(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111095256 B
(45)授权公告日 2023.12.01

(21)申请号 201980004374.1

(22)申请日 2019.04.26

(65)同一申请的已公布的文献号
申请公布号 CN 111095256 A

(43)申请公布日 2020.05.01

(85)PCT国际申请进入国家阶段日
2020.03.06

(86)PCT国际申请的申请数据
PCT/CN2019/084523 2019.04.26

(87)PCT国际申请的公布数据
WO2019/137564 EN 2019.07.18

(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 魏长征 闫莺 赵博然 宋旭阳 杜华兵

(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 艾佳

(51)Int.Cl.
G06F 21/64(2006.01)
G06Q 20/40(2006.01)

(56)对比文件
WO 2019072297 A2,2019.04.18
CN 107844704 A,2018.03.27
CN 109461076 A,2019.03.12
WO 2018058441 A1,2018.04.05
佚名.TEE硬件隐私合约链(含标准合约链)的框架和功能概述.https://cloud.tencent.com/developuer/article'/1408971.2019,全文.
张宪;蒋钰钊;闫莺.区块链隐私技术综述.信息安全研究.2017,(第11期),23-31.
Raymond Cheng et al..Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution.https://arxiv.org/abs/1804.05141v1.2018,第4-5页第3.2章节及图1.

审查员 胡振洲

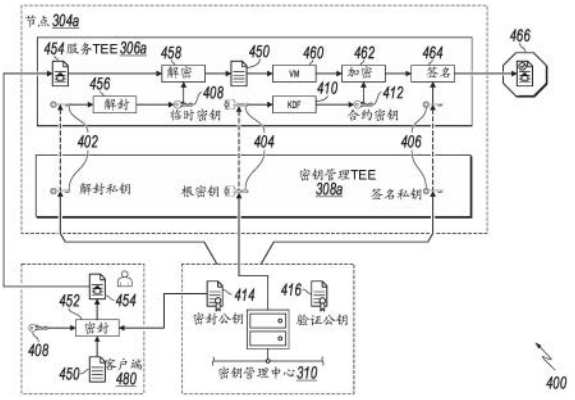
权利要求书2页 说明书13页 附图6页

(54)发明名称

在可信执行环境中安全地执行智能合约操作

(57)摘要

本文公开了用于在可信执行环境(TEE)中安全地执行智能合约操作的方法、系统和装置,包括计算机存储介质上编码的计算机程序。所述方法之一包括由参与区块链网络的区块链节点接收用于执行由区块链节点承载的服务TEE中的一个或多个软件指令的请求,其中所述请求由与服务TEE相关联的公钥进行加密;使用与服务TEE相关联的第一私钥对所述请求进行解密,其中第一私钥与公钥配对;响应于对所述请求进行了解密,执行一个或多个软件指令以产生执行结果;使用与服务TEE相关联的客户端加密密钥对所述执行结果进行加密以产生加密结果;使用与服务TEE相关联的第二私钥对加密结果进行签名,以产生签名的加密结果。



CN 111095256 B

1.一种计算机实现的用于在可信执行环境TEE中安全地执行智能合约操作的方法,所述方法包括:

参与区块链网络的区块链节点接收用于执行由所述区块链节点承载的服务TEE中的与智能合约相关联的一个或多个软件指令的请求;其中,所述请求和与所述服务TEE相关联的客户端加密密钥由与所述服务TEE相关联的公钥进行加密;所述一个或多个软件指令由所述客户端加密密钥进行加密;所述区块链节点还承载密钥管理TEE,所述密钥管理TEE存储与所述服务TEE相关联的第一私钥和第二私钥,并且在基于进行由所述密钥管理TEE发起的本地认证来认证所述服务TEE的身份之后,所述密钥管理TEE将所述第一私钥和所述第二私钥提供给所述服务TEE;

所述区块链节点在所述服务TEE中使用所述第一私钥对所述请求和所述客户端加密密钥进行解密,并使用解密后的所述客户端加密密钥对所述一个或多个软件指令进行解密;其中,所述第一私钥与所述公钥配对;

响应于对所述请求和所述一个或多个软件指令进行了解密,所述区块链节点在所述服务TEE中执行所述一个或多个软件指令以产生执行结果;

所述区块链节点在所述服务TEE中使用所述客户端加密密钥对所述执行结果进行加密,以产生加密结果;以及

所述区块链节点在所述服务TEE中使用所述第二私钥对所述加密结果进行签名,以产生签名的加密结果。

2.如权利要求1所述的计算机实现的方法,其中,所述公钥是第一公钥,并且所述客户端加密密钥是第二公钥或基于密钥导出函数从根密钥导出的对称密钥之一。

3.如权利要求2所述的计算机实现的方法,其中,

在基于进行由所述密钥管理TEE发起的本地认证来认证所述服务TEE的身份之后,所述密钥管理TEE将所述根密钥提供给所述服务TEE。

4.如权利要求2所述的计算机实现的方法,其中,

所述第一私钥、所述第二私钥和所述根密钥是由密钥管理中心生成的,并且

在基于进行由所述密钥管理中心发起的远程认证来认证所述密钥管理TEE的身份之后,所述第一私钥、所述第二私钥和所述根密钥被提供给所述密钥管理TEE。

5.如权利要求2所述的计算机实现的方法,其中,响应于所述服务TEE的重启操作,所述密钥管理TEE向所述服务TEE提供所述第一私钥和所述根密钥。

6.如权利要求2所述的计算机实现的方法,其中,

所述根密钥是基于所述智能合约的状态从所述密钥管理TEE中存储的多个根密钥中选择的。

7.如权利要求4所述的计算机实现的方法,其中,所述第一公钥是由所述密钥管理中心生成的并被提供给客户端以对所述请求进行加密。

8.如权利要求7所述的计算机实现的方法,其中,所述密钥管理中心存储与所述第二私钥相对应的验证公钥,并将所述验证公钥提供给所述客户端以验证所述签名的加密结果。

9.一种用于在可信执行环境TEE中安全地执行智能合约操作的系统,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的一个或多个计算机可读存储器,

所述指令能够由所述一个或多个处理器执行以执行权利要求1-8中任一项所述的方法。

10.一种用于在可信执行环境TEE中安全地执行智能合约操作的装置,所述装置包括用于进行权利要求1-8中任一项所述的方法的多个模块。

在可信执行环境中安全地执行智能合约操作

技术领域

[0001] 本文涉及在可信执行环境中安全地执行智能合约操作。

背景技术

[0002] 分布式账本系统(DLS),也可以被称为共识网络和/或区块链网络,使参与的实体能够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,DLS通常被称为区块链网络。一种类型的区块链网络的示例可以包括为选择的一组实体提供的联盟区块链网络,其控制共识处理,并且联盟区块链网络包括访问控制层。

[0003] 智能合约是在区块链上执行的程序。智能合约包含一组预定义规则,根据所述规则,所述智能合约的各方同意彼此交互。如果满足智能合约的预定义规则,则智能合约中定义的协议将被自动强制执行。智能合约通常具有防篡改功能,并且促进、验证和强制执行协议或交易的协商或执行。

[0004] 在联盟区块链网络中,因为只有选定组的节点控制共识处理,所以攻击者必须获得对相对较少数量的节点的控制以影响共识处理。尽管已经提出了用于解决联盟区块链网络中的这些类型的安全问题的技术,但是更有效且安全的解决方案将是有利的。

发明内容

[0005] 本文描述了用于在区块链节点执行的可信执行环境(TEE)中安全地执行所请求的智能合约操作的技术。更具体地,本文的实施例使得区块链节点能够在TEE内以安全且可验证的方式执行智能合约操作,使得各方可以信任在其中执行操作的环境未被篡改或损害。

[0006] 本文还提供了耦接到一个或多个处理器并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,当所述指令由所述一个或多个处理器执行时,所述指令将促使所述一个或多个处理器按照本文提供的方法的实施例执行操作。

[0007] 本文还提供了用于实施本文提供的所述方法的系统。所述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并且其上存储有指令的计算机可读存储介质,当所述指令由所述一个或多个处理器执行时,所述指令将导致所述一个或多个处理器按照本文提供的方法的实施例执行操作。

[0008] 应了解,依据本文的方法可以包括本文描述的方面和特征的任意组合。也就是说,根据本文的方法不限于本文具体描述的方面和特征的组合,还包括所提供的方面和特征的任意组合。

[0009] 以下在附图和描述中阐述了本文的一个或多个实施例的细节。根据说明书和附图以及权利要求书,本文的其他特征和优点将显现。

附图说明

[0010] 图1是示出了可以用于执行本文的实施例的环境的示例的图。

[0011] 图2是示出根据本文的实施例的架构的示例的图。

[0012] 图3是示出根据本文的实施例的系统的示例的图。

[0013] 图4是示出根据本文的实施例的系统的示例的图。

[0014] 图5描绘了可以根据本文的实施例执行的处理的示例。

[0015] 图6描绘了根据本文的实施例的装置的模块的示例。

[0016] 各附图中相同的附图标记和名称表示相同的元件。

具体实施方式

[0017] 本文描述了用于在区块链节点执行的可信执行环境(TEE)中安全地执行所请求的智能合约操作的技术。更具体地，本文的实施例使得区块链节点能够在TEE内以安全且可验证的方式执行智能合约操作，使得各方可以信任在其中执行操作的环境未被篡改或损害。

