



(12)发明专利申请

(10)申请公布号 CN 110335042 A

(43)申请公布日 2019.10.15

(21)申请号 201910563802.6

(22)申请日 2019.06.26

(71)申请人 阿里巴巴集团控股有限公司

地址 英属开曼群岛大开曼资本大厦一座四  
层847号邮箱

(72)发明人 张文彬

(74)专利代理机构 北京博思佳知识产权代理有  
限公司 11415

代理人 李威

(51)Int.Cl.

G06Q 20/38(2012.01)

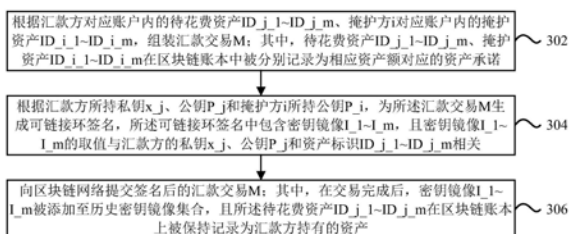
权利要求书5页 说明书25页 附图6页

(54)发明名称

基于环签名的匿名交易方法及装置

(57)摘要

本说明书一个或多个实施例提供一种基于环签名的匿名交易方法及装置,该方法可以包括:根据汇款方对应账户内的待花费资产、掩护方对应账户内的掩护资产,组装汇款交易;其中,待花费资产、掩护资产在区块链账本中被分别记录为相应资产额对应的资产承诺;根据汇款方所持私钥、公钥和掩护方所持公钥,为所述汇款交易生成可链接环签名,所述可链接环签名中包含密钥镜像,且密钥镜像的取值与汇款方的私钥、公钥和资产标识相关;向区块链网络提交签名后的汇款交易;其中,在交易完成后,密钥镜像被添加至历史密钥镜像集合,且所述待花费资产在区块链账本上被保持记录为汇款方持有的资产。



1. 一种基于环签名的匿名交易方法,包括:

根据汇款方对应账户内的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、掩护方 $i$ 对应账户内的掩护资产 $ID_{i_1} \sim ID_{i_m}$ ,组装汇款交易 $M$ ;其中,待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、掩护资产 $ID_{i_1} \sim ID_{i_m}$ 在区块链账本中被分别记录为相应资产额对应的资产承诺;

根据汇款方所持私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 所持公钥 $P_i$ ,为所述汇款交易 $M$ 生成可链接环签名,所述可链接环签名中包含密钥镜像 $I_1 \sim I_m$ ,且密钥镜像 $I_1 \sim I_m$ 的取值与汇款方的私钥 $x_j$ 、公钥 $P_j$ 和资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关;

向区块链网络提交签名后的汇款交易 $M$ ;其中,在交易完成后,密钥镜像 $I_1 \sim I_m$ 被添加至历史密钥镜像集合,且所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 在区块链账本上被保持记录为汇款方持有的资产。

2. 根据权利要求1所述的方法,通过下述公式计算所述密钥镜像 $I_1 \sim I_m$ :

$$I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d}), d \in [1, m];$$

其中, $\text{Hash}_G()$ 为椭圆曲线到其自身的哈希函数。

3. 根据权利要求1所述的方法,所述掩护方包括以下任一或其组合:所述汇款交易 $M$ 的实际收款方、区别于所述汇款方和所述实际收款方的其他用户。

4. 根据权利要求1所述的方法,

当不存在找零时,所述汇款交易 $M$ 的交易收款方为实际收款方;当存在找零时,所述汇款交易 $M$ 的交易收款方为所述汇款方和所述实际收款方;或,

所述交易收款方包括所述实际收款方和所述汇款方;其中,当不存在找零时,所述汇款方对应的转账额为0;或,

所述交易收款方包括所述实际收款方、所述汇款方、区别于所述实际收款方和所述汇款方的掩护方;其中,当不存在找零时,所述汇款方和作为交易收款方的掩护方对应的转账额为0;当存在找零时,所述汇款方对应的转账额为找零额、作为交易收款方的掩护方对应的转账额为0。

5. 根据权利要求1所述的方法,还包括:

针对所述汇款交易 $M$ 的各个交易收款方对应的转账额,分别生成相应的范围证明,所述范围证明被组装至所述汇款交易 $M$ 中,以用于证明相应的转账额不小于0。

6. 根据权利要求1所述的方法,

所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、所述资产 $ID_{i_1} \sim ID_{i_m}$ 为相应的历史交易的交易输出;或,

所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 被从汇款方对应的账户余额中划分而生成、所述资产 $ID_{i_1} \sim ID_{i_m}$ 被从掩护方 $i$ 对应的账户余额中划分而生成。

7. 根据权利要求1所述的方法,根据汇款方所持私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 所持公钥 $P_i$ ,为所述汇款交易 $M$ 生成可链接环签名,包括:

根据待花费资产 $ID_{j_1} \sim ID_{j_m}$ 对应的资产额 $t_{j_1} \sim t_{j_m}$ 、随机数 $r_{j_1} \sim r_{j_m}$ 和资产承诺 $PC(t_{j_1}, r_{j_1}) \sim PC(t_{j_m}, r_{j_m})$ ,以及交易收款方 $Q_1 \sim Q_u$ 对应的转账额 $t'_1 \sim t'_u$ 、随机数 $r'_1 \sim r'_u$ 和转账额承诺 $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ ,确定对应于汇款方的伪公钥 $P''_j = [PC(t_{j_1}, r_{j_1}) + \dots + PC(t_{j_m}, r_{j_m})] - [PC(t'_1, r'_1) + \dots + PC(t'_u, r'_u)]$ 、对应于汇款方的伪私钥 $r'' = (r_{j_1} + \dots + r_{j_m}) - (r'_1 + \dots + r'_u)$ ,  $u \geq$

1;

根据掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>对应的资产承诺PC<sub>{i,1}</sub>~PC<sub>{i,m}</sub>,确定对应于掩护方i的伪公钥P''<sub>i</sub>=[PC<sub>{i,1}</sub>+...+PC<sub>{i,m}</sub>]-[PC(t'<sub>1</sub>,r'<sub>1</sub>)+...+PC(t'<sub>u</sub>,r'<sub>u</sub>)], $i \in [1, j-1] \cup [j+1, n]$ ;

根据汇款方对应的私钥x<sub>j</sub>、公钥P<sub>j</sub>、伪私钥r''、伪公钥P''<sub>j</sub>,掩护方i对应的公钥P<sub>i</sub>、伪公钥P''<sub>i</sub>,为所述汇款交易M生成可链接环签名。

8.根据权利要求7所述的方法,还包括:

根据汇款方对应的伪私钥r''、伪公钥P''<sub>j</sub>,生成密钥镜像I<sub>\_(m+1)}=r''×Hash\_G(P''<sub>j</sub>);其中,所述可链接环签名还包含所述密钥镜像I<sub>\_(m+1)}</sub>。</sub>

9.根据权利要求7所述的方法,根据汇款方对应的私钥x<sub>j</sub>、公钥P<sub>j</sub>、伪私钥r''、伪公钥P''<sub>j</sub>,掩护方i对应的公钥P<sub>i</sub>、伪公钥P''<sub>i</sub>,为所述汇款交易M生成可链接环签名,包括:

分别生成对应于汇款方的中间参数L<sub>j\_d</sub>、R<sub>j\_d</sub>、L<sub>j\_(m+1)}</sub>、R<sub>j\_(m+1)}</sub>,以及对应于掩护方i的中间参数L<sub>i\_d</sub>、R<sub>i\_d</sub>、L<sub>i\_(m+1)}</sub>、R<sub>i\_(m+1)}</sub>, $d \in [1, m]$ ;其中,中间参数L<sub>j\_d</sub>与L<sub>i\_d</sub>之间符合环形取值规则、中间参数L<sub>j\_(m+1)}</sub>与L<sub>i\_(m+1)}</sub>之间符合环形取值规则、中间参数R<sub>j\_d</sub>与R<sub>i\_d</sub>之间符合环形取值规则、中间参数R<sub>j\_(m+1)}</sub>与R<sub>i\_(m+1)}</sub>之间符合环形取值规则,且中间参数L<sub>j\_d</sub>、R<sub>j\_d</sub>、L<sub>j\_(m+1)}</sub>、R<sub>j\_(m+1)}</sub>、L<sub>i\_d</sub>、R<sub>i\_d</sub>、L<sub>i\_(m+1)}</sub>、R<sub>i\_(m+1)}</sub>的取值与至少一个被选取的随机数和/或其衍生数值相关;

根据被选取的随机数和/或其衍生数值,生成针对所述汇款交易M的可链接环签名。

10.根据权利要求9所述的方法,

$P_j = x_j \times G$ ,G为椭圆曲线的基点, $|G|=p$ 且p为素数, $0 < x_j < p$ ;

生成对应于汇款方的中间参数L<sub>j\_d</sub>、R<sub>j\_d</sub>,包括:根据在所述椭圆曲线所处的数域Z<sub>q</sub>中选取的随机数a<sub>d</sub>,计算中间参数L<sub>j\_d</sub>、R<sub>j\_d</sub>,使得 $L_{j_d} = a_d \times G$ 、 $R_{j_d} = a_d \times \text{Hash}_G(P_j, ID_{j_d})$ ;其中,Hash\_G()为从所述椭圆曲线到其自身的哈希函数;

生成对应于汇款方的中间参数L<sub>j\_(m+1)}</sub>、R<sub>j\_(m+1)}</sub>,包括:根据在所述椭圆曲线所处的数域Z<sub>q</sub>中选取的随机数a<sub>(m+1)}</sub>,计算中间参数L<sub>j\_(m+1)}</sub>、R<sub>j\_(m+1)}</sub>,使得 $L_{j_(m+1)} = a_{(m+1)} \times G$ 、 $R_{j_(m+1)} = a_{(m+1)} \times \text{Hash}_G(P''_j)$ ;

生成对应于掩护方i的中间参数L<sub>i\_d</sub>、R<sub>i\_d</sub>、L<sub>i\_(m+1)}</sub>、R<sub>i\_(m+1)}</sub>,包括:根据中间参数L<sub>j\_d</sub>、R<sub>j\_d</sub>的取值,生成中间参数L<sub>i\_d</sub>、R<sub>i\_d</sub>、L<sub>i\_(m+1)}</sub>、R<sub>i\_(m+1)}</sub>,使得 $L_{i_d} = (s_{i_d} \times G + c_i \times P_i) \bmod p$ 、 $R_{i_d} = (s_{i_d} \times \text{Hash}_G(P_i, ID_{i_d}) + c_i \times I_d) \bmod p$ 、 $L_{i_(m+1)} = [s_{i_(m+1)} \times G + c_i \times P''_i] \bmod p$ 、 $R_{i_(m+1)} = [s_{i_(m+1)} \times \text{Hash}_G(P''_i) + c_i \times I_{(m+1)}] \bmod p$ 、 $I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d})$ 、 $I_{(m+1)} = r'' \times \text{Hash}_G(P''_j)$ ;其中,s<sub>i\_1</sub>~s<sub>i\_(m+1)}</sub>为数域Z<sub>q</sub>中的随机数,当i=1时 $c_1 = \text{Hash}(M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}})$ 、当 $i \in [2, j-1] \cup [j+1, n]$ 时 $c_i = \text{Hash}(M, L_{(i-1)_1}, R_{(i-1)_1}, \dots, L_{(i-1)_{(m+1)}}, R_{(i-1)_{(m+1)}})$ ,Hash()为从所述椭圆曲线到数域Z<sub>q</sub>的哈希函数;

被选取的随机数和/或其衍生数值包括:随机数s<sub>i\_1</sub>~s<sub>i\_(m+1)}</sub>、衍生数值c<sub>1</sub>、衍生数值s<sub>j\_1</sub>~s<sub>j\_(m+1)}</sub>;其中, $s_{j_d} = (a_d - c_j \times x_j) \bmod p$ 、 $s_{j_(m+1)} = [a_{(m+1)} - c_j \times r''] \bmod p$ ,当j的取值被确定为1时 $c_j = \text{Hash}(M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}})$ 、当j的取值被确定为属于[2,n]时 $c_j = \text{Hash}(M, L_{(j-1)_1}, R_{(j-1)_1}, \dots, L_{(j-1)_{(m+1)}}, R_{(j-1)_{(m+1)}})$ 。

11. 根据权利要求1所述的方法,还包括:

向区块链网络发起资产删除请求,以从区块链账本中删除所述汇款方已花费的至少一部分资产。

12. 一种基于环签名的匿名交易方法,包括:

接收汇款交易M,所述汇款交易M由汇款方根据自身对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>组装生成;在交易完成后,资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产;

获取所述汇款交易M的可链接环签名包含的密钥镜像I<sub>1</sub>~I<sub>m</sub>,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

验证所述可链接环签名,所述可链接环签名由汇款方根据自身所持的私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持的公钥P<sub>i</sub>而生成;

当满足交易执行条件时,执行所述汇款交易M;所述交易执行条件包括:所述密钥镜像I<sub>1</sub>~I<sub>m</sub>不属于历史密钥镜像集合、所述可链接环签名通过验证;其中,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>在交易完成后被添加至所述历史密钥镜像集合。

13. 根据权利要求12所述的方法,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>由汇款方通过下述公式计算得到:

$$I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d}), d \in [1, m];$$

其中,Hash<sub>G</sub>()为椭圆曲线到其自身的哈希函数。

14. 根据权利要求12所述的方法,所述掩护方包括以下任一或其组合:所述汇款交易M的实际收款方、区别于所述汇款方和所述实际收款方的其他用户。

15. 根据权利要求12所述的方法,

当不存在找零时,所述汇款交易M的交易收款方为实际收款方;当存在找零时,所述汇款交易M的交易收款方为所述汇款方和所述实际收款方;或,

所述交易收款方包括所述实际收款方和所述汇款方;其中,当不存在找零时,所述汇款方对应的转账额为0;或,

所述交易收款方包括所述实际收款方、所述汇款方、区别于所述实际收款方和所述汇款方的掩护方;其中,当不存在找零时,所述汇款方和作为交易收款方的掩护方对应的转账额为0;当存在找零时,所述汇款方对应的转账额为找零额、作为交易收款方的掩护方对应的转账额为0。

16. 根据权利要求12所述的方法,还包括:

根据汇款交易M所含的范围证明,验证各个交易收款方对应的转账额是否均不小于0;

其中,所述交易执行条件还包括:各个交易收款方对应的转账额均不小于0。

17. 根据权利要求12所述的方法,

所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、所述资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>为相应的历史交易的交易输出;或,

所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>被从汇款方对应的账户余额中划分而生成、所述资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>被从掩护方i对应的账户余额中划分而生成。

18. 根据权利要求12所述的方法,所述交易执行条件还包括:资产ID<sub>k\_d</sub>归属于公钥P<sub>k</sub>的所有方,k∈[1,n]、d∈[1,m]、i∈[1,j-1]∪[j+1,n]。

19. 根据权利要求12所述的方法,所述可链接环签名由汇款方根据对应于自身的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r''$ 和伪公钥 $P''_j$ ,以及对应于掩护方 $i$ 的公钥 $P_i$ 和伪公钥 $P''_i$ 而生成,使得当所述可链接环签名通过验证时,所述汇款交易 $M$ 被确认为输入与输出等额;

其中,伪公钥 $P''_j = [PC(t_{j_1}, r_{j_1}) + \dots + PC(t_{j_m}, r_{j_m})] - [PC(t'_{1_1}, r'_{1_1}) + \dots + PC(t'_{u_1}, r'_{u_1})]$ 、伪私钥 $r'' = (r_{j_1} + \dots + r_{j_m}) - (r'_{1_1} + \dots + r'_{u_1})$ 、伪公钥 $P''_i = [PC\{i, 1\} + \dots + PC\{i, m\}] - [PC(t'_{1_1}, r'_{1_1}) + \dots + PC(t'_{u_1}, r'_{u_1})]$ ,  $i \in [1, j-1] \cup [j+1, n]$ , 资产标识 $ID_{j_1} \sim ID_{j_m}$ 对应于资产额 $t_{j_1} \sim t_{j_m}$ 、随机数 $r_{j_1} \sim r_{j_m}$ 和资产承诺 $PC(t_{j_1}, r_{j_1}) \sim PC(t_{j_m}, r_{j_m})$ , 掩护资产 $ID_{i_1} \sim ID_{i_m}$ 对应于资产承诺 $PC\{i, 1\} \sim PC\{i, m\}$ , 交易收款方 $Q_1 \sim Q_u$ 对应于转账额 $t'_{1_1} \sim t'_{u_1}$ 、随机数 $r'_{1_1} \sim r'_{u_1}$ 和转账额承诺 $PC(t'_{1_1}, r'_{1_1}) \sim PC(t'_{u_1}, r'_{u_1})$ ,  $u \geq 1$ 。

20. 根据权利要求19所述的方法,所述可链接环签名还包括密钥镜像 $I_{(m+1)} = r'' \times \text{Hash}_G(P''_j)$ ;

其中,所述交易执行条件还包括:密钥镜像 $I_{(m+1)}$ 不属于所述历史密钥镜像集合。

21. 根据权利要求19所述的方法,汇款方根据对应于自身的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r''$ 、伪公钥 $P''_j$ ,掩护方 $i$ 对应的公钥 $P_i$ 、伪公钥 $P''_i$ ,分别生成对应于汇款方的中间参数 $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}$ ,以及对应于掩护方 $i$ 的中间参数 $L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$ ,并根据与中间参数 $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}$ 、 $L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$ 的取值相关的随机数和/或其衍生数值而生成所述可链接环签名,  $d \in [1, m]$ ;验证所述可链接环签名,包括:

根据所述环签名所含的随机数和/或其衍生数值,计算中间参数 $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}, L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$ ,以验证中间参数 $L_{j_d}$ 与 $L_{i_d}$ 之间是否符合环形取值规则、中间参数 $L_{j_{(m+1)}}$ 与 $L_{i_{(m+1)}}$ 之间是否符合环形取值规则、中间参数 $R_{j_d}$ 与 $R_{i_d}$ 之间是否符合环形取值规则、中间参数 $R_{j_{(m+1)}}$ 与 $R_{i_{(m+1)}}$ 之间是否符合环形取值规则。

22. 根据权利要求21所述的方法,

$P_j = x_j \times G$ ,  $G$ 为椭圆曲线的基点,  $|G| = p$ 且 $p$ 为素数,  $0 < x_j < p$ ;

所述环签名所含的随机数和/或其衍生数值包括: $s_{k_1} \sim s_{k_{(m+1)}}, c_1, k \in [1, n]$ ;

中间参数 $L_{j_d}$ 与 $L_{i_d}$ 之间的环形取值规则包括: $L_{k_d} = (s_{k_d} \times G + c_k \times P_k) \bmod p$ ;其中, $s_{k_d}$ 属于所述椭圆曲线所处的数域 $Z_q$ ,  $\text{Hash}()$ 为从所述椭圆曲线到数域 $Z_q$ 的哈希函数;

中间参数 $L_{j_{(m+1)}}$ 与 $L_{i_{(m+1)}}$ 之间的环形取值规则包括: $L_{k_{(m+1)}} = [s_{k_{(m+1)}} \times G + c_k \times P''_k] \bmod p$ ;其中, $s_{k_{(m+1)}}$ 属于数域 $Z_q$ ;

中间参数 $R_{j_d}$ 与 $R_{i_d}$ 之间的环形取值规则包括: $R_{k_d} = (s_{k_d} \times \text{Hash}_G(P_k, ID_{k_d}) + c_k \times I_d) \bmod p$ ,  $I_d$ 被包含于所述环签名中;

中间参数 $R_{j_{(m+1)}}$ 与 $R_{i_{(m+1)}}$ 之间的环形取值规则包括: $R_{k_{(m+1)}} = [s_{k_{(m+1)}} \times \text{Hash}_G(P''_k) + c_k \times I_{(m+1)}] \bmod p$ ,  $I_{(m+1)}$ 被包含于所述环签名中;

