RSCoinJoin:基于环签名的混币方案

桂开叶 李盛恩
(山东建筑大学计算机科学与技术学院 山东 济南 250100)

摘 要 针对混币方案 CoinShuffle 中完成混币交易耗时较多的问题,提出一种基于环签名的混合方案。用户公告参与混币的输入、输出地址并由最后一个用户将地址集合发布到网络中;用户确认自己的输出地址是否在集合中,如果存在则发起混币交易,并对交易进行签名,直到最后一个用户签名后将交易发布。实验结果表明,RSCoinJoin 在参与混币用户数是 50 时,完成一笔交易的平均时间为 2 s,比现有的混合方案速度更快。

关键词 区块链 匿名性 不可链接性 混币

中图分类号 TP301 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2024.03.017

RSCOINJOIN: MIXED-CURRENCY SCHEME BASED ON RING SIGNATURE

Gui Kaiye Li Sheng'en
(*School of Computer Science and Technology, Shandong Jianzhu University, Jinan 250100, Shandong, China*)

Abstract In order to solve the problem that CoinShuffle takes much time to complete the mixed-currency transaction, a mixed-currency scheme based on ring signature is proposed. The user announced the input and output addresses of the mixed currency, and the address set was published on the network by the last user. The user confirmed whether his output address was in the collection, initiated a mixed-currency transaction if it existed, and signed the transaction until the last user signed and published the transaction. The experimental results show that when the number of users of RSCoinJoin is 50, the average time to complete a transaction is 2 second, which is faster than the existing hybrid scheme.

Keywords Blockchain Anonymous Unlinkability Mixed-currency

0 引 言

为了实现去中心化的匿名交易,摆脱信任机制的限制,比特币首次登上了去中心化的舞台[1]。此后,区块链技术不仅在金融领域快速发展,也应用到各个领域中。例如在医疗领域有 Mettler[2]将区块链技术应用于公共医疗保健管理;化学工业中 Sikorski 等[3]挖掘了区块链技术在支持和提高效率方面的潜力,并指出了该技术对工业生产中机器对机器(Machine-to-Machine,M2M)的促进作用;Kim 等[4]通过在以太坊区块链平台上应用可追溯性约束,指出区块链在供应链上的应用价值;教育领域中 Sharples 等[5]实现了智力工作和相关声誉奖励的永久性分布式记录。

比特币系统去中心化的特点要求系统拥有强安全性。安全性要求系统在保证资金安全的同时还应该保证用户信息的匿名性。区块链的匿名性有两方面:(1) 假名性,用户使用该系统时不会直接暴露真实身份;(2) 不可链接性,没有人能够通过交易信息分析出地址与地址之间、交易与交易之间和地址与用户之间的关系[6]。比特币系统中公私钥的生成采用非实名制,并且一个用户可以拥有多对公私钥。因此,比特币拥有很好的假名性。但是 Ron 等[7]利用比特币完整的历史记录,分析了其相关交易图的许多统计属性,发现相关联的用户试图通过事务图中许多长链和分叉合并结构来隐藏交易事实。此外利用"污点"分析、跟踪付款、IP 地址监控和网络蜘蛛等方式很容易破坏比特币的不可链接性,即比特币系统无法实现不可链接性。

收稿日期:2020 - 10 - 17。**桂开叶**,硕士生,主研领域:区块链匿名性研究。**李盛恩**,教授。

所以,保持交易的不可链接性是加强比特币匿名性的关键。

目前增强交易不可链接性的主流方法有混币(Mixing)、替代币(Altcoin)和加密交易(Confidential Transaction,CT)。但是对于类似比特币这样公开所有交易信息的系统来说,基于混币思想的保护方案更具针对性。

混币按照是否有第三方信任存在可分为中心化混币和去中心化混币。中心化混币中存在混合器。参与混合的每个用户以加密形式发送一个新的地址给混合器,混合器对新地址进行解密并随机打乱地址集合,然后将比特币发送到每个输出地址。中心化混合交易被应用于实践,但它们存在两个严重的缺点:(1) 混合器可能会偷钱,而且永远不会还给用户;(2) 混合器知道输出地址属于某个输入地址。因此,用户的匿名性依赖于混合过程无日志记录或不公开输入和输出地址之间的关系。随着中心化混合偷币恶性事件发生,去中心化的混合方案开始出现并被应用。

去中心化混币的实现方式有两种:(1) 多用户参与,指在同一个系统中,同一笔交易有多个用户参与,即一笔交易中包含多个输入和输出;(2) 两个用户交易,并与不同的用户发生多次交易。无论是一轮交易还是多轮交易,其目的都是切断输入地址和输出地址之间的对应关系,使恶意节点无法获知地址与地址之间的联系,或者很难从交易数据中分析出地址之间的关系,从而增强隐私性。

去中心化混币仍然存在女巫攻击、DoS 攻击等诸多安全威胁,并且为了提高安全性,加密解密操作又带来了完成一笔混合交易的效率问题。正如张奥等[8]从资产安全性、是否抵抗 DoS 攻击、是否抵抗女巫攻击和隐私性等方面对多个混币方案进行分析得出的结果一样。针对上述问题,本文主要研究去中心化混币方案对不可链接性的保护以及如何提高交易效率。