[0018] 为了提供本文实施例的进一步背景，并且如上所述，分布式账本系统(DLS)，又可以被称为共识网络(例如，由点对点节点组成)和区块链网络，使参与的实体能够安全地、不可篡改地进行交易并存储数据。尽管术语区块链通常与特定网络和/或用例相关联，但是本文使用区块链来一般地指代DLS而不涉及任何特定用例。

[0019] 区块链是以交易不可篡改的方式存储交易的数据结构。因此，区块链上记录的交易是可靠且可信的。区块链包括一个或多个区块。链中的每个区块通过包含在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。每个区块还包括时间戳、自身的加密哈希值以及一个或多个交易。已经被区块链网络中的节点验证的交易经哈希处理并被编码到默克尔(Merkle)树中。Merkle树是一种数据结构，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连接。此处理沿着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。声称是存储在树中的交易的哈希值可以通过确定其是否与树的结构一致而被快速验证。

[0020] 区块链是用于存储交易的去中心化或至少部分去中心化的数据结构，而区块链网络是通过广播、验证和确认交易等来管理、更新和维护一个或多个区块链的计算节点的网络。如上所述，区块链网络可作为公有区块链网络、私有区块链网络或联盟区块链网络被提供。本文中参考联盟区块链网络进一步详细描述了本文的实施例。然而，可以预期，本文实施例可以在任何适当类型的区块链网络中实现。

[0021] 通常，联盟区块链网络在参与实体之间是私有的。在联盟区块链网络中，共识处理由经授权的一组节点控制，所述节点可以被称为共识节点，一个或多个共识节点由各自的实体(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。

[0022] 在一些示例中，在联盟区块链网络内，提供作为跨所有节点复制的区块链的全局区块链。也就是说，所有共识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)，在联盟区块链网络内实施共识协议。例如，联盟区块链网络可以实现实用拜占庭容错(PBFT)共识，下面将进一步详细描述。

[0023] 图1是示出了可以用于执行本文的实施例的环境100的示例的图。在一些示例中，示例性环境100使实体能够参与到联盟区块链网络102中。示例性环境100包括计算设备

106,108以及网络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)和后台系统。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。

[0024] 在所描绘的示例中,计算系统106、108可以各自包括能够作为节点参与至联盟区块链网络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、平板计算设备以及智能电话。在一些示例中,计算系统106、108承载一个或多个计算机实施的服务,用于与联盟区块链网络102进行交互。例如,计算系统106可以承载第一实体(例如,用户A)的计算机实施的服务,例如第一实体使用其管理与一个或多个其他实体(例如,其他用户)的交易的交易管理系统。计算系统108可以承载第二实体(例如,用户B)的计算机实施的服务、例如第二实体使用其管理与一个或多个其他实体(例如,其他用户)的交易的交易管理系统。在图1的示例中,联盟区块链网络102被表示为节点的点对点网络(Peer-to-Peer network),并且计算系统106、108分别提供参与联盟区块链网络102的第一实体和第二实体的节点。

[0025] 图2描绘了根据本文的实施例的概念架构200的示例。所述概念架构200包括实体层202、托管服务层204和区块链网络层206。在所描绘的示例中,实体层202包括三个参与者,参与者A、参与者B和参与者C,每个参与者具有各自的交易管理系统208。

[0026] 在所描绘的示例中,托管服务层204包括用于每个交易管理系统210的接口210。在一些示例中,各自的交易管理系统208使用协议(例如,超文本传输协议安全(HTTPS))通过网络(例如,图1的网络110)与相应的接口210通信。在一些示例中,每个接口210提供各自的交易管理系统208与区块链网络层206之间的通信连接。更具体地,接口210与区块链网络层206的区块链网络212通信。在一些示例中,使用远程过程调用(RPC)进行接口210与区块链网络层206之间的通信。在一些示例中,接口210“承载”用于各自的交易管理系统208的区块链网络节点。例如,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)。

[0027] 如本文所述,提供作为点对点网络的区块链网络212,所述区块链网络212包括在区块链216中不可篡改地记录信息的多个节点214。尽管示意性地描绘了单个区块链216,但是提供了区块链216的多个副本,并且跨区块链网络212维护区块链216的多个副本。例如,每个节点214存储区块链的副本。在一些实施例中,区块链216存储与在参与联盟区块链网络的两个或更多个实体之间执行的交易相关联的信息。

[0028] 区块链(例如,图2的区块链216)由一系列区块的链组成,每个区块存储数据。示例性数据包括表示两个或更多个参与者之间的交易的交易数据。尽管本文通过非限制性示例使用了“交易”,但是可以预期,任何适当的数据可以被存储在区块链中(例如,文档、图像、视频、音频)。示例性交易可以包括但不限于有价物的交换(例如,资产、产品、服务、货币)。交易数据被不可篡改地存储在区块链中。也就是说,交易数据不能改变。

[0029] 在将交易数据存储在区块中之前,对交易数据进行哈希处理。哈希处理是将交易数据(作为字符串数据提供)转换为固定长度哈希值(也作为字符串数据提供)的处理。不可能对哈希值进行去哈希处理(un-hash)以获取交易数据。哈希处理确保即使交易数据轻微改变也会导致完全不同的哈希值。此外,如上所述,哈希值具有固定长度。也就是说,无论交易数据的大小如何,哈希值的长度都是固定的。哈希处理包括通过哈希函数处理交易数据以生成哈希值。哈希函数的示例包括但不限于输出256位哈希值的安全哈希算法(SHA)-

256。

[0030] 多个交易的交易数据被哈希处理并存储在区块中。例如，提供两个交易的哈希值，并对它们本身进行哈希处理以提供另一个哈希值。重复此处理，直到针对所有要存储在区块中的交易提供单个哈希值为止。该哈希值被称为Merkle根哈希值，并被存储在区块的头中。任何交易中的更改都会导致其哈希值发生变化，并最终导致Merkle根哈希值发生变化。

[0031] 通过共识协议将区块添加到区块链。区块链网络中的多个节点参与共识协议，并执行将区块添加到区块链中的操作。这种节点被称为共识节点。如上介绍的PBFT用作共识协议的非限制性示例。共识节点执行共识协议以将交易添加到区块链，并更新区块链网络的整体状态。

[0032] 进一步详细地，共识节点生成区块头，对区块中的所有交易进行哈希处理，并将哈希值成对地组合以生成进一步的哈希值，直到为区块中的所有交易提供单个哈希值(Merkle根哈希值)为止。将此哈希值添加到区块头中。共识节点还确定区块链中最近的区块(即，添加到区块链中的最后一个区块)的哈希值。共识节点还向区块头添加随机数(nonce)值和时间戳。

[0033] 通常，PBFT提供容忍拜占庭故障(例如，故障节点、恶意节点)的实用拜占庭状态机复制。这通过假设将发生故障(例如，假设存在独立节点故障和/或由共识节点发送的操纵消息)而在PBFT中实现。在PBFT中，以包括主共识节点和备共识节点的序列提供共识节点。定期更改主共识节点。通过区块链网络内的共识节点就区块链网络的世界状态达成一致来将交易添加到区块链。在此处理中，在共识节点之间传输消息，并且每个共识节点证明从指定的对等节点接收消息，并验证在传输期间所述消息未被修改。

[0034] 在PBFT中，在多个阶段提供共识协议，所有共识节点以同一状态开始。首先，客户端向主共识节点发送请求以调用服务操作(例如，在区块链网络内执行交易)。响应于接收所述请求，主共识节点将所述请求多播到备共识节点。所述备共识节点执行所述请求，并且每个备共识节点都向客户端发送回复。客户端等待直到收到阈值数量的回复。在一些示例中，客户端等待接收f+1个回复，其中f是区块链网络内可以容忍的故障共识节点的最大数量。最终结果是，足够数量的共识节点对于要添加到区块链的记录的顺序达成一致，并且所述记录被接受或拒绝。

[0035] 在一些区块链网络中，用密码学来维护交易的隐私。例如，如果两个节点想要保持交易隐私，以使得区块链网络中的其他节点不能看出交易的细节，则这两个节点可以对交易数据进行加密处理。示例性加密处理包括但不限于对称加密和非对称加密。对称加密是指使用单个密钥既进行加密(从明文生成密文)又进行解密(从密文生成明文)的加密处理。在对称加密中，同一密钥可用于多个节点，因此每个节点都可以对交易数据进行加密/解密。

[0036] 非对称加密使用密钥对，每个密钥对包括私钥和公钥，私钥仅对于相应节点是已知的，而公钥对于区块链网络中的任何或所有其他节点是已知的。节点可以使用另一个节点的公钥来加密数据，并且该加密的数据可以使用其他节点的私钥被解密。例如，再次参考图2，参与者A可以使用参与者B的公钥来加密数据，并将加密数据发送给参与者B。参与者B可以使用其私钥来解密该加密数据(密文)并提取原始数据(明文)。使用节点的公钥加密的消息只能使用该节点的私钥解密。

