利用环盲签名+仲裁的认证混币方案

方志鹏, 李晓宇

引用本文

方志鹏, 李晓宇. 利用环盲签名+仲裁的认证混币方案[J]. 计算机科学, 2025, 52(11): 390-397.

FANG Zhipeng, LI Xiaoyu. Using Ring Blind Signature+Arbitration Authentication Mixed Coin Scheme [J]. Computer Science, 2025, 52(11): 390-397.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.241000048

利用环盲签名+仲裁的认证混币方案

方志鹏[1]　李晓宇[2]
1 郑州大学网络空间安全学院　郑州 450003
2 郑州大学计算机与人工智能学院　郑州 450001
(1665198588@qq.com)

摘　要　区块链是一种分布式账本技术,具有去中心化、不可篡改、数据公开等特性。但数据公开导致区块链存在隐私泄露的安全隐患。引入混币中心作为中介切断了转账者和接收者之间的关联,可以达到保护交易双方隐私的目的,然而它仍然存在一些安全漏洞,例如混币中心仍然能够掌握这个关联关系,混币中心可能伪造转账,转账者可能否认交易等。因此,提出了基于环盲签名的仲裁认证混币技术,利用环盲签名解决混币中心知道关联的问题,利用仲裁认证解决混币中心以及用户违规行为的问题。所提方法相比传统混币方案具有不可比拟的优势,可以很好地解决传统混币方案存在的问题,具有匿名性、不可否认性、不可伪造性、防Dos性等特性,完善了传统的混币服务,可以进一步保护用户隐私。所提方案响应时间与用户数、混币中心数均呈正相关,响应时间相比Mixcoin与Blindcoin方案略长,但比Coinjoin和Coinshuffle方案短;同时,相对于其他方案,所提方案能有效地防范用户和混币中心的欺骗行为,更好地保护交易隐私。

关键词:区块链;隐私泄露;混币中心;环盲签名;匿名性
中图分类号　TP309

Using Ring Blind Signature+Arbitration Authentication Mixed Coin Scheme

FANG Zhipeng[1] and LI Xiaoyu[2]
1 School of Cyber Science and Engineering,Zhengzhou University,Zhengzhou 450003,China
2 School of Computer Science and Artificial Intelligence,Zhengzhou University,Zhengzhou 450001,China

Abstract　Blockchain is a distributed ledger technology with the characteristics of decentralization,non-tampering,and data disclosure. However,data disclosure has led to the security risk of privacy leakage in the blockchain. The introduction of the mixing center as an intermediary cuts off the connection between the transferor and the receiver,and achieves the purpose of protecting the privacy of both parties to the transaction,but it still has some security loopholes,such as the mixing center can still grasp this association,the mixing center may forge the transfer,and the transferor may deny the transaction. Therefore,a quorum-blind signature based on arbitration authentication mixing technology is proposed,which uses ring-blind signatures to solve the problem of association between the mixing center,and uses arbitration authentication to solve the problem of the mixing center and user violations. Compared with the traditional coin mixing scheme,it has incomparable advantages,which can well solve the problems existing in the traditional coin mixing scheme,and has the characteristics of anonymity,non-repudiation,non-forgery,anti-Dos,etc.,which improves the traditional coin mixing service and can further protect user privacy. The response time of this scheme is positively correlated with the number of users and the number of mixing centers. Compared to the Mixcoin and Blindcoin schemes,the response time is slightly longer,but shorter than that of Coinjoin and Coinshuffle schemes. Additionally,compared to other schemes,this scheme can effectively prevent deception by users and mixing centers,better protecting transaction privacy.

Keywords　Blockchain,Privacy breaches,Coin mixing center,Ring-blind signatures,Anonymity

1　引言

近些年,比特币发展迅速。比特币作为加密货币,由于具有去中心化、透明、防止重复交易等特点,发布至今已经成为最流行的加密数字货币[1]。随着比特币被广泛应用于各个领域,其核心技术区块链也得到越来越多的重视及发展应用[2]。区块链作为一种公开的帐本系统,具有去中心化、不可篡改、数据公开等特性[3],但同时也增加了隐私泄露的风险。相对于传统的中心化架构,区块链机制不依赖特定中心节点处理和存储数据,因此能够避免集中式服务器单点崩溃和数

到稿日期:2024-10-11　返修日期:2025-02-12
基金项目:国家自然科学基金(61876016)
This work was supported by the National Natural Science Foundation of China(61876016).
通信作者:李晓宇(iexyli@zzu.edu.cn)

据泄露的风险,但是交易信息公开可验证使得攻击者可以轻易获得区块链中的所有交易信息[4],而区块链的不可篡改性使得交易信息写入区块链后一旦发生隐私泄露[5],将无法被修改和删除,敏感信息一旦泄露就无法挽救。因此,区块链系统在走向应用之前,必须解决隐私泄露问题,要更加重视隐私保护,为用户提供完整的隐私保护服务[6]。

区块链面临的隐私问题主要分为用户交易隐私威胁和身份隐私威胁两大类[7]。

1)用户交易隐私威胁,即在比特币交易网站,根据用户公钥可以获取与该公钥地址关联交易的详细信息。通过比特币论坛、推特等网站获取用户公开的公钥地址,追踪用户资金来源与使用情况,计算用户余额。通过分析比特币系统交易规律及交易特征,攻击者能将公钥与用户身份相关联,获取资金流向与资金余额,给用户带来安全隐患。

对于交易隐私威胁,早期的保护技术采用了数字加密技术,即将需要存储的明文交易信息转换为加密后的密文进行存储,如此,即使不怀好意的一方获取了区块链上存储的交易数据,也会因不知道解密密钥、不知道加密机制等原因而无法获取真正需要的信息。数字加密技术属于密码学的部分,数字加密包括对称密码体制、非对称密码体制、混合密码体制等。其可以对明文进行加密的特性还可以应用于比特币交易中的匿名通信。

2)用户身份隐私威胁。由于在比特币系统中,用户不需要提供自己的身份信息,而是通过公钥实现双方间的转账交易,因此攻击者通过公钥无法还原交易者的身份信息,但他们可以通过下载比特币系统交易数据,分析地址间的关联性,不断减小交易关系图,从而降低区块链地址的匿名性。

