

可监管的比特币隐私保护混淆服务

包子健^{1,2}, 王庆豪^{1,2}, 张永欣^{1,2}, 王斌^{1,2}, 鲁宁^{1,2}, 史闻博^{1,2}

(1. 东北大学计算机科学与工程学院, 辽宁 沈阳 110089;

2. 东北大学秦皇岛分校计算机科学与通信工程学院, 河北 秦皇岛 066004)

摘要: 随着比特币隐私保护研究的深入, 比特币作为一种新型“数字货币”变得更加难以监管。针对该问题, 提出了一种可监管的比特币隐私保护混淆方案 RBmix。RBmix 模型使用公平盲签名算法, 并引入可信第三方, 具有可监管性、匿名性、可扩展性、比特币兼容性以及抗 DoS 攻击性。实验结果表明 RBmix 协议具有良好的扩展性和执行效率。

关键词: 比特币; 隐私保护; 可监管; 公平盲签名

中图分类号: TP311

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2019037

Regulatory Bitcoin privacy-preserving mixing service

BAO Zijian^{1,2}, WANG Qinghao^{1,2}, ZHANG Yongxin^{1,2}, WANG Bin^{1,2}, LU Ning^{1,2}, SHI Wenbo^{1,2}

1. School of Computer Science and Engineering, Northeastern University, Shenyang 110089, China

2. School of Computer and Communication Engineering, Northeastern University, Qinhuangdao 066004, China

Abstract: With the deepening of research on Bitcoin privacy protection, Bitcoin, a new type of digital currency, has become more difficult to regulate. A Bitcoin privacy protection confusion scheme with regulatory RBmix is proposed for this problem. The model of RBmix uses a fair blind signature algorithm and introduces trusted third parties with regulatory, anonymity, scalability, Bitcoin compatibility, and anti-DoS aggression. Experimental results show that the RBmix protocol has good scalability and execution efficiency.

Key words: Bitcoin, privacy-preserving, regulatory, fair blind signature

收稿日期: 2019-05-18; 修回日期: 2019-06-29

通信作者: 史闻博, shiwb@neuq.edu.cn

基金项目: 国家自然科学基金资助项目(No.61472074, No.U1708262); 中央高校基本科研专项基金资助项目(No.N172304023)

Foundation Items: The National Natural Science foundation of China (No.61472074, U1708262), Fundamental Research Funds for the Central Universities(No.N172304023)

论文引用格式: 包子健, 王庆豪, 张永欣, 等. 可监管的比特币隐私保护混淆服务[J]. 网络与信息安全学报, 2019, 5(4): 40-51.

BAO Z J, WANG Q H, ZHANG Y X, et al. Regulatory Bitcoin privacy-preserving mixing service[J]. Chinese Journal of Network and Information Security, 2019, 5(4): 40-51.

1 引言

比特币^[1]是一种新型的“数字货币”，由于具有去中心化、不可篡改、匿名性等特点，一经公布就受到了社会各界的广泛关注。近几年，比特币发展迅速，交易规模不断扩大。截止到2019年1月，比特币的市值已经达到665亿美元，全球用户数量高达1000万，平均日交易额达到49亿美元^[2]。目前，比特币的总量约1769万个，预计至2045年，99.95%的比特币将会发行完毕。

随着比特币的发展，其面临的隐私泄露问题日益突出。虽然比特币用户与其地址之间的无关联性可以在一定程度上保护用户的隐私^[3]，但比特币的交易数据对全网公开，攻击者能够通过分析交易集合威胁比特币系统的隐私安全。近期的研究表明^[4-8]，通过对交易进行分析以及使用一些现实攻击的方法，攻击者可以轻松地获取用户的隐私。因此，隐私保护逐渐成为比特币领域的重要研究方向之一。目前，许多学者针对比特币隐私问题提出了相应隐私保护方案。

比特币隐私保护方案可以保证用户的隐私安全，但也会导致不法分子利用其进行黑市交易、跨境洗钱等非法活动。现有的大多数交易机制建立在银行或第三方支付平台的信用基础上，可信的第三方机构保证了用户交易的安全性，且能够对非法用户进行追踪与处罚。而在比特币系统中，执法部门很难对违法的比特币交易进行追溯和处罚。由于缺少可监管性，世界各国对比特币都持谨慎态度：俄罗斯、泰国等国严格限制比特币的流通，美国等接受比特币的国家强调要将比特币纳入国家监管体系中^[9]。我国对此也采取了相应措施，早在2013年，中国央行等五部委就发布了《关于防范比特币风险的通知》^[10]，其中明确指出了比特币存在的洗钱风险。2017年9月，中国央行等七部委发布了《关于防范代币发行融资风

险的公告》^[11]，进一步对比特币等“数字货币”的风险问题进行申明。随后，银保监会于2018年4月宣布所有ICO平台和比特币交易已经安全退出中国^[12]。因此，比特币作为一种影响范围极广的新型“数字货币”，不仅需要解决自身隐私保护存在的问题，而且有必要加强其可监管性，以适应国家政策的需求。