[0037] 非对称加密用于提供数字签名,这使得交易中的参与者能够确认交易中的其他参与者以及交易的有效性。例如,节点可以对消息进行数字签名,而另一个节点可以根据参与者A的该数字签名来确认该消息是由该节点发送的。数字签名也可以用于确保消息在传输过程中不被篡改。例如,再次参考图2,参与者A将向参与者B发送消息。参与者A生成该消息的哈希值,然后使用其私钥加密该哈希值以提供作为加密哈希值的数字签名。参与者A将该数字签名附加到该消息上,并将该具有数字签名的消息发送给参与者B。参与者B使用参与者A的公钥解密该数字签名,并提取哈希值。参与者B对该消息进行哈希处理并比较哈希值。如果哈希值相同,则参与者B可以确认该消息确实来自参与者A,且未被篡改。

[0038] 在一些实施例中,区块链网络的节点和/或与区块链网络通信的节点可以使用TEE进行操作。在高级别,TEE是与硬件(一个或多个处理器、存储器)的操作环境(例如,操作系统(OS)、基本输入/输出系统(BIOS))隔离的该硬件内的可信环境。更详细地,TEE是处理器的单独的安全区域,其确保主处理器内执行的代码以及在主处理器内加载的数据的机密性和完整性。在处理器内,TEE与OS并行运行。至少部分所谓的可信应用程序(TA)在TEE内执行,并且可以访问处理器和存储器。通过TEE,TA免受主OS中运行的其他应用程序的影响。此外,TEE将TA在TEE内加密地彼此隔离。

[0039] TEE的示例包括由美国加利福尼亚州圣克拉拉的英特尔公司提供的软件保护扩展(SGX)。尽管本文通过示例讨论了SGX,但是可以预期本,文的实施例可以使用任何适当的TEE来实现。

[0040] SGX提供基于硬件的TEE。在SGX中,可信硬件是中央处理单元(CPU)的核心,并且物理存储器的一部分被隔离以保护选择的代码和数据。存储器的隔离部分被称为飞地(enclave)。更具体地,飞地被提供作为存储器中的飞地页面高速缓存(EPC)并被映射到应用程序地址空间。存储器(例如,DRAM)包括用于SGX的保留随机存储器(PRM)。PRM是最低BIOS级别的连续存储器空间,并且不能被任何软件访问。每个EPC是由OS分配以在PRM中加载应用程序数据和代码的存储器集(例如,4KB)。EPC元数据(EPCM)是各个EPC的入口地址,并确保每个EPC只能由一个飞地共享。也就是说,单个飞地可以使用多个EPC,而EPC专用于单个飞地。

[0041] 在执行TA期间,处理器当访问存储在飞地中的数据时以所谓的飞地模式操作。在飞地模式下的操作对每个存储访问强制执行额外的硬件检查。在SGX中,TA被编译为可信部分和不可信部分。例如OS、BIOS、特权系统代码、虚拟机管理器(VMM)、系统管理模式(SMM)等不可访问可信部分。在操作中,TA运行并创建存储器的PRM内的飞地。由飞地内的可信部分执行的可信函数由不可信部分调用,并且在飞地内执行的代码将数据视为明文数据(未加密),并且对数据的外部访问被拒绝。可信部分提供对调用的加密响应,并且TA继续执行。

[0042] 可以执行认证处理以验证预期编码(例如,TA的可信部分)在提供SGX的TEE内正在安全地执行。通常,认证处理包括TA从质询者(例如,区块链网络中的另一节点、区块链网络的密钥管理系统(KMS))接收认证请求。作为回应,TA请求其飞地产生远程认证,也被称为引文。产生远程认证包括从飞地发送到所谓的引证飞地的本地认证,其验证本地认证并通过使用非对称认证密钥对本地认证进行签名将本地认证转换为远程认证。所述远程认证(引文)被提供给质询者(例如,区块链网络的KMS)。

[0043] 质询者使用认证验证服务来验证远程认证。对于SGX,英特尔提供英特尔认证服务

(IAS),该服务从质询者接收远程认证,并验证该远程认证。更具体地,IAS处理远程认证,并提供指示远程认证是否被验证的报告(例如,认证验证报告(AVR))。如果没有被验证,则可以指示错误。如果被验证(预期代码在TEE中正在安全执行),则质询者可以开始或继续与TA交互。例如,响应于该验证,KMS(作为质询者)可以向执行TEE的节点发出非对称加密密钥(例如,公钥和私钥对)(例如,通过密钥交换处理,例如椭圆曲线Diffie-Hellman(ECDH))以使节点能够与其他节点和/或客户端安全地通信。

[0044] 在一些区块链网络中,可以执行所谓的智能合约。智能合约可以被描述为具有影响各方的合约条款的现实世界法律合约的数字表示。在示例上下文中,在联盟区块链网络内实施、存储、更新(根据需要)并执行智能合约。与智能合约相关联的合约方(例如,买方和卖方)被表示为联盟区块链网络中的节点。在一些示例中,合约方可以包括与智能合约相关联(例如,作为智能合约的当事方)的实体(例如,商业企业)。

[0045] 更详细地,智能合约被提供作为区块链(例如,区块链网络内的节点)上执行的计算机可执行程序。智能合约包含一组预定义规则,根据所述规则,所述智能合约的各方同意彼此交互。如果满足智能合约的预定义规则,则智能合约中定义的协议将被自动执行。智能合约通常具有防篡改功能,并且促进、验证和强制执行协议或交易的协商或执行。

[0046] 图3是示出根据本文的实施例的系统300的示例的图。如图所示,系统300包括区块链网络302,区块链网络302包括区块链节点304a-d。区块链节点304a-d包括服务TEE 306a-d和密钥管理(KM)TEE 308a-d。节点304a-d可以访问智能合约服务逻辑330。密钥管理中心310可通信地耦接到节点304a-d。

[0047] 节点304a-d中的每个是参与区块链网络302并且有助于维护与区块链网络302(未示出)相关联的区块链的区块链节点。如上所述,节点304a-d可以参与与区块链网络302相关联的共识处理,可以将交易收集到区块中以添加到区块链,可以处理区块链网络302的用户请求的交易,可以执行智能合约中编码的操作,并进行与区块链管理相关的其他任务。在一些实施例中,每个节点可以是包括一个或多个处理器、存储设备和其他组件的计算设备(例如,服务器)。在一些情况下,节点304a-d通过通信网络(未示出)彼此通信并且与参与区块链网络302的其他节点通信。对于图3的其余描述,节点304a将作为示例被描述,应理解节点304b-d还可以包括节点304a的特征。

[0048] 节点304a包括服务TEE 306a。在一些实施例中,服务TEE 306a是使用TEE技术(例如,英特尔SGX)实现的安全应用环境。服务TEE 306a可以执行一个或多个软件程序或库。出于本文的目的,服务TEE 306a指的是安全环境(TEE)以及在进行所述操作的TEE内执行的软件。在一些实施例中,服务TEE 306a执行由加密的客户端请求指定的智能合约操作,并输出与智能合约操作相关联的加密结果。相对于图4以下更详细地描述了该功能。

[0049] 节点304a还包括密钥管理TEE(KM TEE)308a。在一些实施例中,KM TEE 308a是使用TEE技术(例如,英特尔SGX)实现的安全应用环境。KM TEE 308a可以执行一个或多个软件程序或库。出于本文的目的,KM TEE 308a指的是安全环境(TEE)以及在进行所述操作的TEE内执行的软件。在一些实施例中,KM TEE 308a从密钥管理中心310获得加密密钥,如以下参考图4更详细描述的。

[0050] 密钥管理中心310可以生成、存储并维护加密密钥。密钥管理中心310还可以认证KM TEE 308a-d的身份,并通过远程认证和密钥部署处理320向节点304a-d提供加密密钥。

在一些实施例中，密钥管理可以进一步向客户端提供加密密钥以与节点304a-d交互。以下相对于图4更详细地描述了该功能。在一些实施例中，密钥管理中心310可以是通过通信网络(未示出)与区块链网络302的一个或多个节点通信的一个或多个服务器或其他计算设备。密钥管理中心310还可以包括耦接到密钥管理中心310或可通过通信网络访问的一个或多个存储设备，用于存储加密密钥和其他数据。

[0051] 在一些情况下，密钥管理中心310操作以在进行加密密钥部署之前认证KM TEE 308a-d的身份。例如，在将一个或多个加密密钥(下面描述)提供给KM TEE 308a之前，密钥管理中心310可以验证KM TEE 308a的真实性。该验证确保KM TEE 308a执行的软件在被供应之后未被篡改。在一些实施例中，验证可以包括远程认证处理320，诸如如上所描述的。

[0052] 在KM TEE 308a-d从密钥管理中心310获得一个或多个加密密钥之后，密钥可以被转发到服务TEE 306a-d以执行密码操作。在一些情况下，尽管KM TEE和服务TEE对(例如，KM TEE 308a和服务TEE 306a)在单个节点(例如，节点304a)上操作，但它们每个都具有它们自己的独立TEE。结果，在KM TEE 308a-d和服务TEE 306a-d之间通信的信息通过不可信区域被发送。在这种情况下，KM TEE 308a-d可以例如通过进行本地认证处理来认证服务TEE 306a-d的身份。

