



(21) 申请号 202310095224.4

(22) 申请日 2019.03.27

(65) 同一申请的已公布的文献号
申请公布号 CN 116132162 A

(43) 申请公布日 2023.05.16

(62) 分案原申请数据
201980004196.2 2019.03.27

(73) 专利权人 蚂蚁链技术有限公司
地址 新加坡美芝路128号国浩时代城#20-01

(72) 发明人 余逸荣

(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 申亚辉

(51) Int.Cl.

H04L 9/40 (2022.01)

H04L 67/63 (2022.01)

H04L 9/32 (2006.01)

(56) 对比文件

CN 107395349 A, 2017.11.24

CN 108259594 A, 2018.07.06

审查员 张伟

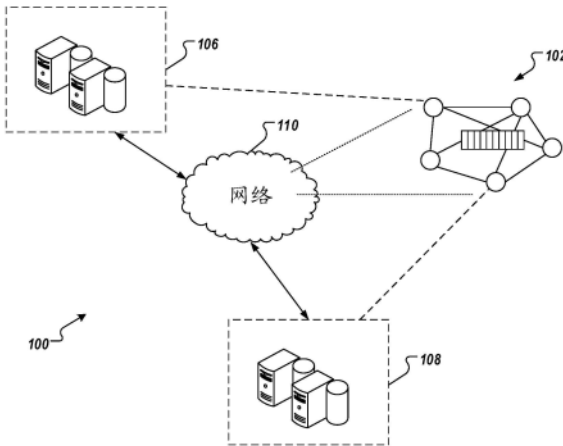
权利要求书1页 说明书18页 附图6页

(54) 发明名称

使用高可用性的可信执行环境检索区块链网络的公共数据

(57) 摘要

一种用于增强区块链网络安全性的方法、系统和装置,包括编码在计算机存储介质上的计算机程序。实施方式包括接收针对来自数据源的数据的请求;将所述请求发送至位于区块链网络外部并且包括多节点集群的中继系统,该多节点集群包括多个中继系统节点;接收从中继系统节点提供的结果,该结果被使用中继系统节点的私钥数字地签名;验证中继系统节点被注册;响应于验证了中继系统节点被注册而基于中继系统节点的公钥和结果的数字签名来验证结果的完整性;响应于验证了结果的完整性而将结果发送至客户端。



1. 一种计算机实现的用于从位于区块链网络外部的数据源检索数据的方法,所述方法应用于在所述区块链网络内执行的中继系统智能合约,所述方法包括:

从所述区块链网络内的客户端接收针对来自所述数据源的数据的请求;

将所述请求发送至位于所述区块链网络外部的中继系统的中继系统控制器,以使得所述中继系统控制器选择具有可用状态的中继系统节点,并且将所述请求发送到所述中继系统节点;其中,所述中继系统控制器周期性向多个中继系统节点发送状态查询,将预设时间窗内反馈了状态响应的中继系统节点的状态记录为可用;

接收从所述中继系统节点提供的结果,所述结果具有使用所述中继系统节点的私钥生成的数字签名,所述结果包括所请求的来自所述数据源的数据;

响应于验证了所述中继系统节点被注册在所述中继系统智能合约上,基于所述中继系统节点的公钥和所述数字签名验证所述结果的完整性,以及响应于验证了所述结果的完整性,将所述结果发送至所述客户端。

2. 根据权利要求1所述的方法,所述基于所述中继系统节点的公钥和所述数字签名验证所述结果的完整性,包括:

通过将第一哈希值与第二哈希值进行比较来验证所述结果的完整性,所述第一哈希值是通过使用所述公钥对所述数字签名进行解密确定的,所述第二哈希值是使用所述结果和哈希函数计算的。

3. 根据权利要求1所述的方法,其中,所述中继系统节点执行可信执行环境TEE,以及所述中继系统节点的所述公钥和所述私钥是在所述TEE的认证处理期间提供的。

4. 根据权利要求3所述的方法,其中,中继系统控制器对每个中继系统节点执行所述认证处理,所述中继系统控制器向所述中继系统智能合约提供每个中继系统节点的公钥。

5. 根据权利要求1所述的方法,其中,所述数据源包括基于互联网的数据源。

6. 根据权利要求1所述的方法,其中,所述客户端包括客户端智能合约。

7. 根据权利要求1所述的方法,其中,所述中继系统控制器将预设时间窗内未反馈状态响应的中继系统节点的状态记录为不可用。

8. 根据权利要求3所述的方法,其中,所述TEE包括:软件保护扩展SGX。

9. 一种用于从位于区块链网络外部的数据源检索数据的装置,所述装置包括用于执行权利要求1至8中的任一项所述的方法的多个模块。

10. 一种用于从位于区块链网络外部的数据源检索数据的系统,包括:

一个或多个计算机;以及

一个或多个计算机可读存储器,其耦接至所述一个或多个计算机并且其上存储有指令,所述指令能够由所述一个或多个计算机执行以执行权利要求1至8中的任一项所述的方法。

使用高可用性的可信执行环境检索区块链网络的公共数据

技术领域

[0001] 本文涉及从外部数据源向区块链网络提供数据。

背景技术

[0002] 分布式账本系统(DLS),也可以称为共识网络和/或区块链网络,使参与实体能够安全且永久地存储数据。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。区块链网络的类型示例可以包括为一组选定实体提供的联盟区块链网络,所述实体控制共识处理,并且所述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先定义的规则,在所述规则下智能合约同意的各方彼此交互。如果智能合约的预定义规则得到满足,则智能合约中定义的协议自动执行。智能合约通常是防篡改的,并且可以促进、验证和执行协议或交易的谈判或执行。

[0004] 在一些情况下,在区块链网络内运行的智能合约需要来自区块链网络外部的输入来评估预先定义的规则并执行相应的动作。然而,智能合约本身不能直接访问外部数据源。因此,中继代理可被用来检索外部数据,并将数据提交给区块链以通过智能合约处理。但是,此过程可能会导致安全问题,诸如潜在的攻击向量(例如,分布式拒绝服务(DDoS)攻击)。此外,每个客户端会需要对远程代理分别进行身份验证,这会妨碍可扩展性,并且增加资源开销(例如,处理器、带宽)。在一些情况下,客户端提交的每个请求都由客户端已经验证过的某个中继代理处理。如果中继代理失败或无法访问,则客户端请求不能被正确处理,从而导致服务不可用。

[0005] 尽管已经提出了解决与从外部数据源的数据检索相关的安全性和其他问题的技术,但解决这些问题的更有效的方案将是有利的。

发明内容

[0006] 本文描述了从外部数据源检索数据以供在区块链网络内处理的技术。

[0007] 本文的实施方式涉及一种包括多节点集群的中继系统,该多节点集群被用于以可验证和高可用性的方式从外部数据源检索公共可用的数据和/或服务。在一些实施方式中,对多节点集群中的多个中继系统节点中的每个执行远程认证,所述远程认证分别为每个中继系统节点生成密钥对(公钥、私钥)。每个中继系统节点使用可信执行环境(TEE)操作。中继系统智能合约被用于中继系统节点的远程认证,其可以公开审核,消除了个别客户重复远程认证的需要。经验证的中继系统节点由中继系统智能合约注册以供使用。中继系统控制器可以周期性检查和记录多节点集群中每个中继系统节点的状态。中继系统控制器将每个客户端请求分配给多节点集群中的可用中继系统节点,以查询外部数据源。使用中继系统节点的私钥对包括查询结果的响应进行数字签名。中继系统智能合约可以验证该响应是否是由注册的中继系统节点发送的。响应的完整性可通过中继系统智能合约使用中继系统节点的公钥来验证。

[0008] 本文中描述的主题作为特定实施方式提供,实现了一个或多个以下技术优点。在一些实施方式中,提供用于从外部数据源检索或访问数据和/或服务的多节点集群,其中多节点集群中的中继系统节点的状态由中继系统控制器周期性检查和记录。如本文所述,通过将中继系统节点部署在集群中,中继系统控制器可以自动将客户服务请求分配给集群中可用的中继系统节点,从而避免由于个别中继系统节点故障而导致服务不可用。因此,本文的实施方式提高了用于查询互联网数据源的中继系统的整体服务可用性。在一些实施方式中,确保从外部数据源返回到区块链网络的响应的完整性。因此,本文的实施方式提高了区块链网络与中继系统的组件之间通信的完整性,该中继系统的组件被用于检索区块链网络外部的数据。通过这种方式,减少了恶意用户的潜在攻击通道从而增强了安全性。在一些实施方式中,中继系统有助于避免用户与中继系统节点之间的直接接触,从而避免暴露中继系统节点的位置或访问点。因此,中继系统节点不太可能被网络上的恶意参与者以多种形式发现和攻击,例如,诸如分布式拒绝服务 (DDoS) 攻击。这提高了中继系统节点的安全性,从而进一步提高了区块链网络与中继系统节点之间通信的安全性。

[0009] 本文也提供一个或多个非暂时性计算机可读存储介质,其耦接至一个或多个处理器并且其上存储有指令,当所述指令由一个或多个处理器执行时,促使所述一个或多个处理器按照本文提供的方法的实施方式执行操作。

[0010] 本文还提供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至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,当所述指令由一个或多个处理器执行时,促使所述一个或多个处理器按照本文提供的方法的实施方式执行操作。

[0011] 可理解的是,根据本文的方法可以包括本文描述的方面和特征的任意结合。也就是,根据本文的方法不限于本文具体描述的方面和特征的结合,而是包括所提供的方面和特征的任意结合。

[0012] 本文的一个或多个实施方式的细节在附图和以下的描述中阐述。本文的其他特征和优点将从描述和附图以及权利要求而显见。

附图说明

[0013] 图1为示出可被用于执行本文的实施方式的环境示例的图示。

[0014] 图2为根据本文的实施方式的概念性架构的示例的图示。

[0015] 图3为根据本文的实施方式的系统示例的图示。

[0016] 图4绘出根据本文的实施方式的信号流示例。

[0017] 图5绘出根据本文的实施方式的信号流示例。

[0018] 图6绘出根据本文的实施方式的信号流示例。

[0019] 图7绘出根据本文的实施方式可执行的处理示例。

[0020] 图8绘出根据本文的实施方式的设备的模块示例。

[0021] 在不同的附图中,相同的附图标记和标识表示相同的元件。

具体实施方式

[0022] 本文描述了从外部数据源检索数据以在区块链网络内处理的技术。本文的实施方

式涉及一种中继系统,该中继系统包括被用于以可验证和高可用性的方式从外部数据源检索或访问数据和/或服务的多节点集群。在一些实施方式中,对多节点集群中的多个中继系统节点中的每一个执行远程认证,远程认证为每个中继系统节点分别产生密钥对(公钥、私钥)。每个中继系统节点使用可信执行环境(TEE)操作。中继系统智能合约被用于中继系统节点的远程认证,其可以被公开审核,消除了单个客户端重复远程认证的需要。经验证的中继系统节点由中继系统智能合约注册以供使用。中继系统控制器可以周期性检查和记录多节点集群中每个中继系统节点的状态。中继系统控制器将客户端请求分配给集群中可用的中继系统节点,以查询外部数据源。使用中继系统节点的私钥对包括查询结果的响应进行数字签名。中继系统智能合约可以验证该响应是否是由注册的中继系统节点发送的。响应的完整性可通过中继系统智能合约使用中继系统节点的公钥来验证。

