(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110612697 B
(45)授权公告日 2023.11.07

(21)申请号 201780090574.4
(22)申请日 2017.05.09
(65)同一申请的已公布的文献号
申请公布号 CN 110612697 A
(43)申请公布日 2019.12.24
(85)PCT国际申请进入国家阶段日
2019.11.08
(86)PCT国际申请的申请数据
PCT/CN2017/083597 2017.05.09
(87)PCT国际申请的公布数据
WO2018/205137 EN 2018.11.15
(73)专利权人 埃森哲环球解决方案有限公司
地址 爱尔兰都柏林
(72)发明人 马国 孙冠毅 谢斌
(74)专利代理机构 北京市金杜律师事务所 11256
专利代理师 马明月
(51)Int.Cl.
H04L 9/06(2006.01)
(56)对比文件
CN 1243596 A,2000.02.02
US 2017013047 A1,2017.01.12
CN 101490687 A,2009.07.22
朱扬勇;熊赟.大数据的若干基础研究方向.大数据.2017,(02),全文.
审查员 李晓琳

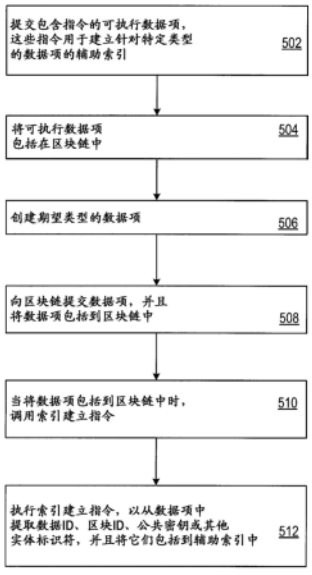
权利要求书3页 说明书10页 附图9页

(54)发明名称

用于高效信息检索的数据存储层索引的方法和系统

(57)摘要

一种安全数据系统促进广泛数据存储层(例如区块链)的高效搜索。系统可以创建针对在区块链中记录的预定义类型的数据元素的索引。系统可以通过调用在可执行数据元素(例如智能合约)中存储的可执行指令来生成索引,该可执行数据元素被记录在区块链中,并且与预定义类型的数据元素相关联。索引促进在区块链中对预定义类型的数据元素的快速查询。



CN 110612697 B

1.一种电子系统,包括:

存储器,所述存储器被配置为存储:

数据存储层,所述数据存储层包括包含数据元素的链接数据区块;以及

索引结构,所述索引结构包括针对所述链接数据区块中的预定义类型的数据元素的索引条目;以及

注入电路装置,所述注入电路装置与所述存储器通信,所述注入电路装置被配置为通过以下方式响应包括新数据元素的新数据区块到所述数据存储层中的所述链接数据区块的链接:

确定所述新数据元素具有所述预定义类型;

生成针对所述新数据元素的索引条目,所述索引条目包括针对所述新数据元素的、所述数据存储层内的位置参考;以及

将所述索引条目插入到所述索引结构中。

2.根据权利要求1所述的系统,其中所述数据存储层存在于区块链系统节点内,并且所述链接数据区块构成区块链的副本。

3.根据权利要求1所述的系统,其中所述数据元素包括包含指令的可执行数据元素,所述指令用于生成所述索引条目并将所述索引条目插入到所述索引结构中。

4.根据权利要求3所述的系统,其中所述注入电路装置被配置为从所述新数据元素调用所述可执行数据元素中的所述指令,以在所述新数据元素与所述数据存储层中的所述链接数据区块链接之后,生成所述索引条目并将所述索引条目插入到所述索引结构中。

5.根据权利要求3所述的系统,其中,

所述注入电路装置还被配置为生成针对所述新数据元素的索引控制数据元素,并且将所述索引控制数据元素链接到所述数据存储层中的所述链接数据区块;并且

所述注入电路装置被配置为在所述新数据元素和所述索引控制数据元素与所述数据存储层中的所述数据区块链接之后,从所述索引控制数据元素调用所述可执行数据元素中的所述指令。

6.根据权利要求1所述的系统,其中所述索引条目还包括描述所述预定义类型的所述新数据元素的数据特性。

7.根据权利要求6所述的系统,其中所述位置参考包括数据区块标识符、数据元素标识符或两者。

8.根据权利要求1所述的系统,其中所述索引结构被存储在所述数据存储层中的所述链接数据区块外部。

9.根据权利要求1所述的系统,还包括查询电路装置,所述查询电路装置被配置为:

接收对所述预定义类型的数据元素中的所述新数据元素的查询;

标识与所述预定义类型的所述数据元素相关联的所述索引结构;

从所述索引结构检索所述索引条目;以及

响应于所述查询,返回从所述索引条目获得的所述位置参考。

10.根据权利要求9所述的系统,其中所述位置参考包括针对所述预定义类型的所述数据元素的、所述数据存储层内的所述位置参考。

11.根据权利要求9所述的系统,其中所述数据元素包括包含指令的可执行数据元素,

所述指令用于标识所述索引结构并检索所述索引条目。

12.根据权利要求11所述的系统，其中所述查询被嵌入查询数据元素中，并且所述查询电路装置还被配置为在所述查询数据元素与所述链接数据区块链接之后，从所述查询数据元素调用所述可执行数据元素中的所述指令。

13.一种计算机实现的方法，包括：

接收包含指令的可执行数据元素，所述指令用于生成针对预定义类型的数据元素的索引条目，并且将所生成的所述索引条目插入到针对所述预定义类型的索引结构中；

链接所述可执行数据元素与数据存储层中的链接数据区块；

接收所述预定义类型的新数据元素；

链接所述新数据元素与所述存储层中的所述链接数据区块；以及

调用与所述链接数据区块链接的所述可执行数据元素中的所述指令，以在所述新数据元素与所述链接数据区块的所述链接之后，生成针对所述新数据元素的索引条目并将所述索引条目插入到所述索引结构中，

其中所述索引条目包括针对所述新数据元素的、所述数据存储层内的位置参考。

14.根据权利要求13所述的方法，其中所述可执行数据元素中的所述指令从所述新数据元素被调用。

15.根据权利要求13所述的方法，还包括：

生成针对所述新数据元素的索引控制数据元素；以及

链接所述索引控制数据元素与所述存储层中的所述链接数据区块，并且其中所述可执行数据元素中的所述指令从所述索引控制数据元素被调用。

16.根据权利要求13所述的方法，其中所述索引结构被存储在所述数据存储层中的所述链接数据区块外部。

17.根据权利要求13所述的方法，还包括：

接收对所述预定义类型的数据元素中的所述新数据元素的查询；

标识与所述预定义类型相关联的所述索引结构；

从所述索引结构检索所述索引条目；以及

响应于所述查询，返回从所述索引条目获得的所述位置参考。

18.根据权利要求17所述的方法，其中所述可执行数据元素中的所述指令还包括用于所述索引结构的所述标识和所述索引条目的所述检索的指令。

19.根据权利要求18所述的方法，其中所述查询被嵌入查询数据元素中，所述方法还包括：

链接所述查询数据元素与所述存储层中的所述链接数据区块；以及

调用所述可执行数据元素中的所述指令，所述指令用于在所述查询数据元素与所述存储层中的所述链接数据区块链接之后，标识所述索引结构并从所述查询数据元素检索所述索引条目。

20.一种电子系统，包括：

存储器，所述存储器被配置为存储：

数据存储层，所述数据存储层包括包含数据元素的链接数据区块；以及

索引结构，所述索引结构包括用于所述链接数据区块中的预定义类型的数据元素的索

引条目;以及

注入电路装置,所述注入电路装置与所述存储器通信,所述注入电路被配置为:

链接包含用于生成索引条目的指令的可执行数据元素,并且将针对所述预定义类型的数据元素的所述索引条目插入所述数据存储层中的所述链接数据区块中;

接收新数据元素;

确定所述新数据元素具有所述预定义类型;

生成针对所述预定义类型的所述新数据元素的索引控制数据元素;

链接所述新数据元素与所述数据存储层中的所述链接数据区块;

链接所述索引控制数据元素与所述数据存储层中的所述链接数据区块;以及

通过在所述新数据元素和所述索引控制数据元素与所述数据存储层中的所述链接数据区块链接之后从所述索引控制数据元素调用所述可执行数据元素中的所述指令,来生成针对所述新数据元素的索引条目并将所述索引条目插入到所述索引结构中,

其中所述索引条目包括针对所述新数据元素的、所述数据存储层内的位置参考。

用于高效信息检索的数据存储层索引的方法和系统

技术领域

[0001] 本公开涉及安全数据系统，并且涉及在安全数据存储层(诸如区块链)中更高效地定位数据元素。

背景技术

[0002] 受巨大的客户需求推动，电子和通信技术的飞速发展已经导致安全数据系统被广泛采用，这些系统采用密码安全数据存储层，例如区块链。在许多实际应用中，区块链促进信息共享。在广泛的数据存储层中定位并检索数据的效率的提高将有助于推动这种安全数据系统的进一步采用。

附图说明

[0003] 图1图示了示例安全分散的数据处理和存储系统。

[0004] 图2示出了图1的安全数据处理和存储节点的示例。

[0005] 图3图示了存储在图1的节点中的区块链。

[0006] 图4示出了用于区块链中的数据元素的辅助索引系统。

[0007] 图5示出了用于创建并更新辅助索引的逻辑流程。

[0008] 图6示出了用于创建并更新辅助索引的另一逻辑流程。

[0009] 图7示出了用于创建并更新辅助索引的时间线。

[0010] 图8图示了用于在辅助索引和区块链中查询数据元素的逻辑流程。

[0011] 图9示出了用于在辅助索引和区块链中查询数据元素的另一逻辑流程。

具体实施方式

[0012] 传统上，描述实体之间关系的数据元素，诸如与货币或服务交换有关的数据，由诸如银行的第三方维持并处理。因此，数据元素的完整性依赖于第三方的可信赖性以及如何保护这些数据元素在例如第三方控制的服务器中免遭篡改。最近已经开发了各种数据存储层(例如区块链系统)，以在一大组非信任节点之间分散(decentralize)这些数据元素的处理和存储。以下描述将区块链参考作为示例实现上下文，但技术解决方案适用于其他数据存储层。