[0053] 本地认证可以允许飞地在同一本地平台内向另一飞地证实其身份或真实性。例如，KM TEE 308a可以发送质询以验证服务TEE 306a的真实性。在接收质询时，服务TEE 306a可以请求节点304a的硬件(例如，CPU)生成报告，该报告包括服务TEE 306a存在于节点304a上的加密证据。报告可以被提供给KM TEE 308a以验证飞地报告是由节点304a在同一平台上生成的。在一些情况下，可以基于对称密钥系统来进行本地认证，其中仅验证报告的KM TEE 308a和生成报告的飞地硬件知道对称密钥，所述对称密钥被嵌入在节点304a的硬件平台中。

[0054] 在通过本地认证对服务TEE 306a-d进行认证之后，KM TEE 308a-d可以将一个或多个加密密钥提供给服务TEE 306a-d。在一些情况下，KM TEE 308a-d可以响应于服务TEE 306a-d的认证提供加密密钥，或者可以响应于服务TEE 306a-d的一个或多个请求提供密钥。

[0055] 智能合约服务逻辑330包括一个或多个智能合约定义。节点304a-304d从智能合约服务逻辑330执行特定操作(例如，根据客户端的请求，如图4所示)。在一些实施例中，智能合约服务逻辑330中的智能合约定义包括由区块链网络302的节点执行的指令。智能合约服务逻辑330可以包括由区块链网络302(未示出)维护的一个或多个区块链中存储的智能合约定义。

[0056] 图4是示出根据本文的实现方式的系统400的示例的图。如图所示，系统400包括节点304a(包括服务TEE 306a和KM TEE 308a)以及相对于图3描述的密钥管理中心310。系统400还包括通信地耦接到密钥管理中心310的客户端480。

[0057] 在操作中，系统400可以安全地执行智能合约指令并产生加密的操作结果(例如，包括在区块链中)。如上所述，密钥管理中心310可以在用加密密钥信任之前进行远程认证以认证KM TEE 308a的身份。在KM TEE 308被认证之后，密钥管理中心310可以向节点304a的KM TEE 308a提供解封私钥402、根密钥404和签名私钥406。密钥管理中心310还承载密封公钥414和验证公钥416。密钥管理中心310将这些密钥提供给授权客户端，以对与服务TEE

306a相关联的各种数据进行加密和解密，如下所述。

[0058] 如图所示，密钥管理中心310将密封公钥414提供给客户端480。在一些情况下，密钥管理中心310认证客户端480，并且如果客户端480被授权访问密封公钥414，则仅提供该密封公钥414。密钥管理中心310可以查询内部或外部许可资源以做出该确定。密封公钥414与提供给KM TEE 308a的解封私钥402相关联。密封公钥414和解封私钥402形成密钥对，意味着可以使用解封私钥402对用密封公钥414加密的数据进行解密。

[0059] 客户端480识别所请求的合约操作450，其是由部署在服务TEE 306a中的以太坊虚拟机(VM)460执行的智能合约操作。在一些情况下，智能合约操作450包括以智能合约编程语言编码的一个或多个指令，用于由操作为执行该语言的指令的VM执行。智能合约操作450可以包括针对与请求合约操作450相关联的智能合约的执行状态。在执行智能合约期间，区块链网络的多个节点分别执行智能合约的每个指令，并且在完成所述指令之后产生指示所述智能合约的执行状态的结果。执行状态可以包括与智能合约相关联的数据。所述合约的每个执行的指令可以改变数据的内容(例如，存储将由智能合约中的后续指令使用的值)。在执行智能合约的指令之后，区块链网络的节点在执行指令后对新执行状态达成共识。对于在智能合约中执行的每个指令进行该共识处理，从而就智能合约的执行路径以及最终关于执行的最终结果达成共识。

[0060] 在452处，客户端480对在数字信封454中所请求的合约操作450进行编码(或密封)，以便传输到由节点304a执行的服务TEE 306a。例如，客户端480生成临时对称密钥408并使用密钥408对所请求的合约操作450进行加密。然后，客户端480使用密封公钥414对临时对称密钥408进行加密，并且连接加密的合约操作450和加密密钥408以产生数字信封454。

[0061] 客户端480将数字信封454发送到节点304a，在节点304a将数字信封454提供给服务TEE 306a。在一些情况下，客户端480可以将数字信封454发送到多个节点304a-d以请求处理所请求的合约操作450。在一些情况下，客户端480可以发送使用针对于特定节点的密封公钥创建的数字信封。在相同的密封公钥414和解封私钥402与所有节点304a-d相关联的情况下，客户端480还可以将数字信封454广播到节点304a-d。

[0062] 服务TEE 306a从客户端480接收数字信封454，并从数字信封454恢复所请求的合约操作450。如图所示，服务TEE 306a使用从KM TEE 308a获得的解封私钥402对数字信封454进行解码。在一些情况下，服务TEE 306a使用解封私钥402对临时对称密钥408解密(解封)(在456处)，然后使用临时对称密钥408对所请求的合约操作450进行解密(在458处)。

[0063] 然后，服务TEE 306a使用服务TEE 306a中部署的VM 460执行所请求的合约操作450。在一些实施例中，VM 460可以是被配置为执行智能合约编程语言的指令的VM(例如以太坊VM或其他类型的VM)。在一些情况下，VM 460可以在操作450的执行期间访问服务TEE 306a外部的资源，例如，外部服务器、区块链、数据库或由操作450指示的其他资源。在一些实施例中，可以限制或拒绝访问外部资源，使得操作的整体执行仅取决于服务TEE 306a中存储的数据(例如智能合约状态)。这种类型的限制可以进一步降低篡改操作450的执行的可能性。

[0064] 由VM 460执行操作450可以产生一个或多个结果。在一些情况下，所述结果可以包括在执行操作450之后智能合约的执行状态，如上所述。在462处，智能合约操作450的结果

由服务TEE 306a使用合约密钥412进行加密。基于密钥导出函数(KDF)从根密钥404导出合约密钥412(在410处)。在一些示例中,可以基于诸如基于HMAC的提取-扩展密钥导出函数(HKDF)或伪随机函数(PRF)的迭代哈希算法进行KDF。合约密钥可以由KM TEE 308a提供给服务TEE 306a。在一些实施例中,根密钥404可以是与节点304a相关联的对称加密密钥。根密钥404还可以包括可以从根密钥404导出的一个或多个子密钥。合约密钥412可以是这些子密钥之一。在一些情况下,在462处根密钥404本身可以用于对结果进行加密。

[0065] 在对结果进行加密之后,在464处,服务TEE 308a使用由KM TEE 308a提供给服务TEE 306a的签名私钥406对加密结果进行签名,以便产生签名结果466。这可以允许第三方(例如,客户端)稍后使用由密钥管理中心310维护的验证公钥416(与签名私钥406相应地配对)来验证签名结果。在一些情况下,由签名私钥406对加密结果进行签名可以包括对加密结果与用于对所述结果加密的合约密钥412一起进行加密。在这种情况下,持有验证公钥416的第三方可以首先对合约密钥412进行解密,并进一步使用合约密钥412对所述结果进行解密。

[0066] 在一些情况下,服务TEE 306a可以将签名结果466存储在区块链中。如上所述,持有验证公钥416的第三方可以使用密钥来对结果466进行解密以便进行检验。例如,客户端480可以从密钥管理中心310检索验证公钥416(例如,如前所述经过认证),并且可以使用验证公钥416访问签名结果466并对签名结果466进行解密。然后,客户端480可以请求服务TEE 306a执行智能合约中的下一操作,可以将所请求的下一操作以及智能合约的执行状态(来自解密的签名结果466)包括在发送到服务TEE 306a的数字信封中。

[0067] 图5描绘了可以根据本文的实施例执行的处理的示例。在502处,参与区块链网络(例如,302)的区块链节点(例如,304a)接收用于执行由区块链节点承载的服务TEE中的一个或多个软件指令的请求,其中所述请求由与服务TEE相关联的公钥进行加密。

[0068] 在504处,所述区块链节点使用与服务TEE相关联的第一私钥对所述请求进行解密,其中所述第一私钥与所述公钥配对。

[0069] 在506处,所述区块链节点执行一个或多个软件指令以产生加密结果。

[0070] 在508处,所述区块链节点使用与服务TEE相关联的客户端加密密钥对执行结果进行加密,以产生加密结果。

[0071] 在510处,所述区块链节点使用与服务TEE相关联的第二私钥对加密结果进行签名,以产生签名的加密结果。

[0072] 在一些情况下,所述公钥是第一公钥,并且所述客户端加密密钥是第二公钥或基于密钥导出函数从根密钥导出的对称密钥之一。

[0073] 在一些情况下,区块链节点还承载密钥管理TEE,该密钥管理TEE存储第一私钥和/或第二私钥,并且在基于进行由密钥管理TEE发起的本地认证来认证服务TEE的身份之后,密钥管理TEE将第一私钥、第二私钥和根密钥提供给服务TEE。

[0074] 在一些情况下,第一私钥、第二私钥和根密钥是由密钥管理中心生成的,并且在基于进行由密钥管理中心发起的本地认证来认证密钥管理TEE的身份之后,被提供给密钥管理TEE。