为保护交易双方身份隐私,可以使用混币技术[8]切断输入地址与输出地址的联系,从而起到保护隐私的作用。混币技术分为中心化混币技术[9]和非中心化混币技术[10]。中心化混币中参与混币的用户首先将资金发送给混币中心,然后由混币中心代理转账给接收地址,由于资金经过了混币中心的处理,攻击者很难发现参与混币交易的双方地址。非中心化混币的核心思想是通过将多个交易合并成一个交易,隐藏交易输入方和输出方的对应关系。对于一个从多输入到多输出的交易,潜在攻击者无法通过阅读交易信息确定输入和输出之间的关系。

混币技术可以有效地对外屏蔽交易的"发送者地址-接收者地址"之间的关联,但混币中心仍然知道这个关联。为了修复这个漏洞,可以在交易过程中使用数字签名[11]中的盲签名技术[12],使混币中心在执行混币时同样无法获知"发送者地址-接收者地址"之间的关联。

然而,上述混币方案仍然可能存在一定风险。第一,混币中心可能伪造用户的转账要求,把收到的资金转给其他地址;第二,在混币中心已经按照用户要求转账到指定地址后,用户可能会否认自己发出过转账要求,从而要求混币中心重新转账。为了解决这两个问题,本文提出了利用环盲签名加仲裁的认证混币方案。仲裁签名机制,即仲裁方对交易进行认证来保证不会出现违规操作。而为了进一步保护用户隐私,让混币服务器也无法联系转入方和转出方,采用了环盲签名机制来保护隐私,并使用数字加密技术加密通信内容来提防外来攻击者。本文方案中的混币中心不知道具体为谁服务,且混币中心有多个,接收用户预存资金的混币中心与转账给目标地址的混币中心不是同一个而且彼此不知道对方,从而在保证交易顺利安全进行的同时进一步提高了隐私保护程度。

2 相关技术

2.1 环盲签名

环签名是在数字签名的基础上为了满足签名者隐私保护的应用需求提出的一种签名方案[13]。环签名与群签名[14]类似,群签名方案中,一个群体中的任意一个成员可以以匿名的方式代表整个群体对消息进行签名从而达到匿名的效果。环签名相比群签名有其独特的地方,环签名作为一种特殊的群签名,最早是由 Rivest 等[13]于 2001 年在研究如何匿名身份的情况下提出的数字签名。环签名是一种简化的群签名,环签名中只有环成员没有管理者,在进行签名时,签名者无需成员环中其他成员的帮助(协作),甚至可以不让环中其他成员知晓,只需要用自己的私钥和其他成员的公钥就能实现签名;在验证签名时环签名仅可验证签名来自群组成员,但是无法知晓具体是哪个成员。

盲签名也是在数字签名的基础上满足对签名信息内容的隐私保护的一种签名方案。盲签名方案中,消息拥有者对消息进行盲化处理,签名者无法获知所签消息的具体内容并完成签名发送给消息拥有者,消息拥有者可以对盲签名结果进行脱盲处理,从而得到原始消息的数字签名,而签名者无法将该脱盲后的消息与自己签署的消息相对应,以此达到隐私保护的目的。

本文方案使用的是将以上两种签名方案结合的技术,是同时满足签名者和消息发送者的隐私保护的方案,即环盲签名。消息拥有者将消息发送给环中成员,经过环盲签名,可以得到环中某成员对该消息的签名,验证者只能验证签名来自于环成员却无法知道确切的签名者,同时签名者对所签信息的具体内容无法获知。

算法过程可参考文献[15],具体如下:

1)系统建立

令 $G1$ 为由 p 生成的循环加法群,阶为 q;$G2$ 为相同阶的循环乘法群。e 是一个双线性对 $e:G1\times G1\rightarrow G2$。令 $H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\rightarrow G_1$,$H_3:G_2\rightarrow Z_q^*$ 皆为 Hash 函数。

系统中存在一个可信中心 KGC,随机选择 $k\in Z_q^*$,并设置 $P_{pub}=kp$。KGC 公开系统参数 $\{G1,G2,e,q,p,P_{pub},H1,H2,H3\}$,$k$ 为系统主密钥。

2)密钥生成

对于身份为 $ID_i\in\{0,1\}^*$ 的用户 i,KGC 为其生成签名密钥 $K_i=kH_2(ID_i)$。

3)环盲签名

令 m 为待签名消息,$L=\{1,2,\cdots,N\}$ 是签名者环,对应的签名者身份信息为 $\{ID_1,ID_2,\cdots,ID_N\}$。真实签名者身份为 ID_s。

用户和签名者之间执行以下协议,在协议的最后,用户得

到一个签名者对消息 m 的环盲签名。

(1)用户第一轮

①用户随机选取 $t\in_R Z_q^*$，$Q\in_R G_1$；

②用户计算 $D=H_1(m)$，$V=C_{s+1}=e(Q,p)^D$；

③发送 V 和 D 给签名者环。

(2)签名者第一轮

①对于每一个 $i\in\{s+1,\cdots,N-1,0,1,\cdots,s-1\}$，随机选取 $U_i\in_R G_1$；

②计算 $C_{i+1}=[e(P_{pub},H_3(C_i)H_2(ID_i))e(U_i,p)]^D$；

③计算 $U_s=-H_3(C_s)K_s$，$U'=\sum_{i=1}^{N}U_i$，因此签名者计算得到 $C_{s+2},C_{s+3},\cdots,C_N,C_1,C_2,\cdots,C_s$ 以及用户发来的 $V=C_{s+1}$；

④令 σ_C 为 $C_1,C_2,\cdots,C_N$ 的一个变换；

⑤发送 σ_C 和 U' 给用户。

(3)用户第二轮

在用户收到 σ_C 和 U' 后，用户计算 $U_1=Q+U'$，$U=tU_1$，$V_1=t\,H_1(m)p$，$V_2=t^2\,H_1(m)p$，$V_3=tP_{pub}$。