其中,当 $h=1$ 时 $c_1 = \text{Hash}(M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}})$ 、当 $h \in [2, n]$ 时 $c_h = \text{Hash}(M, L_{(h-1)_1}, R_{(h-1)_1}, \dots, L_{(h-1)_{(m+1)}}, R_{(h-1)_{(m+1)}})$ 。

23. 根据权利要求1所述的方法,还包括:

根据所述汇款方向区块链网络发起的资产删除请求,从区块链账本中删除所述汇款方已花费的至少一部分资产。

24. 一种基于环签名的匿名交易装置,包括:

交易组装单元,根据汇款方对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>,组装汇款交易M;其中,待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>在区块链账本中被分别记录为相应资产额对应的资产承诺, $i \in [1, j-1] \cup [j+1, n]$ ;

签名生成单元,根据汇款方所持私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持公钥P<sub>i</sub>,为所述汇款交易M生成可链接环签名,所述可链接环签名中包含密钥镜像I<sub>1</sub>~I<sub>m</sub>,且密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

交易提交单元,向区块链网络提交签名后的汇款交易M;其中,在交易完成后,密钥镜像I<sub>1</sub>~I<sub>m</sub>被添加至历史密钥镜像集合,且所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产。

25. 一种基于环签名的匿名交易装置,包括:

交易接收单元,接收汇款交易M,所述汇款交易M由汇款方根据自身对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>组装生成, $i \in [1, j-1] \cup [j+1, n]$ ;在交易完成后,资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产;

镜像获取单元,获取所述汇款交易M的可链接环签名包含的密钥镜像I<sub>1</sub>~I<sub>m</sub>,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

签名验证单元,验证所述可链接环签名,所述可链接环签名由汇款方根据自身所持的私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持的公钥P<sub>i</sub>而生成;

交易执行单元,当满足交易执行条件时,执行所述汇款交易M;所述交易执行条件包括:所述密钥镜像I<sub>1</sub>~I<sub>m</sub>不属于历史密钥镜像集合、所述可链接环签名通过验证;其中,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>在交易完成后被添加至所述历史密钥镜像集合。

26. 一种电子设备,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器通过运行所述可执行指令以实现如权利要求1-11中任一项所述的方法。

27. 一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如权利要求1-11中任一项所述方法的步骤。

28. 一种电子设备,包括:

处理器;

用于存储处理器可执行指令的存储器;

其中,所述处理器通过运行所述可执行指令以实现如权利要求12-23中任一项所述的方法。

29. 一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如权利要求12-23中任一项所述方法的步骤。

## 基于环签名的匿名交易方法及装置

### 技术领域

[0001] 本说明书一个或多个实施例涉及区块链技术领域,尤其涉及一种基于环签名的匿名交易方法及装置。

### 背景技术

[0002] 区块链技术(也被称之为,分布式账本技术)是一种去中性化的分布式数据库技术,具有去中心化、公开透明、不可篡改、可信任等多种特点,适用于诸多对数据可靠性具有高需求的应用场景中。

### 发明内容

[0003] 有鉴于此,本说明书一个或多个实施例提供一种基于环签名的匿名交易方法及装置。

[0004] 为实现上述目的,本说明书一个或多个实施例提供技术方案如下:

[0005] 根据本说明书一个或多个实施例的第一方面,提出了一种基于环签名的匿名交易方法,包括:

[0006] 根据汇款方对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>,组装汇款交易M;其中,待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>在区块链账本中被分别记录为相应资产额对应的资产承诺;

[0007] 根据汇款方所持私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持公钥P<sub>i</sub>,为所述汇款交易M生成可链接环签名,所述可链接环签名中包含密钥镜像I<sub>1</sub>~I<sub>m</sub>,且密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

[0008] 向区块链网络提交签名后的汇款交易M;其中,在交易完成后,密钥镜像I<sub>1</sub>~I<sub>m</sub>被添加至历史密钥镜像集合,且所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产。

[0009] 根据本说明书一个或多个实施例的第二方面,提出了一种基于环签名的匿名交易方法,包括:

[0010] 接收汇款交易M,所述汇款交易M由汇款方根据自身对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>组装生成;在交易完成后,资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产;

[0011] 获取所述汇款交易M的可链接环签名包含的密钥镜像I<sub>1</sub>~I<sub>m</sub>,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

[0012] 验证所述可链接环签名,所述可链接环签名由汇款方根据自身所持的私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持的公钥P<sub>i</sub>而生成;

[0013] 当满足交易执行条件时,执行所述汇款交易M;所述交易执行条件包括:所述密钥镜像I<sub>1</sub>~I<sub>m</sub>不属于历史密钥镜像集合、所述可链接环签名通过验证;其中,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>在交易完成后被添加至所述历史密钥镜像集合。

[0014] 根据本说明书一个或多个实施例的第三方面,提出了一种基于环签名的匿名交易装置,包括:

[0015] 交易组装单元,根据汇款方对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>,组装汇款交易M;其中,待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>在区块链账本中被分别记录为相应资产额对应的资产承诺, $i \in [1, j-1] \cup [j+1, n]$ ;

[0016] 签名生成单元,根据汇款方所持私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持公钥P<sub>i</sub>,为所述汇款交易M生成可链接环签名,所述可链接环签名中包含密钥镜像I<sub>1</sub>~I<sub>m</sub>,且密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

[0017] 交易提交单元,向区块链网络提交签名后的汇款交易M;其中,在交易完成后,密钥镜像I<sub>1</sub>~I<sub>m</sub>被添加至历史密钥镜像集合,且所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产。

[0018] 根据本说明书一个或多个实施例的第四方面,提出了一种基于环签名的匿名交易装置,包括:

[0019] 交易接收单元,接收汇款交易M,所述汇款交易M由汇款方根据自身对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>组装生成, $i \in [1, j-1] \cup [j+1, n]$ ;在交易完成后,资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>在区块链账本上被保持记录为汇款方持有的资产;

[0020] 镜像获取单元,获取所述汇款交易M的可链接环签名包含的密钥镜像I<sub>1</sub>~I<sub>m</sub>,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>的取值与汇款方的私钥x<sub>j</sub>、公钥P<sub>j</sub>和资产标识ID<sub>j\_1</sub>~ID<sub>j\_m</sub>相关;

[0021] 签名验证单元,验证所述可链接环签名,所述可链接环签名由汇款方根据自身所持的私钥x<sub>j</sub>、公钥P<sub>j</sub>和掩护方i所持的公钥P<sub>i</sub>而生成;

[0022] 交易执行单元,当满足交易执行条件时,执行所述汇款交易M;所述交易执行条件包括:所述密钥镜像I<sub>1</sub>~I<sub>m</sub>不属于历史密钥镜像集合、所述可链接环签名通过验证;其中,所述密钥镜像I<sub>1</sub>~I<sub>m</sub>在交易完成后被添加至所述历史密钥镜像集合。

[0023] 根据本说明书一个或多个实施例的第五方面,提出了一种电子设备,包括:

[0024] 处理器;

[0025] 用于存储处理器可执行指令的存储器;

[0026] 其中,所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

[0027] 根据本说明书一个或多个实施例的第六方面,提出了一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如第一方面所述方法的步骤。

[0028] 根据本说明书一个或多个实施例的第七方面,提出了一种电子设备,包括:

[0029] 处理器;

[0030] 用于存储处理器可执行指令的存储器;

[0031] 其中,所述处理器通过运行所述可执行指令以实现如第二方面所述的方法。

[0032] 根据本说明书一个或多个实施例的第八方面,提出了一种计算机可读存储介质,其上存储有计算机指令,该指令被处理器执行时实现如第二方面所述方法的步骤。



## 附图说明

- [0033] 图1是一示例性实施例提供的一种示例环境的示意图。
- [0034] 图2是一示例性实施例提供的一种概念架构的示意图。
- [0035] 图3是一示例性实施例提供的一种基于环签名的匿名交易方法的流程图。
- [0036] 图4是一示例性实施例提供的一种资产账户模型的示意图。
- [0037] 图5是一示例性实施例提供的一种生成可链接环签名的流程图。
- [0038] 图6是一示例性实施例提供的另一种基于环签名的匿名交易方法的流程图。
- [0039] 图7是一示例性实施例提供的一种验证可链接环签名的流程图。
- [0040] 图8是一示例性实施例提供的一种设备的结构示意图。
- [0041] 图9是一示例性实施例提供的一种基于环签名的匿名交易装置的框图。
- [0042] 图10是一示例性实施例提供的另一种设备的结构示意图。
- [0043] 图11是一示例性实施例提供的另一种基于环签名的匿名交易装置的框图。

## 具体实施方式

[0044] 这里将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所述的方式并不代表与本发明一个或多个实施例相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本发明一个或多个实施例的一些方面相一致的装置和方法的例子。

[0045] 需要说明的是:在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中,其方法所包括的步骤可以比本说明书所描述的更多或更少。此外,本说明书中所描述的单个步骤,在其他实施例中可能被分解为多个步骤进行描述;而本说明书中所描述的多个步骤,在其他实施例中也可能被合并为单个步骤进行描述。

[0046] 图1是一示例性实施例提供的一种示例环境的示意图。如图1所示,示例环境100允许实体参与区块链网络102。区块链网络102可以为公有类型、私有类型或联盟类型的区块链网络。示例环境100可以包括计算设备104、106、108、110、112和网络114;在一实施例中,网络114可以包括局域网(Local Area Network, LAN)、广域网(Wide Area Network, WAN)、因特网或其组合,并连接至网站、用户设备(例如计算设备)和后端系统。在一实施例中,可以通过有线和/或无线通信方式访问网络114。

[0047] 在某些情况下,计算设备106、108可以是云计算系统的节点(未显示),或者每个计算设备106、108可以是单独的云计算系统,包括由网络互连并作为分布式处理系统工作的多台计算机。

[0048] 在一实施例中,计算设备104~108可以运行任何适当的计算系统,使其能够作为区块链网络102中的节点;例如,计算设备104~108可以包括但不限于服务器、台式计算机、笔记本电脑、平板电脑计算设备和智能手机。在一实施例中,计算设备104~108可以归属于相关实体并用于实现相应的服务,例如该服务可以用于对某一实体或多个实体之间的交易进行管理。

[0049] 在一实施例中,计算设备104~108分别存储有区块链网络102对应的区块链账本。

计算设备104可以是(或包含)用于提供浏览器功能的网络服务器,该网络服务器可基于网络114提供与区块链网络102相关的可视化信息。在一些情况下,计算设备104可以不参与区块验证,而是监控区块链网络102以确定其他节点(譬如可以包括计算设备106-108)何时达成共识,并据此生成相应的区块链可视化用户界面。

[0050] 在一实施例中,计算设备104可接收客户端设备(例如计算设备110或计算设备112)针对区块链可视化用户界面发起的请求。在一些情况下,区块链网络102的节点也可以作为客户端设备,比如计算设备108的用户可以使用运行在计算设备108上的浏览器向计算设备104发送上述请求。

[0051] 响应于上述请求,计算设备104可以基于存储的区块链账本生成区块链可视化用户界面(如网页),并将生成的区块链可视化用户界面发送给请求的客户端设备。如果区块链网络102是私有类型或联盟类型的区块链网络,对区块链可视化用户界面的请求可以包括用户授权信息,在生成区块链可视化用户界面并发送给请求的客户端设备之前,可以由计算设备104对该用户授权信息进行验证,并在验证通过后返回相应的区块链可视化用户界面。

[0052] 区块链可视化用户界面可以显示在客户端设备上(例如可显示在图1所示的用户界面116中)。当区块链账本发生更新时,用户界面116的显示内容也可以随之发生更新。此外,用户与用户界面116的交互可能导致对其他用户界面的请求,例如显示区块列表、区块详情、交易列表、交易详情、账户列表、账户详情、合约列表、合约详情或者用户对区块链网络实施搜索而产生的搜索结果页面等。

[0053] 图2是一示例性实施例提供的一种概念架构的示意图。如图2所示,该概念架构200包括实体层202、托管服务层204和区块链网络层206。例如,实体层202可以包括三个实体:实体1、实体2和实体3,每个实体都有各自的交易管理系统208。

[0054] 在一实施例中,托管服务层204可以包括每个事务管理系统208对应的接口210。例如,各个事务管理系统208使用协议(例如超文本传输协议安全(HTTPS)等)通过网络(例如图1中的网络114)与各自的接口210通信。在一些例子中,每个接口210可以提供各自对应的交易管理系统208与区块链网络层206之间的通信连接;更具体地,接口210可与区块链网络层206的区块链网络212通信。在一些例子中,接口210和区块链网络层206之间的通信可以使用远程过程调用(Remote Procedure Calls,RPCs)而实现。在一些例子中,接口210可以向交易管理系统208提供用于访问区块链网络212的API接口。

[0055] 如本文所述,区块链网络212以对等网络的形式提供,该对等网络包括多个节点214,这些节点214分别用于对区块链数据所形成的区块链账本216进行持久化;其中,图2中仅示出了一份区块链账本216,但区块链网络212中可以存在多份区块链账本216或其副本,比如每一节点214可以分别维护一份区块链账本216或其副本。

[0056] 需要指出的是:在本说明书中所描述的交易(transaction),是指用户通过区块链的客户端创建,并需要最终发布至区块链的分布式数据库中的一笔数据。其中,区块链中的交易,存在狭义的交易以及广义的交易之分。狭义的交易是指用户向区块链发布的一笔价值转移;例如,在传统的比特币区块链网络中,交易可以是用户在区块链中发起的一笔转账。而广义的交易是指用户向区块链发布的一笔具有业务意图的业务数据;例如,运营方可以基于实际的业务需求搭建一个联盟链,依托于联盟链部署一些与价值转移无关的其它类

型的在线业务(比如,租房业务、车辆调度业务、保险理赔业务、信用服务、医疗服务等),而在这类联盟链中,交易可以是用户在联盟链中发布的一笔具有业务意图的业务消息或者业务请求。

[0057] 区块链一般被划分为三种类型:公有链(Public Blockchain),私有链(Private Blockchain)和联盟链(Consortium Blockchain)。此外,还有多种类型的结合,比如私有链+联盟链、联盟链+公有链等不同组合形式。其中去中心化程度最高的是公有链。公有链以比特币、以太坊为代表,加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等。而且,各参与者(即节点)可自由加入以及退出网络,并进行相关操作。私有链则相反,该网络的写入权限由某个组织或者机构控制,数据读取权限受组织规定。简单来说,私有链可以为一个弱中心化系统,参与节点具有严格限制且少。这种类型的区块链更适用于特定机构内部使用。联盟链则是介于公有链以及私有链之间的区块链,可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织;参与者通过授权加入网络并组成利益相关联盟,共同维护区块链运行。

[0058] 通过区块链网络所采用的分布式架构,以及区块所采用的链式结构,使得信息可以永久、无篡改地记录在各个区块链节点统一维护的区块链账本中。但是,由于区块链账本完全公开,导致信息隐私性无法得到保障。例如,任意用户可以在任意区块链节点上查询区块链账本,以获知某一账户持有的资产、某一交易的转账额等信息,而这些可能都是敏感的、需要隐藏的信息。

[0059] 处于隐私保护的目,相关技术中提出了基于承诺的匿名交易或机密交易(Confidential Transaction)方案,可以将每个账户持有的资产额、交易所涉及的转账额等,均生成为相应的承诺数额,且区块链账本中仅记载该承诺数额、而非直接记载明文的资产额、交易额等。例如,当采用Pedersen承诺机制时,假定原始数额为 $t$ ,相应的承诺数额可以为 $PC(t, r) = r \times G + t \times H$ ,其中 $G$ 、 $H$ 为椭圆曲线上的随机生成元, $r$ 为随机数,并且 $r$ 的取值仅由账户持有者、交易参与者等掌握,使得无关人员仅根据 $PC(t, r)$ 的取值将无法反推出原始数额 $t$ 。同时,承诺数额还具有同态特性,使得承诺数额之间可以直接参与计算,譬如 $PC(t_1, r_1) - PC(t_2, r_2) = PC(t_1 - t_2, r_1 - r_2)$ 。但是,区块链节点在验证交易时无法根据承诺数额确定相关条件是否被满足,比如交易的汇入额等于汇出额或其他条件,需要提供相关证明信息才可以确保交易顺利完成。

[0060] 此外,用户在区块链网络中发起交易时需要签名。例如,当用户A希望花费自己在区块链中持有的一笔资产时,可以发起一笔区块链交易并使用该用户A持有的私钥 $x_j$ 进行签名。相应地,通过该用户A所持私钥 $x_j$ 对应的公钥 $P_j$ ,即可对上述签名进行验证。但是,对签名的直接验证也暴露了用户A为相应签名的签名方,从而导致了用户A的隐私泄露。

[0061] 出于保护签名方身份的目的,相关技术中提出了基于环签名的处理方案,用户A可以将自身持有的公钥 $P_j$ 隐藏在一组公钥 $(P_1, \dots, P_n)$ 中,其中公钥 $P_1 \sim P_{j-1}$ 、 $P_{j+1} \sim P_n$ 分别属于其他用户;然后,用户A通过自身持有的私钥 $x_j$ 和上述的一组公钥 $(P_1, \dots, P_n)$ 生成签名,那么验证方能够验证签名是由上述的一组公钥 $(P_1, \dots, P_n)$ 中的某一公钥对应的私钥所生成,但是并不能够确定具体为哪一公钥,从而通过上述的一组公钥 $(P_1, \dots, P_n)$ 对签名方的身份实现了隐藏。

[0062] 可以理解的是:当上文描述为 $(P_1, \dots, P_n)$ 的形式时,虽然看似是从 $P_1$ 开始、

P<sub>n</sub>结束的一组公钥,但实际上对于验证方而言并不能够确定各个公钥之间的顺序,使得这组公钥对验证方而言相当于呈现为无首尾的环形结构,因而称为环签名。

[0063] 虽然环签名方案可以对签名方的身份进行隐藏,但是应用于区块链网络的交易场景时,会导致出现“双花”问题。例如,区块链网络可以采用UTXO(Unspent Transaction Output,未花费的交易输出)模型进行资产管理:用户持有的区块链资产均被记录为相应交易的输出,每笔交易以一个或多个未花费的交易输出作为其输入,并相应产生一个或多个输出。典型的,UTXO被应用于比特币及其衍生的密码货币所采用。当环签名方案被应用在基于UTXO模型的区块链网络时,同一笔资产可能被多笔交易分别引用,但由于签名方的身份被环签名方案所隐藏,使得验证方无法检查出同一笔资产被重复引用,从而造成“双花”问题。

[0064] 因此,相关技术中提出了对上述环签名方案的改进方案,称为可链接环签名(Linkable Spontaneous Anonymous Group Signature,LSAG),可以生成用于对签名方进行标记的key-image(密钥镜像),但并不会暴露该签名方在签名所用的一组环签名中所对应的公钥,从而既能够确保对签名方的身份隐藏,又能够基于key-image解决“双花”问题。

[0065] 以门罗币(Monero)为例。门罗币采用UTXO(Unspent Transaction Output,未花费的交易输出)模型实现资产管理,该模型下的所有资产均为相应区块链交易的交易输出,且区块链网络上产生的所有资产被统一管理,其中每一资产均存在唯一对应的公私钥对,用户可以通过持有的公私钥对来花费相应的资产。例如,当签名方(如汇款交易中的汇款方)持有的某一资产对应于私钥x<sub>j</sub>、公钥P<sub>j</sub>时,可以按照公式 $I = x_j \times \text{Hash}(P_j)$ 生成相应的key-image,那么只要该资产先前被花费过,区块链节点就会记录有相同取值的key-image,从而据此识别出“双花”问题。

