文献引用格式：徐鹤语，马兆丰，叶可可，等．基于群签名的联盟链跨链身份隐私保护技术[J]．信息安全与通信保密，2022(10):12-24.
XU Heyu,MA Zhaofeng,YE Keke,et al.Cross-Chain Identity Privacy Protection Technology for Consortium Blockchain Based on Group Signature[J].Information Security and Communications Privacy,2022(10):12-24.

基于群签名的联盟链跨链身份隐私保护技术*

徐鹤语[1]，马兆丰[1]，叶可可[2]，段鹏飞[1]，罗守山[1]
（1. 北京邮电大学 网络空间安全学院，北京 100876；2. 中移动信息技术有限公司 研发创新中心，北京 102200）

摘　要：为了解决联盟链在参与数据互通、信息交换、跨链交互中身份隐私泄露的问题，提出了一种满足跨链监管要求，基于联盟链跨链交易的可控匿名身份隐私保护模型。考虑到各联盟链身份异构，数字证书的实名特性，提出一种基于群签名的联盟链跨链交易背书策略。群签名基于SDH假设和双线性群中的决策性假设，满足群的安全性特征和正确性要求。能够实现对跨链信息的正确签名上链，达到匿名共享信息的目的。

关键词：跨链监管；身份隐私；可控匿名；群签名
中图分类号：TP309.2　　**文献标志码：**A　　**文章编号：**1009-8054(2022)10-0012-13

Cross-Chain Identity Privacy Protection Technology for Consortium Blockchain Based on Group Signature

XU Heyu[1], MA Zhaofeng[1], YE Keke[2], DUAN Pengfei[1], LUO Shoushan[1]
（1.School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China;
2.China Mobile Information Technology Co., Ltd., Beijing 102200, China）

Abstract: In order to solve the problem of identity privacy leakage in the data exchange, information exchange and cross-chain interaction of the consortium blockchain, a controllable anonymous identity privacy protection model based on cross-chain transaction is proposed to match the requirements of cross-chain supervision. Considering the identity heterogeneity of consortium blockchain and the real name features of digital certificates, a cross-chain transaction endorsement strategy based on group

* 收稿日期：2022-07-29；修回日期：2022-09-20　Received date: 2022-07-29; Revised date: 2022-09-20
基金项目：北京市自然科学基金项目（No.M21034）；国家重点研发计划项目（No.2020YFB1005500）
Foundation Item: Beijing Municipal Natural Science Foundation (No.M21034); National Key Research and Development Program (No.2020YFB1005500)

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

signatures is proposed. Group signature is based on the SDH assumption and the decision assumption in bilinear groups, which satisfies the security features and correctness requirements of groups. It can realize the correct signature on the cross-chain information and achieve the purpose of anonymous information sharing.

Key words: cross-chain supervision; identity privacy; controllable anonymous; group signature

0 引 言

随着区块链技术的不断发展，区块链能够提供的服务也越来越丰富。区块链具有去中心化、防篡改等特点，这使其成为一种信任体系构造技术，有利于破除传统互联网架构下的数据孤岛问题，也有利于优化金融供应生产关系。然而，随着区块链技术的不断成熟，以及与医疗、金融、数字版权等领域的融合，领域交叉应用对区块链跨链和跨链身份隐私保护的需求日益增长[1-7]。

白杰等人[8]指出，由于区块链之间缺少统一的通信，大多数公司间无法互相协同。同时，跨链合约的执行较为困难。现实世界的资产流动尤其是数字版权，需要多方参与，执行担保监督等工作，而局限于一个链的合约无法完全完成这些工作。许永鑫、郭子彦等人[9-10]指出，区块链在优化供应链金融中扮演了非常重要的角色。区块链可以很好地解决供应链金融中的凭证信任问题，但同时也存在信息共享困难的问题，不同链之间无法直接实现信息共享。

传统联盟链的身份管理系统大多基于公钥基础设施（Public Key Infrastructure，PKI）进行证书颁发和身份认证。但每条链独立存在，没有一个统一的身份管理系统，无法进行跨链的身份认证，形成了身份管理的信息孤岛[11]。身份缺失的同时也导致在进行跨链信息交换时无法确认信息是否可信。如何在跨链网络中为不同的链提供统一的身份标识以解决跨链交易中的认证问题，以及如何保护应用链在跨链交易网络中的身份信息，是区块链跨链应用进一步扩大需要解决的问题。因此，本文提出了一种基于群签名的可监管的身份隐私保护跨链交易模型，其与中继链跨链网络相结合，在不改变应用链架构与中继链架构的基础上实现对跨链交易信息的身份匿名化，为避免匿名的滥用，该模型支持管理员对匿名消息的去匿名化，实现了跨链交易的监管。

1 背景知识和相关介绍

1.1 区块链技术

区块链作为一种新型互联网技术，具有高度去中心化、高信赖的特征，是一种数据网络存储技术。其是分布式网络技术与加密技术相结合的技术产物。区块链的概念源于中本聪[12]在2008年发表的论文，其提出了一种加密数字货币——比特币，可以满足无监管的不可信双方的交易需求。之后开发者引入了智能合约的

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

概念，实现了区块链的可编程特性。区块链技术是一系列计算机和加密技术的结合，结合了密码学、对等网络通信、共识机制、智能合约编程等技术手段。从数据结构来看，区块链是一条按时间顺序将包含可信交易的数据区块连接起来的链，由密码学算法保证其不可篡改伪造，通过对等网络和共识机制来生成和更新数据。

随着应用的增加，区块链网络根据是否具有控制访问权限机制以及是否集中化拥有控制权主体，将区块链系统分为公有链（如以太坊）、联盟链（如 Hyperledger、趣链）和私有链 3 种类型 [13]。其中，公有链完全公开透明，无任何身份认证授权；联盟链需要身份授权准入机制，记录维护由事先预备的节点负责；私有链由单一的节点参与网络维护。

