(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 6 月 11 日 (11.06.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/114350 A1

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

(21) 国际申请号: PCT/CN2019/122394

(22) 国际申请日: 2019 年 12 月 2 日 (02.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811495812.2 2018年12月7日 (07.12.2018) CN

(71) 申请人: 腾 讯 科 技 (深 圳) 有 限 公 司 (**TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED**) [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(72) 发明人: **李茂材 (LI, Maocai)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **蓝虎 (LAN, Hu)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **王宗友 (WANG, Zongyou)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **周开班 (ZHOU, Kaiban)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **屠海涛 (TU, Haitao)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **张劲松 (ZHANG, Jinsong)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **时一防 (SHI, Yifang)**; 中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **杨常青 (YANG,**

(54) **Title:** METHOD FOR RECORDING DATA BLOCK IN BLOCK CHAIN NETWORK, ACCOUNTING NODE, AND MEDIUM

(54) **发明名称:** 在区块链网络中记录数据区块的方法、记账节点和介质

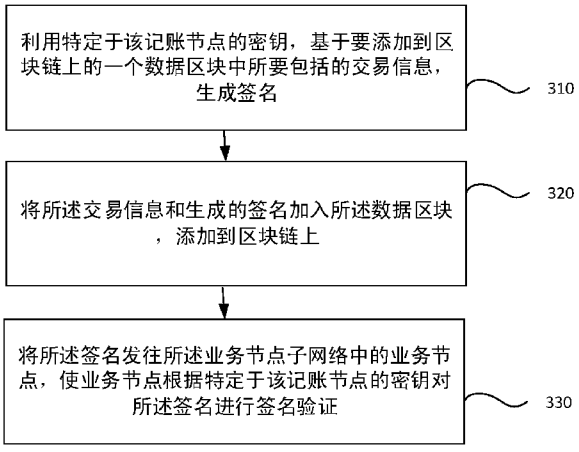


图 6

(57) **Abstract:** The present invention provides a method for recording a data block in a block chain network, an accounting node, and a medium. The block chain network comprises an accounting node sub-network and a service node sub-network. The accounting node sub-network comprises an accounting node for recording a data block on a block chain, and the service node sub-network comprises a service node for verifying the data block recorded on the block chain by the accounting node. The method comprises: generating a signature on the basis of transaction information to be comprised in a data block to be added to a block chain by using a secret key specific to an accounting node; adding the transaction information and the generated signature to the data block, and adding the transaction information and the generated signature to the block chain; and sending the signature to a service node in the service node sub-network, so that the service node performs signature verification on the signature according to the secret key specific to the accounting node.

WO 2020/114350 A1

[见续页]

Changqing)；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **孔利(KONG, Li)**；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **朱耿良(ZHU, Gengliang)**；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **丁勇(DING, Yong)**；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **刘区城(LIU, Qucheng)**；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **陈秋平(CHEN, Qiuping)**；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。 **王鹏(WANG, Peng)**；中国广东省深圳市南山区高新区科技中一路腾讯大厦35层, Guangdong 518057 (CN)。

(74) **代理人**：**北京德琦知识产权代理有限公司(DEQI INTELLECTUAL PROPERTY LAW CORPORATION)**；中国北京市海淀区知春路1号学院国际大厦7层, Beijing 100083 (CN)。

(81) **指定国**(除另有指明，要求每一种可提供的国家保护)：AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

根据细则4.17的声明：

— 关于申请人有权要求在先申请的优先权(细则4.17(iii))

本国际公布：

— 包括国际检索报告(条约第21条(3))。

(57) **摘要**：本公开提供了一种在区块链网络中记录数据区块的方法、记账节点和介质。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。所述方法包括：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；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；将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。

在区块链网络中记录数据区块的方法、记账节点和介质

本申请要求于2018年12月7日提交中国专利局、申请号为201811495812.2、申请名称为“在区块链网络中记录数据区块的方法、记账节点和介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本公开涉及区块链领域，具体涉及一种在区块链网络中记录数据区块的方法、记账节点和介质。

背景技术

在传统的区块链网络中，记账共识和见证完全发生在超级节点形成的共识网络之中，每个超级节点既充当向区块链上记录数据区块的记账节点，又充当共识和见证节点，区块链网络外的其他使用方只能无条件信任由超级节点组成的共识网络。

但是，往往区块链网络外的其他使用方才是真正与区块链上记录的数据区块有利益关系的当事人。例如，在传统的发票区块链网络中，开票方开出发票后，将开票事件通过区块链网络中与该开票方对应的超级节点记账，该超级节点根据开票事件生成数据区块，该数据区块在所有超级节点之间进行共识，然后记录在区块链上。开票方和收票方是利益相关的当事人，却不能见证记账过程，只能无条件信任由超级节点组成的共识网络。如果超级节点集体作恶，利益相关的当事人完全没有办法。这种记账权的垄断导致区块链网络的可信度和公正性大大降低。

发明内容

本公开的一个目的在于提出一种在区块链网络中记录数据区块的方法、记账节点和介质，能够提高区块链网络的可信度和公正性。

根据本公开实施例的一方面，公开了一种在区块链网络中记录数据区块的方法，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：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；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；将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。

根据本公开实施例的一方面，公开了一种在区块链网络中记录数据区块的记账节点，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，所述方法包括：签名生成单元，用于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；上链单元，用于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；发布单元，用于将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。

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，用于存储计算机可读指令；一个或多个处理器，用于读取所述存储器存储的计算机可读指令，以执行如上所述的在区块链网络中记录数据区块方法。

根据本公开实施例的一方面，公开了一种计算机可读存储介质，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在区块链网络中记录数据区块方法。

鉴于相关技术中每个超级节点既充当向区块链上记录数据区块的记账节点，又充当共识和见证节点，区块链网络外的其他使用方只能无条件信任由超级节点组成的共识网络的现状，本公开实施例将记账节点子网络和业务节点子网络分开，提出了记账与见证分离的双层共识网络方案。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，那么对全网的交易数据进行见证的全部节点都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，系统的运转更加透明；而相比传统的去中心化公链方案，本方案更可控也更便于监管。

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。

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。

附图简要说明

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特征及优点将变得更加显而易见。

图 1A-1C 示出了根据本公开实施例的在区块链网络中记录数据区块的方法的三种体系构架示意图。

图 2A-2C 示出了根据本公开实施例的在区块链网络中记录数据区块的方法分别应用在供应链金融、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示意图。

图 3A-3G 示出了根据本公开实施例的在区块链网络中记录数据区块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示意图。

图 4A-4G 示出了根据本公开实施例的在区块链网络中记录数据区块的方法应用在电子发票应用场景下的业务节点显示界面示意图。

图 5A-5G 示出了根据本公开实施例的在区块链网络中记录数据区块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示意图。

图 6 示出了根据本公开实施例的在区块链网络中记录数据区块的方法的流程图。

图 7 示出了根据本公开实施例的在区块链网络中记录数据区块的方法的流程图。

图 8 示出了根据本公开实施例的在区块链网络中记录数据区块的方法的流程图。

图 9 示出了根据本公开实施例的图 8 中步骤 333 的一个具体实现的流程图。

图 10 示出了根据本公开实施例的图 8 中步骤 333 的一个具体实现的流程图。

图 11 示出了根据本公开实施例的图 10 中步骤 33313 的一个具体实现的流程图。

图 12 示出了根据本公开实施例的在区块链网络中记录数据区块的方法的流程图。

图 13 示出了根据本公开实施例的图 6 中步骤 310 的一个具体实现的流程图。

图 14 示出了根据本公开实施例的选取执行在区块链网络中记录数据区块的方法的记账节点的流程图。

图 15 示出了根据本公开实施例的图 14 中步骤 430 的一个具体实现的流程图。

图 16 示出了根据本公开实施例的图 15 中步骤 4303 的一个具体实现的流程图。

图 17 示出了根据本公开实施例的选取执行在区块链网络中记录数据区块的方法的记账节点的流程图。

图 18 示出了根据本公开实施例的图 17 中步骤 530 的一个具体实现的流程图。

图 19 示出了根据本公开实施例的数据区块的结构示意图。

图 20 示出了根据本公开实施例的记账节点之间进行共识的过程的示意图。

图 21 示出了根据本公开实施例的在区块链网络中记录数据区块的记账节点的模块示意图。

图 22 示出了根据本公开实施例的记账节点的硬件结构示意图。

具体实施方式

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。

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。

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。

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。

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。业务节点 11 也可以向记账节点请求相应的交易数据。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 可以是业务节点子网络 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 可以是产生各种需上链的交易信息的交易方的终端。业务节点 11 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 传递过来的消息后，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，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。

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的体系构架的不同之处在于，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。代理节点12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。

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的体系构架的不同之处在于，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，为了满足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。因此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。

图2A示出了根据本公开实施例的在区块链网络中记录数据区块的方法应用在供应链金融的应用场景下的场景构架示意图。

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需要外包到其它生产企业去生产。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，而在这个过程中向生产企业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的价款中划转出一部分货款用于该零件或组成部分的采购的担保。这样，生产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货款，而是可以等到收到整个设备或产品的采购方的实际货款时才将这部分货款付给零件或组成部分的生产企业。

该业务在传统的区块链网络中难以实施，这是由于由银行设置了所有的记账节点，而这个网络是封闭的。制造企业与整个设备或产品的订购方订立了总采购合同后，或者与零件或组成部分的生成方签订了分采购合同后，都需要将这些合同传给银行设置的记账节点进行上链，银行设置的各记账节点可以互相监督和见证，但供销链上的各企业节点却不能监督和见证，因此，无法取得供应链各企业节点的信任。然而，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分离，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企业节点终端，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。

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后，从总采购合同的价款中拨出一部分用于轮胎的采购，并与轮胎制造商订立第一分采购合同，再拨出另一部分用于车零部件的采购，并与车零部件供应商订立第二分采购合同。轮胎制造商以与汽车制造商订立的第一分采购合同为依据，再从该第一分采购合同的价款中拨出一部分用于制造轮胎所需橡胶的采购，并与橡胶生产商订立第三分采购合同。这样，就建立起了层层采购关系。

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、车零部件供应商分别订立第一和第二分采购合同，或者轮胎制造商与橡胶生产商订立第三分采购合同时，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进行上链，而是按照区块打包要求（例如达到预设的条数或大小），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。生成签名的方法可以包括：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，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。

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

在发送签名的同时还发送交易信息的情况下，业务节点 11 获取特定于记账节点 21 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。

在发送签名的同时还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。

在发送签名的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。每个业务节点 11 都和区块链管理方签订有智能合约，智能合约中有业务节点的权限数据。记账节点 21 根据该业务节点 11 的权限数据，对于该数据区块中该业务节点有权获取的交易信息，向该业务节点 11 返回该交易信息。对于该数据区块中该业务节点 11 无权获取的交易信息，仅向该业务节点 11 返回该交易信息的哈希值。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，提高了信息安全。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，就达到既隐藏交易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 也可以验证接收到的非隐藏的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，说明记账节点 21 作恶，从而达到了监督的目的。

下面结合图 3A-3G 说明供应链金融应用场景下记账和见证的大体过程。图 3A-3G 是根据本公开实施例的在区块链网络中记录数据区块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。

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。

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，业务节点 11 就获取特定于该记账节点的密钥（例如通过请求认证中心获取），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，还没有获得数据区块中的交易信息。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。

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 获取智能合约中的权限数据。记账节点 21 根据该业务节点 11 的权限数据，对于该数据区块中该业务节点 11 有权获取的交易信息，向该业务节点 11 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。

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。

图 2B 示出了根据本公开实施例的在区块链网络中记录数据区块的方法应用在电子发票的应用场景下的场景构架图。

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。然而，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 分离，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。

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。

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发票时，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 按照区块打包要求将交易信息打包成数据区块。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进行上链并将签名发送给各业务节点 11，这些过程与图 2A 所示的过程类似。

与签名同时发送到各业务节点 11 的还可以包括数据区块中的交易信息，或者交易

信息的摘要。在发送签名的同时发送交易信息的情况下和发送签名的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。这与上面图 2A 所示的过程类似，因此可以参照以上结合图 2A 所示的相关描述。另外，在发送签名的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，验证过程也与上面图 2A 所示的过程类似，故不赘述。

图 4A-4G 示出了根据本公开实施例的在区块链网络中记录数据区块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记账和见证的大体过程。

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。

然后，业务节点 11 进行签名验证，根据验证结果显示图 4C 所示的签名验证失败的界面或图 4D 所示的签名验证成功的界面。如果显示签名验证成功的界面，业务节点 11 可以向记账节点 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 所示的内容验证失败的界面或图 4G 所示的内容验证成功的界面。这些过程与图 3C-3G 所示的过程类似，故不赘述。

图 2C 示出了根据本公开实施例的在区块链网络中记录数据区块的方法应用在法定数字货币的应用场景下的场景构架图。

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。在这种情况下，本公开实施例提出的记账节点子网络 2 和业务节点子网络 1 分离的方案，完全避免了这一问题。首先，记账节点子网络 2 的每个记账节点 21 属于官方。任一业务节点 11 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 21 记录到区块链上。但是，业务节点子网络 1 中的每个业务节点 11 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。

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进行上链并将签名发送给各业务节点 11，这些过程与图 2A 所示的过程类似。

与签名同时发送到各业务节点 11 的还可以包括数据区块中的交易信息，或者交易信息的摘要。在发送签名的同时发送交易信息的情况下和发送签名的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。这与上面图 2A 所示的过程类似，因此可以参照以上结合图 2A 所示的相关描述。另外，在发送签名的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，验证过程也与上面图 2A 所示的过程类似，故不赘述。

图 5A-5G 示出了根据本公开实施例的在区块链网络中记录数据区块的方法应用在法定数字货币的应用场景下的业务节点显示界面图，这些界面图表示了在法定数字货币的应用场景下记账和见证的大体过程。

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 公司法定数字货币 3000 个单位。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。

然后，业务节点 11 进行签名验证，根据验证结果显示图 5C 所示的签名验证失败的界面或图 5D 所示的签名验证成功的界面。如果显示签名验证成功的界面，业务节点 11 可以向记账节点 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 所示的内容验证失败的界面或图 5G 所示的内容验证成功的界面。这些过程与图 3C-3G 所示的过程类似，故不赘述。

如图 6 所示，根据本公开的实施例，提供了一种在区块链网络中记录数据区块的方法。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中的一个记账节点 21 执行。所述方法包括:

步骤 310、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；

步骤 320、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；

步骤 330、将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。

下面对上面步骤 310-330 进行详细描述。

在步骤 310 中，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。

特定于记账节点的密钥是预先由认证中心为每个记账节点分配的、专用于其对交易信息进行签名所使用的密钥。一般来说，签名的过程是这样的：将待签名的消息施加摘要运算，得到待签名的消息的摘要，然后用签名使用的密钥对摘要加密，得到了签名。对签名进行验证时，需要利用解签名使用的密钥对签名解密，得到了待签名的消息的摘要，然后对待签名的消息重新施加同样的摘要运算，得到重新确定的摘要。如果解密得到的摘要与重新确定的摘要一致，则签名验证成功。通过签名验证，能够验证出待签名的消息是否是签名者所发出的、以及消息是否完整。如果该消息不是签名者所发，或者消息在传输过程中丢失了一部分，签名验证均不通过。

签名使用的密钥和解签名使用的密钥可以相同，即对称密钥的情形，也可以不相同，即非对称密钥的情形。

在对称密钥的情形中，可以事先由认证中心（图中未示出，属于独立于记账节点子网络的一个起认证作用的节点）为每个记账节点发放一个特定于该记账节点的密钥，并把该密钥与该记账节点的对应关系记录在认证中心。在一个实施例中，可以在每个记账节点设立时，由记账节点向认证中心请求，由认证中心为记账节点发放特定于该记账节点的密钥。在另一个实施例中，可以在每个记账节点需要生成签名时，由记账节点向认证中心请求，由认证中心为记账节点发放特定于该记账节点的密钥。

在一个实施例中，分配给记账节点的密钥可以在发送给记账节点的同时广播到业务节点子网络中的每个业务节点，这样，业务节点对签名解密时就可以利用该密钥进行解密。在另一个实施例中，分配给记账节点的密钥可以应业务节点的请求发送给业务节点。即，业务节点在对签名解密因而需要该密钥时，向认证中心进行请求，由认证中心将该密钥发送给业务节点，供业务节点对签名进行解密。

在非对称密钥的情形中，可以事先由认证中心为每个记账节点生成一对公私钥，将私钥发放给记账节点，并把公钥向业务节点子网络中的所有业务节点广播，或者把该私钥与该记账节点的对应关系记录在认证中心，等待业务节点需要与该私钥对应的公钥时向认证中心请求。在一个实施例中，可以在每个记账节点设立时，由记账节点向认证中心请求，由认证中心生成上述公私钥。在另一个实施例中，可以在每个记账节点需要生成签名时，由记账节点向认证中心请求，由认证中心生成公私钥。

在一个实施例中，公钥可以在生成之后立即广播到业务节点子网络中的每个业务节点。在另一个实施例中，公钥可以应业务节点的请求发送给业务节点。即，业务节点在对签名解密因而需要该公钥时，向认证中心进行请求。由认证中心将该公钥发送

给业务节点，供业务节点对签名进行解密。

在一个实施例中，步骤 310 中，当业务节点 11 通过代理节点 12 向记账节点 21 发送交易信息时，记账节点 21 可以将接收到的该交易信息作为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，对该交易信息施加签名算法，生成签名。

在另一个实施例中，步骤 310 中，当业务节点 11 通过代理节点 12 向记账节点 21 发送交易信息时，记账节点 21 不急于将接收到的该交易信息作为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，对该交易信息施加签名算法，生成签名，而是将其放在缓存中，等待缓存中缓存了足够数量的交易信息时，才将其打包在一个数据区块中，生成签名，并上链。该实施例的好处是，提高数据区块的利用效率。在一个数据区块中，可能装有多条交易信息，从而避免区块链上的数据区块过多过于分散，也减少了区块上链的工作负荷。

该实施例中，如图 13 所示，步骤 310 包括:

步骤 3101、接收来自业务节点的待上链交易信息并缓存;

步骤 3102、如果缓存中的待上链交易信息达到预设的区块打包要求，将缓存中的待上链交易信息作为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;

步骤 3103、从认证中心获取特定于该记账节点的密钥;

步骤 3104、利用从认证中心获取的密钥，对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实施签名算法，生成签名。

在步骤 3101 中，待上链交易信息是业务节点完成交易后需要记录在区块链上的交易信息，如图 3A、4A、5A 界面上显示的信息。记账节点接收到该信息后，不立即打包成数据区块，而是先缓存。等到缓存中的待上链交易信息达到预设的区块打包要求，才将缓存中的待上链交易信息作为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。

在步骤 3102 中，在一个实施例中，所述区块打包要求包括以下中的至少一项:

缓存中的待上链交易信息的总大小达到预定大小阈值;

缓存中的待上链交易信息的总条数达到预定条数阈值;

缓存中的待上链交易信息中最早缓存的一条待上链交易信息的缓存时间距离当前时间达到预定时间阈值。

在区块打包要求是缓存中的待上链交易信息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 条交易信息，分别是 0.8Mb 和 1.5Mb，如果这时又接收到一条待上链交易信息，大小为 2Mb，这样 0.8Mb+1.5Mb+2Mb=4.3Mb>4Mb,此时就可以为这 3 条交易信息生成一个数据区块，从而避免为每一条交易信息生成一个数据区块的资源浪费。

在区块打包要求是缓存中的待上链交易信息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 条交易信息，如果这时又接收到一条待上链交易信息，此时就可以为这 5 条交易信息生成一个数据区块，从而避免为每一

条交易信息生成一个数据区块的资源浪费。

在区块打包要求是缓存中的待上链交易信息中最早缓存的一条待上链交易信息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，如果待上链交易信息在 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信息生成一个数据区块，从而避免从请求上链到真正上链的时延过长。

在实践中，经常需要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信息的总大小达到预定大小阈值，或者缓存中的待上链交易信息中最早缓存的一条待上链交易信息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信息生成一个数据区块的资源浪费，又避免了在一段时间接收的交易信息不够多而造成无限制的等待。

