(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110851496 A
(43)申请公布日 2020.02.28

(21)申请号 201911031824.4

(22)申请日 2018.12.07

(62)分案原申请数据
201811495810.3 2018.12.07

(71)申请人 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 杨常青 周开班 时一防 蓝虎 张劲松 丁勇 刘区城 朱耿良 陈秋平

(74)专利代理机构 深圳市隆天联鼎知识产权代理有限公司 44232
代理人 王鹏健

(51)Int.Cl.
G06F 16/2458(2019.01)
G06F 16/27(2019.01)
G06Q 40/04(2012.01)
G06F 21/60(2013.01)
G06F 21/62(2013.01)
H04L 9/32(2006.01)

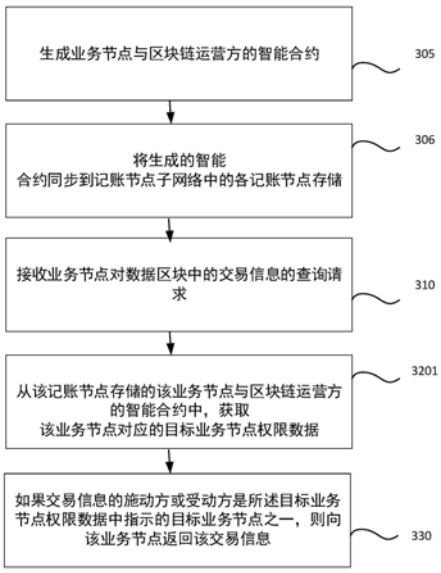
权利要求书3页 说明书24页 附图27页

(54)发明名称

在区块链网络中查询交易信息的方法、装置、记账节点和介质

(57)摘要

本公开提供了一种在区块链网络中查询交易信息的方法、装置、记账节点和介质。区块链网络包括记账节点子网络和业务节点子网络。所述方法由记账节点子网络中的记账节点执行，所述方法包括：生成业务节点与区块链运营方的智能合约；将生成的智能合约同步到记账节点子网络中的各记账节点存储；接收业务节点对数据区块中的交易信息的查询请求；从记账节点存储的业务节点与区块链运营方的智能合约中，获取业务节点对应的目标业务节点权限数据；若交易信息的施动方或受动方是目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。本公开使得查询区块链上交易信息的用户只能查询到与自己相关的交易信息，从而防止交易信息外泄。



CN 110851496 A

1.一种在区块链网络中查询数据区块中的交易信息的方法,其特征在于,所述区块链网络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,所述方法由记账节点子网络中的一个记账节点执行,所述方法包括:

生成业务节点与区块链运营方的智能合约;

将生成的智能合约同步到记账节点子网络中的各记账节点存储;

接收业务节点对数据区块中的交易信息的查询请求;

从所述记账节点存储的所述业务节点与区块链运营方的智能合约中,获取所述业务节点对应的目标业务节点权限数据;

如果所述交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一,则向所述业务节点返回所述交易信息。

2.根据权利要求1所述的方法,其特征在于,生成业务节点与区块链运营方的智能合约,包括:

发布合约模板,所述合约模板中含有合约函数;

接收利用所述合约函数设置的该业务节点的目标业务节点权限数据;

将所述目标业务节点权限数据整合到所述合约模板中,形成该业务节点与区块链运营方的智能合约。

3.根据权利要求1所述的方法,其特征在于,生成业务节点与区块链运营方的智能合约,包括:

接收来自业务节点的智能合约生成请求,所述智能合约生成请求中指示业务节点所属单位的下属单位或管辖单位的业务节点;

根据业务节点所属单位的下属单位或管辖单位的业务节点,确定目标业务节点权限数据;

将所述权限数据整合到所述合约模板中,形成该业务节点与区块链运营方的智能合约。

4.根据权利要求3所述的方法,其特征在于,根据业务节点所属单位的下属单位或管辖单位的业务节点,确定目标业务节点权限数据,包括:

将所述业务节点、所述业务节点所属单位的下属单位或管辖单位的业务节点,确定为目标业务节点权限数据中指示的目标业务节点。

5.一种在区块链网络中查询数据区块中的交易信息的方法,其特征在于,所述区块链网络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,所述方法由记账节点子网络中的一个记账节点执行,所述方法包括:

生成业务节点与区块链运营方的智能合约;

将生成的智能合约加入与该业务节点对应的智能合约区块,记录在区块链上;

接收业务节点对数据区块中的交易信息的查询请求;

从区块链上与该业务节点对应的智能合约区块,获取该业务节点与区块链运营方的智能合约;

从该智能合约中,获取该业务节点对应的目标业务节点权限数据;

如果所述交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向所述业务节点返回所述交易信息。

6.根据权利要求5所述的方法，其特征在于，生成业务节点与区块链运营方的智能合约，包括：

发布合约模板，所述合约模板中含有合约函数；

接收利用所述合约函数设置的该业务节点的目标业务节点权限数据；

将所述目标业务节点权限数据整合到所述合约模板中，形成该业务节点与区块链运营方的智能合约。

7.根据权利要求5所述的方法，其特征在于，生成业务节点与区块链运营方的智能合约，包括：

接收来自业务节点的智能合约生成请求，所述智能合约生成请求中指示业务节点所属单位下属单位或管辖单位的业务节点；

根据业务节点所属单位下属单位或管辖单位的业务节点，确定目标业务节点权限数据；

将所述权限数据整合到所述合约模板中，形成该业务节点与区块链运营方的智能合约。

8.根据权利要求7所述的方法，其特征在于，根据业务节点所属单位的下属单位或管辖单位的业务节点，确定目标业务节点权限数据，包括：

将所述业务节点、所述业务节点所属单位的下属单位或管辖单位的业务节点，确定为目标业务节点权限数据中指示的目标业务节点。

9.根据权利要求5所述的方法，其特征在于，将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上，包括：

将生成的智能合约与该业务节点的标识对应存储在该智能合约区块的区块体；

对生成的区块体施加摘要运算和签名运算，得到摘要和签名；

将所述摘要、签名以及区块链上前一区块的摘要，加入智能合约区块的区块头；

将该智能合约区块在记账节点子网络的所有记账节点间进行共识后，记录在区块链上。

10.根据权利要求9所述的方法，其特征在于，从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约，包括：

从区块链上记录的智能合约区块的区块体中，查找该业务节点的标识；

获取该区块体中与该标识对应的智能合约，作为该业务节点与区块链运营方的智能合约。

11.一种在区块链网络中查询数据区块中的交易信息的装置，其特征在于，所述区块链网络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，所述装置包括：

第一生成单元，用于生成业务节点与区块链运营方的智能合约；

同步单元，用于将生成的智能合约同步到记账节点子网络中的各记账节点存储；

查询请求接收单元，用于接收业务节点对数据区块中的交易信息的查询请求；

目标业务节点权限数据获取单元，用于从所述记账节点存储的所述业务节点与区块链运营方的智能合约中，获取所述业务节点对应的目标业务节点权限数据；

交易信息返回单元，用于如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

12.一种在区块链网络中查询数据区块中的交易信息的装置，其特征在于，所述区块链网络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，所述装置包括：

第二生成单元，用于生成业务节点与区块链运营方的智能合约；

上链单元，用于将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上；

查询请求接收单元，用于接收业务节点对数据区块中的交易信息的查询请求；

目标业务节点权限数据获取单元，用于从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约，并从该智能合约中获取该业务节点对应的目标业务节点权限数据；

交易信息返回单元，用于如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

13.一种记账节点，其特征在于，包括：

存储器，存储有计算机可读指令；

处理器，读取存储器存储的计算机可读指令，以执行权利要求1-4中的任一个所述的方法，或执行权利要求5-10中的任一个所述的方法。

14.一种计算机程序介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行权利要求1-4中的任一个所述的方法，或执行权利要求5-10中的任一个所述的方法。

在区块链网络中查询交易信息的方法、装置、记账节点和介质

[0001] 本申请是2018年12月07日提交的、申请号为201811495810.3、发明名称为“在区块链网络中查询交易信息的方法、记账节点和介质”的分案申请。

技术领域

[0002] 本公开涉及区块链领域，具体涉及一种在区块链网络中查询数据区块中的交易信息的方法、装置、记账节点和介质。

背景技术

[0003] 传统的区块链网络中，上链的交易数据被区块链网络中的每个记账节点全量冗余存储。每个记账节点都可以查看区块链上的全部交易信息。如果某个企业希望自己的上链交易信息具有隐私性，不被其它企业查看，是做不到的。

[0004] 因此，期望有一种隐私性好的区块链网络，使得查询区块链上交易信息的用户只能查询到与自己相关的交易信息，从而防止交易信息外泄。

发明内容

[0005] 本公开的一个目的在于使得查询区块链上交易信息的用户只能查询到与自己相关的交易信息，从而防止交易信息外泄。

[0006] 根据本公开实施例的一方面，公开了一种在区块链网络中查询数据区块中的交易信息的方法，所述区块链网络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，所述方法由记账节点子网络中的一个记账节点执行，所述方法包括：生成业务节点与区块链运营方的智能合约；将生成的智能合约同步到记账节点子网络中的各记账节点存储；接收业务节点对数据区块中的交易信息的查询请求；从所述记账节点存储的所述业务节点与区块链运营方的智能合约中，获取所述业务节点对应的目标业务节点权限数据；如果所述交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向所述业务节点返回所述交易信息。

[0007] 根据本公开实施例的一方面，公开了一种在区块链网络中查询数据区块中的交易信息的方法，所述区块链网络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，所述方法由记账节点子网络中的一个记账节点执行，所述方法包括：生成业务节点与区块链运营方的智能合约；将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上；接收业务节点对数据区块中的交易信息的查询请求；从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约；从该智能合约中，获取该业务节点对应的目标业务节点权限数据；如果所述交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向所述业务节点返回所述交易信息。

[0008] 根据本公开实施例的一方面，公开了一种在区块链网络中查询数据区块中的交易信息的装置，所述区块链网络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，所述装置包括：第一生成单元，用于生成业务节点与区块链运营方的智能合约；同步单元，用于将生成的智能合约同步到记账节点子网络中的各记账节点存储；查询请求接收单元，用于接收业务节点对数据区块中的交易信息的查询请求；目标业务节点权限数据获取单元，用于从所述记账节点存储的所述业务节点与区块链运营方的智能合约中，获取所述业务节点对应的目标业务节点权限数据；交易信息返回单元，用于如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0009] 根据本公开实施例的一方面，公开了一种在区块链网络中查询数据区块中的交易信息的装置，所述区块链网络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，所述装置包括：第二生成单元，用于生成业务节点与区块链运营方的智能合约；上链单元，用于将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上；查询请求接收单元，用于接收业务节点对数据区块中的交易信息的查询请求；目标业务节点权限数据获取单元，用于从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约，并从该智能合约中获取该业务节点对应的目标业务节点权限数据；交易信息返回单元，用于如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0010] 根据本公开实施例的一方面，公开了一种记账节点，包括：存储器，存储有计算机可读指令；处理器，读取存储器存储的计算机可读指令，以执行如上所述的方法。

[0011] 根据本公开实施例的一方面，公开了一种计算机程序介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行如上所述的方法。

[0012] 本公开实施例中，记账节点子网络与业务节点子网络是分开的。记账节点子网络中的记账节点会对上链的交易信息发生共识。业务节点子网络中的业务节点不会对上链的交易信息发生共识，这为交易信息不泄密提供了初步的可能性。在此基础上，记账节点接收到业务节点对数据区块中的交易信息的查询请求，获取该业务节点对应的目标业务节点权限数据。这个目标业务节点权限数据指示了该业务节点能够查询哪些目标业务节点相关的交易信息。如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则说明这个交易信息是在业务节点的权限范围内的，业务节点有权查询它，向该业务节点返回该交易信息。这样，使得查询区块链上交易信息的用户只能查询到与自己相关的交易信息，从而防止交易信息外泄。

[0013] 本公开的其他特性和优点将通过下面的详细描述变得显然，或部分地通过本公开的实践而习得。

[0014] 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的，并不能限制本公开。

附图说明

[0015] 通过参照附图详细描述其示例实施例，本公开的上述和其它目标、特征及优点将变得更加显而易见。

[0016] 图1A-1C示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法的三种体系构架图。

[0017] 图2A-2C示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在供应链金融、电子发票、法定数字货币三种不同的应用场景下的场景构架图。

[0018] 图3A-3G示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在供应链金融应用场景下的业务节点显示界面图，这些界面图表示了供应链金融应用场景下从交易信息上链到查询交易信息并验证数据区块内容的大体过程。

[0019] 图4A-4G示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在电子发票应用场景下的业务节点显示界面图，这些界面图表示了电子发票应用场景下从交易信息上链到查询交易信息并验证数据区块内容的大体过程。

[0020] 图5A-5G示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在法定数字货币应用场景下的业务节点显示界面图，这些界面图表示了法定数字货币应用场景下从交易信息上链到查询交易信息并验证数据区块内容的大体过程。

[0021] 图6示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法的流程图。

[0022] 图7示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法的流程图。

[0023] 图8示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法的流程图。

[0024] 图9示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法的流程图。

[0025] 图10示出了根据本公开一个实施例的在图10中步骤305的一个具体流程图。

[0026] 图11示出了根据本公开一个实施例的在图10中步骤305的另一个具体流程图。

[0027] 图12示出了根据本公开一个实施例的确定执行所述在区块链网络中查询数据区块中的交易信息的方法的记账节点的流程图。

[0028] 图13示出了根据本公开一个实施例的图12中步骤430的详细流程图。

[0029] 图14示出了根据本公开一个实施例的图13中步骤4303的详细流程图。

[0030] 图15示出了根据本公开一个实施例的确定执行所述在区块链网络中查询数据区块中的交易信息的方法的记账节点的流程图。

[0031] 图16示出了根据本公开一个实施例的图15中步骤530的详细流程图。

[0032] 图17示出了根据本公开一个实施例的根据交易信息的施动方或受动方、以及目标业务节点权限数据的比较，判断是否向业务节点返回交易信息的示例图。

[0033] 图18A-B示出了根据本公开两个实施例的在区块链网络中查询数据区块中的交易信息的交互流程图。

[0034] 图19示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信

息的记账节点的模块框图。

[0035] 图20示出了根据本公开一个实施例的记账节点的硬件结构图。

具体实施方式

[0036] 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，提供这些示例实施方式使得本公开的描述将更加全面和完整，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。附图仅为本公开的示意性图解，并非一定是按比例绘制。图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。

[0037] 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示例实施方式中。在下面的描述中，提供许多具体细节从而给出对本公开的示例实施方式的充分理解。然而，本领域技术人员将意识到，可以实践本公开的技术方案而省略所述特定细节中的一个或更多，或者可以采用其它的方法、组元、步骤等。在其它情况下，不详细示出或描述公知结构、方法、实现或者操作以避免喧宾夺主而使得本公开的各方面变得模糊。

[0038] 附图中所示的一些方框图是功能实体，不一定必须与物理或逻辑上独立的实体相对应。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。

[0039] 下面先参照图1A-1C描述一下本公开实施例所应用的体系构架和整体流程。

[0040] 图1A示出了本公开实施例所应用的一种区块链网络的体系构架。区块链网络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11。记账节点子网络2和业务节点子网络1之间通过代理节点12连接。代理节点12是业务节点子网络1的一个业务节点，但是比较特殊的一个业务节点。它负责将记账节点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信息的交易方的终端。它们产生了交易信息，但没有权利直接记录到区块链上，必须通过一个记账节点21将交易信息记录到区块链上。由少数记账节点21统一记账，也有利于事务的统一处理和监管，而业务节点11能够通过记账节点21经由代理节点12发送来的信息进行交易信息上链的监督和见证。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民众监督的场景中有十分重要的意义。记账节点子网络2中，每个记账节点21产生一个数据区块后，广播到其它记账节点21进行共识，然后进行上链。图1A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，向周围的业务节点11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，层层传播，达到了该消息在业务节点子网络1的每个业务节点11的传播。

[0041] 图1B示出了本公开实施例所应用的另一种区块链网络的体系构架。该体系构架与图1A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，采取广播网络的模式。代理节点12接收到从记账节点21传递过来的消息，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的传播。

[0042] 图1C示出了本公开实施例所应用的另一种区块链网络的体系构架。该体系构架与图1A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的子区块链上。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。

[0043] 图2A示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在供应链金融的应用场景下的场景构架图。

[0044] 供应链金融是这样一种业务：制造企业生产一个设备或产品，往往不一定是自己的企业生产该设备或产品的所有零件或组成部分，其中一些零件或组成部分的生产需要外包到其它企业去生产。制造企业虽然与订货方提前订立了供销合同，但只有在生产出来整个设备或产品时才能够拿到货款，而在这个过程中采购零件或组成部分的钱需要自己垫付，造成制造企业资金周转困难。因此，产生了这样一种需求，即制造企业可以凭整个设备或产品订立的总采购合同(其中有价款和订购方信息)到银行进行担保，当需要进行零件或组成部分的采购时，以在银行担保过的整个设备或产品的总采购合同为依据，从该设备或产品的总采购合同中价款中划转出一部分用于该零件或组成部分的采购的担保。这样，生成零件或组成部分的企业可以放心进行该零件或组成部分的生产，由于由银行担保，不用担心该划转出的一部分货款收不到。同时，制造企业此时并没有真正拿出这笔钱，而是等到得到整个设备或产品的采购方的实际货款时才将相应一部分付给零件或组成部分的生产商。

[0045] 在传统的区块链网络中，由于由银行设置了所有的记账节点，而这个网络是封闭的，供销链上的各节点企业是与供应链金融的数据区块上链利益相关的节点，却不能监督和见证，只能完全信任这个利益无关方的由记账节点组成的记账网络。例如，制造企业与整个设备或产品的订购方订立了总采购合同，或者与零件或组成部分的生成方签订了分采购合同，都需要将这些合同传给银行设置的记账节点上链。这时，银行设置的各记账节点可以互相监督和见证，但供销链上的各节点企业却不能监督和见证。另外，在传统的区块链网络中，与当前供销链无关的其它任何企业节点，也可能通过对应的记账节点查询到当前供销链上的企业节点上链的任何交易信息。因此，带来了极大的交易信息泄露隐患。

[0046] 然而，在图2A中，由于记账节点子网络2与业务节点子网络1分开，记账节点子网络

2专用于记账，而业务节点子网络1包含了供销链上的各节点企业终端，对记账节点21的记账进行见证。一旦记账节点21集体作弊，见证的各业务节点11会保留有具体记账节点作恶的证据。同时，业务节点需要查询交易信息时，不是所有的交易信息都可以向该业务节点返回，而是根据其与区块链运营方的智能合约中该业务节点的权限数据，确定是否向该业务节点返回交易数据。这样，与当前供销链无关的其它任何企业节点就不能查询到当前供销链上的企业节点上链的任何交易信息，消除了交易信息泄露隐患。

[0047] 在一个汽车供应链金融的例子中，如图2A所示，各业务节点11包括汽车制造商终端、轮胎制造商终端、橡胶生产商终端、车零部件供应商终端、银行终端等。汽车制造商与汽车订购方订立了总采购合同，从总采购合同的价款中拨出一部分用于轮胎的采购，再拨出相应的部分用于车零部件的采购。轮胎制造商以与汽车制造商订立的合同为依据，再从该合同的价款中拨出一部分用于制造轮胎所需橡胶的采购。这样，就建立起了层层采购关系。

[0048] 当汽车制造商与汽车订购方订立了总采购合同，或者汽车制造商与轮胎制造商、车零部件供应商订立分采购合同，或者轮胎制造商与橡胶生产商订立分采购合同时，将相应的交易信息传递给代理节点12，由代理节点12选择一个记账节点21。代理节点12将相应的交易信息发送给选择的记账节点21缓存。记账节点21一般不会单独为一条交易信息打包成一个数据区块上链，而是按照区块打包要求(例如凑齐足够的条数或大小)，打包成一个数据区块。事先给每个记账节点分配签名用的密钥，该密钥是特定于该记账节点的。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。生成签名的方法是先对数据区块中的交易信息生成摘要，再用特定于该记账节点的密钥对摘要利用签名算法签名。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，在所有记账节点21之间进行共识后上链，同时将签名通过代理节点12发送到业务节点子网络中的每个业务节点11。

[0049] 与签名同时发送到各业务节点11的还可以有数据区块中的交易信息，或者交易信息的摘要。

[0050] 在同时发送交易信息的情况下，业务节点11获取特定于记账节点的密钥。在非对称公私钥对的情况下，记账节点21在记账的过程中采用的密钥是由认证中心(CA)分配给记账节点21的私钥。在分配私钥的同时，还为记账节点21分配一个公钥。该公钥存储在认证中心。业务节点11就可以从认证中心请求到为该记账节点21分配的公钥。这个公钥就是业务节点11获取到的特定于记账节点的密钥。业务节点11用该密钥对所述签名进行解密，得到所述数据区块中的交易信息的摘要。业务节点11对同时接收到的所述数据区块中的交易信息计算摘要。如果计算出的摘要与解密得到的摘要一致，则签名验证成功。

[0051] 在同时发送交易信息的摘要(例如摘要和签名放在区块头中一起发送)的情况下，业务节点11获取特定于该记账节点的密钥，例如从认证中心请求到为该记账节点21分配的公钥。业务节点11用特定于该记账节点的密钥对所述签名进行解密，得到所述数据区块中的交易信息的摘要。如果与签名同时接收到的摘要与解密得到的摘要一致，则签名验证成功。

[0052] 在同时发送交易信息的摘要(例如摘要和签名放在区块头中一起发送，该摘要可以是根据该数据区块中要包括的每条交易信息的哈希值计算出的默克尔树根)的情况下，业务节点11是接收不到每个交易信息的。业务节点11要查看交易信息时，需要向记账节点

21请求。这时，记账节点21获取该业务节点对应的目标业务节点权限数据(一般从业务节点实现与区块链运营方订立的智能合约中得到)，该目标业务节点权限数据指示着该业务节点允许访问哪些目标业务节点相关的交易信息。如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。这样，就达到了一些单位不希望自己的交易信息被无关方看到的目的，提高了上链交易信息的隐私性。

