(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110326013 A
(43)申请公布日 2019.10.11

(21)申请号 201880011524.7

(22)申请日 2018.11.07

(85)PCT国际申请进入国家阶段日
2019.08.12

(86)PCT国际申请的申请数据
PCT/CN2018/114401 2018.11.07

(87)PCT国际申请的公布数据
WO2019/072265 EN 2019.04.18

(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 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
代理人 艾佳

(51)Int.Cl.
G06Q 20/10(2006.01)

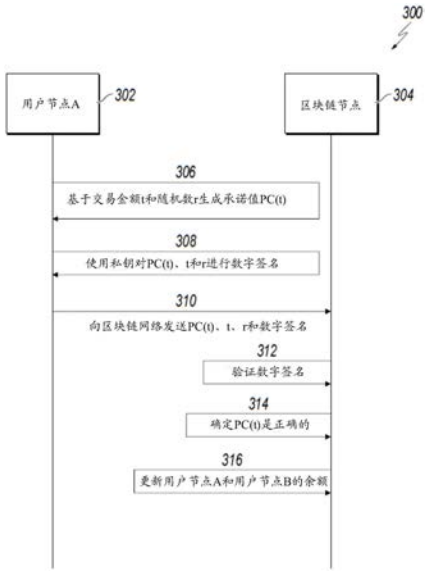
权利要求书1页 说明书8页 附图6页

(54)发明名称

在账户模型下支持公开交易和私有交易的区块链系统

(57)摘要

本公开的实施方式包括:由区块链的共识节点接收交易数据和交易数据的数字签名。交易数据包括承诺值、随机数和交易金额,该交易金额要从第一用户节点的公开账户或私有账户转账至第二用户节点的公开账户或私有账户。共识节点使用第一用户节点的公钥验证交易数据的数字签名。然后,如果基于随机数和承诺方案该承诺值是正确的,并且在转账交易金额之前,交易金额小于或等于第一用户节点的公开账户或私有账户的余额,则确定交易金额是有效的。



CN 110326013 A

1.一种计算机实现的用于基于账户模型验证区块链交易的方法,包括:

由区块链网络的共识节点接收交易数据和所述交易数据的数字签名,其中,所述交易数据包括承诺值、随机数和交易金额,所述交易金额要从第一用户节点的公开账户或私有账户转账至第二用户节点的公开账户或私有账户,所述数字签名是通过使用所述第一用户节点的私钥对所述交易数据进行数字签名而生成的,以及所述承诺值是基于所述随机数和所述交易金额使用承诺方案而生成的;

使用所述第一用户节点的公钥验证所述交易数据的所述数字签名;以及

如果基于所述随机数和所述承诺方案确定所述承诺值是正确的,并且在转账所述交易金额之前,所述交易金额小于或等于所述第一用户节点的公开账户或私有账户的余额,则确定所述交易金额是有效的。

2.如权利要求1所述的计算机实现的方法,其中,

所述公开账户具有能够由所述共识节点查看的公开余额,

所述私有账户具有能够使用相应用户节点的私钥查看的私有余额。

3.如权利要求1所述的计算机实现的方法,其中,所述交易金额是从与所述第一用户节点相关联的公开账户至与所述第二用户节点相关联的私有账户的。

4.如权利要求1所述的计算机实现的方法,其中,所述交易金额是从所述第一用户节点的私有账户至所述第二用户节点的公开账户的,并且所述方法还包括:

从所述第一用户节点接收范围证据,所述范围证据证明所述交易金额小于或等于所述第一用户节点的私有账户的余额;以及

如果基于所述范围证据确定所述交易金额小于或等于所述第一用户节点的私有账户的余额,则确定所述转账有效。

5.如权利要求2所述的计算机实现的方法,还包括:

如果所述转账有效,则基于所述交易金额更新所述第一用户节点的公开账户或私有账户的余额,以及所述第二用户节点的公开账户或私有账户的余额。

6.如权利要求5所述的计算机实现的方法,其中,基于使用所述承诺方案生成的所述交易金额的承诺值和所述私有账户的余额的承诺,更新所述私有账户的余额。

7.如权利要求1所述的计算机实现的方法,其中,所述承诺方案是同态的。

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中一个或多个所述的方法执行操作。

9.一种系统,包括:

计算设备;和

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中一个或多个所述的方法执行操作。

在账户模型下支持公开交易和私有交易的区块链系统

背景技术

[0001] 区块链网络，也可以被称为区块链系统、共识网络、分布式账本系统(DLS)网络或区块链，使得参与的实体能够安全地并且不可篡改地存储数据。区块链可以被描述为交易的账本，并且区块链的多个副本跨区块链网络存储。区块链的示例性类型可包括公有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，并开放参与共识处理。私有区块链针对特定实体提供，该实体集中控制读写权限。

[0002] 区块链用在加密货币网络中，加密货币网络使得参与者能够使用加密货币进行交易以买/卖物品和/或服务。通用的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后续交易中被花费的新输出。跟踪用户的未被花费的交易，并计算未被花费的交易的总和作为该用户拥有的用于花费的余额。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其大于或等于交易金额。这与传统银行业务相当。

[0003] 区块链包括一系列区块，每个区块包含在网络中执行的一个或多个交易。每个区块可被类比为账本中的一页，而区块链本身是账本的完整副本。各个交易被确认并被添加到区块，该区块被添加到区块链。区块链的副本是遍布网络中的节点复制的。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，实施加密技术。

发明内容

[0004] 本公开的实施方式包括：计算机实现的用于在区块链网络的账户余额模型下保护公开和私有交易数据的隐私的方法。更具体地，本公开的实施方式涉及在区块链网络内的账户余额模型下实现私有交易和公开交易。以这种方式，并且如本文进一步详细描述的，用户可以自由地选择每个交易是区块链网络内的公开交易还是私有交易。

