计算机科学
COMPUTER SCIENCE

基于代理人的区块链双向混币协议

冯艺萌, 冯雁, 谢四江, 张青

引用本文

冯艺萌, 冯雁, 谢四江, 张青. 基于代理人的区块链双向混币协议[J]. 计算机科学, 2025, 52(8): 385-392.

FENG Yimeng, FENG Yan, XIE Sijiang, ZHANG Qing. Proxy-based Bidirectional Coin Mixing Mechanism of Blockchain [J]. Computer Science, 2025, 52(8): 385-392.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.240600079

基于代理人的区块链双向混币协议

冯艺萌[1]　冯　雁[1,2]　谢四江[1,2]　张　青[1]
1 北京电子科技学院网络空间安全系　北京 100070
2 中国科学技术大学　合肥 230026
(fengyimenglw@163.com)

摘　要　针对区块链交易图谱分析可能泄露用户隐私,第三方混币服务商不可信的情况,提出了一种无需第三方的基于代理人的双向混币协议 PBShuffle。协议过程无需第三方混币服务商参与,采用代理人向汇总用户传递输出地址的方式,代理人由参与者在所有参与者中随机选择,需进行两轮混合,分别向两名汇总用户传递输出地址。协议利用双重加密方式实现对输出地址传递过程中的隐私保护,代理人仅能解密使用汇总用户公钥加密过的加密消息,汇总用户仅能得知消息由代理人传递,无法得出消息的源头参与者。通过理论分析可知协议在不可连接性、可验证性和健壮性3方面具有较高的安全性。与 CoinShuffle 的对比实验表明,在参与用户数量较多的情况下,PBShuffle 具有更高的效率和更低的开销,更适用于实际应用。

关键词:区块链;隐私保护;混币协议;加密;匿名性
中图分类号　TP309

Proxy-based Bidirectional Coin Mixing Mechanism of Blockchain

FENG Yimeng[1],FENG Yan[1,2],XIE Sijiang[1,2] and ZHANG Qing[1]
1 Cyberspace Security Department,Beijing Electronic Science and Technology Institute,Beijing 100070,China
2 University of Science and Technology of China,Hefei 230026,China

Abstract　Aiming at the situation that blockchain transaction mapping analysis may leak users' privacy and the third-party mixing service providers are not trustworthy,this paper proposes an agent-based bidirectional mixing protocol PBShuffle without the need of a third party. The protocol process does not require the participation of a third-party mixing service provider,and it adopts the method of delivering the output address to the aggregated users through an agent. The agent is randomly selected by the participant among all participants and needs to perform two rounds of mixing to deliver output addresses to two aggregated users respectively. The protocol utilizes double encryption to achieve privacy protection in the process of output address delivery,the agent can only decrypt the encrypted message encrypted with the public key of the aggregated user,and the aggregated user can only know that the message is delivered by the agent,and cannot derive the source participant of the message. The protocol is theoretically analyzed to be highly secure in terms of non-connectivity,verifiability and robustness. Comparison experiments with CoinShuffle show that PBShuffle has higher efficiency and lower overhead in the case of a larger number of participating users,and is more suitable for practical applications.

Keywords　Blockchain,Privacy protection,Coin mixing mechanism,Encryption,Anonymity

1　引言

2008年,中本聪提出了一种通过去中心化、点对点网络来实现数字货币的方法,该系统采用了区块链技术来确保交易的安全性和透明性[1]。区块链是一种去中心化、分布式账本技术,由一系列按时间顺序排列的数据块(区块)组成,每个区块包含一定数量的交易记录,并使用密码学方法保证数据的不可篡改性和可追溯性。比特币(Bitcoin)是区块链技术最知名的应用之一,它通过未花费交易输出(Unspent Transaction Output,UTXO)模型管理比特币的流通。UTXO是区块链上每一笔未花费交易的输出,记录了比特币的数量和所有者地址。在传统的金融体系中,用户的交易信息往往被记录在银行或其他金融机构的系统中,容易被泄露或被用于不良目的,而比特币基于区块链技术采用密码技术和去中心化的设计,使得交易的真实性能够得到确认,并且无需暴露交易参与者的身份信息,但需要将交易在网络上公开,因此网络中的

到稿日期:2024-06-12　返修日期:2024-09-11
基金项目:科技创新2030—重大项目(2021ZD0300705);中央高校基本科研业务费资金(32820230057Z0114)
This work was supported by the Innovation Program for Quantum Science and Technology(2021ZD0300705) and Fundamental Research Funds for the Cental Universitles(32820230057Z0114).
通信作者:冯雁(fengy@besti.edu.cn)

恶意节点可以通过分析交易中包含的数据得到用户的个人信息，窃取用户的个人隐私，故区块链的隐私保护势在必行。

目前针对区块链的隐私保护方案主要分为 3 类：基于混币技术的隐私保护方案、基于离链支付协议的隐私保护方案以及基于密码学的隐私保护方案[2]。混币技术通过将多个交易混合在一起，使得追踪者难以确定每个交易的真正来源和目的地。相比于基于离链支付协议的隐私保护方案和基于密码学的隐私保护方案，基于混币技术的隐私保护方案可以兼容现有区块链，容易实现，但仍存在第三方混币服务器不可信、恶意节点混入窃听、恶意节点拒绝服务等安全威胁。