1.2 跨链技术架构

跨链（Cross-Chain）是容许加密货币资产跨越不同的区块链使用和保存。跨链技术的关键在于执行智能合约，设计共同的通信协议，完成共同的跨链接入接口，从而实现多个独立运行的区块链之间的信息及资产的原子性转移或互换。目前，跨链的架构方案如下：公证人机制、侧链 / 中继、哈希锁定和分布式私钥控制。其中，公证人架构中存在中心化的风险，哈希时间锁和分布式私钥控制方式存在应用的局限性，而侧链增加了网络的复杂度，也存在新的安全风险 [14]。相较之下，中继链架构下的操作应用场景广，且可拓展性强，能适用于大部分跨链要求。

1.3 群签名

群签名是数字签名的一种，其目的在于允许成员代表群签名消息，同时不泄露身份。换而言之，看到签名的人可以用公钥验证该消息是否是合法群成员签署的，但无法得知实名身份。同时，群成员无法滥用这种匿名机制，因为群签名支持群管理员使用秘密信息来打开签名，证实身份。

一个完善的群签名方案需要满足以下几个要求：

（1）群特性。只有群中成员能够代表群体签名。

（2）验证简洁。接收者可以用公钥完成签名验证。

（3）匿名保护。接收者不能得知签名者在群体中的实名身份。

（4）可追踪。群体中的成员或可信赖机构可以根据秘密信息打开签名。

知名的群签名方案包括由 Camenisch 等人 [15] 于 1997 年提出的 CS97 群签名方案。CS97 以离散对数作为理论基础。而本文采用的是 Boneh 等人 [16] 于 2004 年提出的 BBS 短群签名方案。BBS 短群签名基于强 DH 假设，即 SDH（Strong Diffie-Hellman，SDH）和线性决策假设。

1.4 研究现状

当前基于联盟链的身份信息管理研究主要集中在链内的去中心化身份认证和跨链的身份认证管理方面。在提供匿名化身份认证方面还有所欠缺。

1.4.1 身份管理研究现状

Cachin[17] 针对以 fabric 为代表的联盟链架构，提出了一种新的联盟链身份认证机制以改进联盟链的交易背书。主要创新在于对注册和

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

交易分开授权，实现了一定的匿名性，但同时大量的交易证书带来了存储和维护的瓶颈。Liang 等人[18]提出一种组签名与证书授权中心（Certificate Authority，CA）机构相结合的满足匿名的跨链身份认证协议。主 CA 提供身份认证证书，授权应用链加入中继链。在应用链系统中，所有节点具有唯一身份标识 ECERT。应用链中指定的组管理节点根据 ECERT 给要进行跨链的节点颁发组成员证书 GCERT。需要进行跨链事务的节点根据自己的 ECERT 向组管理节点申请 TCERT，并用 GCERT 进行签名保证身份信息。该跨链交易协议虽然可以保证交易过程中的身份匿名，但多个证书的交互与管理使得系统面临证书管理上的瓶颈。王洒洒等人[19]也针对异构应用链的跨链问题提出了一种跨链系统的身份标识认证模型。不过该模型解决的是同一个应用链需加入多个跨链系统中的重复认证问题，与本文关注的跨链中的身份隐私有所不同。

Axon 等人[20]针对区块链 PKI 架构不关注隐私的问题，设计了一种满足隐私感知的 PKI 架构，使得公钥与身份不关联。Conti 等人[21]针对信息中心网络（Information Centric Networking，ICN）中身份认证负担较大的问题，提出了一种轻量级的实现方式。利用区块链构造了一种高效轻量级分布移动生产者认证协议，用于 ICN 中的安全移动管理，解决了移动网络和 BC 中易受网络攻击的问题。Zhang 等人[22]主要利用区块链的安全特性，提出了一种完全分布式的用户认证框架，利用智能合约进行访问权限控制，智能合约保证了权限的授予。王姝爽等人[23]对应用链接入跨链时的安全过程和跨链中的身份标识做了相关研究，给出了一种轻量级的身份标识方案，但同样是基于证书与公私密钥对，没有关注跨链中的身份隐私问题。

1.4.2 跨链身份授权研究现状

Wang 等人[24]提出了一种去中心化身份（Decentralized Identifier，DID）与可信证书（Verifiable Credentials，VC）相结合的跨链可信资产转移流程。其中，链内用户身份通过唯一 DID 进行身份标识，完整的身份信息存储在中继链上，包含多个公钥，可以简化同一个用户参与多链的流程。但同时中继链需要维护所有应用链及其用户的身份元信息和完整信息。随着业务的增长，中继链的存储负担过重。Shao 等人[25]针对物联网身份认证和跨链通信，基于身份加密（Identity-Based Encryption，IBE）协议，设计了物联网区块链中的跨链通信机制。其通过在每个区块链上设置代理节点，代理节点需与链公证员通信获得私钥。区块链上的每个节点可通过代理节点进行跨链，代理节点之间可以直接跨链通信。该机制虽保证了跨链的身份认证，但是公证员机制的跨链方案存在第三方是否可信以及性能瓶颈的问题。Jiang 等人[26]利用联盟链与公证人相结合的方式，把若干物联网区块链集合到一个财团区块链控制站中，所有跨车联网子集的访问必须经由控制站成员审查。Wang 等人[27]利用区块链优化应用的跨域认证。所有认证通过根 CA 执行，设计了一个跨域证书认证协议。虽然实现了证书的分布式，但认证过程依旧依赖于 CA 的可靠性和性能。