[0005] 在一些实施方式中，动作包括：区块链网络的共识节点接收交易数据和交易数据的数字签名，其中，所述交易数据包括承诺值、随机数和交易金额，所述交易金额将要从第一用户节点的公开账户或私有账户转账至第二用户节点的公开账户或私有账户，所述数字签名是通过使用所述第一用户节点的私钥对所述交易数据进行数字签名生成的，所述承诺值是基于所述随机数和所述交易金额使用承诺方案生成的；使用所述第一用户节点的公钥验证所述交易数据的所述数字签名；以及如果基于所述随机数和所述承诺方案所述承诺值是正确的，并且在转账所述交易金额之前，所述交易金额小于或等于所述第一用户节点的公开账户或私有账户的余额，则确定所述交易金额是有效的。其他实施方式包括相应的系统、装置和计算机程序，所述计算机程序编码在计算机存储设备上并被配置成执行所述方法的操作。

[0006] 这些和其它实施方式可以各自可选地包括以下特征中的一个或多个：

[0007] 第一特征，可与以下特征中的任何特征组合，其中，所述公开账户具有可由所述共

识节点查看的公开余额,并且所述私有账户具有可使用相应用户节点的私钥查看的私有余额。

[0008] 第二特征,可与先前或以下特征中的任何特征组合,其中,所述交易金额是从与所述第一用户节点相关联的公开账户至与所述第二用户节点相关联的私有账户的。

[0009] 第三特征,可与先前或以下特征中的任何特征组合,其中,所述交易金额是从所述第一用户节点的私有账户至所述第二用户节点的公开账户的,并且所述方法还包括:从所述第一用户节点接收范围证据,所述范围证据证明所述交易金额小于或等于所述第一用户节点的私有账户的余额;并且如果基于所述范围证据所述交易金额小于或等于所述第一用户节点的私有账户的余额,则确定所述转账有效。

[0010] 第四特征,可与先前或以下特征中的任何特征组合,还包括:如果所述转账有效,则基于所述交易金额更新所述第一用户节点的公开账户或私有账户的余额,以及更新所述第二用户节点的公开账户或私有账户的余额。

[0011] 第五特征,可与先前或以下特征中的任何特征组合,其中,基于所述交易金额的所述承诺值和使用所述承诺方案生成的所述私有账户的余额的承诺,更新所述私有账户的余额。

[0012] 第六特征,可与先前或以下特征中的任何特征组合,其中,所述承诺方案是同态的。

[0013] 本公开还提供了一种用于实现本文提供的方法的系统。该系统包括一个或多个处理器以及耦接到该一个或多个处理器且其上存储有指令的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,使得所述一个或多个处理器按照本文提供的方法的实施方式来执行操作。

[0014] 应当理解,根据本公开的方法可以包括本文所述的方面和特征的任何组合。也就是说,根据本公开的方法不限于本文具体描述的方面和特征的组合,而还包括所提供的方面和特征的任何组合。

[0015] 以下在附图和说明书中阐述了本公开的一个或多个实施方式的细节。从说明书和附图以及从权利要求书来看,本公开的其它特征和优点将是显而易见的。

附图说明

[0016] 图1描绘了可以用于执行本公开实施方式的示例性环境。

[0017] 图2描绘了根据本公开实施方式的示例性概念架构。

[0018] 图3描绘了根据本公开实施方式的区块链交易的示例性验证处理。

[0019] 图4描绘了根据本公开实施方式的从公开账户至私有账户的示例性区块链交易。

[0020] 图5描绘了根据本公开实施方式的从私有账户至公开账户的示例性区块链交易。

[0021] 图6描绘了可根据本公开实施方式执行的示例性方法。

[0022] 在各个附图中,相同的附图标记表示相同的元件。

具体实施方式

[0023] 本公开的实施方式包括:计算机实现的用于在区块链网络的账户余额模型(在此也称为账户模型)下保护公开和私有交易数据的隐私的方法。更具体地说,本公开的实施方

式涉及在区块链网络内的账户余额模型下实现私有交易和公开交易。以这种方式，并且如本文进一步详细描述的，用户可以自由地选择每个交易是区块链网络内的公开交易还是私有交易。在一些实施方式中，动作包括：区块链网络的共识节点接收交易数据和交易数据的数字签名，其中，所述交易数据包括承诺值、随机数和交易金额，该交易金额要从第一用户节点的公开账户或私有账户转账至第二用户节点的公开账户或私有账户，所述数字签名是通过使用所述第一用户节点的私钥对所述交易数据进行数字签名生成的，所述承诺值是基于随机数和交易金额使用承诺方案生成的；使用第一用户节点的公钥验证交易数据的数字签名；以及如果基于所述随机数和所述承诺方案所述承诺值是正确的，并且在转账所述交易金额之前，所述交易金额小于或等于第一用户节点的公开账户或私有账户的余额，则确定交易金额是有效的。

[0024] 为本公开的实施方式提供进一步的背景，并且如上所述，区块链网络也可以称为共识网络(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。

[0025] 在公有区块链中，共识处理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公有区块链，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)必须按顺序对每个区块签名，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)。尽管术语“区块链”通常指代比特币网络，但是，如本文所使用的，在不特指比特币网络的情况下，区块链通常指分布式账本。

[0026] 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，这是因为该区块链账本跨所有节点复制的。也即，所有节点相对于区块链都处于完全共识状态。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)。

[0027] 鉴于上述背景，本文更详细地描述了本公开的实施方式。更具体地，且如上所述，本公开的实施方式涉及在区块链网络内的账户余额模型下实现私有交易和公开交易。以这种方式，并且如本文进一步详细描述的，用户可以自由地选择每个交易是区块链网络内的公开交易还是私有交易。

[0028] 根据本公开的实施方式，基于账户模型的账户结构实现公开账户之间的交易、私有账户之间的交易以及公开账户和私有账户之间的交易。针对不同的账户类型可以实施适当的隐私保护方案。以这种方式，用户(例如，网络中的节点)可基于隐私偏好选择是使用公开账户还是私有账户来执行交易。