[0053] 如果不向业务节点返回交易信息(业务节点没有权限)，可以向其返回交易信息的哈希值。由于默克尔树根仅凭每条交易信息的哈希值就可以计算出，这样，就达到既隐藏信息又不影响数据区块中的内容验证的目的。该业务节点11可以对获取到的非隐藏的交易信息计算哈希值，根据这些哈希值和接收到的隐藏的交易信息的哈希值计算出默克尔树根，与区块头中包含的默克尔树根比较，如果一致，则说明数据区块的内容没有被篡改，内容验证通过。而业务节点11也可以接收到的从非隐藏的交易信息中验证该交易信息是否与自己发给记账节点21的交易信息一致。如不一致，说明业务节点11作恶，达到了监督的目的。

[0054] 本公开实施例主要是针对上述接收业务节点对数据区块中的交易信息的查询请求后，获取该业务节点对应的目标业务节点权限数据，并与交易信息的施动方或受动方进行对比，从而确定是否向业务节点返回交易信息的过程的。

[0055] 下面结合图3A-3G说明供应链金融应用场景下从交易信息上链到查询并验证的大体过程。图3A-3G是根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在供应链金融应用场景下的业务节点显示界面图。

[0056] 如图3A所示，B汽车厂以A销售商采购B汽车厂1000万采购订单为基础，用1000万中的200万作保，委托C轮胎厂生产200万售价的轮胎。B汽车厂的业务员在B汽车厂的业务节点11录入以上交易信息后，点击“提交到记账节点”选项，交易信息通过代理节点12发送到记账节点21。记账节点21将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放在一个区块体中。记账节点21还生成这些交易信息的摘要，如图3B的默克尔树根。记账节点21还利用特定于该记账节点的密钥，基于该数据区块中的交易信息，生成签名。将默克尔树根、签名以及区块链上前一数据区块的摘要一同放在区块头中。区块头和区块体组成上链的数据区块，经所有记账节点21共识后上链。

[0057] 记账节点21还将区块头发送到每个业务节点11。在业务节点11的屏幕上显示默克尔树根、签名以及区块链上前一数据区块的摘要，如图3B所示。这时，记账节点21就获取特定于该记账节点的密钥(例如通过请求认证中心)，用特定于该记账节点的密钥对所述签名进行解密，得到所述数据区块中的交易信息的摘要，即默克尔树根。如果接收到的区块头中的默克尔树根与解密得到的默克尔树根不一致，则签名验证失败，显示如图3C所示的界面。如果接收到的区块头中的默克尔树根与解密得到的默克尔树根一致，则签名验证成功，显示如图3D所示的界面。由于在以上的过程中，业务节点11仅获得了数据区块的区块头，还没有获得区块头中的交易信息。此时，在图3D的界面中询问用户是否请求该数据区块中的交易信息。

[0058] 如果用户选择“是”，业务节点11通过代理节点12向记账节点21请求交易信息。记账节点21获取业务节点11的目标业务节点权限数据，其指示了该业务节点11有权查询哪些目标业务节点的交易信息。如果交易信息的施动方或受动方恰好是所述目标业务节点权限

数据中指示的目标业务节点之一，则说明该业务节点有这样的查询权限，向该业务节点返回该交易信息，如图3E中交易信息ID 000083的具体信息、交易信息ID 000153的具体信息。对于该数据区块中该业务节点11无权获取的交易信息，如交易信息ID 000258的交易信息、交易信息ID 000256的交易信息、交易信息ID 078365的交易信息、交易信息ID 018387的交易信息，仅向给业务节点11返回哈希值，如图3E所示。

[0059] 当用户在图3E的界面上选择“进行内容验证”后，对于图3E中交易信息ID 000083的具体信息、交易信息ID 000153的具体信息，业务节点11计算其哈希值，然后再与接收到的交易信息ID 000258的交易信息的哈希值、交易信息ID 000256的交易信息的哈希值、交易信息ID 078365的交易信息的哈希值、交易信息ID 018387的交易信息的哈希值一起，计算出默克尔树根，与区块头中包含的默克尔树根进行比较，从而进行内容验证。如果记账节点21篡改过数据区块的内容，则计算出的默克尔树根与区块头中包含的默克尔树根不一致，显示如图3F所示的“内容验证失败”的界面。如果计算出的默克尔树根与区块头中包含的默克尔树根一致，显示如图3G所示的“内容验证成功”的界面。

[0060] 图2B示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在电子发票的应用场景下的场景构架图。

[0061] 在传统的电子发票的区块链应用场景中，地税局向开票企业发放发票，开票企业向领票人开出发票，领票人向领票人所在的报销单位报销发票。所有这些交易都需要上链，即记录到区块链上。但是，地税局、开票企业、报销单位这些节点不是记账节点21。它们要委托对应的记账节点或超级节点将这些交易记录在区块链上。所有这些记账节点或超级节点都是国税部门统一设置的。它们之间可以互相监督和见证，但地税局、开票企业、报销单位这些节点是发票的直接关系人，却不能监督和见证，只能完全信任记账节点21。另外，任何企业都可以通过其对应的记账节点查询区块链上任何交易信息。但在某些情况下，企业的发票相关信息并不希望被其它企业获知。在本公开实施例中，由于记账节点子网络2与业务节点子网络1分开，记账节点子网络2专用于记账，而业务节点子网络1包含了这些发票利益相关的节点，对记账节点21的记账进行见证。一旦记账节点21集体作弊，见证的各业务节点11会保留有具体记账节点作恶的证据。当任何一个业务节点1需要查询数据区块中的交易信息时，记账节点要获取该业务节点对应的目标业务节点权限数据，该目标业务节点权限数据指示了该业务节点有权查询哪些目标业务节点相关的交易信息。如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息，反之则不返回交易信息。通过这种方法，保证了上链交易信息的隐私性。在业务节点没有权限的情况下，向该业务节点不返回交易信息，但返回交易信息的哈希值，从而保证业务节点利用哈希值同样可以对区块头中的默克尔树根进行验证，达到内容验证的目的。

[0062] 在一个电子发票的例子中，如图2B所示，各业务节点11包括开票单位终端、报销人手机、报销单位终端、地税局终端等。

[0063] 当地税局为开票单位发放发票，或者开票单位开出发票，或者报销人到报销单位报销时，将相应的交易信息(发票所有权的转移)传递给代理节点12，由代理节点12选择一个记账节点21。代理节点12将相应的交易信息发送给选择的记账节点21缓存。然后，记账节点21按照区块打包要求打包成数据区块。记账节点21基于数据区块中的交易信息，生成签

名，将签名加入数据区块的区块头后上链并将签名发送给业务节点11，这些过程与结合图2A所示的过程类似。

[0064] 与签名同时发送到各业务节点11的还可以有数据区块中的交易信息，或者交易信息的摘要。在同时发送交易信息的情况下和同时发送摘要的情况下，在业务节点11的签名验证方式不同，但在业务节点11处都能进行签名验证。这与上面结合图2A所示的过程类似，可以参照以上结合图2A所示的相关描述。另外，在同时发送交易信息的摘要的情况下，业务节点11可以进行数据区块的内容验证，验证过程也与上面结合图2A所示的过程类似，故不赘述。

[0065] 图4A-4G示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在电子发票应用场景下的业务节点显示界面图，这些界面图表示了电子发票应用场景下交易信息上链、查询并验证的大体过程。

[0066] 如图4A所示，在2018年10月22日，刘山到彩虹电脑公司为所在单位宏生公司购买一台电脑，花了3000元。彩虹电脑公司为刘山开具了一张发票，交易ID为000083。彩虹电脑公司的工作人员录入以上信息后，点击“提交到记账节点”选项，交易信息通过代理节点12发送到记账节点21。记账节点21将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放在一个区块体中。记账节点21还生成默克尔树根和签名，将默克尔树根、签名以及区块链上前一数据区块的摘要一同放在区块头中。记账节点21将数据区块上链，并将区块头发送到每个业务节点11。在业务节点11的屏幕上显示默克尔树根、签名以及区块链上前一数据区块的摘要，如图4B所示。

[0067] 然后，记账节点21进行签名验证，根据验证结果显示图4C或图4D的界面，并向记账节点21请求交易信息，显示图4E所示的获取的交易信息或交易信息的哈希值的界面，然后根据内容验证的验证结果，分别显示图4F-4G的界面。这些过程与图3C-3G所示的过程类似，故不赘述。

[0068] 图2C示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在法定数字货币的应用场景下的场景构架图。

[0069] 在传统的例如比特币的民间数字货币的场景以下，比特币的流转过程中的每一笔交易，都由交易的当事方进行上链。每个当事方既可以作为记账节点进行上链操作，也可以见证其它节点上链的数据区块。由于每个节点既作为记账节点，又作为见证节点，使得公众对于这种数字货币的使用比较信赖。然而，在法定数字货币的场景下，该数字货币由官方发行，必须由官方进行监管，而公众又需要对其信任，防止官方记账节点集体作弊，产生了现有网络体系面对政府监管和民众信任的平衡方面的问题。而且，现有比特币区块链网络中，每个节点既作为记账节点，又作为见证节点，这样每个节点的用户都能看到区块链上记录的所有交易信息，而有些单位的交易信息是不希望暴露给所有人的，又产生了隐私保护的问题。

[0070] 在这种情况下，本公开实施例的记账节点子网络和业务节点子网络分开的方案，完全避免了这一问题。首先，记账节点子网络的每个记账节点属于官方。任一业务节点处发生了法定数字货币的交易，都要将该法定数字货币的交易通过对应的记账节点记录到区块链上。但是，业务节点子网络中的每个业务节点可以对记账节点21的记账进行见证。一旦记账节点21集体作弊，见证的各业务节点11会保留有具体记账节点作恶的证据，兼顾了政府

监管和民众信任。同时，业务节点要想查询交易信息，获取该业务节点对应的目标业务节点权限数据，该目标业务节点权限数据指示了该业务节点有权查询哪些目标业务节点相关的交易信息。如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。在业务节点不具有权限时，虽然不向其返回交易信息，但返回交易信息的哈希值，通过该哈希值同样可以验证区块头中的默克尔树根，实现内容验证。

[0071] 在一个法定数字货币的例子中，如图2C所示，各业务节点11包括法定数字货币流通中涉及的各个交易终端。当发送法定数字货币的交易信息时，交易终端将相应的交易信息(法定数字货币所有权的转移)传递给代理节点12，由代理节点12选择一个记账节点21。代理节点12将相应的交易信息发送给选择的记账节点21缓存。然后，记账节点21按照区块打包要求打包成数据区块。记账节点21基于数据区块中的交易信息，生成签名，将签名加入数据区块的区块头后上链并将签名发送给业务节点11，这些过程与结合图2A所示的过程类似。

[0072] 与签名同时发送到各业务节点11的还可以有数据区块中的交易信息，或者交易信息的摘要。在同时发送交易信息的情况下和同时发送摘要的情况下，在业务节点11的签名验证方式不同，但在业务节点11处都能进行签名验证。这与上面结合图2A所示的过程类似，可以参照以上结合图2A所示的相关描述。另外，在同时发送交易信息的摘要的情况下，业务节点11可以进行数据区块的内容验证，验证过程也与上面结合图2A所示的过程类似，故不赘述。

[0073] 图5A-5G示出了根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法应用在法定数字货币应用场景下的业务节点显示界面图，这些界面图表示了法定数字货币应用场景下记账和见证的大体过程。

[0074] 如图5A所示，在2018年8月29日，因X公司从Y公司买入一台售价3000单位的法定数字货币的家具，付给Y公司人民币3000单位的法定数字货币。X公司的经办人录入以上信息后，点击“提交到记账节点”选项，交易信息通过代理节点12发送到记账节点21。记账节点21将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放在一个区块体中。记账节点21还生成默克尔树根和签名，将默克尔树根、签名以及区块链上前一数据区块的摘要一同放在区块头中。记账节点21将数据区块上链，并将区块头发送到每个业务节点11。在业务节点11的屏幕上显示默克尔树根、签名以及区块链上前一数据区块的摘要，如图5B所示。

[0075] 然后，记账节点21进行签名验证，根据验证结果显示图5C或图5D的界面，并向记账节点21请求交易信息，显示图5E所示的获取的交易信息或交易信息的哈希值的界面，然后根据内容验证的验证结果，分别显示图5F-5G的界面。这些过程与图3C-3G所示的过程类似，故不赘述。

[0076] 如图6所示，根据本公开的一个实施例，提供了一种在区块链网络中查询数据区块中的交易信息的方法。如图1A-1C所示，所述区块链网络包括记账节点子网络2和业务节点子网络1。所述记账节点子网络2包括将数据区块记录到区块链上的记账节点21。所述业务节点子网络1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11。所述方法由记账节点子网络2中的一个记账节点21执行。所述方法包括：

[0077] 步骤310、接收业务节点对数据区块中的交易信息的查询请求；

[0078] 步骤320、获取该业务节点对应的目标业务节点权限数据，该业务节点有权查询所述目标业务节点权限数据中指示的目标业务节点的交易信息；

[0079] 步骤330、如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0080] 下面对步骤310-330进行详细描述。

[0081] 在步骤310中，记账节点接收业务节点对数据区块中的交易信息的查询请求可以有多种方式。一种实施方式中，记账节点可以通过代理节点接收业务节点对数据区块中的交易信息的查询请求，代理节点是业务节点子网络中一个特殊的节点，用来在业务节点与记账节点之间传递信息。业务节点发送查询请求，要先发送到代理节点，由代理节点再发送到记账节点子网络中相应的一个记账节点对查询请求进行相应，如何选择记账节点，将在下文中详细描述。另一种实施方式中，业务节点可以直接将查询请求发送到记账节点。业务节点选择记账节点的方法可以与代理节点选择记账节点的方法相同。

[0082] 在步骤320中，记账节点获取该业务节点对应的目标业务节点权限数据。目标业务节点权限数据指示了该业务节点有权查询哪些目标业务节点的交易信息。该业务节点有权查询所述目标业务节点权限数据中指示的目标业务节点的交易信息。

[0083] 在一个实施例中，在每个记账节点事先维护一种业务节点与目标业务节点权限数据的对应关系表。记账节点可以通过查询该对应关系表，获取该业务节点对应的目标业务节点权限数据。

[0084] 在另一个实施例中，每个业务节点与区块链运营方事先订立有智能合约。可以从业务节点与区块链运营方的智能合约中，获取该业务节点对应的目标业务节点权限数据。关于如何生成智能合约，在后面的实施例中描述。

[0085] 在步骤330中，如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0086] 众所周知，交易是一方引起另一方的行为。引起行为的一方就是施动方，被引起行为的一方就是受动方。例如，在开出电子发票的交易中，开票单位终端就是施动方，领票人终端就是受动方。在法定数字货币的转移交易中，法定数字货币的转出方终端就是施动方，法定数字货币的转入方终端就是受动方。

[0087] 如图17所示，每条交易信息包括施动方信息和受动方信息。施动方信息包括施动方有关的信息，受动方信息包括受动方有关的信息。例如，开出电子发票的事件中，施动方信息包括开票单位名称、开票单位纳税人识别号、开票人姓名、开票时间、开票金额等，受动方信息包括领票人姓名、领票人联系方式、领票人所在报销单位等。交易信息中的施动方有两种表示方式，一种是直接用施动方名称(例如开票单位名称、法定数字货币转出单位名称等)表示(如图17中交易信息TX3的施动方为A，表示交易信息TX3的施动方是名称为A的单位终端)，另一种是用其它交易信息表示，表示本交易信息的施动方是该其它交易信息的受动方(如图17中交易信息TX1、TX2的施动方是TX0，表示交易信息TX1、TX2的施动方是交易信息TX0的受动方；TX4的施动方是TX1+TX2，表示交易信息TX4的施动方是交易信息TX1和TX2的受动方)。

[0088] 例如，电子发票报销交易信息中的施动方可以是电子发票开票交易信息中的受动方，即开票事件中领取了电子发票的领票人回所在单位报销时，其变成了施动方。多个领票

人在同一单位联合报销时，报销交易信息中的施动方可能来自多个开票交易信息中的受动方。

[0089] 目标业务节点权限数据指示着该业务节点有权查询的目标业务节点。如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则这个交易信息要么施动方落在允许的权限之内，要么受动方落在允许的权限之内，都是可以向其返回交易信息的。

[0090] 在一个实施例中，在步骤320之后，所述方法还包括：如果该交易信息的施动方是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0091] 如上所述，交易信息中的施动方有两种表示方式，一种是直接用施动方名称表示，另一种是用其它交易信息表示，表示本交易信息的施动方是该其它交易信息的受动方。这样，如果该交易信息的施动方是后一种表示方式，即该交易信息的施动方是另一交易信息的受动方，该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，这种情况下也变相相当于该交易信息的施动方其实也是所述目标业务节点权限数据中指示的目标业务节点之一，该业务节点也应该有权查询该目标业务节点交易信息。

[0092] 如图17所示，交易信息TX4的施动方用TX1+TX2表示，即交易信息TX4的施动方是交易信息TX1的受动方、和交易信息TX2的受动方。例如，交易信息TX4是电子发票报销的交易信息，交易信息TX1和TX2分别是两个电子发票开票的交易信息。交易信息TX1中，A1是领票人。交易信息TX2中，B是领票人。TX4的施动方TX1+TX2表示TX1的受动方(即领票人A1)和TX2的受动方(即领票人B)一起报销。因此，表面上交易信息TX4的施动方用TX1+TX2表示，实际上，它的施动方是A1+B。这样，如果目标业务节点权限数据指示该业务节点A有权查询业务节点A和A1(A1是A的一个子公司)的交易信息，则A1+B中的A1是业务节点A针对其有权查询交易信息的。因此，可以向该业务节点返回交易信息。

[0093] 该实施例克服了在是交易信息的施动方用其它交易信息表示(即，本交易信息的施动方是该其它交易信息的受动方)时，有可能单独从交易信息的施动方或受动方来判断是否是所述目标业务节点权限数据中指示的目标业务节点之一不正确的问题，因为在这种情况下，交易信息的施动方实质上是所述目标业务节点权限数据中指示的目标业务节点之一，但形式上不是，因此造成误判。该实施例提高了确定是否应向业务节点返回交易信息的准确性。

[0094] 在一个实施例中，在步骤320之后，所述方法还包括：步骤330、如果交易信息的施动方或受动方既不是所述目标业务节点权限数据中指示的目标业务节点之一，也不是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息的哈希值。

[0095] 即，在上述两种情形中(第一种情形是交易信息的施动方或受动方本身是所述目标业务节点权限数据中指示的目标业务节点之一，第二种情形是该交易信息的施动方是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一)，都应当认为该业务节点有权查询该交易信息。如果不属于这两种情形，即交易信息的施动方或受动方既不是所述目标业务节点权限数据中指示的目标业务节点之一，也不是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点

权限数据中指示的目标业务节点之一，则认为该业务节点无权查询该交易信息，这时是不应向该业务节点返回交易信息的，为了内容验证，可以仅返回交易信息的哈希值。

[0096] 由于默克尔树根仅凭每条交易信息的哈希值就可以计算出，这样，该业务节点11可以对获取到的非隐藏的交易信息计算哈希值，根据这些哈希值和接收到的隐藏的交易信息的哈希值计算出默克尔树根，与区块头中包含的默克尔树根比较，如果一致，则说明数据区块的内容没有被篡改，内容验证通过，从而达到防止记账节点篡改交易信息内容的目的。

[0097] 在一个实施例中，如图7所示，步骤310包括：接收业务节点对数据区块中的交易信息的查询请求和用特定于该业务节点的私钥对该查询请求生成的签名。另外，在步骤320之前，所述方法还包括：步骤312、用特定于该业务节点的公钥对该签名进行验证，其中，只有在验证成功的情况下，才获取该业务节点对应的目标业务节点权限数据。

[0098] 相比于图6的实施例，图7的实施例增加了对业务节点的身份进行验证的过程，如果业务节点的身份不合格，即不是注册在区块链网络(包括业务节点子网络和记账节点子网络)中的节点，其是无权查询任何上链的交易信息，在进行施动方和受动方与权限数据的核对前，就要将其拒绝。通过这种方式，进一步保证了区块链网络上查询上链交易信息的安全性。

[0099] 判断业务节点的身份是否合格，即是否是注册在区块链网络上的节点，可以通过签名进行验证。认证中心向业务节点发放特定于该业务节点的私钥，同时将特定于业务节点的公钥存储在认证中心，或者发放给代理节点，或者广播到记账节点子网络中的每个记账节点。这样，业务节点因为拥有特定于该业务节点的私钥，就可以用特定于该业务节点的私钥对该查询请求生成签名。签名的方法包括先用预定摘要算法求出查询请求的摘要，再对该摘要用特定于该业务节点的私钥加密。当记账节点或代理节点得到该签名后，对该签名进行验证。

[0100] 在一个实施例中，步骤312包括：

[0101] 获取特定于该业务节点的公钥；

[0102] 利用所述特定于该业务节点的公钥对所述签名进行解密，得到所述查询请求的摘要；

[0103] 利用预定摘要算法对该查询请求计算摘要；

[0104] 如果计算出的摘要与解密得到的摘要一致，则验证成功。

[0105] 可以看出，该验证的过程是完全与生成签名的过程对应的。利用所述特定于该业务节点的公钥对所述签名进行解密，得到所述查询请求的摘要。这个摘要与生成签名的过程中生成的摘要应该是一致的。因此，用生成摘要时的摘要算法对查询请求再算一遍摘要，如果得到的摘要与解密后的摘要相同，则验证成功。如果不相同，则验证失败，拒绝该查询请求。

[0106] 在一个实施例中，认证中心向业务节点发放特定于该业务节点的私钥可以在业务节点注册到区块链网络后立即进行。该实施例中，业务节点向区块链网络中负责区块链网络注册的节点发送注册请求后，负责区块链网络注册的节点读取注册请求中的业务节点注册信息并存储，同时通知认证中心向业务节点发放特定于该业务节点的私钥。

[0107] 在一个实施例中，认证中心向业务节点发放特定于该业务节点的私钥可以业务节点发送对交易信息的查询请求之前才执行。该实施例中，业务节点向区块链网络中负责区

块链网络注册的节点发送注册请求后，负责区块链网络注册的节点读取注册请求中的业务节点注册信息并存储，同时通知认证中心该业务节点已注册，但不急于发放特定于该业务节点的私钥，而是等到该业务节点要发送查询请求之前，业务节点向认证中心发送私钥请求。认证中心查询到该业务节点已注册后，为其分配特定于该业务节点的私钥。