[0066] 但是,由于每份资产均存在唯一对应的公私钥对,使得一笔交易包含多份资产的情况下,就需要相应的多组公私钥对,例如当一笔交易包含m份资产时,签名方需要维护m组公私钥对,极大地造成了公私钥对的维护成本。

[0067] 为此,本说明书提出了新的技术方案,使得签名方仅需要维护一组公私钥对,便可针对涉及多份资产的交易生成可链接环签名,并且能够满足机密交易对证明信息的需求,下面将结合实施例进行描述。

[0068] 图3是一示例性实施例提供的一种基于环签名的匿名交易方法的流程图。如图3所示,该方法应用于客户端设备,可以包括以下步骤:

[0069] 步骤302,根据汇款方对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>,组装汇款交易M;其中,待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>在区块链账本中被分别记录为相应资产额对应的资产承诺。

[0070] 如前所述,出于对所持资产进行保密的目的,汇款方和其他任意用户所持有的资产,在区块链账本上均记录为相应的承诺数额、而非直接记录明文的资产数额。以待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>为例,ID<sub>j\_1</sub>~ID<sub>j\_m</sub>为资产标识,以用于区分不同资产;假定待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>的资产额为t<sub>j\_1</sub>~t<sub>j\_m</sub>,那么区块链账本上可以记录为资产额t<sub>j\_1</sub>~t<sub>j\_m</sub>对应的资产承诺PC(t<sub>j\_1</sub>,r<sub>j\_1</sub>)~PC(t<sub>j\_m</sub>,r<sub>j\_m</sub>),r<sub>j\_1</sub>~r<sub>j\_m</sub>为随机数。由于随机数r<sub>j\_1</sub>~r<sub>j\_m</sub>的存在,使得数额t<sub>j\_1</sub>~t<sub>j\_m</sub>生成的资产承诺PC(t<sub>j\_1</sub>,r<sub>j\_1</sub>)~PC(t<sub>j\_m</sub>,r<sub>j\_m</sub>)具有随机性,除了掌握随机数r<sub>j\_1</sub>~r<sub>j\_m</sub>的汇款方之外,其他用户仅

能够看到资产承诺 $PC(t_{j_1}, r_{j_1}) \sim PC(t_{j_m}, r_{j_m})$ ，且无法据此反推出相应的资产额 $t_{j_1} \sim t_{j_m}$ 。

[0071] 类似地，对于掩护资产 $ID_{i_1} \sim ID_{i_m}$ 而言， $ID_{i_1} \sim ID_{i_m}$ 为资产标识，以用于区分不同资产；假定掩护资产 $ID_{i_1} \sim ID_{i_m}$ 的资产额为 $t_{i_1} \sim t_{i_m}$ ，那么区块链账本上可以记录为资产额 $t_{i_1} \sim t_{i_m}$ 对应的资产承诺 $PC(t_{i_1}, r_{i_1}) \sim PC(t_{i_m}, r_{i_m})$ ， $r_{i_1} \sim r_{i_m}$ 为随机数。例如，掩护方1持有掩护资产 $ID_{1_1} \sim ID_{1_m}$ ，相应的资产额为 $t_{1_1} \sim t_{1_m}$ ，那么区块链账本上可以记录为资产额 $t_{1_1} \sim t_{1_m}$ 对应的资产承诺 $PC(t_{1_1}, r_{1_1}) \sim PC(t_{1_m}, r_{1_m})$ ， $r_{1_1} \sim r_{1_m}$ 为仅掩护方1持有的随机数。

[0072] 举例而言，区块链账本上可以采用类似于[标识，资产承诺]的形式对资产进行记录和存储。例如，上述的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 可以被记录为 $[ID_{j_1}, PC(t_{j_1}, r_{j_1})] \sim [ID_{j_m}, PC(t_{j_m}, r_{j_m})]$ 、掩护方 $i$ 对应的掩护资产 $ID_{i_1} \sim ID_{i_m}$ 可以被记录为 $[ID_{i_1}, PC\{i, 1\}] \sim [ID_{i_m}, PC\{i, m\}]$ 。当然，此处仅为示例，区块链账本实际可以采用其他形式。例如，当存在多种资产类型时，可以采用类似于[类型，标识，资产承诺]的形式对资产进行记录和存储，那么在计算资产额、执行交易等过程中，需要考虑资产类型所带来的影响，比如不同类型的资产之间存在资产额的比例换算等。再者，除了直接记录“资产承诺”之外，还可以同时存储其他信息；以待花费资产 $ID_{j_m}$ 为例，可以记录为 $[ID_{j_m}, E(t_{j_m}, r_{j_m})]$ ，其中 $E(t_{j_m}, r_{j_m}) = [PC(t_{j_m}, r_{j_m}), E(t_{j_m}), E(r_{j_m})]$ ， $E(t_{j_m})$ 和 $E(r_{j_m})$ 分别为资产额 $t_{j_m}$ 和随机数 $r_{j_m}$ 对应的同态密文，可由汇款方的同态加密公钥(对公钥 $P_j$ 进行同态加密得到)分别对资产额 $t_{j_m}$ 和随机数 $r_{j_m}$ 进行加密后得到。为了便于理解，下文均以[标识，资产承诺]的资产形式进行举例说明。

[0073] 如前所述，本说明书采用“账户”形式对用户持有的资产进行管理，例如可以借鉴UTXO模型和相关技术中诸如以太坊等采用的账户模型，实现了基于“账户”形式的资产管理模型，即资产账户模型。资产账户模型可以为每一用户分别生成对应的账户，并基于账户对用户持有的资产进行管理。譬如图4是一示例性实施例提供的一种资产账户模型的示意图，该图4所示为汇款方对应的账户 $A_j$ 。与上述的账户模型不同的是，账户 $A_j$ 中并非直接记录汇款方的账户余额，而是记录了汇款方持有的资产，比如资产 $[ID_{j_1}, PC(t_{j_1}, r_{j_1})]$ 、 $[ID_{j_2}, PC(t_{j_2}, r_{j_2})]$ 等，这些资产之间可以通过一一对应的资产标识予以明确区分。每一账户存在唯一对应的账户地址(Account ID)，可以据此对不同账户予以区分。同时，所有账户的信息都记录于区块链账本上，使得通过查询区块链账本，即可获知每一账户所含的资产；当然，由于资产额在区块链账本上被记录为相应的承诺数额，因而并不会暴露用户的资产持有情况，可以保护用户隐私。

[0074] 资产账户模型中维护的资产可以存在多种类型。例如，与UTXO模型相类似的，资产账户模型中的资产可以为相应的历史交易的交易输出，比如待花费资产 $ID_{j_1} \sim ID_{j_m}$ 为汇款方先前参与的历史交易形成的交易输出，且汇款方在这些交易中处于“收款方”的角色，再比如掩护资产 $ID_{i_1} \sim ID_{i_m}$ 为掩护方 $i$ 先前参与的历史交易形成的交易输出，且掩护方 $i$ 在这些交易中处于“收款方”的角色。再例如，与账户模型相类似的，资产账户模型可以存在相应的账户余额，并主动对该账户余额的至少一部分进行划分，以形成具有一定资产额的资产，比如待花费资产 $ID_{j_1} \sim ID_{j_m}$ 被从汇款方对应的账户余额中划分而生成、掩护资产 $ID_{i_1} \sim ID_{i_m}$ 被从掩护方 $i$ 对应的账户余额中划分而生成。对于资产由账户余

额中划分生成的情况,可以将所有资产余额均划分为相应的资产进行管理,也可以将部分账户余额划分为资产、剩余的账户余额仍以数值的形式进行维护(图4中未示出这一数值)。

[0075] 在汇款方对应账户内的所有资产中,待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>可以为汇款方所持有的任意资产。当然,在实际选取待花费资产时,还需要参考汇款交易M涉及的汇款额,并确保待花费资产的资产额之和不小于汇款额。汇款额为汇款方需要向各个实际收款方转账的数额,这些数额由汇款方与各个实际收款方预先协商确定,也可以由汇款方自行确定。

[0076] 从汇款交易M的款项输入角度而言,涉及到汇款方和掩护方的角色,而从款项输出角度而言,涉及到实际收款方与交易收款方的角色。在这些角色中,部分角色之间可能存在一定重叠。

[0077] 对于汇款方和掩护方而言,根据汇款方对应账户内的待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、掩护方i对应账户内的掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>来组装汇款交易M,再加上上下文中生成的可链接环签名,使得掩护方i可以对汇款方进行身份隐藏,使得其他用户无法确定究竟在“汇款方和掩护方i”中的哪个用户支出了资产。这里,掩护方可以包括区别于汇款方之外的任意用户,比如该掩护方可以包括汇款交易M的实际收款方,譬如当汇款方为用户A、实际收款方为用户B和用户C时,通过将用户B和用户C配置为掩护方,不仅可使用户B、用户C对用户A进行身份隐藏,甚至由于用户B和用户C同时属于“交易汇款方”和“交易收款方”,从而带来更强的迷惑作用。再比如,掩护方可以包括区别于汇款方和实际收款方的其他用户,譬如当汇款方为用户A、实际收款方为用户B和用户C时,可以将不相干的用户D配置为掩护方,以用于对用户A进行身份隐藏。又比如,掩护方可以同时包括上述的实际收款方和其他用户,譬如当汇款方为用户A、实际收款方为用户B和用户C时,可以将用户B、用户C和用户D配置为掩护方,以用于对用户A进行身份隐藏。

[0078] 对于实际收款方与交易收款方而言:在一实施例中,交易收款方可以为实际收款方,此时还满足待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>对应的资产额 $t_{j_1}$ ~ $t_{j_m}$ 之和与各个实际收款方对应的转账额之和恰好相等,即不存在找零。在另一实施例中,除了实际收款方之外,交易收款方还可以包括汇款方,这时可能存在两种情况:一种情况下,并非特意将汇款方设定为交易收款方,而是由于待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>对应的资产额 $t_{j_1}$ ~ $t_{j_m}$ 之和大于各个实际收款方对应的转账额之和,因而存在需返回至汇款方的找零,且找零额(即汇款方对应的转账额)为资产额 $t_{j_1}$ ~ $t_{j_m}$ 之和与转账额之和的差值;另一种情况下,虽然不存在找零,但仍然可以将汇款方设定为交易收款方,使得汇款方可以对实际收款方起到一定的掩护作用,并且此时可以将汇款方对应的转账额设为0,以避免影响原有的转账操作。在又一实施例中,交易收款方可以包括区别于实际收款方和汇款方的掩护方,由掩护方对实际收款方实现身份隐藏,并且掩护方对应的转账额为0;当然,除了掩护方之外,交易收款方可以同时包括汇款方:当不存在找零时,汇款方和掩护方对应的转账额均为0;当存在找零时,汇款方对应的转账额为找零额、掩护方对应的转账额为0。

[0079] 根据实际情况,可以仅通过掩护方对汇款方进行身份隐藏,也可以进一步针对实际收款方进行身份隐藏。在一实施例中,汇款交易M的参与者可以同时包括汇款方、实际收款方和区别于两者的掩护方,这些用户组成共n个参与者,并且该n个参与者均同时参与汇款交易的汇款与收款,从而同时对汇款方和实际收款方进行身份隐藏。而且,由于每个参与者均同时参与汇款和收款,因而可以使得汇款方与实际收款方之间实现身份混淆,从而进

一步增加身份隐藏的可靠性。

[0080] 假定汇款交易M的交易收款方为 $Q_1 \sim Q_u$ ,对应的转账额分别为 $t'_1 \sim t'_u$ ,其中 $1 \leq u \leq n$ 。在汇款交易M中,与前述待花费资产对应的资产额 $t_{j_1} \sim t_{j_m}$ 相类似的,转账额 $t'_1 \sim t'_u$ 在汇款交易M中被分别记录为对应的转账额承诺 $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ , $r'_1 \sim r'_u$ 为随机数。其中,随机数 $r'_1 \sim r'_u$ 可由汇款方确定,并通过诸如链下通道告知相应的收款方(通常仅需要告知实际收款方),使得各个收款方可以基于随机数 $r'_1 \sim r'_u$ 进行验证,比如收款方w可以验证 $PC(t'_w, r'_w) = t'_w \times G + r'_w \times H$ 是否成立,以及交易完成后对得到的转账额承诺 $PC(t'_w, r'_w)$ 对应的资产进行管理。

[0081] 在机密交易中,需要证明汇款交易M中的转账额 $t'_1 \sim t'_u$ 都不小于0。汇款方可以利用相关技术中的零知识证明技术,为转账额 $t'_1 \sim t'_u$ 分别生成相应的范围证明 $RP_1 \sim RP_u$ ,以用于证明 $t'_1 \geq 0 \sim t'_u \geq 0$ ,并将这些范围证明 $RP_1 \sim RP_u$ 添加至汇款交易M的交易内容中。其中,所采用的零知识证明技术可以为区间证明(Range Proof)技术,譬如Bulletproofs方案等,本说明书并不对此进行限制。

[0082] 步骤304,根据汇款方所持私钥 $x_j$ 、公钥 $P_j$ 和掩护方i所持公钥 $P_i$ ,为所述汇款交易M生成可链接环签名,所述可链接环签名中包含密钥镜像 $I_1 \sim I_m$ ,且密钥镜像 $I_1 \sim I_m$ 的取值与汇款方的私钥 $x_j$ 、公钥 $P_j$ 和资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关。

[0083] 汇款方需要维护一组公私钥对,比如私钥 $x_j$ 和公钥 $P_j$ 。在确定这组公私钥对之前,需要取定一个数域 $Z_q$ 和该数域上的一条椭圆曲线,比如椭圆曲线Ed25519等,令G、H为该椭圆曲线的两个随机的生成元,其中 $|G| = p$ 为一个素数(譬如不小于某一预设数值),并在数值范围 $(0, p)$ 中选取汇款方的私钥 $x_j$ ,相应的公钥为 $P_j = x_j \times G$ 。对于掩护方等其他用户而言,均通过类似的方式确定出各自唯一对应的公私钥对。

[0084] 密钥镜像 $I_1 \sim I_m$ 与汇款方提供的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 之间一一对应,分别用于验证相应的待花费资产是否已花费,从而解决“双花”问题。其中,由于密钥镜像 $I_1 \sim I_m$ 的取值与相应资产的资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关,使得即便所有密钥镜像均采用同一组公私钥对(即汇款方的私钥 $x_j$ 和公钥 $P_j$ ),也可以基于资产标识 $ID_{j_1} \sim ID_{j_m}$ 之间的取值差异,确保生成的密钥镜像 $I_1 \sim I_m$ 之间完全不同,因而无需为每一资产分别维护一组公私钥对,可以在解决“双花”问题的同时,使得每一账户所需维护的公私钥对的数量与交易所含的资产数量无关。例如, $I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d})$ , $d \in [1, m]$ ;其中, $\text{Hash}_G()$ 为上述椭圆曲线到其自身的哈希函数。

[0085] 根据待花费资产对应的资产承诺 $PC(t_{j_1}, r_{j_1}) \sim PC(t_{j_m}, r_{j_m})$ ,以及前述的转账额承诺 $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ ,可以计算得到 $P''_j = [PC(t_{j_1}, r_{j_1}) + \dots + PC(t_{j_m}, r_{j_m})] - [PC(t'_1, r'_1) + \dots + PC(t'_u, r'_u)]$ ;以及,根据待花费资产对应的随机数 $r_{j_1} \sim r_{j_m}$ 、转账额对应的随机数 $r'_1 \sim r'_u$ ,可以计算得到 $r'' = (r_{j_1} + \dots + r_{j_m}) - (r'_1 + \dots + r'_u)$ ;以及,根据待花费资产对应的资产额 $t_{j_1} \sim t_{j_m}$ 、转账额 $t'_1 \sim t'_u$ ,可以计算得到 $t'' = (t_{j_1} + \dots + t_{j_m}) - (t'_1 + \dots + t'_u)$ 。那么,如前所述的同态特性,可以确定 $P''_j = PC(r'', t'') = r'' \times G + t'' \times H$ 。又由于汇款方需要确保 $t_{j_1} + \dots + t_{j_m} = t'_1 + \dots + t'_u$ ,使得 $t'' = 0$ ,因而可以确定 $P''_j = r'' \times G$ 。

[0086] 那么,从形式上可以看出上述的“ $P''_j = r'' \times G$ ”与公私钥对之间的关系“ $P_j = x_j \times G$ ”相似,并且如下文所述,掩护方i必然满足 $P''_i \neq r'' \times G$ ,因而可以将 $r''$ 视为对应于汇款

方的一种私钥、 $P''_j$ 为 $r''$ 对应的公钥,而为了区别于汇款方对应的公私钥对,可以将 $r''$ 视为汇款方对应的伪私钥、 $P''_j$ 视为汇款方对应的伪公钥。类似地,可以将 $P''_i$ 视为掩护方 $i$ 对应的伪公钥;例如,可以计算得到掩护方 $i$ 对应的参数 $P''_i = [PC\{i,1\} + \dots + PC\{i,m\}] - [PC(t'_1, r'_1) + \dots + PC(t'_u, r'_u)]$ ,  $i \in [1, j-1] \cup [j+1, n]$ 。同时,可以计算得到掩护方 $i$ 所持的 $m$ 份资产对应的资产额之和与转账额 $t'_1 \sim t'_u$ 之和的差值 $t''_i$ ,以及可以计算得到掩护方 $i$ 所持的 $m$ 份资产对应的随机数之和与转账额 $t'_1 \sim t'_u$ 对应的随机数 $r'_1 \sim r'_u$ 之和的差值 $r''_i$ 。

[0087] 基于同态特性可以确定 $P''_i = r''_i \times G + t''_i \times H \neq r'' \times G$ 。可见,参数 $P''_j$ 和 $r''$ 均唯一对应于汇款方、参数 $P''_i$ 唯一对应于掩护方 $i$ ,因而可以将 $r''$ 视为汇款方对应的伪私钥、 $P''_j$ 视为汇款方对应的伪公钥,以及将 $P''_i$ 视为掩护方 $i$ 对应的伪公钥。

[0088] 根据汇款方对应的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r''$ 、伪公钥 $P''_j$ ,掩护方 $i$ 对应的公钥 $P_i$ 、伪公钥 $P''_i$ ,为汇款交易 $M$ 生成可链接环签名,可以高效、紧凑地实现下述两方面的验证功能:一方面,由于伪公钥 $P''_j$ 与伪私钥 $r''$ 之间满足 $P''_j = r'' \times G$ 、伪公钥 $P''_i$ 与伪私钥 $r''$ 之间满足 $P''_i \neq r'' \times G$ ,所以当根据伪私钥 $r''$ 、伪公钥 $P''_j$ 和 $P''_i$ 生成可链接环签名时,如果该可链接环签名通过验证,就能够证明在伪公钥( $P''_1, \dots, P''_n$ )中存在某一伪公钥的取值等于 $r'' \times G$ ,并且这个伪公钥对应于前述的 $t'' = 0$ ,能够使得汇款交易 $M$ 的输入与输出等额;另一方面,当根据汇款方对应的私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 对应的公钥 $P_i$ 生成可链接环签名时,如果该可链接环签名通过验证,就能够证明该可链接环签名是由公钥( $P_1, \dots, P_n$ )中的某一公钥对应的私钥进行签名得到,从而在不暴露汇款方身份的前提下,完成身份验证。当然,在不考虑验证汇款交易 $M$ 的输入与输出是否相等的情况下,也可以直接根据汇款方对应的私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 对应的公钥 $P_i$ 生成可链接环签名,而不需要利用汇款方对应的伪私钥 $r''$ 、伪公钥 $P''_j$ 和掩护方 $i$ 对应的伪公钥 $P''_i$ ,本说明书并不对此进行限制。

