(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110073633 B
(45)授权公告日 2023.03.31

(21)申请号 201880004853.9
(22)申请日 2018.11.07
(65)同一申请的已公布的文献号
申请公布号 CN 110073633 A
(43)申请公布日 2019.07.30
(85)PCT国际申请进入国家阶段日
2019.06.05
(86)PCT国际申请的申请数据
PCT/CN2018/114344 2018.11.07
(87)PCT国际申请的公布数据
WO2019/072264 EN 2019.04.18
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛乔治镇医院路27号开曼企业中心
(72)发明人 马宝利 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
专利代理师 林祥
(51)Int.Cl.
H04L 9/00(2022.01)
H04L 9/08(2006.01)
H04L 9/30(2006.01)
G06Q 20/38(2012.01)
(56)对比文件
任雯.密文医学图像可逆信息隐藏算法的研究.《中国优秀博硕士学位论文全文数据库(硕士) 信息科技辑》.2018,第11页.
审查员 安佳

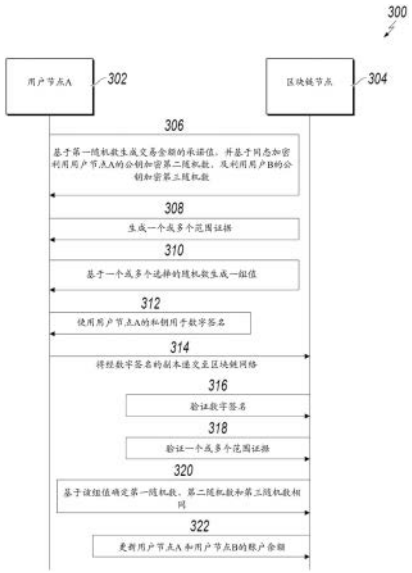
权利要求书2页 说明书12页 附图8页

(54)发明名称

使用同态加密的区块链数据保护

(57)摘要

本公开的实施方式包括从第一账户接收余额转账的第一金额的基于第一随机数生成的承诺值的经数字签名的副本、利用所述第一账户的公钥加密的所述余额转账的所述第一金额和所述第一随机数、利用第二账户的公钥加密的所述余额转账的第二金额和第二随机数、和基于一个或多个选择的随机数生成的一组值。所述第一账户确定所述第一金额与所述第二金额是否相同、以及所述第一随机数与所述第二随机数是否相同,并基于所述余额转账金额的所述第一金额更新所述第一账户的余额和所述第二账户的余额。



CN 110073633 B

1.一种由区块链网络的共识节点执行的计算机实施方法,包括:

从第一账户接收要从所述第一账户转账至第二账户的余额转账的第一金额的基于第一随机数生成的承诺值的经数字签名的副本、基于概率性同态加密HE算法利用所述第一账户的公钥加密的所述余额转账的所述第一金额和第二随机数、基于所述概率性HE算法利用所述第二账户的公钥加密的所述余额转账的第二金额和第三随机数、一个或多个范围证据、和基于一个或多个选择的随机数生成的一组值;其中,

由r*、t*、z1*和z2*表示所述选择的随机数,且所述选择的随机数用于生成a、b、c和d,其中a=r*+xr、b=t*+xt、c=z1*+xz1、d=z2*+xz2,r是所述第一随机数,t是所述余额转账的所述第一金额,x是哈希值,z1和z2是用于基于所述概率性HE算法对所述余额转账的所述第二金额和所述第三随机数进行加密的随机数;

利用所述第一账户的公钥,验证对应于所述经数字签名的副本的数字签名,其中所述第一账户的公钥与用于生成所述数字签名的私钥对应;

确定所述一个或多个范围证据证实所述余额转账的金额大于零、且小于或等于所述第一账户的余额;

基于所述一组值确定所述第一金额与所述第二金额是否相同、以及所述第一随机数与所述第二随机数和第三随机数是否相同;以及

若所述第一金额与所述第二金额相同、且所述第一随机数与所述第二随机数和第三随机数相同,则基于所述余额转账的所述第一金额通过概率性同态加密HE算法更新所述第一账户的余额和所述第二账户的余额。

2.如权利要求1所述的计算机实施方法,其中,利用同态承诺方案生成所述承诺值。

3.如权利要求2所述的计算机实施方法,其中,所述承诺方案为佩德森承诺方案。

4.如权利要求1所述的计算机实施方法,其中,所述概率性HE算法是Okamoto-Uchiyama算法。

5.如权利要求1所述的计算机实施方法,其中,还基于C、D和E生成所述一组值,其中

$C=g^{r*}h^{t*}$、$D=u2^{r*}v2^{z1*}$、$E=u2^{t*}v2^{z2*}$,

其中,g、h、u2和v2为椭圆曲线的生成元,

x是基于对C、D和E进行哈希处理生成的。

6.如权利要求5所述的计算机实施方法,其中,基于概率性HE的特性确定所述第一金额与所述第二金额是否相同、以及所述第一随机数与所述第二随机数和所述第三随机数是否相同。

7.如权利要求6所述的计算机实施方法,其中,若以下条件成立,则确定所述第一金额与所述第二金额相同、并且所述第一随机数与所述第三随机数相同:

$g^{a}h^{b}=CT^{x}$、$u2^{a}v2^{c}=DZ_B1^{x}$且$u2^{b}v2^{d}=EZ_B2^{x}$,

其中,$T=g^{r}h^{t}$是所述余额转账的金额的承诺值,

$Z\_B1=u2^{r}v2^{z1}$、$Z\_B2=u2^{t}v2^{z2}$。

8.一种耦接到一个或多个处理器且其上存储有指令的非暂态计算机可读存储介质,当由所述一个或多个处理器执行所述指令时,促使所述一个或多个处理器根据权利要求1-7中任一项所述的方法执行操作。

9.一种系统,包括:

计算设备,以及

耦接到所述计算设备且其上存储有指令的计算机可读存储设备,当由所述计算设备执行所述指令时,促使所述计算设备根据权利要求1-7中任一项所述的方法执行操作。

使用同态加密的区块链数据保护

背景技术

[0001] 区块链网络,还可被称为区块链系统、共识网络、分布式账本系统网络或区块链,使得参与的实体能够安全地且不可篡改地存储数据。区块链可被描述为交易的账本系统,且账本的多个副本被存储于区块链网络中。区块链的示例类型可以包括公有区块链、许可区块链和私有区块链。公有区块链对所有实体开放使用区块链,并开放参与共识过程。许可区块链类似于公有区块链但仅对有加入许可的实体开放。为特定实体提供私有区块链,该实体集中控制读写权限。

[0002] 区块链用于加密货币网络,加密货币网络使得参与者可以使用加密货币进行交易以买/卖物品和/或服务。通用加密货币包括比特币(Bitcoin)。在加密货币网络中,记账模型用于记录用户之间的交易。示例性记账模型包括未被花费交易输出(UTXO)模型和账户余额模型。在UTXO模型中,每个交易花费来自先前交易的输出并生成可以在随后交易中被花费的新输出。追踪用户的未被花费的交易,且计算用户的所有未被花费的交易的和作为该用户拥有的余额。在账户余额模型中,追踪每个用户的账户余额作为全局状态。对于每个交易,检查花费的账户的余额以确保余额大于或等于交易金额。这可以与传统银行业务对比。

[0003] 区块链账本包括一系列区块,每个区块包含一个或多个在网络中执行的交易。每个区块可以被类比为账本中的一页,而区块链本身就是账本的完整副本。各个交易被确认并被添加至区块,该区块被添加至区块链。区块链账本的副本遍布网络中的节点复制。以这种方式,对区块链的状态形成了全局共识。此外,至少在公有网络的情况下,区块链对所有节点开放查看。为保护区块链用户的隐私可实施加密技术。

[0004] 在账户余额模型下,可以使用承诺方案以隐藏交易双方当事人承诺的值。可以根据当事人对选择或值的承诺的需求产生承诺方案,并随后可以将该值传达给所涉及的其他当事人。例如,在交互佩德森承诺(Pedersen Commitment,PC)中,当事人A可以通过发送基于随机值r生成的承诺值PC(t,r)来承诺交易金额t。承诺值被生成,并且当事人B只能通过获取随机数r显露交易金额t。

发明内容

[0005] 本公开的实施方式包括用于在无需用户确认、交互及显露交易金额或账户余额的情况下,对区块链交易进行隐私保护验证的计算机实施方法。更具体地,本公开的实施方式涉及基于承诺方案和同态加密验证区块链用户之间的交易,而不将交易金额、账户余额或用于生成承诺的随机数显露给其他区块链节点。

[0006] 在一些实施方式中,动作包括:从第一账户接收要从所述第一账户转账到第二账户的余额转账的第一金额的基于第一随机数生成的承诺值的经数字签名的副本、使用所述第一账户的公钥加密的所述余额转账的所述第一金额和所述第一随机数、使用所述第二账户的公钥加密的所述余额转账的第二金额和第二随机数、一个或多个范围证据、以及基于一个或多个所选择的随机数生成的一组值;使用所述第一账户的公钥验证与所述经数字签名的副本对应的数字签名,所述第一账户的公钥与用于生成所述数字签名的私钥对应;确

定所述一个或多个范围证据证实所述余额转账的金额大于零、且小于或等于所述第一账户的余额;基于所述一组值确定所述第一金额与所述第二金额是否相同、并且所述第一随机数与所述第二随机数是否相同;以及如果所述第一金额与所述第二金额相同、并且所述第一随机数与所述第二随机数相同,则基于所述余额转账的所述第一金额更新所述第一账户的余额和所述第二账户的余额。

[0007] 这些和其他实施方式可以各自可选地包括以下特征中的一个或多个:使用同态承诺方案生成所述承诺值;所述承诺方案是佩德森承诺(Pedersen Commitment)方案;基于概率性同态加密(HE)算法,使用所述第一账户的公钥加密所述余额转账的所述第一金额和所述第一随机数,并且基于所述概率性HE算法,使用所述第二账户的公钥加密所述余额转账的所述第二金额和所述第二随机数;所述概率性HE算法是Okamoto-Uchiyama HE算法;所选择的随机数由r*、t*、z1*和z2*表示,并且所选择的随机数用于生成a、b、c和d,其中a=r*+xr、b=t*+xt、c=z1*+xz1、d=z2*+xz2,r是所述第一随机数,t是所述余额转账的所述第一金额,x是哈希值;还基于C、D和E生成所述一组值,其中$C=g^{r*}h^{t*}$、$D=u2^{r*}v2^{z1*}$、$E=u2^{t*}v2^{z2*}$,g、h、u2和v2是椭圆曲线的生成元,x是基于对C、D和E进行哈希处理生成的;基于概率性HE的特性确定所述第一金额与所述第二金额是否相同、以及所述第一随机数与所述第二随机数是否相同;如果以下条件成立,则确定所述第一金额与所第二金额相同、并且所述第一随机数与所述第二随机数相同:$g^ah^b=CT^x$、$u2^av2^c=DZ_B1^x$且$u2^bv2^d=EZ_B2^x$,$T=g^rh^t$是所述余额转账的金额的承诺值,$Z\_B1=u2^rv2^{z1}$、$Z\_B2=u2^tv2^{z2}$,z1和z2是用于基于所述概率性HE方案加密所述余额转账的所述第二金额和所述第二随机数的随机数;以及基于HE更新所述第一账户的余额和所述第二账户的余额。

