(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109921897 B
(45)授权公告日 2022.06.17

(21)申请号 201910190063.0

(22)申请日 2019.03.13

(65)同一申请的已公布的文献号
申请公布号 CN 109921897 A

(43)申请公布日 2019.06.21

(73)专利权人 北京柏链基石科技有限公司
地址 100015 北京市朝阳区酒仙桥路10号1幢166室

(72)发明人 公鑫 刘涛 邹杰 刘健

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
专利代理师 刘昕 南霆

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 67/10(2022.01)
G06Q 20/38(2012.01)

(56)对比文件
CN 107294729 A,2017.10.24
CN 108389044 A,2018.08.10
WO 2018229633 A1,2018.12.20
US 2017344580 A1,2017.11.30
WO 2018224943 A1,2018.12.13

审查员 安佳

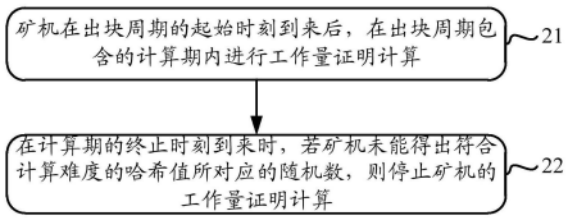
权利要求书2页 说明书15页 附图5页

(54)发明名称

工作量证明计算的触发方法、装置、计算设备及存储介质

(57)摘要

本发明公开了一种工作量证明计算的触发方法，以解决现有技术中由于一些矿机，受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，但最后可能仍然难以获得出块权利，从而导致无谓资源耗费较大的问题。方法包括：矿机在出块周期的起始时刻到来后，在所述出块周期包含的计算期内进行工作量证明计算；所述起始时刻基于指定事件确定；所述计算期的终止时刻，被设置为早于所述出块周期的终止时刻；在所述计算期的终止时刻到来时，若所述矿机未能得出符合计算难度的哈希值所对应的随机数，则停止所述矿机的所述工作量证明计算。本发明还公开一种工作量证明计算的触发装置、计算设备及计算机可读存储介质。



CN 109921897 B

1.一种工作量证明计算的触发方法,其特征在于,包括:

步骤41,全节点通过对等网络通信获取全节点集群中其他全节点的节点信息,其中,节点信息包括IP地址、VRF公钥、转账地址;

步骤42,全节点在出块周期起始时刻到来时,基于私钥以及VRF生成第一随机数,并将生成的第一随机数广播给全节点集群中的其他全节点;

接收全节点集群中的至少两个全节点分别基于各自的私钥以及VRF生成并发送来的第二随机数;

步骤43,全节点基于拜占庭容错算法,对第一随机数和第二随机数进行投票以选出目标随机数,并将目标随机数作为指令发送给矿机,或者承载在指令中发送给矿机;

步骤44,矿机接收到全节点发送的目标随机数后,开始进行工作量证明计算;

步骤45,矿机判断是否基于设定计算难度计算出符合条件的哈希值;若基于设定计算难度计算出符合需求的哈希值,执行步骤46;若未基于设定计算难度计算出符合需求的哈希值,执行步骤47;

步骤46,矿机基于设定计算难度计算出符合需求的哈希值、基于设定计算难度计算出符合条件的哈希值时所用的第三随机数,以及接收到的目标随机数,生成携带有基于设定计算难度计算出符合需求的哈希值、目标随机数和第三随机数的区块,并发送区块给包括全节点在内的全节点集群进行验证,而后执行步骤49;

步骤47,矿机判断是否接收到其他节点计算出的经验证符合需求的哈希值或是否达到计算期终止时刻;若是,执行步骤48;若否,执行步骤45;

步骤48,一方面,矿机等待全节点集群对区块的验证结果;另一方面,矿机等待下一轮工作量证明计算任务的开始——即等待下一轮工作量证明计算期内由全节点发送的指令的到来;

步骤49,全节点判断是否接收到由矿机在本计算期内计算得到的符合条件的哈希值,即判断是否接收到区块;若是,执行步骤410;若否,执行步骤411;

