



(12) 发明专利

(10) 授权公告号 CN 110720204 B

(45) 授权公告日 2022. 06. 03

(21) 申请号 201880036713.X

(22) 申请日 2018.12.19

(65) 同一申请的已公布的文献号
申请公布号 CN 110720204 A

(43) 申请公布日 2020.01.21

(85) PCT国际申请进入国家阶段日
2019.12.02

(86) PCT国际申请的申请数据
PCT/CN2018/122145 2018.12.19

(87) PCT国际申请的公布数据
W02019/072298 EN 2019.04.18

(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 应鹏飞 刘正

(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.

H04L 9/40 (2022.01)

H04L 9/32 (2006.01)

H04L 67/1097 (2022.01)

G06F 3/06 (2006.01)

G06Q 20/06 (2012.01)

G06Q 20/22 (2012.01)

(56) 对比文件

CN 107809484 A, 2018.03.16

CN 106372533 A, 2017.02.01

CN 108062202 A, 2018.05.22

审查员 张浩

权利要求书3页 说明书8页 附图4页

(54) 发明名称

基于共享秘密的区块链存储方法、存储介质及系统

(57) 摘要

本申请的实施方式包括接收用以将数据项存储在区块链网络中的请求,并且作为响应:将所述数据项划分为多个数据块;将每个所述数据块分配给所述区块链网络中的不同节点,其中,每个节点将分配的数据块存储在私有维护的分布式哈希表中;和将与每个所述数据块相关联的信息存储在由所述区块链网络维护的区块链中,所述信息包括每个所述数据块的存储位置。



1. 一种计算机实施的用于在区块链网络中分布式存储数据的方法,所述方法包括:
接收用以将数据项存储在所述区块链网络中的请求;
响应于接收到所述请求:
将所述数据项划分为多个数据块;
将每个所述数据块分配给所述区块链网络中的不同节点,其中,每个节点将所述分配的数据块存储在私有维护的分布式哈希表中;和
将与每个所述数据块相关联的信息存储在由所述区块链网络维护的区块链中,所述信息包括每个所述数据块的用于标识网络中数据位置的文件路径。
2. 如权利要求1所述的方法,还包括:
接收用以检索已存储的数据项的请求;和
响应于接收到用以检索所述已存储的数据项的请求:
基于存储在所述区块链中的、包括每个所述数据块的位置的所述信息,从所述分配的节点检索每个已存储的数据块;
根据所述已存储的数据块重建所述已存储的数据项;和
发送对用以检索所述已存储的数据项的请求的响应,其中,所述响应包括所述重建的数据项。
3. 如权利要求1所述的方法,还包括:
在所述区块链中存储用于根据已存储的数据块恢复所述数据项的指令。
4. 如权利要求2所述的方法,其中,重建所述已存储的数据项,包括:
拼接所述检索到的数据块,以生成所述数据项的副本。
5. 如权利要求2所述的方法,还包括:
将与用以检索所述已存储的数据项的请求相关的记录存储在所述区块链中。
6. 如权利要求2所述的方法,其中,检索每个所述已存储的数据块、根据所述已存储的数据块重建所述已存储的数据项、以及发送对用以检索的所述请求的响应是由存储在所述区块链中并在所述区块链网络上运行的智能合约执行的。
7. 如权利要求1所述的方法,其中,每个所述分布式哈希表存储所述数据块的文件路径、所述数据块的值以及相关节点的标识。
8. 一种非暂态计算机可读存储介质,其耦接到一个或多个计算机并配置有能由所述一个或多个计算机执行的指令,以:
接收用以将数据项存储在区块链网络中的请求;
响应于接收到所述请求:
将所述数据项划分为多个数据块;
将每个所述数据块分配给所述区块链网络中的不同节点,其中,每个节点将所述分配的数据块存储在私有维护的分布式哈希表中;和
将与每个所述数据块相关联的信息存储在由所述区块链网络维护的区块链中,所述信息包括每个所述数据块的用于标识网络中数据位置的文件路径。
9. 如权利要求8所述的非暂态计算机可读存储介质,还配置有由所述一个或多个计算机可执行的指令,以:
接收用以检索已存储的数据项的请求;和

响应于接收到用以检索所述已存储的数据项的请求；

基于存储在所述区块链中的、包括每个所述数据块的位置的所述信息，从所述分配的节点检索每个已存储的数据块；

根据所述已存储的数据块重建所述已存储的数据项；和

发送对用以检索所述已存储的数据项的请求的响应，其中，所述响应包括所述重建的数据项。

10. 如权利要求8所述的非暂态计算机可读存储介质，配置有由所述一个或多个计算机可执行的指令，以：

在所述区块链中存储用于根据已存储的数据块恢复所述数据项的指令。

11. 如权利要求9所述的非暂态计算机可读存储介质，其中，重建所述已存储的数据项，包括：

拼接所述检索到的数据块以生成所述数据项的副本。

12. 如权利要求9所述的非暂态计算机可读存储介质，配置有能由所述一个或多个计算机执行的指令，以：将与用以检索所述已存储的数据项的请求相关的记录存储在所述区块链中。

13. 如权利要求9所述的非暂态计算机可读存储介质，其中，检索每个所述已存储的数据块、根据所述已存储的数据块重建所述已存储的数据项、以及发送对用以检索的所述请求的响应是由存储在所述区块链中并在所述区块链网络上运行的智能合约执行的。

