(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111837115 B
(45)授权公告日 2024.09.10

(21)申请号 201980004379.4
(22)申请日 2019.07.11
(65)同一申请的已公布的文献号
申请公布号 CN 111837115 A
(43)申请公布日 2020.10.27
(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/CN2019/095617 2019.07.11
(87)PCT国际申请的公布数据
WO2019/179538 EN 2019.09.26
(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 卓海振
(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 16/2458(2006.01)
G06Q 20/40(2006.01)
G06Q 40/04(2006.01)

(56)对比文件
CN 107807984 A,2018.03.16
CN 109726229 A,2019.05.07

审查员 赵婷

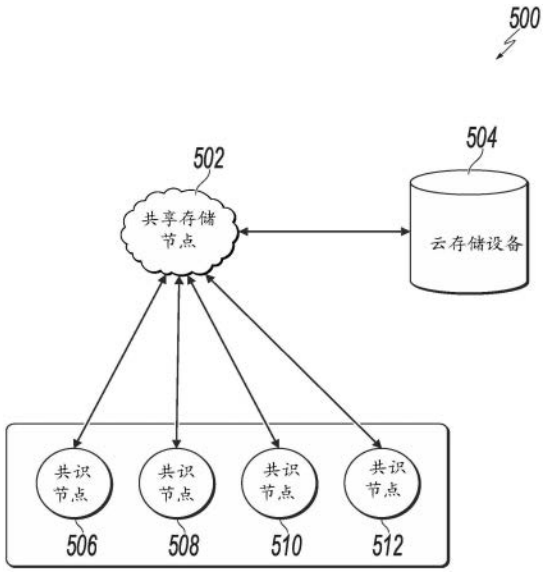
权利要求书1页 说明书15页 附图9页

(54)发明名称

共享的区块链数据存储

(57)摘要

本文公开了用于通信和共享的区块链数据的方法、系统、和装置,包括编码在计算机存储介质上的计算机程序。所述方法之一包括:区块链网络中的共识节点将与区块链的当前区块相关联的当前状态信息发送到区块链网络外部具有授权证明的可信节点;向所述可信节点发送哈希值,以检索存储在历史状态树中的账户状态;接收针对发送所述哈希值的响应中的所述账户状态;以及基于所述哈希值验证所述账户状态是否为所述区块链的一部分。



CN 111837115 B

1.一种计算机实现的用于通信共享的区块链数据的方法,所述方法包括:

区块链网络中的共识节点将与区块链的当前区块相关联的当前状态信息发送到所述区块链网络外部具有授权证明的可信节点,其中,所述共识节点存储所述当前状态信息,所述可信节点将与所述区块链的每个区块相关联的历史状态信息存储为历史状态树,所述历史状态树包括值为与所述区块链网络相关联的账户的账户状态、键为与所述账户状态对应的哈希值的键值对KVP;

所述共识节点向所述可信节点发送哈希值,以检索存储在所述历史状态树中的账户状态;

所述共识节点接收针对发送所述哈希值的响应中的所述账户状态;以及

所述共识节点基于所述哈希值验证所述账户状态为所述区块链的一部分。

2.根据权利要求1所述的方法,其中,当前状态树包括值为与所述当前区块相关联的账户状态、键为与所述当前状态树的节点相对应的节点ID的KVP。

3.根据前述任一权利要求所述的方法,其中,当前状态树中包括的每个键还包括与所述当前区块相对应的区块ID。

4.根据权利要求1或2所述的方法,其中,所述共识节点发送的所述当前状态信息包括基于与所述共识节点相关联的私钥生成的数字签名。

5.根据权利要求1或2所述的方法,其中,发送所述当前状态信息进一步包括:

将所述当前状态信息和所述当前状态信息的哈希值作为KVP发送给所述可信节点。

6.根据权利要求1或2所述的方法,其中,验证所述账户状态是所述区块链的一部分是基于以下执行的:

对所述账户状态进行哈希处理以生成经哈希处理的账户状态,以及

将所述经哈希处理的账户状态与所述哈希值进行比较。

7.根据权利要求1或2所述的方法,其中,所述可信节点在本地或云存储设备上存储历史状态信息。

8.根据权利要求1或2所述的方法,其中,当前状态树和所述历史状态树被存储为固定深度默克尔树。

9.一种用于通信共享的区块链数据的系统,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计算机可读存储器,所述指令能由所述一个或多个处理器执行以执行权利要求1至8中任一项所述的方法。

10.一种用于通信共享的区块链数据的装置,所述装置包括用于执行权利要求1-8中任一项所述的方法的多个模块。

共享的区块链数据存储

技术领域

[0001] 本文涉及区块链数据的共享存储。

背景技术

[0002] 分布式账本系统(DLS),也可称为共识网络和/或区块链网络,使得参与的实体能够安全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。区块链网络类型的示例可以包括公共区块链网络、私有区块链网络和联盟区块链网络。为选定的实体群组提供联盟区块链网络,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] 基于区块链的程序可以由诸如以太坊的分布式计算平台执行。例如,以太坊虚拟机(EVM)为以太坊中的智能合约提供运行环境。以太坊区块链可以被视为基于交易的状态机。以太坊中的状态数据可以集合成一个被称为世界状态的全局共享状态。世界状态包括以太坊账户地址和账户状态之间的映射。世界状态可以存储在诸如默克尔帕特里夏树(Merkle Patricia tree,MPT)的数据结构中。

[0004] 除了状态数据,区块链网络还可以存储其他类型的数据,例如区块数据和索引数据。区块数据可以包括区块头和区块体。区块头可以包括特定区块的身份信息,并且区块体可以包括用该区块确认的交易。当越来越多的交易进入区块链时,状态数据和区块数据的大小可能会变得非常大。在一些DLS中,即使不频繁访问某些旧的区块数据或状态数据,每个节点也会存储整个区块链副本,这会占用大量存储空间。

[0005] 因此,期望减少存储在DLS中的至少一些节点上的数据量,以节省存储成本而不显著影响处理效率。

发明内容

[0006] 本文描述了用于通信和共享区块链数据的技术。这些技术通常涉及:区块链网络中的共识节点将与区块链的当前区块相关联的当前状态信息发送到所述区块链网络外部具有授权证明的可信节点,其中,所述共识节点存储所述当前状态信息,所述可信节点将与所述区块链的每个区块相关联的历史状态信息存储为历史状态树,所述历史状态树包括值为与所述区块链网络相关联的账户的账户状态、键为与所述账户状态相对应的哈希值的键值对(KVP);所述共识节点向所述可信节点发送哈希值,以检索存储在所述历史状态树中的账户状态;所述共识节点接收针对发送所述哈希值的响应中的所述账户状态;以及所述共识节点基于所述哈希值验证所述账户状态为所述区块链的一部分。

[0007] 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进行操作。

[0008] 本文还提供了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,当该指令由

所述一个或多个处理器执行时,该指令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。

[0009] 应当理解的是,根据本文的方法可包括本文描述的方面和特征的任何组合。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何组合。

[0010] 在附图和以下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,本文的其他特征和优点将显现。

附图说明

[0011] 图1描绘了可用于执行本文实施例的环境的示例。

[0012] 图2描绘了根据本文实施例的架构的示例。

[0013] 图3描绘了根据本文实施例的固定深度默克尔树(FDMT)数据结构的示例。

[0014] 图4描绘了根据本文实施例的用于存储区块链数据的数据库的示例。

[0015] 图5描绘了根据本文实施例的使用共享存储的区块链网络的示例。

[0016] 图6描绘了根据本文实施例的使用共享存储的区块链网络的另一示例。

[0017] 图7描绘了根据本文实施例的使用共享存储的区块链网络的又一示例。

[0018] 图8描绘了可根据本文实施例执行的处理的示例。

[0019] 图9描绘了根据本文实施例的装置的模块的示例。

[0020] 各附图中相似的附图标记和名称表示相似的元件。

具体实施方式

[0021] 本文描述了用于通信和共享的区块链数据的技术。这些技术通常涉及:区块链网络中的共识节点将与区块链的当前区块相关联的当前状态信息发送到所述区块链网络外部具有授权证明的可信节点,其中,所述共识节点存储所述当前状态信息,所述可信节点将与所述区块链的每个区块相关联的历史状态信息存储为历史状态树,所述历史状态树包括值为与所述区块链网络相关联的账户的账户状态、键为与所述账户状态相对应的哈希值的键值对(KVP);所述共识节点向所述可信节点发送哈希值,以检索存储在所述历史状态树中的账户状态;所述共识节点接收针对发送所述哈希值的响应中的所述账户状态;以及所述共识节点基于所述哈希值验证所述账户状态为所述区块链的一部分。

[0022] 本文中描述的技术产生若干技术效果。例如,所述主题的实施例可以允许在不显著降低计算效率的同时节省区块链节点的存储资源。由于历史状态树中的大多数数据都是不频繁被使用的“冷”数据,因此通过仅将“冷”数据保存在共享存储节点中,可以显著提高跨区块链网络的存储空间使用率。如果共享存储节点是POA节点或基于PBFT共识通过投票选举的,则历史状态树仅需要被存储在共享存储节点中,而不必存储在每个区块链节点上。如果共享存储节点是没有POA的一部分区块链共识节点,则对于具有N个共识节点的区块链网络,其中,N等于3f+1、3f+2或3f+3,f是故障共识节点的最大数量,(N-f-1)/N个区块链共识节点仅需要将“热”数据存储为当前状态树,而无需将“冷”和“热”数据都存储为历史状态树。

[0023] 此外,对于将f+1个节点用作共享存储节点来存储历史状态树的N个共识节点的区

块链网络,最多可以容忍f个故障共识节点。换句话说,节省存储空间不会损害数据可靠性。通过容忍f个故障共识节点并仅在f+1个节点上保存整个区块链副本,可以适当地为区块链网络中的共识节点服务。由于f+1个共享存储节点确保了系统的可靠性,因此可以提高数据安全性,并且相对地独立于底层服务平台的安全级别。

