(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114640468 B
(45)授权公告日 2024.01.26

(21)申请号 202210255503.8
(22)申请日 2022.03.16
(65)同一申请的已公布的文献号
申请公布号 CN 114640468 A
(43)申请公布日 2022.06.17
(73)专利权人 安顺职业技术学院
地址 561000 贵州省安顺市西秀区工业园区两六路安顺职业技术学院蔡官校区
(72)发明人 高丹 欧君 李高俊 范玮 季小艳
(74)专利代理机构 贵州昀博知识产权代理有限公司 52125
专利代理师 石文义
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 9/00(2022.01)

(56)对比文件
CN 106503994 A,2017.03.15
CN 113489733 A,2021.10.08
CN 113595971 A,2021.11.02
CN 113836222 A,2021.12.24
CN 114065265 A,2022.02.18
US 2020244634 A1,2020.07.30

审查员 刘娟

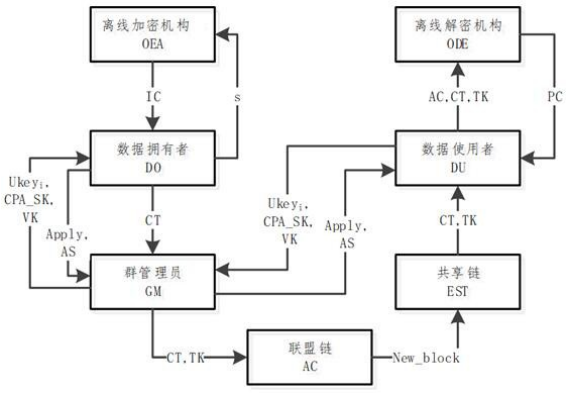
权利要求书4页 说明书9页 附图3页

(54)发明名称

一种基于在线离线属性加密的区块链隐私保护方法

(57)摘要

本发明公开了一种基于在线离线属性加密的区块链隐私保护方法,所述保护方法涉及区块链系统和多个实体模块,所述实体模块包括有数据拥有者DO、数据使用者DU、群管理员GM、离线加密机构OEA、离线解密机构ODE、联盟链AC和共享链EST;所述区块链系统用于为实体模块提供分布式可信的数据存储云服务器系统,其实现方式包括以下过程,系统初始化阶段,用户注册阶段,加密阶段,群签名认证阶段,数据使用者解密阶段和追责阶段。采用本发明所述的保护方法,实现了对数据拥有者和验证者的双向追溯,增加了数控的安全性。



CN 114640468 B

1.一种基于在线离线属性加密的区块链隐私保护方法,其特征在于:所述保护方法涉及区块链系统和多个实体模块,所述实体模块包括有数据拥有者DO、数据使用者DU、群管理员GM、离线加密机构OEA、离线解密机构ODE、联盟链AC和共享链EST;所述区块链系统用于为实体模块提供分布式可信的数据存储云服务器系统,其实现方式包括以下过程,系统初始化阶段,用户注册阶段,加密阶段,群签名认证阶段,数据使用者解密阶段和追责阶段;所述保护方法通过在线离线属性加密算法,利用区块链结合离线加密机构及离线解密机构,在减小用户的计算开销的同时,实现细粒度的用户访问控制,并通过共享链和联盟链的双链控制,防止了单点故障问题,防止用户和验证者之间出现共谋,同时,通过群签名验证,实现了对数据拥有者和验证者的双向追溯,增加了数控的安全性;其具体实现方式包括以下过程,数据拥有者DO将访问结构发送给离线加密机构ODE,离线加密机构基于时间周期树和访问结构计算中间密文并返回给数据拥有者DO,数据拥有者DO利用中间密文对数据进行加密,并将密文发送到区块链系统中的云服务器系统;数据使用者通过云服务器系统搜索关键字并得到相匹配的密文;而数据使用者DU将密文发送到离线解密机构ODE,离线解密机构ODE基于数据使用者DO的属性和密钥对密文进行部分解密,得到转换密文,并将转换密文返回给数据使用者DO;数据使用者DO利用转换密钥对转换密文进行解密,即得到数据。

2.根据权利要求1所述的一种基于在线离线属性加密的区块链隐私保护方法,其特征在于,所述系统初始化阶段的具体实现方式为:

(1)在系统初始化阶段,确定系统初始化相关属性:数据拥有者运行系统建立算法SystemSetup(1^{λ})→(PK,MSK),即输入一个安全系数λ,系统生成公钥PK,所述$PK=(G_1,G_2,g,p,e,g^{a},g^{\beta},e(g,g)^{\alpha},\{\varphi_j\},\{h_j\},\mathrm{H}_0,\mathrm{H}_1,\mathrm{H}_2)$,MSK=(α,a,γ);

其中,G1,G2为素数p阶循环群,g为G1的生成元;e为双线性映射:G1×G1→G2;随机数α,a,β∈Z_p;j表示属性个数;选择j个随机数$h_j\in G_1$;哈希函数H0:{0,1}→G1,H1:{0,1}→G2,H2:{0,1}→G2;

(2)群管理员GM初始化:群管理员运行系统建立算法GMSetup(PK)→(GMKey,GMPK,GMSK),输入公钥PK,系统生成每个群管理员GM的密钥GMKey,群公钥GMPK和群追踪密钥GMSK;

GMKey=γ_i,$GMPK=(g,g_1,u^{\sigma_1},v,g_1^{\gamma_i})$,GMSK=($\delta_1$,$\delta_2$),$u^{\sigma_1}=v^{\sigma_2}=h$;

其中,i表示群管理员个数;γ_i表示i个随机数;g1为G1的生成元;随机数δ_1,$\delta_2\in Z_p$;u,v∈G_1;

(3)联盟链AC初始化:ACSetup(PK,id)→(SignMK,SignPK),输入公钥PK,系统生成联盟链签名主密钥SignMK和各节点签名私钥SignPK;在联盟链中,分为主要节点和次要节点,主要节点负责区块链的维护工作并为新加入的区块分发id和签名私钥;

$$SignMK=(ke,[ks]P_2,\sum^{k}[ke_k]P_2),\quad SignPK=[\sum^{k}ke_kT]P_1,\ \mathrm{T}=\mathrm{H}_1(\mathrm{id}||\mathrm{hid},\mathrm{N})+\mathrm{ks};$$

其中,k表示联盟链中密钥生成中心AAk的个数;ks,kek为密钥生成中心的随机数,且ks,ke_k∈[1,N-1],kek被k个密钥生成中心分别持有,N为有限域;P2为G2的生成元,P1为G1的生成元;id为联盟链中各个次要节点的唯一标识,为主要节点颁发的一串随机数;hid表示隐藏。

3.根据权利要求1所述的一种基于在线离线属性加密的区块链隐私保护方法,其特征在于,所述用户注册阶段的具体实现方式为:

(1)用户获取用户私钥片段UKeyi:GMKeyGen(PK)→UKeyi;用户向群管理员GM提出注册申请Apply,若群管理员GM同意后,i个群管理员将为用户分别生成相应的用户私钥片段UKeyi,并将用户私钥片段UKeyi发送给用户;而在区块链中,用户可细分为数据拥有者DO和数据使用者DU;

$$UKey_i = g_1^{1/(\gamma_i + x)}$$;

其中,随机数$x \in Z_p$;