14. 如权利要求8所述的非暂态计算机可读存储介质，其中，每个所述分布式哈希表存储所述数据块的文件路径、所述数据块的值以及相关节点的标识。

15. 一种系统，包括：

一个或多个计算机；和

一个或多个计算机可读存储器，其耦接到所述一个或多个计算机并配置有能由所述一个或多个计算机执行的指令，以：

接收用以将数据项存储在区块链网络中的请求；

响应于接收到所述请求；

将所述数据项划分为多个数据块；

将每个所述数据块分配给所述区块链网络中的不同节点，其中，每个节点将所述分配的数据块存储在私有维护的分布式哈希表中；和

将与每个所述数据块相关联的信息存储在由所述区块链网络维护的区块链中，所述信息包括每个所述数据块的用于标识网络中数据位置的文件路径。

16. 如权利要求15所述的系统，还配置有由所述一个或多个计算机可执行的指令，以：

接收用以检索已存储的数据项的请求；和

响应于接收到用以检索所述已存储的数据项的请求；

基于存储在所述区块链中的、包括每个所述数据块的位置的所述信息，从所述分配的节点检索每个已存储的数据块；

根据所述已存储的数据块重建所述已存储的数据项；和

发送对用以检索所述已存储的数据项的请求的响应，其中，所述响应包括所述重建的数据项。

17. 如权利要求15所述的系统,配置有能由所述一个或多个计算机执行的指令,以在所述区块链中存储用于根据已存储的数据块恢复所述数据项。

18. 如权利要求16所述的系统,其中,重建所述已存储的数据项包括:
拼接所述检索到的数据块以生成所述数据项的副本。

基于共享秘密的区块链存储方法、存储介质及系统

背景技术

[0001] 分布式账本 (DLS), 还可被称为共识网络和/或区块链网络, 使得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 (例如, 加密货币) 的情况下, DLS 通常被称为区块链网络。区块链网络的示例类型可以包括公有区块链网络、私有区块链网络和联盟区块链网络。公有区块链网络对所有实体开放使用 DLS, 并开放参与共识处理。私有区块链网络针对特定实体提供, 该实体集中控制读写权限。联盟区块链网络针对选择的实体组群提供, 该实体组群控制共识处理, 并且联盟区块链网络包括访问控制层。

[0002] 在一些情况下, 区块链的每个实体例如在私有哈希表中存储和控制自己的数据。虽然这种数据存储方案增加了数据安全性和隐私性, 但它使数据共享和实体合作变得困难。

发明内容

[0003] 本申请的实施方式包括计算机实施的用于区块链上的分布式存储数据的方法。更具体地, 本申请的实施方式涉及使用分布式哈希表和多方计算来改善区块链上的数据安全性和数据共享。

[0004] 在一些实施方式中, 所述方法包括: 接收用以将数据项存储在区块链网络中的请求, 并且作为响应: 将所述数据项划分为多个数据块; 将每个所述数据块分配给所述区块链网络中的不同节点, 其中, 每个节点将所述分配的数据块存储在私有维护的分布式哈希表中; 并且将与每个所述数据块相关联的信息存储在由所述区块链网络维护的区块链中, 所述信息包括每个所述数据块的存储位置; 接收用以检索所述已存储的数据项的请求, 并且作为响应: 基于存储在所述区块链中的、包括每个所述数据块的位置的所述信息, 从所述分配的节点中检索每个已存储的数据块; 根据所述已存储的数据块重建所述已存储的数据项; 并发送对用以检索所述已存储的数据项的请求的响应, 其中, 所述响应包括所述重建的数据项。其他实施方式包括对应的系统、装置和计算机程序, 所述计算机程序被配置为执行所述方法的操作, 并编码在计算机存储设备上。

[0005] 这些和其他实施方式可以各自可选地包括以下一个或多个特征:

[0006] 在一些情况下, 将与每个数据块相关联的信息存储在所述区块链中包括: 将每个数据块的路径存储在所述区块链中。

[0007] 在一些实施方式中, 在所述区块链中存储用于根据所述已存储的数据块恢复所述数据项的指令。

[0008] 在一些情况下, 重建所述已存储的数据项包括: 拼接 (concatenate) 所述检索到的数据块以生成所述数据项的副本。

[0009] 在一些情况下, 将与用以检索所述已存储的数据项的请求相关的记录存储在所述区块链中。

[0010] 在一些实施方式中, 检索每个已存储的数据块、根据所述已存储的数据块重建所述已存储的数据项、以及发送对用以检索的所述请求的响应是由存储在所述区块链中并在

所述区块链网络上运行的智能合约执行的。

[0011] 在一些情况下,每个分布式哈希表存储所述数据块的文件路径、所述数据块的值以及相关节点的标识。

[0012] 一些实施方式可以包括耦接到一个或多个处理器且其上存储有指令的非暂态计算机可读存储介质,当由所述一个或多个处理器执行所述指令时,促使所述一个或多个处理器根据本文提供的方法的实施方式执行操作。

[0013] 一些实施方式可以包括系统,所述系统包括计算设备和耦接到所述计算设备且其上存储有指令的计算机可读存储设备,当由所述计算设备执行所述指令时,促使所述计算设备根据本文提供的方法的实施方式执行操作。

[0014] 本申请还提供了耦接到一个或多个处理器且其上存储有指令的非暂态计算机可读存储介质,当由所述一个或多个处理器执行所述指令时,促使所述一个或多个处理器根据本文提供的方法的实施方式执行操作。