[0029] 公开账户可以具有可由共识节点查看的账户余额。私有账户可以具有可使用账户的所有者(用户)的私钥查看的账户余额。可以使用同态加密来加密私有账户余额，或者通过同态承诺方案来承诺。这样，私有账户余额不能由区块链网络中的其他节点确定。还可基于承诺方案隐藏进出私有账户的交易金额，以基于同态加密更新私有账户余额。

[0030] 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、108和网络110。在一些示例中，网络110包括局域网、广域网(WAN)、因特网或其组合，并且连接网络站点、用户设备(LAN)例如，计算设备)和后端系统。在一些示例中，网络110可以通过有线和/或无线通信链路被访问。

[0031] 在所描述的示例中，计算系统106、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电话。在一些示例中，计算系统106、108承载一个或多个由计算机实施的服务，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它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它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，并且计算系统106、108分别提供参与至公有区块链102中的第一实体和第二实体的节点。

[0032] 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。在所描述的示例中，实体层202包括三个实体，实体1(E1)、实体2(E2)和实体3(E3)，每个实体具有对应的交易管理系统208。

[0033] 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的区块链或DLS接口210。在一些示例中，各个交易管理系统208利用通信协议(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DLS接口210通信。在一些示例中，每个DLS接口210提供各个交易管理系统208与区块链层206之间的通信连接。更具体地，每个DLS接口210使得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，DLS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，DLS接口210“承载”用于各个交易管理系统208的区块链节点。例如，DLS接口210提供用于访问区块链网络212的应用编程接口(API)。

[0034] 如本文所述，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。尽管示意性地描绘了单个区块链216，但是在区块链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存储与在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。

[0035] 本公开公开了可在区块链网络内的账户余额模型下、实现基于承诺方案执行私有交易和公开交易的方法。以这种方式，用户可以自由地选择每个交易或用于交易的账户是公开的还是私有的。

[0036] 图3描绘了示出根据本公开实施方式的区块链交易的示例性验证处理300的泳道图。为了说明示例性验证处理300，假定由用户节点A 302向用户节点B(图3中未示出)执行资金转账交易，并且该交易由用户节点A 302提交到区块链节点304以进行验证。用户节点A 302和用户节点B各自可以包括公开账户和私有账户。公开账户的余额可以被区块链网络中的所有节点查看。私有账户的余额仅可由账户拥有者(用户)使用私钥才能查看。根据本公开的实施方式，用户节点可以选择是使用公开账户还是私有账户来公开地还是私下地执行

交易。

[0037] 在306,用户节点A 302基于交易金额t和随机数r生成承诺值。该承诺值可以通过同态承诺方案来生成。示例性承诺方案包括但不限于佩德森承诺(Pedersen Commitment,PC)。尽管本文参考PC进一步详细描述了本公开的实施方式,但是可以预期,可以使用任何适当的承诺方案来实现本公开的实施方式。

[0038] 例如,使用PC,承诺值是可表示为PC(t)＝rG+tH的密文,其中G和H可以是椭圆曲线的生成元,PC(t)是曲线点的标量乘法,t是被承诺的值。PC承诺方案具有同态性,即,$PC(t_1)+PC(t_2)=PC(t_1+t_2)$。密文PC(t)的持有者可以通过使用随机数r来验证交易金额t。在308,用户节点A 302使用私钥对承诺值PC(t)、交易金额t和随机数r进行数字签名。在310,用户节点A302向区块链节点304提交承诺值PC(t)、交易金额t、随机数r和数字签名。

[0039] 在一些实施方式中,可以从用户节点A 302的私有账户发送交易金额t。对于私有账户,该账户是否具有足够的余额来转账交易金额t不能由区块链的其他节点直接验证。在这种情况下,用户节点A 302可以生成一个或多个范围证据,以示出交易金额t大于或等于零、且小于或等于用户节点A 302的私有账户的余额。

[0040] 在312,区块链节点304使用用户节点A 302的公钥来验证承诺值PC(r,t)、交易金额t和随机数r的数字签名。如果数字签名正确,则示例性验证处理300进行到314。

[0041] 在314,区块链节点304验证承诺值PC(t)是否正确以及交易金额t是否有效。为了验证PC(t)是否正确,可以使用接收到的随机数r和交易金额t来生成表示为PC'(r,t)的PC。如果PC'(r,t)等于所述接收到的承诺PC(r,t),则承诺PC(r,t)被验证为交易金额t的正确承诺。在一些实施方式中,如果交易金额t大于或等于零、且小于或等于用户节点A 302的账户的账户余额,则区块链节点304可以验证交易金额t是有效的,其中,该交易金额是基于一个或多个范围证据从用户节点A 302的账户转账的。

[0042] 在316,区块链节点304更新区块链上的用户节点A 302和用户节点B的余额,并将该区块链广播到区块链网络中的其余节点。对于公开账户交易,基于交易类型,该交易金额可以从公开账户的余额中直接减去或者直接添加到公开账户的余额中。对于私有账户交易,交易金额t可以使用为PC(t)的PC被承诺,并从私有账户余额s中减去或添加到私有账户余额s中,该私有账户余额s也使用为PC(s)的PC被承诺。因为PC是同态的,因此PC(s)±PC(t)＝PC(s±t)。本文中参考图4和图5更详细地描述更新公开账户余额和私有账户余额的细节。

[0043] 图4描绘了示出根据本公开实施方式的从公开账户至私有账户的示例性交易400的框图。如示例性交易400所示,在交易之前,用户节点A 402具有公开账户余额u,以及使用PC被承诺并被表示为PC(v)的私有账户余额v。用户节点B 406具有公开账户余额x,并且私有账户余额y使用PC被承诺并被表示为PC(y)。用户节点A 402可以通过向区块链网络408发送承诺值PC(t)、交易金额t和对应于该承诺值的随机数a的经数字签名的副本,从其公开账户向用户节点B 406的私有账户提交交易。在使用诸如图3的示例性处理300的验证处理验证了交易金额t的承诺值PC(t)之后,可以更新用户节点A 402和用户节点B 406的账户。在由区块链网络408验证交易之后,从用户节点A 402的公开账户中减去交易金额t,并将其添加到用户节点B 406的私有账户。在交易之后,用户节点A 400具有公开账户余额u-t和私有账户余额PC(v)。用户节点B 406具有公开账户余额x和私有账户余额PC(y+t)。

