(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 110349021 B
(45)授权公告日 2020.08.25

(21)申请号 201910562997.2
(22)申请日 2019.06.26
(65)同一申请的已公布的文献号
申请公布号 CN 110349021 A
(43)申请公布日 2019.10.18
(73)专利权人 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 40/04(2012.01)

审查员 梁静静

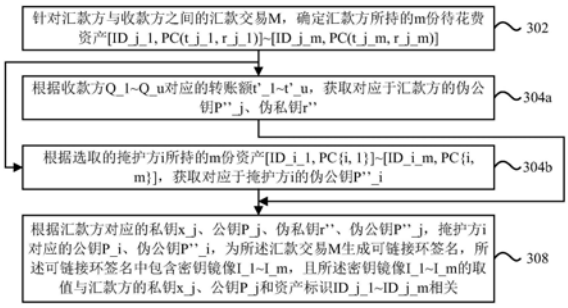
权利要求书5页 说明书21页 附图6页

(54)发明名称

区块链中实现机密交易的方法及装置

(57)摘要

本说明书一个或多个实施例提供一种区块链中实现机密交易的方法及装置，该方法可以包括：针对汇款交易M，确定汇款方所持的m份待花费资产；根据收款方Q_1～Q_u对应的转账额，获取对应于汇款方的伪公钥、伪私钥；根据选取的掩护方i所持的m份资产，获取对应于掩护方i的伪公钥；根据汇款方对应的私钥、公钥、伪私钥、伪公钥，掩护方i对应的公钥、伪公钥，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～I_m，且所述密钥镜像I_1～I_m的取值与汇款方的私钥、公钥和资产标识相关。



CN 110349021 B

1.一种区块链中实现机密交易的方法,包括:

针对汇款方与收款方之间的汇款交易M,确定汇款方所持的m份待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)];其中,ID_j_1～ID_j_m为资产标识、t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺;

根据收款方Q_1～Q_u对应的转账额t'_1～t'_u,获取对应于汇款方的伪公钥P"_j=[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]、对应于汇款方的伪私钥r"=(r_j_1+...+r_j_m)-(r'_1+...+r'_u);其中,PC(t'_1,r'_1)～PC(t'_u,r'_u)为转账额承诺、r'_1～r'_u为随机数,u≥1;

根据选取的掩护方i所持的m份资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}],获取对应于掩护方i的伪公钥P"_i=[PC{i,1}+…+PC{i,m}]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)],i、j∈[1,n],i、j和n为正整数,i≠j,n≥2;

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,所述可链接环签名中包含密钥镜像I_1～I_m,且所述密钥镜像I_1～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～ID_j_m相关。

2.根据权利要求1所述的方法,还包括:

生成转账额t'_1～t'_u对应的范围证明RP_1～RP_u,以添加至所述汇款交易M中;其中,所述范围证明RP_1～RP_u用于证明t'_1≥0～t'_u≥0。

3.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～I_m:

I_d=x_j×Hash_G(P_j,ID_j_d),d∈[1,m];

其中,Hash_G()为椭圆曲线到其自身的哈希函数。

4.根据权利要求1所述的方法,还包括:

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"×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)。

5.根据权利要求1所述的方法,

所述待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]、所述资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{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,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_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,PC{i,1}]～[ID_i_m,PC{i,m}]被从掩护方i对应的账户余额中划分而生成。

6.根据权利要求1所述的方法,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,包括:

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∈[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;

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。

7.根据权利要求6所述的方法,

P_j=x_j×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_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×G、R_j_d=a_d×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_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)×G、R_j_(m+1)=a_(m+1)×Hash_G(P”_j);

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×G+c_i×P_i)mod p、R_i_d=(s_i_d×Hash_G(P_i,ID_i_d)+c_i×I_d)mod p、L_i_(m+1)=[s_i_(m+1)×G+c_i×P”_i]mod p、R_i_(m+1)=[s_i_(m+1)×Hash_G(P”_i)+c_i×I_(m+1)]mod p,I_d=x_j×Hash_G(P_j,ID_j_d)、I_(m+1)=r”×Hash_G(P”_j);其中,s_i_1～s_i_(m+1)为数域Z_q中的随机数,当i=1时c_1=Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))、当i∈[2,j-1]∪[j+1,n]时c_i=Hash(M,L_(i-1)_1,R_(i-1)_1,……,L_(i-1)_(m+1),R_(i-1)_(m+1)),Hash()为从所述椭圆曲线到数域Z_q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_i_1～s_i_(m+1)和衍生数值s_j_1～s_j_(m+1),c_1被选取为衍生数值;其中,s_j_d=(a_d-c_j×x_j)mod p、s_j_(m+1)=[a_(m+1)-c_j×r”]mod p,当j的取值被确定为1时c_j=Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))、当j的取值被确定为属于[2,n]时c_j=Hash(M,L_(j-1)_1,R_(j-1)_1,……,L_(j-1)_(m+1),R_(j-1)_(m+1))。

8.一种区块链中实现机密交易的方法,包括:

获取汇款交易M的可链接环签名包含的密钥镜像I_1～I_m,所述密钥镜像I_1～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～ID_j_m相关;其中,资产标识ID_j_1～ID_j_m对应于汇款方持有的资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)],t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺;

验证所述可链接环签名,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;当所述可链接环签名通过验证时,资产额t_j_1～t_j_m之和被确定为与收款方Q_1～Q_u对应的转账额t’_1～t’_u之和相等;其中,P”_j=[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]、r”=(r_j_1+...+r_j_m)-(r’_1+...+r’_u),掩护方i持有资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]、P”_i=[PC{i,1}+…+PC{i,m}]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)],PC(t’_1,r’_1)～PC(t’_u,r’_u)为转账额承诺、r’_1～r’_u为随机数,u≥1,i、j∈[1,n],i、j和n为正整数,i≠j,n≥2;

当满足交易执行条件时,执行所述汇款交易M;其中,所述交易执行条件包括:所述密钥镜像I_1～I_m不同于历史密钥镜像、所述可链接环签名通过验证。

9.根据权利要求8所述的方法,还包括:

根据汇款交易M所含的范围证明RP_1～RP_u,验证转账额t'_1～t'_u是否满足t'_1≥0～t'_u≥0;

其中,所述交易执行条件还包括:满足t'_1≥0～t'_u≥0。

10.根据权利要求8所述的方法,所述密钥镜像I_1～I_m由汇款方通过下述公式计算得到:

I_d=x_j×Hash_G(P_j,ID_j_d),d∈[1,m]。

11.根据权利要求8所述的方法,所述可链接环签名还包括密钥镜像I_(m+1)=r"×Hash_G(P"_j);

其中,所述交易执行条件还包括:密钥镜像I_(m+1)不同于历史密钥镜像。

12.根据权利要求8所述的方法,

所述待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]、所述资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{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,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_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,PC{i,1}]～[ID_i_m,PC{i,m}]被从掩护方i对应的账户余额中划分而生成。

13.根据权利要求8所述的方法,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∈[1,n]、d∈[1,m]。

14.根据权利要求8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∈[1,m];验证所述可链接环签名,包括:

根据所述可链接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。

15.根据权利要求14所述的方法,

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

所述可链接环签名所含的随机数和/或其衍生数值包括:s_k_1～s_k_(m+1)、c_1,k∈[1,n];其中,c_1被选取为衍生数值;

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×G+c_k×P_k)mod 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;

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)×G+c_k×P"_k]mod 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×Hash_G(P_k,ID_k_d)+c_k×I_d)mod p,I_d被包含于所述可链接环签名中;

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)×Hash_G(P"_k)+c_k×I_(m+1)]mod p,I_(m+1)被包含于所述可链接环签名中;

其中,当h＝1时c_1＝Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))、当h∈[2,n]时c_k＝Hash(M,L_(h-1)_1,R_(h-1)_1,……,L_(h-1)_(m+1),R_(h-1)_(m+1))。

16.一种区块链中实现机密交易的装置,包括:

资产确定单元,针对汇款方与收款方之间的汇款交易M,确定汇款方所持的m份待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)];其中,ID_j_1～ID_j_m为资产标识、t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺;

第一获取单元,根据收款方Q_1～Q_u对应的转账额t'_1～t'_u,获取对应于汇款方的伪公钥P"_j＝[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]、对应于汇款方的伪私钥r"＝(r_j_1+...+r_j_m)-(r'_1+...+r'_u);其中,PC(t'_1,r'_1)～PC(t'_u,r'_u)为转账额承诺、r'_1～r'_u为随机数,u≥1;

第二获取单元,根据选取的掩护方i所持的m份资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}],获取对应于掩护方i的伪公钥P"_i＝[PC{i,1}+…+PC{i,m}]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)],i、j∈[1,n],i、j和n为正整数,i≠j,n≥2;

签名单元,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,所述可链接环签名中包含密钥镜像I_1～I_m,且所述密钥镜像I_1～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～ID_j_m相关。

17.一种区块链中实现机密交易的装置,包括:

镜像获取单元,获取汇款交易M的可链接环签名包含的密钥镜像I_1～I_m,所述密钥镜像I_1～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～ID_j_m相关;其中,资产标识ID_j_1～ID_j_m对应于汇款方持有的资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)],t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺;