针对该问题，本文提出了一种可监管的比特币隐私保护混淆服务RBmix，本文的主要贡献如下。

1) 提出将RSA公平盲签名算法用于比特币混淆服务，并引入可信第三方来提供可监管性，在必要时，可信第三方可以追溯资金的来源。

2) 使用OP_RETURN交易构造了不可篡改的公告板机制，并利用Tor匿名网络在网络层保证用户的隐私安全。

3) 协议在保证可监管性的同时，还具有匿名性、可扩展性、可追责性、比特币兼容性和抗DoS攻击性。

4) 实验结果表明，RBmix协议具有良好的扩展性和执行效率，完成1000用户的混淆操作大约需要135s。

2 相关工作

目前，针对比特币隐私保护的方案包括基于P2P形式的方案，如Coinjoin^[13]、Coinswap^[14]等，基于混淆服务商的Mixcoin^[15]、Blindcoin^[16]方案以及改进币Zerocoin^[17]和Zerocash^[18]方案。针对“数字货币”监管问题提出的方案，包括可监管交易系统BPCSS^[19]以及英国央行提出的RSCoin^[20]。

Coinjoin方案由比特币核心开发人员Grey Maxwell提出。在Coinjoin中，由多个用户将等额的比特币作为输入构造交易，并检查自己的比特币地址是否已经写入交易中，如果已经写入，则进行签名。该交易获得所有用户的签名后，就

会被发布到比特币网络中,此时一次 Coinjoin 交易完成。Coinjoin 提高了比特币的匿名性,但是也存在一些不足。例如, Coinjoin 交易内部用户知晓所有用户输入和输出的关系,无法抵御拒绝服务(DoS, denial of service)攻击,且其交易大小受到比特币交易大小的限制。

Coinswap 协议主要针对利用中间人进行交易的场景。为了防止中间人偷取比特币,该协议使用了散列锁与多重签名机制,保证了支付方与中间人和中间人与收款方的交易在同一时间段执行。但是,方案只适用于点对点交易的场景,而且同一时间需要 6 笔比特币交易才能够完成一次支付,交易费用和网络资源消耗较大。

CoinShuffle^[21]使用了匿名组通信协议 Dissent^[22]。该方案没有第三方角色,避免了匿名服务费和比特币交易时间等开销,所需的只有很小的通信开销。Tim 等提出了改进的匿名通信协议,并设计了 CoinShuffle++方案^[23],提高了协议效率。而 SecureCoin^[24]与 CoinShuffle 类似,同样利用了去中心化的高效匿名比特币协议。上述几种协议具有较好的匿名性,但都依赖于匿名通信协议。

Bonneau 提出了基于混淆节点的 Mixcoin 方案。该方案使用多个混淆节点进行混淆服务,前一个混淆节点混淆后的结果作为后一个节点的输入,只要其中一个节点不泄露隐私,那么整个协议就能够保证隐私性。Blindcoin 基于 Mixcoin 方案,利用了盲签名保证混淆服务商无法获取用户输入地址和输出地址之间的联系。同时,该方案将 Mixcoin 中的多次混淆服务缩减到了一次,减少了混淆开销。但是,由于缺少监管机制,这两种方案都面临着用户资金被服务商盗窃的风险。

Zerocoin 方案利用零知识证明技术,将用户的比特币转化为比特币侧链上的零币。用户使用零币时,需要利用零知识证明方案证明该枚零币

对应之前的一枚比特币且未被使用。Zerocoin 曾提出软分叉方案为比特币提供隐私保护,但是被比特币开发人员拒绝。随后, Sasson 等提出了 Zerocash 方案。该方案使用非交互式的零知识证明 zkSNARK^[25]来保证交易的隐私安全,实现了交易金额的保密性。但是, Zerocash 需要在初始化阶段销毁一对加密密钥,密钥是否安全销毁直接影响整个系统的安全性。

BPCSS 是基于比特币的可监管交易系统,为客户与商家之间的“数字货币”交易提供服务。在系统中,消费者以匿名形式交易来确保隐私安全,而商家则需要进行商业登记。政府财务监督单位可以审查系统中的所有交易信息,并用于税收征收的审计参考。BPCSS 引入了数字交易收据机制,为交易纠纷提供更可靠的证据,从而帮助消费者维护自己的权益。

RSCoin 是由英国央行提出的一种新型“数字货币”模型。该模型由央行和央行授权的商业机构 mintettes 构成,央行完全控制货币产生, mintettes 则负责维护交易账本,包括收集交易、校验交易以及交易上链。针对现有加密货币系统的不足, RSCoin 致力于解决“数字货币”的可扩展性、可控的货币发行以及通用性等问题,实现了一种受中央银行控制的、可扩展的“数字货币”,为可监管“数字货币”的实现提供了雏形。

目前,比特币监管问题成为各界学者研究的热点问题之一。Kevin^[26]等曾就“数字货币”的监管问题进行了研究,主张结合现有法律构建一个凝聚力和适当规模的“数字货币”监管模式,以应对“数字货币”带来的挑战。可见,可监管性是“数字货币”进入国家层面的必要属性。

3 预备知识

本协议主要借助比特币 OP_RETURN 技术、RSA 盲签名技术以及 Tor 匿名网络。接下来对这

3 个技术原理进行介绍。

3.1 比特币 OP_RETURN 交易构造

公告板机制^[27]在密码学中有很广泛的应用，通常用于多方沟通非机密数据，它不需要安全的信道，公告板上的数据可供任何人查看与审计。公告板应该具有分布式结构、时序性、防篡改性、可公开审计等特点^[28]。

本文使用比特币系统中的 OP_RETURN^[29]来构造基于比特币系统的公告板机制。OP_RETURN 脚本的样式如下。

OP_RETURN <DATA>

由于存储数据需要消耗比特币，所以比特币系统中 OP_RETURN 存储的信息通常是数据的散列值。散列值存储在区块链中，能有效保证数据的完整性和不可篡改性，其散列算法为 32 byte 的 SHA256。同时，很多应用都在其前面加上前缀辅助认定相关的内容，如电子公正服务的证明材料采用了 8 个字节的前缀“DOCPROOF”。

