

基于可追踪环签名的联盟链身份隐私保护方法

任正伟^{1,2}, 余易晋¹

(1. 武汉科技大学 计算机科学与技术学院, 湖北 武汉 430065;

2. 智能信息处理与实时工业系统湖北省重点实验室(武汉科技大学), 湖北 武汉 430065)

摘要:作为目前被广泛使用的一种区块链,联盟链相较于公有链虽然具有更好的隐私性,但也仍然面临着因去匿名化方法而导致用户身份隐私泄露的问题。为了保护联盟链中用户的身份隐私,并且增加系统的容错性,提出了将可追踪环签名和实用拜占庭容错结合的联盟链身份隐私保护方法。该方法的核心思想是通过可追踪环签名来使联盟链中用户的身份具有条件匿名性,条件匿名性指的是用户在一定条件下是匿名的,即用户在正常交易时是匿名的,而当用户之间产生交易纠纷时,也可以对交易相关用户的身份进行去匿名化。此外,将可追踪环签名与实用拜占庭容错相结合,去匿名化的任务由联盟链中的节点通过实用拜占庭容错完成,减少了联盟链中心机构的权利和责任,即使用户对中心机构具有匿名性,也保证系统在中心机构出错时能够正常运行。通过实验分析和对比,该方案能够在合理的计算开销内保护用户身份隐私,并且保证较高的安全性和容错性。

关键词:区块链;联盟链;身份隐私;可追踪环签名;实用拜占庭容错

中图分类号:TP309

文献标识码:A

文章编号:1673-629X(2024)03-0102-08

doi:10.3969/j.issn.1673-629X.2024.03.016

A Method of Identity Privacy Protection in Consortium Blockchain Based on Traceable Ring Signature

REN Zheng-wei^{1,2}, YU Yi-jin¹

(1. School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430065, China;

2. Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System

(Wuhan University of Science and Technology), Wuhan 430065, China)

Abstract: As a branch of blockchain that is widely used at present, consortium blockchain has stronger privacy than the public chain in blockchain, but there are still some de-anonymization methods that can reveal the identity privacy of users in consortium blockchain. In order to protect the identity privacy of users in consortium blockchain and increase the robustness of system, we propose a consortium blockchain identity privacy protection method combining traceable ring signature and practical byzantine fault tolerance. Its core idea is to make the identity of users in the consortium blockchain conditional anonymity through traceable ring signature, and conditional anonymity refers to that the user is anonymous under certain conditions, that is, the user is anonymous during normal transactions. When a transaction dispute occurs between users, the identity of the transaction related users can also be de-anonymization. In addition, combining traceable ring signature with practical byzantine fault tolerance, the task of de-anonymization is completed by the nodes in the consortium blockchain through practical byzantine fault tolerant, which reduces the power and responsibility of the central authority of the consortium blockchain, not only makes the user anonymous to the central authority, but also ensures that the system can operate normally when the central authority fails. Through experimental analysis and comparison, the proposed scheme can protect user identity privacy and ensure high security and fault tolerance within a reasonable computational cost.

Key words: blockchain; consortium blockchain; identity privacy; traceable ring signature; practical byzantine fault tolerance

0 引言

区块链具有去中心化、不可篡改和不可伪造等特

点,能够应用于很多领域^[1]。目前,根据中心化程度的不同,区块链主要可分为三类,即公有链、联盟链和私

收稿日期:2023-05-10

修回日期:2023-09-12

基金项目:国家自然科学基金(61902285);武汉引力与固体潮国家野外科学观测研究站开放研究基金资助课题(WHYWZ202109)

作者简介:任正伟(1986-),男,博士,副教授,通信作者,CCF会员(13082M),研究方向为区块链安全与隐私、数据安全;余易晋(1999-),男,硕士研究生,研究方向为区块链隐私保护。

有链。其中,公有链也被称为非许可链,用户无需授权就可以参与其中。联盟链和私有链也被称为许可链,用户需要通过验证并获得授权后才能加入到系统中^[2]。相较于公有链,联盟链具有处理事务快和隐私性强等优点;相较于私有链,联盟链具有可扩展性强和适用范围广等优点。因此,联盟链在商品溯源、供应链管理 and 公共慈善等场景下都有广泛的应用^[3]。

然而,在实际应用中,区块链用户的身份隐私保护是一个亟待解决的问题,虽然大部分区块链都具有一定的匿名性,但是攻击者仍能通过动态监听和静态分析等方式获得用户的身份隐私^[4]。即使在隐私性较强的联盟链中,内部的节点也可以使用地址聚类^[5]等去匿名化方法获得用户的身份隐私。此外,在联盟链中,由于用户的身份验证和授权是由中心机构负责的,中心机构完全掌握着用户的身份信息,一旦中心机构受到攻击,用户的身份隐私就会被泄漏。

对上述问题,研究人员提出了一些方法以进一步保护用户的身份隐私。这些方法主要分为三类:混合服务、环签名和非交互式零知识证明^[4]。混合服务可以防止攻击者通过分析将交易发送者或交易接收者相关联,从而获得用户的身份,但是需要有足够多的用户参与其中。而环签名无需其它用户参与,签名者就可以生成隐藏其身份的签名,但环签名为用户提供完全匿名性的身份保护,这种完全匿名性会使得用户的身份难以被追查。非交互式零知识证明可以在用户不泄露额外信息的情况下证明自己的身份是有效的,其实现的也是用户身份的完全匿名。

