(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110460590 B
(45)授权公告日 2022.07.19

(21)申请号 201910678072.4

(22)申请日 2018.12.07

(65)同一申请的已公布的文献号
申请公布号 CN 110460590 A

(43)申请公布日 2019.11.15

(62)分案原申请数据
201811497483.5 2018.12.07

(73)专利权人 深圳市智税链科技有限公司
地址 518000 广东省深圳市南山区粤海街道麻岭社区科技中一路腾讯大厦2401

(72)发明人 李茂材 王宗友 孔利 周开班 杨常青 张劲松 蓝虎 时一防 丁勇 刘区城 朱耿良 陈秋平

(74)专利代理机构 深圳市联鼎知识产权代理有限公司 44232
专利代理师 王鹏健

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/1095(2022.01)
H04L 67/104(2022.01)
H04L 9/32(2006.01)

(56)对比文件
CN 107197036 A,2017.09.22
CN 107197036 A,2017.09.22
CN 108537549 A,2018.09.14
CN 107135661 A,2017.09.05
CN 108111299 A,2018.06.01
CN 108696502 A,2018.10.23
CN 108810119 A,2018.11.13
CN 107077674 A,2017.08.18
CN 108683630 A,2018.10.19
US 2018253464 A1,2018.09.06
WO 2018067232 A1,2018.04.12
于雷等.区块链全局账本数据的拆分技术研究.《高技术通讯》.2017,
Mitsuaki Nakasumi.Information Sharing for Supply Chain Management Based on Block Chain Technology.《2017 IEEE 19th Conference on Business Informatics (CBI)》.2017,

审查员 邓成

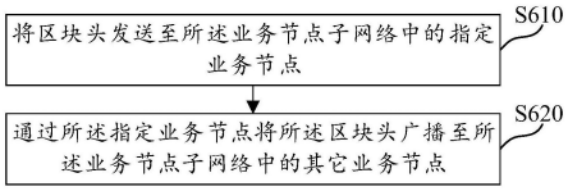
权利要求书3页 说明书17页 附图7页

(54)发明名称

区块链系统的数据管理方法、装置、介质及电子设备

(57)摘要

本申请的实施例提供了一种区块链系统的数据管理方法、装置、介质及电子设备。区块链系统包括记账节点子网络和业务节点子网络，记账节点子网络包括将数据区块记录到区块链上的记账节点，业务节点子网络包括对记账节点记录到区块链上的数据区块进行验证的业务节点，该数据管理方法由记账节点子网络中的记账节点执行，该数据管理方法包括：在生成数据区块后，将生成的数据区块的区块头发送至业务节点子网络中的指定业务节点；通过所述指定业务节点将所述区块头发布至业务节点子网络中，以向业务节点子网络通知新生成的数据区块的信息。本申请实施例的技术方案可以在保证数据安全性的前提下，方便地将记账节点子网络中的数据发送至业务节点子网络中。



CN 110460590 B

1.一种区块链系统的数据管理方法,其特征在于,所述区块链系统包括记账节点子网络和业务节点子网络,所述记账节点子网络包括记账节点,所述业务节点子网络包括业务节点,所述数据管理方法由所述记账节点子网络中的记账节点执行,所述数据管理方法包括:

在生成数据区块后,将生成的数据区块的区块头发送至所述业务节点子网络中的指定业务节点;

通过所述指定业务节点将所述区块头发布至所述业务节点子网络中,以向所述业务节点子网络通知新生成的数据区块的信息;

若接收到所述业务节点子网络中的目标业务节点对指定数据区块中包含的交易数据的获取请求,则获取所述目标业务节点的权限信息,所述获取请求中包含有所述目标业务节点的地址信息,所述地址信息中包含有所述目标业务节点的公钥哈希、所述目标业务节点所属的上级节点的标识信息和所述上级节点的签名信息;

根据所述获取请求中所包含的地址信息,确定所述目标业务节点所属的上级节点,并根据所述目标业务节点所属的上级节点对所述获取请求中所包含的签名信息进行验证;

若对所述获取请求中所包含的签名信息验证通过,则根据所述目标业务节点的权限信息,在所述目标业务节点所属的上级节点对应的数据中查询并获取所述目标业务节点有权获取的交易数据,将查询到的交易数据返回至所述目标业务节点。

2.根据权利要求1所述的区块链系统的数据管理方法,其特征在于,通过所述指定业务节点将所述区块头发布至所述业务节点子网络中,包括:

通过所述指定业务节点将所述区块头广播至所述业务节点子网络中的其它业务节点。

3.根据权利要求1所述的区块链系统的数据管理方法,其特征在于,通过所述指定业务节点将所述区块头发布至所述业务节点子网络中,包括:

以所述指定业务节点作为发送节点将所述区块头发送至离所述发送节点最近的业务节点,并将接收到所述区块头的业务节点作为发送节点继续进行发送,直至所述业务节点子网络中的业务节点均接收到所述区块头。

4.根据权利要求3所述的区块链系统的数据管理方法,其特征在于,将所述区块头发送至离所述发送节点最近的业务节点,包括:

确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离;

将所述区块头发送至与所述发送节点最近的业务节点,其中,若接收到所述区块头的业务节点之前已经接收到所述区块头,则向所述发送节点反馈拒绝消息;

若接收到所述拒绝消息,则根据所述距离由近至远的顺序继续将所述区块头发送至其它业务节点,直至接收到接受消息。

5.根据权利要求4所述的区块链系统的数据管理方法,其特征在于,确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离,包括:

接收所述业务节点子网络中的其它业务节点广播的定位信息;

根据每个其它业务节点广播的定位信息,以及所述发送节点的定位信息,计算每个其它业务节点与所述发送节点之间的距离。

6.根据权利要求5所述的区块链系统的数据管理方法,其特征在于,接收业务节点子网

络中的其它业务节点广播的定位信息，包括：周期性接收业务节点子网络中的其它业务节点广播的定位信息；

根据每个其它业务节点广播的定位信息，以及所述发送节点的定位信息，计算每个其它业务节点与所述发送节点之间的距离，包括：根据最近一次接收到的每个其它业务节点广播的定位信息，以及所述发送节点的定位信息，计算每个其它业务节点与所述发送节点之间的距离。

7.根据权利要求3所述的区块链系统的数据管理方法，其特征在于，在将所述区块头发送至离所述发送节点最近的业务节点之前，还包括：

向分发进度记录服务器发送请求，以使所述分发进度记录服务器查询业务节点子网络中未接收到所述区块头的业务节点的标识，其中，任一业务节点在接收到所述区块头后向所述分发进度记录服务器发送记录请求；

接收所述分发进度记录服务器返回的未接收到所述区块头的业务节点的标识；

在未接收到所述区块头的业务节点中确定离发送节点距离最近的业务节点。

8.根据权利要求1所述的区块链系统的数据管理方法，其特征在于，获取所述目标业务节点的权限信息，包括：

根据所述获取请求中包含的所述目标业务节点的标识信息，获取所述目标业务节点的认证信息；

基于所述认证信息获取所述目标业务节点的权限信息。

9.根据权利要求1所述的区块链系统的数据管理方法，其特征在于，在获取所述目标业务节点的权限信息之后，所述数据管理方法还包括：

将所述指定数据区块中包含的所述目标业务节点无权获取的交易数据的哈希值返回至所述目标业务节点，以使所述目标业务节点根据其有权获取的交易数据和所述无权获取的交易数据的哈希值计算默克尔树根，以对获取到的交易数据进行验证。

10.根据权利要求1所述的区块链系统的数据管理方法，其特征在于，所述权限信息中的权限包括以下中的一种或多种：

允许查看的交易数据所对应的请求上链业务节点；

允许查看的交易数据所对应的交易类型；

允许查看的交易数据所对应的上链时间。

11.一种区块链系统的数据管理装置，其特征在于，所述区块链系统包括记账节点子网络和业务节点子网络，所述记账节点子网络包括记账节点，所述业务节点子网络包括业务节点，所述记账节点包括所述数据管理装置，所述数据管理装置包括：

发送单元，用于在生成数据区块后，将生成的数据区块的区块头发送至所述业务节点子网络中的指定业务节点；

发布单元，用于通过所述指定业务节点将所述区块头发布至所述业务节点子网络中，以向所述业务节点子网络通知新生成的数据区块的信息；

获取单元，用于在接收到所述业务节点子网络中的目标业务节点对指定数据区块中包含的交易数据的获取请求时，获取所述目标业务节点的权限信息，所述获取请求中包含有所述目标业务节点的地址信息，所述地址信息中包含有所述目标业务节点的公钥哈希、所述目标业务节点所属的上级节点的标识信息和所述上级节点的签名信息；

处理单元，用于根据所述获取请求中所包含的地址信息，确定所述目标业务节点所属的上级节点，并根据所述目标业务节点所属的上级节点对所述获取请求中所包含的签名信息进行验证；以及若对所述获取请求中所包含的签名信息验证通过，则根据所述目标业务节点的权限信息，在所述目标业务节点所属的上级节点对应的数据中查询并获取所述目标业务节点有权获取的交易数据，将查询到的交易数据返回至所述目标业务节点。

12.一种计算机可读介质，其上存储有计算机程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求1至10中任一项所述的区块链系统的数据管理方法。

13.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器实现如权利要求1至10中任一项所述的区块链系统的数据管理方法。

区块链系统的数据管理方法、装置、介质及电子设备

[0001] 本申请是2018年12月07日提交的、申请号为201811497483.5、发明名称为“区块链系统的数据管理方法、装置、介质及电子设备”的分案申请。

技术领域

[0002] 本申请涉及计算机及通信技术领域，具体而言，涉及一种区块链系统的数据管理方法、装置、介质及电子设备。

背景技术

[0003] 区块链网络是由众多节点共同组成的一个端到端的去中心化网络，每个节点都允许获得一份完整的数据库拷贝，即节点间各信息完全共享，各节点之间基于一套共识机制来共同维护整个区块链。

[0004] 在区块链系统的一种应用场景中，可能需要将区块链网络中的数据发送至区块链网络之外的业务节点，在这种应用场景下，如何将区块链网络中的数据发送至区块链网络之外的业务节点成为亟待解决的技术问题。

发明内容

[0005] 本申请的实施例提供了一种区块链系统的数据管理方法、装置、介质及电子设备，进而至少在一定程度上可以在保证数据安全性的前提下，方便地将记账节点子网络中的数据发送至业务节点子网络中。

[0006] 本申请的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本申请的实践而习得。

[0007] 根据本申请实施例的一个方面，提供了一种区块链系统的数据管理方法，所述区块链系统包括记账节点子网络和业务节点子网络，所述记账节点子网络包括将数据区块记录到区块链上的记账节点，所述业务节点子网络包括对记账节点记录到区块链上的数据区块进行验证的业务节点，所述数据管理方法由所述记账节点子网络中的记账节点执行，所述数据管理方法包括：在生成数据区块后，将生成的数据区块的区块头发送至所述业务节点子网络中的指定业务节点；通过所述指定业务节点将所述区块头发布至所述业务节点子网络中，以向所述业务节点子网络通知新生成的数据区块的信息。

[0008] 根据本申请实施例的一个方面，提供了一种区块链系统的数据管理装置，所述区块链系统包括记账节点子网络和业务节点子网络，所述记账节点子网络包括记账节点，所述业务节点子网络包括业务节点，所述记账节点包括所述数据管理装置，所述数据管理装置包括：发送单元，用于在生成数据区块后，将生成的数据区块的区块头发送至所述业务节点子网络中的指定业务节点；发布单元，用于通过所述指定业务节点将所述区块头发布至所述业务节点子网络中，以向所述业务节点子网络通知新生成的数据区块的信息。

