示，计算$h_2(CEHR_{\mathcal{P}_i})$和解密CEHR的时间消耗与电子病历大小有关。对于$\mathcal{H}_1$，验证签名的时间开销为48.198ms。对于场景二，$\mathcal{D}_2$的时间开销与场景一相同。对于$\mathcal{H}_1$，需要额外的开销，其中，$\mathcal{H}_1$计算签名Sig_2的时间开销为12.985ms，向$\mathcal{H}_2$发送交易的gas开销为176589。对于$\mathcal{H}_2$的开销，与场景一中$\mathcal{H}_1$的开销相同。

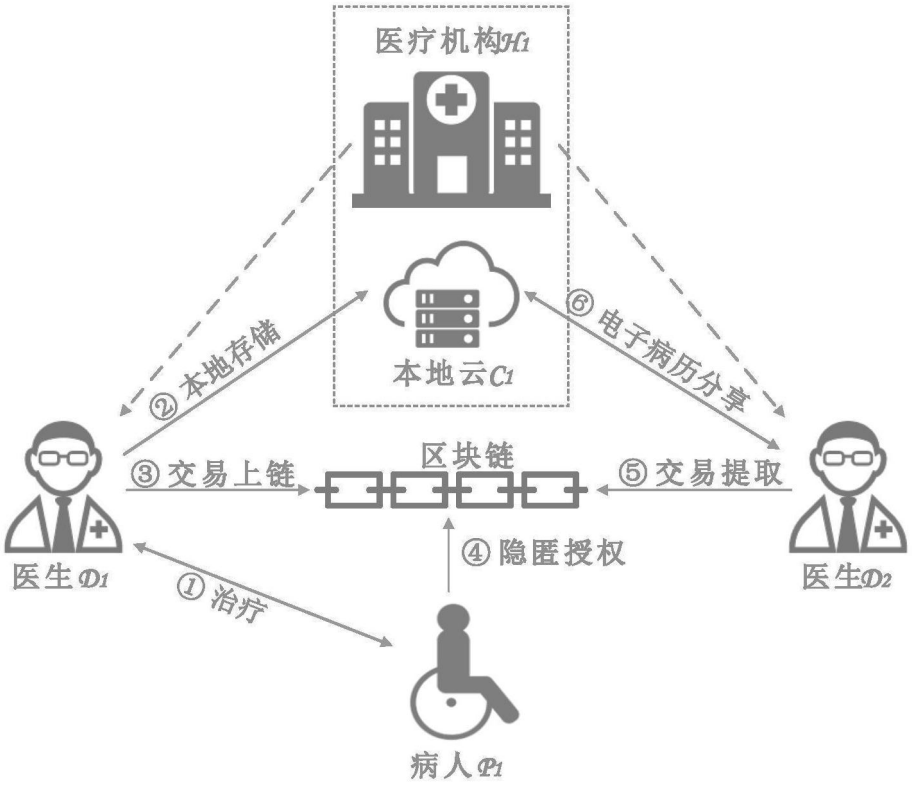

医疗机构H1
本地云C1
②本地存储
⑥电子病历分享
③交易上链
区块链
⑤交易提取
