(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 110998580 A
(43)申请公布日 2020.04.10

(21)申请号 201980003360.8

(22)申请日 2019.04.29

(85)PCT国际申请进入国家阶段日
2019.12.31

(86)PCT国际申请的申请数据
PCT/CN2019/084941 2019.04.29

(87)PCT国际申请的公布数据
WO2019/137566 EN 2019.07.18

(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 李艳鹏

(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.
G06F 21/60(2006.01)

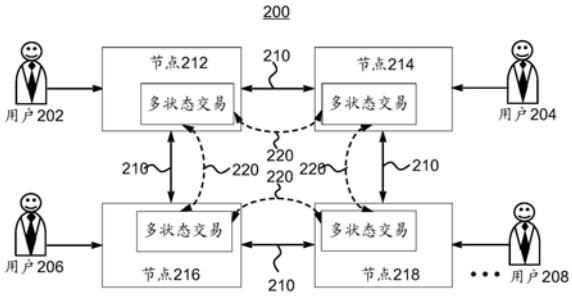
权利要求书2页 说明书10页 附图5页

(54)发明名称

在区块链系统中确认交易有效性的方法和设备

(57)摘要

这里公开了在区块链系统中确认交易有效性的方法、设备和装置，包括存储在计算机可读介质上的计算机程序。所述方法之一包括：验证所述交易的第一部分签名；验证所述交易的第二部分签名；以及响应于确定基于所述第一部分签名和所述第二部分签名的累积签名分数达到签名阈值，确认所述交易有效。



CN 110998580 A

1.一种计算机实现的用于在区块链系统中确认交易有效性的方法,所述方法包括:

验证所述交易的第一部分签名;

验证所述交易的第二部分签名;以及

响应于确定基于所述第一部分签名和所述第二部分签名的累积签名分数达到签名阈值,确认所述交易有效。

2.如权利要求1所述的方法,还包括:

提供所述交易的所述第一部分签名;以及

在所述区块链系统中广播所述第一部分签名。

3.如权利要求2所述的方法,还包括:

生成所述交易的哈希值;以及

利用私钥对所生成的所述哈希值进行加密,以生成所述第一部分签名。

4.如前述任一权利要求所述的方法,还包括:

对所述第一部分签名进行解密以获得第一哈希值;

生成所述交易的第二哈希值;以及

如果所获得的所述第一哈希值与所生成的所述第二哈希值匹配,则确定所述第一部分签名有效。

5.如权利要求4所述的方法,还包括:

如果所获得的所述第一哈希值与所生成的所述第二哈希值不匹配,则确定所述第一部分签名无效。

6.如前述任一权利要求所述的方法,还包括:

当所述累积签名分数等于或大于预定阈值权重值时,确定所述累积签名分数达到所述签名阈值。

7.如前述任一权利要求所述的方法,还包括:

通过确定与多个部分签名分别对应的权重值的和,获得所述累积签名分数。

8.如权利要求1-5中任一项所述的方法,还包括:

当所述区块链系统中提供部分签名的节点的数量等于或大于预定阈值数时,确定所述累积签名分数达到所述签名阈值。

9.如前述任一权利要求所述的方法,其中,所述第一部分签名和所述第二部分签名由所述区块链系统中的第一节点提供。

10.如权利要求1-8中任一项所述的方法,其中,

所述第一部分签名由所述区块链系统中的第一节点提供,以及

所述第二部分签名由所述区块链系统中的第二节点提供。

11.如权利要求10所述的方法,还包括:

所述第一节点基于传输控制协议/互联网协议TCP/IP与所述第二节点通信。

12.如权利要求10-11中任一项所述的方法,还包括:

所述第一节点基于传输层安全/安全套接层TLS/SSL协议与所述第二节点通信。

13.如权利要求10-12中任一项所述的方法,还包括:

所述区块链系统中的第三节点提供所述交易的第三部分签名;

所述第三节点在所述区块链系统中广播所述第三部分签名;

所述区块链系统中的一个或多个其他节点验证所述交易的所述第三部分签名;以及

由不同的节点迭代对另一部分签名的所述提供、所述广播和所述验证,直到所述累积签名分数达到所述签名阈值。

14.一种计算机实现的用于在区块链系统中确认交易有效性的方法,所述方法包括:

提供所述交易的部分签名;

在所述区块链系统中广播所述部分签名;

验证所述交易的所述部分签名;以及

响应于确定基于所述部分签名的累积签名分数达到签名阈值,确认所述交易有效。

15.如权利要求14所述的方法,还包括:

生成所述交易的哈希值;以及

利用私钥对所生成的所述哈希值进行加密,以生成所述部分签名。

16.如权利要求14-15中任一项所述的方法,还包括:

对所述部分签名进行解密以获得第一哈希值;

生成所述交易的第二哈希值;以及

如果所获得的所述第一哈希值与所生成的所述第二哈希值匹配,则确定所述部分签名有效。

17.如权利要求16所述的方法,还包括:

如果所获得的所述第一哈希值与所生成的所述第二哈希值不匹配,则确定所述部分签名无效。

18.如权利要求14-17中任一项所述的方法,还包括:

当所述累积签名分数等于或大于预定阈值权重值时,确定所述累积签名分数达到所述签名阈值。

19.如权利要求14-18中任一项所述的方法,还包括:

通过确定与多个部分签名分别对应的权重值的总和,获得所述累积签名分数。

20.如权利要求14-17中任一项所述的方法,还包括:

当所述区块链系统中提供部分签名的节点的数量等于或大于预定阈值数时,确定所述累积签名分数达到所述签名阈值。

21.一种用于在区块链系统中确认交易有效性的设备,所述设备包括:

一个或多个处理器;和

耦接到所述一个或多个处理器并且其上存储有指令一个或多个计算机可读存储器,所述指令由所述一个或多个处理器执行以执行权利要求1到20中任一项所述的方法。

22.一种用于在区块链系统中确认交易有效性的装置,所述装置包括用于执行权利要求1至20中任一项所述的方法的多个模块。

23.一种其中存储有指令的非暂态计算机可读介质,当所述指令由设备的处理器执行时,使所述设备执行权利要求1至20中任一项所述的方法。

在区块链系统中确认交易有效性的方法和设备

技术领域

[0001] 本文总体上涉及计算机技术，更具体地，涉及在区块链系统中确认交易有效性的方法和设备。

背景技术

[0002] 区块链系统，也称为分布式账本系统(DLS)或共识系统，可以使参与的实体安全地且不可篡改地存储数据。在不引用任何特定用例的情况下，区块链系统可以包括任何DLS，并且可以被用于公有、私有和联盟区块链网络。公有区块链网络对所有实体开放使用该系统并参与共识处理。私有区块链网络为特定实体提供，该特定实体集中控制读写权限。联盟区块链网络为选择的实体群组提供，该实体群组控制共识处理，并包括访问控制层。

[0003] 区块链系统维护一个或多个区块链。区块链是用于存储诸如交易之类的数据的数据结构，其可以防止数据被恶意方篡改和操纵。

[0004] 传统上，可以通过来自多方的许可来确认交易有效性。例如，公司支票可能需要来自公司的不同部门的两个或更多个签名，合同可能需要两个或更多个合同方执行等。管理员或中央实体可手动地或以电子方式收集来自多方的签名，还可以将签名提供给区块链系统进行验证。