对消息 m 的环盲签名为 $\sigma=(m,\sigma_C,V_1,V_2,V_3,U)$。

(4)签名校验

验证对消息 m 的环签名 $\sigma=(m,\sigma_C,V_1,V_2,V_3,U)$ 是否有效，验证者只要校验：

$$\prod_{i\in\sigma_C}C_i=[e(V_3,\sum_{i=1}^{N}H_3(C_i)H_2(ID_i))e(U,p)]^{H_1(m)} \tag{1}$$

$$e(V_3,V_1)=e(P_{pub},V_2) \tag{2}$$

若式(1)和式(2)均通过，则该签名为一个合法的环签名，否则拒绝该签名。

2.2 混币技术

混币技术分为去中心化混币和中心化混币，这两种方案的目的都是切断交易输出地址与输入地址之间的联系，让攻击者无法将交易双方联系起来。但其实现方式各不相同。去中心化混币方案的核心特点是混币过程不经过第三方节点的方案，最早由 GregoryMaxwell 在比特币论坛上提出的 Coinjoin 方案的核心思想是将多个交易的输入地址和输出地址合并，只对外展示一个大的输入地址集合和输出地址集合，以此来隐藏交易输入方和输出方的对应关系。最早的中心化混币方案是由 Bonneau 提出的在不改变比特币协议情况下为用户提供混币服务保护隐私的方案——Mixcoin。用户将比特币发送到混合服务器，混合服务器将交易内容混合处理后，将比特币发送至输出地址，以此来切断输入地址和输出地址之间的联系。此外，为了进一步提高匿名性，Mixcoin 要求多用户同时使用相同金额进行混币，使得攻击者无法锁定交易用户。

2.3 混合加密技术

消息加密方案是消息发送方通过加密算法将明文信息加密成密文信息发送给消息接收方，消息接收方通过解密算法将密文信息还原成明文信息。如此，攻击者即使成功拦截通信并获取了信息，但也会因没有解密密钥而无法获取真实有效的原始数据。加密方案又分为对称加密算法和非对称加密算法。对称加密算法指发送方使用密钥加密信息成密文之后发送给接收方，接收方使用同一个密钥解密接收来的密文成明文。对称加密算法中常用的算法包括 DES，3DES，AES，DESX，RC4，RC5 等。非对称加密算法的基本思想是：在数据通信时，通信双方有两把密钥，即一把公钥和一把私钥，这两把密钥是一一对应的关系。当消息发送方向接收方发出信息时，首先发送方用接收方的公钥对要传出的数据进行加密并发送给接收方，然后接收方用自己的私钥把密文解成明文，且只有接收方的私钥可以解开。非对称加密算法中常用的算法包括 RSA、SM2(国密)、DH、DSA、ECDSA、ECC 等。

对称加密算法无法很好地解决秘钥配送的问题，而非对称加密算法的加密和解密时间长、效率低。混合加密[16]是将这两种方案进行结合，即用对称加密算法对应的对称密钥加密要传输的信息，然后用公钥密码算法对应的接收方公钥加密对称加密的密钥。接收方先用私钥解密密文获得对称密钥，然后使用该对称密钥解密密文获取原始数据。这种方案解决了公钥密码速度慢的问题，并通过公钥密码解决了对称密码的密钥配送问题。

3 利用环盲签名+仲裁的认证混币方案

区块链上隐私泄露的后果是非常严重的，为保护交易隐私，本文提出了基于环盲签名的仲裁混币方案，它消除了传统的中心化混币技术的漏洞，具有更高的安全性。传统混币技术确实割裂了转账者和接收者的交易链接，非常有效地保护了用户隐私，但是在传统中心化混币技术中，混币中心知晓转账者-接收者的关联关系，它有可能泄露此信息。本文提出建立多个混币中心，转账指令随机传递给其中一个混币中心，混币中心彼此独立地执行自己收到的转账指令。初始化时，转账者将资金发送到某个混币中心的账户中存起来，同时该混币中心代表所有混币中心生成环盲签名。需要转账时，转账方将转账指令和去盲化之后的环盲签名发给随机选择的混币中心。这样一来，混币中心可以通过验证环盲签名来证实转账者的合法性，但是无法获知转账者的身份，也无法掌握转账者-接收者的关联关系。另外，由于存在多个混币中心，接收预存资金并生成环盲签名的混币中心与执行转账指令的混币中心不是同一个，这进一步提高了交易的匿名程度。

虽然上述方法保证了用户匿名，但仍然可能存在问题，例如转账者否认要求混币中心转账，或者混币中心伪造转账。这两类问题都将导致交易无法顺利进行，针对此问题，本文提出了仲裁机制，即加入一个仲裁方来确保交易的顺利进行，转账者先向混币中心转账并获取混币中心返回的盲签名，然后转账者将交易信息、盲签名等发送给仲裁方，仲裁方验证通过后发送指令到混币中心要求其完成转账。若转账者否认要求混币中心转账，仲裁方可以获取转账者提交过的交易记录，发现转账者撒谎后执行处罚。混币中心也无法伪造转账，因为转账指令只能由仲裁方发出，如果混币中心自行转账，仲裁方便会对其进行相应的处罚。

本文方案用环盲签名技术来完成交易过程的匿名性，即在切断输入输出之间联系的基础上，混币中心不知道具体为谁服务，而转账者也不知道具体是哪一个混币中心为自己服务。本文方案引入仲裁方来保证交易的顺利进行，并对违规的一方进行处罚。此外，在通信过程中使用混合加密技术加密通信内容，让外来攻击者即使获取到消息，也无法获知具体

内容。本文系统由转账者、混币中心、仲裁 3 部分组成。

3.1 模型

转账者：转账者是使用本文系统提供服务的角色。转账者的目的是顺利地从转账者的当前账户将比特币转账到接收者地址（可以是另一个用户，也可以是用户的另一个地址），同时期望不泄露自己的各种隐私信息，包括混币中心也无法获取转账者的隐私信息。转账者通过环盲签名与混币中心通信来达到对混币中心匿名的目的。

混币中心：混币中心是本文系统提供服务的角色。混币中心接收转账者发送过来的比特币，按照仲裁发送来的信息（转账者提供的输出地址）完成转账。混币中心同样对外匿名，转账者也不知道具体是哪一个或哪几个混币中心为自己提供服务。混币中心通过提供服务来获取报酬，同时为了防止其私吞比特币，需要提供押金注册后才可以提供服务。