根据混合过程中是否需要可信第三方的参与，混币技术可分为中心化混币和去中心化混币。在中心化混币方面，Bonneau 等[3]提出的 Mixcoin 是比特币混合协议的重要里程碑，它为混合过程提供了强有力的问责保证。Blindcoin 对 Mixcoin 协议进行了修改，引入了盲签名方案和公共日志[4]。TumbleBit 是另一种在比特币网络上实现的匿名支付协议[5]，它通过结合零知识证明和 RSA 谜题，确保了支付交易的参与者的身份和交易金额都是匿名的。在去中心化混币方面，Coinswap 是一种双方混币协议，通过建立一个 2 对 2 的托管协议来实现交易的匿名性[6]。CoinJoin 是另一种通过多个参与者共同创建混币交易来保护交易匿名性的多方混币协议[7]，它允许参与者共同创建一个混币交易，并确保每个参与者可以独立验证。受到 CoinJoin 和 Dissent 等协议的启发，CoinShuffle 协议采用了类似的思路，也不需要任何第三方参与[8]。Ziegeldorf 等[9]提出了 CoinParty 协议，该协议基于解密混合网络和阈值签名的组合，将阈值签名应用于比特币混合，实现了比其他相关方法高出几个数量级的匿名性。

本协议基于 CoinShuffle 进行改进，提出了一种去中心化的基于代理人的双向混币协议 PBShuffle。采用代理人和双混币的方式实现输出地址的传递，输出地址通过加密的方式对代理人进行隐藏，参与用户通过增加代理人实现与输出地址的分离。同时，双向混币形式下的两名汇总用户可减小汇总用户作恶的可能性。

2 基础知识

2.1 交易

比特币的交易过程可以分为创建交易、交易全网广播、全网验证区块并确认交易和全网同步实现交易写入共识区块链 4 个阶段，如图 1 所示[10]。

1）创建交易。在进行交易之前，用户需要确认他们拥有足够的比特币资金。用户的比特币资金以 UTXO 的形式分散存储在区块链的若干区块中。用户通过钱包软件构建交易，指定输入 UTXO 和输出地址，并使用私钥进行签名。用户的钱包软件会跟踪其 UTXO 列表，以管理其比特币资产。如果钱包软件没有维护 UTXO 列表，它会向比特币网络中的完全节点查询这些信息，从而确定是否可以构建交易。每个交易都包含交易输入和输出，以及该交易的哈希值，如图 2 所示。这些交易在构建时可以离线进行，并且可以由非本人进行构造。

2）交易全网广播。一旦构建了交易，它将被广播到比特币网络中的其他节点。这些节点会验证交易的有效性，确保交易输入的资金来源有效，即验证上一个交易的输出确实未被花费过，以防止双重支付。此外，收到交易的节点还会验证签名是否正确。如果验证通过，该节点会将交易转发给相邻节点；如果验证失败，则直接丢弃该交易。矿工节点将验证通过的交易放入自己的交易池，判断当前交易池的大小，如果达到了区块的大小，则将交易池中的交易打包为区块。

3）全网验证区块并确认交易。矿工节点将打包好的区块广播到网络中，其他节点会验证该区块的有效性。除了验证区块头部哈希值是否符合共识协议中要求的工作量外，其他节点还会验证区块中每一笔交易的有效性。只有当区块及其包含的所有交易都通过验证后，其他节点才会将该区块加入自身的区块链中，并将其命名为第 N 号区块。N 表示该区块在区块链中的高度。

4）全网同步实现交易写入共识区块链。经过一段时间后，会有新的区块加入，当区块得到 6 个区块的确认后，可认为此时区块得到了全网共识。因为，在比特币的挖矿协议下，一旦一个区块得到 6 个区块的确认，要制造分叉并赶上原链条的概率就变得非常小。

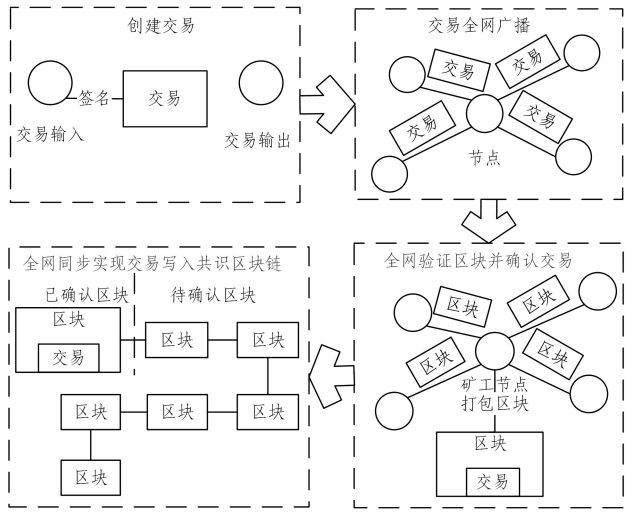


图 1 比特币交易流程

Fig. 1 Bitcoin transaction process

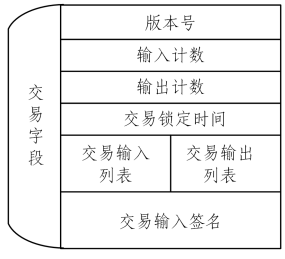


图 2 交易字段

Fig. 2 Transaction fields

2.2 混合交易

混合交易是一种提高比特币用户匿名性的方法，其基本思想是通过将多个用户的比特币混合在一起，使得外界无法准确地将输入和输出关联起来。

构造一笔比特币混合交易通常需要一组用户参与。最简单的混合交易形式可以通过借助可信第三方混合服务器来完成，如图 3 所示。具体流程如下：

1）用户向第三方混合服务器发送参数申请混币，服务器返回接收地址、签名承诺和其他相关参数。用户将自己的比特币转移到由混合服务器提供的接收地址，并将新输出地址加密发送给混合服务器。