[0009] 在本申请的一些实施例中，基于前述方案，所述发布单元配置为：通过所述指定业务节点将所述区块头广播至所述业务节点子网络中的其它业务节点。

[0010] 在本申请的一些实施例中，基于前述方案，所述发布单元配置为：以所述指定业务节点作为发送节点将所述区块头发送至离所述发送节点最近的业务节点，并将接收到所述区块头的业务节点作为发送节点继续进行发送，直至所述业务节点子网络中的业务节点均接收到所述区块头。

[0011] 在本申请的一些实施例中，基于前述方案，所述发布单元配置为：确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离；将所述区块头发送至与所述发送节点最近的业务节点，其中，若接收到所述区块头的业务节点之前已经接收到所述区块头，则向所述发送节点反馈拒绝消息；若接收到所述拒绝消息，则根据所述距离由近至远的顺序继续将所述区块头发送至其它业务节点，直至接收到接受消息。

[0012] 在本申请的一些实施例中，基于前述方案，所述发布单元配置为：接收所述业务节点子网络中的其它业务节点广播的定位信息；根据每个其它业务节点广播的定位信息，以及所述发送节点的定位信息，计算每个其它业务节点与所述发送节点之间的距离。

[0013] 在本申请的一些实施例中，基于前述方案，所述发布单元配置为：周期性接收业务节点子网络中的其它业务节点广播的定位信息；根据最近一次接收到的每个其它业务节点广播的定位信息，以及所述发送节点的定位信息，计算每个其它业务节点与所述发送节点之间的距离。

[0014] 在本申请的一些实施例中，基于前述方案，所述区块链系统的数据管理装置还包括：确定单元，用于向分发进度记录服务器发送请求，以使所述分发进度记录服务器查询业务节点子网络中未接收到所述区块头的业务节点的标识，其中，任一业务节点在接收到所述区块头后向所述分发进度记录服务器发送记录请求；接收所述分发进度记录服务器返回的未接收到所述区块头的业务节点的标识；在未接收到所述区块头的业务节点中确定离发送节点距离最近的业务节点。

[0015] 在本申请的一些实施例中，基于前述方案，所述的区块链系统的数据管理装置还包括：获取单元，用于在接收到所述业务节点子网络中的目标业务节点对指定数据区块中包含的交易数据的获取请求时，获取所述目标业务节点的权限信息；处理单元，用于根据所述目标业务节点的权限信息，将所述指定数据区块中包含的所述目标业务节点有权获取的交易数据返回至所述目标业务节点。

[0016] 在本申请的一些实施例中，基于前述方案，所述获取单元配置为：根据所述获取请求中包含的所述目标业务节点的标识信息，获取所述目标业务节点的认证信息；基于所述认证信息获取所述目标业务节点的权限信息。

[0017] 在本申请的一些实施例中，基于前述方案，所述处理单元还用于：将所述指定数据区块中包含的所述目标业务节点无权获取的交易数据的哈希值返回至所述目标业务节点，以使所述目标业务节点根据其有权获取的交易数据和所述无权获取的交易数据的哈希值计算默克尔树根，以对获取到的交易数据进行验证。

[0018] 在本申请的一些实施例中，基于前述方案，所述获取请求中包含有所述目标业务节点的地址信息，所述地址信息中包含有所述目标业务节点的标识信息、所述目标业务节点所属的上级节点的标识信息和所述上级节点的签名信息；所述处理单元还用于：根据所述获取请求中所包含的地址信息，确定所述目标业务节点所属的上级节点，并根据所述目标业务节点所属的上级节点对所述获取请求中所包含的签名信息进行验证；若对所述获取

请求中所包含的签名信息验证通过，则基于所述目标业务节点的权限信息，在所述目标业务节点所属的上级节点对应的数据中查询并获取所述目标业务节点有权获取的交易数据。

[0019] 在本申请的一些实施例中，基于前述方案，所述权限信息中的权限包括以下中的一种或多种：允许查看的交易数据所对应的请求上链业务节点；允许查看的交易数据所对应的交易类型；允许查看的交易数据所对应的上链时间。

[0020] 根据本申请实施例的一个方面，提供了一种计算机可读介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如上述实施例中所述的区块链系统的数据管理方法。

[0021] 根据本申请实施例的一个方面，提供了一种电子设备，包括：一个或多个处理器；存储装置，用于存储一个或多个程序，当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器实现如上述实施例中所述的区块链系统的数据管理方法。

[0022] 在本申请的一些实施例所提供的技术方案中，通过将区块链系统分为记账节点子网络和业务节点子网络，记账节点子网络包括将数据区块记录到区块链上的记账节点，业务节点子网络包括对记账节点记录到区块链上的数据区块进行验证的业务节点，使得能够将区块链系统的记账过程与业务处理过程进行分离，进而既能够通过记账节点子网络来维护全量的数据区块，保证数据区块的安全性，又能够通过业务节点子网络来实现灵活的数据访问，比如分层级的不同权限的数据访问等。通过将生成的数据区块的区块头发送至业务节点子网络中的指定业务节点，并通过该指定业务节点将该区块头发布至业务节点子网络，以向业务节点子网络通知新生成的数据区块的信息，使得业务节点子网络中的业务节点既能够获知共识节点子网络中新生成的数据区块，又能够避免将整个数据区块全部发送至业务节点子网络而导致数据区块中的交易数据被泄露的问题。

[0023] 应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本申请。

附图说明

[0024] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本申请的实施例，并与说明书一起用于解释本申请的原理。显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。在附图中：

[0025] 图1至图3示出了本申请实施例所应用的区块链系统的体系构架示意图；

[0026] 图4示意性示出了根据本申请的一个实施例的区块链系统的数据管理方法的流程图；

[0027] 图5示出了根据本申请的一个实施例的数据区块在进行共识的过程示意图；

[0028] 图6示意性示出了根据本申请的一个实施例的将数据区块的区块头发布至业务节点子网络中的流程图；

[0029] 图7示意性示出了根据本申请的一个实施例的将数据区块的区块头发布至业务节点子网络中的流程图；

[0030] 图8示意性示出了根据本申请的一个实施例的将区块头发送至离发送节点最近的

业务节点的流程图；

[0031] 图9示意性示出了根据本申请的一个实施例的生成默克尔树根的流程图；

[0032] 图10示出了根据本申请的一个实施例的业务节点的地址结构示意图；

[0033] 图11示意性示出了根据本申请的一个实施例的区块链系统的数据管理方法的流程图；

[0034] 图12示意性示出了根据本申请的一个实施例的区块链系统的数据管理方法的流程图；

[0035] 图13示意性示出了根据本申请的一个实施例的区块链系统的数据管理装置的框图；

[0036] 图14示意性示出了根据本申请的一个实施例的区块链系统的数据管理装置的框图；

[0037] 图15示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

具体实施方式

[0038] 现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例；相反，提供这些实施方式使得本申请将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。

[0039] 此外，所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施例中。在下面的描述中，提供许多具体细节从而给出对本申请的实施例的充分理解。然而，本领域技术人员将意识到，可以实践本申请的技术方案而没有特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知方法、装置、实现或者操作以避免模糊本申请的各方面。

[0040] 附图中所示的方框图仅仅是功能实体，不一定必须与物理上独立的实体相对应。即，可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

[0041] 附图中所示的流程图仅是示例性说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解，而有的操作/步骤可以合并或部分合并，因此实际执行的顺序有可能根据实际情况改变。

[0042] 图1示出了本申请实施例所应用的一种区块链系统的体系构架。区块链系统包括记账节点子网络2和业务节点子网络1。记账节点子网络2包括对数据区块进行共识并将数据区块记录到区块链上的记账节点21。业务节点子网络1包括业务节点11，业务节点11可以对记账节点记录到区块链上的数据区块进行验证，或者可以向记账节点请求相应的交易数据。

[0043] 具体的，业务节点11对记账节点记录到区块链上的数据区块进行验证可以包括以下步骤：记账节点子网络中的一个记账节点21利用特定于该记账节点的密钥，基于要添加到区块链上的一个数据区块中所要包括的交易信息，生成签名；记账节点21将所述交易信息和生成的签名加入所述数据区块，添加到区块链上；记账节点21将所述签名发往所述业务节点子网络中的业务节点，业务节点根据特定于该记账节点的密钥对所述签名进行签名验证，以实现业务节点11对记账节点记录到区块链上的数据区块进行验证。记账节点子网

络中的记账节点负责向区块链记录数据区块，业务节点子网络中的业务节点负责见证记账节点记录的结果。具体地，记账节点基于要添加到区块链上的一个数据区块中所要包括的交易信息，生成签名，然后将所述交易信息和生成的签名加入所述数据区块，进行上链。所述签名发往所述业务节点子网络中的业务节点，使业务节点根据特定于该记账节点的密钥对所述签名进行签名验证。业务节点子网络中的业务节点通过验证区块上记账节点签名可以对全网的交易数据进行见证。记账网络虽然拥有垄断的记账权，但是因为数据区块有了代表记账者身份的数字签名，所以一切行为都是公开可追溯的。如果记账节点集体作恶，那么见证网络中的全部节点都讲将保留有具体记账节点作恶的证据。相比传统中心化系统和私有链，这个方案中，系统的运转是更加透明的；而相比传统的去中心化公链方案，本方案是更可控也更便于可监管的。

[0044] 在本申请的一个实施例中，记账节点子网络2和业务节点子网络1之间可以通过代理节点12连接，代理节点12可以是业务节点子网络1的一个业务节点，其负责将记账节点21要向业务节点11传递的信息传递给业务节点11。业务节点11是产生各种需上链的交易数据的交易方的终端，也可以是从记账节点子网络2中查询交易数据的终端。业务节点11产生的交易数据在通过代理节点12传输至记账节点21，然后经过共识后记录到区块链上，有利于交易数据的统一处理和监管，而业务节点11也可以通过记账节点21经由代理节点12发送来的信息进行交易数据上链的监督和见证，这在某些既需要统一监管、但又怕监管的节点集体作弊因而需要监督的场景中有十分重要的意义。

[0045] 在图1所示的结构中，业务节点子网络1采用P2P网络模式。P2P网络是一种在对等者(Peer)之间分配任务和工作负载的分布式应用架构，是对等计算模型在应用层形成的一种组网或网络形式，即“点对点”或者“端对端”网络。其可以定义为：网络的参与者共享他们所拥有的一部分硬件资源(处理能力、存储能力、网络连接能力、打印机等)，这些共享资源通过网络提供服务和内容，能被其它对等节点直接访问而无需经过中间实体。在此网络中的参与者既是资源、服务和内容的提供者，又是资源、服务和内容的获取者。因此，在业务节点子网络1中，当代理节点12接收到从记账节点21传递过来的消息后，向周围的业务节点11进行传播，周围的业务节点11接收到该消息，再向其周围的业务节点11传递，达到了该消息在业务节点子网络1的每个业务节点11之间的传播。

[0046] 图2示出了本申请实施例所应用的另一种区块链系统的体系构架。该体系构架与图1中所示的体系构架不同之处在于：在业务节点子网络1中没有采取P2P网络模式，而是采取广播网络的模式。具体地，代理节点12在接收到从记账节点21传递过来的消息后，将该消息广播到业务节点子网络1中的其它业务节点11。这样，也实现了该消息在业务节点子网络1的每个业务节点11之间的传播。