1 CoinShuffle

1.1 方案概述

为了确保可验证性,CoinShuffle 协议遵循 CoinJoin 范式[9]:一组用户共同创建一笔混合交易,每个用户都可以单独验证自己在进行该交易时不会赔钱。并且在存在欺诈的情况下,被欺骗的用户可以拒绝签署交易。

CoinShuffle 主要分为 3 个阶段,包括公告(announcement)、洗牌(shuffling)和交易验证(transaction verification),只有协议因为不合法因素没有成功运行,才进入一个额外的纠错(blame)阶段。协议假设每个参与者提供的地址持有的比特币数量相等,该地址将成为混合交易中的一个输入地址,来自该参与者的每条消息都应该使用该地址的私钥进行签名。下面是每个阶段的概述。

1) 公告。每一个参与者生成一对新的临时公钥和私钥并广播公钥,公钥用于密文解密,且该公钥和私钥仅在本次混合交易中有效,下一次混合交易开始时将重新生成。

2) 洗牌。每个参与者创建一个新的比特币地址,该地址是他在混合交易中的输出地址。混币交易中,所有参与者被编号,即 $1,2,\cdots,N$。参与者执行洗牌操作:参与者 i 希望接收到参与者 $i-1$ 的密文,收到密文后,先使用参与者 $i-1$ 的公钥进行解密,再将自己的输出地址添加到输出地址集合并进行洗牌操作,即无规则地打乱输出地址集合,并使用参与者 $i+1$ 的公钥来创建输出地址的分层加密。然后将密文进行广播,参与者 $i+1$ 收到密文后继续上述操作,直到参与者 N 完成上述操作。

3) 交易验证。每个参与者都可以单独验证他的输出地址是否在集合中。若参与者 i 确定自己的输出地址存在,则创建一个尚未签名的混合交易,并用他的比特币签名密钥在交易上签名,并广播签名。接收到所有其他参与者的签名后,每个参与者都能够创建一个拥有完整签名的混合交易。因此,该混合交易是有效的,可以提交到比特币网络。

4) 纠错。在上述阶段的每个步骤中,每个参与者检查所有其他参与者是否遵守协议。如果某些参与者违背了协议,诚实的参与者会广播违背信息,协议将进入纠错阶段,然后执行该阶段的操作对行为不端的参与者进行识别并排除。将行为不端的参与者排除之后协议继续运行。在三种情况下,参与者会进入纠错阶段。第一,如果某个参与者在其输入地址中没有足够的比特币来执行混合交易,或者在混合协议完成之前,他提前将输入地址中的比特币消费了,则进入纠错阶段,在这两种情况下,比特币网络都为不当行为提供了证据;第二,如果洗牌没有正确执行,则进入纠错阶段,在这种情况下,参与者可以广播他们的临时公钥以及他们收到的密文。该信息允许每个参与者重放其他参与者的计算结果,并暴露行为不合法的一方;第三,参与者在协议的广播中出现不合法行为,例如在公告阶段向不同的参与者发送不同的公钥,所有的参与者在创建混合交易之前交换消息,以确保没有不合法参与

者,如果存在不合法行为,则进入纠错阶段。由于所有协议消息都是加密的,因此可以识别出不合法的参与者,两个不同但属于同一发送者的密文提供了不合法行为的证据。

上述阶段的执行过程如图 1 所示。本次交易有 Alice、Bob 和 Charlie 参与,他们分别被编号为 1、2、3,$N=3$,然后他们各自生成一对公私密钥(如图 1 所示,第一列为私钥,第二列为公钥),并且广播他们的公钥和输入地址。公告阶段结束以后每个人拥有自己的公私钥和其余 $N-1$ 个参与者的公钥,还有 N 个人的输入地址。当参与者收 N 个输入地址后,进入第二阶段。在该阶段中,从 Alice 开始,将输出地址 A' 使用 Bob 的公钥加密并广播,该密文只有 Bob 才能打开,Bob 收到以后将密文解密,再加入自己的输出地址 B',并打乱该输出地址集合,再使用 Charlie 的公钥对该集合进行加密并广播,当 Charlie 收到密文后重复解密洗牌操作,唯一不同的是 Charlie 是编号为 N 参与者,所以 Charlie 使用自己的私钥对集合进行加密并广播。阶段二结束以后,所有参与者验证自己的输入地址和输出地址是否在集合,如果没问题则创建混合交易并附上自己的签名并广播该交易(该交易没有所有输入地址的签名,不是合法的),当收到所有参与者的签名后,可以成功创建混合交易并发布到比特币网络中。相反,如果一个输出地址丢失,如图 1 中第 3 个步骤 Transaction Verification(attack)列表中的第三行所示,D'已经取代了 C',所以 Charlie 发现自己的输出地址不在集合中,Charlie 拒绝广播交易签名,交易无法收到地址 C 的签名,所以不能成为合法交易,参与者 C 进入纠错阶段,找出哪些参与者违背了协议规定,找出以后将违反规定的参与者剔除并继续混合操作。