仲裁：仲裁对交易进行认证，从而保证交易的顺利进行。仲裁可以让转账者无法否认自己做出的转账要求，还可以让混币中心无法伪造转账以及无法拒绝服务。同时，一旦转账者或混币中心做出违规操作，仲裁方可以对其进行处罚，没收违规方在系统内的比特币。

3.2 参数

本文使用到的参数及其定义如表 1 所列。

表 1 参数定义

Table 1 Parameter definition

符号	相关定义
M	转账金额
m	转账者假名
add	转账地址
G_1	循环加法群
e	双线性对
$H1,H2,H3$	3 种 hash 函数
K_i	环成员签名密钥
M_0	服务费
P	交易指令
$sign$	环签名
G_2	循环乘法群
k	系统主密钥
i	环成员编号
ID_i	环成员身份信息
$\{G1,G2,e,q,p,P_{pub},H1,H2,H3\}$	KGC 公开系统参数
$\{t,Q,D,V,U_i,C_i,U_s,U',C',U_1,U,V_1,V_2,V_3,m\}$	环盲签名过程参数
K_u	转账者对称密钥
K_m	混币中心对称密钥
$E()$	AES 加密算法
$D()$	AES 解密算法
PK_i/SK_i	区块链系统对应的公钥/私钥
K_a	仲裁对称密钥
$Hash_a()$	仲裁私钥签名

3.3 混币方案

本文方案中混币中心组成一个签名者环，转账者预存资金后加入混币服务系统，系统为其生成 ID 和签名密钥，然后请求其转账的混币中心获取签名，该混币中心返回一个环盲签名给转账者，转账者脱盲后得到环签名。转账者使用此环签名生成交易指令并转发给仲裁，仲裁认证通过后指示任意混币中心完成转账。系统模型如图 1 所示。

完成系统注册的具体步骤如下：

1）加入本文系统的混币中心需要提供相应的押金到系统账户才可以加入本文系统，通过提供混币服务获取报酬，系统为其分配资金进行转账服务，押金金额远大于分配资金。系统的所有混币中心组成一个环，并进行环盲签名的初始化。

2）令 G_1 为由 p 生成的循环加法群，阶为 q；G_2 为相同阶的循环乘法群。e 是一个双线性对 $e:G1\times G1\rightarrow G2$。令 $H_1:\{0,1\}^*\rightarrow Z_q^*$，$H_2:\{0,1\}^*\rightarrow G_1$，$H_3:G_2\rightarrow Z_q^*$ 皆为 Hash 函数。系统中存在一个可信中心 KGC，随机选择 $k\in Z_q^*$，并设置 $P_{pub}=kp$。KGC 公开系统参数 $\{G1,G2,e,q,p,P_{pub},H1,H2,H3\}$，$k$ 为系统主密钥。$L=\{1,2,\cdots,N\}$ 是混币中心对应的签名者环，对应的签名者身份信息为 $\{ID_1,ID_2,\cdots,ID_N\}$。

3）区块链系统为转账者、混币中心、仲裁分配一对公钥 PK_i 和私钥 SK_i，AES 算法为转账者生成一个对称密钥 K_u，为混币中心生成对称密钥 K_m。对称加密技术 AES 和非对称加密技术 RSA 组成混合加密技术。混合加密用于加密交易过程中系统各方传递的信息数据，以确保被攻击者截获传递的信息数据后不会造成任何损失。

4）混币系统建立和维护一个公共的转账记录册，每一个混币中心每次收到一个仲裁发来的转账指令后，先查看公共的转账记录册（只包含假名与是否转账）中是否已经执行过转账，若已执行则拒绝转账，若未执行则进行转账操作并将假名和已转账登记在转账记录册中。

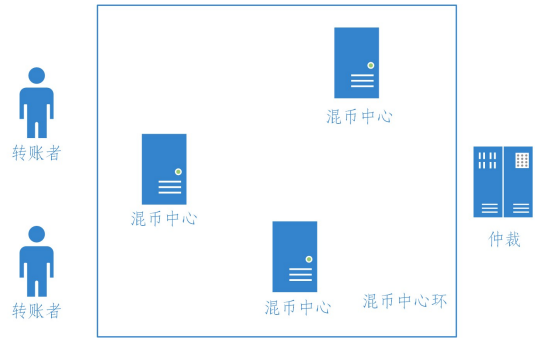

图 1 系统模型

Fig. 1 System model

转账者预存资金的过程如图 2 所示，具体步骤如下：

1）转账者转账固定金额 $M+M_0$（M 为转账金额，M_0 为服务费）到任意混币中心后，可使用假名 m 加入系统，系统为其生成一个 $ID_i\in\{0,1\}^*$，KGC 为其生成签名密钥 $K_i=kH_2(ID_i)$。混币中心收到 $M+M_0$ 后，将 $M_0/2$ 转到自己的押金地址，将 $M_0/2$ 转交给仲裁方，由仲裁方将另一半服务费转发给另一个参与此交易的混币中心。

2）转账者随机选择 $t\in_R Z_q^*$，$Q\in_R G_1$，计算 $D=H1(m)$，$V=C_{s+1}=e(Q,p)^D$ 并将 V 和 D 发送给步骤 1）中自己转账的混币中心。

3）该混币中心对于每一个 $i\in\{s+1,\cdots,N-1,0,1,\cdots,s-1\}$，随机选取 $U_i\in_R G_1$，并计算 $C_{i+1}=[e(P_{pub},H_3(C_i)H_2(ID_i))e(U_i,p)]^D$，计算 $U_s=-H_3(C_s)K_s$，$U'=\sum_{i=1}^{N}U_i$，混币中心计算得到 $C_{s+2},C_{s+3},\cdots,C_N,C_1,C_2,\cdots,C_s$ 以及转账者发来的 $V=C_{s+1}$。令 C' 为 $C_1,C_2,\cdots,C_N$ 的一个变换，将 C' 和

U'用对称密钥K_m加密得到$E(C',U')$，用转账者的公钥PK_u加密对称密钥K_m得到$Pk_u(K_m)$，将$E(C',U')$和$Pk_u(K_m)$发送给转账者。