[0008] 本公开还提供了耦接到一个或多个处理器且其上存储有指令的一个或多个非暂态计算机可读存储介质,当由所述一个或多个处理器执行所述指令时,促使所述一个或多个处理器根据本文提供的方法的实施方式执行操作。

[0009] 本公开还提供了用于实现本文所提供方法的系统。该系统包括一个或多个处理器、以及耦接到所述一个或多个处理器且其上存储有指令的一个或多个非暂态计算机可读存储介质,当由所述一个或多个处理器执行所述指令时,促使所述一个或多个处理器根据本文提供的方法的实施方式执行操作。

[0010] 可以理解的是根据本公开的方法可以包括本文所述的方面和特征的任意组合。也即,根据本公开的方法不限于本文所述的方面和特征的组合,但也包括所提供的方面和特征的任意组合。

[0011] 本公开的一个或多个实施方式的细节将在下文结合附图和描述进一步阐述。本公开的其他特征或优点将从描述和附图以及权利要求中显而易见。

附图说明

[0012] 图1描绘了可用于执行本公开实施方式的示例性环境。

[0013] 图2描绘了根据本公开实施方式的示例性概念性架构。

[0014] 图3描绘了根据本公开实施方式的基于同态加密的区块链交易的隐私保护验证的示例性方法。

[0015] 图4描绘了根据本公开实施方式的基于同态加密的示例性区块链交易。

[0016] 图5描绘了根据本公开实施方式的基于同态加密的区块链交易的隐私保护验证的另一示例性方法。

[0017] 图6描绘了根据本公开实施方式的基于同态加密的另一示例性区块链交易。

[0018] 图7描绘了可以根据本公开实施方式执行的示例性过程。

[0019] 图8描绘了可以根据本公开实施方式执行的另一示例性过程。

[0020] 各附图中的相同附图标记表示相同元件。

具体实施方式

[0021] 本公开的实施方式包括用于在无需用户确认、交互及显露交易金额或账户余额的情况下，对区块链交易进行隐私保护验证的计算机实施方法。更具体地，本公开的实施方式涉及基于承诺方案和同态加密(HE)来验证区块链用户之间的交易，而不对其他区块链节点显露交易金额、账户余额或用于生成承诺的随机数。

[0022] 为本公开实施方式提供进一步的背景，如上所述的，区块链网络又可被称为共识网络(例如，由点对点节点组成)、分布式账本系统、或简称为区块链，使得参与的实体能够安全地且不可篡改地进行交易并存储数据。区块链可被提供为公有区块链、私有区块链或联盟区块链。本文将参考在参与的实体之间公开的公有区块链网络进行进一步详述本公开的实施方式。然而，可以预测的是，可以在任何合适类型的区块链中实现本公开的实施方式。

[0023] 在公有区块链中，共识过程由共识网络的节点控制。例如，数百、数千甚至数百万的实体可以参与到公有区块链中，每个实体操作该公有区块链中的至少一个节点。因此，就参与的实体而言，公有区块链可被视为公有网络。在一些示例中，大部分实体(节点)必须对每个区块签名，以使区块有效并被添加至区块链中。示例性公有区块链包括在比特币网络中使用的区块链，该比特币网络是点对点支付网络(加密货币网络)。虽然本文所用术语“区块链”通常指代比特币网络，但是在不特指比特币网络的情况下，区块链通常指分布式账本。

[0024] 通常来说，公有区块链支持公开交易。在区块链内公开交易被所有节点共享，且该区块链账本跨所有节点复制。也即，所有节点相对于区块链都处于完美共识状态。为达成共识(例如，同意将区块添加至区块链)，在区块链网络内实施共识协议。示例性共识协议包括但不限于，在比特币网络中实施的工作量证明(POW)。

[0025] 鉴于以上背景，本文进一步详细描述了本公开的实施方式。更具体地，并且如上所述，本公开的实施方式涉及基于承诺方案和HE验证区块链用户之间的交易，而不对其他区块链节点显露交易金额、账户余额或用于生成承诺的随机数。

[0026] 根据本公开的实施方式，可以基于承诺验证区块链交易并将其记录至区块链(账本)中，而不显露交易账户余额、交易金额或用于生成承诺的随机数。例如佩德森承诺(PC)的承诺方案，可以用于利用随机数生成交易金额的承诺。可以利用概率性HE或确定性HE对交易金额和随机数加密。交易金额和随机数也可以用于生成一组值，作为用于基于HE的特性验证交易的证据。可以在不显露账户余额、交易金额或随机数的情况下，由区块链节点利用交易的承诺、加密的交易金额、加密的随机数和证据来验证交易是否有效。

[0027] 图1描绘了可用于执行本公开实施方式的示例性环境100。在一些示例中，示例性

环境100使得实体能够参与至公有区块链102中。示例性环境100包括计算系统106、计算系统108和网络110。在一些示例中，网络110包括局域网(LAN)、广域网(WAN)、因特网或其组合，并且连接网络站点、用户设备(例如，计算设备)和后端系统。在一些示例中，可以通过有线和/或无线通信链路来访问网络110。

[0028] 在所描述的示例中，计算系统106、计算系统108可以各自包括能够作为节点参与至公有区块链102中的任何适当的计算系统。示例性计算设备包括但不限于服务器、台式计算机、膝上型计算机、平板计算设备和智能手机。在一些示例中，计算系统106、计算系统108承载一个或多个由计算机120实施的服务，用于与公有区块链102交互。例如，计算系统106可以承载第一实体(例如，用户A)的由计算机120实施的、例如交易管理系统的服务，第一实体使用该交易管理系统管理其与一个或多个其他实体(例如，其他用户)的交易。计算系统108可以承载第二实体(例如，用户B)的由计算机120实施的、例如交易管理系统的服务，第二实体使用该交易管理系统管理其与一个或多个其他实体(例如，其他用户)的交易。在图1的示例中，公有区块链102被表示为节点的点对点网络(Peer-to-Peer network)，并且计算系统106、计算系统108分别提供参与到公有区块链102的第一实体和第二实体的节点。

[0029] 图2描绘了根据本公开实施方式的示例性概念架构200。示例性概念架构200包括实体层202、承载服务层204和公有区块链层206。在所描绘的示例中，实体层202包括三个实体，实体1(E1)、实体2(E2)和实体3(E3)，每个实体具有相应的交易管理系统208。

[0030] 在所描述的示例中，承载服务层204包括用于每个交易管理系统208的区块链接口210。在一些示例中，各个交易管理系统208使用通信协议(例如，超文本传输协议安全(HTTPS))通过网络(例如，图1的网络110)与各个区块链接口210通信。在一些示例中，每个区块链接口210提供各个交易管理系统208和区块链层206之间的通信连接。更具体地，每个区块链接口210使各个实体能够进行记录在区块链层206的区块链网络212中的交易。在一些示例中，区块链接口210与区块链层206之间的通信是使用远程过程调用(RPC)进行的。在一些示例中，区块链接口210“承载”用于各个交易管理系统208的区块链节点。例如，区块链接口210提供用于访问区块链网络212的应用程序编程接口(API)。

[0031] 如本文所述的，区块链网络212被提供为包括多个节点214的点对点网络，所述多个节点214在区块链216中不可篡改地记录信息。尽管示意性地描述了单个区块链216，但是在区块链网络212中可以提供并维护区块链216的多个副本。例如，每个节点214存储区块链216的副本。在一些实施方式中，区块链216存储与参与公有区块链的两个或更多个实体之间进行的交易相关联的信息。

[0032] 图3描绘了根据本公开实施方式的基于HE的区块链交易的隐私保护验证的示例性方法300。在较高层面上，示例性方法300由用户节点A 302、用户节点B(图3中未示出)和被称为共识节点的区块链节点304执行。可以进行从用户节点A 302至用户节点B的例如转账的交易。为保护账户隐私，用户节点A 302可以基于随机数r利用例如PC的承诺方案生成交易金额t的承诺。可以将利用PC生成的承诺表达为PC(r,t)。用户节点A 302还可以基于用户节点B的公钥利用HE对随机数加密。这可以被表达为HE(r)。可以将交易金额t的表达为(PC(r,t),HE(r))的密文传输至用户节点B。在接收到密文之后，用户节点B可以利用私钥对随机数r解密。用户节点B可以利用随机数r对交易金额t解密。为证实交易的有效性，区块链节点304可以将承诺中的随机数与利用HE加密的随机数对比。若所述随机数匹配，则区块链节

点304通过交易数据的零知识确定交易有效。示例方法300的更多细节将在下文对图3的描述中讨论。

[0033] 在306，用户节点A 302基于第一随机数生成交易金额的承诺值，并基于HE利用用户节点A 302的公钥对第二随机数加密、以及利用用户节点B的公钥对第三随机数加密。第一随机数、第二随机数和第三随机数可以是相同的随机数r，其被用于利用承诺方案生成交易金额t的承诺。在一些实施方式中，承诺方案可以具有双指数的形式，例如PC。使用PC作为非限制性示例，通过第一随机数r生成的承诺值可以被表达为$PC(r,t)=g^{r}h^{t}$，其中g和h可以是椭圆曲线的生成元，PC(r,t)是曲线点的标量相乘，t是被承诺的交易金额。可以理解的是，其他基于HE的承诺方案，例如Okamoto-Uchiyama(OU)HE以及Boneh-Goh-Nissim HE也可以用于生成承诺值。

[0034] 对利用用户节点A 302的公钥加密得到的加密第二随机数r可以被表达为HE_A(r)。对利用用户节点B的公钥加密得到的加密第三随机数r可以被表达为HE_B(r)。