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;当所述可链接环签名通过验证时,资产额t_j_1～t_j_m之和被确定为与收款方Q_1～Q_u对应的转账额t'_1～t'_u之和相等;其中,P"_j＝[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]、r"＝(r_j_1+...+r_j_m)-(r'_1+...+r'_u),掩护方i持有资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]、P"_i＝[PC{i,1}+…+PC{i,m}]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)],PC(t'_1,r'_1)～PC(t'_u,r'_u)为转账额承诺、r'_1～r'_u为随机数,u≥1,i、j∈[1,n],i、j和n为正整数,i≠j,n≥2;

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;其中,所述交易执行条件包括:所述密钥镜像I_1～I_m不同于历史密钥镜像、所述可链接环签名通过验证。

18.一种电子设备,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1-7中任一项所述的方法。

19.一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1-7中任一项所述方法的步骤。

20.一种电子设备，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8-15中任一项所述的方法。

21.一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8-15中任一项所述方法的步骤。

区块链中实现机密交易的方法及装置

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，尤其涉及一种区块链中实现机密交易的方法及装置。

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区块链中实现机密交易的方法及装置。

[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，提出了一种区块链中实现机密交易的方法，包括：

[0006] 针对汇款方与收款方之间的汇款交易M，确定汇款方所持的m份待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]；其中，ID_j_1～ID_j_m为资产标识、t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺；

[0007] 根据收款方Q_1～Q_u对应的转账额t’_1～t’_u，获取对应于汇款方的伪公钥P”_j＝[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]、对应于汇款方的伪私钥r”＝(r_j_1+...+r_j_m)-(r’_1+...+r’_u)；其中，PC(t’_1,r’_1)～PC(t’_u,r’_u)为转账额承诺、r’_1～r’_u为随机数；

[0008] 根据选取的掩护方i所持的m份资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]，获取对应于掩护方i的伪公钥P”_i＝[PC{i,1}+…+PC{i,m}]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]，i∈[1,j-1]∪[j+1,n]；

[0009] 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，所述可链接环签名中包含密钥镜像I_1～I_m，且所述密钥镜像I_1～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～ID_j_m相关。

[0010] 根据本说明书一个或多个实施例的第二方面，提出了一种区块链中实现机密交易的方法，包括：

[0011] 获取汇款交易M的可链接环签名包含的密钥镜像I_1～I_m，所述密钥镜像I_1～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～ID_j_m相关；其中，资产标识ID_j_1～ID_j_m对应于汇款方持有的资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]，t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,

r_j_m)为资产承诺;

[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;当所述可链接环签名通过验证时,资产额t_j_1～t_j_m之和被确定为与收款方Q_1～Q_u对应的转账额t’_1～t’_u之和相等;其中,P”_j=[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]、r”=(r_j_1+...+r_j_m)-(r’_1+...+r’_u),掩护方i持有资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]、P”_i=[PC(i,1)+…+PC(i,m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)],PC(t’_1,r’_1)～PC(t’_u,r’_u)为转账额承诺、r’_1～r’_u为随机数,i∈[1,j-1]∪[j+1,n];

[0013] 当满足交易执行条件时,执行所述汇款交易M;其中,所述交易执行条件包括:所述密钥镜像I_1～I_m不同于历史密钥镜像、所述可链接环签名通过验证。

[0014] 根据本说明书一个或多个实施例的第三方面,提出了一种区块链中实现机密交易的装置,包括:

[0015] 资产确定单元,针对汇款方与收款方之间的汇款交易M,确定汇款方所持的m份待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)];其中,ID_j_1～ID_j_m为资产标识、t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺;

[0016] 第一获取单元,根据收款方Q_1～Q_u对应的转账额t’_1～t’_u,获取对应于汇款方的伪公钥P”_j=[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]、对应于汇款方的伪私钥r”=(r_j_1+...+r_j_m)-(r’_1+...+r’_u);其中,PC(t’_1,r’_1)～PC(t’_u,r’_u)为转账额承诺、r’_1～r’_u为随机数;

[0017] 第二获取单元,根据选取的掩护方i所持的m份资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}],获取对应于掩护方i的伪公钥P”_i=[PC{i,1}+…+PC{i,m}]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)],i∈[1,j-1]∪[j+1,n];

[0018] 签名单元,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,所述可链接环签名中包含密钥镜像I_1～I_m,且所述密钥镜像I_1～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～ID_j_m相关。

[0019] 根据本说明书一个或多个实施例的第四方面,提出了一种区块链中实现机密交易的装置,包括:

[0020] 镜像获取单元,获取汇款交易M的可链接环签名包含的密钥镜像I_1～I_m,所述密钥镜像I_1～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～ID_j_m相关;其中,资产标识ID_j_1～ID_j_m对应于汇款方持有的资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)],t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺;

[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;当所述可链接环签名通过验证时,资产额t_j_1～t_j_m之和被确定为与收款方Q_1～Q_u对应的转账额t’_1～t’_u之和相等;其中,P”_j=[PC(t_j_1,r_j_1)+…+PC(t_

j_m,r_j_m)]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]、r"＝(r_j_1+...+r_j_m)-(r'_1+...+r'_u)，掩护方i持有资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]、P"_i＝[PC(i,1)+…+PC(i,m)]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]，PC(t'_1,r'_1)～PC(t'_u,r'_u)为转账额承诺、r'_1～r'_u为随机数，i∈[1,j-1]∪[j+1,n]；

[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；其中，所述交易执行条件包括：所述密钥镜像I_1～I_m不同于历史密钥镜像、所述可链接环签名通过验证。

[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区块链中实现机密交易的方法的流程图。

[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区块链中实现机密交易的方法的流程图。

[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区块链中实现机密交易的装置的框图。

[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区块链中实现机密交易的装置的框图。

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描述的实施方式并不代表与本说明书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、本说明书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合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，以获知某一用户持有的资产、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] 处于隐私保护的目的，相关技术中提出了基于承诺的机密交易(Confidential Transaction)方案，可以将每个用户持有的资产额、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×G+t×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的取值仅由资产持有者、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(t1,r1)-PC(t2,r2)＝PC(t1-t2,r1-r2)。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,……,P_n)中，其中公钥P_1～P_j-1、P_j+1～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,……,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,……,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,……,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,……,P_n)的形式时，虽然看似是从P_1开始、P_n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_j、公钥P_j时，可以按照公式I＝x_j×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区块链中实现机密交易的方法的流程图。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，针对汇款方与收款方之间的汇款交易M，确定汇款方所持的m份待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]。

[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_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]为例，ID_j_1～ID_j_m为资产标识、t_j_1～t_j_m为资产额，区块链账本上记录为资产额t_j_1～t_j_m对应的资产承诺PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)，r_j_1～r_j_m为随机数。由于随机数r_j_1～r_j_m的存在，使得数额t_j_1～t_j_m生成的资产承诺PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)具有随机性，除了掌握随机数r_j_1～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)～PC(t_j_m,r_j_m)，且无法据此反推出相应的资产额t_j_1～t_j_m。

[0071] 虽然此处以[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]的形式对相应的资产进行了列举，但在区块链账本上并不一定采用[标识，资产承诺]的形式进行记录和存储，比如可以采用其他形式或进一步包含其他信息等，本说明书并不对此进行限制。

[0072] 当采用相关技术中的UTXO模型时，诸如上述的汇款方或下述的收款方、掩护方等，每一用户均可以存在一组公私钥对，这组公私钥对唯一对应于相应的用户。同时，虽然并未针对每一用户建立账户、没有基于账户对用户持有的资产进行管理，而是对所有资产进行统一管理，但是通过在公私钥对与资产之间建立关联关系，相当于可以通过公私钥对有效管理用户持有的资产，其效果相当于针对每一用户建立了账户并基于账户对用户持有的资产进行管理，并且用户此时仅需维护一组公私钥对，而不同资产之间则通过资产标识予以区分，无需针对每一资产分别维护一组公私钥对。

[0073] 当然，本说明书也可以采用“账户”形式实现资产管理。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。同时，基于账户A_j的存在，使得汇款方只需要维护对应于该账户A_j的一组公私钥对，比如私钥x_j、公钥P_j，即可针对该账户A_j下的所有资产进行统一管理，而无需为每一资产分别维护一组公私钥对、区别于门罗币采用的技术方案，可以极大地降低汇款方和其他用户对于

公私钥对的维护成本。

[0074] 当采用UTXO模型时，每一资产为相应的历史交易的交易输出。而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,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_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，再比如资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{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,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]被从汇款方对应的账户余额中划分而生成、资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{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] 在汇款方所持有的所有资产中，待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]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。

[0076] 步骤304a，根据收款方Q_1～Q_u对应的转账额t’_1～t’_u，获取对应于汇款方的伪公钥P”_j、伪私钥r”。

[0077] 前述的汇款额为汇款方需要向各个收款对象汇款的数额，这些数额由汇款方与各个收款对象预先协商确定，也可以由汇款方自行确定。其中，收款对象与上述的收款方Q_1～Q_u之间存在一定的对应关系。其中u≥1，表明可以存在一个或多个收款方。