④隐匿授权
医生D1
①治疗
医生D2
病人P1

图1

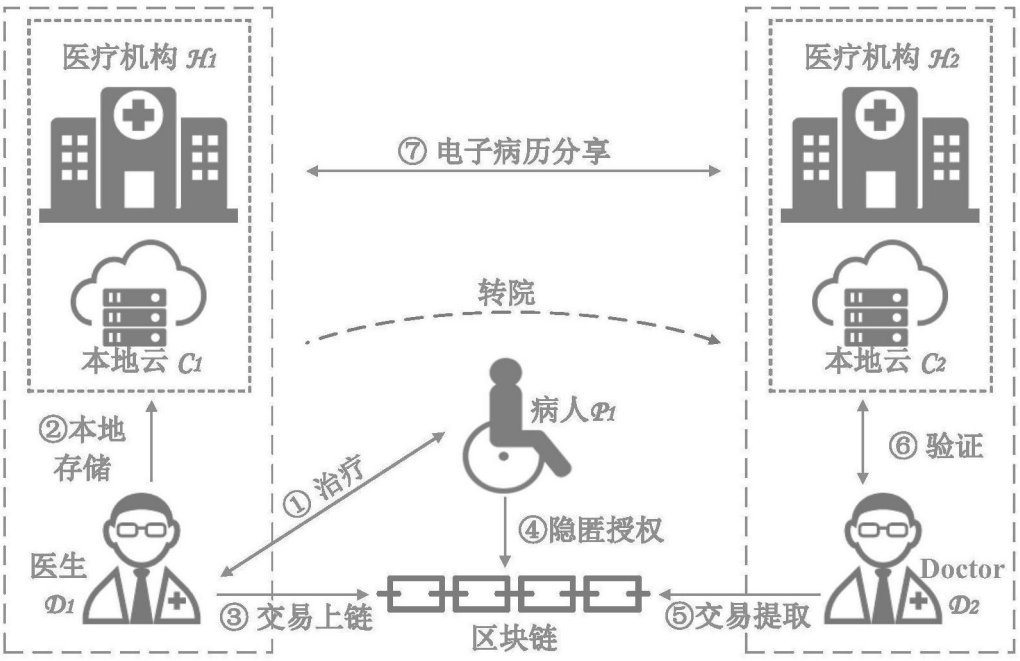

医疗机构 H1
医疗机构 H2
⑦电子病历分享
转院
本地云 C1
本地云 C2
病人P1
②本地存储
⑥验证
①治疗
④隐匿授权
医生 D1
Doctor D2
③交易上链
区块链
⑤交易提取

图2

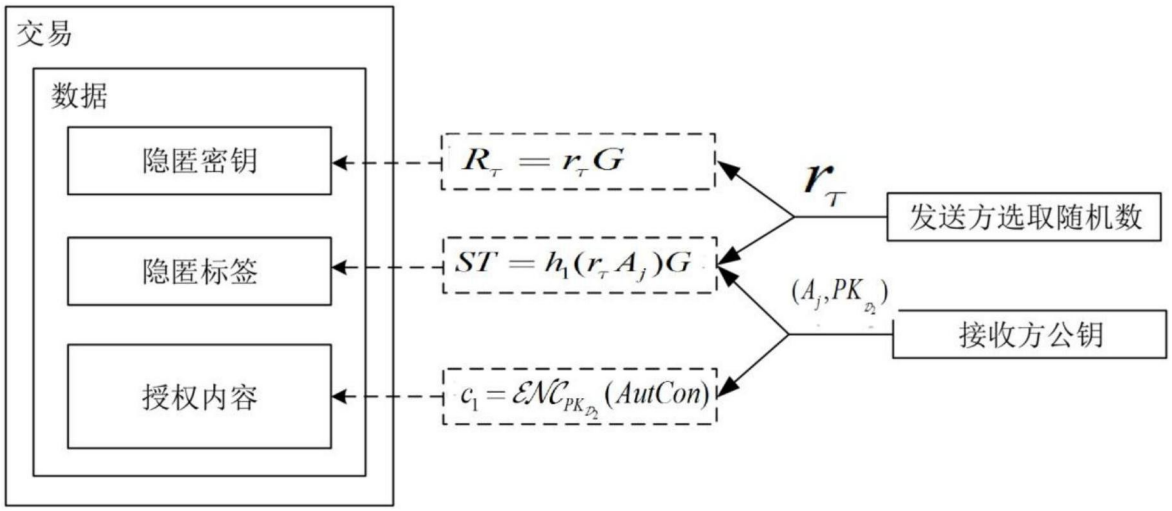

交易
数据
隐匿密钥
隐匿标签
授权内容
$R_\tau = r_\tau G$
$ST = h_1(r_\tau A_j)G$
$c_1 = \mathcal{ENC}_{PK_{D_2}}(AutCon)$
r_τ
发送方选取随机数
(A_j, PK_{D_2})
接收方公钥