步骤410,全节点基于拜占庭容错算法,对接收到的携带有目标随机数、第三随机数和由矿机在本计算期内计算得到的符合条件的哈希值的区块进行合法性验证,当验证通过时,将该区块作为最终区块,进行全网广播,而后执行步骤412;

步骤411,判断计算期是否结束;若是,执行步骤412;若否,执行步骤49;

步骤412,等待当前出块周期的终止时刻到来,也即等待当前出块周期时间耗尽,以便在接收到全节点发送来的指令时,响应于指令,开始下一出块周期的工作量证明计算;

其中,所述全节点集群为由全节点构成的集合;所述计算期的终止时刻,被设置为早于所述出块周期的终止时刻。

2.一种工作量证明计算的触发装置,用于执行如权利要求1所述的工作量证明计算的触发方法,其特征在于,包括:

计算模块,用于在出块周期的起始时刻到来后,在所述出块周期包含的计算期内进行工作量证明计算;所述起始时刻基于指定事件确定;

停止模块,用于在预设的计算期终止时刻到来时,若未能基于设定计算难度计算出符合需求的哈希值对应的随机数,则停止所述工作量证明计算。

3.一种工作量证明计算的触发装置,用于执行如权利要求1所述的工作量证明计算的

触发方法，其特征在于，包括：

指令发送模块，用于发送用于触发工作量证明计算的指令；

监控模块，用于监控是否存在满足预定条件的矿机；所述预定条件包括：在出块周期的起始时刻到来后，在所述出块周期包含的计算期内进行工作量证明计算，且在预设的计算期终止时刻到来时，未能基于设定计算难度计算出符合需求的哈希值对应的随机数；所述起始时刻基于指定事件确定；所述计算期的终止时刻，被设置为早于所述出块周期的终止时刻；

指示模块，用于指示满足所述预定条件的矿机停止所述工作量证明计算。

4.一种计算设备，其特征在于，包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如权利要求1所述的工作量证明计算的触发方法的步骤。

5.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1所述的工作量证明计算的触发方法的步骤。

工作量证明计算的触发方法、装置、计算设备及存储介质

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种工作量证明计算的触发方法、装置、计算设备及计算机可读存储介质。

背景技术

[0002] 区块链(BlockChain)技术作为一种分布式账本技术，具有去中心化、分布式共识、匿名和可追溯特性，被认为是最有前途的技术之一。作为分布式网络的一种应用，如何在分布式网络中达成共识、选择出块节点，是区块链必须要解决的问题之一。目前主流的共识机制主要有工作量证明(Proof of Work，POW)和权益证明(Proof of Stake，POS)两种。POW和POS分别采用了计算力和权益持有的比率两种方法来选择出块节点。

[0003] 其中，POW共识机制以算力作为基础，由区块链网络全网内的所有矿机在出块周期内进行枚举与哈希值运算，最先计算出符合条件的随机数的矿机将可以获得本次出块权利，进而进行出块。采用现有技术这样的出块方式，对于一些矿机而言，受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，但最后可能仍然难以获得出块权利，从而导致无谓资源耗费较大。

[0004] 以单个出块周期为例，单个出块周期的起始时刻和终止时刻的示意图如图1所示。其中，T0为起始时刻，从该时刻起，矿机开始进行枚举与哈希值运算；T1为终止时刻，矿机在该时刻终止工作量证明计算，即，基于设定计算难度计算出符合需求的哈希值，或，在该时刻接收到用于告知本出块周期内验证通过的符合需求的哈希值(即告知已有矿机获得本出块周期的出块权利)的广播。