[0023] 为本文的实施方式提供进一步的背景,如上所述,分布式账本系统(DLS),也可称为共识网络(例如,由对等节点组成)和区块链网络,使参与实体能够安全地、不可篡改地进行交易和存储数据。尽管术语区块链通常与特定网络和/或用例相关联,但是在不参考任何特定用例的情况下,本文中使用的区块链通常是指DLS。

[0024] 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,记录在区块链上的交易是可靠的且可信赖的。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、其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编入默克尔(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。这个过程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。

[0025] 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的网络。如上所述,区块链网络可以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方式。然而,可以预期,本文的实施方式可以在任何适当类型的区块链网络中实现。

[0026] 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,共识处理由授权的节点集控制,所述节点可以称为共识节点,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,十(10)个实体(例如,金融机构、保险公司)组成的联盟可以操作一个联盟区块链网络,每个实体操作联盟区块链网络中的至少一个节点。

[0027] 在一些示例中,在联盟区块链网络中,全局区块链被提供作为跨所有节点复制的区块链。也就是说,所有共识节点对于全局区块链都处于完全共识状态。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施实用拜占庭容错(practical Byzantine fault tolerance, PBFT)共识,下文进一步详细描述。

[0028] 图1是示出可被用于执行本文的实施方式的环境100的示例的图示。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和网络110。在一些示例中,网络110包括局域网(LAN)、广域网(WAN)、互联网或其组合,并连接网站、用户设备(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/或无线通信链路来访问。

[0029] 在所示的示例中,计算系统106、108可以各自包括能够作为节点参与到联盟区块链网络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、笔记本电脑、平板计算设备和智能手机。在一些示例中,计算系统106、108承载用于与联盟区块链网络102交互的一个或多个计算机实现的服务。例如,计算系统106可以承载第一实体(例如,用户A)的计算机实现服务,诸如第一实体用于管理其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)的计算机实现的服务,诸如第二实体用于管理其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表示为节点的点对点网络(Peer-to-Peer network),计算系统106、108分别提供参与到联盟区块链网络102中的第一实体和第二实体的节点。

[0030] 图2描述了根据本文实施方式的概念架构200的示例。概念架构200包括实体层202、承载服务层204和区块链网络层206。在所描述的示例中,实体层202包括三个参与者,参与者A、参与者B和参与者C,每个参与者都有各自的交易管理系统208。

[0031] 在所示的示例中,承载服务层204包括用于每个交易管理系统208的接口210。在一些示例中,各交易管理系统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中的网络110)与其对应的接口210通信。在一些示例中,每个接口210在相应的交易管理系统208与区块链网络层206之间提供通信连接。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,接口210与区块链网络层206之间的通信是使用远程程序调用(RPC)来进行的。在一些示例中,接口210为各自的交易管理系统208“承载”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)。

[0032] 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(peer-to-peer)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,但是在区块链网络212中提供并维护了区块链216的多个副本。例如,每个节点214存储区块链的副本。在一些实施方式中,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进行的交易相关联的信息。

[0033] 区块链(例如,图2的区块链216)由一系列区块组成,每个区块存储数据。示例性数据包括代表两个或更多个参与者之间的交易的交易数据。虽然在本文中以非限制性示例的方式使用交易,但可以预期,任何适当的数据都可以存储在区块链中(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)。交易数据不可篡改地存储在区块链中。也就是说,交易数据不能被改变。

[0034] 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)转换为固定长度的哈希值(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中的微小变化也会导致完全不同的哈希值。此外,如上所述,哈希值具有固定的长度。也就是说,不管交易数据的大小,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产生哈希值。哈希函数的示例包括但不限于安全哈希算法(SHA-256),其输出256位

哈希值。

[0035] 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。

[0036] 区块通过共识协议被添加到区块链。区块链网络中的多个节点参与到共识协议中,并进行工作以将区块添加到区块链中。这些节点被称为共识节点。上文介绍的PBFT被用作共识协议的非限制性示例。共识节点执行共识协议以向区块链添加交易,并更新区块链网络的整体状态。

[0037] 进一步详细地,共识节点产生区块头,对区块中的所有交易进行哈希处理,并成对地组合哈希值以生成额进一步哈希值,直到为区块中的所有交易提供单个哈希值(Merkle根哈希值)。这个哈希值被添加到区块头。共识节点还确定区块链中最近区块的哈希值(即,添加到区块链的最新版块)。共识节点还向区块头添加随机数(nonce)和时间戳。

[0038] 通常,PBFT提供实用拜占庭状态机复制,其容许拜占庭错误(例如,故障节点、恶意节点)。这在PBFT中通过假设故障会发生(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)来实现。在PBFT中,共识节点按包括主共识节点和备共识节点的顺序提供。主共识节点周期性更改。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协议而将交易添加到区块链。在这个过程中,消息在共识节点之间传输,每个共识节点证明消息是从指定的节点接收并验证消息在传输过程中没有被修改。

[0039] 在PBFT中,共识协议分多个阶段提供,所有共识节点都以相同的状态开始。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)。为了响应接收请求,主共识节点将请求多播到备共识节点。备共识节点执行请求,每个节点都向客户端发送一个回复。客户端等待,直到接收到阈值数量的回复。在一些示例中,客户端等待接收到 $f+1$ 个回复,其中 f 是区块链网络中可以容忍的最大错误共识节点数。最终结果是,有足够数量的共识节点就要添加到区块链的记录的顺序达成一致,并且记录要么被接受,要么被拒绝。

[0040] 在一些区块链网络中,用密码学来维护交易隐私。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就不能看出交易的细节,那么这些节点就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进行加密(从明文生成密文)和解密(从密文生成明文)的加密过程。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加密/解密交易数据。

[0041] 非对称加密使用密钥对,每个密钥对都包括私钥和公钥,私钥仅为各自节点所知,公钥为区块链网络中的任何或所有其他节点所知。一个节点可以使用另一个节点的公钥加密数据,而加密的数据可以使用另一个节点的私钥解密。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可以使用其私钥解密加密数据(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。

[0042] 非对称加密用于提供数字签名,使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,一个节点可以对一条消息进行数字签名,另一个节点可以根据参

与者A的数字签名确认该消息是由该节点发送的。数字签名还可以用于确保消息在传输过程中不会被篡改。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生成消息的哈希值,然后使用其私钥对哈希值进行加密,以提供数字签名作为加密哈希值。参与者A将数字签名附加到消息上,并将带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的公钥解密数字签名,并提取哈希。参与者B对消息进行哈希处理并比较哈希值。如果哈希值相同,参与者B可以确认消息确实来自参与者A,并且没有被篡改。

[0043] 在一些实施方式中,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来操作。在较高层面上,TEE是与硬件的操作环境(例如,操作系统(OS)、基本输入/输出系统(BIOS))隔离的硬件(一个或多个处理器、存储器)内的可信环境。更详细地,TEE是确保代码执行的机密性和完整性的处理器的独立安全区域以及主处理器中加载的数据。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(TAs)在TEE内执行,并且可以访问处理器和存储器。通过TEE,TA被保护免受主OS中运行的其他应用程序的影响。此外,TEE以密码学方式在TEE内将TAs彼此隔离。

[0044] 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)。尽管本文以示例的方式讨论了SGX,但可以预期本文的实施方式可以使用任何适当的TEE来实现。

[0045] SGX提供基于硬件的TEE。在SGX中,可信硬件是中央处理器(CPU)的死区,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,飞地被提供为存储器中的飞地页面缓存(EPC),并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级别的连续存储空间,并且不能被任何软件访问。每个EPC都是存储器集(例如4KB),其由OS分配以在PRM中加载应用程序数据和代码。EPC元数据(EPCM)是各个EPC的入口地址,并且确保每个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,而一个EPC专用于单个飞地。

[0046] 在执行TA期间,处理器在访问存储在飞地中的数据时以所谓的飞地模式操作。飞地模式下的操作对每个存储器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。可信部分不可被例如OS、BIOS、特权系统代码、虚拟机管理器(VMM)、系统管理模式(SMM)等访问。在操作中,TA运行并在存储器的PRM内创建飞地。飞地内的可信部分执行的可信功能被不可信部分调用,在飞地内执行的代码将数据视为明文数据(未加密),对数据的外部访问被拒绝。可信部分对调用提供加密响应,TA继续执行。

[0047] 可执行认证处理以验证预期代码(例如,TA的可信部分)在提供SGX的TEE内安全执行。通常,认证处理包括TA接收来自质询者(例如,区块链网络中的另一个节点、区块链网络的密钥管理系统KMS)的认证请求。作为响应,TA要求其飞地生成远程认证,也称为引用(quote)。生成远程认证包括将本地认证从飞地发送到所谓的引用飞地,该引用飞地验证本地认证并通过使用非对称认证密钥对本地认证签名从而将本地认证转换为远程认证。远程认证(引用)被提供给质询者(例如,区块链网络的KMS)。

[0048] 质询者使用认证验证服务来验证远程认证。对于SGX,Intel提供Intel认证服务(IAS),其接收来自质询者的远程认证并验证远程认证。更具体地,IAS处理远程认证并提供报告(例如,认证验证报告(AVR)),该报告指示远程认证是否得到验证。如果未被验证,则可以指示错误。如果经过验证(预期代码在TEE中安全地执行),质询者可以发起或继续与TA交

互。例如,响应于验证,KMS(作为质询者)可以对执行TEE的节点发布非对称加密密钥(例如,公钥和私钥对)(例如,通过密钥交换处理,诸如椭圆曲线Diffie-Hellman(ECDH)),以使节点能够与其他节点和/或客户端安全通信。

[0049] 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。在示例背景下,智能合约在联盟区块链网络内被实施、存储、更新(按照需要)和执行。与智能合约相关的合约方(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(例如,作为智能合约的当事方)相关联的实体(例如,商业企业)。

[0050] 更详细地,智能合约被提供为在区块链上执行的计算机可执行程序(例如,区块链网络内的节点)。智能合约包含一组预定义规则,在所述预定义规则下智能合约的各方同意彼此交互。如果智能合约的预定义规则得到满足,则自动执行智能合约中定义的协议。智能合约通常是防篡改的,并且可以促进、验证和强制实施协议或交易的谈判或执行。