[0089] 除了上述的密钥镜像 $I_1 \sim I_m$ 之外,汇款方还可以根据伪私钥 $r''$ 和伪公钥 $P''_j$ 生成的密钥镜像 $I_{(m+1)} = r'' \times \text{Hash}_G(P''_j)$ ,从而与密钥镜像 $I_1 \sim I_m$ 构成共 $m+1$ 个密钥镜像,共同用于解决“双花”问题。实际上,由于伪私钥 $r''$ 和伪公钥 $P''_j$ 的取值都具有随机性,使得不同交易产生的伪私钥 $r''$ 和伪公钥 $P''_j$ 必然不同,所以在根据伪私钥 $r''$ 和伪公钥 $P''_j$ 生成密钥镜像 $I_{(m+1)}$ 时,可使密钥镜像 $I_{(m+1)}$ 与相应交易之间形成一一对应关系,因而通过将密钥镜像 $I_{(m+1)}$ 与历史密钥镜像进行比较,以识别出针对汇款交易 $M$ 的重放(replay)问题:如果密钥镜像 $I_{(m+1)}$ 存在相同的历史密钥镜像,就表明汇款交易 $M$ 发生了重放。

[0090] 步骤306,向区块链网络提交签名后的汇款交易 $M$ ;其中,在交易完成后,密钥镜像 $I_1 \sim I_m$ 被添加至历史密钥镜像集合,且所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 在区块链账本上被保持记录为汇款方持有的资产。

[0091] 区块链节点在收到汇款交易 $M$ 后,可以将密钥镜像 $I_1 \sim I_m$ 与历史密钥镜像集合进行比对,以确定历史密钥镜像集合中是否存在与密钥镜像 $I_1 \sim I_m$ 相同的历史密钥镜像。历史密钥镜像集合用于存储先前已花费的资产对应的密钥镜像。如果存在与密钥镜像 $I_1 \sim I_m$ 中的某一密钥镜像相同的历史密钥镜像,表明该密钥镜像对应的资产已经被花费,即出现了“双花”问题,应当阻止汇款交易 $M$ 的执行。而如果密钥镜像 $I_1 \sim I_m$ 不属于历



史密钥镜像集合,则表明密钥镜像 $I_1 \sim I_m$ 对应的资产 $ID_{j_1} \sim ID_{j_m}$ 均未被花费,在其他交易执行条件被满足的情况下,可以执行汇款交易 $M$ ;并且,当汇款交易 $M$ 完成后,密钥镜像 $I_1 \sim I_m$ 对应的资产 $ID_{j_1} \sim ID_{j_m}$ 均被花费,因而需要将密钥镜像 $I_1 \sim I_m$ 添加至历史密钥镜像集合中,以用于后续检测与密钥镜像 $I_1 \sim I_m$ 相关的“双花”问题。

[0092] 在诸如以太坊所采用的账户模型中,当汇款方通过交易花费一笔款项后,相应账户内的账户余额随即发生更新,即扣除被花费的款项额,从而确保账户余额的准确性。但在本说明书的技术方案中,在汇款交易 $M$ 完成后,虽然汇款方对应账户内的资产 $ID_{j_1} \sim ID_{j_m}$ 被花费,但是并不立即对汇款方对应账户进行更新,即无需立即删除汇款方对应账户内的资产 $ID_{j_1} \sim ID_{j_m}$ ,使得任意用户通过区块链账本查询汇款方对应账户时,不会在汇款交易 $M$ 完成后察觉到资产变化,避免基于资产变化而暴露汇款方在汇款交易 $M$ 中承担的真实身份。同时,虽然汇款方对应账户内同时包含已花费和未花费的资产,但是基于对上述历史密钥镜像集合的维护,可以确保汇款方实际仅能够对未花费的资产进行花费,并准确检测出汇款方对已花费的资产所实施的“双花”操作。

[0093] 当然,为了避免账户内累积的资产过多、增加区块链节点的维护成本,也为了方便各个用户对自身账户内资产进行管理,用户可以对自身账户内的已花费资产进行清理。以上述的汇款方为例,该汇款方可以向区块链网络发起资产删除请求,以从区块链账本中删除该汇款方已花费的至少一部分资产;例如,汇款方可以指定所需删除的资产对应的资产标识,或者汇款方可以指定一时间段(可以指定时间段的两侧端点;如果仅指定左侧端点,则时间段为从该左侧端点对应时刻至今;如果仅指定右侧端点,则时间段为从账户创建至该右侧端点对应时刻)并删除该时间段内产生或被花费的所有资产。

[0094] 基于上述描述可知,汇款方生成的汇款交易 $M$ 可以包括下述交易内容:

[0095] 1) 汇款方、掩护方 $i$ 及其资产:  $\{[P_1:ID_{1_1}, \dots, ID_{1_m}], [P_2:ID_{2_1}, \dots, ID_{2_m}], \dots, [P_n:ID_{n_1}, \dots, ID_{n_m}]\}$ , 其中 $P_1 \sim P_n$ 分别为汇款方和掩护方的公钥,比如汇款方对应的公钥 $P_j$ 、掩护方 $i$ 对应的公钥 $P_i, i \in [1, j-1] \cup [j+1, n]$ 。

[0096] 2) 交易收款方及其转账额:  $\{[Q_1, PC(t'_1, r'_1)], [Q_2, PC(t'_2, r'_2)], \dots, [Q_u, PC(t'_u, r'_u)]\}$ 。

[0097] 3) 范围证明 $RP_1 \sim RP_u$ 。

[0098] 当然,汇款交易 $M$ 还可以包含区块链网络中所需的其他交易内容,可以参考相关技术中的相关要求,此处不再一一列举。

[0099] 然后,汇款方可以针对上述汇款交易 $M$ 的交易内容进行哈希计算,而参数 $M$ 可以表征计算得到的哈希值,且汇款方可以针对该哈希值 $M$ 生成可链接环签名。当然,汇款方也可以直接针对整个交易内容生成可链接环签名,这可能带来相对更大的计算量。

[0100] 下面结合图5对根据汇款方对应的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r''$ 、伪公钥 $P''_j$ ,掩护方 $i$ 对应的公钥 $P_i$ 、伪公钥 $P''_i$ ,为汇款交易 $M$ 生成可链接环签名的过程进行描述;其中,图5是一示例性实施例提供的一种生成可链接环签名的流程图。如图5所示,可以包括以下步骤:

[0101] 步骤502,生成密钥镜像 $I_1 \sim I_{(m+1)}$ 。

[0102] 生成密钥镜像 $I_1 \sim I_{(m+1)}$ 的过程可以参考前述内容,此处不再赘述。

[0103] 其中,  $I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d}), d \in [1, m]; I_{(m+1)} = r'' \times \text{Hash}_G(P''_j)$ 。

[0104] 步骤504a,计算中间参数 $L_{j\_d}$ 、 $R_{j\_d}$ 。

[0105] 汇款方可以从数域 $Z_q$ 中选取随机数 $a_d$ (即 $a_1 \sim a_m$ ),并按照下述公式计算中间参数 $L_{j\_d}$ 、 $R_{j\_d}$ :

$$[0106] \quad L_{j\_d} = a_d \times G$$

$$[0107] \quad R_{j\_d} = a_d \times \text{Hash}_G(P_j, ID_{j\_d})$$

[0108] 因此,汇款方可以计算得到 $L_{j\_d}:L_{j\_1} \sim L_{j\_m}$ ,以及 $R_{j\_d}:R_{j\_1} \sim R_{j\_m}$ 。

[0109] 进一步地,汇款方可以生成对应于掩护方 $i$ 的中间参数 $L_{i\_d}$ 、 $R_{i\_d}$ ,包括:根据中间参数 $L_{j\_d}$ 、 $R_{j\_d}$ 的取值,分别生成中间参数 $L_{i\_d}$ 、 $R_{i\_d}$ ,将在下述步骤506~510中进行描述。

[0110] 步骤504b,计算中间参数 $L_{j_{(m+1)}}$ 、 $R_{j_{(m+1)}}$ 。

[0111] 汇款方可以从数域 $Z_q$ 中选取随机数 $a_{(m+1)}$ ,并按照下述公式计算中间参数 $L_{j_{(m+1)}}$ 、 $R_{j_{(m+1)}}$ :

$$[0112] \quad L_{j_{(m+1)}} = a_{(m+1)} \times G$$

$$[0113] \quad R_{j_{(m+1)}} = a_{(m+1)} \times \text{Hash}_G(P''_j)$$

[0114] 因此,汇款方可以计算得到 $L_{j_{(m+1)}}$ 和 $R_{j_{(m+1)}}$ 。进一步地,汇款方可以生成对应于掩护方 $i$ 的中间参数 $L_{i_{(m+1)}}$ 、 $R_{i_{(m+1)}}$ ,将在下述步骤506~510中进行描述。

[0115] 步骤506,计算中间参数 $L_{(j+1)_d} \sim L_{n\_d}$ 、 $R_{(j+1)_d} \sim R_{n\_d}$ 、 $L_{(j+1)_{(m+1)}} \sim L_{n_{(m+1)}}$ 、 $R_{(j+1)_{(m+1)}} \sim R_{n_{(m+1)}}$ 。

[0116] 当 $i = j+1 \sim n$ 时,中间参数 $L_{i\_d}$ 、 $R_{i\_d}$ 的计算过程符合下述公式:

$$[0117] \quad L_{i\_d} = (s_{i\_d} \times G + c_i \times P_i) \bmod p$$

$$[0118] \quad R_{i\_d} = [s_{i\_d} \times \text{Hash}_G(P_i, ID_{i\_d}) + c_i \times I_d] \bmod p$$

[0119] 同时,中间参数 $L_{i_{(m+1)}}$ 、 $R_{i_{(m+1)}}$ 的计算过程符合下述公式:

$$[0120] \quad L_{i_{(m+1)}} = [s_{i_{(m+1)}} \times G + c_i \times P''_i] \bmod p$$

$$[0121] \quad R_{i_{(m+1)}} = [s_{i_{(m+1)}} \times \text{Hash}_G(P''_i) + c_i \times I_{(m+1)}] \bmod p$$

[0122] 在计算过程中,涉及到 $s_{(j+1)_d} \sim s_{n\_d}$ 、 $s_{(j+1)_{(m+1)}} \sim s_{n_{(m+1)}}$ ,均为数域 $Z_q$ 中的随机数。以及,在计算过程中,涉及到 $c_{(j+1)} \sim c_n$ ,其计算过程符合下述公式: $c_i = \text{Hash}[M, L_{(i-1)_1}, R_{(i-1)_1}, \dots, L_{(i-1)_{(m+1)}}, R_{(i-1)_{(m+1)}}]$ ,其中 $\text{Hash}()$ 为从上述椭圆曲线到数据 $Z_q$ 上的哈希函数。

[0123] 在步骤504a-b中已经计算得到 $L_{j\_d}$ 、 $R_{j\_d}$ 、 $L_{j_{(m+1)}}$ 、 $R_{j_{(m+1)}}$ 的情况下,基于 $L_{j\_d}$ 、 $R_{j\_d}$ 计算得到 $i \in [j+1, n]$ 时的中间参数 $L_{i\_d}$ 、 $R_{i\_d}$ ,即上述的 $L_{(j+1)_d} \sim L_{n\_d}$ 、 $R_{(j+1)_d} \sim R_{n\_d}$ 。具体的,首先根据 $L_{j\_d}$ 、 $R_{j\_d}$ 、 $L_{j_{(m+1)}}$ 、 $R_{j_{(m+1)}}$ 的取值计算得到 $c_{(j+1)} = \text{Hash}[M, L_{j_1}, R_{j_1}, \dots, L_{j_{(m+1)}}, R_{j_{(m+1)}}]$ ,并根据随机数 $s_{(j+1)_d}$ 和计算得到的 $c_{(j+1)}$ 计算 $L_{(j+1)_d}$ 、 $R_{(j+1)_d}$ ,即:根据随机数 $s_{(j+1)_1}$ 和计算得到的 $c_{(j+1)}$ 计算 $L_{(j+1)_1}$ 、 $R_{(j+1)_1}$ ,根据随机数 $s_{(j+1)_2}$ 和计算得到的 $c_{(j+1)}$ 计算 $L_{(j+1)_2}$ 、 $R_{(j+1)_2}$ ,……,根据随机数 $s_{(j+1)_m}$ 和计算得到的 $c_{(j+1)}$ 计算 $L_{(j+1)_m}$ 、 $R_{(j+1)_m}$ ;然后根据 $L_{(j+1)_d}$ 、 $R_{(j+1)_d}$ 的取值计算得到 $c_{(j+2)}$ ,并根据随机数 $s_{(j+2)_d}$ 和计算得到的 $c_{(j+2)}$ 计算 $L_{(j+2)_d}$ 、 $R_{(j+2)_d}$ ;以此类推,直至计算得到 $L_{n\_d}$ 、 $R_{n\_d}$ 。

[0124] 类似地,根据随机数 $s_{i_{(m+1)}}$ 、伪公钥 $P''_i$ 、计算得到的 $c_i$ 和密钥镜像 $I_{(m+1)}$ ,

可以分别按照前述公式计算得到中间参数 $L_{(j+1)} \sim L_{n_{(m+1)}}、R_{(j+1)} \sim R_{n_{(m+1)}}$ ,此处不再一一赘述。

[0125] 步骤508,计算中间参数 $L_{1\_d}、R_{1\_d}、L_{1_{(m+1)}}、R_{1_{(m+1)}}$ 。

[0126] 中间参数 $L_{1\_d}、R_{1\_d}$ 的计算过程符合下述公式:

[0127]  $L_{1\_d} = (s_{1\_d} \times G + c_{1\_d} \times P_{1\_d}) \bmod p$

[0128]  $R_{1\_d} = (s_{1\_d} \times \text{Hash}_G(P_{1\_d}, ID_{1\_d}) + c_{1\_d} \times I_{1\_d}) \bmod p$

[0129] 而中间参数 $L_{1_{(m+1)}}、R_{1_{(m+1)}}$ 的计算过程符合下述公式:

[0130]  $L_{1_{(m+1)}} = [s_{1_{(m+1)}} \times G + c_{1_{(m+1)}} \times P_{1_{(m+1)}}] \bmod p$

[0131]  $R_{1_{(m+1)}} = [s_{1_{(m+1)}} \times \text{Hash}_G(P_{1_{(m+1)}}) + c_{1_{(m+1)}} \times I_{1_{(m+1)}}] \bmod p$

[0132] 其中, $s_{1\_d}$ 和 $s_{1_{(m+1)}}$ 均为数域 $Z_q$ 中的随机数、 $c_{1\_d} = \text{Hash}[M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}}]$ 。由于各个中间参数之间符合环形取值规则,因而虽然为了便于描述而将中间参数表达为 $L_{1\_d} \sim L_{n\_d}、R_{1\_d} \sim R_{n\_d}、L_{1_{(m+1)}} \sim L_{n_{(m+1)}}、R_{1_{(m+1)}} \sim R_{n_{(m+1)}}$ ,但是 $L_{1\_d}、R_{1\_d}、L_{1_{(m+1)}}、R_{1_{(m+1)}}$ 并非排列在首位, $L_{n\_d}、R_{n\_d}、L_{n_{(m+1)}}、R_{n_{(m+1)}}$ 也并非排列在末位,实际上应当认为 $L_{1\_d}$ 与 $L_{n\_d}$ 之间相邻、 $R_{1\_d}$ 与 $R_{n\_d}$ 之间相邻、 $L_{1_{(m+1)}}$ 与 $L_{n_{(m+1)}}$ 之间相邻、 $R_{1_{(m+1)}}$ 与 $R_{n_{(m+1)}}$ 之间相邻。所以,当 $c_{1\_d} = \text{Hash}[M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}}]$ 时,实质上也符合上述步骤506处所描述的 $c_i = \text{Hash}[M, L_{(i-1)_1}, R_{(i-1)_1}, \dots, L_{(i-1)_{(m+1)}}, R_{(i-1)_{(m+1)}}]$ ,即 $c_{1\_d}$ 与 $c_{(j+1)} \sim c_n$ 的计算公式一致。

[0133] 步骤510,计算中间参数 $L_{2\_d} \sim L_{(j-1)\_d}、R_{2\_d} \sim R_{(j-1)\_d}、L_{2_{(m+1)}} \sim L_{(j-1)_{(m+1)}}、R_{2_{(m+1)}} \sim R_{(j-1)_{(m+1)}}$ 。

[0134] 当 $i=2 \sim j-1$ 时,中间参数 $L_{i\_d}、R_{i\_d}$ 的计算过程符合下述公式:

[0135]  $L_{i\_d} = (s_{i\_d} \times G + c_{i\_d} \times P_{i\_d}) \bmod p$

[0136]  $R_{i\_d} = (s_{i\_d} \times \text{Hash}_G(P_{i\_d}, ID_{i\_d}) + c_{i\_d} \times I_{i\_d}) \bmod p$

[0137] 同时,中间参数 $L_{i_{(m+1)}}、R_{i_{(m+1)}}$ 的计算过程符合下述公式:

[0138]  $L_{i_{(m+1)}} = [s_{i_{(m+1)}} \times G + c_{i_{(m+1)}} \times P_{i_{(m+1)}}] \bmod p$

[0139]  $R_{i_{(m+1)}} = [s_{i_{(m+1)}} \times \text{Hash}_G(P_{i_{(m+1)}}) + c_{i_{(m+1)}} \times I_{i_{(m+1)}}] \bmod p$

[0140] 在计算过程中,涉及到 $s_{2\_d} \sim s_{(j-1)\_d}、s_{2_{(m+1)}} \sim s_{(j-1)_{(m+1)}}$ ,均为数域 $Z_q$ 中的随机数。以及,在计算过程中,涉及到 $c_2 \sim c_{(j-1)}$ ,其计算过程符合下述公式: $c_i = \text{Hash}(M, L_{(i-1)_1}, R_{(i-1)_1}, \dots, L_{(i-1)_{(m+1)}}, R_{(i-1)_{(m+1)}})$ 。

[0141] 因此,在步骤508中已经计算得到 $L_{1\_d}、R_{1\_d}、L_{1_{(m+1)}}、R_{1_{(m+1)}}$ 的情况下,可以基于 $L_{1\_d}、R_{1\_d}、L_{1_{(m+1)}}、R_{1_{(m+1)}}$ 计算得到 $i \in [2, j-1]$ 时的中间参数 $L_{i\_d}、R_{i\_d}$ ,即上述的 $L_{2\_d} \sim L_{(j-1)\_d}、R_{2\_d} \sim R_{(j-1)\_d}$ 。具体的,首先根据 $L_{1\_d}、R_{1\_d}、L_{1_{(m+1)}}、R_{1_{(m+1)}}$ 的取值计算得到 $c_2$ ,并根据随机数 $s_{2\_d}$ 和计算得到的 $c_2$ 计算 $L_{2\_d}、R_{2\_d}$ ,即:根据随机数 $s_{2_1}$ 和计算得到的 $c_2$ 计算 $L_{2_1}、R_{2_1}$ ,根据随机数 $s_{2_2}$ 和计算得到的 $c_2$ 计算 $L_{2_2}、R_{2_2}$ ,……,根据随机数 $s_{2_m}$ 和计算得到的 $c_2$ 计算 $L_{2_m}、R_{2_m}$ ;然后根据 $L_{2\_d}、R_{2\_d}$ 的取值计算得到 $c_3$ ,并根据随机数 $s_{3\_d}$ 和计算得到的 $c_3$ 计算 $L_{3\_d}、R_{3\_d}$ ;以此类推,直至计算得到 $L_{(j-1)\_d}、R_{(j-1)\_d}$ 。

[0142] 类似地,根据随机数 $s_{i_{(m+1)}}、$ 伪公钥 $P_{i_{(m+1)}}、$ 计算得到的 $c_i$ 和密钥镜像 $I_{(m+1)}$ ,可以分别按照前述公式计算得到中间参数 $L_{2_{(m+1)}} \sim L_{(j-1)_{(m+1)}}、R_{2_{(m+1)}} \sim R_{(j-1)_{(m+1)}}$ 。

