·网络空间安全·　　文章编号：1000-3428(2022)06-0132-07　　文献标志码：A　　中图分类号：TP311

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

（东北林业大学 信息与计算机工程学院，哈尔滨 150040）

摘　要：区块链技术的去中心化、数据难篡改等特性使其在溯源问题上体现出明显优势，基于区块链的溯源系统可以解决传统系统中信息孤岛、共享程度低以及数据可篡改等问题，从而保证数据的可追溯性。然而，区块链溯源系统中的数据可追溯性与用户隐私保护之间难以取得平衡。提出一种结合群签名、隐私地址协议、零知识证明以及属性加密的分布式可监管隐私保护方案。对群签名的群管理员机制进行改进，设置多群管理员生成用户私钥片段，用户根据返回的私钥片段计算自身私钥，并根据需要有选择性地对溯源数据进行属性加密，同时为链上数据设置特定的访问结构，以实现数据与用户的“一对多”通信。群管理员利用群公钥对交易双方的身份进行追踪与追责。符合数据特定访问结构的用户通过自身的属性私钥对密文进行解密从而获取数据信息。实验结果表明，该方案能在保证数据可追溯并实现交易双方监管的同时，提高链上数据的隐私保护水平，与现有隐私保护方案相比安全性更高。

关键词：区块链；监管；群签名；隐私地址；属性加密

开放科学（资源服务）标志码（OSID）：

中文引用格式：李莉，杜慧娜，李涛.基于群签名与属性加密的区块链可监管隐私保护方案[J].计算机工程，2022，48(6)：132-138.

英文引用格式：LI L，DU H N，LI T.Blockchain supervisable privacy protection scheme based on group signature and attribute encryption[J].Computer Engineering，2022，48(6)：132-138.

Blockchain Supervisable Privacy Protection Scheme Based on Group Signature and Attribute Encryption

LI Li，DU Huina，LI Tao

（College of Information and Computer Engineering，Northeast Forestry University，Harbin 150040，China）

【Abstract】The decentralization of blockchain technology and difficulty of data tampering provide it with obvious advantages in traceability.Traceability systems based on blockchain can solve information island，low sharing degree，and data tampering problems in traditional systems to ensure the traceability of data.However，balancing data traceability and user privacy protection is difficult in blockchain traceability systems.To solve this，a distributed supervised privacy protection scheme combining group signature，privacy address protocol，zero-knowledge proof，and attribute encryption is proposed. By improving the group administrator mechanism of group signature and setting multiple group administrators to generate user private key fragments，users can calculate their private keys according to the returned private key fragments，selectively encrypt the attribute of traceability data as required，and set a specific access structure for the data on the chain to realize "one to many" communication between data and users.The group administrator uses the group public key to track and hold accountable both parties to the transaction.Users who conform to the specific data access structure decrypt the ciphertext using their attribute private key to obtain data information. The experimental results show that the scheme can ensure the data traceability，realize the supervision of both parties，and even improve the privacy protection level of data on the chain.It has higher security than existing privacy protection schemes.

【Key words】blockchain；supervision；group signature；private address；attribute encryption

DOI：10. 19678/j. issn. 1000-3428. 0062464

0　概述

溯源系统通常被用来展示商品生产各环节的状态信息，但是，供应链的复杂性使得传统溯源系统缺乏透明度以及存在可追溯性差、数据不同步等问题[1-2]。区块链作为一种分布式账本技术[3]，其去中心化、难篡改等特点能在溯源系统的建立中发挥重要作用[4-5]。但是，在目前的区块链溯源系统中，多采用将完全可见数

基金项目：黑龙江省教育科学规划课题-重点课题（GJB1421251）。

作者简介：李　莉（1977—），女，副教授、博士，主研方向为先进软件工程技术、区块链技术、大型分布式计算；杜慧娜、李　涛，硕士研究生。

收稿日期：2021-08-24　　**修回日期：**2021-10-29　　**E-mail：**lli@nefu.edu.cn

据上链的方法以保证数据的可追溯性，这带来了一定的用户隐私泄露风险。过多的隐私保护又将使得交易不可监管，这在需要监管机构介入的溯源应用中不可接受[6-7]，因此，在对交易双方身份进行有效监管的同时实现用户的隐私保护成为一个研究热点。

在区块链隐私保护方面，MONERO[8]通过环签名技术，使用签名用户与其他用户的公钥对交易信息进行签名，使得攻击者无法从签名中确定交易发起者的身份，从而保护了用户的隐私。零币使用zk-SNARKs零知识证明[9]对交易信息进行完全隐藏，有效地保护了信息的隐匿性。李龚亮等[10]提出一种既能对交易进行加密又能支持零知识证明的隐私保护方案，实现了交易数据的完全隐匿。但是，以上方法多采用将数据完全隐藏的方式来保护用户的隐私安全，这在需要监管介入的溯源系统中并不适用。