[0044] 图5描绘了示出根据本公开实施方式的从私有账户至公开账户的示例性交易500的框图。如示例性交易500中所示，在交易之前，用户节点A 502具有公开账户余额u，并且私有账户余额v使用PC被承诺并被表示为PC(v)。用户节点B 506具有公开账户余额x，并且私有账户余额y使用PC被承诺并被表示为PC(y)。用户节点A 502可以通过发送承诺值PC(t)、交易金额t、对应于该承诺值的随机数a以及一个或多个范围证据的经数字签名的副本，从其私有账户向用户节点B 506的公开账户提交交易。该一个或多个范围证据可用于向区块链网络508证明0≤t≤v。在使用诸如图3的示例性处理300的验证处理验证了交易金额t的承诺值PC(t)之后，可以更新用户节点A 502和用户节点B 506的账户。在由区块链网络508验证交易之后，从用户节点A的私有账户减去交易金额t，并将其添加到用户节点B 506的公开账户。在交易之后，用户节点A 502具有公开账户余额u和私有账户余额PC(v-t)。用户节点B 504具有公开账户余额x+t和私有账户余额PC(y)。

[0045] 图6描绘了可以根据本公开实施方式执行的示例性方法600。为了清楚地呈现，以下描述结合本说明书中的其他附图的上下文一般地描述了示例性方法600。然而，将理解，示例性方法600可由例如任何适当的系统、环境、软件和硬件，或者系统、环境、软件和硬件的组合来执行。在一些实施方式中，示例性方法600的各个步骤可以并行地、组合地、循环地或以任何顺序运行。

[0046] 在602，区块链网络的共识节点接收交易数据和该交易数据的数字签名。在一些实施方式中，所述交易数据包括承诺值、随机数和交易金额，该交易金额要从第一用户节点的公开账户或私有账户转账至第二用户节点的公开账户或私有账户。数字签名是通过使用第一用户节点的私钥对交易数据进行数字签名而生成的。承诺值是基于随机数和交易金额使用承诺方案而生成的。在一些实施方式中，承诺方案是同态的。在一些实施方式中，交易金额是从与第一用户节点相关联的公开账户至与第二用户节点相关联的私有账户的。在一些实施方式中，交易金额是从与第一用户节点相关联的私有账户至第二用户节点的公开账户的。在这样的情况下，共识节点还可以从第一用户节点接收范围证据，该范围证据证明交易金额小于或等于第一用户节点的私有账户的余额。

[0047] 在604，共识节点使用第一用户节点的公钥验证交易数据的数字签名。

[0048] 在606，如果基于所述随机数和所述承诺方案所述承诺值是正确的，则共识节点确定交易金额是有效的。在转账交易金额之前，共识节点还确定交易金额小于或等于第一用户节点的公开账户或私有账户的余额。在一些实施方式中，交易金额是从第一用户节点的私有账户至第二用户节点的公开账户的。在这样的情况下，确定余额转账有效还包括基于范围证据确定交易金额是否小于或等于与第一用户节点相关联的私有账户的余额。

[0049] 在一些实施方式中，示例性方法600还可以包括更新与第一用户节点相关联的公开账户或私有账户的余额，以及与第二用户节点相关联的公开账户或私有账户的余额。如果交易金额有效，则可以基于该交易金额执行更新。在一些实施方式中，基于交易金额的承诺值和使用承诺方案生成的私有账户的余额的承诺，更新私有账户的余额。

[0050] 本文中描述的主题的实施方式可被实施，以便实现特定的优点或技术效果。例如，本公开的实施方式允许区块链网络支持公开账户之间的交易、私有账户之间的交易以及公开账户和私有账户之间的交易。这样，无论账户类型如何，都可以实现适当的隐私保护，因此，区块链网络的用户节点可基于隐私偏好灵活地选择从其公开账户或私有账户发送和接

收资金。

[0051] 所描述的方法允许增强各种移动计算设备的账户/数据安全性。可以基于承诺方案来承诺私有账户的余额。这样，可基于承诺验证私有账户的余额，而不显露账户的实际账户余额。可基于该承诺方案承诺进出私有账户的交易金额，以在交易后更新私有账户，而不显露转账的实际金额。以这种方式，提供了对私有账户交易的安全性的更多控制。

[0052] 所描述的方法可以通过区块链的有效更新来确保计算机资源的有效使用(例如，处理周期、网络带宽和存储器使用)。通过更简单的共识处理，可以更快且更安全地进行账户操作。