[0051] 在一些情况下,在区块链网络内执行的智能合约需要来自区块链网络外部的输入来评估预定义规则并执行相应的动作。通过非限制性示例,智能合约可能需要基于股票报价来做出决定,所述股票报价来自区块链网络外部的数据源。作为另一非限制性示例,智能合约可能需要基于在区块链网络外部维护的账户的账户信息来做出决定。但是,智能合约本身不能直接查询外部数据源。

[0052] 传统方法包括使用中继代理来检索外部数据并将数据提交给区块链,以供智能合约处理。但是,此处理可能导致诸如安全信息的泄漏(例如,访问外部数据源可能需要的凭据)的安全问题。例如,传统方法可以使用TEE来证明中继代理已经诚实地执行了指定的查询请求。但是,由于区块链的开放性,所有查询请求对于区块链网络中的所有用户(节点)都是可见的。因此,对于需要访问需访问控制(例如,查询)的外部数据源的查询请求,存在权限泄漏的风险。例如,存在请求字符串可能被截取、修改和重放的风险,从而导致信息泄漏或其他问题。

[0053] 在一种使用SGX的传统方法中,在飞地(飞地程序)中执行的TA或TA的一部分作为中继节点来访问外部数据源。例如,飞地程序可以向基于互联网的数据源发送查询请求(例如,HTTPS请求),并可以向发起请求的智能合约提供响应。在一些示例中,提供了隐私字段功能,其可被用于使用飞地的公钥对敏感信息(例如,访问凭据)进行加密。在一些示例中,中继节点使用飞地的私钥对隐私字段进行解密,调用HTTPS客户端来访问基于互联网的目标数据源,接收请求的数据,并使用私钥对返回的数据进行数字签名。在数字签名后,数据将被返回到发起请求的智能合约。

[0054] 然而,这种传统方法具有缺点。直接对隐私字段进行加密的示例性缺点是带有隐私字段密文的请求没有完整性保护。例如,用户在请求中携带加密的API密钥字段以请求基于互联网的数据源的所有授权信息。攻击者可以拦截通信。尽管攻击者无法直接解密出API密钥信息的明文,但攻击者可以修改请求以使用相同的隐私字段来构造访问信息的请求,并将其发送到中继节点。这可能导致敏感信息(例如,凭证)的泄漏。

[0055] 鉴于以上背景,本文的实施方式旨在使用中继系统和TEE查询外部数据源(例如,基于互联网的数据源)。更具体地,如本文进一步详细描述,本文的实施方式提供了包括多个中继系统节点的多节点集群,每个节点执行TEE。每个中继系统节点的状态被维护,并

且响应于对外部数据的客户端请求,可从多节点集群选取中继系统节点。通过这种方式,中继系统的可用性得到保证。本文的实施方式进一步提供了授权请求完整性检查,同时保护敏感信息(例如,凭证)。通过这种方式,如本文进一步详细描述,本文的实施方式解决了传统方法的缺点,例如防止用户权限泄漏。

[0056] 图3是示出根据本文的实施方式的系统300的示例的图示。如所示出的,系统300包括区块链302、中继系统控制器308、包括多个中继系统节点310的多节点集群309、认证服务312和网络314(例如,互联网)。在所描述的示例中,区块链302包括客户端智能合约304和中继系统智能合约306。通常,中继系统智能合约306、中继系统控制器308和中继系统节点310提供中继系统,该中继系统使得区块链302外部的数据能够被检索并在区块链302内使用。

[0057] 在一些实施方式中,中继系统节点310使用TEE技术(例如,Intel SGX)来实施。通常,认证服务312为客户端智能合约304验证中继系统节点310的合法性。认证服务的示例包括上面描述的IAS。如本文所述,中继系统智能合约306、中继系统控制器308和中继系统节点310作为中继系统一起操作,以将来自客户端智能合约304的数据或请求中继到网络314(例如,通过网络314可访问的外部数据源),并将数据或请求结果从网络314中继到客户端智能合约304。

[0058] 客户端智能合约304是作为从网络314请求数据或服务的请求者操作的智能合约。在一些实施方式中,客户端智能合约304的线下所有者(例如,客户端或用户(未示出))可以向客户端智能合约304发送数据或请求,或在客户端智能合约304生成数据或服务请求。数据或请求可以是数据报元素。客户端智能合约304与中继系统合约306通信地耦接。例如,客户端智能合约304可以向中继系统智能合约306发送请求,并从中继系统智能合约306接收请求结果。

[0059] 如上所述,中继系统智能合约306、中继系统控制器308和中继系统节点310一起作为中继系统操作,以将来自客户端智能合约304的数据或请求中继到网络314,并将来自网络314的数据或请求结果中继到客户端智能合约304。中继系统智能合约306是中继系统内充当区块链302的前端的智能合约。中继系统智能合约306包括到客户端智能合约304的应用程序接口(API)或作为到客户端智能合约304的应用程序接口(API)操作,以处理来自客户端智能合约304的请求并将该请求中继到中继系统的其他组件(例如,中继系统控制器308),以及处理来自中继系统控制器308的请求结果并将该请求结果中继到客户端智能合约304。在一些实施方式中,中继系统智能合约306在将请求结果中继到客户端智能合约304之前验证与请求结果相关联的签名。简而言之,中继系统智能合约306是在区块链302与区块链302外部的中继系统组件(例如,中继系统控制器308)之间提供接口的智能合约。中继系统智能合约306接受来自区块链302内执行的组件(例如,客户端智能合约304)的请求,并返回相应的响应。

[0060] 中继系统控制器308包括任何合适的计算机、处理器、模块或计算元件,用于将来自中继系统智能合约306的请求中继到中继系统节点310,并将来自中继系统节点310的请求结果中继到中继系统智能合约306。因此,中继系统控制器308作为监控实体操作,该监控实体监控中继系统智能合约306的状态,因为中继系统智能合约306没有与网络314直接连接。

[0061] 中继系统控制器308还中继指示中继系统节点310从中继系统节点310到认证服务

312的合法性的认证证据320。在一些实施方式中,认证证据320包括中继系统节点310的测量值322和中继系统节点310的签名326。中继系统节点310的测量值322可以包括中继系统节点310的初始状态的哈希值。认证证据320中包括的中继系统节点310的签名326可以包括使用中继系统节点310的认证密钥签名的中继系统节点310的测量值322。

[0062] 在一些实施方式中,中继系统节点310的认证密钥包括增强隐私标识 (EPID) 私钥。EPID是Intel提供的用于在保护隐私的同时认证可信系统的算法。通常,网络的每个成员(例如,计算机或服务器)都被分配EPID私钥以用于对认证证据签名,网络中认证证据的验证者存储与网络的其他成员的EPID私钥配对的EPID公钥。每个成员都可以使用其自己的EPID私钥生成认证证据的签名,验证者可以使用EPID公钥验证其他成员的签名。因此,EPID密钥可被用于证明设备(诸如计算机或服务器)是可信的设备。

[0063] 认证证据320可进一步包括由中继系统节点310生成的公钥324。如果认证证据320包括中继系统节点310产生的公钥324,中继系统节点310的签名326包括测量值322,以及使用中继系统节点310的认证密钥签名的公钥324。

[0064] 中继系统节点310包括任何合适的服务器、计算机、模块或计算元素,以接收和完成来自区块链302的请求。例如,中继系统节点310可以接收和处理来自客户端的链下服务请求,并查询网络314中的外部数据源,例如,启用HTTPS的互联网服务。在处理来自客户端或客户端智能合约304的请求之前,中继系统节点310可以生成认证证据320并将认证证据320发送给认证服务312以验证中继系统节点310的合法性。在一些实施方式中,中继系统节点310生成包括公钥324和私钥的密钥对,并且将公钥324包括在认证证据320中。公钥324可由中继系统控制器308进一步被中继到中继系统智能合约306,以用于将来在中继系统智能合约306与中继系统节点310之间的通信。例如,中继系统节点310可以使用私钥对请求结果签名,并且中继系统智能合约306可以使用公钥324来验证签名的请求结果。

[0065] 在图3所描绘的示例中,多个中继系统节点310可以形成多节点集群309。集群的每个中继系统节点310在认证处理期间由中继系统智能合约306单独验证。因此,多节点集群309的每个经验证的中继系统节点310可被用于查询互联网数据源314。

[0066] 认证服务312包括任何合适的服务器、计算机、模块或计算元件,以验证由中继系统控制器308从中继系统节点310转发的认证证据320的合法性。如上所述,认证证据320包括中继系统节点310的测量值322、中继系统节点310的签名326和/或中继系统节点310生成的公钥324。在接收到认证证据320后,认证服务312验证认证证据320中的中继系统节点310的签名326,并生成认证验证报告 (AVR) 330。

[0067] 认证服务312使用认证服务312的认证密钥来验证认证证据320中的签名326。在一些实施方式中,认证服务312的认证密钥包括EPID公钥,该EPID公钥与中继系统节点310用于对认证证据320签名的EPID私钥配对。在验证认证证据320中的签名之后,认证服务312生成AVR 330,AVR 330包括认证证据320、指示认证证据320中的签名326是否有效的验证结果334以及认证服务312的签名336。

[0068] 在一些实施方式中,AVR 330包括认证证据320,不包括中继系统节点310的签名326。例如,AVR 330可以包括中继系统节点310的测量值322、中继系统节点310生成的公钥324、验证结果334和认证服务312的签名336。在一些实施方式中,认证服务312的签名336包括使用认证服务312的报告签名密钥(例如,认证服务312用于对认证验证报告签名的私钥)

签名的认证证据320和验证结果334。注意报告签名密钥可以与认证服务312的认证密钥不同。

[0069] 如图3中所示的中继系统可被用于从外部数据源检索公共可用数据和/或服务。整个检索过程包括三个阶段。在第一阶段中,中继系统智能合约306对多节点集群309中的中继系统节点310进行认证,并注册(存储)已认证的中继系统节点310。在第二阶段中,中继系统控制器308检查多节点集群309中的中继系统节点310的状态,并确定可使用的中继系统节点310。在第三阶段中,客户端智能合约304通过中继系统智能合约306、中继系统控制器308和多节点集群309中的可用中继系统节点310从外部数据源314检索公共可用的数据和/或服务。

[0070] 图4示出了根据本文的实施方式的信号流400的示例。信号流400表示认证验证处理。为方便起见,该处理将被描述为由位于一个或多个位置并根据本文适当地编程的一台或多台计算机的系统执行。例如,适当编程的分布式系统(例如,图1的区块链系统100;图3的系统300)可以执行该处理。

[0071] 通常,在操作中,中继系统控制器308从中继系统节点310接收认证证据,并将认证证据发送给认证服务312以验证认证证据。中继系统控制器308接收来自认证服务312的AVR,该AVR基于认证证据中对中继系统节点310的签名的验证而指示中继系统节点310的合法性。中继系统控制器308将包括认证服务312的签名的AVR进一步中继至中继系统智能合约306。

