计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210600242

一种可追溯的比特币混淆方案

于七龙　鲁　宁　史闻博
东北大学秦皇岛分校计算机与通信工程学院　河北 秦皇岛 066004
(yuqilong@neuq.edu.cn)

摘　要　混淆技术是以比特币为代表的数字货币隐私保护的重要手段,然而,比特币中的混淆技术一方面保护了用户隐私,另一方面却为勒索病毒、比特币盗窃等非法活动提供了便利。针对该问题,提出了一种可追溯的比特币混淆方案,该方案旨在保护合法用户隐私的同时,可对非法资产混淆进行追溯。该方案在中心化比特币混淆基础上引入可信第三方分发用户签名密钥与监管混淆过程,用户签名密钥由基于双线性群和强 Diffie-Hellman 假设的群签名算法构造,以提供签名的匿名性与可追溯性。当有资产追溯需求时,可信第三方通过系统私钥打开用户签名以确定混淆输出地址,从而确定非法资产转移路径。安全分析表明,该方案不用修改当前比特币系统数据结构即可实施,可对非法资产混淆转移路径进行追溯,同时保护合法用户隐私与资产安全,且可抗拒绝服务攻击。此外,该方案为数字货币隐私保护研究提供了参考方向。

关键词:区块链;隐私保护;比特币混淆;可追溯;群签名
中图法分类号　TP309

Traceable Mixing Scheme for Bitcoin

YU Qi-long, LU Ning and SHI Wen-bo
School of Computer and Communication Engineering, Northeastern University at Qinhuangdao, Qinhuangdao, Hebei 066004, China

Abstract　Mixing is an important way for privacy protection among digital currency such as Bitcoin. However, on the one hand, Bitcoin mixing protects user privacy, on the other hand, it facilitates the transfer of assets for illegal activities such as ransomware and Bitcoin theft. In this paper, we propose a traceable scheme for Bitcoin mixing. The scheme aims to protect the privacy of legitimate users and can trace the illegal assets. The system is regulated by trusted third party, user anonymity and traceability based on the group signature which is constructed by bilinear groups and strong Diffie-Hellman assumption. When there is a need for tracing, the regulator can determine the signed user through the system private key, so as to determine the illegal asset transfer path. Security analysis shows that the scheme can trace the illegal asset transfer without modifying the current Bitcoin system, meanwhile, the solution provide privacy protection and asset safety for legitimate users. Furthermore, the scheme provides a reference direction for the research on digital currency privacy protection.

Keywords　Blockchain, Privacy protection, Bitcoin mixing, Traceable, Group signature

1　引言

比特币是一种去中心化的电子现金系统[1]。比特币所有交易存储于基于区块链的公开账本,任何用户都可获取账户地址、账户余额等信息[2]。虽然比特币依靠假名机制提供了一定程度的匿名性,但仍难以抵抗地址关联分析[3]、交易图谱分析[4-5]和找零地址分析[6]等攻击方式,攻击者可通过交易分析确定不同地址的关联关系,从而获得用户的账户数量、账户余额、交易记录等隐私信息。如文献[2]通过完整账本数据构建交易网络,发掘用户间的资产流动信息;文献[3]通过交易图谱聚合用户交易行为,可在零知识情况下进一步推测地址的关联关系;文献[5]通过区块链钱包的应用特征,挖掘出40%左右用户的真实身份。对此,针对比特币现有的数据结构及交易模式,急需相关机制来保护用户地址关联关系、用户资产等隐私数据。

为保护用户隐私,研究者提出比特币混淆策略,即不同用户通过交易交换资产来达到混淆用户地址、提高隐私性与匿名性的目的,典型方案有 CoinJoin[7]、CoinShuffle[8]、CoinParty[9]、Mixcoin[10]、BlindCoin[11]等。然而,隐私保护是一把双刃剑,一方面,比特币混淆可增强用户的匿名性,保护用户敏感信息,另一方面,比特币混淆为用户进行非法资产转移提供了便利,如勒索病毒 Wannacry[12]、黑市购物网站 Silk Road[13]、庞

到稿日期:2021-06-29　返修日期:2021-07-14
基金项目:国家自然科学基金(62072093,U1708262);河北省自然科学基金(F2020501013)
This work was supported by the National Natural Science Foundation of China(62072093,U1708262) and Natural Science Foundation of Hebei Province,China(F2020501013).
通信作者:史闻博(shiwb@neuq.edu.cn)

氏骗局[14]、比特币盗窃[15]等非法活动，均通过比特币混淆进行非法资产转移。一个好的比特币混淆方案不仅应保护用户隐私，还应避免助长违法犯罪活动，因此比特币混淆应对隐私保护有所区分，对于合法资产混淆，隐私保护需防止用户敏感信息泄露；对于非法资产混淆，比特币混淆应提供资产追溯功能，避免成为犯罪逃匿工具。

针对非法比特币资产混淆追溯的问题，本文提出了一种可追溯的比特币混淆方案。首先，该方案引入混淆服务商提供比特币混淆服务，并引入可信第三方监管混淆过程，第三方分发用于用户地址传递的签名私钥，必要时，可由第三方与服务商协作打开用户签名以确定用户身份；其次，基于群签名的隐私性与可验证性，该方案采用基于双线性群和强 Diffie-Hellman 假设的群签名算法构造用户签名方案，在保证签名算法安全性的同时，提供签名追溯功能。