发明内容

[0005] 在一个实施例中，提供一种计算机实现的用于在区块链系统中确认交易有效性的方法，所述方法包括：验证所述交易的第一部分签名(partial signature)；验证所述交易的第二部分签名；以及响应于确定基于所述第一部分签名和所述第二部分签名的累积签名分数达到签名阈值，确认所述交易有效。

[0006] 在另一实施例中，提供一种计算机实现的用于在区块链系统中确认交易有效性的方法，所述方法包括：提供所述交易的部分签名；在所述区块链系统中广播所述部分签名；验证所述交易的所述部分签名；以及响应于确定基于所述部分签名的累积签名分数达到签名阈值，确认所述交易有效。

[0007] 在另一实施例中，提供一种用于在区块链系统中确认交易有效性的设备，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并且其上存储有指令的一个或多个计算机可读存储器，其中，所述指令可由所述一个或多个处理器执行以执行上述方法。

[0008] 在另一实施例中，一种其中存储有指令的非暂态计算机可读介质，当所述指令由设备的处理器执行时，使所述设备执行以上在区块链系统中确认交易有效性的方法。

附图说明

[0009] 包含在本文中并构成其一部分的附图示出了实施例。在参考附图的以下描述中，除非另有说明，否则不同附图中的相同附图标记表示相同或相似的元件。

[0010] 图1是根据实施例的区块链系统的示意图。

[0011] 图2是根据实施例的用于在区块链系统中确认交易有效性的方法的示意图。

[0012] 图3是根据实施例的用于在区块链系统中确认交易有效性的方法的流程图。

[0013] 图4是根据实施例的用于在区块链系统中由节点提供部分签名的方法的流程图。

[0014] 图5是根据实施例的用于在区块链系统中验证部分签名的方法的流程图。

[0015] 图6是根据实施例的用于在区块链系统中确认交易有效性的设备的示意图。

[0016] 图7是根据实施例的用于在区块链系统中确认交易有效性的装置的示意图。

具体实施方式

[0017] 本文的实施例提供了用于在区块链系统中确认交易有效性的方法和设备。基于共识,区块链系统中的多个节点均可使用私钥为交易提供部分签名。共识群组中的其他节点可使用与该私钥配对的公钥验证部分签名。签名-验证处理可以继续直到累积签名分数达到签名阈值。

[0018] 本文中公开的实施例具有一种或多种技术效果。在一些实施例中,所述方法和设备提供了在区块链系统中具有为交易提供他们各自的部分签名的能力的多个节点。这消除了对管理员或中央中介的需要,从而提高了交易的安全性和效率,并且降低了交易的成本。在其他实施例中,所述方法和设备对以下操作进行迭代:节点为交易提供部分签名,节点广播该部分签名,以及由一个或多个其他节点验证该部分签名,直到累积签名分数达到签名阈值。这允许只要累积签名分数达到签名阈值,交易就可被确认,从而加快了确认处理并避免了可能不需要的额外确认。在其他实施例中,多个节点中的每个节点具有他们自己的私钥,以生成该节点用于交易的部分签名,而不向其他节点泄露该私钥。这允许进一步提高交易的安全性。在其他实施例中,所述方法和设备可动态地移除无效节点并准许新节点加入。这允许保持交易的完整性。在其他实施例中,多个节点并行或基本上同时提供他们的部分签名。这使得无需由多方顺序地对交易进行签名或许可,从而提高了交易确认处理的灵活性和效率。

[0019] 以下描述提供了实施例的细节。在实施例中,区块链是以交易不可篡改且随后可被验证的方式存储数据(例如,交易)的数据结构。区块链包括一个或多个区块。每个区块通过包括区块链中紧邻其之前的前一区块的加密哈希值(cryptographic hash)链接到该前一区块。每个区块还可以包括时间戳、其自身的加密哈希值以及一个或多个交易。通常已经被区块链系统的节点验证的交易经哈希处理并编入例如默克尔(Merkle)树的数据结构中。在Merkle树中,在该树的叶节点处的数据是经哈希处理的,并且在该树的每个分支中的所有哈希值在该分支的根处级联(concatenated)。此处理沿着该树持续一直到整个树的根,在整个树的根处存储了代表树中所有数据的哈希值。通过确定哈希值是否与树的结构一致而可快速验证该哈希值是否为存储在该树中的交易的哈希值。

[0020] 区块链系统包括用于管理、更新和维护一个或多个区块链的计算节点的网络。网络可以是公有区块链网络、私有区块链网络或联盟区块链网络。在公有区块链网络中,共识处理由共识网络的节点控制。例如,诸如数百、数千或甚至数百万个实体的许多实体可以在公有区块链网络中操作,并且每个实体操作该公有区块链网络中的至少一个节点。因此,公有区块链网络可以被认为是关于参与实体的公有网络。有时,大多数实体(节点)必须按顺序对每个区块签名才能使该区块有效并被添加到区块链网络的区块链中。公有区块链网络

的示例包括利用分布式账本(称为区块链)的特定点对点支付网络。

[0021] 通常,公有区块链网络可以支持公开交易。公开交易为公有区块链网络内的所有节点共享,并存储在全局区块链中。全局区块链是跨所有节点复制的区块链,并且所有节点相对于全局区块链处于完全共识状态。为了达成共识(例如,同意向区块链添加区块),在公有区块链网络内实施共识协议。共识协议的示例包括工作量证明(POW)(例如,在一些加密货币网络中实施)、权益证明(POS)和权限证明(POA)。

[0022] 通常,可以为特定实体提供私有区块链网络,该特定实体集中控制读写权限。该实体控制哪些节点能够参与到区块链网络中。因此,私有区块链网络通常被称为权限网络,其限制允许谁参与网络以及它们的参与级别(例如,仅在某些交易中)。可以使用各种类型的访问控制机制(例如,现有参与者投票添加新实体,监管机构可以控制准入)。

[0023] 通常,联盟区块链网络在参与的实体之间是私有的。在联盟区块链网络中,共识处理由授权的节点集控制,一个或多个节点由相应的实体(例如,金融机构、保险公司)操作。例如,由十(10)个实体(例如,金融机构、保险公司)组成的联盟可以操作联盟区块链网络,每个实体可以操作联盟区块链网络中的至少一个节点。因此,联盟区块链网络可以被认为是关于参与实体的私有网络。在一些示例中,每个区块必须经每个实体(节点)签名才能有效并被添加到区块链中。在一些示例中,每个区块必须经至少实体(节点)的子集(例如,至少7个实体)签名才能有效并被添加到区块链中。

[0024] 图1示出了根据实施例的区块链系统100的示意图。参考图1,区块链系统100可以包括被配置为在区块链120上操作的多个节点,例如,节点102-110。节点102-110可以形成例如点对点(P2P)网络的网络112。节点102-110均可以是被配置为存储区块链120的副本的计算设备,例如计算机或计算机系统,或者可以是在计算设备上运行的软件,诸如处理或应用。节点102-110均可以具有唯一标识。节点102-110可以通过有线通信或无线通信彼此通信。这种通信可以采用诸如传输控制协议/互联网协议(TCP/IP)之类的可靠协议。

[0025] 区块链120可以包括数据块形式的记录的增长列表,例如图1中的区块B1-B5。区块B1-B5均可以包括时间戳、前一区块的加密哈希值,以及本区块的可以是诸如货币交易之类的交易的数据。例如,如图1所示,区块B5可以包括时间戳、区块B4的加密哈希值和区块B5的交易数据。而且,例如可以对前一区块执行哈希操作以生成前一区块的加密哈希值。哈希操作可以通过诸如SHA-256的哈希算法将各种长度的输入转换为固定长度的加密输出。