[0035] 在一些实施方式中，公钥HE加密可以是确定性HE，其可根据诸如Paillier HE、Benaloh HE、OU HE、Naccache-Stern HE、Damgard-Jurik HE或Boneh-Goh-Nissim HE等的概率性HE方案通过将随机数设置为固定值而被获取。在一些实施方式中，满足线性特征HE(a+b)＝HE(a)+HE(b)和$HE(ab)=HE(b)^{a}$的确定性HE方案可以用于本公开，其中a和b是用于HE的明文。

[0036] 在一些示例中，T＝PC(r,t)、T'＝HE_A(r)和T"＝HE_B(r)，并且交易金额的密文可被表达为(T,T'和T")。若满足示例条件，则可以确定交易有效。首先，交易金额t大于或等于零且小于或等于用户节点A 302的账户余额s_A。其次，通过用户节点A 302的私钥对交易进行数字签名以证实交易是由用户节点A 302授权的。再次，承诺PC(r,t)中的随机数r与密文HE_A(r)中使用用户节点A302的公钥加密的r和密文HE_B(r)中使用用户节点B的公钥加密的r分别相等。

[0037] 在一些实施方式中，密文也可以被分解成发送金额(t')的密文和接收金额(t")的密文，其中发送金额(t')的密文可被表达为(PC(r',t'),HE_A(r'))，接收金额(t")的密文可被表达为(PC(r",t"),HE_B(r"))。在此情况下，还需要确定发送金额t'与接收金额t"相等以验证交易。

[0038] 在308，用户节点A 302生成一个或多个范围证据。在一些实施方式中，范围证据可以包括范围证据RP1以表示交易金额t大于或等于零，以及范围证据RP2以表示交易金额t小于或等于用户节点A的账户余额。

[0039] 在310，用户节点A 302基于一个或多个选择的随机数使用HE生成一组值。标记为Pf的该组值可以包括用于证实承诺PC(r,t)中的随机数r与密文HE_A(r)和HE_B(r)中分别利用用户节点A 302和用户节点B的公钥加密的r相等的证据。在一些实施方式中，可以选择两个随机数r1和t1以计算t1的被标记为(T1,T1',T1")的另一组密文，其中$T1=g^{r1}h^{t1}$、T1'＝HE_A(r1)、T1"＝HE_B(r1)。可以计算两个附加的证据r2和t2:r2＝r1+xr、t2＝t1+xr，其中x是T1、T1'和T1"的哈希值。可将该组值标记为Pf＝(T1,T1',T1",r2,t2)。

[0040] 在312，用户节点A 302利用其私钥对密文(T',T',T")、密文(T1,T1'T1")、r2、t2、范围证据RP1和RP2以及用户节点A 302和用户节点B的公钥进行数字签名。由用户节点A 302添加的数字签名可以用于表明交易是由用户节点A 302授权的。在314，将经数字签名的

副本递交至区块链网络。

[0041] 在316,区块链节点304利用用户节点A 302的公钥验证数字签名。区块链节点304可以是能够证实区块链网络中的交易的有效性的共识节点。若区块链节点304利用该公钥不能验证用户节点A 302的数字签名,则可以确定该数字签名错误,并可以拒绝该交易。在一些实施方式中,区块链节点304还可以包括反双花机制。区块链节点304可以验证交易是否已被执行或记录。若交易已经被执行,则可以拒绝该交易。否则,可以进行交易验证。

[0042] 在318,区块链节点304验证一个或多个范围证据。例如,范围证据RP1可以用于证实交易金额t大于或等于零,且范围证据RP2可以用于证实交易金额t小于或等于用户节点A 302的账户余额。

[0043] 在320,区块链节点304基于该组值确定第一随机数、第二随机数以及第三随机数相同。在一些实施方式中,确定过程包括基于上述确定性HE的特性确定示例条件$g^{r2}h^{t2}=T^{x}T1$、HE_A(r2)＝T'^{x}T1'以及HE_B(r2)＝T"^{x}T1"是否为真。若为真,则其可以表明承诺中的随机数与利用用户节点A 302和用户节点B的公钥同态加密的随机数相同,且交易有效。

[0044] 在322,区块链节点304更新用户节点A 302和用户节点B的账户余额。可以基于HE的特性执行余额更新而不显露用户节点A 302或用户节点B的账户余额。本文将参考图4进一步描述账户余额的更新。

[0045] 图4描绘了根据本公开实施方式的基于HE的示例性区块链交易400。如示例性区块链交易400中所示,用户节点A 402向用户节点B 406转账交易金额t。在交易之前,用户节点A 402的账户余额为s_A,且用户节点B 406的账户余额为s_B。

[0046] 使用本文参考图3描述的加密方案和交易过程作为示例,可以基于PC利用随机数r_A对账户余额s_A加密,且基于HE对随机数r_A加密。账户余额s_A的密文可被表达为(S_A,S'_A)＝($g^{r\_A}h^{s\_A}$,HE_A(r_A)),其中g和h可以是椭圆曲线的生成元以用于生成账户余额s_A的PC。类似地,可以基于PC利用随机数r_B对用户节点B 406的账户余额s_B加密。账户余额s_B的密文可被表达为(S_B,S'_B)＝($g^{r\_B}h^{s\_B}$,HE_A(r_B))。

[0047] 在404,用户节点A 402可以将数字签名添加至用于验证交易的一系列证据中,并将经数字签名的副本递交至区块链网络408。参考图3如上所述,上述证据可以包括交易金额的密文(T,T',T")、一个或多个范围证据(RP1,RP2)以及其他证据(T1,T1',T1",r2,t2)。

[0048] 在交易之后,用户节点A 402的账户余额可被表达为s_A-t',且用户节点B 406的账户余额可被表达为s_B+t",其中t'是由用户节点A 402发送的金额,且t"是由用户节点B接收的金额。用户节点A 402在交易后的账户余额的密文可以表达为(S_A-T,S'_A-T'),用户节点B 406在交易之后的账户余额的密文可被表达为(S_B+T,S'_B+T")。因为S_A、S'_A、S_B、S'_B、T、T'、T"均是利用双指数形式的HE加密的,因此可以在它们的加密形式下进行加减运算而无需解密成明文值。

[0049] 图5描绘了根据本公开实施方式的基于HE的区块链交易的隐私保护验证的另一示例性方法500。在较高层面上,示例性方法500由用户节点A 502、用户节点B(图5中未示出)以及可被称为共识节点的区块链节点504执行。可以进行从用户节点A 502至用户节点B的例如转账的交易。为保护账户隐私,用户节点A 502可以基于随机数r利用例如PC的承诺方案生成交易金额t的承诺。利用PC生成的承诺可被表达为PC(r,t)。用户节点A 502还可以利用具有双指数形式的HE(例如OU)对交易金额t和随机数r加密。

[0050] 交易金额t的密文可以被递交至区块链网络。在接收到密文之后，区块链节点504可以确定隐藏在PC中的随机数r是否与OU中分别利用用户节点A 502的公钥和用户节点B的公钥加密的随机数r匹配。此外，区块链节点504可以确定隐藏在PC中的交易金额t是否与OU中分别利用用户节点A 502的公钥和用户节点B的公钥加密的交易金额t匹配。若随机数和交易金额都匹配，则区块链节点504可基于交易数据的零知识验证该交易有效。

[0051] 在506，用户节点A 502基于第一随机数生成第一交易金额的承诺值，且使用用户节点A 502的公钥对第一交易金额和第一随机数加密。使用用户节点B的公钥对第二交易金额和第二随机数加密。第一交易金额和第二交易金额可以为相同的交易金额t。第一随机数和第二随机数可以是相同的随机数r，以用于利用承诺方案生成交易金额t的承诺。在一些实施方式中，承诺方案可以具有双指数形式、例如PC。使用PC作为示例，通过第一随机数r生成的承诺值可以被表达为$PC(r,t)=g^{r}h^{t}$，其中g和h可以是椭圆曲线的生成元，PC(r,t)是曲线点的标量相乘，t是被承诺的交易金额。可以理解的是，其他基于HE的承诺方案，例如OU HE以及Boneh-Goh-Nissim HE也可以用于生成承诺值。

[0052] 用户节点A 502还可以利用用户节点A 502的公钥对第一随机数和第一交易金额加密，并利用用户节点B的公钥对第二随机数和第二交易金额加密。在一些实施方式中，随机数和交易金额的加密可以基于概率性HE、例如OU。使用OU作为示例，利用用户节点A 502的公钥加密的第一随机数和第一交易金额可被分别表达为$OU_A(r)=u1^{r}v1^{y1}$和$OU_A(t)=u1^{t}v1^{y2}$，其中u1和v1分别为椭圆曲线的生成元，且y1和y2为用于生成OU_A(r)和OU_A(t)的随机数。加密的第二随机数和第二交易金额分别表达为$OU_B(r)=u2^{r}v2^{z1}$和$OU_B(t)=u2^{t}v1^{z2}$，其中u2和v2为椭圆曲线的生成元，且z1和z2分别为用于生成OU_B(r)和OU_B(t)的随机数。概率性OU满足OU(a+b)＝OU(a)*OU(b)的特性，其中a和b为用于OU的明文。

[0053] 交易金额t的密文可被表达为(PC(r,t),OU_A(r),OU_A(t),OU_B(r),OU_B(t))。若符合以下示例条件，则可以确定交易有效。首先，交易金额t大于或等于零，且小于或等于用户节点A 502的账户余额s_A。其次，交易是利用用户节点A 502的私钥数字签名的，以证实交易是由用户节点A 502授权的。再次，承诺PC(r,t)中的随机数r与密文OU_A(r)和OU_B(r)中分别利用用户节点A 502和用户节点B的公钥加密的r相同。最后，承诺PC(r,t)中的交易金额t与密文OU_A(r)和OU_B(r)中分别利用用户节点A 502和用户节点B的公钥加密的t相同。

[0054] 在一些实施方式中，密文也可以被分解成发送金额为(t')的密文和接收金额为(t")的密文，发送金额为(t')的密文可表达为(PC(r',t'),OU_A(r'),OU_A(t'))，接收金额为(t")的密文可表达为(PC(r",t"),OU_B(r"),OU_B(t"))。在这种情况下，还需要确定发送金额t'等于接收金额t"以验证交易。

[0055] 在508，用户节点A 502生成一个或多个范围证据。在一些实施方式中，范围证据可以包括范围证据RP1以显示交易金额t大于或等于零，以及范围证据RP2以显示交易金额t小于或等于用户节点A的账户余额。