[0015] 本申请还提供了一种用于实施本文提供的方法的系统。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的其上存储有指令的计算机可读存储介质,当由所述一个或多个处理器执行所述指令时,促使所述一个或多个处理器根据本文提供的方法的实施方式执行操作。

[0016] 应了解,根据本申请的方法可包括本文所述的方面和特征的任意组合。也就是说,根据本申请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。

[0017] 本申请的一个或多个实施方式的细节将在下文结合附图和描述进一步阐述。本申请的其他特征或优点将从描述和附图以及权利要求中显而易见。

附图说明

[0018] 图1描绘了可用于执行本申请实施方式的示例性环境。

[0019] 图2描绘了根据本申请实施方式的示例性概念架构。

[0020] 图3描绘了区块链中实施分布式存储数据方案的示例性系统。

[0021] 图4描绘了可根据本申请实施方式执行的示例性处理。

[0022] 各附图中的相同附图标记表示相同的元件。

具体实施方式

[0023] 本申请的实施方式包括:计算机实施的用于区块链上的分布式存储数据的方法。更具体地,本申请的实施方式涉及使用分布式哈希表和多方计算来改善区块链上的数据安全性和数据共享。在一些实施方式中,所述方法包括:接收用以将数据项存储在区块链网络中的请求,并且作为响应:将所述数据项划分为多个数据块;将每个数据块分配给区块链网络中的不同节点,其中,每个节点将所述分配的数据块存储在私有维护的分布式哈希表中;并且将与每个数据块相关联的信息存储在由区块链网络维护的区块链中,该信息包括每个数据块的存储位置;接收用以检索所述已存储的数据项的请求,并且作为响应:基于存储在区块链中的、包括每个数据块的位置的信息,从分配的节点中检索每个已存储的数据块;根据已存储的数据块重建已存储的数据项;并且发送对用以检索所述已存储的数据项的请求

的响应,其中,所述响应包括重建的数据项。

[0024] 为本申请的实施方式提供进一步的背景,如上所述的,分布式账本系统(DLS),又可被称为共识网络(例如,由点对点节点组成)和区块链网络,使得参与的实体能够安全地且不可篡改地进行交易并存储数据。虽然术语区块链通常与比特币加密货币网络相关联,但是本文所使用的区块链一般指不参考任何特定用例情况下的DLS。如上所述,区块链网络可以被提供为公有区块链网络、私有区块链网络或联盟区块链网络。

[0025] 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,数百、数千甚至数百万个实体可以协同运作公有区块链网络,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的实体的公有网络。在一些示例中,大多数实体(节点)必须对每个区块签名,以使该区块有效并被添加到区块链网络的区块链(分布式账本)中。示例性公有区块链网络包括比特币网络,比特币网络是点对点支付网络。比特币网络利用被称为区块链的分布式账本。如上所述,然而,术语区块链通常用于指代分布式账本,而不特指比特币网络。

[0026] 通常,公有区块链网络支持公开交易。在公有区块链网络内公开交易被所有节点共享,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。也就是说,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,同意将区块添加至区块链),在公有区块链网络内实施共识协议。示例性共识协议包括但不限于在比特币网络中实施的工作量证明(POW)。

[0027] 通常,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。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,仅在一些交易中)。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,监管机构可以控制权限)。

[0028] 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,对于参与实体而言,联盟区块链网络可以被认为是私有网络。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。

[0029] 本文参考公有区块链网络进一步详细描述了本申请的实施方式,该公有区块链网络在参与的实体之间是公有的。然而,可以预期,可以在任何合适类型的区块链网络中实现本申请的实施方式。

[0030] 鉴于以上背景,本文进一步详细描述了本申请的实施方式。更具体地,并且如上所述,本申请的实施方式涉及使用分布式哈希表和多方计算来改进区块链上的数据安全性和数据共享。

[0031] 在一些实施方式中,数据项被划分为不同的部分,并且每个部分被存储在参与区块链网络的实体的哈希表中。每个实体或外部服务可以使用部署在区块链上的例如智能合约的程序,来查看数据并对数据执行操作。因此,虽然没有单个实体可以访问整个数据,但是每个实体仍然可以获得数据的某些度量。

[0032] 图1描绘了可用于执行本申请实施方式的示例性环境100。在一些示例中,示例性环境100使得实体能够参与到区块链网络102中。区块链网络102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。示例性环境100包括计算系统106、108和网络110。在一些示例中,网络110包括局域网(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)和后端系统。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。

[0033] 在所描述的示例中,计算系统106、108可以各自包括能够作为节点参与到区块链网络102中的任何合适的计算系统。示例性计算设备包括但不限于服务器、台式计算机、膝上型计算机、平板计算设备和智能电话。在一些示例中,计算系统106、108承载一个或多个由计算机实施的服务,用于与区块链网络102交互。例如,计算系统106可以承载第一实体(例如,用户A)的由计算机实施的、例如交易管理系统的服务,第一实体使用该交易管理系统管理它与一个或多个其他实体(例如,其他用户)的交易。计算系统108可以承载第二实体(例如,用户B)的由计算机实施的、例如交易管理系统的服务,第二实体使用该交易管理系统管理它与一个或多个其他实体(例如,其他用户)的交易。在图1的示例中,区块链网络102被表示为节点的点对点网络,且计算系统106、108分别提供参与区块链网络102的第一实体和第二实体的节点。

[0034] 图2描绘了根据本申请实施方式的概念性架构200的示例。示例概念性架构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包括三个实体,实体1(E1)、实体2(E2)和实体3(E3),每个实体具有对应的交易管理系统208。