[0072] 在开始时,在向中继系统节点310质询认证证据之前,中继系统控制器308获得中继系统节点310的测量值(例如,初始状态的摘要)。在一些实施方式中,中继系统控制器308从中继系统节点310获得测量值。在可选实施方式中,中继系统控制器308从中继系统节点310的开发者获得测量值。中继系统控制器308将中继系统节点310的测量值转发给中继系统智能合约306。中继系统智能合约306注册(存储)中继系统节点310的测量值,以供将来使用。例如,中继系统智能合约306可以将存储的测量值与从认证服务312接收的AVR中的另一测量值进行比较。

[0073] 在图4的示例中,中继系统控制器308向中继系统节点310发送(410)认证请求(例如,质询)。认证请求被发送到中继系统节点310,以请求指示中继系统节点310的合法性或有效性的认证证据。在一些实施方式中,认证证据包括中继系统节点310的测量值和中继系统节点310的签名。中继系统节点310的测量值可以包括中继系统节点310的初始状态的哈希值。例如,中继系统节点310的测量值可以包括在中继系统节点310上实现的处理代码的哈希值。

[0074] 响应于认证请求,中继系统节点310生成(412)认证证据。如上所述,认证证据指示中继系统节点310的合法性或有效性,并且可以包括中继系统节点310的测量值和签名。在一些实施方式中,认证证据还包括由中继系统节点310生成的公钥。例如,中继系统节点310可以使用预定的诸如Rivest-Shamir-Adleman (RSA) 算法的密钥生成算法生成包括私钥和公钥的随机加密密钥对。在一些示例中,公钥被提供在将要发送给中继系统智能合约306的认证证据中,并可被用于中继系统智能合约306与中继系统节点310之间的未来通信。例如,中继系统节点310可以使用私钥对请求结果签名,中继系统智能合约306可以使用公钥来验证签名的请求结果。

[0075] 在一些实施方式中,中继系统节点310的测量值包括中继系统节点310的初始状态的哈希值。认证证据中的中继系统节点310的签名包括使用中继系统节点310的认证密钥签名的测量值和由中继系统节点310生成的公钥。在一些实施方式中,中继系统节点310的认证密钥包括EPID私钥。使用EPID私钥签名的认证证据可以由验证者使用与EPID私钥配对的EPID公钥来验证,以证明生成认证证据的设备的真实性。

[0076] 中继系统节点310向中继系统控制器308发送(414)认证证据。发送给中继系统控制器308的认证证据可以包括中继系统节点310的测量值、中继系统节点310生成的公钥和中继系统节点310的签名,中继系统节点310的签名包括使用中继系统节点310的EPID私钥签名的测量值和公钥。

[0077] 中继系统控制器308将认证证据转发(416)给认证服务312。在一些实施方式中,中继系统控制器308向认证服务312发送认证验证请求。认证验证请求包括从中继系统节点310发送的认证证据和一些补充信息,诸如例如,指示中继系统节点310是否使用SGX平台服务的描述符。

[0078] 响应于接收到中继系统控制器308转发的认证证据,认证服务312验证(418)该认证证据。如前所述,认证证据包括中继系统节点310的测量值、中继系统节点310生成的公钥和中继系统节点310的签名。认证服务312可通过使用认证服务312的认证密钥验证认证证据中的中继系统节点310的签名来验证认证证据。例如,认证服务312可以使用认证验证服务器的EPID公钥验证中继系统节点310的签名,该EPID公钥与中继系统节点310用于对认证证据签名的EPID私钥配对。

[0079] 如果认证服务312确定认证证据中中继系统节点310的签名有效,认证服务312可以确定中继系统节点310是真实或合法的设备。如果认证服务312确定认证证据中中继系统节点310的签名无效,认证服务312可以确定中继系统节点310是不真实的或是非法设备,并拒绝来自中继系统节点310的任何后续数据和请求。

[0080] 认证服务312基于认证证据的验证而生成(420)AVR。在一些实施方式中,AVR可以包括中继系统节点310的认证证据、认证验证结果和认证服务312的数字签名。在一些实施方式中,AVR可包括中继系统节点310的认证证据,不包括中继系统节点310的签名。例如,AVR可以包括中继系统节点310的测量值、中继系统节点310生成的公钥、认证验证结果和认证服务312的签名。

[0081] AVR中的认证验证结果指示中继系统节点310的签名是否有效。例如,认证验证结果可以包括指示中继系统节点310的签名有效的值“valid”或者“OK”,或者可以包括指示签名无效的值“invalid”。

[0082] 在一些实施方式中,认证服务312的签名包括使用报告签名密钥签名的认证证据和认证验证结果。报告签名密钥可以是认证服务312用于对AVR签名的私钥。在一些实施方式中,报告签名密钥是由认证服务312使用预先确定的密钥生成算法生成的。例如,可以使用RSA安全哈希算法(SHA) 256生成报告签名密钥。注意到报告签名密钥与认证服务312用于验证认证证据的认证密钥(例如EPID公钥)不同。

[0083] 在一些实施方式中,认证服务312向中继系统控制器308发送(422)AVR。如上所述,AVR包括加密地签名的中继系统节点310的身份验证报告,并且可以包括中继系统节点310的认证证据、认证验证结果和认证服务312的数字签名。

[0084] 在一些实施方式中,在从认证服务312接收到AVR后,中继系统控制器308将AVR转发(424)到中继系统智能合约306。中继系统智能合约306验证(426)AVR。例如,中继系统智能合约306可以验证AVR中认证服务312的签名。在一些实施方式中,中继系统智能合约306使用报告签名证书来验证认证服务312的签名。报告签名证书可以是X.509数字证书。报告签名证书可以包括公钥,该公钥由认证服务312生成并且与认证服务312用于对AVR签名的报告签名密钥配对。如果中继系统智能合约306验证AVR中认证服务312的签名是有效的,中继系统智能合约306确定AVR确实是由认证服务312发送的。如果中继系统智能合约306确定AVR中认证服务312的签名是无效的,中继系统智能合约306确定认证验证报告是不真实的,并且将拒绝AVR。中继系统智能合约306可进一步检查AVR中的认证验证结果,以确定中继系统节点310的认证证据是否有效。在一些实施方式中,中继系统智能合约306进一步将认证证据中的测量值与中继系统智能合约306中预先存储的测量值进行比较,以确定认证证据是否有效。

[0085] 响应于确定AVR是真实的以及中继系统节点310的认证证据是有效的,中继系统智能合约306将中继系统节点310注册(428)为有效或合法的设备。中继系统智能合约306可以进一步存储认证证据中包括的并且由中继系统节点310生成的公钥。所述公钥将被中继系统智能合约306用于中继系统智能合约306与中继系统节点310之间的未来通信。

[0086] 图5示出根据本文的实施方式的信号流500的示例。信号流500表示根据本文的实施方式的用于检查多节点集群309的中继系统节点310的节点状态的处理。为方便起见,该处理将被描述为由位于一个或多个位置并根据本文适当地编程的一台或多台计算机的系统执行。例如,适当编程的分布式系统(例如,图1的区块链系统100;图3的系统300)可以执行该处理。

[0087] 通常,在操作中,中继系统控制器308周期性地向多节点集群309中的中继系统节点310发送状态请求。中继系统节点310在接收到状态请求时以状态响应进行答复。中继系统控制器308基于中继系统节点310的状态响应来记录中继系统节点310的状态。

[0088] 更详细地,中继系统控制器308向多节点集群309的中继系统节点310a发送状态请求(502)。多节点集群309包括多个中继系统节点310,例如,310a和310b。注意,图5被示出为包括中继系统节点310a和310b仅出于示意性的目的。多节点集群309可以包括任意适当数量的中继系统节点310。

[0089] 中继系统节点310a处理(504)状态请求并向中继系统控制器308发送(506)状态响应。例如,如果中继系统节点310a处于正常状态,它可以向中继系统控制器308发送状态确认消息。作为另一示例,如果中继系统节点310a处于异常状态,它可能不会响应状态请求。

[0090] 中继系统控制器308基于中继系统节点310a的状态响应来记录(508)中继系统节点310a的状态。例如,如果中继系统控制器308从中继系统节点310接收到状态确认消息,则其将中继系统节点310a的状态记录为“可用”。作为另一示例,如果中继系统节点310a在预定的时间窗口内没有响应,中继系统控制器308将中继系统节点310a的状态记录为“不可用”。

[0091] 中继系统控制器308可以向集群中的其他中继系统节点310发送状态请求,例如,诸如中继系统节点310b。中继系统控制器308可以向中继系统节点310b发送(510)状态请求,中继系统节点310b处理(512)状态请求,并向中继系统控制器308发送(514)状态响应。

中继系统控制器308基于中继系统节点310b的状态响应来记录(516)中继系统节点310b的状态。

[0092] 如上所述,中继系统控制器308周期性地查询集群中中继系统节点310的节点状态,并记录中继系统节点310的状态。稍后,当接收到来自外部数据源的数据查询时,中继系统控制器308可以选择被记录为可用于处理查询的中继系统节点310之一。

[0093] 图6示出用于执行数据检索的处理600的示例。为方便起见,处理500将被描述为由位于一个或多个位置并根据本文适当地编程的一台或多台计算机的系统执行。例如,适当编程的分布式系统(例如,图1的区块链系统100和图3的系统300)可以执行处理600。

[0094] 通常,在操作中,客户端智能合约304生成将由中继系统智能合约306中继到中继系统控制器308的请求。中继系统控制器308选择多节点集群309中可用的中继系统节点310。所选的中继系统节点310查询互联网数据源314。在一些示例中,互联网数据源314是公共数据源,访问不需要凭证。中继系统节点310接收来自互联网数据源314的响应,中继系统智能合约306验证该响应并根据本文的实施方式返回给客户端智能合约304。

[0095] 更详细地,客户端智能合约304从基于互联网的数据源314发送(602)数据或服务的请求。将该请求从客户端智能合约304发送到中继系统智能合约306。在一些示例中,请求可以是对公共可访问网站的公共可用数据的请求。请求可以包括明文部分,例如,诸如互联网数据源314的网址(URL)和一个或多个请求参数(例如,表示所请求的数据和/或服务的参数)。响应于接收到请求,中继系统智能合约306将请求作为日志消息转发(604)到中继系统控制器308。

[0096] 中继系统控制器308从多节点集群309中的多个中继系统节点310中选择(606)一个中继系统节点310。例如,如本文所述,中继系统控制器308周期性地查询多节点集群309中的中继系统节点310,并记录中继系统节点310的状态。在一些示例中,中继系统控制器308从集群中可用的中继系统节点310中随机选择一个中继系统节点310。在其他示例中,中继系统控制器308从集群的中继系统节点310中选择一个可用的且具有最小工作负载的中继系统节点310。