使用 OP_RETURN 进行相关操作，可以保证上述公告板应该具有的性质。首先，比特币区块链作为 P2P 网络，天生具有抗 DoS 攻击的性质，每一个全节点都拥有所有的区块信息，不存在传统公告板技术中的单点故障问题。同时，区块链以区块的形式不断累加，并按照时间的顺序排列，可以保证公告板的有序性。区块链本身也是防篡改的，拥有全网 51% 算力发动攻击所付出的代价远远超过可能得到的收益。如同上文提到，比特币区块链上的数据任何人都可以随时查看，因此区块链作为公告板能够达到公开审计的性质。

3.2 RSA 公平盲签名协议

盲签名是一种特殊类型的数字签名，由 Chaum 于 1982 年提出^[30]。使用盲签名，其他人无法知道被盲化信息的内容，且在盲化的信息上进行签名，等同于在原始信息上签名。盲签名的具体流程如下：接收者盲化原始信息后发送给签

名者，签名者对盲化后的信息签名后再返还给接收者。接收者将消息去盲化，最终得到签名者关于原始信息的正确签名。

盲签名增加了电子支付的匿名性，但是容易被违法分子利用进行一些非法操作。于是 Stadler 等^[31]提出了一种公平盲签名协议。在必要时，该协议能够被可信第三方揭开签名，实现消息的追溯。

RSA 公平盲签名协议是一种基于第三方的公平盲签名方案。该协议基于普通盲签名和公平盲签名协议，利用 RSA 算法增加了协议的安全性。协议保证了在登记和签名过程中用户消息不被修改，且能在必要时对消息发送者进行追踪。

3.3 Tor 匿名网络

Tor^[32]匿名网络又被称为洋葱路由匿名代理网络，其核心技术是美国海军研究室开发的第三代洋葱路由器系统。Tor 匿名网络的研发初衷是用于保护政府机关的数据通信隐私，现在已经被广泛应用在民间企业、组织、机构、家庭以及个人的安全数据传输等场合。

Tor 匿名网络类似于分布式的虚拟专用网络 (VPN, virtual private network)。用户使用时，先在本地环境下运行洋葱代理服务器，该代理服务器会周期性地与其他代理服务器交流。当用户浏览网页时，请求消息会经过多跳 IP 地址，最终到达真正的目的地址。Tor 网络中的路由器之间进行点对点加密，如果需要看到底层的核心信息，则需要将每层加密层层剥开，每次经过一个客户端，就好像洋葱的一层皮，故被称为洋葱路由。

4 RBmix 协议设计

4.1 协议模型

比特币隐私保护方案中常用的模型是中心化服务模型。现实生活中，用户的真实身份和比特币地址之间的联系可能已经被外界知晓。因此，

用户希望通过混淆服务商来切断身份和地址的联系。中心化的服务商对用户的交易进行混淆操作,切断交易输入输出之间的联系,同时收取服务费。但现有的中心化服务模型有服务商知晓用户隐私信息、不可追责等缺点。

本文在中心化服务商模型的基础上,引入了可信第三方机构,保证了模型的可追责性,使用盲签名确保混淆服务商无法关联用户的输入地址和输出地址。协议模型将比特币中的 UTXO 模型抽象为简单的账户模型,用户拥有的是比特币地址和对应的金额。协议模型如图 1 所示。用户 Alice 希望通过混淆服务,将自己可能已经被外界知晓的比特币地址 K_{in} 上的资金转移到安全的地址 K_{out} 上。 K_{out} 一般是全新生成的比特币地址,从而防止该地址被攻击者联系到实际身份。协议模型包含如下 3 种角色。

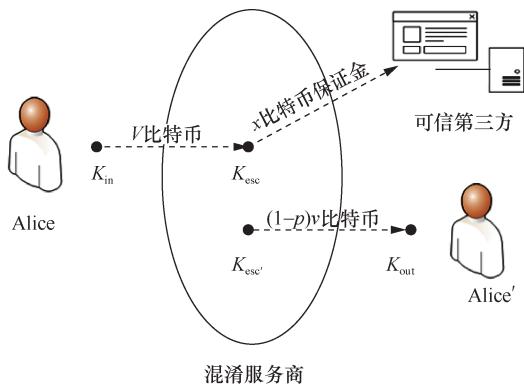


图 1 协议模型

1) 用户: 用户为了自身的隐私安全,愿意支付一定的费用给混淆服务提供商,通过服务商的帮助将比特币转移到外界攻击者无法联系真实身份的新地址(输出地址)中。图 1 中, Alice 代表用户的旧身份, Alice' 代表用户的新身份。

2) 混淆服务商: 服务商通过提供混淆服务获取利益,现实中有多个竞争的服务商,服务商通过信誉度、混淆费用等方式吸引用户购买其混淆服务从而获取利益。

3) 可信第三方: 交易前,用户和服务商都需要在可信第三方注册。用户将目标比特币地址和身份信息提交给可信第三方进行注册。混淆服务商向可信第三方提交自身信息和一定数量的保证金进行注册。无论用户还是服务商进行非法操作,可信第三方都能够进行有效的追责与惩罚处理。