[0026] 节点102-110可以被配置为对区块链120执行操作。例如,当节点(例如,节点102)想要将新数据存储到区块链120上时,该节点可以生成要被添加到区块链120的新区块,并将该新区块广播到网络112中的例如节点104-110的其他节点。基于新区块的合法性,例如,其签名和交易的有效性,其他节点可以确定接受该新区块,使得节点102和其他节点可以将新区块添加到它们各自的区块链120的副本中。重复该处理,可以将越来越多的数据区块添加到区块链120。

[0027] 在实施例中,区块链系统100可以根据一个或多个智能合约操作。每个智能合约可以是计算机代码形式的计算机协议,其被纳入到区块链120中,以促进、验证或施行合约的协商或执行。例如,区块链系统100的用户可以使用诸如C++、Java、Solidity、Python等编程语言将商定的条款编程为智能合约,并且当满足条款时,可以由区块链系统100自动执行智能合约,例如执行交易。又例如,智能合约可以包括多个子例程或函数,每个子例程或函数

可以是执行指定任务的一系列程序指令。智能合约可以是在全部或部分没有人工交互情况下执行的操作代码。

[0028] 在实施例中，可以基于加密算法在区块链系统100中认证交易。加密算法可以提供包括私钥和公钥的密钥对。私钥可以与特定用户相关联并且可以对表示例如由用户发起的交易的数据进行加密。对表示交易的数据进行加密也可被称为对交易进行签名。公钥可以被提供给区块链系统100中的另一用户以对经加密的数据进行解密，来验证交易是否确实被该特定用户授权。解密还可以被称为签名验证。在实施例中，区块链系统100可以支持多个加密算法，诸如RSA(Rivest-Shamir-Adleman)算法、椭圆曲线数字签名算法(ECDSA)、SM2算法等。

[0029] 在实施例中，可以对区块链系统100中的交易执行多签名。多签名是允许用户群组对同一交易进行签名的技术。

[0030] 图2是根据实施例的用于在诸如区块链系统100(图1)的区块链系统中确认交易有效性的方法200的示意图。区块链系统包括诸如节点212、214、216和218的多个节点，他们的操作类似于区块链系统100中的节点。

[0031] 参考图2，区块链系统可以具有多个用户，例如分别使用区块链系统中的节点212、214、216和218的用户202、204、206和208。用户202-208可以被授权对交易提供他们的部分签名，并且还可以被称为签名机构。部分签名可以是每个签名机构可提供的、表示由提供该部分签名的特定签名机构对交易的授权的签名。仅出于说明的目的，在该实施例中，假设用户202、204、206和208分别使用节点212、214、216和218，但方法200不限于此。例如，用户202、204、206和208中的一个以上或所有用户可以使用区块链系统中的同一节点，例如节点212或节点214。还例如，除了图2中所示的用户202之外，附加用户可以使用节点212。作为另一示例，使用节点的用户可以通过该节点或与该节点通信的用户终端提供部分签名。在一些实施例中，用户202-208可以彼此相关，例如，他们是同一组织的不同部门的主管。在一些实施例中，用户202-208可以彼此不相关，例如用户202可以是设在美国的公司的代表，用户204可以是日本的大学的代表，用户206可以是中国的研究机构的代表，用户208可以是德国的政府官员。所需签名机构的数量可取决于交易的特性。通常，签名机构越多，可以反映出交易的有效性的置信度就越高。

[0032] 交易可以是需要来自多个用户的部分签名的任何交易。例如，交易可以是货币转账、资产转移、智能合约的执行、智能合约的修改等。

[0033] 在实施例中，交易可以具有多个状态并且可以被称为多状态交易。多状态交易可以是需要多个步骤或多个用户来执行的交易。在图2中示出的实施例中，多状态交易是需要多个签名机构来提供他们的部分签名的多签名交易。每个签名机构可以对交易执行签名操作以提供部分签名。在一些实施例中，签名机构的操作可以记录在交易历史中。

[0034] 在实施例中，用户202、204、206和208因此节点212、214、216和218可以形成共识群组以对交易协作地执行多签名。该共识群组可以是例如只有具有签名机构的节点才可加入的权限组，从而确保了交易的安全性。共识群组可由发起交易的用户或由具有签名机构的用户、或者由区块链系统或智能合约的创建者来初始化。共识群组中的节点212-218可以使用协议210彼此互连。协议210可以是安全加密协议，例如传输层安全/安全套接层(TLS/SSL)协议，或者可以在通信中提供隐私和数据完整性的任何当前已知的或未来开发的协

议。应当理解，尽管图2示出了节点212和214之间、节点214和218之间、节点216和218之间、以及节点212和216之间的互连，但是这仅出于说明的目的。可以在区块链系统中的每个节点与任意剩余节点之间建立互连。

[0035] 在实施例中，作为共识群组的成员，每个节点可以同意执行多状态交易的该节点的部分，使得群组成员可协作地验证交易。例如，每个节点可以同意提供部分签名，以验证由其他节点提供的部分签名，从而在满足交易的签名阈值的情况下确认交易有效。在一些实施例中，节点212-218均可以执行诸如以下的操作：生成部分签名并且将该部分签名广播到区块链系统，使得共识群组中的其它节点可基于共识算法220来验证该部分签名。在一些实施例中，节点212-218均可以接收用户终端生成的部分签名，以提供部分签名。如果基于部分签名的累积签名分数达到签名阈值，则该交易的多签名完成，并且该交易被确认。例如，可以通过确定与已被验证的部分签名对应的权重值的当前和，或者已被验证的部分签名的当前数量，来获得累积签名分数。在实施例中，共识算法220可以是以下中的任何一个：实用拜占庭容错(PBFT)、蜜獾(Honey Badger)、工作量证明(POW)、权益证明(POS)、委托权益证明(DCOI)、或贪婪最重可观察子树(GHOST)。应当理解，尽管图2示出了在节点212和214之间、节点214和218之间、节点216和218之间、以及节点212和216之间达成共识，但是这仅出于说明的目的。可以在区块链系统中的每个节点与任何剩余节点之间达成共识。

[0036] 在实施例中，交易可以由广播交易请求的节点发起。例如，在图2中示出的实施例中，与用户202对应的节点212可以通过在区块链系统中广播交易请求来发起交易，并且该交易请求可以包括交易数据。在一些实施例中，用户202是交易的发起者，但不是签名机构。在其他实施例中，用户102是交易的发起者，也是签名机构。因此，交易请求可以包括节点212对交易的部分签名。仅出于说明的目的，在示出的实施例中，假设交易请求不包括节点212的部分签名。

[0037] 在实施例中，在接收到交易请求时，节点214、216和218均可以对交易执行他们各自的部分签名。例如，共识群组可以采用私钥/公钥加密/解密算法，诸如RSA算法，共识群组中的每个节点具有节点自己的私钥。在一些实施例中，可在节点自身生成私钥，而不向任何其他节点泄露信息，增强了交易的安全性。私钥可以是在节点生成的安全随机数，或者仅被节点所知的任何密码。节点214可以使用哈希函数来生成交易的哈希值，并使用该节点的私钥对该哈希值进行加密，以生成该节点的交易的部分签名。节点214随后可以将该节点的部分签名广播到区块链系统，使得共识群组中的其他节点也可以对交易进行签名。