图3

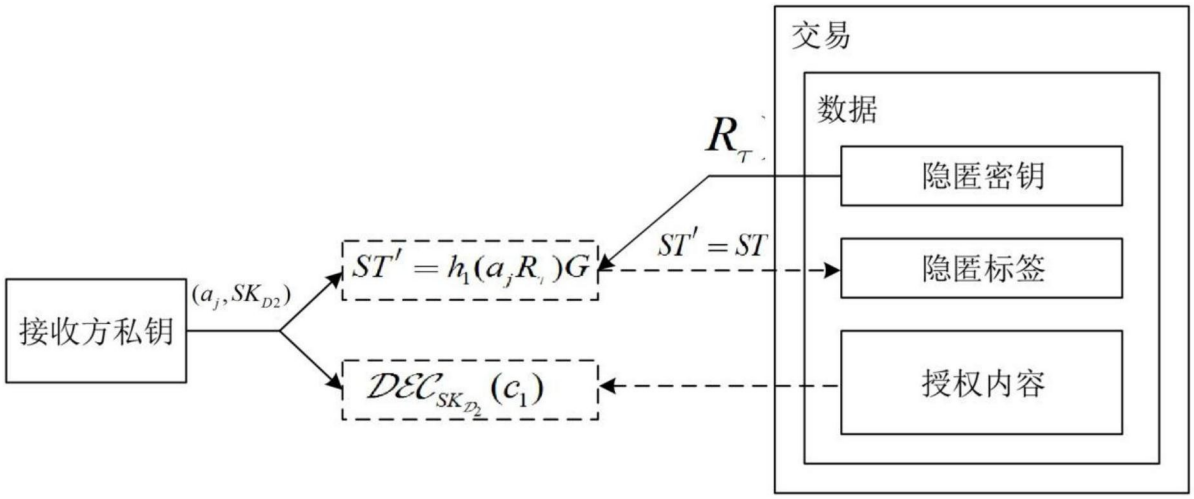

交易
数据
隐匿密钥
隐匿标签
授权内容
R_τ
$ST' = ST$
$ST' = h_1(a_j R_\tau)G$
$\mathcal{DEC}_{SK_{D_2}}(c_1)$
接收方私钥
(a_j, SK_{D2})

图4

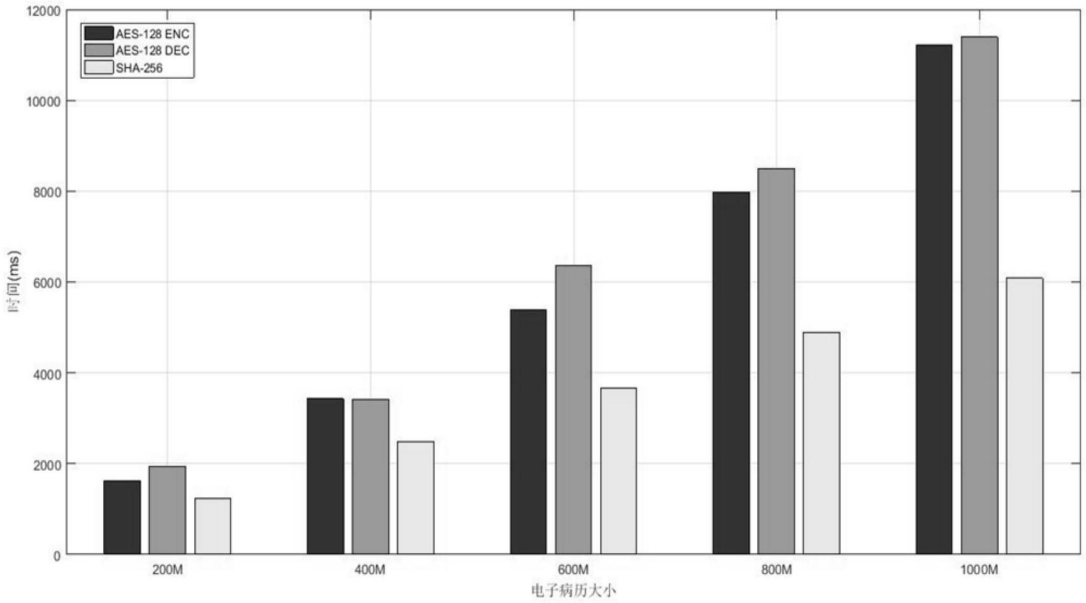

AES-128 ENC
AES-128 DEC
SHA-256
时间(ms)
12000
10000
8000
6000
4000
2000
0
200M
400M
600M
800M
1000M
电子病历大小

图5