4.2 协议核心设计

协议核心分为以下 4 个步骤。

1) 混淆服务商注册阶段: 混淆服务商将 x 比特币资金存储在可信第三方的地址中。当混淆服务商窃取用户资金时,可信第三方可以通过没收保证金进行惩罚。

2) 用户注册阶段: 用户需要将相关比特币地址和自身信息提交给可信第三方进行注册。

3) 混淆阶段: 使用盲签名对输出地址 K_{out} 进行盲化。Tor 匿名网络可以保护用户网络层的安全。

4) 追责阶段: 若恶意服务商窃取了用户资金,可信第三方将没收服务商的保证金进行惩罚。如果用户使用混淆货币进行违法操作,可信第三方可以打开盲签名,确认违规用户的身份。

4.3 用户与混淆服务商注册阶段

(1) 初始化参数

混淆服务商 (M): 初始化自身的身份信息 ID_{M-J} (J 为服务商的序号, M 表示混淆服务商), 随机选择两个不相等的质数 p 和 q 使 $n=pq$, 并计算 n 的欧拉函数 $\varphi(n)=(p-1)(q-1)$ 。随机选择一个整数 e , 使 $1 < e < \varphi(n)$, 且 e 与 $\varphi(n)$ 互质, 并计算 e 对于 $\varphi(n)$ 的模反元素 d 。服务商公布自己的公钥信息 (e, n) , 保存私钥信息 (d, n) , 用于盲签名算法。同时, 服务商拥有用于传统数字签名的公私钥对 (M_{pub}, M_{priv}) 。

用户 (U): 初始化身份信息 ID_{U-I} (I 为用户的序号, U 表示用户), 用户拥有自身公钥 U_{pub} 和私钥 U_{priv} 。

可信第三方 (T): 拥有自身公钥 T_{pub} 和私钥 T_{priv} 。可信第三方可以是政府针对混淆服务设置的机构。

(2) 用户注册阶段

在参与和服务商的交互过程之前, 用户需要先将输出地址和自己的身份信息 ID_{U-I} 在可信第三方注册和验证, 如图 2 所示。

具体过程如下。

① 用户选择随机数 r , 使 $\gcd(r, n)=1$, 并计算 $[K_{out}]A_C = r^e \cdot H(K_{out}) \bmod n$, 得到盲化后的消息 $[K_{out}]A_C$, 其中 $H()$ 表示散列算法。

② 用户使用 T_{pub} 对信息 $\{K_{out}, r, ID_{U-I}\}$ 加密后, 将 $\{K_{out}, r, ID_{U-I}\} T_{pub}$ 和 $\{[K_{out}]A_C\} U_{priv}$ 一同发送给可信第三方进行用户身份和输出地址的注册。

③ 可信第三方根据消息 $\{K_{out}, r, ID_{U-I}\}$ 计算出 $[K_{out}]A_C' = r^e \cdot H(K_{out}) \bmod n$, 并检查 $[K_{out}]A_C'$ 与 $[K_{out}]A_C$ 是否相等。若相等, 则用户注册成功, 可信第三方存储元组信息 $\{K_{out}, r, ID_{U-I}\}$ 。反之, 则拒绝用户的请求行为。

④ 可信第三方在确认等式成立后, 使用自己的私钥 T_{priv} 对 $[K_{out}]A_C$ 进行签名, 并将签名后的值 $\{[K_{out}]A_C\} T_{priv}$ 发送给用户。

⑤ 用户收到签名后, 使用可信第三方公布的公钥 T_{pub} 验证签名。若验证成功, 则本次注册完成。

(3) 混淆服务商注册阶段

混淆服务商将自身的身份 ID_{M-J} 发送给可信第三方, 同时发送 x 比特币至可信第三方的比特币账户 (x 为保证金的金额)。若混淆商窃取用户的资金, 诚实的用户可以拿出证据发送给可信第三方。可信第三方将使用该服务商的保证金进行赔付, 同时对该服务商实施惩罚, 如图 3 所示。

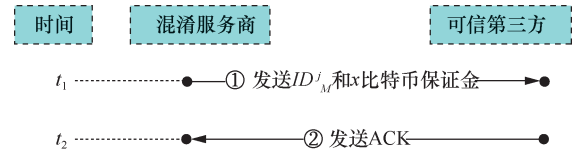


图3 混淆服务商注册阶段流程

4.4 混淆协议阶段

本文的协议参数信息如表 1 所示, 其中部分关键参数将在 4.6 节进行分析。混淆阶段流程如图 4 所示。具体过程如下。

1) 混淆服务商将自身期望的参数 v 、 w 、 p 发送到公告板上 (p 为服务商提出的服务费率; w 为等待的区块确认数; v 为混币的数量)。由于市场上会有多个相互竞争的混淆服务商, 用户可以根据混淆服务商的价格、服务质量等因素来选择合适的服务商。

2) 假设用户 A 选择了服务商 M 为其服务。A 需要在 t_1 时间前向服务商 M 发送自身期望的协议参数, 其中 $D=\{v, w, p, t_1, t_2, t_3, t_4, t_5, K_{in}\}$ 。同时,