[0097] 中继系统控制器308向在606处确定的中继系统节点310发送请求(608)。在一些示例中,中继系统控制器308发送请求,该请求带有将要接收请求的中继系统节点310(例如,中继系统控制器308选择的中继系统节点310)的指示符。例如,该请求可以由中继系统控制器308修改以包括中继系统节点310的标识符(例如,URL)。

[0098] 响应于接收到请求,中继系统节点310查询(610)互联网数据源314。例如,中继系统节点310可以制定查询以请求(例如,使用HTTP GET方法)来自互联网数据源314的数据。在一些示例中,查询可以包括一个或多个请求参数。响应于接收到查询,互联网数据源314处理(612)查询以提供响应。例如,互联网数据源314可以处理一个或多个请求参数,以识别响应一个或多个请求参数的数据,并提供包括该数据的结果。互联网数据源314将结果发送(614)到中继系统节点310。

[0099] 中继系统节点310处理(616)结果以提供响应。根据本文的实施方式,中继系统节点310使用其私钥对结果签名以提供响应。如本文所述,私钥是在中继系统节点310的远程认证期间生成的。更详细地,结果或结果的至少一部分(例如,数据)由中继系统节点310通过哈希函数处理,以提供第一哈希值。哈希函数的示例包括但不限于SHA-256。中继系统节

点310基于第一哈希值和私钥来生成数字签名。例如,通过提供数字签名的签名算法来处理第一哈希值和私钥。中继系统节点310提供包括结果(例如,数据)和数字签名的响应。中继系统节点310向中继系统控制器308发送响应(618),中继系统控制器308向中继系统智能合约306发送响应(620)。

[0100] 中继系统智能合约306处理(622)响应,以验证响应是否由注册的中继系统节点310发送的并确保响应的完整性。如前所述,中继系统智能合约306注册(存储)在认证期间认证的中继系统节点310。在一些实施方式中,响应可以包括中继系统节点310的唯一标识(例如,URL),并且中继系统智能合约306可以将响应中的标识与注册的中继系统节点310的标识(例如,URL)进行匹配。如果匹配成功,中继系统智能合约306确定该响应是由注册的中继系统节点310发送的,并可以继续检查该响应的完整性。如果匹配不成功,中继系统智能合约306确定该响应不是由注册的中继系统节点310发送的并且可以拒绝响应。

[0101] 根据本公开的实施方式,中继系统智能合约306通过哈希函数(例如,SHA-256)进一步处理结果(例如,数据),以提供第二哈希值。中继系统智能合约306通过验证算法来处理中继系统节点310的数字签名和公钥,以提供第一哈希值。例如,中继系统智能合约306使用公钥对数字签名进行解密以显示第一哈希值。如本文所述,公钥是在中继系统节点310的远程认证期间生成的。

[0102] 中继系统智能合约306基于第一哈希值和第二哈希值来验证响应的完整性。例如,中继系统智能合约306将第一哈希值与第二哈希值进行比较。如果第一哈希值和第二哈希值不同,则该响应已被篡改并且是不可信的。因此,中继系统智能合约306不会将结果(例如,数据)提供给任何下游组件(例如,客户端智能合约),和/或可以标记错误。如果第一哈希值和第二哈希值相同,则响应的完整性是完整的。因此,中继系统智能合约306向客户端智能合约304提供(624)结果(例如,数据),以便进一步处理。

[0103] 图7示出可根据本文的实施方式执行的示例性处理700的示例。在一些实施方式中,示例性处理700可以使用一个或多个计算机可执行程序来执行,该一个或多个计算机可执行程序使用一台或多台计算设备执行。在一些示例中,示例性处理700可由用于检索区块链网络外部的数据的中继系统执行(例如,中继系统智能合约306、中继系统控制器308、图3的中继系统节点310)。

[0104] 接收请求(702)。例如,图3的中继系统控制器308通过中继系统智能合约306接收来自客户端智能合约304的请求。在一些示例中,如本文所述,客户端智能合约304生成包括要查询的数据源的标识(例如,URL)和一个或多个请求参数的请求。选择中继系统节点310(704)。例如,中继系统控制器308选择多节点集群309中的一个可用中继系统节点310。在一些实施方式中,中继系统控制器308随机选择集群中可用的中继系统节点310。在可选的实施方式中,中继系统控制器308选择集群中的中继系统节点310中具有最小工作负载的可用中继系统节点310。发送请求(706)。例如,中继系统控制器308将请求转发到所选择的中继系统节点310。

[0105] 查询数据源(708)。例如,中继系统节点310构建包括其接收到的请求(例如,初始请求)的一个或多个请求参数的查询(例如,新请求)。例如,新请求可以包括明文数据元,该明文数据元包括要查询的互联网数据源314的网址和一个或多个请求参数。中继系统节点310使用该查询来查询基于互联网的数据源314。

[0106] 从数据源接收结果(710)。在一些示例中,基于互联网的数据源314处理查询,并向中继系统节点310返回请求结果(例如,数据值)。准备响应(712),并且发送该响应(714)。例如,中继系统节点310可以生成签名,该签名包括使用中继系统节点310的私钥签名的请求结果,如本文所述。中继系统节点310用于对请求结果签名的私钥是在中继系统节点310的早期远程认证期间生成的。

[0107] 接收响应并确定该响应是否有效(716)。例如,中继系统智能合约306处理响应,以验证该响应是否是由注册的中继系统节点310发送的,并确保响应的完整性。在一些实施方式中,响应可以包括中继系统节点310的唯一标识(例如,URL),中继系统智能合约306可以将该标识与注册的中继系统节点310的标识(例如,URL)匹配。如果匹配成功,中继系统智能合约306确定该响应是由注册的中继系统节点310发送的,并可以继续检查响应的完整性。如果匹配不成功,中继系统智能合约306确定该响应不是由注册的中继系统节点310发送的。

[0108] 为了检查响应的完整性,中继系统智能合约306基于请求结果(例如,数据值)计算哈希值。然后,中继系统智能合约306使用公钥获得请求结果的哈希值,并确定其是否与计算出的哈希值匹配。如果两个哈希值匹配,中继系统智能合约306确定请求结果有效。如果两个哈希值不匹配,中继系统智能合约306确定请求结果无效,并可以拒绝请求结果。如果响应不是由注册的中继系统节点310发送的和/或请求结果无效,则指示错误(718),并且示例性处理700结束。如果响应是由注册的中继系统节点310发送的,则请求结果有效,并且请求结果的完整性保持不变,则使用请求结果(720)。例如,结果被提供给客户端智能合约304以供进一步处理。

[0109] 如本文所述,本文的实施方式相比传统系统实现了一个或多个技术效果。在一些实施方式中,中继系统节点的多节点集群被提供用于从外部数据源检索或访问数据和/或服务,其中,由中继系统控制器周期性地检查和记录多集群中的中继系统节点的状态。如本文所述,通过将中继系统节点部署在多节点集群中,中继系统控制器可以将客户端服务请求自动分配给多节点集群中的可用中继系统节点,避免因单个节点故障而导致服务不可用。因此,本文的实施方式提高了用于查询互联网数据源的中继系统的整体服务可用性。在一些实施方式中,确保了从外部数据源提供回区块链网络的响应的完整性。因此,本文的实施方式提高了区块链网络与中继系统的组件之间通信的完整性,中继系统的组件被用于检索区块链网络外部的数据。通过这种方式,减少了恶意用户的潜在攻击通道以增强安全性。在一些实施方式中,中继系统避免用户和中继系统节点之间的直接接触,从而避免暴露中继系统节点的位置或访问点。因此,中继系统节点不太可能被网络上的恶意参与者以多种形式发现和攻击,例如,诸如DDoS攻击。这提高了中继系统节点的安全性,从而进一步提高了区块链网络与中继系统节点之间通信的安全性。

[0110] 图8示出根据本文的实施方式的装置800的模块示例。装置800可以是在区块链网络内执行的中继系统智能合约的示例实施方式。在一些示例中,中继系统智能合约向区块链网络外部的中继系统的一个或多个组件发出请求并接收来自这些组件的响应,以及查询区块链网络外部的数据源。

[0111] 装置800可对应于以上所述的实施方式,装置800包括以下:接收模块802,用于接收针对来自数据源的数据的请求;发送模块804,用于将请求发送到区块链网络外部的多节

点集群,该多节点集群包括多个中继系统组件;接收模块806,用于接收来自多节点集群的中继系统组件的结果,该结果被使用中继系统组件的私钥数字地签名;验证模块808,用于验证中继系统组件是否被注册在中继系统智能合约上;验证模块810,用于响应于验证了中继系统组件被注册,基于中继系统组件的公钥和结果的数字签名来验证结果的完整性;以及发送模块812,用于响应于验证了结果的完整性,将结果发送到区块链网络内的客户端。

[0112] 通常,本文中描述的主题的创新方面可以通过以下操作实现:在区块链网络内执行的中继系统智能合约而接收针对来自数据源的数据的请求,中继系统智能合约将请求发送至中继系统,该中继系统在区块链网络外部并且包括多节点集群,所述多节点集群包括多个中继系统节点,中继系统智能合约接收从多节点集群的中继系统节点提供的结果,该结果被使用中继系统节点的公钥数字地签名,中继系统智能合约验证中继系统节点被注册在中继系统智能合约上;响应于中继系统节点被注册,中继系统智能合约基于中继系统节点的公钥和结果的数字签名验证结果的完整性,以及响应于验证了结果的完整性,将结果发送到区块链网络内的客户端。

[0113] 以上和其他实施方式可以各自可选地单独或以组合形式包括一个或多个以下特征:中继系统控制器周期性地向多节点集群中的多个中继系统节点发送状态查询,并从多个中继系统节点接收状态响应;如果在预定时间窗内从多节点集群中的中继系统节点接收到状态响应,则中继系统控制器将中继系统节点的状态记录为可用;如果在预定时间窗内没有从多节点集群中的中继系统节点接收到状态响应,则中继系统控制器将中继系统节点的状态记录为不可用;中继系统控制器选择多节点集群中的具有可用状态的中继系统节点,并将请求发送到该中继系统节点;中继系统智能合约通过将第一哈希值与第二哈希值进行比较来验证结果的完整性,第一哈希值是通过使用公钥对数字签名进行解密确定的,第二哈希值是使用该结果和哈希函数计算的;中继系统节点执行可信执行环境(TEE),中继系统节点的私钥和公钥是在TEE的认证处理期间提供的;中继系统控制器对多节点集群中的每个中继系统节点执行认证处理,中继系统控制器向中继系统智能合约提供每个中继系统组件的公钥;数据源包括基于互联网的数据源;客户端包括客户端智能合约。

[0114] 在先前实施方式中示出的系统、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。

[0115] 在前面的实施方式中所示的系统、装置、模块或单元可以使用计算机芯片或实体来实现,或者可以使用具有特定功能的产品来实现。典型的实现设备是计算机,计算机可以是个人计算机、笔记本电脑、移动电话、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、游戏机、平板电脑、可穿戴设备或这些设备的任何组合。