在步骤 3103 中，从认证中心获取特定于该记账节点的密钥。

如上所述，可以在该记账节点设立时，该记账节点向认证中心请求特定于该记账节点的密钥，也可以在需要签名时（例如在步骤 3102 之后）向认证中心请求特定于该记账节点的密钥。在对称密钥的情形下，特定于该记账节点的密钥是认证中心向记账节点发放的唯一密钥。在非对称密钥的情形下，特定于该记账节点是密钥是认证中心为记账节点生成的私钥。

在步骤 3104 中，利用从认证中心获取的密钥，对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实施签名算法，生成签名。

签名算法如上所述，包括摘要算法和对摘要的加密方法。在一个实施例中，摘要是默克尔树根。

在一个实施例中，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，通过以下方式生成默克尔树根：

确定数据区块中的每个交易信息的哈希值；

将数据区块中的交易信息按照进入缓存的顺序排序，将顺序排在第奇数位的交易信息和紧随其后的顺序排在第偶数位的交易信息组成一个信息对；

将每个信息对的两个交易信息的哈希值进行哈希运算，得到该信息对的哈希值；

将各个信息对按照进入缓存的顺序排序，将顺序排在第奇数位的信息对和紧随其后的顺序排在第偶数位的信息对组成一个更上一级的信息对，将每个更上一级的信息对中的两个信息对的哈希值进行哈希运算，得到该更上一级的对的哈希值，直到得到最上一级的信息对的哈希值，即为默克尔树根。

在本发明的另一个实施例中，如果顺序排在最后一个奇数位的交易信息是缓存中的最后一个交易信息，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构成一个信息对；如果顺序排在最后一个奇数位的信息对是缓存中的最后一个信息对，将该信息对进行复制，该最后一个信息对和复制后的信息对构成一个更上一级的信息对，按照这种方式得到的默克尔树称为二叉树。

例如，缓存中有 9 条交易信息，按进入缓存的时间顺序分别是 A1-A9，要放到数据区块中进行上链。A1-A2 组成一个信息对 B1，对 A1 的哈希值和 A2 的哈希值进行哈希值运算，得到 B1 的哈希值；A3-A4 组成一个信息对 B2，对 A3 的哈希值和 A4 的哈希值进行哈希值运算，得到 B2 的哈希值；A5-A6 组成一个信息对 B3，对 A5 的哈希值和 A6 的哈希值进行哈希值运算，得到 B3 的哈希值；A7-A8 组成一个信息对 B4，对 A7 的哈希值和 A8 的哈希值进行哈希值运算，得到 B4 的哈希值；将 A9 复制一份得到 A10，A9 和 A10 组成一个信息对 B5，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。

针对 B1-B5，B1-B2 组成一个更上层的信息对 C1，对 B1 的哈希值和 B2 的哈希值进行哈希值运算，得到 C1 的哈希值；B3-B4 组成一个更上层的信息对 C2，对 B3 的哈希值和 B4 的哈希值进行哈希值运算，得到 C2 的哈希值；将 B5 复制一份得到 B6，B5 和 B6 组成一个信息对 C3，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。

针对 C1-C3，C1-C2 组成一个更上层的对 D1，对 C1 的哈希值和 C2 的哈希值进行哈希值运算，得到 D1 的哈希值；将 C3 复制一份得到 C4，C3 和 C4 组成一个信息对 D2，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。

针对 D1-D2，对 D1 的哈希值和 D2 的哈希值进行哈希值运算，得到默克尔树根。

在步骤 320 中，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。

在一个实施例中，数据区块不分区块头和区块体，而是作为一个整体，将所述交易信息和签名加入数据区块的整体。在进一步的实施例中，每个数据区块中可以加入区块链中前一数据区块的摘要。它的作用是，由于每个数据区块中包括前一数据区块的信息，而该数据区块本身的摘要又包含在区块链上其后的数据区块中，这样，相邻数据区块互相关联，一旦某一数据区块被篡改，其后一数据区块中包含的该数据区块的摘要就会与其不对应，从而识别出篡改，保证了区块链上存储信息的安全性。

在另一个实施例中，数据区块不分区块头和区块体，而是作为一个整体，将交易信息、由交易信息计算出的摘要、以及签名加入数据区块的整体。摘要可以是上面介绍过的默克尔树根。交易信息不同，经摘要算法运算得到的摘要也不同，因此依据摘要能够区分不同的区块体内容，即交易信息。摘要可以用于检索数据区块。在一些实施例中，业务节点验证签名时也需要利用摘要。同样，如上所述，在每个数据区块中也可以加入区块链中前一数据区块的摘要。

在另一个实施例中，数据区块分为区块头和区块体。区块体是数据区块的主体，其中包含有数据区块存储的交易信息。区块头是数据区块的头部，其不含有交易信息，而是含有辅助性信息，包括基于本数据区块中的所有交易信息计算出的摘要（例如默克尔树根）、签名以及前一数据区块的摘要。因此，在该实施例中，将交易信息加入区块体中，将摘要（例如默克尔树根）和签名加入区块头中。前一数据区块的摘要的作

用如上所述。通过签名验证，可以防止记账节点集体作弊的行为。

在一个实施例中，步骤 320 包括:

将所述交易信息和生成的签名加入所述数据区块，发送到记账节点子网络中的所有记账节点中的领导记账节点;

由领导记账节点将所述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;

当共识成功后，由领导记账节点将所述数据区块添加到区块链上。

领导记账节点是由记账节点子网络中的各个记账节点选举出来的、并在共识算法中进行共识的发起操作和共识结果的收集操作的记账节点。它可以是固定的一个记账节点，也可以是实时按照已有的选举算法选举出来的，故不赘述。

图 20 示出了根据本公开实施例的由领导记账节点将所述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。

参考图 20，在请求阶段，客户端（即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他未处于领导状态的记账节点（例如，记账节点 B、C、D...）；继续进入追加响应阶段，由其他记账节点将接收到的共识内容广播至其他各记账节点，并在领导记账节点 A 接收到预设数量（2f+1）的其他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。在反馈阶段，领导记账节点 A 在接收到预设数量（2f+1）的其他区块链节点反馈确认通过时，则判定完成共识并向客户端反馈共识完成的结果。其中，f 是小于（N-1）/3 的所有整数中的最大整数，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。

当共识成功后，领导记账节点就可以将所述数据区块添加到区块链上，即完成上链。

在步骤 330 中，将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。

如上所述，签名的过程一般是将待签名的消息施加摘要运算，得到待签名的消息的摘要，然后用签名使用的密钥对摘要加密，得到签名。对签名验证一般是利用解签名使用的密钥对签名解密，得到解密后的摘要，与待签名的消息的真正摘要进行对比。因此，在签名验证时，需要知道待签名的消息的摘要，或者知道待签名的消息本身，然后按照摘要算法重新计算摘要。相对应地，将所述签名发往所述业务节点子网络中的业务节点的同时，还要将数据区块中包括的交易信息的摘要发送给业务节点，或者将数据区块中包括的交易信息发送给业务节点，以便业务节点能重新计算出摘要。

在一个实施例中，在数据区块中不分区块头和区块体的情形下，将数据区块中包括的交易信息的摘要发送给业务节点可以包括：将所述摘要和签名放在一个消息中发

送给业务节点。在另一个实施例中，在数据区块中包含区块头和区块体的情形下，将数据区块中包括的交易信息的摘要发送给业务节点可以包括：将所述摘要和签名所在的区块头发送给业务节点。

在一个实施例中，在数据区块中不分区块头和区块体的情形下，将数据区块中包括的交易信息发送给业务节点可以包括：将所述交易信息放在一个消息中发送给业务节点。在另一个实施例中，在数据区块中包含区块头和区块体的情形下，将数据区块中包括的交易信息发送给业务节点可以包括：将所述交易信息所在的区块体发送给业务节点。

在将签名和数据区块中包括的交易信息同时发送给业务节点的实施例中，步骤330包括：

将所述签名和数据区块中的交易信息发送到所述业务节点子网络中的业务节点，使得业务节点执行：获取特定于该记账节点的密钥；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；对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。

在一个实施例中，获取特定于该记账节点的密钥可以包括：

获取发送所述签名和交易信息的记账节点的标识；

向认证中心发送密钥请求，所述密钥请求中包含有记账节点的标识；

从认证中心接收与该标识对应的特定于记账节点的密钥。

在记账节点将签名和交易信息放在一个消息中发到业务节点的情况下，在一个实施例中，可以将记账节点的标识放置在该消息的一个专用的记账节点标识字段中发送。这样，业务节点从该记账节点标识字段中可以读取所述记账节点的标识。

接着，业务节点将该记账节点的标识放置在密钥请求中的一个专用字段，认证中心接收到密钥请求后，从该专用字段中可以读出记账节点的标识。如上所述，由于认证中心在给各记账节点生成特定于记账节点的密钥时，已经将这些密钥与记账节点的标识对应存储，因此，当认证中心读出记账节点的标识后，就可以获取与该标识对应存储的密钥，即为特定于该记账节点的密钥。在对称密钥的情况下，该特定于记账节点的密钥就是为记账节点生成的唯一密钥。在非对称密钥的情况下，该特定于记账节点的密钥是为记账节点生成的公私钥对中的公钥。

业务节点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。然后，业务节点对所述数据区块中的交易信息重新计算一遍摘要。业务节点用的摘要算法应该与记账节点用的摘要算法相同。这时，如果记账节点未作弊，传输过程中信息也无丢失，重新计算出的摘要应该与解密得到的摘要一致，如不一致则说明记账节点有作弊行为或者传输过程中信息丢失，签名验证失败。否则，签名验证成功。

该实施例的好处是，将签名和交易信息同时发给业务节点，让业务节点根据交易信息重新计算一遍摘要，该摘要是业务节点亲自重新计算的，确保了数据来源的可靠

性，提高了签名验证的准确性。

以上所述是将数据区块中包括的交易信息和签名同时发送给业务节点的实施例，在该实施例中，业务节点根据交易信息验证签名。在另外的实施例中，将交易信息的摘要和签名同时发送给业务节点，业务节点根据交易信息的摘要验证签名。这样做的好处是，可以将交易信息隐藏而不提供给业务节点。业务节点虽然不知道交易信息，但根据摘要同样可以对签名进行验证。通过这种方式，既不会暴露可能是其它业务节点上报的、不希望该业务节点知道的交易信息，又能够进行验证。

因此，该实施例中，如图 7 所示，步骤 320 包括：步骤 321，将所述交易信息、生成的签名连同对该数据区块中要包括的交易信息计算出的摘要加入所述数据区块，添加到区块链上。步骤 330 包括：步骤 331，将所述签名和所述摘要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、接收到的摘要对所述签名进行签名验证。

在一个实施例中，步骤 321 中的数据区块可以不分区块头和区块体，将交易信息、签名以及摘要一同加入数据区块的整体中。在另一个实施例中，步骤 321 中的数据区块包括区块头和区块体，将交易信息放入区块体中，将签名和摘要放入区块头中，并添加到区块链上。

在一个实施例中，步骤 331 中将签名和摘要发往业务节点可以通过将签名和摘要放在一个消息中发送的方式实现。在另一个实施例中，在签名和摘要已经被放入区块头的情况下，可以将区块头发送到业务节点。

在一个实施例中，根据特定于该记账节点的密钥和接收到的摘要对所述签名进行签名验证的具体过程包括：

获取特定于该记账节点的密钥；

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；

如果接收到的摘要与解密得到的摘要一致，则签名验证成功。

获取特定于该记账节点的密钥可以采用以上所述的向认证中心发送密钥请求，并从认证中心接收与该记账节点的标识对应的特定于该记账节点的密钥的方式，故不赘述。特定于该记账节点的密钥可以是分配给该记账节点的唯一密钥，也可以是分配给该记账节点的公私密钥对中的公钥。

与前面所述的用交易信息来验证签名的情形不同的是，由于本实施例中业务节点接收到了记账节点发送的交易信息的摘要，因此，可以直接用该接收的摘要与解密得到的摘要比较，如果一致，则签名验证成功。如果不一致，则签名验证失败。该实施例的优点在于完全隐藏交易信息，提高了交易信息的安全性，同时又保证了正常的签名验证。

如图 8 所示，在数据区块包括区块头和区块体的情况下，交易信息加入区块体，而摘要和签名（可选地，还有区块链中上一区块的摘要）加入区块头。该实施例中，

步骤 321 包括：步骤 3211，将所述交易信息加入数据区块的区块体；步骤 3212，将所述摘要和签名加入数据区块的区块头；步骤 3213，将所述数据区块添加到区块链上。

如图 19 所示，每条交易信息包括交易信息的输入和交易信息的输出。交易信息的输入是指交易的发起方的相关交易信息，交易信息的输出是指交易的承受方的相关交易信息。例如，在开出电子发票这一交易中，发起方是开票单位，则开票单位的名称、纳税人识别号、账户名、开户行、电子发票号等就成为交易信息的输入，而报销人的姓名、手机、付款账户的账号、开户行等就成为交易信息的输出。在图 19 中，将各交易信息写入数据区块的区块体中。摘要（本区块的默克尔树根）和签名写入数据区块的区块头中，同时写入区块头的还有区块链上前一数据区块的摘要。区块头与区块体共同构成了数据区块。如图 19 所示，一个区块的默克尔树根是由区块体中每个交易信息的哈希值按照上面实施例所描述的方式层层进行哈希运算而最终得到的。图 19 中的虚线箭头表示，这些数据区块可能是有联系的，一个数据区块中的一个交易信息的输出恰恰是另一个数据区块中一个交易信息的输入。例如，当电子发票开票时，报销人的姓名、手机、所在的报销单位、付款账户的账号、开户行等是相应数据区块中交易信息的输出。当报销人回所在单位报销时，报销人的姓名、手机、付款账户的账号、开户行等又成为了报销这个交易信息的输入。

在该实施例中，在上述上链过程完成后，步骤 331 包括：步骤 333，将所述区块头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、所述区块头中的摘要对所述区块头中的签名进行签名验证。

在步骤 333 中，如图 9 所示，在一个实施例中，将所述区块头发往所述业务节点子网络中的业务节点，包括：

步骤 33311、将所述区块头发往代理节点，所述代理节点是所述业务节点子网络中的一个业务节点；

步骤 33312、通过代理节点，将所述区块头广播到所述业务节点子网络中所述代理节点以外的其它业务节点。

该实施例是针对图 1B 所示的网络体系构架。在该体系构架中，代理节点通过广播的方式与业务节点子网络中的所有业务节点通信。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。

业务节点子网络除了可以采用图 1B 所示的广播消息的通信方式外，还可以采用如图 1A 所示的 P2P 式的网络通信方式。P2P 网络，即对等计算机网络，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。在 P2P 网络环境中，彼此连接的多台计算机之间都处于对等的地位，各台计算机有相同的功能，无主从之分，一台计算机既可作为服务器，设定共享资源供网络中其他计算机所使用，又可以作为工作站，整个网络一般来说不依赖专用的集中服务器，也没有专用的工作站。网络中的每一台计算机既能充当网络服务的请求者，又对其它计算机的请求做出响应，提供资源、服务和内容。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业务节点，直到业务节点子网络中的所有业务节点都接收到该区块头为止。

在一个采用 P2P 组网形式的实施例中，如图 10 所示，所述将所述区块头发往所述业务节点子网络中的业务节点，包括:

步骤 33311: 将所述区块头发往代理节点，所述代理节点是所述业务节点子网络中的一个业务节点;

步骤 33313: 将代理节点作为发送节点，将所述区块头发送到尚未接收到该区块头的其它业务节点中离所述发送节点最近的业务节点，并以接收到该区块头的业务节点作为发送节点发送该区块头，直到所有其它业务节点都接收到该区块头。

在步骤 33313 中，由于已经接收到所述区块头的业务节点重复接收同样的区块头没有意义，因此，每个业务节点确定接收区块头的业务节点时，除了要考虑优先发送给离其最近的业务节点（以减少传输等待时间）外，还要考虑要发送给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，就完成了区块头逐节点的安全下发，同时避免了下发负担集中在一个业务节点上，实现了负载均衡。

在一个实施例中，如图 11 所示，步骤 33313 包括:

步骤 333131: 确定所述业务节点子网络中除所述发送节点之外的所有其它业务节点与所述发送节点的距离;

步骤 333132、向所述距离最小的其它业务节点发送所述区块头，其中，如果接收到所述区块头的其它业务节点之前已经接收到该区块头，向所述发送节点发送拒绝应答;

步骤 333133: 如果接收到拒绝应答，则向距离第二小的其它业务节点发送所述区块头，直到接收到接受应答。

在一个实施例中，在步骤 333131 中，确定所述业务节点子网络中除所述发送节点之外的所有其它业务节点与所述发送节点的距离可以包括:

周期性接收从所述业务节点子网络中除所述发送节点之外的所有其它业务节点广播的定位信息;

按照最近一次接收到的除所述发送节点之外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。

发送节点周期性（例如每隔 5s）接收业务节点子网络中所有其它业务节点的定位信息。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。每个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所有其它业务节点。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。

通过以上计算出的距离，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，但该距离最小的其它业务节点有可能已经接到过该区块头。因此，本公开实施例通过让接收到区块头的其它业务节点发送接受应答或拒绝应答来来避免将区块头重复发给某个业务节点。接受应答或拒绝应答的区别在于，其某一个特定标志字段放置不同的字符或字符串，以表示接受应答或拒绝应答。这样，发送节点可以通过识别接收到的应答中的该特定标志字段，识别接收到该应答是接受应答还是拒绝应答。如果是接受应答，就表示接收到该区块头的其它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。如果是拒绝应答，就表示接收到该区块头的其它业务节点之前接收到过该区块头，因此拒绝了该区块头。这时，就要找到所述距离第二小的其它业务节点，再向其发送区块头，并判断该其它业务节点反馈的是拒绝应答还是接受应答，如果仍然是拒绝应答，就要找到距离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应答还是接受应答的判断。也就是说，如果接收到拒绝应答，就根据其它业务节点与发送节点之间的距离由近至远的顺序继续将区块头发送至其它业务节点，直到接收到接受应答。

找到尚未接收到该区块头的其它业务节点中、离所述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、离所述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，通过上述向所述距离最小的其它业务节点发送所述区块头，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进行接受应答或拒绝应答的方式，少设置了一个服务器，从而节省网络资源，避免网络拥塞。

业务节点进行签名验证后，得到一个成功或失败的验证结果。下面进一步描述得到验证结果后的进一步处理。

尽管一个业务节点可能签名验证失败，但由于业务节点是民间的，其不具有任何处理权，这样，作恶的记账节点仍然可以继续作恶。但是，如果只要有一个业务节点签名验证失败就禁止其验证出作恶的记账节点继续运行，也是不妥的，因为该业务节点也有可能是恶意指控，或者验证失败是因为信息传输错误而非记账节点作恶。因此，

本公开实施例可以设置仲裁服务器，专门用于收集所有业务节点的签名验证结果，并对记账节点是否作恶进行仲裁。

在一个实施例中，仲裁服务器的一种仲裁方式是只要有一个业务节点针对所述区块头中的签名的签名验证结果是验证失败，就由仲裁服务器进行重新签名验证。如果签名验证仍然失败，则由人工进行调查，并采取进一步的处理措施。

在该实施例中，在步骤 333 之后，所述方法进一步包括:

由业务节点将签名验证结果以及所述区块头发送到仲裁服务器，其中，只要有一个业务节点针对所述区块头中的签名的签名验证结果是验证失败，就由仲裁服务器根据特定于该记账节点的密钥、所述区块头中的摘要对所述区块头中的签名进行签名验证。

也就是说，所有业务节点都将签名验证结果以及区块头发送到仲裁服务器。将区块头发送到仲裁服务器的意义是仲裁服务器可以依据该区块头进行重新签名验证。该实施例中，只要有一个业务节点针对所述区块头中的签名的签名验证结果是验证失败，就由仲裁服务器根据特定于该记账节点的密钥、所述区块头中的摘要对所述区块头中的签名进行签名验证，其验证的方法与各业务节点进行签名验证的方法相同。在该实施例中，如果仲裁服务器仍然验证失败，则要经过人工核实并最终判断该记账节点是否作恶，从而达到了只要有一丝作恶嫌疑都详细排查的效果，保证了记账节点作恶排查的准确度。