[0056] 在510，用户节点A 502基于一个或多个选择的随机数利用HE生成一组值。标注为Pf的该组值可以包括用于证实承诺PC(r,t)中的随机数r与密文OU_A(r)和OU_B(r)中加密的r相同的证据，以及承诺PC(r,t)中的交易金额t与密文OU_A(r)和OU_B(r)中加密的t相同的证据。在一些实施方式中，可以选择四个随机数r*、t*、z1*和z2*来计算标注为(C,D,E)的

另一组密文，其中C＝$g^{r*}h^{t*}$、D＝$u2^{r*}v2^{z1*}$且E＝$u2^{t*}v2^{z2*}$，其中g、h、u2和v2是椭圆曲线的生成元。可计算四个附加证据a、b、c和d:a＝r*+xr、b＝t*+xt、c＝z1*+xz1和d＝z2*+xz2，其中x是g、h、u2、v2、C、D和E的哈希函数。该组值可被标注为Pf＝(C,D,E,a,b,c,d)。

[0057] 在512，用户节点A 502使用其私钥对密文(PC(r,t),OU_A(r),OU_A(t),PC(r,t),OU_B(r),OU_B(t))、范围证据RP1和RP2以及该组值Pf进行数字签名。由用户节点A 502添加的数字签名可以用于显示交易是由用户节点A 502授权的。在514，将经数字签名的副本递交至区块链网络。

[0058] 在516，区块链节点504利用用户节点A 502的公钥验证数字签名。区块链节点504可以是能够证实在区块链网络上的交易的有效性的共识节点。若区块链节点504利用用户节点A的公钥不能验证数字签名，则该数字签名可被确定为错误，并且交易可被拒绝。在一些实施方式中，区块链节点504还可以包括反双花机制。区块链节点504可以验证交易是否已被执行或记录。若交易已经被执行，则交易可被拒绝。否则，可以进行交易验证。

[0059] 在518，区块链节点504验证一个或多个范围证据。例如，范围证据RP1可以用于证实交易金额t大于或等于零，且范围证据RP2可以用于证实交易金额t小于或等于用户节点A 502的账户余额。

[0060] 在520，区块链节点504基于该组值确定第一交易金额是否与第二交易金额相同，以及第一随机数是否与第二随机数相同。在一些实施方式中，确定过程包括确定$g^{a}h^{b}$＝CT^{x}、$u2^{a}v2^{c}$＝DZ_B1^{x}以及$u2^{b}v2^{d}$＝$EZ+B2^{x}$是否为真，其中T＝$g^{r}h^{t}$是第一交易金额t的承诺值、Z_B1＝$u2^{r}v2^{z1}$、Z_B2＝$u2^{t}v2^{z2}$、且z1和z2是用于基于概率性HE方案对第二交易金额和第二随机数加密的随机数。若确定为真，则可以指示承诺中的随机数和交易金额分别与利用用户节点A 502和用户节点B的公钥同态加密的随机数和交易金额相等，且交易有效。

[0061] 在522，区块链节点504更新用户节点A 502和用户节点B的账户余额。可以基于HE的特性执行账户余额更新而不显露用户节点A 502和/或用户节点B的账户余额。

[0062] 图6描绘了根据本公开实施方式的基于HE的另一示例性区块链交易600。如示例性交易600所示，用户节点A 602将交易金额t转账至用户节点B 606。在交易之前，用户节点A 602具有为s_A的账户余额，且用户节点B 606具有为s_B的账户余额。

[0063] 在一些示例中，可使用本文参考图5描述的加密方案和交易过程，基于PC利用随机数r_A隐藏账户余额s_A。可基于OU对随机数r_A和账户余额加密。账户余额s_A的密文可被表达为(S_A,R_A,Q_A)＝($g^{r\_A}h^{s\_A}$,OU_A(r_A),OU_A(s_A))，其中g和h可以为椭圆曲线的生成元以用于生成账户余额s_A的PC。类似地，可基于PC利用随机数r_B对用户节点B 606的账户余额s_B加密。账户余额s_B的密文可被表达为(S_B,R_B,Q_B)＝($g^{r\_B}h^{s\_B}$,OU_B(r_B),OU_B(s_B))。

[0064] 在604，用户节点A 602可以向用于验证交易的证据添加数字签名，并将经数字签名的副本递交至区块链网络608中。这里参考图5所描述的，证据可以包括交易金额的密文(PC(r,t),OU_A(r),OU_A(t),OU_B(r),OU_B(t))、一个或多个范围证据(RP1,RP2)和其他证据(C,D,E,a,b,c,d)。

[0065] 在交易之后，用户节点A 602的账户余额可被表达为s_A-t，且用户节点B 606的账户余额可被表达为s_B+t。在交易之后，用户节点A 602的账户余额的密文可被表达为(S_A-T,R_A-Y_A1,Q_A-Y_A2)，其中Y_A1＝OU_A(r)且Y_A2＝OU_A(t)。在交易之后，用户节点B

606的账户余额的密文可被表达为(S_B+T,R_B+Z_B1,Q_B+Z_B2),其中Z_B1＝OU_B(r)且Z_B2＝OU_B(t)。因为S_A、S_B、R_A、R_B、Q_A、Q_B、Y_A1、Y_A2、Z_B1、Z_B2和T是利用具有双指数形式的HE加密的,因此可以在它们的加密形式下进行加减运算而无需解密成明文值。

[0066] 图7描绘了可根据本公开实施方式执行的示例性过程700。为清楚地呈现,在本说明书中以下描述在其他附图的背景下总体地描述方法700。然而,应当理解示例性过程700可以例如通过任何系统、环境、软件和硬件或者系统、环境、软件和硬件的组合合理来执行。在一些实施方式中,示例性过程700的步骤可以以并行、组合、循环或任何顺序进行。

[0067] 在702,共识节点从第一账户接收待从第一账户向第二账户转账的交易金额的、基于第一随机数生成的承诺值的经数字签名的副本。共识节点还可以从第一账户接收利用第一账户的公钥加密的第二随机数、利用第二账户的公钥加密的第三随机数、一个或多个范围证据以及基于一个或多个选择的随机数利用HE生成的一组值。在一些实施方式中,使用基于HE的承诺方案生成承诺值。在一些实施方式中,基于确定性HE方案对第二随机数和第三随机数加密。

[0068] 在一些实施方式中,通过(T1,T1',T1",r2,t2)表示该组值,其中r2＝r1+xr、t2＝t1+xt,r1和t1表示一个或多个选择的随机数,且r表示第一随机数,t表示余额转账金额。在一些示例中,$T1=g^{r1}h^{t1}$、T1'＝HE_A(r1)、T1"＝HE_B(r1),其中g和h是椭圆曲线的生成元,HE_A(r1)是基于利用第一账户的公钥对r1进行HE生成的,且HE_B(r1)是基于利用第二账户的公钥对r1进行HE生成的。在一些示例中,x是基于对T1、T1'和T1"进行哈希处理生成的。

[0069] 在704,共识节点利用第一账户的与用于生成数字签名的私钥相对应的公钥,验证与经数字签名的副本相对应的数字签名。

[0070] 在706,共识节点确定一个或多个范围证据证实余额转账金额是否大于零,且小于或等于第一账户的余额。

[0071] 在708,共识节点基于该组值确定第一随机数、第二随机数和第三随机数是否相同。在一些实施方式中,若以下条件成立,则确定第一随机数、第二随机数和第三随机数相同:$g^{r2}h^{t2}=T^{x}T1$、HE_A(r2)＝T'^{x}T1'且HE_B(r2)＝$T"^{x}$T1",其中$T=g^{r}h^{t}$是余额转账金额的承诺值,T'＝HE_A(r)且T"＝HE_B(r),HE_A(r)是基于利用第一账户的公钥对r进行HE生成的,HE_B(r)是基于利用第二账户的公钥对r进行HE生成的,HE_A(r2)是基于利用第一账户的公钥对r2进行HE生成的,以及HE_B(r2)是基于利用第二账户的公钥对r2进行HE生成的,x是基于对g、h、T1、T1'和T1"进行哈希处理生成的。在一些实施方式中,T、T'和T"形成交易金额t的密文。

[0072] 在710,若第一随机数、第二随机数和第三随机数相同,则共识节点基于交易金额更新第一账户的余额和第二账户的余额。在一些实施方式中,更新第一账户的余额和第二账户的余额是基于HE进行的。

[0073] 图8描绘了可根据本公开实施方式执行的另一示例性过程800。为清楚地呈现,在本说明中以下描述在其他附图的执行背景下总体地描述示例过程800。然而,应该理解示例性过程800可以例如通过任何系统、环境、软件和硬件或者系统、环境、软件和硬件的组合合理进行。在一些实施方式中,示例性过程800的步骤可以以并行、组合、循环或任何顺序进行。

[0074] 在802,共识节点从第一账户接收待从第一账户向第二账户转账的第一交易金额

的承诺值的经数字签名的副本。在一些示例中，基于第一随机数生成该承诺值的经数字签名的副本。共识节点还接收利用第一账户的公钥加密的第一交易金额和第一随机数、利用第二账户的公钥加密的第二余额转账金额和第二随机数、一个或多个范围证据、以及基于一个或多个选择的随机数利用HE生成的一组值。在一些实施方式中，利用PC方案生成承诺值。在一些实施方式中，基于概率性HE算法使用第一账户的公钥对第一余额转账金额和第一随机数加密。在一些示例中，基于概率性HE算法使用第二账户的公钥对第二余额转账金额和第二随机数加密。在一些实施方式中，概率性HE算法为Okamoto-Uchiyama HE算法。

[0075] 在一些实施方式中，通过(C,D,E,a,b,c,d)表示该组值，其中a＝r*+xr、b＝t*+xt、c＝z1*+xz1且d＝z2*+xz2，r*、t*、z1*和z2*表示一个或多个选择的随机数，r表示第一随机数，t表示第一余额转账金额，$C=g^{r*}h^{t*}$，$D=u2^{r*}v2^{z1*}$，$E=u2^{t*}v2^{z2*}$，g、h、u2和v2为椭圆曲线的生成元，且x表示对C、D和E进行哈希处理。