2）混合服务器对这些加密地址进行解密和随机洗牌，然后重新分配比特币到每个地址。

3）用户验证生成的混合交易是否将正确的金额发送到他们的输出地址。如果验证通过，用户对混合服务器的承诺参数进行销毁；否则用户公开承诺。

但是，这种混合方式存在一些严重的安全和隐私问题。首先，如果混合服务器遭受黑客攻击或被内部人员利用，用户的交易数据可能会被窃取，甚至用户的资金可能会被盗取。其次，如果混合服务器记录和分析交易数据，它有可能推断出输入和输出地址之间的关系，从而破坏用户的匿名性。

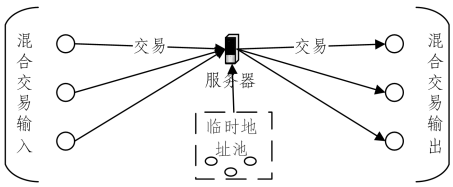


图 3 混合交易方法一

Fig. 3 Mixing transaction method one

基于 Maxwell 提出的 CoinJoin 可以实现无需借助可信第三方混合服务器也可完成交易的混合交易形式。这种方式的原理是，生成一个包含多个输入地址的混合交易，每个输入地址对应一个用户的比特币，如图 4 所示。

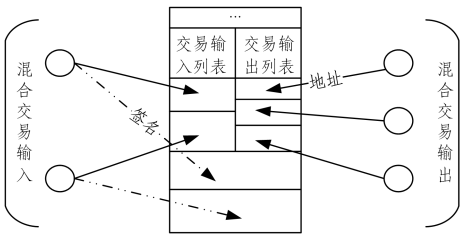


图 4 混合交易方法二

Fig. 4 Mixing transaction method two

在此方式中，每个用户只能验证自己的输出地址是否收到了预期的正确金额，而无法查看其他用户的输出地址的收入信息，这种设计确保了用户的匿名性。只有掌握了输入地址对应私钥的用户才能对交易进行签名，这确保了只有合法的用户才能消费这些资金。这种协议防止了未经授权的访问和资金损失，确保了交易的有效性和安全性。

混币协议应达成不可链接性、可验证性和健壮性的安全和隐私要求。

1）不可链接性：在混合交易顺利完成后，诚实的参与者的输入和输出地址之间将无法或很难建立关联。

2）可验证性：攻击者无法通过任何手段窃取或破坏诚实参与者的加密货币。

3）健壮性：即使在网络中存在恶意节点的情况下，协议仍然能够达成预期，成功执行。

由于区块链网络需要一定的时间来达成共识并验证交易的有效性，恶意参与者可以利用这一时间差提交多个相互冲突的交易，造成双重花费攻击，可能会引发混合交易的失效。混币协议的核心目标是保护交易的隐私性，在此基础上可以增加双重花费防护协议，确保交易的有效性，为交易提供额外的安全层。

3 PBShuffle 协议

混币协议通过将多笔交易混合在一起，混淆交易路径，使得外部观察者难以通过交易图谱分析追踪交易的真实来源和目的，从而保护用户隐私并增强交易安全性。混合多笔交易的结果是输入地址$\{I_1, I_2, \cdots, I_{n_1}\}$的资产转移到$\{O_1, O_2, \cdots, O_{n_2}\}$，$I_i$ 为第 i 名用户的输入地址，O_i 为第 i 名用户的输出地址，n_1 为输入地址的数量，n_2 为输出地址的数量，二者可不相等。同时应注意，用户不知晓其他用户输入地址和输出地址的对应关系。

PBShuffle 分为初始化阶段、混合阶段、交易阶段和问责阶段 4 个阶段。初始化阶段协商必要参数；混合阶段分为两轮混合，每轮混合参与用户都需要通过代理人将自己的输出地址加密发送给汇总用户；交易阶段由尾汇总用户确定好所有参与用户的验证结果后构造交易；在每个阶段，每名用户都需要对自己的操作进行签名，以便在问责阶段确定问题节点。

协议中的代理人是由参与者随机选择的节点，负责将经过两层加密的输出地址解密一层后传递给汇总用户，起到中转作用。汇总用户是被选出的两名用户，负责接收并处理代理人传递的加密输出地址。第一轮混合中的汇总用户为头汇总用户，第二轮混合中的汇总用户为尾汇总用户。

3.1 初始化阶段

步骤 1 参与用户通过引导协议寻找到其他参与用户，例如通过公告板，或其他专门为此目的设置的点对点协议。通常情况下，引导协议应尝试做到将恶意节点抵制到协议之外。之后有共同需求的参与者另外商定通道用于发送消息，例如商定一个新的会话符和使用一种编码来确保协议消息与比特币交易是不同的。

步骤 2 每名参与用户 n_i 生成参与混币的公私钥对(k_i, p_i)和广播 $k_i, I_i, \sigma_i(I_i)$，即公布公钥 k_i 及输入地址 I_i，σ_i 表示用户 i 的签名，为了简化表示，假设签名的消息可以从其签名中提取出来。

步骤 3 协商混币参数，包括混币金额 V 和混币时间 T。统一的混币金额用于防止攻击者通过分析资产转入/转出差额来获取用户输入/输出地址关系；混币时间用于防止恶意节点拖延，使得混币无法结束。此时可验证参与者是否有足够的混币金额 V，若没有，则进入步骤 13。