4)转账者收到$E(C',U')$和$Pk_u(K_m)$后用自己的私钥SK_u解密得到对称密钥K_m，对称密钥解密$E(C',U')$得到C'和U'计算$U_1=Q+U'$，$U=tU_1$，$V_1=tH_1(m)p$，$V_2=t^2H_1(m)p$，$V_3=tP_{pub}$。得到环盲签名为$sign=(m,C',V_1,V_2,V_3,U)$。

$$\coprod_{i\in\sigma_c}C_i=[e(V_3,\sum_{i=1}^{N}H_3(C_i)H_2(ID_i))e(U,p)]^{H_1(m)} \tag{3}$$

$$e(V_3,V_1)=e(P_{pub},V_2) \tag{4}$$

验证两个等式是否成立，若成立则接受此盲签名，若不成立则继续向步骤1中的混币中心申请，直到成功为止。

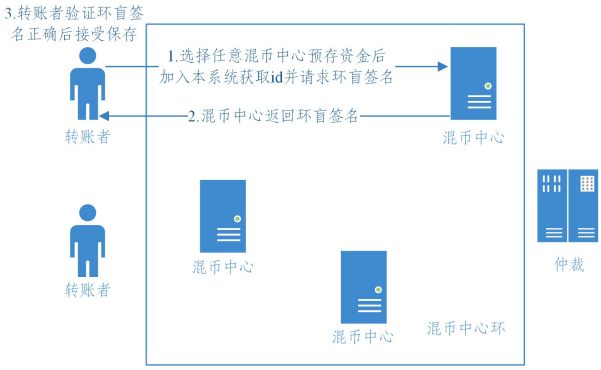

图2 转账者预存资金的过程

Fig. 2 Process of the remitter depositing funds

仲裁认证转账指令的过程如图3所示，具体步骤如下：

1)转账者将交易指令P(包含环签名$sign$、转账地址add、假名m等信息)用AES算法的对称密钥K_u加密得到$E(P)$，用仲裁公钥PK_a加密对称密钥K_u后得到$PK_a(K_u)$，将$E(P)$和$PK_a(K_u)$发送给仲裁。

2)仲裁收到$E(P)$和$PK_a(K_u)$后用自己的私钥SK_a解密得到对称密钥K_u，用对称密钥解密$E(P)$得到交易指令P，查看假名m是否已执行过转账：若已经执行，则拒绝接受转账请求；若未执行，则验证签名信息$sign$对应的两个等式是否成立，验证通过则将交易指令用自己的私钥SK_a进行签名得到$Hash_a(P)$，然后使用对称密钥K_a加密交易指令P和$Hash_a(P)$得到$E(P,Hash_a(P))$，之后用随机挑选的混币中心的公钥SK_m加密对称密钥得到$SK_m(K_a)$，最后向该混币中心发送$E(P,Hash_a(P))$和$SK_m(K_a)$，并将服务费$M_0/2$发送到该混币中心押金地址。

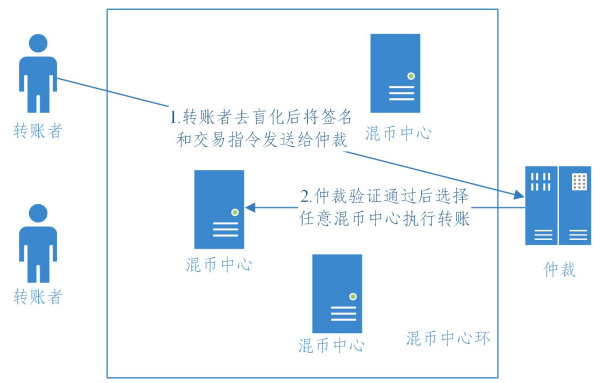

图3 仲裁认证转账指令的过程

Fig. 3 Process of arbitration certification transfer instructions

混币中心执行转账的过程如图4所示，具体步骤如下：

1)混币中心收到仲裁的转账指令后用自己的私钥解密得到K_a，然后用对称密钥解密$E(P,Hash_a(P))$得到P，$Hash_a(P)$，用仲裁公钥SK_a验证仲裁签名，通过后解析指令P，验证环签名$sign$对应的两个等式是否成立。然后查看公共的转账记录册中是否已经执行过转账，若已执行则拒绝转账。

2)若上述验证均通过，则直接向转账地址发送M比特币，并将假名和“已转账”登记在转账记录册中，同时保存转账交易记录用于违规处理时的验证。若某一过程验证不通过则拒绝此次转账请求。

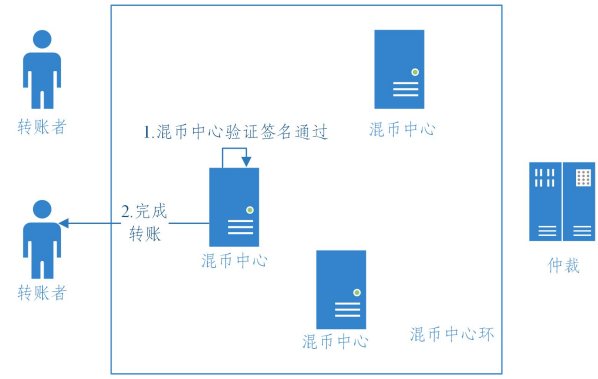

图4 混币中心执行转账的过程

Fig. 4 Process of mixing center executes transfer

由于接收钱和转账都是随机的，因此平均之后混币中心资金出入是平衡的。为防止混币中心因亏空无法转账，采用动态调整策略：多个混币中心可以都预存一定量的准备金并进行动态调整，规定若超过一定阈值则转给其他混币中心，若少于阈值则申请补足。混币中心退出时返还分配资金并从系统分配的押金地址取出所有资金(包括原本的押金和报酬)，也可以只取报酬继续提供服务。

若交易中某一过程无法顺利进行则进入审计阶段，若只是某一方计算错误导致交易梗阻，则重新执行梗阻前的操作。若发现存在恶意违规如转账者否认要求转账或者混币中心伪造转账、拒绝服务等问题，仲裁方通过分析找出违规的一方，随后对违规方进行处罚。如果违规的是转账者，由于转账者在要求转账前已经将比特币发送给混币中心了，可以没收转账者剩余的比特币同时将此转账者踢出并拉黑，不再为其提供服务。如果违规的是混币中心，由于混币中心在注册时提供了押金，因此可以没收其押金，并将其踢出系统。不管是转账者还是混币中心，进行违规操作都将得不偿失，因此本文系统可以很好地保证交易顺利进行。

