(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 112907369 A
(43)申请公布日 2021.06.04

(21)申请号 202110173395.5

(22)申请日 2021.02.08

(71)申请人 网易(杭州)网络有限公司
地址 310052 浙江省杭州市滨江区长河街道网商路599号4幢7层

(72)发明人 胡志鹏 赖奕宇 曹崇瑞

(74)专利代理机构 北京超凡宏宇专利代理事务所(特殊普通合伙) 11463
代理人 钟扬飞

(51)Int.Cl.
G06Q 40/04(2012.01)
G06F 21/60(2013.01)
G06F 21/64(2013.01)
G06F 16/23(2019.01)

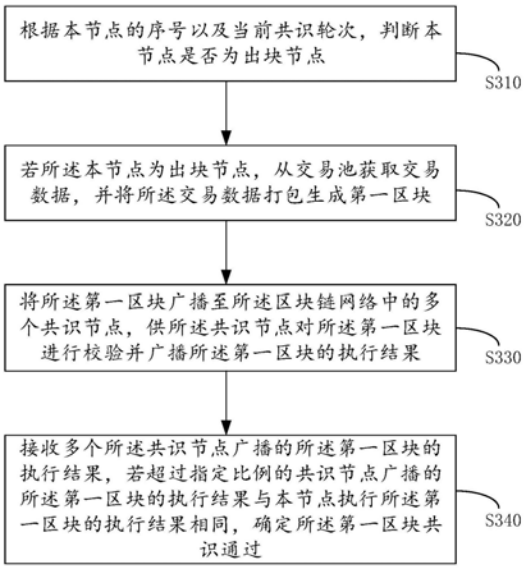
权利要求书2页 说明书10页 附图4页

(54)发明名称

基于区块链的数据共识方法及装置、电子设备、存储介质

(57)摘要

本申请提供一种基于区块链的数据共识方法及装置、电子设备、存储介质，该方法由区块链网络中的任一区块链节点执行，该方法包括：根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点；若本节点为出块节点，从交易池获取交易数据，并将交易数据打包生成第一区块；将第一区块广播至区块链网络中的多个共识节点，供共识节点对第一区块进行校验并广播第一区块的执行结果；接收多个共识节点广播的第一区块的执行结果，若超过指定比例的共识节点广播的第一区块的执行结果与本节点执行第一区块的执行结果相同，确定第一区块共识通过。上述方案可以提供共识效率，缩短共识时间。



CN 112907369 A

1.一种基于区块链的数据共识方法,其特征在于,所述方法由区块链网络中的任一区块链节点执行,包括:

根据本节点的序号以及当前共识轮次,判断本节点是否为出块节点;

若所述本节点为出块节点,从交易池获取交易数据,并将所述交易数据打包生成第一区块;

将所述第一区块广播至所述区块链网络中的多个共识节点,供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果;

接收多个所述共识节点广播的所述第一区块的执行结果,若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同,确定所述第一区块共识通过。

2.根据权利要求1所述的方法,其特征在于,所述根据本节点的序号以及当前共识轮次,判断本节点是否为出块节点,包括:

根据所述区块链网络的总节点数量,计算所述当前共识轮次除以所述总节点数量的余数;

判断本节点的序号是否等于所述余数,确定本节点是否为所述出块节点。

3.根据权利要求2所述的方法,其特征在于,所述判断本节点的序号是否等于所述余数,确定本节点是否为所述出块节点,包括:

若本节点的序号等于所述余数,确定本节点为所述出块节点。

4.根据权利要求1所述的方法,其特征在于,所述从交易池获取交易数据,并将所述交易数据打包生成第一区块,包括:

从交易池获取交易数据;

计算所述交易数据的哈希值,以及并利用自身私钥对所述哈希值进行加密,生成签名信息;

将所述交易数据、所述交易数据的哈希值、签名信息以及所述当前共识轮次打包生成所述第一区块。

5.根据权利要求1所述的方法,其特征在于,所述方法还包括:

若本节点不是出块节点,当接收到出块节点广播的第二区块时,对所述第二区块进行校验,并广播所述第二区块的执行结果;

接收所述区块链网络中除本节点以外,其余区块链节点对所述第二区块的执行结果;

若超过指定比例的区块链节点广播的所述第二区块的执行结果与本节点执行所述第二区块的执行结果相同,确定所述第二区块共识通过。

6.根据权利要求5所述的方法,其特征在于,所述对所述第二区块进行校验,并广播所述第二区块的执行结果,包括

对所述第二区块包含的签名信息进行验签,得到出块节点的公钥;

根据所述出块节点的公钥,校验当前共识轮次是否由所述出块节点出块;

在校验通过后,执行所述第二区块包含的交易数据,并广播所述第二区块的执行结果。

7.根据权利要求6所述的方法,其特征在于,所述根据所述出块节点的公钥,校验当前共识轮次是否由所述出块节点出块,包括:

根据当前共识轮次和总节点数量,计算目标出块的节点序号;

从公钥集合列表中获取所述节点序号对应的节点公钥；

判断所述节点公钥是否与所述出块节点的公钥一致，若一致，确定当前共识轮次由所述出块节点出块，校验通过。

8.根据权利要求6所述的方法，其特征在于，所述执行所述第二区块包含的交易数据，并广播所述第二区块的执行结果，包括：

执行所述第二区块包含的交易数据，并将执行所述交易数据产生的状态变更数据写入缓存区；

对所述缓存区的状态变更数据计算哈希值，得到结果哈希值；

利用自身私钥对所述结果哈希值进行加密，得到节点签名信息；

广播所述第二区块对应的包含所述结果哈希值和节点签名信息的执行结果。

9.根据权利要求6所述的方法，其特征在于，还包括：

在校验通过后，将所述第二区块存储至数据库中；

若所述第二区块共识通过，将执行所述第二区块中的交易数据产生的状态变更数据存储到所述数据库中。

10.根据权利要求1所述的方法，其特征在于，所述执行结果包括第一区块对应的结果哈希值和所述共识节点对所述结果哈希值的节点签名信息；若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过，包括：