在区块链的用户身份监管和访问权限控制方面，张思亮等[11]提出一种基于环签名、零知识证明、隐私地址的可追踪账本交易隐私保护方案，该方案可以有效地实现监管人对用户身份的追踪。李佩丽等[12]对群签名进行改进，实现了交易双方身份的监管。王震等[13]通过监管方对用户的匿名证书进行解密从而实现监管。姜轶涵等[14]基于零知识证明、同态加密等，设计一种可以对一段时间内所有用户的交易金额进行审计的方案，从而实现了交易内容的追踪。谢绒娜[15]与田有亮等[16]通过访问权限细粒度划分来提高数据安全性。

经过分析可以发现：现存溯源系统研究大多将完全可见的数据上链以保证数据的可溯源性，这增加了用户隐私泄露的可能性；现存隐私保护技术大多采用将数据完全隐匿的方式来保证用户的隐私安全，但是，在要求数据可追溯与监管的溯源系统中并不适用；现存可监管方案大多通过引入单管理员角色进行交易或数据监管，此时管理员拥有绝对的权限，如果管理员是恶意的，可能导致用户隐私泄露。

本文提出一种基于群签名与属性加密的双重隐私保护方案，以解决区块链溯源中隐私保护与数据可追溯性难以平衡的问题。使用群签名实现用户身份的加密与监管，利用可选择的属性加密方案，使得用户自主选择是否对部分隐私数据进行相应的属性加密从而实现数据访问权限控制。对群签名进行改进，在区块链系统中使用多群管理员机制群签名策略，以解决传统群签名在区块链溯源用户监管方面的不足。

1　技术背景

本文相关技术背景介绍如下：

1）BBS04群签名。在群签名方案中[17]，一个群体中的任何一个群成员都可以以匿名的形式代表群体对消息进行签名，且群签名可公开验证。BONEH等[18]于2004年提出一种短群签名方案，该方案构造了强度小于200 Byte的签名，安全性基于具有双线性映射群的q-SDH，相对于RAS签名更简单且更短。BBS04群签名的简短性可节省链上存储空间，且其可追踪性能够很好地应用于有监管者介入的区块链溯源系统。但是，单个群管理员拥有至高的权限，一旦其产生恶意想法，有可能导致数据泄露，威胁用户的隐私安全。因此，需要引入多群管理员机制，使得群管理员之间相互制约，这也符合区块链的去中心化原则。

2）DKSAP隐私地址协议。隐私地址协议是一种用于保护交易接收方隐私安全的技术。发送方在创建交易时为交易接收方随机生成一个接收地址，且该隐私地址可以被交易接收方所计算与打开。通过每次交易来更换用户的交易接收地址，可以更好地保护接收方的隐私安全。本文使用隐私地址保护交易接收方的隐私安全，攻击者无法通过数据分析来获取交易接收方的信息，且群管理员可以对接收方进行监管。

3）Bulletproofs零知识证明。Bulletproofs[19]是BUNZ等于2018年提出的一种知识系统的零知识证明，可用于证明一个秘密的存在。Bulletproofs支持范围证明的聚合，可证明m个承诺存在于给定的范围内，其边际成本较低且不需要可信设置。本文所提方案应用Bulletproofs零知识的范围证明，对用户的撤销状态进行范围证明，通过证明所验证的撤销标记是否在[0，1]范围内来判断用户的撤销状态。

4）CP-ABE属性加密。属性加密是一种新型的加密技术[20]，其将用户的访问权限与用户的身份属性相关联，为密文设定访问结构，只有属性基与访问结构相对应才可以对数据进行访问。

2　区块链溯源可监管双重隐私保护方案

2.1　隐私保护目标

本文隐私保护方案的目标如下：

1）实现用户隐私保护与用户可监管之间的平衡。现存溯源系统大多将完全透明的数据上链以保证数据的可追溯与可监管，该方式提高了用户信息及数据泄露的可能性，本文方案考虑隐私保护与用户监管2个方面，目标是在保护用户隐私的同时实现用户的监管。

2）改进目前溯源系统中的数据可溯源访问机制。本文方案的目标是在保护用户隐私的同时实现数据的可追溯，应用属性加密“一对多”的数据细粒度访问特点，使得溯源系统中的数据可被多人访问又不被所有人可见。

3）引入监管角色，在实现用户身份追踪的同时保证用户隐私。鉴于溯源系统需要监管介入且监管机构不唯一的特性，本文应用群签名实现用户的监管，对群签名进行改进，设置多群管理员机制，解决单群管理员权限过高所带来的隐私泄露风险，在实现可监管的同时提高方案的安全性。同时，将隐私地址协议与群签名相融合，实现交易接收方追踪。

2.2　方案设计

本文方案要实现溯源系统中交易双方身份的追踪，同时设置多群管理员机制以符合区块链的去中心化原则。根据溯源系统中的具体场景设置4种角色，分别

是签名者、验证者、群管理员、数据查看者：签名者对溯源信息进行签名；验证者验证消息是否为群成员所签并对数据进行广播；群管理员为用户生成私钥并对签名者的身份进行追踪；数据查看者查看链上溯源数据。

本文方案提供双重隐私保护：第一重使用群签名为用户提供身份隐私保护同时实现用户身份的可追踪；第二重使用属性加密为用户与溯源数据设置特定的访问结构，实现数据的细粒度访问控制。方案框架如图1所示。