在以上方案的基础上，本文对混淆方案的匿名性、资产安全性、抗拒绝服务攻击性、兼容性等方面进行了理论性能分析，结果显示，该方案与现有比特币系统兼容，且具有良好的匿名性、资产安全性、抗拒绝服务攻击性等性能。

本文第 2 节介绍了相关工作及本文的贡献；第 3 节介绍了签名算法的相关背景知识；第 4 节介绍了本文提出的比特币混淆方案；第 5 节对本文方案进行了安全性与性能分析；最后总结全文并展望未来。

2 相关工作

比特币混淆是比特币隐私保护的重要途径。比特币混淆用于混淆不同地址间的关联关系，按照参与角色的不同，比特币混淆可分为去中心化混淆与中心化混淆两种方案。去中心化混淆由不同用户自发共同组建一笔交易，从而混淆用户输入地址与接收地址的关联关系，此类方案有 CoinJoin[7]，CoinShuffle[8]，CoinParty[9]等。去中心化混淆可在不依赖第三方节点的情况下有效避免资金偷窃、服务费等问题，但在执行混淆过程中，存在用户寻找其他混淆用户困难的问题，且恶意节点可通过违规操作以较低成本实现拒绝服务攻击。中心化混淆由第三方服务商提供混淆服务，服务商接受若干用户资产后再返还用户，从而割裂用户输入地址与接收地址的关联关系，此类方案有 BitLaundry[16]，Mixcoin[10]，BlindCoin[11]等。中心化混淆简单易行，但面临资产被服务商窃取的风险，且服务商知晓用户输出地址与接收地址的映射关系，存在用户信息泄露的风险。

针对区块链公开账本中的用户隐私泄露问题，研究者提出了账本数据加密方案[17-18]。2013 年，Miers 等[19]基于比特币提出 ZeroCoin 方案，该方案通过基于强 RSA 假设的密码累加器将比特币转换为私密资产，用户通过知识签名零知识证明秘密资产与比特币的对应关系，从而隐藏资产的关联关系。2014 年，Sasson 等[20]提出了 ZeroCash 方案，该方案中用户可隐藏交易的输入地址、输出地址及交易金额等隐私信息，并通过零知识证明技术验证交易的正确性。以上方案均可有效保护用户隐私，但比特币网络不支持加密交易，因此以上方案均无法直接用于比特币系统。

为避免数字货币助长违法犯罪，研究者提出了数字货币的监管方案。2014 年，Ateniese 等[21]提出了可认证的比特币，所有用户地址由可信第三方认证，将认证后的地址嵌入第三方的签名，进而实现对用户身份的识别与追踪。2019 年，Wu 等[22]提出可监管的数字货币方案，所有用户交易时需嵌入只有监管方可解密的密文，密文中包含签名与货币私钥，每次交易时监管方记录私钥所有者，从而记录所有货币走向。以上方案可有效避免非法资产转移等违法交易，但这些方案均与比特币的 UTXO 结构不兼容，无法直接用于比特币混淆。

此外，针对比特币混淆资产盗窃问题，研究者提出可监管的比特币混淆方案。2019 年，Bao 等[23]提出了可监管的比特币隐私保护混淆方案，该方案利用公平的 RSA 盲签名算法隐藏输入地址与输出地址的映射关系，利用公告板机制实现公开审计，同时引入可信第三方监管混淆过程。该方案具有良好的资产安全性与匿名性，但可信第三方仅能监管服务商活动，无法追溯非法资产转移。同年，Fei 等[24]提出基于多混淆服务商的强匿名混淆方案，用户向经过可信第三方认证的服务商进行混淆输入以换取资产凭证，并通过该凭证向其他服务商兑换混淆资产，以达到混淆的目的。该方案中用户也可向监管方举报服务商的非法行为，以获得良好的资产安全性，且通过多服务商提高匿名性，但该方案也无法直接追踪用户非法资产的转移路径。

总之，现有部分比特币混淆方案或可提供资产追溯功能，但难以兼顾匿名性及资产安全性等其他功能。如 BitLaundry[16]，MixCoin[10]等典型中心化混淆方案，因服务商知晓参与比特币混淆的用户输入地址与接收地址的映射关系，当需要追溯非法资产时，服务商可直接查询记录获得资产的流动方向，然而，该类比特币混淆方案对服务商无匿名性可言，存在服务商泄露用户隐私及窃取用户资产的风险。

与上述工作相比，本方案利用群签名技术构造用户签名，可信第三方在监管服务商的同时，还监管用户签名过程，当需要追溯非法资产时，由可信第三方打开用户签名来确定用户身份，以追溯资产走向。此外，该方案还具有了良好的匿名性、资产安全性、抗拒绝服务攻击性等性能，且与比特币的 UTXO 模型兼容。