[0024] 为本文实施例提供进一步的背景,并且如上所述,分布式账本系统(DLS),又可称为共识网络(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,本文使用"区块链"来一般地指代DLS。

[0025] 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括在链中紧邻其之前的前一个区块的加密哈希值链接到该前一个区块。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,在树的叶节点处的数据经哈希处理,并且在树的每个分支中的所有哈希值在该分支的根处级联(concatenate)。该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。通过确定哈希值是否与该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。

[0026] 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。本文参考联盟区块链网络更详细地描述了本文的实施例。然而,可以预期,本文的实施例可以在任何适当类型的区块链网络中实现。

[0027] 通常,联盟区块链网络在参与实体间是私有的。在联盟区块链网络中,共识处理由可被称为共识节点的授权的节点集控制,一个或多个共识节点由相应的实体(例如,金融机构、保险公司)操作。例如,由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,每个实体操作联盟区块链网络中的至少一个节点。

[0028] 在一些示例中,在联盟区块链网络内,全局区块链被提供为跨所有节点复制的区块链。也就是说,所有的共识节点相对于全局区块链处于完全状态共识。为了达成共识(例如,同意将区块添加到区块链),在联盟区块链网络内实现共识协议。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。

[0029] 图1描绘了可用于执行本文实施例的环境100的示例的图。在一些示例中,环境100使得实体能够参与至联盟区块链网络102中。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(LAN)、广域网(WAN)、因特网或其组合,并且连接网站、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。在一些示例中,网络110使得能够与联盟区块链网络102通信或在联盟区块链网络102内通信。通常,网络110表示一个或多个通信网络。在一些情况下,计算系统106、108可以是云计算系统(未示出)的节点,或者每个计算系统106、108可以是单独的云计算系统,该云计算系统包括通过网络互连的、并且用作分布式处理系统的多个计算机。

[0030] 在所描绘的示例中,计算设备106、108可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设备。计算设备的示例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,计算设备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,计算设备106可承载第一实体(例如,用户A)的计算机实施的、例如交易管理系统的服务,例如,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。计算设备108可承载第二实体(例如,用户B)的由计算机实施的、例如交易管理系统的服务,例如,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,联盟区块链网络102被示出为节点的点对点网络,计算设备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。

[0031] 图2描绘了根据本文实施例的架构200的示例。示例性概念架构200包括分别对应于参与者A、参与者B和参与者C的参与者系统202、204、206。每个参与者(例如,用户、企业)参与到被提供为点对点网络的区块链网络212中,该点对点网络包括多个节点214,至少一些节点将信息不可篡改地记录在区块链216中。如本文进一步详述,尽管在区块链网络212中示意性地描述了单个区块链216,但是在区块链网络212上提供并维护区块链216的多个副本。

[0032] 在所描绘的示例中,每个参与者系统202、204、206分别由参与者A、参与者B和参与者C提供或代表参与者A、参与者B和参与者C,并且在区块链网络中作为各自的节点214发挥作用。如本文所使用的,“节点”通常是指连接到区块链网络212并且使相应的参与者能够参与到区块链网络中的单个系统(例如,计算机、服务器)。在图2的示例中,参与者与每个节点214对应。然而,可以预期,一个参与者可以操作区块链网络212内的多个节点214,和/或多个参与者可以共享一个节点214。在一些示例中,参与者系统202、204、206使用协议(例如,超文本传输协议安全(HTTPS))和/或使用远程过程调用(RPC)与区块链网络212通信或通过区块链网络212进行通信。

[0033] 节点214可以在区块链网络212内具有不同的参与程度。例如,一些节点214可以参与共识处理(例如,作为将区块添加到区块链216的矿工节点),而其他节点214不参与此共识处理。作为另一示例,一些节点214存储区块链216的完整副本,而其他节点214仅存储区块链216的一部分的副本。例如,数据访问特权可以限制相应的参与者在其相应的系统内存储的区块链数据。在图2的示例中,参与者系统202、204、206分别存储区块链216的完整副本216’、216”、216”’。

[0034] 区块链(例如,图2的区块链216)包括区块的链,每个区块存储数据。数据的示例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(例如,文档、图像、视频、音频)可以存储在区块链中。交易的示例可以包括但不限于交换有价物(例如,资产、产品、服务、货币)。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。

[0035] 在将交易数据存储至区块中之前,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。无法对哈希值进行去哈希处理以获得交易数据。哈希处理确保即使交易数据中的轻微更改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。

[0036] 多个交易的交易数据被哈希处理并存储在区块中。例如,提供了两个交易的哈希值,并对它们自身进行哈希处理以提供另一个哈希值。重复该处理,直到对于所有要存储在区块中的交易提供单个哈希值为止。该哈希值被称为默克尔(Merkle)根哈希值,并存储在区块的头中。任何交易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。

[0037] 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工作。这样的节点被称为共识节点。上文介绍的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。

[0038] 更详细地,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)。将此哈希值添加到区块头中。共识节点还确定区块链中最新的区块(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。

[0039] 通常,PBFT提供容忍拜占庭错误(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经操纵的消息)在PBFT中实现的。在PBFT中,在包括主共识节点和备共识节点的序列中提供共识节点。主共识节点会定期更改。通过由区块链网络内的所有共识节点对区块链网络的全局状态达成一致,将交易添加到区块链中。在该处理中,消息在共识节点之间传输,并且每个共识节点证明消息是从指定的对等节点接收的,并验证在传输期间消息未被篡改。

[0040] 在PBFT中,共识协议是在所有共识节点始于相同的状态的情况下分多个阶段提供的。首先,客户端向主共识节点发送用以调用服务操作(例如,在区块链网络内执行交易)的请求。响应于接收到该请求,主共识节点将该请求组播到备共识节点。备共识节点执行该请求,并且各自向客户端发送回复。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就将记录添加到区块链的顺序达成一致,该记录被接受或者被拒绝。

[0041] 在一些区块链网络中,实施密码学以维护交易的隐私。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,则这两个节点可对交易数据进行加密处理。加密处理的示例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加密(从明文生成密文)又解密(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,这样每个节点可对交易数据进行加密/解密。

[0042] 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使用参与者B的公钥来加密数据,并将该加密的数据发送给参与者B。参与者B可以使用它的私钥解对该加密的数据(密文)进行解密并提取出原始数据(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。

[0043] 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,而另一个节点可以基于参与

者A的该数字签名来确认该消息是由该节点发送的。数字签名还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向参与者B发送一条消息。参与者A生成该消息的哈希值,随后使用其私钥对该哈希值进行加密,以提供作为加密的哈希值的数字签名。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,并且未被篡改。

[0044] 如前所述,区块链网络可以存储不同类型的数据,例如状态数据,区块数据和索引数据。状态数据通常被存储为内容寻址状态树(例如MPT或FDMT)。内容寻址状态树本质上是增量式的。即,通过添加新的树结构而不是更新现有状态树来反映账户状态的变化。因此,当将区块不断添加到区块链时,内容寻址状态树的大小会变得非常大。另一方面,树中的大多数数据是不频繁被使用的历史状态数据。就存储资源的使用而言,将这些历史状态数据存储在每个区块链节点中可能效率很低。

[0045] 在FDMT存储方案下,状态数据可以分为与当前区块相关联的当前状态数据和与区块链的所有区块相关联的历史状态数据。为了节省存储资源而不实质影响计算效率,可以将历史状态数据存储在一个或多个可信存储位置或通过投票选举的一个或多个共享存储节点上。然后可以由区块链网络的其他节点共享对所述历史状态数据的访问。

[0046] 除了共享历史状态数据之外,还可以共享区块数据。替代存储在区块链上生成的每个交易和区块,常规共识节点可以存储区块头而不是整个区块。当需要验证区块链交易时,共识节点可以查询存储完整区块的共享存储节点。由于共识节点存储与当前区块相关联的当前状态数据,因此此类数据可用于执行智能合约。因此,通过共享历史状态数据和区块数据,区块链网络的存储消耗可被减少而不显著降低交易的处理效率。

[0047] 图3描绘了根据本文实施例的FDMT数据结构300的示例。在FDMT下,账户状态可以作为键值对(KVP)存储在历史状态树302和当前状态树304的结构中。键对应于唯一标识区块链账户的地址。历史状态树302可以包括区块链的可用状态信息的完整副本。当前状态树304可以包括当前区块的状态信息。因此,当前状态树304的大小可以明显小于历史状态树302的大小。

[0048] 在一些实施例中,当前状态树304可以是位置寻址状态树。对于位置寻址状态树,当前状态树304的节点值可以基于唯一地标识该节点的键(即,节点ID)来检索。当新节点被添加到当前状态树304时,节点值可以与其唯一的节点ID(例如,当前状态树304的ID 1-1、ID 2-1等)相关联,而不必考虑其内容。在一些情况下,当前状态树304的KVP可以表示为<node ID,node value>。在一些情况下,KVP中的键可以进一步包括节点值的对应区块ID。在这种情况下,节点ID可以充当键的前缀,而区块ID可以充当键的后缀。然后可以将当前状态树304的KVP表示为<node ID+block ID,node value>。

[0049] 在一些实施例中,历史状态树302可以是内容寻址状态树。对于内容寻址状态树,每个账户值都可以具有与信息内容本身的值唯一关联的内容地址。为了从历史状态树302检索信息,可以提供内容标识,从中可以确定和检索账户值的位置。类似于MPT,历史状态树302的每个节点可以包括指向树的下一节点的指针的哈希值(例如,历史状态树302下的Hash1、Hash2和Hash3)。沿着指针的路径,最后一个元素存储键的末端部分的哈希值(例如,

历史状态树302下的Hash4、Hash5、Hash6和Hash7)以及与这些键配对的值。历史状态树302的KVP可以表示为<hash(node value),node value>。

[0050] 由于内容寻址树的节点地址取决于节点值,因此可以将新状态信息作为附加树结构添加到历史状态树302中而不是对现有树进行更改,从而保留树结构并提高数据存储/检索效率。