步骤 4 通过随机排序选出头尾两名用户作为汇总用户。

3.2 混合阶段

3.2.1 头混合

此轮混合中，每名用户通过代理人将输出地址传递给头汇总用户，流程如图 5 所示。

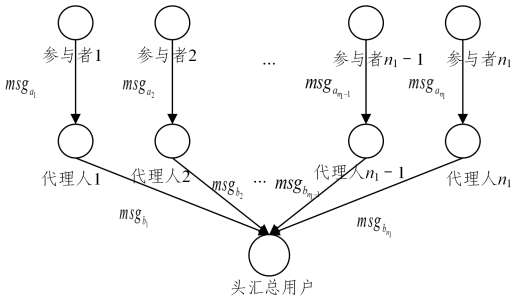


图 5 头混合流程

Fig. 5 Head blending process

步骤 5 每名参与者使用头汇总用户的公钥加密自己的输出地址，之后参与者在所在小组中选择此轮混合的代理人，并使用代理人公钥对已加密过的输出地址再次加密，得到广播给代理人的消息 msg_a：

$$msg_{a_i}=\sigma_i(k_{b_i}(k_{\text{head}}(O_i))) \tag{1}$$

其中，O_i 表示第 i 名用户的输出地址集合，k_{head} 表示头汇总用户的公钥，b_i 表示被第 i 名用户所选中的代理人，k_{b_i} 表示代理人 b_i 的公钥，σ_i 表示第 i 名用户的签名。

如果参与者拥有两个或两个以上输出地址，可选择多个代理人逐条发送，如图 6 所示。如果没有输出地址，则可以不发送。

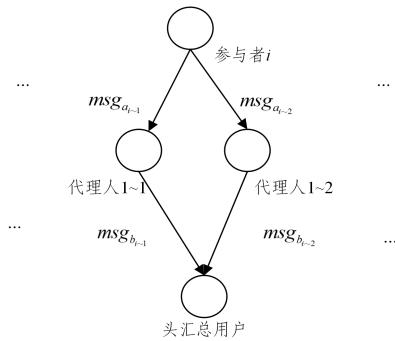


图 6 多个输出地址处理方法

Fig. 6 Multiple output address handling

步骤 6 代理人使用私钥解密后将结果 msg_b 广播：

$$msg_{b_i}=\sigma_{b_i}(k_{\text{head}}(O_1),k_{\text{head}}(O_2),\cdots,k_{\text{head}}(O_m)) \tag{2}$$

其中，m 表示代理人收到 m 名用户的输出地址消息。

如果存在一条消息没有代理人可以成功解密，则进入步骤 14。

代理人的解密操作是协议顺利进行的关键环节之一。成功解密并广播消息后，汇总用户能够接收到所有参与用户的输出地址信息(以加密形式)，进而执行后续步骤。如果代理人无法解密某条消息，则表明存在潜在的协议执行问题，协议将进入问责阶段，在此阶段可以更快速识别和剔除问题节点。

步骤 7 头汇总用户解密所有消息后，将输出地址升序排列并哈希处理，广播消息 $result_{\text{head}}$，如图 7 所示。

$$result_{\text{head}}=\sigma_{\text{head}}(hash(\{O_1,O_2,\cdots,O_{n_2}\}))$$

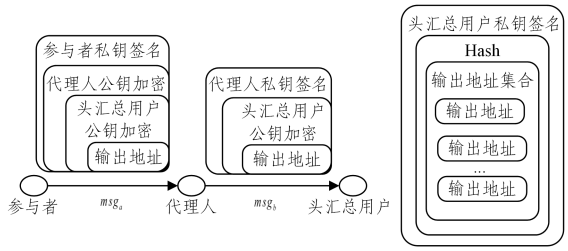


图 7 头混合消息传递

Fig. 7 Head blending message delivery

如果存在一条消息头汇总用户无法成功解密，则进入步骤 14。

3.2.2 尾混合

此轮混合中，每名用户通过代理人将输出地址传递给尾汇总用户，流程如图 8 所示。

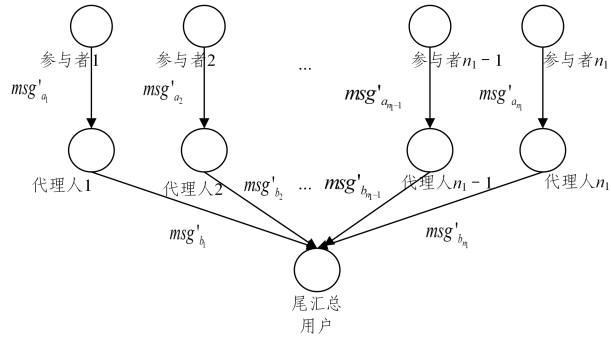


图 8 尾混合流程

Fig. 8 Tail blending process

步骤 8 参与者选择此轮混合的代理人，使用尾混合用户和代理人的公钥对输出地址双重加密，并签名广播消息 msg_a'。

$$msg'_{a_i}=\sigma_i(k_{b_i'}(k_{\text{tail}}(O_i))) \tag{3}$$

其中，k_{tail} 表示头汇总用户的公钥，b_i' 表示被第 i 名用户所选中的代理人，$k_{b_i'}$ 表示代理人 b_i' 的公钥。

与步骤 5 相同，如果参与者拥有两个或两个以上输出地址，则可选择多个代理人逐条发送。如果没有输出地址，则可以不发送。

步骤 9 同样地，代理人解密后将结果 msg_b' 签名广播。

$$msg'_{b_i}=\sigma_{b_i'}(k_{\text{tail}}(O_1),k_{\text{tail}}(O_2),\cdots,k_{\text{tail}}(O_m)) \tag{4}$$