从所述节点签名信息中验签得到所述共识节点的公钥；

校验每个共识节点的公钥，若所述共识节点广播的所述结果哈希值与本节点执行所述第一区块得到的结果哈希值相同，共识计数器加一，得到共识通过总数；

若所述共识通过总数大于三分之二的总节点数量，确定所述第一区块共识通过。

11.一种基于区块链的数据共识装置，其特征在于，所述装置包括：

节点判断模块，根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点；

交易打包模块，用于在本节点为出块节点时，从交易池获取交易数据，并将所述交易数据打包生成第一区块；

区块广播模块，用于将所述第一区块广播至区块链网络中的多个共识节点，供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果；

区块判断模块，用于接收多个所述共识节点广播的所述第一区块的执行结果，若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过。

12.一种电子设备，其特征在于，所述电子设备包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器被配置为执行权利要求1-10任意一项所述的基于区块链的数据共识方法。

13.一种计算机可读存储介质，其特征在于，所述存储介质存储有计算机程序，所述计算机程序可由处理器执行以完成权利要求1-10任意一项所述的基于区块链的数据共识方法。

基于区块链的数据共识方法及装置、电子设备、存储介质

技术领域

[0001] 本申请涉及区块链技术领域，特别涉及一种基于区块链的的数据共识方法及装置、电子设备、计算机可读存储介质。

背景技术

[0002] 拜占庭容错技术是一类分布式计算领域的容错技术。拜占庭假设是对现实世界的模型化，由于硬件错误、网络拥塞或中断以及遭到恶意攻击等原因，计算机和网络可能出现不可预料的行为。拜占庭容错技术被设计用来处理这些异常行为，并满足所要解决的问题的规范要求。

[0003] 目前，pbft(实用拜占庭容错算法)被作为联盟链的共识算法。PBFT算法可以保证如果有3f+1的节点的话，即使其中有f个错误或者没有响应，依然可以得出共识的正确结果。PBFT算法的基本流程主要有以下四步：

[0004] 1)客户端发送请求给主节点;2)主节点广播请求给其它节点，节点执行PBFT算法的三阶段共识流程(三个阶段分别是pre-prepare阶段(预准备阶段)，prepare阶段(准备阶段)，commit阶段(提交阶段))。3)节点处理完三阶段流程后，返回消息给客户端。4)客户端收到来自2f+1个节点的相同消息后，代表共识已经正确完成。

[0005] 在pbft中，是一个三阶段的共识流程，即一个区块从提案到确认过程中，需要历经三个阶段，每个阶段需要至少有2f+1个节点达成共识，一个区块的确认需要共识三次，共识效率较低，速度慢。

发明内容

[0006] 本申请实施例提供了一种基于区块链的数据共识方法，用以提高共识效率，缩短共识时间。

[0007] 本申请实施例提供了一种基于区块链的数据共识方法，所述方法由区块链网络中的任一区块链节点执行，包括：

[0008] 根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点；

[0009] 若所述本节点为出块节点，从交易池获取交易数据，并将所述交易数据打包生成第一区块；

[0010] 将所述第一区块广播至所述区块链网络中的多个共识节点，供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果；

[0011] 接收多个所述共识节点广播的所述第一区块的执行结果，若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过。

[0012] 在一实施例中，所述根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点，包括：

[0013] 根据所述区块链网络的总节点数量，计算所述当前共识轮次除以所述总节点数量

的余数；

[0014] 判断本节点的序号是否等于所述余数，确定本节点是否为所述出块节点。

[0015] 在一实施例中，所述判断本节点的序号是否等于所述余数，确定本节点是否为所述出块节点，包括：

[0016] 若本节点的序号等于所述余数，确定本节点为所述出块节点。

[0017] 在一实施例中，所述从交易池获取交易数据，并将所述交易数据打包生成第一区块，包括：

[0018] 从交易池获取交易数据；

[0019] 计算所述交易数据的哈希值，以及并利用自身私钥对所述哈希值进行加密，生成签名信息；

[0020] 将所述交易数据、所述交易数据的哈希值、签名信息以及所述当前共识轮次打包生成所述第一区块。

[0021] 在一实施例中，所述方法还包括：

[0022] 若本节点不是出块节点，当接收到出块节点广播的第二区块时，对所述第二区块进行校验，并广播所述第二区块的执行结果；

[0023] 接收所述区块链网络中除本节点以外，其余区块链节点对所述第二区块的执行结果；

[0024] 若超过指定比例的区块链节点广播的所述第二区块的执行结果与本节点执行所述第二区块的执行结果相同，确定所述第二区块共识通过。

[0025] 在一实施例中，所述对所述第二区块进行校验，并广播所述第二区块的执行结果，包括

[0026] 对所述第二区块包含的签名信息进行验签，得到出块节点的公钥；

[0027] 根据所述出块节点的公钥，校验当前共识轮次是否由所述出块节点出块；

[0028] 在校验通过后，执行所述第二区块包含的交易数据，并广播所述第二区块的执行结果。

[0029] 在一实施例中，所述根据所述出块节点的公钥，校验当前共识轮次是否由所述出块节点出块，包括：

[0030] 根据当前共识轮次和总节点数量，计算目标出块的节点序号；

[0031] 从公钥集合列表中获取所述节点序号对应的节点公钥；

[0032] 判断所述节点公钥是否与所述出块节点的公钥一致，若一致，确定当前共识轮次由所述出块节点出块，校验通过。

[0033] 在一实施例中，所述执行所述第二区块包含的交易数据，并广播所述第二区块的执行结果，包括：

[0034] 执行所述第二区块包含的交易数据，并将执行所述交易数据产生的状态变更数据写入缓存区；

[0035] 对所述缓存区的状态变更数据计算哈希值，得到结果哈希值；

[0036] 利用自身私钥对所述结果哈希值进行加密，得到节点签名信息；

[0037] 广播所述第二区块对应的包含所述结果哈希值和节点签名信息的执行结果。

[0038] 在一实施例中，所述方法还包括：

[0039] 在校验通过后，将所述第二区块存储至数据库中；

[0040] 若所述第二区块共识通过，将执行所述第二区块中的交易数据产生的状态变更数据存储到所述数据库中。

[0041] 在一实施例中，所述执行结果包括第一区块对应的结果哈希值和所述共识节点对所述结果哈希值的节点签名信息；若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过，包括：