[0038] 在实施例中，对于每个私钥，存在与该私钥配对的对应公钥。公钥对共识群组中的所有节点开放。在一些实施例中，公钥可以在区块链中被注册，或者被预先提供给共识群组中的其他节点。在一些实施例中，公钥可以连同签名一起被发送到群组中的其他节点。

[0039] 在实施例中，在接收到从节点214发送的部分签名时，共识群组中的其他节点可以验证节点214的部分签名的有效性。例如，节点212、216和218均可以使用与节点214的私钥配对的公钥对所接收的部分签名进行解密，以获得第一哈希值。此外，节点212、216和218自身均可以生成针对该交易的第二哈希值。如果节点212、216和218中的所有节点或大多数节点确定从解密处理获得的第一哈希值与生成的第二哈希值匹配，则节点214的部分签名被验证。否则，节点214的部分签名被确定为无效。

[0040] 在实施例中，节点216还可以为交易提供该节点的部分签名。类似于节点214，节点

216可以使用例如RSA算法，通过生成针对该交易的哈希值，并使用该节点的私钥对该哈希值进行加密，来生成该交易的部分签名。节点216随后可以将该节点的部分签名广播到共识群组中的其他节点以进行验证。

[0041] 在实施例中，在接收到从节点216发送的部分签名时，共识群组中的其他节点可以验证节点216的部分签名的有效性。例如，节点212、214和218均可以使用与节点216的私钥配对的公钥来对所接收的部分签名进行解密，并获得第一哈希值。此外，节点212、214和218均可以生成针对该交易的第二哈希值。如果节点212、214和218中的所有节点或大多数节点确定从解密处理获得的第一哈希值与所生成的第二哈希值匹配，则节点216的部分签名被验证。这种签名-验证处理可以在共识群组中的节点内进行迭代，直到累积签名分数达到签名阈值。

[0042] 在一个实施例中，基于节点214和216的部分签名的累积签名分数可以达到签名阈值，因此基于两个部分签名确认交易有效。在另一实施例中，可能需要额外的部分签名以使累积签名分数达到签名阈值来确认交易有效。

[0043] 签名阈值可以是完成多签名所需的预定权重值或预定数量个部分签名。在一些实施例中，签名阈值可被表示为百分比值。例如，签名阈值100％表示要求所有签名机构提供他们的部分签名以对交易完成多签名。签名阈值可通过签名机构之间的共识确定、或通过共识群组中具有确定签名阈值的权利的机构确定、或通过区块链系统的创建者确定。通常，签名阈值越大，交易的有效性的置信度就越高。

[0044] 在实施例中，各个权重值可被分配给共识群组的每个用户(也即节点)。权重值可表示给定签名机构的重要性或对确认交易的贡献。例如，在图2中示出的实施例中，权重值10％、50％、30％和10％可分别分配给用户202、204、206和208，也即节点212、214、216和218，其表示节点214的部分签名对确认交易的贡献最大。与签名机构相关联的权重值可以通过签名机构之间的共识确定、或通过共识群组中具有分配权重值的权利的机构确定，或通过区块链系统的创建者确定。

[0045] 在图2中示出的实施例中，如果分配给节点214的权重值为50％，并且签名阈值为90％，则在验证节点214的部分签名后，交易尚未被确认。因此，接着是第二部分签名。例如，节点216可以为该交易提供该节点的部分签名。如果分配给节点216的权重值为30％，则在验证节点216的部分签名之后，累积签名分数为80％，仍小于为90％的签名阈值，因此交易仍未被确认。因此，接着是第三部分签名。例如，节点218可以提供该节点的部分签名。如果分配给节点218的权重值为10％，则累积签名分数为90％，达到为90％的签名阈值，因此，多个用户完成了多签名，交易有效并被视为可执行。

[0046] 在实施例中，如果共识群组发现签名机构进行伪造(例如，在签名中提供假实体)因此对应的节点是无效节点，其余节点可以通过共识将该无效节点从网络永久地或暂时地移除，并移除无效节点提供的部分签名。此外，通过共识，剩余的签名机构可以许可新的签名机构加入。通过动态地从所述群组中移除无效节点并在组群中准许新节点加入，可以保持交易的完整性。

[0047] 以上实施例提供了一种用于在区块链系统中对交易执行多签名的方法。基于共识，每个节点可以使用私钥对交易提供部分签名，并且共识群组中的其他节点可以使用与该私钥配对的公钥来验证该部分签名。签名-验证处理可以继续，直到累积签名分数达到签

名阈值，从而，可以在不涉及管理员或中央实体的情况下对交易执行多签名。相应地，实施例可以消除对中央中介的需要，从而提高了交易的安全性和效率，并且降低了交易的成本。

[0048] 图3是根据实施例的用于在区块链系统中确认交易有效性的方法300的流程图。参考图3，在步骤310中，发起交易，并将签名请求广播到具有签名机构的所有用户，诸如图2中的用户202-208。每个用户可以使用区块链系统中的节点，诸如图2中的节点212-218，并且用户可以形成共识群组以对交易协作地执行多签名。在一些实施例中，一个以上或所有用户可以通过区块链系统中的同一节点提供他们的部分签名。交易可以由与共识群组中的用户对应的节点，或与不在共识群组中的用户对应的节点发起和广播。交易可以是需要来自多个用户的多个部分签名的任何交易或电子文档。

[0049] 在步骤320中，共识群组中的、诸如图2中的节点212的节点提供交易的部分签名，提供部分签名的顺序可以通过节点之间的共识来确定。在一些实施例中，可以基于图4中示出的方法提供部分签名。

[0050] 参考图4，根据实施例的用于在区块链系统中节点提供部分签名的方法400的流程图。如图4所示，在步骤410中，共识群组中的、诸如图2中的节点212的第一节点生成交易的哈希值。在步骤420中，使用节点的私钥对所生成的哈希值进行加密，以生成部分签名。私钥可以是节点的密钥，密钥的信息不泄露给共识群组中的其他节点。私钥可以与公钥配对，并且公钥对共识群组中的其他节点开放。

[0051] 现在参照回图3，一旦生成了部分签名，则在步骤330中，就将该部分签名广播给区块链系统中的共识群组中的所有其他节点。该广播可以使用诸如TLS/SSL协议之类的安全通信协议。

[0052] 在步骤340中，通过区块链系统中的共识群组中的、诸如图2中的节点214、216和218的其他节点，验证广播的部分签名。在一些实施例中，可以通过如图5中所示的方法来验证部分签名。

[0053] 参照图5，根据实施例的用于在区块链系统中由共识群组中的多个节点验证部分签名的方法500的流程图。如图5所示，在步骤510中，共识群组中的其他节点对从第一节点广播的部分签名进行解密，并获得哈希值。在一些实施例中，多个签名机构可以使用该第一节点，并且还可以由第一节点对从第一节点广播的、由多个签名机构之一提供的部分签名进行解密。解密处理可以通过使用与第一节点的私钥配对的公钥来执行。

[0054] 此外，在步骤520中，共识群组中的每个其他节点使用哈希函数生成哈希值。在步骤530中，将步骤510中所获得的哈希值与在步骤520中所生成的哈希值进行比较。如果所获得的哈希值与所生成的哈希值匹配，则在步骤540中，第一节点的部分签名被确定为有效。否则，在步骤550中，第一节点的部分签名被确定为无效。在实施例中，如果所有或大多数其他节点确定第一节点的部分签名有效，则第一节点的部分签名可以被确认。在一些实施例中，基于共识，未确认的签名可以从区块链系统中被移除，并且提供无效部分签名的节点可以被终止或被新节点替换。