[0076] 在804，共识节点利用第一账户的与用于生成数字签名的私钥相对应的公钥，验证与经数字签名的副本相对应的数字签名。

[0077] 在806，共识节点确定一个或多个范围证据证实余额转账金额是否大于零，且小于或等于第一账户的余额。

[0078] 在808，共识节点基于该组值确定第一金额是否与第二金额相同，以及第一随机数是否与第二随机数相同。在一些实施方式中，若以下条件成立，则确定第一金额与第二金额相同且第一随机数与第二随机数相同：$g^{a}h^{b}=CT^{x}$、$u2^{a}v2^{c}=DZ_B1^{x}$且$u2^{b}v2^{d}=EZ_B2^{x}$，其中$T=g^{r}h^{t}$是余额转账金额的承诺值，$Z\_B1=u2^{r}v2^{z1}$，$Z\_B2=u2^{t}v2^{z2}$。在一些示例中，z1和z2是用于基于概率性HE方案对第二交易金额和第二随机数加密的随机数。

[0079] 在810，若第一金额与第二金额相同且第一随机数与第二随机数相同，则共识节点基于第一余额转账金额更新第一账户的余额和第二账户的余额。在一些实施方式中，更新第一账户的余额和第二账户的余额是基于HE进行的。

[0080] 本申请中所描述主题的实施方式可被实施以实现特定优点或技术效果。例如，本公开的实施方式允许区块链节点的账户余额和区块链节点的交易金额在交易期间是隐私的。资金转移的接收方不需要确认交易或使用随机数验证承诺，交易验证可以是非互动性的。区块链节点可以基于HE和承诺方案验证交易以允许零知识证明。

[0081] 所述方法能够提高各种移动计算设备的账户/数据安全性。账户余额和交易金额可以基于HE被加密并通过承诺方案被隐藏。照此，共识节点在交易之后可以基于HE的特性更新账本中的账户余额，而不显露账户的真实账户余额。因为不需要将随机数发送至接收方以确认交易，所以数据泄露的风险可被降低，并且需要更少的用于管理随机数的计算和存储资源。

[0082] 本申请中描述的实施方式和操作可以在数字电子电路中或者在计算机软件、固件、包括本申请中公开的结构的硬件中或它们中一个或多个的组合中实现。这些操作可被实施为由数据处理装置对存储在一个或多个计算机可读存储设备上的、或从其他资源接收的数据执行的操作。数据处理装置、计算机或计算设备可以包括，包括诸如可编程处理器、计算机、片上系统或以上一个或多个或组合的，用于处理数据的装置、设备和机器。装置可以包括专用逻辑电路，例如，中央处理单元(CPU)、现场可编程门阵列(FPGA)或专用集成电路(ASIC)。装置还可包括为所讨论的计算机程序创建执行环境的代码，例如，构成处理器固

件、协议栈、数据库管理系统、操作系统(例如一个操作系统或多个操作系统的组合)、跨平台运行时间环境、虚拟机或者它们之中一个或多个的组合的代码。装置和执行环境可以实现各种不同的计算模型基础设施,例如网页服务、分布式计算和网格计算基础设施。

[0083] 计算机程序(又称,例如,程序、软件、软件应用、软件模块、软件单元、脚本或代码)可以以任何形式的编程语言编写,包括编译语言或演绎性语言、说明性语言或程序性语言,并且它可以配置为任何形式,包括作为独立程序,或者作为模块、组件、子程序、对象或适合在计算环境中使用的其他单元。程序可存储在:保存其他程序或数据的文件的一部分中(例如,存储在标记语言文档中的一个或多个脚本)、专用于所讨论的程序的单个文件中或者多个协调文件中(例如,存储一个或多个模块,子程序或部分代码的多个文件)中。计算机程序可以在一台计算机或者位于一个站点或由通信网络互联的分布在多个站点上的多台计算机执行。

[0084] 用于执行计算机程序的处理器包括,例如,通用和专用微型处理器两者,和任意种类的数码计算机的任意一个或多个处理器。通常,处理器将从只读存储器或随机存取存储器或其两者接收指令和数据。计算机的重要元件为用于根据指令进行操作的处理器和用于存储指令和数据的一个或多个存储设备。通常,计算机还将包括一个或多个用于存储数据的大型存储设备,或可操作地耦接以从所述大型存储设备接收数据或向其转发数据,或两者。计算机可嵌入在另一个设备中,例如,移动电话、个人数字助理(PDA)、游戏控制台、全球定位系统(GPS)接收器或便携式存储设备。适用于存储计算机程序指令和数据的设备包括非易失性存储器、介质和存储设备,包括,例如,半导体存储设备、磁盘和磁光盘。处理器和存储器可补充有专用逻辑电路或集成在专用逻辑电路中。

[0085] 移动设备可以包括手机、用户设备(UE)、移动电话(例如,智能电话)、平板电脑、可穿戴设备(例如,智能手表和智能眼镜)、人体内的植入设备(例如,生物传感器、人工耳蜗植入)、或其它类型的移动设备。移动设备可以无线地(例如,使用射频(RF)信号)与各种(下文描述的)通信网络通信。移动设备可以包括用于确定移动设备当前环境的特征的传感器。传感器可以包括相机、麦克风、接近传感器、GPS传感器、运动传感器、加速度测量计、环境光传感器、湿度传感器、陀螺仪、指南针、气压计、指纹传感器、面部识别系统、RF传感器(例如,WiFi和蜂窝无线电)、热量传感器或其它类型的传感器。例如,相机可以包括带有可动或固定镜头的前置或后置相机、闪光灯、图像传感器和图像处理器。相机可以是能够捕捉用于面部和/或虹膜识别的细节的百万像素相机。相机与数据处理器和存储在存储器中或可远程访问的认证数据一起可以形成面部识别系统。面部识别系统或者一个或多个传感器,例如,麦克风、运动传感器、加速度测量计、GPS传感器或RF传感器可以用于用户认证。

[0086] 为提供用于与用户的交互,实施方式可以在具有显示设备和输入设备的计算机上实现,例如,用于向用户显示信息的液晶显示器(LCD)或有机发光二极管(OLED)/虚拟现实(VR)/增强现实(AR)显示器以及用户可提供输入至计算机的触摸屏、键盘和指示设备。其他种类的设备也可以用于提供与用户的交互;例如,提供给用户的反馈可是任何形式的感官反馈,例如视觉反馈,听觉反馈或触觉反馈;且可以以任何形式接收来自用户的输入,包括声学、语音或触觉输入。此外,计算机可通过向用户使用的设备发送文档并从用户使用的设备接收文档来与用户交互;例如,通过响应于从网页浏览器接收到的请求向客户设备上的网页浏览器发送网页。

[0087] 实施方式可以使用计算设备实现，计算设备通过有线或无线数字数据通信(或其组合)的任意形式或媒介互联，例如，通信网络。互联设备的示例为通常彼此远离的、通常通过通信网络交互的客户端和服务器。客户端，例如，移动设备，可以自身与服务器或通过服务器进行交易，例如进行买、卖、支付、给予、发送或贷款交易，或认证以上交易。这种交易可以是实时的使得操作和响应在时间上接近，例如个体感觉操作和响应基本上是同时发生的，对于在个体的操作之后的响应的时间差小于一毫秒(ms)或小于一秒(s)，或在不考虑系统的处理限制的情况下，响应没有主动延迟。

[0088] 通信网络的示例包括局域网(LAN)、无线电接入网(RAN)、城域网(MAN)和广域网(WAN)。通信网络可以包括所有或部分因特网、其他通信网络或通信网络的组合。可以根据各种协议和标准在通信网络上传输信息，包括长期演进网络(LTE)、5G、IEEE 802、因特网协议(IP)或其他协议或协议的组合。通信网络可以在连接的计算设备之间传输音频、视频、生物特征或认证数据或其他信息。

[0089] 作为单独实施方式描述的特征可以组合实施、在单个实施方式中实施，然而被描述为单个实施方式的特征可以在多个实施方式中分别单独实现，或在任何合适的子组合中实现。按特定顺序描述的和要求保护的操作不应理解为必须以该顺序进行，也不是所有示出的操作都必须被执行(一些操作可以是可选的)。适当地，可以进行多任务或并行处理(或多任务和并行处理的组合)。