[0075] 在一些情况下,响应于服务TEE的重启操作,由密钥管理TEE将第一私钥和根密钥提供给服务TEE。

[0076] 在一些情况下，一个或多个软件指令与智能合约相关联，并且所述根密钥是基于智能合约的状态从密钥管理TEE中存储的多个根密钥中选择的。

[0077] 在某些情况下，第一公钥是由密钥管理中心生成的，并被提供给客户端以对请求进行加密。

[0078] 在一些情况下，所述区块链节点接收到的请求还包括使用客户端加密密钥对一个或多个软件指令进行加密。

[0079] 在某些情况下，用第一私钥对请求进行解密还包括：使用第一私钥对客户端加密密钥进行解密；以及使用客户端加密密钥对一个或多个软件指令进行解密。

[0080] 图6描绘了根据本文的实施例的装置600的模块的示例。装置600可以是在区块链网络内执行的区块链节点的示例实施例。装置600可以对应于上述实施例，并且装置600包括以下：接收模块602，接收用于执行由区块链节点承载的服务TEE中的一个或多个软件指令的请求，其中所述请求由与服务TEE相关联的公钥进行加密；解密模块604，使用与服务TEE相关联的第一私钥对所述请求进行解密，其中所述第一私钥与所述公钥配对；执行模块606，执行一个或多个软件指令以产生执行结果；加密模块608，使用与服务TEE相关联的客户端加密密钥对所述执行结果进行加密，以产生加密结果；签名模块610，使用与服务TEE相关联的第二私钥对加密结果进行签名，以产生签名的加密结果。

[0081] 在先前实施例中示出的系统、装置、模块或单元可以通过使用计算机芯片或实体来实现，或者可以通过使用具有特定功能的产品来实现。典型的实施例设备是计算机，计算机可以是个人计算机、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、可穿戴设备或这些设备的任意组合。

[0082] 对于装置中每个模块的功能和角色的实施例处理，可以参考前一方法中相应步骤的实施例处理。为简单起见，这里省略了细节。

[0083] 由于装置实施例基本上对应于方法实施例，对于相关部分，可以参考方法实施例中的相关描述。先前描述的装置实施例仅是示例。被描述为单独部分的模块可以是或不是物理上分离的，并且显示为模块的部分可以是或不是物理模块，可以位于一个位置，或者可以分布在多个网络模块上。可以基于实际需求来选择一些或所有模块，以实现本文方案的目标。本领域普通技术人员无需付出创造性劳动就能理解和实现本申请的实施例。

[0084] 再次参考图6，它可以被解释为示出在区块链网络内执行并且用作执行主体的区块链节点的内部功能模块和结构。本质上，执行主体可以是电子设备，电子设备包括下面：一个或多个处理器；以及被配置为存储一个或多个处理器的可执行指令的存储器。

[0085] 本文中描述的技术产生一种或多种技术效果。例如，所描述的技术使得联盟区块链网络的各方能够验证网络中负责执行智能合约操作并且针对这些操作的结果达成共识的区块链节点未被攻击者破坏。该验证具有减少防止或降低攻击者控制一个或多个区块链节点并成功篡改智能合约操作或共识处理的执行的可能性的效果，从而通往更能抵御攻击的联盟区块链网络的更安全的实施例。

[0086] 所描述的主题的实施例可以包括单独或组合的一个或多个特征。一个实施例包括一种计算机实现的方法，包括以下动作：由参与区块链网络的区块链节点接收用于执行由区块链节点承载的服务TEE中的一个或多个软件指令的请求，其中所述请求由与服务TEE相

关联的公钥进行加密;由区块链节点在服务TEE中使用与服务TEE相关联的第一私钥对所述请求进行解密,其中所述第一私钥与所述公钥配对;响应于对所述请求进行了解密,由区块链节点在服务TEE中执行一个或多个软件指令以产生执行结果;由区块链节点在服务TEE中使用与服务TEE相关联的客户端加密密钥对所述执行结果进行加密,以产生加密结果;以及,由区块链节点在服务TEE中使用与服务TEE相关联的第二私钥对所述加密结果进行签名,以产生签名的加密结果。

[0087] 前述和其他描述的实施例可以各自可选地包括以下特征中的一个或多个:

[0088] 第一特征,可与以下任何特征组合,指定所述公钥是第一公钥,并且所述客户端加密密钥是第二公钥或基于密钥导出函数从根密钥导出的对称密钥之一。

[0089] 第二特征,可与前述或以下特征中的任何特征组合,指定所述区块链节点还承载密钥管理TEE,该密钥管理TEE存储第一私钥和/或第二私钥,并且在基于进行由密钥管理TEE发起的本地认证来认证服务TEE的身份之后,所述密钥管理TEE将第一私钥、第二私钥和根密钥提供给服务TEE。

[0090] 第三特征,可与前述或以下特征中的任何特征组合,指定第一私钥、第二私钥和根密钥是由密钥管理中心生成的,并且在基于进行由密钥管理中心发起的远程认证来认证密钥管理TEE的身份之后,被提供给密钥管理TEE。

[0091] 第四特征,可与前述或以下特征中的任何特征组合,指定响应于服务TEE的重启操作,由密钥管理TEE向服务TEE提供第一私钥和根密钥。

[0092] 第五特征,可与前述或以下特征中的任何特征组合,指定所述一个或多个软件指令与智能合约相关联,并且其中所述根密钥是基于智能合约的状态从密钥管理TEE中存储的多个根密钥中选择的。

[0093] 第六特征,可与前述或以下特征中的任何特征组合,指定所述第一公钥是由密钥管理中心生成的并被提供给客户端以对所述请求进行加密。

[0094] 第七特征,可与前述或以下特征中的任何特征组合,指定由所述区块链节点接收到的请求还包括使用客户端加密密钥对一个或多个软件指令进行加密。

[0095] 第八特征,可与前述或以下特征中的任何特征组合,指定使用第一私钥对所述请求进行解密还包括:使用第一私钥对客户端加密密钥进行解密;并且使用客户端加密密钥对一个或多个软件指令进行解密。

[0096] 第九特征,可与前述或以下特征中的任何特征组合,指定所述密钥管理中心存储与第二私钥相对应的验证公钥,并将验证公钥提供给客户端以验证签名的加密结果。

[0097] 本文中描述的主题、动作以及操作的实施例可以在数字电子电路、有形体现的计算机软件或固件、计算机硬件中实现,包括本文中公开的结构及其结构等同物,或者它们中的一个或多个的组合。本文中描述的主题的实施例可以被实现为一个或多个计算机程序,例如,一个或多个计算机程序指令模块,编码在计算机程序载体上,用于由数据处理装置执行或控制数据处理装置的操作。例如,计算机程序载体可以包括具有编码或存储在其上的指令的一个或多个计算机可读存储介质。所述载体可以是有形的非暂态计算机可读介质,例如磁盘、磁光盘或光盘、固态驱动器、随机存取存储器(RAM)、只读存储器(ROM)或其他类型介质。可选地或附加地,载体可以是人工生成的传播信号,例如,机器生成的电、光或电磁信号,其被生成来编码信息用于传输到合适的接收器装置以供数据处理装置执行。计算机

存储介质可以是或部分是机器可读存储设备、机器可读存储基板、随机或串行存取存储器设备或它们中的一个或多个的组合。计算机存储介质不是传播信号。

[0098] 计算机程序也可以被称为或描述为程序、软件、软件应用程序、app、模块、软件模块、引擎、脚本或代码，可以以任何形式的编程语言编写，包括编译或解释性语言、声明或过程性语言；并且它可以被配置为任何形式，包括作为独立程序，或者作为模块、组件、引擎、子例程或适合在计算环境中执行的其他单元，该环境可以包括由通信数据网络互联的在一个或多个位置的一台或多台计算机。

[0099] 计算机程序可以但非必须对应于文件系统中的文件。计算机程序可以被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、子程序或代码部分的多个文件。

[0100] 用于执行计算机程序的处理器包括，例如，通用微处理器和专用微处理器两者，和任意种类数码计算机的任意一个或多个处理器。通常，处理器将从耦接到所述处理器的非暂态计算机可读介质接收用于执行的计算机程序的指令以及数据。

[0101] 术语“数据处理装置”包括用于处理数据的所有类型的装置、设备和机器，包括例如可编程处理器、计算机或者多个处理器或计算机。数据处理装置可以包括专用逻辑电路，例如FPGA(现场可编程门阵列)、ASIC(专用集成电路)或GPU(图形处理单元)。除了硬件，该装置还可以包括为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、操作系统或者它们中的一个或多个的组合的代码。

[0102] 本文中描述的处理和逻辑流程可以由一台或多台计算机或处理器执行一个或多个计算机程序来进行，以进行通过对输入数据进行运算并生成输出的操作。处理和逻辑流程也可以由例如FPGA、ASIC、GPU等的专用逻辑电路或专用逻辑电路与一个或多个编程计算机的组合来执行。

[0103] 适合于执行计算机程序的计算机可以基于通用微处理器和/或专用微处理器，或任何其他种类的中央处理单元。通常，中央处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的元件可以包括用于执行指令的中央处理单元以及用于存储指令和数据的一个或多个存储器设备。中央处理单元和存储器可以补充有专用逻辑电路或集成在专用逻辑电路中。