[0108] 在一个实施例中，认证中心向记账节点或代理节点发放特定于该业务节点的公钥可以在认证中心向业务节点发放特定于该业务节点的私钥之后立即进行，即，认证中心在向业务节点发放特定于该业务节点的私钥后立即将特定于该业务节点的公钥发放到记账节点或代理节点。但在另一个实施例中，认证中心向记账节点或代理节点发放特定于该业务节点的公钥可以在记账节点或代理节点需要对业务节点发过来的签名进行解密时进行。在记账节点或代理节点接收到查询请求和对该查询请求的签名后，先向认证中心请求特定于该业务节点的公钥，然后，认证中心向记账节点或代理节点发放特定于该业务节点的公钥。

[0109] 如图18A和18B所示，进行签名验证的过程可以在代理节点进行，也可以在记账节点进行。

[0110] 在图18A的实施例中，进行签名验证的过程可以在代理节点进行。业务节点创建查询请求并用特定于业务节点的私钥签名。业务节点将查询请求和签名发送到代理节点。代理节点获取特定于业务节点的公钥，对签名进行验证。如果验证成功，代理节点继续将查询请求发送到记账节点，由记账节点根据业务节点的目标业务节点权限数据对交易信息的施动方或受动方进行验证，如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，或者如果该交易信息的施动方是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息，否则返回交易信息的哈希值。

[0111] 在图18B的实施例中，进行签名验证的过程可以在记账节点进行。业务节点创建查询请求并用特定于业务节点的私钥签名。业务节点将查询请求和签名发送到代理节点，代理节点转发到记账节点。记账节点获取特定于业务节点的公钥，对签名进行验证。如果验证成功，记账节点根据业务节点的目标业务节点权限数据对交易信息的施动方或受动方进行验证，如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，或者如果该交易信息的施动方是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息，否则返回交易信息的哈希值。

[0112] 如图8所示，在一个实施例中，在步骤310之前，所述方法还包括：

[0113] 步骤305、生成业务节点与区块链运营方的智能合约；

[0114] 步骤306、将生成的智能合约同步到记账节点子网络中的各记账节点存储。

[0115] 该实施例中，步骤320包括：

[0116] 步骤3201、从该记账节点存储的该业务节点与区块链运营方的智能合约中，获取该业务节点对应的目标业务节点权限数据。

[0117] 该实施例中，每个业务节点与区块链运营方的智能合约都会存储在记账节点子网络中的各记账节点中。该实施例的好处是，由于智能合约都在各个记账节点本地存储，大大提高了向业务节点返回交易信息或哈希值的处理速度。

[0118] 智能合约是存储着业务节点在查询交易信息方面的权限数据(包括目标业务节点权限数据)的合约,它是业务节点与区块链运营方事先订立的。

[0119] 目标业务节点权限数据是指示该业务节点有权查询哪些目标业务节点的交易信息的数据,它表明:交易信息的施动方或受动方必须带有哪些目标业务节点中的至少一个,该业务节点才允许查询;或者,该交易信息的施动方是另一交易信息的受动方,而该另一交易信息的受动方必须带有哪些目标业务节点中的至少一个,该业务节点才允许查询。例如,A公司有两个分公司A1和A2,该业务节点A对应的目标业务节点权限数据可能就会指示,该业务节点A能够查询的目标业务节点包括A、A1、A2。一旦交易信息的施动方或受动方中含有A、A1、A2中的至少一个,或者,该交易信息的施动方是另一交易信息的受动方,而该另一交易信息的受动方中含有A、A1、A2中的至少一个,则业务节点A有权查询该交易信息,可以向其返回交易信息,否则只能返回交易信息的哈希值。

[0120] 在一个实施例中,如图10所示,步骤305包括:

[0121] 步骤3051、发布合约模板,所述合约模板中含有合约函数;

[0122] 步骤3052、接收利用所述合约函数设置的该业务节点的目标业务节点权限数据;

[0123] 步骤3053、将所述目标业务节点权限数据整合到所述合约模板中,形成该业务节点与区块链运营方的智能合约。

[0124] 合约模板是对于所有业务节点与区块链运营方的智能合约都适用于的合约样式。每个智能合约都可以套用该样式,只不过其中具体的权限数据不同而已。它是智能合约中除掉随着不同业务节点而不同的权限数据之后的格式段。合约函数是合约中设置的函数,用户通过调用该函数,可以设置目标业务节点权限数据。发布合约模板可以包括向该记账节点发布合约模板,也可以包括向记账节点子网络中所有记账节点发布合约模板。在前者的情况下,操作该记账节点的管理员可以在审核业务节点的具体情况后,为该业务节点确定权限数据并输入该记账节点。在后者的情况下,任一个记账节点的管理员都可以在审核业务节点的具体情况后,为该业务节点确定权限数据并输入该记账节点。

[0125] 审核的业务节点的具体情况包括业务节点所属单位下属单位或管辖单位的业务节点。每个业务节点是一个单位中的终端。业务节点所属单位就是该终端归属的单位。例如,发票开票企业的一台电脑作为业务节点,其所述单位就是该发票开票企业。该业务节点所属单位可能是它的分公司。另外,该业务节点所属单位可能是一个职能部门,其管辖单位就是该职能部门管辖的所有单位。例如,XX市地税局的管辖单位可以是XX市所有纳税单位。管理员可以将所述业务节点、以及该业务节点所属单位下属单位或管辖单位的业务节点确定为目标业务节点权限数据中指示的目标业务节点。例如,A公司有两个分公司A1、A2,可以将A、A1、A2确定为目标业务节点权限数据中指示的目标业务节点,即当交易信息施动方或受动方中出现A、A1、A2中的一个时,或者当该交易信息的施动方是另一交易信息的受动方,而该另一交易信息的受动方是A、A1、A2中的一个时,认为A公司具有对该交易信息的查询权限。

[0126] 管理员确定权限数据后,就在记账节点利用所述合约函数设置该业务节点的权限数据,这样,该记账节点就接收到利用所述合约函数设置的该业务节点的目标业务节点权限数据,将所述目标业务节点权限数据整合到所述合约模板中,就形成了该业务节点与区块链运营方的智能合约。

[0127] 该实施例的优点是，合约模板提供合约函数，让管理员根据业务节点的情况灵活设置目标业务节点权限数据，提高了目标业务节点权限数据设置的灵活性。

[0128] 在一个实施例中，如图11所示，步骤305包括：

[0129] 步骤3054、接收来自业务节点的智能合约生成请求，所述智能合约生成请求中指示业务节点所属单位下属单位或管辖单位的业务节点；

[0130] 步骤3055、根据业务节点所属单位下属单位或管辖单位的业务节点，确定目标业务节点权限数据；

[0131] 步骤3056、将所述权限数据整合到所述合约模板中，形成该业务节点与区块链运营方的智能合约。

[0132] 该实施例中，业务节点要生成智能合约时，发送一个智能合约生成请求，所述智能合约生成请求中指示业务节点所属单位下属单位或管辖单位的业务节点。记账节点接收该该智能合约生成请求后，根据业务节点所属单位下属单位或管辖单位的业务节点，自动确定目标业务节点权限数据，并将自动确定的所述目标业务节点权限数据整合到所述合约模板中。

[0133] 该实施例的优点是，实现了智能合约生成的自动化。

[0134] 上述的自动确定权限数据的方法如下。

[0135] 在一个实施例中，步骤3055包括：将所述业务节点、所述业务节点所属单位下属单位或管辖单位的业务节点，确定为目标业务节点权限数据中指示的目标业务节点。例如，A公司有两个分公司A1、A2，可以将A、A1、A2确定为目标业务节点权限数据中指示的目标业务节点。

[0136] 该实施例与如上所述的管理员根据该业务节点所属单位下属单位或管辖单位的业务节点确定目标业务节点权限数据的方法类似，只不过它是由机器直接将接收到的智能合约生成请求中的该业务节点所属单位下属单位或管辖单位的业务节点、以及所述业务节点本身，确定为目标业务节点权限数据，实现了确定的自动化。

[0137] 在另一个实施例中，智能合约不是实现存储在记账节点子网络的每个记账节点中，而是上链记录。这样，每个记账节点需要从智能合约中获取权限数据时，可以上链查找。该实施例的优点是，相比于每个记账节点内部维护一个数据库存储每个业务节点的智能合约，节省了节点内部存储空间的占用。

[0138] 如图9所示，在该实施例中，在步骤310之前，所述方法包括：

[0139] 步骤305、生成业务节点与区块链运营方的智能合约；

[0140] 步骤307、将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上。

[0141] 相应地，步骤320包括：

[0142] 步骤3202、从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约；

[0143] 步骤3203、从该智能合约中，获取该业务节点的目标业务节点权限数据。

[0144] 图9的步骤305与图8的步骤305相同，故不赘述。

[0145] 在一个实施例中，步骤307包括：

[0146] 将生成的智能合约与该业务节点标识对应存储在该智能合约区块的区块体；

[0147] 对生成区块体施加摘要运算和签名运算，得到摘要和签名；

[0148] 将所述摘要、签名以及区块链上前一区块的摘要，加入智能合约区块的区块头；

[0149] 将该智能合约区块在记账节点子网络的所有记账节点间进行共识后，记录在区块链上。

[0150] 业务节点标识的作用是便于在步骤3202中获取与业务节点对应的智能合约。

[0151] 摘要和签名、以及区块链上前一区块的摘要的作用如前结合图2A-2C、图3A-3G、图4A-4G、图5A-5G所述，故不赘述。

[0152] 关于智能合约区块在记账节点子网络的所有记账节点间进行共识，目前有很多共识算法，故不赘述。

[0153] 相应地，步骤3202可以包括：

[0154] 从区块链上记录的智能合约区块的区块体中，查找该业务节点的标识；

[0155] 获取该区块体中与该标识对应的智能合约，作为该业务节点与区块链运营方的智能合约。

[0156] 在一个实施例中，可以在智能合约区块的区块头上添加特定标识，依靠该特定标识可以从区块链上的所有数据区块中定位到智能合约区块。该实施例的优点是，相对于在所有数据区块中逐一搜索业务节点的标识，大大提高了搜索业务节点的智能合约的效率。

[0157] 如上所述，根据本公开一个实施例的在区块链网络中查询数据区块中的交易信息的方法由记账节点子网络中的一个记账节点执行。下面详细描述该记账节点的选出过程。

[0158] 在一个实施例中，如图12所示，执行所述方法的记账节点从记账节点子网络中按照以下方式选出。在一个实施例中，业务节点的查询请求先发送给代理节点，由代理节点按照以下步骤选出记账节点：

[0159] 步骤410、获取记账节点子网络中每个记账节点的处理负荷；

[0160] 步骤420、确定记账节点子网络中每个记账节点到发送所述查询请求的业务节点的距离；

[0161] 步骤430、基于所述处理负荷和所述距离，确定执行所述方法的记账节点。

[0162] 处理负荷是表示记账节点正在处理的任务的负担的参数。在一个实施例中，处理负荷可以用记账节点未处理完的任务数来衡量。这里的任务包括交易信息上链任务和查询任务。这些未处理完的任务数就能够代表记账节点的处理负荷。

[0163] 在一个实施例中，步骤410包括：

[0164] 获取每个记账节点定期发送的处理负荷并存储；

[0165] 将记账节点最近一次存储的记账节点的处理负荷作为获取的该记账节点的处理负荷。

[0166] 也就是说，在该实施例中，处理负荷可以由各记账节点定期(例如，每隔5秒)发送给代理节点。代理节点维护一张处理负荷表，该处理负荷表中记录接收到的各记账节点定期广播的处理负荷。这样，代理节点就可以将记账节点最近一次存储的记账节点的处理负荷作为获取的该记账节点的处理负荷。

[0167] 在该实施例中，代理节点被动接收记账节点定期发送的处理负荷。在另一个实施例中，代理节点主动查询记账节点的处理负荷。在该实施例中，步骤410包括：

[0168] 向记账节点子网络中每个记账节点发送处理负荷查询请求；

[0169] 接收每个记账节点发送来的该记账节点的处理负荷。

[0170] 在一个实施例中，步骤420中，确定记账节点子网络中每个记账节点到发送所述查询请求的业务节点的距离，包括：

[0171] 向记账节点子网络中每个记账节点、以及发送所述查询请求的业务节点发出定位信息请求；

[0172] 从各记账节点、以及发送所述查询请求的业务节点接收各记账节点、以及发送所述查询请求的业务节点的定位信息；

[0173] 利用各记账节点、以及发送所述查询请求的业务节点的定位信息，确定各记账节点到发送所述查询请求的业务节点的距离。

[0174] 每个业务节点和记账节点都可以具有GPS等定位系统，因此，它们从自身具有的GPS定位系统中就能够获得自身的定位信息。当接收到代理节点发来的定位信息请求时，将从GPS系统中获得的自身的定位信息发送给代理节点。当代理节点获得了各记账节点、以及发送所述查询请求的业务节点的定位信息后，利用这些定位信息，就能够确定出各记账节点到发送所述查询请求的业务节点的距离。

[0175] 在上述实施例中，获得定位信息采用的是由代理节点主动请求的方式，与处理负荷一样，该定位信息也可以采用由各记账节点、以及发送所述查询请求的业务节点定期向代理节点发送的方式，故不赘述。

[0176] 该实施例的优点是，在确定执行所述方法的记账节点时，不仅考虑到每个记账节点的处理负荷，还考虑到每个记账节点离发送所述查询请求的业务节点的距离。虽然，可能某一记账节点的处理负荷最小，但是该记账节点离发送所述查询请求的业务节点可能非常远，将其选为执行所述方法的记账节点，增加了网络传输负担，也降低了查询处理速度。该实施例综合考虑了距离和处理负荷，比单纯根据距离或处理负荷来确定执行查询的记账节点的方案，既能大致均衡每个记账节点的处理负荷，又不给网络造成太大传输负担。

[0177] 在一个实施例中，如图13所示，步骤430可以包括：

[0178] 步骤4301、基于记账节点子网络中每个记账节点的所述处理负荷，确定每个记账节点的第一分数；

[0179] 步骤4302、基于记账节点子网络中每个记账节点的所述距离，确定每个记账节点的第二分数；

[0180] 步骤4303、基于每个记账节点的第一分数和第二分数，确定执行所述方法的记账节点。

[0181] 在步骤4301中，基于记账节点子网络中每个记账节点的所述处理负荷，确定每个记账节点的第一分数可以采取查找预先设置的处理负荷与第一分数对应关系表的形式。该处理负荷与第一分数对应关系表预先设置，其中处理负荷越大，第一分数越低。例如：

[0182]

处理负荷（未处理完的任务数）	第一分数
0-1	5
2-4	4
5-9	3
10-19	2
20-49	1

[0183]

50以上	0

[0184] 表1处理负荷与第一分数对应关系表

[0185] 步骤4302中，基于记账节点子网络中每个记账节点的所述距离，确定每个记账节点的第二分数可以采取查找预先设置的距离与第二分数对应关系表的形式。该距离与第二分数对应关系表预先设置，其中距离越大，第二分数越低。例如：

[0186]

距离	第二分数
50米之内	5
50-200米	4
200-1000米	3
1000-5000米	2
5000-20000米	1
20000米以上	0

[0187] 表2距离与第二分数对应关系表

[0188] 有了每个记账节点的第一分数和第二分数，就可以根据第一分数和第二分数确定执行所述方法的记账节点。该实施例的优点在于，将记账节点子网络中每个记账节点的所述处理负荷、和记账节点子网络中每个记账节点的所述距离这两个因素对选择执行所述方法的记账节点的影响分数化，提高了选择执行所述方法的记账节点的精确性。

[0189] 在一个实施例中，如图14所示，步骤4303包括：

[0190] 步骤43031、确定每个记账节点的第一分数和第二分数的加权和；

[0191] 步骤43032、基于所述加权和，确定执行所述方法的记账节点。

[0192] 在步骤43031中，确定加权和时，为第一分数和第二分数分配的权重可以是根据经验预设的。

[0193] 在步骤43032中，可以将所述加权和最大的记账节点，确定为接收所述待上链交易信息的记账节点，也可以将加权和大于预定加权和阈值的记账节点中任选一个，作为接收所述待上链交易信息的记账节点。可以认为，只要加权和大于预定加权和阈值，其都是负荷不算太大且距离发送待上链交易信息的业务节点不算太远的，选取哪一个作为执行所述方法的记账节点都是一样的。按照后一种方式，还有利于负载的均衡，防止在相同时间都选择加权和最大的记账节点，又造成该加权和最大的记账节点显然超负荷状态。

[0194] 该实施例的优点是，基于每个记账节点的第一分数和第二分数的加权和，确定接收所述待上链交易信息的记账节点，相比于基于第一分数和第二分数的和或平均值确定接

收所述待上链交易信息的记账节点的方案，充分考虑到了第一分数和第二分数对于确定执行所述方法的记账节点的贡献的差异性，提高了确定执行所述方法的记账节点的合理性。

[0195] 上述确定接收所述待上链交易信息的记账节点的实施例主要针对图1A-1B的在记账节点子网络端没有分支记账节点子网络的情况。但在图1C所示的记账节点子网络端分为分支记账节点子网络的实施例中，则是另外一种情况。

[0196] 在该实施例中，查询请求中带有交易信息类型，例如是供应链金融交易，或电子发票交易，或法定数字货币交易。记账节点子网络中的记账节点预先按照处理的交易信息类型分类，分成的每一类的记账节点分别组成相应的一个分支记账节点子网络，例如，供应链金融交易分支记账节点子网络，或电子发票交易分支记账节点子网络，或法定数字货币交易分支记账节点子网络，每个分支记账节点子网络专门处理与一种交易类型对应的交易类型。因此，代理节点要根据查询请求中携带的交易信息类型，将该查询请求发到相应类型的分支记账节点子网络中的一个记账节点中。为了达到这一点，在代理节点中存储记账节点标识和交易信息类型对应关系表，记账节点标识和处理的交易信息类型对应记录在记账节点标识和交易信息类型对应关系表中。

[0197] 在该实施例中，如图15所示，执行所述方法的记账节点从记账节点子网络中按照以下方式选出：

[0198] 步骤510、获取查询请求中的交易信息类型；

[0199] 步骤520、从记账节点标识和交易信息类型对应关系表中，查找与查询请求中的交易信息类型对应的记账节点标识；

[0200] 步骤530、从找到的记账节点标识的记账节点中，确定接收所述待上链交易信息的记账节点。

[0201] 该实施例的好处是，对于图1C所示的记账节点子网络端分为分支记账节点子网络的体系构架，提出了一种适合该体系构架的合理选择执行所述方法的记账节点的方式。

[0202] 在一个实施例中，查询请求中的交易信息类型字段中包含交易信息类型。步骤510中，可以直接从该交易信息类型字段读出交易信息类型。

[0203] 由于代理节点上设置有记账节点标识和交易信息类型对应关系表，在一个实施例中，步骤520中，从该表中，可以查找到与查询请求中的交易信息类型对应的记账节点标识。

[0204] 如图16所示，在一个实施例中，步骤530包括：

[0205] 步骤5301、确定每个找到的记账节点标识的记账节点的处理负荷；

[0206] 步骤5302、确定每个找到的记账节点标识的记账节点到发送所述查询请求的业务节点的距离；

[0207] 步骤5303、基于所述处理负荷和所述距离，确定执行所述方法的记账节点。

[0208] 步骤5301-5303的具体实现过程与步骤410-430的具体实现过程类似，区别仅在于图16的实施例中确定处理负荷和到发送所述查询请求的业务节点的距离的记账节点的范围仅限于步骤520中找到的与查询请求中的交易信息类型对应的记账节点标识的记账节点，不是记账节点子网络中的所有记账节点，故不赘述。

[0209] 根据本公开的一个实施例，如图19所示，还提供了一种在区块链网络中查询数据区块中的交易信息的记账节点。所述区块链网络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。所述记账节点包括：

[0210] 查询请求接收单元610，用于接收业务节点对数据区块中的交易信息的查询请求；

[0211] 目标业务节点权限数据获取单元620，用于获取该业务节点对应的目标业务节点权限数据，该业务节点有权查询所述目标业务节点权限数据中指示的目标业务节点的交易信息；

[0212] 第一交易信息返回单元630，用于如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0213] 可选地，所述记账节点还包括：

[0214] 第二交易信息返回单元(未示)，用于如果该交易信息的施动方是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息。

[0215] 可选地，所述记账节点还包括：

[0216] 哈希值返回单元(未示)，用于如果交易信息的施动方或受动方既不是所述目标业务节点权限数据中指示的目标业务节点之一，也不是另一交易信息的受动方，而该另一交易信息的受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息的哈希值。