[0053] 本文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。

[0054] 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。

[0055] 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。

[0056] 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。

[0057] 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。

[0058] 本公开的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。

[0059] 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。

[0060] 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)。

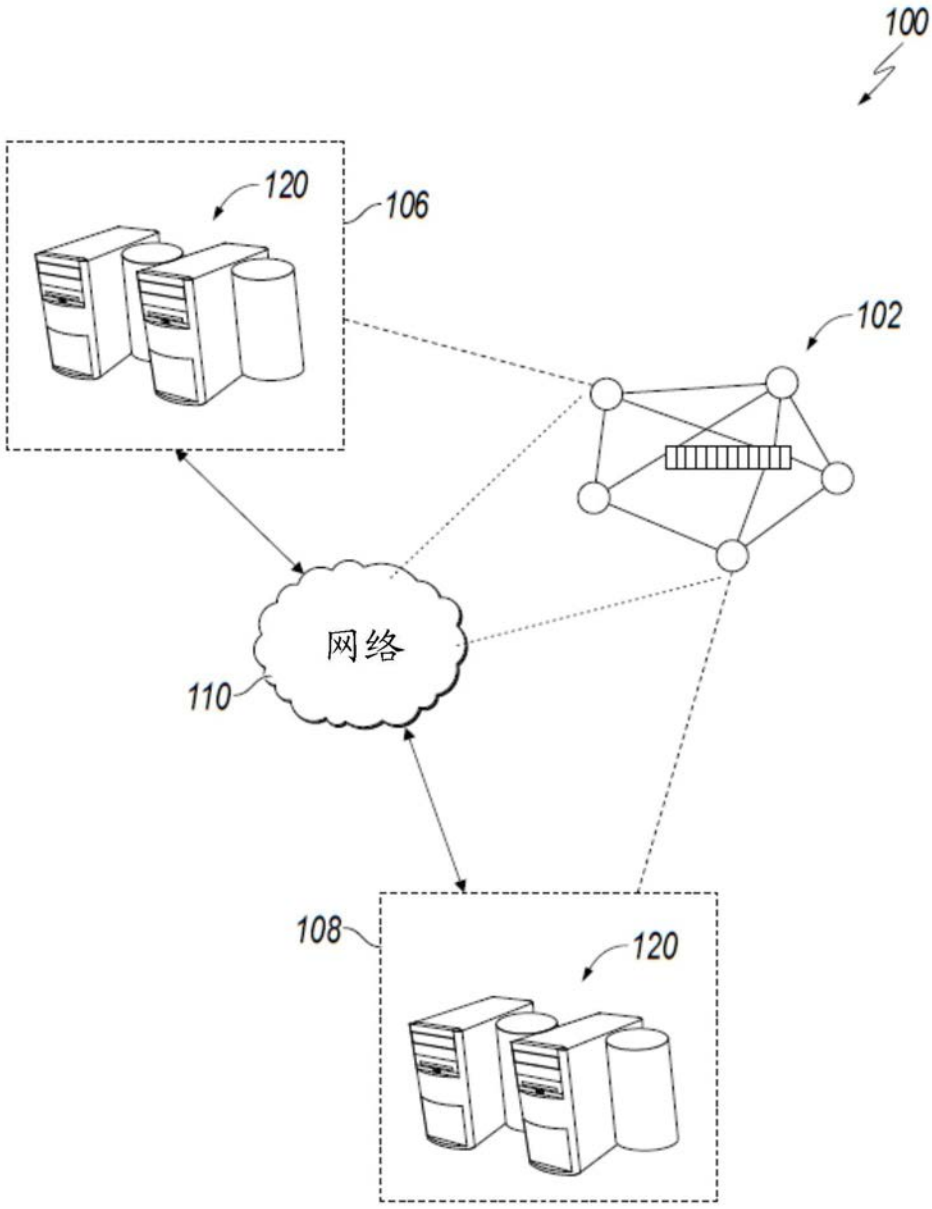


图1

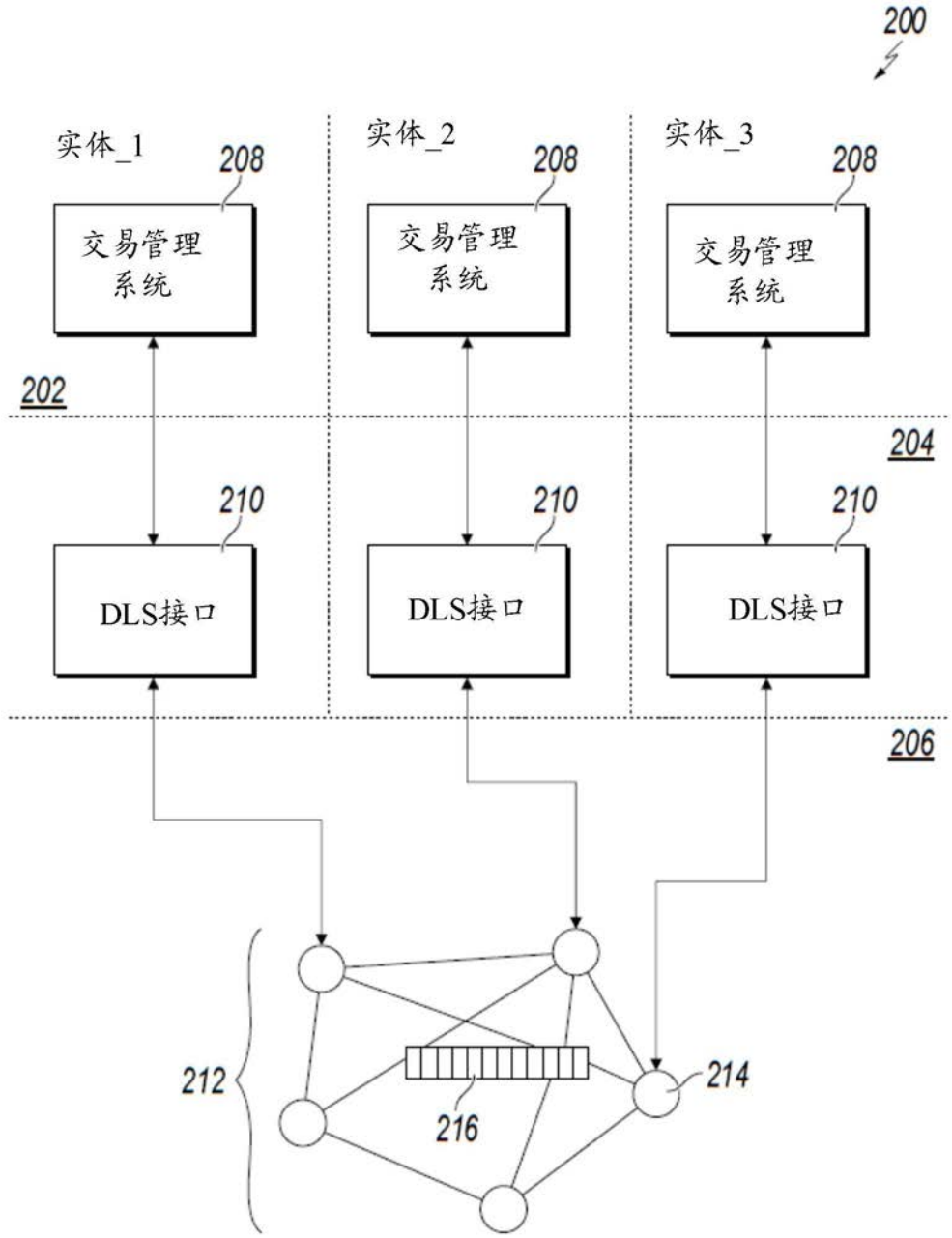

200
实体_1
208
交易管理系统
实体_2
208
交易管理系统
实体_3
208
交易管理系统
202
204
210
DLS接口
210
DLS接口
210
DLS接口
206
212
216
214