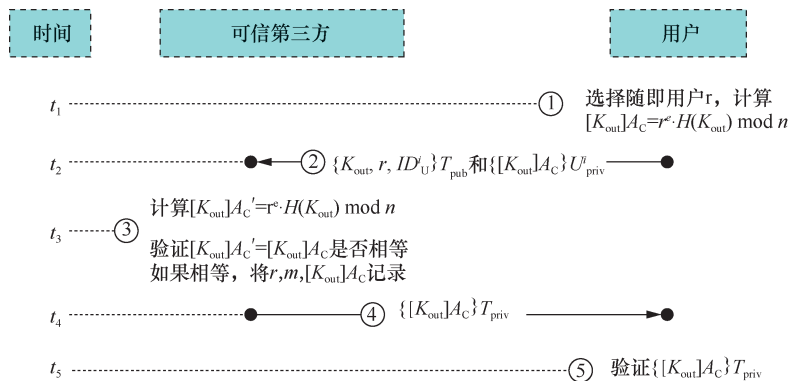


图2 用户注册阶段流程

表 1 协议参数信息

参数	含义
A	Alice 的真实身份
A'	Alice 的隐藏身份, 即 Alice 使用 Tor 匿名网络隐藏身份
K_{in}	A 的支付地址, 可能已经被链接到自身的真实身份
K_{out}	A 期望的交付地址, 一般由用户新创建的比特币地址
K_{esc}	M 接受 A 转钱的地址, 对于每个用户都生成一个对应的唯一地址
K_{esc}'	M 往地址 K_{out} 转钱的地址
A_C	盲签名中的盲化函数
A_C'	盲签名中的去盲函数
$[K_{out}]A_C$	使用盲化函数将 K_{out} 进行盲化
x	混淆服务商存储到可信第三方的比特币金额
p	支付的混淆服务费用的比率
v	混淆的单位金额
w	比特币系统中的区块确认个数

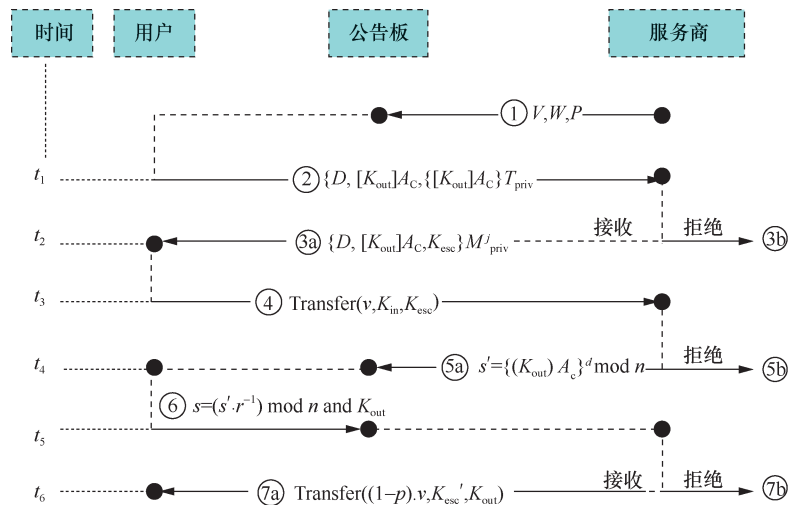


图 4 混淆阶段流程

用户 A 将 K_{out} 盲化后的值 $[K_{out}]A_C$ 以及可信第三方的签名 $\{[K_{out}]A_C\}T_{priv}$ 发送给服务商 M。

3a) 若服务商 M 接受了用户 A 的服务请求, 则用自身私钥 M_{priv} 对 $\{D, [K_{out}]A_C\}$ 和比特币接收地址 K_{esc} 签名, 并在 t_2 之前发送给用户 A。

3b) 若用户期望的收费率 p 过低或其他原因导致服务商 M 选择不接受用户的请求, 则结束本

次协议。用户可以向其他的混淆服务商发送请求。

4) 用户 A 收到混淆服务商同意参数的确认信息, 会将约定好的 v 比特币在 t_3 之前从地址 K_{in} 转入到 K_{esc} 中。

5a) M 等待步骤 4) 中的交易获得比特币网络中 w 个区块的确认, 再计算 $s' = \{[K_{out}]A_C\}^d \bmod n$ 。需要注意的是, 该步是对盲消息签名的过程, M

对 $[K_{out}]A_C$ 签名, 而不是 K_{out} 。因此, 服务商 M 无法知道 K_{in} 和 K_{out} 之间的联系。 M 需要在 t_4 之前发送 $\{[K_{out}]A_C\}M_{priv}$ 到比特币公告板。

5b) 若服务商 M 在收到用户 A 的转账交易后, 未在事先约定的时间 t_4 之前将确认信息发送给用户。用户 A 会认为混淆服务商拒绝了此次服务。此时, 用户 A 需要将之前的交易和请求信息, 以及比特币转账交易 $Transfer(v, K_{in}, K_{esc})$ 发送给可信第三方。可信第三方确认这些证据后, 会从对应服务商 x 比特币的保证金中支付 v 比特币给用户, 同时对服务商实施相应的惩罚。

6) 用户 A 收到 s' 后, 使用去盲函数 A_C' 计算出服务商签名的信息 $s=(s' \cdot r^{-1}) \bmod n$ 。在 t_5 时间内, 用户使用Tor匿名网络在IP层进行伪装, 并将 K_{out} 的签名和 K_{out} 发送至公告板上。使用Tor匿名网络是为了防止攻击者在IP层实施攻击, 将用户和 K_{out} 地址联系起来。此时, 若用户拒绝将 K_{out} 的签名和 K_{out} 发送至公共板上, 则用户将不会受到服务商的服务, 且转给服务商的资金将无法动用, 得不偿失。