[0047] 图3示出了本申请实施例所应用的另一种区块链系统的体系构架。该体系构架与图1所示的体系构架不同之处在于：其记账节点子网络2分成了多个分支记账节点子网络。每个分支记账节点子网络可以负责某一种类型的交易信息的记录。例如，某一企业可能具有供应链金融业务，可能需要将供销过程中产生的合同信息、货款赊欠等信息记录到区块链上，同时该企业还要开具发票，也要把开票信息、发票报销信息等记录到区块链上。这时，为了有利于记账节点被同一部门监管的需要，可能记录供应链金融业务交易的记账节点和记录发票流转过程中的交易的记账节点要分属于不同部门。例如，记录供应链金融业务交

易的记账节点是银行设置的记账终端，而记录发票流转过程中的交易的记账节点是国税局设置的记账终端。而供应链金融业务交易和记录发票流转过程中的交易可能也最终会记录在不同分支的记账节点子网络上。这时，代理节点12要根据从业务节点11发来的交易信息中携带的交易类型，将该交易信息发送到与该交易类型对应的分支记账节点子网络中。

[0048] 需要说明的是，在图1至图3所示的区块链系统的体系构架中，代理节点12位于业务节点子网络1中，在本申请的其它实施例中，代理节点12也可以位于共识节点子网络2中，或者独立于业务节点子网络1和共识节点子网络2。

[0049] 图1至3所示的区块链系统的体系架构可以应用在电子发票的应用场景中，以下详细进行阐述：

[0050] 在本申请的一个实施例中，记账节点子网络中的记账节点可以是各个税务总局终端，比如由部署在多个地区的税务总局终端分别作为一个记账节点来构成记账节点子网络。业务节点子网络中的各个业务节点可以是地方税局终端、开票代理服务商终端、开票企业终端、个人用户终端等。

[0051] 当记账节点子网络中的记账节点生成数据区块后(该数据区块中可能包含开具的发票信息等)，可以将生成的数据区块的区块头发布至业务节点子网络，以向业务节点子网络通知新生成的数据区块的信息，同时又可以避免直接将数据区块发送至业务节点子网络中而导致数据区块中的数据被无访问权限的角色(比如个人用户无法查看与其无关的发票信息等)非法窃取的问题。业务节点子网络中的业务节点在接收到数据区块的区块头后，可以得知记账节点子网络中新产生的数据区块，进而可以向记账节点子网络请求获取指定数据区块中包含的交易数据(比如通过代理节点向记账节点子网络发送交易数据的获取请求)。记账节点子网络中记账节点在接收到对指定数据区块中包含的交易数据的获取请求之后，可以获取到发送获取请求的业务节点的权限信息，然后根据该权限信息将指定数据区块中包含的该业务节点有权获取的交易数据返回给该业务节点。比如省税局能够访问与本省相关的发票信息、市税局只能访问与本市相关的发票信息、区税局只能访问与本区相关的发票信息、开票代理服务商只能访问其代理的企业相关的发票信息等。

[0052] 以下对本申请实施例的区块链系统的数据管理方案的实现细节进行详细阐述：

[0053] 图4示意性示出了根据本申请的一个实施例的区块链系统的数据管理方法的流程图，如图1至图3所示，该区块链系统包括记账节点子网络2和业务节点子网络1，记账节点子网络2包括记账节点21，业务节点子网络1包括业务节点11。图4所示的区块链系统的数据管理方法可以由记账节点子网络2中的记账节点21来执行，并且图4所示的各个步骤可以是记账节点子网络2中的任意一个记账节点全部执行的，也可以是由多个记账节点配合完成的，这多个记账节点中的每个记账节点仅执行其中的部分步骤。参照图4所示，该区块链系统的数据管理方法至少包括步骤S410至步骤S430，详细介绍如下：

[0054] 在步骤S410中，在生成数据区块后，将生成的数据区块的区块头发布至所述业务节点子网络，以向所述业务节点子网络通知新生成的数据区块的信息。

[0055] 在本申请的一个实施例中，数据区块可以是根据业务节点子网络中的业务节点发送的待上链交易数据(比如开票数据，发票流转数据等)打包生成的。比如当接收到交易数据后可以先缓存起来，当满足以下至少一项打包要求时可以对缓存的交易数据进行打包生成数据区块：

[0056] 缓存中的待上链交易数据的总大小达到预定大小阈值；

[0057] 缓存中的待上链交易数据的总条数达到预定条数阈值；

[0058] 缓存中的待上链交易数据中最早缓存的一条待上链交易数据的缓存时间距离当前时间达到预定时间阈值。

[0059] 在本申请的一个实施例中，在区块打包要求是缓存中的待上链交易数据的总大小超过预定大小阈值的情况下，例如，预定大小阈值为4Mb，缓存中原来有2条交易数据，分别是0.8Mb和1.5Mb，如果这时又接收到一条待上链交易数据，大小为2Mb，这样0.8Mb+1.5Mb+2Mb＝4.3Mb>4Mb，此时就可以为这3条交易数据生成一个数据区块，避免为每一条交易数据生成一个数据区块的资源浪费。

[0060] 在本申请的一个实施例中，在区块打包要求是缓存中的待上链交易数据的总条数超过预定条数阈值的情况下，例如，预定条数阈值为5，缓存中原来有4条交易数据，如果这时又接收到一条待上链交易数据，此时就可以为这5条交易数据生成一个数据区块，避免为每一条交易数据生成一个数据区块的资源浪费。

[0061] 在本申请的一个实施例中，在区块打包要求是缓存中的待上链交易数据中最早缓存的一条待上链交易数据的缓存时间距离当前时间达到预定时间阈值的情况下，例如，预定时间阈值为24小时，如果待上链交易数据在2018年4月25日11:27:01放入缓存，在4月26日11:27:01就可以为该待上链交易数据生成一个数据区块，避免从请求上链到真正上链的时延过大。

[0062] 在实践中，可以将上述中的一条或多条结合使用。例如，如果缓存中的待上链交易数据的总大小达到预定大小阈值，或者缓存中的待上链交易数据中最早缓存的一条带上链交易数据的缓存时间距离当前时间达到预定时间阈值，都可以生成一个数据区块。这样，既避免了为一个交易数据生成一个数据区块而造成资源浪费，又避免了在一段时间接收到的交易数据不够多而造成无限制的等待。

[0063] 在本申请的一个实施例中，当生成数据区块后，可以将生成的数据区块发布至记账节点子网络中由各个记账节点进行共识，当共识成功之后，将数据区块添加在区块链上。

[0064] 具体地，在本申请的一个实施例中，如图5所示为本申请实施例的由领导记账节点将数据区块广播到记账节点子网络中的其它记账节点进行共识的过程。其中，客户端(可以是形成要记录在区块链上的数据区块的记账节点)发起共识请求，并将共识请求发送至处于领导状态的领导记账节点A；继续进入添加实体阶段，由领导记账节点A将共识请求所对应的数据区块广播至记账节点子网络中其它未处于领导状态的记账节点(记账节点B、C、D…)；继续进入追加响应阶段，由其它记账节点将接收到的共识内容广播至其它各记账节点，并在接收到预设数量(2f+1)的其它记账节点所广播的共识内容一致时，进入确认阶段，各记账节点再将确认结果反馈至领导记账节点A。领导记账节点A在接收到预设数量(2f+1)的其它区块链节点反馈确认通过时，则判定完成共识向客户端反馈共识完成的结果。其中，f是小于(N-1)/3的最大整数，N是记账节点子网络中记账节点的数量。f是算法能容忍的记账节点子网络中作恶记账节点的数量。

[0065] 当共识成功后，记账节点子网络中的各个记账节点就可以将数据区块添加到区块链上，即完成上链。

[0066] 在本申请的一个实施例中，数据区块的区块头中不包含有具体的交易数据，这样

在将数据区块的区块头发布至业务节点子网络中之后，业务节点子网络中的业务节点只会知道记账节点子网络中新产生了数据区块，而不会获取到数据区块中的具体交易数据。

[0067] 在本申请的一个实施例中，如图6所示，步骤S410中将生成的数据区块的区块头发布至业务节点子网络中的过程，包括：

[0068] 步骤S610，将区块头发送至所述业务节点子网络中的指定业务节点。

[0069] 步骤S620，通过所述指定业务节点将所述区块头广播至所述业务节点子网络中的其它业务节点。

[0070] 该实施例是针对图2中所示的区块链系统的体系构架。在该体系构架中，可以将业务节点子网络中的一个业务节点作为代理节点，然后通过广播的方式向业务节点子网络的所有业务节点发送数据区块的区块头。该实施例的好处在于，可以快速将区块头通知到业务节点子网络中的所有业务节点。

[0071] 业务节点子网络除了可以采用图2所示的广播消息的通信方式，还可以采用如图1和图3所示的P2P式的网络通信方式。在P2P的业务节点子网络中，代理节点可以将区块头发送到其周围的业务节点，接收到该区块头的业务节点再将区块头发送到该业务节点周围的其它业务节点，直到业务节点子网络的所有业务节点都接收到该区块头为止。

[0072] 在一个P2P组网形式的实施例中，如图7所示，将所述区块头发布至业务节点子网络中的过程，包括：

[0073] 步骤S710，将区块头发送至所述业务节点子网络中的指定业务节点。

[0074] 步骤S720，以所述指定业务节点作为发送节点将所述区块头发送至离所述发送节点最近的业务节点，并将接收到所述区块头的业务节点作为发送节点继续进行发送，直至所述业务节点子网络中的业务节点均接收到所述区块头。

[0075] 在步骤S720中，由于已经接收到区块头的业务节点重复接收同样的区块头没有意义，因此，每个业务节点确定要发送区块头的下一个业务节点时，除了要考虑优先发送给离其近的业务节点(以减少传输等待时间)外，还要考虑要传送到还没有接收到该区块头的业务节点。这样，每个业务节点都只需要将区块头发送到一个业务节点，这个业务节点是未接收到该区块头的其它业务节点中离自己最近的业务节点。这样，就完成了区块头逐个节点的安全下发，同时避免下发负担集中在一个业务节点上，实现了负载均衡。

[0076] 在本申请的一个实施例中，如图8所示，步骤S720中将区块头发送至离发送节点最近的业务节点，可以包括如下步骤：

[0077] 步骤S810，确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离。

[0078] 步骤S820，将所述区块头发送至与所述发送节点最近的业务节点，其中，若接收到所述区块头的业务节点之前已经接收到所述区块头，则向所述发送节点反馈拒绝消息。

[0079] 步骤S830，若接收到所述拒绝消息，则根据所述距离由近至远的顺序继续将所述区块头发送至其它业务节点，直至接收到接受消息。

[0080] 在本申请的一个实施例中，在步骤S810中，确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离可以包括：周期性(例如每隔5秒)接收从业务节点子网络中的其它业务节点广播的定位信息，按照最近一次接收到的每个其它业务节点广播的定位信息、以及发送节点的定位信息，计算每个其它业务节点与所述发

送节点的距离。

[0081] 在本申请的一个实施例中，定位信息是各业务节点从自身的定位系统(例如节点上安装的GPS系统)获得的业务节点的位置信息。业务节点从其安装的定位系统上获得自己的定位信息，然后周期性(例如每隔5秒)广播到业务节点子网络中的其它业务节点。而发送节点也可以从自身的定位系统中获得其自身的定位信息。由于定位信息的广播和更新是周期性的，周期比较短，可以将发送节点最近一次接收到的每个其它业务节点广播的定位信息就看成是每个其它业务节点的当前定位信息，这样，按照最近一次接收到的每个其它业务节点广播的定位信息、以及发送节点的定位信息，就可以计算出每个其它业务节点与所述发送节点的距离。