1)\_(m+1), 此处不再一一赘述。

[0143] 步骤512, 生成环签名。

[0144] 基于上述步骤的处理过程, 可以得到密钥镜像 $I_1, \dots, I_{(m+1)}$ 、 $c_1, s_{1\_d} \sim s_{(j-1)\_d}, s_{(j+1)\_d} \sim s_{n\_d}, s_{1\_(m+1)} \sim s_{(j-1)\_(m+1)}, s_{(j+1)\_(m+1)} \sim s_{n\_(m+1)}$ , 而 $s_{j\_d}, s_{j\_(m+1)}$ 需要签名方按照下述公式进行计算得到:

$$[0145] \quad s_{j\_d} = (a_d - c_j \times x_j) \bmod p$$

$$[0146] \quad s_{j\_(m+1)} = (a_{(m+1)} - c_j \times r^j) \bmod p$$

$$[0147] \quad c_j = \begin{cases} \text{Hash}[M, L_{n\_1}, R_{n\_1}, \dots, L_{n\_(m+1)}, R_{n\_(m+1)}], & j=1 \\ \text{Hash}[M, L_{(j-1)\_1}, R_{(j-1)\_1}, \dots, L_{(j-1)\_(m+1)}, \\ R_{(j-1)\_(m+1)}], & j \in [2, n] \end{cases}$$

[0148] 其中, 虽然上述公式中将 $c_j$ 的取值划分为2种情况, 但首先参数 $j$ 的取值实际上是固定的, 比如参数 $j$ 的取值固定为1或者固定为 $[2, n]$ 中的某一数值, 这一点应当与上述的参数 $i, e$ 区分开(参数 $i$ 存在 $n-1$ 个取值, 分别为 $1 \sim j-1$ 和 $j+1 \sim n$ , 参数 $e$ 存在 $m$ 个取值, 分别为 $1 \sim m$ ); 同时, 与上文对 $c_1$ 的描述相类似的: 由于各个中间参数之间符合环形取值规则, 因而虽然为了便于描述而将中间参数表达为 $L_{1\_d} \sim L_{n\_d}, R_{1\_d} \sim R_{n\_d}, L_{1\_(m+1)} \sim L_{n\_(m+1)}, R_{1\_(m+1)} \sim R_{n\_(m+1)}$ , 但是 $L_{1\_d}, R_{1\_d}, L_{1\_(m+1)}, R_{1\_(m+1)}$ 并非排列在首位,  $L_{n\_d}, R_{n\_d}, L_{n\_(m+1)}, R_{n\_(m+1)}$ 也并非排列在末位, 实际上应当认为 $L_{1\_d}$ 与 $L_{n\_d}$ 之间相邻、 $R_{1\_d}$ 与 $R_{n\_d}$ 之间相邻、 $L_{1\_(m+1)}$ 与 $L_{n\_(m+1)}$ 之间相邻、 $R_{1\_(m+1)}$ 与 $R_{n\_(m+1)}$ 之间相邻。所以, 当 $c_1 = \text{Hash}(M, L_{n\_1}, R_{n\_1}, \dots, L_{n\_(m+1)}, R_{n\_(m+1)})$ 时, 实质上符合 $c_j = \text{Hash}(M, L_{(j-1)\_1}, R_{(j-1)\_1}, \dots, L_{(j-1)\_(m+1)}, R_{(j-1)\_(m+1)})$ 。

[0149] 因此, 汇款方可以生成环签名 $[I_1, \dots, I_{(m+1)}, c_1, s_{1\_1}, \dots, s_{1\_(m+1)}, \dots, s_{n\_1}, \dots, s_{n\_(m+1)}]$ , 其中包含密钥镜像 $I_1 \sim I_{(m+1)}$ 、随机数 $s_{i\_1} \sim s_{i\_(m+1)}$ 、衍生数值 $s_{j\_1} \sim s_{j\_(m+1)}$ 和 $c_1$ 。

[0150] 图6是一示例性实施例提供的另一种基于环签名的匿名交易方法的流程图。如图6所示, 该方法应用于区块链节点, 由区块链节点对图3所示实施例中生成的可链接环签名进行验证, 以及对汇款交易 $M$ 实施其他必要的验证操作, 可以包括以下步骤:

[0151] 步骤602, 接收汇款交易 $M$ , 所述汇款交易 $M$ 由汇款方根据自身对应账户内的待花费资产 $ID_{j\_1} \sim ID_{j\_m}$ 、掩护方 $i$ 对应账户内的掩护资产 $ID_{i\_1} \sim ID_{i\_m}$ 组装生成; 在交易完成后, 资产 $ID_{j\_1} \sim ID_{j\_m}$ 在区块链账本上被保持记录为汇款方持有的资产。

[0152] 如前所述, 出于对所持资产进行保密的目的, 汇款方和其他任意用户所持有的资产, 在区块链账本上均记录为相应的承诺数额、而非直接记录明文的资产数额。以待花费资产 $ID_{j\_1} \sim ID_{j\_m}$ 为例,  $ID_{j\_1} \sim ID_{j\_m}$ 为资产标识, 以用于区分不同资产; 假定待花费资产 $ID_{j\_1} \sim ID_{j\_m}$ 的资产额为 $t_{j\_1} \sim t_{j\_m}$ , 那么区块链账本上可以记录为资产额 $t_{j\_1} \sim t_{j\_m}$ 对应的资产承诺 $PC(t_{j\_1}, r_{j\_1}) \sim PC(t_{j\_m}, r_{j\_m})$ ,  $r_{j\_1} \sim r_{j\_m}$ 为随机数。由于随机数 $r_{j\_1} \sim r_{j\_m}$ 的存在, 使得数额 $t_{j\_1} \sim t_{j\_m}$ 生成的资产承诺 $PC(t_{j\_1}, r_{j\_1}) \sim PC(t_{j\_m}, r_{j\_m})$ 具有随机性, 除了掌握随机数 $r_{j\_1} \sim r_{j\_m}$ 的汇款方之外, 其他用户仅能够看到资产承诺 $PC(t_{j\_1}, r_{j\_1}) \sim PC(t_{j\_m}, r_{j\_m})$ , 且无法据此反推出相应的资产额 $t_{j\_1} \sim t_{j\_m}$ 。

[0153] 类似地,对于掩护资产 $ID_{i_1} \sim ID_{i_m}$ 而言, $ID_{i_1} \sim ID_{i_m}$ 为资产标识,以用于区分不同资产;假定掩护资产 $ID_{i_1} \sim ID_{i_m}$ 的资产额为 $t_{i_1} \sim t_{i_m}$ ,那么区块链账本上可以记录为资产额 $t_{i_1} \sim t_{i_m}$ 对应的资产承诺 $PC(t_{i_1}, r_{i_1}) \sim PC(t_{i_m}, r_{i_m})$ ,  $r_{i_1} \sim r_{i_m}$ 为随机数。例如,掩护方1持有掩护资产 $ID_{1_1} \sim ID_{1_m}$ ,相应的资产额为 $t_{1_1} \sim t_{1_m}$ ,那么区块链账本上可以记录为资产额 $t_{1_1} \sim t_{1_m}$ 对应的资产承诺 $PC(t_{1_1}, r_{1_1}) \sim PC(t_{1_m}, r_{1_m})$ ,  $r_{1_1} \sim r_{1_m}$ 为仅掩护方1持有的随机数。

[0154] 举例而言,区块链账本上可以采用类似于[标识,资产承诺]的形式对资产进行记录和存储。例如,上述的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 可以被记录为 $[ID_{j_1}, PC(t_{j_1}, r_{j_1})] \sim [ID_{j_m}, PC(t_{j_m}, r_{j_m})]$ 、掩护方 $i$ 对应的掩护资产 $ID_{i_1} \sim ID_{i_m}$ 可以被记录为 $[ID_{i_1}, PC\{i, 1\}] \sim [ID_{i_m}, PC\{i, m\}]$ 。当然,此处仅为示例,区块链账本实际可以采用其他形式。例如,当存在多种资产类型时,可以采用类似于[类型,标识,资产承诺]的形式对资产进行记录和存储,那么在计算资产额、执行交易等过程中,需要考虑资产类型所带来的影响,比如不同类型的资产之间存在资产额的比例换算等。再者,除了直接记录“资产承诺”之外,还可以同时存储其他信息;以待花费资产 $ID_{j_m}$ 为例,可以记录为 $[ID_{j_m}, E(t_{j_m}, r_{j_m})]$ ,其中 $E(t_{j_m}, r_{j_m}) = [PC(t_{j_m}, r_{j_m}), E(t_{j_m}), E(r_{j_m})]$ ,  $E(t_{j_m})$ 和 $E(r_{j_m})$ 分别为资产额 $t_{j_m}$ 和随机数 $r_{j_m}$ 对应的同态密文,可由汇款方的同态加密公钥(对公钥 $P_j$ 进行同态加密得到)分别对资产额 $t_{j_m}$ 和随机数 $r_{j_m}$ 进行加密后得到。为了便于理解,下文均以[标识,资产承诺]的资产形式进行举例说明。

[0155] 如前所述,本说明书采用“账户”形式对用户持有的资产进行管理,可以参考前述结合图4的相关描述,此处不再赘述。总之,基于本说明书中的资产账户模型,可以为每一用户分别生成对应的账户,并基于账户对用户持有的资产进行管理。

[0156] 从汇款交易M的款项输入角度而言,涉及到汇款方和掩护方的角色,而从款项输出角度而言,涉及到实际收款方与交易收款方的角色。在这些角色中,部分角色之间可能存在一定重叠。

[0157] 对于汇款方和掩护方而言,根据汇款方对应账户内的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、掩护方 $i$ 对应账户内的掩护资产 $ID_{i_1} \sim ID_{i_m}$ 来组装汇款交易M,再加上上下文中生成的可链接环签名,使得掩护方 $i$ 可以对汇款方进行身份隐藏,使得其他用户无法确定究竟在“汇款方和掩护方 $i$ ”中的哪个用户支出了资产。这里,掩护方可以包括区别于汇款方之外的任意用户,比如该掩护方可以包括汇款交易M的实际收款方,譬如当汇款方为用户A、实际收款方为用户B和用户C时,通过将用户B和用户C配置为掩护方,不仅可使用户B、用户C对用户A进行身份隐藏,甚至由于用户B和用户C同时属于“交易汇款方”和“交易收款方”,从而带来更强的迷惑作用。再比如,掩护方可以包括区别于汇款方和实际收款方的其他用户,譬如当汇款方为用户A、实际收款方为用户B和用户C时,可以将不相干的用戶D配置为掩护方,以用于对用户A进行身份隐藏。又比如,掩护方可以同时包括上述的实际收款方和其他用户,譬如当汇款方为用户A、实际收款方为用户B和用户C时,可以将用户B、用户C和用戶D配置为掩护方,以用于对用户A进行身份隐藏。

[0158] 对于实际收款方与交易收款方而言:在一实施例中,交易收款方可以为实际收款方,此时还满足待花费资产 $ID_{j_1} \sim ID_{j_m}$ 对应的资产额 $t_{j_1} \sim t_{j_m}$ 之和与各个实际收款方对应的转账额之和恰好相等,即不存在找零。在另一实施例中,除了实际收款方之外,

交易收款方还可以包括汇款方,这时可能存在两种情况:一种情况下,并非特意将汇款方设定为交易收款方,而是由于待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>对应的资产额 $t_{j_1}$ ~ $t_{j_m}$ 之和大于各个实际收款方对应的转账额之和,因而存在需返回至汇款方的找零,且找零额(即汇款方对应的转账额)为资产额 $t_{j_1}$ ~ $t_{j_m}$ 之和与转账额之和的差值;另一种情况下,虽然不存在找零,但仍然可以将汇款方设定为交易收款方,使得汇款方可以对实际收款方起到一定的掩护作用,并且此时可以将汇款方对应的转账额设为0,以避免影响原有的转账操作。在又一实施例中,交易收款方可以包括区别于实际收款方和汇款方的掩护方,由掩护方对实际收款方实现身份隐藏,并且掩护方对应的转账额为0;当然,除了掩护方之外,交易收款方可以同时包括汇款方:当不存在找零时,汇款方和掩护方对应的转账额均为0;当存在找零时,汇款方对应的转账额为找零额、掩护方对应的转账额为0。

[0159] 根据实际情况,可以仅通过掩护方对汇款方进行身份隐藏,也可以进一步针对实际收款方进行身份隐藏。在一实施例中,汇款交易M的参与者可以同时包括汇款方、实际收款方和区别于两者的掩护方,这些用户组成共n个参与者,并且该n个参与者均同时参与汇款交易的汇款与收款,从而同时对汇款方和实际收款方进行身份隐藏。而且,由于每个参与者均同时参与汇款和收款,因而可以使得汇款方与实际收款方之间实现身份混淆,从而进一步增加身份隐藏的可靠性。

[0160] 假定汇款交易M的交易收款方为 $Q_1$ ~ $Q_u$ ,对应的转账额分别为 $t'_1$ ~ $t'_u$ ,其中 $1 \leq u \leq n$ 。在汇款交易M中,与前述待花费资产对应的资产额 $t_{j_1}$ ~ $t_{j_m}$ 相类似的,转账额 $t'_1$ ~ $t'_u$ 在汇款交易M中被分别记录为对应的转账额承诺 $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ , $r'_1$ ~ $r'_u$ 为随机数。其中,随机数 $r'_1$ ~ $r'_u$ 可由汇款方确定,并通过诸如链下通道告知相应的收款方(通常仅需要告知实际收款方),使得各个收款方可以基于随机数 $r'_1$ ~ $r'_u$ 进行验证,比如收款方w可以验证 $PC(t'_w, r'_w) = t'_w \times G + r'_w \times H$ 是否成立,以及交易完成后对得到的转账额承诺 $PC(t'_w, r'_w)$ 对应的资产进行管理。

[0161] 在诸如以太坊所采用的账户模型中,当汇款方通过交易花费一笔款项后,相应账户内的账户余额随即发生更新,即扣除被花费的款项额,从而确保账户余额的准确性。但在本说明书的技术方案中,在汇款交易M完成后,虽然汇款方对应账户内的资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>被花费,但是并不立即对汇款方对应账户进行更新,即无需立即删除汇款方对应账户内的资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>,使得任意用户通过区块链账本查询汇款方对应账户时,不会在汇款交易M完成后察觉到资产变化,避免基于资产变化而暴露汇款方在汇款交易M中承担的真实身份。同时,虽然汇款方对应账户内同时包含已花费和未花费的资产,但是基于对历史密钥镜像集合的维护,可以确保汇款方实际仅能够对未花费的资产进行花费,并准确检测出汇款方对已花费的资产所实施的“双花”操作。

[0162] 当然,为了避免账户内累积的资产过多、增加区块链节点的维护成本,也为了方便各个用户对自身账户内资产进行管理,用户可以对自身账户内的已花费资产进行清理。以上述的汇款方为例,该汇款方可以向区块链网络发起资产删除请求,以从区块链账本中删除该汇款方已花费的至少一部分资产;例如,汇款方可以指定所需删除的资产对应的资产标识,或者汇款方可以指定一时间段(可以指定时间段的两侧端点;如果仅指定左侧端点,则时间段为从该左侧端点对应时刻至今;如果仅指定右侧端点,则时间段为从账户创建至该右侧端点对应时刻)并删除该时间段内产生或被花费的所有资产。

[0163] 步骤604a,获取所述汇款交易M的可链接环签名包含的密钥镜像 $I_1 \sim I_m$ ,所述密钥镜像 $I_1 \sim I_m$ 的取值与汇款方的私钥 $x_j$ 、公钥 $P_j$ 和资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关。

[0164] 汇款方需要维护一组公私钥对,比如私钥 $x_j$ 和公钥 $P_j$ 。在确定这组公私钥对之前,需要取定一个数域 $Z_q$ 和该数域上的一条椭圆曲线,比如椭圆曲线Ed25519等,令 $G$ 、 $H$ 为该椭圆曲线的两个随机的生成元,其中 $|G|=p$ 为一个素数(譬如不小于某一预设数值),并在数值范围 $(0, p)$ 中选取汇款方的私钥 $x_j$ ,相应的公钥为 $P_j = x_j \times G$ 。对于掩护方等其他用户而言,均通过类似的方式确定出各自唯一对应的公私钥对。

[0165] 密钥镜像 $I_1 \sim I_m$ 与汇款方提供的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 之间一一对应,分别用于验证相应的待花费资产是否已花费,从而解决“双花”问题。其中,由于密钥镜像 $I_1 \sim I_m$ 的取值与相应资产的资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关,使得即便所有密钥镜像均采用同一组公私钥对(即汇款方的私钥 $x_j$ 和公钥 $P_j$ ),也可以基于资产标识 $ID_{j_1} \sim ID_{j_m}$ 之间的取值差异,确保生成的密钥镜像 $I_1 \sim I_m$ 之间完全不同,因而无需为每一资产分别维护一组公私钥对,可以在解决“双花”问题的同时,使得每一账户所需维护的公私钥对的数量与交易所含的资产数量无关。例如, $I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d}), d \in [1, m]$ ;其中, $\text{Hash}_G()$ 为上述椭圆曲线到其自身的哈希函数。

[0166] 区块链节点在收到汇款交易M后,可以将密钥镜像 $I_1 \sim I_m$ 与历史密钥镜像集合进行比对,以确定历史密钥镜像集合中是否存在与密钥镜像 $I_1 \sim I_m$ 相同的历史密钥镜像。历史密钥镜像集合用于存储先前已花费的资产对应的密钥镜像。如果存在与密钥镜像 $I_1 \sim I_m$ 中的某一密钥镜像相同的历史密钥镜像,表明该密钥镜像对应的资产已经被花费,即出现了“双花”问题,应当阻止汇款交易M的执行。而如果密钥镜像 $I_1 \sim I_m$ 不属于历史密钥镜像集合,则表明密钥镜像 $I_1 \sim I_m$ 对应的资产 $ID_{j_1} \sim ID_{j_m}$ 均未被花费,在其他交易执行条件被满足的情况下,可以执行汇款交易M;并且,当汇款交易M完成后,密钥镜像 $I_1 \sim I_m$ 对应的资产 $ID_{j_1} \sim ID_{j_m}$ 均被花费,因而需要将密钥镜像 $I_1 \sim I_m$ 添加至历史密钥镜像集合中,以用于后续检测与密钥镜像 $I_1 \sim I_m$ 相关的“双花”问题。

[0167] 步骤604b,验证所述可链接环签名,所述可链接环签名由汇款方根据自身所持的私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 所持的公钥 $P_i$ 而生成。

[0168] 可链接环签名可以由汇款方直接根据自身对应的私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 对应的公钥 $P_i$ 生成,而不需要利用下述汇款方对应的伪私钥 $r'$ 、伪公钥 $P''_j$ 和掩护方 $i$ 对应的伪公钥 $P''_i$ 。此时,如果该可链接环签名通过验证,就能够证明该可链接环签名是由公钥 $(P_1, \dots, P_n)$ 中的某一公钥对应的私钥进行签名得到,从而在不暴露汇款方身份的前提下,完成身份验证。