此外,研究者也提出了具有条件匿名性的群签名方案。但是,在联盟链中,群签名的去匿名化依赖于中心机构,会使得用户对于中心机构不具有匿名性并且联盟链的运作依赖于中心机构,因此,群签名也不能很好地保护联盟链中用户的身份隐私。

为此,该文提出了一种基于可追踪环签名的身份隐私保护方法,以保护联盟链中用户的身份隐私。该方法结合了可追踪环签名和实用拜占庭容错协议,利用可追踪环签名实现用户身份的条件匿名性,既能保证包括中心机构在内的其他参与方不能获得用户的身份,又能在出现纠纷时揭露不诚实方的身份。而且,在文中方法中,去匿名化是由联盟链中的节点通过实用拜占庭容错协议来实现的,一方面使得中心机构在此过程中也无法获得用户身份,另一方面也增加了系统的容错性。总的来说,该文基于上述问题能够实现以下改进:

(1)利用可追踪环签名实现用户身份的条件匿名性,并将中心机构去匿名化的权利交给联盟链中的节点,使其无法将匿名交易和用户的真实身份关联起来。

(2)增加了检测机制,保证了只有交易相关节点才能提出去匿名化请求,并且恶意的去匿名化请求会被检测,提高了方案的安全性。

(3)匿名交易的去匿名化交由联盟链中节点使用实用拜占庭容错来完成,既让中心机构减少了资源消耗,也保证了它无法发挥功能时系统能够继续运行,增加了系统的容错性。

1 相关工作

由于区块链给用户身份隐私提供的保护是有限度的,已有研究工作提出了区块链中用户的身份隐私保护方法。例如,在近几年被纳入到区块链体系中用来保护用户的身份隐私的混合服务,主要分为两类:集中式和分布式。在集中式混合服务方案中,混合服务是由混合服务提供商充当的混合器完成,Mixcoin^[6]解决了混合服务提供商可能由攻击者假扮来窃取用户资产的问题,但是存在混合服务提供商会泄露用户身份的问题。为此,Blindcoin^[7]使用盲签名来防止混合服务提供商获得混合服务中输入地址和输出地址的关联。尽管如此,集中式混合服务仍然存在需要等待足够的用户参与混合服务而导致交易延迟增加、混合服务提供商易受攻击以及需要提交手续费等问题;在分布式混合服务中,交易的参与者之间自行协商混合服务的细节,Coinjoin^[8]避免了集中式混合服务中混合服务提供商易受攻击和需要支付手续费的问题,然而参与者知道混合服务中地址配对的详细信息,并且其能够通过提供虚假交易信息来妨碍混合服务的正常进行^[3]。Coinshuffle^[9]和 XIM^[10]以匿名通信的方式解决了地址配对泄露的问题,但是参与者仍可以妨碍混合服务的正常进行。最重要的是这些混合服务都需要等待定量的参与者才能进行。

而可以自主生成的环签名^[11]和非交互式零知识证明^[12]能够解决上述问题。文献[13]使用环签名来保护用户的身份隐私,然而环签名由于其不可链接性和完全匿名性容易产生一票多投和双重花费等安全问题。使用非交互式零知识证明的区块链 Zerocoin^[14],主要思想是用户首先铸造一枚硬币,然后用一枚没有历史使用记录的硬币来代替,并使用非交互式零知识证明保证硬币的有效性,但是 Zerocoin 局限于通过防止攻击者分析用户的资金流向来获取用户的身份。此外,由于环签名和非交互式零知识证明为用户提供完全匿名性,不适合需要监管的联盟链。根据联盟链所需的匿名程度来看,具有条件匿名性的群签名比较适合。文献[15]使用群签名保护联盟链中用户的身份隐私,但是该方案中群签名的验证以及用户的追踪依赖于中心机构(群管理员),并且中心机构能够自主对

用户的群签名去匿名化,系统的容错性和安全性较低。

与群签名类似的还有可追踪环签名,其分为主动追踪和被动追踪。主动可追踪环签名以文献[16]提出的自可追溯性为起点,用户可以提供相关数据证明自己是真正的签名者,也可以由可信第三方^[17]或者接收者^[18]收集环成员的相关数据来对可追踪环签名去匿名化。在区块链身份隐私保护方案^[19]中,去匿名化的请求由用户提出,中心机构(审计节点)进行去匿名化,这可能导致用户恶意提出去匿名化请求来暴露目标用户的真实身份,而且如果中心机构受到攻击或者产生错误,系统无法正常运行。在区块链身份隐私保护方案^[20]中,去匿名化的请求由第三方提出,中心机构(审计节点)进行去匿名化,虽然能够防止用户恶意提出去匿名化请求,但是系统的运行也依赖中心机构。此外,在文献[19-20]方案中,中心机构也能够自主对可追踪环签名去匿名化。被动可追踪环签名^[21]在一

定的条件下用户的签名会被链接或者被追踪,支持多种电子货币的应用层协议 Cryptonote^[22]就使用了修改后的可追踪环签名来保护用户的身份隐私。与之类似的还有使用多层可链接自发组签名^[23]的门罗币^[24],然而,针对这类被动可追踪环签名,恶意用户可以针对同一事件发表多个具有相同意见的签名来发起拒绝服务攻击,使其它节点忙于验证签名,而恶意用户的身份不会因此暴露^[25]。

2 方案设计

2.1 系统架构

文中方案包括三个参与方,分别是用户、中心机构和联盟链节点,其架构以及主要流程如图1所示。用户在联盟链中的活动以节点的身份进行,在联盟链之外的活动以用户的身份进行。