[0055] 现在参照回图3，在步骤350中，将累积签名分数与签名阈值进行比较。累积签名分数可以基于分配给共识群组中的每个节点的权重值来确定。签名阈值可以考虑交易和签名用户的特性通过共识来确定。

[0056] 如果累积签名分数等于或大于签名阈值，则在步骤360中，针对交易完成了多签

名，该交易被确认并被视为可执行。另一方面，如果累积签名分数小于签名阈值，则收集更多的部分签名。例如，可以迭代步骤320-350：提供部分签名、广播部分签名、验证部分签名并将更新的累积签名分数与签名阈值进行比较，直到累积签名分数等于或大于签名阈值。

[0057] 在签名和验证部分签名时，上述实施例使用交易的哈希值的加密和解密。然而，该方法不限于此。在一些实施例中，可以使用可在区块链系统中唯一地标识交易的任何字符串或ID替代哈希值。这样的标识字符串可以通过任何当前已知的函数或未来开发的函数生成。

[0058] 在以上实施例中，共识群组的多个用户依次提供他们的部分签名，例如，多个用户依次生成他们的部分签名。然而，签名处理不限于此。多个用户可以并行提供他们的部分签名。例如，多个用户可以同时生成他们的部分签名。这去除了签名顺序，提高了处理的灵活性和效率。

[0059] 应当理解，上述公开的方法可以用于各种类型的区块链网络，诸如公有区块链网络、私有区块链网络或联盟区块链网络。

[0060] 图6是根据实施例的用于在区块链系统中确认交易有效性的设备600的示意图。例如，设备600可以作为区块链系统中的、诸如图1中的节点102的节点操作。设备600可以采取任何形式，包括但不限于台式计算机、膝上型计算机、服务器计算机、平板电脑、智能手机或智能手表、或者任何其他形式。参考图6，设备600可以包括通过总线610相互通信的处理器620、用户接口630、存储器640和通信接口650。

[0061] 处理器620可以包括一个或多个专用处理单元、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、或各种其他类型的处理器或处理单元。处理器620与存储器640耦接，并且被配置为执行存储在存储器640中的指令。

[0062] 通信接口650可以促进设备600与区块链系统中的、诸如节点102-110(图1)的其他节点实现的设备之间的通信。在一些实施例中，通信接口650可以支持一个或多个通信标准，诸如互联网标准或包括TCP/IP和TLS/SSL协议的协议、综合业务数字网(ISDN)标准等。在一些实施例中，通信接口650可以包括以下中的一个或多个：局域网(LAN)卡、线缆调制解调器、卫星调制解调器、数据总线、线缆、无线通信信道、基于无线电的通信信道、蜂窝通信信道、基于互联网协议(IP)的通信设备、或者用于有线和/或无线通信的其他通信设备。在一些实施例中，通信接口650可以基于公有云基础设施、私有云基础设施、以及混合公有/私有云基础设施。

[0063] 存储器640可以存储处理器可执行指令和数据。计算机可执行指令和数据可以包括共识算法642。当被处理器620执行时，共识算法642允许设备600执行诸如以下的操作：与区块链系统中的其他节点形成共识群组，生成用于交易的部分签名，将该部分签名广播到区块链系统中的共识群组中的其他节点，验证其他节点提供的部分签名，通过将累积签名分数与签名阈值进行比较来确定是否完成了多签名等。

[0064] 存储器640还可以存储私钥644。私钥644可以是由处理器620生成的安全随机数、或设备600的拥有者指定的密码。私钥644可以与保存在存储器640中的公钥配对。

[0065] 存储器640可以是任何类型的易失性存储器设备或非易失性存储器设备，或者他们的组合，诸如静态随机存取存储器(SRAM)、电可擦除可编程只读存储器(EEPROM)、可擦除可编程只读存储器(EPROM)、可编程只读存储器(PROM)、只读存储器(ROM)、磁存储器、闪存、

或者磁盘或光盘。

[0066] 用户接口630可以包括被配置为显示对交易执行多签名的进展的显示器以及向处理器620发送用户命令的输入设备等。显示器可以包括但不限于阴极射线管(CRT)、液晶显示器(LCD)、发光二极管(LED)、气体等离子体、触摸屏或用于向用户显示信息的其他图像投影设备。输入设备可以是用于从用户向处理器620提供数据和控制信号的任何类型的计算机硬件装置。输入设备可包括但不限于键盘、鼠标、扫描仪、数字相机、操纵杆、轨迹球、光标方向键、触摸屏监视器或音频/视频管理器等。

[0067] 在一些实施例中,设备600可仅承载区块链系统中的一个节点,诸如1中的节点102。在一些实施例中,设备600可以承载多于一个节点,从而降低了区块链系统的硬件成本。例如,设备600可承载属于同一组织的若干不同节点。

[0068] 图7是根据实施例的用于在区块链系统中确认交易有效性的装置700的示意图。例如,装置700可以作为区块链系统中的、诸如图1中的节点102的节点操作。此外,例如,装置700可实现软件处理,并且可以对应于方法300(图3)。参考图7,装置700可以包括验证模块706和确认模块708。

[0069] 在一些实施例中,验证模块706可以验证交易的部分签名,诸如交易的第一部分签名和第二部分签名。确认模块708可以响应于确定基于交易的诸如第一部分签名和第二部分签名的部分签名的累积签名分数达到签名阈值,确认交易有效。

[0070] 在一些实施例中,装置700还可以包括签名模块702和广播模块704。签名模块702可以为交易提供部分签名,诸如第一部分签名。广播模块704可以在区块链系统中广播部分签名。

[0071] 上述模块中的每一个可以被实现为软件或硬件,或者软件和硬件的组合。例如,可以使用执行存储在存储器中的指令的处理器来实现上述模块中的每一个。而且,例如,每个上述模块可以用一个或多个专用集成电路(ASIC)、数字信号处理器(DSP)、数字信号处理设备(DSPD)、可编程逻辑器件(PLD)、现场可编程门阵列(FPGA)、控制器、微控制器、微处理器或其他电子组件执行所描述的方法来实现。进一步地,例如,上述模块中的每一个可以通过使用计算机芯片或实体来实现,或者通过使用具有特定功能的产品来实现。在一个实施例中,装置700可以是计算机,并且计算机可以是个人计算机、膝上型计算机、蜂窝电话、照相手机、智能手机、个人数字助理、媒体播放器、导航设备、电子邮件接收和发送设备、游戏台、平板电脑、可穿戴设备或这些设备的任何组合。

[0072] 对于装置700中每个模块的功能和角色的实现过程,可以参考上述方法中的相应步骤。为简单起见,这里省略了细节。

[0073] 在一些实施例中,计算机程序产品可以包括非暂态计算机可读存储介质,其上存储有计算机可读程序指令,用于使处理器执行上述方法。

[0074] 计算机可读存储介质可以是有形设备,其可以存储供指令执行设备使用的指令。计算机可读存储介质可以是例如(但不限于)电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或前述的任何合适的组合。计算机可读存储介质的更具体示例的非详尽列表包括以下内容:便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM)、静态随机存取存储器(SRAM)、便携式光盘只读存储器(CD-ROM)、数字通用光盘(DVD)、记忆棒、软盘、例如在其上记录有指令的凹槽中的穿孔