[0217] 可选地，所述查询请求接收单元610用于：

[0218] 接收业务节点对数据区块中的交易信息的查询请求和用特定于该业务节点的私钥对该查询请求生成的签名；

[0219] 所述装置还包括：

[0220] 签名验证单元(未示)，用于用特定于该业务节点的公钥对该签名进行验证，其中，只有在验证成功的情况下，才获取该业务节点对应的目标业务节点权限数据。

[0221] 可选地，所述签名验证单元用于：

[0222] 获取特定于该业务节点的公钥；

[0223] 利用所述特定于该业务节点的公钥对所述签名进行解密，得到所述查询请求的摘要；

[0224] 利用预定摘要算法对该查询请求计算摘要；

[0225] 如果计算出的摘要与解密得到的摘要一致，则验证成功。

[0226] 可选地，所述记账节点还包括：

[0227] 智能合约生成单元，用于生成业务节点与区块链运营方的智能合约；

[0228] 同步单元，用于将生成的智能合约同步到记账节点子网络中的各记账节点存储。

[0229] 所述目标业务节点权限数据获取单元进一步用于：

[0230] 从该记账节点存储的该业务节点与区块链运营方的智能合约中，获取该业务节点对应的目标业务节点权限数据。

[0231] 可选地，所述装置还包括：

[0232] 智能合约生成单元，用于生成业务节点与区块链运营方的智能合约；

[0233] 上链单元，用于将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上。

[0234] 所述目标业务节点权限数据获取单元进一步用于：

[0235] 从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约；

[0236] 从该智能合约中，获取该业务节点对应的目标业务节点权限数据。

[0237] 可选地，所述智能合约生成单元进一步用于：

[0238] 发布合约模板，所述合约模板中含有合约函数；

[0239] 接收利用所述合约函数设置的该业务节点的目标业务节点权限数据；

[0240] 将所述目标业务节点权限数据整合到所述合约模板中，形成该业务节点与区块链运营方的智能合约。

[0241] 可选地，所述智能合约生成单元进一步用于：

[0242] 接收来自业务节点的智能合约生成请求，所述智能合约生成请求中指示业务节点所属单位下属单位或管辖单位的业务节点；

[0243] 根据业务节点所属单位下属单位或管辖单位的业务节点，确定目标业务节点权限数据；

[0244] 将所述权限数据整合到所述合约模板中，形成该业务节点与区块链运营方的智能合约。

[0245] 可选地，所述根据业务节点所属单位下属单位或管辖单位的业务节点，确定目标业务节点权限数据，包括：

[0246] 将所述业务节点、所述业务节点所属单位下属单位或管辖单位的业务节点，确定为目标业务节点权限数据中指示的目标业务节点。

[0247] 可选地，所述执行所述方法的记账节点从记账节点子网络中按照以下方式选出：

[0248] 获取记账节点子网络中每个记账节点的处理负荷；

[0249] 确定记账节点子网络中每个记账节点到发送所述查询请求的业务节点的距离；

[0250] 基于所述处理负荷和所述距离，确定执行所述方法的记账节点。

[0251] 可选地，所述基于所述处理负荷和所述距离，确定执行所述方法的记账节点，包括：

[0252] 基于记账节点子网络中每个记账节点的所述处理负荷，确定每个记账节点的第一分数；

[0253] 基于记账节点子网络中每个记账节点的所述距离，确定每个记账节点的第二分数；

[0254] 基于每个记账节点的第一分数和第二分数，确定执行所述方法的记账节点。

[0255] 根据本公开实施例的在区块链网络中查询数据区块中的交易信息的方法可以由图20的在区块链网络中查询数据区块中的交易信息的记账节点21实现。下面参照图20来描述根据本公开实施例的在区块链网络中查询数据区块中的交易信息的记账节点21。图20显示的在区块链网络中查询数据区块中的交易信息的记账节点21仅仅是一个示例，不应对本公开实施例的功能和使用范围带来任何限制。

[0256] 如图20所示，在区块链网络中查询数据区块中的交易信息的记账节点21以通用计算设备的形式表现。在区块链网络中查询数据区块中的交易信息的记账节点21的组件可以包括但不限于：上述至少一个处理单元810、上述至少一个存储单元820、连接不同系统组件(包括存储单元820和处理单元810)的总线830。

[0257] 其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元810执行，使得所述处理单元810执行本说明书上述示例性方法的描述部分中描述的根据本发明各种示例性实施方式的步骤。例如，所述处理单元810可以执行如图6中所示的各个步骤。

[0258] 存储单元820可以包括易失性存储单元形式的可读介质，例如随机存取存储单元(RAM)8201和/或高速缓存存储单元8202，还可以进一步包括只读存储单元(ROM)8203。

[0259] 存储单元820还可以包括具有一组(至少一个)程序模块8205的程序/实用工具8204，这样的程序模块8205包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

[0260] 总线830可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

[0261] 在区块链网络中查询数据区块中的交易信息的记账节点21也可以与一个或多个外部设备700(例如键盘、指向设备、蓝牙设备等)通信，还可与一个或者多个使得用户能与该在区块链网络中查询数据区块中的交易信息的在区块链网络中查询数据区块中的交易信息的记账节点21交互的设备通信，和/或与使得该在区块链网络中查询数据区块中的交易信息的记账节点21能与一个或多个其它计算设备进行通信的任何设备(例如路由器、调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口650进行。并且，在区块链网络中查询数据区块中的交易信息的记账节点21还可以通过网络适配器860与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器860通过总线830与在区块链网络中查询数据区块中的交易信息的记账节点21的其它模块通信。应当明白，尽管图中未示出，可以结合在区块链网络中查询数据区块中的交易信息的记账节点21使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0262] 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，根据本公开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、终端装置、或者网络设备等)执行根据本公开实施方式的方法。

[0263] 在本公开的示例性实施例中，还提供了一种计算机程序介质，其上存储有计算机可读指令，当所述计算机可读指令被计算机的处理器执行时，使计算机执行上述方法实施例部分描述的方法。

[0264] 根据本公开的一个实施例，还提供了一种用于实现上述方法实施例中的方法的程序产品，其可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备，例如个人电脑上运行。然而，本发明的程序产品不限于此，在本文件中，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。

[0265] 所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、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。可读存储介质的更具体的例子(非穷举的列表)包括:具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

[0266] 计算机可读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，其中承载了可读程序代码。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。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、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。

[0267] 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、光缆、RF等等，或者上述的任意合适的组合。

[0268] 可以以一种或多种程序设计语言的任意组合来编写用于执行本发明操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算设备上执行、部分地在用户设备上执行、作为一个独立的软件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网(LAN)或广域网(WAN)，连接到用户计算设备，或者，可以连接到外部计算设备(例如利用因特网服务提供商来通过因特网连接)。

[0269] 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，根据本公开的实施方式，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。

[0270] 此外，尽管在附图中以特定顺序描述了本公开中方法的各个步骤，但是，这并非要求或者暗示必须按照该特定顺序来执行这些步骤，或是必须执行全部所示的步骤才能实现期望的结果。附加的或备选的，可以省略某些步骤，将多个步骤合并为一个步骤执行，以及/或者将一个步骤分解为多个步骤执行等。

[0271] 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，根据本公开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、移动终端、或者网络设备等)执行根据本公开实施方式的方法。

[0272] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其它实施方案。本申请旨在涵盖本公开的任何变型、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公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由所附的权利要求指出。

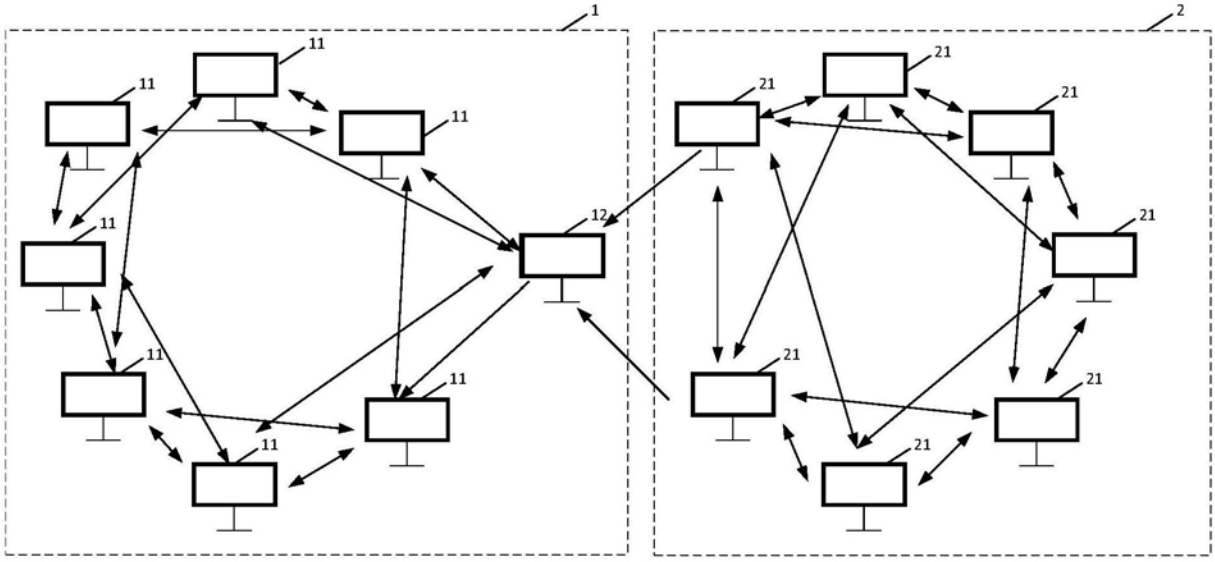


图1A

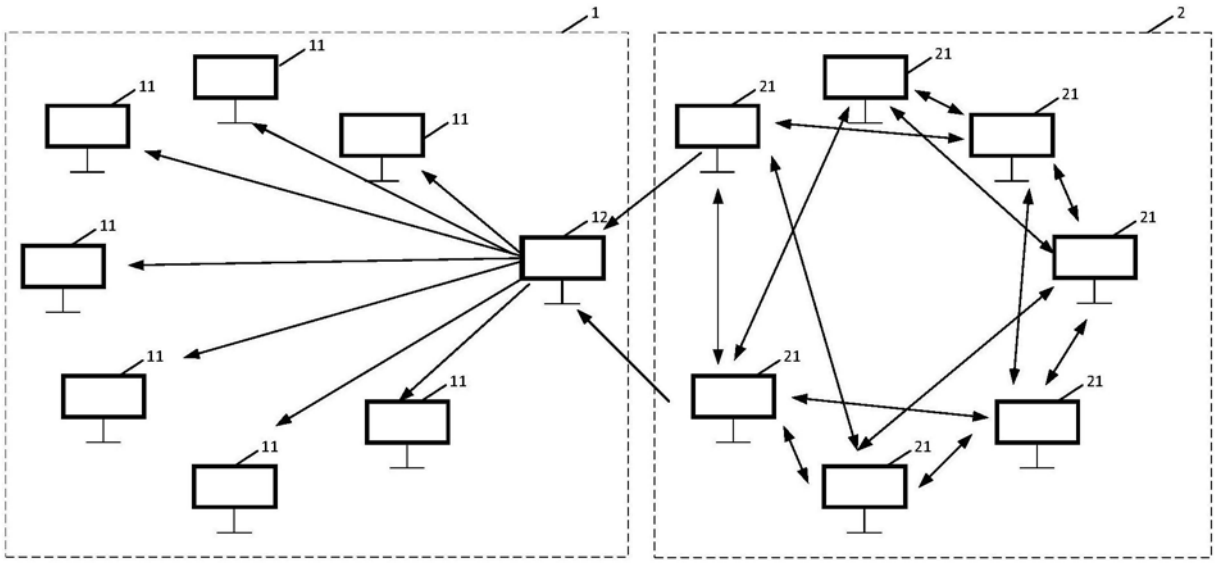


图1B

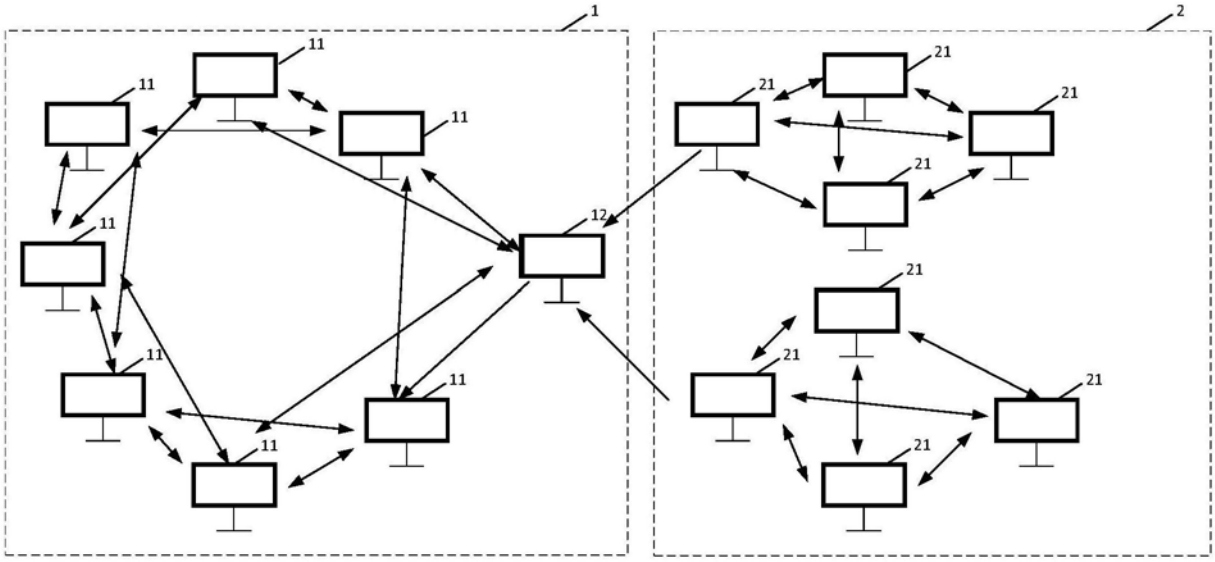

1
11
11
11
11
11
11
11
12
2
21
21
21
21
21
21
21
21

图1C

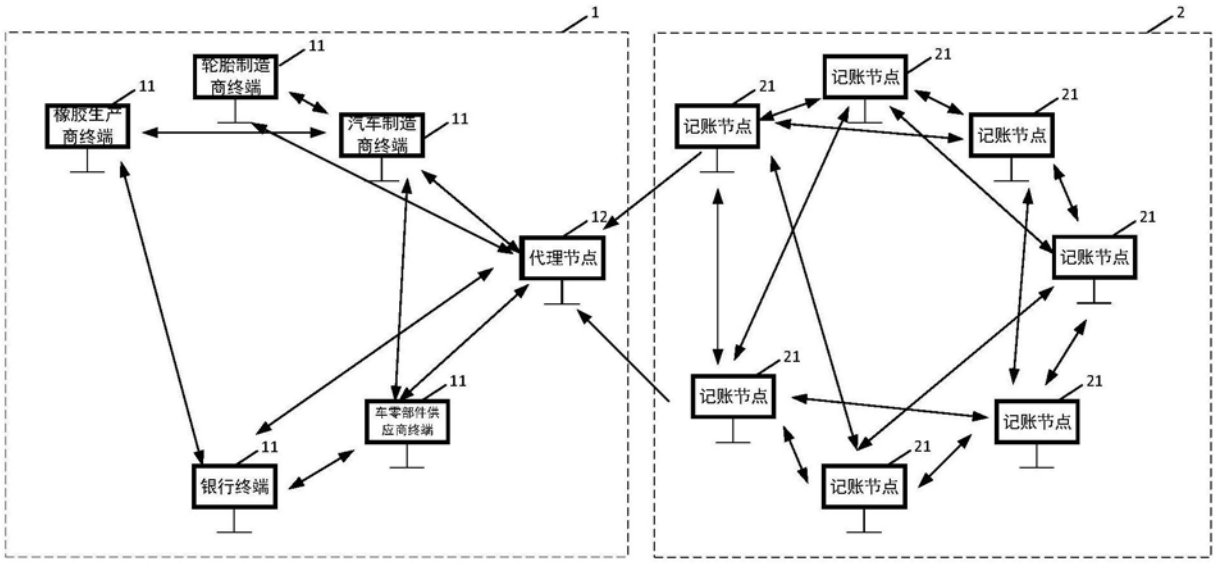

1
轮胎制造商终端
11
橡胶生产商终端
11
汽车制造商终端
11
代理节点
12
车零部件供应商终端
11
银行终端
11
2
记账节点
21
记账节点
21
记账节点
21
记账节点
21
记账节点
21
记账节点
21
记账节点
21

图2A

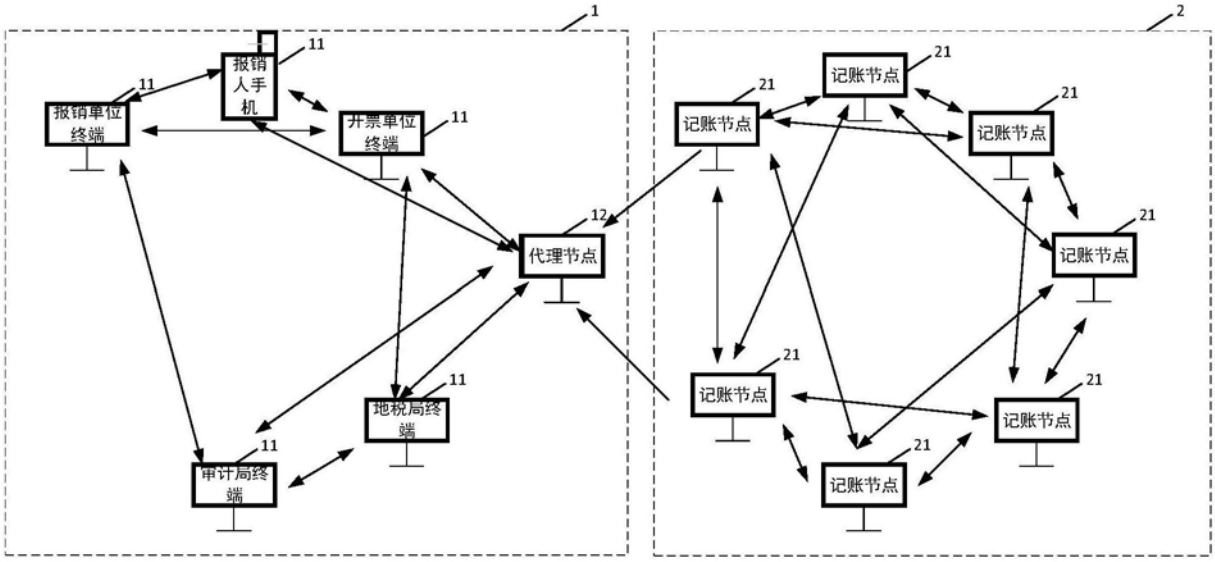

1
报销人手机
报销单位终端
开票单位终端
代理节点
地税局终端
审计局终端
11
12
2
记账节点
21

图2B

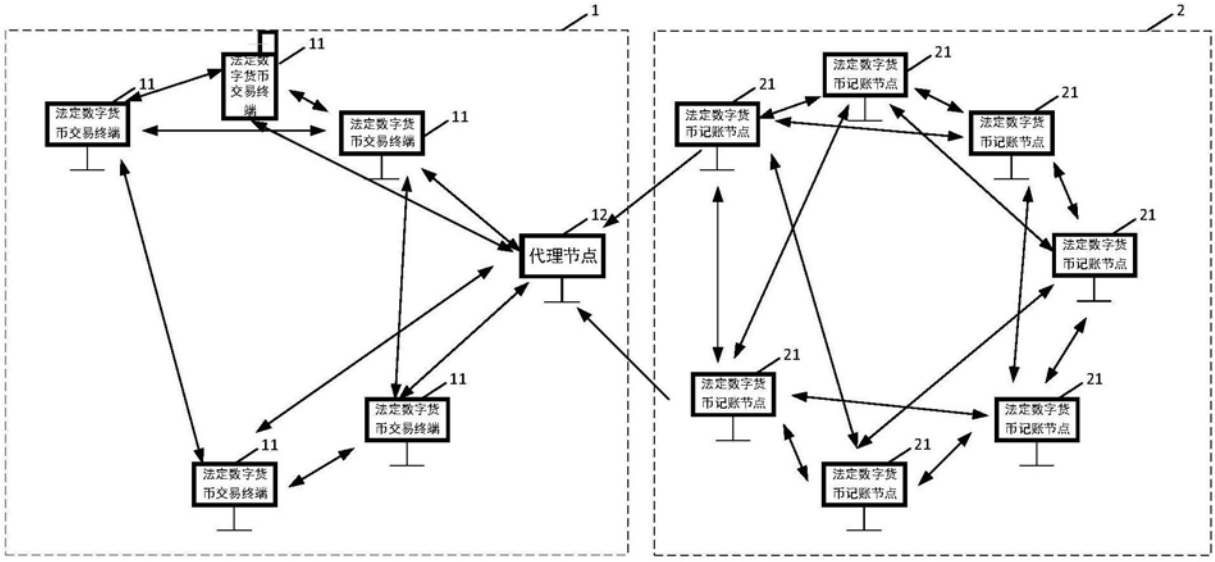

1
法定数字货币交易终端
代理节点
11
12
2
法定数字货币记账节点
21

图2C

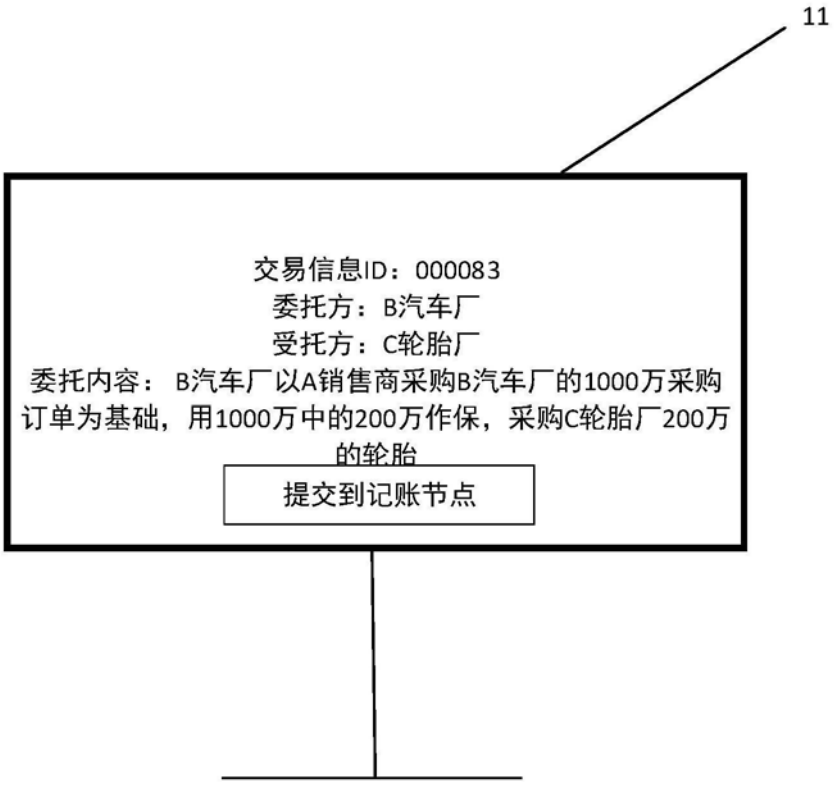

11
交易信息ID：000083
委托方：B汽车厂
受托方：C轮胎厂
委托内容： B汽车厂以A销售商采购B汽车厂的1000万采购订单为基础，用1000万中的200万作保，采购C轮胎厂200万的轮胎
提交到记账节点