[0116] 对于装置中每个单元的功能和作用的实现过程,可以参考前面方法中相应步骤的实现过程。为了简单起见,这里省略了细节。

[0117] 由于装置实施方式基本上对应于方法实施方式,对于相关部分,可以参考方法实施方式中的相关描述。前面描述的装置实施方式仅为示例。描述为独立部分的单元可以是或可以不是物理独立的,显示为单元的部分可以是或可以不是物理单元,可以位于一个位

置,或者可以分布在多个网络单元上。一些或全部模块可以基于实际需求来选择,以实现本文的技术方案的目标。本领域的普通技术人员可以理解和实现本文的实施方式,而无需创造性的努力。

[0118] 本文中描述的主题的实施方式以及动作和操作可以在数字电子电路、有形的计算机软件或固件、计算机硬件(包括本文中公开的结构及其结构等效物)中实施,或者可以在他们的一个或多个的组合中实施。本文中描述的主题的实施方式可以实施为一个或多个计算机程序,例如,计算程序指令的一个或多个模块,编码在计算机程序载体上,以供数据处理装置执行或者控制数据处理装置的操作。载体可以是有形的非暂时性计算机存储介质。备选地或者附加地,载体可以是人工产生的传播信号,例如,机器产生的电信号、光信号或电磁信号,其被产生以编码信息以便传输到适当的接收装置,以供数据处理装置执行。计算机存储介质可以是机器可读存储设备、机器可读存储基板、随机或串行访问存储设备或他们的一个或多个的组合,或者可以是机器可读存储设备、机器可读存储基板、随机或串行访问存储设备或他们的一个或多个的组合的一部分。计算机存储介质不是传播信号。

[0119] 术语“数据处理装置”包括用于处理数据的各种设备、装置和机器,包括例如可编程处理器、计算机或多处理器或计算机。数据处理装置可包括专用逻辑电路,例如,现场可编程门阵列(FPGA)、专用集成电路(ASIC)或图形处理单元(GPU)。除硬件外,该设备还可包括为计算机程序创建执行环境的代码,例如,构成处理器固件的代码、协议栈、数据库管理系统、操作系统或他们的一个或多个的组合。

[0120] 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、应用程序、模块、软件模块、引擎、脚本或代码,可以用任何形式的编程语言(包括编译或解释语言、声明性或程序性语言)编写;它可以用任何形式部署,包括作为独立程序或作为模块、组件、引擎、子程序或其他适合在计算环境中执行的单元,该环境可包括由数据通信网络在一个或多个位置互连的一台或多台计算机。

[0121] 计算机程序可以但不必与文件系统文件相对应。计算机程序可以存储在保存其他程序或数据的文件的一部分中,例如,标记语言文档中的一个或多个脚本、专用于相关程序的单个文件或多个协调文件中,例如,存储一个或多个模块、子程序或部分代码的文件。

[0122] 本文中所述的过程和逻辑流可由一台或多台计算机执行,该一台或多台计算机执行一个或多个计算机程序以通过操作输入数据和产生输出来执行操作。过程和逻辑流也可以通过专用逻辑电路(例如,FPGA、ASIC或GPU)或专用逻辑电路与一台或多台编程计算机的组合来执行。

[0123] 适用于执行计算机程序的计算机可以基于通用或专用微处理器或两者,或任何其他类型的中央处理器。通常,中央处理器将从只读存储器或随机存取存储器或两者接收指令和数据。计算机的元件可以包括用于执行指令的中央处理器和用于存储指令和数据的一个或多个存储器设备。中央处理器和存储器可以由专用逻辑电路来补充或合并。

[0124] 通常,计算机还将包括一个或多个大容量存储设备,或可操作地耦接以从一个或多个大容量存储设备接收数据或将数据传输到一个或多个大容量存储设备。大容量存储设备可以是,例如,磁盘、磁光盘、光盘或固态驱动器。然而,计算机不需要有这样的设备。此外,计算机可以嵌入其他设备中,例如,移动电话、个人数字助理(PDA)、移动音频或视频播

放器、游戏机、全球定位系统 (GPS) 接收器或便携式存储设备 (例如, 通用串行总线 (USB) 闪存驱动器), 仅举几个例子。

[0125] 为提供与用户的交互, 本文中所述的主题的实施方式可在计算机上实现或者配置为与计算机通信, 该计算机具有用于向用户显示信息的显示设备 (例如, LCD (液晶显示器) 显示器) 以及用户可通过其提供输入至该计算机的输入设备, 例如, 键盘和指向设备, 例如鼠标、轨迹球或触摸板。其他类型的设备也可以被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; 用户的输入可以以任何形式接收, 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进行交互; 例如, 通过响应从Web浏览器接收的请求而向用户设备上的Web浏览器发送网页, 或者通过与在用户设备上运行的应用程序 (例如, 智能手机或电子设备) 交互。此外, 计算机可以通过向个人设备 (例如, 运行消息应用程序的智能手机) 发送文本消息或其他形式的消息, 并接收来自用户的响应消息来与用户交互。

[0126] 本文关于系统、装置和计算机程序组件使用术语“配置为”。对于一台或多台计算机的系统, 配置为执行特定操作或动作是指该系统已在其上安装了运行时导致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。对于一个或多个计算机程序, 配置为执行特定操作或动作是指一个或多个程序包括在由数据处理装置执行时使装置执行操作或动作的指令。对于专用逻辑电路, 配置为执行特定操作或动作是指该电路具有执行操作或动作的电子逻辑。

[0127] 尽管本文包含许多具体实施方式细节, 但不应解释为对权利要求的范围限制, 权利要求的范围由权利要求自身限定, 而应解释为对具体实施方式的特定特征的描述。本文在单独实施方式的上下文中描述的某些特征也可以在单个实施方式中组合实现。相反, 在单个实施方式的上下文中描述的各种特征也可以单独地或在任何合适的子组合中在多个实施方式中实现。此外, 尽管以上特征可被描述为以某些组合起作用, 甚至最初也可以这样声称, 但所声称组合的一个或多个特征在某些情况下可以从该组合删除, 权利要求可以指向子组合或子组合的变型。

[0128] 同样地, 尽管操作按照特定顺序在附图中绘出以及在权利要求书中陈述, 但这不应理解为要求按照所示的特定顺序或顺次顺序执行此类操作, 或执行所有示出的操作以获得期望的结果。在某些情况下, 多任务和并行处理可能是有利的。此外, 上述实施方式中各种系统模块和组件的分离不应理解为在所有实施方式中都需要这样的分离, 并且应理解所述程序组件和系统通常可以一起集成在单个软件产品中或打包成多个软件产品。

[0129] 主题的具体实施方式已被描述。其他实施方式在随附权利要求的范围内。例如, 权利要求中所述的操作可以按照不同的顺序执行, 并且仍然可以获得期望的结果。作为一个示例, 附图中所示的过程不一定需要所示的特定顺序或顺次顺序来获得期望的结果。在一些情况下, 多任务和并行处理可能是有利的。