本文方案中，仲裁只对转账指令进行认证，以确保转账指令的可靠性和不可否认性，仲裁本身也不能获得发送者地址-接收者地址之间的关联，不能获取交易隐私，因此不要求仲裁是忠诚的，但要求仲裁必须履行认证职责，一旦仲裁停止服务，混币系统就无法实施了。为了减少对仲裁的依赖性，可以考虑设置多个仲裁互相独立地工作，多个仲裁共享“已认证转账指令集”以避免用户重发同一个转账指令，从而防止用户重复转账。因此，一个仲裁停止服务并不会影响混币系统的

正常工作,而所有仲裁同时停止服务的概率极小,可以忽略。另一方面,多个仲裁也可以并行工作,分担任务,提高混币系统的工作效率。

4 方案分析

4.1 匿名性

本文方案中,交易发送者选定一个随机数作为自己的假名,然后将资金和盲化假名转给随机选出的一个混币中心。混币中心利用环盲签名技术返回一个环盲签名给发送者,发送者去盲化得到对假名的环盲签名。随后,发送者将签名和转账指令一起(通过仲裁中转)发给随机选出的另一个混币中心。混币中心验证环盲签名有效,进而执行转账指令给接收方。需要注意的是,环盲签名是对于发送者假名的签名,所以混币中心只能够得到假名而无法确定真正的发送者的身份(或者地址)。换句话说,混币中心无法获取交易发送者地址-接收者地址的关联,保护了交易隐私。另一方面,当仲裁接收到发送者的转账指令时,它只能看到假名和转账指令(含接收者地址),而得不到任何发送者地址的信息,所以,仲裁同样无法获取交易发送者地址-接收者地址的关联。因此,本文方案中交易的匿名性得到了充分保证。

4.2 不可否认性

在本文方案中,发送者发出的转账指令都必须先经过仲裁认证。仲裁对转账指令进行签名,再发送给混币中心。当混币中心收到转账指令后,它首先验证仲裁签名,签名验证通过之后才执行转账指令。如果发送者否认自己曾经发出转账指令,混币中心只需出示仲裁签名就可以证明发送者在说谎。另一方面,仲裁对于每一个假名的转账指令都只签名认证一次,发送者无法重复转账。所以,本文方案杜绝了发送者实施的"预存一笔资金,多次花费"的欺骗行为。

4.3 不可伪造性

常见的盲化混币方案中,由于发送者隐藏了自己的身份,因此它难于证明某一笔交易的转账指令是自己发出的。后果是不忠诚的混币中心可能会伪造一条转账指令,声称是某个假名(发送者)发出的,从而拒绝为该假名(发送者)再服务,达到侵吞发送者的预存资金的目的。

在本文方案中,每一条转账指令都必须由仲裁签名认证,而混币中心无法伪造仲裁的签名,且它伪造的转账指令是无效的。所以,混币中心伪造转账指令的欺骗行为是不可能成功的。

4.4 防 Dos 性

在许多混币技术中,攻击者进行 DoS 攻击主要通过冒充用户对混币中心发送大量请求,且拒绝配合转移资金来干扰混币中心对合法用户提供服务。在本文方案中,用户请求服务时,获取混币中心签名前需要先将资金转给混币中心且每笔交易需要向混币中心提供相应报酬。攻击者如果进行 DoS 攻击,则需要付出巨大经济代价,得不偿失。

4.5 安全性分析

本文方案中,即使恶意节点获取到交易过程的信息,但是由于交易全程进行匿名通信,恶意节点没有密钥,无法得到明文信息。接受转账的混币中心只知道盲化后的用户假名信息和发送地址信息,执行转账的混币中心只知道用户的假名信息和接收地址信息,所以混币中心无法知道转账方-接收方的关联信息,仲裁同样只知道用户的假名信息和接收地址信息,也无法获取转账方-接收方的关联信息。因此本文方案的安全性可以得到保证。

4.6 与其他混币方案的对比分析

在 Mixcoin 方案中,转出方用户不再直接将比特币转账给接收方用户,而是先将比特币发送到一个中央混币服务器,混币服务器将多笔交易混合后分别发送给接收方。为了提高匿名性,Mixcoin 要求多用户使用相同金额进行混币。通过混币服务器的混合处理,可以隐藏交易的输入地址和输出地址之间的联系,提高了攻击者分析交易的难度,保证了用户交易隐私。

Blindcoin[17] 针对 Mixcoin 在匿名性上的弱点,使用盲签名对其进行了改进,用户对输出地址采用盲签名,使混币中心能提供混币服务的同时不会获取交易输入地址与输出地址的映射关系,同时混淆方也不能打破用户的匿名。但 Blindcoin 降低了 Mixcoin 对于外部实体的匿名集大小。

Maxwell 提出了另一种混合比特币的方案——CoinJoin。CoinJoin 方案构建了一种交易:让数百个交易发起者同时向数百个交易接收者转一定数额的比特币。当用户要求的输出地址出现在输出地址列表时,用户才会对交易进行签名。攻击者无法通过这笔交易来证明这几百个地址的控制者间的存在联系,因为交易的参与方互相不认识,只是恰好在同一时间发起交易而已。但是该方案需要用户自发寻找其他同时发起混淆交易的用户。

Coinjoin 无法避免攻击者加入导致破坏交易混合,为了解决这一问题,Ruffing 等[18] 提出了更好的混合系统 CoinShuffle。CoinShuffle 方案的灵感源于 Coinjoin,最大的技术创新是引入纠查机制,每次混合失败都能找到恶意节点,用户可以避开恶意节点进行下一轮操作。Coinjoin 允许多笔交易输入合并构成一笔交易,当用户要求的输出地址出现在输出地址列表时,用户才会对交易进行签名。该协议遵循:一组用户共同创建一个混合交易,并且每个用户可以独自确认自己不会丢失金钱,一旦受到欺骗,用户拒绝对交易进行签名。