[0078] 在一些情况下，资产额t_j_1～t_j_m之和与汇款对象对应的转账额之和恰好相等，此时收款对象与收款方Q_1～Q_u等同，即收款方Q_1～Q_u均为收款对象，汇款对象对应的转账额即为上述的转账额t’_1～t’_u。在另一些情况下，资产额t_j_1～t_j_m之和并不恰好等于汇款对象对应的转账额之和，而是资产额t_j_1～t_j_m之和大于汇款对象对应的转账额之和，此时将差额(数额t_j_1～t_j_m之和减去汇款对象对应的转账额之和)作为汇款方的找零额，并将汇款方添加为某一个收款方，从而由u-1个汇款对象和汇款方自身组成收款方Q_1～Q_u。可见，无论是否存在找零额，都需要确保t_j_1+…+t_j_m＝t’_1+…+t’_u，使得汇款交易M的汇入额与汇出额相等。

[0079] 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)～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，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×G+r’_w×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等。

[0080] 根据待花费资产对应的资产承诺PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)、转账额承诺PC(t’_1,r’_1)～PC(t’_u,r’_u)，可以计算得到P”_j＝[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]；以及，根据待花费资产对应的随机数r_

j_1～r_j_m、转账额对应的随机数r'_1～r'_u，可以计算得到r"＝(r_j_1+...+r_j_m)-(r'_1+...+r'_u)；以及，根据待花费资产对应的资产额t_j_1～t_j_m、转账额t'_1～t'_u，可以计算得到t"＝(t_j_1+…+t_j_m)-(t'_1+…+t'_u)。那么，如前所述的同态特性，可以确定P"_j＝PC(r",t")＝r"×G+t"×H。又由于汇款方可以确保t_j_1+…+t_j_m＝t'_1+…+t'_u，使得t"＝0，因而可以确定P"_j＝r"×G。

[0081] 如前所述，汇款方只需要维护一组公私钥对。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为一个大素数(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×G。对于掩护方、收款方等其他用户而言，均通过类似的方式确定出各自唯一对应的公私钥对。

[0082] 那么，从形式上可以看出上述的"P"_j＝r"×G"与公私钥对之间的关系"P_j＝x_j×G"相似，并且如下文所述，掩护方i必然满足P"_i≠r"×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。

[0083] 步骤304b，根据选取的掩护方i所持的m份资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]，获取对应于掩护方i的伪公钥P"_i。

[0084] 与上文相类似的，可以计算得到掩护方i对应的参数P"_i＝[PC{i,1}+…+PC{i,m}]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]，i∈[1,j-1]∪[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～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～t'_u对应的随机数r'_1～r'_u之和的差值r"_i。因此，基于同态特性可以确定P"_i＝r"_i×G+t"_i×H≠r"×G。

[0085] 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。

[0086] 步骤306，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，所述可链接环签名中包含密钥镜像I_1～I_m，且所述密钥镜像I_1～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～ID_j_m相关。

[0087] 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"×G、伪公钥P"_i与伪私钥r"之间满足P"_i≠r"×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,……,P"_n)中存在某一伪公钥的取值等于r"×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,……,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。

[0088] 密钥镜像I_1～I_m与汇款方提供的待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_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～I_m的取值与相应资产的资产标识ID_j_1～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～ID_j_m之间的取值差异，确保生成的密钥镜像I_1～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，使得每一用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×Hash_G(P_j,ID_j_d)，d∈[1,m]；其中，Hash_G()为上述椭圆曲线到其自身的哈希函数。

[0089] 除了上述的密钥镜像I_1～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”×Hash_G(P”_j)，从而与密钥镜像I_1～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] 在机密交易中，除了交易的汇入额与汇出额相等之外，还需要一些其他的证明信息，比如证明汇款交易M中的转账额t’_1～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～t’_u分别生成相应的范围证明RP_1～RP_u，以用于证明t’_1≥0～t’_u≥0，并将这些范围证明RP_1～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。

[0091] 因此，汇款方生成的汇款交易M可以包括下述交易内容：

[0092] 1)汇款方、掩护方i及其资产：{[P_1:ID_1_1,…,ID_1_m],[P_2:ID_2_1,…,ID_2_m],…,[P_n:ID_n_1,…,ID_n_m]}，其中P_1～P_n分别为相应汇款对象(汇款方或掩护方)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。

[0093] 2)收款方及其转账额：{[Q_1,PC(t’_1,r’_1)],[Q_2,PC(t’_2,r’_2)],…,[Q_u,PC(t’_u,r’_u)]}。

[0094] 3)范围证明RP_1～RP_u。

[0095] 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。

[0096] 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。

[0097] 下面结合图5对可链接环签名的生成过程进行描述；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：

[0098] 步骤502，生成密钥镜像I_1～I_(m+1)。

[0099] 生成密钥镜像I_1～I_(m+1)的过程可以参考前述内容，此处不再赘述。

[0100] 其中，I_d＝x_j×Hash_G(P_j,ID_j_d)，d∈[1,m]；I_(m+1)＝r”×Hash_G(P”_j)。

[0101] 步骤504a,计算中间参数L_j_d、R_j_d。

[0102] 汇款方可以从数域Z_q中选取随机数a_d(即a_1～a_m),并按照下述公式计算中间参数L_j_d、R_j_d:

[0103] L_j_d＝a_d×G

[0104] R_j_d＝a_d×Hash_G(P_j,ID_j_d)

[0105] 因此,汇款方可以计算得到L_j_d:L_j_1～L_j_m,以及R_j_d:R_j_1～R_j_m。

[0106] 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。

[0107] 步骤504b,计算中间参数L_j_(m+1)、R_j_(m+1)。

[0108] 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):

[0109] L_j_(m+1)＝a_(m+1)×G

[0110] R_j_(m+1)＝a_(m+1)×Hash_G(P”_j)

[0111] 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。

[0112] 步骤506,计算中间参数L_(j+1)_d～L_n_d、R_(j+1)_d～R_n_d、L_(j+1)_(m+1)～L_n_(m+1)、R_(j+1)_(m+1)～R_n_(m+1)。

[0113] 当i＝j+1～n时,中间参数L_i_d、R_i_d的计算过程符合下述公式:

[0114] L_i_d＝(s_i_d×G+c_i×P_i)mod p

[0115] R_i_d＝[s_i_d×Hash_G(P_i,ID_i_d)+c_i×I_d]mod p

[0116] 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:

[0117] L_i_(m+1)＝[s_i_(m+1)×G+c_i×P”_i]mod p

[0118] R_i_(m+1)＝[s_i_(m+1)×Hash_G(P”_i)+c_i×I_(m+1)]mod p

[0119] 在计算过程中,涉及到s_(j+1)_d～s_n_d、s_(j+1)_(m+1)～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)～c_n,其计算过程符合下述公式:c_i＝Hash[M,L_(i-1)_1,R_(i-1)_1,……,L_(i-1)_(m+1),R_(i-1)_(m+1)],其中Hash()为从上述椭圆曲线到数据Z_q上的哈希函数。

[0120] 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∈[j+1,n]时的中间参数L_i_d、R_i_d,即上述的L_(j+1)_d～L_n_d、R_(j+1)_d～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)＝Hash[M,L_j_1,R_j_1,……,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。

[0121] 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)_(m+1)～L_n_(m+1)、R_(j+1)_(m+1)～R_n_(m+1),此处不再一一赘述。

[0122] 步骤508,计算中间参数L_1_d、R_1_d、L_1_(m+1)、R_1_(m+1)。

[0123] 中间参数L_1_d、R_1_d的计算过程符合下述公式:

[0124] L_1_d＝(s_1_d×G+c_1×P_1)mod p

[0125] R_1_d＝(s_1_d×Hash_G(P_1,ID_1_d)+c_1×I_d)mod p

[0126] 而中间参数L_1_(m+1)、R_1_(m+1)的计算过程符合下述公式:

[0127] L_1_(m+1)＝[s_1_(m+1)×G+c_1×P”_1]mod p

[0128] R_1_(m+1)＝[s_1_(m+1)×Hash_G(P_1)+c_1×I_(m+1)]mod p

[0129] 其中,s_1_d和s_1_(m+1)均为数域Z_q中的随机数、c_1＝Hash[M,L_n_1,R_n_1,……,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～L_n_d、R_1_d～R_n_d、L_1_(m+1)～L_n_(m+1)、R_1_(m+1)～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＝Hash[M,L_n_1,R_n_1,……,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＝Hash[M,L_(i-1)_1,R_(i-1)_1,……,L_(i-1)_(m+1),R_(i-1)_(m+1)],即c_1与c_(j+1)～c_n的计算公式一致。

[0130] 步骤510,计算中间参数L_2_d～L_(j-1)_d、R_2_d～R_(j-1)_d、L_2_(m+1)～L_(j-1)_(m+1)、R_2_(m+1)～R_(j-1)_(m+1)。

[0131] 当i＝2～j-1时,中间参数L_i_d、R_i_d的计算过程符合下述公式:

[0132] L_i_d＝(s_i_d×G+c_i×P_i)mod p

[0133] R_i_d＝(s_i_d×Hash_G(P_i,ID_i_d)+c_i×I_d)mod p

[0134] 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:

[0135] L_i_(m+1)＝[s_i_(m+1)×G+c_i×P”_i]mod p

[0136] R_i_(m+1)＝[s_i_(m+1)×Hash_G(P”_i)+c_i×I_(m+1)]mod p

[0137] 在计算过程中,涉及到s_2_d～s_(j-1)_d、s_2_(m+1)～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～c_(j-1),其计算过程符合下述公式:c_i＝Hash(M,L_(i-1)_1,R_(i-1)_1,……,L_(i-1)_(m+1),R_(i-1)_(m+1))。

[0138] 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∈[2,j-1]时的中间参数L_i_d、R_i_d,即上述的L_2_d～L_(j-1)_d、R_2_d～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。

[0139] 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_2_(m+1)～L_(j-1)_(m+1)、R_2_(m+1)～R_(j-

1)_(m+1)，此处不再一一赘述。

[0140] 步骤512，生成环签名。

[0141] 基于上述步骤的处理过程，可以得到密钥镜像I_1，……，I_(m+1)、c_1、s_1_d～s_(j-1)_d、s_(j+1)_d～s_n_d、s_1_(m+1)～s_(j-1)_(m+1)、s_(j+1)_(m+1)～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：

[0142] s_j_d＝(a_d-c_j×x_j)mod p

[0143] s_j_(m+1)＝(a_(m+1)-c_j×r")mod p

[0144] $$c\_j=\begin{cases} Hash\left[M,L\_n\_1,R\_n\_1,\cdots\cdots,L\_n\_(m+1),R\_n\_(m+1)\right], j=1 \\ Hash\left[M,L\_(j-1)\_1,R\_(j-1)\_1,\cdots\cdots,L\_(j-1)\_(m+1),\right. \\ \left.R\_(j-1)\_(m+1)\right], j\in[2,n] \end{cases}$$

[0145] 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～j-1和j+1～n，参数e存在m个取值，分别为1～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～L_n_d、R_1_d～R_n_d、L_1_(m+1)～L_n_(m+1)、R_1_(m+1)～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＝Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))时，实质上也符合c_j＝Hash(M,L_(j-1)_1,R_(j-1)_1,……,L_(j-1)_(m+1),R_(j-1)_(m+1))。

[0146] 因此，汇款方可以生成环签名[I_1,…,I_(m+1),c_1,s_1_1,…,s_1_(m+1),…,s_n_1,…,s_n_(m+1)]，其中包含密钥镜像I_1～I_(m+1)、随机数s_i_1～s_i_(m+1)、衍生数值s_j_1～s_j_(m+1)和c_1。

[0147] 图6是一示例性实施例提供的另一种区块链中实现机密交易的方法的流程图。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：

[0148] 步骤602，获取汇款交易M的可链接环签名包含的密钥镜像I_1～I_m，所述密钥镜像I_1～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～ID_j_m相关。

[0149] 资产标识ID_j_1～ID_j_m对应于汇款方持有的资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]，t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺。当然，区块链节点上仅维护资产对应的资产标识和资产承诺，而并不会直接维护明文的资产额和随机数。只有汇款方自身才会掌握其所持资产的资产额和随机数，其他用户则无法获知，从而实现对资产信息的隐藏。

[0150] 如前所述，汇款方仅维护一组公私钥对，即私钥x_j和公钥P_j，但是通过引入资产标识ID_j_1～ID_j_m，可以确保生成的密钥镜像I_1～I_m之间互不相同，并且与相应的资产之间一一对应，可以通过密钥镜像检查相应资产是否存在“双花”问题。例如，I_d＝x_j×Hash_G(P_j,ID_j_d)，d∈[1,m]。相应地，区块链节点可以保存所有已花费交易所含的密钥镜像，即历史密钥镜像。同时，区块链节点可以将上述的密钥镜像I_1～I_m与历史密钥镜像

进行比较:如果存在相同的历史密钥镜像,就表明相应的资产已经被花费,存在“双花”问题;如果不存在相同的历史密钥镜像,就表明相应的资产未被花费。

[0151] 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”×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。

[0152] 步骤604,验证所述可链接环签名,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;当所述可链接环签名通过验证时,资产额t_j_1～t_j_m之和被确定为与收款方Q_1～Q_u对应的转账额t’_1～t’_u之和相等。

[0153] 汇款方对应的伪公钥P”_j=[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]、伪私钥r”=(r_j_1+...+r_j_m)-(r’_1+...+r’_u)。同时,根据掩护方i持有资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}],汇款方可以计算出掩护方i对应的伪公钥P”_i=[PC{i,1}+…+PC{i,m}]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)],i∈[1,j-1]∪[j+1,n]。其中,PC(t’_1,r’_1)～PC(t’_u,r’_u)为转账额承诺、r’_1～r’_u为随机数。

[0154] 对于可链接环签名的生成过程,可以参考图3、图5等所示的实施例,此处不再赘述。

[0155] 如前所述,通过验证可链接环签名,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”×G、伪公钥P”_i与伪私钥r”之间满足P”_i≠r”×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,……,P”_n)中存在某一伪公钥的取值等于r”×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,……,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。

[0156] 步骤606,当满足交易执行条件时,执行所述汇款交易M;其中,所述交易执行条件包括:所述密钥镜像I_1～I_m不同于历史密钥镜像、所述可链接环签名通过验证。

[0157] 如前所述,可链接环签名中还可能包含密钥镜像I_(m+1);相应的,交易执行条件还可以包括:密钥镜像I_(m+1)不同于历史密钥镜像。

[0158] 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∈[1,n]、d∈[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。

[0159] 在机密交易中,除了交易的汇入额与汇出额相等之外,还需要一些其他的证明信息,比如证明汇款交易M中的转账额t’_1～t’_u都不小于0。而转账额承诺PC(t’_1,r’_1)～PC(t’_u,r’_u)是汇款方根据转账额t’_1～t’_u、随机数r’_1～r’_u而生成,且转账额t’_1～t’_u和随机数r’_1～r’_u只有汇款方和收款方Q_1～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～RP_u实施验证操作，以确定转账额t'_1～t'_u是否满足t'_1≥0～t'_u≥0。那么，交易执行条件还可以包括：所有转账额均不小于0。

[0160] 下面结合图7对可链接环签名的验证过程进行描述；其中，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：

[0161] 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∈[1,n]、d∈[1,m]。

[0162] 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。

[0163] 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_k_d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_k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。

[0164] 步骤704，根据s_k_1～s_k_(m+1)依次计算L_k_1～L_k_(m+1)、R_k_1～R_k_(m+1)。

[0165] 步骤706，根据L_n_1～L_n_(m+1)、R_n_1～R_n_(m+1)计算c_1'，验证c_1'是否等于c_1。

[0166] 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_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R_j_d与R_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_(m+1)与R_i_(m+1)之间是否符合环形取值规则。

[0167] 例如，当环签名所含的随机数和/或其衍生数值包括：s_1_1～s_1_(m+1)，…，s_n_1～s_n_(m+1)、c_1时，中间参数L_j_d与L_i_d之间的环形取值规则可以包括：

[0168] L_k_d＝(s_k_d×G+c_k×P_k)mod p，h∈[1,n]

[0169] $$c\_k=\begin{cases} Hash\left[M,L\_n\_1,R\_n\_1,\cdots\cdots,L\_n\_(m+1),R\_n\_(m+1)\right],k=1 \\ Hash\left[M,L\_(j-1)\_1,R\_(j-1)\_1,\cdots\cdots,L\_(j-1)\_(m+1),\right. \\ \left.R\_(j-1)\_(m+1)\right],k\in[2,n] \end{cases}$$

[0170] 中间参数L_j_(m+1)与L_i_(m+1)之间的环形取值规则包括：

[0171] L_k_(m+1)＝[s_k_(m+1)×G+c_k×P"_k]mod p

[0172] 中间参数R_j_d与R_i_d之间的环形取值规则包括：

[0173] R_k_d＝[s_k_d×Hash_G(P_k,ID_k_d)+c_k×I_d]mod p

[0174] 中间参数R_j_(m+1)与R_i_(m+1)之间的环形取值规则包括：

[0175] R_k_(m+1)＝[s_k_(m+1)×Hash_G(P”_k)+c_k×I_(m+1)]mod p

[0176] 那么，验证方可以首先根据s_1_d、c_1、G、P_1和p生成L_1_d，即L_1_1～L_1_m，以及根据s_1_d、c_1、P_1、ID_1_d、I_d和p生成R_1_d，即R_1_1～R_1_m；以及，验证方根据s_1_(m+1)、c_1、G、P”_1和p生成L_1_(m+1)，根据s_1_(m+1)、c_1、P”_1、I_(m+1)和p生成R_1_(m+1)。

[0177] 然后，验证方可以根据M、L_1_d、R_1_d、L_1_(m+1)和R_1_(m+1)生成c_2，并根据s_2_d、c_2、G、P_2和p生成L_2_d，根据s_2_d、c_2、P_2、ID_2_d、I_d和p生成R_2_d，根据s_2_(m+1)、c_2、G、P”_2和p生成L_2_(m+1)，以及根据s_2_(m+1)、c_2、P”_2、I_(m+1)和p生成R_2_(m+1)；以此类推，直至验证方根据M、L_(n-1)_d、R_(n-1)_d、L_(n-1)_(m+1)和R_(n-1)_(m+1)生成c_n，并根据s_n_d、c_n、G、P_n和p生成L_n_d，根据s_n_d、c_n、P_n、ID_n_d、I_d和p生成R_n_d，根据s_n_(m+1)、c_n、G、P”_n和p生成L_n_(m+1)，以及根据s_n_(m+1)、c_n、P”_n、I_(m+1)和p生成R_n_(m+1)。