综上，目前跨链的身份管理存在以下不足。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

首先，跨链的身份管理大多需要中继链进行统一身份的存储，如果涉及多链交互，还需要存储多个密钥对。其一定程度上统一了异构链的身份标识问题，但也存在中继链负荷过大的瓶颈。其次，大多数跨链身份认证策略未考虑在匿名跨链事务中如何完成身份信任。并且能够满足匿名需求的认证方案存在多个需要管理的证书，需要通过频繁交互来完成证书颁发和身份认证，其存储开销较大且流程不够简洁。

因此，本文提出一种基于群签名的中继链跨链身份信息保护方案。能够实现应用链间的信息共享，同时保护身份信息，允许管理员进行监管，以解决区块链间信息孤岛的问题。

2　跨链监管下的身份标识架构

2.1　跨链模型的分层架构

针对多应用链用户在跨链互操作间存在的信任传递、跨链访问、身份隐私保护等问题，提出了一种面向跨链系统中的身份认证方案，既能满足跨链中的身份信任要求，又能满足用户对身份隐私保护的要求，实现可控的匿名认证。首先介绍跨链系统的分层架构模型，跨链采用不需要可信第三方的中继模式进行。跨链模型分层架构中的角色符号与表示如表 1 所示。

表 1　分层架构角色表示

符号	表示
R	中继链
A,B	需要跨链的应用链
Pier	跨链网关
Broker	跨链管理合约
Transfer	跨链业务合约

由中继链 R 系统负责身份注册、身份认证、身份维护管理以及跨链交易的验证和转发等。在中继架构模型中，中继模块提供身份注册合约、身份认证合约，以及交易所需的认证合约。根据跨链传输协议（Inter Blockchain Transfer Protocol，IBTP）包解析出链类型和交易证明等信息，交易的验证，存证交易。确保交易的合法性，保障交易安全。

应用链 A,B 间的跨链交易通过与跨链网关交互，执行对应的跨链合约，完成跨链交易。应用链是需要通过跨链架构连接的区块链主体，通过完成中继链上的身份注册和认证，可以加入跨链网络中，拥有在跨链网络中的唯一身份标识，与跨链网络中其他应用链进行跨链交互。

跨链合约是部署在应用链上的智能合约，负责跨链事件的执行。为了方便管理，跨链合约分为 broker 和其他业务合约。业务合约在 broker 上注册后方可生效。

Pier跨链网关负责完成跨链中的监听、路由、代理转发等工作，同时把跨链事务转换成 IBTP 通信协议的格式，并提交到中继链上。Pier 中的分层与功能对应关系如表 2 所示。

表 2　Pier 分层架构

层次	功能
应用链插件	应用链交互
交互层	监听、验证、执行
中继层	路由、同步交易、网络转发

2.2　应用链数字身份注册与身份标识

为了保证跨链事务的安全性和隐私性，每一个进行交互的应用链需要拥有在跨链联

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

盟链中的唯一身份标识，身份标识可以通过执行身份注册合约获得。DID 身份标识架构如图 1 所示。

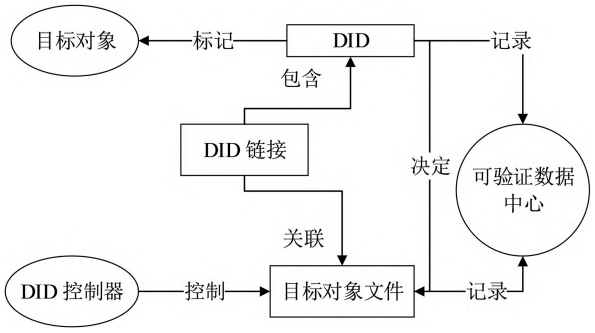

图 1　DID 身份标识架构

注册接口由应用链插件开发实现。数字身份满足 Web3 的 DID 标准。DID 作为一种新型的可验证、分布式的数字身份标识，相比于证书具有更强的身份隐私保护 [28-29]，可以由用户控制其身份属性的披露。据 Web3 标准指出，DID 标准由 DID 和 DID 文档组成。DID 是一个简单的文本字符串，包含方案标识符、DID 方法标识符和 DID 方法的特定标识符结构。DID 实例可以解释为一个 DID 文档，DID 文档包含与 DID 相关的信息，例如以加密的方式对 DID 控制器进行身份验证的方法。

跨链的身份标识通常采用 DID 身份标识，应用链的身份标识结构如下：id:{did identification: relay chain identifier:application chain name:}，例如 did:relaychain:chain_test: 为一个链的 DID 标识。用户 DID 的身份标识结构如下：id:{did ID:relaychain ID:userchain ID:ueserchain address:}，例如 {did:relaychain:chain_test:0x111111111:} 为一个用户的 DID 标识。应用链的身份注册流程如图 2 所示。

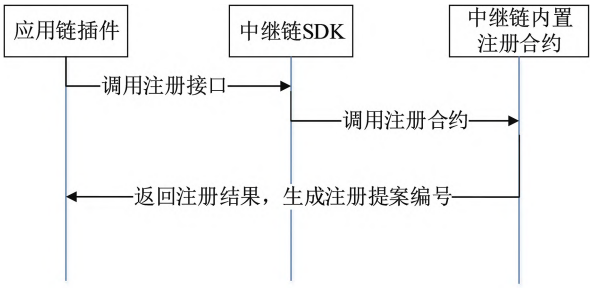

图 2　应用链的身份注册流程

应用链的公私钥对和交易地址等信息由注册合约执行结果返回。注册提案经中继链管理节点投票通过后生效。应用链及其应用节点获得唯一身份标识，可以参与跨链事务。

3　可监管的身份隐私保护跨链交易模型

3.1　跨链交易身份可控匿名认证方案

目前主流的联盟链在跨链事务的身份认证中依旧采用基于数字证书的实名认证方案，通过向交易方提供实名的数字证书来证实合法身份。这满足了交易的安全性，但是没法为需要匿名交易的用户提供服务。为了符合跨链身份隐私保护的要求，需要提供一种可控匿名身份隐私保护模型，能够做到验证证书与实名身份的剥离，同时允许管理员监管，保证匿名不被滥用。