[0013] 区块链系统消除了对信任的第三方的需要。在区块链系统中，数据元素被存储为数据区块的链(即区块链)的形式的可公开访问的数据单元，这些数据单元具有被分发到各种区块链节点的多个副本。区块链系统中的数据完整性是使用数字签名、共识机制和其他防数据篡改算法来实现的。然而，存储这些数据元素的区块链可以使用不同于例如传统的关系数据库或非关系数据库的原理来组织。与为快速信息检索设计的这些传统数据库不同，直接向区块链查询信息可能是涉及遍历整个数据区块的链的低效且耗时的过程。在本公开中，与区块链系统集成的辅助索引提供了一种用于从包括区块链的数据存储层进行快速信息搜索和检索的技术解决方案。

[0014] 图1图示了用于安全和分散的数据处理和存储的示例系统100，诸如区块链平台。系统100包括经由通信网络120彼此通信的分散节点102、104、106、108和110。通信网络120可以基于例如互联网协议(IP)，并且可以包括有线或无线接入网、局域网、广域网和其他计算机网络的组合。

[0015] 系统100的每个节点可以是用于例如存储、维持、更新、处理和查询受保护数据的软件和硬件的组合(以下称为区块链)。每个节点可以基于单个计算机、一组集中式或分布式计算机或者由云计算服务提供者托管的单个或一组虚拟机。

[0016] 作为示例，在图2中，安全数据处理和存储系统100的节点，诸如节点102，被示出为包括一组计算机201，诸如计算机203、205和207。计算机201可以包括通信接口202、系统电路装置204、输入/输出(I/O)接口206、存储装置209和显示电路装置208，该显示电路装置在本地或对于远程显示(例如在本地或远程机器上运行的web浏览器中)生成机器界面210。机器界面210和I/O接口206可以包括GUI、触敏显示器、语音或面部识别输入、按钮、开关、扬声器和其他用户界面元件。I/O接口206的附加示例包括麦克风、视频和静止图像照相机、耳机和麦克风输入/输出插孔、通用串行总线(USB)连接器、存储卡插槽和其他类型的输入。I/O接口206可以进一步包括磁性或光学介质接口(例如CDROM或DVD驱动器)、串行和并行总线接口以及键盘和鼠标接口。

[0017] 通信接口202可以包括无线发送器和接收器(“收发器”)212以及收发器212的发送和接收电路装置所使用的任何天线214。收发器212和天线214可以例如在IEEE 802.11的任何版本(例如802.11n或802.11ac)下支持Wi-Fi网络通信。通信接口202还可以包括有线收发器216。有线收发器216可以为大范围的通信协议中的任何通信协议提供物理层接口，大范围的通信协议诸如任何类型的以太网、电缆数据服务接口规范(DOCSIS)、数字订户线路(DSL)、同步光学网络(SONET)或其他协议。节点102的计算机201经由通信接口202和通信网络120与区块链系统100的其他节点通信。

[0018] 存储器209可以用于本地存储节点102的区块链的副本。存储装置209可以进一步用于存储区块链的辅助索引。备选地，计算机201可以经由通信接口202和通信网络120与用于存储区块链的副本的网络存储装置230通信。网络存储器230可以是集中式或分布式的。例如，网络存储装置230可以由云计算服务提供者远程托管。

[0019] 系统电路装置204可以包括硬件、软件、固件或任何组合的其他电路装置。系统电路装置204可以例如用一个或多个片上系统(SoC)、专用集成电路(ASIC)、微处理器、分立模拟和数字电路和其他电路装置来实现。系统电路装置204可以包括注入电路装置，该注入电路装置与区块链和系统100的其他部分交互，用于实现与区块链的维持、存储、处理、验证、索引以及其他方面有关的任何期望功能性。仅作为一个示例，系统电路装置204可以包括一个或多个指令处理器218和存储器220。存储器220存储例如控制指令224和操作系统222。在一种实现中，处理器218执行控制指令224和操作系统222，以实施与区块链有关的任何期望功能性。区块链的控制指令224可以被实现为具有多层的软件堆栈。

[0020] 返回图1，实体142、144、146、148和150可以经由图1的区块链节点参与区块链系统100。在一种实现中，区块链系统100的每个节点可以支持一个参与实体。在另一实现中，每个节点可以支持多个参与实体或参与实体的多个用户。为了成为系统100的节点，可以在该节点处的计算机上安装区块链软件堆栈。在软件堆栈的顶部，应用层可以提供由软件堆栈

的较低层支持的各种区块链功能。这些功能可以包括例如加密数据元素、提交用于插入到区块链中的数据元素、验证要提交的数据元素、经由共识机制在区块链中创建新数据区块、存储区块链的本地副本以及其他功能。

[0021] 如图1所示，区块链系统100的配置和功能可以由区块链协议130支配。区块链协议130可以定义参与实体如何加密数据元素。区块链协议130可以进一步指定被加密数据元素的格式，使得被加密数据元素可以被参与实体和区块链系统中的节点解密并理解。区块链协议130可以附加地指定上述功能的类型以及应该如何实施这些功能。区块链协议130可以附加地指定参与实体和节点的可能角色。例如，区块链节点可以作为能够执行所有区块链功能的全功能节点参与。备选地，区块链节点可以仅参与执行区块链功能的子集之一。区块功能的每个子集可以包含来自可用区块链功能的多个区块链功能。区块链功能的可能子集可以在区块链协议130中被指定。参与实体可以选择子集之一，并且安装用于执行在所选子集中包括的功能的对应软件堆栈。在另一实现中，区块链协议130可以允许参与实体选择功能的任何组合并相应地配置其节点，而不是遵循区块链协议130的规定子集之一。

[0022] 图3示出了在区块链系统100的节点中存储的区块链300的示例副本，该节点具有存储区块链的本地副本的功能。如图3所示，区块链的副本可以包括一系列链接的数据区块302、304、306、308和310，每个数据区块由区块ID(B0、B1、B2和Bn)唯一标识。每个数据区块可以包括多个数据元素，诸如区块304的T10、T11和T12，...以及区块310的Tn0、Tn1和Tn2。每个数据元素除了包括数据之外，还可以包括数据ID。区块302可以是充当区块链的头部的特殊数据区块或起源区块，并且可以不包含实际数据元素。数据区块中的数据元素可以包括参与实体希望存储在区块链中的任何类型的数据。例如，数据元素可以是描述实体之间的关系(例如两方之间的货币或服务交易)的类型。作为另一示例，数据元素可以包括计算机指令，这些计算机指令用于自动执行嵌入在计算机指令中以及实体之间的协定或合约的规定。在区块链中存储的这种类型的数据元素可以被称为可执行数据元素或智能合约。如下面更详细地描述的，可执行数据元素中的计算机指令的一个或多个段的执行可以由区块链中的其他数据元素来调用和从其他数据元素调用。

[0023] 可以使用各种密码技术来实现每个数据区块中数据元素的真实性。例如，可以使用基于公钥和私钥密码术的数字签名来确保要插入到区块链中的数据元素确实来自其宣告的提交实体。特别地，参与区块链系统并且希望将数据元素存储在区块链中的每个实体可以拥有私钥，该私钥始终保持秘密。公钥可以源自私钥，并且可以被使得可公开获得。当实体希望将数据元素存储在区块链中时，实体可以在将数据提交以插入在区块链中之前首先使用私钥对数据元素进行加密。有权访问实体的公钥的任何人都可以解密被加密的数据元素。当使用公钥解密时，对被加密数据的任何篡改都将导致数据无法读取。如此，使用私钥的加密表示实体对数据元素的数字签名，并且容易检测到对被加密数据的任何篡改。

[0024] 区块链300的数据区块302、304、306、308和310被顺序创建并将链接成链。在一个示例实现中且如图3所示，数据区块与其紧邻的前一个数据区块之间的链接可以是哈希值，而不是数据结构中的传统指针。特别地，数据区块可以通过在紧邻的前一区块中包括数据元素的哈希值(在此被称为链接哈希值)，来链接到其紧邻的前一数据区块。例如，在图3中，区块304中的数据元素的哈希值Hash 1可以被包括在紧接在区块304之后的数据区块306中，作为链接哈希值。如此，数据区块306与数据区块304链接。用于计算块中包含的数据元

素的哈希值的算法例如可以基于但不限于SHA256哈希。

[0025] 如图3所示，可以进一步使用签名代码对包含数据元素的区块链系统的每个数据区块进行签名。签名代码可以备选地被称为一次性随机数(nonce)。数据区块的签名代码用于帮助根据区块链协议130检测数据区块的篡改。例如，当签名代码和数据区块中的数据元素的组合的哈希值包含具有预定义哈希模式的哈希部分时，根据区块链协议130可以认为数据区块签名代码是有效的。预定义的哈希模式可以由区块链协议(例如，在哈希值的开始处的预定义数目的前导零)来指定。因此，用于区块的签名代码可以通过解决困难的密码问题来计算。在以上示例实现中，签名代码可以被计算为使得计算出的签名代码和数据元素的组合的哈希值符合签名协议。例如，计算区块304的签名代码1，使得数据区块304的签名代码1、数据元素T10、T11和T12的组合的SHA256哈希与区块签名协议兼容，例如，由预定义数量的零前导。对签名区块中的数据的任何篡改将导致该区块的哈希值与签名协议不兼容。

[0026] 可以通过一次附加一个数据区块来创建区块链300。具体地，可以向区块链系统广播来自区块链系统的各个节点的加密(或数字签名)的数据元素。然后可以将这些加密的数据元素收集到数据区块中，以便存储到区块链中。区块链协议130可以指定共识算法或机制。共识算法可以控制如何验证新数据元素、如何从已验证的新数据元素组装新数据区块以及如何将新块广播到区块链节点、检查它并将其接受到区块链中。