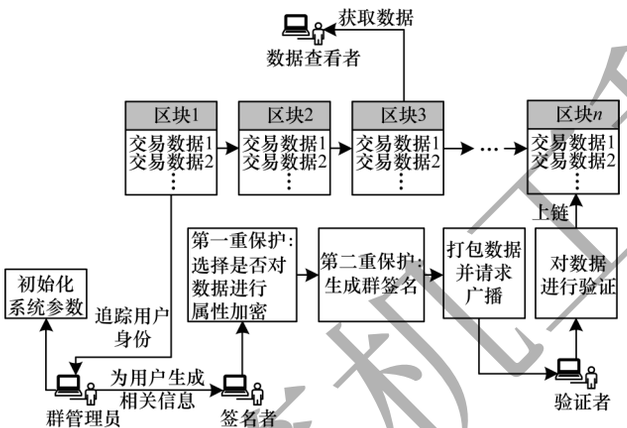

图1 本文方案框架

Fig.1 The framework of this scheme

本文方案的实现步骤具体如下：

步骤1 根据共识机制选出一定数量的群管理员并为其分配密钥。

步骤2 系统初始化。生成群公钥、群管理员私钥、属性密钥、监管密钥等。

步骤3 用户注册。系统为用户生成公钥、属性密钥，各群管理员为用户生成私钥片段，用户通过计算获得自己的私钥。

步骤4 生成上链数据。交易发起方调用智能合约选择是否为溯源信息设置访问结构，并申请将溯源信息广播到区块链。

步骤5 验证消息合法性。验证者对交易发起方的身份进行验证并执行验证通过的广播请求。

步骤6 身份追踪。群管理员进行投票决定是否对交易进行追踪，如果投票值大于群管理员数量的2/3，则对交易进行追踪。

步骤7 数据共享。用户访问数据信息，如果用户设置了属性加密，在用户属性密钥与数据访问结构一致时允许访问；如果没有设置属性加密，则可直接对数据进行访问。

2.3 系统初始化

系统初始化主要完成2个任务，即初始化系统相关属性并为监管角色（群管理员）生成相关密钥。具体步骤如下：

1）在共识阶段选出 $t(t\geqslant 1)$ 个群管理员，系统为各群管理员分发公钥 Y。

2）随机选取 G 的生成元 g_2，g_1 由同构映射 $\psi(g_2)$ 产生。选取 $h\xleftarrow{R}G_1 1_{G_1}$ 和 $\delta_1,\delta_2\xleftarrow{R}Z_p^*$，令 $u,v\in G_1(u^{\delta_2}=h)$，每个GM的密钥为 $\gamma_j\left(\gamma_j\xleftarrow{R}Z_p^*\right)$ 且 $w_j=g_2^{\gamma_j}$。

3）设置系统属性集为 $S_j=\{s_1,s_2,\cdots,s_n\}$。

4）初始化一个空的撤销列表RL与投票值 T_r，其中，RL用来存储撤销用户的撤销标记，T_r 用来收集其他管理员在追踪问题上的意见（支持与不支持）。

5）生成群公钥为：

$$\mathrm{gpk}=(g_1,g_2,h,u,v,\{w_j|1\leqslant j\leqslant t\})$$

群追踪密钥为：

$$\mathrm{gmsk}=(\delta_1,\delta_2)$$

2.4 用户注册

用户提出注册申请，各群管理员为用户生成私钥片段并返回，用户通过计算获得自己的私钥与ID。具体过程如下：

1）用户 i 向所有群管理员提出注册申请，并提交用户属性集 $S_i=\{s_1,s_2,\cdots,s_n\}$。

2）各群管理员生成用户 i 的私钥片段 $A_{i_j}\leftarrow g_1^{1/(\gamma_j+x_i)},x\in Z_p$，并通过安全信道发送给用户 i，用户 i 计算私钥 $A_i\leftarrow g_1^{\sum_{j=1}^{m}1/(\gamma_j+x_i)}$。

3）用户计算自己的ID，$\mathrm{ID}_i=g_1^{A_i}$。

4）由 g_1^u 以及用户属性集生成用户属性密钥SK，$\mathrm{SK}=\{K=g_1^u g_2^v,L=g_1^t,Ks=h_s^t,\forall s\in S,t\in Z_p\}$。

2.5 上链数据生成

对溯源信息进行处理，假设用户Bob向用户Alice购买产品，相关数据为 m，m 包含商品的生产日期、生产地点、原料、交易金额等信息，Bob与Alice的密钥对分别为 $(\mathrm{ID}_{\mathrm{Alice}},A_{\mathrm{Alice}})$ 和 $(\mathrm{ID}_{\mathrm{Bob}},A_{\mathrm{Bob}})$。上链数据生成过程如下：