[0178] 进一步地，验证方可以按照上述针对c_k的计算公式，计算得到c_1’＝Hash[M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1)]。之所以此处采用c_1’，是为了区分于环签名所含的c_1，那么验证方可以将该c_1’与环签名所含的c_1进行比较：如果c_1’与c_1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～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～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。

[0179] 步骤708，验证范围证明RP_1～RP_u。

[0180] 验证方从汇款交易M的交易内容中获取范围证明RP_1～RP_u并验证，以确定相应的转账额t’_1～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。

[0181] 步骤710，验证密钥镜像I_1～I_(m+1)是否已存在。

[0182] 在一实施例中，验证方可以将密钥镜像I_1～I_(m+1)与历史密钥镜像进行比较，从而确定密钥镜像I_1～I_(m+1)是否已存在。如果密钥镜像I_1～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～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。

[0183] 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，在逻辑层面上形成区块链中实现机密交易的装置。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。

[0184] 请参考图9，在软件实施方式中，该区块链中实现机密交易的装置可以包括：

[0185] 资产确定单元91，针对汇款方与收款方之间的汇款交易M，确定汇款方所持的m份待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]；其中，ID_j_1～ID_

j_m为资产标识、t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺；

[0186] 第一获取单元92，根据收款方Q_1～Q_u对应的转账额t'_1～t'_u，获取对应于汇款方的伪公钥P"_j＝[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]、对应于汇款方的伪私钥r"＝(r_j_1+...+r_j_m)-(r'_1+...+r'_u)；其中，PC(t'_1,r'_1)～PC(t'_u,r'_u)为转账额承诺、r'_1～r'_u为随机数，u≥1；

[0187] 第二获取单元93，根据选取的掩护方i所持的m份资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]，获取对应于掩护方i的伪公钥P"_i＝[PC{i,1}+…+PC{i,m}]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)]，i∈[1,j-1]∪[j+1,n]；

[0188] 签名单元94，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，所述可链接环签名中包含密钥镜像I_1～I_m，且所述密钥镜像I_1～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～ID_j_m相关。

[0189] 可选的，还包括：

[0190] 证明生成单元95，生成转账额t'_1～t'_u对应的范围证明RP_1～RP_u，以添加至所述汇款交易M中；其中，所述范围证明RP_1～RP_u用于证明t'_1≥0～t'_u≥0。

[0191] 可选的，通过下述公式计算所述密钥镜像I_1～I_m：

[0192] I_d＝x_j×Hash_G(P_j,ID_j_d)，d∈[1,m]；

[0193] 其中，Hash_G()为椭圆曲线到其自身的哈希函数。

[0194] 可选的，还包括：

[0195] 镜像生成单元96，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"×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)。

[0196] 可选的，

[0197] 所述待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]、所述资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]为相应的历史交易的交易输出；或，

[0198] 所述待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_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,PC{i,1}]～[ID_i_m,PC{i,m}]被从掩护方i对应的账户余额中划分而生成。

[0199] 可选的，签名单元94具体用于：

[0200] 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∈[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；

[0201] 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。

[0202] 可选的，

[0203] P_j＝x_j×G，G为椭圆曲线的基点，|G|＝p且p为素数，0<x_j<p；

[0204] 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×G、R_j_d＝a_d×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；

[0205] 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)×G、R_j_(m+1)＝a_(m+1)×Hash_G(P”_j)；

[0206] 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×G+c_i×P_i)mod p、R_i_d＝(s_i_d×Hash_G(P_i,ID_i_d)+c_i×I_d)mod p、L_i_(m+1)＝[s_i_(m+1)×G+c_i×P”_i]mod p、R_i_(m+1)＝[s_i_(m+1)×Hash_G(P”_i)+c_i×I_(m+1)]mod p，I_d＝x_j×Hash_G(P_j,ID_j_d)、I_(m+1)＝r”×Hash_G(P”_j)；其中，s_i_1～s_i_(m+1)为数域Z_q中的随机数，当i＝1时c_1＝Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))、当i∈[2,j-1]∪[j+1,n]时c_i＝Hash(M,L_(i-1)_1,R_(i-1)_1,……,L_(i-1)_(m+1),R_(i-1)_(m+1))，Hash()为从所述椭圆曲线到数域Z_q的哈希函数；

[0207] 被选取的随机数和/或其衍生数值包括：随机数s_i_1～s_i_(m+1)、衍生数值c_1、衍生数值s_j_1～s_j_(m+1)；其中，s_j_d＝(a_d-c_j×x_j)mod p、s_j_(m+1)＝[a_(m+1)-c_j×r”]mod p，当j的取值被确定为1时c_j＝Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))、当j的取值被确定为属于[2,n]时c_j＝Hash(M,L_(j-1)_1,R_(j-1)_1,……,L_(j-1)_(m+1),R_(j-1)_(m+1))。

[0208] 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，在逻辑层面上形成区块链中实现机密交易的装置。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。

[0209] 请参考图11，在软件实施方式中，该区块链中实现机密交易的装置可以包括：

[0210] 镜像获取单元1101，获取汇款交易M的可链接环签名包含的密钥镜像I_1～I_m，所述密钥镜像I_1～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～ID_j_m相关；其中，资产标识ID_j_1～ID_j_m对应于汇款方持有的资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]，t_j_1～t_j_m为资产额、r_j_1～r_j_m为随机数、PC(t_j_1,r_j_1)～PC(t_j_m,r_j_m)为资产承诺；

[0211] 签名验证单元1102，验证所述可链接环签名，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；当所述可链接环签名通过验证时，资产额t_j_1～t_j_m之和被确定为与收款方Q_1～Q_u对应的转账额t’_1～t’_u之和相等；其中，P”_j＝[PC(t_j_1,r_j_1)+…+PC(t_j_m,r_j_m)]-[PC(t’_1,r’_1)+…+PC(t’_u,r’_u)]、r”＝(r_j_1+...+r_j_m)-(r’_1+...+r’_u)，掩护方i持有资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]、P”_i＝[PC{i,1}

+…+PC{i,m}]-[PC(t'_1,r'_1)+…+PC(t'_u,r'_u)],PC(t'_1,r'_1)～PC(t'_u,r'_u)为转账额承诺、r'_1～r'_u为随机数,i∈[1,j-1]∪[j+1,n],u≥1;

[0212] 交易执行单元1103,当满足交易执行条件时,执行所述汇款交易M;其中,所述交易执行条件包括:所述密钥镜像I_1～I_m不同于历史密钥镜像、所述可链接环签名通过验证。

[0213] 可选的,还包括:

[0214] 范围验证单元1104,根据汇款交易M所含的范围证明RP_1～RP_u,验证转账额t'_1～t'_u是否满足t'_1≥0～t'_u≥0;

[0215] 其中,所述交易执行条件还包括:满足t'_1≥0～t'_u≥0。

[0216] 可选的,所述密钥镜像I_1～I_m由汇款方通过下述公式计算得到:

[0217] I_d=x_j×Hash_G(P_j,ID_j_d),d∈[1,m]。

[0218] 可选的,所述可链接环签名还包括密钥镜像I_(m+1)=r"×Hash_G(P"_j);

[0219] 其中,所述交易执行条件还包括:密钥镜像I_(m+1)不同于历史密钥镜像。

[0220] 可选的,

[0221] 所述待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_j_m)]、所述资产[ID_i_1,PC{i,1}]～[ID_i_m,PC{i,m}]为相应的历史交易的交易输出;或,

[0222] 所述待花费资产[ID_j_1,PC(t_j_1,r_j_1)]～[ID_j_m,PC(t_j_m,r_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,PC{i,1}]～[ID_i_m,PC{i,m}]被从掩护方i对应的账户余额中划分而生成。

[0223] 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∈[1,n]、d∈[1,m]。

[0224] 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∈[1,m];签名验证单元1102具体用于:

[0225] 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。

[0226] 可选的,

[0227] P_j=x_j×G,G为椭圆曲线的基点,|G|=p且p为素数,0<x_j<p;

[0228] 所述环签名所含的随机数和/或其衍生数值包括:s_k_1～s_k_(m+1)、c_1,k∈[1,n];

[0229] 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×G+c_k×P_k) mod 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;

[0230] 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)×G+c_k×P”_k]mod p;其中,s_k_(m+1)属于数域Z_q;

[0231] 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×Hash_G(P_k,ID_k_d)+c_k×I_d)mod p,I_d被包含于所述环签名中;

[0232] 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)×Hash_G(P”_k)+c_k×I_(m+1)]mod p,I_(m+1)被包含于所述环签名中;

[0233] 其中,当h＝1时c_1＝Hash(M,L_n_1,R_n_1,……,L_n_(m+1),R_n_(m+1))、当h∈[2,n]时c_k＝Hash(M,L_(h-1)_1,R_(h-1)_1,……,L_(h-1)_(m+1),R_(h-1)_(m+1))。