图2

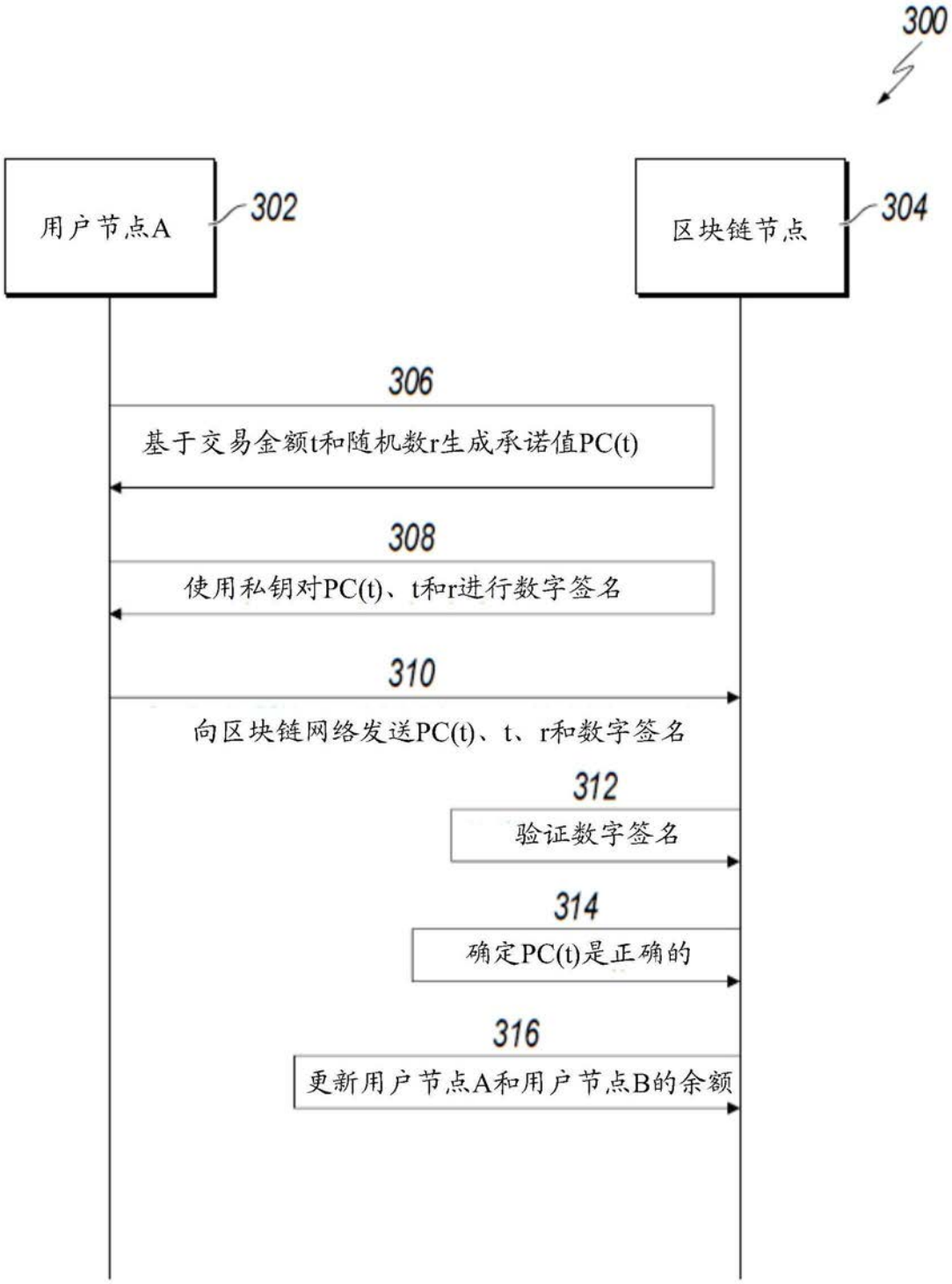

300
用户节点A
302
区块链节点
304
306
基于交易金额t和随机数r生成承诺值PC(t)
308
使用私钥对PC(t)、t和r进行数字签名
310
向区块链网络发送PC(t)、t、r和数字签名
312
验证数字签名
314
确定PC(t)是正确的
316
更新用户节点A和用户节点B的余额