与步骤 6 相同，如果存在一条消息没有代理人可以成功解密，则进入步骤 14。

步骤 10 尾混合用户解密所有输出地址，将结果升序排列并签名，广播消息 $result_{\text{tail}}$。

$$result_{\text{tail}}=\sigma_{\text{tail}}(\{O_1,O_2,\cdots,O_n\}) \tag{5}$$

尾混合阶段消息传递流程如图 9 所示。

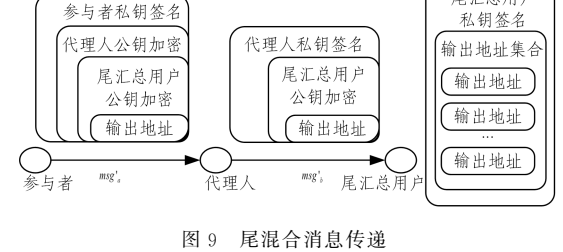


图 9 尾混合消息传递

Fig. 9 Tail blending message delivery

与步骤 7 相同，如果存在一条消息尾汇总用户无法成功解密，则进入步骤 14。

3.3 交易阶段

步骤 11 在此阶段每名参与者需要对尾汇总用户公布的输出地址列表签名。参与者需要验证两个部分：1）头汇总用户与尾汇总用户公布列表哈希结果是否相同；2）列表中是否含有自己的输出地址。若两步验证均为肯定结果，参与者使用自己的输入地址对应的私钥（该私钥不是混币协商过程中生成的私钥 p_i）对 $result_{tail}$ 进行签名并广播；若验证不成功，则拒绝签名，混币交易无法生成，进入步骤 14。如果在生成交易的过程中有参与者发现存在行为不端的参与者提前花费了本次混合的预留资金，则同样进入步骤 13。

步骤 12 直到每名参与者接收到所有参与者签名的输出地址列表，才生成交易，并将其提交至区块链网络。至此，PBShuffle 协议结束。

3.4 问责阶段

此阶段的主要任务是判断行为不端的参与者并将其剔除。以上每个阶段都有可能进入问责阶段，下面对几种情况进行具体分析。

步骤 13 在参与者 i 收到参与者 j 发布的包含签名 σ_j 的输入地址 I_j 信息后，检查 j 的余额以确保有足够的资金进行交易。如果 j 的余额小于金额 V，则进入此步骤。参与者 i 广播一条签名消息，解释进入问责阶段的原因：参与者 j 余额不足以进行交易。

步骤 14 如果在交易阶段有参与者验证不成功，则可以公布参与此次混合的临时私钥 p_i，解密收到的消息，找到行为不端的参与者。

步骤 15 参与者可能会在任何时候通过简单的脱机来被动地破坏协议运行，而不是主动地实施行为不端，这可能是恶意的，也可能是由于网络故障或不对称连接。因此，本协议设置了混币时间 T，当超出 T，自动进入此步骤。参与者可通过公布其收到的消息来找出有问题的参与者。

在问责阶段结束时，至少会有一个行为不端的参与者被识别出来，需要将其排除，其余参与者可以重新建立会话，在没有行为不端的参与者的情况下开始新的协议运行。

4 协议分析

4.1 功能分析

表 1 列出了一些混币协议的功能。

表 1 几种混币协议的功能对比

Table 1 Comparison of several coin mixing mechanisms

方案	兼容现有区块链系统（以比特币为代表）	用户全程在线	收取混币费用	一定程度抵御拒绝服务攻击
CoinParty	√	×	√	√
文献[11]	√	×	√	√
Blindcoin	√	×	√	√
TumbleBit	√	×	√	√
CoinShuffle	√	√	×	×
TTShuffle[12]	√	√	×	√
IMShuffle[13]	√	√	×	√
PBShuffle	√	√	×	√

CoinParty 协议通过共同托管地址和阈值签名实现了高度的匿名性，但参与者不需要全程在线。然而，这种设计可能导致资金提前锁定，增加了资金丢失的风险。相比之下，PBShuffle 允许用户全程在线，实时参与混币过程，提高了资金的安全性和灵活性。

Blindcoin 协议引入了盲签名和公共日志来增强 Mixcoin 的匿名性，但它依赖于可信的第三方混币服务器。与 Blindcoin 不同，PBShuffle 完全去中心化，无需任何第三方参与，从而避免了第三方信任问题和潜在的单点故障。

TumbleBit 通过零知识证明和 RSA 谜题实现了匿名支付，但它主要用于跨链支付，并不直接适用于比特币网络的混币。相比之下，PBShuffle 专注于比特币网络的混币过程，具有更高的兼容性和实用性。

TTShuffle，IMShuffle 和 PBShuffle 是对 CoinShuffle 的不同改进，因此实现的功能与其相同。CoinShuffle 采用随机选择最后一个节点的方式，但无法有效抵御拒绝服务攻击。TTShuffle 和 IMShuffle 采用分层设计，一定程度地抵御了拒绝服务攻击。PBShuffle 通过双轮混合机制和混币时间限制，也在一定程度上预防了拒绝服务攻击。此外，收取混币费用可以抵御拒绝服务攻击。

4.2 安全性分析

4.2.1 不可链接性

若攻击者没有参与到混币会话中，那么他只能看到一笔混合交易，在他试图链接输入地址和输出地址的过程中，他所收集到的只有交流过程中公布的各种消息，这些消息都是被加密过的，攻击者很难破解。虽然最终公布的输出地址集合未被加密，但攻击者没有中间消息的支撑也无法推断输入地址和输出地址的链接关系。