[0234] 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。

[0235] 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。

[0236] 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。

[0237] 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。

[0238] 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。

[0239] 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。

[0240] 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。

[0241] 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”。

[0242] 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。

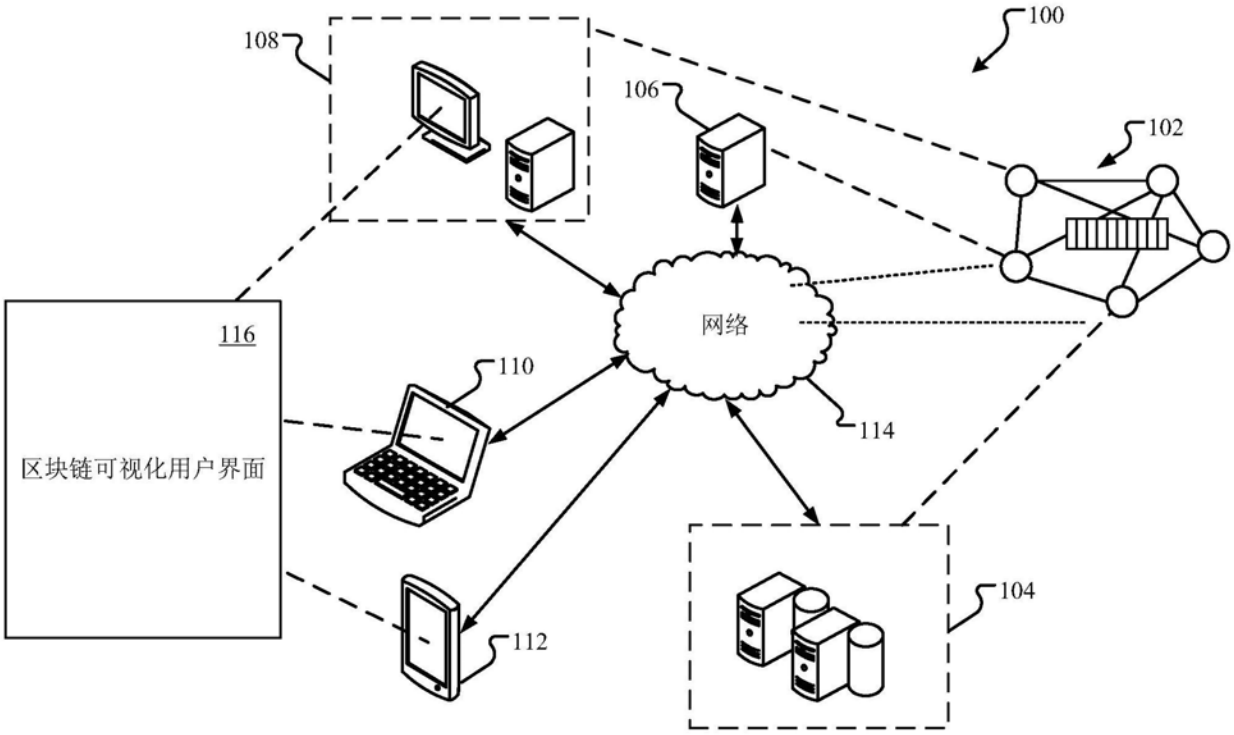


图1

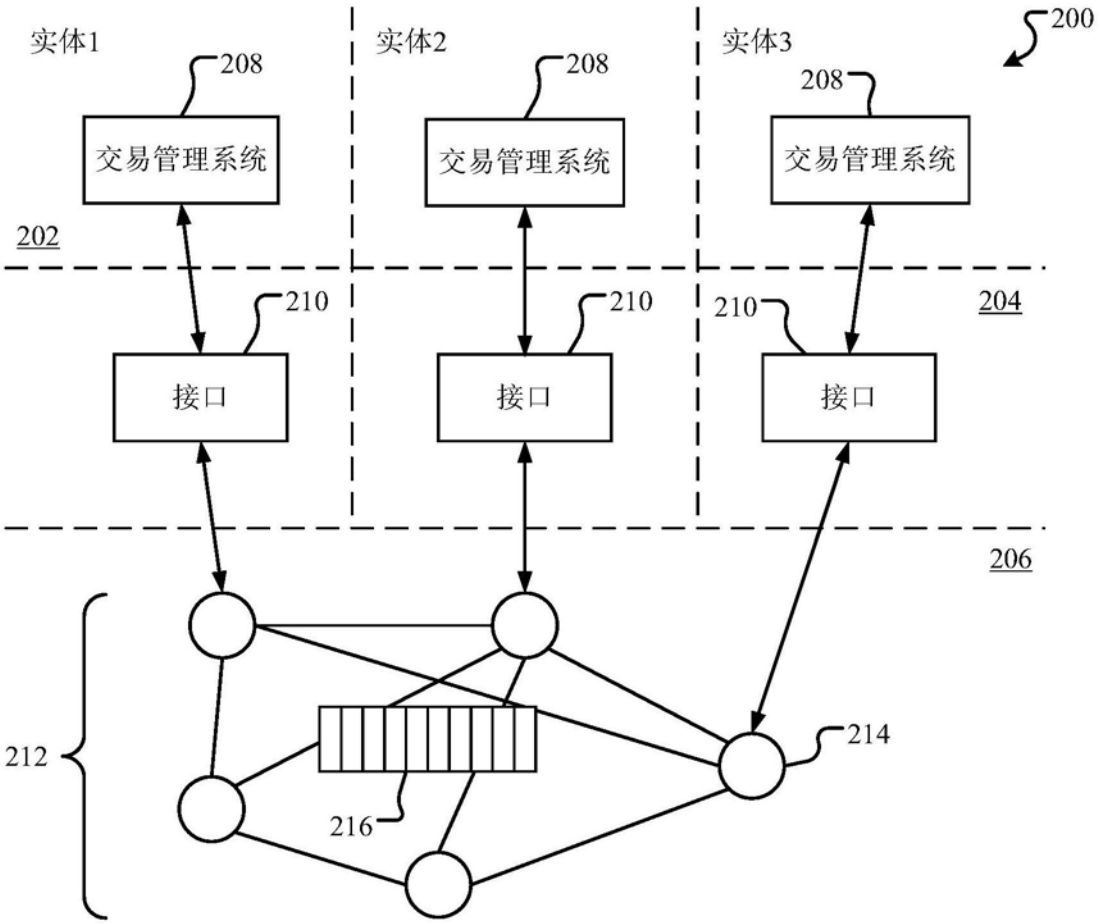

实体1
实体2
实体3
200
208
208
208
交易管理系统
交易管理系统
交易管理系统
202
204
210
210
210
接口
接口
接口
206
212
214
216

图2

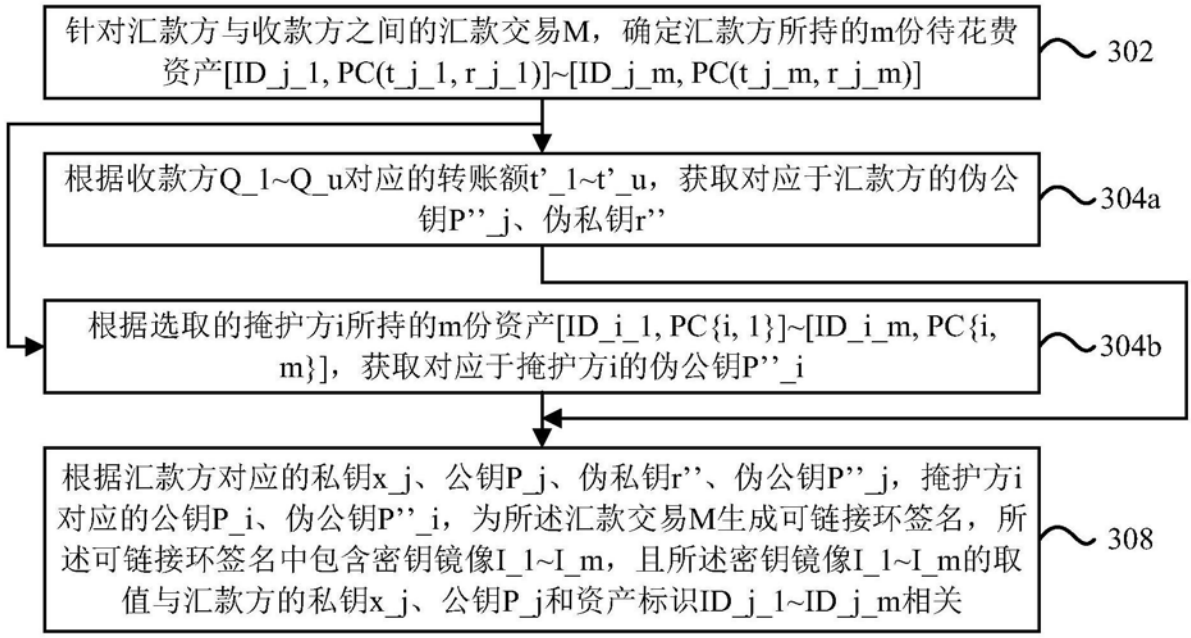

针对汇款方与收款方之间的汇款交易M，确定汇款方所持的m份待花费资产[ID_j_1, PC(t_j_1, r_j_1)]~[ID_j_m, PC(t_j_m, r_j_m)]
302
根据收款方Q_1~Q_u对应的转账额t'_1~t'_u，获取对应于汇款方的伪公钥P''_j、伪私钥r''
304a
根据选取的掩护方i所持的m份资产[ID_i_1, PC{i, 1}]~[ID_i_m, PC{i, m}]，获取对应于掩护方i的伪公钥P''_i
304b
根据汇款方对应的私钥x_j、公钥P_j、伪私钥r''、伪公钥P''_j，掩护方i对应的公钥P_i、伪公钥P''_i，为所述汇款交易M生成可链接环签名，所述可链接环签名中包含密钥镜像I_1~I_m，且所述密钥镜像I_1~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~ID_j_m相关
308