在现有的中继链跨链架构上对该方案进行改进。由中继链管理节点作为群管理员，联盟链以唯一身份标识作为加入群的凭证，以群签名代替数字证书认证身份的合法性，最终实现匿名的身份认证。此方案包括群的创建、群成员加入、签名消息、验证消息和打开身份。方案各个部分的关系如图 3 所示。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

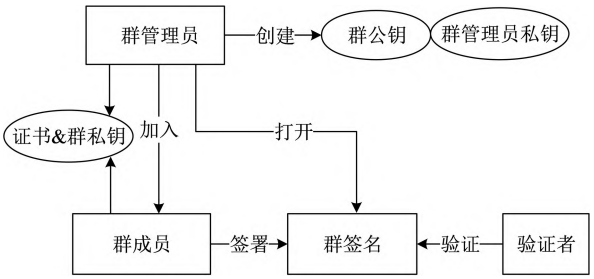

图 3　方案内容

由中继链管理员完成群的创建，生成群公钥、群管理员私钥和一系列的群成员私钥，并向所有群成员公开群公钥，保密群管理员私钥以及成员私钥。应用链凭借在中继链中的唯一身份标识，可以向中继链管理员请求一组群成员证书，并获得群成员私钥。应用链在进行匿名的跨链事务时可以用群签名代替数字证书签名。同在群中的其他跨链成员可根据群公钥完成对签名的验证，从而实现身份认证。

该方案的主要步骤如下文所述。

（1）群的创建。由中继链管理节点执行，首先考虑满足双线性映射的两个群 G_1 和 G_2，其各自的生成元为 g_1 和 g_2，且 SDH 假设成立于 (G_1,G_2)，决策线性假设成立于 G_1。

Step1　选择一个随机数 n 作为群成员数量。

Step2　选择 $h \underline{R} G_1 \setminus \{1_{G_1}\}$。

Step3　选择 $\xi_1,\xi_2 \underline{R} Z_p^*$，选择 $u,v \in G_1$，满足 $u^{\xi_1}=v^{\xi_2}=h$，选择 $\gamma \underline{R} Z_p^*, w=g_2^{\gamma}$，群中成员私钥形如 (A,x)，其中选择 $x \underline{R} Z_p^*, A \leftarrow g_1^{\frac{1}{\gamma+x}}$。

Step4　群公钥 $gpk=(g_1,g_2,h,u,v,w)$，群管理员私钥 $gmsk=(\xi_1,\xi_2)$，群成员私钥 $gsk=(A,x)$。

（2）签名。由应用链完成消息签名，作为对消息的背书，证明消息来源的可信。

Step1　给出 (gpk,gsk,M)，其中 M 为待签名消息。

Step2　选择两个随机数 $\alpha,\beta \underline{R} Z_p$，计算 $T_1=u^{\alpha}$，$T_2=v^{\beta}$，$T_3=Ah^{\alpha+\beta}$。

Step3　计算两个辅助值 $\varsigma_1=x\alpha$ 和 $\varsigma_2=x\beta$。

Step4　从 Z_p 中随机选择 5 个随机数 r_α，r_β，r_x，r_{ς_1}，r_{ς_2}。

Step5　计算 5 个中间值 R_1，R_2，R_3，R_4，R_5：

$$\begin{aligned} R_1&=u^{r_\alpha}\\ R_2&=v^{r_\beta}\\ R_3&=e(T_3,g_2)^{r_x}\cdot e(h,w)^{-r_\alpha-r_\beta}\cdot e(h,g_2)^{-r_{\varsigma_1}-r_{\varsigma_2}}\\ R_4&=T_1^{r_x}\cdot u^{-r_{\varsigma_1}}\\ R_5&=T_2^{r_x}\cdot v^{-r_{\varsigma_2}} \end{aligned} \quad (1)$$

生成挑战 c：$hash(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$。

Step6　计算响应 s_α，s_β，s_x，s_{ς_1}，s_{ς_2}：

$$\begin{aligned} s_\alpha&=r_\alpha+c\alpha\\ s_\beta&=r_\beta+c\beta\\ s_x&=r_x+cx\\ s_{\varsigma_1}&=r_{\varsigma_1}+c\varsigma_1\\ s_{\varsigma_2}&=r_{\varsigma_2}+c\varsigma_2 \end{aligned} \quad (2)$$

式中：c 为生成的 $hash$ 挑战；x 为签名成员私钥。其余为上述步骤选择的随机数和计算的辅助值。

给出签名 $\sigma \leftarrow (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\varsigma_1},s_{\varsigma_2})$。

（3）验证。所有参与到中继链群中的应用链都可充当验证者，验证该条消息是否来自合法的群成员。

Step1　根据收到的签名计算 $\widetilde{R_1}$，$\widetilde{R_2}$，$\widetilde{R_3}$，$\widetilde{R_4}$，$\widetilde{R_5}$。

Step2　其中

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

$$\begin{aligned}
\widetilde{R_1} &= u^{s_\alpha} / T_1^c \\
\widetilde{R_2} &= u^{s_\beta} / T_2^c \\
\widetilde{R_3} &= e(T_3, g_2)^{s_x} \cdot e(h,w)^{-s_\alpha - s_\beta} \cdot \\
&\quad e(h,g_2)^{-s_{\xi_1} - s_{\xi_2}} \cdot (e(T_3,w) / e(g_1,g_2))^c \\
\widetilde{R_4} &= T_1^{s_x} / u^{s_{\xi_1}} \\
\widetilde{R_5} &= T_2^{s_x} / v^{s_{\xi_2}}
\end{aligned} \tag{3}$$