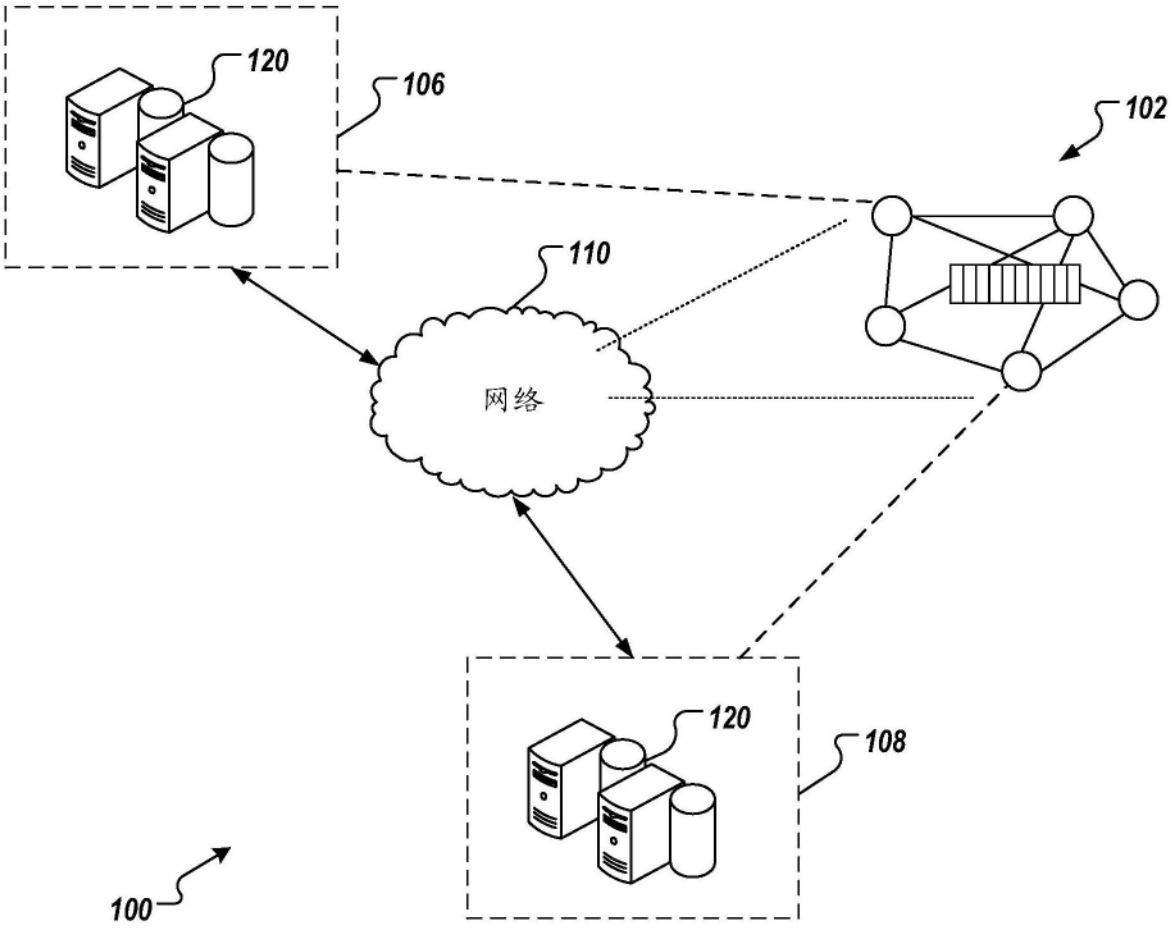


图1

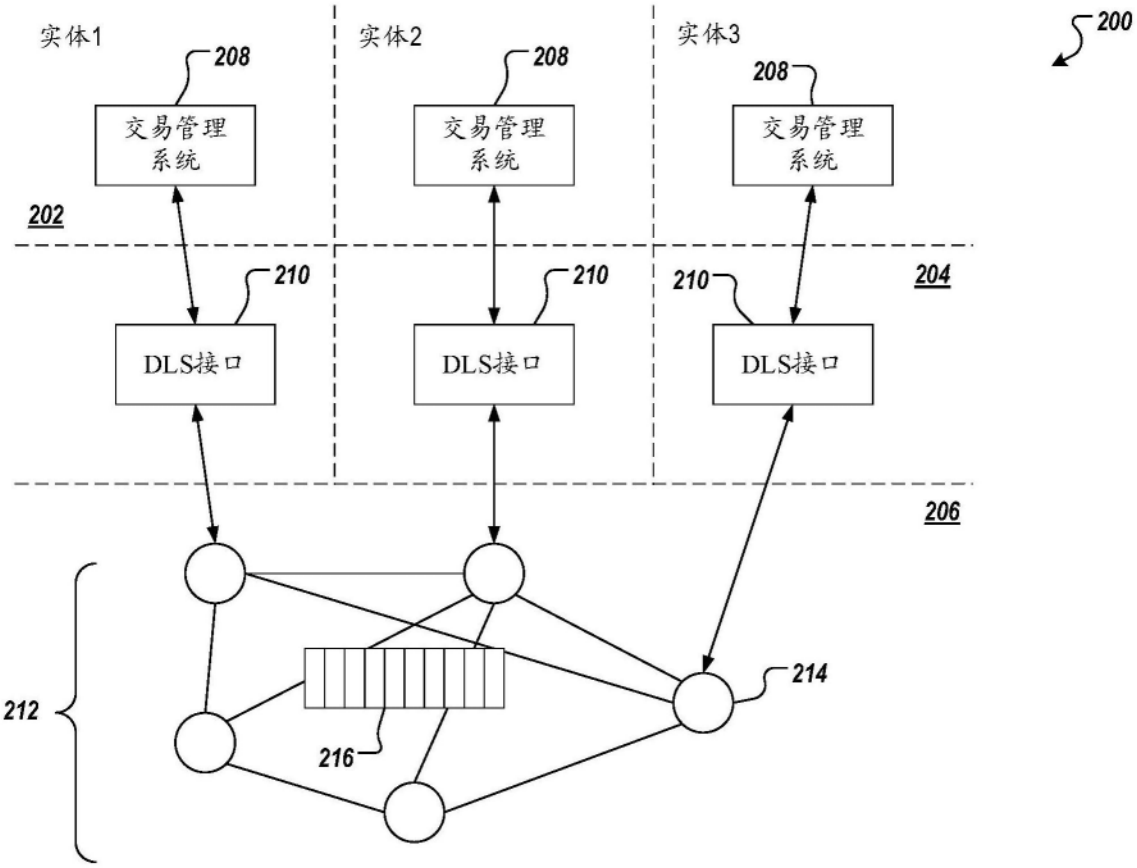

实体1
实体2
实体3
200
208
208
208
交易管理系统
交易管理系统
交易管理系统
202
204
206
210
210
210
DLS接口
DLS接口
DLS接口
212
214
216

图2

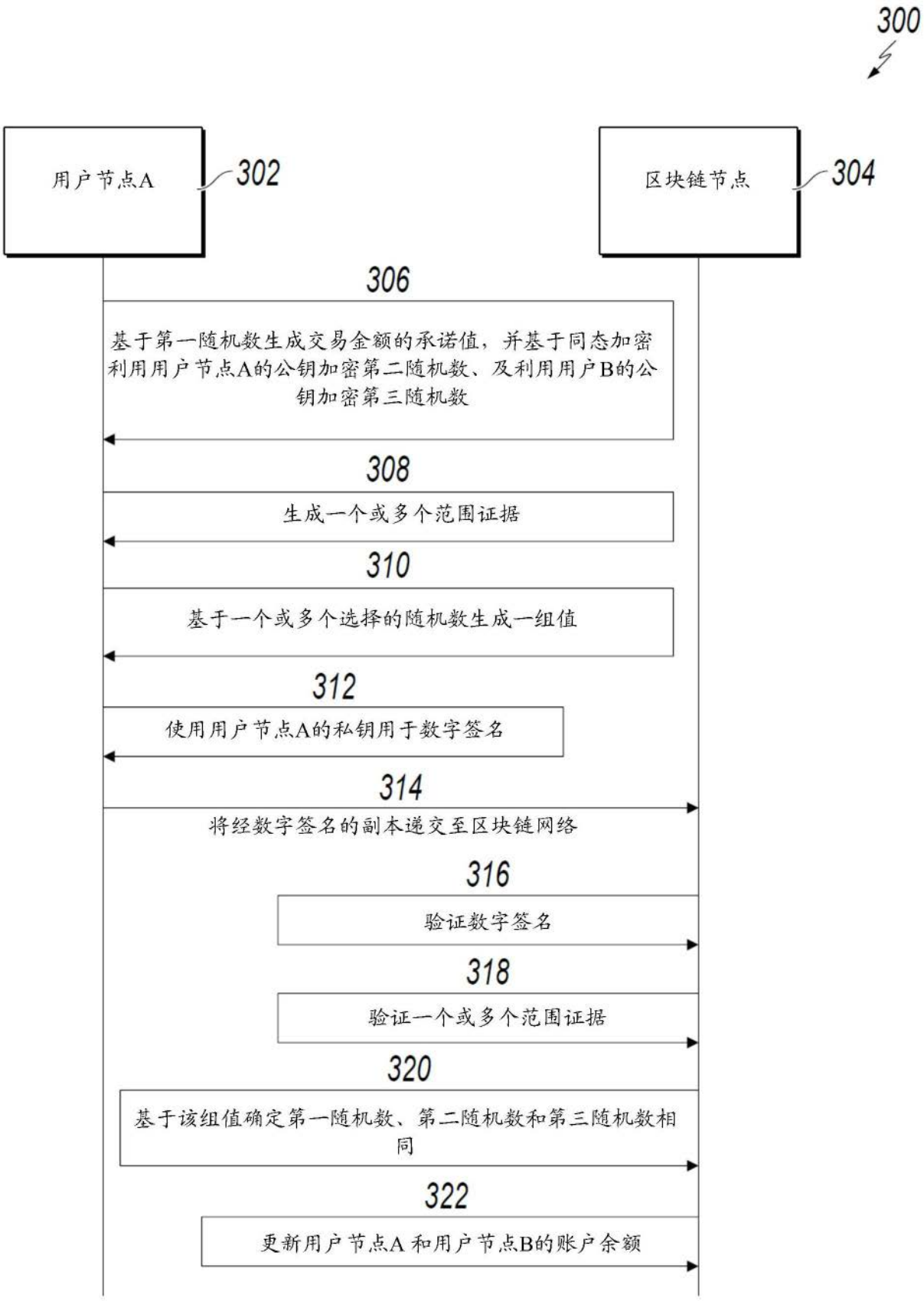

300
用户节点A
302
区块链节点
304
306
基于第一随机数生成交易金额的承诺值，并基于同态加密利用用户节点A的公钥加密第二随机数、及利用用户B的公钥加密第三随机数
308
生成一个或多个范围证据
310
基于一个或多个选择的随机数生成一组值
312
使用用户节点A的私钥用于数字签名
314
将经数字签名的副本递交至区块链网络
316
验证数字签名
318
验证一个或多个范围证据
320
基于该组值确定第一随机数、第二随机数和第三随机数相同
322
更新用户节点A和用户节点B的账户余额