1）用户Alice生成一个临时密钥对 (R,r)，其中，$R=rG$，该密钥对随交易传输，同时根据 $ty=H(r\cdot\mathrm{ID}_{\mathrm{Bob}})=H(\mathrm{ID}_{\mathrm{Bob}}\cdot R)$，计算共享秘密 ty 并使用群公钥进行加密，发送方使用 $\mathrm{ID}_{\mathrm{Bob}}\cdot g_1^{ty}$ 生成消息接收方所共有的临时地址 $S.A$。

2）Alice选取指数 $\alpha,\beta\xleftarrow{R}Z_p$，计算 $T_1\leftarrow u^{\alpha}$，$T_2\leftarrow v^{\beta}$，$T_3\leftarrow A_i h^{\alpha+\beta}$，随机选择盲化因子 r_α、r_β、r_x、r_{δ_1}、r_{δ_2}，计算：

$$R_1\leftarrow u^{\gamma_\alpha}$$

$$R_2\leftarrow u^{\gamma_\beta}$$

$$R_3\leftarrow \hat{e}(T_3,g_2)^{r^*}\times\prod_{i=1}^{t}\hat{e}(h,w_i)^{-r_\alpha-r_\beta}\times\hat{e}(h,g_2)^{-m(r_{\delta_1}-r_{\delta_2})}$$

$$R_4\leftarrow T_1^{r_x}\times u^{-r_{\delta_1}}$$

$$R_5\leftarrow T_2^{r_x}\times v^{-r_{\delta_2}}$$

3）使用Hash函数计算询问值：

$$c\leftarrow H(M\|T_1\|T_2\|T_3\|R_1\|R_2\|R_3\|R_4\|R_5)$$

4）根据 c 生成参数，其中：

$$\sigma_1\leftarrow x\alpha$$

$$\sigma_2\leftarrow x\beta$$

$$s_\alpha\leftarrow r_\alpha+c\alpha$$

$$s_\beta\leftarrow r_\beta+c\beta$$

$$s_x\leftarrow r_x+cx$$

$$s_{\sigma_1}\leftarrow r_{\sigma_1}+c\sigma_1$$

$$s_{\sigma_2}\leftarrow r_{\sigma_2}+c\sigma_2$$

5）生成Alice撤销标记的Bulletproofs零知识证明，通过该证明可以在不获取用户撤销标记具体值的情况下验证Alice身份的合法性，步骤如下：

构造 a_L、a_R，使得 $<a_L,2>=\mathrm{reg}$，$a_R=a_L-1$，构造 a_L、a_R 的承诺 $A=h^{\alpha}g^{a_L}h^{\alpha_R}$。

随机选取盲化因子 $s_L\in Z_p^n$、$s_R\in Z_n^p$、$\theta\in Z_p$，构造 s_L、s_R 的承诺 $S=h^{\rho}g^{s_L}h^{s_R}$。

计算：

$y=H(A,S)$

$z=H(A,S,y)$

$T_i=g^{t_i}h^{\tau_i},i=\{1,2\}$

$x=H(T_1,T_2,z)$

$l=l(x)=a_L-z+s_L\cdot x$

$r=r(x)=y^n\circ(a_R+z+s_R\cdot x)+z^2\cdot 2$

$t(x)=<l(x),r(x)>$

$\tau(x)=\tau_1\cdot x+\tau_2\cdot x^2+z^2\cdot\gamma,\gamma\in Z_P$

$\varepsilon=\alpha+\theta\cdot x$

构造关于reg的承诺 $V=g^{\mathrm{reg}}h^{\gamma}$。由此，零知识证明 $\eta=\{\tau(x),\varepsilon,t(x),l(x),r(x)\}$。

6）签名为：

$\sigma\leftarrow(M,T_1,T_2,T_3,c,s_{\alpha},s_{\beta},s_x,s_{\sigma_1},s_{\sigma_2},\boldsymbol{S}.A,t,\eta)$

7）加密产品相关信息 m，输入明文 m、gmsk以及访问策略 $(\boldsymbol{M},\rho)$，返回密文CT。其中，$\mathrm{CT}=\{C=me(g_1,g_1)^{u^{\delta_1}v^{\delta_2}ty},C=g_1^{ty\delta_1},(C_i=g^{u\lambda_i\delta_1}h_{\rho_i}^{-r_i})_{p\in(1,l)}\}$，$\boldsymbol{M}$ 为 $1\times n$ 的访问矩阵，M_i 表示矩阵中的第 i 行，函数 ρ 将 M_i 映射到属性，记 $\rho\{1,2,\cdots,l\}\rightarrow\{1,2,\cdots,n\}$，$ty$ 为共享秘密，p 为随机值。

8）将产品相关信息CT、撤销标记的知识证明 η、加密后的共享秘密 ty、签名等信息广播给验证节点。

2.6　消息合法性验证

消息合法性验证过程如下：

1）对零知识证明 η 进行验证，判断用户的身份是否合法。验证步骤为：计算 $h_i'=h_i^{y^{-i+1}}$；判断 $g^{t(x)}h^{\tau_x}=V^{z^2}\cdot T_1^{x}\cdot T_2^{x^2}$ 是否成立；判断 $AS^x\cdot g^{-z}\cdot h'^{z\cdot y\vec{e}^n\cdot 2}=h^{\mu}g^{l}$ 是否成立；判断 $t(x)=<l(x),r(x)>$ 是否成立。若以上判断均成立，则接收，即该用户身份合法。