在上述实施例中，如果仲裁服务器重新进行签名验证的验证结果仍然是验证失败，并且人工核实后证明确实是记账节点作恶，仲裁服务器可以向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块。记账节点接收到该停止运行指令时将停止运行。区块链上已经记录的错误的数据区块不能删除，这是由区块链的性质决定的，但是可以增加一个数据区块，指示该记录错误的数据区块无效，即增加包括该数据区块无效的指示的数据区块。

在一个实施例中，仲裁服务器的一种仲裁方式是，在达到预设数量阈值的业务节点针对同一区块头中的签名的签名验证结果都是验证失败的情况下，才采取进一步的处理措施。这是考虑到，某个业务节点可能恶意投诉，但需要向区块链上记录交易的业务节点比参与记账的记账节点多得多，因此少数的业务节点可能恶意投诉，但多个业务节点联合起来恶意投诉同一数据区块的上链是不现实的。因此，可以预先设置一个数量阈值，只有超过该数量阈值的业务节点针对同一数据区块的签名验证均失败，仲裁服务器才会采取相应的措施。而且，一旦达到该数量阈值的业务节点都签名验证失败，基本可以断定该记账节点一定作弊，可以直接采取惩罚措施，即记账节点停止运行，向区块链上增加指示该记录的数据区块无效的数据区块。

在该实施例中，在步骤 333 之后，所述方法还包括：由业务节点将签名验证结果发送到仲裁服务器，其中，如果超过 f 个业务节点的签名验证结果是验证失败，仲裁服务器向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该

数据区块无效的指示的数据区块，其中，f是不大于（N-1）/3的所有整数中的最大整数，N是业务节点子网络中业务节点的个数。

实验表明，如果N是业务节点子网络中业务节点的个数，f是联合起来恶意投诉的业务节点的最大可能数目，则可以将f确定为不大于（N-1）/3的所有整数中的最大整数。如果超过f个业务节点的签名验证结果是验证失败，其已经超过了业务节点联合起来恶意投诉的最大可能数目，则可以断定记账节点是在作恶，因此，不需要进一步的人工核实，仲裁服务器可以直接采取惩罚措施，即向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块。该实施例的优点是，基于上报失败的验证结果的业务节点的数目来判断是否向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块，从而在一定程度上避免人工核实的繁琐。

上述签名验证使各业务节点能够通过对记账节点生成的签名进行验证来保证数据区块是记账节点生成的，这样，一旦以后发现该数据区块中有任何问题，就都是记账节点作恶的证据。因此，上述的签名验证对于提高区块链上数据区块记账的可信度具有重要意义。为了进一步防止记账节点篡改数据区块中的交易信息，在本公开进一步的实施例中，在签名验证之后还采用内容验证，即验证记账节点记录在数据区块中的各交易数据是否是真实的。

在该实施例中，对该数据区块中要包括的交易信息计算出的摘要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。默克尔树根的计算方式上文已描述。在步骤333后，如图12所示，在一个实施例中，所述方法还包括:

步骤340: 接收业务节点对该数据区块中的交易信息的请求;

步骤350: 获取该业务节点的权限数据;

步骤360: 根据该业务节点的权限数据，对于该数据区块中该业务节点有权获取的交易信息，向该业务节点返回该交易信息，而对于该数据区块中该业务节点无权获取的交易信息，向该业务节点返回该交易信息的哈希值，从而，该业务节点根据接收到的交易信息和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，从而进行内容验证。

在数据区块上链后，记账节点把区块头发到业务节点子网络的各业务节点的情况下，各业务节点是看不到数据区块中的区块体内的各交易信息的。这样，实现了交易信息的隐藏。当业务节点想要看到数据区块中的交易信息时，其要向记账节点发送对数据区块中的交易信息的请求。然而，记账节点只把业务节点有权查看的交易信息（例如其自己请求上链的交易信息、或其下属单位请求上链的交易信息）发送给其查看，对于那些无权查看的交易信息（例如其它业务节点请求上链的信息），禁止其查看，达到对各单位的信息既上链又防止泄露的目的。但是，对于其无权查看的交易信息，向业务节点返回该交易消息的哈希值。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信息，但知道这些交易信息的哈希值，同样可以最后计算出上

述默克尔树根。业务节点计算出的默克尔树根与记账节点返回的数据区块的区块头内的默克尔树根进行比对，就可以进行内容验证。如果两个默克尔树根一致，则说明记账节点对每个交易信息都没有篡改。如果两个默克尔树根不一致，则存在记账节点篡改了其中一些交易消息，导致最后业务节点重新计算的默克尔树根与区块头中的默克尔树根不一致的可能。

业务节点的权限数据是指表示业务节点有权获得数据区块中哪些交易信息、无权获得哪些交易信息的数据。在一个实施例中，权限数据中的权限包括以下中的一种或多种:

允许查看的交易信息所对应的请求上链业务节点;

允许查看的交易信息所对应的交易类型;

允许查看的交易信息所对应的上链时间。

允许查看的交易信息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信息的权限。在一个实施例中，可以规定一个业务节点只能查看自己请求上链的交易信息。假设有一个业务节点 A，可能其权限数据中规定，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 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、以及其下属所有单位的业务节点请求上链的交易信息。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，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 A1-A7，这样，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。

允许查看的交易信息所对应的交易类型是指允许查看哪些交易类型的交易信息的权限。在数据区块的交易信息中携带有交易类型。交易类型例如发票交易、供应链金融交易、法定数字货币交易等。在发票交易中，可能地税局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信息，因此就可以将数据区块中关于发票的交易信息全向其返回，对于数据区块中其它类型的交易信息仅向其返回哈希值。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信息，因此就可以将数据区块中关于供应链金融的交易信息全向其返回，对于数据区块中其它类型的交易信息仅向其返回哈希值。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信息，因此就可以将数据区块中关于法定数字货币的交易信息全向其返回，对于数据区块中其它类型的交易信息仅向其返回哈希值。

允许查看的交易信息所对应的上链时间是指允许查看哪个时间段上链的交易信息的权限。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信息。

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信息所对应的请求上链业务节点、允许查看的交易信息所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 的交易信息。

在一个实施例中，在步骤 310 之前，所述方法可以包括:

响应于业务节点向区块链网络的注册请求，获取与该业务节点对应的入网合约，所述入网合约中含有所述业务节点的权限数据;

将所述入网合约加入数据区块，添加到区块链上。

在该实施例中，步骤 350 包括:

从区块链上获取所述入网合约;

从所述入网合约中获取该业务节点的权限数据。

在业务节点申请加入区块链网络时，向一个记账节点发起注册请求。同时，区块链网络运维的工作人员根据该业务节点的性质和经营状况，为其核定能够查看交易信息的权限，将相应的权限数据写入入网合约，并将入网合约输入记账节点。这样，该记账节点就获取到了与该业务节点对应的入网合约，所述入网合约中含有所述业务节点的权限数据。该记账节点可以将该业务节点的标识与该入网合约对应加入一个数据区块的区块体中，添加到区块链上。这样，在接收到业务节点对该数据区块中的交易信息的请求后，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，根据请求的业务节点的标识，就可以在区块链中找到与该业务节点的标识对应存储的入网合约，并从中读取权限数据。

业务节点根据接收到的交易信息和哈希值计算出默克尔树根的过程与上面所述的记账节点根据数据区块中的所有交易信息生成默克尔树根的过程类似，只不过在上面所述的记账节点根据数据区块中的所有交易信息生成默克尔树根的过程中，所有的交易信息都要计算出哈希值再根据这些哈希值生成默克尔树根，而在业务节点处，有些交易信息的哈希值是直接接收到的，不用再计算。

上述实施例的好处是，可以在签名验证的基础上，再进行内容验证，从而进一步防止记账节点篡改交易信息内容，同时使得交易信息对非相关用户保密，防止交易信息泄露。

与上面签名验证之后的进一步处理类似，所述方法在内容验证之后也可以包括进一步的处理。即，在一个实施例中，在步骤 360 之后，所述方法还可以包括:

由业务节点将内容验证结果、所述业务节点接收到的交易信息和哈希值、以及区块头中包含的默克尔树根发送到仲裁服务器，其中，只要有一个业务节点针对该数据区块的内容验证结果是验证失败，就由仲裁服务器根据接收到的交易信息和哈希值重新计算默克尔树根，并与区块头中包含的默克尔树根比较，从而进行内容验证。

该实施例中，所有业务节点都将内容验证结果以及所述业务节点接收到的交易信息和哈希值、以及区块头中包含的默克尔树根发送到仲裁服务器。只要有一个业务节点的内容验证结果是验证失败，就由仲裁服务器根据接收到的交易信息和哈希值、以及区块头中包含的默克尔树根进行重新内容验证，如果仍然验证失败，则还要经过人工核实，以便最终判断该记账节点是否作恶。这样，达到了只要有一丝作恶嫌疑都详

细排查的效果，保证了记账节点作恶排查的准确度。

在另一个实施例中，在步骤 360 之后，所述方法包括:

由业务节点将内容验证结果发送到仲裁服务器，其中，如果超过 f 个业务节点的内容验证结果是验证失败，则仲裁服务器向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块，其中，f 是不大于（N-1）/3 的所有整数中的最大整数，N 是业务节点子网络中业务节点的个数。

实验表明，如果 N 是业务节点子网络中业务节点的个数，f 是联合起来恶意投诉的业务节点的最大可能数目，则可以将 f 确定为不大于（N-1）/3 的所有整数中的最大整数。如果超过 f 个业务节点的内容验证结果是验证失败，其已经超过了业务节点联合起来恶意投诉的最大可能数目，则可以断定记账节点是在作恶，因此，不需要进一步的人工核实，仲裁服务器可以直接采取惩罚措施，即向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块。该实施例的优点是，基于上报失败的验证结果的业务节点的数目来判断是否向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块，从而在一定程度上避免人工核实的繁琐。

如上所述，本公开实施例的在区块链网络中记录数据区块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。

在一个实施例中，如图 14 所示，接收来自业务节点的待上链交易信息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，业务节点的待上链交易信息先发送给代理节点，由代理节点按照以下步骤选出记账节点:

步骤 410: 获取记账节点子网络中每个记账节点的处理负荷;

步骤 420: 确定记账节点子网络中每个记账节点到发送所述待上链交易信息的业务节点的距离;

步骤 430: 基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点。

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待上链交易信息数来衡量。当业务节点希望将一条待上链交易信息上链时，将其发送给记账节点。记账节点接收到后，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，生成摘要和签名，将交易信息、摘要和签名封装成一个数据区块，还要在记账节点之间进行共识，然后将数据区块上链。只要记账节点接收到一条待上链交易信息，还未将其上链，都属于未处理完。这些未处理完的待上链交易信息数就能够代表记账节点的处理负荷。

在一个实施例中，步骤 410 包括:

获取每个记账节点定期发送的处理负荷并存储;

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。

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。

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:

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;

接收每个记账节点发送来的该记账节点的处理负荷。

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待上链交易信息的业务节点的距离，包括:

向记账节点子网络中每个记账节点、以及发送所述待上链交易信息的业务节点发出定位信息请求;

从各记账节点、以及发送所述待上链交易信息的业务节点接收各记账节点、以及发送所述待上链交易信息的业务节点的定位信息;

利用各记账节点、以及发送所述待上链交易信息的业务节点的定位信息，确定各记账节点到发送所述待上链交易信息的业务节点的距离。

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、以及发送所述待上链交易信息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待上链交易信息的业务节点的距离。

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、以及发送所述待上链交易信息的业务节点定期向代理节点发送的方式，故不赘述。

该实施例的优点是，在确定接收所述待上链交易信息的记账节点时，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待上链交易信息的业务节点的距离。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待上链交易信息的业务节点可能非常远，如果将其选为接收所述待上链交易信息的记账节点，则增加了网络传输负担，也降低了上链处理速度。但如果某一记账节点离发送所述待上链交易信息的业务节点非常近，但其处理负荷很大，也会降低上链处理速度。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接收所述待上链交易信息的记账节点的方案，既能大致均衡每个记账节点的处理负荷，又不会给网络造成太大的传输负担。

在一个实施例中，如图 15 所示，步骤 430 可以包括:

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;

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；

步骤 4303：基于每个记账节点的第一分数和第二分数，确定接收所述待上链交易信息的记账节点。

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方式。该处理负荷与第一分数对应关系表预先可以设置，其中处理负荷越大，第一分数越低。例如：

处理负荷（未处理完的待上链交易信息数）	第一分数
0-1	5
2-4	4
5-9	3
10-19	2
20-49	1
50 以上	0

表 1　处理负荷与第一分数对应关系表

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方式。该距离与第二分数对应关系表可以预先设置，其中距离越大，第二分数越低。例如：

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

表 2　距离与第二分数对应关系表

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接收所述待上链交易信息的记账节点。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接收待上链交易信息的记账节点的影响分数化，提高了选择接收待上链交易信息的记账节点的精确性。

在一个实施例中，如图 16 所示，步骤 4303 包括：

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；

步骤 43032：基于所述加权和，确定接收所述待上链交易信息的记账节点。

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。

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，也可以在加权和大于预定加权和阈值的记账节点中随机选择一个，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记账节点，选取哪一个作为接收所述待上链交易信息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，防止在同一时间段内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超负荷运行。

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接收所述待上链交易信息的记账节点的贡献的差异性，提高了确定接收所述待上链交易信息的记账节点的合理性。

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应用于图 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划分为多个分支记账节点子网络的实施例中，则是下面要介绍的一种情况。

在该实施例中，待上链交易信息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，分成的每一类记账节点分别组成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信息。因此，代理节点要根据待上链交易信息中携带的交易信息类型，将该待上链交易信息发送到相应类型的分支记账节点子网络中的一个记账节点。为了实现这一点，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。

在该实施例中，如图 17 所示，接收来自业务节点的待上链交易信息的记账节点从记账节点子网络中按照以下方式选出：

步骤 510：获取待上链交易信息中的交易信息类型；

步骤 520：从记账节点标识和交易信息类型对应关系表中，查找与待上链交易信息中的交易信息类型对应的记账节点标识；

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。

该实施例的好处是，对于图 1C 所示的记账节点子网络端划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接收来自业务节点的待上链交易信息的记账节点的方式。

在一个实施例中，待上链交易信息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。

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待上链交易信息中的交易信息类型对应的记账节点标识。

如图 18 所示，在一个实施例中，步骤 530 包括:

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;

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待上链交易信息的业务节点的距离;

步骤 5303: 基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点。

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 18 的实施例中确定处理负荷和到发送所述待上链交易信息的业务节点的距离的记账节点的范围仅限于步骤 520 中找到的与待上链交易信息中的交易信息类型对应的记账节点标识的记账节点，而不是记账节点子网络中的所有记账节点，故不赘述。

根据本公开的一个实施例，如图 21 所示，还提供了一种在区块链网络中记录数据区块的记账节点。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:

签名生成单元 610，用于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;

上链单元 620，用于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;

发布单元 630，用于将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。

在一个实施例中，所述发布单元 630 进一步用于:

将所述签名和数据区块中的交易信息发送到所述业务节点子网络中的业务节点，使得业务节点执行: 获取特定于该记账节点的密钥; 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; 对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。

在一个实施例中，上链单元 620 进一步用于: 将所述交易信息、生成的签名连同对该数据区块中要包括的交易信息计算出的摘要加入所述数据区块，添加到区块链上;

在一个实施例中，发布单元 630 进一步用于: 将所述签名和所述摘要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、接收到的摘要对所述签名进行签名验证。

在一个实施例中，所述根据特定于该记账节点的密钥、接收到的摘要对所述签名

进行签名验证，包括：

获取特定于该记账节点的密钥；

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；

如果接收到的摘要与解密得到的摘要一致，则签名验证成功。

在一个实施例中，上链单元 620 进一步用于：

将所述交易信息加入数据区块的区块体；

将所述摘要和签名加入数据区块的区块头；

将所述数据区块添加到区块链上。

在该实施例中，发布单元 630 进一步用于：

将所述区块头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、所述区块头中的摘要对所述区块头中的签名进行签名验证。

在一个实施例中，所述将所述区块头发往所述业务节点子网络中的业务节点，包括：

将所述区块头发往代理节点，所述代理节点是所述业务节点子网络中的一个业务节点；

通过代理节点，将所述区块头广播到所述业务节点子网络中所述代理节点以外的其它业务节点。

在一个实施例中，所述将所述区块头发往所述业务节点子网络中的业务节点，包括：

将所述区块头发往代理节点，所述代理节点是所述业务节点子网络中的一个业务节点；

将代理节点作为发送节点，将所述区块头发送到尚未接收到该区块头的其它业务节点中离所述发送节点最近的业务节点，并以接收到该区块头的业务节点作为发送节点发送该区块头，直到所有其它业务节点都接收到该区块头。

在一个实施例中，所述将所述区块头发送到尚未接收到该区块头的其它业务节点中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所有其它业务节点与所述发送节点的距离；

向所述距离最小的其它业务节点发送所述区块头，其中，如果接收到所述区块头的其它业务节点之前已经接收到该区块头，向所述发送节点发送拒绝应答；

如果接收到拒绝应答，则向距离第二小的其它业务节点发送所述区块头，直到接收到接受应答。

在一个实施例中，所述确定所述业务节点子网络中除所述发送节点之外的所有其它业务节点与所述发送节点的距离包括：

周期性接收从所述业务节点子网络中除所述发送节点之外的所有其它业务节点广

播的定位信息;

按照最近一次接收到的除所述发送节点之外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。

在一个实施例中，在将所述区块头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、所述区块头中的摘要对所述区块头中的签名进行签名验证之后，由业务节点将签名验证结果以及所述区块头发送到仲裁服务器，其中，只要有一个业务节点针对所述区块头中的签名的签名验证结果是验证失败，就由仲裁服务器根据特定于该记账节点的密钥、所述区块头中的摘要对所述区块头中的签名进行签名验证。

在一个实施例中，在将所述区块头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、所述区块头中的摘要对所述区块头中的签名进行签名验证之后，由业务节点将签名验证结果发送到仲裁服务器，其中，如果超过 f 个业务节点的签名验证结果是验证失败，仲裁服务器向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块，其中，f 是不大于（N-1）/3 的所有整数中的最大整数。

在一个实施例中，对该数据区块中要包括的交易信息计算出的摘要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。所述记账节点还包括:

请求接收单元，用于接收业务节点对该数据区块中的交易信息的请求;

权限数据获取单元，用于获取该业务节点的权限数据;

返回单元，用于根据该业务节点的权限数据，对于该数据区块中该业务节点有权获取的交易信息，向该业务节点返回该交易信息，而对于该数据区块中该业务节点无权获取的交易信息，向该业务节点返回该交易信息的哈希值，从而，该业务节点根据接收到的交易信息和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，从而进行内容验证。

在一个实施例中，该业务节点根据接收到的交易信息和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，从而进行内容验证之后，由业务节点将内容验证结果、所述业务节点接收到的交易信息和哈希值、和区块头中包含的默克尔树根发送到仲裁服务器，其中，只要有一个业务节点针对该数据区块的内容验证结果是验证失败，由仲裁服务器根据接收到的交易信息和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，从而进行内容验证。

在一个实施例中，该业务节点根据接收到的交易信息和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，从而进行内容验证之后，由业务节点将内容验证结果发送到仲裁服务器，其中，如果超过 f 个业务节点的内容验证结果是验证失败，则仲裁服务器向生成所述数据区块的记账节点发出停止运行指令，并向区块链上增加包括该数据区块无效的指示的数据区块，其中，f 是不大于（N-1）/3 的所有整数中的最大整数，N 是业务节点子网络中业务节点的个数。

在一个实施例中，所述签名生成单元进一步用于：

接收来自业务节点的待上链交易信息并缓存；

如果缓存中的待上链交易信息达到预设的区块打包要求，将缓存中的待上链交易信息作为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；