发明内容

[0005] 本发明实施例提供一种工作量证明计算的触发方法，用以解决现有技术中算力相对较弱的矿机在竞争出块权利时，存在的无谓的资源浪费较大的问题。

[0006] 本发明实施例还提供一种工作量证明计算的触发装置，一种计算设备以及一种计算机可读存储介质。

[0007] 本发明实施例采用下述技术方案：

[0008] 第一方面，本发明实施例提供了一种工作量证明计算的触发方法，所述方法包括：

[0009] 矿机在出块周期的起始时刻到来后，在所述出块周期包含的计算期内进行工作量证明计算；

[0010] 所述起始时刻基于指定事件确定；所述计算期的终止时刻，被设置为早于所述出块周期的终止时刻；

[0011] 在预设的计算期终止时刻到来时，若所述矿机未能基于设定计算难度计算出符合需求的哈希值对应的随机数，则停止所述矿机的所述工作量证明计算。

[0012] 第二方面，本发明实施例提供了一种工作量证明计算的触发方法，所述方法包括：

[0013] 发送用于触发工作量证明计算的指令；

[0014] 监控是否存在满足预定条件的矿机;所述预定条件包括:在出块周期的起始时刻到来后,在所述出块周期包含的计算期内进行工作量证明计算,且在预设的计算期终止时刻到来时,未能基于设定计算难度计算出符合需求的哈希值对应的随机数;所述起始时刻基于指定事件确定;所述计算期的终止时刻,被设置为早于所述出块周期的终止时刻;

[0015] 若是,则指示满足所述预定条件的矿机停止所述工作量证明计算。

[0016] 第三方面,本发明实施例提供了工作量证明计算的触发装置,所述装置包括计算模块和停止模块,其中:

[0017] 计算模块,用于矿机在出块周期的起始时刻到来后,在所述出块周期包含的计算期内进行工作量证明计算;所述起始时刻基于指定事件确定;所述计算期的终止时刻,被设置为早于所述出块周期的终止时刻;

[0018] 停止模块,用于在预设的计算期终止时刻到来时,若所述矿机未能基于设定计算难度计算出符合需求的哈希值对应的随机数,则停止所述矿机的所述工作量证明计算。

[0019] 第四方面,本发明实施例提供了一种工作量证明计算的触发装置,所述装置包括指令发送模块,监控模块和指示模块,其中:

[0020] 指令发送模块,用于发送用于触发工作量证明计算的指令;

[0021] 监控模块,用于监控是否存在满足预定条件的矿机;所述预定条件包括:在出块周期的起始时刻到来后,在所述出块周期包含的计算期内进行工作量证明计算,且在预设的计算期终止时刻到来时,未能基于设定计算难度计算出符合需求的哈希值对应的随机数;所述起始时刻基于指定事件确定;所述计算期的终止时刻,被设置为早于所述出块周期的终止时刻;

[0022] 指示模块,用于指示满足所述预定条件的矿机停止所述工作量证明计算。

[0023] 第五方面,本发明实施例提供了一种计算设备,包括:存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序,所述计算机程序被所述处理器执行时实现如上所述的任意一种工作量证明计算的触发方法的步骤。

[0024] 第六方面,本发明实施例提供了一种计算机可读存储介质,所述计算机可读存储介质上存储有计算机程序,所述计算机程序被处理器执行时实现如上所述的任意一种工作量证明计算的触发方法的步骤。

[0025] 本发明实施例采用的上述至少一个技术方案能够达到以下有益效果:

[0026] 采用本发明实施例提供的方法,首先,矿机在出块周期的起始时刻到来后,在出块周期包含的计算期内进行工作量证明计算,有效控制了矿机在整个出块周期内进行工作量证明计算的时间长度;其次,计算期的终止时刻被设置为早于出块周期的终止时刻,且当计算期的终止时刻到来时,若矿机未能得出符合计算难度的哈希值所对应的随机数,则停止工作量证明计算。对于算力相对较弱的矿机而言,可以避免矿机受限于其算力相对较弱,在出块周期的全时段内均可能需要进行枚举与哈希值运算,然而,最后可能仍然难以获得出块权利,从而导致无谓的资源耗费较大的问题。

附图说明

[0027] 此处所说明的附图用来提供对本发明的进一步理解,构成本发明的一部分,本发明的示意性实施例及其说明用于解释本发明,并不构成对本发明的不当限定。在附图中:

[0028] 图1为本发明实施例提供的一种单个出块周期的起始时刻和终止时刻的示意图；

[0029] 图2a为本发明实施例提供的工作量证明计算的触发方法的实现流程示意图；

[0030] 图2b为本发明实施例提供的计算期、计算期起始时刻、计算期终止时刻与出块周期的关系示意图；

[0031] 图3为本发明实施例提供的工作量证明计算的触发方法的实现流程示意图；

[0032] 图4a为本发明实施例提供的工作量证明计算的触发方法的实现流程及可以适用的一种系统架构示意图；

[0033] 图4b为本发明实施例提供的工作量证明计算的触发方法的实现流程示意图；

[0034] 图5为本发明实施例提供工作量证明计算的触发装置的具体结构示意图；

[0035] 图6为本发明实施例提供工作量证明计算的触发装置的具体结构示意图；

[0036] 图7为本发明实施例提供的一种计算设备的结构示意图。

具体实施方式

[0037] 为使本发明的目的、技术方案和优点更加清楚，下面将结合本发明具体实施例及相应的附图对本发明技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0038] 以下结合附图，详细说明本发明各实施例提供的技术方案。

[0039] 实施例1

[0040] 为解决现有技术中由于一些算力相对较弱的矿机，受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，但最后可能仍然难以获得出块权利，从而导致资源耗费较大的问题，本发明实施例提供一种工作量证明计算的触发方法。

[0041] 该方法的执行主体，可以为区块链网络中的的矿机，所述矿机可以是各种类型的计算设备，比如可以是台式计算机、膝上型计算机、笔记本电脑、台式计算机、蜂窝电话、智能电话、智能手表、可佩戴计算设备或可植入计算设备等用户终端，也可以是服务器等。

[0042] 为便于描述，本发明实施例以该方法的执行主体为具备计算功能的计算设备为例，对该方法进行介绍。本领域技术人员可以理解，本发明实施例以该计算设备为例对方法进行介绍，仅是一种示例性说明，并不对本方案对应的权利要求保护范围构成限制。

[0043] 具体地，本发明实施例提供的该方法的实现流程如图2a所示，包括如下步骤：

[0044] 步骤21，矿机在出块周期的起始时刻到来后，在所述出块周期包含的计算期内进行工作量证明计算；

[0045] 所述起始时刻基于指定事件确定；

[0046] 所述指定事件，可以包括但不限于：接收到全节点发送的用于触发工作量证明计算的指令；

[0047] 所述指令中可以包括全节点集群基于拜占庭容错算法投票选出的目标随机数；其中，全节点集群可以是投票选取出的，且选取出的全节点可以质押一定数量的虚拟币以防全节点作恶；所述全节点集群为由全节点构成的集合。

[0048] 所述计算期的终止时刻，可以被设置为早于出块周期的终止时刻。

[0049] 采用将计算期的终止时刻设置为早于出块周期的终止时刻的方式，相当于在已有

的两种停止工作量证明计算的触发条件——“计算出符合计算难度的哈希值所对应的随机数”和“接收到符合计算难度的哈希值所对应的随机数的广播”之外，新增了一种新的适时触发矿机停止工作量证明计算的条件。

[0050] 由于计算期的终止时刻可以是一个经验值，在实际应用中可以通过设置，使得计算期的终止时刻在满足早于出块周期的终止时刻的同时，尽量保证算力相对较弱的矿机能够有足够长的时间进行工作量证明计算，从而可以在节省矿机处理资源的同时，对矿机可用的工作量证明计算耗时不会过于缩减。

[0051] 步骤21中，矿机在计算期内进行工作量证明计算，具体包括：所述矿机在所述计算期的起始时刻到来后，在所述计算期内进行工作量证明计算；

[0052] 其中，计算期的起始时刻可以晚于出块周期的起始时刻；

[0053] 或，计算期的起始时刻可以与出块周期的起始时刻相同。

[0054] 例如，可以采用如下方式实现计算期的起始时刻晚于出块周期的起始时刻：

[0055] 第一，矿机接收全节点发送的用于触发工作量证明计算的指令；

[0056] 所述指令可以在滞后于出块周期起始时刻的第二时刻生成；

[0057] 其中，关于全节点如何生成该指令，例如可以采用如下方法：

[0058] 全节点A在出块周期起始时刻，执行基于全节点A的私钥以及可验证随机函数(Verifiable Random Function，VRF)生成第一随机数的运算。