[0051] 图4描绘了根据本文实施例的用于存储区块链数据的数据库400的示例。数据库400可以是例如LevelDB或RocksDB的键值数据库。数据库400可以在FDMT数据结构下存储数据,该结构包括用于存储历史状态树的历史数据库410和用于存储当前状态树的当前数据库412。对于图4中描绘的四个区块,区块i-2 402、区块i-1 404和区块i 406是先前完成的区块。区块i+1 408是当前区块。每个区块可以具有区块头和区块体。区块头可以包括诸如世界状态的根哈希值的信息。根哈希值可以用作状态树的安全且唯一的标识。换句话说,根哈希值可以加密地取决于账户状态。区块体可以包括相应区块的已确认交易。

[0052] 历史数据库410可以存储历史状态树。当前数据库412可以存储当前状态树。历史状态树可以存储历史账户状态、当前状态树可以存储当前账户状态。以太坊区块链账户可以包括外部拥有的账户和合约账户。外部拥有的账户可以由私钥控制,并且不与用于执行智能合约的任何代码关联。合约账户可以通过其与用于执行智能合约的代码相关联的合约代码来控制。

[0053] 以太坊账户的状态可以包括四个组分:随机值、余额、代码哈希值和存储根。如果该账户是外部拥有的账户,则随机数可以表示从该账户地址发送的交易的数量。余额可以代表该账户拥有的数字资产。代码哈希值可以是空字符串的哈希值。存储根可以为空。如果该账户是合约账户,则随机数可以表示该账户创建的合约数量。余额可以代表该账户拥有的数字资产。代码哈希值可以是与账户关联的虚拟机代码的哈希值。存储根可以存储与存储树关联的根哈希值。存储树可以通过对账户的存储内容的哈希值进行编码来存储合约数据。

[0054] 历史状态树可以包括始于创世区块的区块链账户状态的完整副本,并且可以根据交易执行进行更新。例如,存储在先前区块i-1 404中的根哈希值是在区块i-1 404完成时世界状态的根哈希值。世界状态与存储在区块i-1 404以及在区块i-1 404之前的区块中的所有交易相关联。类似地,存储在当前区块i+1 408中的根哈希值是与存储在区块i+1 408和区块i+1 408之前的区块中的所有交易关联的世界状态的根哈希值。

[0055] 当前状态树可以包括由于新添加到当前区块i+1 408的交易而被更新或添加的状态信息。如在图3的描述中所讨论的,历史状态树可以将状态信息存储为表示为内容可寻址的<hash(node value),node value>的KVP。在一些实施例中,可以基于一个或多个与位置相关的ID来对当前状态树进行位置寻址。例如,当前状态树可以将状态信息存储为表示为<node ID,node value>的KVP,其中节点值可以基于其相应节点ID来寻址。作为另一示例,KVP中的键可以是节点ID和与节点值的对应的区块ID的组合。节点ID可以用作键的前缀,而区块ID可以用作键的后缀,以用于遍历FDMT或MPT的值。

[0056] 图5描绘了根据本文实施例的使用共享存储的区块链网络500的示例。在高层面,区块链网络500包括多个共识节点506、508、510和512,共享存储节点502以及可通信地耦合到共享存储节点502的云存储设备504。共享存储节点502可以是具有授权证明(POA)的节

点。在一些情况下,可以基于共享存储节点502的状态来提供POA。例如,共享存储节点502可以是由区块链网络500的部署者管理的节点。在这种情况下,共享存储节点502可以是区块链网络500的一部分或在区块链网络500之外。在一些情况下,可以通过投票获得POA。例如,假设区块链网络包括3f+1个节点(在图5所示的示例中f＝1,当共享存储节点502参与区块链网络500的共识时),最多可容忍的故障共识节点或拜占庭节点(行为失败或行为恶意的节点)为f。这样,如果2f+1个节点投票(由其各自的数字签名进行背书)选举共享存储节点502,则2f+1个投票可用作信任共享存储节点502的POA。

[0057] 如在对图4的讨论中所描述的,在FDMT数据结构下,当前状态数据可以与历史状态数据分离。当前状态数据可以被存储为当前状态树,其包括与当前区块相关联的状态信息,诸如根据新添加到当前区块的交易而更新或添加的状态数据。在以太坊类型的系统中,与当前区块相关联的状态信息可以被视为频繁被虚拟机检索以执行智能合约的“热”数据。历史状态数据可以存储为历史状态树,该树可以包括始于创世区块的区块链的账户状态的完整副本。与存储在历史状态树中的先前区块关联的状态信息可以被视为“冷”数据,访问这些数据以执行智能合约的频率较低。

[0058] 内容寻址状态树(例如,MPT或历史状态树)中的数据本质上是增量式的。即,账户状态因新的区块的添加而导致的更改不会改变现有的历史状态树,而是通过向历史状态树添加新的树结构来反映。因此,由于新区块的产生,历史状态树的大小可能会变得非常大。由于历史状态树中的大多数数据都是不频繁被使用的“冷”数据,因此就存储资源的使用而言,将这些数据存储在每个区块链节点中可能效率很低。

[0059] 为了节省存储资源而不显著降低计算效率,可以将历史状态树存储在与共享存储节点502相关联的历史数据库(诸如图4中描述的历史数据库410)、或可通信地耦接到共享存储节点502的云存储设备504中。在一些实施例中,共享存储节点502可以向共识节点506、508、510和512共享对历史状态树的访问。云存储设备504可以是在云上提供存储服务的存储设备,诸如网络附加存储(NAS)或对象存储服务(OSS)。

[0060] 在一些实施例中,当交易被处理进入当前区块时,与交易相关联的状态数据可以由共识节点506、508、510和512中的一个或多个发送到共享存储节点502以进行存储。在一些实施例中,共识节点506、508、510和512中的一个或多个可以将状态数据和状态数据的哈希值作为KVP发送给共享存储节点502。在接收到状态数据或KVP之后,共享存储节点502可以验证接收到的状态数据或KVP是否已在本地存储或存储在云存储设备504中。如果是,则共享存储节点502可以拒绝或放弃接收到的状态数据。否则,共享存储节点502可以计算所述状态数据的哈希值或验证所接收到的哈希值是所述状态数据的哈希值,并将所述哈希值和所述状态数据存储到历史状态树。

[0061] 在一些实施例中,共享存储节点502可以验证状态数据是否是区块链的有效状态数据。共享存储节点502可以计算接收到的状态数据的哈希值。如前所述,共享存储节点502可以存储历史状态树,该历史状态树是内容寻址的并且包括区块链的状态信息的完整副本。然后,计算出的哈希值可被用于基于区块链的世界状态根哈希值(例如,使用Merkle证明)来验证状态数据是否为区块链的一部分。如果哈希值被验证为区块链的一部分,则可以将该状态数据确定为内容寻址数据。

[0062] 当共识节点506、508、510和512中的任何一个需要从共享存储节点502检索状态数

据时,可以将对应的哈希值发送到共享存储节点502。由于存储在共享存储节点502中的历史状态树是内容寻址的,因此所述哈希值可以被用作用以对产生哈希值的对应状态数据进行寻址的键。在基于该哈希值识别出对应的状态数据之后,共享存储节点502可以将识别出的状态数据发送回共识节点。接收状态数据的共识节点可以对接收到的状态数据进行哈希处理,以验证该状态数据是否为内容寻址的。如果是,则可以将状态数据确定为真实的。否则,状态数据是不真实的。如果状态数据不真实,则共识节点可以选择将共享存储节点502报告为故障节点(或拜占庭节点)。如果区块链网络500中存在存储历史状态树的其他节点,则共识节点可将所述哈希值发送到一个或多个其他节点以检索对应的状态数据。

[0063] 图6描绘了根据本文实施例的使用共享存储的区块链网络600的另一示例。在高层面,区块链网络600包括多个共识节点606、608、610和612,多个共享存储节点602和604,以及可通信地耦接到所述多个共享存储节点602和604中的一个或多个的云存储设备614。在一些情况下,共享存储节点602和604可以是具有POA的节点,诸如由区块链网络600的部署者管理的节点。在这种情况下,共享存储节点602和604可以是区块链网络600的一部分或在区块链网络600之外。在一些情况下,可以通过投票获得POA。例如,假设区块链网络包括3f+1个节点(在图6所示的示例中f=1,当共享存储节点602和604均不参与区块链网络600的共识时)、3f+2个节点(当共享存储节点602和604之一参与区块链网络600的共识时)、或3f+3个节点(当共享存储节点602和604均参与区块链网络的共识时),其中,f是拜占庭节点的最大数量,如果2f+1个节点投票(由他们各自的数字签名进行背书)选举共识节点作为共享存储节点,则可以将2f+1个投票用作信任共享存储节点的POA。

[0064] 如前所述,为了节省存储资源而不显著降低计算效率,可以将历史状态树存储在与共享存储节点602和604相关联的历史数据库(诸如图4中描述的历史数据库410)、或可通信地耦接到共享存储节点602和604的云存储设备614中。共享存储节点602和604可以向共识节点606、608、610和612共享对历史状态树的访问。云存储设备614可以是可以在云上提供存储服务的存储设备,例如NAS或OSS。

[0065] 当交易被处理成当前区块时,与该交易相关联的状态数据可以由共识节点606、608、610和612中的一个或多个发送到共享存储节点602和604进行存储。在一些实施例中,共识节点606、608、610和612中的一个或多个可以将状态数据和状态数据的哈希值作为KVP发送给共享存储节点602和604。在接收到状态数据之后,共享存储节点602和604可以验证接收到的状态数据或KVP是否已在本地存储或存储在云存储设备614中。如果是,则共享存储节点602和604可以拒绝或放弃接收到的状态数据。否则,共享存储节点602和604可以计算状态数据的哈希值或验证接收到的哈希值是该状态数据的哈希值,并将所述哈希值和状态数据存储到历史状态树。

[0066] 在一些实施例中,共享存储节点602和604可以验证状态数据是否是区块链的有效状态数据。如前所述,共享存储节点602和604可以存储历史状态树,该历史状态树是内容寻址的并且包括区块链的状态信息的完整副本。共享存储节点602和604可以计算接收到的状态数据的哈希值。然后,计算出的哈希值可用于基于区块链的世界状态根哈希值(例如,使用Merkle证明)来验证状态数据是否为区块链的一部分。如果是,则可以将状态数据确定为内容寻址的。