[0042] 从所述节点签名信息中验签得到共识节点的公钥；

[0043] 校验每个共识节点的公钥，若所述共识节点广播的所述结果哈希值与本节点执行所述第一区块得到的结果哈希值相同，共识计数器加一，得到共识通过总数；

[0044] 若所述共识通过总数大于三分之二的总节点数量，确定所述第一区块共识通过。

[0045] 本申请实施例还提供了一种基于区块链的数据共识装置，所述装置包括：

[0046] 节点判断模块，根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点；

[0047] 交易打包模块，用于在本节点为出块节点时，从交易池获取交易数据，并将所述交易数据打包生成第一区块；

[0048] 区块广播模块，用于将所述第一区块广播至区块链网络中的多个共识节点，供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果；

[0049] 区块判断模块，用于接收多个所述共识节点广播的所述第一区块的执行结果，若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过。

[0050] 本申请实施例还提供了一种电子设备，所述电子设备包括：

[0051] 处理器；

[0052] 用于存储处理器可执行指令的存储器；

[0053] 其中，所述处理器被配置为执行所述基于区块链的数据共识方法。

[0054] 本申请实施例还提供了一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序可由处理器执行以完成所述基于区块链的数据共识方法。

[0055] 本申请上述实施例提供的技术方案，根据节点序号以及当前共识轮次确定出块节点，通过出块节点打包生成的区块仅广播一次，之后接收共识节点广播的第一区块的执行结果，若超过指定比例的共识节点广播的第一区块的执行结果与本节点执行第一区块的执行结果相同，确定第一区块共识通过。从而一个区块只需发起一次共识，提高了区块的共识效率，节约了共识时间。

附图说明

[0056] 为了更清楚地说明本申请实施例的技术方案，下面将对本申请实施例中所需要使用的附图作简单地介绍。

[0057] 图1是本申请实施例提供的区块链系统的架构示意图；

[0058] 图2是本申请实施例提供的电子设备的结构示意图；

[0059] 图3是本申请实施例提供的基于区块链的数据共识方法的流程示意图；

[0060] 图4是本申请实施例提供的共识节点对第一区块进行校验并广播第一区块的执行

结果的流程示意图；

[0061] 图5是本申请实施例提供的本节点不是出块节点，接收到广播的第二区块之后的执行流程示意图；

[0062] 图6是“三阶段”共识的流程示意图；

[0063] 图7是本申请实施例提供的基于区块链的数据共识装置的框图。

具体实施方式

[0064] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行描述。

[0065] 相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步定义和解释。同时，在本申请的描述中，术语“第一”、“第二”等仅用于区分描述，而不能理解为指示或暗示相对重要性。

[0066] 图1为本申请实施例提供的区块链系统的架构示意图。如图1所示，该区块链系统包括：多个区块链节点100。区块链节点100可以是计算机、服务器或矿机。多个区块链节点100之间通过无线网络连接。

[0067] 其中，多个区块链节点100中有一个区块链节点100可以作为出块节点102，用于打包交易生成区块。为进行区分，除了出块节点102的其余区块链节点100可以称为共识节点103。

[0068] 每个区块链节点100可以根据本节点的序号(selfindex)以及当前共识轮次(round)，判断本节点是否为出块节点102。在一实施例中，区块链节点100可以根据所述区块链网络的总节点数量，计算当前共识轮次除以所述总节点数量(total_num)的余数(round％total_num)；判断本节点的序号是否等于余数(selfindex＝＝round％total_num)，如果等于余数，确定本节点为出块节点102。

[0069] 在一实施例中，如果本节点不是出块节点102，则等待接收出块节点102发送的第二区块。为进行区分，本节点打包的称为第一区块，本节点接收的称为第二区块。如果本节点为出块节点102，则出块节点102需要从交易池获取交易数据，并将所述交易数据打包生成第一区块。出块节点102可以将第一区块广播至区块链网络的多个共识节点103。共识节点103是指除出块节点102以外的其余区块链节点100。第一区块可以包括交易数据、交易数据的哈希值、签名信息以及当前共识轮次。其中，签名信息可以通过出块节点102的私钥对交易数据的哈希值进行加密得到。

[0070] 共识节点103接收到第一区块后，可以对第一区块进行校验，并在校验通过后执行第一区块中的交易数据，广播所述交易数据的执行结果。

[0071] 第一区块包括出块节点102的签名信息，故对第一区块进行校验可以通过对签名信息进行验签得到出块节点102的公钥。共识节点103根据当前共识轮次和总节点数量可以确定目标出块的节点序号。目标出块的节点序号可以认为是共识节点103计算得到的可以打包区块的正确的节点的序号。具体的，可以计算当前共识轮次除以总节点数量的余数，作为目标出块的节点序号。

[0072] 公钥集合列表中存储每个节点的公钥，共识节点103可以从公钥集合列表中获取目标出块的节点序号对应的公钥。判断与验签得到的公钥是否一致，从而校验出块节点102是否正确。如果目标出块的节点序号对应的公钥与验签得到的公钥一致，即当前共识轮次

确实由验签得到的公钥对应的节点出块，则认为出块节点102正确，第一区块校验通过。相反的，如果目标出块的节点序号对应的公钥与验签得到的公钥一致，认为校验不通过，结束处理流程，等待下一个区块的到来。

[0073] 第一区块校验通过后，共识节点103可以将“current_vote(为一个固定值)”为key(键)，第一区块本身为value(值)，通过db组件(数据库组件)，持久化到kv数据库中。

[0074] 第一区块校验通过后，共识节点103可以执行第一区块中的交易数据(列表形式)，并将在执行第一区块的交易数据过程中的全部状态变更数据写入到一个缓存区(HashMap<String,String>commitCache)中，然后对缓存区中数据计算出结果哈希值(commit_hash)。具体可以通过现有组件计算出默克尔根节点的hash值。共识节点103可以将结果哈希值通过自身私钥加密得到节点签名信息，将包含结果哈希值和节点签名信息的执行结果向全网广播。