[0059] 全节点A在第二时刻，根据所述第一随机数，确定所述指令。

[0060] 第二，矿机响应于所述指令，从出块周期内的第一时刻开始，进行工作量证明计算。

[0061] 需要说明的是，由于指令在滞后于出块周期起始时刻的第二时刻生成，那么，矿机一旦接收到该指令，则可以以不早于该指令的接收时刻的时刻作为所述的第一时刻，从该第一时刻开始进行工作量证明计算。

[0062] 采用计算期的起始时刻晚于出块周期的起始时刻的方法，由于矿机根据指令进行工作量证明计算，因此可以有效控制矿机在出块周期内进行工作量证明计算的时间长度，且由于矿机进行工作量证明计算的第一时刻晚于出块周期起始时刻，避免了算力相对较弱的矿机在出块周期的全时段内，均需要进行枚举与哈希值运算，从而可能导致无谓的资源浪费较大的问题。

[0063] 此外，本发明实施例中，可以采用现有相关技术实现计算期的起始时刻与出块周期的起始时刻相同的工作量证明计算的触发方法，此处不再赘述。

[0064] 为直观表述计算期、计算期的起始时刻、计算期的终止时刻与出块周期的关系，说明书附图2b中对计算期起始时刻晚于出块周期起始时刻的出块周期A和计算期起始时刻与出块周期起始时刻相同的出块周期B进行了比较。

[0065] 说明书附图2b中，位于图上方的出块周期，表示出块周期A；位于图下方的出块周期，表示出块周期B；其中，T0表示出块周期的起始时刻、T1表示出块周期的终止时刻、T2表示计算期的起始时刻、T3表示计算期的终止时刻。

[0066] 可选地，矿机在预设的计算期终止时刻到来时，若基于设定计算难度计算出符合需求的哈希值对应的随机数(为便于区分描述，称为第三随机数)，则将所述第三随机数携带在区块中发送给全节点集群进行验证。

[0067] 按照现有技术，矿机在基于设定计算难度计算出符合需求的哈希值(即基于设定计算难度，根据第三随机数计算出符合需求的哈希值)后，会基于该第三随机数生成区块，并将区块广播给区块链网络中的其他矿机进行验证，以确定该矿机是否具备本出块周期的出块权利。

[0068] 而本发明实施例中，矿机在基于设定计算难度计算出符合需求的哈希值后，可以根据全节点集群中各全节点的地址，向全节点集群中各全节点发送区块，从而实现了将区块的验证权集中到全节点集群。由于如前文所述，全节点集群可以是投票选取出的，且选取出的全节点可以质押一定数量的虚拟币以防全节点作恶，因此，这样可以保证由全节点进行区块验证的验证结果是可信的、有效的。

[0069] 相对于现有技术中采用向矿机广播区块进行区块验证的方式，本发明实施例采用的该方式无需数量庞大的矿机进行持续的挖矿计算，可以显著降低资源消耗。同时，区块验证，可以由数量相对较少的全节点(全节点集群中的全节点)进行验证，可以有效解决现有挖矿算法中由于算力垄断导致的恶意分叉的问题，可以大大提高区块链的安全性。

[0070] 需要说明的是，本发明实施例中，可以将目标随机数作为验证区块的依据；

[0071] 例如，区块中可以携带目标随机数，所述目标随机数可以用于全节点集群根据区块中是否包含目标随机数，对区块的合法性进行验证。

[0072] 具体而言，矿机可以根据全节点集群中各全节点的地址，将第三随机数携带在区块中发送给全节点集群进行验证。其中，全节点的地址，可以由全节点预先发送给矿机。全节点集群可以是投票选取出的，且选取出的全节点可以质押一定数量的虚拟币以防全节点作恶；所述全节点集群为由全节点构成的集合。

[0073] 对于全节点而言，若接收到待验证的区块，则可以根据待验证的区块中是否包含目标随机数，对待验证的区块的合法性进行验证；若待验证的区块中包含目标随机数，则确定该区块合法，进而进一步验证该区块中的第三随机数(验证第三随机数为成熟的相关技术，此处不再赘述)；否则，则确定该区块不合法，从而可以丢弃该区块，或者，不再对该区块中的第三随机数进行验证，而是直接判定发送来该区块的矿机没有出块权利。