(2)用户计算:GMKeyGen(PK,S,UKeyi)→(UKey,IDU,CPA_SK);用户通过算法计算自己的用户私钥UKey、用户标识IDU,并向群管理员提交用户属性集AS={a1,a2,...,aj},获得属性加密密钥CPA_SK,离线验证密钥VK;

$$UKey = \prod^{i} UKey_i \quad , \quad IDU = g_1^{Ukey}$$,CPA_SK=$(g^{\alpha}h^{d},z,TK)$, $$TK = (g^{d/z}, \{h_j^{d/z} \mathrm{H}(v_j)^{d/z}\})$$,

VK=$(g^{1/(\beta+\mu)},\mu)$;

其中,vj为用户属性集AS中各属性的权重值;TK为属性加密的密文转换密钥;d,z,为随机数,且$d,z,\mu \in Z_p$。

4.根据权利要求1所述的一种基于在线离线属性加密的区块链隐私保护方法,其特征在于,所述加密阶段的具体实现方式为:

(1)离线加密机构OEA进行离线加密:OEA_Enc(PK)→IC,数据拥有者DO选择一个秘密值s传给离线加密机构;离线加密机构通过秘密值s计算得到中间密文IC,并将中间密文IC发送给数据拥有者DO;

$$IC = (e(g,g)^{\alpha s}, g^{s}, \{g^{a\varepsilon}\varphi_j^{y}, \{\varphi_j^{y} g^{ay}\}, \varepsilon, y, \{\varphi_j^{y} \mathrm{H}(\mathbf{v}_j)\}\})$$;

其中,秘密值$s \in Z_p$;随机数$\varepsilon, y \in Z_p$;

(2)数据拥有者DO进行加密:DO_Enc(PK,IC,VK,Message)→CT,数据拥有者DO通过访问结构AC和中间密文IC对明文Message进行最终加密,得到属性加密密文CT;

$$CT = (AC, Message \oplus \mathrm{H}_1(R), R \cdot e(g,g)^{\alpha s}, g^{s}\{g^{a\varepsilon}\varphi_j^{y}, \varphi_{j\cdot\rho(j)}^{y} g^{ay}, \{\varphi_j^{y} \mathrm{H}_1(\mathbf{v}_j)\}, (\theta_j - \varepsilon), (s-y)\}, C_1)$$, $C_1 = g^{\mu/(\beta+\mu)}, g^{\beta} \cdot g^{\mu}, \mathrm{H}_1(e(g,g)^{\mu}, R \cdot \mathrm{H}_1(\mathrm{Message})$, $$MM = \mathrm{H}_1(Message) \oplus \mathrm{H}_1(R)$$;

其中,$\varphi_{j\cdot\rho(j)}$为属性aj在访问结构AC=(M,ρ(x))中的映射,θ为aj在映射函数ρ(x)中的秘密份额;R为随机密文参数,且$R \in G_2$;M为映射矩阵,M中的每一行对应一个属性。

5.根据权利要求1所述的一种基于在线离线属性加密的区块链隐私保护方法,其特征在于,所述群签名认证阶段的具体实现方式为:

(1)联盟链AC次节点A对密文CT进行签名:AC_Sign(CT,SignMK,SignPK)→(SignCT,DO_Verify),联盟链次节点A对密文CT进行签名,令联盟链中的次节点A通过签名主密钥SignMK和次节点A的签名私钥SignPK进行签名运算,得到联盟链中该次节点对密文CT的群签名SignCT和来源验证值DO_Verify;

$$SignCT = (\mathrm{H}_1(CT \| g^{r_1}, \mathrm{N}), [r_2]([\mathrm{H}_1(\mathrm{id}_A \| \mathrm{hid}, \mathrm{N})]P_2 + [ks]P_2), SS \cdot SignPK_A, SS \cdot SignAG)$$;

$$SignAG=[\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N})+ks]^{-1}[\sum^{k}ke]^2[\mathrm{H}_1(id_{GM}\|\mathrm{hid},\mathrm{N})+ks]^{-1}\bmod \mathrm{N}\ ;$$

$$SS=r_2^{-1}(r_1-\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N}))\ ;$$

$$DO\_Verify=\mathrm{H}_1(\mathbf{M}\|u^{\chi}\|v^{\tau}\|UKeyu^{\sigma_1(\chi+\tau)}\|u^{b_1}\|u^{b_2}\|TT\|v^{-\chi b_3 r_4}\|v^{-\tau b_3 b_5})\ ;$$

$$TT=e(UKey\cdot u^{\sigma_1(\chi+\tau)},g_1)\times\prod^{i}e(h,g_1^{\gamma_i})^{-b_1-b_2}\times e(h,g_1)^{-CT(b_4-b_5)}$$

其中,随机数$r_1,r_2\in[1,N-1]$;idA表示次节点A的id标识;τ,χ为随机数,且$\tau,\chi\in Z_p$;选择随机的盲化因子$b_1,b_2,b_3,b_4,b_5\in Z_p$;

(2)联盟链AC验证阶段:AC_Verify(SignCT)→1/0,联盟链收到密文CT和相应的群签名SignCT,通过算法对群签名进行验证,若证明了该签名由联盟链中的某个节点产生的,则输出1,并;反之,则输出0,并丢弃密文CT;

计算:$U_1=e(SS\cdot SignAG)$,$U_2=e(SS\cdot SignPK_A)$;

验证$U_1=U_2$,若相等,则进行下一步验证;若不相等,则丢弃密文CT;

根据收到的SignCT计算:

$$U3=\mathrm{H}_1(CT'\|e(SS\cdot SignAG),[r_2]([\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N})]P_2+[ks]P_2)\cdot g^{\mathrm{H}_2(CT\|g^{r_1},\mathrm{N})},\mathrm{N})\ ;$$

验证,$U3=\mathrm{H}_1(CT\|g^{r_1},\mathrm{N})$,若相等,则将CT发送到共享链中进行共享;反之,则丢弃密文CT;通过验证可证明密文CT通过了联盟链签名验证;

(3)上链阶段:采用UTXO的形式上链,次节点A将上次交易的编号Number和上次交易的哈希值HLast,和本次交易的群签名SignCT发送到联盟链主节点V中,主节点V生成新生区块New_block,并对区块中的信息进行验证,若验证通过,则并入共享链中,反之,丢弃区块;

在联盟链AC验证阶段,联盟链中各节点寻找共享链中与此新生区块关联的上一次交易信息,并对比新生区块的输入和上一次交易的输出值是否相同,若经过联盟链中大多数节点的同意后,主节点将该新生区块并入共享链中,反之,丢弃该新生区块。

6.根据权利要求1所述的一种基于在线离线属性加密的区块链隐私保护方法,其特征在于,所述数据使用者解密阶段的具体实现方式为:

(1)离线解密机构ODA进行部分解密:ODA_Dec(AC,CT,TK)→PC,数据使用者DU将密文CT和密文转换密钥TK传给离线解密机构ODA;离线加密机构ODA首先检查数据使用者的属性集AS是否满足访问结构AC的要求,若满足,则对密文CT进行部分解密并将部分解密密文PC发送给数据使用者DU;反之,则输出0;

$PC=(AC,MM,R\cdot e(g,g)^{\alpha s},g^{s},e(g,g)^{da\theta/z},C_1)$;

(2)数据使用者DU进行解密:DU_Dec(PC,CPA_SK)→R;数据使用者DU通过属性加密密钥CPA_SK对部分解密密文PC解密,得到随机密文参数R;

$R=R\cdot e(g,g)^{\alpha s}/(e(g^{s},g^{\alpha}h^{d})/e(g,g)^{das})$;

$$Message=\mathrm{H}_1(R)\oplus MM\ 。$$

7.根据权利要求1所述的一种基于在线离线属性加密的区块链隐私保护方法,其特征在于,所述追责阶段的具体实现方式为:

(1)追责数据拥有者DO:DO_Accountability(DO_Verify,GMSK)→idDO,若群管理员投

票通过要求追责数据拥有者后,则可通过来源验证值DO_Verify和群追踪密钥GMSK计算并获取数据拥有者的id;

已知$u^{\sigma_1}=v^{\sigma_2}=h$,则$id_{DO}=id_{DO}h^{\chi+\tau}/u^{\chi\sigma_1}\cdot v^{\tau\sigma_2}$;

(2)追责签名者A:A_Accountability(SignCT,SignPK)→idA;在上链过程中,通过采用群签名验证的方法和UTXO的上链方式,若群管理员投票通过要求追责数据拥有者后,主节点可通过对本次交易进行逐链溯源的方式,找到首发地址进行追责;通过群签名SignCT和签名私钥SignP,提取出签名者A的idA哈希值HID,主节点逐一对比各个子节点的id对应的HID值即可找到签名者的idA。

一种基于在线离线属性加密的区块链隐私保护方法

技术领域

[0001] 本发明涉及的是区块链技术领域,具体地说是一种基于在线离线属性加密的区块链隐私保护方法。

背景技术

[0002] 区块链是基于P2P网络和密码学技术实现的一种可信的分布式数据存储技术,区块链作为一种去中心化的分布式记账系统,基于其不可抵赖性、共识性和透明性,以及不可篡改等特性,越来越受到人们的青睐,并被广泛应用在各种场景中。但是,传统的区块链在实现数据的透明化、可追踪化的同时,户的隐私安全受到了一定的威胁。如何在实现区块链透明可追踪的优点的同时保护用户隐私安全成为了一个研究热点。

[0003] 针对区块链数据可追溯与用户隐私泄漏问题,为了保护用户隐私安全,经检索,参考文献1(“自适应安全的带关键字搜索的外包属性基加密方案”,郭丽峰,王倩丽,计算机应用,2021,41(11):3266－3273)和参考文献2(“支持离线/在线加密及可验证外包解密的CP－WABE方案”,李航,冯朝胜,刘帅南,刘彬,赵开强,电子学报,2020,48(11):2146－2153),都是通过在线/离线的方式,将部分加密计算和部分解密计算外包给离线机构,虽然减少了数据拥有者和数据使用者的计算开销,但是都不能很好的适用于区块链中。参考文献3(“基于群签名与属性加密的区块链可监管隐私保护方案”,李莉,杜慧娜,李涛,计算机工程:1－9[2022－01－04].DOI:10.19678/j.issn.1000－3428.0062464)提出了一种双链结构的区块链隐私保护方案,通过群签名技术和属性加密技术,有效的保护了用户的隐私信息。但该方案的只有一个验证者,不能有效防止验证者和用户的共谋,不能有效的保证信息的真实和透明,且不能很好的适用于计算资源有限的设备。参考文献4(“基于SM9算法可证明安全的区块链隐私保护方案”,杨亚涛,蔡居良,张筱薇,袁征,软件学报,2019,30(06):1692－1704.DOI:10.13328/j.cnki.jos.005745)提出了一种主要应用于联盟链的隐私保护方案,通过验证者群体(即联盟链)的设置,有效的保护了用户的隐私信息。但该方案主要应用于联盟链中,并不能很好的应用到双链结构中,且不能很好的适用于计算资源有限的设备。

[0004] 结合参考文献1至4的特点,为了适用于计算资源有限的设备,在实现细粒度的用户隐私保护的同时,还可同时对数据的拥有者和签名者进行追责,提高数据的安全性,从而提出了一种基于在线离线属性的保护方案。

发明内容

[0005] 本发明所要解决的技术问题是针对背景技术中存在的问题,为了保护用户隐私安全,从而提出一种隐私保护方法,通过在线离线属性加密算法,在减小用户计算开销的同时,实现细粒度的用户访问控制,通过双链设计及群签名验证,实现对用户和验证者的双向追溯,从而提高数据的安全性,具体地说是一种基于在线离线属性加密的区块链隐私保护方法。

[0006] 为解决上述技术问题,本发明所采用的技术方案为:一种基于在线离线属性加密的区块链隐私保护方法,所述保护方法涉及区块链系统和多个实体模块,所述实体模块包括有数据拥有者DO、数据使用者DU、群管理员GM、离线加密机构OEA、离线解密机构ODE、联盟链AC和共享链EST;所述区块链系统用于为实体模块提供分布式可信的数据存储云服务器系统,其实现方式包括以下过程,系统初始化阶段,用户注册阶段,加密阶段,群签名认证阶段,数据使用者解密阶段和追责阶段。

[0007] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述保护方法通过在线离线属性加密算法,利用区块链结合离线加密机构及离线解密机构,在减小用户的计算开销的同时,实现细粒度的用户访问控制,并通过共享链和联盟链的双链控制,防止了单点故障问题,防止用户和验证者之间出现共谋,同时,通过群签名验证,实现了对数据拥有者和验证者的双向追溯,增加了数控的安全性;其具体实现方式包括以下过程,数据拥有者DO将访问结构发送给离线加密机构ODE,离线加密机构基于时间周期树和访问结构计算中间密文并返回给数据拥有者DO,数据拥有者DO利用中间密文对数据进行加密,并将密文发送到区块链系统中的云服务器系统;数据使用者通过云服务器系统搜索关键字并得到相匹配的密文;而数据使用者DU将密文发送到离线解密机构ODE,离线解密机构ODE基于数据使用者DO的属性和密钥对密文进行部分解密,得到转换密文,并将转换密文返回给数据使用者DO;数据使用者DO利用转换密钥对转换密文进行解密,即得到数据。

[0008] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述系统初始化阶段的具体实现方式为:

[0009] (1)在系统初始化阶段,确定系统初始化相关属性:数据拥有者运行系统建立算法SystemSetup(1^{λ})→(PK,MSK),即输入一个安全系数λ,系统生成公钥PK,所述 $PK=(G_1,G_2,g,p,e,g^a,g^\beta,e(g,g)^\alpha,\{\varphi_j\},\{h_j\},H_0,H_1,H_2)$,MSK=(α,a,γ);

[0010] 其中,G1,G2为素数p阶循环群,g为G1的生成元;e为双线性映射:G1×G1→G2;随机数α,a,β∈Z_p;j表示属性个数;选择j个随机数h_j∈G_1;哈希函数H0:{0,1}→G1,H1:{0,1}→G2,H2:{0,1}→G2;

[0011] (2)群管理员GM初始化:群管理员运行系统建立算法GMSetup(PK)→(GMKey,GMPK,GMSK),输入公钥PK,系统生成每个群管理员GM的密钥GMKey,群公钥GMPK和群追踪密钥GMSK;

[0012] GMKey=γ_i,$GMPK=(g,g_1,u^{\sigma_1},v,g_1^{\gamma_i})$,GMSK=$(\delta_1,\delta_2)$,$u^{\sigma_1}=v^{\sigma_2}=h$;

[0013] 其中,i表示群管理员个数;γ_i表示i个随机数;g1为G1的生成元;随机数δ_1,δ_2∈Z_p;u,v∈G_1;

[0014] (3)联盟链AC初始化:ACSetup(PK,id)→(SignMK,SignPK),输入公钥PK,系统生成联盟链签名主密钥SignMK和各节点签名私钥SignPK;在联盟链中,分为主要节点和次要节点,主要节点负责区块链的维护工作并为新加入的区块分发id和签名私钥;