2）在验证通过后，计算：

$$\tilde{R}_1\leftarrow u^{s_{\alpha}}\times T_1^{-c}$$

$$\tilde{R}_2\leftarrow v^{s_{\beta}}\times T_2^{-c}$$

$$\tilde{R}_3\leftarrow \hat{e}(T_3,g_2)^{s_x}\times\prod_{j=1}^{t}\hat{e}(h,w_i)^{-s_{\alpha}-s_{\beta}}\times \hat{e}(h,g_2)^{-m(s_{\delta_1}-s_{\delta_2})}\times\prod_{j=1}^{t}\left[\hat{e}(T_3,w_j)/\hat{e}(g_1,g_2)\right]^{c}$$

$$\tilde{R}_4\leftarrow T_1^{s_x}\times u^{-s_{\delta_1}}$$

$$\tilde{R}_5\leftarrow T_2^{s_x}\times v^{-s_{\delta_2}}$$

然后计算：

$\bar{c}=H(M\|T_1\|T_2\|T_3\|\tilde{R}_1\|\tilde{R}_2\|\tilde{R}_3\|\tilde{R}_4\|\tilde{R}_5)$

如果 $c=\bar{c}$，则签名有效；否则，签名无效。若签名有效，则将验证通过的溯源信息上传到区块链。

2.7　成员撤销

当用户做出不诚信行为或想要主动退出时，群管理员可以对用户执行撤销操作。假设要撤销用户 $1,2,\cdots,r$，撤销列表RL包含所有被撤销用户的私钥。其中，$\mathrm{RL}=\{(A_1,x_1,\mathrm{reg}_1),\cdots,(A_r,x_r,\mathrm{reg}_r)\}$。分如下两种情况讨论：

1）如果是群管理员执行撤销操作，则群管理员将用户的私钥信息加入到撤销列表RL中，同时更新用户的撤销标记，然后发布新的撤销列表RL，若撤销成功，则返回0；否则，返回-1。

2）如果是群成员主动申请撤销操作，则用户先将自己的撤销标记 $(A_i,\mathrm{reg}_i,\sigma)$ 发送给GM，GM验证群成员的身份，如果验证成功，则执行第一种操作。

2.8　身份追踪

在收到对某笔交易的追踪请求时，所有的群管理员共同决定是否对交易进行追踪，当超过2/3的群管理员持赞成意见时，则对交易的参与方进行追踪。追踪过程如下：

1）交易发送方的追踪

通过群公钥计算出用户的私钥，然后对用户信息索引进行读取，获取用户身份信息。

对请求读取数据的CA进行属性集合检验，通过后可读取各群管理员存储的用户密钥片段，然后最多通过 $O(n^t)$（n 为群管理员处注册的用户数）次乘法计算，即可获取用户的身份信息。证明过程如下：

已知 $u^{\delta_1}=v^{\delta_2}=h$，$T_1\leftarrow u^{\alpha}$，$T_2\leftarrow v^{\beta}$，$T_3\leftarrow A_ih^{\alpha+\beta}$，则 $A_i=\dfrac{T_3}{h^{\alpha+\beta}}=\dfrac{T_3}{(u^{\delta_1})^{\alpha}\cdot(v^{\delta_2})^{\beta}}=\dfrac{T_3}{T_1^{\delta_1}\cdot T_2^{\delta_2}}$，证毕。

2）交易接收方的追踪

通过打开签名获取临时交易地址 $S.A$ 以及共享秘密 ty，即可从 $S.A$ 中抽取接收方公钥，追踪到接收方的身份。证明过程如下：

已知 $S.A=\mathrm{ID}_{\mathrm{Bob}}\cdot g_1^{ty}$，$ty=H(r\cdot\mathrm{ID}_{\mathrm{Bob}})=H(\mathrm{ID}_{\mathrm{Bob}}\cdot R)$，$S.A=g_1^{A_i+ty}$，$g_1^{A_i}=S.A/g_1^{ty}$，证毕。

3）追责

根据产品的状态信息判断出责任方，可对违规用户进行撤销操作，从而惩戒恶意行为。

2.9　数据共享

当用户需要查看溯源信息时，发出查看申请，系统根据用户的属性私钥和访问策略 $(\boldsymbol{M},\rho)$ 下的密文CT进行解密，如果用户的属性集能够满足数据的访

问策略，则允许用户对数据进行访问，输出明文 $m\left(m=\frac{C}{e(g_1,g_1)^{uty\delta_1}}\right)$；否则，访问失败。

3 方案分析与实验验证

3.1 方案分析

本文方案性能分析具体如下：

1）匿名性。本文方案将群签名与隐私地址相结合以保护交易双方的身份信息，使用户身份信息对非群管理员不可见，从而保证方案的匿名性。其中，使用多群管理员机制的群签名技术保护用户隐私，追踪密钥仅由群管理员拥有，用户的私钥由群管理员共同生成，且保证了在有少量恶意群管理员节点的情况下无法进行用户身份信息复原。相较单群管理员方案，本文方案拥有更强的匿名性，且其他用户无法获取交易用户的具体信息，从而保护了用户隐私。另外，使用隐私保护技术，每笔交易都生成一个临时地址，该临时地址必须用追踪密钥才可以解密，使得攻击者无法将交易信息进行关联，从而保护了交易接收方的隐私。