[0075] 同理，出块节点102也可以进行第一区块的持久化存储，并执行第一区块中的交易数据，全网广播交易数据的执行结果，出块节点102广播的执行结果可以包括出块节点102执行交易过程中的状态变更数据的结果哈希值以及利用出块节点102的私钥对该结果哈希值加密得到节点签名信息。

[0076] 针对每个区块链节点100而言，如果一个区块链节点100(N0)接收到来自其余区块链节点100(N1、N2、N3…)广播的执行结果，可以从执行结果包含的节点签名信息中验签得到广播执行结果的区块链节点100的公钥，从而确定执行结果是从哪个区块链节点100发送的。区块链节点100(N0)可以判断区块链节点100(N1)广播的结果哈希值是否本区块链节点100(N0)执行第一区块得到的结果哈希值相同，如果相同，则共识计数器加一，同理，继续判断区块链节点100(N2)广播的结果哈希值是否本区块链节点100(N0)执行第一区块得到的结果哈希值相同，如果相同，则共识计数器再加一，以此类推，得到共识通过总数(commit_num)；也就是达成共识的节点数量。若共识通过总数(commit_num)大于三分之二的总节点数量(total_num)，确定所述第一区块共识通过。从而可以保证三分之二以上节点正常运行时，数据不会被篡改。

[0077] 在共识通过后，可以将缓存区的所有内容持久化存储到kv数据库中，然后当前共识轮次round递增一次。

[0078] 图2是本申请实施例提供的电子设备200的结构示意图。该电子设备可以作为上述区块链节点100，该电子设备200可以包括一个或多个处理器201、一个或多个存储处理器可执行指令的存储器202。其中，所述处理器201被配置为执行本申请下述实施例提供的基于区块链的数据共识方法。

[0079] 所述处理器201可以是网关，也可以为智能终端，或者是包含中央处理单元(CPU)、图像处理单元(GPU)或者具有数据处理能力和/或指令执行能力的其它形式的处理单元的设备，可以对所述电子设备200中的其它组件的数据进行处理，还可以控制所述电子设备200中的其它组件以执行期望的功能。

[0080] 所述存储器202可以包括一个或多个计算机程序产品，所述计算机程序产品可以包括各种形式的计算机可读存储介质，例如易失性存储器和/或非易失性存储器。所述易失性存储器例如可以包括随机存取存储器(RAM)和/或高速缓冲存储器(cache)等。所述非易失性存储器例如可以包括只读存储器(ROM)、硬盘、闪存等。在所述计算机可读存储介质上

可以存储一个或多个计算机程序指令，处理器201可以运行所述程序指令，以实现下文所述的基于区块链的数据共识方法。在所述计算机可读存储介质中还可以存储各种应用程序和各种数据，例如所述应用程序使用和/或产生的各种数据等。

[0081] 图3是本申请实施例提供的基于区块链的数据共识方法的流程示意图。如图3所示，该方法可以由区块链网络中的任一区块链节点100执行，该方法包括以下步骤S310-步骤S340。

[0082] 步骤S310：根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点。

[0083] 其中，本节点可以认为是其中一个区块链节点。每个区块链节点可以有各自的序号，例如N0、N1、N2、N3……第一次发起共识叫第一轮，当前共识轮次是指当前时刻是第几轮共识。其中，用于对交易数据进行打包的区块链节点可以称为出块节点，除出块节点以外的区块链节点可以称为共识节点。

[0084] 在一实施例中，判断本节点是否出块节点，可以根据区块链网络的总节点数量total_num，计算所述当前共识轮次round除以所述总节点数量total_num的余数(round％total_num)；判断本节点的序号selfIndex是否等于余数，确定本节点是否为出块节点。在一实施例中，本节点的序号selfIndex等于所述余数(round％total_num)，确定本节点为出块节点，相反则不是出块节点。

[0085] 步骤S320：若所述本节点为出块节点，从交易池获取交易数据，并将所述交易数据打包生成第一区块。

[0086] 为进行区分，本节点作为出块节点时生成的区块，可以称为第一区块。本节点不作为出块节点时，接收到的区块可以称为第二区块。

[0087] 具体的，本节点作为出块节点时，可以从交易池获取交易数据；通过哈希算法计算所述交易数据的哈希值，以及并利用自身私钥对所述哈希值进行加密，生成签名信息。将所述交易数据、所述交易数据的哈希值、签名信息以及所述当前共识轮次打包生成所述第一区块。

[0088] 步骤S330：将所述第一区块广播至所述区块链网络中的多个共识节点，供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果。

[0089] 其中，共识节点是指区块链网络中除出块节点以外的区块链节点。如图4所示，共识节点对第一区块进行校验并广播所述第一区块的执行结果，具体可以包括：步骤S410-步骤S430。

[0090] 步骤S410对第一区块包含的签名信息进行验签，得到出块节点的公钥。

[0091] 步骤S420根据出块节点的公钥，校验当前共识轮次是否由所述出块节点出块；

[0092] 其中，步骤S420具体包括：共识节点根据当前共识轮次round和总节点数量total_num，计算目标出块的节点序号(节点序号＝round％total_num)，即正确的出块节点的序号。之后从公钥集合列表(List<publickey>order_pks)中获取节点序号对应的节点公钥。判断所述节点公钥是否与出块节点的公钥一致，若一致，确定当前共识轮次由出块节点出块，校验通过。在校验通过后，通过现有的db数据库组件，将第一区块存储至kv数据库中。

[0093] 步骤S430在校验通过后，执行第一区块包含的交易数据，并广播所述第二区块的执行结果。

[0094] 其中，步骤S430具体包括：在校验通过后，共识节点执行所述第一区块包含的交易

数据，并将执行所述交易数据产生的状态变更数据写入缓存区(HashMap<String,String> commitCache)；通过哈希算法对缓存区的状态变更数据计算哈希值，得到结果哈希值；利用自身私钥对所述结果哈希值进行加密，得到节点签名信息；广播所述第一区块对应的包含所述结果哈希值和节点签名信息的执行结果。