[0015] $SignMK=(ke,[ks]P_2,\sum_{k=1}^{k}[ke_k]P_2)$, $SignPK=[\sum_{k=1}^{k}ke_kT]P_1$,

[0016] T=H_1(id||hid,N)+ks;

[0017] 其中,k表示联盟链中密钥生成中心AAk的个数;ks,kek为密钥生成中心的随机数,

且ks,ke_k∈[1,N-1],kek被k个密钥生成中心分别持有,N为有限域;P2为G2的生成元,P1为G1的生成元;id为联盟链中各个次要节点的唯一标识,为主要节点颁发的一串随机数;hid表示隐藏。

[0018] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述用户注册阶段的具体实现方式为:

[0019] (1)用户获取用户私钥片段UKeyi:GMKeyGen(PK)→UKeyi;用户向群管理员GM提出注册申请Apply,若群管理员GM同意后,i个群管理员将为用户分别生成相应的用户私钥片段UKeyi,并将用户私钥片段UKeyi发送给用户;而在区块链中,用户可细分为数据拥有者DO和数据使用者DU;

[0020] $UKey_i = g_1^{1/(\gamma_i + x)}$;

[0021] 其中,随机数x∈Z_p;

[0022] (2)用户计算:GMKeyGen(PK,S,UKeyi)→(UKey,IDU,CPA__SK);用户通过算法计算自己的用户私钥UKey、用户标识IDU,并向群管理员提交用户属性集AS={a1,a2,...,aj},获得属性加密密钥CPA__SK,离线验证密钥VK;

[0023] $UKey = \prod_{i=1}^{i} UKey_i$, $IDU = g_1^{Ukey}$,CPA_SK=($g^{\alpha} h^{d}$,z,TK),$TK = (g^{d/z}, \{h_j^{d/z} \mathrm{H}(v_j)^{d/z}\})$,VK=($g^{1/(\beta+\mu)}$,μ);

[0024] 其中,vj为用户属性集AS中各属性的权重值;TK为属性加密的密文转换密钥;d,z,为随机数,且d,z,μ∈Z_p。

[0025] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述加密阶段的具体实现方式为:

[0026] (1)离线加密机构OEA进行离线加密:OEA__Enc(PK)→IC,数据拥有者DO选择一个秘密值s传给离线加密机构;离线加密机构通过秘密值s计算得到中间密文IC,并将中间密文IC发送给数据拥有者DO;

[0027] $IC = (e(g,g)^{\alpha s}, g^s, \{g^{a\varepsilon}\varphi_j^y, \{\varphi_j^y g^{ay}\}, \varepsilon, y, \{\varphi_j^y \mathrm{H}(\mathbf{v}_j)\}\})$;

[0028] 其中,秘密值s∈Z_p;随机数ε,y∈Z_p;

[0029] (2)数据拥有者DO进行加密:DO__Enc(PK,IC,VK,Message)→CT。数据拥有者DO通过访问结构AC和中间密文IC对明文Message进行最终加密,得到属性加密密文CT;

[0030] $CT = (AC, Message \oplus \mathrm{H}_1(R), R \cdot \mathrm{e}(g,g)^{\alpha s}, g^s\{g^{a\varepsilon}\varphi_j^y, \varphi_{j\text{-}\rho(j)}^y g^{ay}, \{\varphi_j^y \mathrm{H}_1(\mathbf{v}_j)\}, (\theta_j - \varepsilon), (s-y)\}, C_1)$,

[0031] C_1=$g^{\mu/(\beta+\mu)}$,g^{β}·g^{μ},H_1(e(g,g)$^{\mu}$,R·H_1(Message),$MM = \mathrm{H}_1(Message) \oplus \mathrm{H}_1(R)$;

[0032] 其中,$\varphi_{j\text{-}\rho(j)}$为属性aj在访问结构AC=(M,ρ(x))中的映射,θ为aj在映射函数ρ(x)中的秘密份额;R为随机密文参数,且R∈G_2;M为映射矩阵,M中的每一行对应一个属性。

[0033] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述群签名认证阶段的具体实现方式为:

[0034] (1)联盟链AC次节点A对密文CT进行签名:AC__Sign(CT,SignMK,SignPK)→(SignCT,DO__Verify)。联盟链次节点A对密文CT进行签名,令联盟链中的次节点A通过签名主密钥SignMK和次节点A的签名私钥SignPK进行签名运算,得到联盟链中该次节点对密文

CT的群签名SignCT和来源验证值DO__Verify。

[0035] $$SignCT=(\mathrm{H}_1(CT\|g^{r_1},\mathrm{N}),[r_2]([\mathrm{H}_1(\mathrm{id}_A\|\mathrm{hid},\mathrm{N})]P_2+[ks]P_2),SS\cdot SignPK_A,SS\cdot SignAG);$$

[0036] $$SignAG=[\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N})+ks]^{-1}[\sum_{k=1}^{k}ke]^2[\mathrm{H}_1(id_{GM}\|\mathrm{hid},\mathrm{N})+ks]^{-1}\bmod \mathrm{N};$$

[0037] $$SS=r_2^{-1}(r_1-\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N}));$$

[0038] $$DO\_Verify=\mathrm{H}_1(\mathbf{M}\|u^{\chi}\|v^{\tau}\|UKeyu^{\sigma_1(\chi+\tau)}\|u^{b_1}\|u^{b_2}\|TT\|v^{-\chi b_3 r_4}\|v^{-\tau b_3 b_5});$$

[0039] $$TT=e(UKey\cdot u^{\sigma_1(\chi+\tau)},g_1)\times\prod_{i=1}^{i}e(h,g_1^{\gamma_i})^{-b_1-b_2}\times e(h,g_1)^{-CT(b_4-b_5)}。$$

[0040] 其中,随机数$r_1,r_2\in[1,N-1]$;idA表示次节点A的id标识;τ,χ为随机数,且$\tau,\chi\in Z_p$;选择随机的盲化因子$b_1,b_2,b_3,b_4,b_5\in Z_p$。

[0041] (2)联盟链AC验证阶段:AC__Verify(SignCT)→1/0。联盟链收到密文CT和相应的群签名SignCT,通过算法对群签名进行验证。若证明了该签名由联盟链中的某个节点产生的,则输出1,并;反之,则输出0,并丢弃密文CT;

[0042] 计算:$U_1=e(SS\cdot SignAG)$,$U_2=e(SS\cdot SignPK_A)$;

[0043] 验证$U_1=U_2$,若相等,则进行下一步验证;若不相等,则丢弃密文CT;

[0044] 根据收到的SignCT计算:

[0045] $$U3=\mathrm{H}_1(CT'\|e(SS\cdot SignAG),[r_2]([\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N})]P_2+[ks]P_2)\cdot g^{\mathrm{H}_2(CT\|g^{r_1},\mathrm{N})},\mathrm{N});$$

[0046] 验证,$U3=\mathrm{H}_1(CT\|g^{r_1},\mathrm{N})$,若相等,则将CT发送到共享链中进行共享;反之,则丢弃密文CT;通过验证可证明密文CT通过了联盟链签名验证;

[0047] (3)上链阶段:采用UTXO的形式上链,次节点A将上次交易的编号Number和上次交易的哈希值HLast,和本次交易的群签名SignCT发送到联盟链主节点V中,主节点V生成新生区块New__block,并对区块中的信息进行验证,若验证通过,则并入共享链中,反之,丢弃区块;

[0048] 在联盟链AC验证阶段,联盟链中各节点寻找共享链中与此新生区块关联的上一次交易信息,并对比新生区块的输入和上一次交易的输出值是否相同,若经过联盟链中大多数节点的同意后,主节点将该新生区块并入共享链中,反之,丢弃该新生区块。