式中：g_1，g_2，h，u，v，w 由公开的群公钥 $gpk=(g_1,g_2,h,u,v,w)$ 得出。其余计算参数由收到的签名 σ 给出。

Step3　计算 $hash=(M,T_1,T_2,T_3,\widetilde{R_1},\widetilde{R_2},\widetilde{R_3},\widetilde{R_4},\widetilde{R_5})$，并比较 c 与第三步得到的 $hash$ 是否相等，若相等，则验证成功。

（4）打开。中继链管理节点可使用其拥有的私钥打开对消息的签名，查看实名身份，监督匿名的使用。

Step1　首先判断 σ 是否为合法签名。

Step2　恢复用户的 A：$A \leftarrow T_3 / (T_1^{\xi_1} \cdot T_2^{\xi_2})$。

3.2　基于群签名的跨链交易背书策略

跨链交易的执行一般由跨链合约进行维护。由跨链协议规范跨链请求需要包含的字段，为保证认证的灵活性，跨链协议包含一段 proof 证明字段，该字段提供中继链验证所需的信息。中继链会根据事先部署的验证策略对交易合法性进行验证。传统的验证策略如 fabric 联盟链采用背书策略，签名基于实名数字证书。当验证方进行验证时必须知道签名者的数字证书和公钥，否则无法满足匿名认证要求。

本节结合 3.1 节提出的可控匿名认证方案，对联盟链交易的背书策略进行改进，实现中继链对跨链交易的认证。首先，应用链凭借注册获得的唯一身份标识申请加入群，中继链核验应用链身份后为其分配群成员私钥，应用链中所有可以充当背书节点的用户都知晓群成员私钥信息。其次，在收到交易提案后，用群私钥对交易执行结果进行签名，完成背书。背书策略的模型与跨链交易流程如图 4 所示。

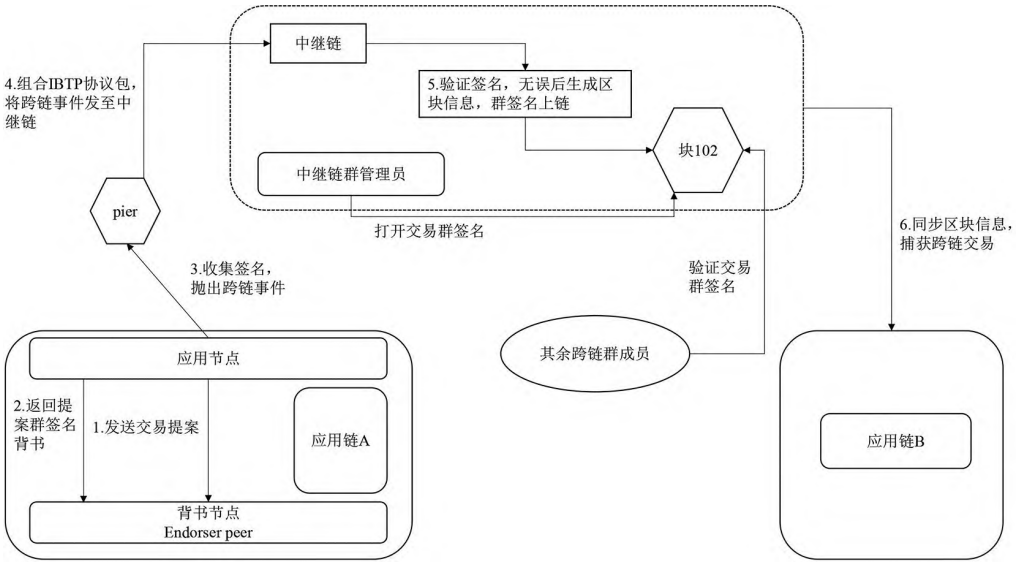

图 4　可控匿名跨链交易背书模型

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

（1）应用链加入群。已在中继链中注册过的应用链需要从中继链群管理员生成的成员私钥组中选择一组私钥，作为签名密钥。

Step1　应用链 A 请求加入群。

Step2　中继链验证是否是已注册的应用链。

Step3　通过验证，中继链从 $(0,n-1)$ 中随机选择一个数 i 。

Step4　私钥组 $gsk(i)$ 为此应用链的群成员私钥。

Step5　以 A 的公钥加密 $gsk(i)$ 结果。

（2）基于群签名的背书。获得签名私钥的应用链成员，可以对交易进行群签名并完成背书。此背书具有匿名性，保护用户身份隐私。

Step1　应用节点进行交易提案，触发执行交易对应的链码，提交给背书节点。

Step2　检查签名提案的消息格式和签名是否正确，包括通道头、签名头等。

Step3　检查交易的 ID 是否唯一，检查是否有权限，查找需要满足的验证策略。

Step4　模拟执行提交的交易链码，记录结果。

Step5　对提案响应执行群签名，构造响应消息返回背书结果。

Step6　应用节点收集到足够的背书后，经由跨链网关打包消息发至中继链。

Step7　中继链执行验证策略，验证背书签名，无误后交易信息上链。

在该背书策略下，所有加入中继链的节点都可以看到交易信息，以及对交易信息的可信背书，无法得知信息提供者的身份。既实现了信息的共享，也实现了对身份的保护。

4　安全性分析

本节主要分析上述跨链交易可控匿名身份隐私保护模型在身份隐私保护方面的有效性。

由模型结构可知，身份隐私的保护依赖于群签名方案。在进行跨链信息交换时，上链对交换信息的群签名而非信息本身，既能证明链上信息的真实合法，又能不泄露信息提供者的身份。即只要群签名方案是安全的，此可控匿名身份隐私保护模型就是有效的。由第 3 节可知，群签名方案的主要环节为对私钥和成员证书的知识签名。下面证明知识签名的安全性。