7a) 服务商 M 获取公告板上的用户信息后, 能够验证 K_{out} 上的签名信息是否来自自己, 但无法知道该信息是哪一次的签名。服务商 M 在 t_6 之前构造交易, 从自身的比特币地址 K_{esc} 转移 $(1-p)v$ 比特币至 K_{out} , 并将该交易发送至比特币交易网络。

7b) 若混淆服务商拒绝转入资金到 K_{out} , 用户 A 会将之前的交易和请求信息, 以及在比特币交易网络中的转账交易 $Transfer(v, K_{in}, K_{esc})$ 发送给可信第三方。可信第三方确认证据后, 将从对应服务商的保证金中返还 v 比特币给用户, 同时对服务商实施相应的惩罚。

4.5 追责阶段

如果恶意混淆服务商窃取了用户资金, 如图4

中的所有(b)操作所示, 可信第三方可以从服务商提交的保证金中拿出 v 比特币偿还给用户, 并对恶意的混淆服务商实施惩罚措施。

如果用户使用混淆服务进行违法操作, 即 K_{out} 中的资金被用于违法操作。可信第三方可以通过 K_{out} 查询之前存储的用户信息元组, 来对应用户身份信息 $ID_{U,I}$, 进而实施惩罚措施。

4.6 协议参数说明

本协议设置了服务费率 p 、区块确认数 w 、混币数 v 、保证金额度 x 等可变参数, 提高了协议的弹性。这些参数的变化, 可能会对协议的效率产生一定影响, 下文将对这些参数进行相关分析。

p 为混淆服务商的服务费率。它使服务商从诚实的行为中获利, 从而减少服务商停止运营或者窃取用户资金的风险。在稳定的情况下, 混淆服务商有两种选择: 一种是诚实地进行操作, 赚取每次混淆交易的收入; 另一种是窃取 K_{esc} 地址中的资金, 并停止运营。因此, p 的取值需要在一段时间内混淆服务商能够赚取的费用和某个时间节点服务商窃取用户资金获得的收益之间进行平衡。另外, p 还会受到混淆服务商之间竞争因素影响, 安全、快速、低费的服务商自然更容易受到用户的欢迎。

w 为比特币区块链上的区块确认数量。协议中使用参数 w 改变区块确认的数量, 来满足不同用户的需求。 w 值越大, 交易越安全, 但相应的混淆时间也越长。一般情况下, 经过6个区块的确认就可以认为该区块上的信息不可再被篡改。因此, 协议中参数 w 默认值为6。

v 为每次混淆的比特币个数。一次混淆需要多个用户同时参与, 且同一批混淆的用户转给混淆服务商的资金数值要保证一致。若用户1转入1比特币, 用户2转入0.5比特币, 则攻击者能够轻松地将输入地址和输出地址关联, 导

致混淆失败。因此,本文提出了需要协商的参数 v , v 值相同的用户将会一起进行混淆操作。需要注意的是,大额的比特币拆分成多个小额资金进行混淆,又利用快速混淆,减少用户等待时间。

x 为服务商的保证金额度。可信的第三方可能是政府或者银行等机构,协议要求 x 值远大于 pv , 从而降低混淆服务商窃取用户资金的概率。另外, x 过高会导致服务商的成本上升,进而转嫁到用户身上,甚至一部分服务商会因为负担过重选择停止运营。

5 性能分析

本节对 RBmix 协议的特性进行分析,具体分析如下。

1) 可监管性: RBmix 协议使用了 RSA 公平盲签名^[26]算法,并引入了可信第三方。一旦用户使用混淆后的货币进行违法操作,可信第三方可以揭示出用户的真实身份并实施惩罚措施,从而保证协议的可监管性。

2) 匿名性: 协议的匿名性由盲签名技术和 Tor 匿名网络来保证,前者直接作用于应用层,而后者则作用在网络层。由上述协议过程可知,签名信息 $\{D, [K_{out}]A_C, K_{esc}\}M_{priv}$ 由混淆服务商发出,用户收到后向 M_{priv} 转移 v 比特币。服务商在收到比特币后,对 K_{out} 进行盲签名,其无法知道具体的 K_{out} 地址信息。用户收到 s' 后,进行去盲化处理,得到 K_{out} 的签名信息 s ,并使用匿名网络将 s 和 K_{out} 发布到公告板上。该 K_{out} 已经被混淆服务商签名,但服务商并不知道对应的是哪一次的签名,更无法知道对应的是哪一个用户的输出地址。匿名网络可以保证攻击者无法在网络层联系用户的输入地址和输出地址。服务商确定是自身的签名后,从自己的 K_{esc}' 向 K_{out} 地址转入 $(1-p)v$ 比特币。整个过程,混

淆服务商无法联系用户的输入地址和输出地址,更无法区分每个用户的输出地址。对于外部攻击者来说,其只能获取比特币区块交易信息和公告板信息,无法找出用户输入地址和输出地址之间的联系。

3) 可扩展性: 对于大规模的用户混淆服务请求,混淆服务商可以动态地增加服务器数量来适应市场需求。而其他分布式的混淆方案往往受限于混淆用户的数量,如 Coinjoin 仅能够支持十位数左右的用户混淆。因此,本文提出的协议具有良好的可扩展性。

4) 可追责性: 用户可以拿出证据证明服务商确实存在违规操作,可信第三方机构证实后会实施相应的惩罚措施,普通用户也会因为混淆服务商信誉度降低而选择其他更加优质的服务商。

5) 比特币兼容性: 整个协议作为一种服务兼容于比特币系统,不需要对比特币进行任何的软分叉和硬分叉操作。混淆服务独立于整个比特币系统运行,希望使用混淆服务的用户可以花费服务费购买混淆服务,从而保护自己的隐私。