[0082] 通过计算出的以上距离，可以找到所有其它业务节点中与发送节点距离最小的其它业务节点，但该其它业务节点有可能已经接到过该区块头。因此，本申请的实施例通过让接收到区块头的其它业务节点发送接受消息或拒绝消息来避免将区块头重复发给某个业务节点。其中，接受消息或拒绝消息的区别在于，其某一个特定标识字段设置为不同的字符或字符串，以表示接受消息或拒绝消息。这样，可以通过识别接收到的消息中的该特定标识字段，以识别接收到的消息是接受消息还是拒绝消息。如果是接受消息，就表示接收到该区块头的业务节点之前没有接收到过该区块头，因此接受了该区块头。如果是拒绝消息，就表示接收到该区块头的业务节点之前接收到过该区块头，因此拒绝了该区块头。如果接收到拒绝消息，就要找到距离发送节点第二小的其它业务节点，再通过向其发送区块头来判断该其它业务节点反馈的是拒绝消息还是接受消息，如果仍然是拒绝消息，就要找到距离发送节点第三小的其它业务节点，再向其发送区块头，进行该其它业务节点反馈的是拒绝消息还是接受消息的判断。也就是说，如果接收到拒绝消息，就根据与发送节点距离由近至远的顺序继续将区块头发送至其它业务节点，直到接收到接受消息。

[0083] 找到尚未接收到该区块头的其它业务节点中、离发送节点最近的业务节点的另一种实施方式是维护一个分发进度记录服务器。每当一个其它业务节点接收到区块头后，就向分发进度记录服务器发出一个记录请求，记录请求中含有该业务节点的标识和区块头的标识(例如其中的默克尔树根)，分发进度记录服务器将该业务节点的标识和区块头的标识对应存储。当发送节点需要确定尚未接收到该区块头的其它业务节点中、离发送节点最近的业务节点时，先向分发进度记录服务器发请求，由分发进度记录服务器查询业务节点子网络中未接收到该区块头的业务节点的标识(从所有业务节点的标识列表中去除已与区块头的标识对应存储的业务节点标识)，发送给发送节点。发送节点在这些未接收到该区块头的业务节点中确定离发送节点距离最小的业务节点。相比而言，通过上述向距离最近的其它业务节点发送区块头，让接收到区块头的其它业务节点根据自己是否之前接收到该区块头来发送接受消息或拒绝消息的方式，少设置了一个服务器，节省网络资源，避免网络拥塞。

[0084] 继续参照图4所示，在步骤S420中，若接收到所述业务节点子网络中的目标业务节点对指定数据区块中包含的交易数据的获取请求，则获取所述目标业务节点的权限信息。

[0085] 在本申请的实施例中，业务节点的权限信息是指表示业务节点有权获得数据区块中哪些交易数据、无权获得哪些交易数据的信息。在本申请的一个实施例中，权限信息中的权限包括以下中的一种或多种：

[0086] 允许查看的交易数据所对应的请求上链业务节点；

[0087] 允许查看的交易数据所对应的交易类型；

[0088] 允许查看的交易数据所对应的上链时间。

[0089] 其中，允许查看的交易数据所对应的请求上链业务节点是指允许查看哪些业务节点请求上链的交易数据的权限。在本申请的一个实施例中，可以规定一个业务节点只能查看自己请求上链的交易数据。假设有一个业务节点A，可能其权限消息中规定允许查看的交易数据所对应的请求上链业务节点就是业务节点A本身，这样只有业务节点A本身请求上链的数据区块才能够被业务节点A查看。在另一个实施例中，可以规定一个业务节点可以查看其自己及其下属所有单位的业务节点请求上链的交易数据。例如，有一个业务节点A，其下属单位的业务节点有A1-A7，这样，业务节点A允许查看的交易信息所对应的请求上链业务节点就是业务节点A和业务节点A1-A7，进而业务节点A和业务节点A1-A7中任一个业务节点请求上链的数据区块都能够被业务节点A查看。

[0090] 允许查看的交易数据所对应的交易类型是指允许查看哪些交易类型的交易数据的权限。在数据区块的交易数据中携带有交易类型。交易类型例如可以是发票交易、供应链金融交易、法定数字货币交易等。在发票交易中，可能地方税务机构的业务节点被允许查看其管辖范围内的所有关于发票的交易数据，因此可以将数据区块中关于发票的交易数据全部向其返回，对于数据区块中其它类型的交易数据仅向其返回哈希值。在供应链金融交易中，可能银行的业务节点被允许查看其管辖范围内的所有关于供应链金融的交易数据，因此可以将数据区块中关于供应链金融的交易数据全向其返回，对于数据区块中其它类型的交易数据仅向其返回哈希值。在法定数字货币交易中，可能法定数字货币的发行机关的业务节点被允许查看其管辖范围内的所有关于法定数字货币流转的交易数据，因此可以将数据区块中关于法定数字货币的交易数据全向其返回，对于数据区块中其它类型的交易数据仅向其返回哈希值。

[0091] 允许查看的交易数据所对应的上链时间是指允许查看哪个时间段上链的交易数据的权限。例如，可以规定业务节点A只能查看最近一年之内上链的交易数据。

[0092] 上述几种权限也可以组合使用。例如，可以将允许查看的交易数据所对应的请求上链业务节点、允许查看的交易数据所述对应的上链时间组合使用。假设有一个业务节点A，其下属单位的业务节点有A1-A7，其权限数据中可能规定：业务节点A可以获得最近一年之内上链的业务节点A、业务节点A1-A7的交易数据。

[0093] 在本申请的一个实施例中，可以根据目标业务节点发送的获取请求中包含的目标业务节点的标识信息，获取目标业务节点的认证信息，然后基于该认证信息获取目标业务节点的权限信息。其中，业务节点的认证信息可以是业务节点事先通过注册获取到的信息，比如业务节点可以向记账节点子网络发送注册请求，然后记账节点子网络可以获取到与该业务节点对应的入网合约，该入网合约中含有该业务节点的认证信息及权限信息，进而将该入网合约加入数据区块并添加到区块链上。由于区块链上的数据区块中所有内容对于记账节点都是完全可见的，因此记账节点在接收到业务节点对该数据区块中的交易数据的请求后，根据请求的业务节点的标识信息，就可以在区块链中找到与该业务节点的标识信息对应存储的入网合约，进而从中读取权限信息。

[0094] 继续参照图4所示，在步骤S430中，根据所述目标业务节点的权限信息，将所述指

定数据区块中包含的所述目标业务节点有权获取的交易数据返回至所述目标业务节点。

[0095] 在本申请的实施例中，在生成数据区块后，记账节点仅把区块头发到业务节点子网络的各业务节点，各业务节点无法获取到数据区块中的区块体中的各交易数据，实现了交易数据的隐藏。当业务节点想要获取到数据区块中的交易数据时，需要向记账节点发送对数据区块中的交易数据的获取请求，而记账节点只把业务节点有权查看的交易数据(例如与其相关的交易数据、或与其下属单位相关的交易数据)发送给其查看，对于那些无权查看的交易数据(例如与其它业务节点相关的交易数据)，禁止其查看，进而使得业务节点既能够获知与其相关的交易数据，又能够避免其它业务节点相关的交易数据遭到泄露的问题。

[0096] 在本申请的一个实施例中，还可以将上述指定数据区块中包含的该目标业务节点无权获取的交易数据的哈希值返回至该目标业务节点，以使该目标业务节点根据其有权获取的交易数据和其无权获取的交易数据的哈希值计算默克尔树根，以对获取到的交易数据进行验证。

[0097] 在本申请的一个实施例中，如图9所示，根据一个数据区块中所包含的交易数据生成默克尔树根的过程具体可以包括如下步骤：

[0098] 步骤S910，计算数据区块中的每个交易数据的哈希值；

[0099] 步骤S920，将数据区块中的交易数据进行排序(比如可以按照进入缓存的顺序来进行排序)，顺序排在第奇数位的交易数据和之后的顺序排在第偶数位的交易数据组成一个对；

[0100] 步骤S930，将每个对的两个交易数据的哈希值进行哈希运算，得到该对的哈希值；

[0101] 步骤S940，将各个对进行排序(比如按照各个对进入缓存的顺序进行排序)，顺序排在第奇数位的对和之后的顺序排在第偶数位的对组成一个更上一级的对，将每个更上一级的对中的两个对的哈希值进行哈希运算，得到该更上一层的对的哈希值，直到得到最上一层的对的哈希值，即为默克尔树根。

[0102] 需要注意的是，在本申请的另一个实施例中，如果顺序排在第奇数位的交易信息是缓存中最后一个交易信息，则对该交易信息进行复制，该最后一个交易信息和复制后的该交易信息以构成一个对；如果顺序排在第奇数位的对是缓存中最后一个对，将该对进行复制，该最后一个对和复制后的对以构成一个更上一级的对，按照这种方式得到的默克尔树为二叉树。例如，数据区块中有9条交易数据，按进入缓存的时间顺序分别是A1-A9。A1-A2组成一个对B1，对A1的哈希值和A2的哈希值进行哈希运算，得到B1的哈希值；A3-A4组成一个对B2，对A3的哈希值和A4的哈希值进行哈希运算，得到B2的哈希值；A5-A6组成一个对B3，对A5的哈希值和A6的哈希值进行哈希运算，得到B3的哈希值；A7-A8组成一个对B4，对A7的哈希值和A8的哈希值进行哈希运算，得到B4的哈希值；将A9复制一份得到A10，对A9的哈希值和A10的哈希值进行哈希值运算，得到B5的哈希值。

[0103] 针对B1-B5而言，B1-B2组成一个更上层的对C1，对B1的哈希值和B2的哈希值进行哈希运算，得到C1的哈希值；B3-B4组成一个更上层的对C2，对B3的哈希值和B4的哈希值进行哈希运算，得到C2的哈希值；将B5复制一份得到B6，对B5的哈希值和B6的哈希值进行哈希值运算，得到C3的哈希值。

[0104] 针对C1-C3而言，C1-C2组成一个更上层的对D1，对C1的哈希值和C2的哈希值进行

哈希运算，得到D1的哈希值；将C3复制一份得到C4，对C3的哈希值和C4的哈希值进行哈希值运算，得到D2的哈希值。

[0105] 针对D1-D2而言，对D1的哈希值和D2的哈希值进行哈希运算，得到默克尔树根。

[0106] 由上述默克尔树根的计算方式可知，如果不知道数据区块中的一些交易数据，但指定这些交易数据的哈希值，同样可以计算出上述默克尔树根。当业务节点计算出的默克尔树根之后，可以与记账节点返回的数据区块的区块头中包含的默克尔树根进行比对，进而可以进行内容验证。如果两个默克尔树根一致，则说明记账节点返回的交易数据没有被篡改；如果两个默克尔树根不一致，则说明记账节点返回的交易数据中可能被篡改了一部分，通过这种方式使得业务节点能够对其获取到的交易数据进行验证，确保了业务节点获取到准确合法的交易数据。