从认证中心获取特定于该记账节点的密钥；

利用从认证中心获取的密钥，对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实施签名算法，生成签名。

在一个实施例中，所述区块打包要求包括以下中的至少一项：

缓存中的待上链交易信息的总大小达到预定大小阈值；

缓存中的待上链交易信息的总条数达到预定条数阈值；

缓存中的待上链交易信息中最早缓存的一条带上链交易信息的缓存时间距离当前时间达到预定时间阈值。

在一个实施例中，所述上链单元进一步用于：

将所述交易信息和生成的签名加入所述数据区块，发送到记账节点子网络中的所有记账节点中的领导记账节点；

由领导记账节点将所述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；

当共识成功后，由领导记账节点将所述数据区块添加到区块链上。

在一个实施例中，所述记账节点从记账节点子网络中按照以下方式选出：

获取记账节点子网络中每个记账节点的处理负荷；

确定记账节点子网络中每个记账节点到发送所述待上链交易信息的业务节点的距离；

基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点。

在一个实施例中，所述基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点，包括：

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；

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；

基于每个记账节点的第一分数和第二分数，确定接收所述待上链交易信息的记账节点。

在一个实施例中，所述基于每个记账节点的第一分数和第二分数，确定接收所述待上链交易信息的记账节点，包括：

确定每个记账节点的第一分数和第二分数的加权和；

基于所述加权和，确定接收所述待上链交易信息的记账节点。

在一个实施例中，所述基于所述加权和，确定接收所述待上链交易信息的记账节点，包括：

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。

在一个实施例中，所述待上链交易信息中带有交易信息类型，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，分成的每一类记账节点分别组成一个分支记账节点子网络，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。所述记账节点从记账节点子网络中按照以下方式选出：

获取待上链交易信息中的交易信息类型；

从记账节点标识和交易信息类型对应关系表中，查找与待上链交易信息中的交易信息类型对应的记账节点标识；

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。

在一个实施例中，所述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，包括：

获取每个找到的记账节点标识的记账节点的处理负荷；

确定每个找到的记账节点标识的记账节点到发送所述待上链交易信息的业务节点的距离；

基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点。

根据本公开实施例的在区块链网络中记录数据区块的方法可以由图 22 的记账节点 21 实现。下面参照图 22 来描述根据本公开实施例的记账节点 21。图 22 显示的记账节点 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。

如图 22 所示，记账节点 21 以通用计算设备的形式表现。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。

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 执行本说明书上述实施例中描述的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。

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。

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。

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。

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记账节点 21 交互的设备通信，和

/或与使得该记账节点 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 850 进行。并且，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。

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。

在本公开的示例性实施例中，还提供了一种计算机可读存储介质，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描述的方法。

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。

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。

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。

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。

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）。

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。

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。

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。

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。

权利要求书

1、一种在区块链网络中记录数据区块的方法，其中，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:

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;

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;

将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。

2、根据权利要求 1 所述的方法，其中，所述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，包括:

将所述交易信息、生成的签名连同对该数据区块中要包括的交易信息计算出的摘要加入所述数据区块，添加到区块链上;

所述将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，包括:

将所述签名和所述摘要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、接收到的摘要对所述签名进行签名验证。

3、根据权利要求 2 所述的方法，其中，所述将所述交易信息、生成的签名连同对该数据区块中要包括的交易信息计算出的摘要加入所述数据区块，添加到区块链上，包括:

将所述交易信息加入数据区块的区块体;

将所述摘要和签名加入数据区块的区块头;

将所述数据区块添加到区块链上;

所述将所述签名和所述摘要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、接收到的摘要对所述签名进行签名验证，包括:

将所述区块头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、所述区块头中的摘要对所述区块头中的签名进行签名验证。

4、根据权利要求 3 所述的方法，其中，所述将所述区块头发往所述业务节点子网络中的业务节点，包括:

将所述区块头发往代理节点，所述代理节点是所述业务节点子网络中的一个业务节点;

通过代理节点，将所述区块头广播到所述业务节点子网络中所述代理节点以外的其它业务节点。

5、根据权利要求 3 所述的方法，其中，所述将所述区块头发往所述业务节点子网

络中的业务节点，包括:

将所述区块头发往代理节点，所述代理节点是所述业务节点子网络中的一个业务节点;

将代理节点作为发送节点，将所述区块头发送到尚未接收到该区块头的其它业务节点中离所述发送节点最近的业务节点，并以接收到该区块头的业务节点作为发送节点发送该区块头，直到所有其它业务节点都接收到该区块头。

6、根据权利要求 5 所述的方法，其中，所述将所述区块头发送到尚未接收到该区块头的其它业务节点中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所有其它业务节点与所述发送节点的距离;

向所述距离最小的其它业务节点发送所述区块头，其中，如果接收到所述区块头的其它业务节点之前已经接收到该区块头，向所述发送节点发送拒绝应答;

如果接收到拒绝应答，则向距离第二小的其它业务节点发送所述区块头，直到接收到接受应答。

7、根据权利要求 3 所述的方法，其中，对该数据区块中要包括的交易信息计算出的摘要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，

在将所述区块头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、所述区块头中的摘要对所述区块头中的签名进行签名验证之后，所述方法还包括:

接收业务节点对该数据区块中的交易信息的请求;

获取该业务节点的权限数据;

根据该业务节点的权限数据，对于该数据区块中该业务节点有权获取的交易信息，向该业务节点返回该交易信息，而对于该数据区块中该业务节点无权获取的交易信息，向该业务节点返回该交易信息的哈希值，从而，该业务节点根据接收到的交易信息和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，从而进行内容验证。

8、根据权利要求 1 所述的方法，其中，所述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，包括:

接收来自业务节点的待上链交易信息并缓存;

如果缓存中的待上链交易信息达到预设的区块打包要求，将缓存中的待上链交易信息作为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;

从认证中心获取特定于该记账节点的密钥;

利用从认证中心获取的密钥，对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实施签名算法，生成签名。

9、根据权利要求 8 所述的方法，其中，所述区块打包要求包括以下中的至少一项:

缓存中的待上链交易信息的总大小达到预定大小阈值;

缓存中的待上链交易信息的总条数达到预定条数阈值;

缓存中的待上链交易信息中最早缓存的一条待上链交易信息的缓存时间距离当前时间达到预定时间阈值。

10、根据权利要求 8 所述的方法，其中，接收来自业务节点的待上链交易信息的记账节点从记账节点子网络中按照以下方式选出：

获取记账节点子网络中每个记账节点的处理负荷；

确定记账节点子网络中每个记账节点到发送所述待上链交易信息的业务节点的距离；

基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点。

11、根据权利要求 10 所述的方法，其中，所述基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点，包括：

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；

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；

基于每个记账节点的第一分数和第二分数，确定接收所述待上链交易信息的记账节点。

12、根据权利要求 11 所述的方法，其中，所述基于每个记账节点的第一分数和第二分数，确定接收所述待上链交易信息的记账节点，包括：

确定每个记账节点的第一分数和第二分数的加权和；

基于所述加权和，确定接收所述待上链交易信息的记账节点。

13、一种在区块链网络中记录数据区块的记账节点，其中，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：

签名生成单元，用于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；

上链单元，用于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；

发布单元，用于将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。

14、一种记账节点，包括：

存储器，用于存储计算机可读指令；

一个或多个处理器，用于读取所述存储器存储的计算机可读指令，以执行权利要求 1-12 中的任一项所述的方法。

15、一种计算机可读存储介质，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 1-12 中的任一项所述的方法。

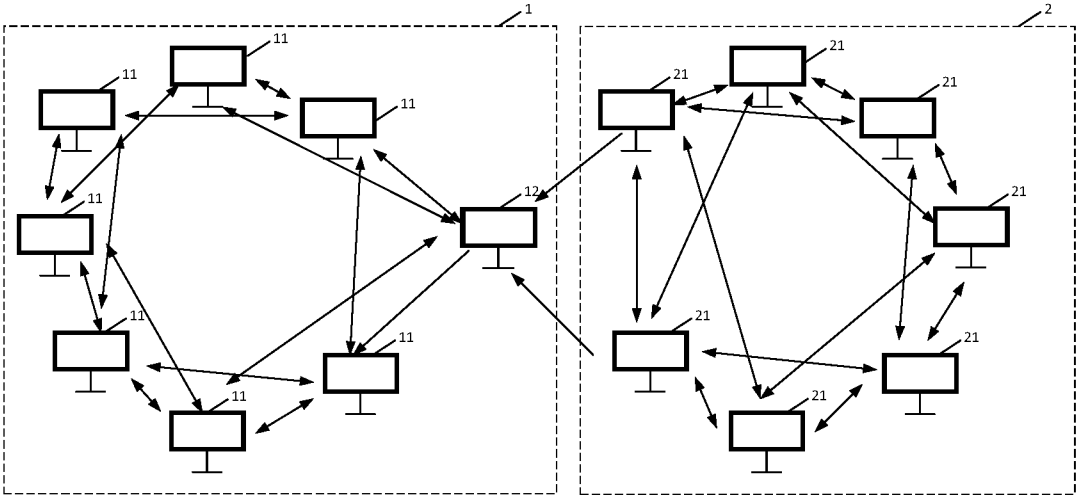


图 1A

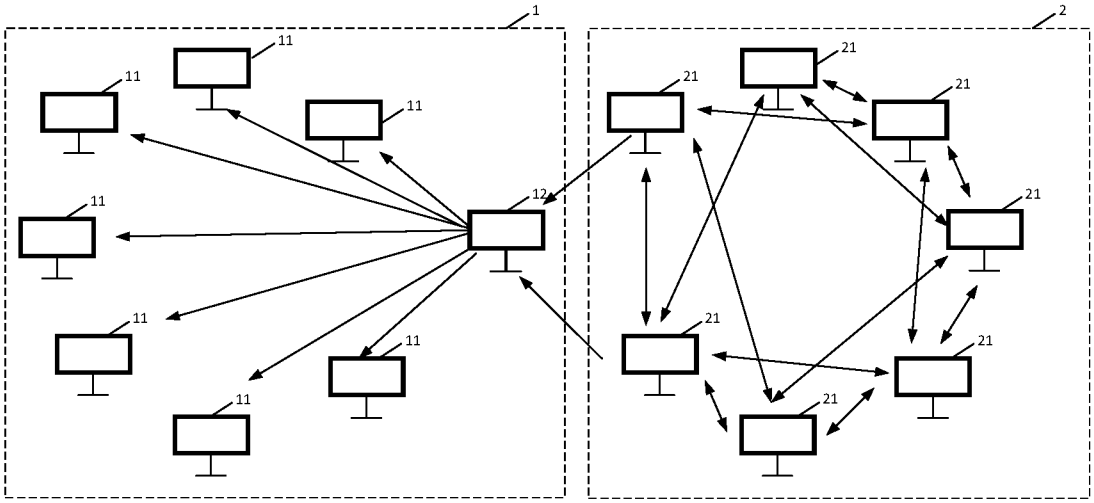


图 1B

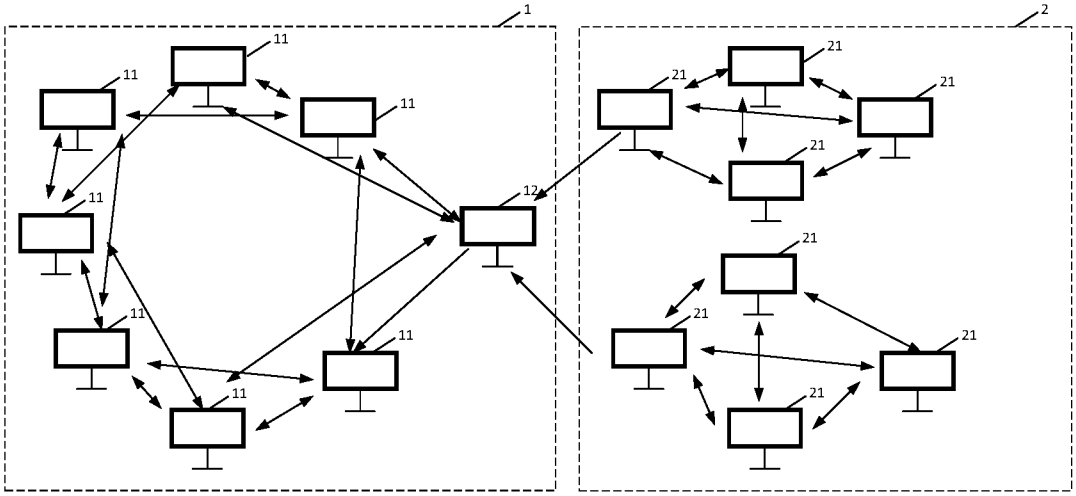


图 1C

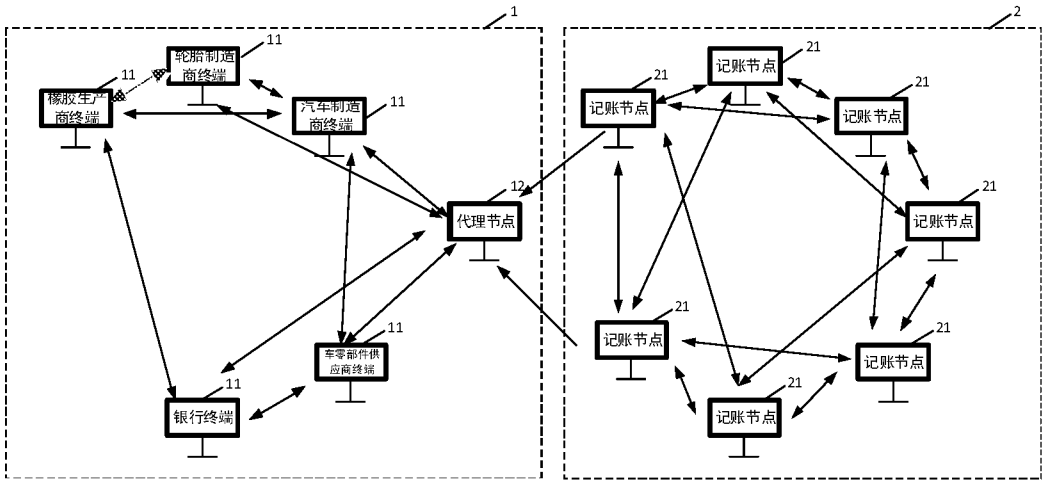

1
2
轮胎制造商终端
橡胶生产商终端
汽车制造商终端
代理节点
车零部件供应商终端
银行终端
记账节点
11
12
21

图 2A

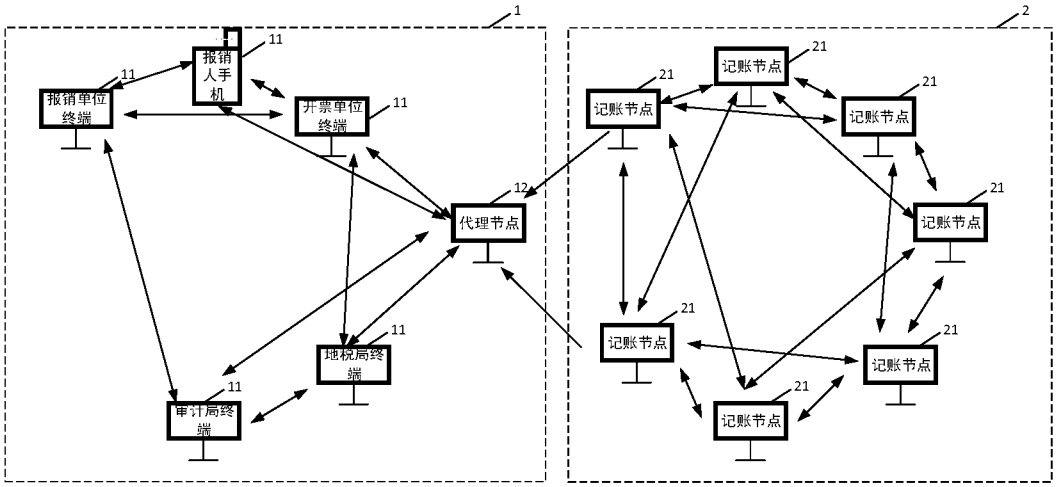

1
2
报销人手机
报销单位终端
开票单位终端
代理节点
地税局终端
审计局终端
记账节点
11
12
21

图 2B

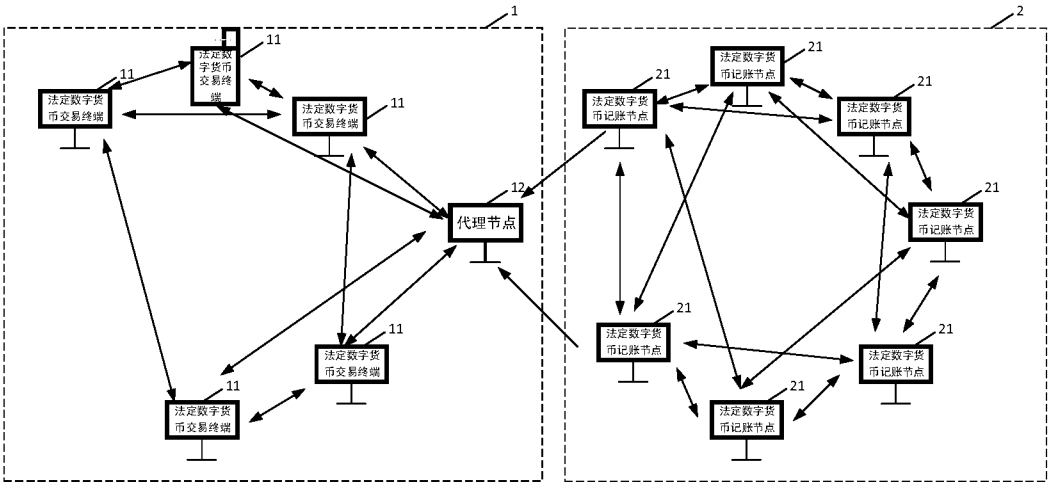

1
2
法定数字货币交易终端
法定数字货币记账节点
代理节点
11
12
21

图 2C

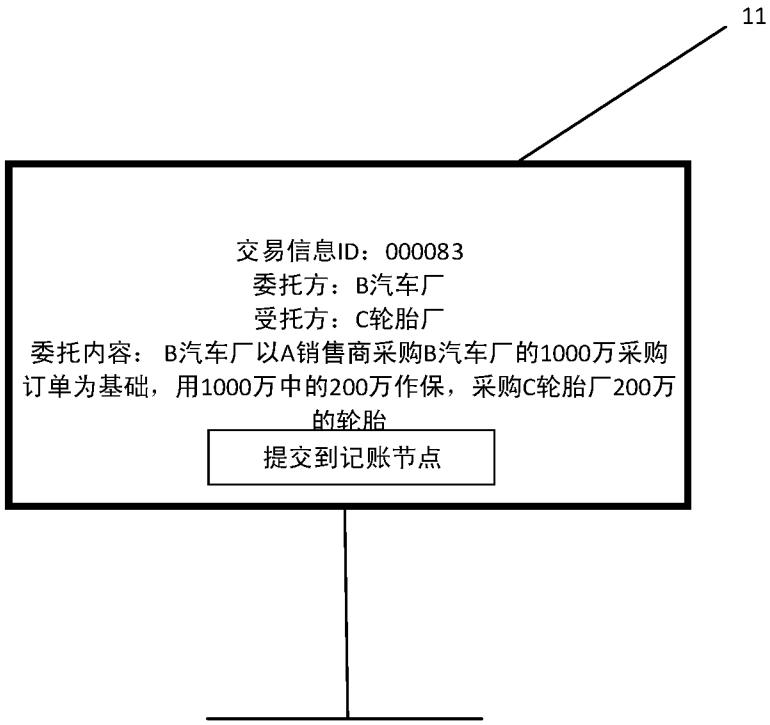

11
交易信息ID：000083
委托方：B汽车厂
受托方：C轮胎厂
委托内容： B汽车厂以A销售商采购B汽车厂的1000万采购订单为基础，用1000万中的200万作保，采购C轮胎厂200万的轮胎
提交到记账节点