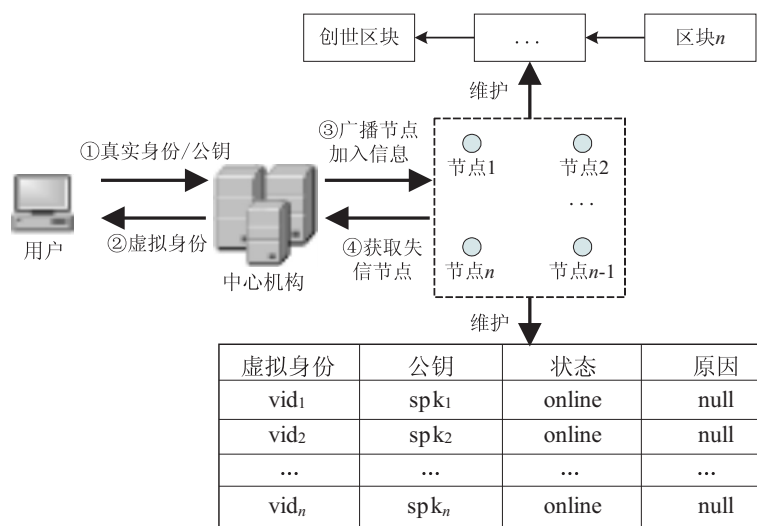


图1 系统架构

(1) 用户。

用户依据联盟链的规则生成自己的公私钥对,然后通过安全信道将自己的真实身份和公钥提交给中心机构。当用户通过中心机构的认证后,中心机构将给予用户联盟链中的虚拟身份,用户则作为节点加入到联盟链中。

(2) 中心机构。

中心机构负责验证用户的真实身份,为合法用户生成联盟链中的虚拟身份,并将用户的虚拟身份与公钥对应后广播至联盟链中。此外,中心机构还需要定期从联盟链中获取节点信息表,并处理其中因失信行为而被注销的用户。

(3) 节点。

节点负责维护联盟链以及维护记录了所有节点状态的节点信息表。此外,节点之间通过可追踪环签名进行匿名交易,并在出现纠纷时对交易进行去匿名化。

2.2 安全假设

(1) 文中方案安全性模型的成立依赖于离散对数问题(Discrete Logarithm, DL)和 Computational Diffie-Hellman(CDH)问题。

(2) 中心机构是不可信的。中心机构可能会被攻击者利用来破坏用户的身份隐私。

(3) 用户与中心机构之间,节点与节点之间存在由相互之间的公私钥加解密建立的安全信道。

2.3 方案构造

文中方案包括四个阶段:用户注册、匿名交易、纠纷解决和用户注销。

在注册阶段,用户向中心机构提供真实身份和公钥,并在通过验证后加入到联盟链中成为节点。在交易阶段,节点通过可追踪环签名和实用拜占庭容错协议进行匿名交易。在纠纷解决阶段,节点通过实用拜占庭容错协议进行去匿名化操作,以揭露和记录失信

节点。在注销阶段,节点广播注销消息以退出联盟链。

2.3.1 注册

设 G_1 是由生成元 P 生成的阶为素数 q 的加法群, G_2 是由生成元 P 生成的阶为素数 q 的乘法群, G_1 和 G_2 之间存在着双线性映射 $e: G_1 \times G_1 \rightarrow G_2$, Z_q^* 表示模 q 整数环, $s \in Z_q^*$ 为系统秘密参数且 $P_0 = sP$, 系统秘密参数 s 由可信第三方保管。 $H: \{0,1\}^* \rightarrow Z_q^*$ 为安全哈希函数。中心机构选取一个随机数 $r_{CA} \in Z_q^*$, 并计算用于签名的公私钥对 $(pk_{CA} = r_{CA}P, sk_{CA} = r_{CA}P_0)$ 。系统公共参数为 $\{G_1, G_2, q, e, Z_q^*, P, P_0, H, pk_{CA}\}$ 。

用户注册的过程如图2所示。当用户 i 要加入联

盟链时,先选取一个随机数 $r_i \in Z_q^*$, 并计算用于签名的公私钥对 $(pk_i = r_iP, sk_i = r_iP_0)$, 再通过安全信道将其真实身份和公钥 pk_i 发送给中心机构。

中心机构在验证用户的真实身份和公钥的合法性后,为用户 i 生成虚拟身份 vid_i , 并保存用户 i 的真实身份和 vid_i 的映射,然后为用户的虚拟身份和公钥生成签名 $Sig_{sk_{CA}}(vid_i || pk_i) || H(vid_i || pk_i)$, 并将该签名广播到联盟链中。

联盟链中的各个节点在验证上述签名的有效性后,将 $(vid_i, pk_i, online, null)$ 加入到各自维护的节点信息表中。至此,用户 i 加入联盟链中成为节点 i 。