3 背景知识

本节对可追溯的比特币混淆方案所牵涉的背景知识进行了详细描述。

3.1 双线性群

G_1 和 G_2 为 p 阶乘法循环群，即 $|G_1|=|G_2|=p$，其中 p 为素数，且 $G_1=\langle g_1\rangle$，$G_2=\langle g_2\rangle$；ψ 是从 G_2 到 G_1 的可计算同构映射，即 $\psi(g_2)=g_1$；若可计算映射 e 为 $G_1\times G_2\to G_T$ 且具有以下属性：

(1)双线性性：对于所有 $\mu\in G_1$，$\nu\in G_2$ 和 $a,b\in\mathbb{Z}_p$，有 $e(\mu^a,\nu^b)=e(\mu,\nu)^{ab}$；

(2)非退化性：$e(g_1,g_2)\neq 1$，其中 1 为单位元；

则称 e 为双线性映射，(G_1,G_2)为双线性群。

3.2 q-SDH 假设

(G_1,G_2)为双线性群，其 q-SDH(q-Strong Diffie-Hell-

man)问题定义为:以$(q+2)$元组$(g_1, g_2, g_2^{\gamma}, g_2^{(\gamma^2)}, g_2^{(\gamma^3)}, \cdots, g_2^{(\gamma^q)})$为输入,以$(g_1^{1/(\gamma+x)}, x)$为输出,其中$\gamma, x \in \mathbb{Z}_p^*$。若在时间$t$范围内满足:

$$\Pr[\mathcal{A}(g_1, g_2, g_2^{\gamma}, g_2^{(\gamma^2)}, g_2^{(\gamma^3)}, \cdots, g_2^{(\gamma^q)}) = (g_1^{1/(\gamma+x)}, x)] \geqslant \varepsilon$$

则称算法$\mathcal{A}$在时间t范围内解决双线性群(G_1, G_2)中的(q, t, ε)-SDH问题具有优势ε。如果时间t范围内算法$\mathcal{A}$在解决双线性群(G_1, G_2)中的(q, t, ε)-SDH问题时不具有优势ε,则称(q, t, ε)-SDH假设成立。

实际中,(q, t, ε)-SDH常省略t和ε,称为q-SDH假设。q-SDH假设与强RSA假设具有相似属性,常用于构造群签名算法。

3.3 线性判断假设

对于$G_1 = \langle g_1 \rangle$,$|G_1| = p$,其中$p$为素数,$u, v, h \in G_1$,而$a, b, c \in \mathbb{Z}_p^*$,以$(u, v, h, u^a, v^b, h^c)$为输入,若$a+b=c$,则输出true,否则输出false。对于$u, v, h, \eta \xleftarrow{R} G_1$,$a, b \xleftarrow{R} \mathbb{Z}_p^*$,若算法$\mathcal{A}$满足:

$$\Pr_{\mathcal{A}} = |\Pr[\mathcal{A}(u, v, h, u^a, v^b, h^{a+b}) = \text{true}] - \Pr[\mathcal{A}(u, v, h, u^a, v^b, \eta) = \text{true}]| \geqslant \varepsilon$$

则称$\mathcal{A}$在时间t内解决G_1中的线性判断问题具有优势ε,如果在时间t内没有算法解决G_1中的线性判断问题,则称(t, ε)线性判断假设成立。

3.4 群签名

群签名[25]是一种特殊的数字签名,可提供对签名者的匿名性与可追踪性。群签名具有以下属性[26]:

(1)每个群成员可用私钥签名;

(2)验证者可用群公钥验证签名合法性,但无法确定具体的签名者;

(3)群管理员可通过特殊的陷门确定签名者身份。

2004年,Boneh等[27]提出基于强Diffie-Hellman假设和双线性映射的短群签名算法,该算法具有完全匿名性,且可通过系统公钥快速打开用户签名以确定用户身份,用于比特币混淆的用户匿名和签名追溯。

4 可追溯的比特币混淆方案

本节对可追溯的比特币混淆方案进行了详细描述。

4.1 方案模型

图1为方案的系统模型图。该方案中包含用户U_i($i=1, 2, \cdots, n$)、服务商S_j($j=1, 2, \cdots, m$)、监管方M3个角色。用户为具有比特币混淆需求的比特币拥有者,其需求是将输入地址$Input_{U_i}$($i=1, 2, \cdots, n$)上的资产安全转移到接收地址$Output_{U_i}$($i=1, 2, \cdots, n$)上,且网络中任何用户均无法关联$Input_{U_i}$与$Output_{U_i}$的关系;服务商为经过监管方认证的比特币混淆服务提供者,服务商以盈利为目的,拥有混淆接收地址$Output_{S_j}$($j=1, 2, \cdots, m$)与混淆输出地址$Input_{S_j}$($j=1, 2, \cdots, m$);监管方为第三方可信机构,提供密钥分发、追溯签名等服务,且监管方掌握服务商的真实身份信息。