[0035] 在所描述的示例中,承载服务层204包括用于每个交易管理系统208的接口210。在一些示例中,各个交易管理系统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提供各个交易管理系统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,接口210与区块链网络层206之间的通信是利用远程过程调用(RPC)来进行的。在一些示例中,接口210“承载”用于各个交易管理系统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)。

[0036] 如本文所述的,区块链网络212被提供为包括多个节点214的点对点网络,所述多个节点214在区块链216中不可篡改地记录信息。尽管示意性地描绘了单个区块链216,但是在区块链网络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存储与参与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。

[0037] 图3描绘了在区块链网络中实施分布式存储数据方案的示例性系统300。系统300包括向应用程序308提供数据的区块链网络,例如图2的区块链网络212。区块链网络中的例如节点214a-214c的每个实体维护分布式哈希表(distributed hash table,DHT),以存储未在区块链216上公布的私有数据。例如,节点214b与DHT 304b相关联,并且节点214c与不同的DHT 304c相关联。

[0038] 在一些实施方式中,希望在区块链网络212中存储数据A 302的用户首先将数据A 302分成两份或更多份,例如A1 302a、A2 302b和A3 302c。每个块数据被发送到不同的节点并在节点的DHT中维护。例如,A1 302a存储在与节点214a相关联的DHT 304a中,A2 302b存

储在与节点214b相关联的DHT 304b中,以及A3 302c存储在与节点214c相关联的DHT 304c中。因此,用户的数据以去中心化的方式存储,并且由于没有一个单独的存储节点具有对用户数据的完全访问权,因此保持了安全性。仅当可信服务从各个存储节点请求和接收各个数据块时,才恢复用户的数据,如下面并参照图4所述。

[0039] 每个节点可以在区块链上公布存储的块数据的路径。例如,在数据A被分块并存储在区块链网络212中之后,存储在区块链216中的区块链交易可以记录每个块数据的位置,其中,该位置包括存储数据的节点以及与该节点相关联的DHT中的内部文件路径。在一些实施方式中,文件路径是统一资源定位符(URL)或用于标识网络中数据位置的其他字符串。然后,该区块链交易被包括在区块链216的最新区块中,使其可被区块链网络212中的所有节点查看。汇总数据A的存储的示例性区块链交易如下表1所示:

[0040]

数据	节点	文件路径	DHT值
A	2	路径1	A1
A	3	路径2	A2
A	4	路径3	A3

[0041] 表1

[0042] 为了使用数据A 302,服务310请求应用程序308从区块链网络212收集块数据。例如,应用程序308可以是存储在区块链216中并在区块链网络212上运行的智能合约程序。应用程序308可以首先搜索区块链216以定位每个块数据被存储在哪里,然后检索并生成该数据A 302的副本。在一个示例中,应用程序308可以拼接块数据A1 302a、A2 302b和A3 302c以生成数据A 302的副本。在另一示例中,应用程序308可以对块数据执行汇总操作以恢复数据A 302。在一些情况下,尽管服务310从应用程序308接收所生成的数据A 302的副本,但是服务310不能访问任何单独的数据块。因此,该访问方案保护了各个节点上的数据安全性和数据隐私。在一个示例中,每个节点可以表示存储有用户在特定银行中的金融交易的银行。该服务试图基于用户过去的金融交易来确定用户的房屋抵押贷款。尽管该服务可以访问用户例如数据A 302的总金融交易,但是该服务不能在任何特定银行中看到该用户的金融交易,例如,块数据A1 302a、A2 302b和A3 302c。

[0043] 在一些情况下,汇总数据A的存储的区块链交易可以包括该数据的每个块的哈希值。应用程序308或处理该块数据的另一应用程序可以使用这些哈希值来验证每个块自首次存储以来未被更改。汇总数据A的存储的区块链交易还可以包括通过连接所有块形成的完整数据集的哈希值,该哈希值可以用于验证数据自最初被分块和存储以来未被更改。

[0044] 在一些情况下,应用程序308可以在区块链216中记录操作。例如,应用程序308可以记录请求数据的服务310的标识、数据检索操作的成功或失败、操作的时间或与操作有关的其他信息。该信息可以用作访问日志,以记录每次检索的特定数据项。

[0045] 在一些实施方式中,一旦应用程序308完成检索数据并且该交易被区块链网络212验证,则每个存储节点可以被奖励由区块链网络212支持的指定数量的数字货币。该奖励可以用作对区块链网络212中参与分布式存储数据方案的节点的激励。然后将检索到的数据返回给服务310以进行进一步的操作。

[0046] 在一些情况下,请求数据可能需要进行身份验证。例如,服务310可能在请求数据时需要提供其标识或其他凭证。该系统可以包括对存储在区块链网络中的每个数据项的权

限,并且可以在根据分块的数据重建数据项之前,基于凭证验证服务310被授权查看数据项。在一些实施方式中,汇总数据A的存储的区块链交易(在上述表1中示出)可以包括每个数据块的权限信息或完整数据项的权限信息。

[0047] 在一些情况下,汇总数据A的存储的区块链交易可以包括数据项的加密哈希值,服务310必须正确解密该哈希值,以证明它被授权访问存储的数据项。例如,在存储有数据项的用户希望自己是唯一有权访问该数据项的情况下,可以使用该用户的公钥加密该哈希值,从而只能使用该用户的私钥解密该加密的哈希值。在一些实施方式中,数据项本身可以在被分块之前被加密并存储在区块链网络中,从而一旦分块被重新组合和恢复,仅允许具有正确密钥的实体解密该内容。