[0169] 可链接环签名可以由汇款方根据自身对应的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r'$ 、伪公钥 $P''_j$ ,以及掩护方 $i$ 对应的公钥 $P_i$ 、伪公钥 $P''_i$ 而生成。其中,伪公钥 $P''_j = [\text{PC}(t_{j_1}, r_{j_1}) + \dots + \text{PC}(t_{j_m}, r_{j_m})] - [\text{PC}(t'_1, r'_1) + \dots + \text{PC}(t'_u, r'_u)]$ 、伪私钥 $r' = (r_{j_1} + \dots + r_{j_m}) - (r'_1 + \dots + r'_u)$ 。同时,根据掩护方 $i$ 持有资产 $[ID_{i_1}, \text{PC}\{i, 1\}] \sim [ID_{i_m}, \text{PC}\{i, m\}]$ ,汇款方可以计算出掩护方 $i$ 对应的伪公钥 $P''_i = [\text{PC}\{i, 1\} + \dots + \text{PC}\{i, m\}] - [\text{PC}(t'_1, r'_1) + \dots + \text{PC}(t'_u, r'_u)]$ ,  $i \in [1, j-1] \cup [j+1, n]$ 。可链接环签名的生成过程可以参考图5所示的实施例,此处不再赘述。而区块链节点通过对该可链接环签名进行验证,可以高效、紧凑地实现下述两方面的验证功能:一方面,由于伪公钥 $P''_j$ 与伪私钥 $r'$ 之间满足

$P''_j=r'' \times G$ 、伪公钥 $P''_i$ 与伪私钥 $r''$ 之间满足 $P''_i \neq r'' \times G$ ,所以当根据伪私钥 $r''$ 、伪公钥 $P''_j$ 和 $P''_i$ 生成可链接环签名时,如果该可链接环签名通过验证,就能够证明在伪公钥( $P''_1, \dots, P''_n$ )中存在某一伪公钥的取值等于 $r'' \times G$ ,并且这个伪公钥对应于前述的 $t''=0$ ,能够使得汇款交易M的汇入额等于汇出额;另一方面,当根据汇款方对应的私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 对应的公钥 $P_i$ 生成可链接环签名时,如果该可链接环签名通过验证,就能够证明该可链接环签名是由公钥( $P_1, \dots, P_n$ )中的某一公钥对应的私钥进行签名得到,从而在不暴露汇款方身份的前提下,完成身份验证。

[0170] 步骤606,当满足交易执行条件时,执行所述汇款交易M;所述交易执行条件包括:所述密钥镜像 $I_1 \sim I_m$ 不属于历史密钥镜像集合、所述可链接环签名通过验证;其中,所述密钥镜像 $I_1 \sim I_m$ 在交易完成后被添加至所述历史密钥镜像集合。

[0171] 可链接环签名中还可以包含密钥镜像 $I_{(m+1)}$ ,该密钥镜像由汇款方根据自身对应的伪私钥 $r''$ 和伪公钥 $P''_j$ 、掩护方 $i$ 对应的伪公钥 $P''_i$ 生成,例如 $I_{(m+1)}=r'' \times \text{Hash}_G(P''_j)$ 。如前所述,密钥镜像 $I_{(m+1)}$ 与相应交易之间存在一一对应的关系,因而通过将密钥镜像 $I_{(m+1)}$ 与历史密钥镜像进行比较,以识别出针对汇款交易M的重放(replay)问题:如果密钥镜像 $I_{(m+1)}$ 存在相同的历史密钥镜像,就表明汇款交易M发生了重放。那么,交易执行条件还可以包括:密钥镜像 $I_{(m+1)}$ 不属于历史密钥镜像集合。

[0172] 当汇款方对应于公钥 $P_j$ 、掩护方 $i$ 对应于公钥 $P_i$ 时,交易执行条件还可以包括:资产 $ID_{k,d}$ 归属于公钥 $P_k$ 的所有方, $k \in [1, n]$ 、 $d \in [1, m]$ 。换言之,区块链节点可以对各个资产的归属情况进行验证。

[0173] 在机密交易中,区块链节点还可以验证汇款交易M中的转账额 $t'_1 \sim t'_u$ 是否均不小于0。而转账额承诺 $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ 是汇款方根据转账额 $t'_1 \sim t'_u$ 、随机数 $r'_1 \sim r'_u$ 而生成,且转账额 $t'_1 \sim t'_u$ 和随机数 $r'_1 \sim r'_u$ 只有汇款方和收款方 $Q_1 \sim Q_u$ 掌握,因而验证方需要通过汇款交易M所含的范围证明 $RP_1 \sim RP_u$ 实施验证操作,以确定转账额 $t'_1 \sim t'_u$ 是否满足 $t'_1 \geq 0 \sim t'_u \geq 0$ ,其中范围证明 $RP_1 \sim RP_u$ 由汇款方生成并添加至汇款交易M中。那么,交易执行条件还可以包括:所有转账额均不小于0。

[0174] 下面结合图7对步骤604b中验证可链接环签名的过程进行描述;其中,

[0175] 图7是一示例性实施例提供的一种验证可链接环签名的流程图。如图7所示,可以包括以下步骤:

[0176] 步骤702,验证标识 $ID_{k,d}$ 对应的资产是否归属于公钥 $P_k$ 的持有方, $k \in [1, n]$ 、 $d \in [1, m]$ 。

[0177] 验证方可以为区块链网络中的区块链节点,该区块链节点在收到汇款方提交的汇款交易M后,可以对该汇款交易M的环签名进行验证;类似地,每一区块链节点均会收到该汇款交易M,并作为验证方而实施验证。其中,汇款交易M可以由客户端设备发送至验证方,或者汇款交易M可由某一验证方从客户端设备收到后转发至其他验证方,或者汇款交易M可由某一验证方从另一验证方处收到后转发至其他验证方。

[0178] 验证方作为区块链节点而维护有全量的区块链账本,使得验证方可以获知每一用户的资产持有情况。汇款交易M中涉及到用户 $k$ (对应于公钥 $P_k$ )持有的资产 $ID_{k,d}$ ,而验证方可以基于维护的资产持有情况来分别验证每一公钥 $P_k$ 与相应资产 $ID_{k,d}$ 之间的对应关系是否成立,即公钥 $P_k$ 的持有者是否拥有标识 $ID_{k,d}$ 对应的 $m$ 份资产。如果每一公钥 $P_k$ 与



相应数组中的标识ID<sub>k\_d</sub>之间的对应关系均成立,可以继续执行后续步骤;如果某一标识对应的资产并不属于公钥P<sub>k</sub>的持有方,验证方可以判定汇款交易M无效,而无需继续执行后续的步骤704~708。

[0179] 步骤704,根据s<sub>k\_1</sub>~s<sub>k\_(m+1)</sub>依次计算L<sub>k\_1</sub>~L<sub>k\_(m+1)</sub>、R<sub>k\_1</sub>~R<sub>k\_(m+1)</sub>。

[0180] 步骤706,根据L<sub>n\_1</sub>~L<sub>n\_(m+1)</sub>、R<sub>n\_1</sub>~R<sub>n\_(m+1)</sub>计算c<sub>1'</sub>,验证c<sub>1'</sub>是否等于c<sub>1</sub>。

[0181] 验证方可以根据环签名所含的随机数和/或其衍生数值,计算中间参数L<sub>j\_d</sub>、R<sub>j\_d</sub>、L<sub>j\_(m+1)</sub>、R<sub>j\_(m+1)</sub>、L<sub>i\_d</sub>、R<sub>i\_d</sub>、L<sub>i\_(m+1)</sub>、R<sub>i\_(m+1)</sub>,以验证中间参数L<sub>j\_d</sub>与L<sub>i\_d</sub>之间是否符合环形取值规则、中间参数R<sub>j\_d</sub>与R<sub>i\_d</sub>之间是否符合环形取值规则、中间参数L<sub>j\_(m+1)</sub>与L<sub>i\_(m+1)</sub>之间是否符合环形取值规则、中间参数R<sub>j\_(m+1)</sub>与R<sub>i\_(m+1)</sub>之间是否符合环形取值规则。

[0182] 例如,当环签名所含的随机数和/或其衍生数值包括:s<sub>1\_1</sub>~s<sub>1\_(m+1)</sub>,...,s<sub>n\_1</sub>~s<sub>n\_(m+1)</sub>、c<sub>1</sub>时,中间参数L<sub>j\_d</sub>与L<sub>i\_d</sub>之间的环形取值规则可以包括:

[0183]  $L_{k_d} = (s_{k_d} \times G + c_k \times P_k) \bmod p, h \in [1, n]$

$$[0184] \quad c_k = \begin{cases} \text{Hash}[M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}}], k=1 \\ \text{Hash}[M, L_{(j-1)_1}, R_{(j-1)_1}, \dots, L_{(j-1)_{(m+1)}}, \\ R_{(j-1)_{(m+1)}}], k \in [2, n] \end{cases}$$

[0185] 中间参数L<sub>j\_(m+1)</sub>与L<sub>i\_(m+1)</sub>之间的环形取值规则包括:

[0186]  $L_{k_{(m+1)}} = [s_{k_{(m+1)}} \times G + c_k \times P''_k] \bmod p$

[0187] 中间参数R<sub>j\_d</sub>与R<sub>i\_d</sub>之间的环形取值规则包括:

[0188]  $R_{k_d} = [s_{k_d} \times \text{Hash}_G(P_k, ID_{k_d}) + c_k \times I_d] \bmod p$

[0189] 中间参数R<sub>j\_(m+1)</sub>与R<sub>i\_(m+1)</sub>之间的环形取值规则包括:

[0190]  $R_{k_{(m+1)}} = [s_{k_{(m+1)}} \times \text{Hash}_G(P''_k) + c_k \times I_{(m+1)}] \bmod p$

[0191] 那么,验证方可以首先根据s<sub>1\_d</sub>、c<sub>1</sub>、G、P<sub>1</sub>和p生成L<sub>1\_d</sub>,即L<sub>1\_1</sub>~L<sub>1\_m</sub>,以及根据s<sub>1\_d</sub>、c<sub>1</sub>、P<sub>1</sub>、ID<sub>1\_d</sub>、I<sub>d</sub>和p生成R<sub>1\_d</sub>,即R<sub>1\_1</sub>~R<sub>1\_m</sub>;以及,验证方根据s<sub>1\_(m+1)</sub>、c<sub>1</sub>、G、P''<sub>1</sub>和p生成L<sub>1\_(m+1)</sub>,根据s<sub>1\_(m+1)</sub>、c<sub>1</sub>、P''<sub>1</sub>、I<sub>(m+1)</sub>和p生成R<sub>1\_(m+1)</sub>。

[0192] 然后,验证方可以根据M、L<sub>1\_d</sub>、R<sub>1\_d</sub>、L<sub>1\_(m+1)</sub>和R<sub>1\_(m+1)</sub>生成c<sub>2</sub>,并根据s<sub>2\_d</sub>、c<sub>2</sub>、G、P<sub>2</sub>和p生成L<sub>2\_d</sub>,根据s<sub>2\_d</sub>、c<sub>2</sub>、P<sub>2</sub>、ID<sub>2\_d</sub>、I<sub>d</sub>和p生成R<sub>2\_d</sub>,根据s<sub>2\_(m+1)</sub>、c<sub>2</sub>、G、P''<sub>2</sub>和p生成L<sub>2\_(m+1)</sub>,以及根据s<sub>2\_(m+1)</sub>、c<sub>2</sub>、P''<sub>2</sub>、I<sub>(m+1)</sub>和p生成R<sub>2\_(m+1)</sub>;以此类推,直至验证方根据M、L<sub>(n-1)\_d</sub>、R<sub>(n-1)\_d</sub>、L<sub>(n-1)\_(m+1)</sub>和R<sub>(n-1)\_(m+1)</sub>生成c<sub>n</sub>,并根据s<sub>n\_d</sub>、c<sub>n</sub>、G、P<sub>n</sub>和p生成L<sub>n\_d</sub>,根据s<sub>n\_d</sub>、c<sub>n</sub>、P<sub>n</sub>、ID<sub>n\_d</sub>、I<sub>d</sub>和p生成R<sub>n\_d</sub>,根据s<sub>n\_(m+1)</sub>、c<sub>n</sub>、G、P''<sub>n</sub>和p生成L<sub>n\_(m+1)</sub>,以及根据s<sub>n\_(m+1)</sub>、c<sub>n</sub>、P''<sub>n</sub>、I<sub>(m+1)</sub>和p生成R<sub>n\_(m+1)</sub>。

[0193] 进一步地,验证方可以按照上述针对c<sub>k</sub>的计算公式,计算得到c<sub>1'</sub> = Hash[M, L<sub>n\_1</sub>, R<sub>n\_1</sub>, ..., L<sub>n\_(m+1)</sub>, R<sub>n\_(m+1)</sub>]。之所以此处采用c<sub>1'</sub>,是为了区分于环签名所含的c<sub>1</sub>,那么验证方可以将该c<sub>1'</sub>与环签名所含的c<sub>1</sub>进行比较:如果c<sub>1'</sub>与c<sub>1</sub>相等,表明

上述的环形取值规则被满足,可以确定:1)在伪公钥 $P_1 \sim P_n$ 中,存在一个伪公钥使得汇款交易M的汇入额等于汇出额;2)环签名由公钥 $P_1 \sim P_m$ 中的某一公钥对应的私钥生成。而如果 $c_1'$ 与 $c_1$ 不相等,表明1)和2)中至少一个不成立,该汇款交易M被确认为无效,无需继续执行下述步骤708。

[0194] 步骤708,验证范围证明 $RP_1 \sim RP_u$ 。

[0195] 验证方从汇款交易M的交易内容中获取范围证明 $RP_1 \sim RP_u$ 并验证,以确定相应的转账额 $t'_1 \sim t'_u$ 是否均满足不小于0。如果满足,则转入步骤710,否则汇款交易M被确认为无效,无需继续执行下述步骤710。

[0196] 步骤710,验证密钥镜像 $I_1 \sim I_{(m+1)}$ 是否已存在。

[0197] 在一实施例中,验证方可以将密钥镜像 $I_1 \sim I_{(m+1)}$ 与历史密钥镜像进行比较,从而确定密钥镜像 $I_1 \sim I_{(m+1)}$ 是否已存在。如果密钥镜像 $I_1 \sim I_{(m+1)}$ 中的任一密钥镜像已存在对应的历史密钥镜像,可以判定汇款交易M无效;如果密钥镜像 $I_1 \sim I_{(m+1)}$ 均不存在对应的历史密钥镜像,可以判定汇款交易M有效,可以执行该汇款交易M、完成汇款操作。

[0198] 图8是一示例性实施例提供的一种设备的示意结构图。请参考图8,在硬件层面,该设备包括处理器802、内部总线804、网络接口806、内存808以及非易失性存储器810,当然还可能包括其他业务所需要的硬件。处理器802从非易失性存储器810中读取对应的计算机程序到内存808中然后运行,在逻辑层面上形成基于环签名的匿名交易装置。当然,除了软件实现方式之外,本说明书一个或多个实施例并不排除其他实现方式,比如逻辑器件抑或软硬件结合的方式等等,也就是说以下处理流程的执行主体并不限定于各个逻辑单元,也可以是硬件或逻辑器件。

[0199] 请参考图9,在软件实施方式中,该基于环签名的匿名交易装置可以包括:

[0200] 交易组装单元91,根据汇款方对应账户内的待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、掩护方i对应账户内的掩护资产 $ID_{i_1} \sim ID_{i_m}$ ,组装汇款交易M;其中,待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、掩护资产 $ID_{i_1} \sim ID_{i_m}$ 在区块链账本中被分别记录为相应资产额对应的资产承诺, $i \in [1, j-1] \cup [j+1, n]$ ;

[0201] 签名生成单元92,根据汇款方所持私钥 $x_j$ 、公钥 $P_j$ 和掩护方i所持公钥 $P_i$ ,为所述汇款交易M生成可链接环签名,所述可链接环签名中包含密钥镜像 $I_1 \sim I_m$ ,且密钥镜像 $I_1 \sim I_m$ 的取值与汇款方的私钥 $x_j$ 、公钥 $P_j$ 和资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关;

[0202] 交易提交单元93,向区块链网络提交签名后的汇款交易M;其中,在交易完成后,密钥镜像 $I_1 \sim I_m$ 被添加至历史密钥镜像集合,且所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 在区块链账本上被保持记录为汇款方持有的资产。

[0203] 可选的,通过下述公式计算所述密钥镜像 $I_1 \sim I_m$ :

[0204]  $I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d}), d \in [1, m]$ ;

[0205] 其中, $\text{Hash}_G()$ 为椭圆曲线到其自身的哈希函数。

[0206] 可选的,所述掩护方包括以下任一或其组合:所述汇款交易M的实际收款方、区别于所述汇款方和所述实际收款方的其他用户。

[0207] 可选的,

[0208] 当不存在找零时,所述汇款交易M的交易收款方为实际收款方;当存在找零时,所

述汇款交易M的交易收款方为所述汇款方和所述实际收款方；或，

[0209] 所述交易收款方包括所述实际收款方和所述汇款方；其中，当不存在找零时，所述汇款方对应的转账额为0；或，

[0210] 所述交易收款方包括所述实际收款方、所述汇款方、区别于所述实际收款方和所述汇款方的掩护方；其中，当不存在找零时，所述汇款方和作为交易收款方的掩护方对应的转账额为0；当存在找零时，所述汇款方对应的转账额为找零额、作为交易收款方的掩护方对应的转账额为0。

[0211] 可选的，还包括：

[0212] 证明生成单元94，针对所述汇款交易M的各个交易收款方对应的转账额，分别生成相应的范围证明，所述范围证明被组装至所述汇款交易M中，以用于证明相应的转账额不小于0。

[0213] 可选的，

[0214] 所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>、所述资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>为相应的历史交易的交易输出；或，

[0215] 所述待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>被从汇款方对应的账户余额中划分而生成、所述资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>被从掩护方i对应的账户余额中划分而生成。

[0216] 可选的，签名生成单元92具体用于：

[0217] 根据待花费资产ID<sub>j\_1</sub>~ID<sub>j\_m</sub>对应的资产额 $t_{j_1} \sim t_{j_m}$ 、随机数 $r_{j_1} \sim r_{j_m}$ 和资产承诺 $PC(t_{j_1}, r_{j_1}) \sim PC(t_{j_m}, r_{j_m})$ ，以及交易收款方 $Q_1 \sim Q_u$ 对应的转账额 $t'_1 \sim t'_u$ 、随机数 $r'_1 \sim r'_u$ 和转账额承诺 $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ ，确定对应于汇款方的伪公钥 $P''_j = [PC(t_{j_1}, r_{j_1}) + \dots + PC(t_{j_m}, r_{j_m})] - [PC(t'_1, r'_1) + \dots + PC(t'_u, r'_u)]$ 、对应于汇款方的伪私钥 $r'' = (r_{j_1} + \dots + r_{j_m}) - (r'_1 + \dots + r'_u)$ ， $u \geq 1$ ；

[0218] 根据掩护资产ID<sub>i\_1</sub>~ID<sub>i\_m</sub>对应的资产承诺 $PC\{i, 1\} \sim PC\{i, m\}$ ，确定对应于掩护方i的伪公钥 $P''_i = [PC\{i, 1\} + \dots + PC\{i, m\}] - [PC(t'_1, r'_1) + \dots + PC(t'_u, r'_u)]$ ， $i \in [1, j-1] \cup [j+1, n]$ ；

[0219] 根据汇款方对应的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r''$ 、伪公钥 $P''_j$ ，掩护方i对应的公钥 $P_i$ 、伪公钥 $P''_i$ ，为所述汇款交易M生成可链接环签名。

[0220] 可选的，还包括：

[0221] 镜像生成单元95，根据汇款方对应的伪私钥 $r''$ 、伪公钥 $P''_j$ ，生成密钥镜像 $I_{(m+1)} = r'' \times \text{Hash}_G(P''_j)$ ；其中，所述可链接环签名还包含所述密钥镜像 $I_{(m+1)}$ 。

[0222] 可选的，签名生成单元92具体用于：

[0223] 分别生成对应于汇款方的中间参数 $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}$ ，以及对应于掩护方i的中间参数 $L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$ ， $d \in [1, m]$ ；其中，中间参数 $L_{j_d}$ 与 $L_{i_d}$ 之间符合环形取值规则、中间参数 $L_{j_{(m+1)}}$ 与 $L_{i_{(m+1)}}$ 之间符合环形取值规则、中间参数 $R_{j_d}$ 与 $R_{i_d}$ 之间符合环形取值规则、中间参数 $R_{j_{(m+1)}}$ 与 $R_{i_{(m+1)}}$ 之间符合环形取值规则，且中间参数 $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}、L_{i_d}, R_{i_d}, L_{i_{(m+1)}}、R_{i_{(m+1)}}$ 的取值与至少一个被选取的随机数和/或其衍生数值相关；