[0074] 例如，对于矿机而言，假设目标随机数为0000f800，第三随机数为000fec80，则矿机可以将第三随机数携带在区块中发送给全节点集群进行验证，且该区块中还可以包括目标随机数0000f800。

[0075] 对于全节点而言，若接收到待验证的区块中包含目标随机数0000f800，则确定该区块合法，进而进一步验证该区块中的第三随机数000fec80(验证第三随机数为成熟的相关技术，此处不再赘述)；

[0076] 若接收到待验证的区块中不包含目标随机数0000f800，则确定该区块不合法，从而可以丢弃该区块，或者，不再对该区块中的第三随机数000fec80进行验证，而是直接判定发送来该区块的矿机没有出块权利。

[0077] 考虑区块链网络全网内算力较低的矿机，受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，但最后可能仍然难以获得出块权利，从而导致无谓资源耗较大的问题，本发明实施例中，还可以包括如下步骤：

[0078] 步骤22，在预设的计算期终止时刻到来时，若所述矿机未能基于设定计算难度计算出符合需求的哈希值对应的随机数，则停止所述矿机的所述工作量证明计算。

[0079] 采用本发明实施例提供的方法，无论是计算期的起始时刻与出块周期的起始时刻相同，或者是计算期的起始时刻晚于出块周期的起始时刻，由于计算期的终止时刻被设置为早于出块周期的终止时刻，因此，计算期的长度均短于出块周期T的长度，可以避免矿机在出块周期的全时段内可能均需要进行枚举与哈希值运算的问题，可以有效降低资源消耗。

[0080] 同时，由于本发明实施例中，矿机在计算期的终止时刻到来时，若未能得出符合计算难度的哈希值所对应的随机数，则停止矿机的工作量证明计算，使矿机进行工作量证明计算被控制在计算期内完成，对于算力相对较弱的矿机而言，可以防止矿机受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，然而，最后可能仍然难以获得出块权利，从而导致无谓资源耗费较大的问题。

[0081] 实施例2

[0082] 如图3所示，本发明实施例提供一种工作量证明计算的触发方法，该方法的执行主体，可以是区块链网络中的全节点，所述全节点可以是各种类型的计算设备。所述的计算设备，比如可以是台式计算机、膝上型计算机、笔记本电脑、蜂窝电话、智能电话、智能电视、智能手表、可佩戴计算设备或可植入计算设备等用户终端，也可以是服务器等。

[0083] 为便于描述，本发明实施例以该方法的执行主体为全节点为例，对该方法进行介绍。本领域技术人员可以理解，本发明实施例以全节点为例对方法进行介绍，仅是一种示例性说明，并不对本方案对应的权利要求保护范围构成限制。

[0084] 以下对全节点的特点进行说明：

[0085] 全节点可以是拥有完整区块链账本的节点，可以同步区块链网络的所有数据，能够独立校验区块链上的所有交易并实时更新数据，负责区块链工作量证明计算结果的验证和广播。全节点可以采用区块链共识机制中的轮流共识机制，即每隔一定时间，可以根据预先设定或者投票的选举方法重新选择全节点。采用这种区块链共识机制，可以保证全节点验证过程中的公平性。

[0086] 此外，考虑到验证过程中验证结果的有效性，本发明实施例中，例如，可以规定让选取出的全节点质押一定数量的虚拟币，当全节点中某节点作恶时，则其余全节点可以通过投票方式扣除其质押的虚拟币。采用这样的方式，可以有效防止全节点作恶。

[0087] 本发明实施例2中，比如可以采用投票选举的方法，从存在于区块链网络的全节点中，选取预设数量的全节点。为便于描述，后文将选取出的预设数量的全节点构成的集合称为全节点集群。当然，本发明实施例2中也可以采用其他方式实现从存在于区块链网络的全节点中选取全节点，比如，可以按照负载均衡的原则选取负载较低的全节点，本发明实施例2对选取方式不做限定。