4.1　签名验证和打开的正确性

签名验证的正确性要求一个不合法的签名不可能使等式成立。对于诚实的签名而言，验证者进行的等式运算必然成立。若证明由验证步骤计算的 $\widetilde{R_1}$，$\widetilde{R_2}$，$\widetilde{R_3}$，$\widetilde{R_4}$，$\widetilde{R_5}$ 与签名者结算的中间变量 R_1，R_2，R_3，R_4，R_5 是相等的，则验证者计算的 $hash=(M,T_1,T_2,T_3,\widetilde{R_1},\widetilde{R_2},\widetilde{R_3},\widetilde{R_4},\widetilde{R_5})$ 就和签名者计算的挑战 $c=hash(M,T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)$ 是相等的，即验证等式是正确的。

证明验证算法中 5 个验证等式的成立。

证明：

Step1　$u^{s_a}/T_1^c=u^{r_a+ca}/u^{ac}=u^{r_a}=R_1$　（4）

式中：计算所需参数由签名 $\sigma\leftarrow(T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\varsigma_1},s_{\varsigma_2})$ 与公开的群公钥 $gpk=(g_1,g_2,h,u,v,w)$ 给出。

Step2　同理可得 $R_2=u^{s_\beta}/T_2^c$ 成立。

Step3

$$\begin{aligned}T_1^{s_x}/u^{s_{\varsigma_1}}&=T_1^{r_x+cx}/u^{r_{\varsigma_1}+c\varsigma_1}=u^{(r_x+cx)\alpha}/u^{r_{\varsigma_1}+c\alpha x}\\&=u^{r_x\alpha}/u^{r_{\varsigma_1}}=T_1^{r_x}/u^{r_{\varsigma_1}}=R_4\end{aligned}\quad(5)$$

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

式中：计算所需参数由签名$\sigma \leftarrow (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\varsigma_1},s_{\varsigma_2})$与公开的群公钥$gpk=(g_1,g_2,h,u,v,w)$给出。

Step4　同理可得$R_5=T_2^{s_x}/v^{s_{\varsigma_2}}$成立。

Step5

$$\begin{aligned}&e(T_3,g_2)^{s_x}\cdot e(h,w)^{-s_\alpha-s_\beta}\cdot e(h,g_2)^{-s_{\varsigma_1}-s_{\varsigma_2}}=\\&e(T_3,g_2)^{r_x+cx}\cdot e(h,w)^{-r_\alpha-r_\beta-c\alpha-c\beta}\cdot\\&e(h,g_2)^{-r_{\varsigma_1}-r_{\varsigma_2}-cx\alpha-cx\beta}=e(T_3,g_2)^{r_x}\cdot\\&e(T_3,g_2{}^x)^c\cdot e(h,w)^{-r_\alpha-r_\beta}\cdot e(h^{-\alpha-\beta},w)^c\cdot\\&e(h,g_2)^{-r_{\varsigma_1}-r_{\varsigma_2}}\cdot e(h^{-\alpha-\beta},g_2{}^x)^c=e(T_3,g_2)^{r_x}\cdot\\&e(h,w)^{-r_\alpha-r_\beta}\cdot e(h,g_2)^{-r_{\varsigma_1}-r_{\varsigma_2}}\cdot e(T_3,g_2{}^x)^c\cdot\\&e(h^{-\alpha-\beta},wg_2{}^x)^c=R_3\cdot e(T_3h^{-\alpha-\beta},wg_2{}^x)^c\cdot\\&e(T_3,w)^{-c}=R_3(e(g_1,g_2)/e(T_3,w))^c\end{aligned}\tag{6}$$

式中：计算所需参数由签名$\sigma \leftarrow (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\varsigma_1},s_{\varsigma_2})$与公开的群公钥$gpk=(g_1,g_2,h,u,v,w)$给出。

Step6　由 Step5 可知：

$$\begin{aligned}&e(T_3,g_2)^{s_x}\cdot e(h,w)^{-s_\alpha-s_\beta}\cdot e(h,g_2)^{-s_{\varsigma_1}-s_{\varsigma_2}}\cdot\\&(e(T_3,w)/e(g_1,g_2))^c=R_3\cdot(e(g_1,g_2)/\\&e(T_3,w))^c\cdot(e(T_3,w)/e(g_1,g_2))^c=R_3\end{aligned}\tag{7}$$

式中：计算所需参数由签名$\sigma \leftarrow (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\varsigma_1},s_{\varsigma_2})$与公开的群公钥$gpk=(g_1,g_2,h,u,v,w)$给出。

综上，只要签名者是诚实的签名者，其将严格按照签名生成算法进行运算，验证者的验证等式成立。

正确的群签名需要保证打开的正确性，即合法的签名一定能通过管理员私钥恢复得到群成员的私钥组，从而获得群成员身份查询响应。

证明：诚实签名者给出签名$\sigma \leftarrow (T_1,T_2,T_3,c,s_\alpha,s_\beta,s_x,s_{\varsigma_1},s_{\varsigma_2})$的前 3 个分量值$T_1$，$T_2$，$T_3$，是成员私钥$gsk=(A,x)$中的$A$在群公钥$gpk=(g_1,g_2,h,u,v,w)$中$(u,v,h)$下的线性加密。根据群初始化算法，存在$u^{\xi_1}=v^{\xi_2}=h$成立，所以群管理员一定可以通过私钥，经由$A\leftarrow T_3/(T_1^{\xi_1}\cdot T_2^{\xi_2})$恢复身份。