2）可追踪性。本文方案通过使用群追踪密钥来计算用户私钥，然后读取本地的用户索引获取到交易发起方的身份，打开签名得到解密后的共享秘密，进而获取接收方的身份信息，实现对交易接收方的追踪。

3）安全性。本文方案基于群签名、属性加密以及隐私地址进行设计，群密钥只保存在群管理员手中，且单个群管理员只负责生成用户的部分密钥，完整的密钥由用户根据各群管理员传回的密钥片段计算生成。因此，不存在单群管理员泄露用户私钥造成用户隐私泄露的可能性。相比传统的单群管理员群签名方案，本文方案具有更高的安全性。使用隐私地址技术，每次交易都为交易接收方生成一个新的地址，使得攻击方无法通过数据分析来获取接收方的地址，提高了接收方的隐私安全性。另外，用户对上传的数据可选择性地设置属性加密，通过为数据设置特定的访问结构实现数据的细粒度访问控制，进一步实现数据的安全保护。

3.2 实验环境

通过实验对本文隐私保护方案进行测试，以验证其正确性以及效率。实验基于联盟链平台 fisco-bcos 进行，fisco-bcos 为对外开源的底层区块链平台，可插入隐私保护算法。共识算法采用PBFT，双线性映射使用pbc库实现，编程语言采用GO语言。实验设备配置为 Ubuntu-20.04.2.0 64位，CPU 为 Intel Core i7-6500U @2.50 GHz。

3.3 正确性测试

本文方案主要实现交易双方身份监管，因此，方案注重能否实现用户身份追踪。本次实验通过模拟恶意节点对消息进行签名能否通过验证，以及合法用户对消息进行签名能否实现身份跟踪，以测试本文方案的正确性。预设4种场景进行测试，实验结果如表1所示。

表1 正确性测试结果

Table 1 Correctness test results

场景	场景内容	预设结果	验证数据组数	验证通过组数	验证失败组数
1	恶意节点对消息进行签名，并发起验证请求	询问值 $c\neq\bar{c}$，验证不通过，丢弃交易	100	0	100
2	合法用户对消息进行签名，并发起验证请求	询问值 $c=\bar{c}$，接受该交易并对其进行广播	100	100	0
3	对合法用户的签名进行追踪	可追踪到交易双方的身份	100	100	0
4	不符合数据访问策略的用户对数据进行访问	无法获取明文	100	0	100

从表1可以看出，本文方案可以正确地实现对用户的身份追踪以及对数据的细粒度访问控制。

3.4 性能对比

3.4.1 方案对比

本节分别从管理员数量、追踪方、是否可对用户进行撤销惩罚以及是否控制数据访问权限4个方面，对本文方案进行分析并将其与其他方案作对比。从表2可以看出，本文方案可以在分化群管理员权限的同时，实现用户双方身份的可追踪与细粒度访问控制，在用户的信息保护方面更具优势。

表2 方案性能对比

Table 2 Schemes performance comparison

方案	群管理员数量	追踪方	是否可对用户进行撤销惩罚	是否控制数据访问权限
本文方案	动态	双方	是	是
文献[11]方案	无	双方	否	否
文献[21]方案	1	单方	是	否
文献[22]方案	2	双方	否	否

3.4.2 计算成本

设$|M|$为模幂运算的计算成本，$|P|$为双线性对运算的计算成本，$|H|$为哈希运算的计算成本。从表3

可以看出，与文献[21]方案相比，本文方案需要更高的时间成本，当群管理员不同时，所消耗的时间成本逐渐增加，在初始化、生成上链数据以及验证阶段，由于需要多群管理员参与，消耗的时间成本与群管理员数量相关。

表3　2种方案各步骤花费的计算成本对比

Table 3　Calculation cost comparison of each step of two schemes

步骤	本文方案	文献[21]方案
初始化	$t\|M\|$	$4\|M\|$
用户注册	$(t+2)\|M\|$	$\|M\|$
生成一次性地址	$2\|H\|$	$3\|M\|+\|H\|$
生成上链数据	$(16+t)\|M\|+(2+t)\|P\|+4\|H\|$（不进行属性加密） $(19+t)\|M\|+(3+t)\|P\|+4\|H\|$（进行属性加密）	$(12+4m)\|M\|+3\|P\|+3m\|H\|$
验证	$(9+3t)\|M\|+(1+4t)\|P\|+\|H\|$	$(12+4m)\|M\|+5\|P\|+3\|H\|$

为了得知本文方案具体的时间代价，在Ubuntu-20.04.2.0系统中编写程序，分别对群管理员个数不同、属性个数不同以及零知识证明情况下所消耗的时间成本进行测试。