[0027] 在一个示例共识算法中，可以周期性地(例如，每10分钟或者大约是由区块链节点求解区块签名代码所需的时间段)收集从节点提交的数据元素。进一步地，各种节点可以根据由区块链协议130指定的数据元素验证规则(例如，数据元素被数字签名，包含在数据元素中的金融交易由于付款人具有足够的余额而是有效的)来参与验证这些数据元素，以将数据元素组装成区块，计算该区块的签名代码，并且将新区块广播到区块链系统以供接受。在一个实现中，广播可接受区块的第一节点将负责将其区块插入到区块链中。用新区块更新各种节点中的区块链副本。必须求解签名代码的该特定算法(有时被称为“工作量证明”)只是可能的共识算法的一个示例。区块链注释可以使用其他共识算法(例如“权益证明”)来验证并创建新数据区块。备选地，将嵌入其数据区块中的数据元素插入到区块链中被称为使数据元素与区块链链接。

[0028] 区块链系统的功能(例如加密并提交数据元素、共识功能(包括数据元素的验证、签名代码的计算以及新数据区块的组装)以及存储区块链的本地副本)可以由各种节点来执行。参与共识算法的节点例如可以被称为矿工。如前所述，节点在参与区块链系统时，可以决定功能的子集，节点可以通过安装对应的软件堆栈来执行该功能的子集。例如，全功能节点可以执行上面讨论的所有功能。然而，功能受限的节点只可以执行功能的所选集。例如，一些节点仅可以参与加密数据元素并将其提交到区块链中。

[0029] 如上所述，区块链的数据区块中的数据元素可以是参与实体希望存储在区块链中的任何类型的数据，包括特殊类型的可执行数据元素(或智能合约)。区块链协议130(图1的130)可以规定用于从其他数据元素调用可执行数据元素中的全部或部分可执行计算机指令的机制和接口。例如，可执行数据元素可以包括可以独立调用的指令部分。这些可执行数据元素中的每一个可以由ID来标识，并且可执行数据元素内的指令的每个部分可以进一步由部分ID来标识。

[0030] 可执行数据元素的全部或部分的执行可以以各种方式和在各种定时下被调用。在一个示例实现中，区块链协议130可以提供一种机制，该机制用于在另一数据元素被插入到新数据区块中并且该新数据区块被验证并由节点之一将其附加到区块链时，从该另一数据元素调用可执行数据元素中的指令的部分的执行。可以根据区块链协议130在调用数据元素中提供调用接口，用于指定例如可执行数据元素的ID、要执行的可执行数据元素内的指令的特定部分的ID以及传递给可执行指令的参数。

[0031] 上面在图1至图3中描述的区块链系统可以用于各种应用中。例如，多个参与实体可以使用区块链系统来共享存储在区块链中的专有信息。例如，合作的半导体电路制造者可以使用区块链系统来共享设计和布局。再如，两家合作医院可以使用区块链系统来共享患者活动和其他信息。医院可以将信息分类为例如不同类型的患者活动，例如患者活动和与不同部门(内科、心内科、支付部门等)的交互。各单独的活动数据可以是专有的，并且由医院根据合作医院之间商定的格式和加密公式进行编码，并且用作数据元素中的数据有效负载。然后可以使用适当的公钥对该数据元素进行进一步加密并将其存储在区块链中。如此，这种数据元素中的专有信息仅可在合作医院之间共享，而不能与区块链中的其他一般参与实体共享。具体地，虽然其他参与实体可以使用公钥来解密区块链中的数据元素以获得封装的数据有效负载，但是这种数据有效负载是专有的，并且只能由合作医院进一步解密。

[0032] 在以上区块链中的信息共享和许多其他区块链应用的上下文中，参与实体可能期望在区块链中查询信息。例如，合作医院之一可能需要搜索另一医院特定部门中的患者活动。对于典型的区块链系统，如果包含特定数据元素的数据区块的数据ID和/或区块ID已知并用作查询密钥，则通常直接从区块链获取特定数据元素。然后可以使用适当的公钥对返回的数据元素进行解密，并且如果数据有效负载是专有的，则可以由查询实体对其进行进一步解密。

[0033] 然而，在一些应用中，要查询的数据元素的数据ID和/或区块ID可能未知。例如，在上面讨论的两家合作医院之间的信息共享应用中，第一医院可能期望找出特定患者到第二医院特定部门的就诊。第一医院可以用于查询区块链的密钥可以是医院特定部门的身份以及特定患者的姓名或公钥。因为与这些患者就诊相关联的数据元素的区块ID和数据ID是未知的，所以可能需要从头到尾遍历区块链，以用于解密并标识存储在区块链中的这些期望数据元素。因为区块链可能变得过大，所以区块链中的这种查询过程可能耗时且低效。

[0034] 在一些其他实现中，随着数据区块以诸如关系数据库的分离数据库的形式被附加到区块链，可以提取并跟踪关于区块链中的数据元素的整个集合的信息，该分离数据库可以使用传统的数据库查询过程来更高效地查询。然而，这种方法要求区块链节点中的附加存储空间，以用于维持并同步分离数据库。这种数据库复制区块链中已经包含的信息，并且通常会消耗大存储空间。

[0035] 在根据本公开的一个示例实现中，为了从区块链高效检索信息，一个实体或合作实体可以创建并更新区块链中的数据元素的子集的辅助索引。数据元素的子集可以包括实体或合作实体感兴趣的数据元素。例如，辅助索引可以由两家合作医院来建立，这两家医院希望共享与这些合作医院中的患者活动有关的数据元素的信息。每个辅助索引可以对应于特定类型的患者活动。辅助索引可以经由执行由合作医院提交到区块链中的可执行数据元

素中的指令来创建并更新。当将特定类型的数据元素的每个子集插入到区块链中时，可以调用用于创建并更新辅助索引的可执行数据元素的执行。进一步地，辅助索引可以被维持在与区块链分离的数据库中。两家医院可以访问辅助索引，以促进从区块链检索与数据元素子集有关的信息，而不必遍历整个区块链。

[0036] 图4更详细地图示了用于区块链中的信息查询的这种辅助索引的示例实现400。具体地，可执行数据元素402可以在根据区块链协议130提交数据元素的正常过程之后被插入到区块链中。例如，这些可执行数据元素可以由希望共享信息的实体同意。这些可执行数据元素可以被执行为建立、维持、更新并查询辅助索引422，以用于促进实体检索信息。每个可执行数据元素可以对应于一个辅助索引(例如404→424、406→426、408→428、410→430)。备选地，可执行数据元素可以包含指令的多个部分，并且指令的每个部分可以对应于辅助索引422之一。

[0037] 每个可执行数据元素和对应的辅助索引可以与区块链中一种特定类型的数据元素相关。因此，辅助索引422可以各自被标识为与数据元素的类型相关联。例如，在两家合作医院之间的信息共享应用的上下文中，辅助索引424可以对应于医院的心内科的所有患者活动，而索引426可以与医院的外科的所有患者活动相关，并且索引428可以对应于患者向医院进行的支付。

[0038] 在一个实现中，每个辅助索引，诸如辅助索引426，可以包括用于如440所示的对应类型的数据元素所涉及的实体的公钥。进一步地，每个索引可以包括对应类型的数据元素的区块ID和/或数据ID。在两个合作医院之间的信息共享应用的上下文中，辅助索引426例如可以包括多个条目。每个条目可以对应于与例如医院的外科中的患者活动有关的数据元素。每个条目可以包括患者的公钥或其他标识符以及数据元素的区块ID(例如b11-b1N)和数据ID(例如t11-t1N)，如图5的440、450和460所示。

[0039] 图5图示了用于创建针对特定类型的数据元素的辅助索引的逻辑流程。实体可以首先向区块链提交可执行数据元素，该可执行数据元素包含用于建立针对特定类型的数据元素的辅助索引的指令(502)。然后，可以经由共识过程由矿工节点将可执行数据元素包括到区块链中(504)。一旦可执行数据元素在区块链中到位，就可以建立针对特定类型的数据元素的辅助索引。具体地，可以创建特定类型的数据元素(506)。然后，可以经由共识过程由矿工节点将特定类型的数据元素提交给区块链并将其包括到区块链中(508)。在将特定类型的数据元素包括在区块链中时，可以调用并自动执行可执行数据元素中用于建立针对特定类型的数据元素的辅助索引的指令(510)。该调用可以通过以下方式来执行：在特定类型的数据元素中包括代码接口，以用于在将特定类型的数据元素提交到区块链时自动调用可执行数据元素中的指令。该代码接口可以由区块链协议130指定。备选地，可执行数据元素中用于建立辅助索引的指令的调用可以在节点的应用层中进行。通过执行辅助索引建立指令，可以从特定类型的数据元素提取数据ID、区块ID、公钥或其他实体标识符等，并且将其包括在特定类型的数据元素的辅助索引中(512)。

[0040] 图6图示了用于创建针对特定类型的数据元素的辅助索引的另一备选逻辑流程。再次，实体可以首先向区块链提交可执行数据元素，该可执行数据元素包含用于建立针对特定类型的数据元素的辅助索引的指令(602)。然后，可以经由共识过程由矿工节点将可执行数据元素包括到区块链中(604)。一旦可执行数据元素到位，就可以建立针对特定类型的

数据元素的辅助索引。具体地，可以创建特定类型的数据元素(606)，并且经由共识过程由矿工节点将特定类型的数据元素包括到区块链中(608)。在将数据元素包括到区块链中时，可以创建具有用于在可执行数据时间内调用索引建立指令的接口的对应索引数据元素(备选地称为索引控制数据元素)(610)。索引数据元素的创建可以由嵌入在数据元素中的代码接口自动发起。备选地，在检测到已经将特定类型的对应数据元素提交到区块链中之后，区块链节点中的应用层可以创建索引数据元素。该索引数据元素就像常规数据元素一样，但包含用于调用可执行数据元素中的指令的接口，这些指令用于建立针对特定类型的数据元素的辅助索引。然后，经由共识过程由矿工节点将索引数据元素包括到区块链中(612)。在将索引数据元素包括在区块链中时，可以调用并自动执行可执行数据元素中用于建立针对特定类型的数据元素的辅助索引的指令(614)。通过执行辅助索引建立指令，可以从特定类型的数据元素提取数据ID、区块ID、公钥或其他实体标识符等，并且将其包括在特定类型的数据元素的辅助索引中(616)。