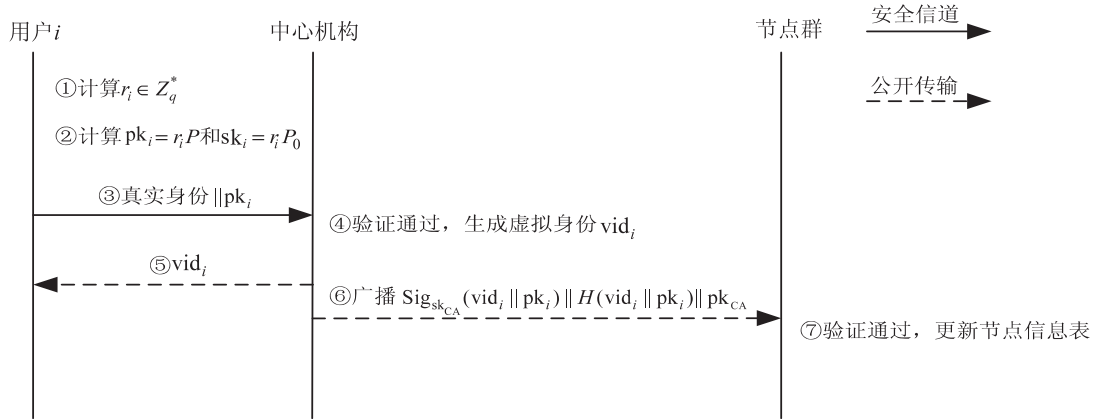


图2 用户注册流程

2.3.2 匿名交易

节点在联盟链中实现匿名交易的过程如图3所示。当节点 a 和节点 b 要进行匿名交易时, a 和 b 首先通过安全信道协商交易 m 并交换各自对 m 的签名, 然后 a 计算 $M = RSig_A(m) || H(Sig_{sk_a}(m) || Sig_{sk_b}(m))$ 。其中, $RSig_A(m)$ 表示 a 在环 A 上用可追踪环签名对交易 m 的签名, $Sig_{sk_a}(m)$ 为 a 对 m 的签名, $Sig_{sk_b}(m)$ 为 b 对 m 的签名。接着, a 使用实用拜占庭容错协议

将 M 上传到联盟链, 并将实用拜占庭容错预准备阶段中的验证签名的步骤改为验证可追踪环签名。

b 获得联盟链上的 M 后, 验证 M 的正确性, 若验证未通过, 则终止与 a 的交易, 若验证通过, 则计算 $M' = RSig_B(m) || H(Sig_{sk_a}(m) || Sig_{sk_b}(m))$, 表示 b 在环 B 上用可追踪环签名对交易 m 的签名, 并使用实用拜占庭容错协议将 M' 上传至联盟链。至此, a 和 b 分别以环 A 和环 B 的身份开始遵守交易 m 。

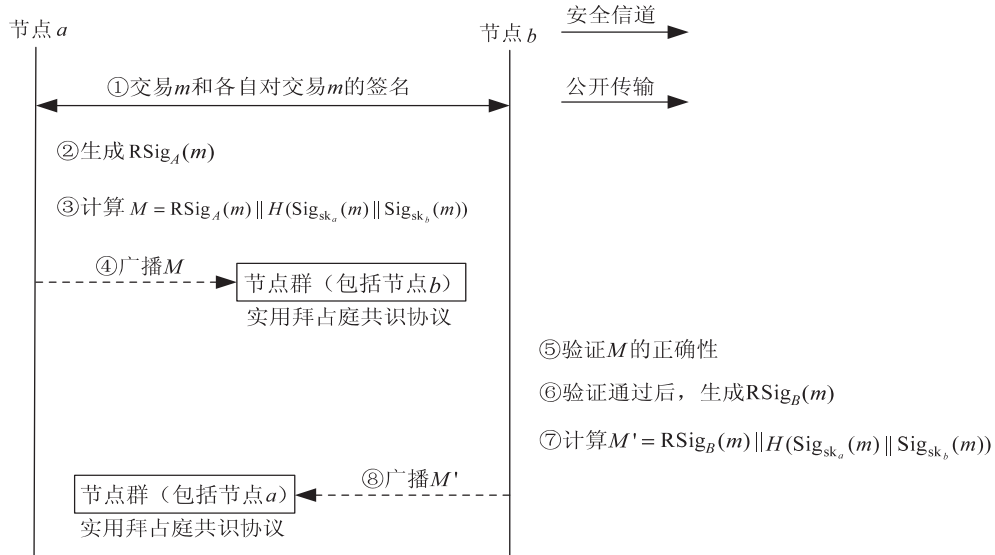


图3 基于可追踪环签名的匿名交易过程

节点 a 生成 $\text{RSig}_A(m)$ 的具体过程如下:

(1) 选择环成员 $L = \{\text{vid}_1, \text{vid}_2, \dots, \text{vid}_n\}$ (包括 vid_a)。

(2) 选择 $x_i, t_i \in Z_q^*$, $\text{TK}_i = t_i r_i P (i = 1, 2, \dots, n)$, $R_i = x_i P (i = 1, 2, \dots, n, i \neq a)$, $T_i = t_i P$ 。

(3) 令 $T = r_a \sum_{i=1}^n t_i P$ 。

(4) 计算 $h_i = H(m, T, R_i) (i = 1, 2, \dots, n, i \neq a)$ 。

(5) 计算 $R_a = x_a \text{pk}_a - \sum_{i=1, i \neq a}^n (R_i + h_i \text{pk}_i)$ 。

(6) 计算 $h_a = H(m, T, R_a)$, $Z = (x_a + h_a) \text{sk}_a$ 。

(7) $\text{RSig}_A(m) = (m, Z, R_i, \text{TK}_i, T, L) (i = 1, 2, \dots, n)$ 。

同理, 节点 b 可得 $\text{RSig}_B(m) = (m, Z', R'_j, \text{TK}'_j, T', L') (j = 1, 2, \dots, o, \text{包括 } o = b)$ 。

2.3.3 解决纠纷

当 a 和 b 产生争议时, 假设联盟链有 $3f + 1$ 个节点, 并且由 a 提出仲裁申请, a 令 $N = \text{Sig}_{\text{sk}_a}(m) \parallel \text{Sig}_{\text{sk}_b}(m)$ 。整个解决纠纷的流程可以分为预准备阶段、准备阶段和确认阶段, 具体过程如下:

(1) 预准备阶段。

预准备阶段主要分为预准备阶段 1 和预准备阶段 2, 预准备阶段 1 主要是 a 向其它节点提出去匿名化请求的过程, 预准备阶段 2 主要是各个节点之间交换对可追踪环签名进行去匿名化所需信息的过程。

① 预准备阶段 1。

a 广播 $\langle \text{Pre-prepare-first}, \text{view}, \text{count}, H(N) \rangle N$, 其中, Pre-prepare-first 表示预准备阶段 1, view 是视图编号, count 是序列号。

a 之外的节点在收到该预准备消息后, 验证视图 (view)、序列号 (count) 和 $H(N)$ 的正确性, 并且 $H(N)$ 已记录在联盟链上, 才会接受预准备消息。如果节点不接受第一阶段的预准备消息则什么都不做。

② 预准备阶段 2。

接受第一阶段预准备消息的节点根据 $H(N)$ 匹配联盟链上的 M 和 M' , 检查 M 中的环成员 L 和 M' 中的环成员 L' 来判断自己是否为环 A 或环 B 的成员。若节点既不是环 A 的成员也不是环 B 的成员, 则什么都不做。

若节点 $i (i = 1, 2, \dots, n, \text{包括 } i = a)$ 是环 A 的成员, 广播 $\langle \text{Pre-prepare-second}, \text{view}, \text{count}, H(N) \rangle \text{Sig}_{\text{sk}_i}(T_i) \parallel H(T_i) \parallel \text{pk}_i$ 。其中, $\text{Pre-prepare-second}$ 表示预准备阶段 2, $T_i = \text{TK}_i r_i^{-1}$, $\text{Sig}_{\text{sk}_i}(T_i)$ 表示 i 使用私钥 sk_i 对 T_i 签名, pk_i 为 i 的公钥;

若节点 $j (j = 1, 2, \dots, o, \text{包括 } j = b)$ 是环 B 的成员, 广播 $\langle \text{Pre-prepare-second}, \text{view}, \text{count}, H(N) \rangle$

$\text{Sig}_{\text{sk}_j}(T'_j) \parallel H(T'_j) \parallel \text{pk}_j$ 。其中, $\text{Pre-prepare-second}$ 表示预准备阶段 2, $T'_j = \text{TK}'_j r_j^{-1}$, $\text{Sig}_{\text{sk}_j}(T'_j)$ 表示 j 使用私钥 sk_j 对 T'_j 签名, pk_j 为 j 的公钥。

收到第二阶段的预准备消息的节点, 验证视图 (view)、序列号 (count) 和 $H(N)$ 的正确性以及签名 $\text{Sig}_{\text{sk}_i}(T_i)$ 和 $\text{Sig}_{\text{sk}_j}(T'_j)$ 的合法性。此外, 为了保证 T_i 和 T'_j 的有效性, 如果上述消息来自环 A 中的成员, 节点通过等式 $e(\text{TK}_i, P) = e(T_i, \text{pk}_i)$ 来判断 T_i 的有效性; 如果上述消息来自环 B , 节点通过等式 $e(\text{TK}'_j, P) = e(T'_j, \text{pk}_j)$ 来判断 T'_j 的有效性。

在每个节点都集齐环 A 和环 B 中所有的 T_i 和 T'_j 后, 首先分别根据公式 1 和公式 2 计算 J 和 K , 然后分别计算 $e(J, \text{pk}_i) (i = 1, 2, \dots, n)$ 和 $e(K, \text{pk}_j) (j = 1, 2, \dots, o)$ 。

当 $e(J, \text{pk}_i) = e(T, P)$ 时, 各个节点可以得出 pk_a , 当 $e(K, \text{pk}_j) = e(T', P)$ 时, 各个节点可以得出 pk_b , 然后节点根据联盟链上的 m 判断是 b 违约还是 a 恶意提出去匿名化请求, 最后将判断结果记录为 E 。

$$J = \sum_{i=1}^n T_i \quad (1)$$

$$K = \sum_{j=1}^m T'_j \quad (2)$$

(2) 准备阶段。

如果节点不接受预准备消息则什么都不做, 而接受了预准备消息的节点 k 向其它节点广播 $\langle \text{Prepare}, \text{view}, \text{count}, H(N) \rangle \text{Sig}_{\text{sk}_k}(E) \parallel H(E) \parallel \text{pk}_k$ 。由于预准备阶段被用来收集去匿名化所需的数据, a 无法在预准备阶段就表达自己的意见, 所以 a 参与发送准备消息。其中, Prepare 表示准备阶段, $\text{Sig}_{\text{sk}_k}(E)$ 表示 k 使用私钥 sk_k 对 E 进行签名, pk_k 为 k 的公钥。

收到准备消息的节点验证视图 (view)、序列号 (count) 和 $H(N)$ 的正确性以及签名 $\text{Sig}_{\text{sk}_k}(E)$ 的合法性。当节点在收到 $2f$ 个与其接受的预准备消息对应的准备消息后 (相同的视图 (view)、序列号 (count) 和 $H(N)$), 将这 $2f + 1$ 个准备消息 (包括自己) 写入临时日志中, 在 $2f + 1$ 个准备消息中至少有 $f + 1$ 个 (包括自己) 相同的为真。