[0048] 图4描绘了可根据本申请实施方式执行的示例性处理400。在一些实施方式中,可以使用由一个或多个计算设备执行的一个或多个计算机可执行程序来执行处理400。为方便起见,处理400将被描述为由例如图3的系统300的系统执行。

[0049] 系统首先接收用以将数据项存储在区块链网络中的请求(402)。例如,用户可以提交银行交易数据以存储在区块链网络中。由于数据以去中心化的方式存储、并且区块链网络中没有单个节点存储整个数据,所以使用本文描述的技术存储数据可以提高区块链网络的安全性。

[0050] 响应于该请求,系统接收数据项并将数据项划分为多个数据块(404)。例如,系统可以使用程序将数据划分为相等大小的块,或者将数据划分为用户指定数量的块。在一些情况下,系统可以记录数据的分块方法,并将分块方法与各个数据块一起存储、或者将分块方法存储在区块链的一个条目中。

[0051] 系统接下来将每个数据块分配给区块链网络中的不同节点,并将与每个数据块相关联的信息存储在区块链中(406)。不同的节点不共享分配的数据并将该分配的数据存储在私有维护的分布式哈希表(DHT)中。例如,分布式哈希表可以存储数据块的文件路径、节点的标识、数据块的值或数据块的值的哈希值。然后,系统将与每个数据块相关联的信息存储在区块链中(408)。例如,系统可在区块链上公布每个数据块的文件路径。因此,数据块的位置对于与区块链交互的任何程序都是公开的。系统可以以随机方式选择存储节点,以确保没有单个节点可以访问所有数据块。在一些实施方式中,系统可以选择存储节点,使得没有节点存储超过一定数量的数据块。结果数据项以去中心化的方式存储,并由于没有存储节点拥有对所有数据块的完全访问权,因此保持了安全性。仅当可信服务请求和接收数据块时,才会恢复数据项。

[0052] 然后,系统接收用以检索已存储的数据项的请求(410)。例如,第三方服务可以请求查看用户的银行交易以确定用户的信誉。该服务可以使用系统支持的应用程序编程接口(API)将请求提交给系统。例如,请求可以是JSON文件格式。此时,数据被块并分散在区块链网络中。

[0053] 为了返回已被分块并存储在区块链网络中的不同节点上的所请求的数据,系统使用应用程序和公布的文件路径从区块链网络中的分配的节点检索每个已存储的数据块(412)。例如,应用程序可以是已被授权访问每个节点的分布式哈希表的智能合约。应用程序可以执行指定的指令以根据数据块重建数据。在一些情况下,首次分块数据时,指令被写入区块链中。然后,系统根据已存储的数据块重建存储的数据项。例如,系统可以拼接多个

数据块,或者添加数据值,例如通过返回数据值的哈希值(414)。在另一示例中,当每个数据块包括来自数据项的非连续数据位时,系统可以交错数据块以重建已存储的数据项。在一些情况下,系统还会在区块链中记录服务的数据请求。该信息可用于基于数据块的大小和存储的长度来补偿存储节点。

[0054] 作为最后一步,系统发送对用以检索已存储的数据项的请求的响应,其中,该响应包括重建的数据项(416)。例如,系统可以将该响应发送到应用程序308。在一些实施方式中,系统在发送响应之前审核数据块和重建的数据项。例如,系统可以通过检查哈希值来审核数据项或各个数据块。

[0055] 所描述的特征可以在数字电子电路,或者在计算机硬件、固件、软件,或在它们的组合中实施。该装置可以在有形体现的信息载体中(例如,在机器可读存储设备中)的计算机程序产品中实施,以由可编程处理器执行;以及可以由执行指令程序的可编程处理器执行的方法步骤,以通过对输入数据进行运算并生成输出来执行所描述的实施方式的功能。所描述的特征可在一个或多个计算机程序中方便地实施,所述一个或多个计算机程序在可编程系统上执行,所述可编程系统包括至少一个可编程处理器,所述至少一个可编程处理器连接至数据存储系统、至少一个输入设备和至少一个输出设备以收发数据和指令。计算机程序是可以在计算机中直接或间接地使用的指令组,用以执行特定活动或带来特定结果。计算机程序可以用任何形式的编程语言编写,包括编译或演绎性语言,并且可以任何形式部署,包括部署为独立程序或部署为模块、组件、子程序或部署为在计算环境中适合使用的另一单元。

[0056] 用于执行指令程序的合适处理器包括,例如,通用和专用微处理器,以及任何类型的计算机的专有处理器或多个处理器之一。通常,处理器从只读存储器和/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处理器和用于存储指令和数据的一个或多个存储器。通常,计算机还可以包括一个或多个用于存储数据文件的大容量存储设备,或可操作地与一个或多个用于存储数据文件的大容量存储设备连接;这些设备包括磁盘,例如内部硬盘和可移动磁盘;磁光盘;和光盘。适合于有形地体现计算机程序指令和数据的存储设备包括所有形式的非易失性存储器,包括例如半导体存储设备,例如EPROM、EEPROM和闪存设备;磁盘,如内部硬盘和可移动磁盘;磁光盘;和CD-ROM和DVD-ROM磁盘。处理器和存储器可以由专用集成电路(ASIC)补充或并入专用集成电路中。

[0057] 为了提供与用户的交互,这些特征可以在具有显示设备以及键盘和指示设备的计算机上实施,诸如阴极射线管(CRT)或液晶显示器(LCD)监视器之类的显示设备用于向用户显示信息,用户可以通过例如鼠标或轨迹球的指示设备以及键盘向计算机提供输入。