图 3A

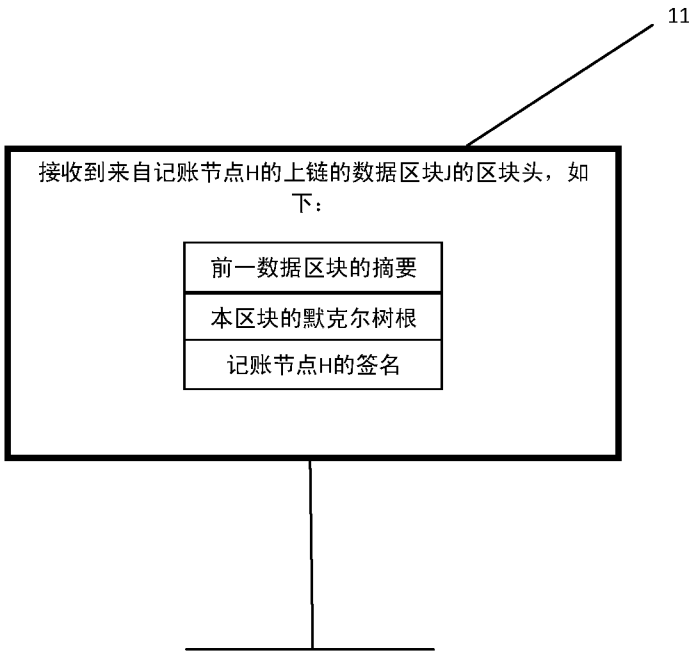

11
接收到来自记账节点H的上链的数据区块J的区块头，如下：
前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名

图 3B

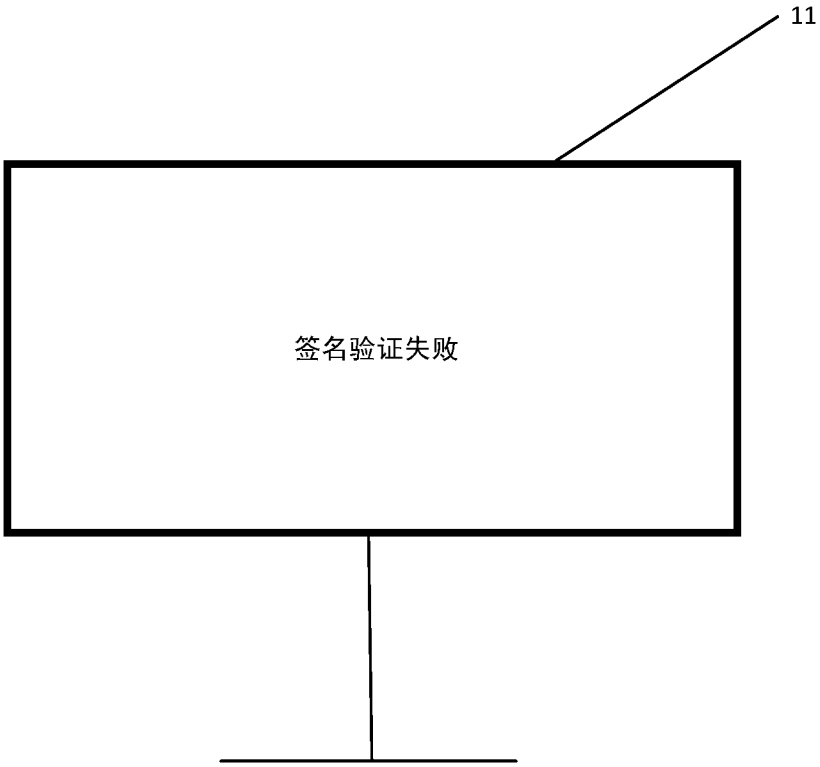


图 3C

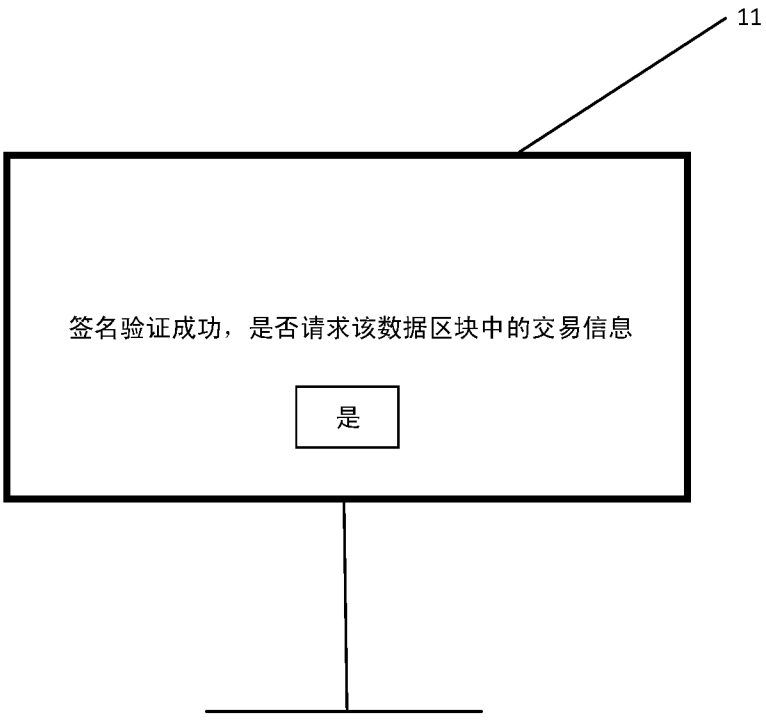


图 3D

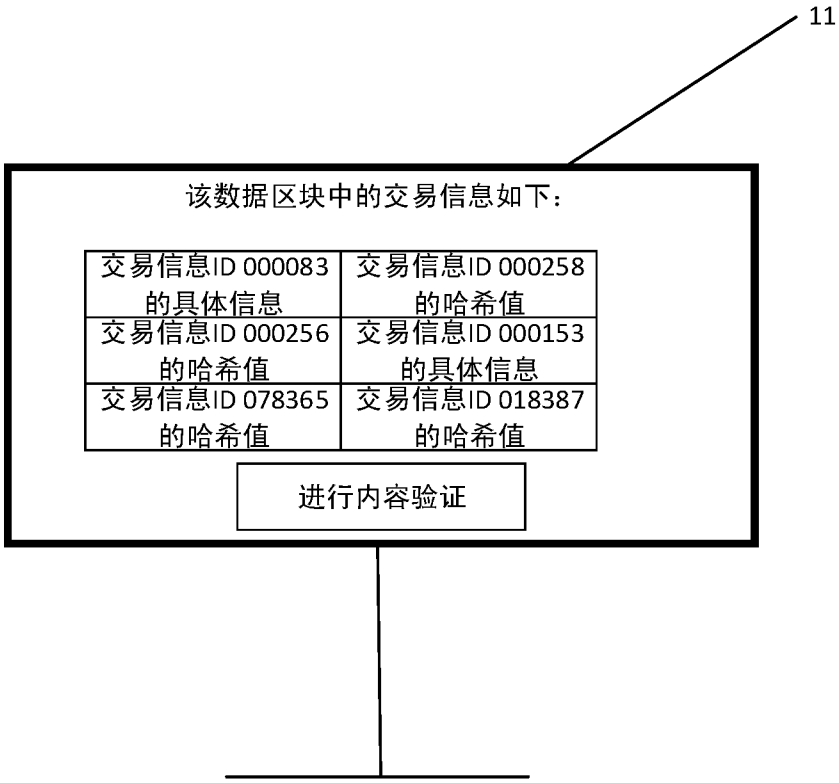

11
该数据区块中的交易信息如下：
交易信息ID 000083的具体信息
交易信息ID 000258的哈希值
交易信息ID 000256的哈希值
交易信息ID 000153的具体信息
交易信息ID 078365的哈希值
交易信息ID 018387的哈希值
进行内容验证

图 3E

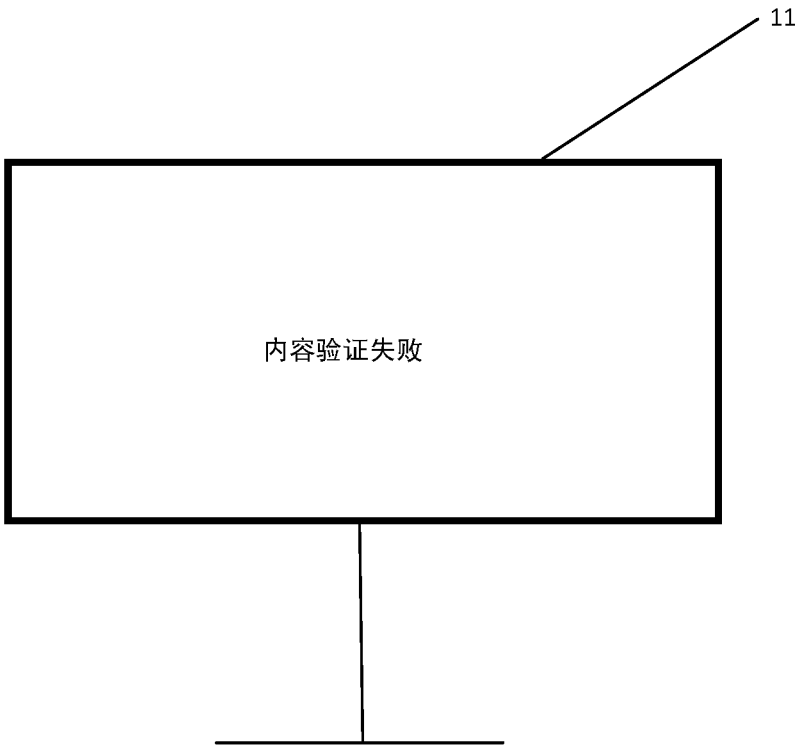

11
内容验证失败

图 3F

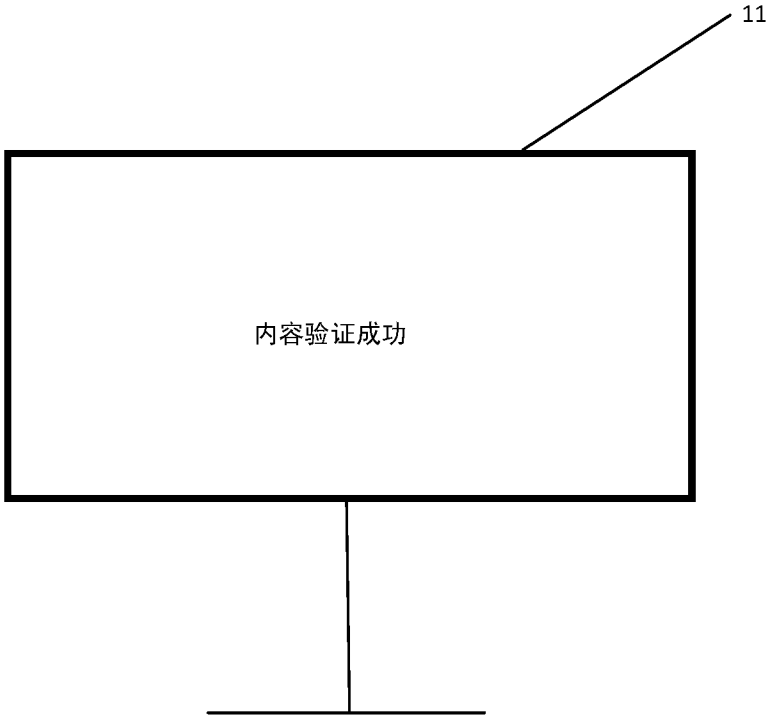

11
内容验证成功

图 3G

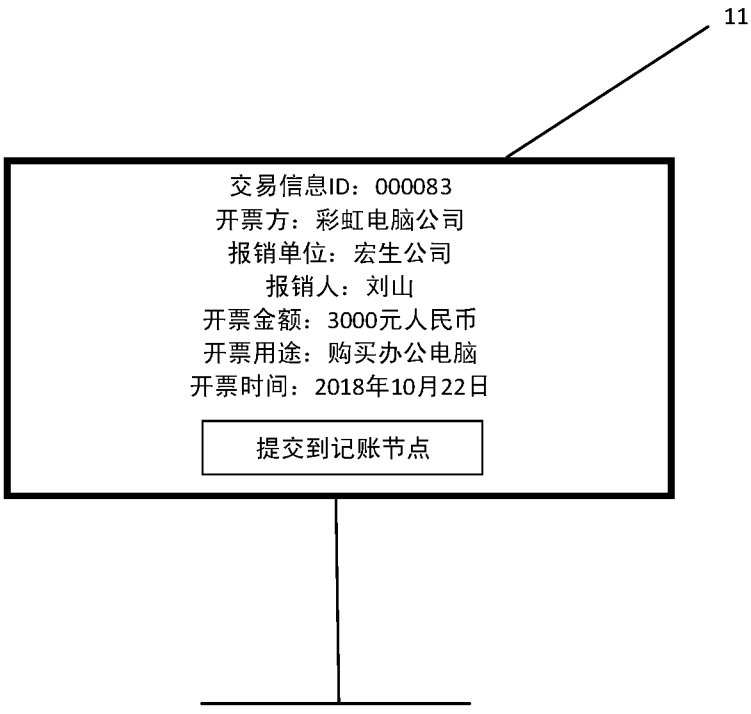

11
交易信息ID：000083
开票方：彩虹电脑公司
报销单位：宏生公司
报销人：刘山
开票金额：3000元人民币
开票用途：购买办公电脑
开票时间：2018年10月22日
提交到记账节点

图 4A

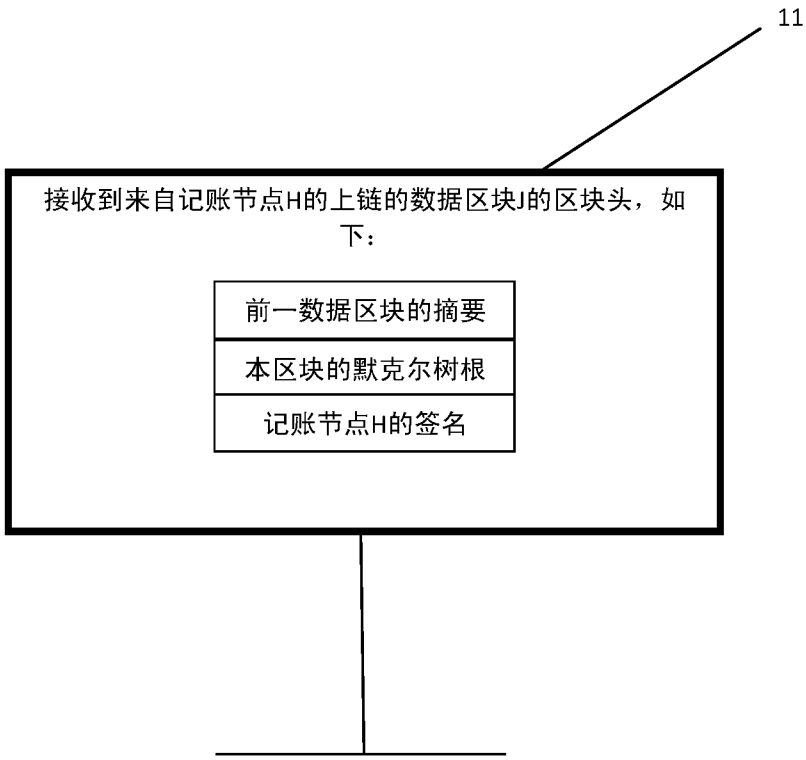

11
接收到来自记账节点H的上链的数据区块J的区块头，如下：
前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名

图 4B

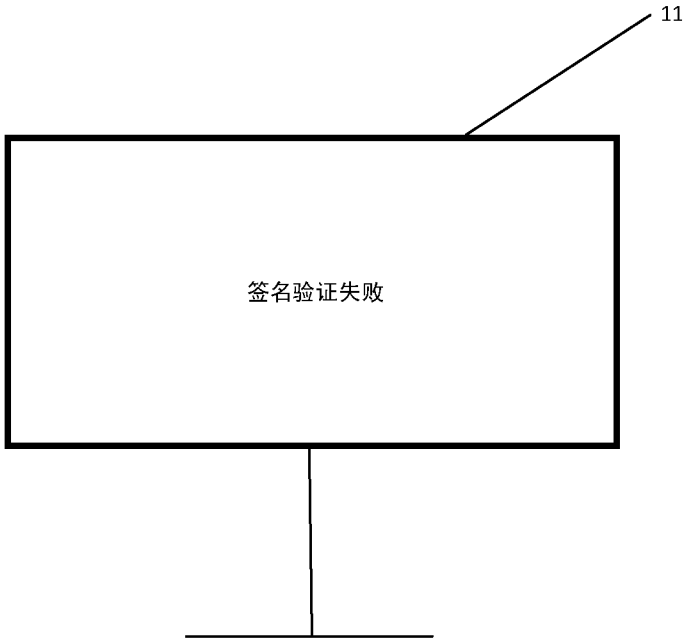

11
签名验证失败

图 4C

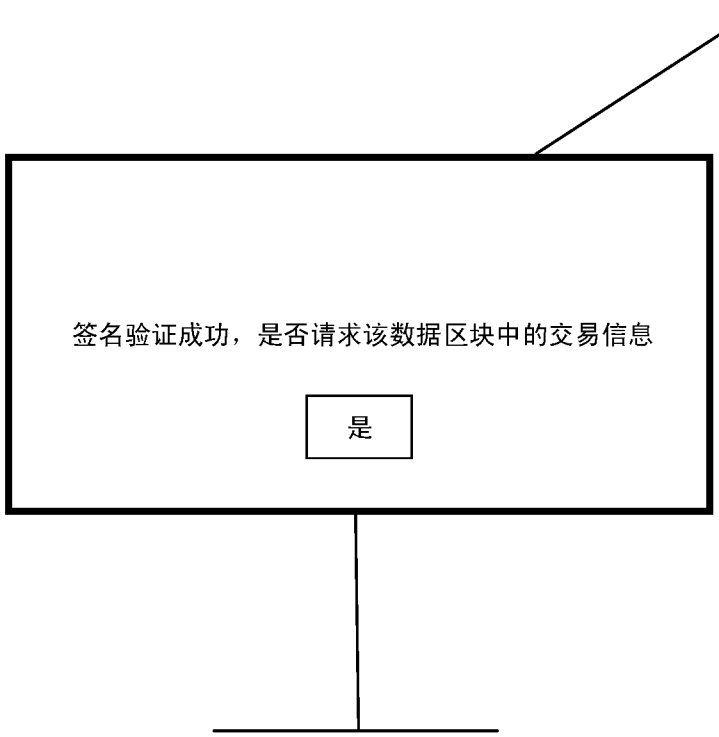

11
签名验证成功，是否请求该数据区块中的交易信息
是

图 4D

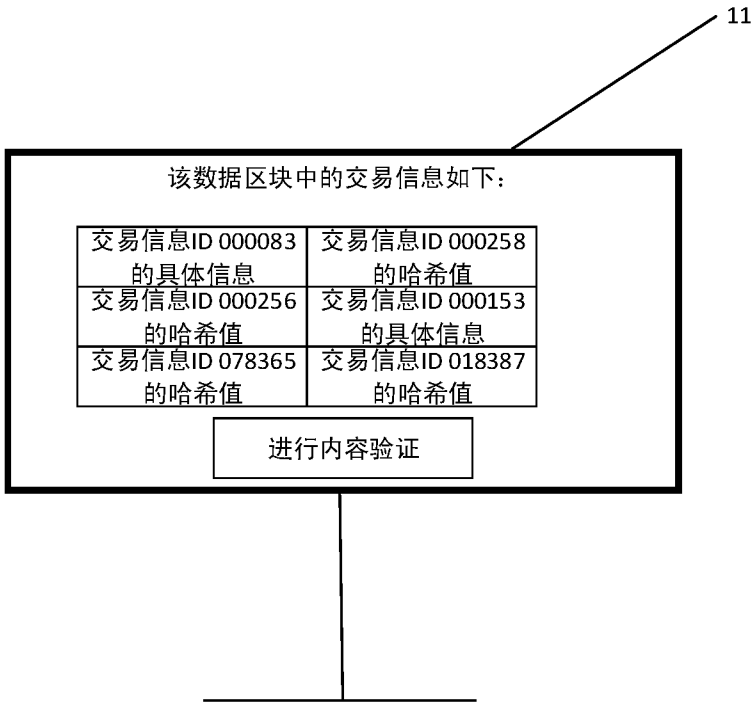

11
该数据区块中的交易信息如下：
交易信息ID 000083 的具体信息
交易信息ID 000258 的哈希值
交易信息ID 000256 的哈希值
交易信息ID 000153 的具体信息
交易信息ID 078365 的哈希值
交易信息ID 018387 的哈希值
进行内容验证