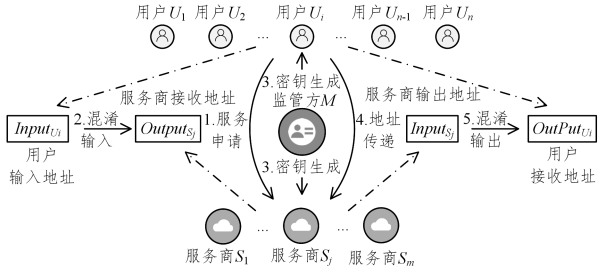

图1 系统模型

Fig. 1 System model

本文方案分为服务申请、混淆输入、密钥生成、地址传递、混淆输出5个阶段,服务申请阶段包括具有比特币混淆需求的用户向服务商发起混淆请求并协商服务参数;混淆输入阶段包括用户将需混淆的比特币通过交易传递给服务商;密钥生成阶段包括监管方确定混淆输入成功后,生成并分发用户签名密钥;地址传递阶段包括用户将用于收取混淆比特币的接收地址匿名传递至服务商,并由服务商进行签名验证;混淆输出阶段包括服务商将混淆后的比特币通过交易传递给用户接收地址。

4.2 方案构造

G_1和G_2是阶为素数p的乘法循环群,G_1的生成元为g_1,G_2的生成元为g_2;$H: \{0,1\}^* \rightarrow \mathbb{Z}_p$为抗碰撞的哈希函数。

图2为方案流程图。其中,初始化过程由监管方完成,用于生成系统公钥、私钥信息;服务申请由用户向服务商发起比特币混淆服务请求,并协商混淆输入时间、密钥分发时间、混淆输出时间等服务参数;混淆输入阶段由用户通过交易完成需混淆的比特币向服务商的转移;密钥生成由监管方在确认混淆输入后向用户分发签名私钥;地址传递由用户对接收地址进行签名后发送至服务商,并由服务商验证签名合法性;混淆输出由服务商完成,在确定用户接受地址合法性后通过交易完成混淆后的比特币输出。

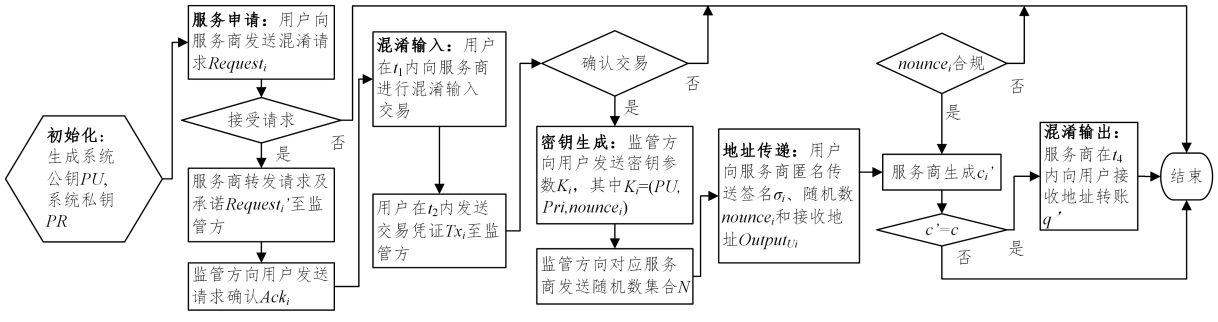

图2 方案流程图

Fig. 2 Flowchart of mixing

(1)初始化

监管方选取相关参数，具体有：$h\in G_1\backslash\{1_{G_1}\}$，$\xi_1,\xi_2,\gamma\in\mathbb{Z}_p^*$，$\omega=g_2^{\gamma}\in G_2$，$\mu,\nu\in G_1$ 且 $\mu^{\xi_1}=\nu^{\xi_2}=h$，输出系统公钥 $PU=\{g_1,g_2,h,\mu,\nu,\omega,H\}$，保留系统私钥 $PR=\{\xi_1,\xi_2,\gamma\}$。

(2)服务申请

本步骤完成用户申请与服务质量参数协商，协商后的服务质量参数由监管方向用户进行服务申请确认。

1)有混淆需求的用户 $U_i(i=1,2,\cdots,n)$向选择的服务商 $S_j(i=1,2,\cdots,n)$发送比特币混淆请求 $Req_i=(t_1,q)$，$(i=1,2,\cdots,n)$，其中 q 为混淆输入金额，t_1 为用户进行混淆输入的最迟时间；

2)若服务商接受用户服务请求，则选择 $r_i\in\mathbb{Z}_p^*$，采用 Pedersen 承诺[28] 算法计算承诺值 $comm=(g_1^{H(Output_{S_j},Input_{S_j},t_1,t_2,t_3,t_4,q)}g_2^{r_i})\bmod p$，其中 $Output_{S_j}$ 为服务商 S_j 提供混淆服务的接收地址，$Input_{S_j}$ 为服务商提供混淆服务的输出地址，t_2 为混淆输入凭据提交最迟时间，t_3 为密钥最迟分发时间，t_4 为服务商进行混淆输出的最迟时间，明显地，$t_1<t_2<t_3<t_4$；

3)服务商将用户请求、混淆输入地址、混淆输出地址、混淆输入金额、操作时间、混淆服务承诺等信息发送至监管方，具体为 $Req_i'=(Req_i,Output_{S_j},Input_{S_j},q,t_1,t_2,t_3,t_4,comm)$；