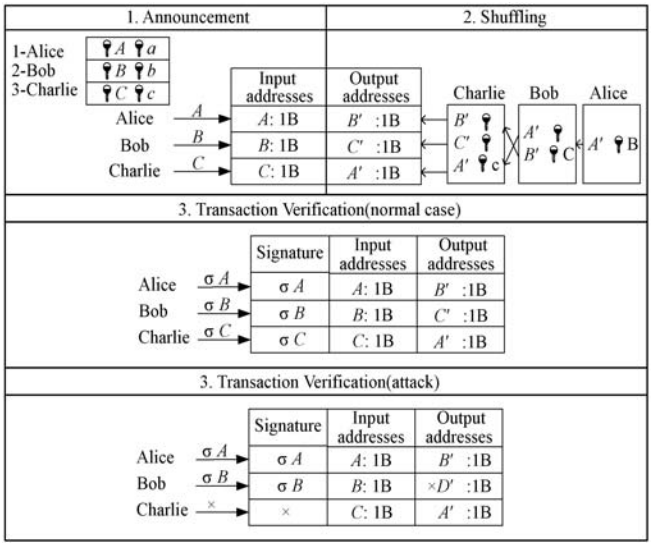

图 1　CoinShuffle 概述

1.2　优　势

CoinShuffle 的优势主要体现在安全性和系统性能两方面。如表 1 常见指标所示,CoinShuffle 实现了三层含义的不可链接;混币交易发布以后和比特币网络普通交易一样可验证;有较好的鲁棒性,在有恶意节点参与的情况下,混币交易仍然可以继续;可防止双花问题的出现,比特币网络中矿工的验证可以使得不存在于 UTXO 的输入地址无法进行交易,或者金额低于指定金额的交易不被认可;通过纠错阶段,可以防止恶意节点发起 DoS 攻击对混币交易造成破坏;自定义混币金额是目前为止,所有混币方案都没有实现的,但是在 CoinShuffle 中可以提供大于混币金额的输入地址,剩余的比特币返回到参与者指定的地址。

表 1　安全性指标

指标	是否实现	指标	是否实现
不可链接性	√	防止双花	√
可验证性	√	防止 DoS 攻击	√
鲁棒性	√	自定义混合金额	×

混币交易的加入对比特币系统的影响如表 2 所示。兼容性:CoinShuffle 协议的部署不需要对比特币协议或数据格式进行任何更改,成功运行 CoinShuffle 协议产生的混币交易同当前比特币的合法交易结构一样。因此,CoinShuffle 于比特币系统兼容。交易费:混币交易是参与者之间自愿达成的协议,混币过程不需要任何的交易费用。网络开销:协议执行成功后,参与者共同创建一个比特币交易,只有一个交易会被发送到网络中,并且该交易必须存储在公开的区块链中,还必须经过网络中所有全节点的验证。因此,CoinShuffle 的执行只在比特币网络节点的存储和计算方面引入了最小的开销。效率较高:直到 CoinShuffle 出现为止,所有的混币方案中,CoinShuffle 是能够解决 DoS 攻击并且效率较高的方案。

表 2　系统性能指标

兼容性	交易费	网络开销	效率
兼容	无	小	较高

1.3　挑　战

虽然 CoinShuffle 能极大地保证资金安全,但是交易的速度和极端情况的出现也暴露出它有待提高的方面。本节通过对 CoinShuffle 在效率和自定义金额处理两方面的分析,总结了 CoinShuffle 协议两个可完善的方面。

图 2 为总运行时间,其中参与者从 5 人到 50 人不等,由实验结果能够得到这样的信息:在局域网中,50 个参与者在没有恶意参与者的情况下创建一笔混币交易大约需要 40 s,而在广域网中,完成交易大约需要 3 min。从参与者人数和完成时间的变化情况可以得出:在全局网络中,时间随参与者的变化而指数倍增加。并且执行时间是在最理想的情况下,即没有恶意参与者的运行环境中,所以混币交易只经过公告、洗牌和交易验证就大约需要 3 min。

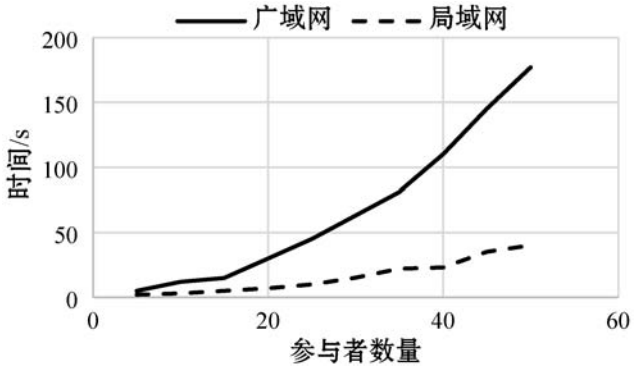

图 2 运行时间

广域网中交易的完成时间在很大程度上受限于网络状况,不便进行分析,但是在局域网中,排除了网络实际状况的干扰,实验环节并没有经过纠错阶段,但是混币还是需要 40 s。原因在于阶段二的洗牌操作将使用一种复杂的混合解密网络。CoinShuffle 协议中的所有消息都是通过密文的方式传递,并且所有参与者的加密解密操作都是顺序执行。