[0107] 在本申请的一个实施例中，业务节点子网络中的各个业务节点之间可能具有层级关系。比如税务总局的下级包括各个省税局；省税局的下级包括各个市税局；市税局的下级包括各个区税局；区税局的下级包括企业、个人、开票代理服务商等；开票代理服务商的下级包括其代理的企业或个人等。由于这种层级关系，使得不同层级的业务节点可访问的信息不相同，比如税务总局可以查询全量的电子发票信息、省税局可以查看本省的电子发票信息、市税局可以查看全市的电子发票信息、个人或企业仅可查看与自己相关的电子发票信息、开票代理服务商可以查看其代理的企业或个人的电子发票信息等。

[0108] 在相关技术中，由于上述层级关系的存在，使得上级业务节点需要维护与下级业务节点之间的关系。比如开票代理服务商需要维护其代理的企业或个人的信息，假设开票代理服务商的数量为n，各个开票代理服务商维护的企业或个人的数量为m，那么会产生一个m×n大小的关系表，随着n和m的增加，该关系表的数据大小将会倍增。为了解决这个问题，本申请实施例中提出了对业务节点的地址结构进行改进的技术方案，即在业务节点的地址信息中添加其所属的上级节点的标识信息和上级节点的签名信息，具体如图10所示，业务节点的地址信息包括父级编号、自身的公钥哈希和父级签名。其中，父级编号表示该业务节点所属的上级节点的标识信息；自身的公钥哈希表示该业务节点自身的标识信息；父级签名表示该业务节点所属的上级节点的签名信息，该签名信息用于对该业务节点的身份进行验证。

[0109] 基于上述的地址结构，在本申请的一个实施例中，目标业务节点可以在对指定数据区块中包含的交易数据的获取请求中添加其地址信息，进而记账节点在接收到该获取请求之后，可以根据该获取请求中所包含的地址信息，确定该目标业务节点所属的上级节点，并根据该目标业务节点所属的上级节点对该获取请求中所包含的签名信息进行验证，若对该获取请求中所包含的签名信息验证通过，则基于该目标业务节点的权限信息，在该目标业务节点所属的上级节点对应的数据中查询并获取该目标业务节点有权获取的交易数据。可见，本申请实施例中通过改进业务节点的地址结构，使得无需维护上级节点与下级节点之间的关系表，进而能够减少关系表的存储成本。

[0110] 图11示意性示出了根据本申请的一个实施例的区块链系统的数据管理方法的流程图，如图1至图3所示，该区块链系统包括记账节点子网络2和业务节点子网络1，记账节点子网络2包括记账节点21，业务节点子网络1包括业务节点11。图11所示的区块链系统的数据管理方法可以由业务节点子网络1中的业务节点11来执行。参照图11所示，该区块链系统

的数据管理方法至少包括步骤S1110至步骤S1130，详细介绍如下：

[0111] 在步骤S1110中，获取记账节点子网络发布至业务节点子网络中的区块头。

[0112] 其中，记账节点子网络生成数据区块的过程，以及将数据区块的区块头发布至业务节点子网络中的过程已经在上述实施例中进行了详细阐述，不再赘述。

[0113] 在步骤S1120中，根据所述记账节点子网络发布的所述区块头，向所述记账节点子网络中的目标记账节点发送对指定数据区块中包含的交易数据的获取请求。

[0114] 在本申请的一个实施例中，业务节点在接收到记账节点子网络发布的区块头之后，可以根据该区块头确定记账节点子网络中产生了新的数据区块，进而可以向目标记账节点发送对指定数据区块中包含的交易数据的获取请求。其中，目标记账节点可以是记账节点子网络中的任意一个记账节点，也可以是记账节点子网络中距离发送获取请求的业务节点最近的一个记账节点，还可以是与发送获取请求的业务节点相对应的一个记账节点。

[0115] 在步骤S1130中，接收所述目标记账节点根据所述获取请求返回的所述指定数据区块中所述目标业务节点有权获取的交易数据。

[0116] 其中，记账节点在接收到业务节点发送的获取请求之后，可以获取到该业务节点的权限信息，进而根据该权限信息获取到该业务节点有权获取的交易数据，这个过程已经在上述实施例中进行了阐述，因此不再赘述。

[0117] 在本申请的一个实施例中，业务节点在接收到指定数据区块中包含的其有权获取的交易数据之后，还可以接收目标记账节点返回的该指定数据区块中包含的其无权获取的交易数据的哈希值，然后根据其有权获取的交易数据和其无权获取的交易数据的哈希值，计算默克尔树根，进而将计算出的默克尔树根和该指定数据区块的区块头中所包含的默克尔树根进行比较，以对接收到的交易数据进行验证。其中，生成默克尔树根的过程已经在上述实施例中进行了阐述，在此不再赘述。

[0118] 在本申请的一个实施例中，由于业务节点之间可能存在层级关系，因此上级业务节点也可以响应下级业务节点发送的交易数据获取请求，具体如图12所示，包括如下步骤：

[0119] 步骤S1210，若接收到与所述目标业务节点存在层级关系且位于所述目标业务节点的下一层级的其它业务节点发送的对目标数据区块中的交易数据的获取请求，则确定所述其它业务节点有权获取的交易数据。

[0120] 在本申请的一个实施例中，目标业务节点确定其它业务节点有权获取的交易数据的过程与上述实施例中记账节点确定业务节点有权获取的交易数据的过程类似，即目标业务节点可以根据其它业务节点发送的获取请求确定其它业务节点的权限信息，进而根据该权限信息确定其它业务节点有权获取的交易数据。并且其它业务节点也可以采用本申请上述实施例中所提出的地址结构，以便于目标业务节点查询该其它业务节点有权获取的交易数据，具体的处理过程请参照上述实施例，在此不再赘述。

[0121] 步骤S1220，将所述目标数据区块中包含的所述其它业务节点有权获取的交易数据发送至所述其它业务节点。

[0122] 在本申请的一个实施例中，在将目标数据区块中包含的其他业务节点有权获取的交易数据发送至其它业务节点之后，还可以将该目标数据区块中包含的该其它业务节点无权获取的交易数据的哈希值返回至该其它业务节点，以使该其它业务节点根据其有权获取的交易数据和其无权获取的交易数据的哈希值计算默克尔树根，以对获取到的交易数据进

行验证。具体可以将计算出的默克尔树根和该目标数据区块的区块头中所包含的默克尔树根进行比较，以对接收到的交易数据进行验证。其中，生成默克尔树根的过程已经在上述实施例中进行了阐述，在此不再赘述。

[0123] 本申请上述实施例的技术方案分别从记账节点子网络中的记账节点的角度和业务节点子网络中的业务节点的角度对本申请实施例的技术方案进行了详细阐述，本申请实施例的技术方案通过将区块链系统分为记账节点子网络和业务节点子网络，使得能够将区块链系统的记账过程与业务处理过程进行分离，进而既能够通过记账节点子网络来维护全量的数据区块，保证数据区块的安全性，又能够通过业务节点子网络来实现灵活的数据访问，比如分层级的不同权限的数据访问等。而通过由记账节点将生成的数据区块的区块头发布至业务节点子网络，以向业务节点子网络通知新生成的数据区块的信息，使得业务节点子网络中的业务节点既能够获知共识节点子网络中新生成的数据区块，又能够避免将整个数据区块全部发送至业务节点子网络而导致数据区块中的交易数据被泄露的问题。此外，记账节点通过在接收到目标业务节点对指定数据区块中包含的交易数据的获取请求时，根据该目标业务节点的权限信息，将该指定数据区块中包含的目标业务节点有权获取的交易数据返回至目标业务节点，使得能够实现对各个业务节点的权限进行控制，实现了更加灵活的数据访问方式。其中，业务节点子网络中的业务节点既可以直接向记账节点子网络中的记账节点发送交易数据获取请求，也可以向其在业务节点子网络中的上级节点(包括直接上级节点和间接上级节点)发送交易数据获取请求。

[0124] 以下介绍本申请的装置实施例，可以用于执行本申请上述实施例中的区块链系统的数据管理方法。对于本申请装置实施例中未披露的细节，请参照本申请上述的区块链系统的数据管理方法的实施例。

[0125] 图13示意性示出了根据本申请的一个实施例的区块链系统的数据管理装置的框图。如图1至图3所示，该区块链系统包括记账节点子网络2和业务节点子网络1，记账节点子网络2包括记账节点21，业务节点子网络1包括业务节点11。其中，记账节点子网络2中的记账节点21可以包括图13所示的区块链系统的数据管理装置1300。

[0126] 参照图13所示，根据本申请的一个实施例的区块链系统的数据管理装置1300，包括：发布单元1302、获取单元1304和处理单元1306。

[0127] 其中，发布单元1302用于在生成数据区块后，将生成的数据区块的区块头发布至所述业务节点子网络，以向所述业务节点子网络通知新生成的数据区块的信息；获取单元1304用于在接收到所述业务节点子网络中的目标业务节点对指定数据区块中包含的交易数据的获取请求时，获取所述目标业务节点的权限信息；处理单元1306用于根据所述目标业务节点的权限信息，将所述指定数据区块中包含的所述目标业务节点有权获取的交易数据返回至所述目标业务节点。

[0128] 在本申请的一个实施例中，发布单元1302配置为：将所述区块头发送至所述业务节点子网络中的指定业务节点；通过所述指定业务节点将所述区块头广播至所述业务节点子网络中的其它业务节点。

[0129] 在本申请的一个实施例中，发布单元1302配置为：将所述区块头发送至所述业务节点子网络中的指定业务节点；以所述指定业务节点作为发送节点将所述区块头发送至离所述发送节点最近的业务节点，并将接收到所述区块头的业务节点作为发送节点继续进行

发送，直至所述业务节点子网络中的业务节点均接收到所述区块头。

[0130] 在本申请的一个实施例中，发布单元1302配置为：确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离；将所述区块头发送至与所述发送节点最近的业务节点，其中，若接收到所述区块头的业务节点之前已经接收到所述区块头，则向所述发送节点反馈拒绝消息；若接收到所述拒绝消息，则根据所述距离由近至远的顺序继续将所述区块头发送至其它业务节点，直至接收到接受消息。

[0131] 在本申请的一个实施例中，获取单元1304配置为：根据所述获取请求中包含的所述目标业务节点的标识信息，获取所述目标业务节点的认证信息；基于所述认证信息获取所述目标业务节点的权限信息。

[0132] 在本申请的一个实施例中，处理单元1306还用于：将所述指定数据区块中包含的所述目标业务节点无权获取的交易数据的哈希值返回至所述目标业务节点，以使所述目标业务节点根据其有权获取的交易数据和所述无权获取的交易数据的哈希值计算默克尔树根，以对获取到的交易数据进行验证。

[0133] 在本申请的一个实施例中，所述获取请求中包含有所述目标业务节点的地址信息，所述地址信息中包含有所述目标业务节点的标识信息、所述目标业务节点所属的上级节点的标识信息和所述上级节点的签名信息；所述处理单元1306还用于：根据所述获取请求中所包含的地址信息，确定所述目标业务节点所属的上级节点，并根据所述目标业务节点所属的上级节点对所述获取请求中所包含的签名信息进行验证；若对所述获取请求中所包含的签名信息验证通过，则基于所述目标业务节点的权限信息，在所述目标业务节点所属的上级节点对应的数据中查询并获取所述目标业务节点有权获取的交易数据。

[0134] 图14示意性示出了根据本申请的一个实施例的区块链系统的数据管理装置的框图。如图1至图3所示，该区块链系统包括记账节点子网络2和业务节点子网络1，记账节点子网络2包括记账节点21，业务节点子网络1包括业务节点11。其中，业务节点子网络1中的业务节点11可以包括图14所示的区块链系统的数据管理装置1400。