4)监管方收到服务商信息后，向用户发送混淆请求确认 $Ack_i=(Req_i',t_1,t_2,t_3,t_4)$。

(3)混淆输入

本步骤完成用户资产混淆输入，用户将需混淆的比特币通过交易转移至服务商，并将交易凭据发送至监管方用于换取签名私钥。

1)参与比特币混淆的用户各自在 t_1 时间内将其输出地址 $Input_{U_i}(i=1,2,\cdots,n)$上的比特币转账至服务商的接收地址 $Output_{S_j}$，转账金额为 q，记为 $Tx_i=(Input_{U_i},Output_{S_j},t_1,q)$；

2)用户在 t_2 时间内发送转账凭据 Tx_i 至监管方。

(4)密钥生成

本步骤完成用户签名私钥生成与分发，并通过随机数防止重放攻击。

1)监管方确认交易后，选取 $x_i\in\mathbb{Z}_p^*$，在 t_3 时间内向已发送转账凭据的用户发送密钥消息 $K_i=(PR_i,PU,nounce_i)$ $(i=1,2,\cdots,n)$，其中 $PR_i=(A_i,x_i)$ 为用户签名私钥，且 $A_i^{x_i+\gamma}=g_1$；PU 为群签名公钥；$nounce_i$ 为监管方生成的随机数；

2)监管方向服务商发送随机数集合 $N=\{nounce_1,nounce_2,\cdots,nounce_i\}(i=1,2,\cdots,n)$。

(5)地址传递

本步骤完成用户接收地址的传递与验证。用户将接收地址及签名通过匿名方式发送至服务商，服务商收取地址后进行合法性验证。

1)用户选择随机数 $\alpha,\beta\in\mathbb{Z}_p^*$，计算：

$\mu^{\alpha}\rightarrow T_1$

$\upsilon^{\beta}\rightarrow T_2$

$A_ih^{\alpha+\beta}\rightarrow T_3$

$x_i\alpha\rightarrow\delta_1$

$x_i\beta\rightarrow\delta_2$

2)用户选择盲因子 $r_\alpha,r_\beta,r_x,r_{\delta_1},r_{\delta_2}\in\mathbb{Z}_p^*$，计算：

$\mu^{r_\alpha}\rightarrow R_1$

$\nu^{r_\beta}\rightarrow R_2$

$e(T_3,g_2)^{r_x}\cdot e(h,\omega)^{-r_\alpha-r_\beta}\cdot e(h,g_2)^{-r_{\delta_1}-r_{\delta_2}}\rightarrow R_3$

$T_1^{r_x}\cdot\mu^{-r_{\delta_1}}\rightarrow R_4$

$T_2^{r_x}\cdot\upsilon^{-r_{\delta_2}}\rightarrow R_5$

3)用户计算：

$H(Output_{U_i},T_1,T_2,T_3,R_1,R_2,R_3,R_4,R_5)\rightarrow c_i$；

4)用户计算：

$s_\alpha=r_\alpha+c\alpha$

$s_\beta=r_\beta+c\beta$

$s_{x_i}=r_{x_i}+cx_i$

$s_{\delta_1}=r_{\delta_1}+c\delta_1$

$s_{\delta_2}=r_{\delta_2}+c\delta_2$

5)用户合成签名：

$(c_i,T_1,T_2,T_3,s_\alpha,s_\beta,s_{x_i},s_{\delta_1},s_{\delta_2})\rightarrow\sigma_i$；

6)采用洋葱路由网络 Tor[29](The Onion Router)等方式，匿名发送接收地址、随机数及签名 $S_i=(Output_{U_i},nounce_i,\sigma_i)$至服务商。

7)服务商验证 $S_i=(Output_{U_i},nounce_i,\sigma_i)$中的 $nounce_i$ 是否合规，如果 $nounce_i\notin N$ 或已收到过该随机数，则结束混淆操作；

8)若 $nounce_i\in N$ 且首次收到该值，则服务商计算：

$\mu^{s_\alpha}/T_1^c\rightarrow R_1'$

$\nu^{s_\beta}/T_2^c\rightarrow R_2'$

$(e(T_3,g_2)^{s_{x_i}}\cdot e(h,\omega)^{-s_\alpha-s_\beta}\cdot e(h,g_2)^{-s_{\delta_1}-s_{\delta_2}}\cdot(e(T_3,\omega)/e(g_1,g_2))^c)\rightarrow R_3'$

$T_1^{s_{x_i}}/\mu_1^{s_{\delta_i}}\rightarrow R_4'$

$T_2^{s_{x_i}}/\upsilon_1^{s_{\delta_i}}\rightarrow R_5'$

9)服务商计算：

$H(Output_{U_i},T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')\rightarrow c_i'$；

10)服务商验证 c_i 是否等于 c_i'，若相等则验证通过，若验证不通过，则结束该用户混淆操作。

(6)混淆输出

服务商在 t_4 时间内从输出地址 $Input_{S_j}$ 向用户接收地址 $Output_{U_i}(i=1,2,\cdots,n)$转账 q'，记为 $Tx_i'=\langle Input_{S_j},Output_{U_i},t_4,q'\rangle$，$(i=1,2,\cdots,n)$。其中，$q-q'$为服务商收取的服务费。