[0095] 步骤S340：接收多个所述共识节点广播的所述第一区块的执行结果，若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过。

[0096] 每个共识节点均可执行上述步骤S410-步骤S430，在校验通过后，广播第一区块的执行结果。本节点(为出块节点时)接收多个共识节点广播的第一区块的执行结果，从执行结果中获得节点签名信息以及结果哈希值。

[0097] 在一实施例中，本节点(为出块节点时)可以从节点签名信息中验签得到共识节点的公钥。之后校验每个共识节点的公钥，具体可以判断该公钥是否区块链网络的在公钥集合列表中，从而避免其他不在区块链网络中的节点参与。如果共识节点的公钥在公钥集合列表中，可以继续判断每个共识节点广播的所述结果哈希值与本节点执行所述第一区块得到的结果哈希值是否相同，如果相同，共识计数器加一。直到完成所有共识节点的结果哈希值的比对，得到共识通过总数。共识通过总数用于指示达成共识的所有节点个数。若共识通过总数大于三分之二的总节点数量，确定第一区块共识通过。如果第一区块共识通过，本节点可以将第一区块以及执行第一区块中的交易数据产生的状态变更数据持久化存储到数据库中。并将当前共识轮次加一，作为下一次共识的当前共识轮次。

[0098] 相反的，如果共识通过总数小于等于三分之二的总节点数量，则第一区块共识不通过，可以认为第一区块被篡改。从而实现数据的防篡改，达成数据的强一致性。

[0099] 本申请上述实施例提供的技术方案，根据节点序号以及当前共识轮次确定出块节点，打包生成的区块仅广播一次，之后接收共识节点广播的第一区块的执行结果，若超过指定比例的共识节点广播的第一区块的执行结果与本节点执行第一区块的执行结果相同，确定第一区块共识通过。从而一个区块只需发起一次共识，提高了区块的共识效率，节约了共识时间。

[0100] 另一方面，步骤S310判断本节点是否为出块节点之后，如果得到本节点不是出块节点(即本节点属于共识节点之一)，如图5所示，可以执行以下步骤S510-步骤S530。

[0101] 步骤S510：当本节点接收到出块节点广播的第二区块时，需要对所述第二区块进行校验，并广播第二区块的执行结果。

[0102] 其中，步骤S510具体包括：对所述第二区块包含的签名信息进行验签，得到出块节点的公钥。根据所述出块节点的公钥，校验当前共识轮次是否由所述出块节点出块。

[0103] 具体的，本节点可以根据当前共识轮次round和总节点数量total_num，计算目标出块的节点序号(节点序号＝round％total_num)，即正确的出块节点的序号。之后从公钥集合列表(List<publickey>order_pks)中获取节点序号对应的节点公钥。判断所述节点公钥是否与出块节点的公钥一致，若一致，确定当前共识轮次由出块节点出块，校验通过。在校验通过后，通过现有的db数据库组件，将第二区块存储至kv数据库中。

[0104] 在校验通过后，本节点执行所述第二区块包含的交易数据，并广播所述第二区块的执行结果。具体的，本节点可以执行第二区块包含的交易数据，并将执行交易数据产生的

状态变更数据写入缓存区(HashMap<String,String>commitCache);通过哈希算法对缓存区的状态变更数据计算哈希值,得到结果哈希值;利用自身私钥对所述结果哈希值进行加密,得到节点签名信息;广播第二区块对应的包含所述结果哈希值和节点签名信息的执行结果。

[0105] 步骤S520:本节点还可以接收区块链网络中除本节点以外,其余区块链节点对第二区块的执行结果。

[0106] 其中,执行结果包括每个区块链节点执行第二区块中的交易数据过程中的状态变更数据的哈希值(即结果哈希值)以及每个区块链节点的私钥对结果哈希值进行加密得到的节点签名信息。故从节点签名信息验签可以得到公钥,从而确定结果哈希值对应的节点身份。

[0107] 步骤S530:若超过指定比例的区块链节点广播的所述第二区块的执行结果与本节点执行所述第二区块的执行结果相同,确定所述第二区块共识通过,可以进行第二区块的上链存储。

[0108] 在一实施例中,本节点(为共识节点之一时)可以从节点签名信息中验签得到区块链节点的公钥。校验该区块链节点的公钥,具体可以判断该公钥是否区块链网络的在公钥集合列表中,从而避免其他不在区块链网络中的节点参与。如果该公钥在公钥集合列表中,可以继续判断该公钥对应节点广播的结果哈希值与本节点执行所述第二区块得到的结果哈希值是否相同,如果相同,共识计数器加一。直到完成所有区块链节点的结果哈希值的比对,得到共识通过总数。共识通过总数用于指示达成共识的所有节点个数。若共识通过总数大于三分之二的总节点数量,确定第二区块共识通过。如果第二区块共识通过,本节点可以将执行第二区块中的交易数据产生的状态变更数据持久化存储到数据库中。并将当前共识轮次加一,作为下一次共识的当前共识轮次。

[0109] 相反的,如果共识通过总数小于等于三分之二的总节点数量,则第二区块共识不通过,可以认为第二区块被篡改。从而实现数据的防篡改,达成数据的强一致性。

[0110] 为充分体现本申请实施例提供的技术方案的效果,下述为本申请提供的一种“三阶段”共识的流程,与本申请“一阶段”共识流程形成对比。图6中,一共有三个节点,分别为n1、n2、n3。而H为handle(处理)的缩写,B为broadcast(广播)的缩写,P为proposal(提议)的缩写,S为sign(签名)的缩写,C为commit(确认)的缩写;H-P为handle_proposal(处理提议区块),H-S为handle_sign(处理签名区块),H-C为handle_commit(处理确认区块);B-P为broadcast_proposal(广播提议区块),B-S为broadcast_sign(广播签名区块),B-C为broadcast_commit(广播确认区块);

[0111] 如图6所示,该“三阶段”共识的流程包括:

[0112] (1)先通过(block_number区块数量+view_nunber视图数量)%node_number(节点数量)来确定出块节点(leader),然后通过leader节点发起并广播第一阶段(proposal提议阶段)的proposal请求;

[0113] (2)全网节点收到proposal请求后,执行handle_proposal(H-P)提议处理,即对消息进行验签,以及系列校验,校验通过后,通过p2p网络全网广播第二阶段(sign签名阶段)的sign请求(B-S);

[0114] (3)当全网节点收到来自p2p网络中的sign请求后,执行handle_sign(H-S)签名处

理，继续对sign请求进行验签处理，以及一系列校验，并进行sign票数归档，如果sign通过票数超过全网节点的2/3后，继续通过p2p网络发起并广播第三阶段的Commit请求(B-C)；

[0115] (4)当全网节点收到来自p2p网络中的commit(确认)请求后，执行handle_commit(H-C)确认处理，继续执行commit请求处理流程，该流程也还是主要对commit请求进行验签处理，以及一系列校验，在进行commit票数归档，如果commit通过票数超过全网节点的2/3后，则可以认为区块达成共识，然后落盘(do-commit)。

[0116] (5)当然，每一个节点在在处理每一阶段的消息后，会立刻判断当前共识是否超时，如果超时，则发起view change(视图切换)，并且，当网络中有2/3以上的节点都对该view change达成一致时，则会重新发起发起共识流程，即重新执行上述步骤(1)-(4)。

[0117] 上述为BPFT算法的工程实现流程，整个流程需要三阶段来保证消息的防篡改以及强一致性。另外这里需要注意的是，三阶段共识的内容为block(区块)，而block的核心则包含一组交易列表集合，proposal、sign以及commit只是block在不同阶段的状态表示，以进行区分。

[0118] 经过对比可知，三阶段共识需要广播三次，共识三次，而本申请实施例提供的技术方案只需广播一次，共识一次，从而提供了共识效率，降低了共识时间。

[0119] 下述为本申请装置实施例，可以用于执行本申请上述基于区块链的数据共识方法实施例。对于本申请装置实施例中未披露的细节，请参照本申请基于基于区块链的数据共识方法实施例。

[0120] 图7为本申请一实施例示出的基于区块链的数据共识装置的框图。如图7所示，该装置包括：节点判断模块710、交易打包模块720、区块广播模块730以及区块判断模块740。

[0121] 节点判断模块710，根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点。

[0122] 交易打包模块720，用于在本节点为出块节点时，从交易池获取交易数据，并将所述交易数据打包生成第一区块。

[0123] 区块广播模块730，用于将所述第一区块广播至区块链网络中的多个共识节点，供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果。

[0124] 区块判断模块740，用于接收多个所述共识节点广播的所述第一区块的执行结果，若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过。

[0125] 上述装置中各个模块的功能和作用的实现过程具体详见上述基于区块链的数据共识方法中对应步骤的实现过程，在此不再赘述。

[0126] 在本申请所提供的几个实施例中，所揭露的装置和方法，也可以通过其它的方式实现。以上所描述的装置实施例仅仅是示意性的，例如，附图中的流程图和框图显示了根据本申请的多个实施例的装置、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段或代码的一部分，模块、程序段或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。在有些作为替换的实现方式中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个连续的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图

中的方框的组合,可以用执行规定的功能或动作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0127] 另外,在本申请各个实施例中的各功能模块可以集成在一起形成一个独立的部分,也可以是各个模块单独存在,也可以两个或两个以上模块集成形成一个独立的部分。

[0128] 功能如果以软件功能模块的形式实现并作为独立的产品销售或使用时,可以存储在一个计算机可读取存储介质中。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来,该计算机软件产品存储在一个存储介质中,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例方法的全部或部分步骤。而前述的存储介质包括:U盘、移动硬盘、只读存储器(ROM,Read-Only Memory)、随机存取存储器(RAM,Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

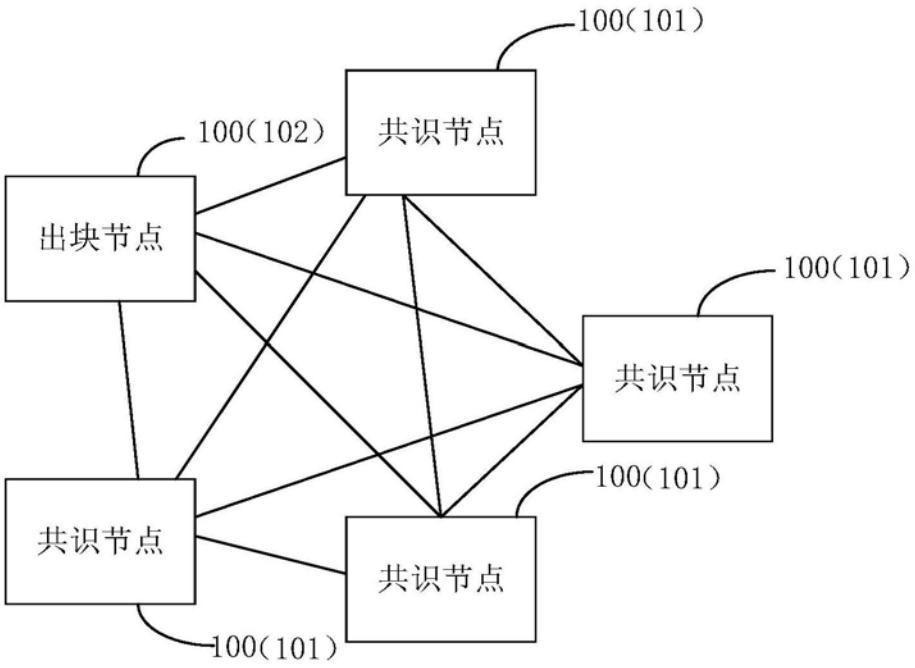

100(101)
共识节点
100(102)
出块节点
100(101)
共识节点
100(101)
共识节点
共识节点
100(101)