[0135] 参照图14所示，根据本申请的一个实施例的区块链系统的数据管理装置1400，包括：获取单元1402、发送单元1404和接收单元1406。

[0136] 其中，获取单元1402用于获取所述记账节点子网络发布至所述业务节点子网络中的区块头；发送单元1404用于根据所述记账节点子网络发布的所述区块头，向所述记账节点子网络中的目标记账节点发送对指定数据区块中包含的交易数据的获取请求；接收单元1406用于接收所述目标记账节点根据所述获取请求返回的所述指定数据区块中所述目标业务节点有权获取的交易数据。

[0137] 在本申请的一个实施例中，所述的区块链系统的数据管理装置1400还包括：处理单元；所述接收单元还用于接收所述目标记账节点返回的所述指定数据区块中所述目标业务节点无权获取的交易数据的哈希值；所述处理单元配置为：根据所述有权获取的交易数据和所述无权获取的交易数据的哈希值，计算默克尔树根，将计算出的所述默克尔树根和所述指定数据区块的区块头中所包含的默克尔树根进行比较，以对接收到的交易数据进行验证。

[0138] 在本申请的一个实施例中，所述的区块链系统的数据管理装置1400还包括：确定单元，用于在接收到与所述目标业务节点存在层级关系且位于所述目标业务节点的下一层

级的其它业务节点发送的对目标数据区块中的交易数据的获取请求时，确定所述其它业务节点有权获取的交易数据；所述发送单元1404还用于将所述目标数据区块中包含的所述其它业务节点有权获取的交易数据发送至所述其它业务节点。

[0139] 在本申请的一个实施例中，发送单元1404还用于：将所述目标数据区块中包含的所述其它业务节点无权获取的交易数据的哈希值返回至所述其它业务节点，以使所述其它业务节点根据其有权获取的交易数据和所述无权获取的交易数据的哈希值计算默克尔树根，以对获取到的交易数据进行验证。

[0140] 图15示出了适于用来实现本申请实施例的电子设备的计算机系统的结构示意图。

[0141] 需要说明的是，图15示出的电子设备的计算机系统1500仅是一个示例，不应对本申请实施例的功能和使用范围带来任何限制。

[0142] 如图15所示，计算机系统1500包括中央处理单元(Central Processing Unit，CPU)1501，其可以根据存储在只读存储器(Read-Only Memory，ROM)1502中的程序或者从存储部分1508加载到随机访问存储器(Random Access Memory，RAM)1503中的程序而执行各种适当的动作和处理。在RAM 1503中，还存储有系统操作所需的各种程序和数据。CPU 1501、ROM 1502以及RAM 1503通过总线1504彼此相连。输入/输出(Input/Output，I/O)接口1505也连接至总线1504。

[0143] 以下部件连接至I/O接口1505：包括键盘、鼠标等的输入部分1506；包括诸如阴极射线管(Cathode Ray Tube，CRT)、液晶显示器(Liquid Crystal Display，LCD)等以及扬声器等的输出部分1507；包括硬盘等的存储部分1508；以及包括诸如LAN(Local Area Network，局域网)卡、调制解调器等的网络接口卡的通信部分1509。通信部分1509经由诸如因特网的网络执行通信处理。驱动器1510也根据需要连接至I/O接口1505。可拆卸介质1511，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器1510上，以便于从其上读出的计算机程序根据需要被安装入存储部分1508。

[0144] 特别地，根据本申请的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本申请的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分1509从网络上被下载和安装，和/或从可拆卸介质1511被安装。在该计算机程序被中央处理单元(CPU)1501执行时，执行本申请的系统中限定的各种功能。

[0145] 需要说明的是，本申请实施例所示的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(Erasable Programmable Read Only Memory，EPROM)、闪存、光纤、便携式紧凑磁盘只读存储器(Compact Disc Read-Only Memory，CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中，计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其

中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线、有线等等，或者上述的任意合适的组合。

[0146] 附图中的流程图和框图，图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，上述模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图或流程图中的每个方框、以及框图或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0147] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现，也可以通过硬件的方式来实现，所描述的单元也可以设置在处理器中。其中，这些单元的名称在某种情况下并不构成对该单元本身的限定。

[0148] 作为另一方面，本申请还提供了一种计算机可读介质，该计算机可读介质可以是上述实施例中描述的电子设备中所包含的；也可以是单独存在，而未装配入该电子设备中。上述计算机可读介质承载有一个或者多个程序，当上述一个或者多个程序被一个该电子设备执行时，使得该电子设备实现上述实施例中所述的方法。

[0149] 应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本申请的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

[0150] 通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本申请实施方式的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质(可以是CD-ROM，U盘，移动硬盘等)中或网络上，包括若干指令以使得一台计算设备(可以是个人计算机、服务器、触控终端、或者网络设备等)执行根据本申请实施方式的方法。

[0151] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本申请的其它实施方案。本申请旨在涵盖本申请的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本申请的一般性原理并包括本申请未公开的本技术领域中的公知常识或惯用技术手段。

[0152] 应当理解的是，本申请并不局限于上面已经描述并在附图中示出的精确结构，并且可以在不脱离其范围进行各种修改和改变。本申请的范围仅由所附的权利要求来限制。