4.3 资产追溯

资产追溯指根据用户 $U_k(1\leqslant k\leqslant n)$的混淆输入地址 $Input_{U_k}$ 确定对应的混淆接收地址 $Output_{U_k}$，从而获取资产走向。为保护合法用户的隐私，资产追溯由监管方与服务商配合完成。

首先，根据 $Input_{U_k}$，监管方可查询私钥分配记录以确定其私钥 $PR_k=(A_k,x_k)$；其次，监管方向服务商索取参与该轮混淆的所有用户签名 $\Sigma=\{\sigma_1,\cdots,\sigma_i,\cdots,\sigma_n\}$，其中，$\sigma_i\leftarrow(c_i,T_1,T_2,T_3,s_\alpha,s_\beta,s_{x_i},s_{\delta_1},s_{\delta_2})$；再次，监管方利用系统私钥

$PR=\{\xi_1,\xi_2,\gamma\}$依次计算：

$$\frac{T_3}{T_1^{\xi_1}\cdot T_2^{\xi_2}}=\frac{A_i h^{\alpha+\beta}}{T_1^{\xi_1}\cdot T_2^{\xi_2}}=\frac{A_i\cdot\mu^{\alpha\xi_1}\cdot\nu^{\beta\xi_2}}{T_1^{\xi_1}\cdot T_2^{\xi_2}}=A_i\ (i=1,2,\cdots,n)$$

直到 A_i 等于 A_k，从而确定 U_k 的签名 σ_k；最后，通过服务商查询记录，确定 σ_k 所对应的 $Output_{U_k}$，最终确定进行非法资产转移的用户的输入地址与输出地址的关联关系，即确定非法资产的转移路径。

5 安全性与性能分析

本节通过理论分析对所提方案的安全性与性能进行了评价。

5.1 安全性分析

5.1.1 匿名性分析

匿名性可分为外部匿名性与内部匿名性，外部匿名性指除服务商与用户本身外的其他用户无法知晓用户输入地址与接收地址的映射关系；内部匿名性指服务商无法知晓用户输入地址与接收地址的映射关系。

对于外部匿名性，方案中混淆服务商可有效隔离用户输入地址与输出地址，在服务商可信的情况下，除非将所有参与混淆服务的用户地址聚类分析，否则攻击者难以关联单一用户的输入地址与输出地址。本文方案通过两个方面来保障外部匿名性，一方面是所有用户操作相互独立，互不影响，用户传递接收地址使用群签名算法签名，除监管方外，所有用户无法知晓签名者的真实身份；另一个方面是方案中用户向服务商传递的接收地址通过 Tor 匿名，确保攻击者无法知晓传递接收地址的真实身份。

对于内部匿名性，方案中群签名算法保证对除监管方之外的所有实体完全匿名，任何用户均无法验证签名者，服务商进行签名验证时，仅验证 $H(Output_{U_i},T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')\rightarrow c'$ 是否与 c 相同，验证信息中无任何用户的个人身份信息。此外，系统中用户以匿名方式(Tor)向服务商传递签名与接收地址，使得服务商无法知晓 $Output_{U_i}$ 与 $Input_{U_i}$、$Output_{U_i}$ 与发送者身份的关联关系。

此外，在资产追溯阶段，为保护合法用户的隐私，追溯阶段由监管方与服务商配合完成。监管方打开签名并确定 $Input_{U_k}$ 与 σ_k 的关联关系，下一步由服务商通过 $Input_{U_k}$ 查询与之对应的 $Output_{U_k}$。该方式可有效避免合法用户的混淆输入地址与接收地址关联关系的泄露，保护合法用户的隐私。

5.1.2 资产安全性分析

资产安全性主要防止服务商窃取参与比特币混淆的用户资产。现有中心化比特币混淆方案主要通过两种方法提高资产安全性。一种是要求服务商提供身份对应的电子签名作为承诺，承诺包含服务商约定的接收地址、输出地址、混淆金额、时间约定等内容，即通过虚拟信用机制增强资产的安全性，若服务商窃取用户资产，则用户可公开承诺及账本记录，破坏服务商的信用；另一种是要求服务商提前向第三方支付保证金[23]，对服务商进行约束。以上方案均能一定程度地提高用户资产的安全性，但当参与混淆的用户足够多、总金额足够大时，服务商可能选择放弃信用及保证金，此时用户无法取回相应资产。

本方案中，服务商接受用户比特币混淆服务请求后，需向监管方发送用户申请、服务参数及以 Pedersen 承诺算法计算的承诺值，服务参数包含服务商接收地址 $Output_{S_j}$、输出地址 $Input_{S_j}$、混淆金额 q、用户混淆输入的最迟时间 t_1、确认交易时间 t_2、最迟密钥分发时间 t_3、混淆输出的最迟时间 t_4。普通用户在 t_1 内进行混淆输入后，需在 t_2 时间前向监管方发送交易凭据 Tx_i，以进行交易确认，若超过 t_4 后用户未接收到混淆输出，则用户可向监管方提出仲裁申请，监管方可追溯交易过程，确定服务商是否窃取用户资产。若确定用户资产被窃，一方面监管方可公开服务商承诺，破坏其信誉，另一方面服务商经过监管方的实名认证，监管方掌握服务商的实际身份，可直接进行资产追回。