图3A

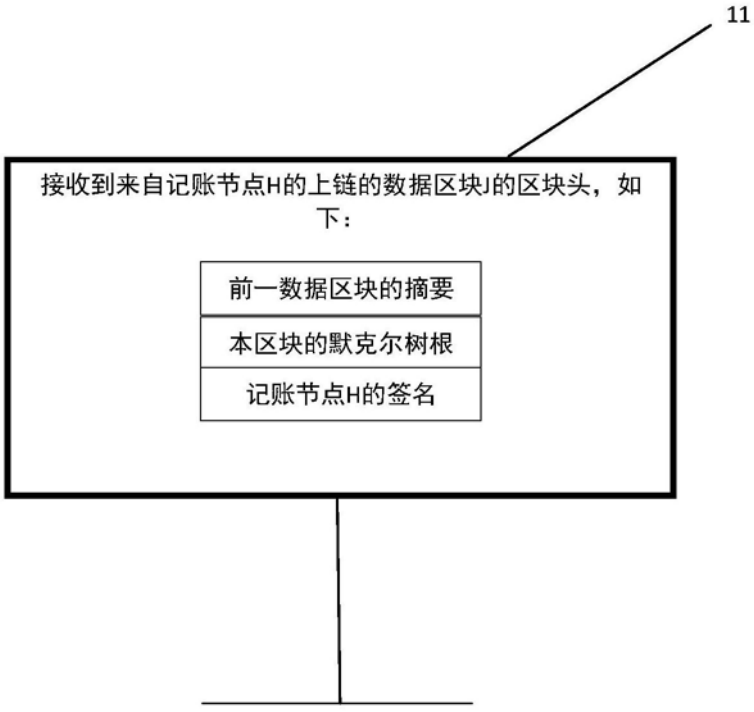

11
接收到来自记账节点H的上链的数据区块J的区块头，如下：
前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名

图3B

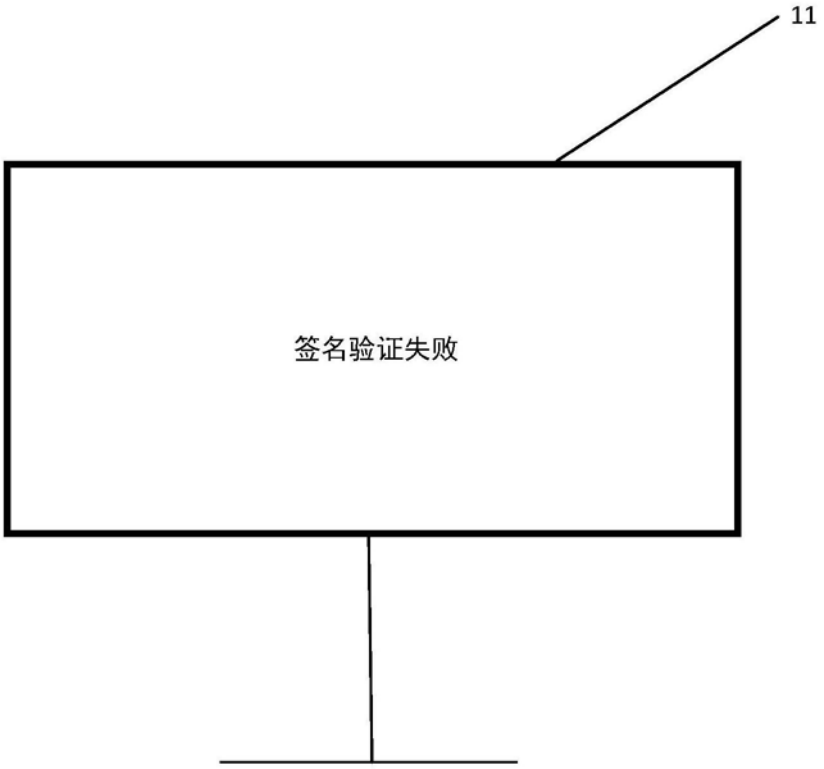


图3C

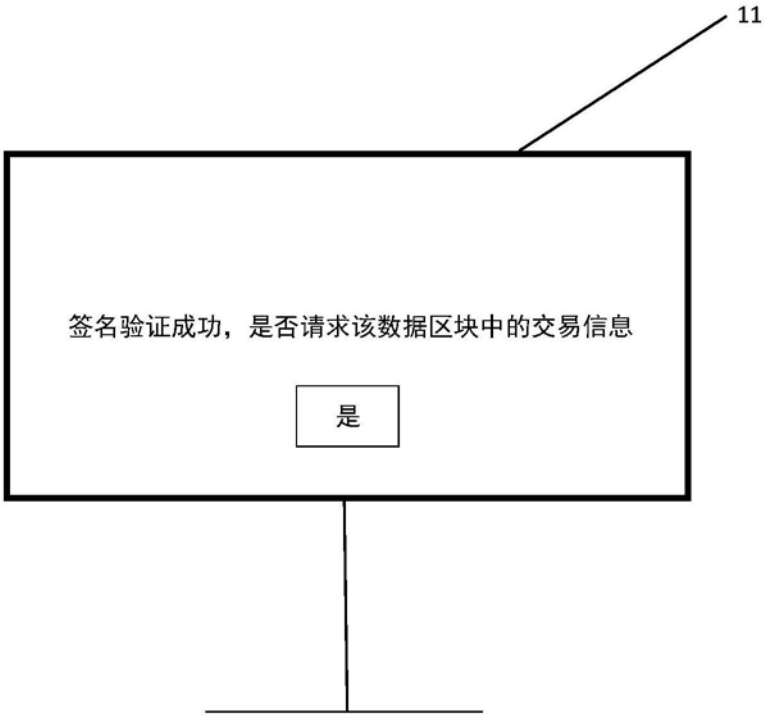


图3D

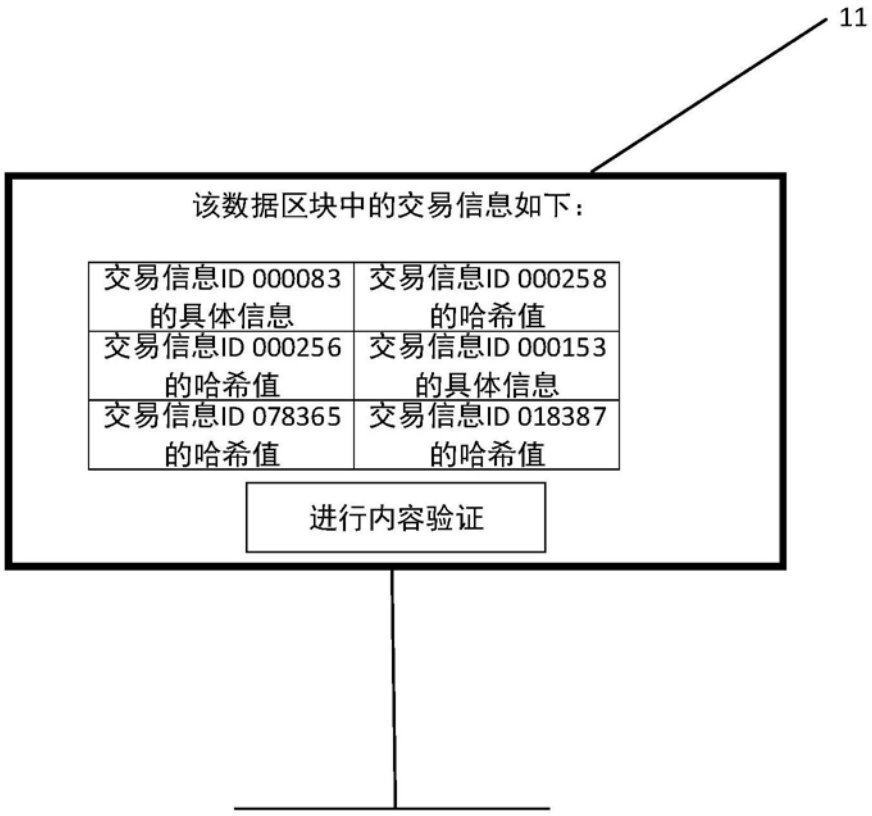

11
该数据区块中的交易信息如下：
交易信息ID 000083的具体信息
交易信息ID 000258的哈希值
交易信息ID 000256的哈希值
交易信息ID 000153的具体信息
交易信息ID 078365的哈希值
交易信息ID 018387的哈希值
进行内容验证

图3E

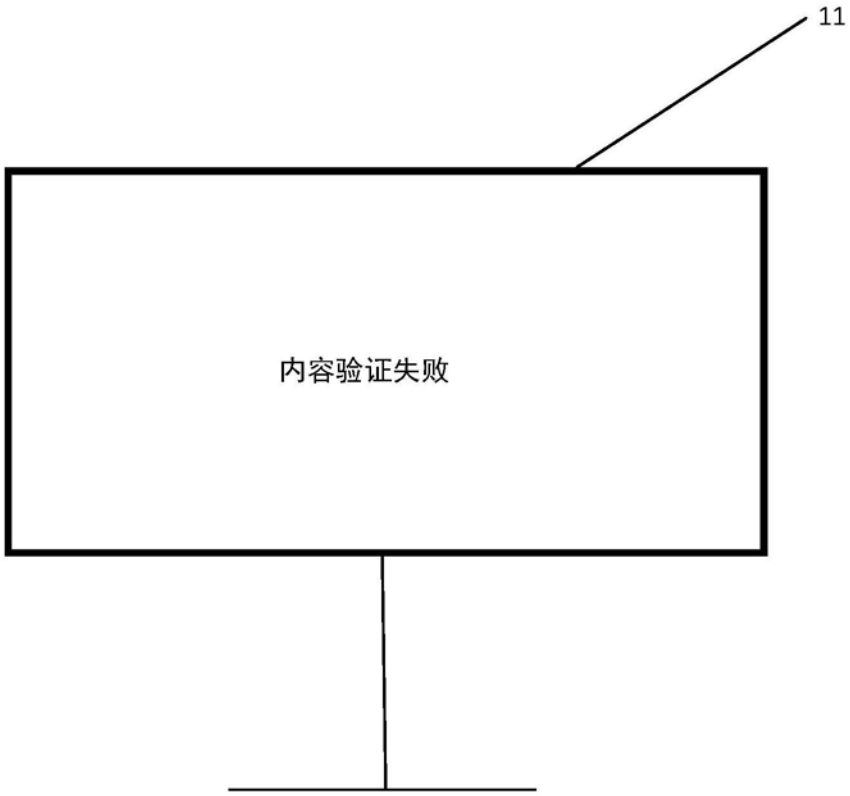


图3F

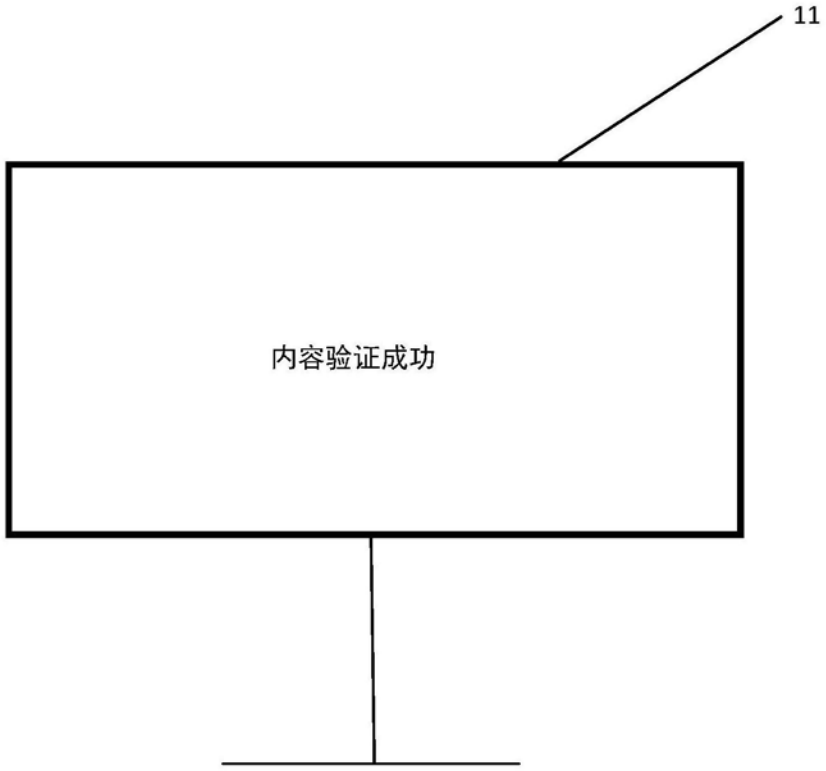


图3G

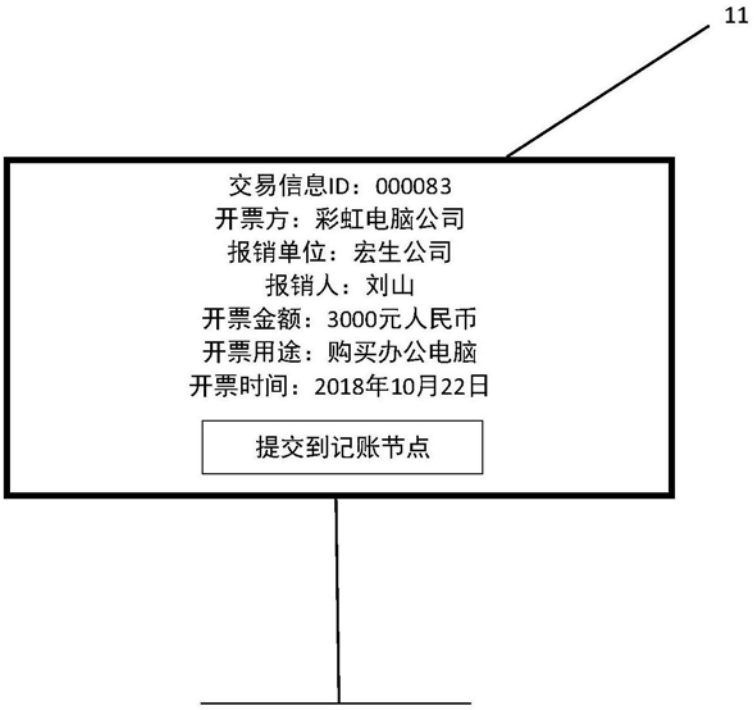

11
交易信息ID：000083
开票方：彩虹电脑公司
报销单位：宏生公司
报销人：刘山
开票金额：3000元人民币
开票用途：购买办公电脑
开票时间：2018年10月22日
提交到记账节点

图4A

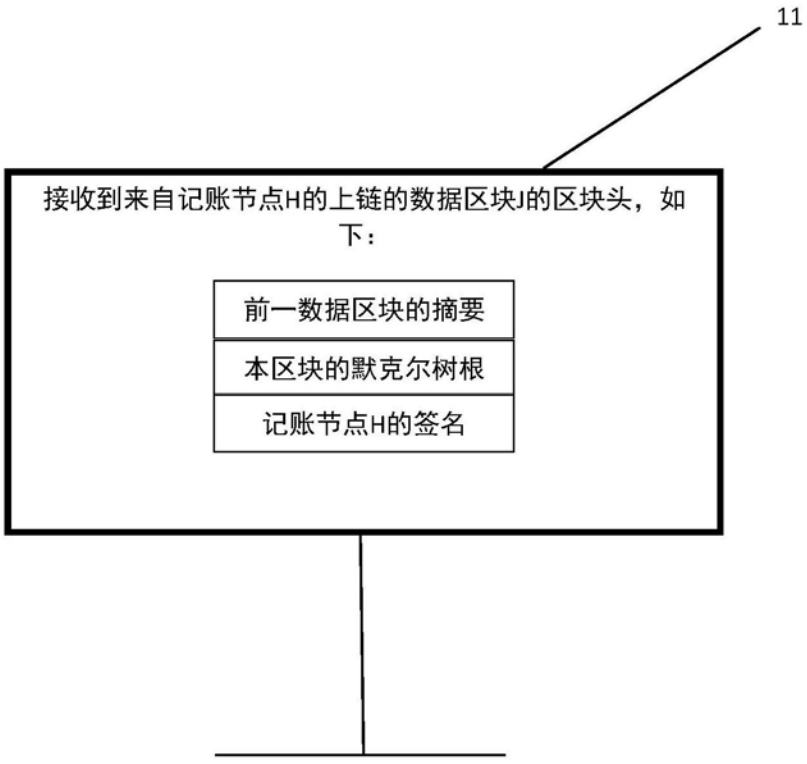

11
接收到来自记账节点H的上链的数据区块J的区块头，如下：
前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名

图4B

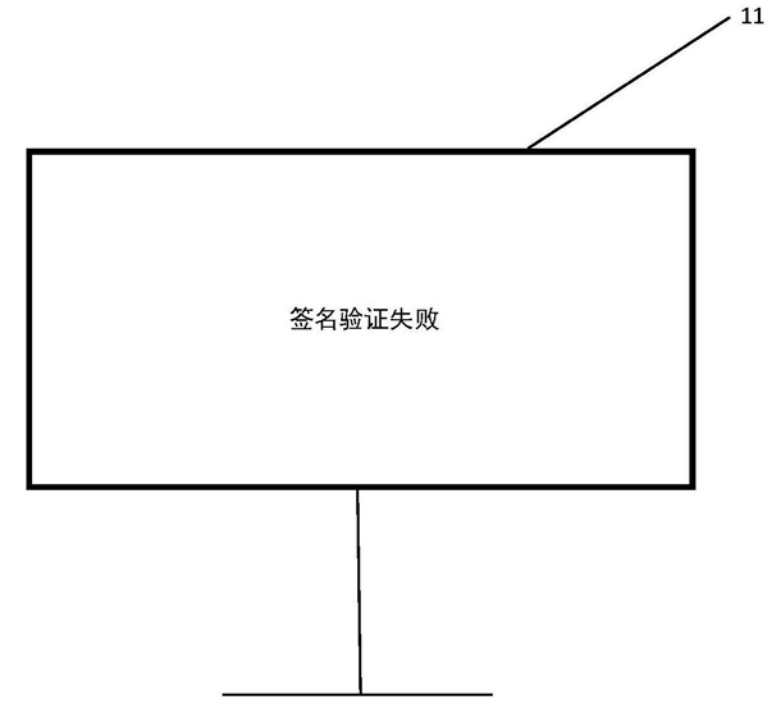


图4C

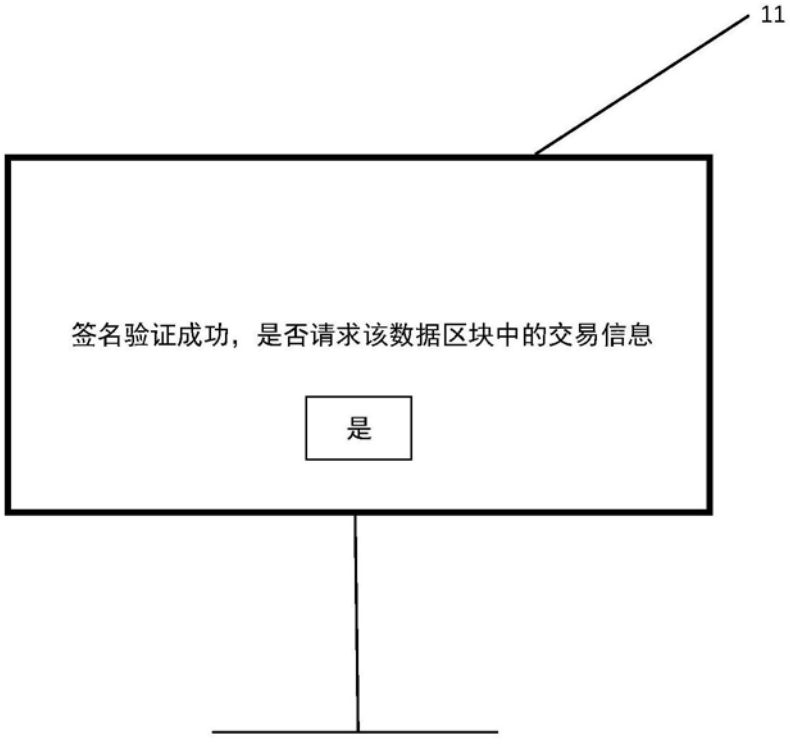


图4D

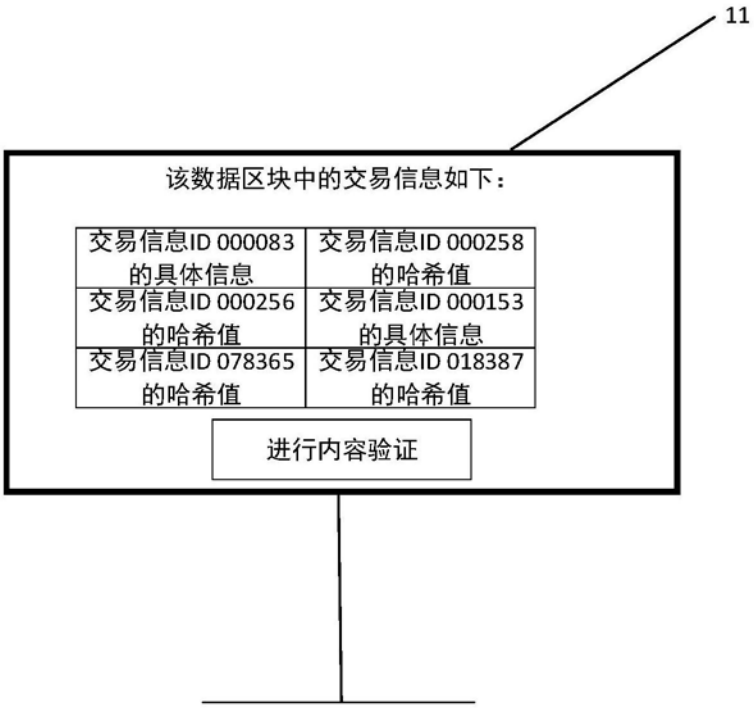

11
该数据区块中的交易信息如下：
交易信息ID 000083的具体信息
交易信息ID 000258的哈希值
交易信息ID 000256的哈希值
交易信息ID 000153的具体信息
交易信息ID 078365的哈希值
交易信息ID 018387的哈希值
进行内容验证