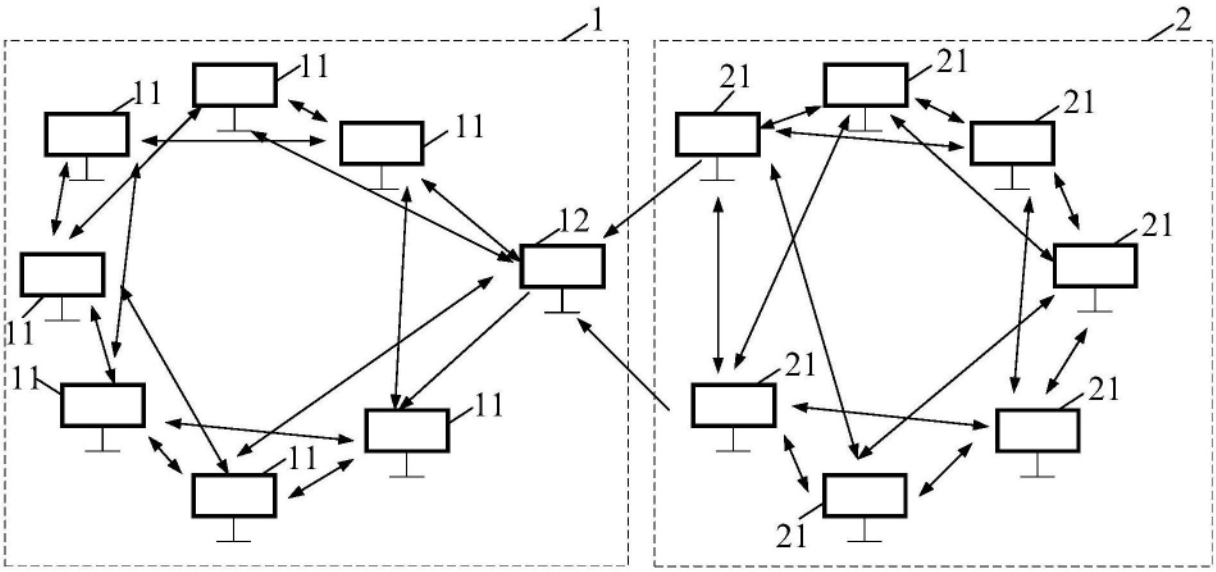


图1

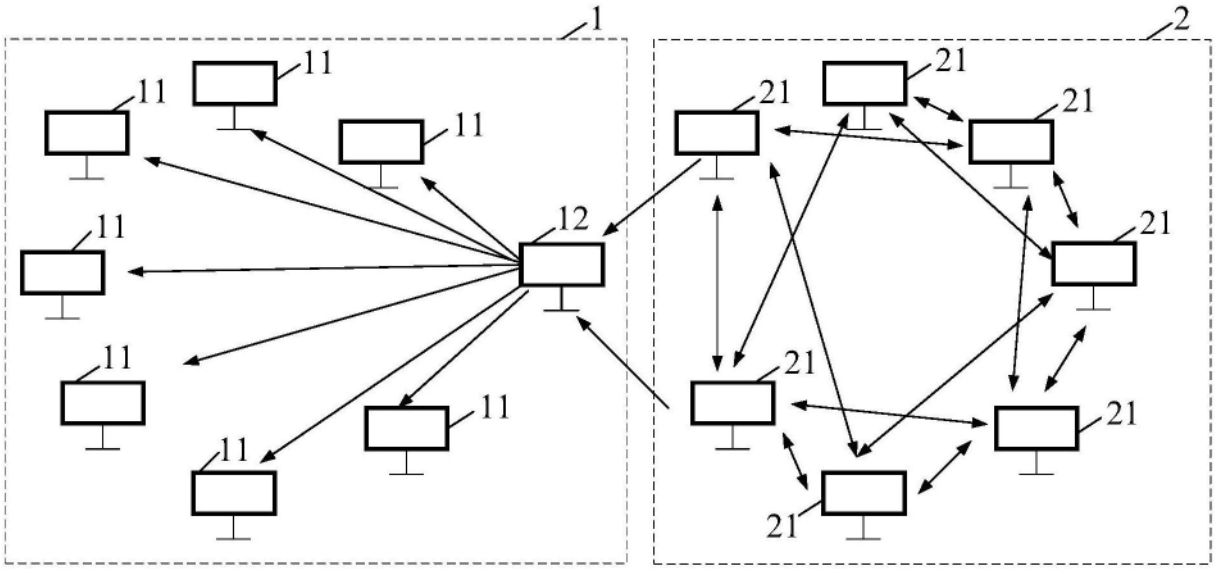


图2

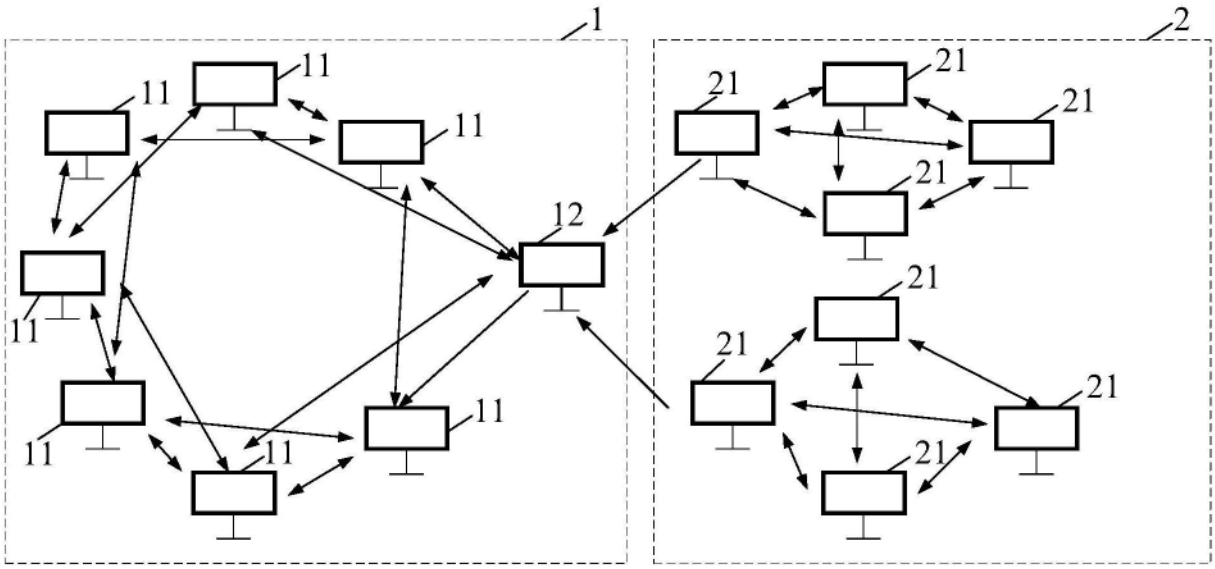

1
2
11
12
21

图3

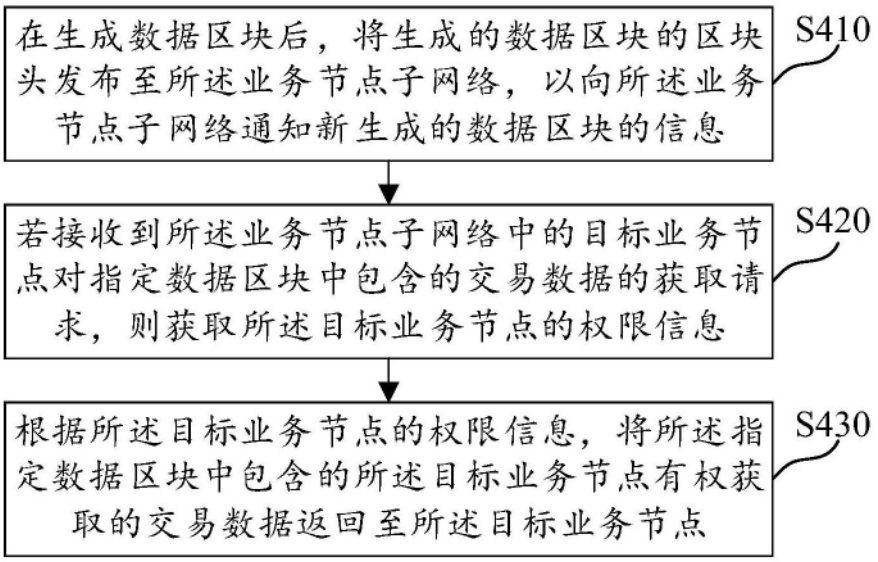

在生成数据区块后，将生成的数据区块的区块头发布至所述业务节点子网络，以向所述业务节点子网络通知新生成的数据区块的信息
S410
若接收到所述业务节点子网络中的目标业务节点对指定数据区块中包含的交易数据的获取请求，则获取所述目标业务节点的权限信息
S420
根据所述目标业务节点的权限信息，将所述指定数据区块中包含的所述目标业务节点有权获取的交易数据返回至所述目标业务节点
S430

图4

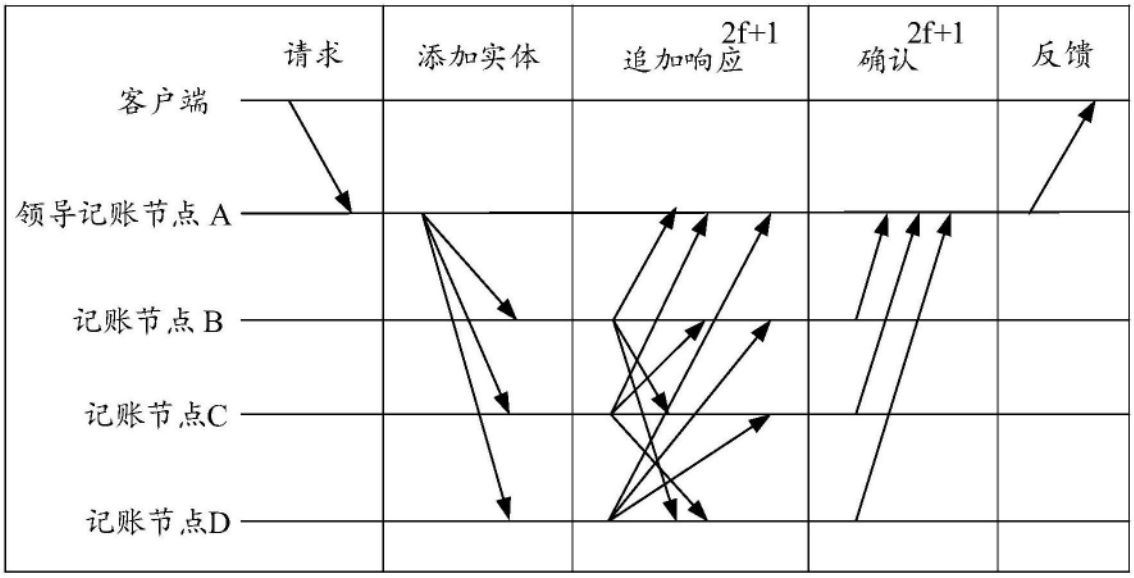

请求
添加实体
2f+1
追加响应
2f+1
确认
反馈
客户端
领导记账节点 A
记账节点 B
记账节点C
记账节点D

图5

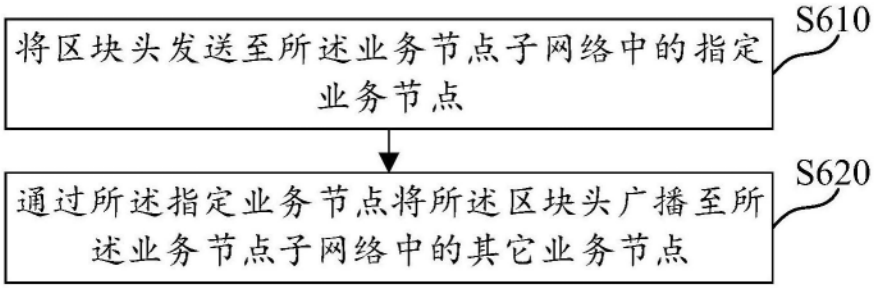

将区块头发送至所述业务节点子网络中的指定业务节点
S610
通过所述指定业务节点将所述区块头广播至所述业务节点子网络中的其它业务节点
S620

图6

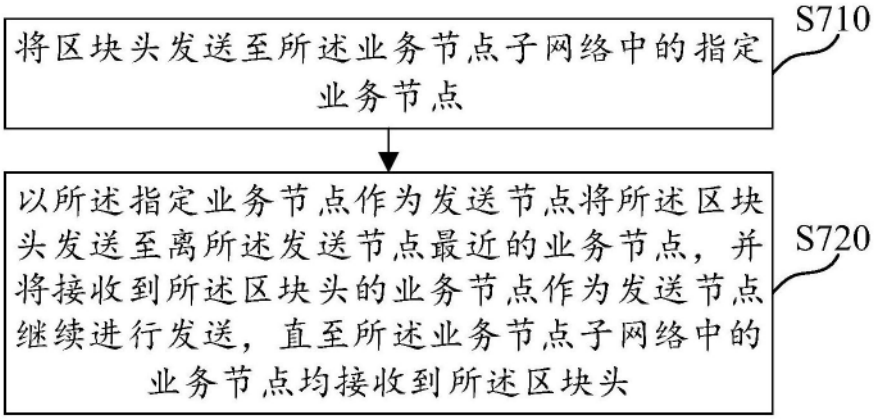

将区块头发送至所述业务节点子网络中的指定业务节点
S710
以所述指定业务节点作为发送节点将所述区块头发送至离所述发送节点最近的业务节点，并将接收到所述区块头的业务节点作为发送节点继续进行发送，直至所述业务节点子网络中的业务节点均接收到所述区块头
S720

图7

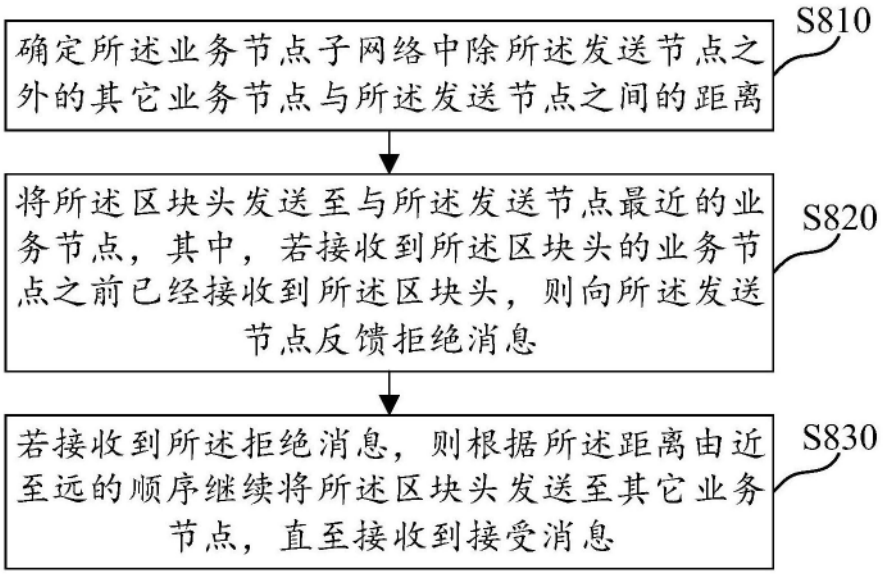

S810
确定所述业务节点子网络中除所述发送节点之外的其它业务节点与所述发送节点之间的距离
S820
将所述区块头发送至与所述发送节点最近的业务节点，其中，若接收到所述区块头的业务节点之前已经接收到所述区块头，则向所述发送节点反馈拒绝消息
S830
若接收到所述拒绝消息，则根据所述距离由近至远的顺序继续将所述区块头发送至其它业务节点，直至接收到接受消息

图8

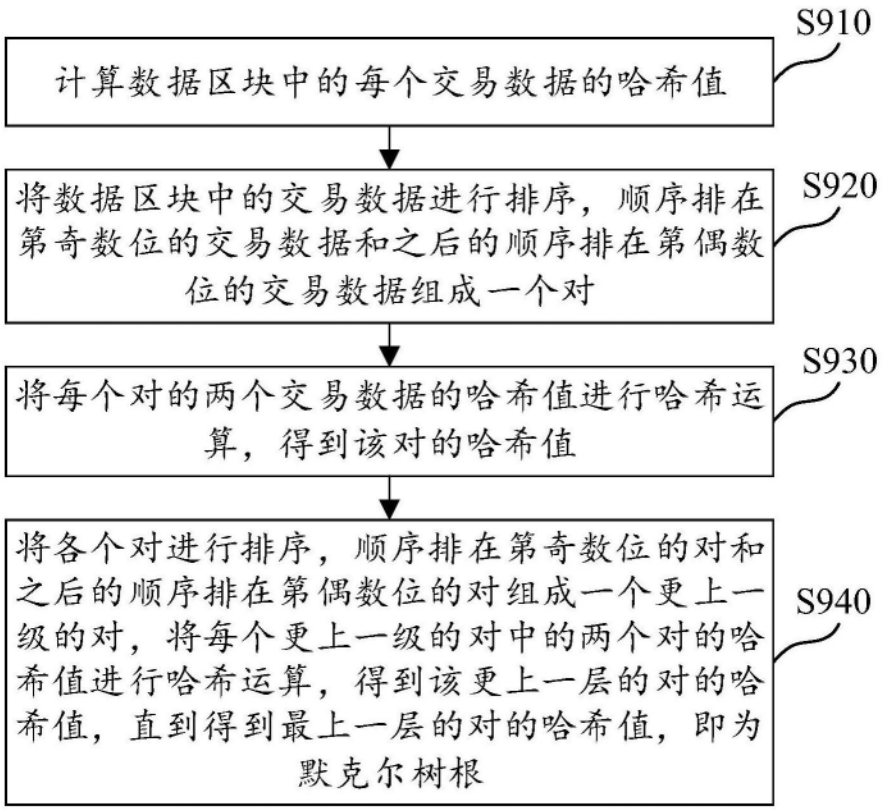

S910
计算数据区块中的每个交易数据的哈希值
S920
将数据区块中的交易数据进行排序，顺序排在第奇数位的交易数据和之后的顺序排在第偶数位的交易数据组成一个对
S930
将每个对的两个交易数据的哈希值进行哈希运算，得到该对的哈希值
S940
将各个对进行排序，顺序排在第奇数位的对和之后的顺序排在第偶数位的对组成一个更上一级的对，将每个更上一级的对中的两个对的哈希值进行哈希运算，得到该更上一层的对的哈希值，直到得到最上一层的对的哈希值，即为默克尔树根