[0088] 全节点集群中的每个全节点，均可以执行本发明实施例2提供的该方法，作为该方法的执行主体。

[0089] 为便于描述，以下以执行主体为全节点集群中的全节点A为例，介绍该方法的具体实现流程，该方法包括如下步骤：

[0090] 步骤31，全节点A发送用于触发工作量证明计算的指令；

[0091] 例如，可以在滞后于出块周期起始时刻的第二时刻发送指令；本发明实施例中，若全节点A在滞后于出块周期起始时刻的第二时刻发送指令，则矿机接收到指令的时刻必定

晚于出块周期起始时刻,进而使得矿机开始进行工作量证明计算的时刻晚于出块周期的起始时刻,即计算期起始时刻滞后于出块周期起始时刻。

[0092] 其中,指令中包含全节点集群基于拜占庭容错算法投票选出的目标随机数;

[0093] 所述目标随机数用于对区块的合法性进行验证。

[0094] 本发明实施例中,所述目标随机数,可以采用下述方式投票选出:

[0095] 第一,根据全节点A的节点信息生成第一随机数;

[0096] 例如,全节点A可以在出块周期起始时刻,根据可验证随机函数的共识算法执行基于全节点A的私钥以及可验证随机函数(Verifiable Random Function,VRF)生成第一随机数的运算。

[0097] 本发明实施例中,根据全节点的私钥以及VRF生成第一随机数,一方面,虽然VRF输入信息是确定的,全网公开,但是其结果是离散的、均匀分布的,因此可以避免全节点伪造结果;另一方面,由于全节点的私钥在全节点之间是相互保密的,可以保证私钥安全性;因此,结合上述分析可知,本发明实施例中采用根据私钥以及可验证随机函数生成的第一随机数的方式,可以防止全节点作弊。

[0098] 第二,全节点A接收全节点集群中的至少两个全节点分别基于各自的私钥以及VRF生成并发送来的第二随机数;

[0099] 例如,假设全节点集群中除全节点A外,至少还包括全节点B、全节点C,全节点B、全节点C分别基于各自的私钥以及VRF生成第二随机数b、c,并发送给全节点A。

[0100] 第三,全节点A基于拜占庭容错算法,从第一随机数和第二随机数中投票选出目标随机数。

[0101] 沿用上例,假设全节点A生成第一随机数a,全节点B、全节点C分别生成第二随机数b、c,且a<b<c,则全节点A基于拜占庭容错算法,从a、b、c中投票选出目标随机数c。假设预设的选取规则为选取最大的随机数,则全节点A投票选出最大随机数。

[0102] 需要说明的是,选取最大的随机数作为目标随机数仅是一种示例性说明,本发明实施例中,还可以选取最小随机数等其余的可以唯一确定的随机数作为目标随机数。

[0103] 其中,本发明实施例中,采用拜占庭容错算法,可以避免上述第一步中由于网络延迟,使得全节点A在预计接收时长内没有接收到某随机数(假设为随机数c),导致全节点A根据预设的选取规则投票选取的目标随机数b与全节点B、全节点C根据预设的选取规则投票选取的目标随机数c不一致,从而,在后续操作中无法明确根据b或是c生成指令的问题。本发明实施例由于采用拜占庭容错算法,所以当出现上述情况时,会将投票数量在投票总数量中的占比较高的c确定为最终的目标随机数,保证了投票选出的目标随机数的唯一性。

[0104] 考虑到区块链网络全网内算力较低的矿机所需的工作量证明计算时长相对较长,会导致资源消耗相对较多,进而若最终未获得出块权利则浪费了处理资源,本发明实施例中,将指令发送给矿机后,所述方法还包括如下步骤:

[0105] 步骤32,全节点A监控是否存在满足预定条件的矿机;

[0106] 所述预定条件包括:在出块周期的起始时刻到来后,在出块周期包含的计算期内进行工作量证明计算,且在计算期的终止时刻到来时,未能得到符合计算难度的哈希值所对应的随机数;

[0107] 所述起始时刻可以基于指定事件确定;

[0108] 所述指定事件，可以包括但不限于：全节点A发送的用于触发工作量证明计算的指令；

[0109] 其中，计算期的起始时刻可以晚于出块周期的起始时刻；

[0110] 或，计算期的起始时刻可以与出块周期的起始时刻相同；

[0111] 所述计算期的终止时刻，可以被设置为早于所述出块周期的终止时刻；

[0112] 采用将计算期的终止时刻设置为早于出块周期的终止时刻的方式，相当于在已有的两种停止工作量证明计算的触发条件——“计算出符合计算难度的哈希值所对应的随机数”和“接收到符合计算难度的哈希值所对应的随机数的广播”之外，新增了一种新的适时触发矿机停止工作量证明计算的条件。