卡或凸起结构的机械编码设备，以及前述的任何合适的组合。

[0075] 用于执行上述方法的计算机可读程序指令可以是汇编指令、指令集架构(ISA)指令、机器指令、机器相关指令、微代码、固件指令、状态设置数据或者以一种或多种编程语言的任意组合编写的源代码或目标代码，该编程语言包括面向对象的编程语言和传统的过程编程语言。计算机可读程序指令可以全部在计算设备上作为独立软件包执行，或者部分在第一计算设备上执行、部分在远离第一计算设备的第二计算设备上执行。在后一种情况下，第二远程计算设备可以通过包括局域网(LAN)或广域网(WAN)的任何类型的网络连接到第一计算设备。

[0076] 计算机可读程序指令可以被提供给通用或专用计算机的处理器或其他可编程数据处理装置以产生机器，使得经由计算机的处理器或其他可编程数据处理装置执行的指令创建用于实施上述方法的装置。

[0077] 附图中的流程图和示图示出了根据本文各种实施例的设备、方法和计算机程序产品的可能实施例的架构、功能和操作。在这方面，流程图或示图中的框可以表示软件程序、代码段或代码的一部分，其包括用于实现特定功能的一个或多个可执行指令。还应注意，在一些替代实施方式中，框中提到的功能可以不按图中所示的顺序发生。例如，连续示出的两个框实际上可以基本上同时执行，或者这些框有时可以以相反的顺序执行，这取决于所涉及的功能。还应注意，示图和/或流程图的每个框以及示图和流程图中的框的组合可以由执行特定功能或动作的专用目的的基于硬件的系统、或者专用目的的硬件和计算机指令的组合来实施。

[0078] 应当理解，为了清楚起见，在单独的实施例的上下文中描述的本文的某些特征也可以在单个实施例中组合提供。相反，为了简洁起见，在单个实施例的上下文中描述的本文的各种特征也可以单独提供或者以任何合适的子组合提供，或者在本文的任何其他所述实施例中合适地提供。除非另有说明，否则在各种实施例的上下文中描述的某些特征不是那些实施例的必要特征。

[0079] 尽管已经结合本文的具体实施例描述了本文，但是显然许多替换、修改和变体对于本领域技术人员而言将是显而易见的。因此，以下权利要求包含落入权利要求的范围内的所有这些替换、修改和变体。

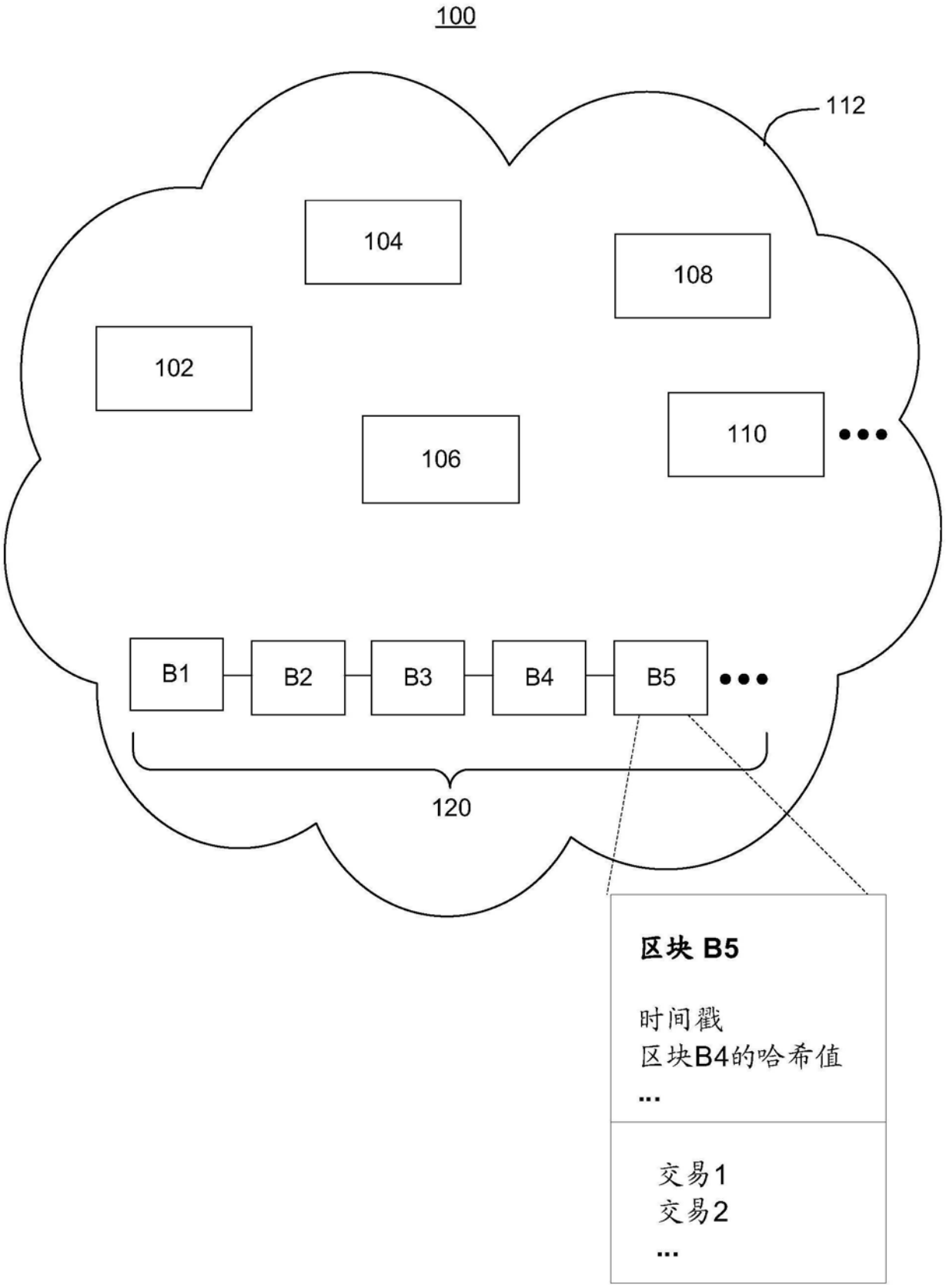

100
112
104
108
102
106
110
B1
B2
B3
B4
B5
120
区块 B5
时间戳
区块B4的哈希值
...
交易1
交易2
...