(3) 确认阶段。

如果节点不接受预准备消息则什么都不做, 接受了准备消息的节点 k 向其它节点广播自己准备阶段判断为真的消息对应的确认消息 $\langle \text{Commit}, \text{view}, \text{count}, H(N) \rangle \text{Sig}_{\text{sk}_k}(E) \parallel H(E) \parallel \text{pk}_k$ 。其中, Commit 表示确认阶段, $\text{Sig}_{\text{sk}_k}(E)$ 表示 k 使用私钥 sk_k 对 E 进行签名, pk_k 为 k 的公钥。

收到确认消息的各个节点验证视图 (view)、序列号 (count) 和 $H(N)$ 的正确性以及签名 $\text{Sig}_{\text{sk}_k}(E)$ 的合

法性。当节点在收到 $2f$ 个与其接受的准备消息所对应的确认消息后,将这 $2f + 1$ 个确认消息(包括自己)写入临时日志中,在 $2f + 1$ 个确认消息中至少有 $f + 1$ 个(包括自己)相同的为真。

最后,每个节点根据临时日志中的内容对各自的节点信息表进行修改,如果是 b 违约,则修改节点信息表中 b 所对应的映射为 $(\text{vid}_b, \text{pk}_b, \text{offline}, \text{default})$, 如果是 a 恶意提出去匿名化请求,则修改节点信息表中 a 所对应的映射为 $(\text{vid}_a, \text{pk}_a, \text{offline}, \text{default})$, 其中 offline 表示用户从联盟链中注销, default 表示用户因为失信行为而注销。整个解决纠纷阶段的流程如图4所示。

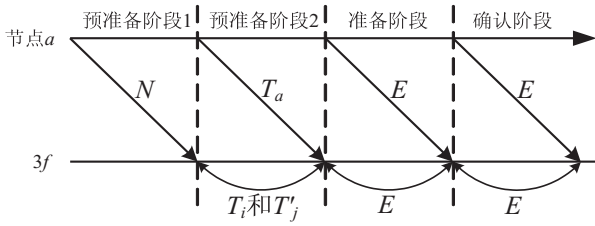


图4 用户解决纠纷流程

2.3.4 注销

当节点 k 退出联盟链,则广播 $\text{Sig}_{\text{sk}_k}(\text{logout} \parallel \text{vid}_k) \parallel H(\text{logout} \parallel \text{vid}_k) \parallel \text{pk}_k$, 其中, $\text{Sig}_{\text{sk}_k}(\text{logout} \parallel \text{vid}_k)$ 表示 k 用私钥 sk_k 对 $\text{logout} \parallel \text{vid}_k$ 签名, logout 表示注销消息, vid_k 表示 k 的虚拟身份, pk_k 表示 k 的公钥。

其它节点在验证上述签名的合法性后,将节点信息表中 k 对应的映射由 $(\text{vid}_k, \text{pk}_k, \text{online}, \text{null})$ 改为 $(\text{vid}_k, \text{pk}_k, \text{offline}, \text{null})$ 。

因为节点信息表由联盟链中的节点共同维护,所以中心机构只需要定期向一定数量的随机节点请求节点信息表,并通过对比节点信息表和自己本地保存的用户真实身份和虚拟身份的映射,找到该节点对应用户的真实身份。

如果表中节点是正常注销,中心机构将删除该节点对应用户;如果表中节点是因为违规行为而注销,中心机构将通过该节点对应用户的真实身份来对用户进行处罚。

3 方案分析

首先对文中方案进行了正确性分析、可追踪性分析和安全性分析,然后将文中方案与其它方案进行对比。

3.1 正确性

以验证 $\text{RSig}_A(m)$ 为例,在交易阶段中,各个节点通过公式3来验证可追踪环签名的合法性。

$$e(Z, P) = e\left(\sum_{i=1}^n (R_i + h_i \text{pk}_i), P_0\right) \quad (3)$$

若公式3成立,则验证通过,判断的过程如下所示:

$$\begin{aligned} e(Z, P) &= e((x_a + h_a) \text{sk}_a, P) = \\ &= e((x_a + h_a) r_a P_0, P) = \\ &= e((x_a + h_a) r_a sP, P) = \\ &= e((x_a + h_a) r_a P, sP) = \\ &= e((x_a + h_a) \text{pk}_a, P_0) = \\ &= e((x_a \text{pk}_a + h_a \text{pk}_a), P_0) = \\ &= e\left(\sum_{i=1, i \neq a}^n (R_i + h_i \text{pk}_i) + R_a + h_a \text{pk}_a, P_0\right) = \\ &= e\left(\sum_{i=1}^n (R_i + h_i \text{pk}_i), P_0\right) \end{aligned}$$

在解决纠纷的预备阶段2中,每个节点验证 T_i 的有效性,具体过程如下所示:

$$e(\text{TK}_i, P) = e(t_i r_i P, P) = e(t_i P, r_i P) = e(T_i, \text{pk}_i)$$

3.2 可追踪性

以得出环 A 中真正签名者节点 a 的公钥为例,在解决纠纷中的预备阶段2中,节点使用环中成员的公钥 pk_i 验证等式 $e(J, \text{pk}_i) = e(T, P)$, 其中 T 由公式4给出,该公式再生成 $\text{RSig}_A(m)$ 的第3步。

$$T = r_a \sum_{i=1}^n t_i P \quad (4)$$

当 $i = a$ 时,上式成立, pk_a 即为可追踪环签名中真正签名者的公钥,具体过程如下所示:

$$\begin{aligned} e(J, \text{pk}_i) &= e\left(\sum_{i=1}^n T_i, r_i P\right) = e\left(\sum_{i=1}^n t_i P, r_i P\right) = \\ &= e\left(r_i \sum_{i=1}^n t_i P, P\right) = e(T, P) \end{aligned}$$