[0224] 根据被选取的随机数和/或其衍生数值，生成针对所述汇款交易M的可链接环签

名。

[0225] 可选的，

[0226]  $P_j = x_j \times G$ ,  $G$ 为椭圆曲线的基点,  $|G| = p$ 且 $p$ 为素数,  $0 < x_j < p$ ;

[0227] 生成对应于汇款方的中间参数 $L_{j\_d}$ 、 $R_{j\_d}$ , 包括: 根据在所述椭圆曲线所处的数域 $Z_q$ 中选取的随机数 $a_d$ , 计算中间参数 $L_{j\_d}$ 、 $R_{j\_d}$ , 使得 $L_{j\_d} = a_d \times G$ 、 $R_{j\_d} = a_d \times \text{Hash}_G(P_j, ID_{j\_d})$ ; 其中,  $\text{Hash}_G()$ 为从所述椭圆曲线到其自身的哈希函数;

[0228] 生成对应于汇款方的中间参数 $L_{j\_ (m+1)}$ 、 $R_{j\_ (m+1)}$ , 包括: 根据在所述椭圆曲线所处的数域 $Z_q$ 中选取的随机数 $a_{(m+1)}$ , 计算中间参数 $L_{j\_ (m+1)}$ 、 $R_{j\_ (m+1)}$ , 使得 $L_{j\_ (m+1)} = a_{(m+1)} \times G$ 、 $R_{j\_ (m+1)} = a_{(m+1)} \times \text{Hash}_G(P''_j)$ ;

[0229] 生成对应于掩护方 $i$ 的中间参数 $L_{i\_d}$ 、 $R_{i\_d}$ 、 $L_{i\_ (m+1)}$ 、 $R_{i\_ (m+1)}$ , 包括: 根据中间参数 $L_{j\_d}$ 、 $R_{j\_d}$ 的取值, 生成中间参数 $L_{i\_d}$ 、 $R_{i\_d}$ 、 $L_{i\_ (m+1)}$ 、 $R_{i\_ (m+1)}$ , 使得 $L_{i\_d} = (s_{i\_d} \times G + c_i \times P_i) \bmod p$ 、 $R_{i\_d} = (s_{i\_d} \times \text{Hash}_G(P_i, ID_{i\_d}) + c_i \times I_d) \bmod p$ 、 $L_{i\_ (m+1)} = [s_{i\_ (m+1)} \times G + c_i \times P''_i] \bmod p$ 、 $R_{i\_ (m+1)} = [s_{i\_ (m+1)} \times \text{Hash}_G(P''_i) + c_i \times I_{(m+1)}] \bmod p$ 、 $I_d = x_j \times \text{Hash}_G(P_j, ID_{j\_d})$ 、 $I_{(m+1)} = r'' \times \text{Hash}_G(P''_j)$ ; 其中,  $s_{i\_1} \sim s_{i\_ (m+1)}$ 为数域 $Z_q$ 中的随机数, 当 $i = 1$ 时 $c_1 = \text{Hash}(M, L_{n\_1}, R_{n\_1}, \dots, L_{n\_ (m+1)}, R_{n\_ (m+1)})$ 、当 $i \in [2, j-1] \cup [j+1, n]$ 时 $c_i = \text{Hash}(M, L_{(i-1)\_1}, R_{(i-1)\_1}, \dots, L_{(i-1)\_ (m+1)}, R_{(i-1)\_ (m+1)})$ ,  $\text{Hash}()$ 为从所述椭圆曲线到数域 $Z_q$ 的哈希函数;

[0230] 被选取的随机数和/或其衍生数值包括: 随机数 $s_{i\_1} \sim s_{i\_ (m+1)}$ 、衍生数值 $c_1$ 、衍生数值 $s_{j\_1} \sim s_{j\_ (m+1)}$ ; 其中,  $s_{j\_d} = (a_d - c_j \times x_j) \bmod p$ 、 $s_{j\_ (m+1)} = [a_{(m+1)} - c_j \times r''] \bmod p$ , 当 $j$ 的取值被确定为1时 $c_j = \text{Hash}(M, L_{n\_1}, R_{n\_1}, \dots, L_{n\_ (m+1)}, R_{n\_ (m+1)})$ 、当 $j$ 的取值被确定为属于 $[2, n]$ 时 $c_j = \text{Hash}(M, L_{(j-1)\_1}, R_{(j-1)\_1}, \dots, L_{(j-1)\_ (m+1)}, R_{(j-1)\_ (m+1)})$ 。

[0231] 可选的, 还包括:

[0232] 资产删除单元96, 向区块链网络发起资产删除请求, 以从区块链账本中删除所述汇款方已花费的至少一部分资产。

[0233] 图10是一示例性实施例提供的一种设备的示意结构图。请参考图10, 在硬件层面, 该设备包括处理器1002、内部总线1004、网络接口1006、内存1008以及非易失性存储器1010, 当然还可能包括其他业务所需要的硬件。处理器1002从非易失性存储器1010中读取对应的计算机程序到内存1008中然后运行, 在逻辑层面上形成基于环签名的匿名交易装置。当然, 除了软件实现方式之外, 本说明书一个或多个实施例并不排除其他实现方式, 比如逻辑器件抑或软硬件结合的方式等等, 也就是说以下处理流程的执行主体并不限于各个逻辑单元, 也可以是硬件或逻辑器件。

[0234] 请参考图11, 在软件实施方式中, 该基于环签名的匿名交易装置可以包括:

[0235] 交易接收单元1101, 接收汇款交易 $M$ , 所述汇款交易 $M$ 由汇款方根据自身对应账户内的待花费资产 $ID_{j\_1} \sim ID_{j\_m}$ 、掩护方 $i$ 对应账户内的掩护资产 $ID_{i\_1} \sim ID_{i\_m}$ 组装生成,  $i \in [1, j-1] \cup [j+1, n]$ ; 在交易完成后, 资产 $ID_{j\_1} \sim ID_{j\_m}$ 在区块链账本上被保持记录为汇款方持有的资产;

[0236] 镜像获取单元1102, 获取所述汇款交易 $M$ 的可链接环签名包含的密钥镜像 $I_1 \sim I_{$

m,所述密钥镜像 $I_1 \sim I_m$ 的取值与汇款方的私钥 $x_j$ 、公钥 $P_j$ 和资产标识 $ID_{j_1} \sim ID_{j_m}$ 相关;

[0237] 签名验证单元1103,验证所述可链接环签名,所述可链接环签名由汇款方根据自身所持的私钥 $x_j$ 、公钥 $P_j$ 和掩护方 $i$ 所持的公钥 $P_i$ 而生成;

[0238] 交易执行单元1104,当满足交易执行条件时,执行所述汇款交易M;所述交易执行条件包括:所述密钥镜像 $I_1 \sim I_m$ 不属于历史密钥镜像集合、所述可链接环签名通过验证;其中,所述密钥镜像 $I_1 \sim I_m$ 在交易完成后被添加至所述历史密钥镜像集合。

[0239] 可选的,所述密钥镜像 $I_1 \sim I_m$ 由汇款方通过下述公式计算得到:

[0240]  $I_d = x_j \times \text{Hash}_G(P_j, ID_{j_d}), d \in [1, m]$ ;

[0241] 其中, $\text{Hash}_G()$ 为椭圆曲线到其自身的哈希函数。

[0242] 可选的,所述掩护方包括以下任一或其组合:所述汇款交易M的实际收款方、区别于所述汇款方和所述实际收款方的其他用户。

[0243] 可选的,

[0244] 当不存在找零时,所述汇款交易M的交易收款方为实际收款方;当存在找零时,所述汇款交易M的交易收款方为所述汇款方和所述实际收款方;或,

[0245] 所述交易收款方包括所述实际收款方和所述汇款方;其中,当不存在找零时,所述汇款方对应的转账额为0;或,

[0246] 所述交易收款方包括所述实际收款方、所述汇款方、区别于所述实际收款方和所述汇款方的掩护方;其中,当不存在找零时,所述汇款方和作为交易收款方的掩护方对应的转账额为0;当存在找零时,所述汇款方对应的转账额为找零额、作为交易收款方的掩护方对应的转账额为0。

[0247] 可选的,还包括:

[0248] 数额验证单元1105,根据汇款交易M所含的范围证明,验证各个交易收款方对应的转账额是否均不小于0;

[0249] 其中,所述交易执行条件还包括:各个交易收款方对应的转账额均不小于0。

[0250] 可选的,

[0251] 所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 、所述资产 $ID_{i_1} \sim ID_{i_m}$ 为相应的历史交易的交易输出;或,

[0252] 所述待花费资产 $ID_{j_1} \sim ID_{j_m}$ 被从汇款方对应的账户余额中划分而生成、所述资产 $ID_{i_1} \sim ID_{i_m}$ 被从掩护方 $i$ 对应的账户余额中划分而生成。

[0253] 可选的,所述交易执行条件还包括:资产 $ID_{k_d}$ 归属于公钥 $P_k$ 的所有方, $k \in [1, n]$ 、 $d \in [1, m]$ 、 $i \in [1, j-1] \cup [j+1, n]$ 。

[0254] 可选的,所述可链接环签名由汇款方根据对应于自身的私钥 $x_j$ 、公钥 $P_j$ 、伪私钥 $r''$ 和伪公钥 $P''_j$ ,以及对应于掩护方 $i$ 的公钥 $P_i$ 和伪公钥 $P''_i$ 而生成,使得当所述可链接环签名通过验证时,所述汇款交易M被确认为输入与输出等额;

[0255] 其中,伪公钥 $P''_j = [\text{PC}(t_{j_1}, r_{j_1}) + \dots + \text{PC}(t_{j_m}, r_{j_m})] - [\text{PC}(t'_{j_1}, r'_{j_1}) + \dots + \text{PC}(t'_{j_u}, r'_{j_u})]$ 、伪私钥 $r'' = (r_{j_1} + \dots + r_{j_m}) - (r'_{j_1} + \dots + r'_{j_u})$ 、伪公钥 $P''_i = [\text{PC}\{i, 1\} + \dots + \text{PC}\{i, m\}] - [\text{PC}(t'_{j_1}, r'_{j_1}) + \dots + \text{PC}(t'_{j_u}, r'_{j_u})]$ ,  $i \in [1, j-1] \cup [j+1, n]$ ,资产标识 $ID_{j_1} \sim ID_{j_m}$ 对应于资产额 $t_{j_1} \sim t_{j_m}$ 、随机数 $r_{j_1} \sim r_{j_m}$ 和资产承诺PC

$(t_{j_1}, r_{j_1}) \sim PC(t_{j_m}, r_{j_m})$ , 掩护资产  $ID_{i_1} \sim ID_{i_m}$  对应于资产承诺  $PC\{i, 1\} \sim PC\{i, m\}$ , 交易收款方  $Q_1 \sim Q_u$  对应于转账额  $t'_1 \sim t'_u$ 、随机数  $r'_1 \sim r'_u$  和转账额承诺  $PC(t'_1, r'_1) \sim PC(t'_u, r'_u)$ ,  $u \geq 1$ 。

[0256] 可选的, 所述可链接环签名还包括密钥镜像  $I_{(m+1)} = r'' \times Hash\_G(P''_j)$ ;

[0257] 其中, 所述交易执行条件还包括: 密钥镜像  $I_{(m+1)}$  不属于所述历史密钥镜像集合。

[0258] 可选的, 汇款方根据对应于自身的私钥  $x_j$ 、公钥  $P_j$ 、伪私钥  $r''$ 、伪公钥  $P''_j$ , 掩护方  $i$  对应的公钥  $P_i$ 、伪公钥  $P''_i$ , 分别生成对应于汇款方的中间参数  $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}$ , 以及对应于掩护方  $i$  的中间参数  $L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$ , 并根据与中间参数  $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}、L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$  的取值相关的随机数和/或其衍生数值而生成所述可链接环签名,  $d \in [1, m]$ ; 验证所述可链接环签名, 包括:

[0259] 根据所述环签名所含的随机数和/或其衍生数值, 计算中间参数  $L_{j_d}, R_{j_d}, L_{j_{(m+1)}}, R_{j_{(m+1)}}、L_{i_d}, R_{i_d}, L_{i_{(m+1)}}, R_{i_{(m+1)}}$ , 以验证中间参数  $L_{j_d}$  与  $L_{i_d}$  之间是否符合环形取值规则、中间参数  $L_{j_{(m+1)}}$  与  $L_{i_{(m+1)}}$  之间是否符合环形取值规则、中间参数  $R_{j_d}$  与  $R_{i_d}$  之间是否符合环形取值规则、中间参数  $R_{j_{(m+1)}}$  与  $R_{i_{(m+1)}}$  之间是否符合环形取值规则。

[0260] 可选的,

[0261]  $P_j = x_j \times G$ ,  $G$  为椭圆曲线的基点,  $|G| = p$  且  $p$  为素数,  $0 < x_j < p$ ;

[0262] 所述环签名所含的随机数和/或其衍生数值包括:  $s_{k_1} \sim s_{k_{(m+1)}}、c_1, k \in [1, n]$ ;

[0263] 中间参数  $L_{j_d}$  与  $L_{i_d}$  之间的环形取值规则包括:  $L_{k_d} = (s_{k_d} \times G + c_k \times P_k) \bmod p$ ; 其中,  $s_{k_d}$  属于所述椭圆曲线所处的数域  $Z_q$ ,  $Hash()$  为从所述椭圆曲线到数域  $Z_q$  的哈希函数;

[0264] 中间参数  $L_{j_{(m+1)}}$  与  $L_{i_{(m+1)}}$  之间的环形取值规则包括:  $L_{k_{(m+1)}} = [s_{k_{(m+1)}} \times G + c_k \times P''_k] \bmod p$ ; 其中,  $s_{k_{(m+1)}}$  属于数域  $Z_q$ ;

[0265] 中间参数  $R_{j_d}$  与  $R_{i_d}$  之间的环形取值规则包括:  $R_{k_d} = (s_{k_d} \times Hash\_G(P_k, ID_{k_d}) + c_k \times I_d) \bmod p$ ,  $I_d$  被包含于所述环签名中;

[0266] 中间参数  $R_{j_{(m+1)}}$  与  $R_{i_{(m+1)}}$  之间的环形取值规则包括:  $R_{k_{(m+1)}} = [s_{k_{(m+1)}} \times Hash\_G(P''_k) + c_k \times I_{(m+1)}] \bmod p$ ,  $I_{(m+1)}$  被包含于所述环签名中;

[0267] 其中, 当  $h=1$  时  $c_1 = Hash(M, L_{n_1}, R_{n_1}, \dots, L_{n_{(m+1)}}, R_{n_{(m+1)}})$ 、当  $h \in [2, n]$  时  $c_k = Hash(M, L_{(h-1)_1}, R_{(h-1)_1}, \dots, L_{(h-1)_{(m+1)}}, R_{(h-1)_{(m+1)}})$ 。

[0268] 可选的, 还包括:

[0269] 资产删除单元 1106, 根据所述汇款方向区块链网络发起的资产删除请求, 从区块链账本中删除所述汇款方已花费的至少一部分资产。

[0270] 上述实施例阐明的系统、装置、模块或单元, 具体可以由计算机芯片或实体实现, 或者由具有某种功能的产品来实现。一种典型的实现设备为计算机, 计算机的具体形式可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的

任意几种设备的组合。

[0271] 在一个典型的配置中,计算机包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0272] 内存可能包括计算机可读介质中的非永久性存储器,随机存取存储器(RAM)和/或非易失性内存等形式,如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0273] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括,但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带、磁盘存储、量子存储器、基于石墨烯的存储介质或其他磁性存储设备或任何其他非传输介质,可用于存储可以被计算设备访问的信息。按照本文中的界定,计算机可读介质不包括暂存电脑可读媒体(transitory media),如调制的数据信号和载波。

[0274] 还需要说明的是,术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含,从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素,而且还包括没有明确列出的其他要素,或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下,由语句“包括一个……”限定的要素,并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0275] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0276] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式,除非上下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[0277] 应当理解,尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息,但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如,在不脱离本说明书一个或多个实施例范围的情况下,第一信息也可以被称为第二信息,类似地,第二信息也可以被称为第一信息。取决于语境,如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0278] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已,并不用以限制本说明书一个或多个实施例,凡在本说明书一个或多个实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本说明书一个或多个实施例保护的范围之内。