若攻击者参与了混币过程，可以分为汇总用户诚实和汇总用户不诚实两种情况。

假设选中的两名汇总用户为诚实的参与者，这意味着在公布汇总列表前，所有代理人发送给汇总用户的消息均被成功接收和解密。由于代理人收到的消息是被汇总用户公钥加密过的消息，代理人没有对应私钥，无法解密，即使代理人知晓是谁发送的此条消息，也无法得知该参与者发送的具体输出地址。同时，两轮混合参与者选择的代理人可不相同，增加了代理人链接的难度。

假设两名汇总用户中存在一名行为不端的参与者，他们收到代理人传递的消息可以解密出具体输出地址，但他们无法得知此条消息的初始发送者，因此无法链接输入输出地址关系。当他们企图破坏此次交易时，可以通过脱机或修改最终汇总结果来阻挠交易，但这种情况下会进入问责阶段，发现并被剔除。并且，选择汇总用户的过程具有随机性，双混币协议大大增加了两名汇总用户联合作恶的成本。

因此，在协议成功运行且未进入问责阶段的情况下，PBShuffle 能够有效地保护交易的隐私性，确保输入地址和输出地址之间的链接不被泄露。即使攻击者能够观察到最后公布的输出地址集合，他们也无法确定哪个输出地址包含了哪个输入地址的比特币，从而保护了用户的隐私。

4.2.2 可验证性

一个诚实的参与者 i 在签署最终的混合交易之前，会进行一系列的验证步骤。

首先，参与者可以验证输出地址列表中是否包含自己的输出地址 O_i，以确保 O_i 没有被排除或替换。

其次，诚实的参与者 i 还会验证发送到其输出地址的货币数量是否与他从输入地址中获得的货币数量相匹配，此步骤可确保在混合过程中没有发生任何未经授权的转移或损失，在 PBShuffle 中，为保护隐私，转移到每个输出地址的货币数量是事先商量好的相同的金额，若存在交易费用，最终发送到输出地址的数量可能会略少于原始输入数量，但诚实的参与者需要确保这种减少是合理和预期的，PBShuffle 并未设置交易费用，若有需要可以在初始化阶段进行协商。

通过执行这些验证步骤，诚实的参与者可以确保混合协议的可验证性，并且只有在确认其货币没有被攻击者窃取或破坏的情况下，才会签署最终的混合交易。这种协议提供了对混合过程透明度的保证，从而增强了加密货币交易的安全性和可信度。

4.2.3 健壮性

在 PBShuffle 的问责阶段中，借助消息的签名以及来自区块链网络的实证材料，揭露参与者的违规行为。当交易创建失败，参与者察觉到协议运行出现障碍时，转入问责阶段。在这一阶段中，诚信的参与者将运用他们累积的信息，来揭露那些行为不端的参与者。

诚实的参与者可以通过仔细比对消息的签名和区块链网络来鉴别出存在不当行为的参与者。通过消息的签名可以找到参与者在协议执行过程中的消息，而区块链网络则能反映出交易的真实性和参与者的行为轨迹。通过深入对比这些信息，诚实的参与者能够精准地识别出那些签名与实际情况不符或交易行为异常的参与者。

即使问责阶段未能直接锁定行为不端的参与者，诚实的参与者依然可以利用手中的信息来重现每个参与者在混合阶段的操作过程。

通过重新执行这些步骤，并仔细对比每个参与者的行为及签名消息，诚实的参与者能够准确找出那些行为与协议规定不符或签名不一致的参与者，从而锁定行为不端的个体。

4.2.4 可能存在的安全风险

尽管 PBShuffle 具备不可链接性、高验证性和健壮性，但在实际应用中仍面临以下潜在安全风险。

1）代理人合谋风险：PBShuffle 通过引入代理人和双向混币机制减小了用户作恶的可能性，但若多个代理人合谋，他们可能共享解密信息，威胁交易隐私。

2）密钥管理风险：参与者需生成和管理公私钥对，若私钥管理不善，可能被泄露或被恶意软件窃取，攻击者可通过解密消息追踪交易。

3）时间同步攻击：混币过程的时间同步对协议成功执行至关重要。恶意参与者可能利用时间差提交冲突交易，导致双重花费攻击。尽管 PBShuffle 设置了混币时间限制，但时间同步攻击仍可能成功。

针对以上安全风险，可在 PBShuffle 中采用一定的安全措施以增强协议安全性，例如：针对代理人合谋风险，可在协议中增加随机性和冗余性，如让参与者随机选择多个代理人，并要求多个代理人同时解密才能获取完整信息；针对密钥管理风险，可增加安全存储和备份等措施；针对时间同步攻击，可引入更复杂的时间同步机制或使用区块链的时间戳功能确保交易顺序。

4.3 效率分析

本节从执行时间、通信代价和交互轮次 3 方面对 PBShuffle 协议进行了仿真测试，并与 CoinShuffle 协议进行了对比分析。

混币协议的核心为混合阶段的输出地址消息传递，假设消息均传递成功及其他阶段均顺利完成，搭建虚拟的对等网络，产生多个参与者节点并加入混币交易，分别实现对两个协议混合阶段输出地址消息传递的模拟。

4.3.1 执行时间

首先，对不同数量的参与者运行了协议，范围为 5 到 50，并通过 50 次重复实验对各混币协议的执行时间取平均值，得到了 CoinShuffle 和 PBShuffle 的执行时间。图 10 给出了在相同网络拓扑中，执行混合阶段所需的总时间。在相同数量的参与者下，PBShuffle 的整体执行时间比 CoinShuffle 要短。