图 4E

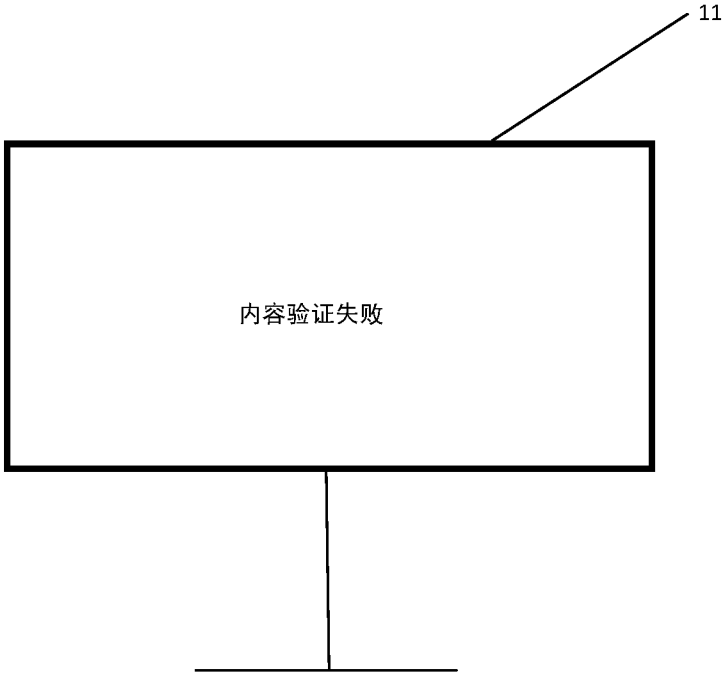


图 4F

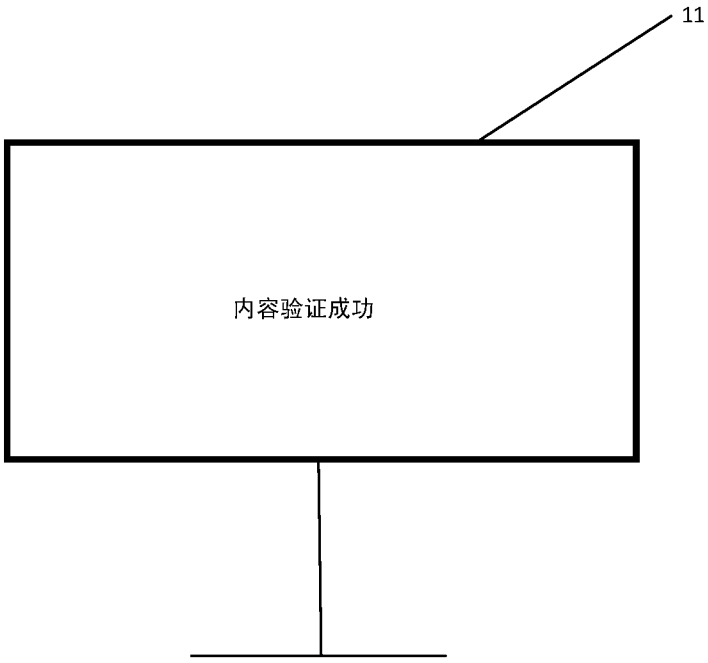


图 4G

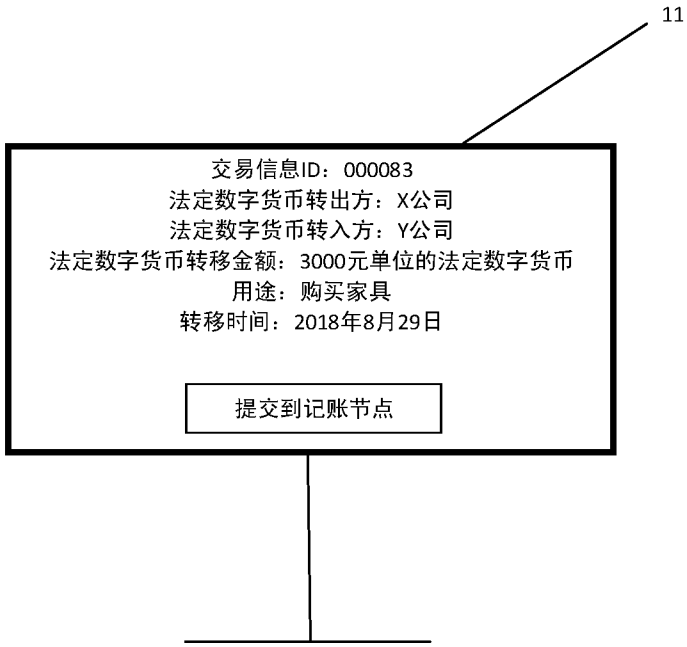

11
交易信息ID：000083
法定数字货币转出方：X公司
法定数字货币转入方：Y公司
法定数字货币转移金额：3000元单位的法定数字货币
用途：购买家具
转移时间：2018年8月29日
提交到记账节点

图 5A

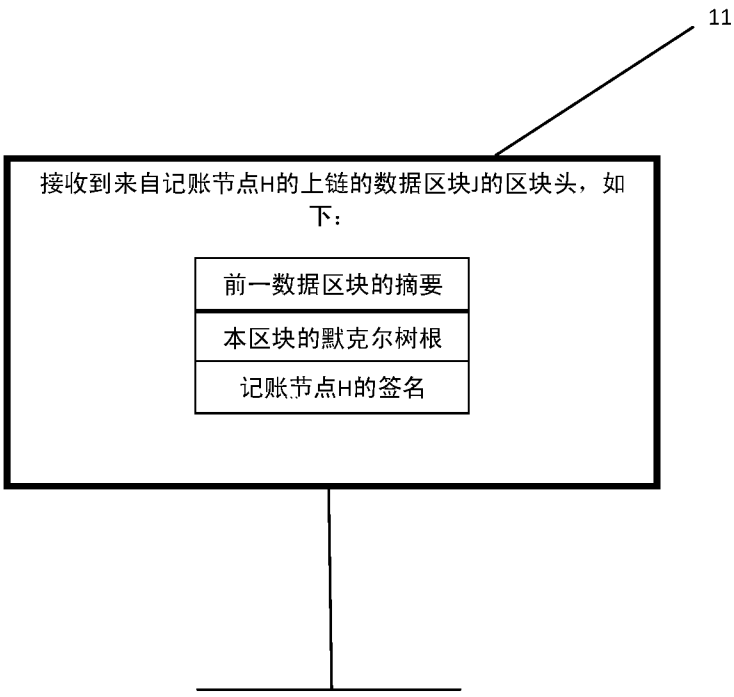

11
接收到来自记账节点H的上链的数据区块J的区块头，如下：
前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名

图 5B

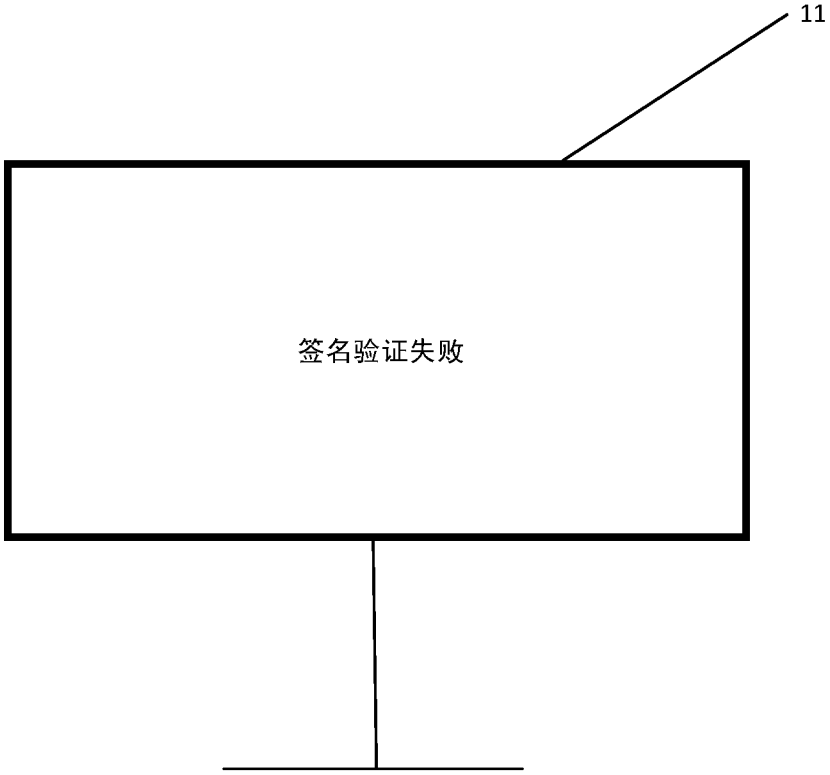


图 5C

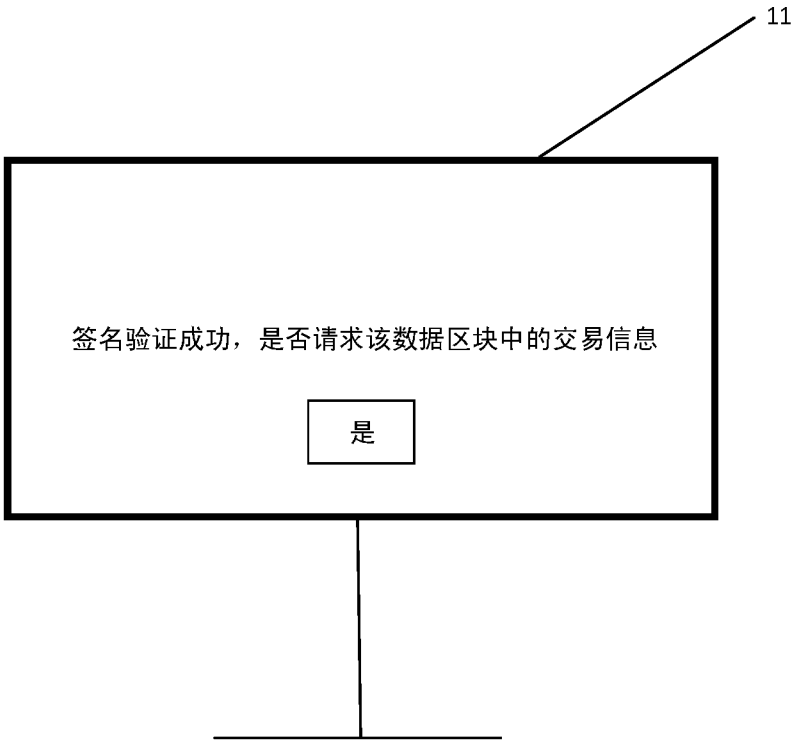


图 5D

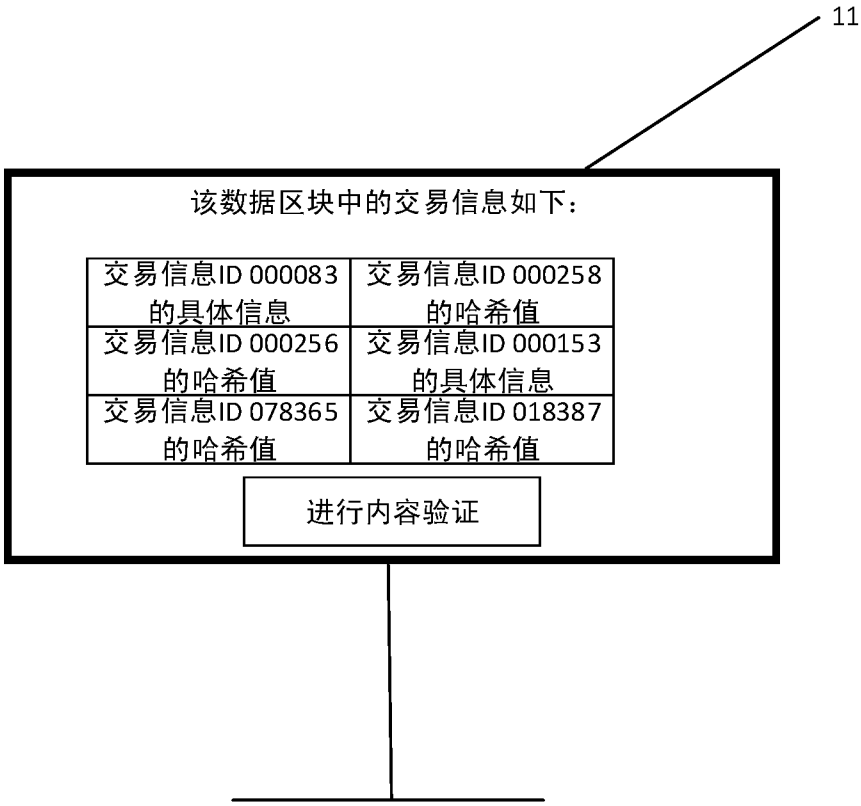

11
该数据区块中的交易信息如下：
交易信息ID 000083的具体信息
交易信息ID 000258的哈希值
交易信息ID 000256的哈希值
交易信息ID 000153的具体信息
交易信息ID 078365的哈希值
交易信息ID 018387的哈希值
进行内容验证

图 5E

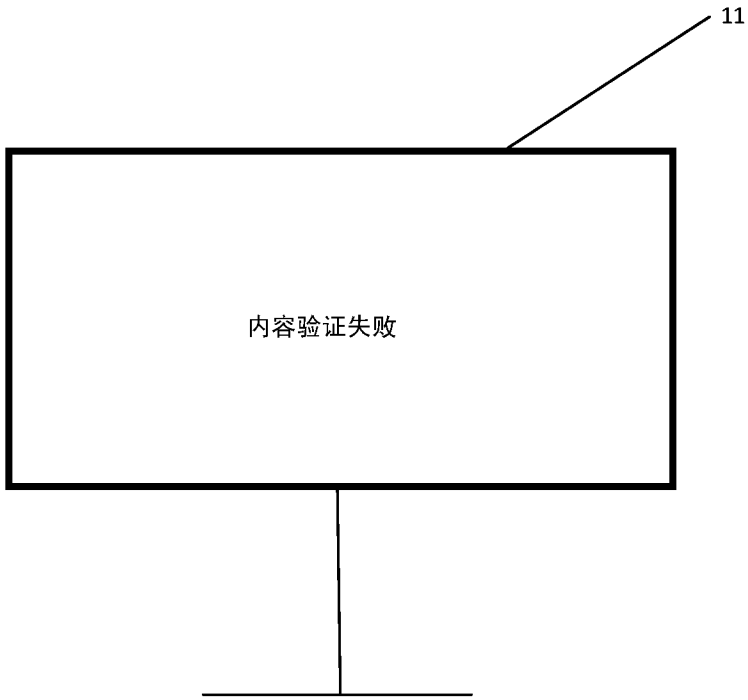

11
内容验证失败

图 5F

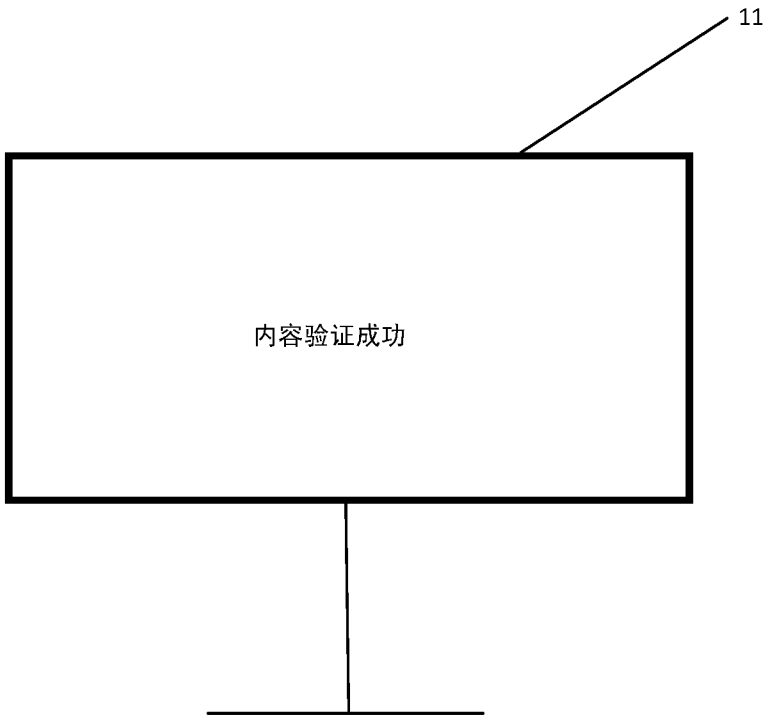

11
内容验证成功

图 5G

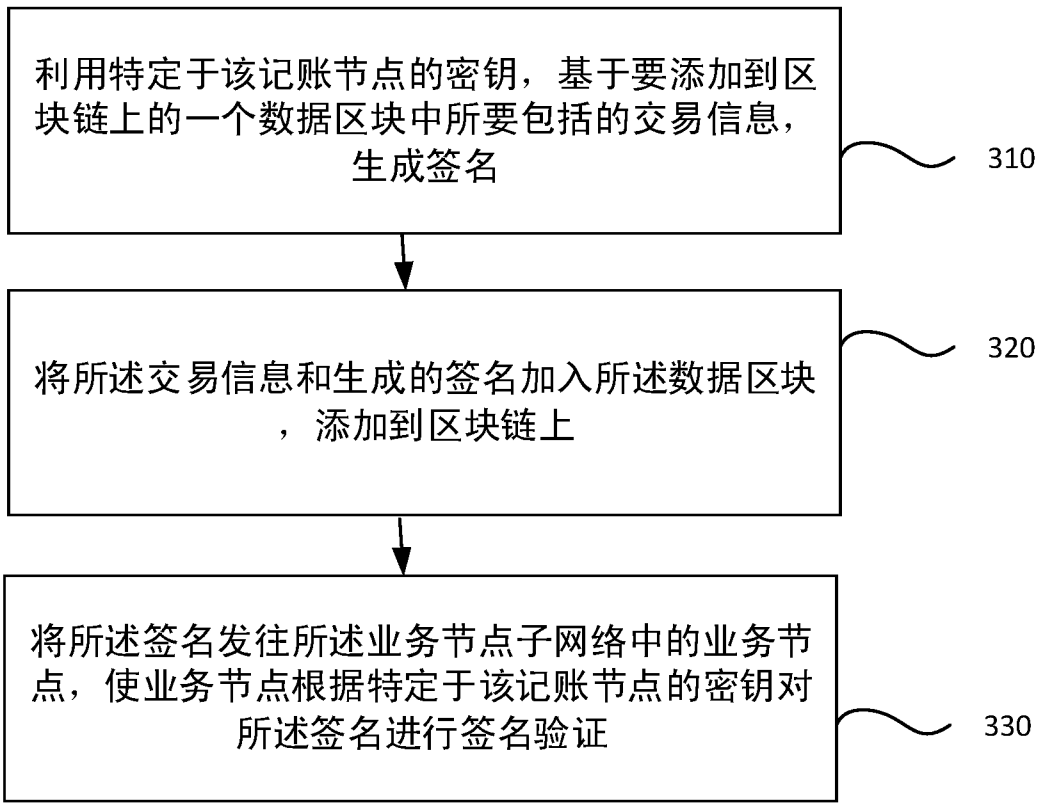

利用特定于该记账节点的密钥，基于要添加到区块链上的一个数据区块中所要包括的交易信息，生成签名
310
将所述交易信息和生成的签名加入所述数据区块，添加到区块链上
320
将所述签名发往所述业务节点子网络中的业务节点，使业务节点根据特定于该记账节点的密钥对所述签名进行签名验证
330