[0041] 图7示出了用于创建特定类型的数据元素的辅助索引的示例时间线。具体地，图7示出了具有三个时间标记t1、t2和t3的时间线701，其中，t1＜t2＜t3。在时间t1之前，诸如两家合作医院H1和H2的实体已经创建了用于建立针对特定类型的数据元素的辅助索引的各种可执行数据元素。这些可执行数据元素可以被包括在例如区块702中。在图7中，在区块702中包括两个分离的可执行数据元素710和711，以用于分别建立针对医院的心内科和外科的患者就诊的辅助索引。备选地，两个可执行数据元素可以驻留在不同的数据区块中。备选地，两个分离的可执行数据元素可以被实现为单个可执行数据元素，其包含两个可标识的指令部分，一个部分用于建立针对医院的心内科的患者就诊的辅助索引，而另一部分用于建立针对医院的外科的患者就诊的辅助索引。

[0042] 在时间t1时，经由共识过程由矿工节点对数据区块704进行验证，并将其接受到区块链中。在各种数据元素中，数据区块704包含描述第一患者P1对H1的心内科的就诊的数据元素712。数据元素712可以直接调用在区块702中的对应可执行数据元素710中的指令，以在心内科辅助索引720中创建条目722。备选地，数据元素712可以创建索引数据元素713，该索引数据元素713调用可执行数据元素710中的指令，以在心内科辅助索引720中创建条目722。因此，在时间t1之后，心内科辅助索引720包含一个条目，并且外科索引730为空。数据元素712和索引数据元素713不需要在同一数据区块中。例如，索引数据元素713可以在后面的数据区块中，例如紧接在保持数据元素712的数据区块之后的数据区块。

[0043] 在时间t2时，经由共识过程由矿工节点对数据区块706进行验证，并将其接受到区块链中。在各种数据元素中，数据区块706包含描述第二患者P2对H2的外科的就诊的数据元素714。再次，数据元素714可以直接调用在区块702中的对应可执行数据元素711中的指令，以在外科辅助索引730中创建条目724。备选地，数据元素714可以创建索引数据元素715，该索引数据元素715调用可执行数据元素711中的指令，以在外科辅助索引730中创建条目724。因此，在时间t2之后，心内科辅助索引720中的条目的数目保持为一，并且外科辅助索引730包含一个条目。

[0044] 在时间t3时，经由共识过程由矿工节点对数据区块708进行验证，并将其接受到区块链中。在各种数据元素中，数据区块708包含描述第三患者P3对H2的心内科和外科的就诊的数据元素716。数据元素716可以直接调用区块702中的两个可执行数据元素710和711中

的指令，以在心内科辅助索引720中创建条目726并在外科辅助索引730中创建条目728。备选地，数据元素716可以创建索引数据元素717，其调用可执行数据元素710和711中的指令，以在心内科辅助索引720中创建条目726并在外科辅助索引730中创建条目728。因此，在时间t3之后，心内科辅助索引720包含两个条目，并且外科辅助索引730包含两个条目。

[0045] 在两家合作的半导体制造者之间的信息共享的另一示例上下文中，半导体制造者可以将为各种设备制造者(半导体制造者的客户)设计的电路布局存储在区块链中。仅举几个示例，电路可以被分为不同的类型，例如模拟功率电路、数字微控制器电路、数字信号处理器电路、加密/解密电路、视频编码电路。按照上述原理，半导体制造者可以建立各种可执行数据元素(一种电路一种可执行数据元素)，以用于为包含这些类型的电路的数据元素建立辅助索引。如此，例如，可以为包含模拟功率电路的数据元素建立图7的辅助索引720，同时可以为包含数字信号处理器电路的数据元素建立索引730。对应地，可执行数据元素710和711可以包含用于建立针对模拟功率电路和数字信号处理器电路的辅助索引的指令。此外，数据元素712可以包含由第一半导体制造者向第一设备制造者提交的模拟功率电路，并且对应的索引数据元素713可以用于调用可执行数据元素710中的指令来建立辅助索引720。数据元素714可以包含由第二半导体制造者向第二设备制造者提交的数字信号处理器电路，并且对应的索引数据元素715可以用于调用可执行数据元素711中的指令，以用于建立针对数字信号处理器电路的辅助索引730。类似地，数据元素716可以包含由第二半导体制造者向第三设备制造者提交的模拟功率电路和数字信号处理器电路这两者，并且对应的索引数据元素717可以用于调用两个可执行数据元素710和711中的指令，以用于建立针对模拟功率电路和数字信号处理器电路的辅助索引720和730。如此，图7中的图示适用于合作半导体制造者之间的信息共享的上下文和许多其他应用上下文。

[0046] 辅助索引720和730可以与区块链分离存储。它们可以被本地存储在属于医院的节点处。备选地，它们可以被存储在云存储空间中。可以向医院和医院同意授予访问权限的实体提供对辅助索引的访问。辅助索引可以以关系数据库的形式或任何其他形式来存储。备选地，辅助索引可以以任何其他形式来维持并且可以针对查询进行优化。例如，辅助索引可以被存储为诸如二进制排序树的数据结构，并且可以使用涉及哈希的优化算法进行优化。因为不需要将辅助索引写回到区块链中，所以不影响主区块链的验证和共识过程。如此，用于传统区块链的所有共识机制均保持完好无损，并且这些共识机制可以独立于用于建立辅助索引的机制的开发而进一步被开发。

[0047] 进一步地，区块链节点中的应用层中的个体或合作实体可以开发用于建立辅助索引的指令。区块链软件堆栈的较低层仅需要为从区块链中的另一数据元素对区块链中的可执行数据元素(智能合约)的函数调用提供机制或接口。如此，上述用于建立并更新辅助索引的过程不要求对区块链节点处的基本软件堆栈进行任何修改。

[0048] 因为辅助索引通过将用于建立辅助索引的指令封装在主区块链中的可执行数据元素中来根据图5和图6创建并更新，所以由用于主区块链的共识机制确保辅助索引更新的完整性。进一步地，辅助索引仅包含实体、数据元素和区块的标识符信息。实际数据仅驻留在主区块链中，并且受到保护，免受篡改。如此，对辅助索引(可能驻留在主区块链之外，因此不受主区块链的篡改检测机制保护)的任何篡改最多导致当在辅助索引中查询数据ID和区块ID时错误标识数据元素或丢失的数据元素(有关查询过程的详细描述，请参见下文)。

主区块链中的实际数据元素不会受到损害。

[0049] 在将特定类型的数据元素提交到区块链与更新特定类型的数据元素的辅助索引之间可能会有时间延迟。由于这种延迟，图6和图7的数据元素和对应的索引数据元素(诸如数据元素712和对应的索引数据元素713)可以驻留在不同的区块中。然而，因为用于建立辅助索引的指令在将数据元素提交给主区块链之后被执行，所以辅助索引中的任何条目都将对应于已经包括在主区块链中的数据元素。可执行数据元素中用于建立辅助索引的指令可以进一步被构造为保证在将对应数据元素跨区块链节点提交到区块链中之前不更新辅助索引。备选地，区块链节点中的应用层可以确保在将对应的数据元素提交到区块链中之后，向区块链提交索引数据元素(参见图6的610)。

[0050] 图8示出了用于经由为特定类型的数据元素建立的辅助索引在区块链中查询信息的逻辑流程。诸如合作医院之一的实体可以提交可执行数据元素，该可执行数据元素包含用于在辅助索引中查询期望类型的数据元素的指令(802)。该可执行数据元素可以与图5的可执行数据元素502或图6的602集成。具体地，可执行数据元素可以包含用于为特定类型的数据元素创建辅助索引的指令部分以及用于查询辅助索引的指令部分。备选地，图8的可执行数据元素802可以与图5的可执行数据元素502或图6的602分离。

[0051] 继续图8，然后可以经由共识过程由矿工节点将用于查询关于特定类型的数据元素的信息的可执行数据元素包括在区块链中(804)。一旦可执行数据元素到位，实体就可以通过直接调用用于查询针对特定类型的数据元素的辅助索引的指令来查询辅助索引(806)。例如，可以执行查询指令，以使用患者姓名或公钥来查询针对特定类型的数据元素的辅助索引。该直接查询可以独立于区块链。例如，辅助索引可以被存储在区块链外部的数据库中，并且查询可以由实体从其区块链节点或从区块链节点外部的任何地方直接进行。对辅助索引的查询可以返回包含与查询准则相匹配的区块ID和/或数据元素ID的输出(808)。然后，实体可以使用返回的区块ID和/或数据ID来从区块链中获得对应的数据元素，使用公钥解密这些数据元素，并且对数据有效负载进一步解码以获得期望信息(810)。

[0052] 图9示出了用于经由为特定类型的数据元素建立的辅助索引在区块链中查询信息的另一备选逻辑流程。诸如合作医院之一的实体可以提交可执行数据元素，该可执行数据元素包含用于在辅助索引中查询期望类型的数据元素的指令(902)。再次，该可执行数据元素可以与图5的可执行数据元素502或图6的602集成。然后可以经由共识过程由矿工节点将用于查询关于特定类型的数据元素的信息的可执行数据元素包括在区块链中(904)。一旦可执行数据元素到位，实体就可以通过使用包含用于调用可执行数据元素的查询指令的接口的查询数据元素来查询辅助索引(906)。首先可以使用共识过程由矿工节点将查询数据元素包括在区块链中(908)。在将查询数据元素包括到区块链中时，可以自动调用用于查询可执行数据元素中的特定类型的数据元素的辅助索引的指令(910)。例如，可以执行查询指令，以使用患者姓名或公钥来查询针对特定类型的数据元素的辅助索引。对辅助索引的查询可以返回包含与查询准则相匹配的区块ID和/或数据元素ID的输出(912)。然后，实体可以使用区块ID和/或数据ID来从区块链中获得对应的数据元素，使用公钥解密这些数据元素，并且对数据有效负载进一步解码以获得期望信息(914)。