[0049] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述数据使用者解密阶段的具体实现方式为:

[0050] (1)离线解密机构ODA进行部分解密:ODA__Dec(AC,CT,TK)→PC,数据使用者DU将密文CT和密文转换密钥TK传给离线解密机构ODA;离线加密机构ODA首先检查数据使用者的属性集AS是否满足访问结构AC的要求,若满足,则对密文CT进行部分解密并将部分解密密文PC发送给数据使用者DU;反之,则输出0;

[0051] $PC=(AC,MM,R\cdot e(g,g)^{\alpha s},g^s,e(g,g)^{da\theta/z},C_1)$;

[0052] (2)数据使用者DU进行解密:DU__Dec(PC,CPA__SK)→R;数据使用者DU通过属性加密密钥CPA__SK对部分解密密文PC解密,得到随机密文参数R;

[0053] $R=R\cdot e(g,g)^{\alpha s}/(e(g^s,g^{\alpha}h^{d})/e(g,g)^{das})$;

[0054] $$Message=\mathrm{H}_1(R)\oplus MM。$$

[0055] 进一步地,本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,其中所述追责阶段的具体实现方式为:

[0056] (1)追责数据拥有者DO:DO__Accountability(DO__Verify,GMSK)→idDO。若群管理员投票通过要求追责数据拥有者后,则可通过来源验证值DO__Verify和群追踪密钥GMSK计算并获取数据拥有者的id;

[0057] 已知$u^{\sigma_1}=v^{\sigma_2}=h$,则$id_{DO}=id_{DO}h^{\chi+\tau}/u^{\chi\sigma_1}\cdot v^{\tau\sigma_2}$;

[0058] (2)追责签名者A:A__Accountability(SignCT,SignPK)→idA;在上链过程中,通过采用群签名验证的方法和UTXO的上链方式,若群管理员投票通过要求追责数据拥有者后,主节点可通过对本次交易进行逐链溯源的方式,找到首发地址进行追责;通过群签名SignCT和签名私钥SignP,提取出签名者A的idA哈希值HID,主节点逐一对比各个子节点的id对应的HID值即可找到签名者的idA。

[0059] 采用本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,与现有技术相比,其有益效果在于:通过在线离线属性加密算法,利用区块链结合离线加密机构及离线解密机构,在减小用户的计算开销的同时,实现细粒度的用户访问控制,适用于计算资源有限的设备,并通过共享链和联盟链的双链控制,防止了单点故障问题,防止用户和验证者之间出现共谋,同时,通过群签名验证,实现了对数据拥有者和验证者的双向追溯,增加了数控的安全性。

附图说明

[0060] 下面结合附图对本发明作进一步详细说明。

[0061] 图1为本发明所述访问结构控制树和LSSS矩阵对应结构示意图;

[0062] 图2为本发明所述实体模块的结构模型示意图;

[0063] 图3为本发明所述保护方法的流程示意框图。

具体实施方式

[0064] 为进一步说明本发明的构思,下面结合附图和实施例对本发明的实施方式作进一步详细描述。以下实施例的详细描述和附图用于示例性地说明本发明的原理,但不能用来限制本发明的范围,即本发明不限于所描述的实施例。

[0065] 本发明所述的一种基于在线离线属性加密的区块链隐私保护方法,首先需要设计一个应用场景,假设存在一个基于云服务平台医患交流平台,用户B是一名网上注册的患者,想在云服务平台上咨询医生并获取治疗建议,但用户B希望能在获取诊疗单的同时,不泄露自己的诊疗信息,能有一个承诺保证该诊疗单来自于正规的注册医生,能在后期发生医疗事故时追责到诊疗的医生和验证者。采用传统的方案并不能很好的应用于以上场景,为了解决以上问题,从而提出一种基于在线离线属性加密的区块链隐私保护方案,该方案适用于计算资源有限的设备,在实现了细粒度的用户隐私保护的同时,可同时对数据的拥有者和签名者进行追责。同时,为便于理解本发明技术方案,会涉及到访问结构及双线性映射的相关知识,下面对访问结构及双线性映射的作相关说明:

[0066] 访问结构:假设存在一个非空的用户属性集A,A={A1,A2,...,An};存在一个非空的访问控制集S,S={S1,S2,...,Sk};若A和S满足$A\subseteq S$,则称集合A为访问控制S下的授权集

合;反之,则称集合A为访问控制S下的未授权集合。在CP—ABE中,若A为授权集合,存在一个矩阵AA,存在一个函数ρ(x),使得矩阵AA中的每一行都能与S中的属性一一映射,则矩阵AA称为LSSS矩阵,且LSSS矩阵的行数等于访问控制树上的叶子节点个数,即属性的个数。如图1所示的访问结构控制树和LSSS矩阵对应图。

[0067] 双线性映射:设G1,G2,G3为素数p阶循环群;存在一个映射关系e:G1×G2→G3,若e为双线性对,则满足:

[0068] A、双线性:任意的a,b∈Zp,都有$e(G_1^a, G_2^b)=e(G_1, G_2)^{ab}$;

[0069] B、非退化性:存在一个G1,G2,使得e(G1,G2)≠1;

[0070] C、可计算性:存在一个有效的算法计算e(G1,G2)。

[0071] 针对上述应用场景,在实现细粒度的用户隐私保护的同时,还可同时对数据的拥有者和签名者进行追责,实现对用户和验证者进行双向追溯,提高数据的安全性,从而提出一种基于在线离线属性加密的区块链隐私保护方法,该保护方法的详细设计方案为:

[0072] 一种基于在线离线属性加密的区块链隐私保护方法,所述保护方法涉及区块链系统和多个实体模块,其结构模型如图2所示,所述实体模块包括有数据拥有者DO、数据使用者DU、群管理员GM、离线加密机构OEA、离线解密机构ODE、联盟链AC和共享链EST;所述区块链系统用于为实体模块提供分布式可信的数据存储云服务器系统,其实现方式包括以下过程,系统初始化阶段,用户注册阶段,加密阶段,群签名认证阶段,数据使用者解密阶段和追责阶段;具体的操作流程如图3所示,具体包括以下过程,数据拥有者DO将访问结构发送给离线加密机构ODE,离线加密机构基于时间周期树和访问结构计算中间密文并返回给数据拥有者DO,数据拥有者DO利用中间密文对数据进行加密,并将密文发送到区块链系统中的云服务器系统;数据使用者通过云服务器系统搜索关键字并得到相匹配的密文;而数据使用者DU将密文发送到离线解密机构ODE,离线解密机构ODE基于数据使用者DO的属性和密钥对密文进行部分解密,得到转换密文,并将转换密文返回给数据使用者DO;数据使用者DO利用转换密钥对转换密文进行解密,即得到数据。

[0073] 1、系统初始化阶段:

[0074] (1)首先是要确定系统初始化相关属性:数据拥有者运行系统建立算法SystemSetup(1^λ)→(PK,MSK),即输入一个安全系数λ,系统生成公钥PK,所述$PK=(G_1,G_2,g,p,e,g^a,g^\beta,e(g,g)^\alpha,\{\varphi_j\},\{h_j\},H_0,H_1,H_2)$,MSK=(α,a,γ);

[0075] 其中,G1,G2为素数p阶循环群,g为G1的生成元;e为双线性映射:G1×G1→G2;随机数α,a,β∈Z_p;j表示属性个数;选择j个随机数h_j∈G_1;哈希函数H0:{0,1}→G1,H1:{0,1}→G2,H2:{0,1}→G2;