上述方案都存在不同程度的问题,影响交易或者隐私保护。Mixcoin 方案存在隐私泄露和资金被盗取、混币方拒绝服务等问题,虽然 Blindcoin 方案解决了 Mixcoin 方案中的隐私问题,但依旧存在资金被盗取、拒绝服务等交易问题。Coinjoin 方案存在攻击者破坏混合问题以及需要自发寻找其他用户参与混淆交易且需要用户同时在线,这个条件极难实现,CoinShuffle 解决了攻击者问题,但也需要混淆时参与者同时在线。

在最新的混币研究中,Wang 等[19] 提出了基于同态加密的区块链混币方案,该方案结合同态加密算法发起验证区块链的匿名交易,保护了用户身份隐私和交易隐私,但交易过程存在违规操作的风险。Yu 等[20] 提出了可追溯的比特币混淆方案,该方案引入可信第三方来监管用户与服务商行为,提高了交易安全性,但是依赖于可信第三方。Song 等[21] 提出基

于中间人的区块链混币机制，采用随机分组和选取中间人的方式实现输出地址的高效传递，在保障隐私的同时缩短了交易运行时间，但仍然存在攻击者扰乱交易的情况。因此，本文提出了保护更为全面完整的方案。

本文方案是在 Mixcoin 方案的基础上实现比 Blindcoin 改进更好的一种优化方案。本文方案解决了中心化混合方案存在的资金盗取和拒绝服务问题以及去中心化混合方案需要多用户同时在线且混合条件难以实现的问题。本文方案使用环盲签名对交易过程进行改进，使用户和混币中心双方都不知道对方的身份，提高匿名性，同时使用仲裁来监管交易的顺利进行，防止双方中的任意一方做出违规操作。

上述方案的对比具体如表 2 所列。

表 2 方案对比

Table 2 Scheme comparison

方案	分类	技术	方案总结
Mixcoin	中心化	混币中心	不可链接；安全性受混币中心影响；存在资金盗取，拒绝服务问题
Blindcoin	中心化	盲签名改进 Mixcoin 方案	不可链接；保护隐私；存在资金盗取，拒绝服务问题
Coinjoin	去中心化	混合交易信息	不可链接；攻击者会破坏混合；需要参与用户同时在线
CoinShuffle	去中心化	纠察机制改进 Coinjoin 方案	不可链接；可以找到恶意节点并在下次交易时避开；需要参与用户同时在线
本文方案	中心化	环盲签名改进 Mixcoin 方案同时引入仲裁机制	不可链接；保护隐私；解决了资金盗取、拒绝服务问题；无需用户同时在线

4.7 与非混币方案对比分析

混币方案可以有效保护交易用户的身份隐私，但是不能保护交易金额隐私。为了规避这种风险，本文方案中，每一个用户预存在混币中心的资金是相同的固定金额，每一次用户转账指令的交易金额都是一样的，从而避免了交易金额隐私的泄露。如果用户希望的转账数额不同于方案规定的固定金额，则用户可以分几次转账。因为每一次用户都是“预存资金在混币中心＋重新获取环盲签名”，所以无论是混币中心还是第三方攻击者都无法将用户的两次转账联系起来，也就是说，不可能获取用户交易金额隐私。本文方案的缺点是用户需要多次预存和多次转账，成本较高。

利用零知识证明、同态加密等技术可以更好地保护交易隐私，然而，目前已有的类似方案（如零币等）都要求对传统的区块链交易结构及交易验证方法进行修改，因而不能适用于比特币、以太坊等传统区块链系统，只能应用于为此新建的区块链系统。如何在不修改现有区块链交易结构的前提下应用零知识证明、同态加密等技术来保护用户交易隐私，是一个重要的研究方向。

5 实验结果与分析

5.1 实验环境及参数配置

硬件环境：CPU 为 Intel(R) Core(TM) i5-9300H，主频为 2.40GHz，内存为 16.0GB，操作系统为 Windows 10 家庭中文版。实验的开发工具：IntelliJ IDEA Community Edition 2021.3，jdk-16.0.1，编程语言为 JAVA。

5.2 实验结果

实验模拟由 N 个用户、M 个混币服务器和 1 个仲裁组成的网络。系统初始化完毕之后，每一个用户随机产生转账指令发给仲裁，仲裁认证后再发给一个随机选择的混币中心。根据方案设计，定义从用户发出转账指令到混币中心验证转账指令合法，可以执行转账交易的时间为混币系统平均响应时间。

图 5 展示了平均响应时间随用户数量增长的变化趋势，可以看到：

1）当混币中心的个数确定时，平均响应时间随着用户数的增长而呈增长趋势。这是因为随着用户数量的增长，仲裁和混币中心的任务量随之增加，仲裁对用户的转账指令的认证时间和混币中心对转账指令的验证时间也相应增加。此外，在用户数量确定的情况下，混币中心的数量越多，平均响应时间越短。原因是执行转账指令的混币中心是在 M 个混币中心里随机选出的，相应地，验证转账指令（以及执行转账交易）的任务也是随机分配给所有混币中心的，因此，混币中心的数量越多，多个中心并行执行任务的速度就越快，系统平均响应时间就越短。

2）随着用户数量的增长，平均响应时间始终近似线性增长，没有出现平均响应时间急剧增长导致系统效率急剧下降甚至瘫痪的情况，说明本文方案具有较好的稳定性和可扩展性。

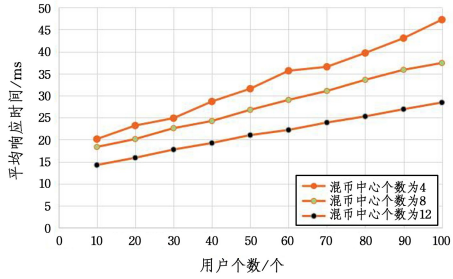

图 5 平均响应时间随用户数量增长的趋势

Fig. 5 Trend of average response time increasing with the growth of the number of users

图 6 为本方案与其他混币方案响应时间的对比。

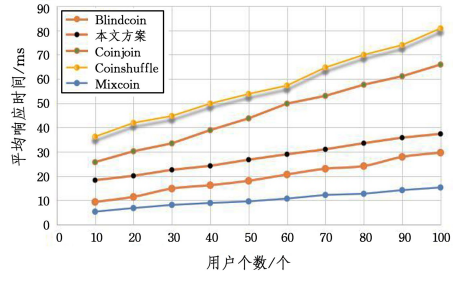

图 6 本文方案与其他混币方案响应时间的对比

Fig. 6 Comparison of response time of the proposed scheme and other coin mixing schemes