[0053] 因此，本公开提供了一种用于在区块链中建立数据元素的子集的辅助索引的机制。辅助索引可以在应用层处建立并更新，而不影响区块链节点的基本软件堆栈。辅助索引

可以被维持在区块链外部。辅助索引促进高效查询区块链中的数据元素，特别是在区块链系统中的信息共享的上下文中。虽然以上公开内容主要在区块链的上下文中进行，但基本原理适用于任何分散的安全数据处理和存储系统。

[0054] 上述方法、设备、处理和逻辑可以以许多不同的方式以及硬件和软件的许多不同组合来实现。例如，实现的全部或部分可以是电路装置，该电路装置包括：指令处理器，诸如中央处理单元(CPU)、微控制器或微处理器；专用集成电路(ASIC)、可编程逻辑器件(PLD)或现场可编程门阵列(FPGA)；或电路装置，该电路装置包括分立逻辑或其他电路组件，包括模拟电路组件、数字电路组件或两者；或其任何组合。作为示例，该电路装置可以包括分立互连硬件组件，和/或可以被组合在单个集成电路芯片上，分布在多个集成电路管芯之间，或者在公共封装中的多个集成电路管芯的多芯片模块(MCM)中被实现。

[0055] 该电路装置可以进一步包括或访问用于由该电路装置执行的指令。指令可以被存储在除了瞬态信号之外的有形存储介质中，诸如闪存、随机存取存储器(RAM)、只读存储器(ROM)、可擦除可编程只读存储器(EPROM)；或存储在磁盘或光盘上，诸如压缩盘只读存储器(CDROM)、硬盘驱动器(HDD)或其他磁盘或光盘上；或存储在另一种机器可读介质中或上。诸如计算机程序产品的产品可以包括存储介质以及存储在该介质中或上的指令，并且这些指令在由设备中的电路装置执行时可以使得设备实现上述或在附图中图示的任何处理。

[0056] 这些实现可以作为电路装置分布在多个系统组件之间，诸如在多个处理器和存储器之间，可选地包括多个分布式处理系统。参数、数据库和其他数据结构可以被分离存储并管理，可以并入到单个存储器或数据库中，可以以许多不同的方式在逻辑上和物理上进行组织，并且可以以许多不同的方式来实现，包括作为数据结构，诸如链表、哈希表、数组、记录、对象或隐式存储机制。程序可以是单个程序的部分(例如子例程)、分离的程序、分布在多个存储器和处理器上或以许多不同的方式实现，诸如在诸如共享库(例如动态链接库(DLL))的库中。例如，DLL可以存储指令，这些指令在由电路装置执行时，执行上述或在附图中图示的任何处理。

[0057] 已经具体描述了各种实现。然而，许多其他实现也是可能的。

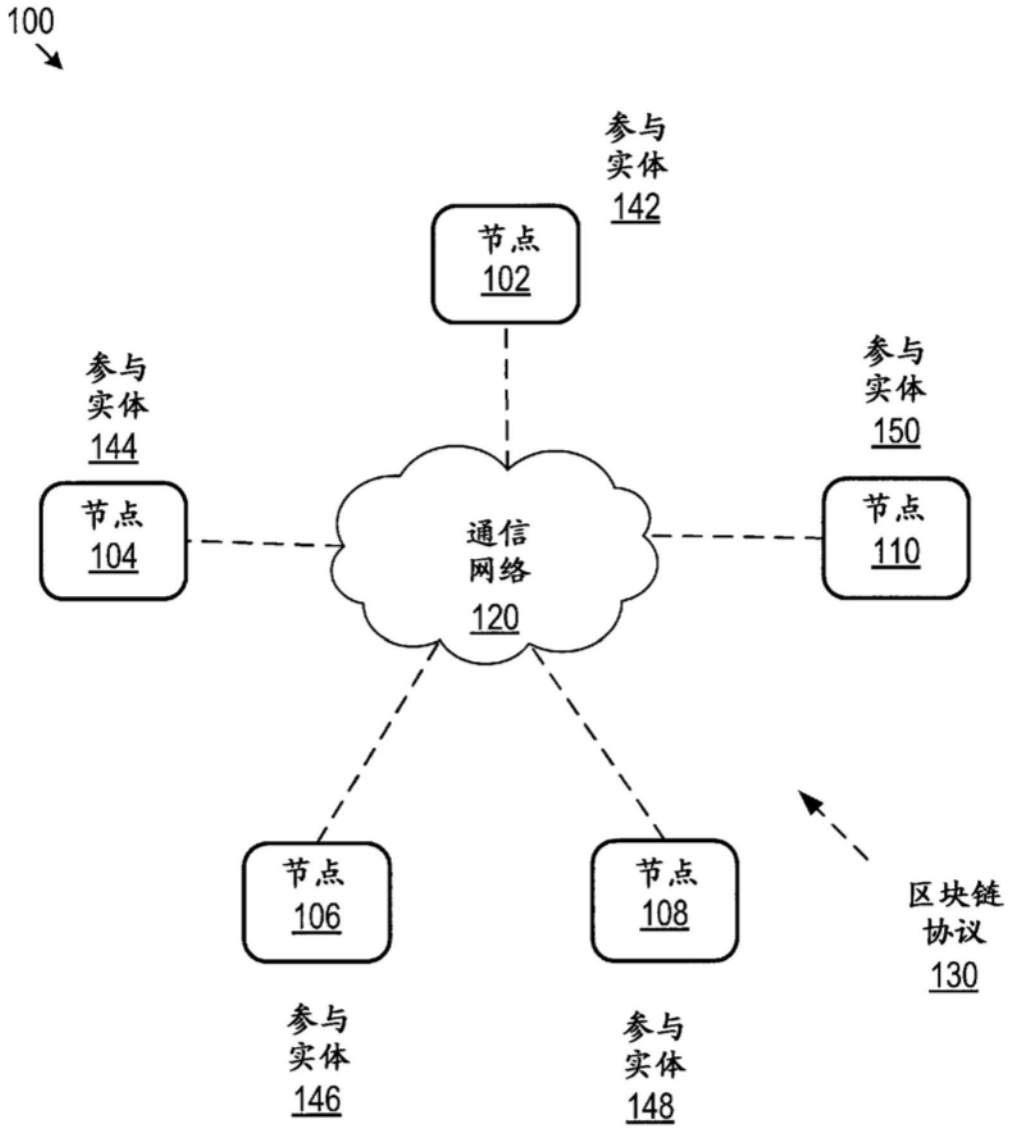

100
参与
实体
142
节点
102
参与
实体
144
节点
104
通信
网络
120
参与
实体
150
节点
110
节点
106
节点
108
区块链
协议
130
参与
实体
146
参与
实体
148