图3

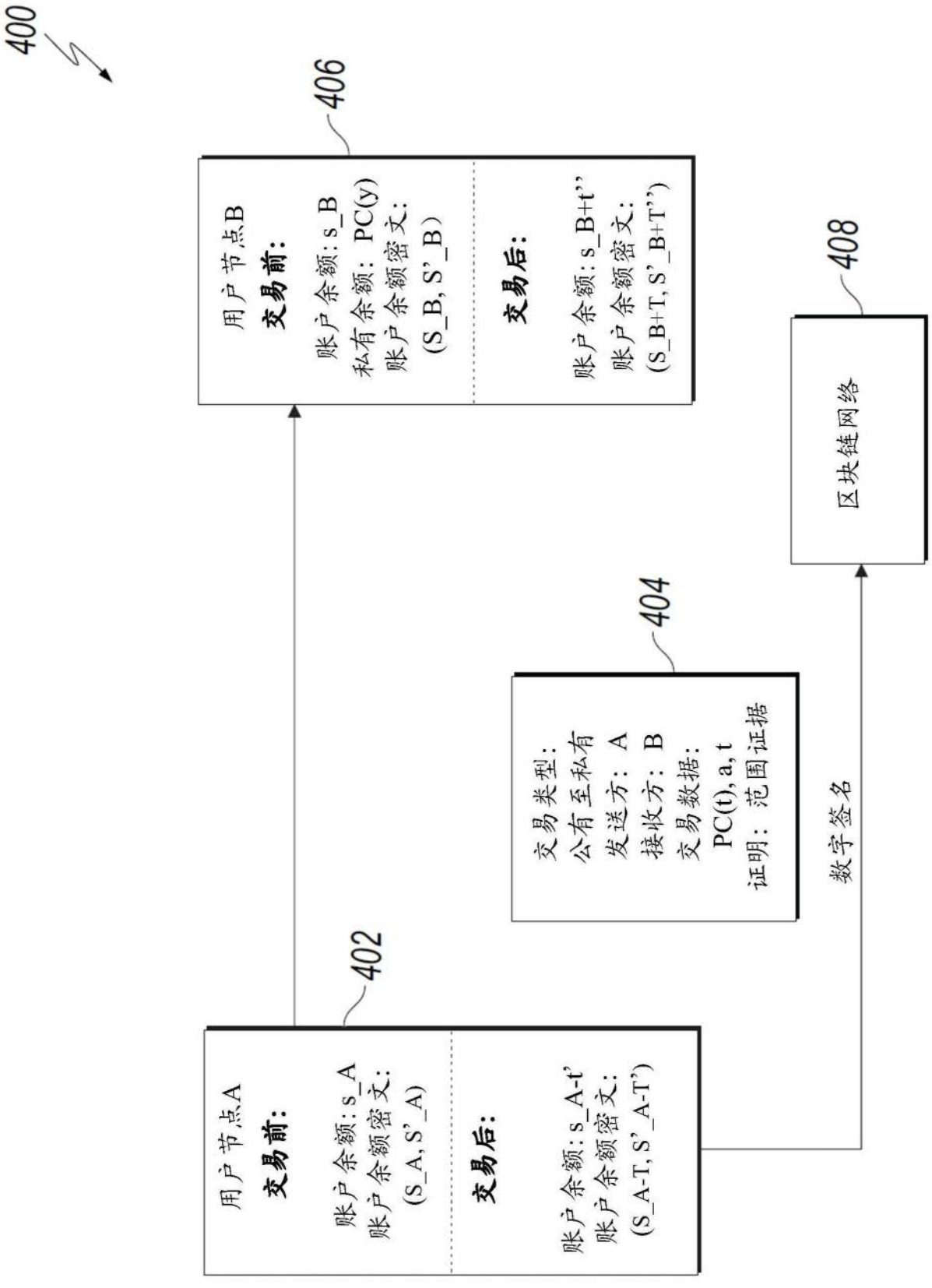

400
406
用户节点B
交易前:
账户余额:s_B
私有余额: PC(y)
账户余额密文:
(S_B, S'_B)
交易后:
账户余额:s_B+t''
账户余额密文:
(S_B+T, S'_B+T'')
408
区块链网络
404
交易类型:
公有至私有
发送方: A
接收方: B
交易数据:
PC(t), a, t
证明: 范围证据
数字签名
402
用户节点A
交易前:
账户余额:s_A
账户余额密文:
(S_A,S'_A)
交易后:
账户余额:s_A-t'
账户余额密文:
(S_A-T,S'_A-T')

图4

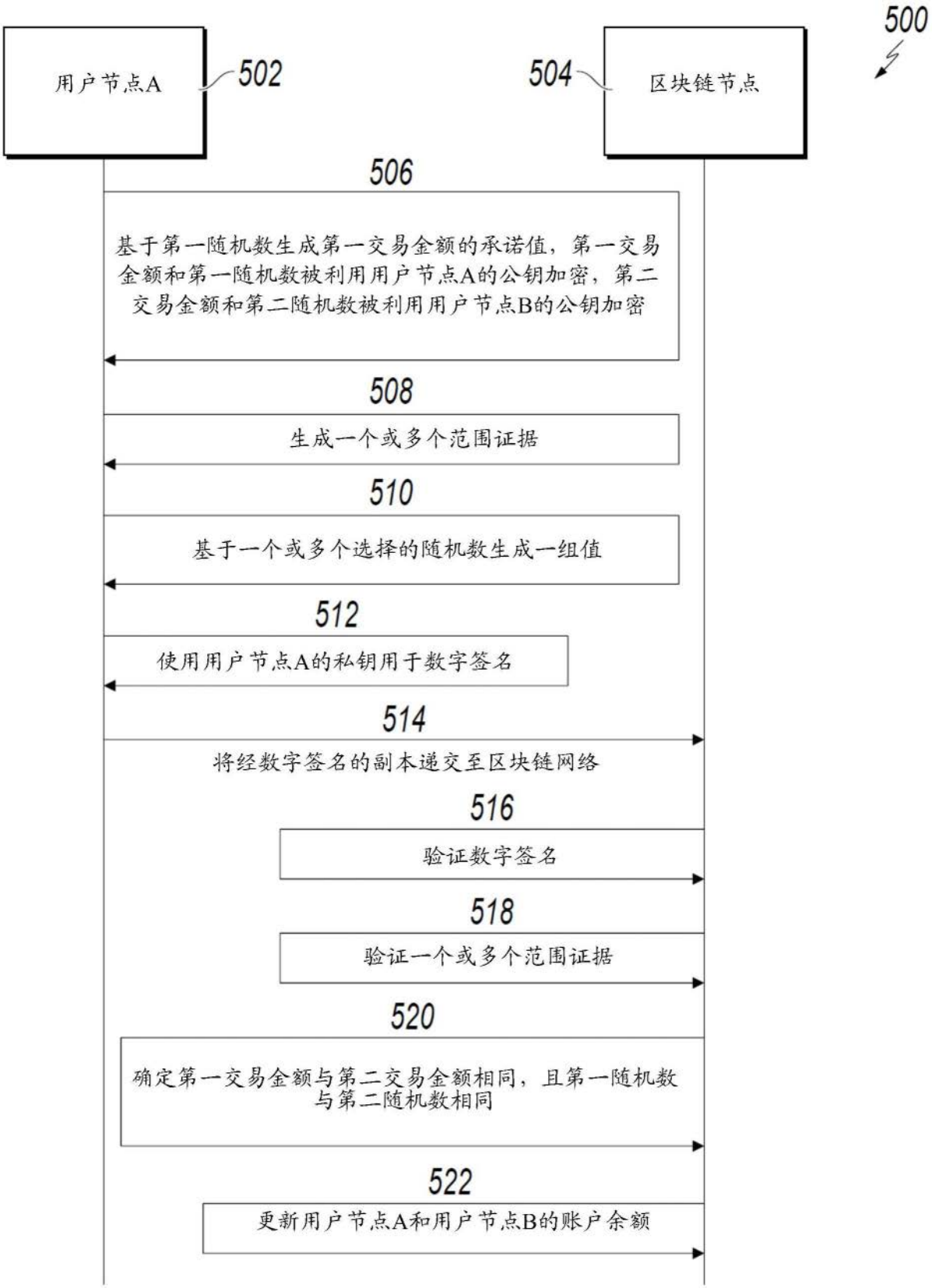

500
用户节点A
502
504
区块链节点
506
基于第一随机数生成第一交易金额的承诺值，第一交易金额和第一随机数被利用用户节点A的公钥加密，第二交易金额和第二随机数被利用用户节点B的公钥加密
508
生成一个或多个范围证据
510
基于一个或多个选择的随机数生成一组值
512
使用用户节点A的私钥用于数字签名
514
将经数字签名的副本递交至区块链网络
516
验证数字签名
518
验证一个或多个范围证据
520
确定第一交易金额与第二交易金额相同，且第一随机数与第二随机数相同
522
更新用户节点A和用户节点B的账户余额

图5

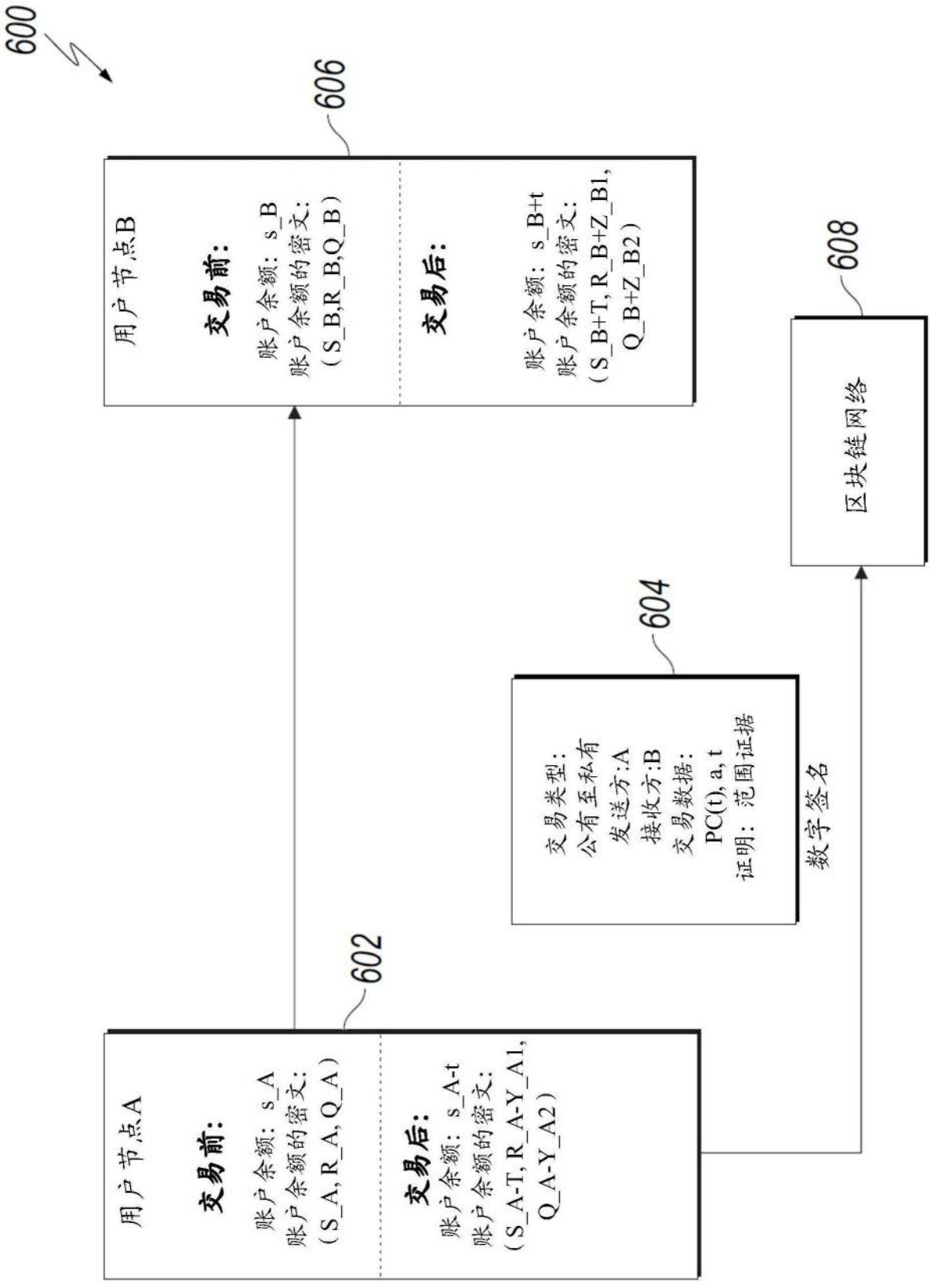

600
606
用户节点B
交易前:
账户余额: s_B
账户余额的密文:
(S_B,R_B,Q_B)
交易后:
账户余额: s_B+t
账户余额的密文:
(S_B+T, R_B+Z_B1,
Q_B+Z_B2)
608
区块链网络
604
交易类型:
公有至私有
发送方:A
接收方:B
交易数据:
PC(t), a, t
证明: 范围证据
数字签名
602
用户节点A
交易前:
账户余额: s_A
账户余额的密文:
(S_A, R_A, Q_A)
交易后:
账户余额: s_A-t
账户余额的密文:
(S_A-T, R_A-Y_A1,
Q_A-Y_A2)