图4E

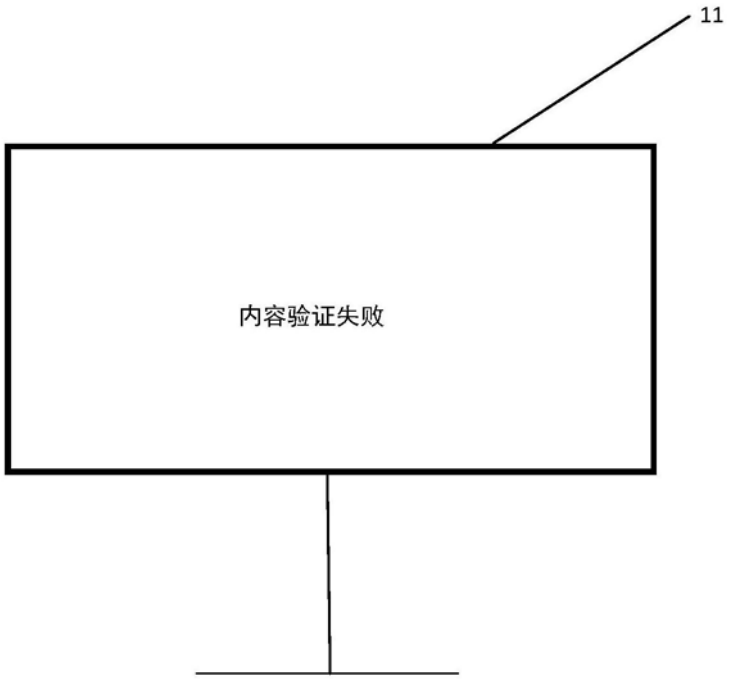

11
内容验证失败

图4F

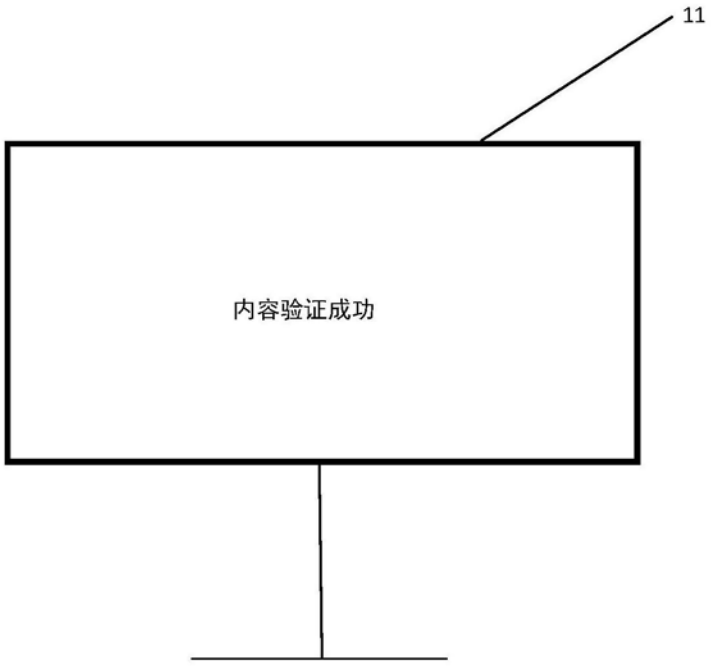

11
内容验证成功

图4G

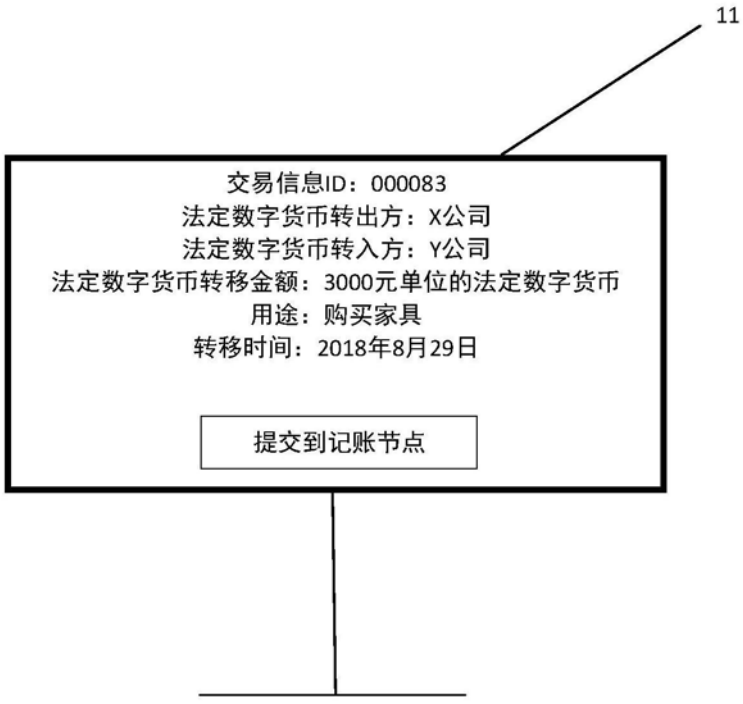

11
交易信息ID：000083
法定数字货币转出方：X公司
法定数字货币转入方：Y公司
法定数字货币转移金额：3000元单位的法定数字货币
用途：购买家具
转移时间：2018年8月29日
提交到记账节点

图5A

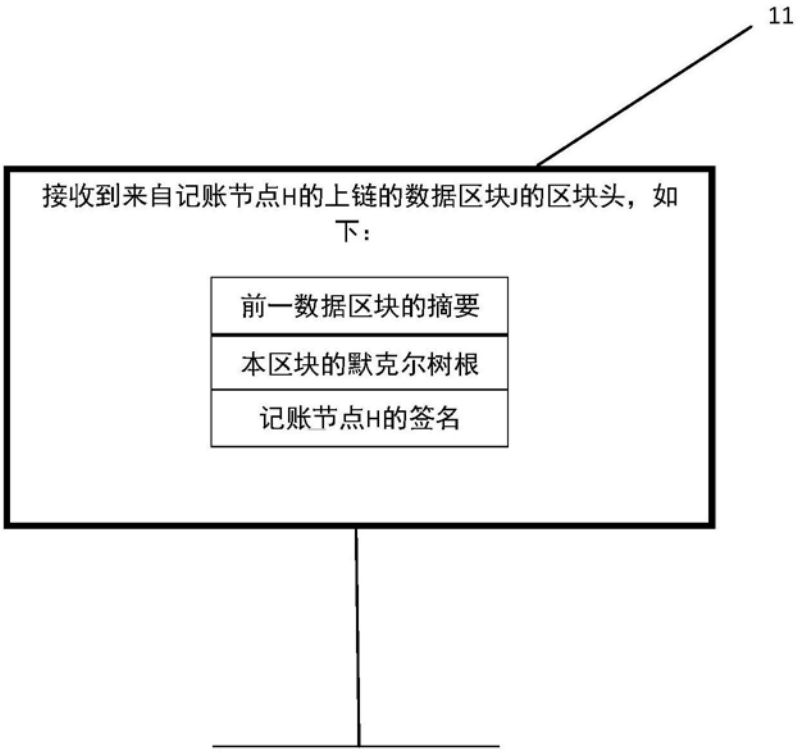

11
接收到来自记账节点H的上链的数据区块J的区块头，如下：
前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名

图5B

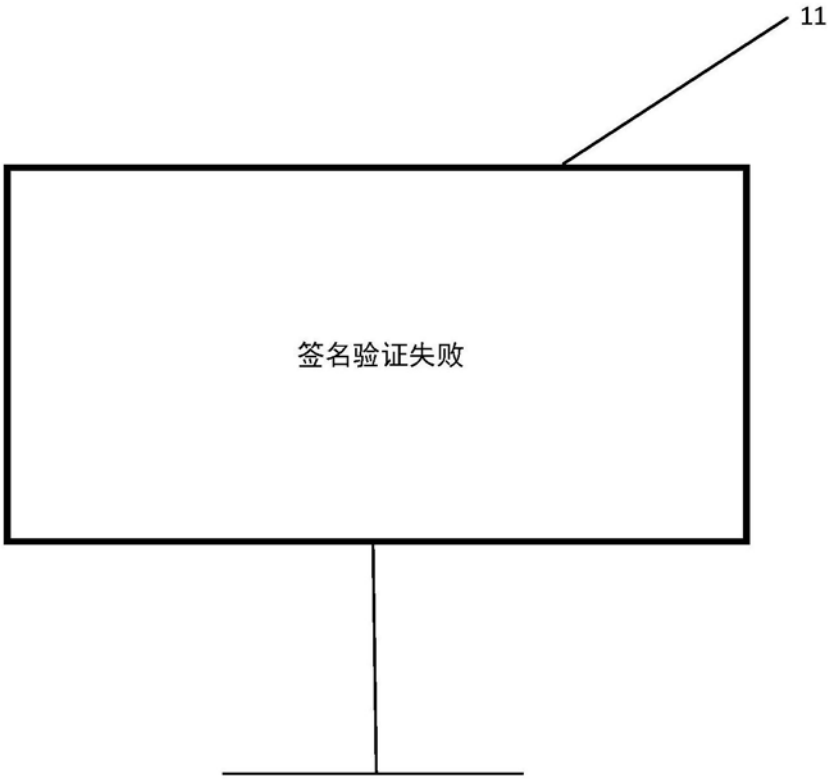

11
签名验证失败

图5C

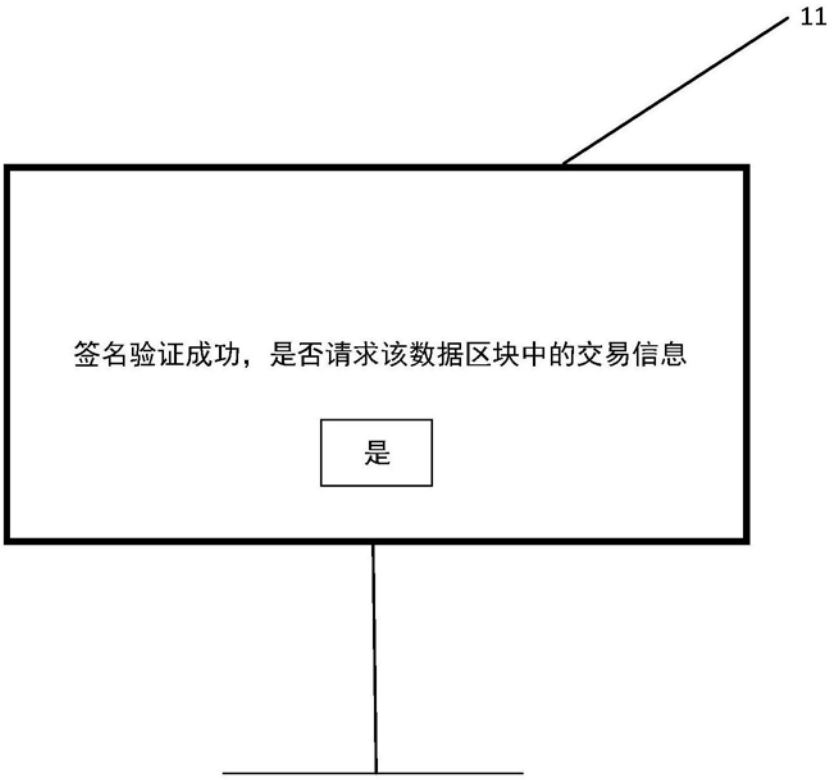

11
签名验证成功，是否请求该数据区块中的交易信息
是

图5D

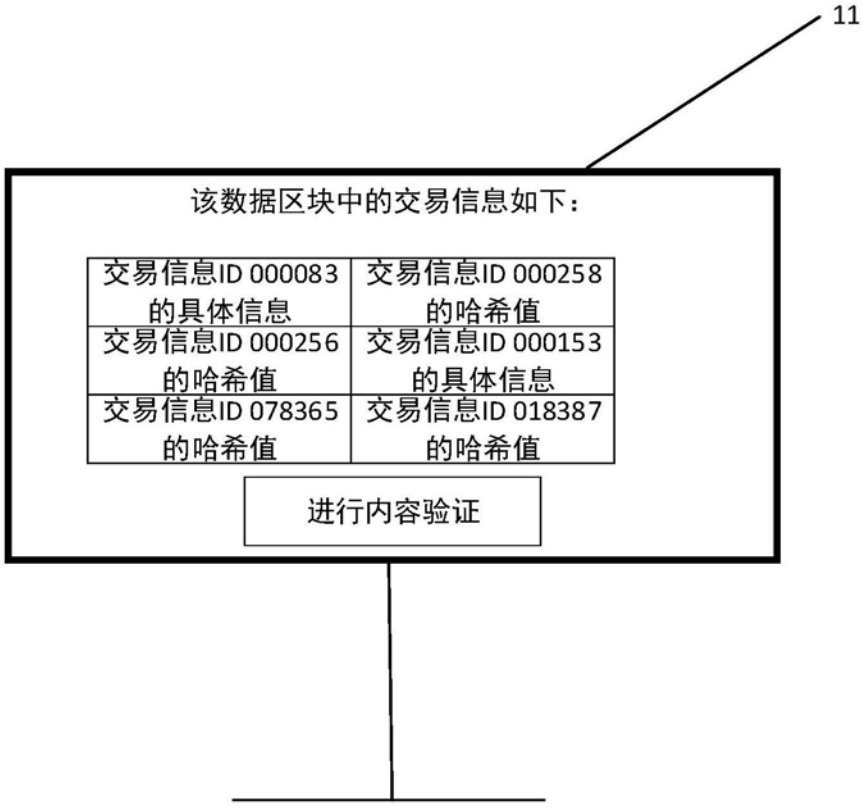

11
该数据区块中的交易信息如下：
交易信息ID 000083 的具体信息
交易信息ID 000258 的哈希值
交易信息ID 000256 的哈希值
交易信息ID 000153 的具体信息
交易信息ID 078365 的哈希值
交易信息ID 018387 的哈希值
进行内容验证

图5E

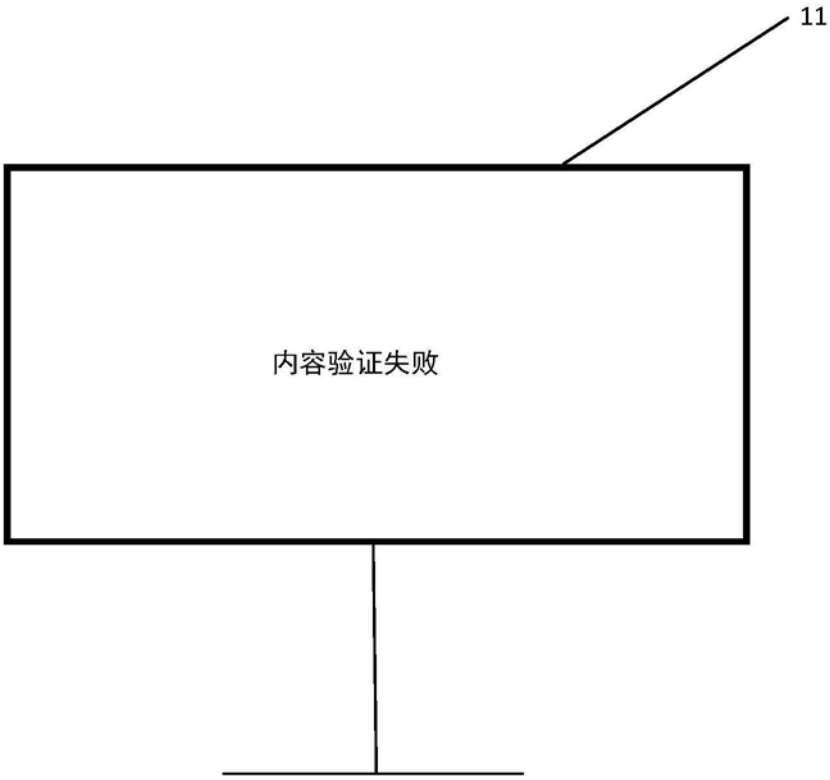


图5F

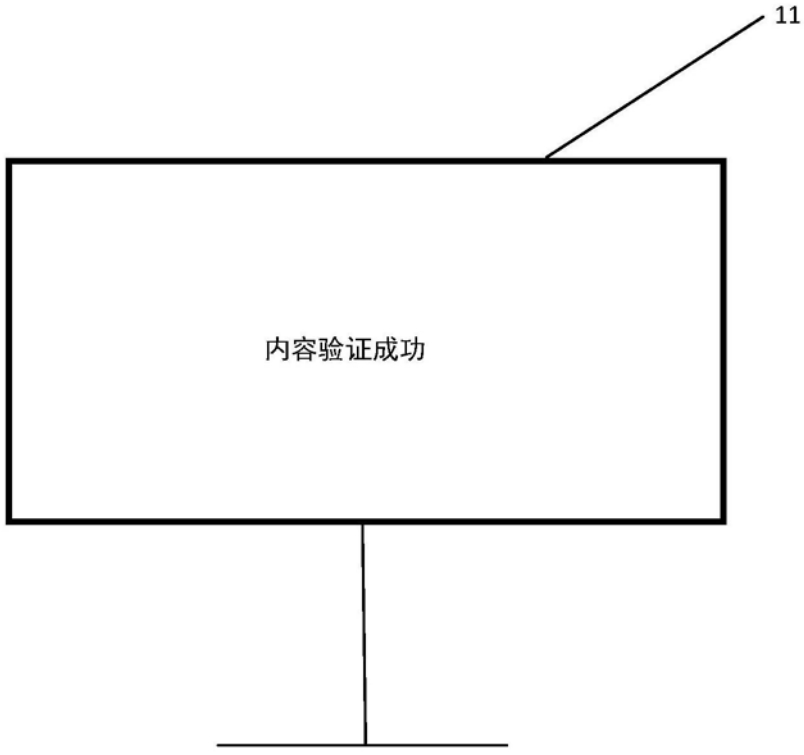


图5G

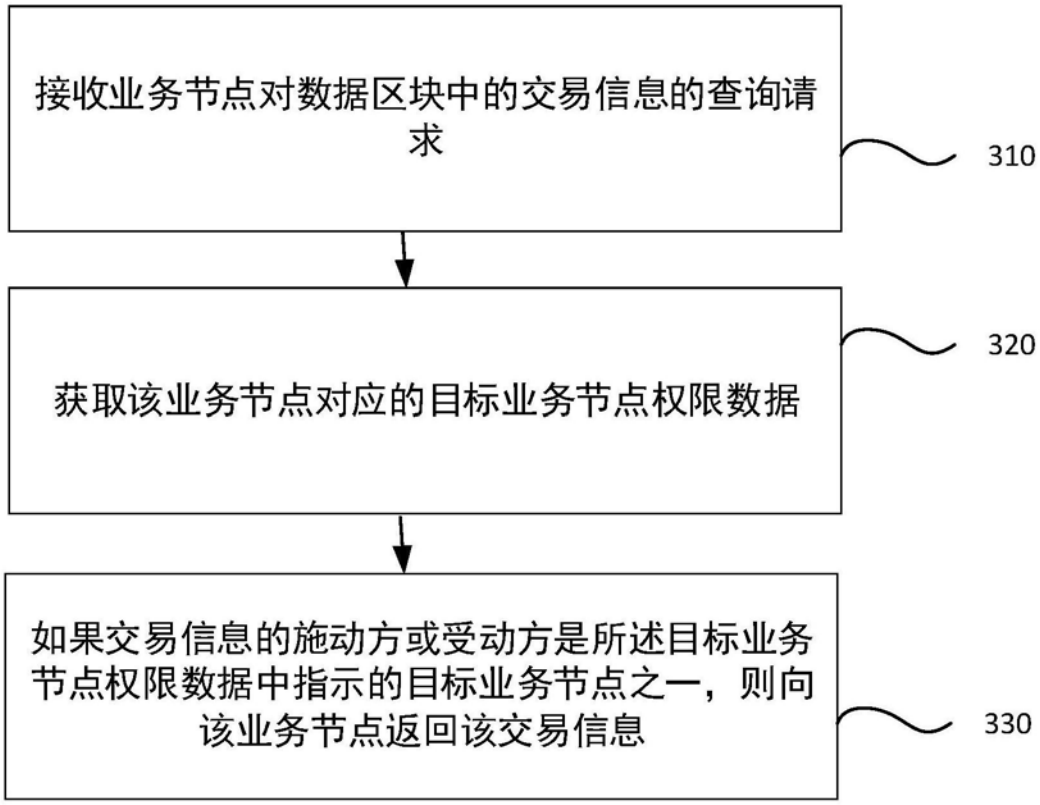

接收业务节点对数据区块中的交易信息的查询请求
310
获取该业务节点对应的目标业务节点权限数据
320
如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息
330