[0058] 这些特征可以在计算机系统中实施,计算机系统包括后端组件、例如数据服务器,或者包括中间件组件、例如应用服务器或因特网服务器,或者包括前端组件、例如具有图形用户界面或因特网浏览器的客户端计算机,或者它们的任意组合。系统的组件可以通过任何形式连接,或通过数字数据通信的媒介连接,例如通信网络。通信网络的示例包括如局域网(LAN)、广域网(WAN)以及形成因特网的计算机和网络。

[0059] 计算机系统可以包括客户端和服务器。客户端和服务器通常彼此远离并且通常通过网络进行交互,例如所描述的网络。客户端和服务器的关系借助于在各个计算机上运行并且彼此具有客户端-服务器关系的计算机程序而产生。

[0060] 另外,附图中描绘的逻辑流程不需要所示的特定次序或先后次序来实现期望的结果。另外,可以为所描述的流程中提供其他步骤,或者可以从所描述的流程中删除步骤,并且可以将其他组件添加到所描述的系统或从所描述的系统移除。因此,其他实施方式在以下权利要求的范围内。

[0061] 已经描述了本文的多个实施方式。然而,应该理解,在不脱离本文的精神和范围的情况下,可以进行各种修改。因此,其他实施方式在以下权利要求的范围内。

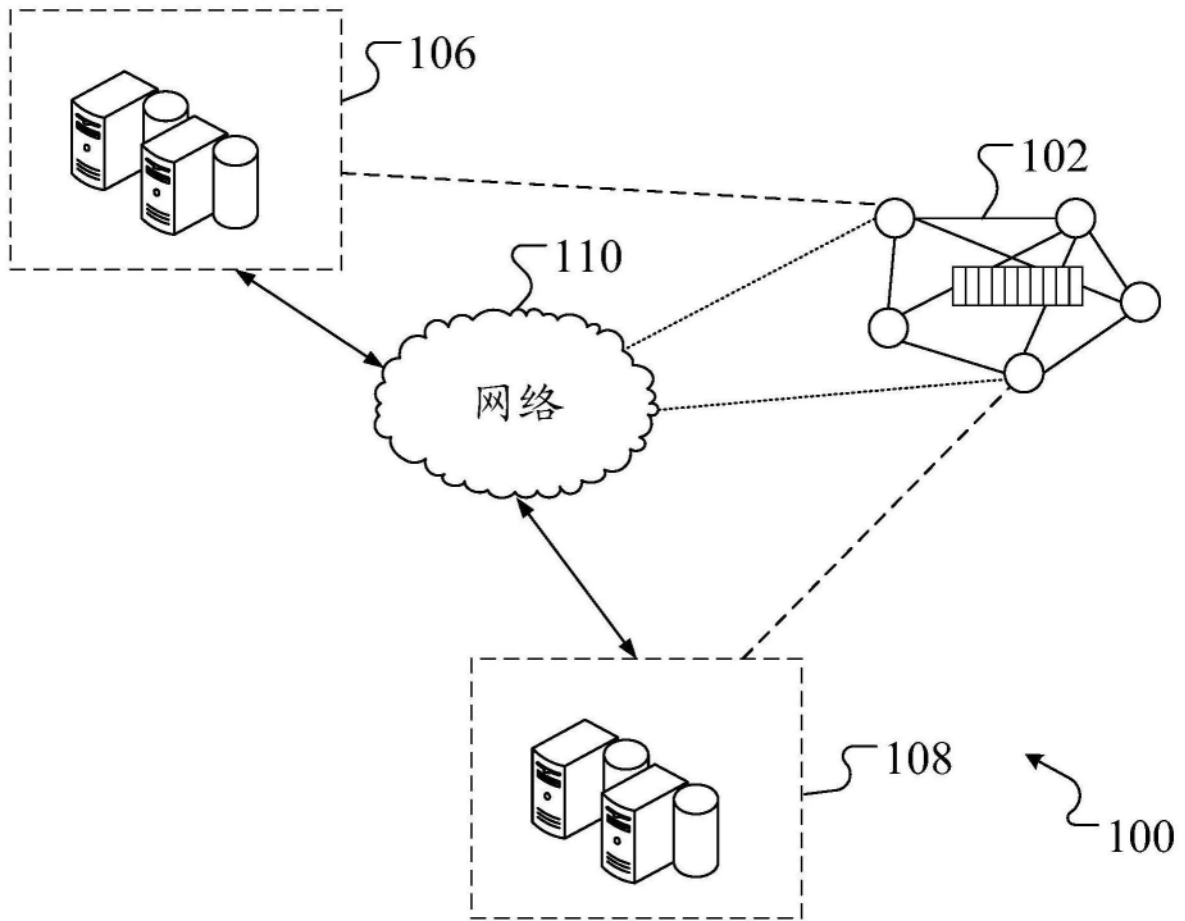


图1

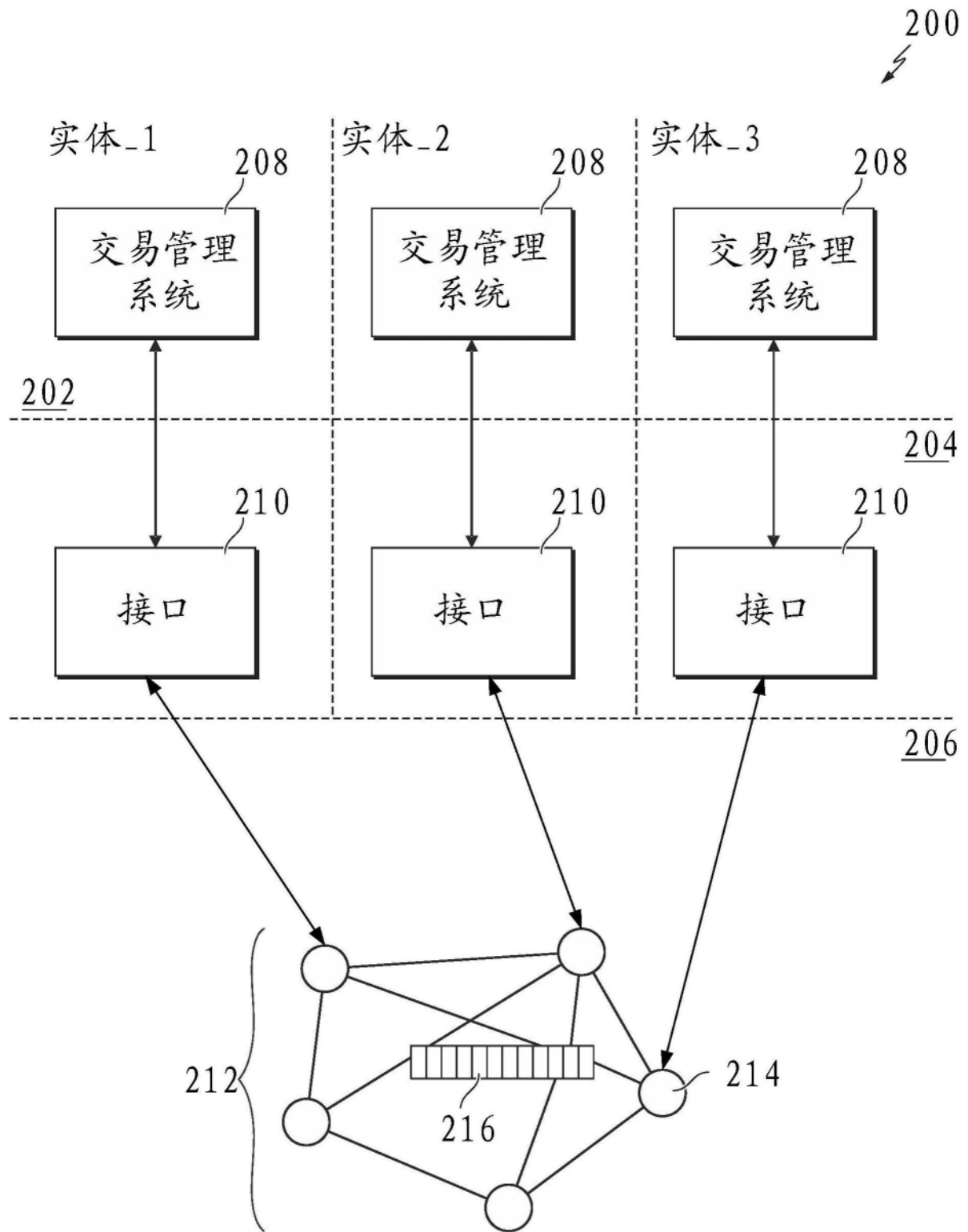


图2

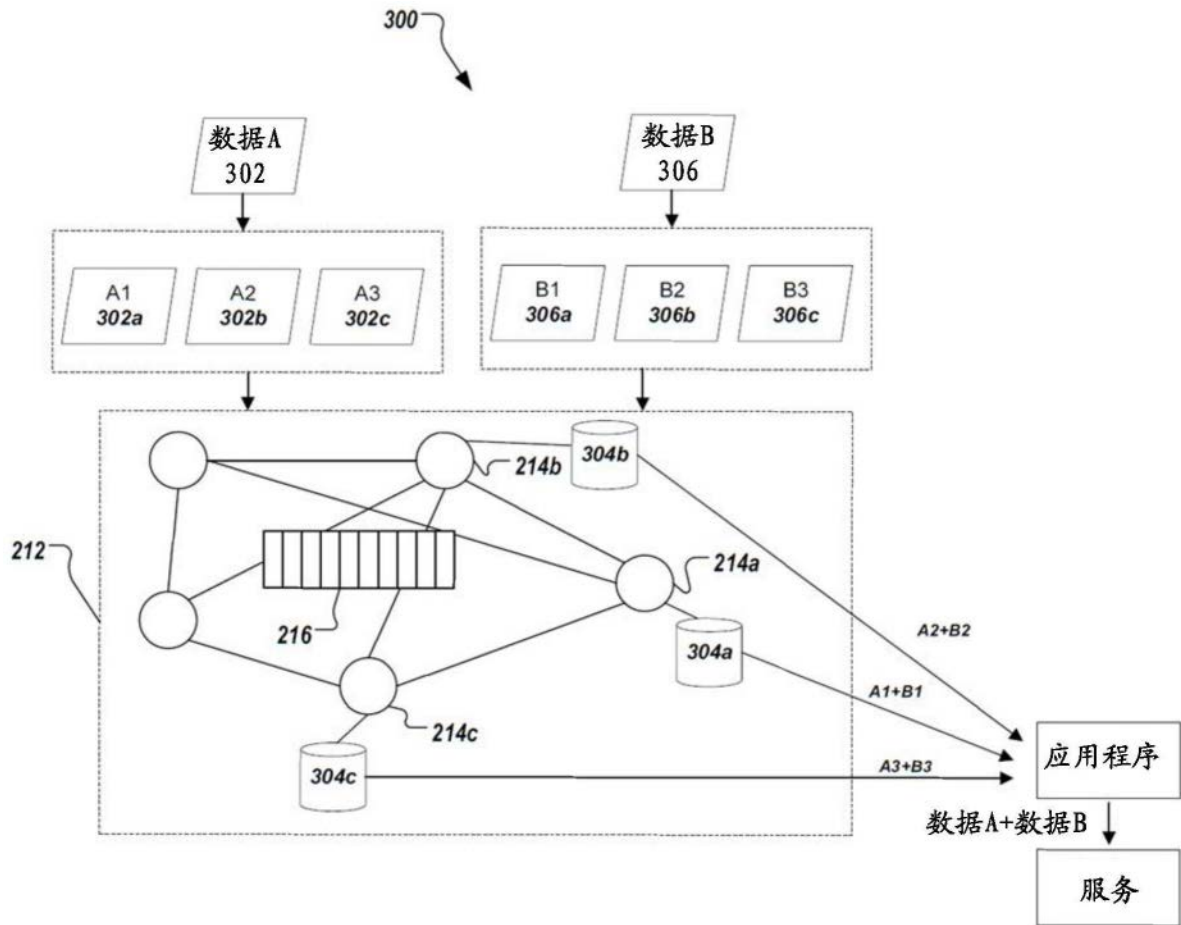


图3

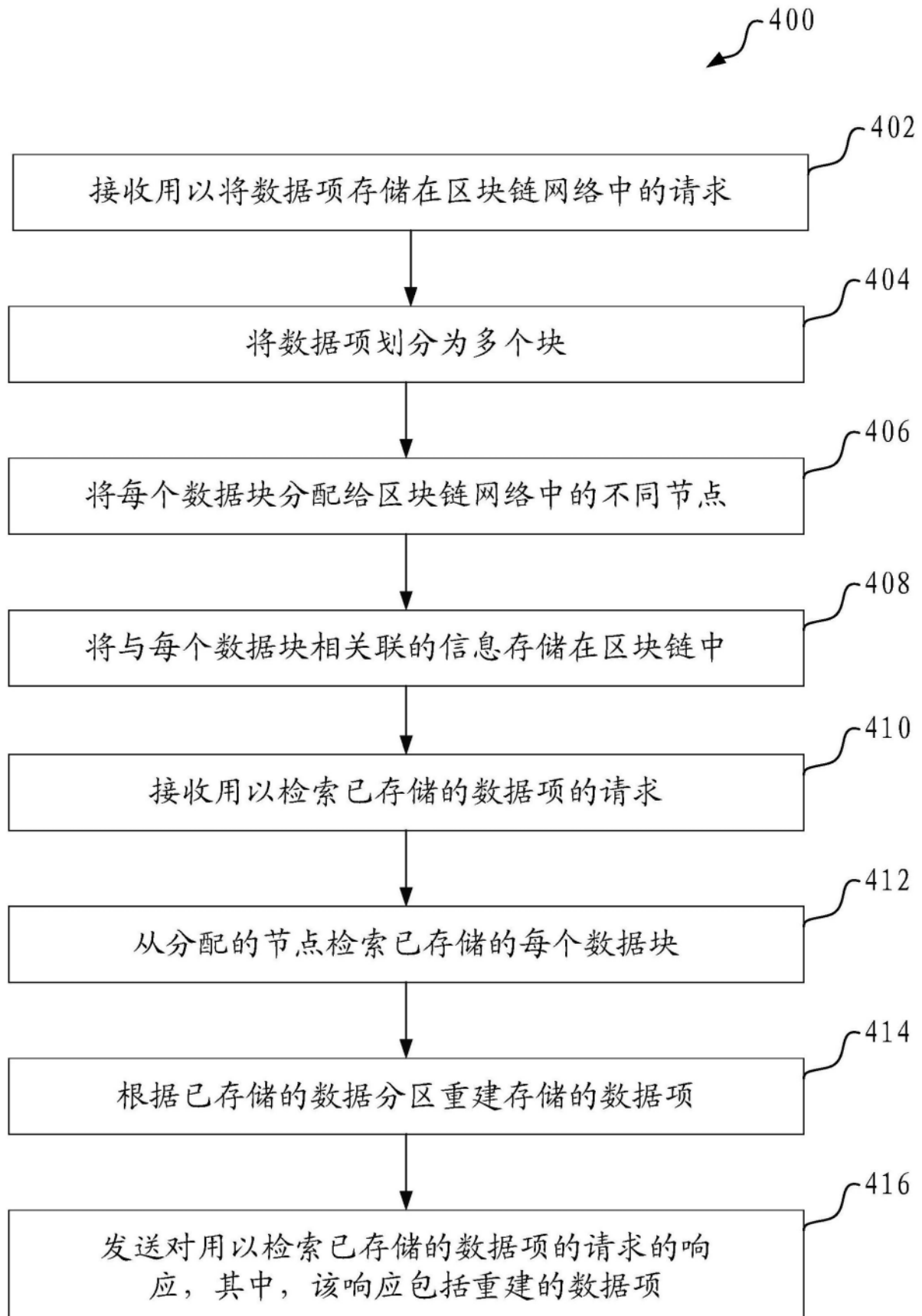


图4