假设每一位参与者进行加密和解密所用时间都相等,共有 n 个用户参与。则在洗牌操作中,除第一个加密者以外,其他参与者将经过两层循环:第一层,$n-1$ 个参与者顺序执行解密和加密广播操作;第二层,参与者 i 进行 $i-1$ 次解密和 i 次加密。随着参与者数量的增加,洗牌操作的时间复杂度为 $n\log n$,这与实验结果相吻合。由于混合交易的安全性取决于参与者集合的大小,参与者越多,安全系数越高,但是付出的时间也越多。

CoinShuffle 中允许输入地址拥有的比特币数量可以大于混合金额,并且在阶段 2 提供返回地址。这样的处理可能会出现如图 3 所示的极端情况,Alice、Bob 和 Charlie 三人参与混合交易,本次混合交易的比特币数量是 1,但是 Alice 和 Bob 都提供了数量为 1 的输入,Charlie 的输入为 3,在输出地址中,通过简单分析就可以知道地址 D' 和地址 C 之间属于同一个用户的关系。所以,在固定混合交易金额的交易中,严格要求输入金额更能保持不可链接性。

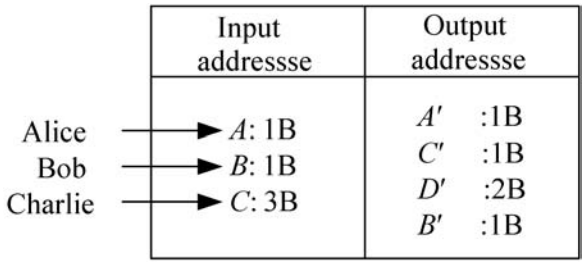

图 3 输入地址金额大于混合金额

2 RSCoinJoin

RSCoinJoin 遵循 Coinjoin 范式,即多个用户共同创建一笔混合交易,一笔混合交易有多个输入地址,多个输出地址;每个用户参与混合的金额相等并且可以确认自己不会有丢失资金;用户在资金不安全的情况下可以拒绝对交易进行签名。本节介绍 RSCoinJoin 的完整过程,包括公告、信息确认和标记三个步骤。

2.1 公 告

用户参与混币交易之前先找到目标金额的混合信息,所有想要混币的用户建立通信链,形成一个成员链,链中成员的信息确认顺序是交易前就规定的,并且每个成员生成一对新的公私钥,并将公钥广播到网络中,所有成员收集网络中所有成员的公钥并保存在本地。

然后成员使用密文的方式分别广播自己的输入、输出地址。RSCoinJoin 为了隐藏消息来源以及广播者的身份,阻止用户和地址之间产生联系,公告阶段采用环签名[10-11]的方式广播输入、输出地址,具体过程如下。

假设要签名的消息为 m,这里的 m 是输入地址或者输出地址,s 是成员链中的签名者(即第 s 个成员),则 s 的公钥为 P_s,私钥为 P_s,成员的数量为 n,其中 n $(n>s\geqslant 1)$。所有环成员的公钥集合为:

$$\{P_1,P_2,\cdots,P_n\} \tag{1}$$

1) 计算环签名。

(1) 获取对称加密密钥。签名者 s 计算对称密钥 k,即需要签名的消息 m 的 Hash 值:

$$k=h(m) \tag{2}$$

(2) 选取随机数 v。签名者 s 从 $\{0,1\}^b$(b 是 Hash 函数结果的位数)中随机且均匀地选取 v 的值。

(3) 选择随机数 x_i。签名者 s 为其他成员从 $\{0,1\}^b$ 中随机且均匀地选取 x_i,其中 $1\leqslant i\leqslant n, i\neq s$,并计算出:

$$y_i=g_i(x_i) \tag{3}$$

(4) 计算 y_s。根据定义,给定其他输入值,对于满足下列方程的 y_s 有一个唯一解,式(4)中 y_s 是未知数。

$$C_{k,v}(y_1,y_2,\cdots,y_{s-1},y_s,y_{s+1},\cdots,y_n)=v \quad (4)$$

(5) 计算 x_s。签名者 s 根据 g_i^{-1} 函数计算 x_s:

$$x_s=g_s^{-1}(ys) \quad (5)$$

(6) 输出环签名。消息 m 的环签名是一个 $2r+1$ 元组:

$$(P_1,P_2,\cdots,P_n;v;x_1,x_2,\cdots,x_n) \quad (6)$$

2) 验证环签名。

(1) 计算 y_i。验证者为 $i=1,2,\cdots,n$ 计算 y_i:

$$y_i=g_i(x_i) \quad (7)$$

(2) 获取对称加密密钥。验证者计算对称密钥 k,即被签名的消息 m 的 Hash 值:

$$k=h(m) \quad (8)$$

(3) 验证环方程。计算式(9)是否成立,若成立,则验证成功,否则拒绝接收消息 m。

$$C_{k,v}(y_1,y_2,\cdots,y_n)=v \quad (9)$$

链中的成员使用自己和其他人的公钥对输入、输出地址进行加密并广播,其他成员收到密文后使用公钥对信息解密,将收集的所有输入、输出地址保存到本地,最终由链尾成员在本地将输出地址随机打乱后,广播输入、输出地址集合。集合被广播后,除非进入标记阶段,否则集合内容无法被修改。