在 CoinShuffle 中，输出地址的传递通过多层加密进行。每位参与者需要等待前一个参与者将加密数据传递给自己，然后解密接收到的消息，并为自己的输出地址添加多层加密，最后传递给下一个参与者。这个过程一直持续到最后一个参与者，该参与者接收到前一个参与者发送的加密数据并解密，此时整个混币交易的混合阶段才算完成。因此，随着参与者数量的增加，加密数据的传递链相应增长，混币协议的执行时间也显著增加。

在 PBShuffle 中，混合阶段允许参与者并发地传递加密数据给代理人，代理人并发地传递加密数据给汇总节点。混合阶段的主要耗时在于汇总节点解密接收到的加密数据。实际上，增加参与者的数量对参与者传递加密数据给汇总节点的时间并没有显著影响。然而，随着参与者数量的增加，汇总节点需要解密的数据量会相应增大，从而导致混合阶段的时间延长。这是因为汇总节点需要处理更多的加密数据，这增加了其解密操作的复杂性和所需时间。因此，尽管参与者之间的数据传递速度可能不受影响，但整个混币过程的总时间仍会随着参与者数量的增加而增长。

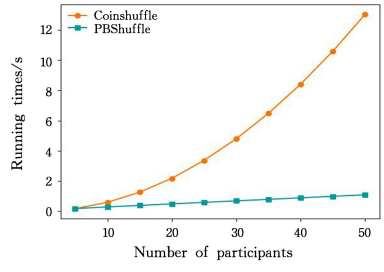


图 10 总执行时间

Fig. 10 Total execution time

图 11 给出了 50 轮不同数量参与者 PBShuffle 执行时间的具体情况。总的执行时间随参与者数量的增加呈线性增

加，且在相同参与者的情况下，不同拓扑结构下的执行时间变化不大。

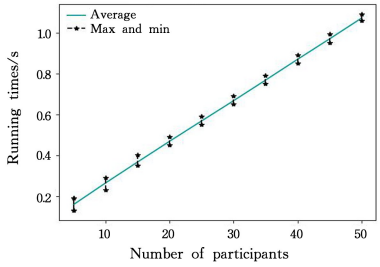


图 11 不同数量参与者执行时间的具体情况

Fig. 11 Specifics of implementation time for different numbers of participants

4.3.2 通信代价

在 CoinShuffle 协议中，通信代价主要来自于参与者在混合阶段向最后一个节点发送加密消息的过程。在 PBShuffle 协议，通信代价主要来自于参与者在混合阶段向代理人发送加密输出地址以及代理人向汇总用户发送加密消息的过程。假设每个加密输出地址的大小为 128 字节（这通常包括地址本身以及必要的加密填充和元数据），且每传递一个消息（包含签名和加密内容）大约需要额外的 64 字节（这包括签名的长度和必要的消息封装格式）。两种协议在相同参与者数量情况下的通信代价对比如图 12 所示。随着参与者数量的增加，CoinShuffle 的通信代价相较于 PBShuffle 显著增加。

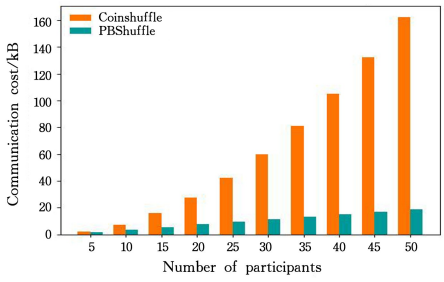


图 12 通信代价对比

Fig. 12 Comparison of communication costs

在 CoinShuffle 的混合阶段，每个参与者节点在层层加密的传递链中，都需要向后一个节点发送加密数据。这些加密数据不仅包含该节点自己的输出地址，还包含之前所有节点的输出地址。因此，随着传递链的延续，后续节点所需发送的数据量逐渐增加，而通信代价也随之增大。每个节点都需要处理并转发前面所有节点的数据，这使得通信成本随着参与者的增加而显著上升。

在 PBShuffle 混合阶段，通信代价的分布更加均衡和高效。加密数据传递的数据量仅与参与者数量相关，而非传递链长度，这意味着通信成本得到了有效控制。PBShuffle 优化了通信模式，显著降低了混合阶段中层层加密传递输出地址所需的通信代价，尤其是在参与者数量较多的情况下，这种优势更加明显。

在实际应用中，即使参与者数量达到几百甚至上千，通信代价也维持在相对较低的水平（例如，1 000 名参与者时的总通信数据量为 1.9 MB）。这表明 PBShuffle 协议受到通信带宽限制小，在通信效率上表现良好，适用于大规模参与者场景。

4.3.3 交互轮次

假设传递一个包含输出地址的消息的交互轮次为单位 1，两种协议在相同参与者数量的情况下的交互轮次对比如图 13 所示。随着参与者数量的增加，PBShuffle 的交互轮次相较于 CoinShuffle 会有所增加。

在 CoinShuffle 中，参与层层加密的节点会按照既定顺序依次进行交互，每个节点之间的交互轮次随着参与者数量的增加而增加。

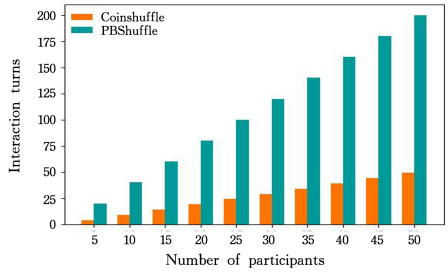


图 13 交互轮次对比

Fig. 13 Comparison of interaction rounds

在 PBShuffle 中，引入了代理人，参与者需要与代理人进行交互，每个代理人再与汇总节点进行交互。因此，PBShuffle 的交互轮次不仅与参与者数量有关，还与代理人数量有关。