[0067] 当共识节点606、608、610和612中的任何一个需要从共享存储节点602或604检索

状态数据时,可以将对应的哈希值发送到与共识节点通信的共享存储节点。在如图6所示的示例中,共识节点606和608可以将哈希值发送到共享存储节点602,共识节点610和612可以将哈希值发送到共享存储节点604。共识节点可以基于地理位置、网络状况、已建立的通信协议、安全考虑等选择用以从中检索状态数据的共享存储节点。应当理解,共识节点606、608、610和612中的任何一个都可以根据本文的不同实施例选择与共享存储节点602和604中的任何一个通信。

[0068] 由于存储在共享存储节点602和604中的历史状态树是内容寻址的,因此哈希值可以用作用于寻址对应状态数据的键。在基于哈希值识别出对应的状态数据之后,对应的共享存储节点602或604可以将识别出的状态数据发送回共识节点。接收状态数据的共识节点可以对接收到的状态数据进行哈希处理,以验证所述状态数据是否为内容寻址的。如果是,则将状态数据确定为真实的。否则,状态数据是不真实的。如果状态数据不真实,则共识节点可以选择将共享存储节点报告为故障节点(或拜占庭节点)。如果区块链网络600中存在存储历史状态树的其他节点,则共识节点可以将所述哈希值发送到一个或多个其他节点以检索对应的状态数据。

[0069] 图7描绘了根据本文实施例的使用共享存储的区块链网络700的又一示例。在高层面,区块链网络700包括多个共识节点706、708、710和712,多个共享存储节点702和704,以及可通信地耦接到所述多个共享存储节点702和704中的一个或多个的云存储设备。共享存储节点702和704可以是具有POA的节点,例如由区块链网络700的部署者管理的节点。在这种情况下,共享存储节点702和704可以是区块链网络700的一部分或在区块链网络700之外。如前所述,POA也可以通过投票获得。例如,假设区块链网络包括3f+1个节点(在图7所示的示例中f=1,当共享存储节点702和704都不参与区块链网络700的共识时)、3f+2个节点(当共享存储节点702和704之一参与区块链网络700的共识时)、或者3f+3个节点(当共享存储节点702和704都参与区块链网络的共识时),其中,f是拜占庭节点的最大数量,如果2f+1个节点投票(由它们各自的数字签名进行背书)选举共识节点作为共享存储节点,可以将2f+1个投票用作信任共享存储节点的POA。

[0070] 为了节省存储资源而不显著降低计算效率,可以将历史状态树存储在与共享存储节点702、704相关联的历史数据库(例如,图4中描述的历史数据库410)上或云存储设备(例如,NAS或OSS)。共享存储节点702和704可向共识节点706、708、710和712共享对历史状态树的访问。

[0071] 在一些实施例中,除了共享来自共享存储节点702和704的历史状态数据之外,还可以共享区块数据。类似于区块链网络的全节点,共享存储节点702和704可以存储区块链的完整副本,其包括在区块链上生成的每个交易和区块。在一些实施例中,共享存储节点702和704可以存储区块链的每个区块的区块体。类似于区块链网络的轻节点,共识节点706、708、710和712可以基于诸如简化支付验证(SPV)之类的方法来存储区块链的每个区块的区块头。SPV可以允许节点验证交易是否已包含在区块中,而无需下载整个区块链。由于共识节点706、708、710和712也存储当前状态树,因此与当前区块相关联的状态数据可被用于执行智能合约。这样,通过共享来自共享存储节点702和704的区块数据,可以在保持直接执行智能合约的能力的同时,进一步减少共识节点706、708、710和712的存储消耗。

[0072] 图8是用于通信和共享的区块链数据的处理800的示例。为方便起见,处理800将被

描述为由位于一个或多个位置、并根据本文被适当地编程的一个或多个计算机的系统执行。例如,被适当地编程的例如图1的计算系统106、108的计算系统中的计算设备,可以执行处理800。

[0073] 在802,区块链网络中的共识节点将与区块链的当前区块相关联的当前状态信息发送到在区块链网络外部具有授权证明的可信节点,其中,共识节点存储当前状态信息,而可信节点将与区块链的每个区块相关联的历史状态信息存储为历史状态树,历史状态树包括值为与区块链网络相关联的账户的账户状态、键为与所述账户状态相对应的哈希值的KVP。

[0074] 在804,共识节点向可信节点发送哈希值,以检索存储在历史状态树中的账户状态。

[0075] 在806,共识节点接收针对发送哈希值的响应中的账户状态。

[0076] 在808,共识节点基于所述哈希值验证所述账户状态是区块链的一部分。

[0077] 在一些情况下,当前状态树包括值为与当前区块相关联的账户状态、键为与当前状态树的节点相对应的节点ID的KVP。

[0078] 在一些情况下,当前状态树中包括的每个键还包括与当前区块相对应的区块ID。

[0079] 在一些情况下,共识节点发送的当前状态信息包括基于与共识节点相关联的私钥生成的数字签名。

[0080] 在一些情况下,发送当前状态信息还包括:将当前状态信息和当前状态信息的哈希值作为KVP发送给可信节点。

[0081] 在一些情况下,验证所述账户状态是区块链的一部分是基于对账户状态进行哈希处理以生成经哈希处理的账户状态,并将所述经哈希处理的账户状态与哈希值进行比较。

[0082] 在一些情况下,可信节点在本地或云存储设备上存储历史状态信息。

[0083] 在一些情况下,当前状态树和历史状态树被存储为固定深度默克尔树。

[0084] 图9是根据本文实施例的装置900的模块的示例的图。

[0085] 装置900可以是被配置为通信和共享的区块链数据的共识节点的实施例的示例。装置900可以对应于上述实施例,并且装置900包括以下:发送模块902,将与区块链的当前区块相关联的当前状态信息发送到区块链网络外部具有授权证明的可信节点,其中,共识节点存储当前状态信息,可信节点将与区块链的每个区块相关联的历史状态信息存储为历史状态树,所述历史状态树包括值为与区块链网络相关联的账户的账户状态、键为与所述账户状态相对应的哈希值的KVP;所述发送模块902将哈希值发送给所述可信节点,以检索存储在所述历史状态树中的账户状态;接收模块904,接收针对发送所述哈希值的响应中的所述账户状态;验证模块906,基于所述哈希值验证所述账户状态为所述区块链的一部分。

[0086] 在可选实施例中,装置900还包括以下:所述当前状态树包括值为与当前区块相关联的账户状态、键为与当前状态树的节点相对应的节点ID的KVP。

[0087] 在可选实施例中,当前状态树中包括的每个键还包括与当前区块相对应的区块ID。

[0088] 在可选实施例中,共识节点发送的当前状态信息包括基于与共识节点相关联的私钥生成的数字签名。

[0089] 在可选实施例中,发送当前状态信息还包括:将当前状态信息和当前状态信息的

哈希值作为KVP发送给可信节点。

[0090] 在可选实施例中,验证所述账户状态是区块链的一部分是基于对账户状态进行哈希处理以生成经哈希处理的账户状态,并将所述经哈希处理的账户状态与所述哈希值进行比较来执行的。

[0091] 在可选实施例中,可信节点在本地或云存储设备上存储历史状态信息。

[0092] 在可选实施例中,当前状态树和历史状态树被存储为固定深度默克尔树。

[0093] 前述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施,或者可以通过使用具有特定功能的产品来实施。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、智能手机、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。

[0094] 对于装置中每个模块的功能和作用的实施处理,可以参考前一方法中对应步骤的实施处理。为了简明,这里省略了细节。

[0095] 由于装置实施基本上对应于方法实施,对于相关部件,可以参考方法实施例中的相关描述。先前描述的装置实施仅是示例。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,以实现本文解决的目标。本领域的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。

[0096] 再次参考图9,其可以被解释为示出了共识节点的内部功能模块和结构。执行主体本质上可以是电子设备,并且该电子设备包括以下: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一个或多个计算机可读存储器。在一些实施例中,一个或多个计算机可读存储器耦接至一个或多个处理器且其上存储有编程指令,所述编程指令能够由所述一个或多个处理器执行以执行如本文中所述的算法、方法、功能、处理、流程和程序。

[0097] 本文中描述的技术产生若干技术效果。例如,主题的实施例可以允许在不显著降低计算效率的同时节省区块链节点的存储资源。由于历史状态树中的大多数数据是不频繁被使用的“冷”数据,因此通过仅将“冷”数据保存在共享存储节点中,可以显著提高跨区块链网络的存储空间使用率。如果共享存储节点是POA节点或基于PBFT共识通过投票选举的,则历史状态树仅需要被存储在共享存储节点中,而不必存储在每个区块链节点上。如果共享存储节点是没有POA的一部分区块链共识节点,则对于具有N个共识节点的区块链网络,其中N等于3f+1、3f+2或3f+3,其中,f是故障共识节点的最大数量,(N-f-1)/N个区块链共识节点仅需要将“热”数据存储为当前状态树,而无需将“冷”和“热”数据都存储为历史状态树。

[0098] 此外,对于将f+1个节点用作共享存储节点来存储历史状态树的、具有N个共识节点的区块链网络,最多可以容忍f个故障共识节点。换句话说,节省存储空间不会损害数据可靠性。通过容忍f个故障共识节点并仅在f+1个节点上保存整个区块链副本,可以适当地为区块链网络中的共识节点服务。由于f+1个共享存储节点确保了系统的可靠性,因此可以提高数据安全性,并且相对地独立于底层服务平台的安全级别。