图1

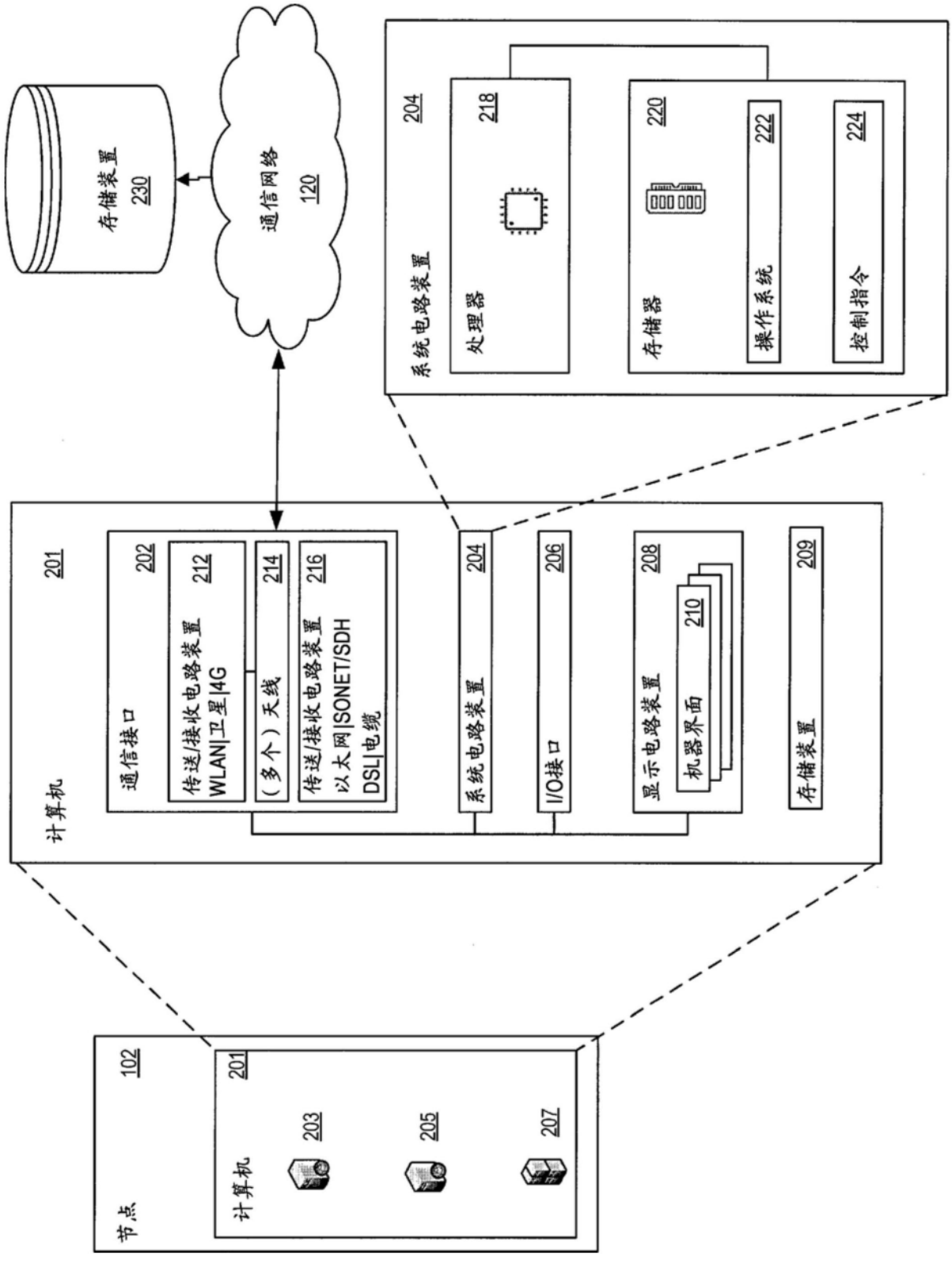

存储装置
230
通信网络
120
系统电路装置
204
处理器
218
存储器
220
操作系统
222
控制指令
224
计算机
201
通信接口
202
传送/接收电路装置
WLAN|卫星|4G
212
(多个)天线
214
传送/接收电路装置
以太网|SONET/SDH
DSL|电缆
216
系统电路装置
204
I/O接口
206
显示电路装置
208
机器界面
210
存储装置
209
节点
102
计算机
201
203
205
207

图2

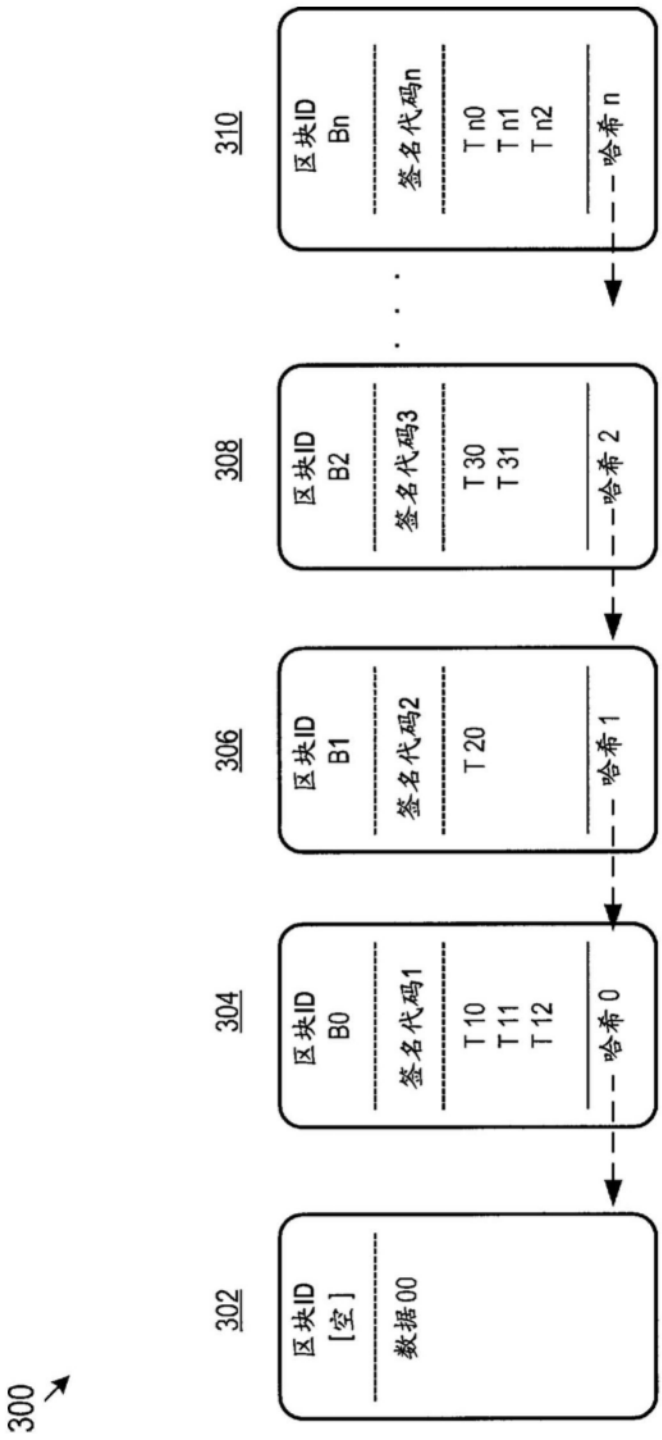

300
302
区块ID
[空]
数据00
304
区块ID
B0
签名代码1
T 10
T 11
T 12
哈希 0
306
区块ID
B1
签名代码2
T 20
哈希 1
308
区块ID
B2
签名代码3
T 30
T 31
哈希 2
310
区块ID
Bn
签名代码n
T n0
T n1
T n2
哈希 n

图3

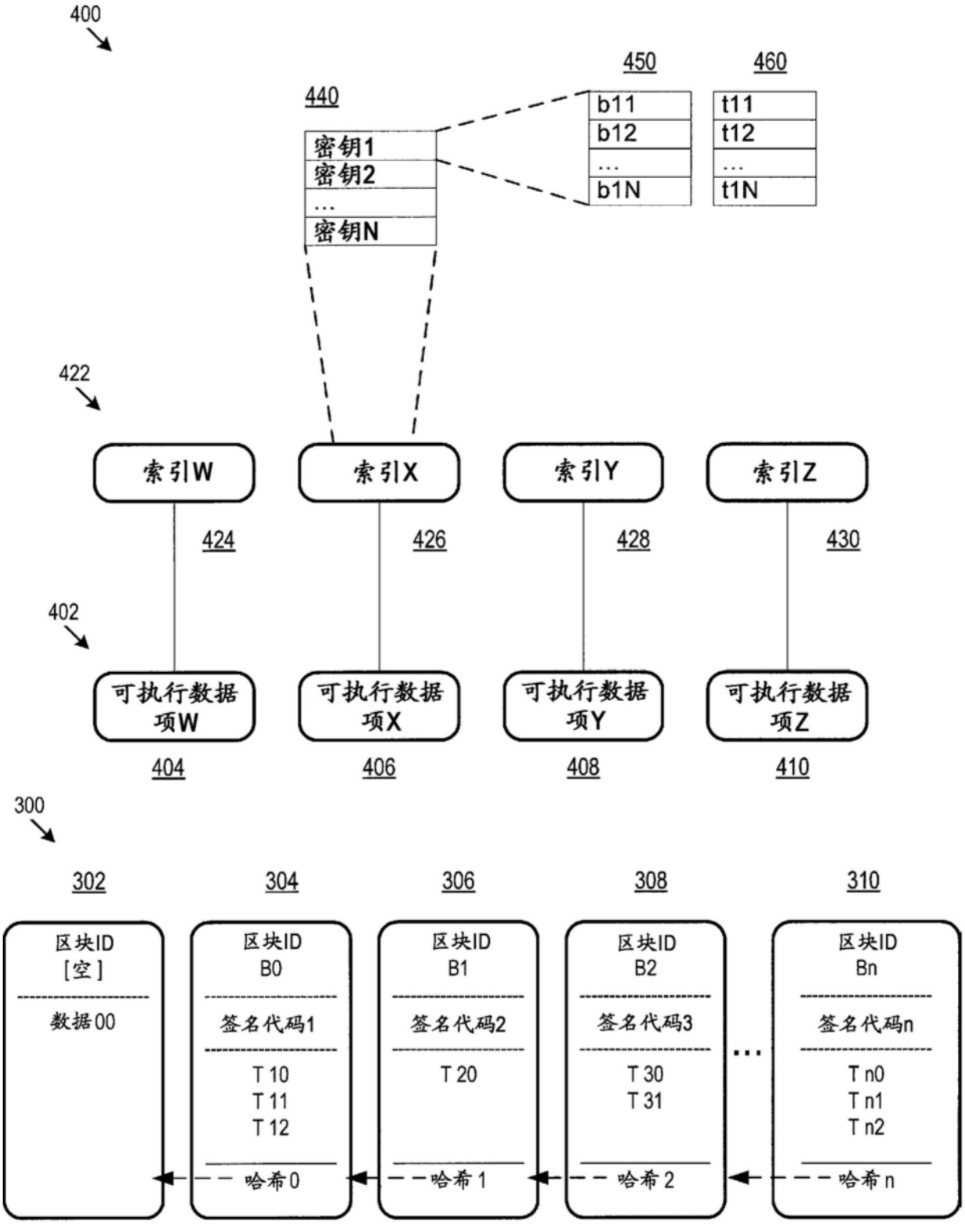

400
450
460
440
密钥1
密钥2
...
密钥N
b11
b12
...
b1N
t11
t12
...
t1N
422
索引W
索引X
索引Y
索引Z
424
426
428
430
402
可执行数据项W
可执行数据项X
可执行数据项Y
可执行数据项Z
404
406
408
410
300
302
304
306
308
310
区块ID
[空]
数据00
区块ID
B0
签名代码1
T 10
T 11
T 12
哈希0
区块ID
B1
签名代码2
T 20
哈希1
区块ID
B2
签名代码3
T 30
T 31
哈希2
区块ID
Bn
签名代码n
T n0
T n1
T n2
哈希n