5.1.3 抗拒绝服务分析

抗拒绝服务攻击用于防止因参与混淆用户有意或无意的违规操作导致所有用户混淆失败。在如 CoinJoin[7]，CoinShuffle[8] 等去中心化混淆方案中，恶意用户可通过拒绝签名、拒绝支付等违规操作导致系统中所有用户的混淆过程失败；CoinParty[9] 通过构建门限托管账户，以参与混淆的用户输入资产作为抵押方式，提高了恶意用户拒绝服务攻击的成本；BitLaundry[16]，MixCoin[10]，BlindCoin[11] 等中心化混淆方案中，抗拒绝服务性能取决于服务商的系统性能。

在本方案中，首先，用户仅与服务商和监管方交互，无法得知任何其他参与混淆用户的交互信息，且每个用户的相关操作相互独立，恶意用户的违规操作不影响其他用户签名与接收地址传递。其次，用户提出的比特币混淆服务申请经服务商与监管方确认后，需先进行混淆输入后才可获得监管方分发的签名私钥，若存在恶意用户拒绝支付，则将直接退出该轮混淆；若恶意用户获得私钥后拒绝签名，则也将因超时自动退出该轮混淆，且会因无混淆输出给自身造成资产损失。此外，服务商接收到加密后的用户接收地址 $Output_{U_i}$ 后，首先会验证签名的合法性，即验证 $H(Output_{U_i},T_1,T_2,T_3,R_1',R_2',R_3',R_4',R_5')\rightarrow c'$ 是否与 c 相同，在保证用户签名合法的情况下，进一步进行混淆输出。

5.1.4 兼容性分析

兼容性指方案是否与当前的比特币系统兼容以允许实际的集成。本方案中，所有交易均不要求改变任何比特币协议，因此与当前比特币结构兼容。

5.2 性能分析

表 1 列出了不同混淆方案的性能对比结果。CoinJoin[7]，CoinShuffle[8]，CoinParty[9] 等典型去中心化比特币混淆方案有良好的外部匿名性与资产安全性，但均面临拒绝服务攻击风险；BitLaundry[16]，MixCoin[10]，BlindCoin[11] 等典型中心化比特币混淆方案虽具有良好的外部匿名性，但普遍存在内部匿名性风险，且用户资产容易被混淆服务商盗窃；以 ZeroCoin[19] 为代表的加密货币，虽具有良好的外部匿名性、内部匿名性与资产安全性，但该方案与比特币现有数据结构不兼容，无法直接应用于比特币或其他数字货币的混淆与隐私保护。此外，BitLaundry[16] 和 MixCoin[10] 方案也提供了比特币混淆的可追溯性，但该功能是以牺牲内部匿名性为代价的。总之，上述方案均无法同时保障用户隐私、系

统健壮性与可追溯性。

表1 不同方案的理论性能

Table 1 Theoretical performance of different scheme

方案名称	中心化	外部匿名性	内部匿名性	资产安全性	抗拒绝服务攻击	可追溯性	比特币系统兼容性
CoinJoin[7]	否	是	否	是	否	否	是
CoinShuffle[8]	否	是	是	是	否	否	是
CoinParty[9]	否	是	是	存在风险	弱	否	是
ZeroCoin[19]	否	是	是	是	是	否	否
BitLaundry[16]	是	是	否	否	弱	是	是
MixCoin[10]	是	是	否	存在风险	弱	是	是
BlindCoin[11]	是	是	是	存在风险	弱	否	是
本文方案	是	是	是	是	强	是	是

本文方案引入第三方监管机构，通过群签名算法的匿名与可验证等特性，提供了比特币混淆的可追溯性。此外，本文方案有效解决了匿名性、资产安全性等问题，并通过提前混淆输入提高了恶意用户的攻击成本，提高了系统的安全性，且方案中每个用户的混淆输入与输出互不影响，保证恶意用户无法通过拒绝签名等方式进行拒绝服务攻击，同时，本文方案不改变比特币的数据结构，可直接应用于现有比特币系统。

结束语 针对传统比特币混淆方案助长非法资金转移等犯罪的问题，本文提出了一种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，利用群签名算法构造用户签名，保证签名的匿名性与可监管性。该方案不用修改当前比特币数据结构即可实施，可实现非法资产转移的追溯，并保护合法用户的隐私。此外，该方案具有匿名性、资产安全性、抗拒绝服务性，且与比特币系统兼容。现有方案中监管方的计算量较大，且比特币混淆执行的时间较长，下一步将对监管细节进行改进，通过分层群签名技术来提升系统性能。

参 考 文 献

[1] NAKAMOTO S. Bitcoin: A Peer-to-Peer Electronic Cash System. [EB/OL]. [2021-05-20]. https://bitcoin.org/bitcoin.pdf.

[2] HE P, YU G, ZHANG Y F, et al. Survey on Blockchain Technology and Its Application Prospect [J]. Computer Science, 2017, 44(4): 1-7.