图6

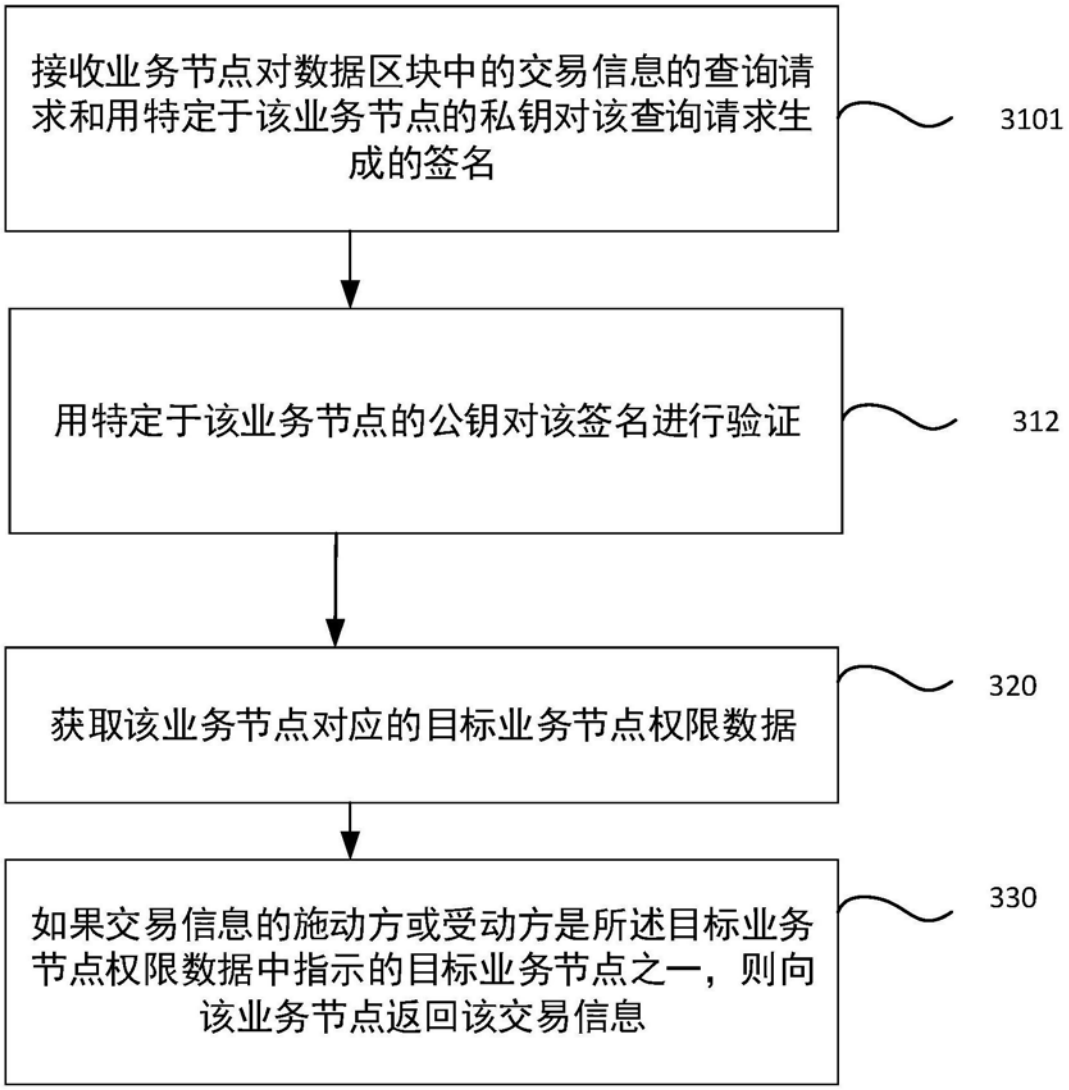

接收业务节点对数据区块中的交易信息的查询请求和用特定于该业务节点的私钥对该查询请求生成的签名
3101
用特定于该业务节点的公钥对该签名进行验证
312
获取该业务节点对应的目标业务节点权限数据
320
如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息
330

图7

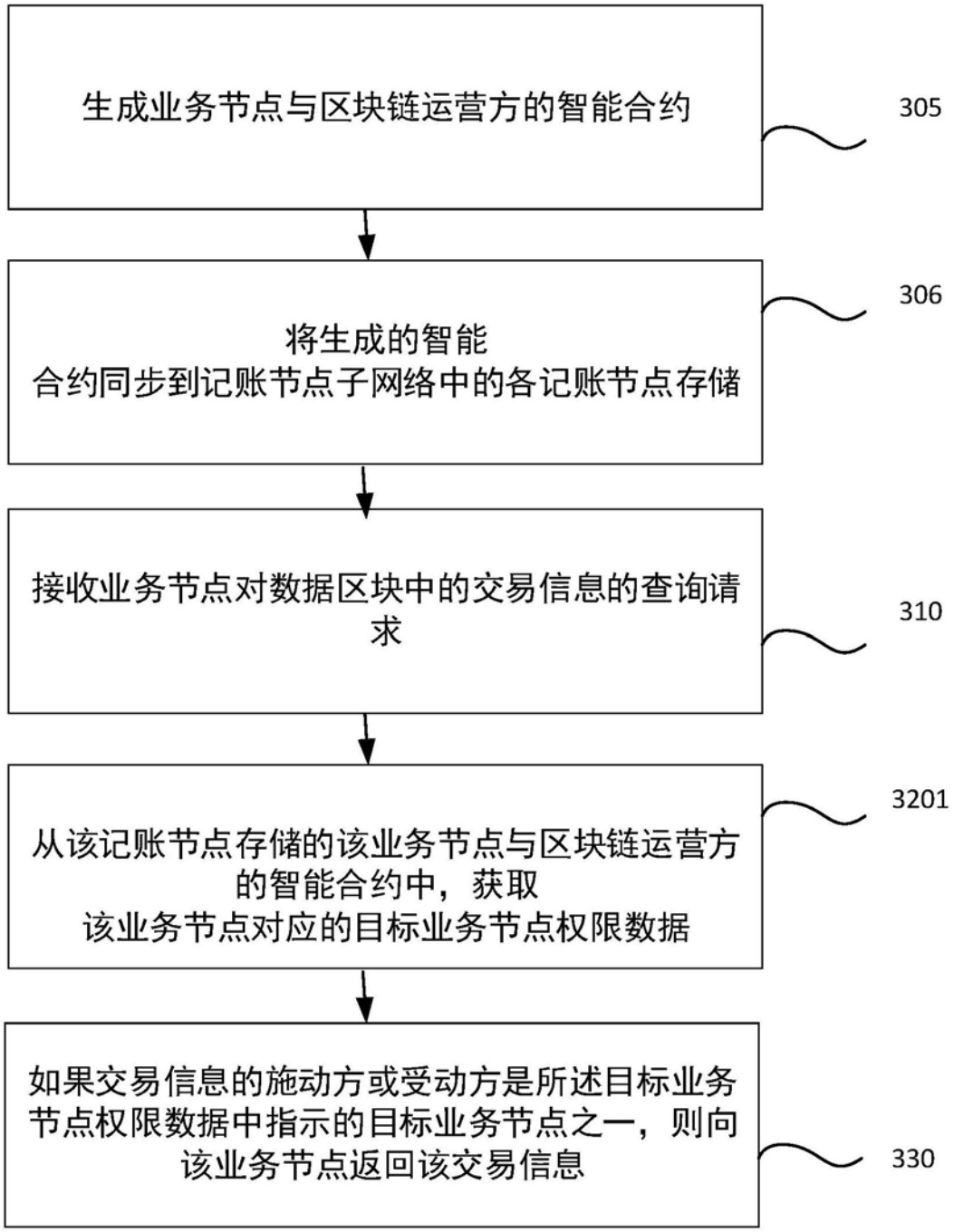

生成业务节点与区块链运营方的智能合约
305
将生成的智能
合约同步到记账节点子网络中的各记账节点存储
306
接收业务节点对数据区块中的交易信息的查询请求
310
从该记账节点存储的该业务节点与区块链运营方的智能合约中，获取
该业务节点对应的目标业务节点权限数据
3201
如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息
330

图8

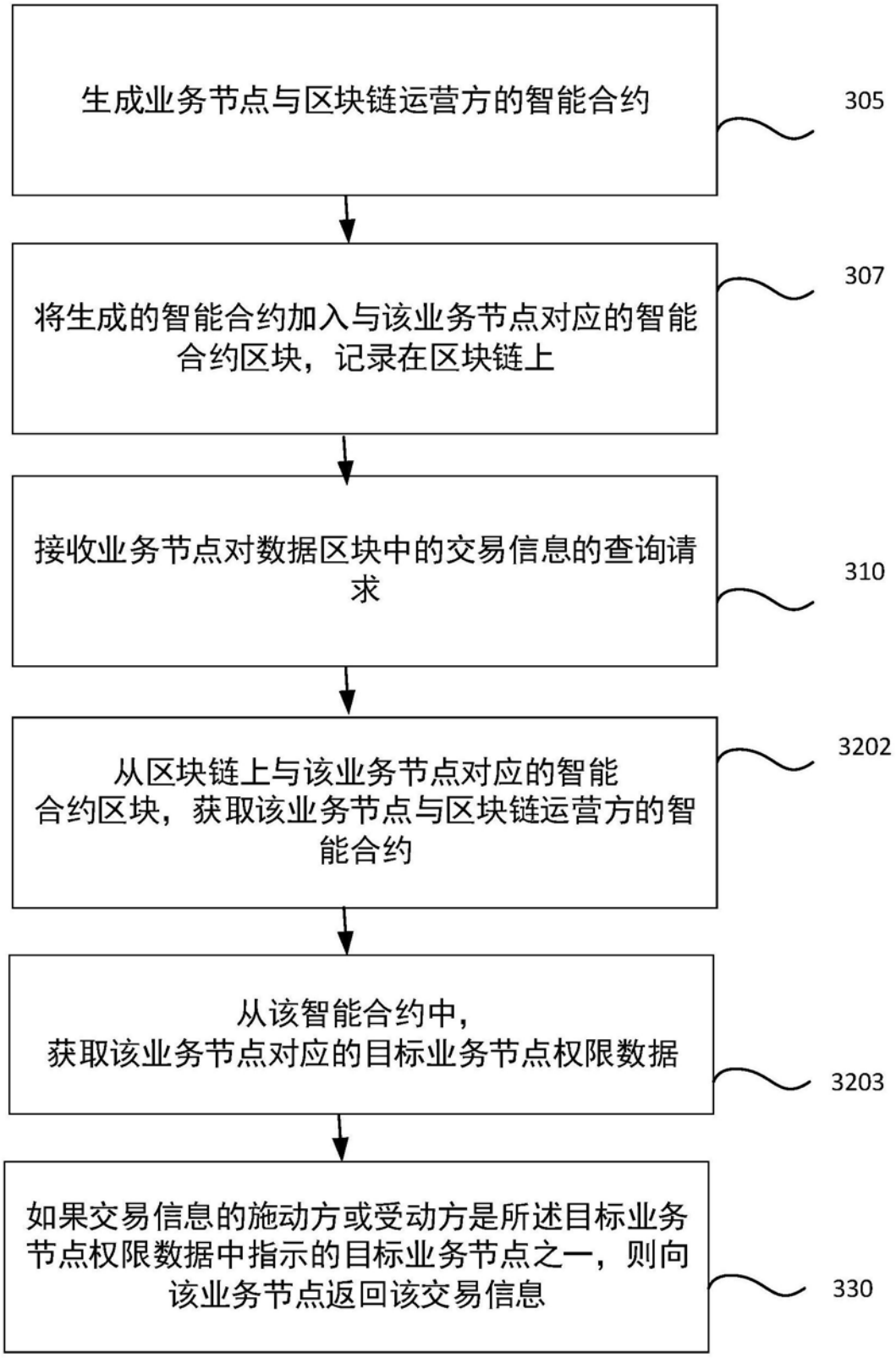

生成业务节点与区块链运营方的智能合约
305
将生成的智能合约加入与该业务节点对应的智能合约区块，记录在区块链上
307
接收业务节点对数据区块中的交易信息的查询请求
310
从区块链上与该业务节点对应的智能合约区块，获取该业务节点与区块链运营方的智能合约
3202
从该智能合约中，获取该业务节点对应的目标业务节点权限数据
3203
如果交易信息的施动方或受动方是所述目标业务节点权限数据中指示的目标业务节点之一，则向该业务节点返回该交易信息
330

图9

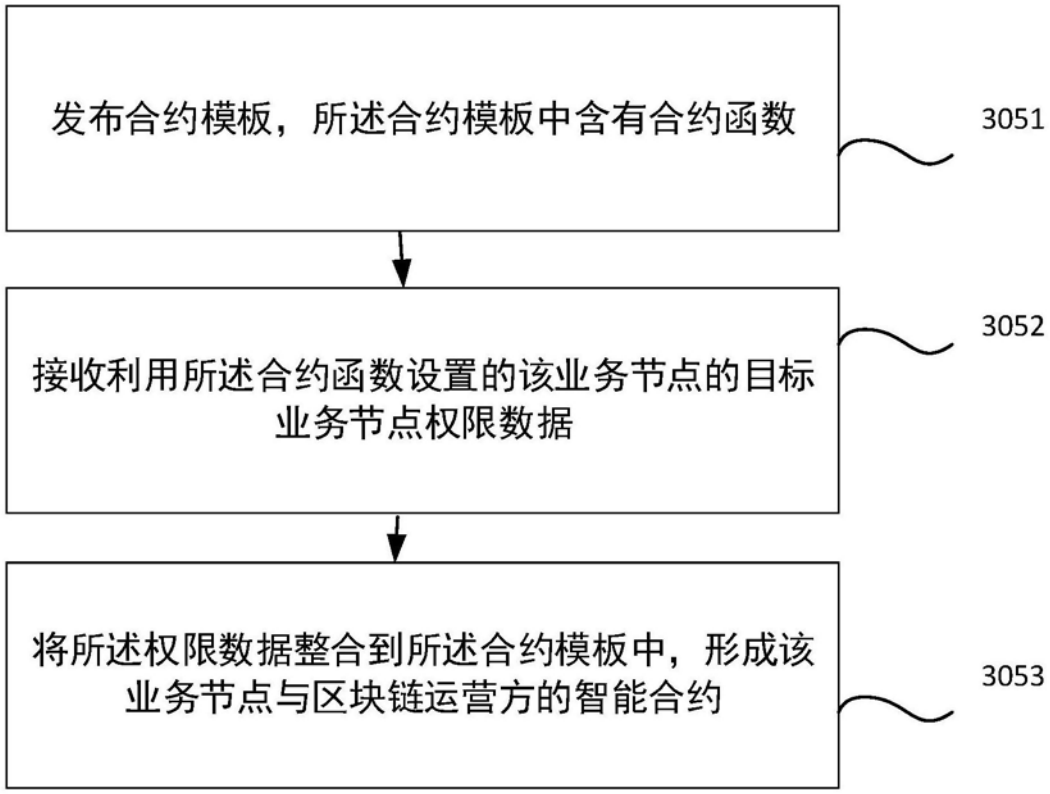

发布合约模板，所述合约模板中含有合约函数
3051
接收利用所述合约函数设置的该业务节点的目标业务节点权限数据
3052
将所述权限数据整合到所述合约模板中，形成该业务节点与区块链运营方的智能合约
3053

图10

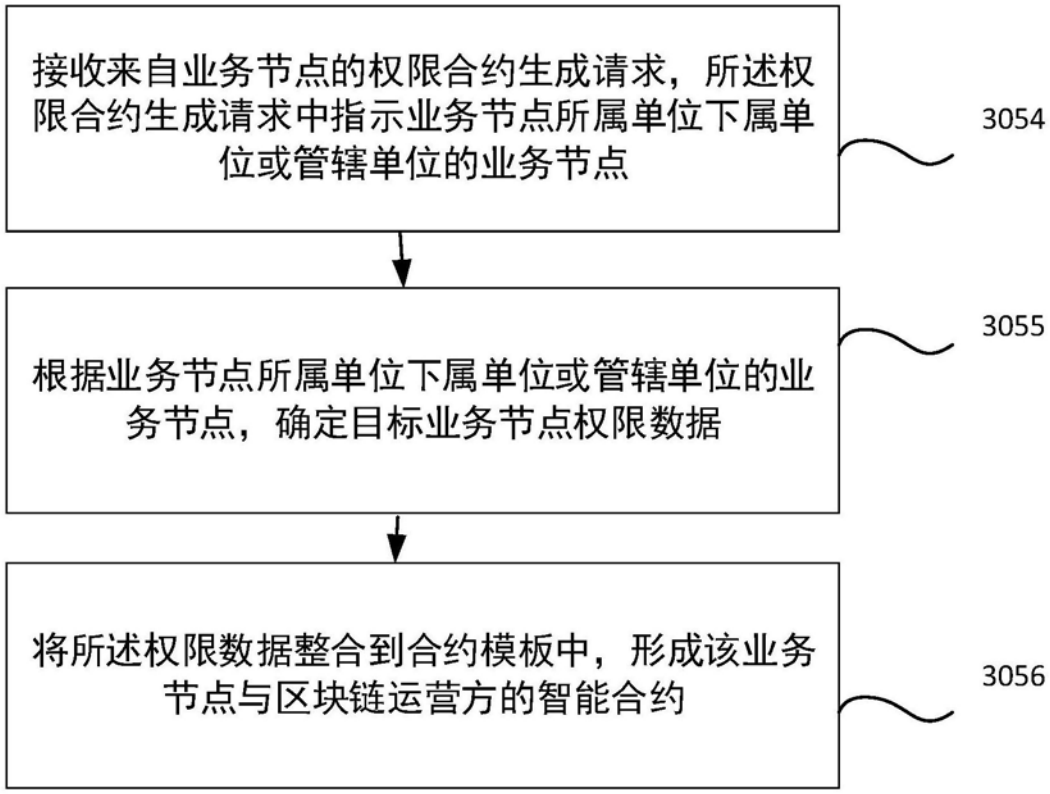

接收来自业务节点的权限合约生成请求，所述权限合约生成请求中指示业务节点所属单位下属单位或管辖单位的业务节点
3054
根据业务节点所属单位下属单位或管辖单位的业务节点，确定目标业务节点权限数据
3055
将所述权限数据整合到合约模板中，形成该业务节点与区块链运营方的智能合约
3056

图11

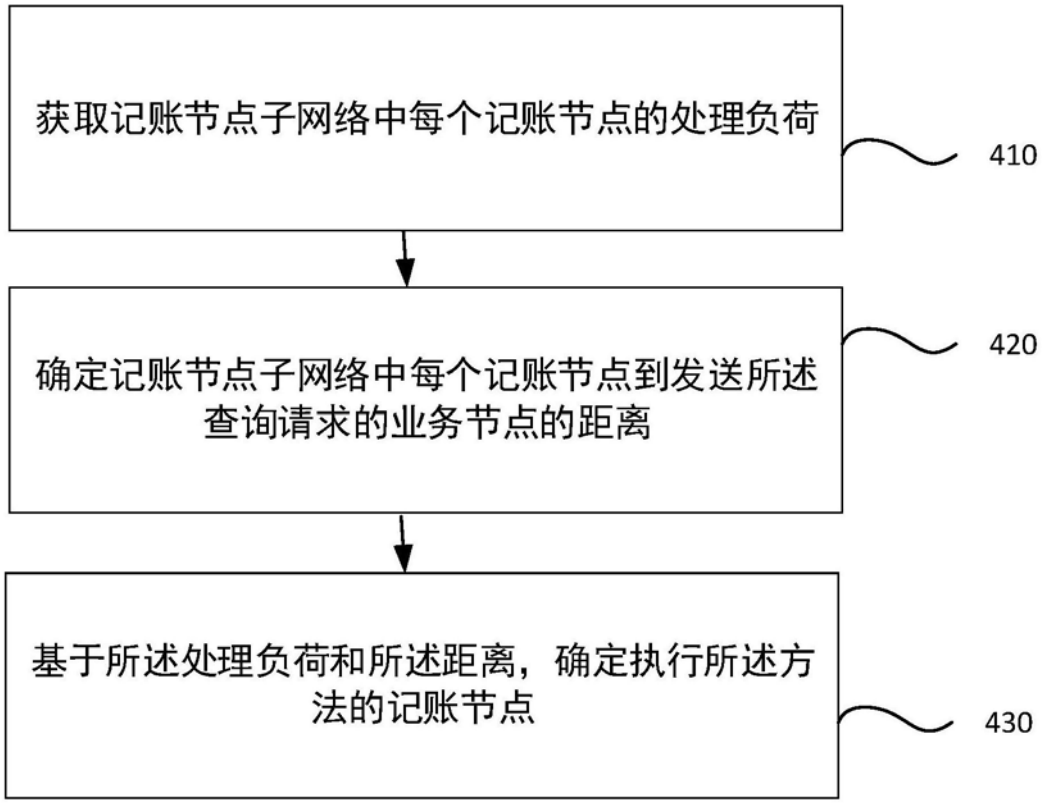

获取记账节点子网络中每个记账节点的处理负荷
410
确定记账节点子网络中每个记账节点到发送所述查询请求的业务节点的距离
420
基于所述处理负荷和所述距离，确定执行所述方法的记账节点
430

图12

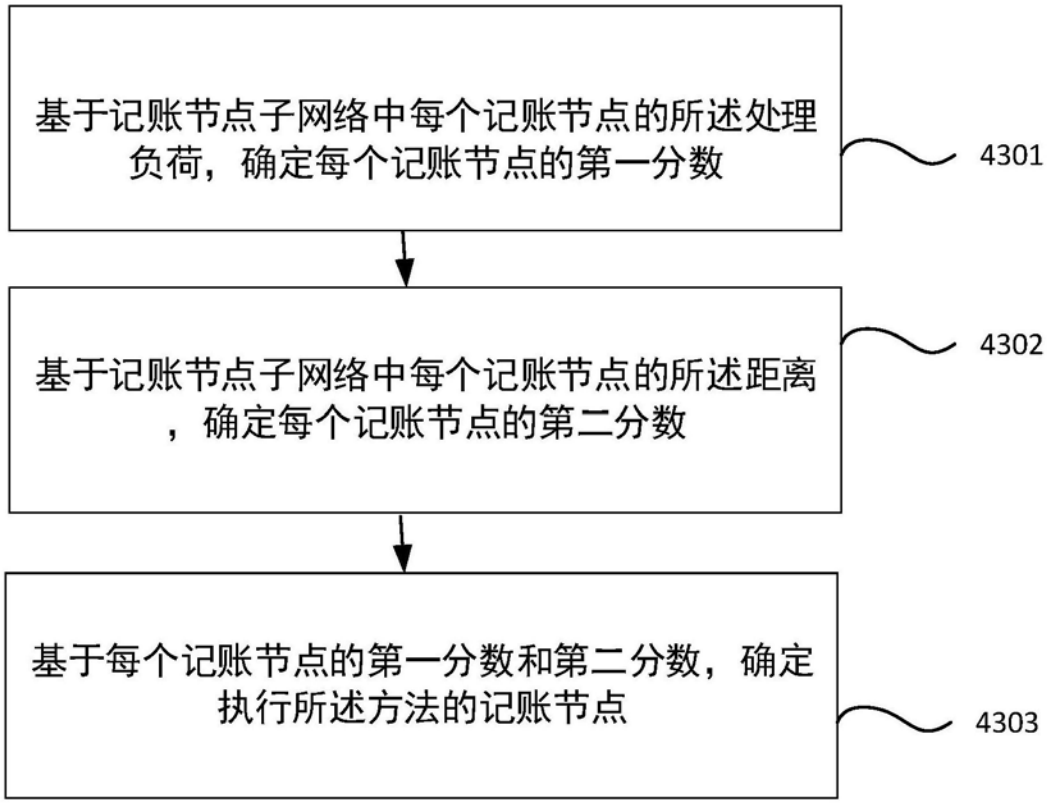

基于记账节点子网络中每个记账节点的所述处理负荷，确定每个记账节点的第一分数
4301
基于记账节点子网络中每个记账节点的所述距离，确定每个记账节点的第二分数
4302
基于每个记账节点的第一分数和第二分数，确定执行所述方法的记账节点
4303