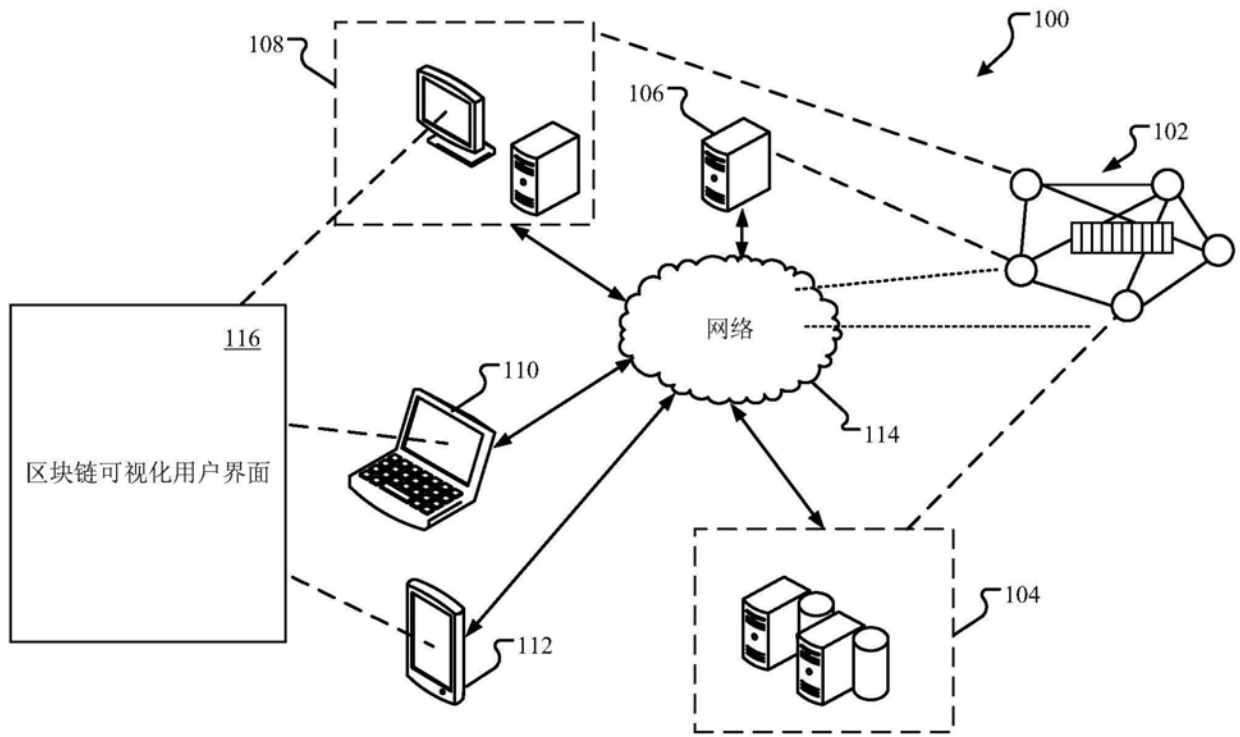


图1



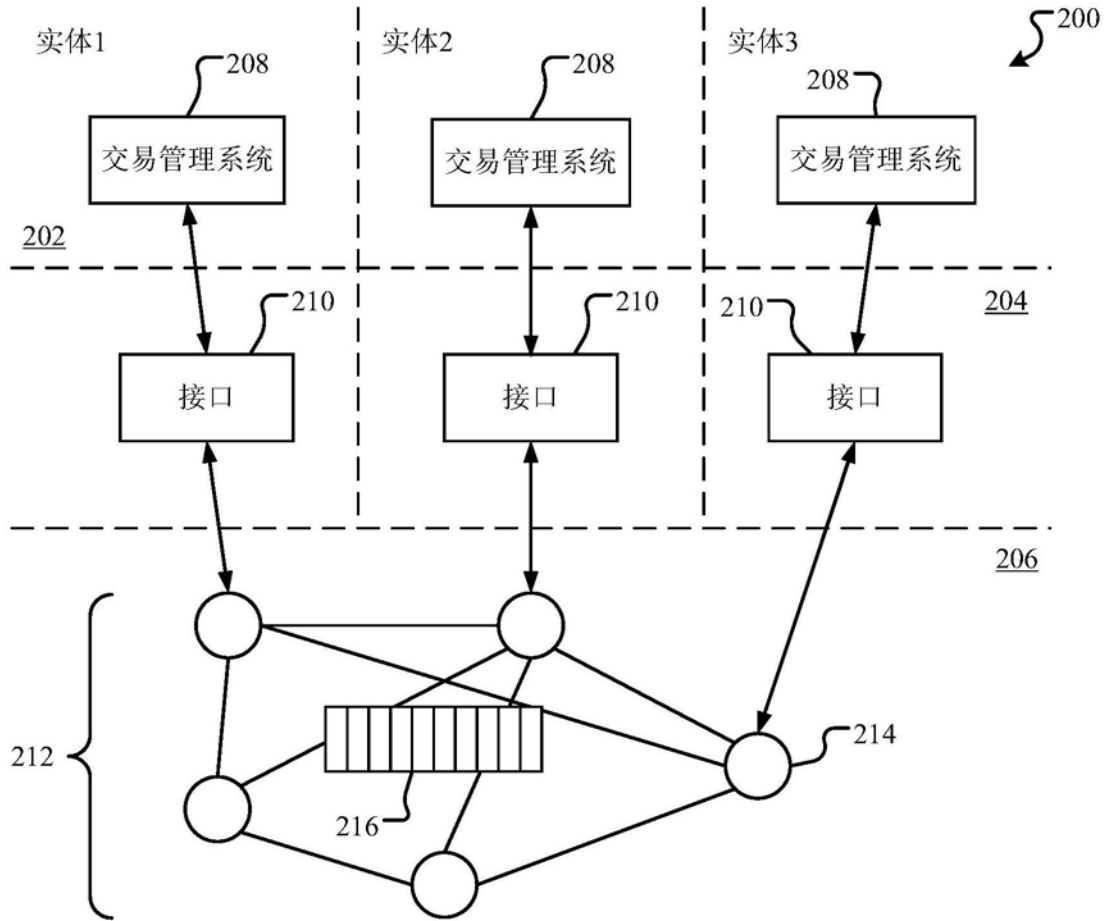


图2

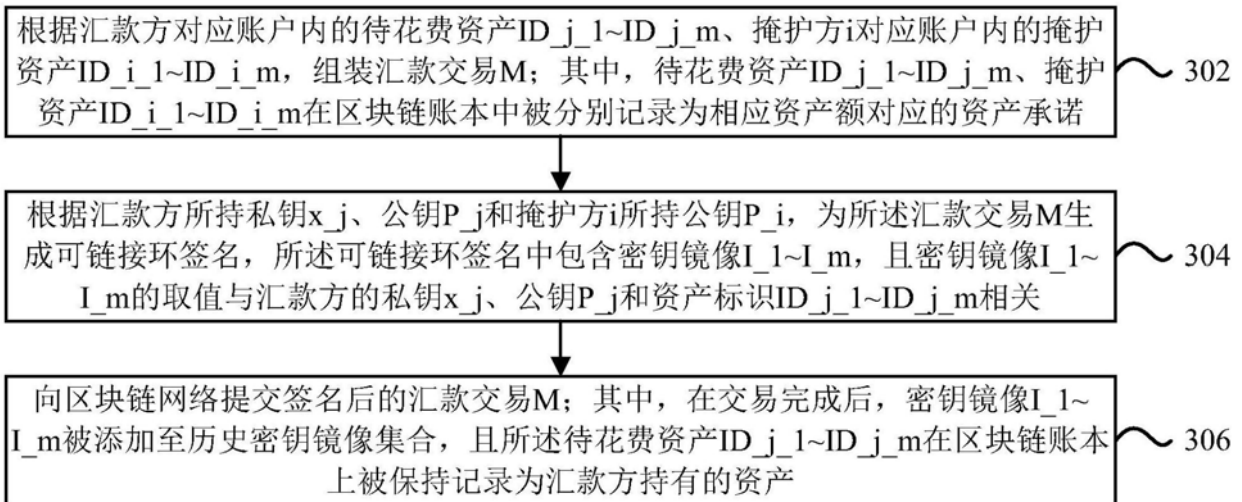


图3

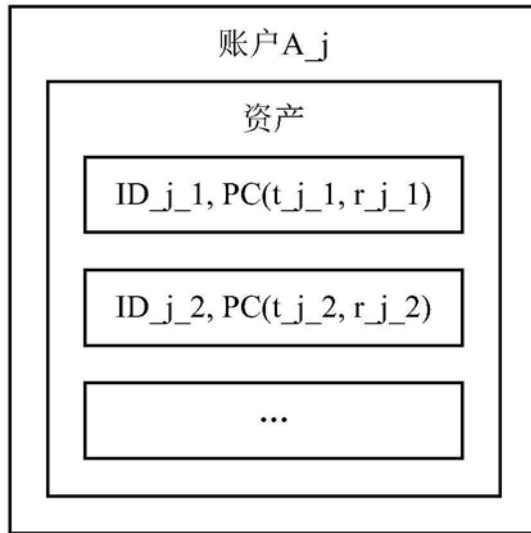


图4

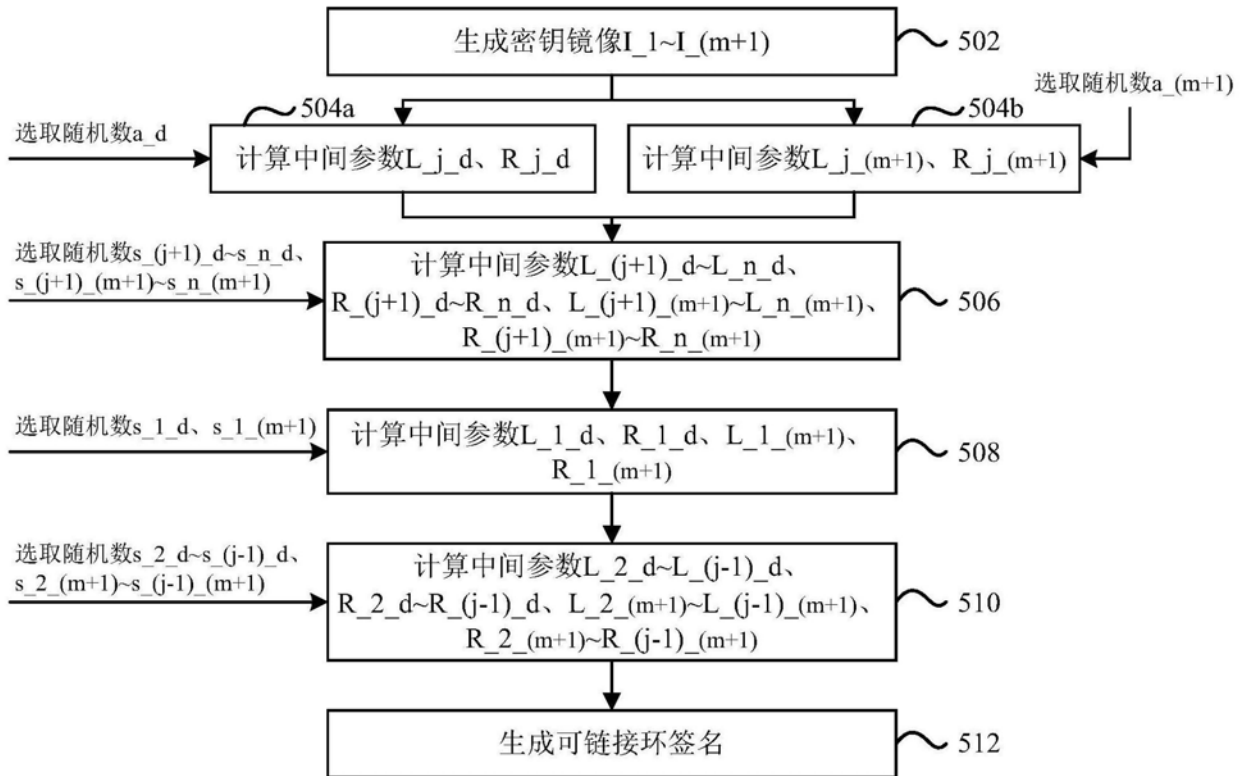


图5

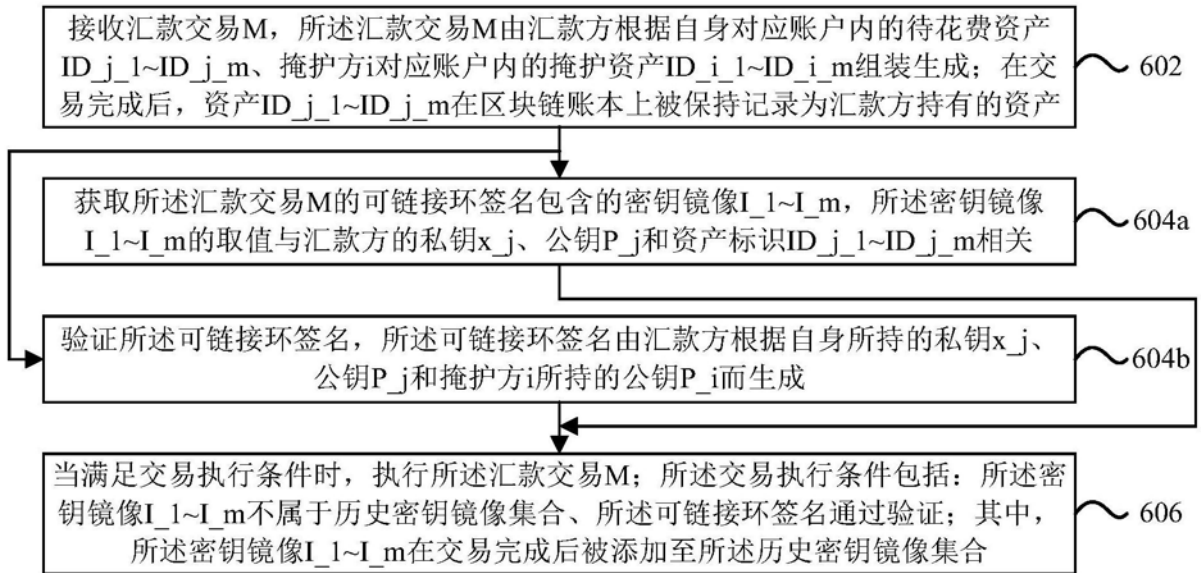


图6

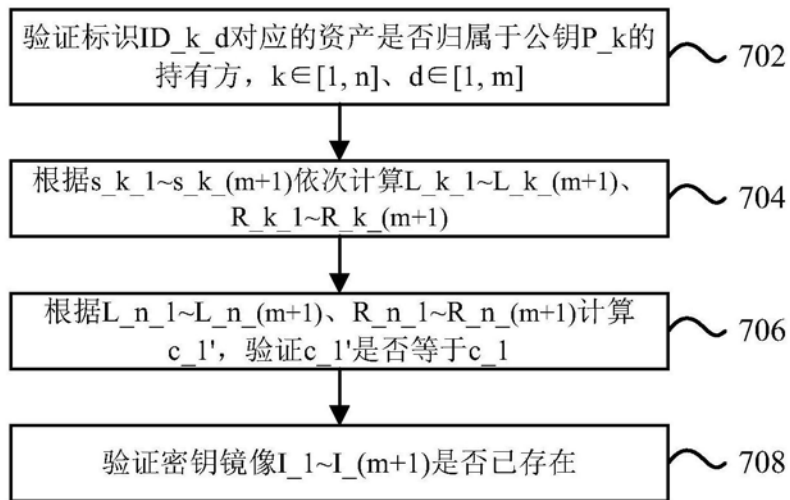


图7

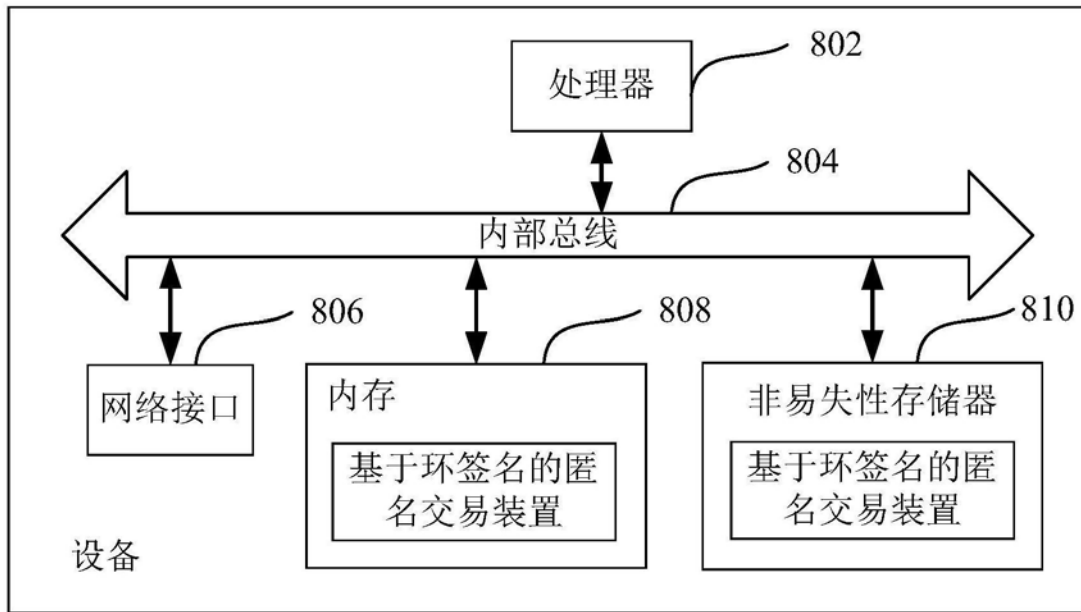


图8

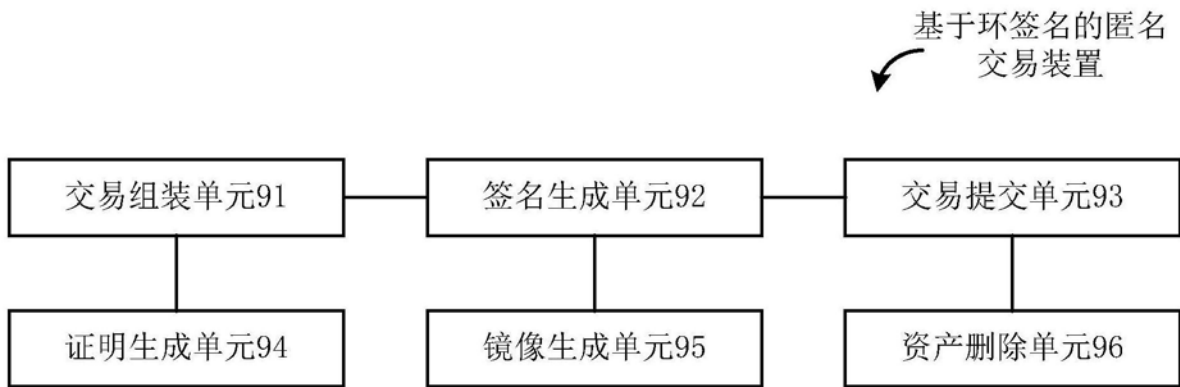


图9

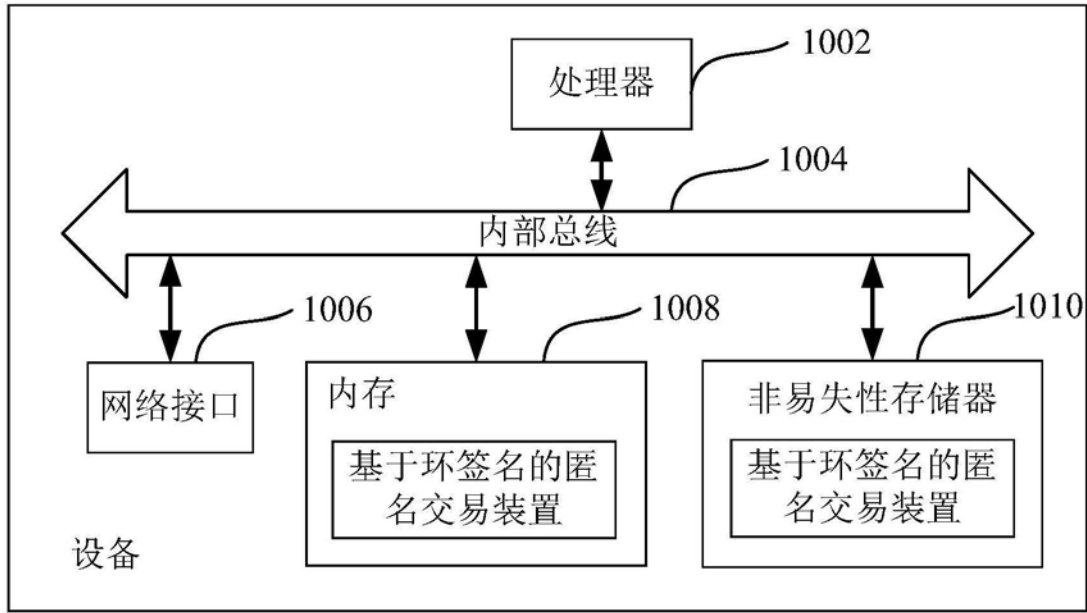


图10

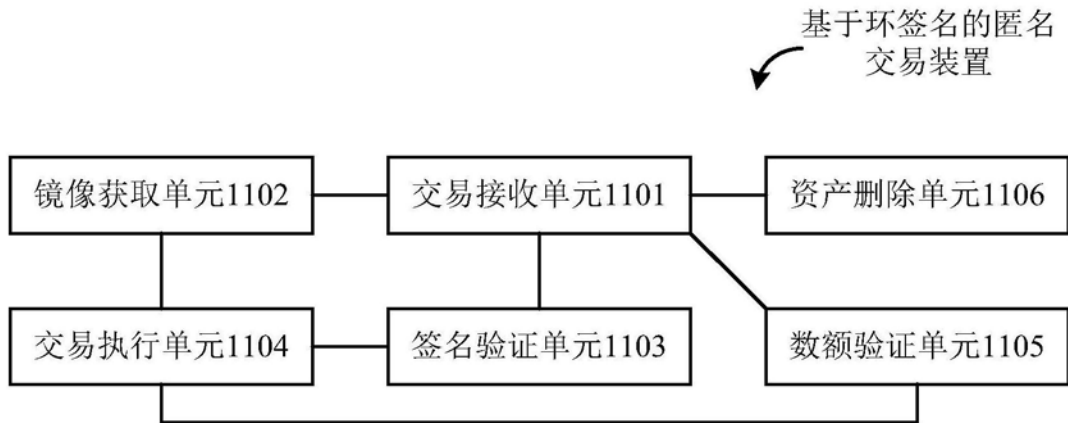


图11