图6

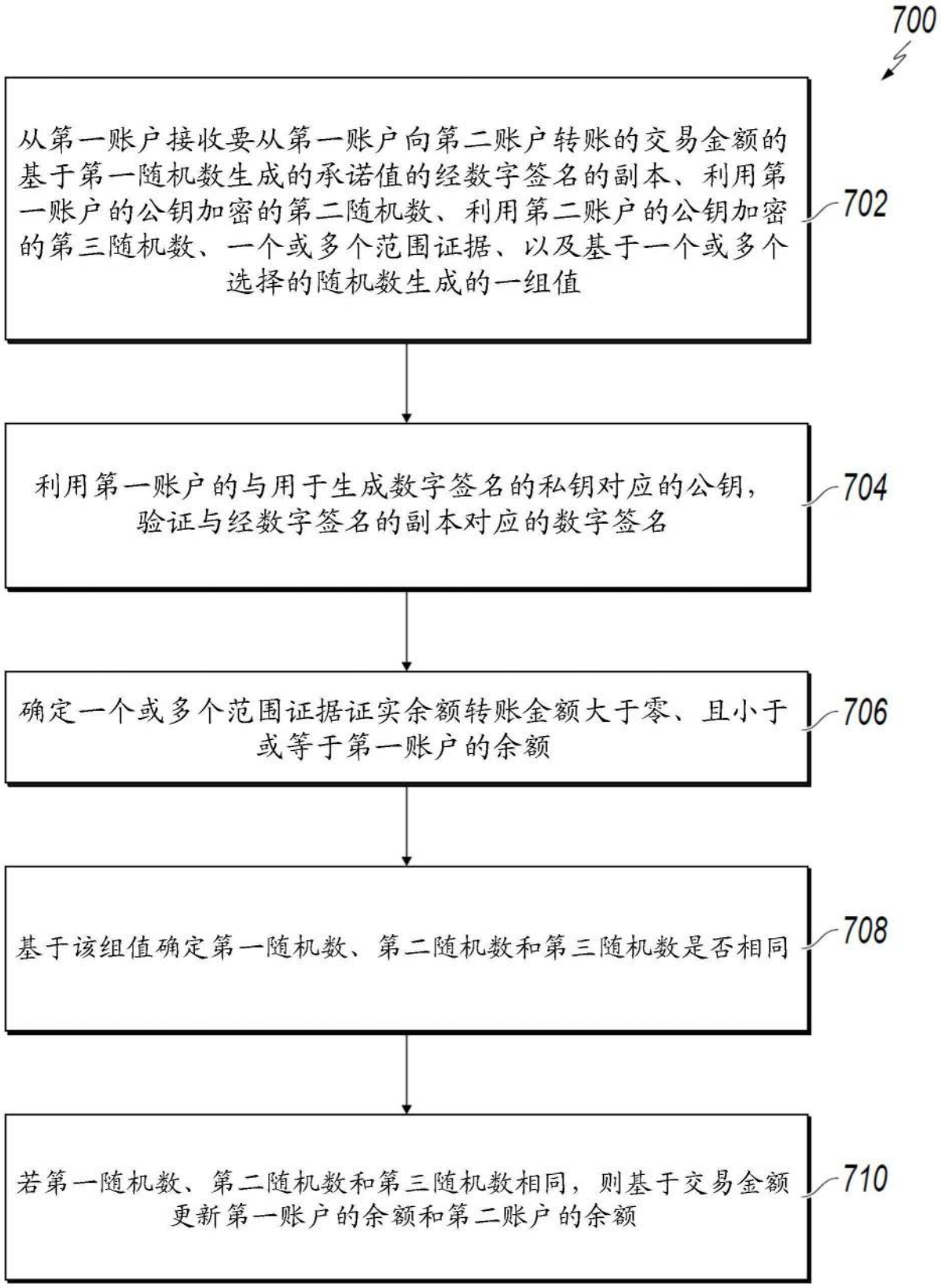

700
从第一账户接收要从第一账户向第二账户转账的交易金额的基于第一随机数生成的承诺值的经数字签名的副本、利用第一账户的公钥加密的第二随机数、利用第二账户的公钥加密的第三随机数、一个或多个范围证据、以及基于一个或多个选择的随机数生成的一组值
702
利用第一账户的与用于生成数字签名的私钥对应的公钥，验证与经数字签名的副本对应的数字签名
704
确定一个或多个范围证据证实余额转账金额大于零、且小于或等于第一账户的余额
706
基于该组值确定第一随机数、第二随机数和第三随机数是否相同
708
若第一随机数、第二随机数和第三随机数相同，则基于交易金额更新第一账户的余额和第二账户的余额
710

图7

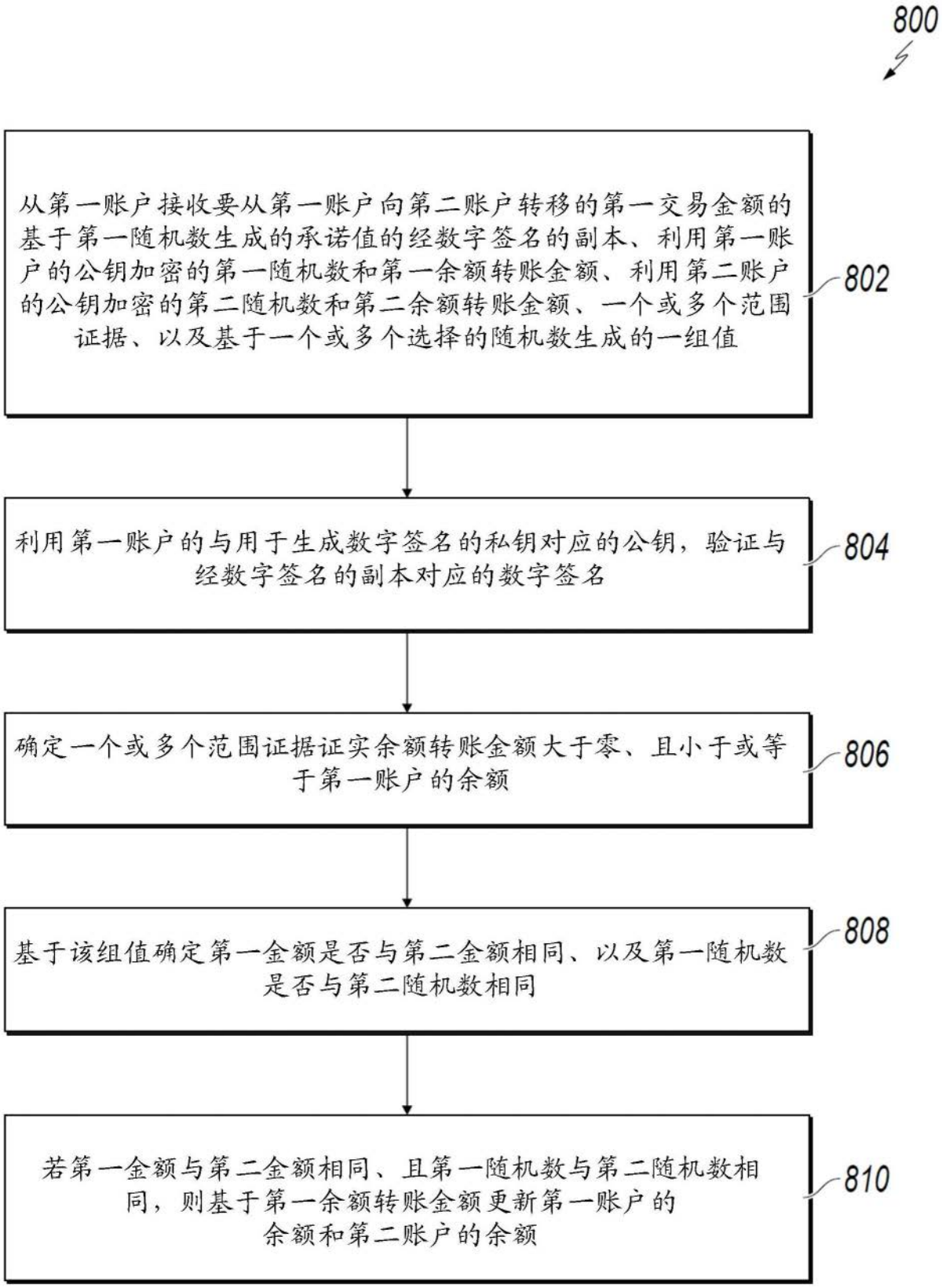

800
从第一账户接收要从第一账户向第二账户转移的第一交易金额的基于第一随机数生成的承诺值的经数字签名的副本、利用第一账户的公钥加密的第一随机数和第一余额转账金额、利用第二账户的公钥加密的第二随机数和第二余额转账金额、一个或多个范围证据、以及基于一个或多个选择的随机数生成的一组值
802
利用第一账户的与用于生成数字签名的私钥对应的公钥，验证与经数字签名的副本对应的数字签名
804
确定一个或多个范围证据证实余额转账金额大于零、且小于或等于第一账户的余额
806
基于该组值确定第一金额是否与第二金额相同、以及第一随机数是否与第二随机数相同
808
若第一金额与第二金额相同、且第一随机数与第二随机数相同，则基于第一余额转账金额更新第一账户的余额和第二账户的余额
810

图8