[0104] 通常，计算机还将包括一个或多个存储设备或可操作地耦接为从一个或多个存储设备接收数据或将数据传输到一个或多个存储设备。存储设备可以是例如磁盘、磁光盘或光盘，固态驱动器或任何其他类型的非暂态计算机可读介质。但是，计算机不需要具有这样的设备。因此，计算机可以耦接到本地和/或远程的一个或多个存储设备，例如一个或多个存储器。例如，计算机可以包括作为计算机的组成部分的一个或多个本地存储器，或者计算机可以耦接到云网络中的一个或多个远程存储器。此外，计算机可以被嵌入在另一个设备中，例如移动电话、个人数字助理(PDA)、移动音频或视频播放器、游戏控制台、全球定位系统(GPS)接收器或例如通用串行总线(USB)闪存驱动器的便携式存储设备，仅举几例。

[0105] 组件可以通过彼此通信地例如电连接或光学连接直接地或经由一个或多个中间组件彼此“耦接”。如果组件中的一个组件集成到另一个组件中，则组件也可以彼此“耦接”。例如，存储组件集成到处理器(例如，L2高速缓存组件)中即“耦接到”处理器中。

[0106] 为了提供与用户的交互，本文中描述的主题的实施例可以在计算机上实现或配置为与该计算机通信，该计算机具有：显示设备，例如，LCD(液晶显示器)监视器，用于向用户显示信息；以及输入设备，用户可以通过该输入设备向该计算机提供输入，例如键盘和例如鼠标、轨迹球或触摸板等的指针设备。其他类型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以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；并且可以接收来自用户的任何形式的输入，包括声音、语音或触觉输入。此外，计算机可以通过向用户使用的设备发送文档和从用户使用的设备接收文档来与用户交互；例如，通过对从用户设备上的web浏览器接收到的请求做出响应来向该web浏览器发送web页面，或者通过与例如智能电话或电子平板电脑等的用户设备上运行的应用程序(app)进行交互。此外，计算机可以通过向个人设备(例如，运行消息应用的智能手机)发送文本消息或其他形式的消息并作为回应接收来自用户的响应消息来与用户交互。

[0107] 本文使用与系统、装置和计算机程序组件有关的术语“被配置为”。对于被配置为执行特定操作或动作的一个或多个计算机的系统，意味着系统已经在其上安装了在运行中促使该系统执行所述操作或动作的软件、固件、硬件或它们的组合。对于被配置为执行特定操作或动作的一个或多个计算机程序，意味着一个或多个程序包括当被数据处理装置执行时促使该装置执行所述操作或动作的指令。对于被配置为执行特定操作或动作的专用逻辑电路，意味着该电路具有执行所述操作或动作的电子逻辑。

[0108] 虽然本文包括许多具体实施细节，但是这些不应被解释为由权利要求书本身限定的对要求保护的范围的限制，而是作为对特定实施例的具体特征的描述。在本文多个单独实施例的上下文中描述的多个特定特征也可以在单个实施例中的组合实现。相反，在单个实施例的上下文中描述的各种特征也可以单独地或以任何合适的子组合在多个实施例中实现。此外，尽管上面的特征可以被描述为以某些组合起作用并且甚至最初被如此要求保护，但是在一些情况下，可以从要求保护的组合中删除来自该组合的一个或多个特征，并且权利要求书可以指向子组合或子组合的变体。

[0109] 类似地，虽然以特定顺序在附图中描绘了操作并且在权利要求书中叙述了操作，但是这不应该被理解为：为了达到期望的结果，要求以所示的特定顺序或依次执行这些操作，或者要求执行所有示出的操作。在一些情况下，多任务并行处理可能是有利的。此外，上述实施例中的各种系统模块和组件的划分不应被理解为所有实施例中都要求如此划分，而应当理解，所描述的程序组件和系统通常可以被一起集成在单个软件产品中或者被打包成多个软件产品。

[0110] 已经描述了主题的特定实施例。其他实施例在以下权利要求书的范围内。例如，权利要求书中记载的动作可以以不同的顺序执行并且仍然实现期望的结果。作为一个示例，附图中描绘的处理无需要求所示的特定顺序或次序来实现期望的结果。在一些情况下，多任务并行处理可能是有利的。