[0099] 所描述的主题的实施例可以单独或组合地包括一个或多个特征。

[0100] 例如,在第一实施例中,一种计算机实现的用于通信共享的区块链数据的方法,所述方法包括:区块链网络中的共识节点将与区块链的当前区块相关联的当前状态信息发送到区块链网络外部具有授权证明的可信节点。其中,所述共识节点存储当前状态信息,所述可信节点将与区块链的每个区块相关联的历史状态信息存储为历史状态树,所述历史状态树包括值为与区块链网络相关联的账户的账户状态、键为与所述账户状态相对应的哈希值的KVP;如果所述可信节点验证了所述当前状态信息是所述区块链的一部分,则所述共识节点验证所述当前状态信息是包括在所述历史状态树中的;所述共识节点向所述可信节点发送哈希值,以检索存储在所述历史状态树中的账户状态;所述共识节点接收针对发送所述哈希值的响应中的所述账户状态;以及所述共识节点基于所述哈希值验证所述账户状态为所述区块链的一部分。

[0101] 前述和其他描述的实施例可各自可选地包括一个或多个以下特征:

[0102] 第一特征,可与以下特征中的任意一个组合,指定所述当前状态树包括值为与所述当前区块相关联的账户状态、键为与所述当前状态树的节点相对应的节点ID的KVP。

[0103] 第二特征,可以与之前或之后特征中的任意一个组合,指定包括在所述当前状态树中的每个键还包括与所述当前区块相对应的区块ID。

[0104] 第三特征,可以与之前或之后特征中的任意一个组合,指定所述共识节点发送的所述当前状态信息包括基于与所述共识节点相关联的私钥生成的数字签名。

[0105] 第四特征,可以与之前或之后特征中的任意一个组合,指定发送所述当前状态信息还包括将所述当前状态信息和当前状态信息的哈希值作为KVP发送给所述可信节点。

[0106] 第五特征,可以与之前或之后特征中的任意一个组合,指定验证所述账户状态是所述区块链的一部分是基于对所述账户状态进行哈希处理以生成经哈希处理的账户状态,并将所述经哈希处理的账户状态与所述哈希值进行比较来执行的。

[0107] 第六特征,可以与之前或之后特征中的任意一个组合,指定所述可信节点在本地或云存储设备上存储历史状态信息。

[0108] 第七特征,可以与之前或之后特征中的任意一个组合,指定将所述当前状态树和所述历史状态树存储为固定深度默克尔树。

[0109] 本文中描述的主题、动作和操作的实施可以在数字电子电路、有形体现的计算机软件或固件、计算机硬件中实施,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实现为一个或多个计算机程序,例如,编码在计算机程序载体上的一个或多个计算机程序指令模块,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一个或多个计算机可读存储介质,其上编码或存储有指令。载体可以是有形的非暂态计算机可读介质,诸如磁盘、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)或其他类型的介质。可选地或附加地,载体可以是人工生成的传播信号,例如,机器生成的电信号、光信号或电磁信号,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可以部分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。

[0110] 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、或声明或

程序性语言;它可以配置为任何形式,包括作为独立程序,或作为模块、组件、引擎、子程序或适合在计算环境中执行的其他单元,该环境可包括由数据通信网络互连的一个或多个位置上的一台或多台计算机。

[0111] 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。

[0112] 用于执行计算机程序的处理器包括:例如,通用和专用微处理器两者,和任意种类的数字计算机的任意一个或多个处理器。通常,处理器将接收用于执行的计算机程序的指令以及来自耦接至处理器的非暂态计算机可读介质的数据。

[0113] 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一个或多个的组合的代码。

[0114] 本文中描述的处理和逻辑流程可以由执行一个或多个计算机程序的一台或多台计算机或处理器执行,以通过对输入数据进行操作并生成输出来执行操作。处理和逻辑流程也可以由例如FPGA、ASIC或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。

[0115] 适合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。计算机的元件可包括用于执行指令的中央处理单元和用于存储指令和数据的一个或多个存储设备。中央处理单元和存储器可以补充有专用逻辑电路或结合在专用逻辑电路中。

[0116] 通常,计算机还将包括或可操作地耦接至一个或多个存储设备,以从一个或多个存储设备接收数据或向一个或多个存储设备发送数据。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,计算机非必需这样的设备。因此,计算机可以耦接到例如一个或多个存储器的本地和/或远程的一个或多个存储设备。例如,计算机可以包括作为计算机的组成部件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,计算机可以嵌入在另一设备中,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,这里仅举几例。

[0117] 组件之间可以通过直接或经由一个或多个中间件进行诸如电连接或光连接地彼此连接通信而彼此“耦接”。如果组件中的一个组件被集成到另一个中,则组件也可以被彼此“耦接”。例如,集成到处理器中的存储组件(例如,L2高速缓存组件)被“耦接到”处理器。

[0118] 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。另外,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,通过将网页发送到用户设备上的web浏览器以响应于从web浏览器接收的请求,或者通过与在例如智能手机或电子平板电脑等的用户设备上运行的应用程序(app)交互。此外,计算机可以通过向个人设备(例如,运行消息收发应用程序的智能手机)轮流发送文本消息或其他形式的消息并且从用户接收响应消息来与用户交互。

[0119] 本文使用与系统、装置和计算机程序组件有关的术语“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操作中使得系统执行该操作或动作的软件、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被数据处理装置执行时促使该装置执行该操作或动作的指令。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该操作或动作的电子逻辑。

[0120] 虽然本文包含许多具体实施细节,但是这些细节不应被解释为由权利要求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。在本文中单个实施例的上下文中描述的多个特征也可以在单个实施例中组合实现。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描述为以某些组合起作用并且甚至最初如此要求保护,但是在一些情况下可以从要求保护的组合中删除该组合的一个或多个特征,并且可以要求保护指向子组合或子组合的变体。

[0121] 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中叙述了操作,但是这不应该被理解为:为了达到理想的效果,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,上述实施例中的各种系统模块和组件的划分不应被理解为在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一起集成在单个软件产品中或打包成多个软件产品。

[0122] 已经描述了主题的特定实施方式。其他实施方式在以下权利要求的范围内。例如,权利要求中记载的动作可以以不同的顺序执行并且仍然实现所期望的结果。作为一个示例,附图中描绘的过程不一定需要所示的特定顺序或次序以实现所期望的结果。在一些情况下,多任务和并行处理可能是有利的。