图9

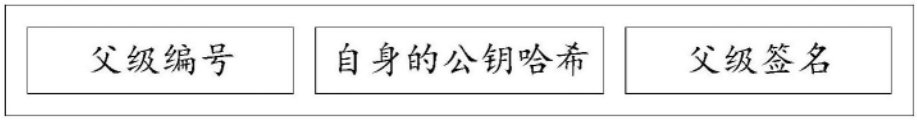

父级编号
自身的公钥哈希
父级签名

图10

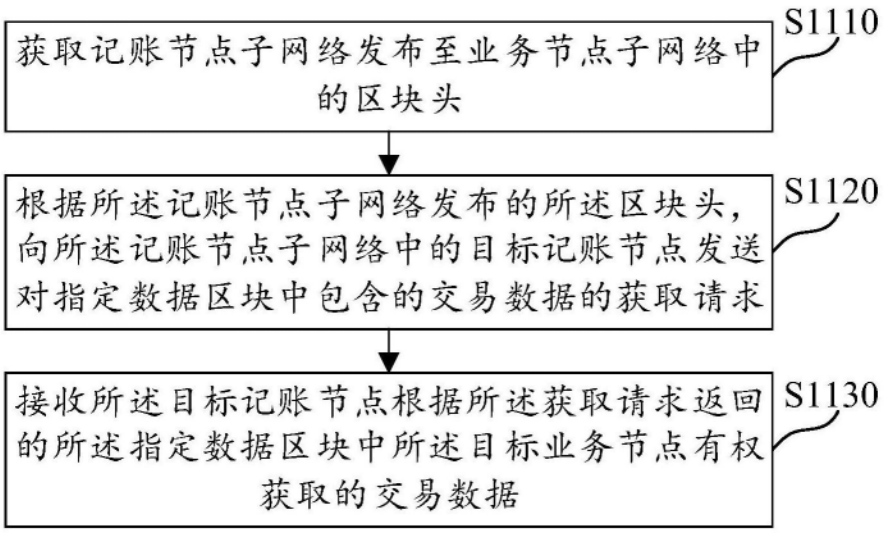

获取记账节点子网络发布至业务节点子网络中的区块头
S1110
根据所述记账节点子网络发布的所述区块头，向所述记账节点子网络中的目标记账节点发送对指定数据区块中包含的交易数据的获取请求
S1120
接收所述目标记账节点根据所述获取请求返回的所述指定数据区块中所述目标业务节点有权获取的交易数据
S1130

图11

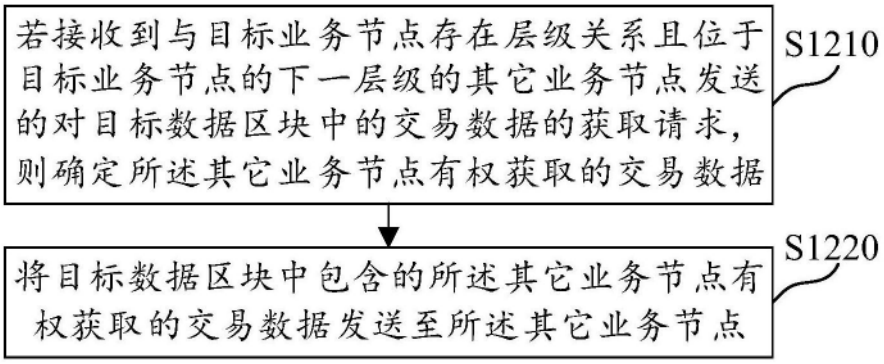

若接收到与目标业务节点存在层级关系且位于目标业务节点的下一层级的其它业务节点发送的对目标数据区块中的交易数据的获取请求，则确定所述其它业务节点有权获取的交易数据
S1210
将目标数据区块中包含的所述其它业务节点有权获取的交易数据发送至所述其它业务节点
S1220

图12

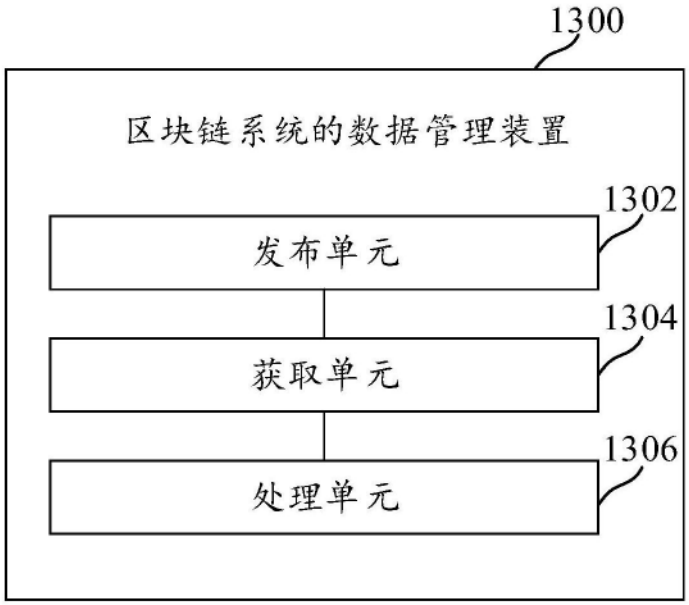

1300
区块链系统的数据管理装置
1302
发布单元
1304
获取单元
1306
处理单元

图13

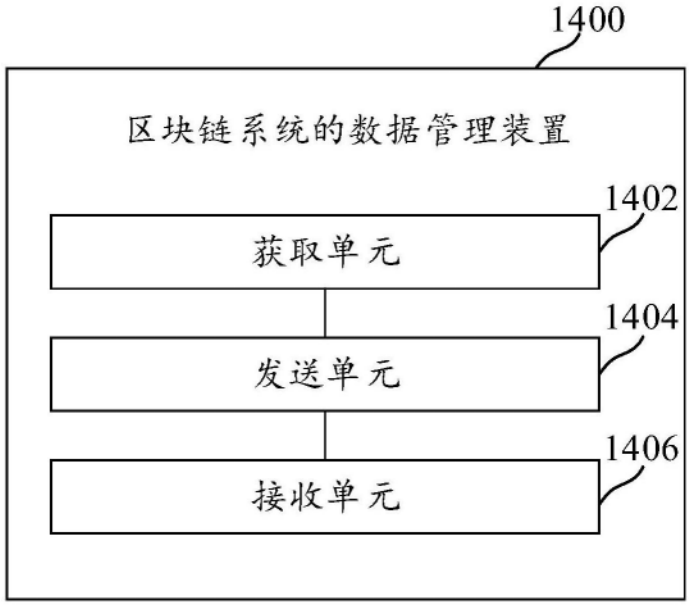

1400
区块链系统的数据管理装置
1402
获取单元
1404
发送单元
1406
接收单元

图14

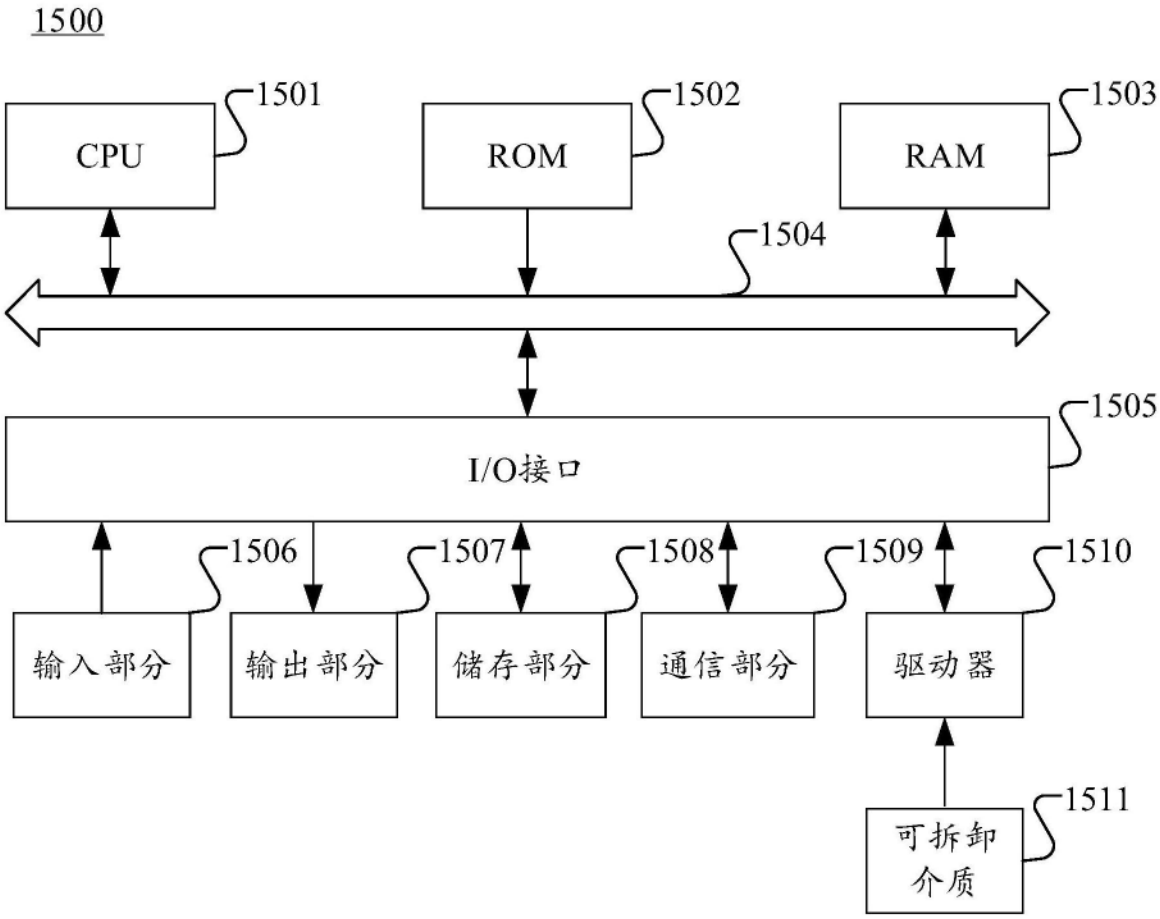

1500
CPU
1501
ROM
1502
RAM
1503
1504
I/O接口
1505
输入部分
1506
输出部分
1507
储存部分
1508
通信部分
1509
驱动器
1510
可拆卸介质
1511

图15