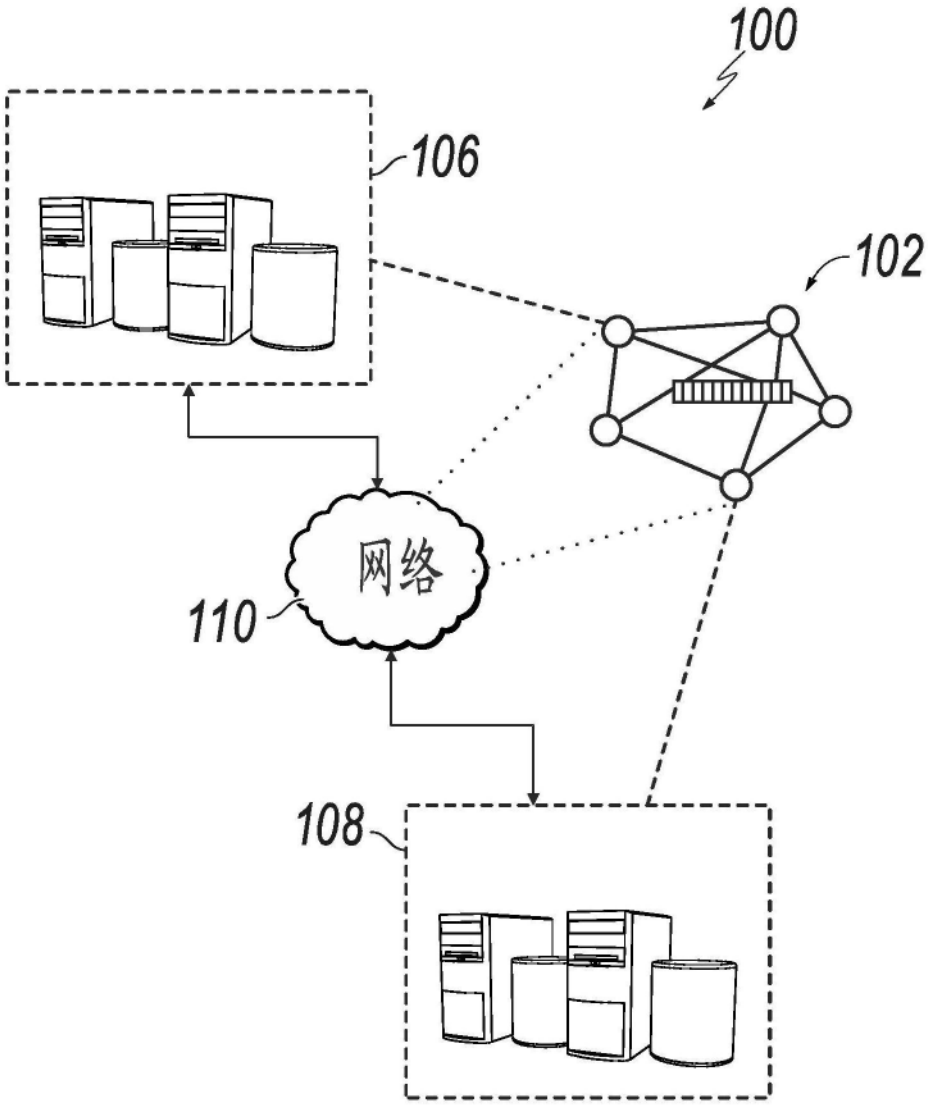


图1

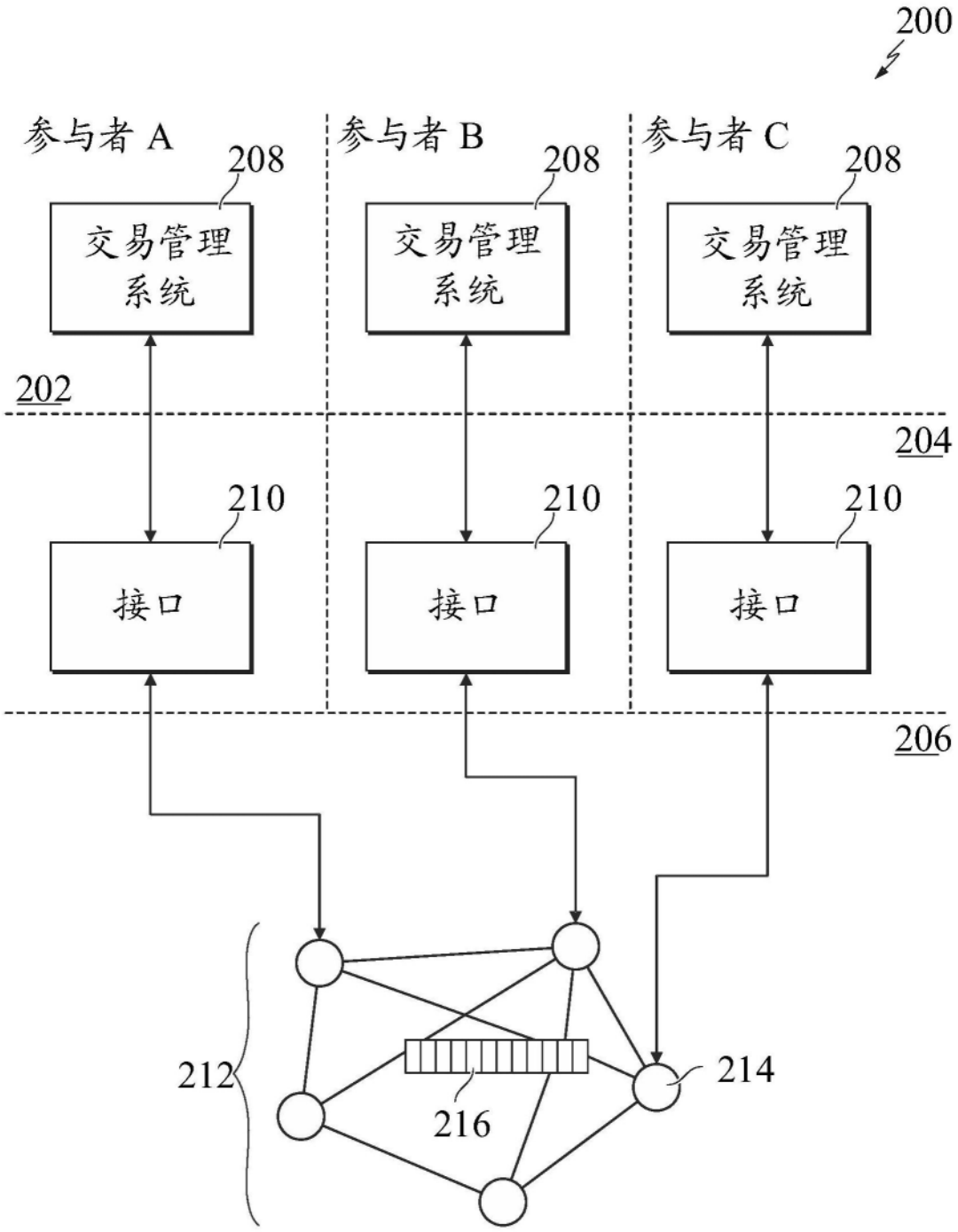

200
参与者 A
参与者 B
参与者 C
208
208
208
交易管理系统
交易管理系统
交易管理系统
202
204
210
210
210
接口
接口
接口
206
212
214
216

图2

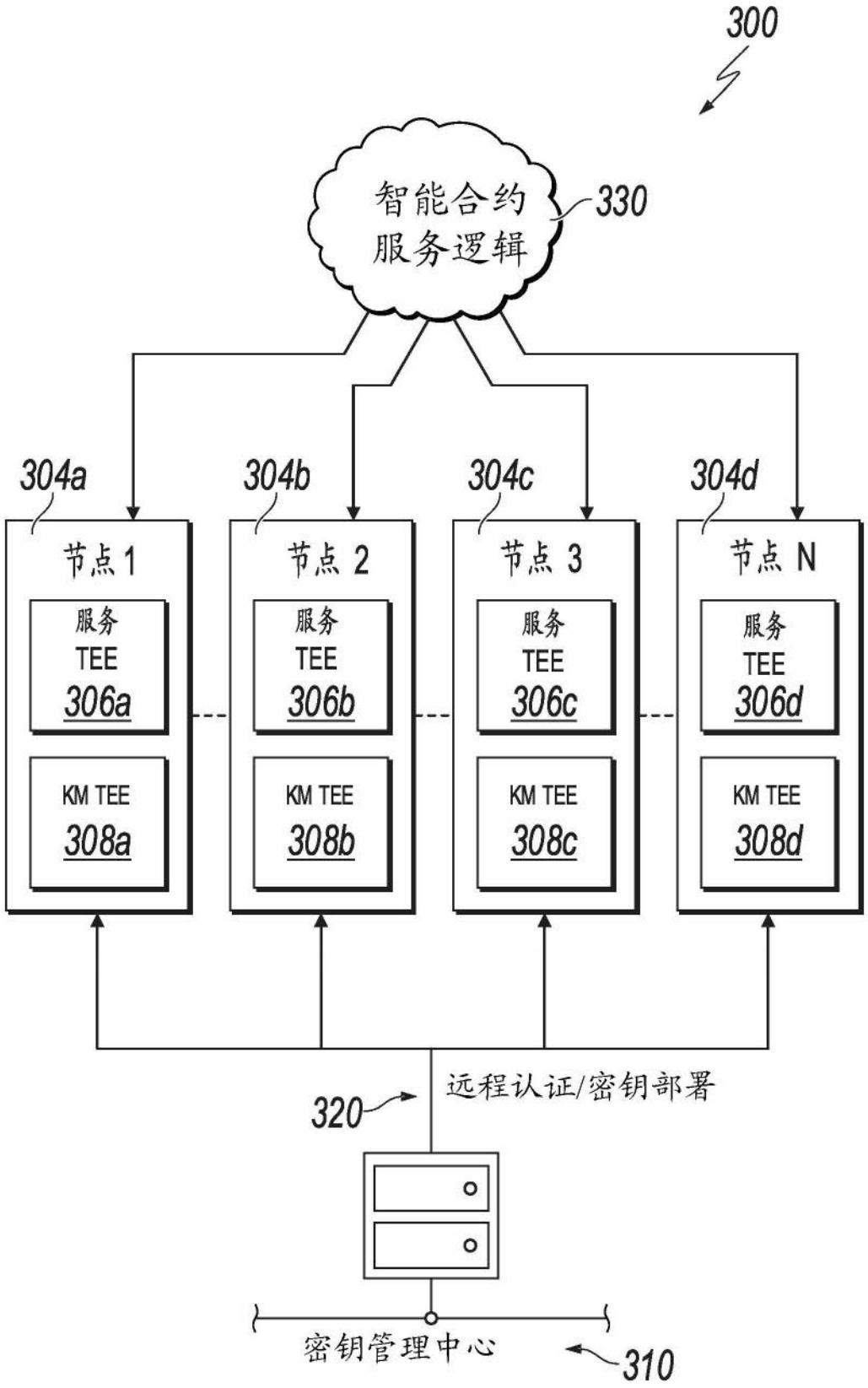

300
智能合约
服务逻辑
330
304a
304b
304c
304d
节点 1
节点 2
节点 3
节点 N
服务
TEE
306a
306b
306c
306d
KM TEE
308a
308b
308c
308d
320
远程认证/密钥部署
密钥管理中心
310

图3

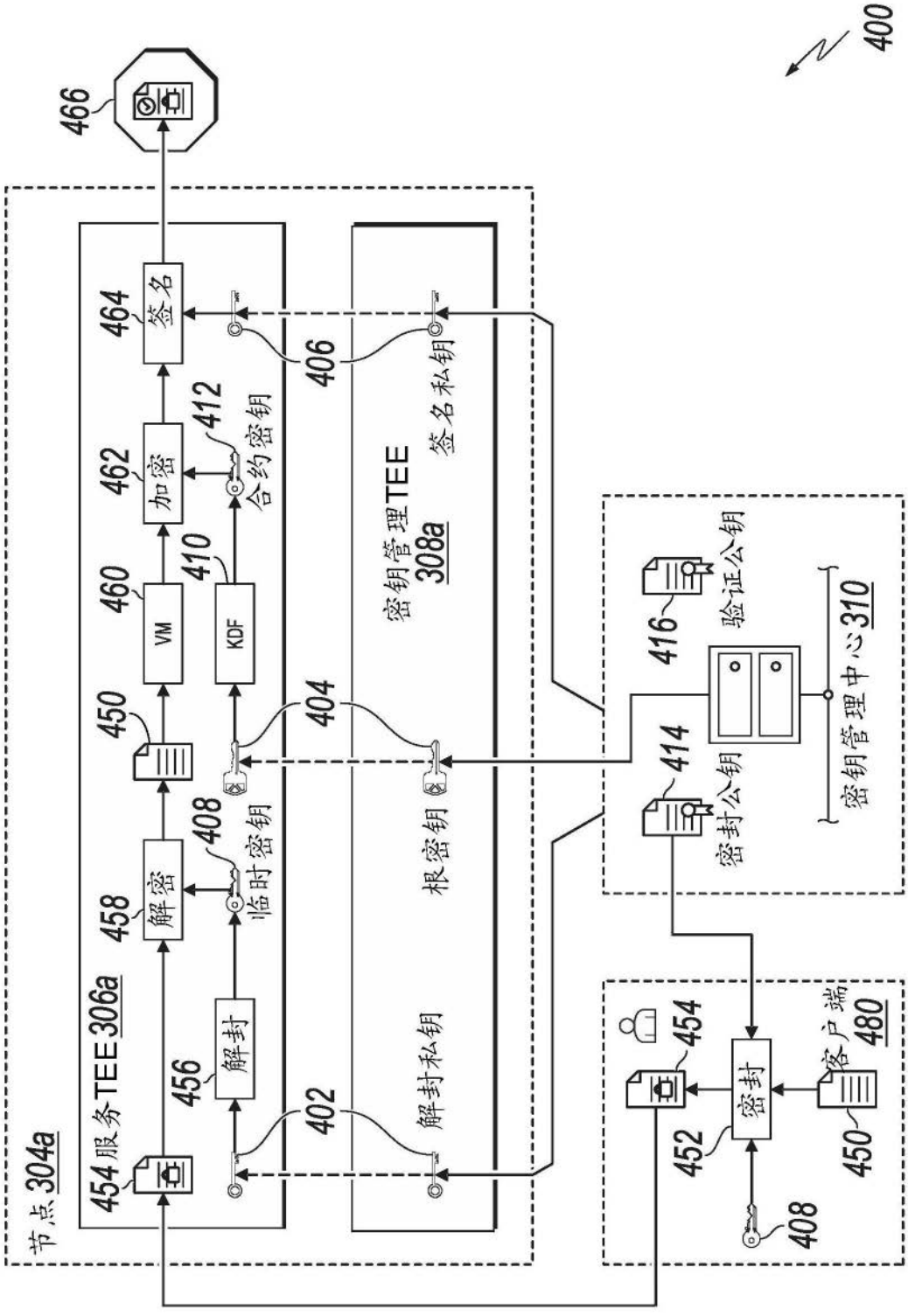

400
466
节点 304a
服务TEE 306a
454
456
458
解密
解封
402
解封私钥
408
临时密钥
450
404
根密钥
密钥管理TEE
308a
签名私钥
406
460
VM
410
KDF
412
合约密钥
462
加密
464
签名
416
验证公钥
414
密封公钥
密钥管理中心 310
454
452
密封
客户端
480
450
408