4.2　签名的完全匿名性

在不知道群管理员私钥的情况下，要恢复出用户成员私钥组是不可能的。

概念 1：SDH 假设

如果在群(G_1,G_2)上没有一个t时间的算法，在求解$q\text{-}SDH$问题时有ε优势，则认为$(q,t,\varepsilon)-SDH$假设成立，Shoup[30]证明了此假设在一般群组中成立。

概念 2：决策线性假设

如果在G_1上没有一个t时间的算法，在解决G_1的决策线性问题时有ε优势，则认为在G_1上，(t,ε)决策线性假设成立。BBS[16]证明了决策线性假设在一般双线性群中成立。

证明：由签名算法得知，生成签名的两个群应满足 SDH 假设和决策线性假设，找不出在固定时间内有优势的破解算法。根据 BBS[16]证明可知，如果线性加密在群G_1上是(t',ε')语义安全的，那么 SDH 群签名(t,q_H,ε)是符合 CPA 完全匿名的。其中$\varepsilon'=\varepsilon$，且$t=t'-q_Ho(1)$，q_H为对手进行哈希函数查询的数量。

4.3　模型安全性分析

本节主要从群成员私钥安全管理和安全分发两个维度对模型进行安全性分析。证明此模型具有不可伪造性和可监督性。

首先，群成员私钥的管理和产生是安全的。由 3.1 节介绍的方案可知，群成员私钥由管理员

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

在计算群公钥时一并计算给出，形成群成员私钥池。群管理员由跨链分层架构中的中继联盟链管理员担任。管理员不参与一般跨链事务，属于中继链治理模块中的节点。一般的应用链节点无法从管理员处获得不属于自己的信息，即无法伪造群签名。

其次，群私钥的分发也是安全的。群私钥由应用链节点向中继链发起加入群的提案，通过身份审查后由中继管理员分发私钥。由 3.2 节介绍的策略可知，中继链在传输群私钥时使用应用链身份标识对应的公钥进行加密传输，保证了群私钥分发的安全性。

最后，该模型的可监督性由群签名打开算法的正确性进行保证，由 4.1 节可知，拥有秘密信息的管理员可以打开诚实的签名。

5 实验结论

本文实验均在虚拟机环境中执行，采用的虚拟机是 VMware Workstation Pro 15。虚拟机的环境配置为 Ubuntu20.04 操作系统。采用 Hyperledger Fabric1.4 作为应用联盟链的底层框架，跨链使用 bitxhub v1.6.2 系统提供的跨链网关和中继链进行，并安装 go1.16.2、Docker20.10.12 等配套环境。签名算法开发采用 go 语言并配合 PBC 密码库进行实现。实验的性能测试包括：背书签名在不同消息大小下，签名和验证的时间效率以及采用了本文的背书策略后链上验证的耗时。

由表 3 可以看出，群签名算法的时间开销随文件大小的增长变化稳定。虽然签名需要产生的辅助变量和计算的等式较多，但大部分可以在收到消息前做预计算，从而节省时间效率。

表 3 签名时间开销

文件大小 /Byte	签名时间 /ms
512	24.63
1 024	24.77
2 048	26.31
3 072	26.68
4 096	26.35
5 120	30.02

由表 4 可以看出，验证签名时的时间开销随文件大小的增长变化稳定。由验证算法可知，验证中进行的计算比较都已由收到的签名给出，不需要从基本参数开始计算，为验证提高了时间效率。

表 4 验证时间开销

文件大小 /Byte	验证时间 /ms
512	23.11
1 024	22.56
2 048	24.72
3 072	24.36
4 096	24.39
5 120	26.88

在测试链上验证性能时，统一选择 1 024 Byte 的消息进行签名，测试跨链节点个数对背书验证时间的影响。

由表 5 可以看出，链上验证的性能主要受发起验证的应用链与存储签名的中继块链之间的传递事务所影响，当网络环境良好时，传输通畅，链上开销可能更小。因此，在单机环境下模拟测试的测试结果同时还受CPU性能影响。综上，链上验证的吞吐量与网络环境、服务器性能都有较大关系。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

表 5　链上验证开销

节点个数	链上验证时间 /ms
2	42.51
4	91.89
8	179.54
16	361.12
32	718.36

6　结　语

综上，群签名在保护消息的匿名性和不可追踪性方面能够满足对身份隐私敏感的应用链的隐私要求。群签名上链的跨链模型对以信息共享和需要信息认证的跨链服务适应良好。同时利用中继链联盟链的治理模式，由治理节点充当群管理员，保证了群管理员私钥安全性的同时，满足了中继链上应用链的验证需求。

参考文献：

[1] MA Z F,WANG X C,JAIN D K,et al.A Blockchain-Based Trusted Data Management Scheme in Edge Computing[J]. IEEE Transactions on Industrial Informatics, 2020,16(3):2013-2021.

[2] MA Z F,WANG L Y,WANG X C,et al.Blockchain-Enabled Decentralized Trust Management and Secure Usage Control of IoT Big Data[J].IEEE Internet of Things Journal,2020,7(5):4000-4015.

[3] MA Z F,MENG J L,WANG J H,et al.Blockchain-Based Decentralized Authentication Modeling Scheme in Edge and IoT Environment[J].IEEE Internet of Things Journal,2021,8(4):2116-2123.

[4] MA Z F,WANG L Y,ZHAO W Z.Blockchain-Driven Trusted Data Sharing with Privacy Protection in IoT Sensor Network[J].IEEE Sensors Journal,2021, 21(22):25472-25479.