图1

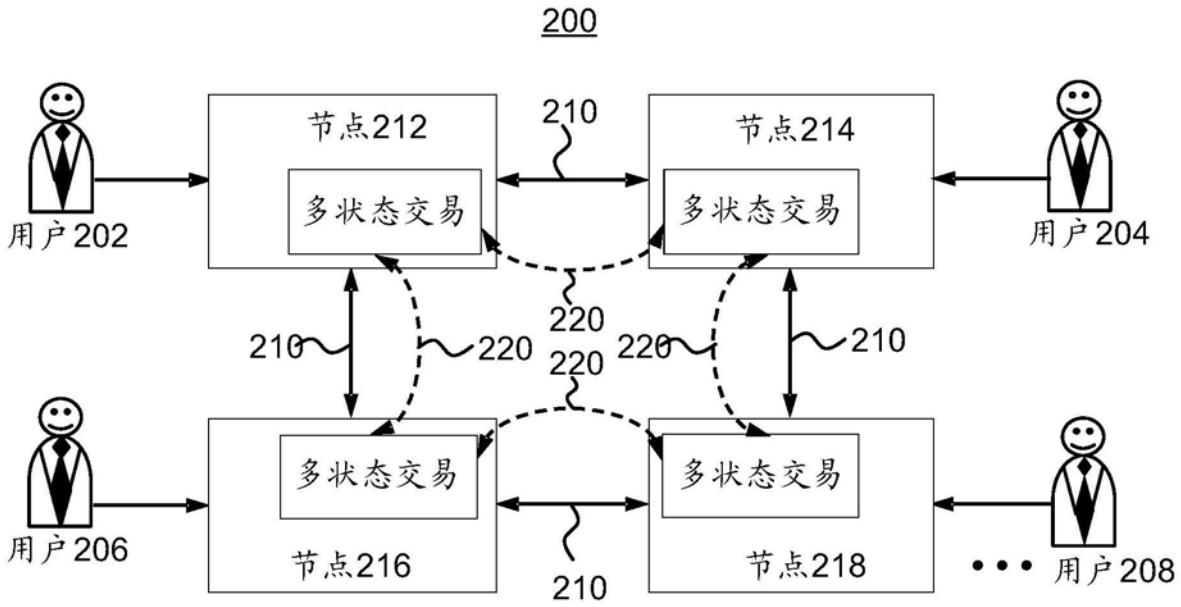

200
节点212
多状态交易
210
节点214
多状态交易
用户202
用户204
220
210
220
220
220
210
多状态交易
多状态交易
用户206
节点216
节点218
用户208
210

图2

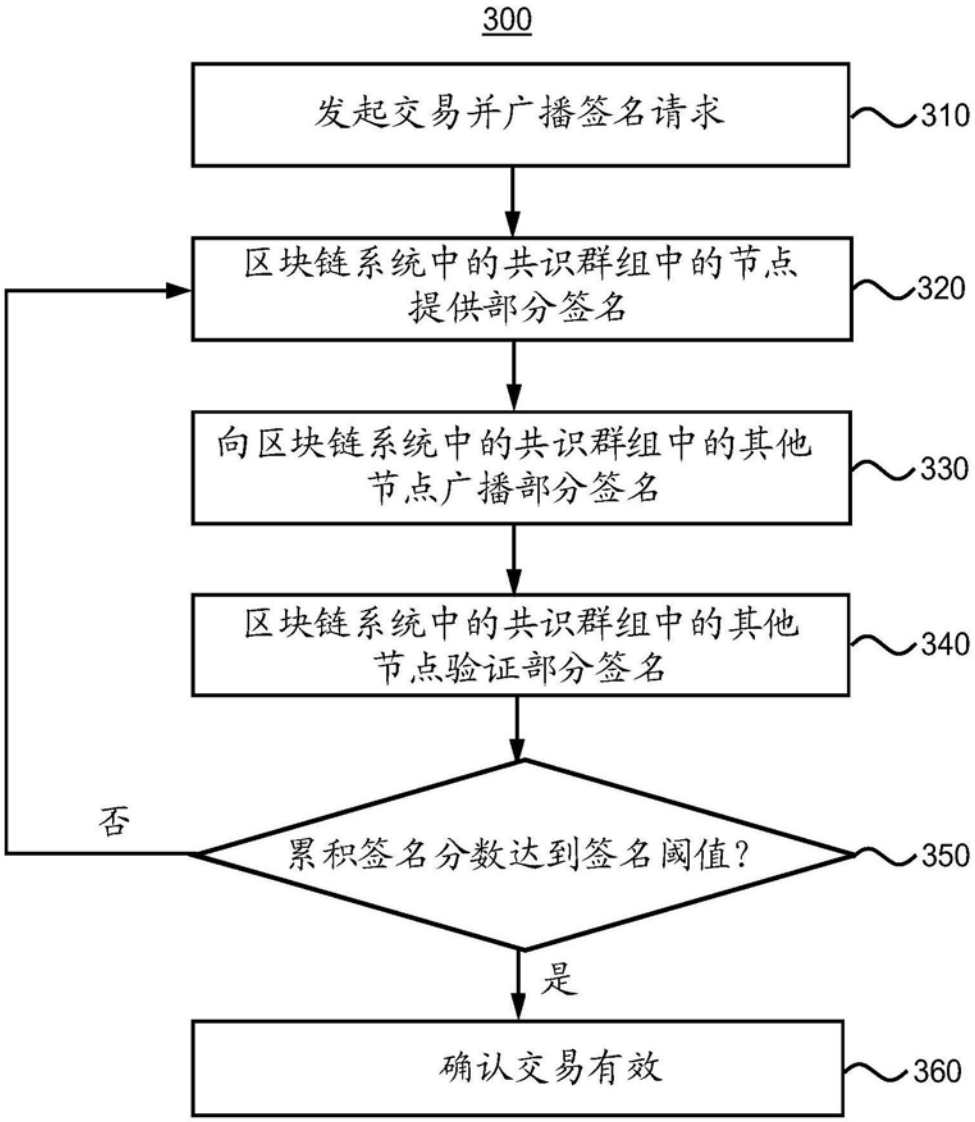

300
发起交易并广播签名请求
310
区块链系统中的共识群组中的节点提供部分签名
320
向区块链系统中的共识群组中的其他节点广播部分签名
330
区块链系统中的共识群组中的其他节点验证部分签名
340
累积签名分数达到签名阈值?
350
否
是
确认交易有效
360