图1

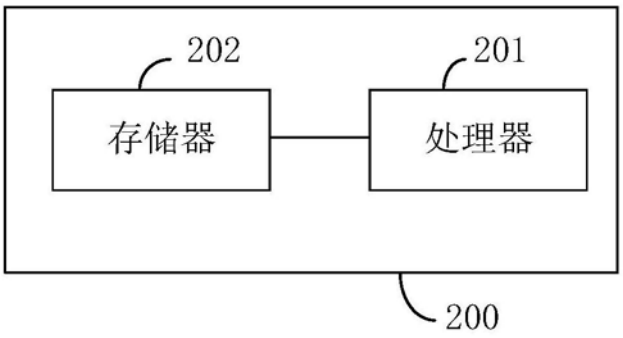

202
201
存储器
处理器
200

图2

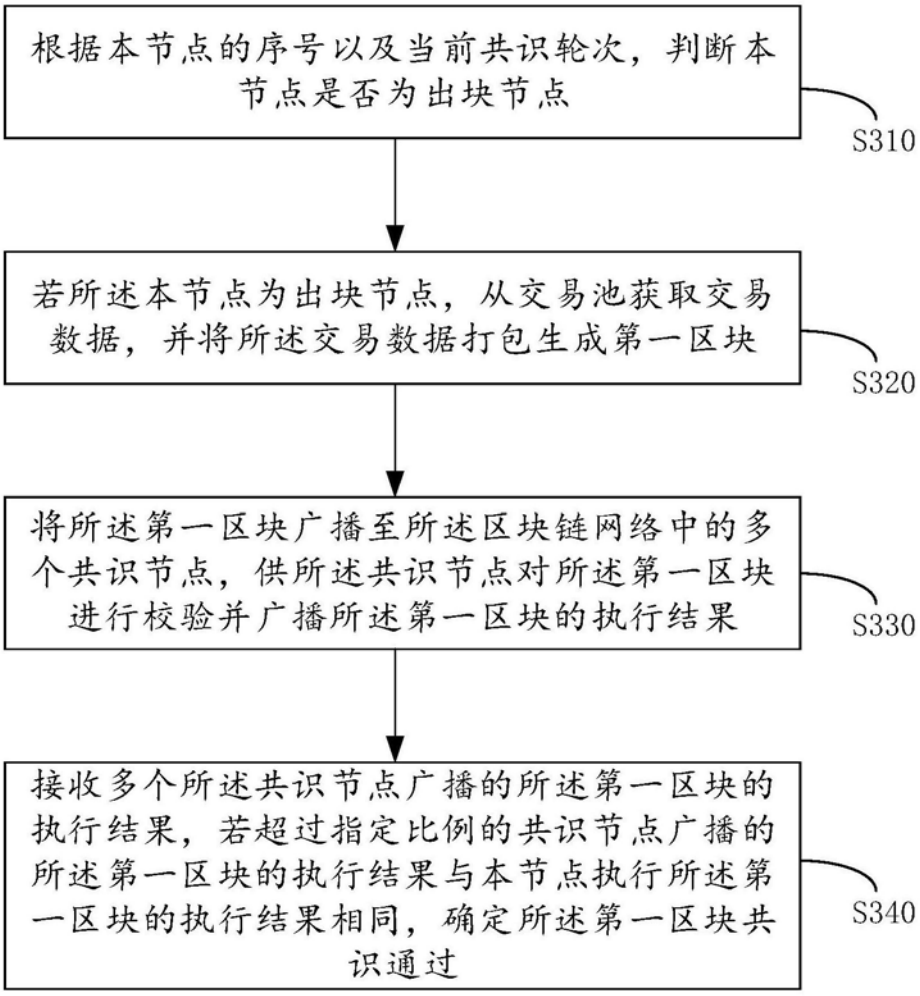

根据本节点的序号以及当前共识轮次，判断本节点是否为出块节点
S310
若所述本节点为出块节点，从交易池获取交易数据，并将所述交易数据打包生成第一区块
S320
将所述第一区块广播至所述区块链网络中的多个共识节点，供所述共识节点对所述第一区块进行校验并广播所述第一区块的执行结果
S330
接收多个所述共识节点广播的所述第一区块的执行结果，若超过指定比例的共识节点广播的所述第一区块的执行结果与本节点执行所述第一区块的执行结果相同，确定所述第一区块共识通过
S340

图3

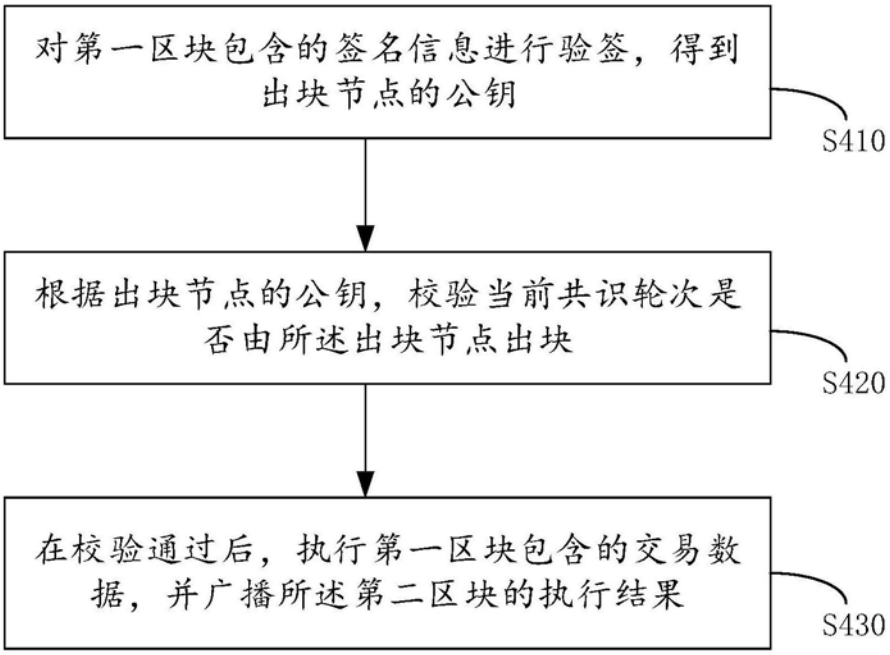

对第一区块包含的签名信息进行验签，得到出块节点的公钥
S410
根据出块节点的公钥，校验当前共识轮次是否由所述出块节点出块
S420
在校验通过后，执行第一区块包含的交易数据，并广播所述第二区块的执行结果
S430