图3

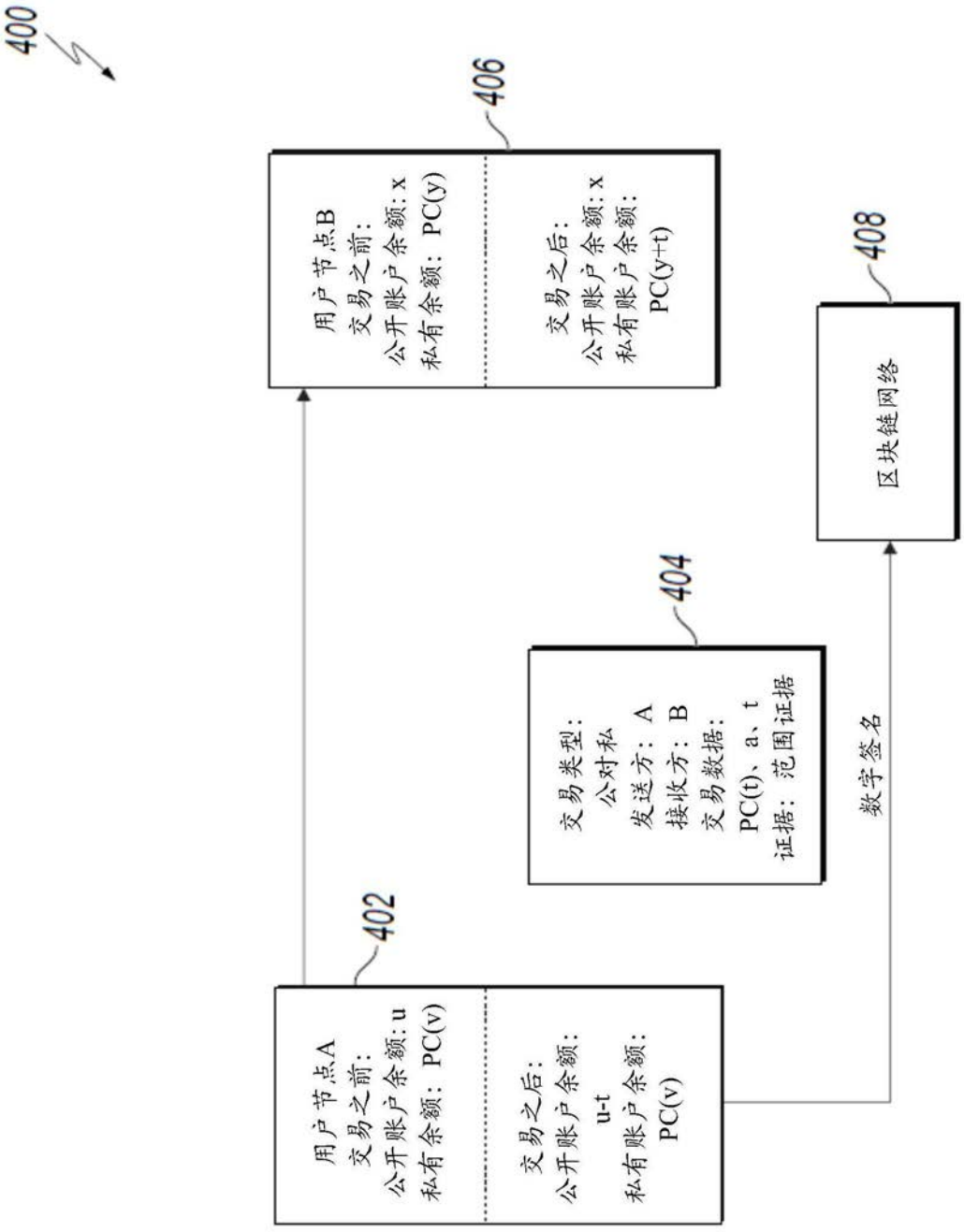

400
406
用户节点B
交易之前:
公开账户余额: x
私有余额: PC(y)
交易之后:
公开账户余额: x
私有账户余额:
PC(y+t)
408
区块链网络
404
交易类型:
公对私
发送方: A
接收方: B
交易数据:
PC(t)、a、t
证据: 范围证据
数字签名
402
用户节点A
交易之前:
公开账户余额: u
私有余额: PC(v)
交易之后:
公开账户余额:
u-t
私有账户余额:
PC(v)