图 6

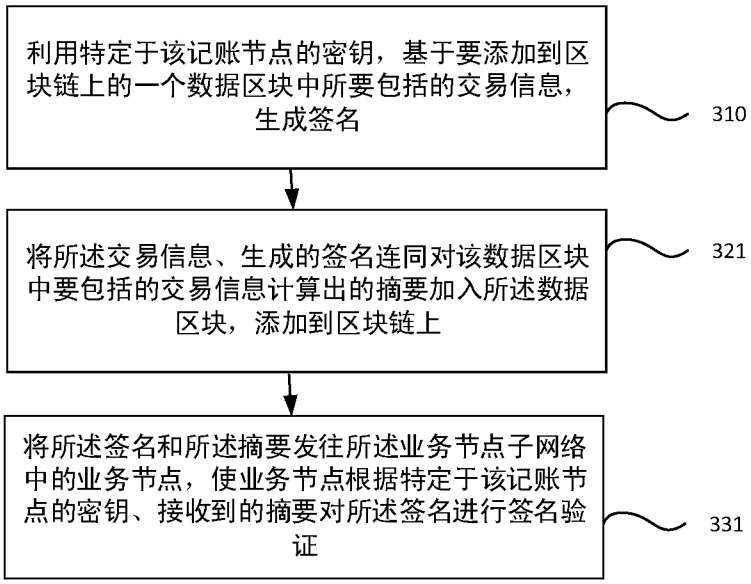

利用特定于该记账节点的密钥，基于要添加到区块链上的一个数据区块中所要包括的交易信息，生成签名
310
将所述交易信息、生成的签名连同对该数据区块中要包括的交易信息计算出的摘要加入所述数据区块，添加到区块链上
321
将所述签名和所述摘要发往所述业务节点子网络中的业务节点，使业务节点根据特定于该记账节点的密钥、接收到的摘要对所述签名进行签名验证
331

图 7

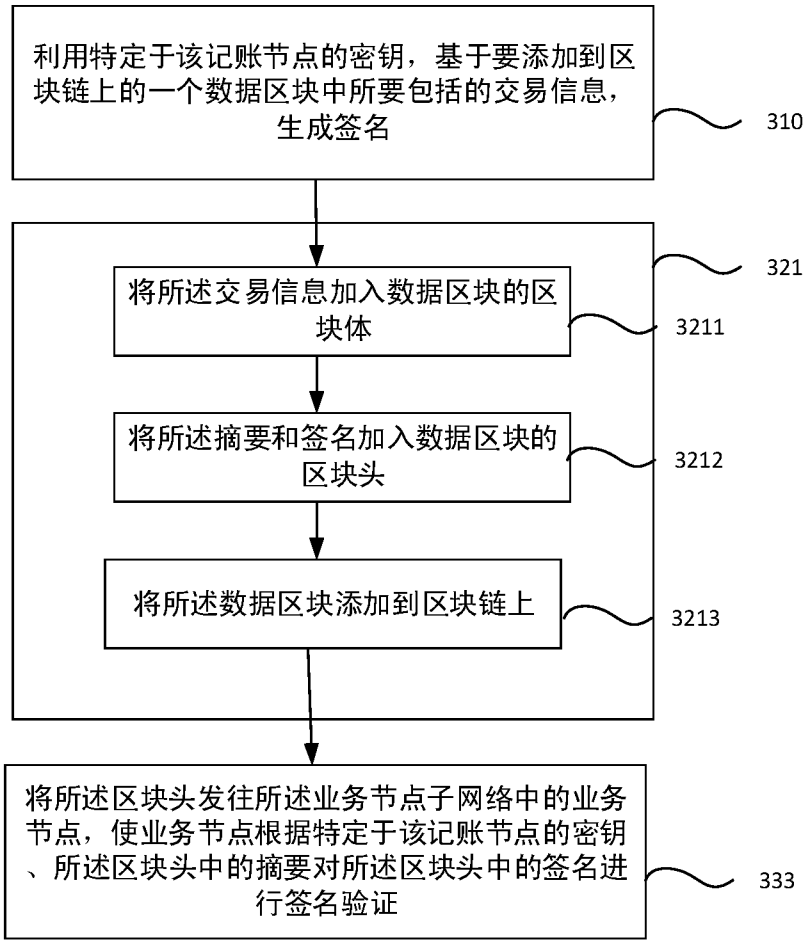

利用特定于该记账节点的密钥，基于要添加到区块链上的一个数据区块中所要包括的交易信息，生成签名
310
321
将所述交易信息加入数据区块的区块体
3211
将所述摘要和签名加入数据区块的区块头
3212
将所述数据区块添加到区块链上
3213
将所述区块头发往所述业务节点子网络中的业务节点，使业务节点根据特定于该记账节点的密钥、所述区块头中的摘要对所述区块头中的签名进行签名验证
333

图 8

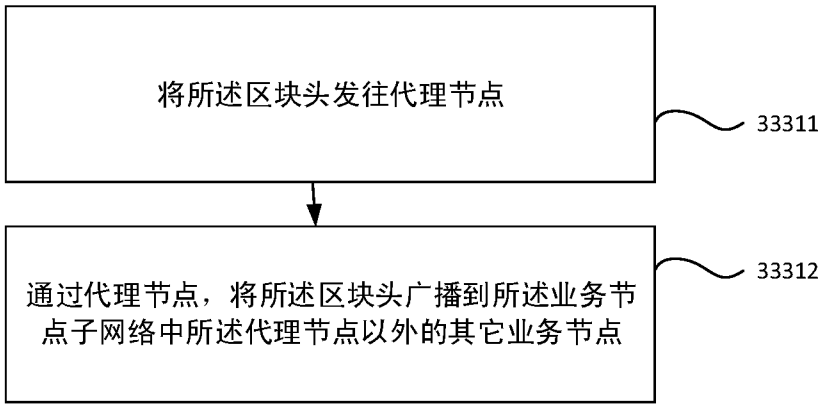

将所述区块头发往代理节点
33311
通过代理节点，将所述区块头广播到所述业务节点子网络中所述代理节点以外的其它业务节点
33312

图 9

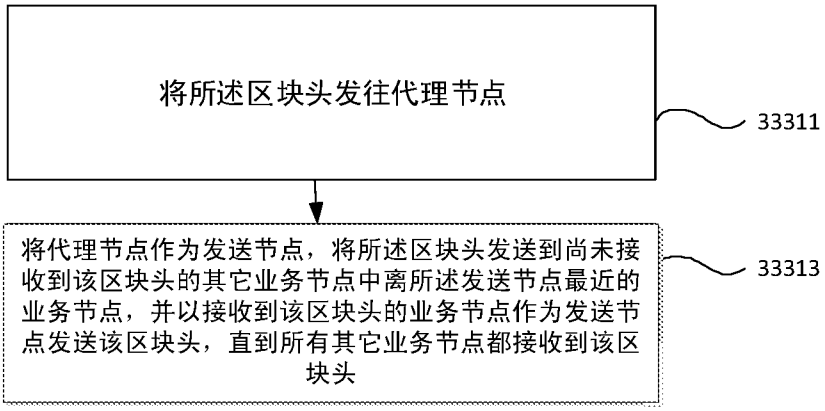

将所述区块头发往代理节点
33311
将代理节点作为发送节点，将所述区块头发送到尚未接收到该区块头的其它业务节点中离所述发送节点最近的业务节点，并以接收到该区块头的业务节点作为发送节点发送该区块头，直到所有其它业务节点都接收到该区块头
33313

图 10

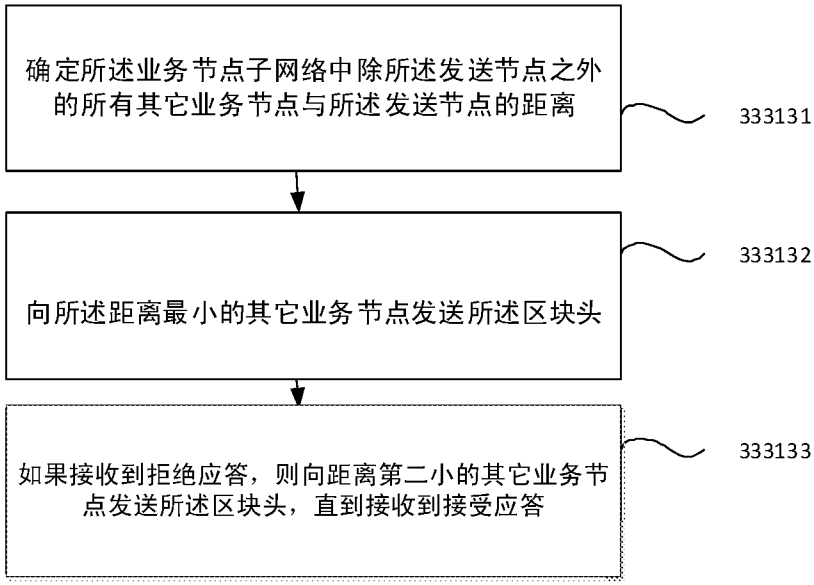

确定所述业务节点子网络中除所述发送节点之外的所有其它业务节点与所述发送节点的距离
333131
向所述距离最小的其它业务节点发送所述区块头
333132
如果接收到拒绝应答，则向距离第二小的其它业务节点发送所述区块头，直到接收到接受应答
333133

图 11

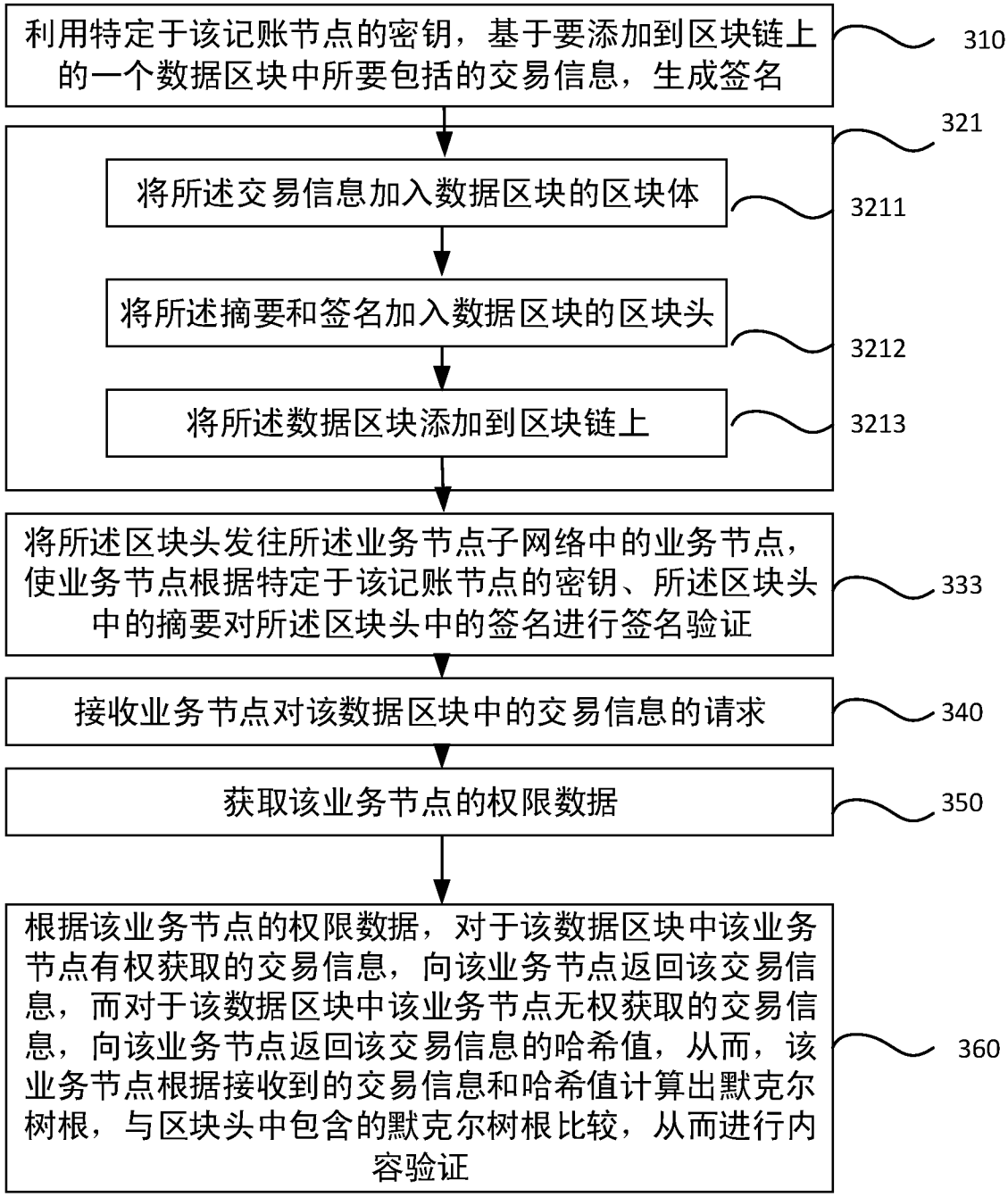

利用特定于该记账节点的密钥，基于要添加到区块链上的一个数据区块中所要包括的交易信息，生成签名
310
321
将所述交易信息加入数据区块的区块体
3211
将所述摘要和签名加入数据区块的区块头
3212
将所述数据区块添加到区块链上
3213
将所述区块头发往所述业务节点子网络中的业务节点，使业务节点根据特定于该记账节点的密钥、所述区块头中的摘要对所述区块头中的签名进行签名验证
333
接收业务节点对该数据区块中的交易信息的请求
340
获取该业务节点的权限数据
350
根据该业务节点的权限数据，对于该数据区块中该业务节点有权获取的交易信息，向该业务节点返回该交易信息，而对于该数据区块中该业务节点无权获取的交易信息，向该业务节点返回该交易信息的哈希值，从而，该业务节点根据接收到的交易信息和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，从而进行内容验证
360

图 12

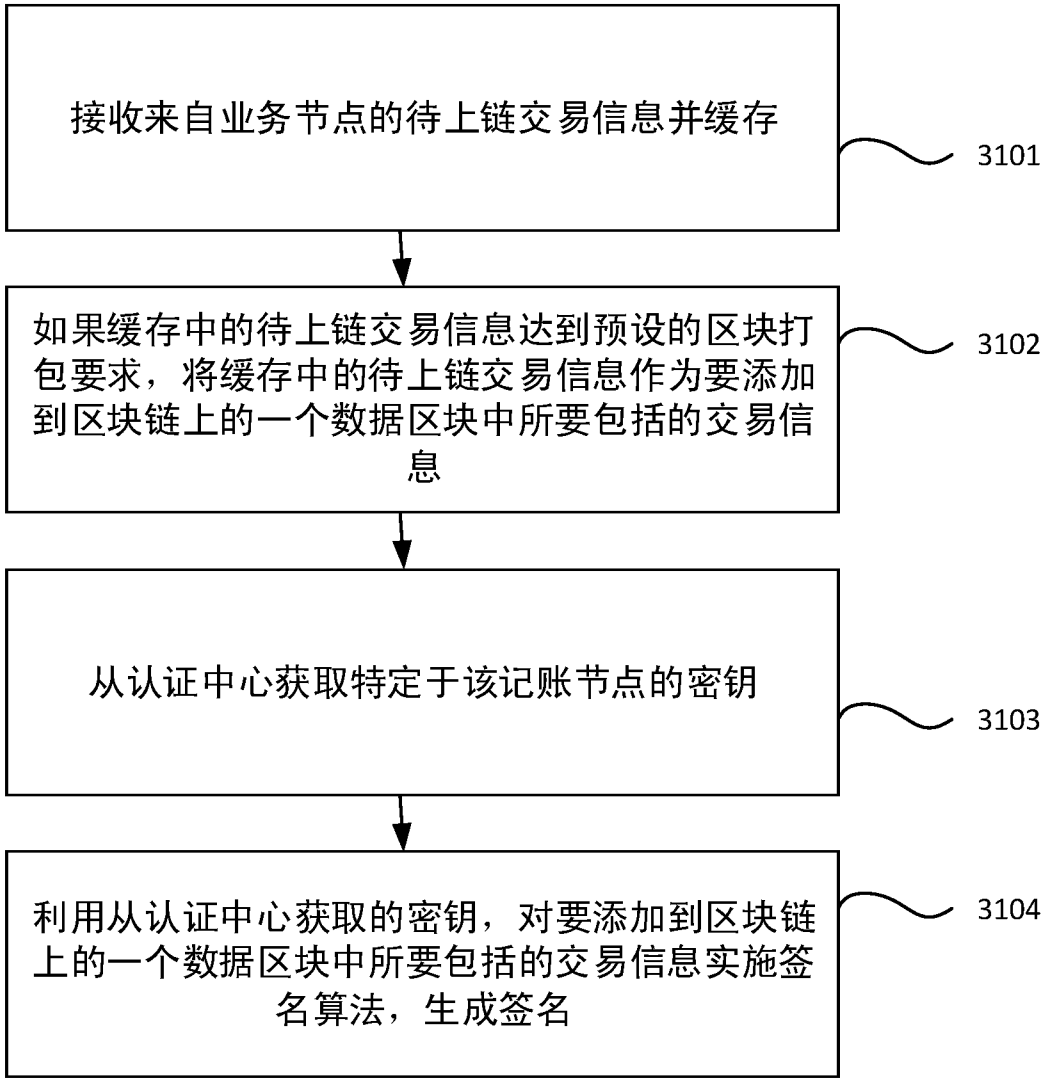

接收来自业务节点的待上链交易信息并缓存
3101
如果缓存中的待上链交易信息达到预设的区块打包要求，将缓存中的待上链交易信息作为要添加到区块链上的一个数据区块中所要包括的交易信息
3102
从认证中心获取特定于该记账节点的密钥
3103
利用从认证中心获取的密钥，对要添加到区块链上的一个数据区块中所要包括的交易信息实施签名算法，生成签名
3104

图 13

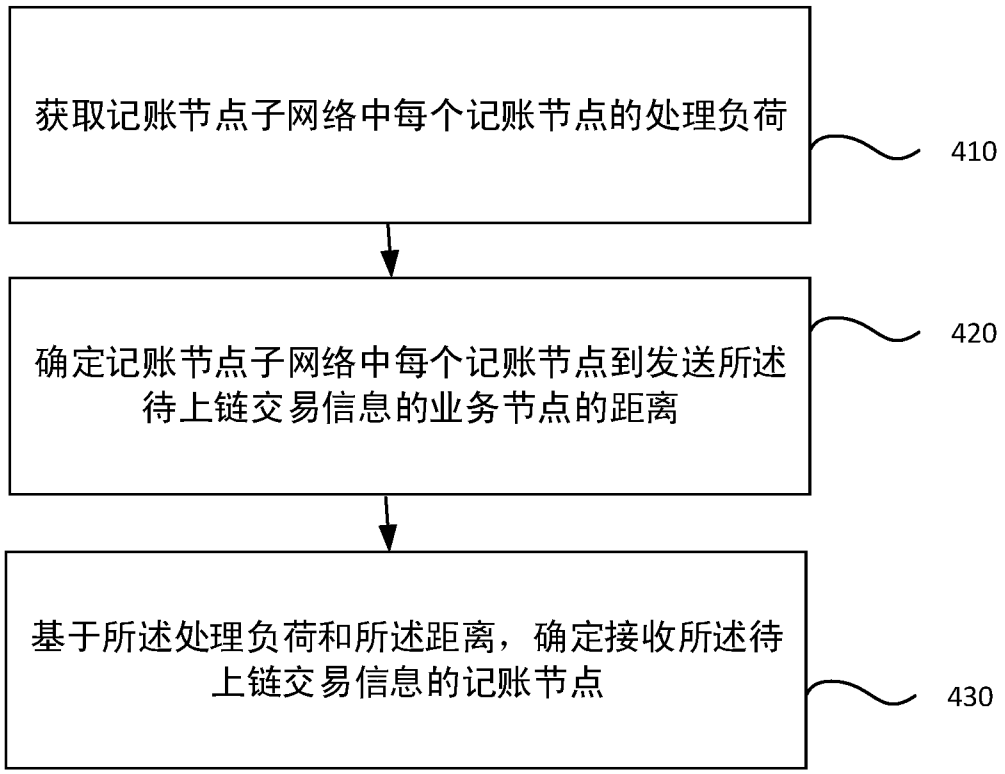

获取记账节点子网络中每个记账节点的处理负荷
410
确定记账节点子网络中每个记账节点到发送所述待上链交易信息的业务节点的距离
420
基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点
430