仅以平均响应时间这个指标而言，本文方案因为引入了仲裁，会花费比简单的混币方案更多的时间，但仍然短于那些复杂的混币方案。而且，本方案可以防止用户否认转账和混币中心伪造转账，这是相对于其他方案的最大优势，从而说明本系统具备实用性。

5.3 实验优化

依据用户数量及响应时间实验数据，用户数量一定时，混币服务器越多，响应时间越短，但是当混币服务器很多时，就会存在许多混币服务器无法参与混币服务获取报酬的情况。因此，当用户数目一定时，设置合适的混币服务器数量，以实现响应时间短且混币服务器的参与率高。若需最大化利用混币服务器，则减少混币服务器数量；若需快速响应，则增加混币服务器数量。

5.4 实验可扩展与实际部署

本文方案中，用户的数量和混币中心的数量均可以根据实际需要增加，实验数据表明，系统的平均响应时间随着用户数量的增长近似呈线性增长，同时平均响应时间随着混币中心数量的增加而下降。混币系统不会出现用户数量增长导致平均响应时间急剧上升甚至工作陷入瘫痪的现象，因此系统具有良好的可扩展性。

另一方面，本文方案只需要所有用户、混币中心、仲裁均拥有一个区块链账户（及对应的公钥-私钥对）。所有混币中心公布自己的区块链地址，仲裁公布自己的公开密钥。所有混币中心在逻辑上组成一个环，每一个混币中心实施环盲签名时，只需要使用系统为其分配的环成员签名密钥，并不需要其他混币中心的配合。换句话说，每一个混币中心都是独立工作的。因此，本文方案的实际部署非常简单，消耗资源很少。

结束语 本文方案很好地解决了比特币交易过程中的隐私保护问题，在传统混币技术的基础上实现进一步匿名，让混币中心也无法获取交易双方地址的关联性；同时混币中心也进行匿名，用户只知道混币中心为自己提供服务，但不知道具体是哪个混币中心。此外，本文方案通过仲裁的参与，保证了混币中心不能伪造用户的转账指令，用户不能否认自己的转账指令和不能重复转账。由此，用户可以在顺利完成交易的同时保证隐私不被泄露。

本文方案虽然很好地保护了用户隐私，但需要依靠可靠仲裁，这无疑加大了混币成本。未来将继续深入研究不需要仲裁的方案，也可以探索利用零知识证明、同态加密等技术实现交易隐私的保护。

参 考 文 献

[1] CHRIS B, ADAM W. Bitcoin ringing the bell for a new asset class [EB/OL]. http://research. ark-invest. com/bitcoin-asset-class.

[2] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. https://bitcoin. org/bitcoin. pdf.

[3] YUAN Y, WANG F Y. Blockchain: The state of the art and future trends [J]. Acta Automatica Sinica, 2016, 42(4): 481-494.

[4] AU M H, LIU J K, FANG J B, et al. A new payment system for enhancing location privacy of electric vehicles [J]. IEEE Transactions on Vehicular Technology, 2014, 63(1): 3-18.

[5] CONTI M, KUMAR E S, LAL C, et al. A s-urvey on securityand privacy issues of Bitcoin [J]. IEEE Communications Surveys & Tutorials, 2017, 20(4): 3416-3452.

[6] WANG H, SONG X F, KE J M, et al. Block-chainand privacy preserving mechanisms in cryptocurrency[J]. Netinfo Security, 2017, 17(7): 32-39

[7] WANG Z H, ZHANG S L, JIN S, et al. Survey on privacy preserving techniques for blockchain[J]. Chinese Journal on internet of Things, 2018, 2(3): 71-81.

[8] CHAUM D L. Untraceable electronic mail, return addresses, and digital pseudonyms [J]. Communications of the ACM, 1981, 24(2): 84-90.

[9] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: Anonymity for Bitcoin with AccountableMixes[M] // Financial Cryptography and Data Security. Berlin: Springer, 2014: 486-504.

[10] MAXWELL G. Coinjoin: Bitcoin privacy for the realworld[EB/OL]. https://bitcointalk. org/index. php?topic=279249. 0.

[11] DIFFIE W, HELLMAN M E. New directions in cryptography [J]. IEEE Transactions on InformationTheory, 1976, 22(6): 644-654.

[12] CHAUM D. Blind signature for untraceable payments [C] // Proceedings of CBYPTO. Berlin: Springer, 1982: 199-203.

[13] RIVEST R L, SHAMIR A, TAUMAN Y. How to leak a secret [C] // ASIACRYPT 2001. 2001: 552-565.

[14] CHAUM D, VAN H E. Group Signatures[C] // LNCS. Berlin: Springer, 1991: 257-265.

[15] CAO G. Research on blind signature and ring signature[D]. Qinghai: Qinghai Normal University, 2010.

[16] PENG J X, ZHAO P, HUI E X. Analysis of AES and RSA Hybrid Encryption Algorithm in Blockchain Applications[J]. Electronic Technology & Software Engineering, 2021(2): 222-224.

[17] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for bitcoin[C] // International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 112-126.

[18] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: practical decentralized coin mixing for Bitcoin[C] // European Symposium on Research in Computer Security. Cham: Springer, 2014: 345-364.

[19] WANG D, LI Z, XIAO B B. Blockchain Coin Mixing Scheme Based on Homomorphic Encryption [J]. Computer Science, 2024, 51(3): 335-339.

[20] YU Q L, LU N, SHI W B. Traceable Mixing Scheme for Bitcoin [J]. Computer Science, 2021, 48(11): 72-78.

[21] SONG J H, LI Z K, ZHANG B C. Coin mixing mechanism in blockchain based on intermediator [J]. Application Research of Computers, 2022, 39(3): 868-873.

FANG Zhipeng, born in 2001, postgraduate. His main research interest is blockchain privacy protection.

LI Xiaoyu, born in 1974, Ph.D, associate professor, is a member of CCF (No. 15010M). His main research interests include blockchain technology and information security.

（责任编辑：何杨）