图4

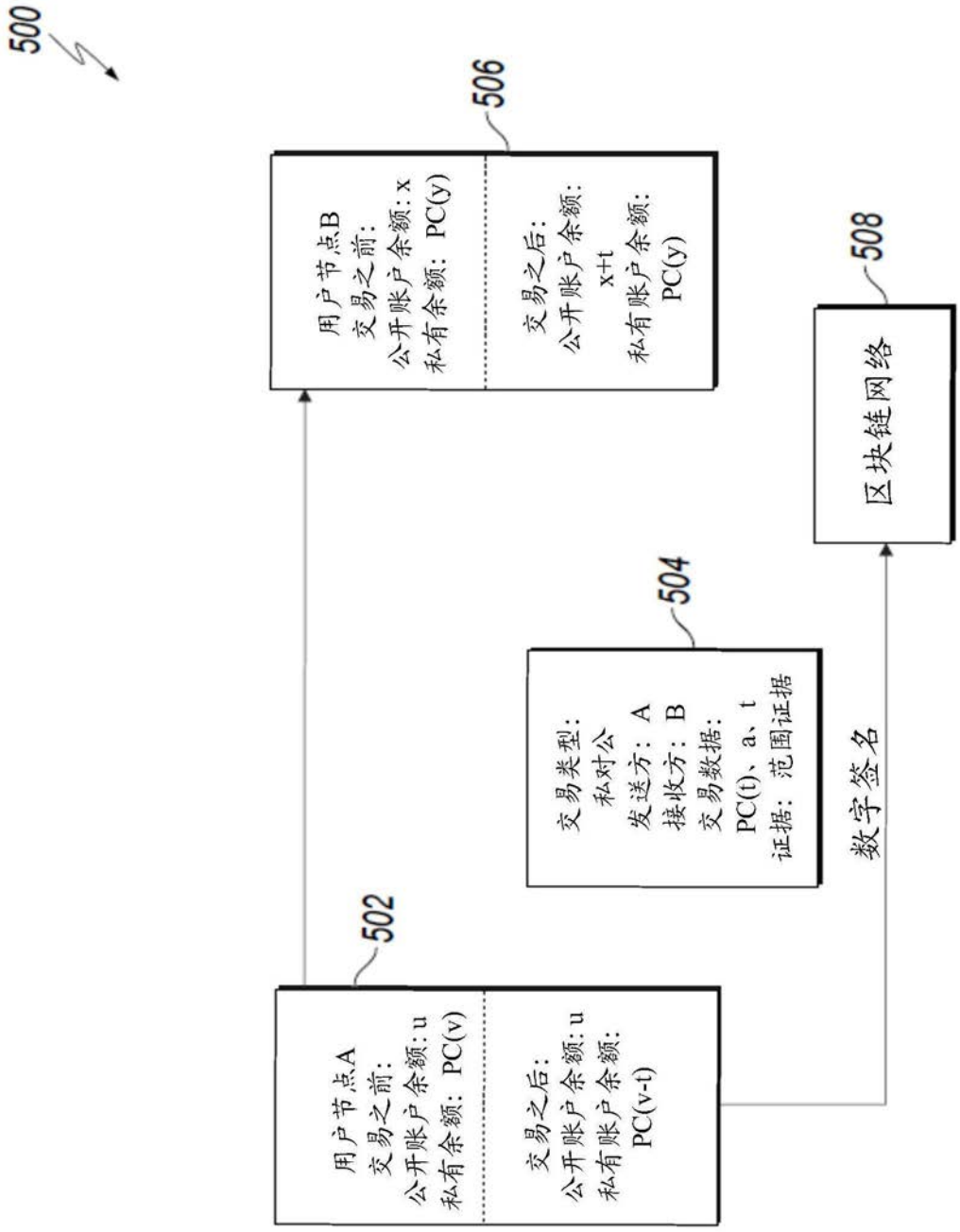

500
506
用户节点B
交易之前:
公开账户余额: x
私有余额: PC(y)
交易之后:
公开账户余额:
x+t
私有账户余额:
PC(y)
508
区块链网络
504
交易类型:
私对公
发送方: A
接收方: B
交易数据:
PC(t)、a、t
证据: 范围证据
数字签名
502
用户节点A
交易之前:
公开账户余额: u
私有余额: PC(v)
交易之后:
公开账户余额: u
私有账户余额:
PC(v-t)

图5

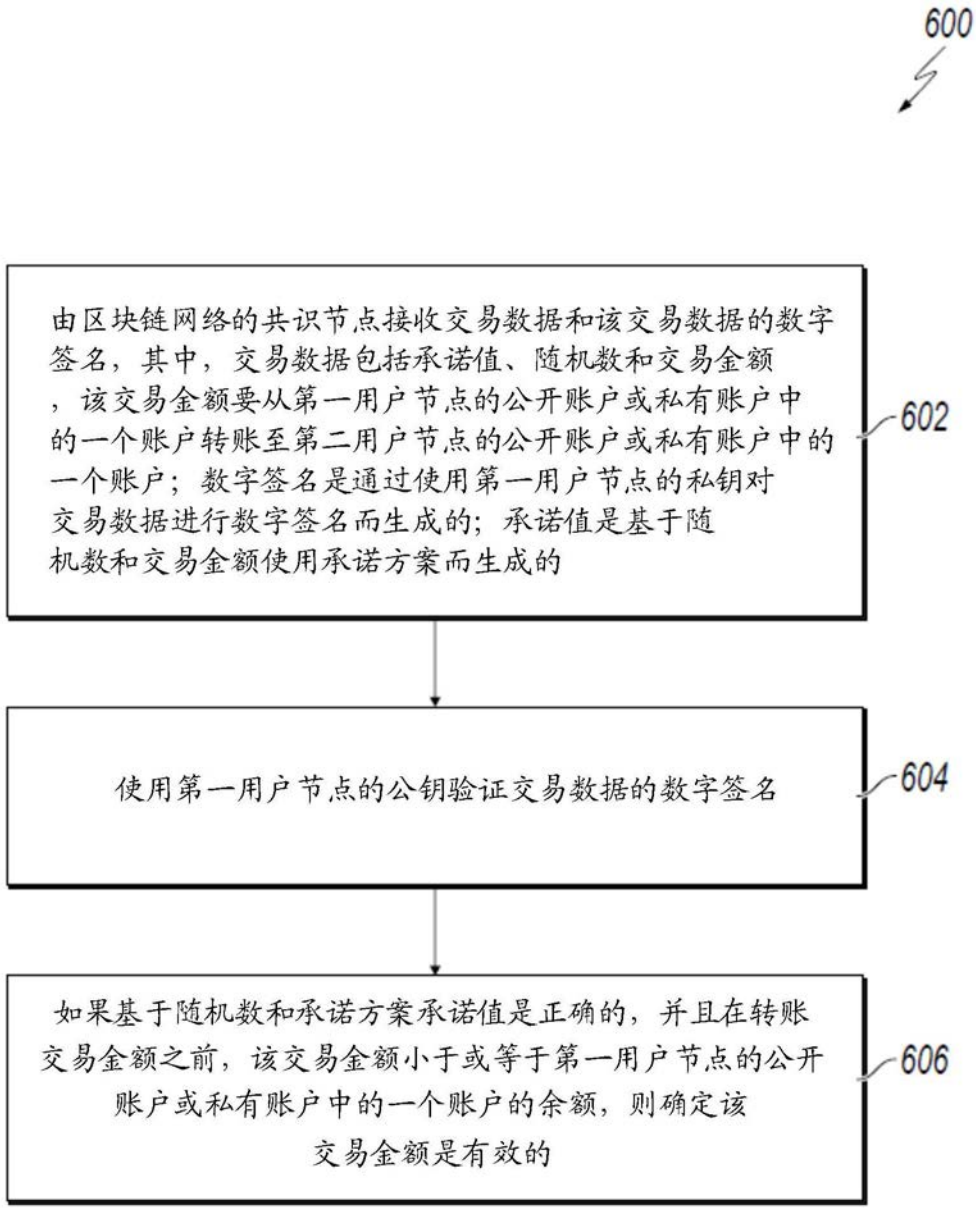

600
由区块链网络的共识节点接收交易数据和该交易数据的数字签名，其中，交易数据包括承诺值、随机数和交易金额，该交易金额要从第一用户节点的公开账户或私有账户中的一个账户转账至第二用户节点的公开账户或私有账户中的一个账户；数字签名是通过使用第一用户节点的私钥对交易数据进行数字签名而生成的；承诺值是基于随机数和交易金额使用承诺方案而生成的
602
使用第一用户节点的公钥验证交易数据的数字签名
604
如果基于随机数和承诺方案承诺值是正确的，并且在转账交易金额之前，该交易金额小于或等于第一用户节点的公开账户或私有账户中的一个账户的余额，则确定该交易金额是有效的
606

图6