[5] MA Z F.Blockchain for Digital Rights Management[J]. Future Generation Computer Systems,2018,89:746-764.

[6] MA Z F.TrustedBaaS：Blockchain-Enabled Distributed and Higher-Level Trusted Platform[J].Computer Networks,2020,183:107600.

[7] 马兆丰 , 高宏民 , 彭雪银 , 等 . 区块链技术开发指南 [M]. 北京：清华大学出版社 ,2021:256-257.

[8] 白杰 , 杨鹏飞 , 孙鲜艳 , 等 . 基于 CNWW3 区块链体系标准建立的数字版权应用 [J]. 信息技术与网络安全 ,2020,39(7):18-30.

[9] 许永鑫 , 张宇宁 . 区块链技术在供应链金融风险控制中的应用研究 [J]. 商场现代化 ,2021(11):1-3.

[10] 郭子彦 . 海通证券运用区块链技术构建数据安全共享体系 [J]. 上海国资 ,2022(5):73-76.

[11] 杨淳 , 李经纬 , 李洪伟 , 等 . 异构身份联盟统一身份标识模型研究 [J]. 信息安全与通信保密 ,2019 (6):27-35.

[12] NAKAMOTO S.Bitcoin: A Peer-to-Peer Electronic Cash System[J/OL].[2022-06-30].http://courses.csail.mit.edu/6.857/2015/files/L07-nakamoto-bitcoin-a-peer-to-peer-electronic-cash-system.pdf.

[13] CASINO F,DASAKLIS T K,PATSAKISA C,et al.A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues[J].Telematics and Informatics,2019,36:55-81.

[14] GUDGEON L,MORENO-SANCHEZ P,ROOS S,et al.SoK: Layer-Two Blockchain Protocols[M]//Financial Cryptography and Data Security.Cham: Springer International Publishing,2020:201-226.

[15] CAMENISCH J,STADLER M.Efficient Group Signature Schemes for Large Groups[M]//Advances in Cryptology CRYPTO '97.Berlin,Heidelberg: Springer Berlin Heidelberg,1997:410-424.

[16] BONEH D,BOYEN X,SHACHAM H.Short Group Signatures[M]//Advances in Cryptology - CRYPTO 2004.Berlin,Heidelberg: Springer Berlin

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

Heidelberg,2004:41-55.

[17] CACHIN C.Architecture of the Hyperledger Blockchain Fabric[C]//Workshop on Distributed Cryptocurrencies and Consensus Ledgers,2016,310:4.

[18] LIANG X B,ZHAO Y,WU J H,et al.A Privacy Protection Scheme for Cross-Chain Transactions Based on Group Signature and Relay Chain[J].International Journal of Digital Crime and Forensics,2022,14(2):1-20.

[19] 王洒洒,戴炳荣,朱孟禄,等.面向跨链系统的用户身份标识认证模型[J].计算机工程与应用,2022,58(19):135-141.

[20] AXON L,GOLDSMITH M.PB-PKI: A Privacy-Aware Blockchain-Based PKI[C]//Proceedings of the 14th International Joint Conference on e-Business and Telecommunications,2017:311-318.

[21] CONTI M.BlockAuth: Blockchain Based Distributed Producer Authentication in ICN[J].Computer Networks,2019,164:106888.

[22] ZHANG L,LI H,SUN L M,et al.Poster: Towards Fully Distributed User Authentication with Blockchain[C]//2017 IEEE Symposium on Privacy-Aware Computing,2017:202-203.

[23] 王姝爽,马兆丰,刘嘉微,等.区块链跨链安全接入与身份认证方案研究与实现[J].信息网络安全,2022,22(6):61-72.

[24] WANG X Y,QIU W W,ZENG L,et al.A Credible Transfer Method of Cross-Chain Assets Based on DID and VC[C]//2021 IEEE 4th International Conference on Information Systems and Computer Aided Education,2021:238-242.

[25] SHAO S S,CHEN F,XIAO X Y,et al.IBE-BCIOT: An IBE Based Cross-Chain Communication Mechanism of Blockchain in IoT[J].World Wide Web,2021,24(5):1665-1690.

[26] JIANG Y,WANG C,WANG Y,et al.A Cross-Chain Solution to Integrating Multiple Blockchains for IoT Data Management[J].Sensors,2019,19(9):E2042.

[27] WANG W T,HU N,LIU X.BlockCAM: A Blockchain-Based Cross-Domain Authentication Model[C]//2018 IEEE Third International Conference on Data Science in Cyberspace,2018:896-901.

[28] SPORNY M,LONGLEY D,SABADELLO M,et al. Decentralized Identifiers (DIDs) v1.0.[EB/OL].(2022-07-19)[2022-09-21].https://www.w3.org/TR/did-core/.

[29] SPORNY M,LONGLEY D,CHADWICK D.Verifiable Credentials Data Model v1.1[EB/OL].(2022-03-03)[2022-09-21].https://www.w3.org/TR/vc-data-model/.

[30] SHOUP V.Lower Bounds for Discrete Logarithms and Related Problems[M]//Advances in Cryptology EUROCRYPT '97.Berlin,Heidelberg: Springer Berlin Heidelberg,1997:256-266.

作者简介：

徐鹤语（2000—），女，硕士研究生，主要研究方向为区块链、身份隐私保护等；

马兆丰（1974—），通讯作者，男，博士，教授，主要研究方向为区块链理论与技术研究、区块链隐私保护；

叶可可（1986—），男，硕士，区块链AU总监，主要研究方向为区块链与相关融合技术研究及应用；

段鹏飞（1995—），男，博士研究生，主要研究方向为区块链及安全技术；

罗守山（1962—），男，博士，教授，主要研究方向为区块链、密码学、网络与信息安全。

(C)1994-2023 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net