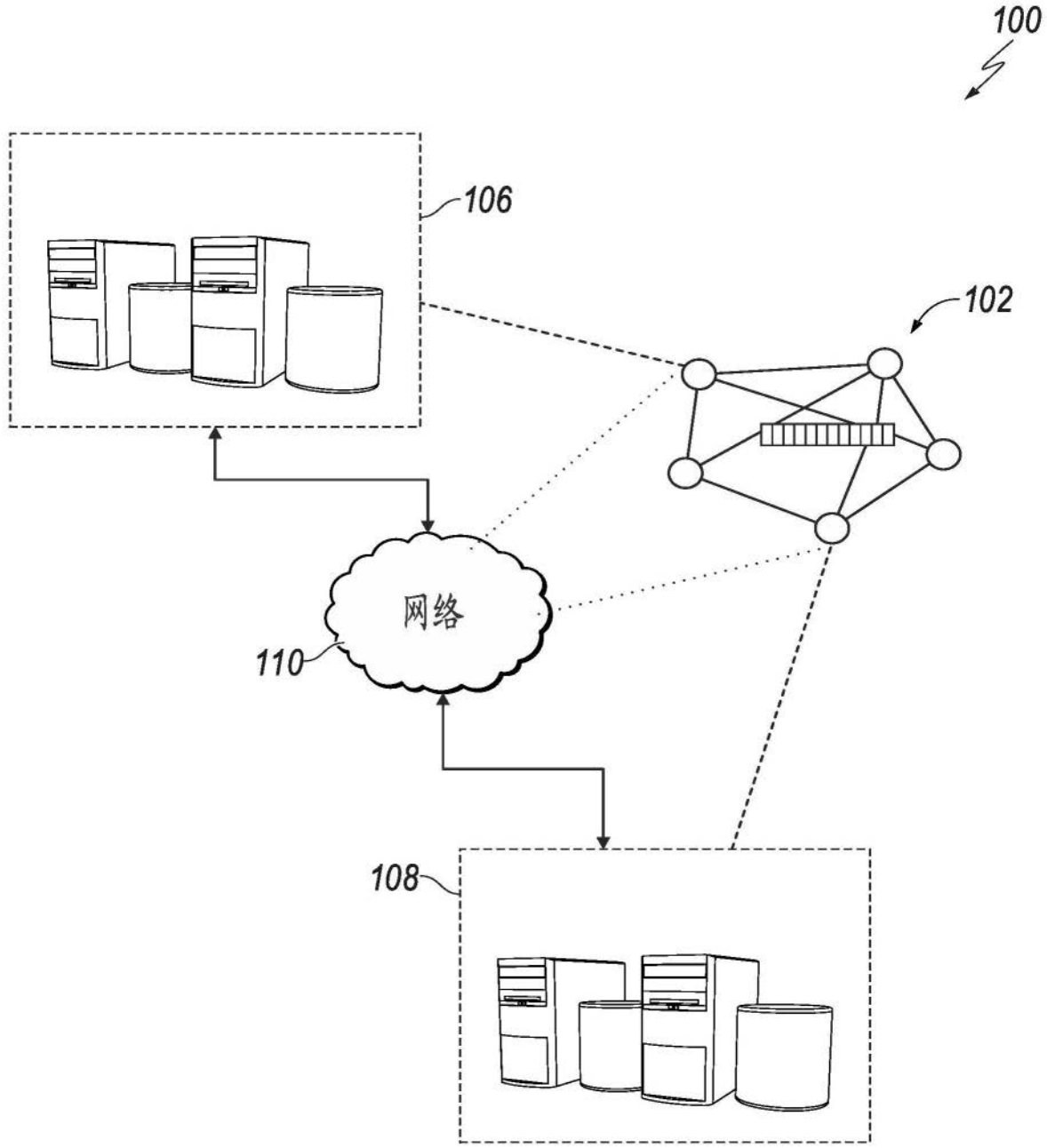


图1

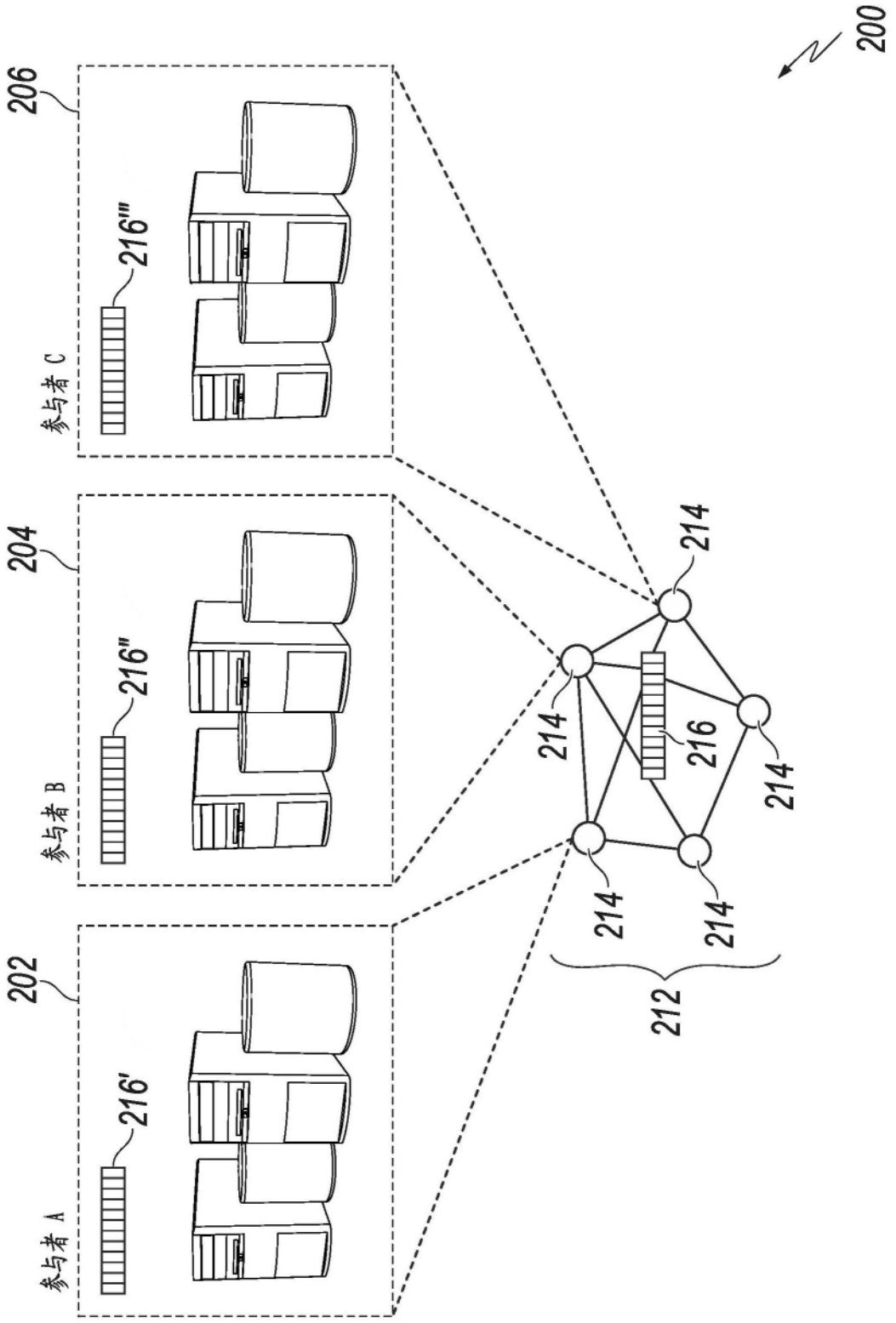

200
206
216'''
参与者 C
204
216''
参与者 B
202
216'
参与者 A
214
214
216
214
214
214
212

图2

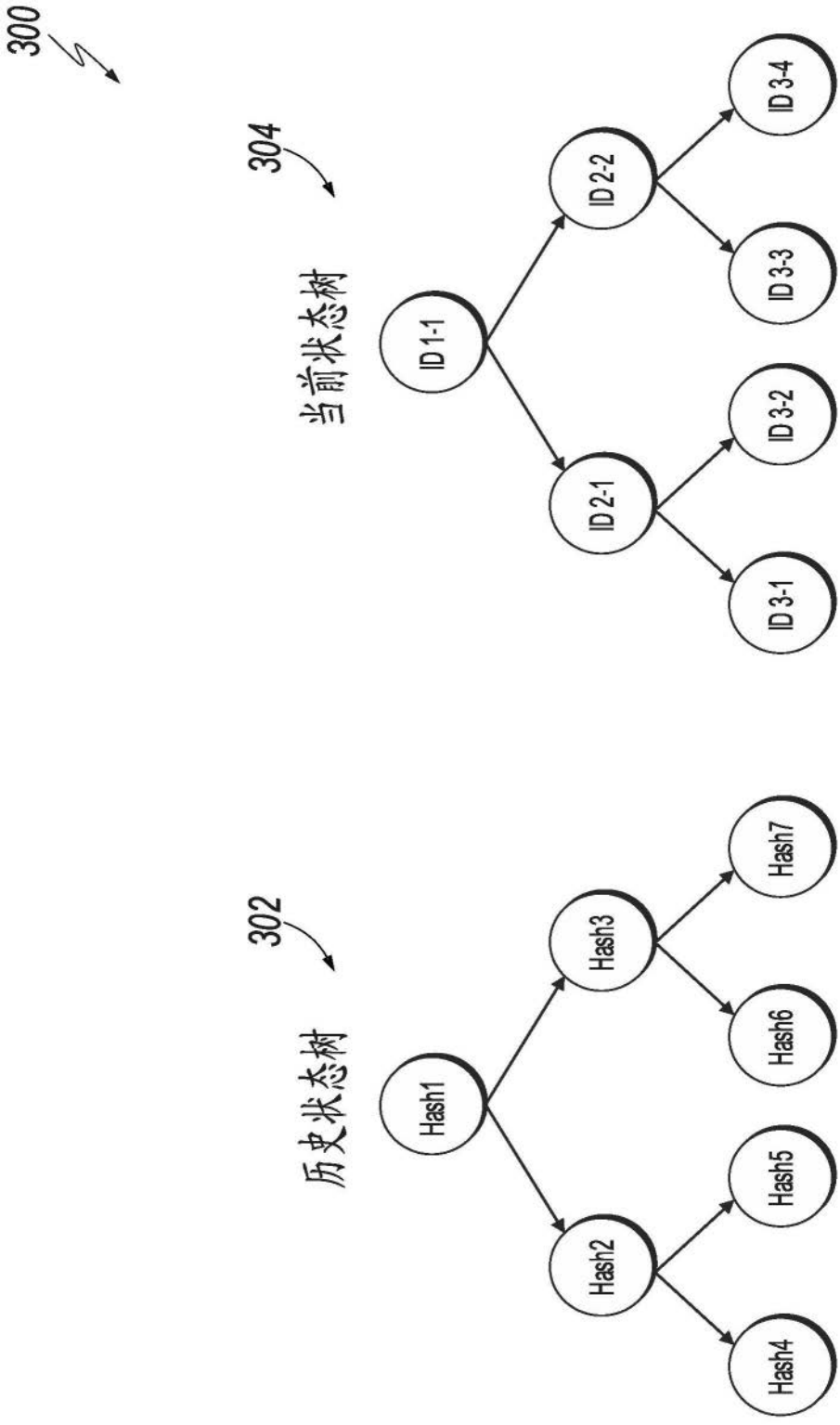

300
304
当前状态树
ID 1-1
ID 2-2
ID 2-1
ID 3-4
ID 3-3
ID 3-2
ID 3-1
302
历史状态树
Hash1
Hash3
Hash2
Hash7
Hash6
Hash5
Hash4