综合上述分析及实验数据，可以得出以下结论：相较于 CoinShuffle，PBShuffle 协议的整体执行时间虽然也会随着参与者数量的增加而变长，但其增速明显小于前者。因此，在参与者数量较多的情况下，PBShuffle 的优势更加明显。虽然 PBShuffle 需要频繁交互，但从计算开销的综合角度来看，PBShuffle 在执行时间和通信代价两方面的显著改进足以弥补这方面的不足。

PBShuffle 协议通过引入代理人的角色，优化了输出地址的传递模式，减小了通信代价，并有效控制了执行时间的增长，使得 PBShuffle 协议能够适应更大规模的参与者群体，为混币交易提供了更加高效和安全的解决方案。

4.3.4 其他因素限制

尽管对比实验结果显示，PBShuffle 在参与者数量较多时相较于 CoinShuffle 效率更高，但在实际使用中仍有其他因素限制其使用效率和适用场景，具体如下。

1）网络延迟和带宽限制：随着参与者数量增加，PBShuffle 在通信代价和执行时间方面的优势逐渐减弱。在网络延迟较高或带宽受限的环境下，协议执行效率可能显著下降。为优化网络性能，可以采用更高效的加密和解密算法，以及优化网络传输协议。

2）代理人负载不均：代理人负责解密和转发加密消息。如果某些代理人因网络状况不佳或硬件性能不足而无法及时处理消息，则可能造成混币过程延迟。为避免这种情况，可以采用增加负载均衡机制，将消息均匀分配给多个其他的代理人，并确保每个代理人有足够的处理能力。

3）对区块链类型的依赖性：PBShuffle 是针对比特币及类

似区块链系统设计的，对于采用不同共识机制或交易模型的区块链系统可能不完全适用。因此，在应用 PBShuffle 协议前，需要仔细评估目标区块链系统的特点和需求，并进行相应修改和优化。

通过考虑这些因素，可以进一步提高 PBShuffle 的使用效率和适用范围。

结束语 PBShuffle 协议通过代理人，将输出地址传递到汇总用户，使得混合协议参与用户无法链接参与用户与输出地址，实现了混合协议对内部的隐私保护。协议过程不需要第三方参与，且代理人得到的消息是密文，无法得知消息内容。理论分析表明，本协议具有不可链接性、可验证性和健壮性，安全性和隐私性好。与 CoinShuffle 协议相比，本协议的通信效率受参与用户数量影响较小，实际应用中效率更高。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System [EB/OL]. (2008-11-01) [2024-05-29]. http://bitcoin.org/bitcoin.pdf.

[2] LI X D, NIU Y K, WEI L B, et al. A Survey of Bitcoin Privacy Protection[J]. Journal of Cryptologic Research, 2019, 6(2): 133-149.

[3] BONNEAU J, NARAYANAN A, MILLER A, et al. Mixcoin: Anonymity for Bitcoin with Accountable Mixes [C]// Proceedings of the 18th International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2014: 486-504.

[4] VALENTA L, ROWAN B. Blindcoin: Blinded, Accountable Mixes for Bitcoin [C]// Proceedings of the International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 112-126.

[5] HEILMAN E, ALSHENIBR L, BALDIMTSI F, et al. TumbleBit: An Untrusted Bitcoin-Compatible Anonymous Payment Hub [C]// Proceedings of the 24th Annual Network and Distributed System Security Symposium. 2017: 158-176.

[6] MAXWELL G. CoinSwap: Transaction Graph Disjoint Trustless Trading [EB/OL]. (2013-10-30) [2024-05-29]. https://bitcointalk.org/index.php?topic=321228.0.

[7] MAXWELL G. CoinJoin: Bitcoin Privacy for the Real World [EB/OL]. (2013-08-22) [2024-05-29]. https://bitcointalk.org/index.php? topic=279249.0.

[8] RUFFING T, MORENO P S, KATE A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin [C]// Proceedings of the European Symposium on Research in Computer Security. Berlin: Springer, 2014: 345-364.

[9] ZIEGELDORF J H, GROSSMANN F, HENZE M, et al. CoinParty: Secure Multi-Party Mixing of Bitcoins [C]// Proceedings of the 5th ACM Conference on Data and Application Security and Privacy. New York: ACM, 2015: 75-86.

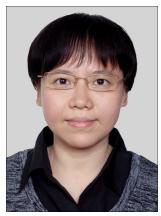
[10] HUANG Y Y, PU J. Learning Blockchain from Zero[M]. Beijing: Tsinghua University Press, 2020: 122-128.

[11] NIEM H, OU Y Y. A Decentralized Obfuscation Scheme for Digital Currency with Customizable Amounts[J]. Journal of Guangdong University of Technology, 2021, 38(1): 64-68.

[12] CHENG Q L, JIN Y. TTShuffle: privacy protection mechanism based on two-tier shuffling in blockchain [J]. Application Research of Computers, 2021, 38(2): 363-366, 371.

[13] 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.

FENG Yimeng, born in 2000, postgraduate. Her main research interests include cyberspace security and blockchain.



FENG Yan, born in 1979, postgraduate, associate professor. Her main research interests include cryptography, network security, and quantum communication network security system.

（责任编辑：喻藜）