[0076] (2)其次是对群管理员GM初始化:群管理员运行系统建立算法GMSetup(PK)→(GMKey,GMPK,GMSK),输入公钥PK,系统生成每个群管理员GM的密钥GMKey,群公钥GMPK和群追踪密钥GMSK;

[0077] GMKey=γ_i,$GMPK=(g,g_1,u^{\sigma_1},v,g_1^{\gamma_i})$,GMSK=($\delta_1$,$\delta_2$),$u^{\sigma_1}=v^{\sigma_2}=h$;

[0078] 其中,i表示群管理员个数;γ_i表示i个随机数;g1为G1的生成元;随机数δ_1,δ_2∈Z_p;u,v∈G_1;

[0079] (3)最后是对联盟链AC初始化:ACSetup(PK,id)→(SignMK,SignPK),输入公钥PK,

系统生成联盟链签名主密钥SignMK和各节点签名私钥SignPK;在联盟链中,分为主要节点和次要节点,主要节点负责区块链的维护工作并为新加入的区块分发id和签名私钥;

[0080] $SignMK=(ke,[ks]P_2,\sum_{k=1}^{k}[ke_k]P_2)$, $SignPK=[\sum_{k=1}^{k}ke_kT]P_1$,

[0081] $T=H_1(id||hid,N)+ks$;

[0082] 其中,k表示联盟链中密钥生成中心AAk的个数;ks,kek为密钥生成中心的随机数,且$ks,ke_k\in[1,N-1]$,kek被k个密钥生成中心分别持有,N为有限域;P2为G2的生成元,P1为G1的生成元;id为联盟链中各个次要节点的唯一标识,为主要节点颁发的一串随机数;hid表示隐藏。

[0083] 2、用户注册阶段:

[0084] (1)用户获取用户私钥片段UKeyi:GMKeyGen(PK)→UKeyi;用户向群管理员GM提出注册申请Apply,若群管理员GM同意后,i个群管理员将为用户分别生成相应的用户私钥片段UKeyi,并将用户私钥片段UKeyi发送给用户;而在区块链中,用户可细分为数据拥有者DO和数据使用者DU;

[0085] $UKey_i=g_1^{1/(\gamma_i+x)}$;

[0086] 其中,随机数$x\in Z_p$;

[0087] (2)用户计算:GMKeyGen(PK,S,UKeyi)→(UKey,IDU,CPA__SK);用户通过算法计算自己的用户私钥UKey、用户标识IDU,并向群管理员提交用户属性集AS={a1,a2,...,aj},获得属性加密密钥CPA__SK,离线验证密钥VK;

[0088] $UKey=\prod_{i=1}^{i}UKey_i$, $IDU=g_1^{Ukey}$,$CPA\_SK=(g^{\alpha}h^{d},z,TK)$,

$TK=(g^{d/z},\{h_j^{d/z}H(v_j)^{d/z}\})$,$VK=(g^{1/(\beta+\mu)},\mu)$;

[0089] 其中,vj为用户属性集AS中各属性的权重值;TK为属性加密的密文转换密钥;d,z,为随机数,且$d,z,\mu\in Z_p$。

[0090] 3、加密阶段:

[0091] (1)离线加密机构OEA进行离线加密:OEA__Enc(PK)→IC,数据拥有者DO选择一个秘密值s传给离线加密机构;离线加密机构通过秘密值s计算得到中间密文IC,并将中间密文IC发送给数据拥有者DO;

[0092] $IC=(e(g,g)^{\alpha s},g^{s},\{g^{a\varepsilon}\varphi_j^{y},\{\varphi_j^{y}g^{ay}\},\varepsilon,y,\{\varphi_j^{y}H(\mathbf{v}_j)\}\})$;

[0093] 其中,秘密值$s\in Z_p$;随机数$\varepsilon,y\in Z_p$;

[0094] (2)数据拥有者DO进行加密:DO__Enc(PK,IC,VK,Message)→CT。数据拥有者DO通过访问结构AC和中间密文IC对明文Message进行最终加密,得到属性加密密文CT;

[0095] $CT=(AC,Message\oplus H_1(R),R\cdot e(g,g)^{\alpha s},g^{s}\{g^{a\varepsilon}\varphi_j^{y},\varphi_{j\cdot\rho(j)}^{y}g^{ay},\{\varphi_j^{y}H_1(\mathbf{v}_j)\},(\theta_j-\varepsilon),(s-y)\},C_1)$,

[0096] $C_1=g^{\mu/(\beta+\mu)}$,$g^{\beta}\cdot g^{\mu}$,$H_1(e(g,g)^{\mu}$,$R\cdot H_1(Message)$,$MM=H_1(Message)\oplus H_1(R)$;

[0097] 其中,$\varphi_{j\cdot\rho(j)}$为属性aj在访问结构AC=(M,ρ(x))中的映射,θ为aj在映射函数ρ(x)中的秘密份额;R为随机密文参数,且$R\in G_2$;M为映射矩阵,M中的每一行对应一个属性。

[0098] 4、群签名认证阶段:

[0099] (1)联盟链AC次节点A对密文CT进行签名:AC__Sign(CT,SignMK,SignPK)→(SignCT,DO__Verify)。联盟链次节点A对密文CT进行签名,令联盟链中的次节点A通过签名主密钥SignMK和次节点A的签名私钥SignPK进行签名运算,得到联盟链中该次节点对密文CT的群签名SignCT和来源验证值DO__Verify。

[0100] $$SignCT=(\mathrm{H}_1(CT\|g^{r_1},\mathrm{N}),[r_2]([\mathrm{H}_1(\mathrm{id}_A\|\mathrm{hid},\mathrm{N})]P_2+[ks]P_2),SS\cdot SignPK_A,SS\cdot SignAG);$$

[0101] $$SignAG=[\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N})+ks]^{-1}[\sum_{k=1}^{k}ke]^2[\mathrm{H}_1(id_{GM}\|\mathrm{hid},\mathrm{N})+ks]^{-1}\bmod \mathrm{N};$$

[0102] $$SS=r_2^{-1}(r_1-\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N}));$$

[0103] $$DO\_Verify=\mathrm{H}_1(\mathbf{M}\|u^{\chi}\|v^{\tau}\|UKeyu^{\sigma_1(\chi+\tau)}\|u^{b_1}\|u^{b_2}\|TT\|v^{-\chi b_3 r_4}\|v^{-\tau b_3 b_5});$$

[0104] $$TT=e(UKey\cdot u^{\sigma_1(\chi+\tau)},g_1)\times\prod_{i=1}^{i}e(h,g_1^{\gamma_i})^{-b_1-b_2}\times e(h,g_1)^{-CT(b_4-b_5)}。$$

[0105] 其中,随机数$r_1,r_2\in[1,N-1]$;idA表示次节点A的id标识;τ,χ为随机数,且$\tau,\chi\in Z_p$;选择随机的盲化因子$b_1,b_2,b_3,b_4,b_5\in Z_p$。

[0106] (2)联盟链AC验证阶段:AC__Verify(SignCT)→1/0。联盟链收到密文CT和相应的群签名SignCT,通过算法对群签名进行验证。若证明了该签名由联盟链中的某个节点产生的,则输出1,并;反之,则输出0,并丢弃密文CT;

[0107] 计算:$U_1=e(SS\cdot SignAG)$,$U_2=e(SS\cdot SignPK_A)$;

[0108] 验证$U_1=U_2$,若相等,则进行下一步验证;若不相等,则丢弃密文CT;