[3] REID F, HARRIGAN M. An Analysis of Anonymity in the Bitcoin System [C]// 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and 2011 IEEE Third International Conference on Social Computing. Boston: IEEE Press, 2011: 1318-1326.

[4] FLEDER M, KESTER M S, PILLAI S. Bitcoin Transaction Graph Analysis. [EB/OL]. (2015-02-06) [2021-01-20]. https://arxiv.org/pdf/1502.01657.pdf.

[5] MICHA O, STEFAN K, KAY H. Structure and Anonymity of the Bitcoin Transaction Graph [J]. Future Internet, 2013, 5(2): 237-250.

[6] ANDROULAKI E, KARAME G O, ROESCHLIN M, et al. Evaluating User Privacy in Bitcoin [C]// International Conference on Financial Cryptography and Data Security. Berlin: Springer Press, 2013: 34-51.

[7] MAXWELL G. CoinJoin: Bitcoin privacy for the real world [EB/OL]. (2021-03-27) [2021-05-27]. https://en.bitcoin.it/wiki/CoinJoin.

[8] RUFFING T, MORENO-SANCHEZ P, KATE A. CoinShuffle: Practical Decentralized Coin Mixing for Bitcoin [C]// European Symposium on Research in Computer Security (ESORICS). Berlin: Springer Press, 2014: 345-364.

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

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

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

[12] BISTARELLI S, MATTEO P, FRANCESCO S. Visualizing Bitcoin Flows of Ransomware: WannaCry One Week Later. [EB/OL]. (2018) [2021-05-20]. http://ceur-ws.org/Vol-2058/paper-13.pdf.

[13] CHRISTIN N. Traveling the silk road: a measurement analysis of a large anonymous online marketplace [C]// The 22nd international conference. New York: ACM, 2013: 213-224.

[14] BARTOLETTI M, PES B, SERUSI S. Data mining for detecting Bitcoin Ponzi schemes [C]// 2018 Crypto Valley Conference on Blockchain Technology (CVCBT). Zug: IEEE Press, 2018: 75-84.

[15] GHOSHAL A. Chinese Bitcoin exchange Bter will pay back users after losing $1.75 million in cyberattack. [EB/OL]. (2015-03-12) [2021-01-22]. https://thenextweb.com/insider/2015/03/12/chinese-bitcoin-exchange-bter-will-pay-back-users-after-losing-1-75-million-in-cyberattack/.

[16] BITCOIN W. BitLaundry. [EB/OL]. (2019-06-10) [2021-06-10]. https://en.bitcoin.it/wiki/BitLaundry.

[17] XU C J, LI X F. Data Privacy Protection Method of Block Chain Transaction [J]. Computer Science, 2020, 47(3): 281-286.

[18] ZHANG X Y, LI Q W, FU F J. Secret Verification Method of Blockchain Transaction Amount Based on Digital Commitment [J/OL]. Computer Science, https://kns.cnki.net/kcms/detail/50.1075.TP.20210209.0955.008.html.

[19] MIERS I, GARMAN C, GREEN M, et al. Zerocoin: Anonymous Distributed E-Cash from Bitcoin [C]// 2013 IEEE Symposium on Security and Privacy (SP). New York: IEEE Press, 2013: 397-411.

[20] SASSON E B, CHIESA A, GARMAN C, et al. Zerocash: Decentralized Anonymous Payments from Bitcoin [C]// 2014 IEEE Symposium on Security and Privacy (SP). New York: IEEE Press, 2014: 459-474.

[21] ATENIESE G, FAONIO A, MAGRI B, et al. Certified Bitcoins [C]// International Conference on Applied Cryptography &

Network Security. Berlin: Springer Press, 2014: 80-96.
[22] WU Y B, FAN H N, WANG X Y, et al. A regulated digital currency[J]. Science China, 2019, 62(3): 32190.
[23] 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(4): 40-51.
[24] FEI T L, GUO J, LU N, et al. A Strong Anonymous Obfuscation Scheme for Bitcoin Based on Trusted Regulator[J]. Journal of CAEIT, 2019(9): 960-966.
[25] CHAUM D, VAN H E. Group Signatures [C]// Proceedings of the 10th Annual International Conference on Theory and Application of Cryptographic Techniques. Berlin: Springer Press, 1991: 257-265.
[26] CUI G H, LI J. An Efficient Group Signature Scheme for Large Groups[J]. Computer Science, 2007(2): 79-81.
[27] BONEH D, BOYEN X, SHACHAM H. Short Group Signatures [C] // Annual International Cryptology Conference. Berlin: Springer Press, 2004: 41-55.
[28] DONG G S, CHEN Y X, FAN J, et al. Research on Privacy Protection Strategies in Blockchain Application [J]. Computer Science, 2019, 46(5): 29-35.
[29] DINGLEDINE R, MATHEWSON N, SYVERSON P F. Tor: The Second-Generation Onion Router[C]// 13th USENIX Security Symposium. USENIX, 2004: 21.

YU Qi-long, born in 1988, postgraduate, is a member of China Computer Federation. His main research interests include blockchain and privacy protection .

SHI Wen-bo, born in 1980, Ph. D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include cryptography and blockchain.