图 4 是一个 6 人参与混合金额为 1 个比特币的混合交易的公告阶段。首先 6 个人分别被编号为 1、2、3、4、5、6,组成一条通信链,然后他们各自产生公私钥对并广播公钥,其余成员收集其他人的公钥保存在本地。然后 6 人分别广播输入、输出地址,最终由成员 6 公布收集到的地址集合如图 4 所示,其中:input addresses 是输入地址,output addresses 是输出地址。由于接收后的地址被成员 6 随机打乱了,所以不能确定公布的地址对之间是否是一一对应的。

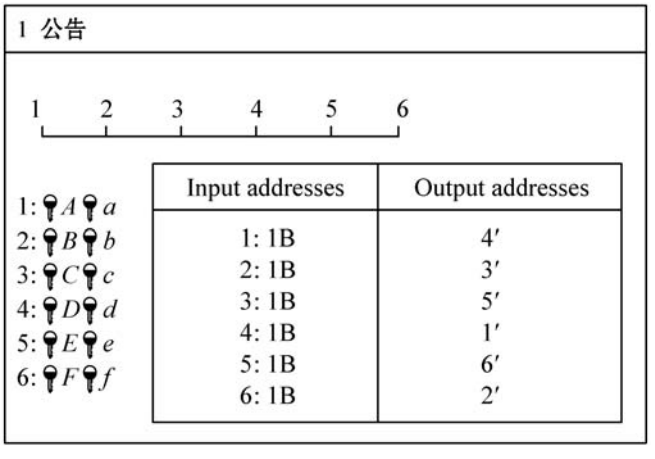

图 4　公告

2.2　信息确认

输入、输出地址集合公布后,从链头成员开始,链头成员确认自己的输入、输出地址是否在该集合中,如果存在,则创建不完整签名的混合交易,使用第二个成员的公钥进行加密并广播,即该交易只有链头成员的签名,是不合法的交易,并且该交易只有第二个成员可以打开。第二个成员收到密文后首先检查前一个成员提供的输入地址是否拥有规定的混合金额,再确认自己的输入、输出地址是否在集合中,若存在,则添加自己的签名并加密发送给下一位成员;若不存在,则报告自己的地址属于哪一种情况(Q_1,Q_2,Q_3),然后使用下一个成员的公钥对密文加密再将密文广播,所有成员 $i(i>1)$ 重复上述操作,当链尾成员 N 收到与集合中地址对数量相等的签名后,则将完整交易发布到网络中。

图 5 展示了混币过程没有恶意节点参加时的信息确认过程。首先成员 1 确认自己的地址,此时地址存在,则附上自己的签名,然后使用成员 2 的公钥将签名信息加密发送到通信链中,只有成员 2 可以打开。所以,成员 2 收到以后确认成员 1 提供的输入地址是否有 1B,此时成员 1 的地址中恰好为 1B,所以附上自己的签名并使用成员 3 的公钥进行加密并广播。

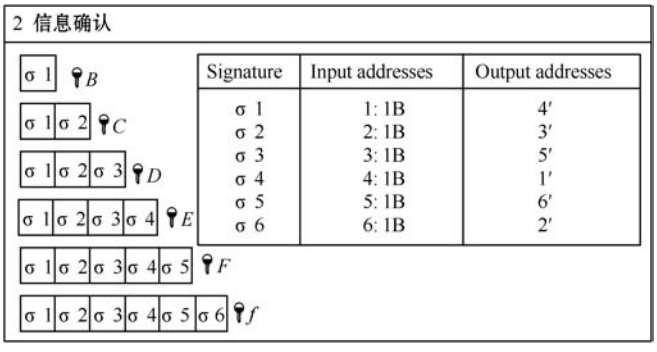

图 5　无恶意节点的信息确认

成员 3、4、5 重复成员 2 的操作,最终成员 6 收到所有人的签名,所有成员 6 加上自己的签名并使用自己的私钥对交易加密,当所有人收到以后,成员 1、2、3、4、5 共同验证成员 6 的地址是否拥有 1B,当成员 6 收到 5 个确认信息后,将交易发布到网络中。

信息确认阶段有两类情况,一是上述成员确认自己的输入、输出地址均在集合中的情况,混币交易正常进行。反之,则是自己的输入、输出地址不在集合中。这种不符合规定的情况一共有如下三种:

Q_1:输入地址存在,但是输出地址被替换。

Q_2:输入地址和输出地址均不存在。

Q_3:输入地址不存在,但是输出地址存在。

针对不同的错误报告(Q_1,Q_2,Q_3),由于签名和输入地址是一一对应的,但是输入、输出地址之间不是对应关系,所以它们问题的产生和解决办法如下:

Q_1、Q_2:成员 i 在这种情况下,输入地址存在,但是输出地址被恶意篡改了。输入、输出地址集合最终是由链尾成员 N 打包的,所以,为了确认链尾成员 N 是否行为合法,则成员 i 向所有成员(除链尾成员以外)请求一份他们收集到的输入、输出集合,若一半以上的成员收集到成员 i 的地址对,则成员 i 公布所有人的集合,并发起 Q_1 计数器,当所有成员确定成员 i 没有说谎时,对计数器进行加一操作,每个成员最多只能进行一次操作,当 Q_1 计数器大于 $N/2$ 时,链尾成员 N 将被排除在交易链之外。

Q_3:成员 i 在这样的情况下直接将交易进行加密转发即可,成员 i 将被排除在交易链之外。

2.3 标 记

交易正常发布时,输入地址的数量、输出地址的数量和签名个数三者相等。但是当数量不等或者地址被替换时,表示有恶意节点发起了攻击,或者参与者想退出交易。为了保证交易可以正常运行,此时应该进行类似于纠错这样的操作,将恶意的参与者公布并从交易链中剔除。

图 6 所示为标记阶段,当发起混币交易时,根据网络状况设计一个限时时间锁 T_{lock},要求所有的交易签名需要在 T_{lock} 时间内完成,一般 T_{lock} 略大于平均时间。在 T_{lock} 时间内交易签名数小于输入、输出地址对时,混币交易自动进入标记阶段,交易成为标记交易,标记交易将锁定交易内的内容。由于标记交易中拥有签名的输入地址被拥有者使用公钥加密,所以该部分的内容只有自己才可以打开,所以收到标记交易的成员打开交易对输出地址集合进行标记,即将自己的输出地址进行标记。当拥有打开权限的用户对输出集合标记以后,没有签名的输入地址和未标记的输出地址将被全部剔除,并由链尾成员发布标记交易。

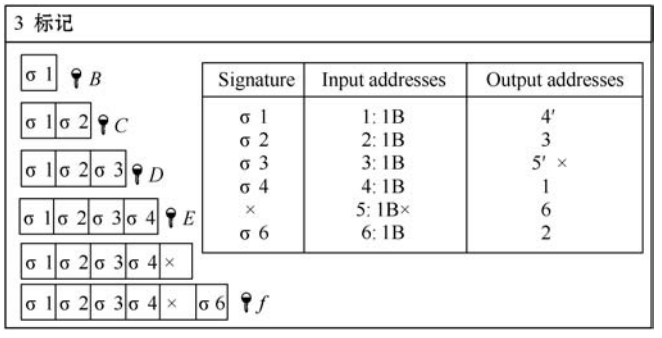

图 6 标 记

3 实验及分析

根据上述 RSCoinJoin 设计方案进行以下几个方面的实验及分析。

3.1 实验环境

操作系统:Windows 10-64 bit;编程语言:Java;开发环境:Eclipse,jdk1.8.0_231;加密 API:bcprov-jdk15;Hash 函数:MessageDigest 中的 SHA256;环签名方案采用基于 RSA 的签名方案。

RSCoinJoin 构建了区块链底层结构,实现了基本的 POW 机制。在实验中,为了进行实验对比,创建一个钱包(Wallet)代表一个参与者,即钱包数量就是参与者数量。

钱包拥有公钥(publicKey)和私钥(privateKey)。公钥为收款地址,私钥用来对交易进行签名,只有知道私钥的人才可以花费钱包中的钱。公私钥的产生使用 Elliptic Curve Cryptography 椭圆曲线算法。

3.2 不可链接性

在公告阶段中,所有的输入、输出地址对均采用环签名的方式广播,根据环签名隐藏消息发送方的特点,其余成员可以对密文进行解密,但是无法知晓该地址对来自哪一个成员。所以,无法将成员与地址建立联系。

信息确认过程中,所有成员对交易进行签名,由于交易从成员链第一个成员开始,每一次签名前每个成员都将随机交换输出地址的位置,所以我们能见到的输入地址和输出地址不是一一对应的关系,从而也就隐藏了输入、输出地址之间的对应信息,大家仅仅知道链上的成员参与了交易,并不知道签名者将资金转入了哪一个地址,所以破坏了地址与地址之间的链接性。

图 7 所示是一笔合法的混币交易,左边存放的是本次交易的输入地址,右边则存放的是输出地址,混币交易金额固定为 1,即每一个输入地址都拥有 1 的加密货币。

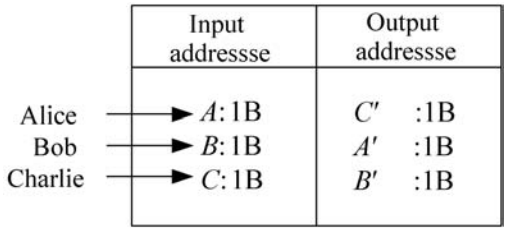

图 7 一次交易

Alice、Bob 和 Charlie 参与了本次交易,交易中的输入地址都是经过成员之间验证的,所以交易保证了每一个成员的输出地址都将收到 1 的加密货币,但是从交易信息上可以看出,输入、输出地址并非一一对应的关系,无法推断出交易的输入地址对应的输出是哪一个输出地址,所以无法知晓货币的真正来源。因此,交易中地址与地址之间的链接性被破坏。并且每笔交易中输出地址是从未出现过的新地址,新地址在下一次使用后将不会再出现,所以交易与交易之间的链接性也被间接中断。