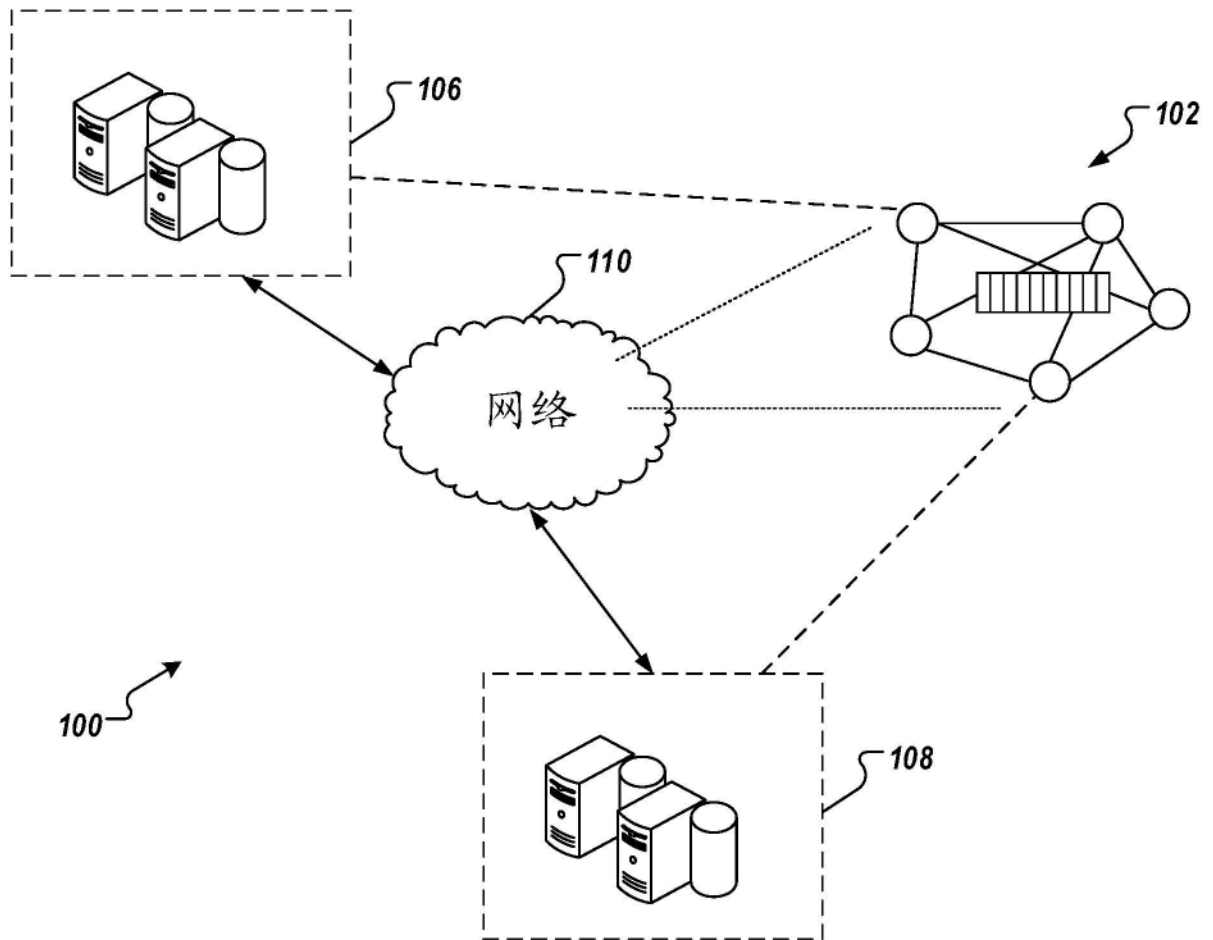


图1

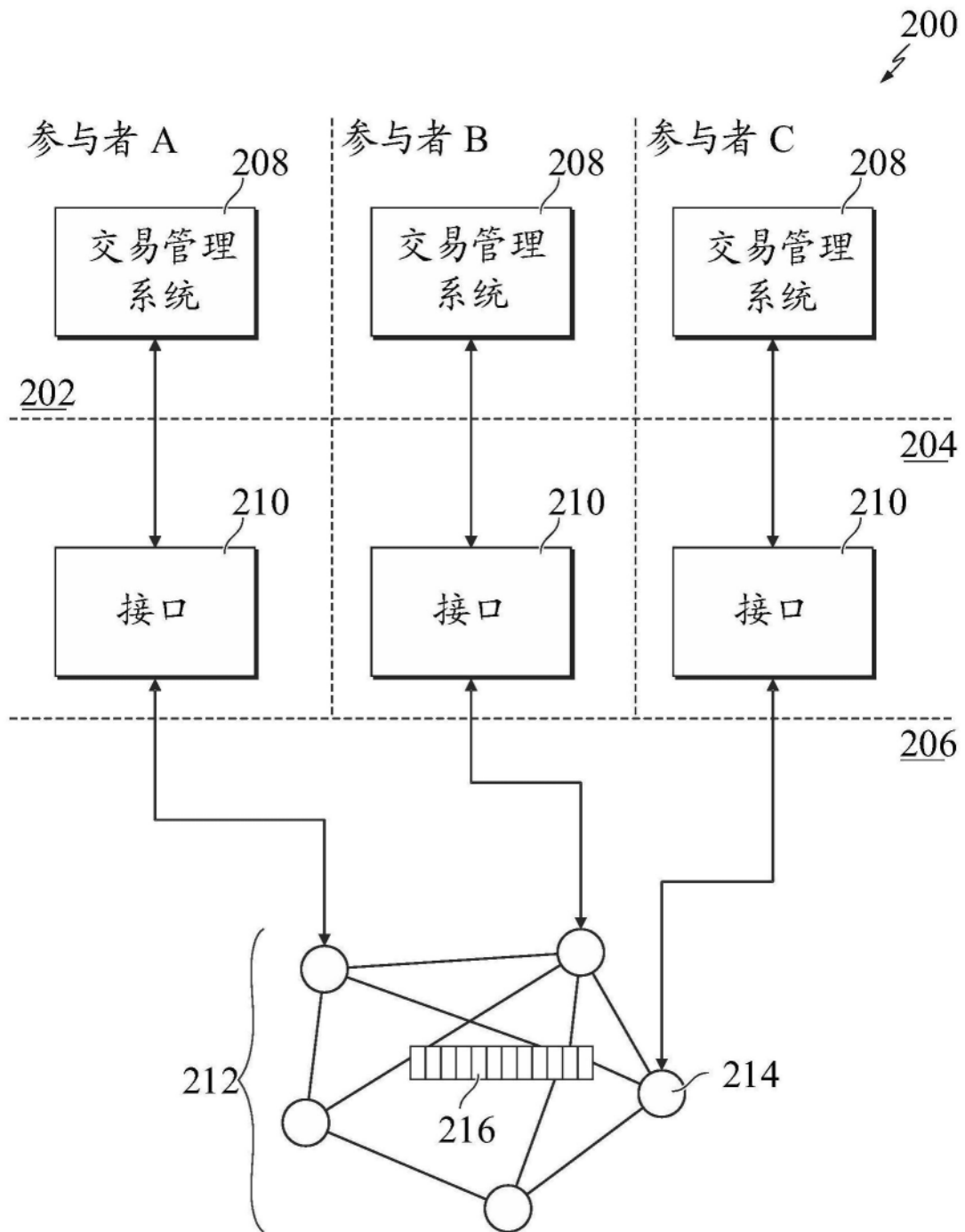


图2

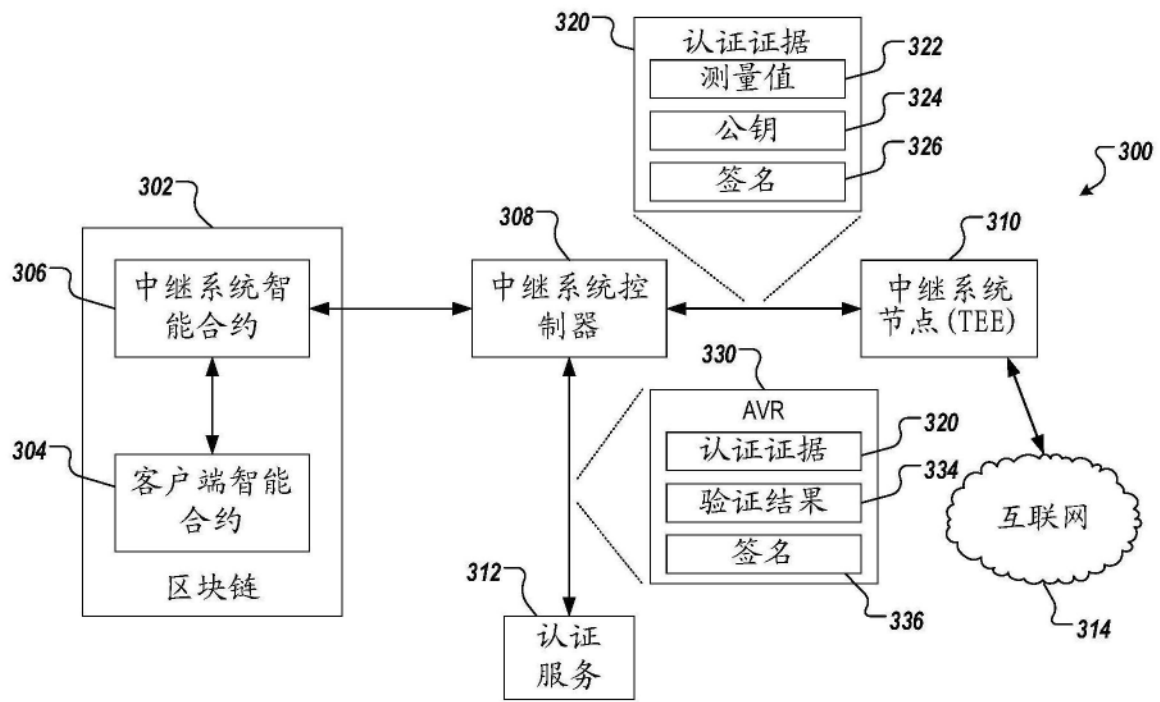


图3

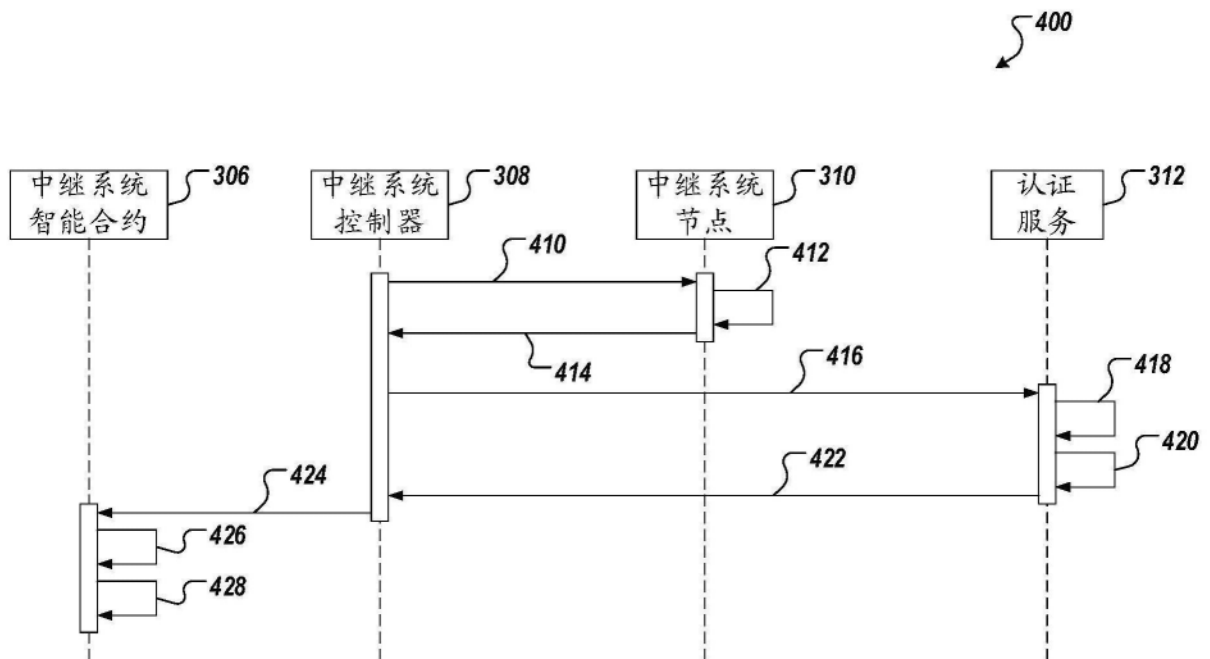


图4