图 14

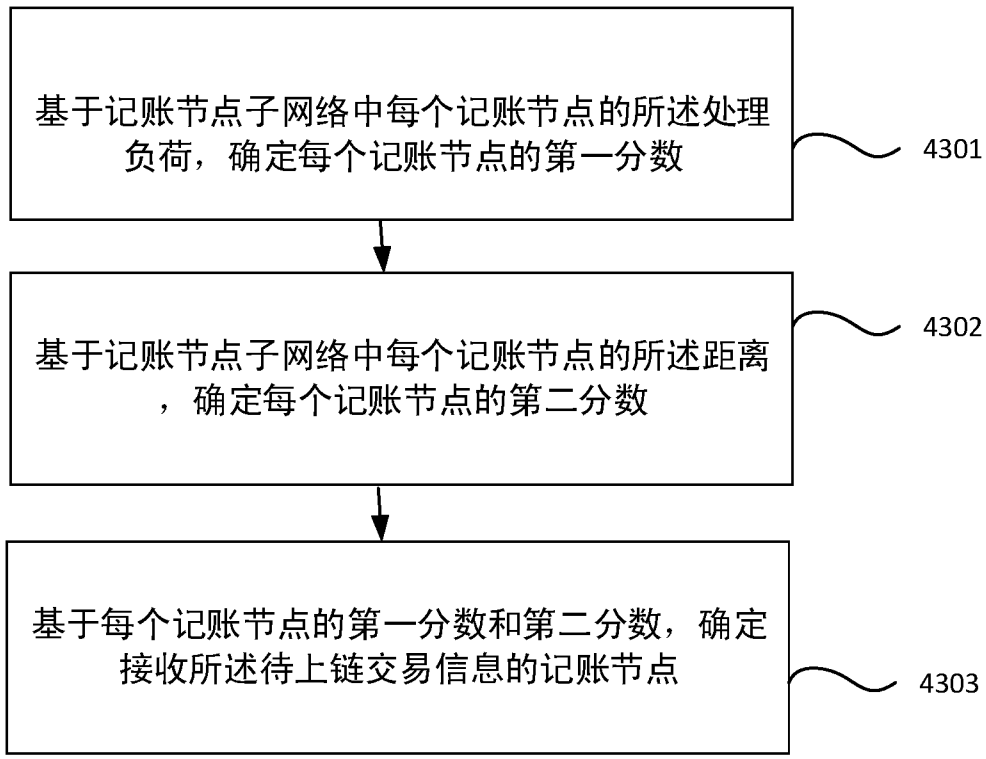

基于记账节点子网络中每个记账节点的所述处理负荷，确定每个记账节点的第一分数
4301
基于记账节点子网络中每个记账节点的所述距离，确定每个记账节点的第二分数
4302
基于每个记账节点的第一分数和第二分数，确定接收所述待上链交易信息的记账节点
4303

图 15

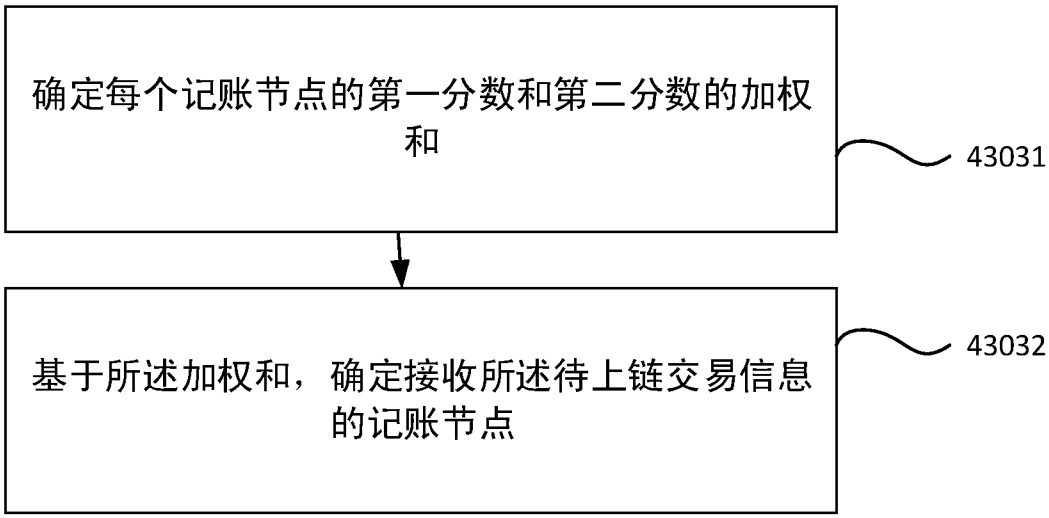

确定每个记账节点的第一分数和第二分数的加权和
43031
基于所述加权和，确定接收所述待上链交易信息的记账节点
43032

图 16

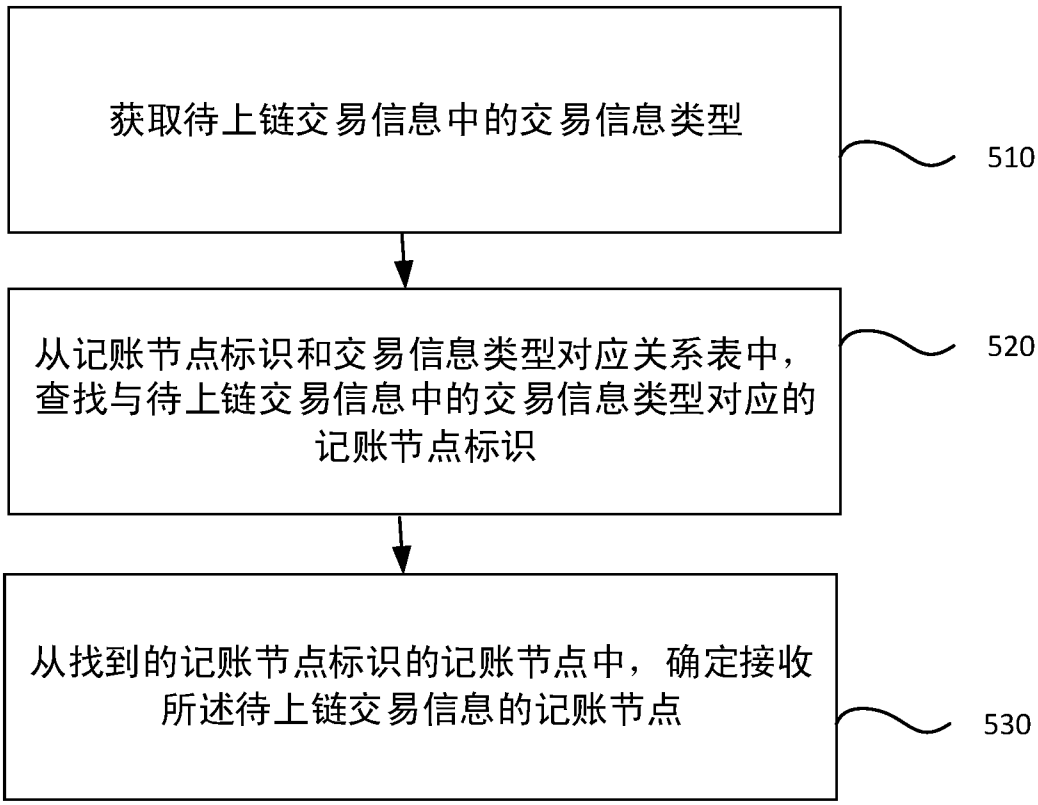

获取待上链交易信息中的交易信息类型
510
从记账节点标识和交易信息类型对应关系表中，查找与待上链交易信息中的交易信息类型对应的记账节点标识
520
从找到的记账节点标识的记账节点中，确定接收所述待上链交易信息的记账节点
530

图 17

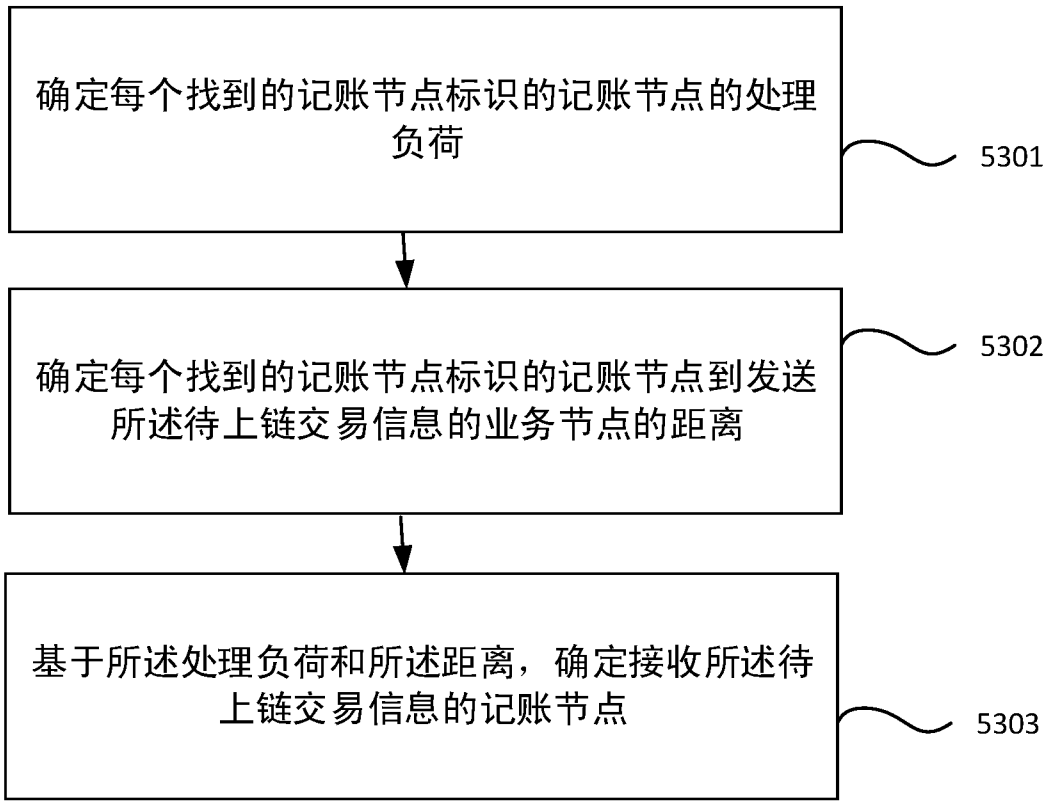

确定每个找到的记账节点标识的记账节点的处理负荷
5301
确定每个找到的记账节点标识的记账节点到发送所述待上链交易信息的业务节点的距离
5302
基于所述处理负荷和所述距离，确定接收所述待上链交易信息的记账节点
5303

图 18

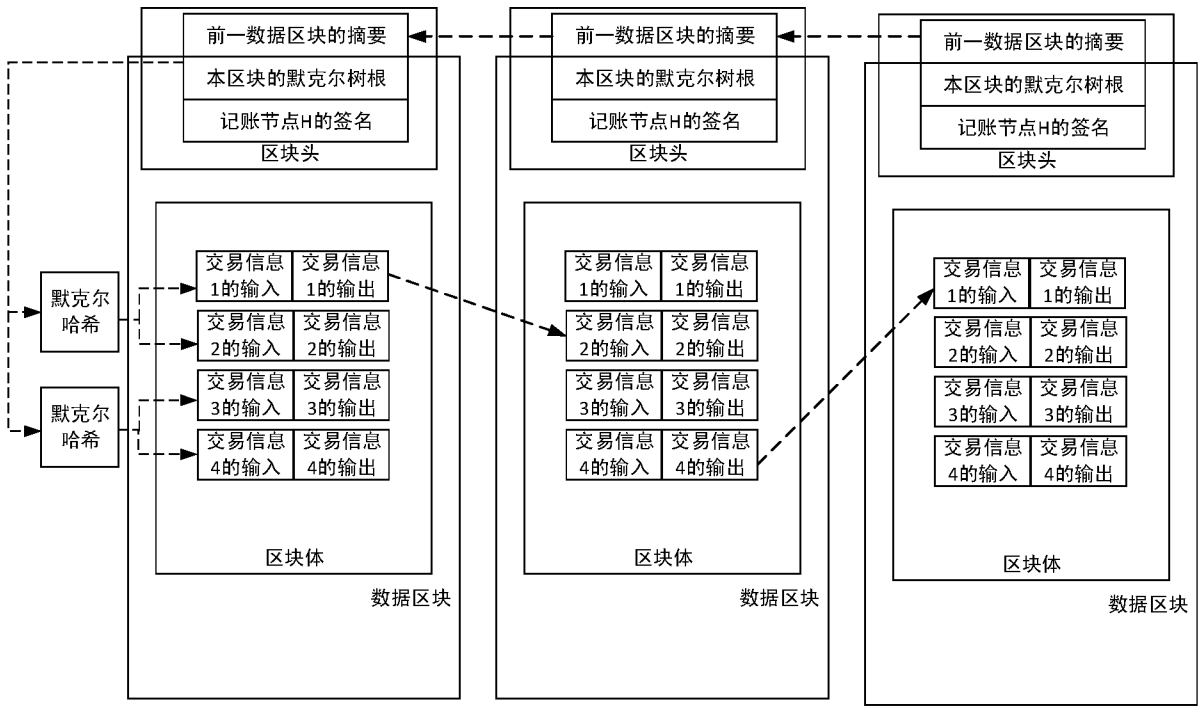

前一数据区块的摘要
本区块的默克尔树根
记账节点H的签名
区块头
默克尔哈希
默克尔哈希
交易信息1的输入
交易信息1的输出
交易信息2的输入
交易信息2的输出
交易信息3的输入
交易信息3的输出
交易信息4的输入
交易信息4的输出
区块体
数据区块

图 19

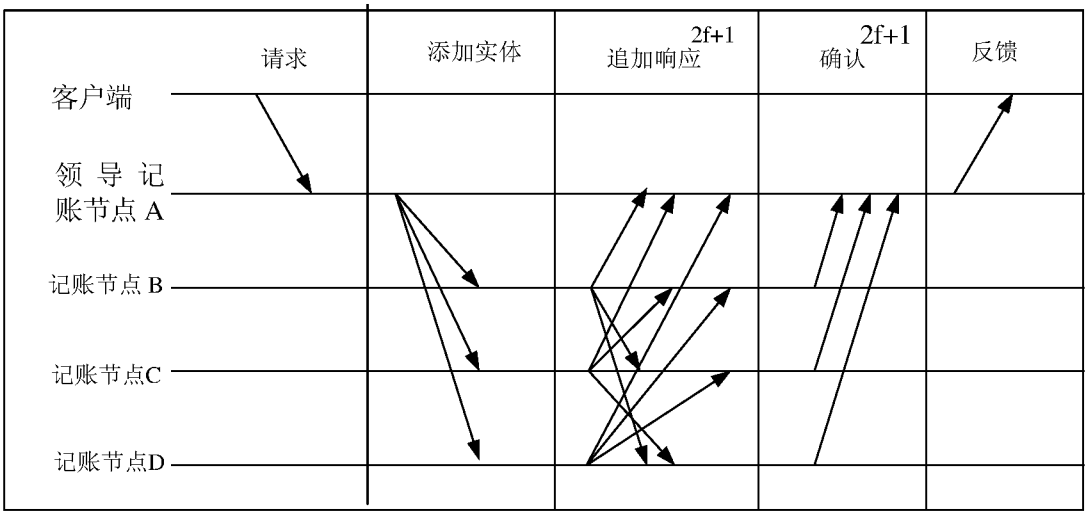

请求
添加实体
2f+1
追加响应
2f+1
确认
反馈
客户端
领导记账节点A
记账节点B
记账节点C
记账节点D

图 20

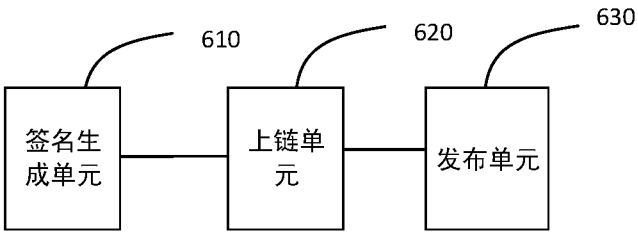

610
620
630
签名生成单元
上链单元
发布单元

图 21

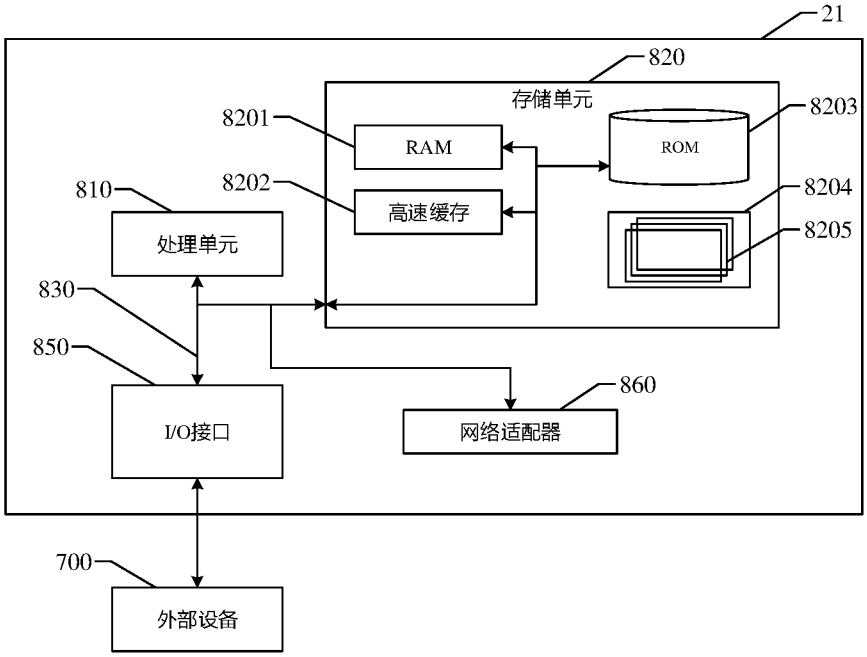

21
820
存储单元
8201
RAM
8203
ROM
8202
高速缓存
8204
8205
810
处理单元
830
850
860
I/O接口
网络适配器
700
外部设备

图 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/122394

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06Q G06F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: 记账节点, 业务节点, 共识节点, 子网, 区块链, 密钥, 签名, 验证, 检验, charge, service, common view, node, subnet, blockchain, key, sign, validate, check, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109447648 A (SHENZHEN ZHISHUILIAN TECH CO., LTD.) 08 March 2019 (2019-03-08) claims 1-15	1-15
X	CN 108717630 A (SHANGHAI DISTRIBUTION INFORMATION TECHNOLOGY CO., LTD.) 30 October 2018 (2018-10-30) description, paragraphs [0083]-[0092]	1-15
A	CN 107292735 A (TANGSHENG (BEIJING) IOT TECHNOLOGY CO., LTD.) 24 October 2017 (2017-10-24) entire document	1-15
A	CN 108234135 A (SINOCHAIN TECHNOLOGY CO., LTD.) 29 June 2018 (2018-06-29) entire document	1-15
A	US 2018068091 A1 (INTEL CORPORATION) 08 March 2018 (2018-03-08) entire document	1-15

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 February 2020	**24 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/122394

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109447648 A	08 March 2019	None	
CN 108717630 A	30 October 2018	None	
CN 107292735 A	24 October 2017	None	
CN 108234135 A	29 June 2018	None	
US 2018068091 A1	08 March 2018	None	

国际检索报告

国际申请号
PCT/CN2019/122394

A. 主题的分类

G06Q 20/38(2012.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06Q G06F H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI, EPODOC, CNPAT, CNKI：记账节点，业务节点，共识节点，子网，区块链，密钥，签名，验证，检验，charge, service, common view, node, subnet, blockchain, key, sign, validate, check, verify

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 109447648 A (深圳市智税链科技有限公司) 2019年 3月 8日 (2019-03-08) 权利要求1-15	1-15
X	CN 108717630 A (上海分布信息科技有限公司) 2018年 10月 30日 (2018-10-30) 说明书第[0083]-[0092]段	1-15
A	CN 107292735 A (唐盛北京物联技术有限公司) 2017年 10月 24日 (2017-10-24) 全文	1-15
A	CN 108234135 A (中链科技有限公司) 2018年 6月 29日 (2018-06-29) 全文	1-15
A	US 2018068091 A1 (INTEL CORPORATION) 2018年 3月 8日 (2018-03-08) 全文	1-15

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 2月 12日	2020年 2月 24日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	王欣
传真号 (86-10)62019451	电话号码 86-(10)-53961617

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/122394

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 109447648 A	2019年 3月 8日	无	
CN 108717630 A	2018年 10月 30日	无	
CN 107292735 A	2017年 10月 24日	无	
CN 108234135 A	2018年 6月 29日	无	
US 2018068091 A1	2018年 3月 8日	无	