图3

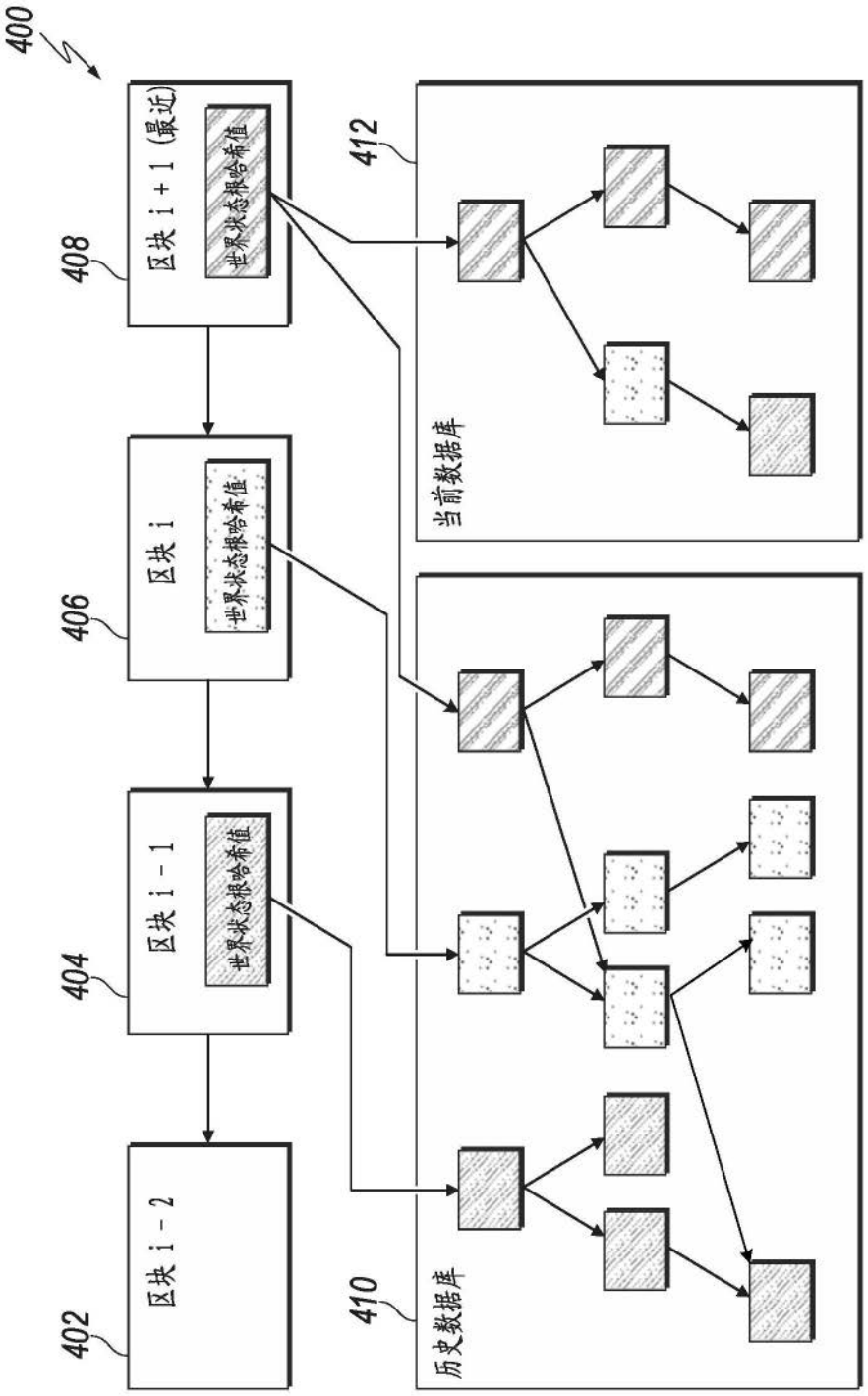

400
区块 i + 1 (最近)
世界状态根哈希值
408
区块 i
世界状态根哈希值
406
区块 i - 1
世界状态根哈希值
404
区块 i - 2
402
412
当前数据库
410
历史数据库