3.3 安全性

文中方案使用已经被证明能够增加用户匿名性的可追踪环签名^[17-18]来防止地址聚类等分析方法的去匿名化攻击,并且通过新增检测机制和结合实用拜占庭容错得到以下两种新的安全特性。

(1)防止节点恶意提出去匿名化请求。

为了防止交易无关节点恶意提出去匿名化请求,在交易阶段,节点通过安全信道交换各自对交易的签名,即只有交易相关节点拥有对交易的签名。在解决纠纷阶段,申请对可追踪环签名去匿名化的节点必须提交所有交易相关节点的签名,联盟链中的其它节点才会接受该节点的去匿名化请求。

为了防止交易相关节点恶意提出去匿名化请求,在解决纠纷阶段,去匿名化将会应用于所有交易相关节点,如果交易相关节点恶意提出去匿名化请求,将会被其它节点通过交易内容判断为失信节点并记录在节点信息表中,最后受到中心机构的处罚。

(2) 对中心机构匿名。

由于文中方案使用可追踪环签名并且限定只有交易相关节点才能提出去匿名化请求,中心机构没有权利自主对用户的可追踪环签名进行去匿名化操作,也无法向环成员提出去匿名化请求,所以用户对于中心机构是匿名的。

3.4 方案对比

文中方案将可追踪环签名与实用拜占庭容错结合,既能保护用户的身份隐私,也能保证较好的容错性

和安全性。

总的来说,相较于文献[13,22]的方案,文中方案具有条件匿名性,可以防止双花攻击和拒绝服务攻击;相较于文献[15,19-20]的方案,文中方案能同时满足防止节点恶意提出去匿名化请求和对中心机构(群管理员和审计节点)匿名两种安全特性,并且拥有较高的容错率。表1是文中方案与其它身份隐私保护方案的对比。

表1 文中方案与其它方案的对比

方案	场景	匿名性	容错性	防止节点恶意提出去匿名化请求	对中心机构匿名
文中方案	联盟链	条件匿名	中	是	是
文献[13]	公有链	完全匿名	高	是	无中心机构
文献[15]	联盟链	条件匿名	低	是	否
文献[19]	联盟链	条件匿名	低	否	否
文献[20]	联盟链	条件匿名	低	是	否
文献[22]	公有链	完全匿名	高	是	无中心机构

4 实验及分析

4.1 实验环境

文中方案的实验环境:CPU为Intel(R)Core(TM)i7-7700HQ,主频为2.80 GHz,2.00 GB内存,操作系统为Ubuntu 21.10,编程语言为C语言,使用的PBC库版本号为0.5.14。

4.2 实验结果及分析

本节测量了四种具有条件匿名性的身份隐私保护方案中系统初始化的时间以及在不同节点数量的环或群中,系统初始化、生成签名、验证签名和追踪签名所需的总时间。

现定义符号 T_E 表示模幂运算的时间, T_M 表示模乘运算的时间, T_{Zr} 表示初始化模 r 整数环的时间, T_G 表示初始化 G_1 群的时间。

(1) 系统初始化。

表2展示了在系统初始化阶段,各个方案所需的理论时间和具体时间。

表2 系统初始化所需的时间

方案	理论时间	具体时间/ms
文中方案	$4T_G+2T_{Zr}+3T_M$	6.42
文献[15]	$3T_G+3T_{Zr}+2T_E+T_M$	5.31
文献[19]	$tT_G+(2t+2n)T_{Zr}+2tT_E+2tT_M$	10.87
文献[20]	$tT_G+(2t+2n)T_{Zr}+2tT_E+2tT_M$	10.92

其中,文中方案和文献[15]方案由用户根据系统生成的公共参数自行生成公私钥,其理论时间是固定不变并且所需时间较少,而文献[19-20]方案由用户根据系统使用秘密共享生成公共参数来生成公私钥,

其所需时间与秘密共享参数(t, n)的设置有关,秘密共享参数(t, n)表示 n 个节点的系统中需要 t 个节点合作才能共享秘密。此次实验中,为了便于测量文献[19-20]方案的秘密共享参数设置为(3,5),远小于实际情况下的参数设置。

(2) 总时间。

图5展示了文中方案、文献[15,19-20]方案这四个具有条件匿名性的身份隐私保护方案在不同数量的环(群)节点的情况下,系统初始化、生成签名、验证签名和追踪签名所需的总时间。

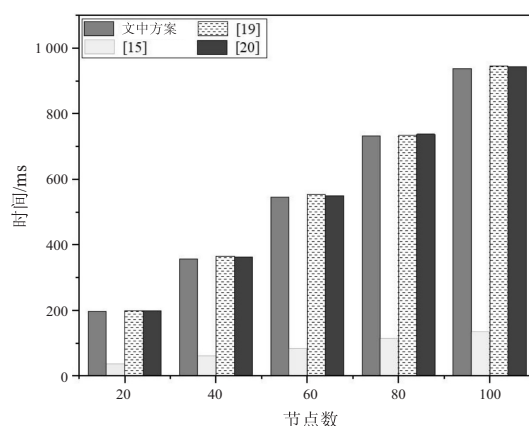


图5 具有条件匿名性的四个方案的总时间

虽然文中方案与文献[19-20]方案使用的都是可追踪环签名,但是文中方案在系统初始化时间上小于文献[19-20]方案,所以文中方案所需的总时间较小,而且文中方案相较于文献[19-20]方案新增了防止节点恶意提出去匿名化请求的安全特性。