图4

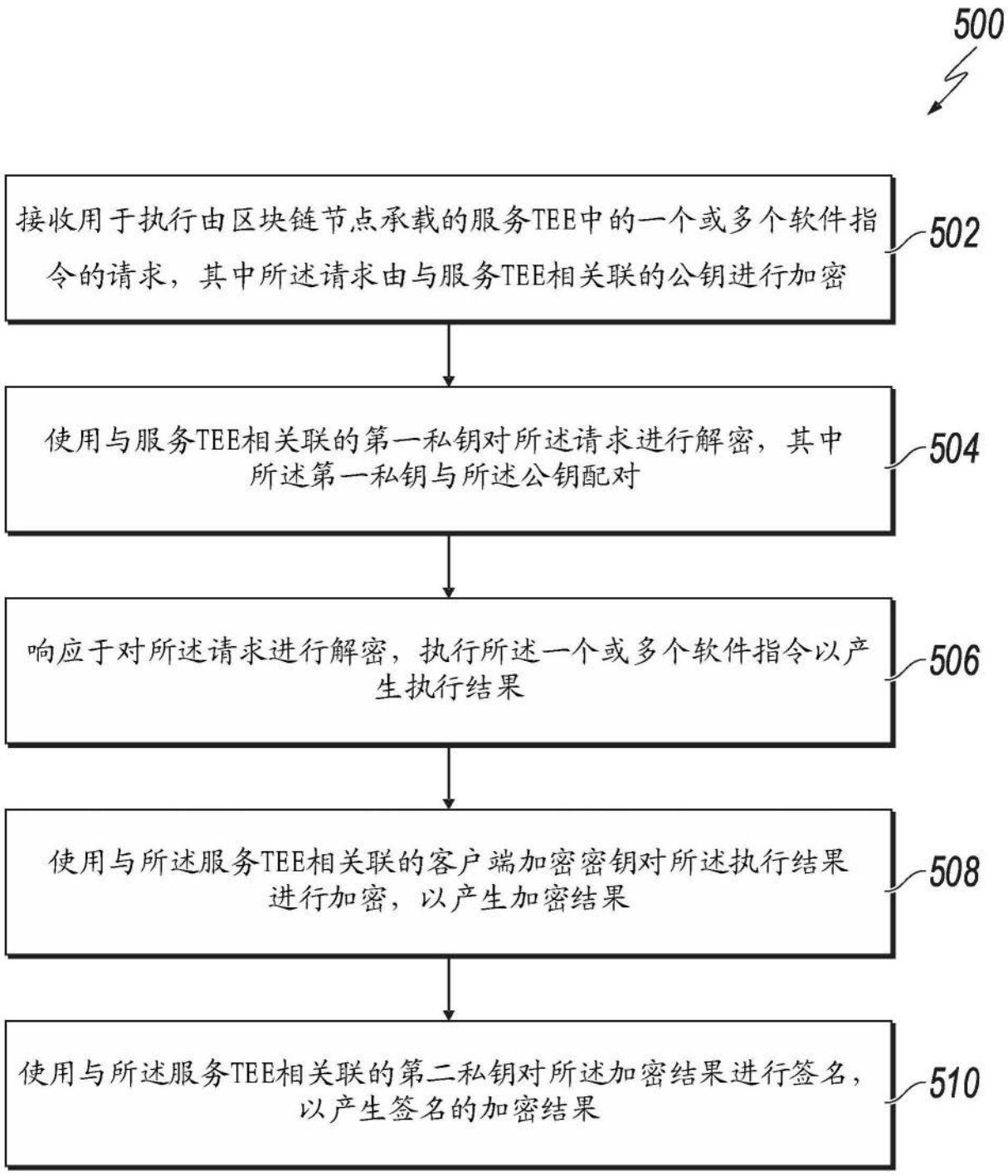

500
接收用于执行由区块链节点承载的服务TEE中的一个或多个软件指令的请求，其中所述请求由与服务TEE相关联的公钥进行加密
502
使用与服务TEE相关联的第一私钥对所述请求进行解密，其中所述第一私钥与所述公钥配对
504
响应于对所述请求进行解密，执行所述一个或多个软件指令以产生执行结果
506
使用与所述服务TEE相关联的客户端加密密钥对所述执行结果进行加密，以产生加密结果
508
使用与所述服务TEE相关联的第二私钥对所述加密结果进行签名，以产生签名的加密结果
510

图5

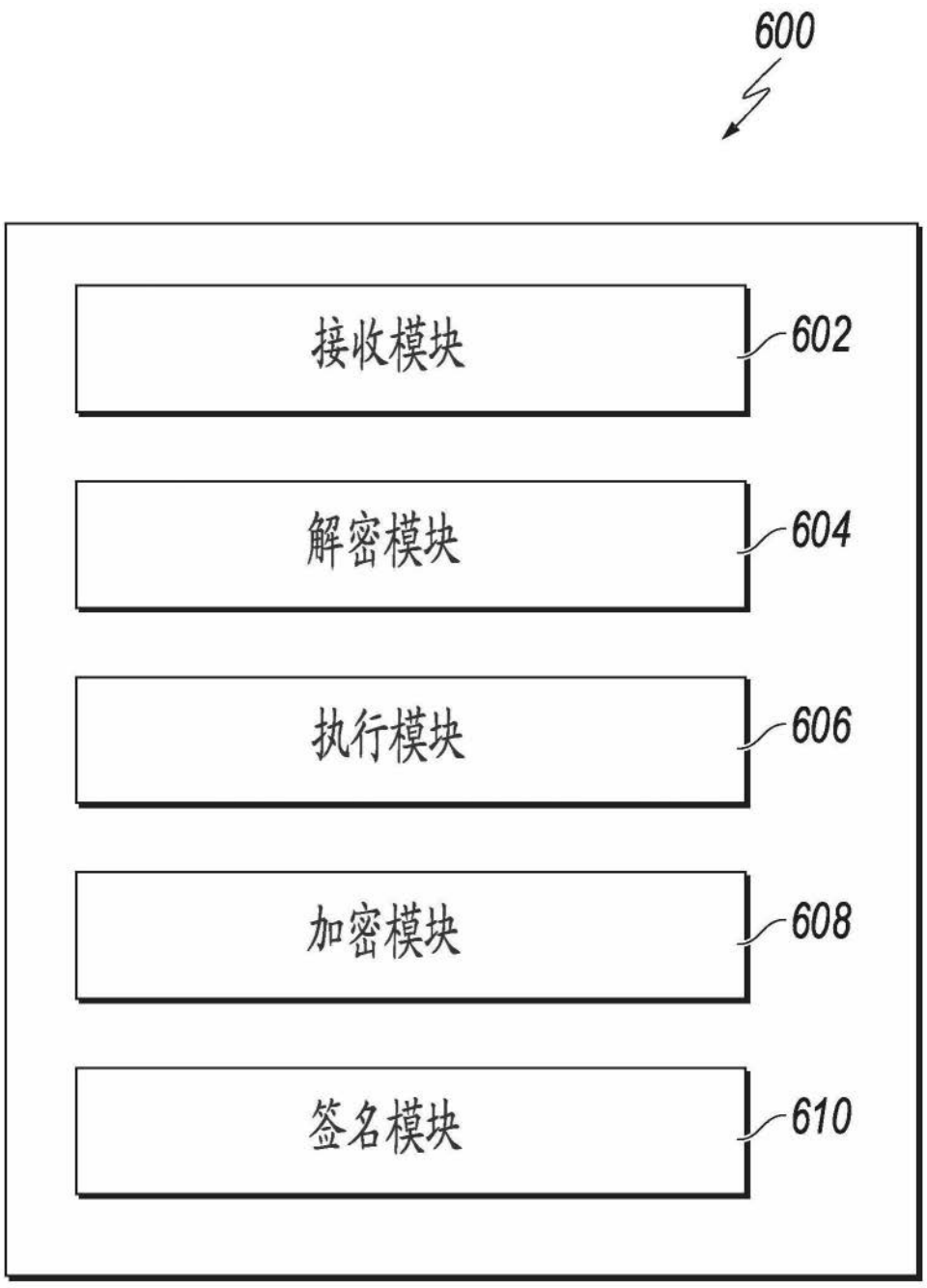


图6