3.3　高效性

实验中使用的是基于 RSA 的环签名,由 RSA 环签名的性能可知一次签名要求对每个非签名者进行一次模幂运算,再加上一次或两次模乘,而验证需要对每个环成员进行一到两次模乘法。从本质上说,生成或验证一个环签名的代价与生成或验证一个常规签名的代价是一样的,即环签名有两方面的优势,第一是隐藏签名发起者,使交易成员之间相互匿名且无法探知;第二是开销和普通签名没有太大差别。所以,即使有数百个环成员,该方案也是切实可行的。

将本文方案的实验结果与 CoinShuffle 进行对比。用户数量在 5 ~ 50 之间时,对比完成交易花费的平均时间如图 8 所示,靠近 X 轴的为本文方案实验 30 次取平均时间的数据,远离 X 轴的是使用 CoinShuffle 完成交易所用时间。可以观察到即使有 50 个用户参与交易,本文方案可以在 2 s 内完成一笔混币交易。而相比于 CoinShuffle 在局域网中完成 50 个参与者的交易花费 40 s 时间,明显提高了很多。

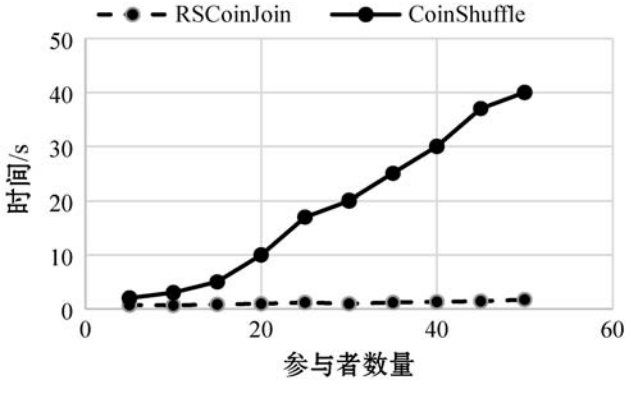

图 8　实验结果及对比

RSCoinJoin 能够在短时间内完成多人交易的原因有两点:1) 方案的公告阶段与 CoinShuffle 不同,公告地址时不经过复杂的解密混合网络,而是通过环签名进行发布,环签名生成或验证的代价与生成或验证一个常规签名的代价是一样的,以本实验方案的 RSA 算法为例,加密时间复杂度为 $O(\log(e)\log^2(n))$,其中 e 一般比较小;解密时间复杂度为 $O(\log(d)\log^2(n))$,其中 d 的值比较大。所以公告地址阶段的时间与参与混币的用户 n 有关。2) 在信息确认阶段,每一个用户仅需要验证最外层签名,不验证签名将面临资金丢失的危险迫使每个签名者必须验证正确后才继续后面的操作。综上所述,本文方案在效率方面有所改进。

4　相关研究

为了实现不可链接性,增强比特币的匿名性,2013 年,Maxwell[12] 首次提出 CoinJoin 思想,并基于 CoinJoin 提出混币方案。CoinJoin 中没有混合器,用户自发寻找想要参与混合的并且混合金额相等的用户,将等额比特币交易输出至新生成的地址,从而混淆交易的输入输出对应关系。CoinJoin 的优点是没有自举问题,即用户参与混币可自发进行,不受第三方信任的限制,且能够达到地址不可链接的目的。但是,CoinJoin 不能防止恶意用户通过拒绝交易发起的 DoS 攻击。

同样为了切断地址之间的联系,Saxena 等[13] 在 2014 年提出一种基于复合签名的混币方案。该方案中,交易不再直接包含交易输入和输出的链接信息,这使常规的地址分析法得出地址关系网成为一个难解问题。但是,方案中未提及怎么处理恶意用户使用假签名或者拒绝交易的 DoS 攻击的解决办法。

Mixcoin 和 Blindcoin 的出现使得 DoS 攻击成为一个占有 51% 算力的难题[14]。因为每个用户仅与混合服务器交互,并且拒绝遵守协议不会影响任何其他用户或减慢混合过程[15]。但是矿池的存在仍不可避免 DoS 攻击的发生。

CoinShuffle ++ 试图从根本上解决 CoinShuffle 的低效率问题。CoinShuffle ++ 与 CoinShuffle 的区别在于地址的混合方式不同,它使用 DiceMix 协议代替了复杂的解密混合网络。作者再次对比不同用户数量下所用的时间,50 个用户使用 CoinShuffle ++ 进行混币时平均时间仅需要 7.2 s[16]。与 CoinShuffle ++ 在纠错阶段的处理相比,CoinShuffle ++ 在最坏的情况下需要 $4+2f$ 次回合,其中 f 是恶意节点的数量,为了减少纠错过程中的通信次数,该协议加入了重复检查的机制,所以在一次恶意交易中会出现多次检查,但是 RSCoinJoin 只需要做一次判断,根据判断结果做检查即可纠错,所以,即使出现恶意节点,RSCoinJoin 也能够在更短的时间内完成混合交易。