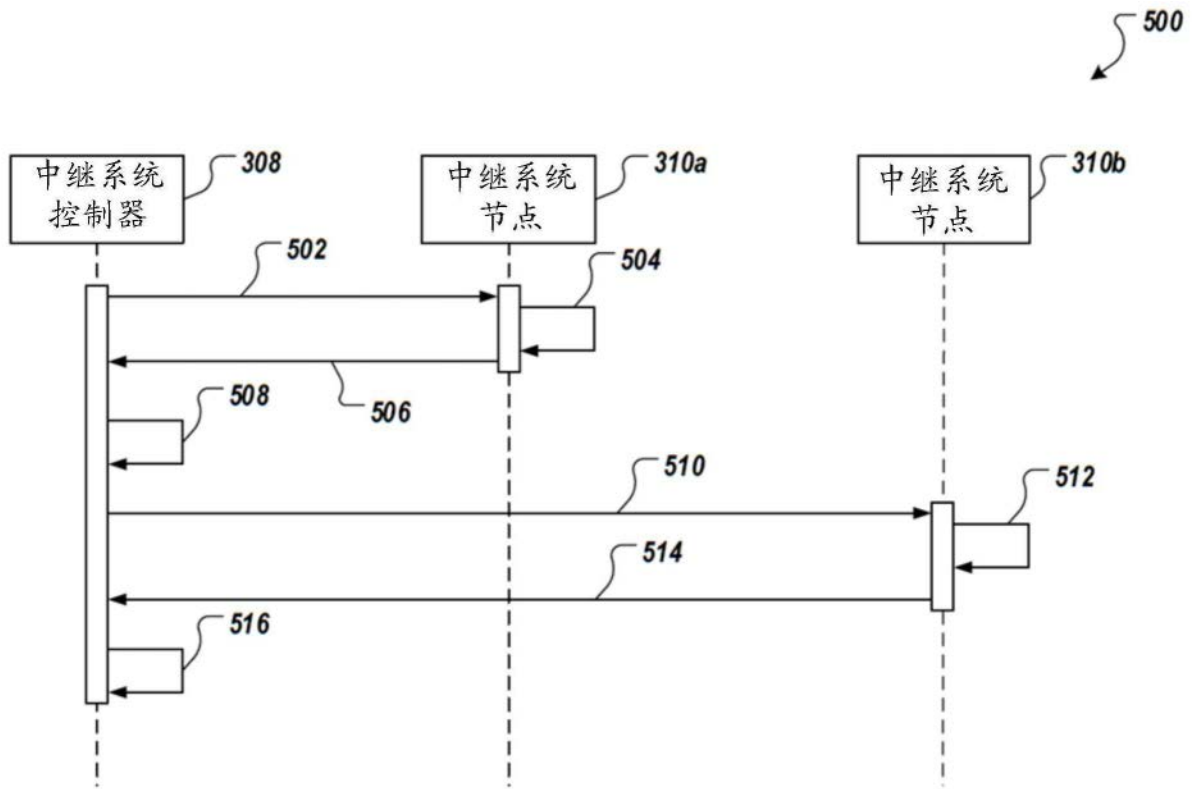


图5

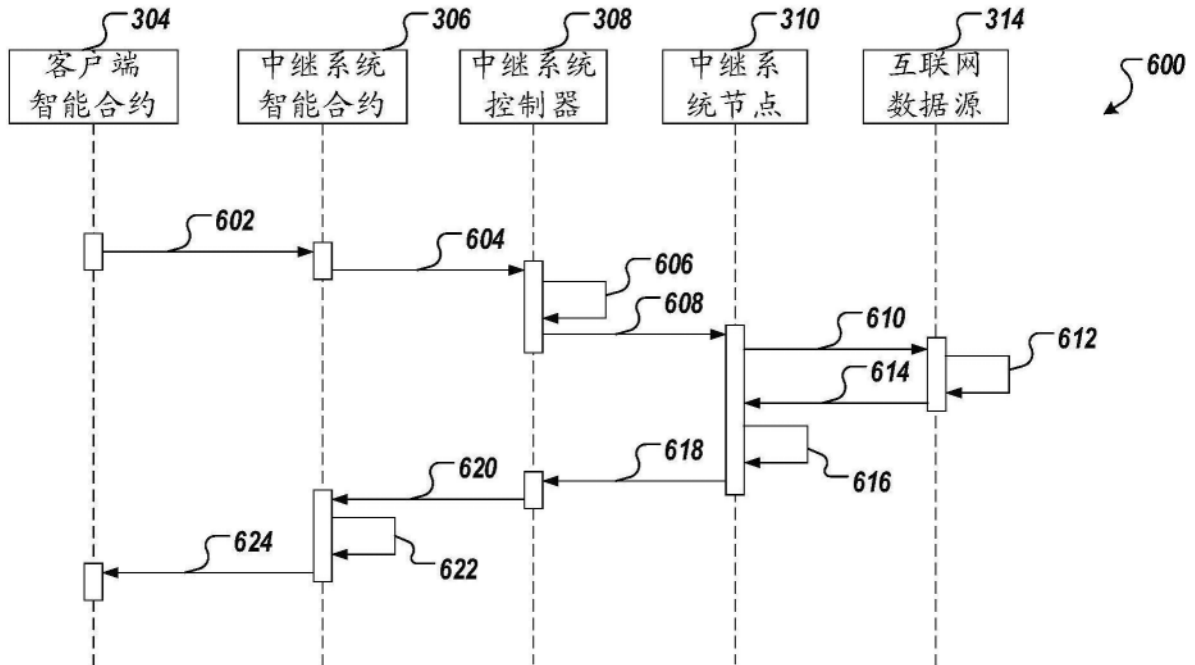


图6

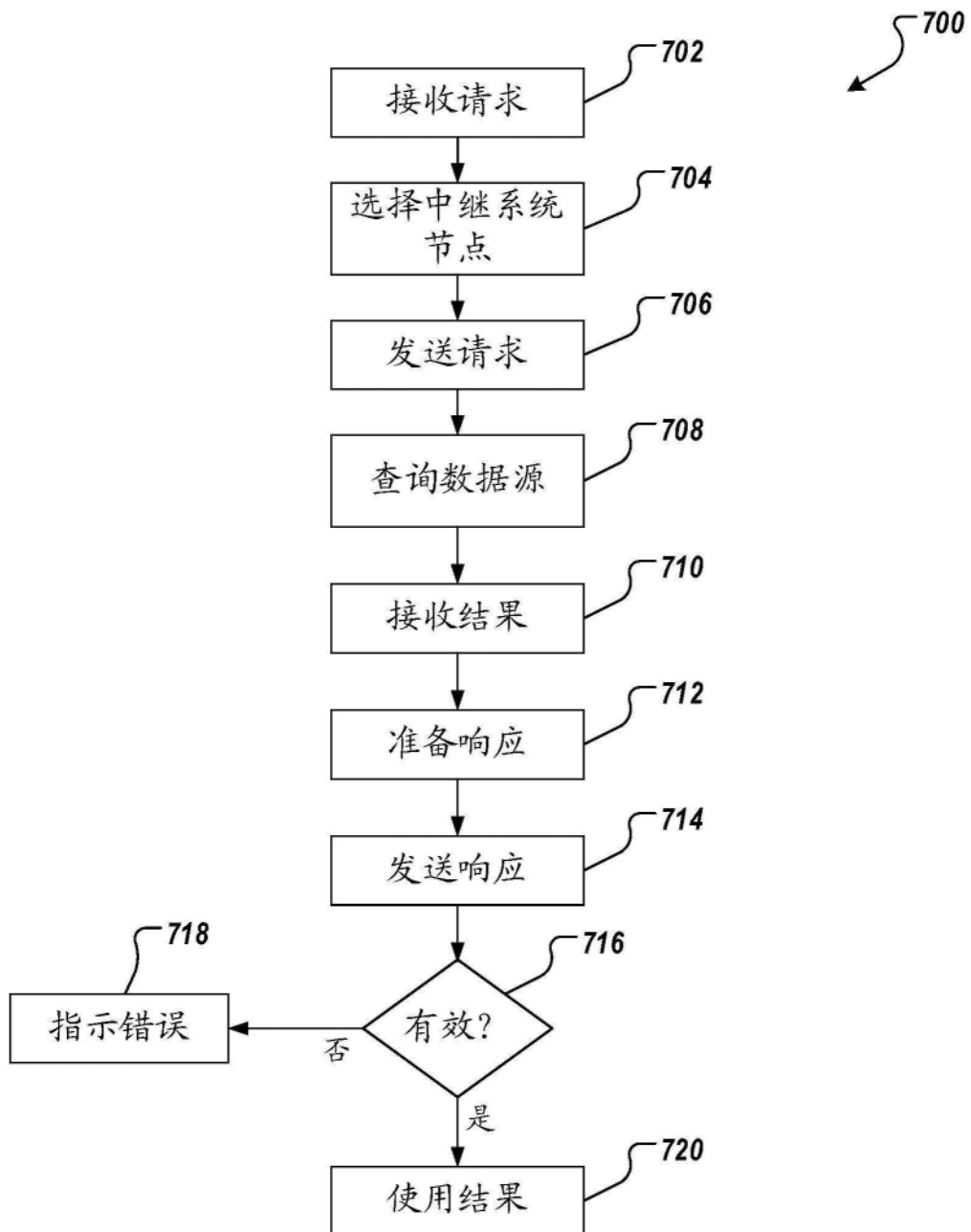


图7

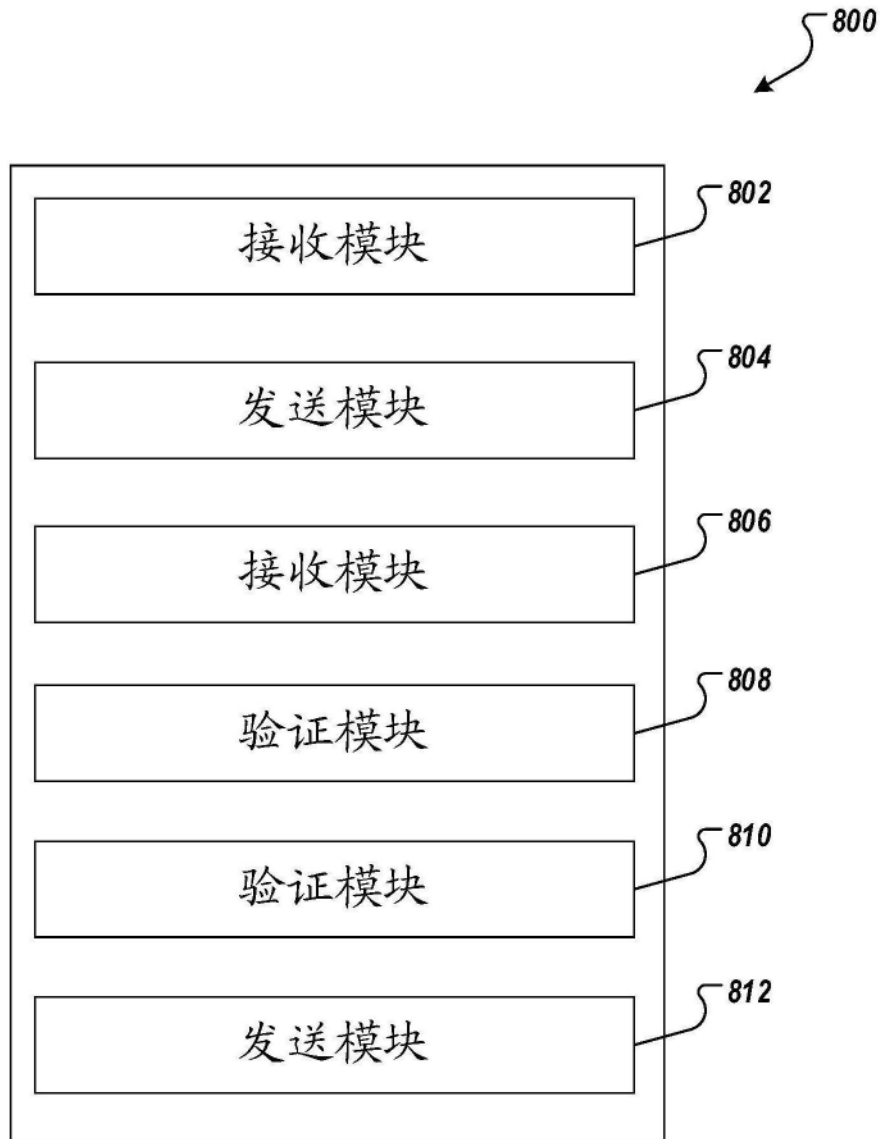


图8