图13

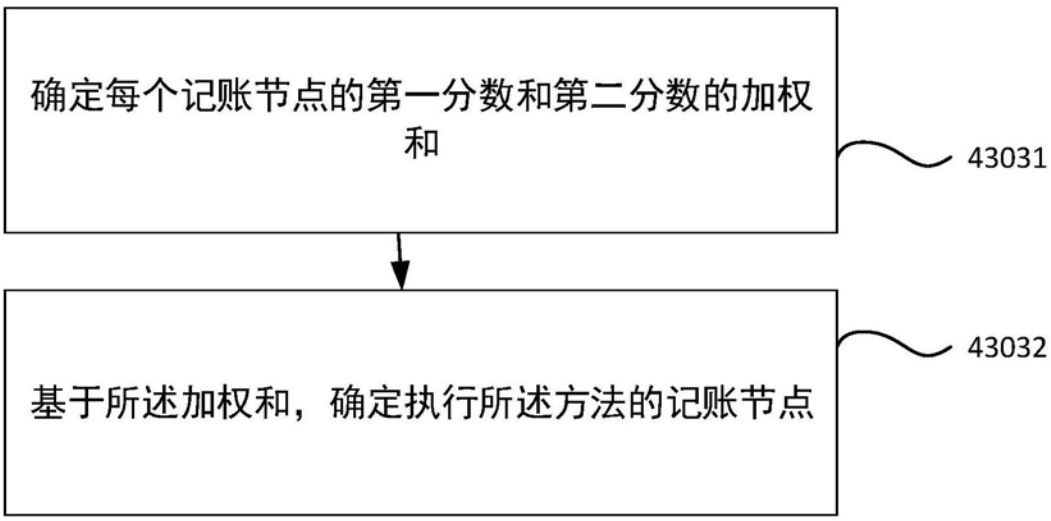

确定每个记账节点的第一分数和第二分数的加权和
43031
基于所述加权和，确定执行所述方法的记账节点
43032

图14

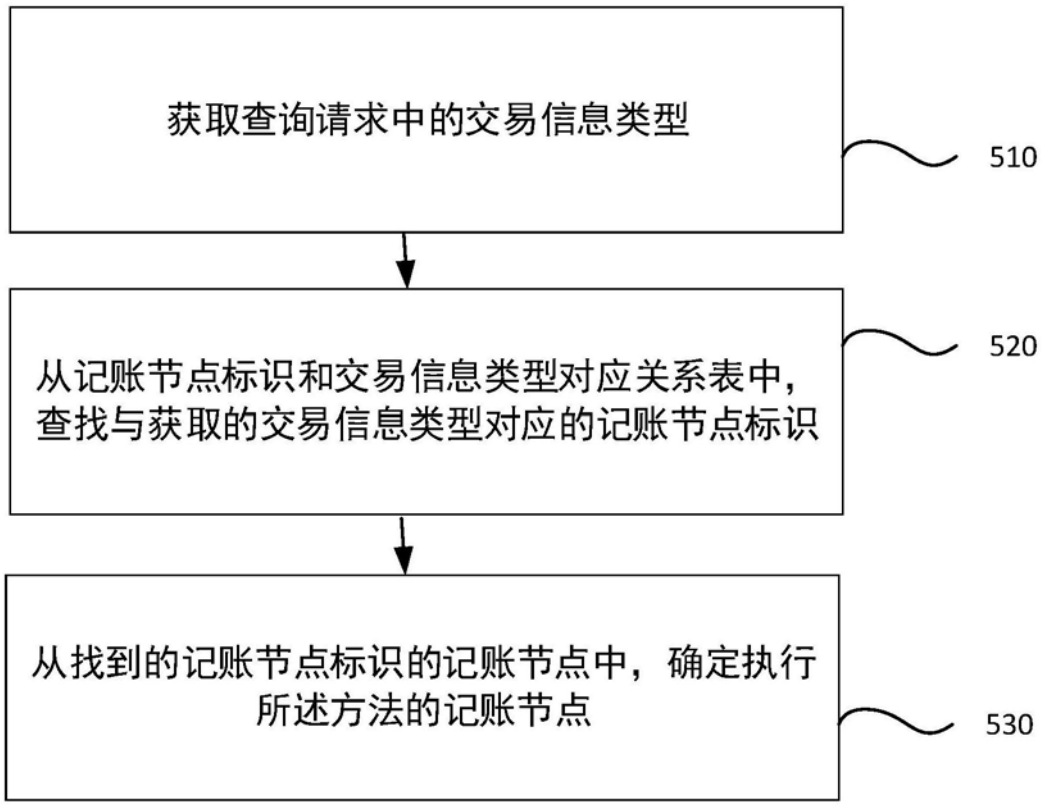

获取查询请求中的交易信息类型
510
从记账节点标识和交易信息类型对应关系表中，查找与获取的交易信息类型对应的记账节点标识
520
从找到的记账节点标识的记账节点中，确定执行所述方法的记账节点
530

图15

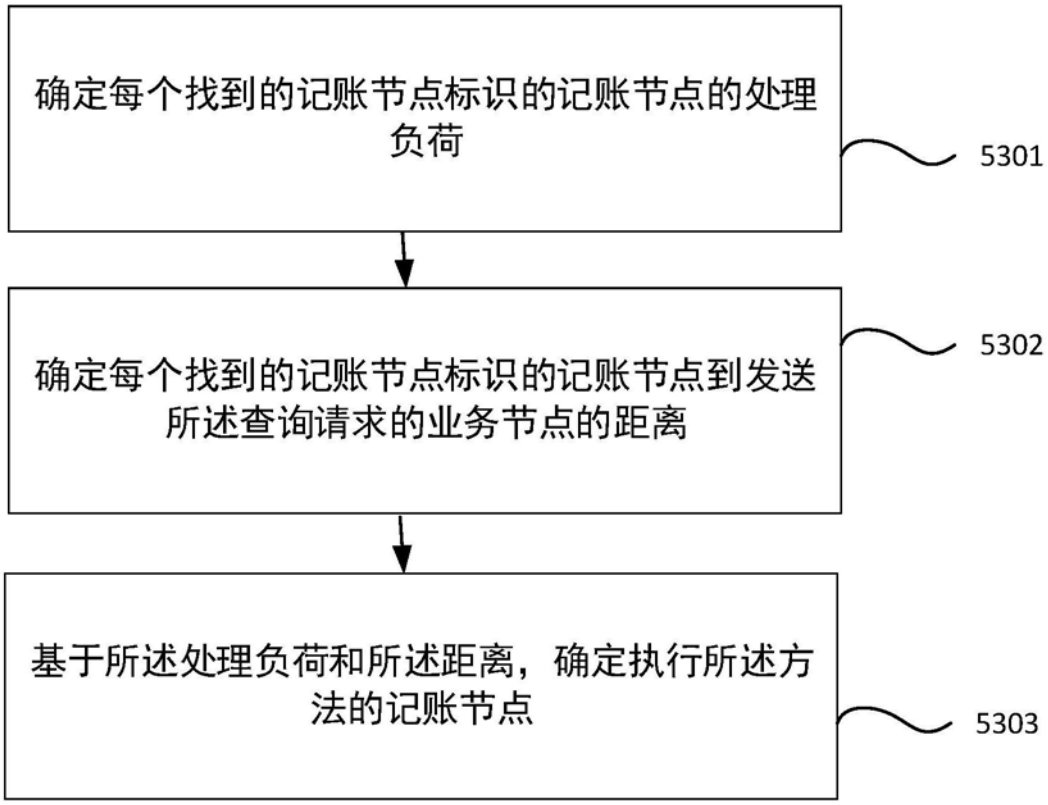

确定每个找到的记账节点标识的记账节点的处理负荷
5301
确定每个找到的记账节点标识的记账节点到发送所述查询请求的业务节点的距离
5302
基于所述处理负荷和所述距离，确定执行所述方法的记账节点
5303

图16

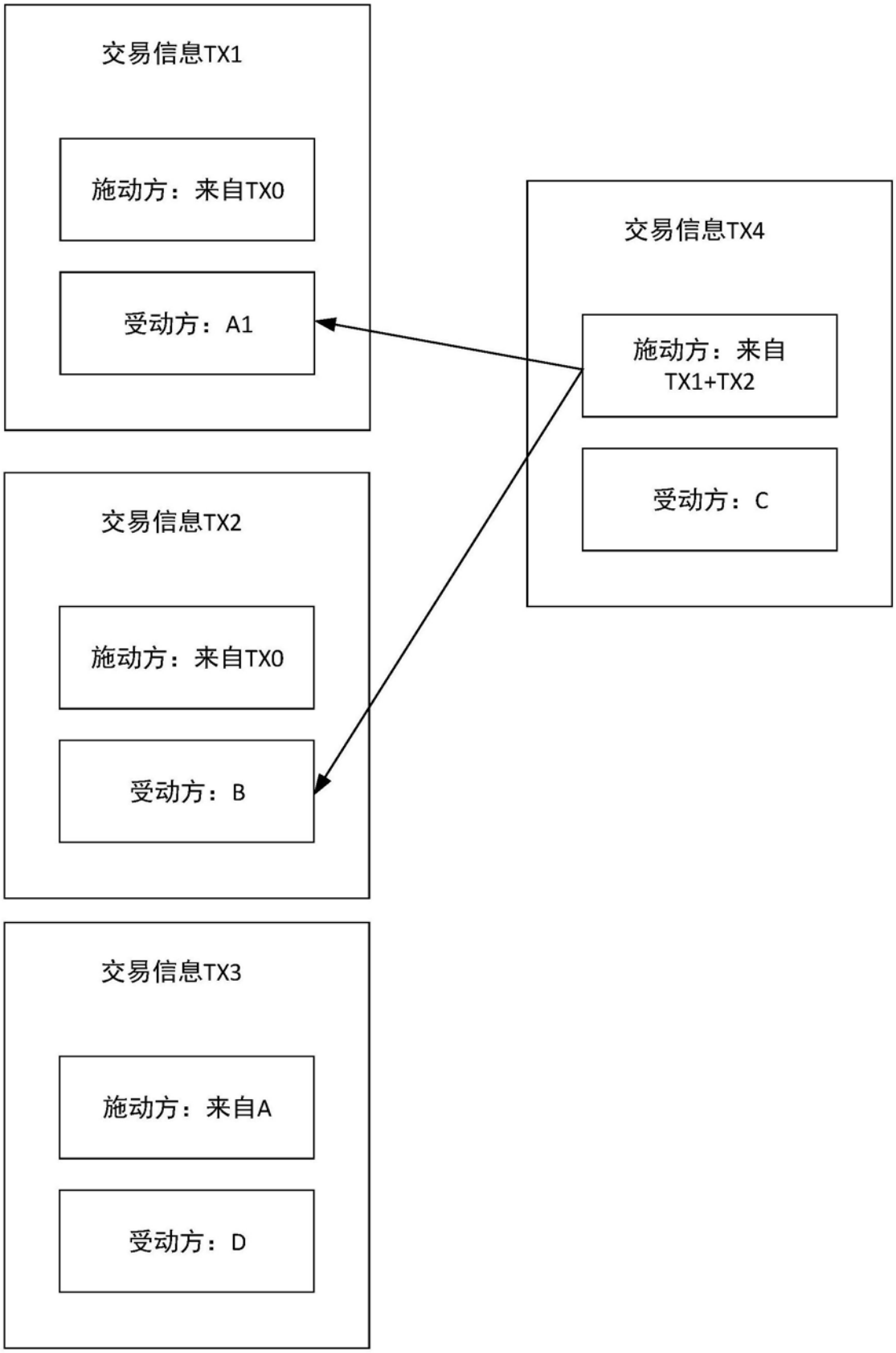

交易信息TX1
施动方：来自TX0
受动方：A1
交易信息TX4
施动方：来自
TX1+TX2
受动方：C
交易信息TX2
施动方：来自TX0
受动方：B
交易信息TX3
施动方：来自A
受动方：D

图17

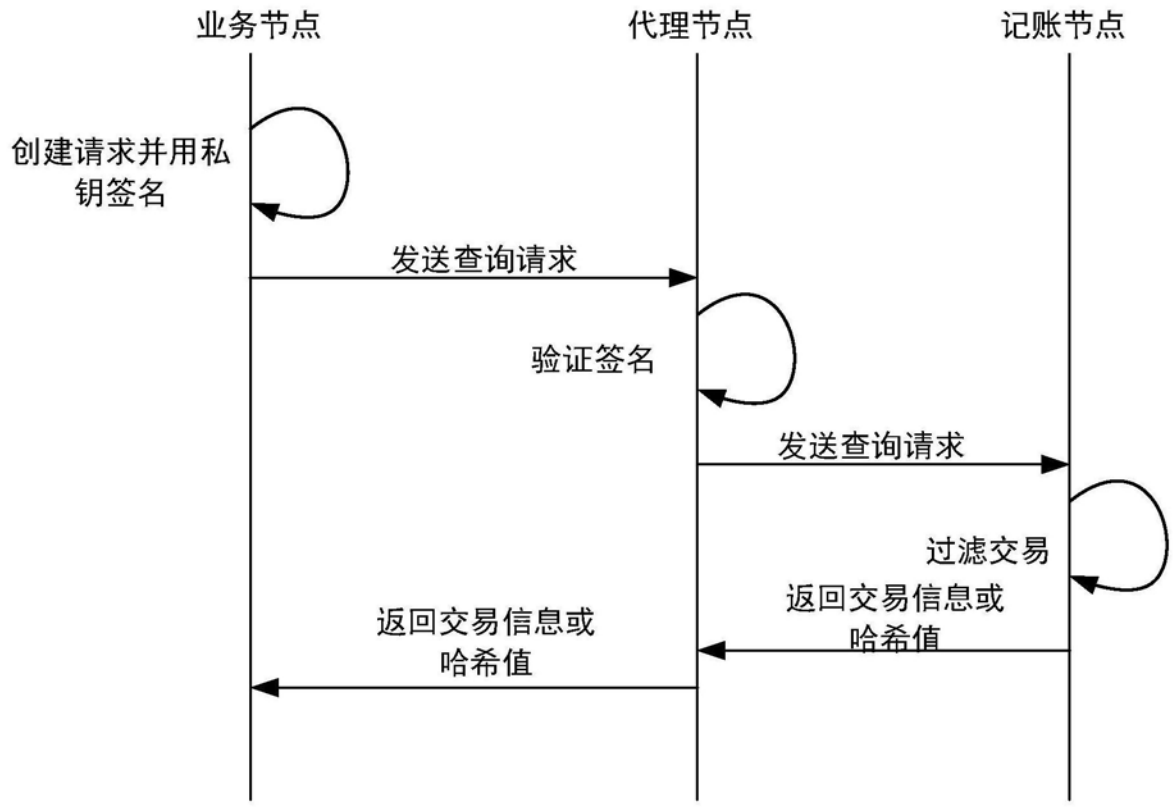

业务节点
代理节点
记账节点
创建请求并用私钥签名
发送查询请求
验证签名
发送查询请求
过滤交易
返回交易信息或哈希值
返回交易信息或哈希值

图18A

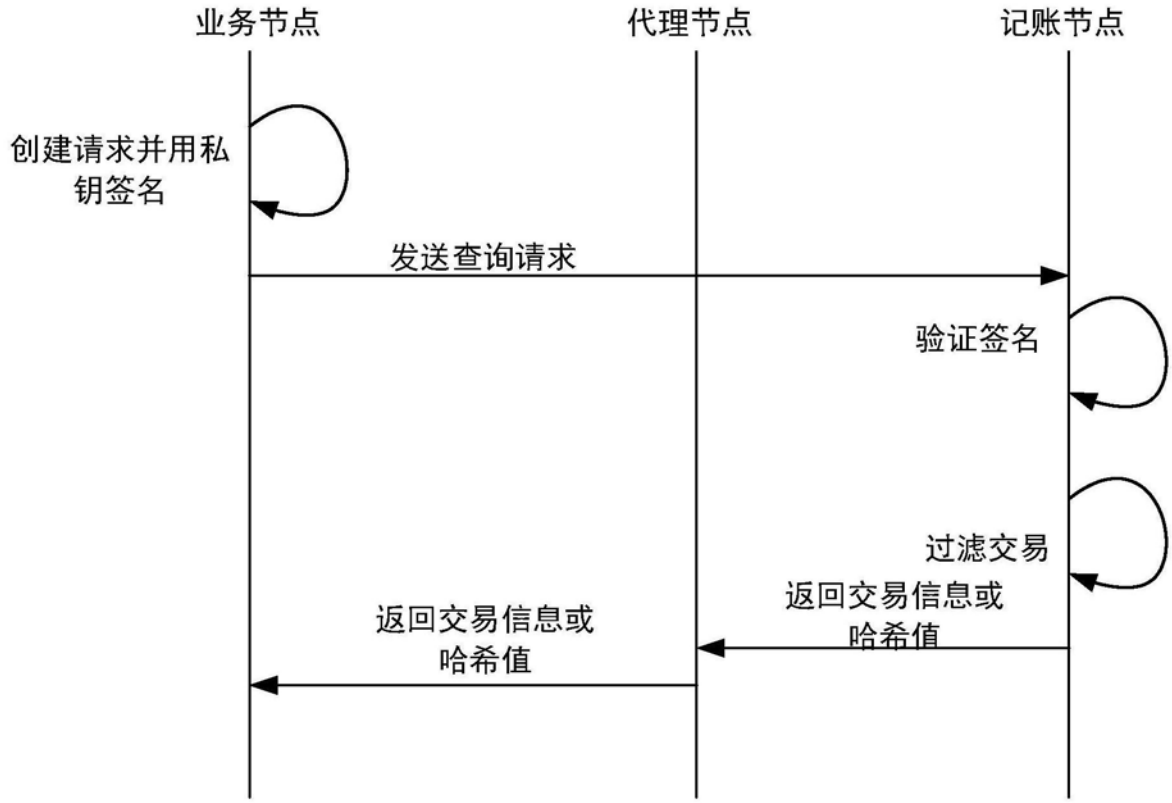

业务节点
代理节点
记账节点
创建请求并用私钥签名
发送查询请求
验证签名
过滤交易
返回交易信息或哈希值
返回交易信息或哈希值

图18B

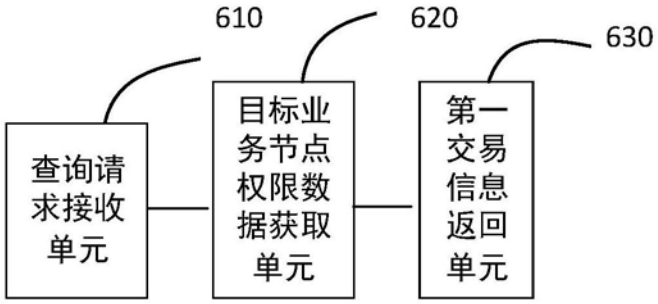

610
620
630
查询请求接收单元
目标业务节点权限数据获取单元
第一交易信息返回单元

图19

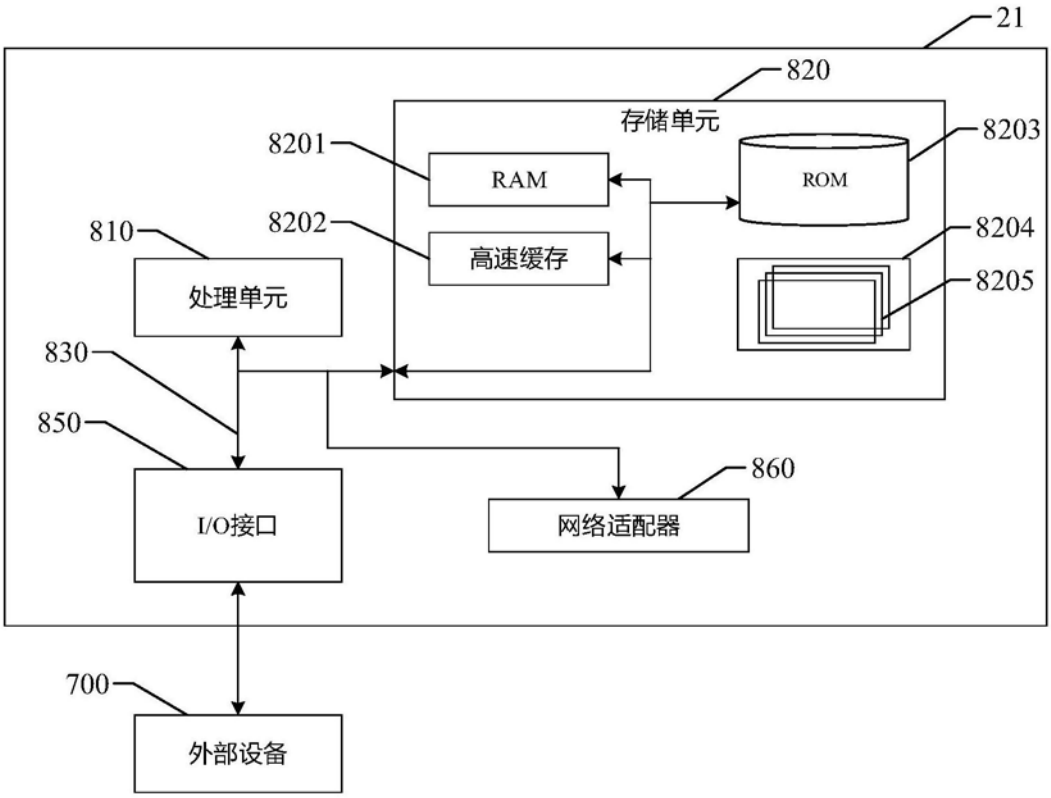

21
820
存储单元
8201
RAM
8203
ROM
8202
高速缓存
8204
8205
810
处理单元
830
850
I/O接口
860
网络适配器
700
外部设备

图20