图3

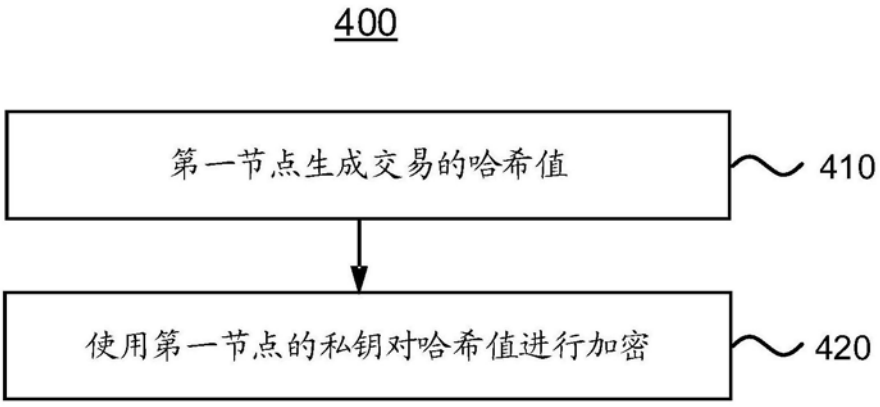

400
第一节点生成交易的哈希值
410
使用第一节点的私钥对哈希值进行加密
420

图4

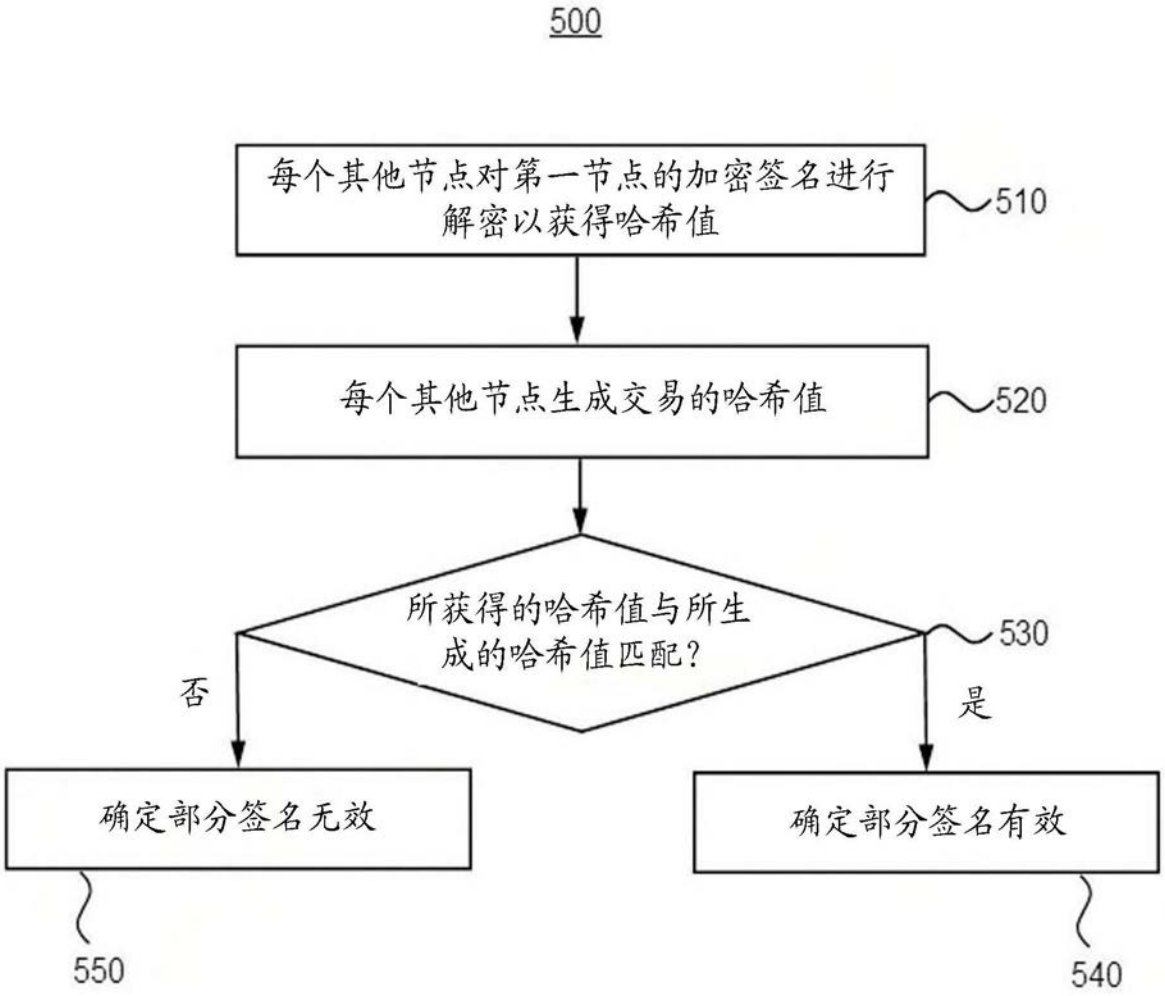

500
每个其他节点对第一节点的加密签名进行解密以获得哈希值
510
每个其他节点生成交易的哈希值
520
所获得的哈希值与所生成的哈希值匹配?
530
否
是
确定部分签名无效
确定部分签名有效
550
540

图5

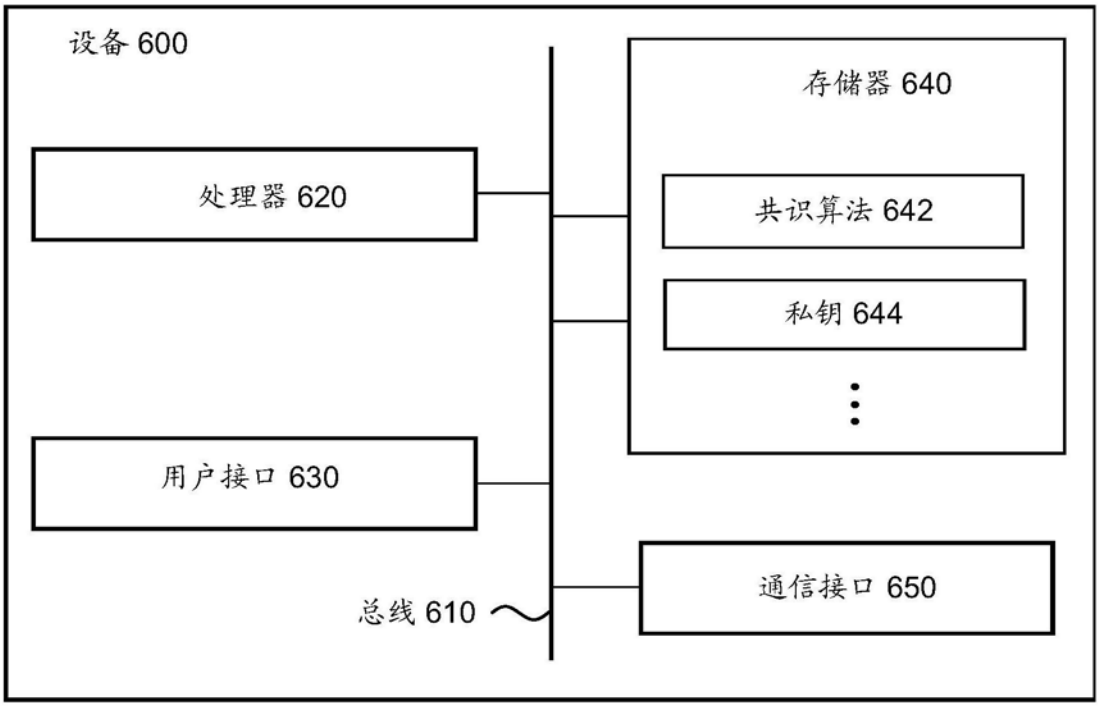

设备 600
存储器 640
处理器 620
共识算法 642
私钥 644
用户接口 630
通信接口 650
总线 610

图6

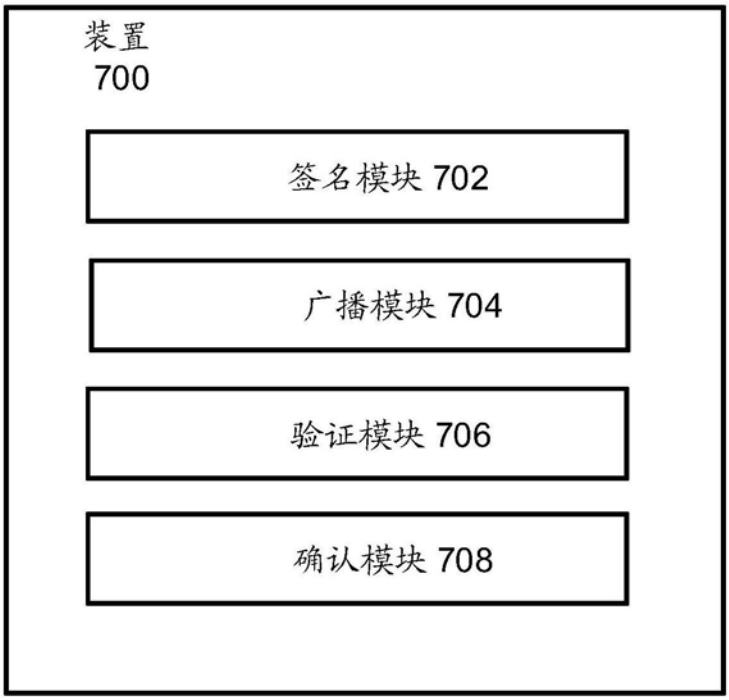

装置
700
签名模块 702
广播模块 704
验证模块 706
确认模块 708

图7