图3

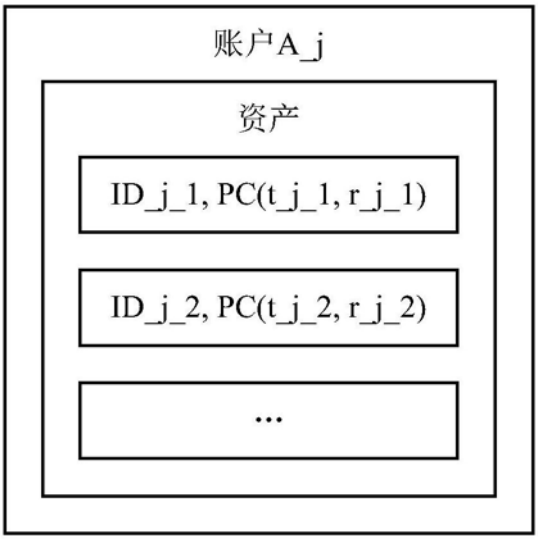

账户A_j
资产
ID_j_1, PC(t_j_1, r_j_1)
ID_j_2, PC(t_j_2, r_j_2)
...

图4

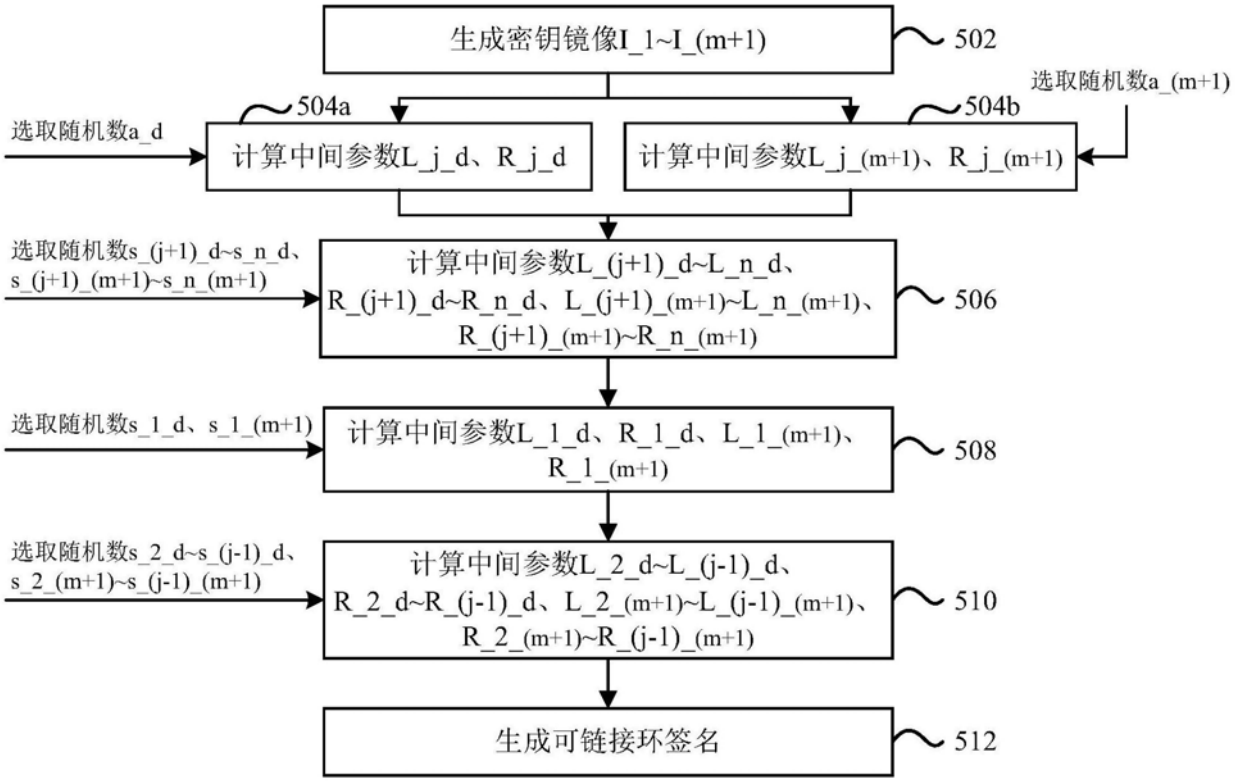

生成密钥镜像I_1~I_(m+1)
502
选取随机数a_(m+1)
504a
504b
选取随机数a_d
计算中间参数L_j_d、R_j_d
计算中间参数L_j_(m+1)、R_j_(m+1)
选取随机数s_(j+1)_d~s_n_d、s_(j+1)_(m+1)~s_n_(m+1)
计算中间参数L_(j+1)_d~L_n_d、R_(j+1)_d~R_n_d、L_(j+1)_(m+1)~L_n_(m+1)、R_(j+1)_(m+1)~R_n_(m+1)
506
选取随机数s_1_d、s_1_(m+1)
计算中间参数L_1_d、R_1_d、L_1_(m+1)、R_1_(m+1)
508
选取随机数s_2_d~s_(j-1)_d、s_2_(m+1)~s_(j-1)_(m+1)
计算中间参数L_2_d~L_(j-1)_d、R_2_d~R_(j-1)_d、L_2_(m+1)~L_(j-1)_(m+1)、R_2_(m+1)~R_(j-1)_(m+1)
510
生成可链接环签名
512

图5

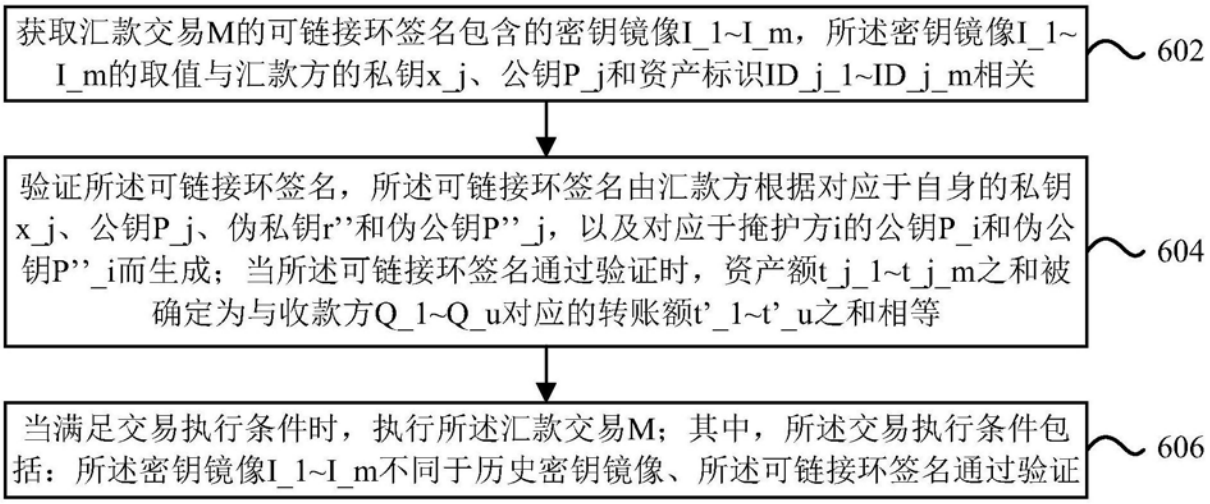

获取汇款交易M的可链接环签名包含的密钥镜像I_1~I_m，所述密钥镜像I_1~I_m的取值与汇款方的私钥x_j、公钥P_j和资产标识ID_j_1~ID_j_m相关
602
验证所述可链接环签名，所述可链接环签名由汇款方根据对应于自身的私钥x_j、公钥P_j、伪私钥r''和伪公钥P''_j，以及对应于掩护方i的公钥P_i和伪公钥P''_i而生成；当所述可链接环签名通过验证时，资产额t_j_1~t_j_m之和被确定为与收款方Q_1~Q_u对应的转账额t'_1~t'_u之和相等
604
当满足交易执行条件时，执行所述汇款交易M；其中，所述交易执行条件包括：所述密钥镜像I_1~I_m不同于历史密钥镜像、所述可链接环签名通过验证
606