图4

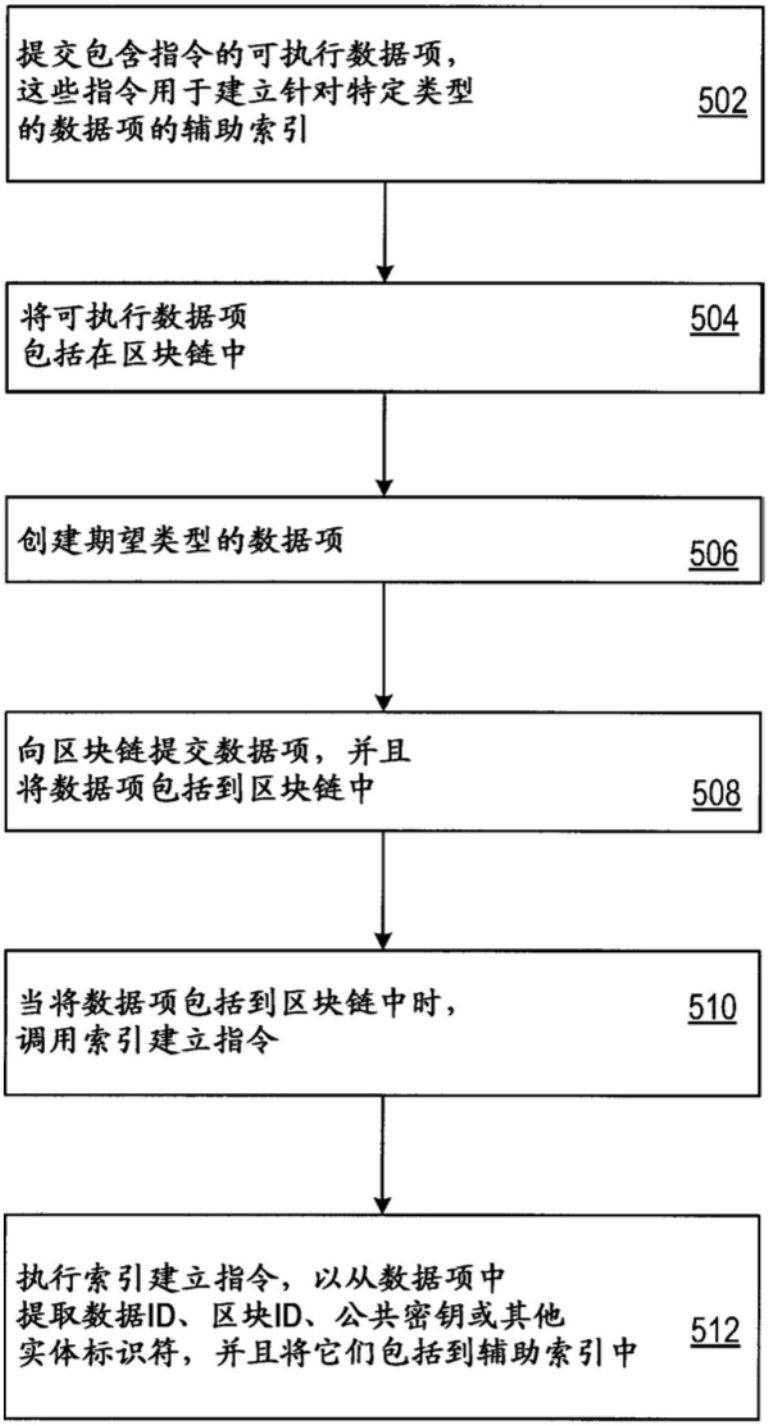

提交包含指令的可执行数据项，这些指令用于建立针对特定类型的数据项的辅助索引
502
将可执行数据项包括在区块链中
504
创建期望类型的数据项
506
向区块链提交数据项，并且将数据项包括到区块链中
508
当将数据项包括到区块链中时，调用索引建立指令
510
执行索引建立指令，以从数据项中提取数据ID、区块ID、公共密钥或其他实体标识符，并且将它们包括到辅助索引中
512

图5

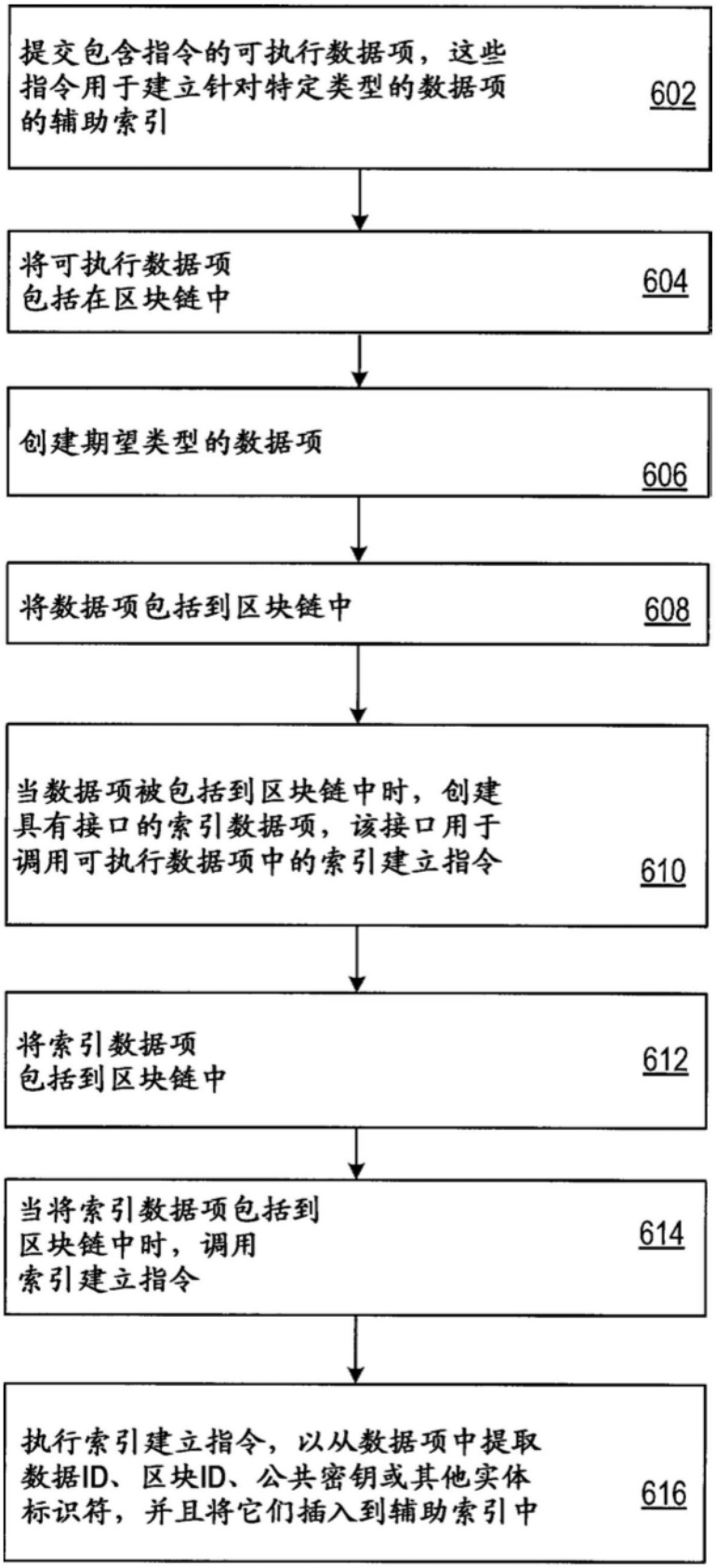

提交包含指令的可执行数据项，这些指令用于建立针对特定类型的数据项的辅助索引
602
将可执行数据项包括在区块链中
604
创建期望类型的数据项
606
将数据项包括到区块链中
608
当数据项被包括到区块链中时，创建具有接口的索引数据项，该接口用于调用可执行数据项中的索引建立指令
610
将索引数据项包括到区块链中
612
当将索引数据项包括到区块链中时，调用索引建立指令
614
执行索引建立指令，以从数据项中提取数据ID、区块ID、公共密钥或其他实体标识符，并且将它们插入到辅助索引中
616