2019 年,李雪莲等[17]提出 CoinExit,CoinExit 是一种可匿名撤销混币参与的比特币混币方案,该方案利用零知识证明使得用户可以匿名退出混币交易,并且增加惩罚和恢复机制强制要求参与用户完成整个交易过程以避免 DoS 攻击。从实验结果可以看出,CoinExit 方案的完成是多项式时间问题。CoinExit 主要想实现的是让参与者匿名撤销交易,即在交易中可申请退出交易过程,而 RSCoinJoin 则着力于提升交易效率。

2020 年,程其玲等[18]提出 TTShuffle 方案。TTShuffle 针对效率低的问题,提出两层洗牌模式:第一层是先对用户进行分组并进行组内洗牌;第二层是在组内选出代表进行组间洗牌。实验表明,TTShuffle 中 40 个参与者混币时间低于 10 s,并且该方案随着参与人数的增加,平均时间反而会减少。TTShuffle 使用了洗牌的思想,每一个参与者都进行分组洗牌,在小组中洗牌的顺序是事先知道的,并且知道本次洗牌的结果来自哪一个节点,这样的相对透明洗牌尽管能够提高效率,但是在一定程度上泄露了节点信息,而 RSCoinJoin 采用环签名的方式隐藏了签名发起者,不仅提高了效率而且匿名性也较强。

综上所述,混币面临的挑战主要有两个方面:(1) 混币金额不能自定义;(2) 混币效率低。本文针对混币效率低的问题提出一种基于环签名的混币交易方案,并通过实验验证和对比分析说明该方案能保护不可链接性的同时还能解决混币效率低的问题。

5 结 语

匿名性需求在信息发达的时代显得越来越重要,尤其在金融贸易方面,在保证资金安全性的同时还要兼顾匿名性,所以关于区块链匿名性这一研究从未停止。本文对已有的混币方案进行分析,总结了匿名性面临的挑战,并提出一种基于环签名的混币方案,不仅解决了地址与地址、交易与交易和地址与用户之间的链接问题,而且拥有更高的效率。

参 考 文 献

[1] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [EB/OL]. (2008 - 10 - 20). [2021 - 03 - 06]. https://bitcoin.org/bitcoin.pdf.

[2] Mettler M. Blockchain technology in healthcare: The revolution starts here[C]//2016 IEEE 18th International Conference on e-Health Networking, Applications and Services, 2016:1 - 3.

[3] Sikorski J, Haughton J, Kraft M. Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Applied Energy,2017,195:234 - 246.

[4] Kim H, Laskowski M. Toward an ontology-driven blockchain design for supply-chain provenance[J]. Intelligent Systems, 2018,25(1):18 - 27.

[5] Sharples M, Domingue J. The blockchain and kudos: A distributed system for educational record, reputation and reward [C]//European Conference on Technology Enhanced Learning,2016:490 - 496.

[6] 付烁,徐海霞,李佩丽,等. 数字货币的匿名性研究[J]. 计算机学报,2019,42(5):1045 - 1062.

[7] Ron D, Shamir A. Quantitative analysis of the full Bitcoin transaction graph[C]//International Conference on Financial Cryptography and Data Security,2013:6 - 24.

[8] 张奥,白晓颖. 区块链隐私保护研究与实践综述[J]. 软件学报,2020,31(5):1406 - 1434.

[9] Ruffing T, Moreno-Sanchez P, Kate A. CoinShuffle: Practical decentralized coin mixing for Bitcoin [C]//European Symposium on Research in Computer Security,2014:345 - 364.

[10] Rivest R, Shamir A, Tauman Y. How to leak a secret[C]// International Conference on the Theory and Application of Cryptology and Information Security,2001:552 - 565.

[11] Rivest R, Shamir A, Tauman Y. How to leak a secret: Theory and applications of ring signatures [M]//Theoretical Computer Science. Springer,2006:164 - 186.

[12] Maxwell G. Coinjoin: Bitcoin privacy for the real world [EB/OL]. (2013 - 08 - 03). [2021 - 03 - 06]. https://bitcointalk.org/index:php? topic = 279249.0.

[13] Saxena A, Misra J, Dhar A. Increasing anonymity in Bitcoin [C]//International Conference on Financial Cryptography and Data Security,2014:122 - 139.

[14] Bonneau J, Narayanan A, Miller A, et al. Mixcoin: Anonymity for Bitcoin with accountable mixes[C]//International Conference on Financial Cryptography and Data Security, 2014:486 - 504.

[15] Valenta L, Rowan B. Blindcoin: Blinded, accountable mixes for Bitcoin[C]//International Conference on Financial Cryptography and Data Security,2015:112 - 126.

[16] Ruffing T, Moreno-Sanchez P, Kate A. P2P mixing and unlinkable Bitcoin transactions[C]//Network and Distributed System Security Symposium,2017.

[17] 李雪莲,王海玉,高军涛,等. 一种匿名可撤销的比特币混淆方案[J]. 电子与信息学报,2019,41(8):1815 - 1822.

[18] 程其玲,金瑜. TTShuffle:一种区块链中基于两层洗牌的隐私保护机制[J]. 计算机应用研究,2020,38(2):363 - 366,371.