图4

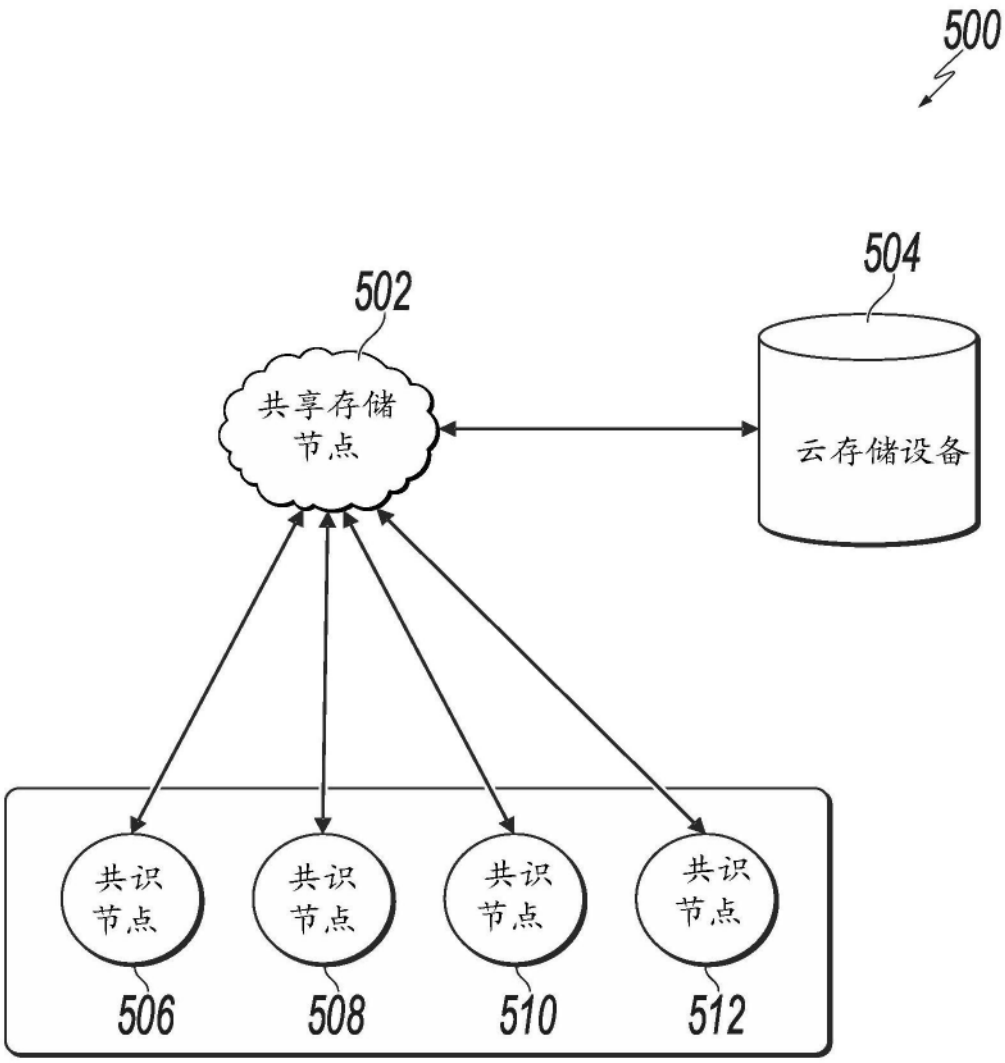


图5

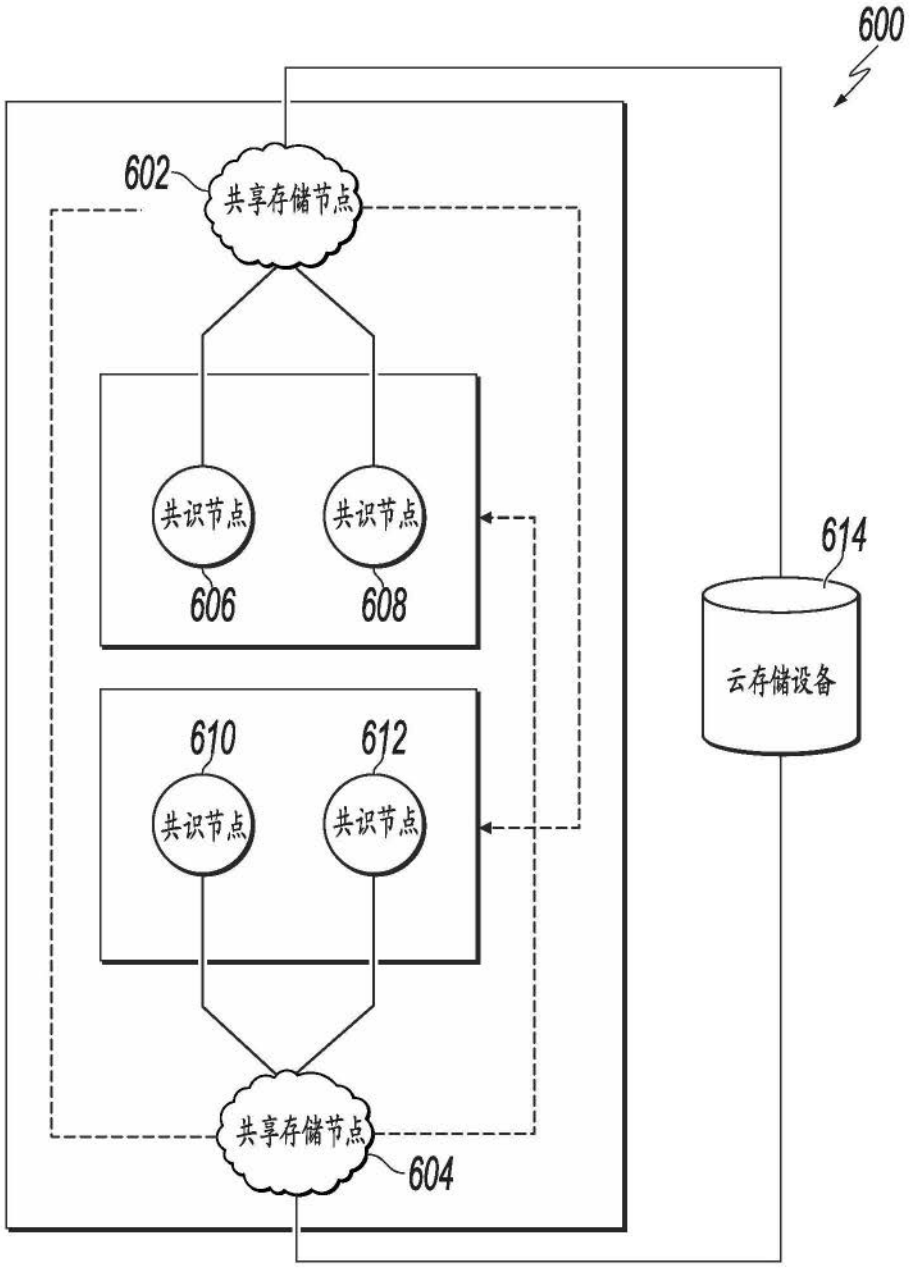

600
602
共享存储节点
共识节点
606
共识节点
608
614
云存储设备
610
共识节点
612
共识节点
共享存储节点
604

图6

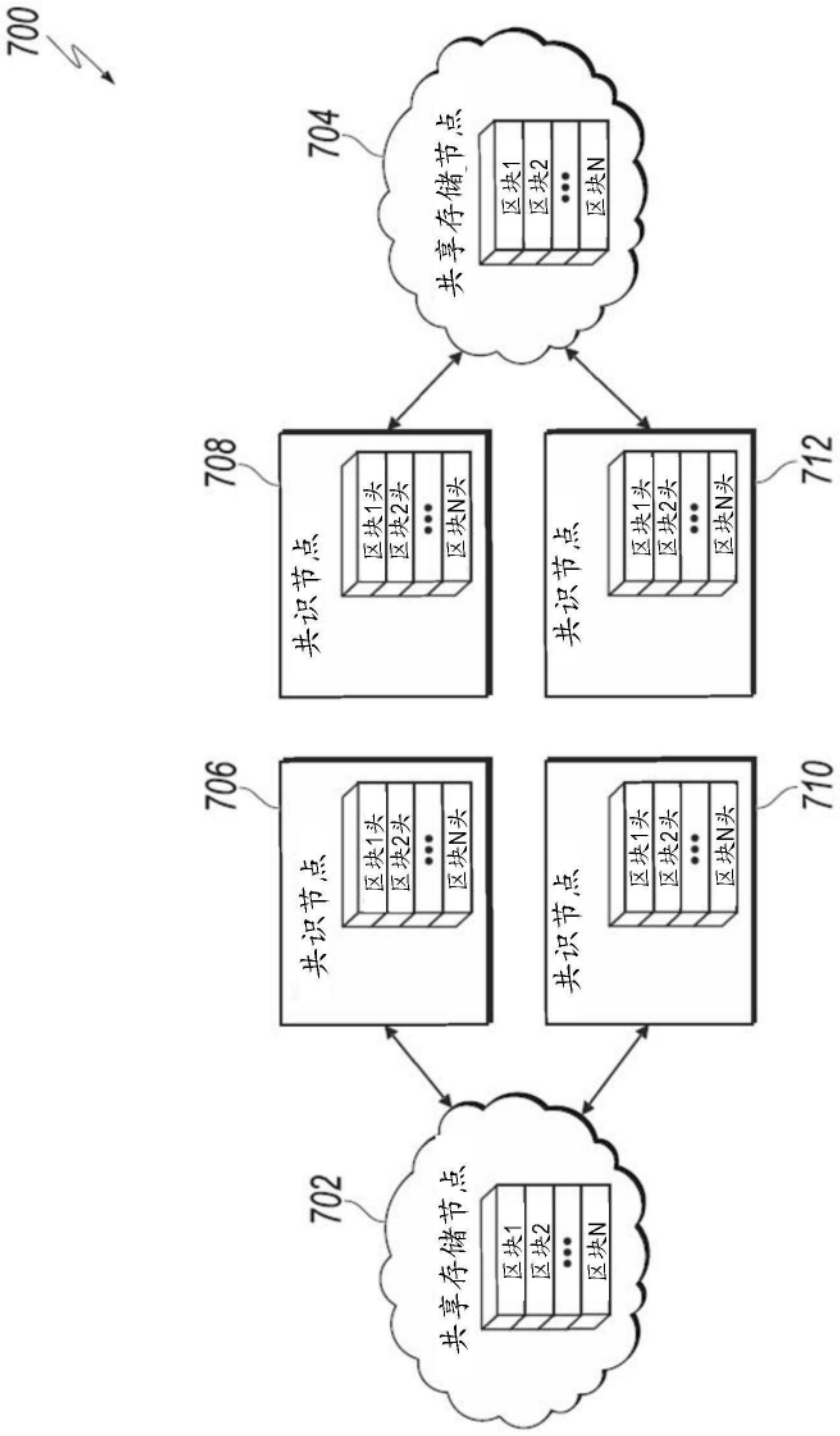

700
704
共享存储节点
区块1
区块2
区块N
708
共识节点
区块1头
区块2头
区块N头
712
共识节点
区块1头
区块2头
区块N头
706
共识节点
区块1头
区块2头
区块N头
710
共识节点
区块1头
区块2头
区块N头
702
共享存储节点
区块1
区块2
区块N

图7

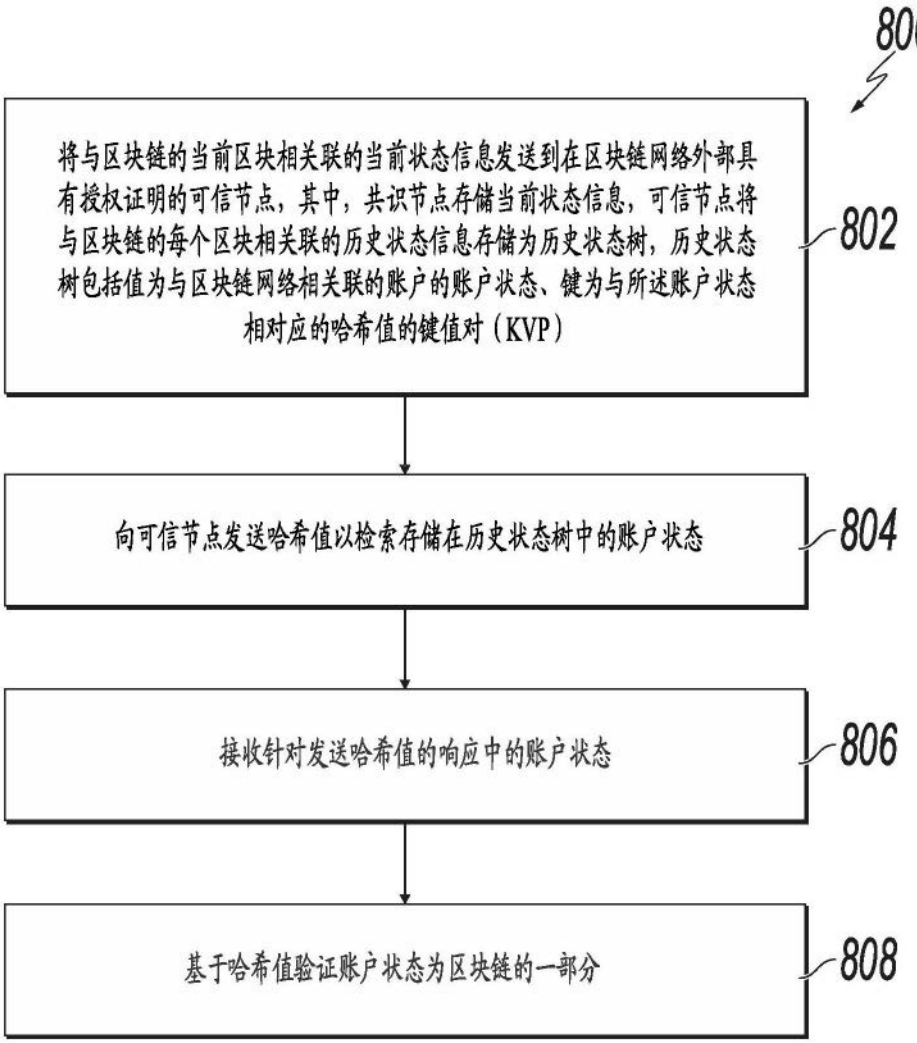

800
将与区块链的当前区块相关联的当前状态信息发送到在区块链网络外部具有授权证明的可信节点，其中，共识节点存储当前状态信息，可信节点将与区块链的每个区块相关联的历史状态信息存储为历史状态树，历史状态树包括值为与区块链网络相关联的账户的账户状态、键为与所述账户状态相对应的哈希值的键值对（KVP）
802
向可信节点发送哈希值以检索存储在历史状态树中的账户状态
804
接收针对发送哈希值的响应中的账户状态
806
基于哈希值验证账户状态为区块链的一部分
808

图8

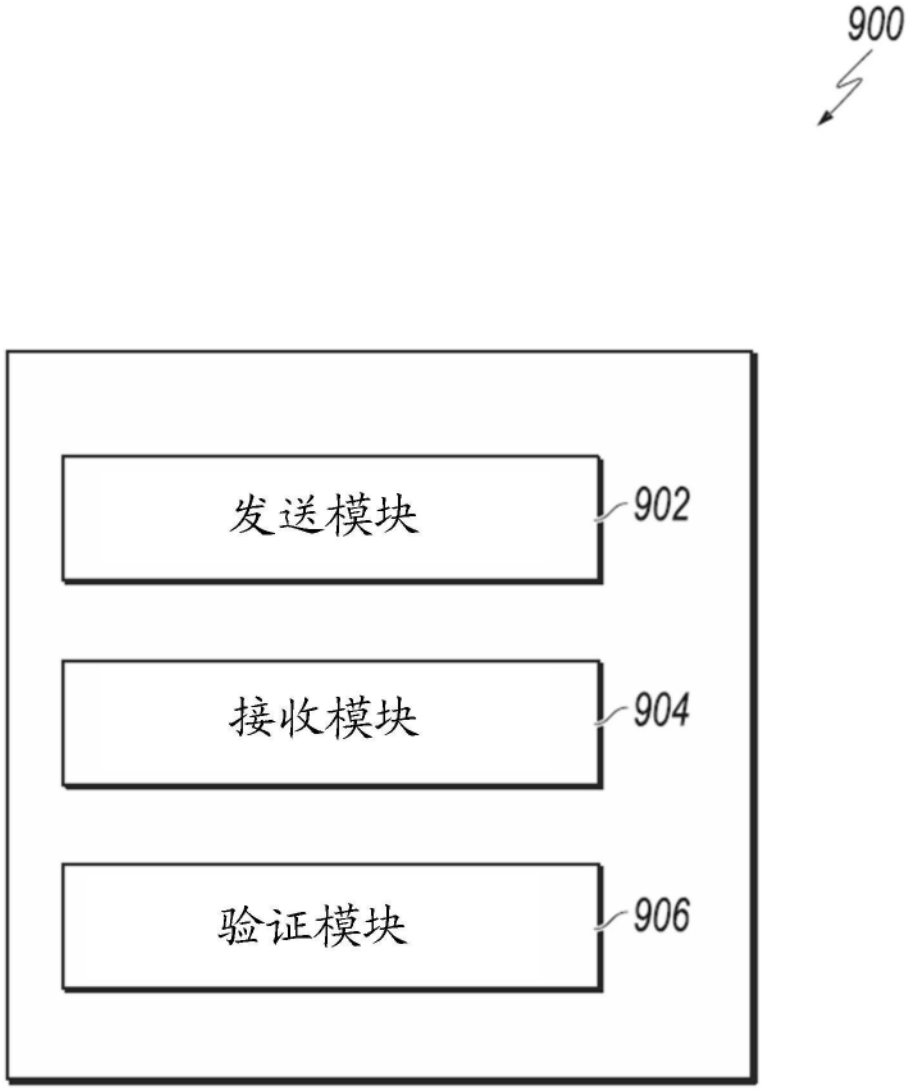


图9