虽然文中方案相较于文献[15]方案需要花费较多时间,但是文中方案对中心机构具有匿名性,并减少

了中心机构的任务,具有更高的安全性和容错性。

5 结束语

针对联盟链中现有的用户身份隐私保护方案不够完善的问题,将可追踪环签名和实用拜占庭容错结合并运用于联盟链中用户的身份隐私保护上,不仅能够保证联盟链中的用户对于其它用户和中心机构都具有条件匿名性,还添加了防止节点恶意提出去匿名化请求的特性,增加了系统的安全性,并且通过结合实用拜占庭容错,增加了系统的容错性。理论和实验表明,该方案既能够保护用户的身份隐私,又能保证较高的安全性和容错性,并且时间开销较为合理。

参考文献:

- [1] 袁 勇,王飞跃. 区块链技术发展现状与展望[J]. 自动化学报,2016,42(4):481-494.
- [2] 邵奇峰,金澈清,张 召,等. 区块链技术:架构及进展[J]. 计算机学报,2018,41(5):969-988.
- [3] Tanmer Technology. Six typical application scenarios of alliance chain in blockchain technology[EB/OL]. (2021-02-22)[2023-04-10]. <http://tanmer.com/blog/582>.
- [4] FENG Q, HE D, ZHADALLY S, et al. A survey on privacy protection in blockchain system[J]. Journal of Network and Computer Applications, 2019, 126:45-58.
- [5] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in bitcoin using p2p network traffic[C]//Proc of financial cryptography and data security: 18th international conference. Christ Church; Springer, 2014:469-485.
- [6] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: anonymity for bitcoin with accountable mixes[C]//Proc of financial cryptography and data security: 18th international conference. Christ Church; Springer, 2014:486-504.
- [7] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for bitcoin[C]//Proc of financial cryptography and data security: FC international workshops, BITCOIN, WAHC, and wearable. San Juan; Springer, 2015:112-126.
- [8] MAXWELL G. Coinjoin: bitcoin privacy for the real world[EB/OL]. (2019-11-12)[2023-04-10]. <https://bitcoin-talk.org/?topic=279249>.
- [9] RUFFING T, MORENO-SANCHEZ P, KATE A. Coinshuffle: practical decentralized coin mixing for bitcoin[C]//Proc of computer security - ESORICS: 19th European symposium on research in computer security. Wroclaw; Springer, 2014:345-364.
- [10] BISSIAS G, OZISIK A P, LEVINE B N, et al. Sybil-resistant mixing for bitcoin[C]//Proc of the 13th workshop on privacy in the electronic society. New York; ACM, 2014:149-158.
- [11] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret[C]//Proc of advances in cryptology - ASIACRYPT: 7th international conference on the theory and application of cryptology and information security gold coast. Gold Coast; Springer, 2001:552-565.
- [12] GROTH J, KOHLWEISS M, MALLER M, et al. Updatable and universal common reference strings with applications to zk - SNARKs[C]//Proc of advances in cryptology - CRYPTO: 38th annual international cryptology conference. Santa Barbara; Springer, 2018:698-728.
- [13] LI X, MEI Y, GONG J, et al. A blockchain privacy protection scheme based on ring signature[J]. IEEE Access, 2020, 8:76765-76772.
- [14] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: anonymous distributed e-cash from bitcoin[C]//Proc of IEEE symposium on security and privacy. Berkeley: IEEE, 2013:397-411.
- [15] 刁一晴,叶阿勇,张娇美,等. 基于群签名和同态加密的联盟链双重隐私保护方法[J]. 计算机研究与发展, 2022, 59(1):172-181.
- [16] KIAYIAS A, TSIOUNIS Y, YUNG M. Traceable signatures[C]//Proc of Eurocrypt. Interlaken; Springer, 2004:571-589.
- [17] 杨华杰, 缪祥华, 朱海韬, 等. 一种高效无证书可追踪环签名方案[J]. 信息安全与技术, 2014, 5(7):32-35.
- [18] 孙庆英, 吴克力, 徐会艳. 一种可追踪签名者的环签密方案[J]. 计算机工程, 2011, 37(16):129-131.
- [19] TANG F, PANG J, CHENG K, et al. Multiauthority traceable ring signature scheme for smart grid based on blockchain[J]. Wireless Communications and Mobile Computing, 2021, 2021:1-9.
- [20] LAI C, MA Z, GUO R, et al. Secure medical data sharing scheme based on traceable ring signature and blockchain[J]. Peer-to-Peer Networking and Applications, 2022, 15(3):1562-1576.
- [21] FUJISAKI E, SUZUKI K. Traceable ring signature[C]//Proc of public key cryptography - PKC: 10th international conference on practice and theory in public-key cryptography. Beijing; Springer, 2007:181-200.
- [22] VAN SABERHAGEN N. CryptoNote v 2.0[EB/OL]. (2013-10-17)[2023-04-10]. <https://cryptonote.org/whitepaper.pdf>.
- [23] NOETHER S, MACKENZIE A. Ring confidential transactions[J]. Ledger, 2016, 1:1-18.
- [24] ALONSO K M. Zero to monero[EB/OL]. (2020-04-04)[2023-04-10]. <https://www.getmonero.org/library/Zero-to-Monero-2-0-0.pdf>.
- [25] SCAFURO A, ZHANG B. One-time traceable ring signatures[C]//Proc of European symposium on research in computer security. Berlin; Springer, 2021:481-500.