[0109] 根据收到的SignCT计算:

[0110] $$U3=\mathrm{H}_1(CT'\|e(SS\cdot SignAG),[r_2]([\mathrm{H}_1(id_A\|\mathrm{hid},\mathrm{N})]P_2+[ks]P_2)\cdot g^{\mathrm{H}_2(CT\|g^{r_1},\mathrm{N})},\mathrm{N});$$

[0111] 验证,$U3=\mathrm{H}_1(CT\|g^{r_1},\mathrm{N})$,若相等,则将CT发送到共享链中进行共享;反之,则丢弃密文CT;通过验证可证明密文CT通过了联盟链签名验证;

[0112] (3)上链阶段:采用UTXO的形式上链,次节点A将上次交易的编号Number和上次交易的哈希值HLast,和本次交易的群签名SignCT发送到联盟链主节点V中,主节点V生成新生区块New__block,并对区块中的信息进行验证,若验证通过,则并入共享链中,反之,丢弃区块;

[0113] 在联盟链AC验证阶段,联盟链中各节点寻找共享链中与此新生区块关联的上一次交易信息,并对比新生区块的输入和上一次交易的输出值是否相同,若经过联盟链中大多数节点的同意后,主节点将该新生区块并入共享链中,反之,丢弃该新生区块。

[0114] 5、数据使用者解密阶段:

[0115] (1)离线解密机构ODA进行部分解密:ODA__Dec(AC,CT,TK)→PC,数据使用者DU将密文CT和密文转换密钥TK传给离线解密机构ODA;离线加密机构ODA首先检查数据使用者的属性集AS是否满足访问结构AC的要求,若满足,则对密文CT进行部分解密并将部分解密密文PC发送给数据使用者DU;反之,则输出0;

[0116] $PC=(AC,MM,R\cdot e(g,g)^{\alpha s},g^s,e(g,g)^{da\theta/z},C_1)$;

[0117] (2)数据使用者DU进行解密:DU__Dec(PC,CPA__SK)→R;数据使用者DU通过属性加密密钥CPA__SK对部分解密密文PC解密,得到随机密文参数R;

[0118] $R=R\cdot e(g,g)^{\alpha s}/(e(g^{s},g^{\alpha}h^{d})/e(g,g)^{das})$；

[0119] $Message=H_1(R)\oplus MM$。

[0120] 6、追责阶段：

[0121] (1)追责数据拥有者DO:DO__Accountability(DO__Verify,GMSK)→idDO。若群管理员投票通过要求追责数据拥有者后，则可通过来源验证值DO__Verify和群追踪密钥GMSK计算并获取数据拥有者的id；

[0122] 已知$u^{\sigma_1}=v^{\sigma_2}=h$，则$id_{DO}=id_{DO}h^{\chi+\tau}/u^{\chi\sigma_1}\cdot v^{\tau\sigma_2}$；

[0123] (2)追责签名者A:A__Accountability(SignCT,SignPK)→idA；在上链过程中，通过采用群签名验证的方法和UTXO的上链方式，若群管理员投票通过要求追责数据拥有者后，主节点可通过对本次交易进行逐链溯源的方式，找到首发地址进行追责；通过群签名SignCT和签名私钥SignP，提取出签名者A的idA哈希值HID，主节点逐一对比各个子节点的id对应的HID值即可找到签名者的idA。

[0124] 采用本发明所述的区块链隐私保护方法，通过在线离线属性加密算法，利用区块链结合离线加密机构及离线解密机构，在减小用户的计算开销的同时，实现细粒度的用户访问控制，适用于计算资源有限的设备，并通过共享链和联盟链的双链控制，防止了单点故障问题，防止用户和验证者之间出现共谋，同时，通过群签名验证，实现了对数据拥有者和验证者的双向追溯，增加了数控的安全性。

[0125] 以上所述仅为本发明的优选实施方式，并不用以限制本发明，对于本领域的技术人员来说，可以有各种更改和变化，凡利用本发明所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

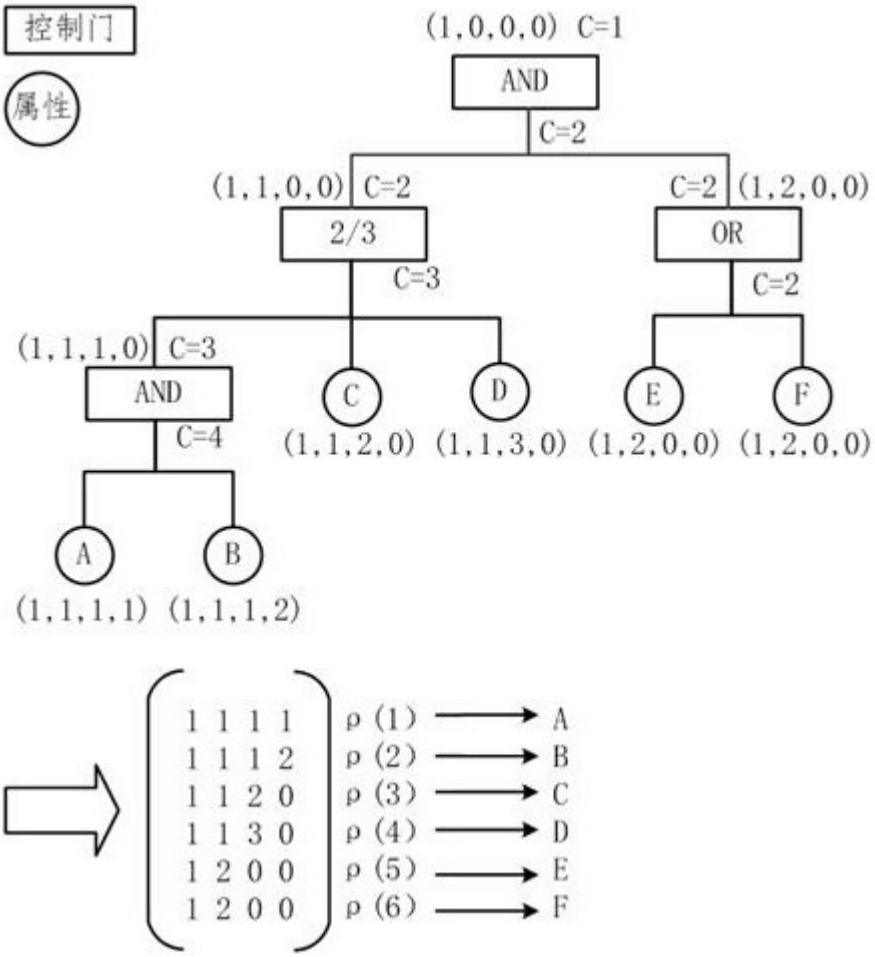

控制门
属性
(1,0,0,0) C=1
AND
C=2
(1,1,0,0) C=2
2/3
C=3
C=2 (1,2,0,0)
OR
C=2
(1,1,1,0) C=3
AND
C=4
C
D
E
F
(1,1,2,0)
(1,1,3,0)
(1,2,0,0)
(1,2,0,0)
A
B
(1,1,1,1)
(1,1,1,2)
1 1 1 1
1 1 1 2
1 1 2 0
1 1 3 0
1 2 0 0
1 2 0 0
ρ(1) → A
ρ(2) → B
ρ(3) → C
ρ(4) → D
ρ(5) → E
ρ(6) → F