图4

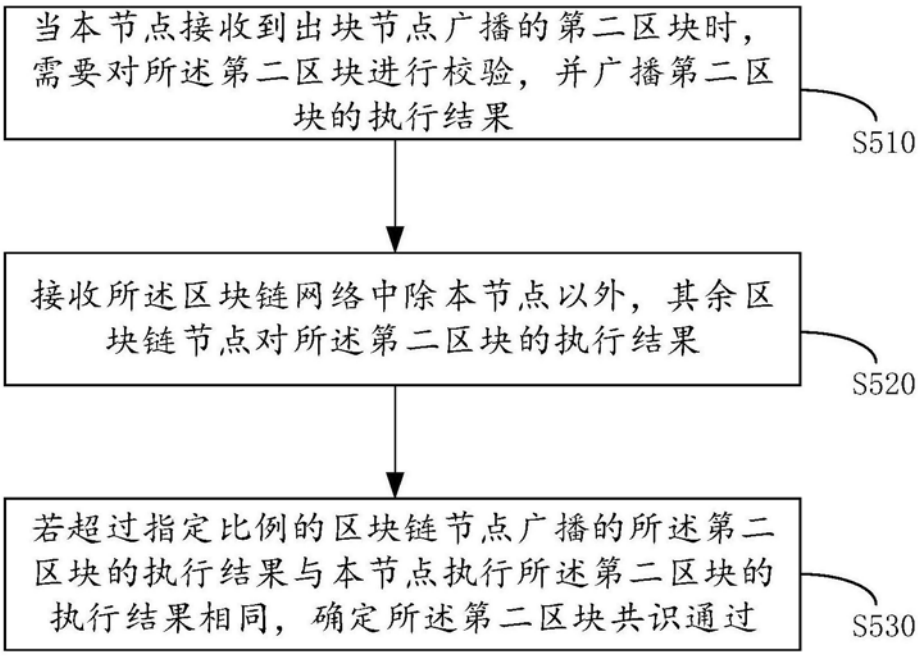

当本节点接收到出块节点广播的第二区块时，需要对所述第二区块进行校验，并广播第二区块的执行结果
S510
接收所述区块链网络中除本节点以外，其余区块链节点对所述第二区块的执行结果
S520
若超过指定比例的区块链节点广播的所述第二区块的执行结果与本节点执行所述第二区块的执行结果相同，确定所述第二区块共识通过
S530

图5

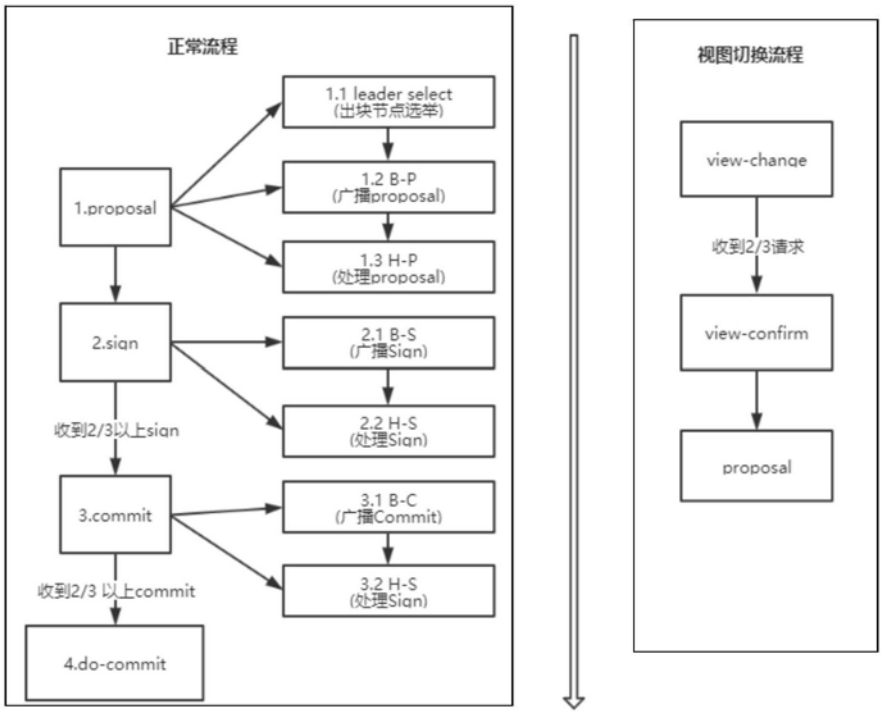

正常流程
1.1 leader select
(出块节点选举)
1.2 B-P
(广播proposal)
1.3 H-P
(处理proposal)
1.proposal
2.sign
2.1 B-S
(广播Sign)
2.2 H-S
(处理Sign)
收到2/3以上sign
3.commit
3.1 B-C
(广播Commit)
3.2 H-S
(处理Sign)
收到2/3 以上commit
4.do-commit
视图切换流程
view-change
收到2/3请求
view-confirm
proposal

图6

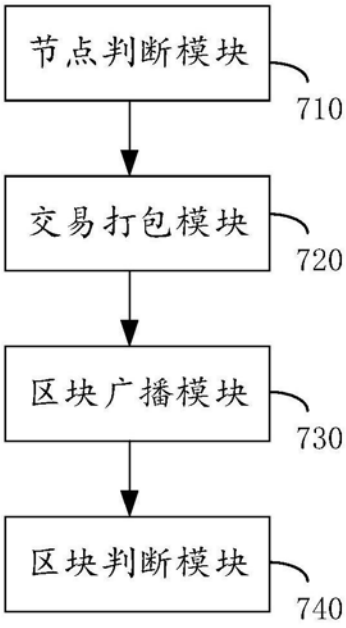

节点判断模块
710
交易打包模块
720
区块广播模块
730
区块判断模块
740

图7