图6

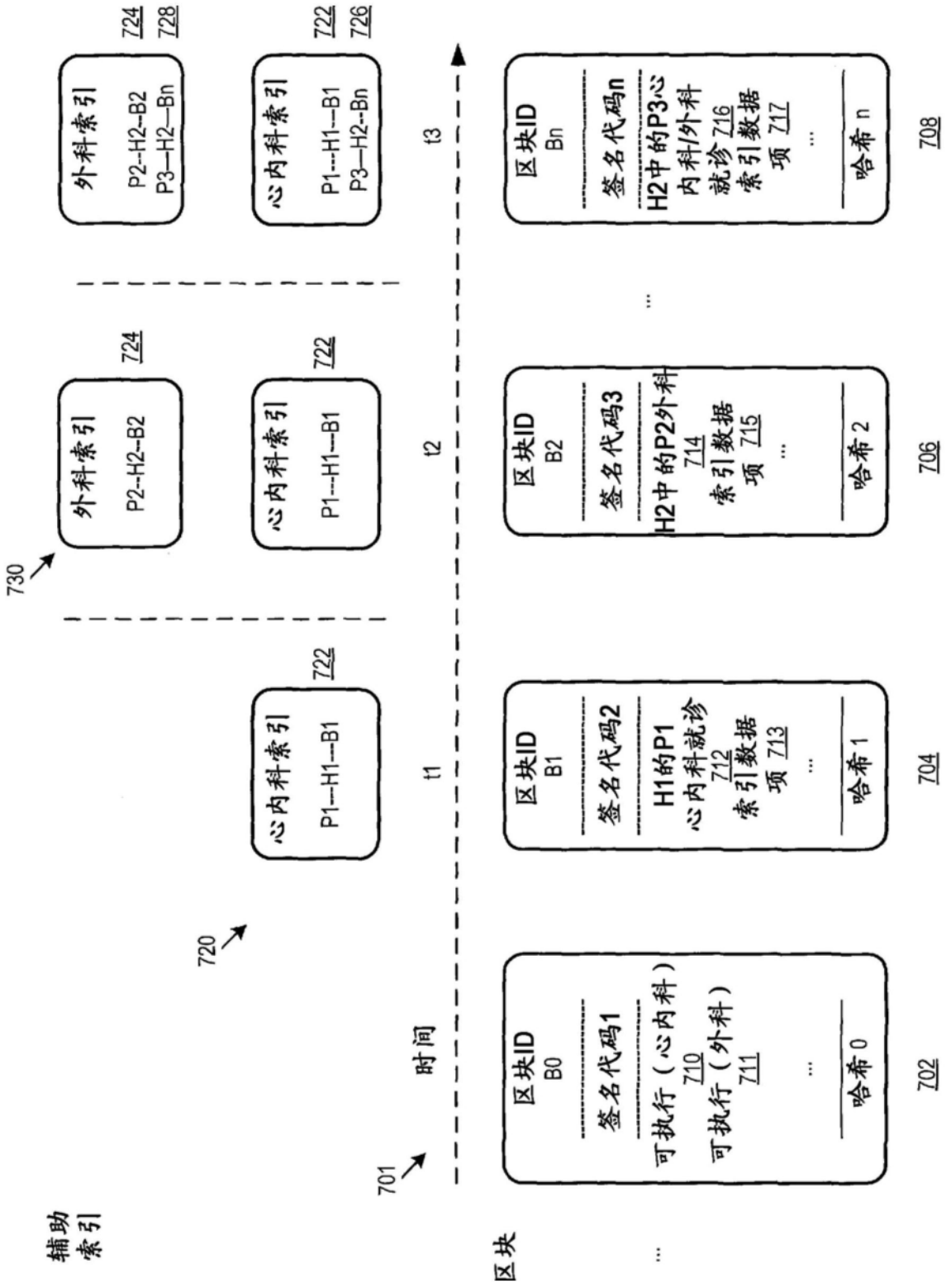

辅助索引
区块
时间
701
720
730
t1
t2
t3
区块ID B0
签名代码1
可执行（心内科）Z10
可执行（外科）Z11
...
哈希 0
Z02
区块ID B1
签名代码2
H1的P1心内科就诊Z12索引数据项 Z13
...
哈希 1
Z04
区块ID B2
签名代码3
H2中的P2外科Z14索引数据项 Z15
...
哈希 2
Z06
区块ID Bn
签名代码n
H2中的P3心内科/外科就诊Z16索引数据项 Z17
...
哈希 n
Z08
心内科索引 P1--H1--B1 Z22
外科索引 P2--H2--B2 Z24
心内科索引 P1--H1--B1 Z22
外科索引 P2--H2--B2 Z24
心内科索引 P1--H1--B1 Z22
外科索引 P2--H2--Bn Z24 Z28
心内科索引 P1--H1--B1 Z22
心内科索引 P3--H2--Bn Z26

图7

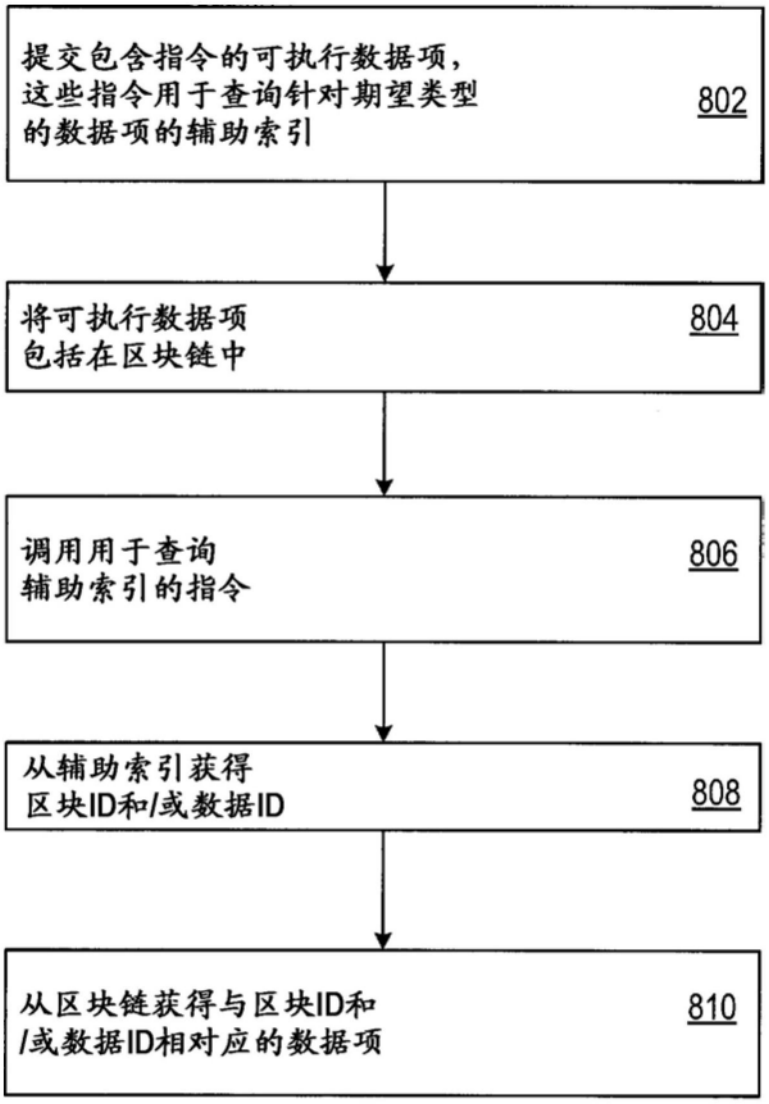

提交包含指令的可执行数据项，这些指令用于查询针对期望类型的数据项的辅助索引
802
将可执行数据项包括在区块链中
804
调用用于查询辅助索引的指令
806
从辅助索引获得区块ID和/或数据ID
808
从区块链获得与区块ID和/或数据ID相对应的数据项
810

图8

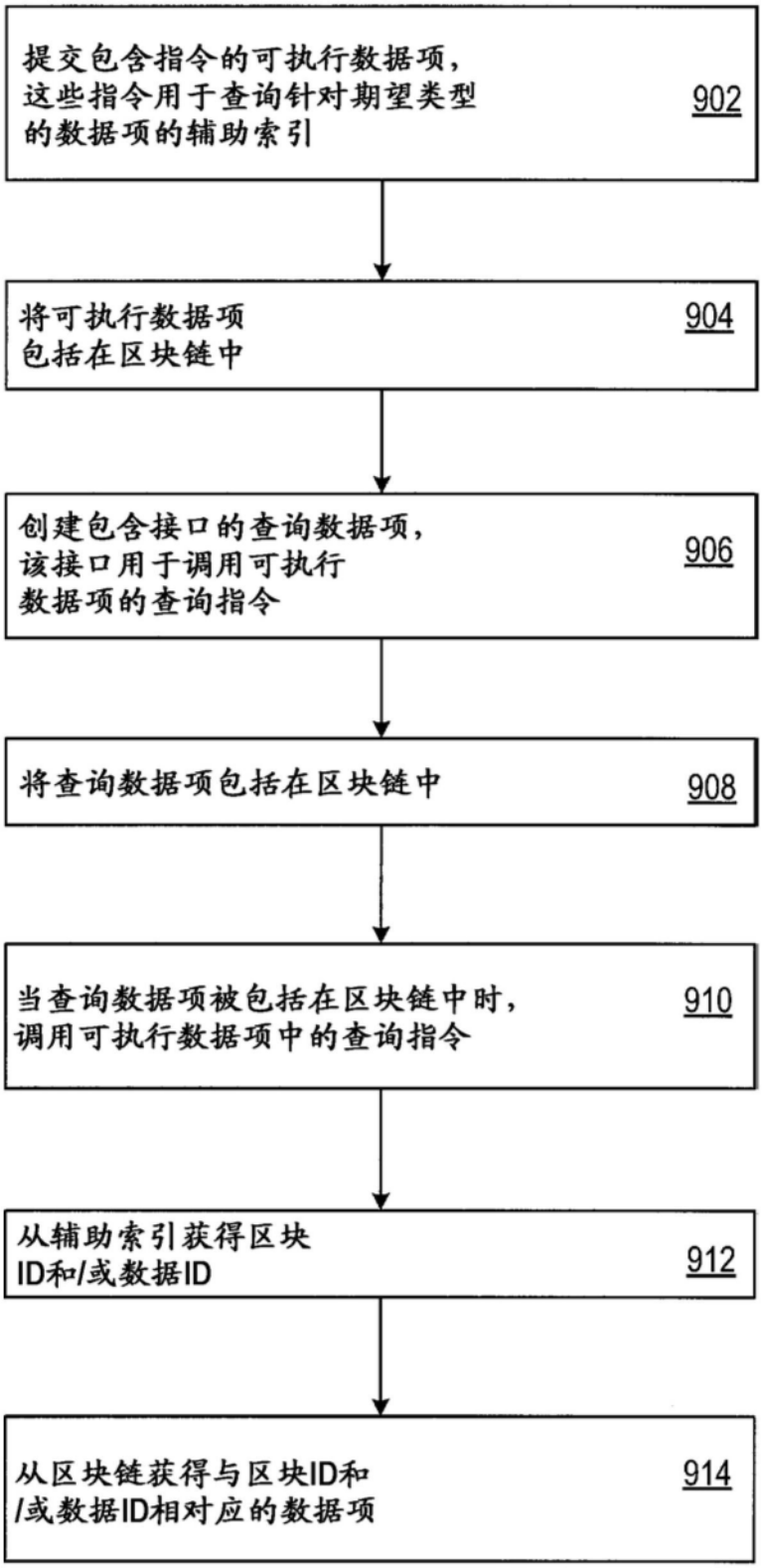

提交包含指令的可执行数据项，这些指令用于查询针对期望类型的数据项的辅助索引
902
将可执行数据项包括在区块链中
904
创建包含接口的查询数据项，该接口用于调用可执行数据项的查询指令
906
将查询数据项包括在区块链中
908
当查询数据项被包括在区块链中时，调用可执行数据项中的查询指令
910
从辅助索引获得区块ID和/或数据ID
912
从区块链获得与区块ID和/或数据ID相对应的数据项
914

图9