图1

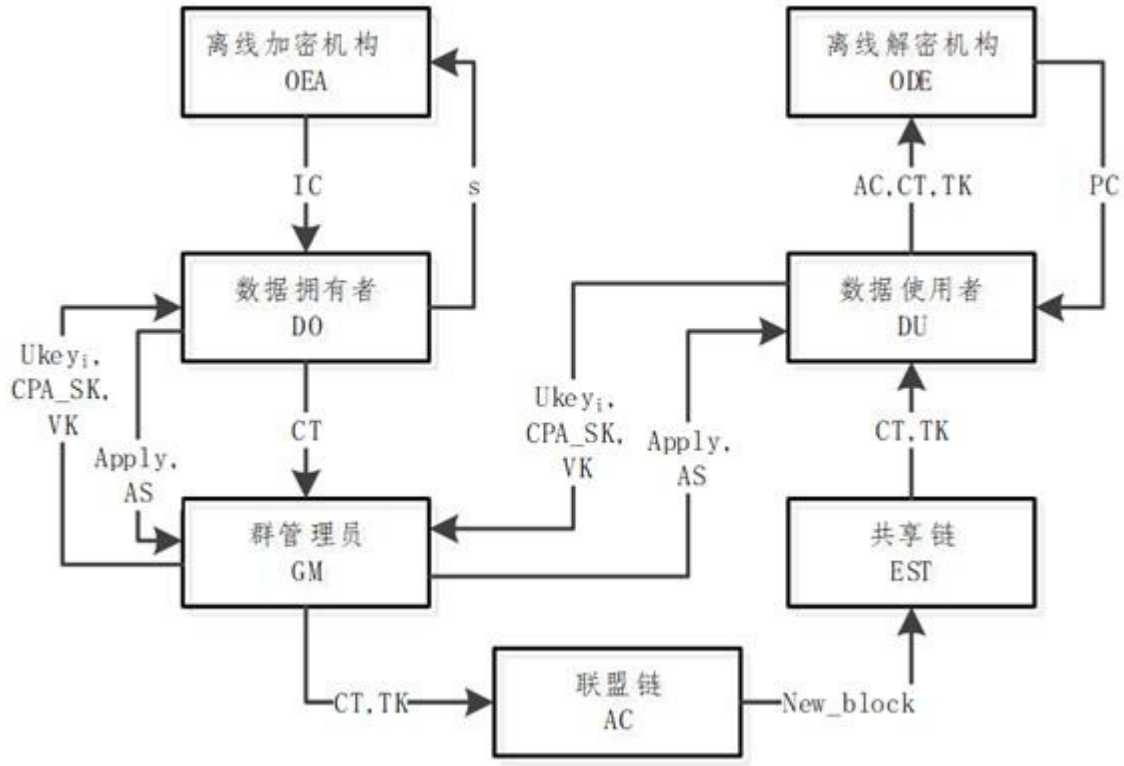

离线加密机构
OEA
离线解密机构
ODE
IC
s
AC,CT,TK
PC
数据拥有者
DO
数据使用者
DU
Ukey$_i$,
CPA_SK,
VK
Apply,
AS
CT
Ukey$_i$,
CPA_SK,
VK
Apply,
AS
CT,TK
群管理员
GM
共享链
EST
CT,TK
联盟链
AC
New_block

图2

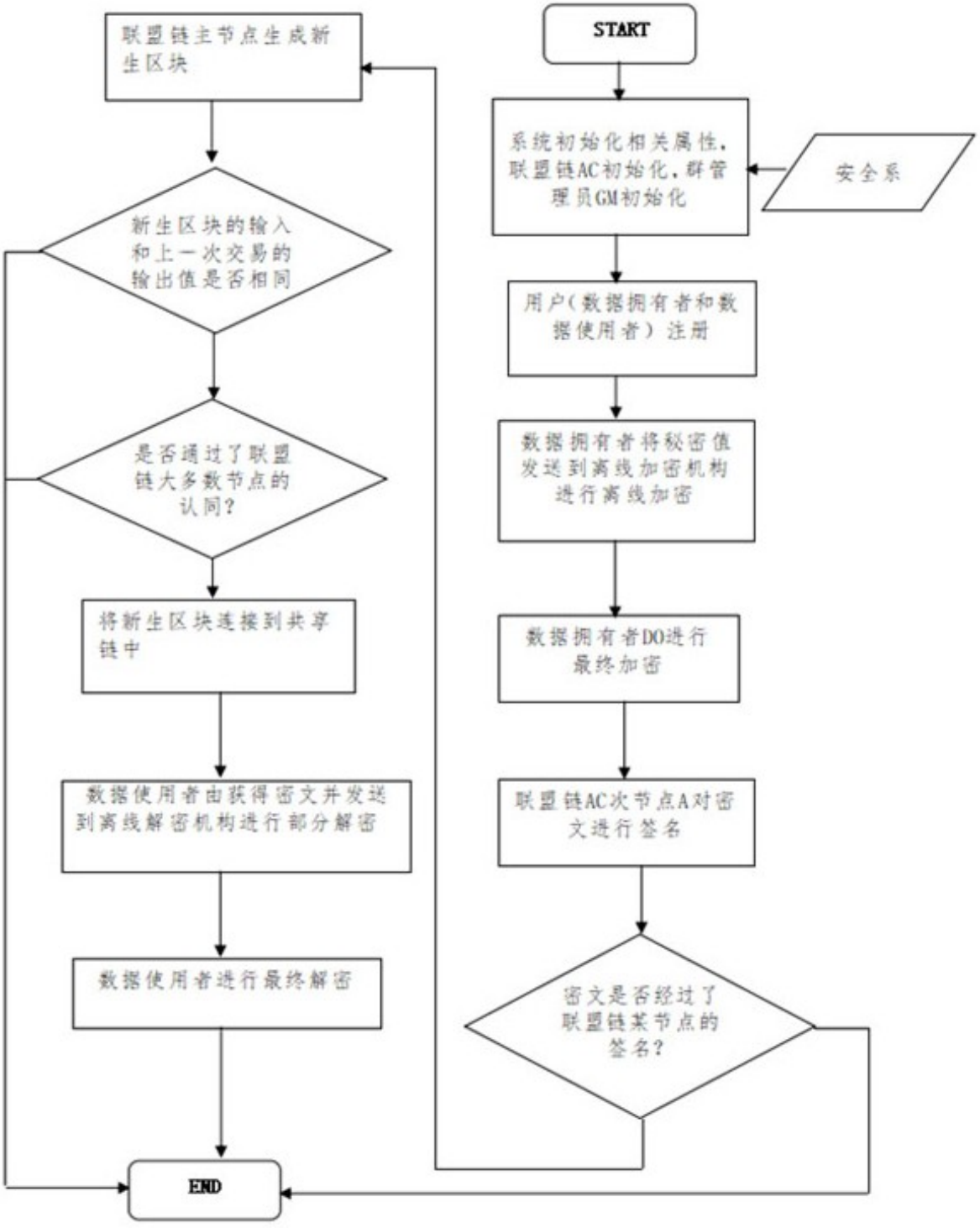

START
系统初始化相关属性，联盟链AC初始化，群管理员GM初始化
安全系
用户（数据拥有者和数据使用者）注册
数据拥有者将秘密值发送到离线加密机构进行离线加密
数据拥有者DO进行最终加密
联盟链AC次节点A对密文进行签名
密文是否经过了联盟链某节点的签名？
联盟链主节点生成新生区块
新生区块的输入和上一次交易的输出值是否相同
是否通过了联盟链大多数节点的认同？
将新生区块连接到共享链中
数据使用者由获得密文并发送到离线解密机构进行部分解密
数据使用者进行最终解密
END

图3