1）群管理员数不同时各阶段所花费的时间

由于本文方案主要花费时间在上链数据生成、验证以及追踪阶段，通过编写程序进行测试，呈现群管理员数量对时间代价的影响，测试结果如图2所示。

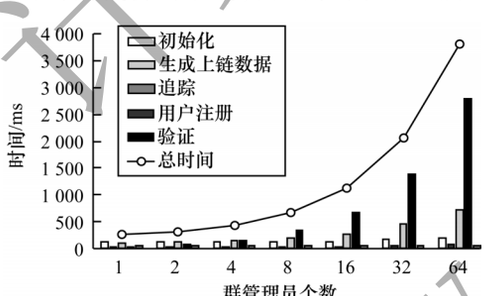

图2　群管理员数量对时间代价的影响

Fig.2　Influence of the number of group administrators on time cost

从图2可以看出，随着群管理员数量的增加，所花费的时间逐渐增多，在群管理员数量为16时，约消耗1 127 ms，在群管理员数量为64时，约消耗3 794 ms，本文方案可以根据实际需要选择群管理员数量，在保证用户身份可追踪且保护用户隐私的情况下，增加毫秒级别的时间是可以接受的。

2）属性个数不同时属性加密所花费的时间

在本文方案中，用户对数据选择性地进行属性加密，从而实现数据的细粒度访问权限控制。由于本文方案中的角色划分种类较少，因此属性集包含的属性值数量较少，对属性个数为4~8时加密算法的时间代价进行测试，结果如图3所示。从图3可以看出，当属性个数分别为4、6、8时，加解密花费的时间代价逐渐上升，其中，当属性个数为4时，加解密分别约消耗324 ms、246 ms，当属性个数为8时，加解密分别约消耗443 ms、382 ms。

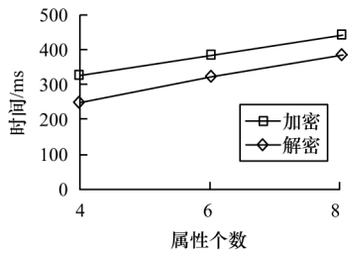

图3　同文件下属性加密所花费的时间

Fig.3　Time spent on attribute encryption under the same file

3）零知识证明生成与验证所花费的时间

本文方案使用零知识证明验证用户的撤销标记，在不泄露用户身份隐私的情况下验证用户身份的合法性。由于本文方案验证撤销标记是否在[0，1]区间内，因此对范围[0，1]进行证明。其中，椭圆曲线群阶为1 024。从图4可以看出，零知识证明生成与验证所花费的时间对方案性能的影响在可接受范围内。

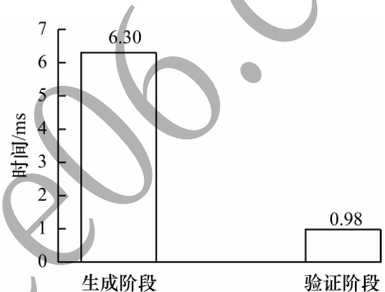

图4　零知识证明生成与验证所花费的时间

Fig.4　Time spent on generation and verification of zero-knowledge proof

综上所述，本文方案所花费的时间在可接受范围内，相较其他单一方向监管的隐私保护方案，本文方案不仅可以实现用户双方的监管与群管理员分权，而且可以选择性地决定是否对数据进行属性加密，在群签名的基础上实现数据的双重保护，安全性更高。

4　结束语

针对基于区块链的溯源系统中数据隐私与可追溯性难以平衡的问题，提出一种区块链可监管双重隐私保护方案。由多群管理员共同生成用户密钥，满足溯源场景对监管介入的需求，同时用户有选择性地对数据进行属性加密，在保证数据可追溯的同时实现数据的细粒度访问控制。实验结果表明，该方案所花费的时间成本在可接受范围内，并且能够实现更高级别的隐私安全。本文方案中群管理员所拥有的权限相等，且追踪时间随着群管理员数目的增加而延长，如何提高追踪效率以及使用分级群签名来对监管机构的权限进行更细粒度的划分，将是下一步的研究方向。

参考文献

[1] CALVÃO F, ARCHER M. Digital extraction: blockchain traceability in mineral supply chains[J]. Political Geography, 2021, 87: 102381.

[2] QIU Z H, ZHU Y F. Traceability anti-counterfeiting system based on the ownership of edge computing on the blockchain [J]. Journal of Ambient Intelligence and Humanized Computing, 2021, 8: 1-14.

[3] 张亮,刘百祥,张如意,等. 区块链技术综述[J]. 计算机工程,2019,45(5):1-12.
ZHANG L, LIU B X, ZHANG R Y, et al. Overview of blockchain technology[J]. Computer Engineering, 2019, 45(5): 1-12. (in Chinese)

[4] UDDIN M. Blockchain Medledger: Hyperledger fabric enabled drug traceability system for counterfeit drugs in pharmaceutical industry [J]. International Journal of Pharmaceutics, 2021, 597: 120235.