6) 抗 DoS 攻击性: 不同于一些比特币隐私保护的协议(如 Coinjoin)很难防止 DoS 攻击,本文的协议设计了保证金和追责制度,可以抵抗 DoS 攻击,任何理性的用户和竞争者都不会攻击服务商。

由于本协议专注于应用层的安全,仅依赖 Tor 匿名网络保证协议在网络层中的匿名性,因此网络层中的其他问题(如网络的强同步性问题)会对本协议产生一定的影响。例如,用户正确执行了协议,但由于网络延迟或攻击者的拦截,服务商未能及时获取转账信息从而影响服务质量,这部分也是未来工作需要解决的问题。

表2 与其他方案的性能对比

方案	可追责性	可扩展性	架构	比特币兼容	抗 DoS 攻击	可监管性
RBmix	√	√	服务	√	√	√
Coinjoin	-	×	服务	√	×	×
Coinswap	-	×	服务	√	√	×
Mixcoin	√	√	服务	√	√	×
Blindcoin	√	√	服务	√	√	×
Zerocoin	-	√	服务	×	√	×

与现有的基于中心服务商架构的混淆方案相比,本协议同时具有可追责性、可扩展性、比特币兼容性、抗 DoS 攻击以及可监管性,其余方案则各有自身的局限性,如 Coinjoin 不具备可追责性、可扩展性、抗 DoS 攻击性和可监管性。具体如表 2 所示。

6 实验测试

本文对 RBmix 协议进行实现,从而验证协议的性能。实验的主要开发语言为 Go 语言,并利用了比特币全节点客户端 Btcd 开源项目,以及比特币用户钱包 Btcwallet 项目。其中,Go 语言版本为 1.8.4, Btcd 版本为 0.12.0-Beta, Btcwallet 版本为 0.7.0-Alpha。

实验利用 Go 语言中的 Goroutine 多线程机制模拟多个用户,使用 Btcd 模拟比特币区块链,并使用 Btcwallet 作为用户比特币钱包,通过设定不同的用户数量集,测试整个系统在不同数量级用户下的运行时间。

实验在比特币测试网络中运行,首先通过 cmd 命令启动 Btcd 和 Btcwallet 以搭建系统运行环境。接着,使用 IntelliJ IDEA 开发工具运行系统工程,并启动服务端。服务端启动成功后,再模拟用户启动客户端,并通过客户端向服务端发送相关的服务请求。实验利用 `http://localhost:8082/` 地址模拟混淆服务商的服务地

址,使用多线程启动多个客户端同时访问服务器,来模拟大量用户进行混淆服务的过程,从而保证性能测试实验的真实性和可靠性。实验结果如图 5 所示。

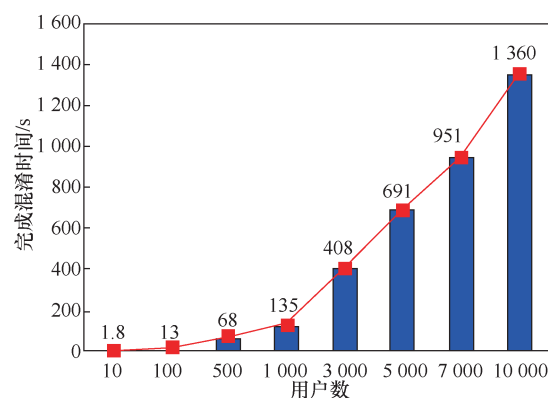


图5 协议实验结果

其中,横轴代表同一时间参与混淆的用户个数,纵轴代表所有用户完成混淆的时间,以秒为单位。当实验运行 1 000 个用户时,大约需要 135 s 来完成相应的操作,5 000 个用户大约需要 691 s, 10 000 个用户大约需要 1 360 s。与预期结果相同,随着用户数量的增长,总运行时间呈线性增长,为每个用户执行混淆的时间大约在 0.2 s。同时,在本实验中,只有一台 PC 作为服务器来执行混淆任务,中心化混淆服务商机制保证了本协议的高度可扩展性,随着用户数量的不断增加,服务商可以设置多个服务器执行并行工作来同时满足所有用户的需求。对于单独的用户来说,比特币区

块 60 min 的确认时间相比较于整个协议流程和交易构造的时间可以忽略不计。

7 结束语

本文分析了比特币隐私保护研究的难点,提出了一种可监管的比特币隐私保护混淆方案。该方案大大降低了中心机构违约的可能性,并保证了必要时协议的可追责能力,为比特币匿名性与可监管性之间的冲突问题提供了新的解决思路。本文通过实验验证了该协议能够在真实的比特币交易环境中良好地运行,且具有高度可扩展性。

参考文献:

- [1] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008: 1-9.
- [2] SYMITSI E, CHALVATZIS K J. The economic value of Bitcoin: a portfolio analysis of currencies, gold, oil and stocks[J]. *Research in International Business and Finance*, 2019, 48: 97-110.
- [3] NARAYANAN A, BONNEAU J, FELTEN E, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction[M]. Princeton University Press, 2016.
- [4] BONNEAU J, MILLER A, CLARK J, et al. Sok: Research perspectives and challenges for bitcoin and cryptocurrencies[C]//IEEE Symposium on Security and Privacy (SP). 2015: 104-121.
- [5] REID F, HARRIGAN M. An analysis of anonymity in the Bitcoin system[M]. *Security and privacy in social networks*. New York: Springer, NY, 2013: 197-223.
- [6] MEIKLEJOHN S, POMAROLE M, JORDAN G, et al. A fistful of Bitcoins: characterizing payments among men with no names[C]//2013 Internet measurement conference. ACM, 2013: 127-140.
- [7] KOSHY P, KOSHY D, MCDANIEL P. An analysis of anonymity in Bitcoin using P2P network traffic[C]. *International Conference on Financial Cryptography and Data Security*. 2014: 469-485.
- [8] PARINO F, BEIRÓ M G, GAUVIN L. Analysis of the Bitcoin blockchain: socio-economic factors behind the adoption[J]. *EPJ Data Science*, 2018, 7(1): 38.
- [9] 樊云慧. 比特币监管的国际比较及我国的策略[J]. *法学杂志*, 2016, 37(10): 116-123.
FAN Y H. International comparison of Bitcoin supervision and China's strategy[J]. *Law Science Magazine*, 2016, 37(10): 116-123.
- [10] 中国人民银行等五部委. 关于防范比特币风险的通知[R]. 2013. Five ministries of China. Announcement on preventing Bitcoin risk[R]. 2013.
- [11] 中国人民银行等七部委. 关于防范代币发行融资风险的公告[R]. 2017. Seven ministries of China. Announcement on the prevention of financing risk of token issuance[R]. 2017.
- [12] 银保监会. 关于国内 ICO 平台和比特币交易通知[R]. 2018. China Banking and Insurance Regulatory Commission. Announcement on domestic ICO platform and Bitcoin transactions[R]. 2018.
- [13] MAXWELL G. CoinJoin: bitcoin privacy for the real world[C]//Post on Bitcoin forum. 2013.
- [14] MAXWELL G. CoinSwap: transaction graph disjoint trustless trading[J]. *CoinSwap: Transaction Graph Disjoint Trustless Trading*, 2013, (10).
- [15] 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.
- [16] VALENTA L, ROWAN B. Blindcoin: blinded, accountable mixes for Bitcoin[C]//International Conference on Financial Cryptography and Data Security. 2015: 112-126.
- [17] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: Anonymous distributed e-cash from Bitcoin[C]//2013 IEEE Symposium on Security and Privacy (SP), 2013: 397-411.
- [18] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: decentralized anonymous payments from Bitcoin[C]//2014 IEEE Symposium on Security and Privacy (SP). 2014: 459-474.
- [19] CHEN P W, JIANG B S, WANG C H. Blockchain-based payment collection supervision system using pervasive Bitcoin digital wallet[C]//Wireless & Mobile Computing, Networking & Communications. 2017.
- [20] DANEZIS G, MEIKLEJOHN S. Centrally banked crypto currencies[C]//Network and Distributed System Security Symposium. 2016.
- [21] 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.
- [22] CORRIGAN-GIBBS H, FORD B. Dissent: accountable anonymous group messaging[C]//The 17th ACM Conference on Computer and Communications Security. 2010: 340-350.
- [23] RUFFING T, MORENO-SANCHEZ P, KATE A. P2P mixing and unlinkable bitcoin transactions[C]//NDSS. 2017.
- [24] IBRAHIM M H. SecureCoin: a robust secure and efficient protocol for anonymous Bitcoin ecosystem[J]. *IJ Network Security*, 2017, 19(2): 295-312.
- [25] GOLDWASSER S, MICALI S, RACKOFF C. The knowledge complexity of interactive proof systems[J]. *SIAM Journal on Computing*, 1989, 18(1): 186-208.
- [26] TU K V, MEREDITH M. Rethinking virtual currency regulation in the Bitcoin age[J]. *Social Science Electronic Publishing*, 2015,

90: 271.

- [27] RAFAELI S. The electronic bulletin board: a computer-driven mass medium[J]. Social Science Micro Review, 1984, 2(3): 123-136.
- [28] VAN DEN HEUVEL A P, COMROE R A, SOBTI A, et al. Bulletin board resource for communication system access[P]. 1994.
- [29] ANTONOPOULOS A M. Mastering Bitcoin: unlocking digital crypto currencies[M]. O'Reilly Media, Inc. 2014.
- [30] CHAUM D. Blind signatures for untraceable payments[C]// Advances in Cryptology. 1983: 199-203.
- [31] STADLER, MARKUS J M PIVETEAU, CAMENISCH J. Fair blind signatures[C]//Advances in Cryptology — EUROCRYPT '95. 1995.
- [32] SYVERSON P, DINGLEDINE R, MATHEWSON N. Tor: the second-generation onion router[C]//Usenix Security. 2004.



张永欣（1996-），男，山东济宁人，东北大学硕士生，主要研究方向为区块链、密码学。



王斌（1992-），男，辽宁鞍山人，东北大学硕士生，主要研究方向为区块链智能合约漏洞检测。

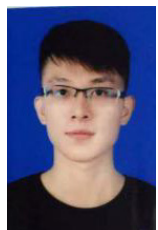
[作者简介]



包子健（1994-），男，安徽黄山人，东北大学硕士生，主要研究方向为区块链隐私保护、区块链系统。



鲁宁（1984-），男，内蒙古包头人，博士，东北大学副教授、硕士生导师，主要研究方向为网络安全。



王庆豪（1995-），男，江苏盐城人，东北大学硕士生，主要研究方向为区块链、可信硬件。



史闻博（1980-），男，河北唐山人，博士，东北大学教授、博士生导师，主要研究方向为密码协议。