图6

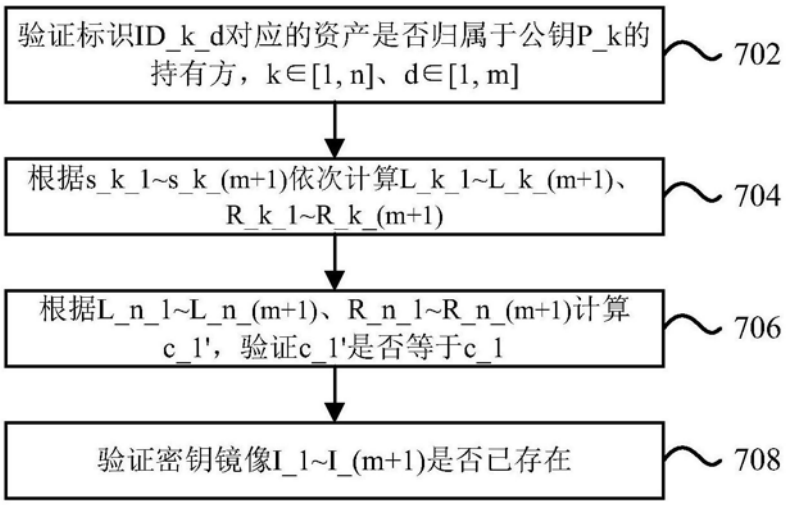

验证标识ID_k_d对应的资产是否归属于公钥P_k的持有方，k∈[1,n]、d∈[1,m]
702
根据s_k_1~s_k_(m+1)依次计算L_k_1~L_k_(m+1)、R_k_1~R_k_(m+1)
704
根据L_n_1~L_n_(m+1)、R_n_1~R_n_(m+1)计算c_1'，验证c_1'是否等于c_1
706
验证密钥镜像I_1~I_(m+1)是否已存在
708

图7

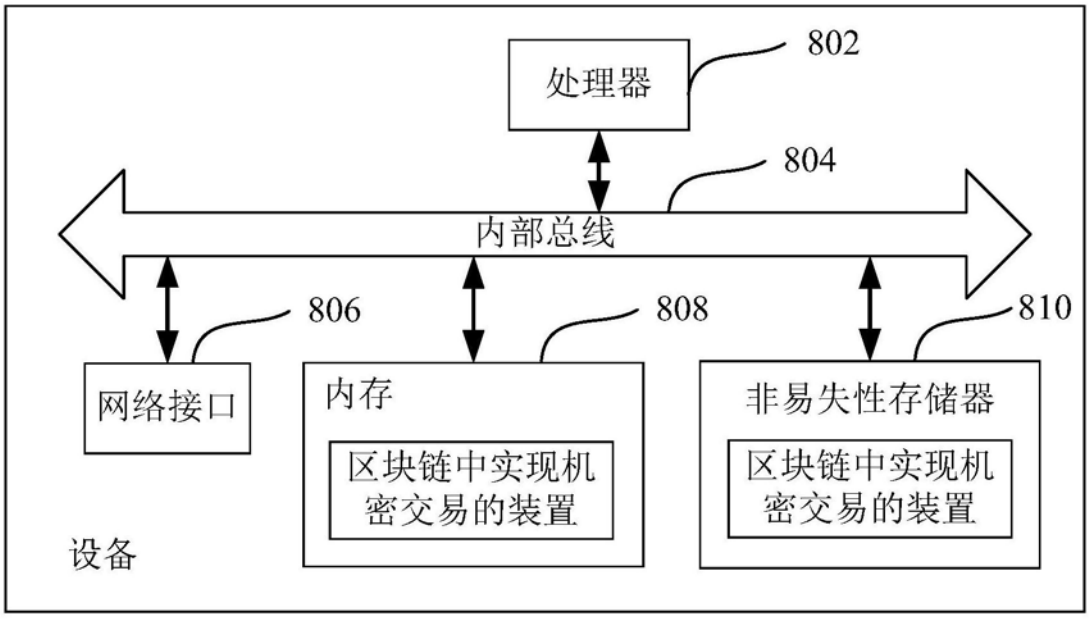

处理器
802
804
内部总线
806
808
810
网络接口
内存
区块链中实现机密交易的装置
非易失性存储器
区块链中实现机密交易的装置
设备

图8

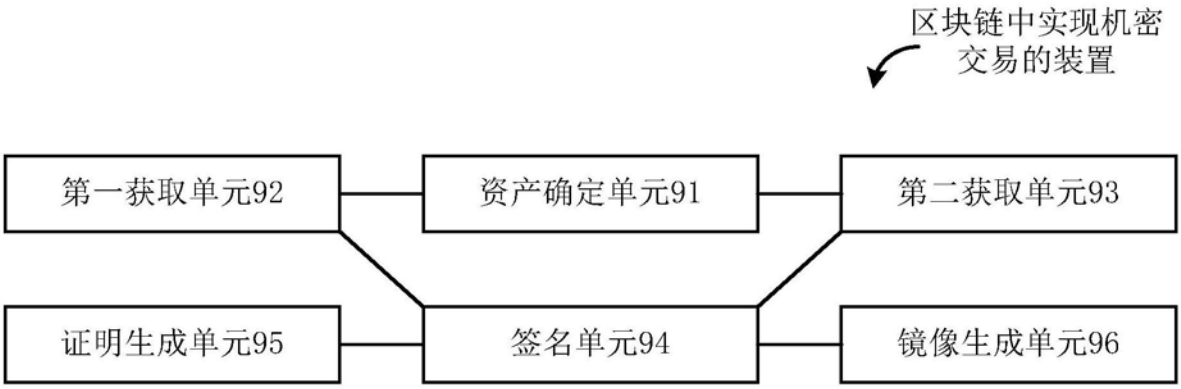

区块链中实现机密交易的装置
第一获取单元92
资产确定单元91
第二获取单元93
证明生成单元95
签名单元94
镜像生成单元96

图9

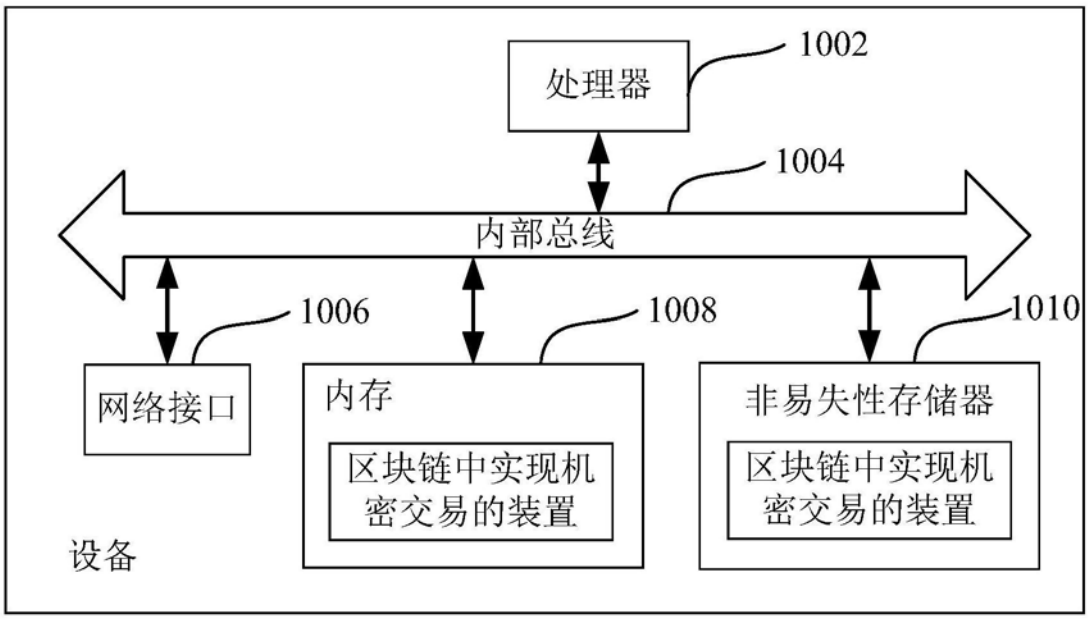

处理器
1002
1004
内部总线
1006
1008
1010
网络接口
内存
区块链中实现机密交易的装置
非易失性存储器
区块链中实现机密交易的装置
设备

图10

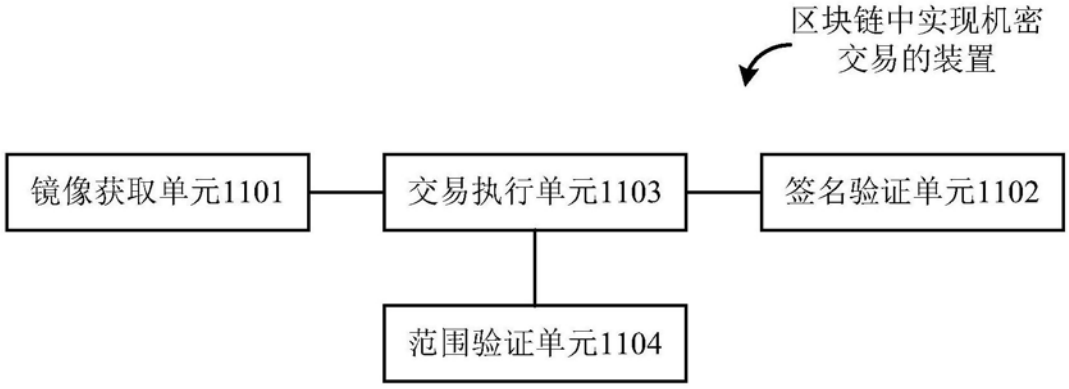

区块链中实现机密交易的装置
镜像获取单元1101
交易执行单元1103
签名验证单元1102
范围验证单元1104

图11