[5] 王志铧,柳平增,宋成宝,等. 基于区块链的农产品柔性可信溯源系统研究[J]. 计算机工程,2020,46(12):313-320.
WANG Z H, LIU P Z, SONG C B, et al. Research on flexible and reliable blockchain-based traceability system for agricultural products[J]. Computer Engineering, 2020, 46(12): 313-320. (in Chinese)

[6] MAJDALAWIEH M, NIZAMUDDIN N, ALARAJ M, et al. Blockchain-based solution for secure and transparent food supply chain network[J]. Peer-to-Peer Networking and Applications, 2021, 14(6): 3831-3850.

[7] 赵维. 基于区块链技术的农业食品安全追溯体系研究[J]. 技术经济与管理研究,2019(1):16-20.
ZHAO W. Research on traceability system of agricultural-food safety based on block chain technology[J]. Journal of Technical Economics & Management, 2019(1): 16-20. (in Chinese)

[8] LI Y N, YANG G M, SUSILO W, et al. Traceable monero: anonymous cryptocurrency with enhanced accountability[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(2): 679-691.

[9] RAHIMI A, MADDAH-ALI M A. Multi-party proof generation in QAP-based zk-SNARKs[J]. IEEE Journal on Selected Areas in Information Theory, 2021, 2(3): 931-941.

[10] 李龚亮,贺东博,郭兵,等. 基于零知识证明的区块链隐私保护算法[J]. 华中科技大学学报(自然科学版),2020,48(7):112-116.
LI G L, HE D B, GUO B, et al. Blockchain privacy protection algorithms based on zero-knowledge proof[J]. Journal of Huazhong UWniversity of Science and Technology (Natural Science Edition), 2020, 48(7): 112-116. (in Chinese)

[11] 张思亮,凌捷,陈家辉. 可追踪的区块链账本隐私保护方案[J]. 计算机工程与应用,2020,56(23):31-37.
ZHANG S L, LING J, CHEN J H. Traceable blockchain ledger privacy protection scheme[J]. Computer Engineering and Applications, 2020, 56(23): 31-37. (in Chinese)

[12] 李佩丽,徐海霞. 区块链用户匿名与可追踪技术[J]. 电子与信息学报,2020,42(5):1061-1067.
LI P L, XU H X. Blockchain user anonymity and traceability technology[J]. Journal of Electronics & Information Technology, 2020, 42(5): 1061-1067. (in Chinese)

[13] 王震,范佳,成林,等. 可监管匿名认证方案[J]. 软件学报,2019,30(6):1705-1720.
WANG Z, FAN J, CHENG L, et al. Supervised anonymous authentication scheme[J]. Journal of Software, 2019, 30(6): 1705-1720. (in Chinese)

[14] 姜轶涵,李勇,朱岩. ACT:可审计的机密交易方案[J]. 计算机研究与发展,2020,57(10):2232-2240.
JIANG Y H, LI Y, ZHU Y. ACT: auditable confidential transaction scheme[J]. Journal of Computer Research and Development, 2020, 57(10): 2232-2240. (in Chinese)

[15] 谢绒娜,李晖,史国振,等. 基于区块链的可溯源访问控制机制[J]. 通信学报,2020,41(12):82-93.
XIE R N, LI H, SHI G Z, et al. Blockchain-based access control mechanism for data traceability [J]. Journal on Communications, 2020, 41(12): 82-93. (in Chinese)

[16] 田有亮,杨科迪,王缵,等. 基于属性加密的区块链数据溯源算法[J]. 通信学报,2019,40(11):101-111.
TIAN Y L, YANG K D, WANG Z, et al. Algorithm of blockchain data provenance based on ABE[J]. Journal on Communications, 2019, 40(11): 101-111. (in Chinese)

[17] GONG B, CUI C, HU M S, et al. Anonymous traceability protocol based on group signature for blockchain[J]. Future Generation Computer Systems, 2022, 127: 160-167.

[18] BONEH D, BOYEN X, SHACHAM H. Short group signatures[M]. Berlin, Germany: Springer, 2004.

[19] BUNZ B, BOOTLE J, BONEH D, et al. Bulletproofs: short proofs for confidential transactions and more [C]// Proceedings of 2018 IEEE Symposium on Security and Privacy. Washington D. C., USA: IEEE Press, 2018: 315-334.

[20] WU Y, ZHANG W, XIONG H, et al. Efficient access control with traceability and user revocation in IoT[J]. Multimedia Tools and Applications, 2021, 80(20): 31487-31508.

[21] 田海博,林会智,罗裴然,等. 一种用户隐私保护数字货币的可监管方案[J]. 西安电子科技大学学报,2020,47(5):40-47.
TIAN H B, LIN H Z, LUO P R, et al. Scheme for being able to regulate a digital currency with user privacy protection[J]. Journal of Xidian University, 2020, 47(5): 40-47. (in Chinese)

[22] 赵晓琦,李勇. 可审计且可追踪的区块链匿名交易方案[J]. 应用科学学报,2021,39(1):29-41.
ZHAO X Q, LI Y. Auditable and traceable blockchain anonymous transaction scheme [J]. Journal of Applied Sciences, 2021, 39(1): 29-41. (in Chinese)

编辑 吴云芳