[0113] 由于计算期的终止时刻可以是一个经验值，在实际应用中可以通过设置，使得计算期的终止时刻在满足早于出块周期的终止时刻的同时，尽量保证算力相对较弱的矿机能够有足够长的时间进行工作量证明计算，从而可以在节省矿机处理资源的同时，对矿机可用的工作量证明计算耗时不会过于缩减。

[0114] 步骤33，若是，则指示满足所述预定条件的矿机停止所述工作量证明计算。

[0115] 若全节点A监控到存在满足预定条件的矿机，则指示满足所述预定条件的矿机停止所述工作量证明计算。

[0116] 所述预定条件包括：在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算，且在计算期的终止时刻到来时，未能得到符合计算难度的哈希值所对应的随机数。

[0117] 采用本发明实施例提供的方法，首先，矿机在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算，有效控制了矿机在整个出块周期内进行工作量证明计算的时间长度；其次，计算期的终止时刻被设置为早于出块周期的终止时刻，且当计算期的终止时刻到来时，若矿机未能得出符合计算难度的哈希值所对应的随机数，则停止工作量证明计算。对于算力相对较弱的矿机而言，可以避免矿机受限于其算力相对较弱，在出块周期的全时段内均可能需要进行枚举与哈希值运算，然而，最后可能仍然难以获得出块权利，从而导致无谓的资源耗费较大的问题。

[0118] 以下通过介绍实施例3，对本发明实施例提供的工作量证明计算的触发方法作进一步说明。

[0119] 实施例3

[0120] 本发明实施例中，提供一种实施工作量证明计算的触发方法的系统架构示意图，如说明书附图4a所示。

[0121] 为实施该方案，第一，可以将出块周期按时间比例划分为三个阶段，分别为准备期、计算期和验证期，在说明书附图4a中简写为准、计、验。

[0122] 例如，出块完整周期为5分钟，按1:1:3时间比例分配，则准备期为1分钟，计算期为1分钟，验证期为3分钟；其中，准备期和出块期可以小于规定的时间，但是不能超过，出块周期固定为5分钟。

[0123] 第二，在该系统架构中，可以通过投票选举的方法，从区块链网络中选出n个全节点，分别记为如图4a中的全节点1、全节点2、全节点3…全节点n。

[0124] 为便于描述，后文将预设数量的全节点构成的集合称为全节点集群。

[0125] 当然，本发明实施例3中也可以采用其他方式实现从存在于区块链网络的全节点中选取全节点，比如，可以按照负载均衡的原则选取负载较低的全节点，本发明实施例3对选取方式不做限定。

[0126] 此外，考虑到验证过程中验证结果的有效性，本发明实施例中，例如，可以规定让选取出的全节点质押一定数量的虚拟币，当全节点中某节点作恶时，则其余全节点可以通过投票方式扣除其质押的虚拟币。采用这样的方式，可以有效防止全节点作恶。

[0127] 第三，如图4a所示，全节点1至全节点n在出块周期中的准备期中生成目标随机数，并将目标随机数发送矿机。

[0128] 第四，矿机接收到目标随机数后，开始进行工作量证明计算，进入计算期，当矿机基于设定计算难度计算出符合条件的哈希值，将基于目标随机数、第三随机数和基于设定计算难度计算出的符合条件的哈希值所生成的区块发送给全节点进行验证。

[0129] 需要说明的是，本发明实施例中，对于第一步与第二步的执行顺序不做限定，第一步与第二步的执行顺序可互换，例如，可以先通过投票选举的方法，从区块链网络中选出n个全节点，然后再按时间比例对出块周期进行划分。

[0130] 具体地，该系统架构中各组成部分在单个出块周期内所执行的操作，如下图4b所示，详细描述如下：

[0131] 为方便描述，以下以全节点A为例，对本发明实施例进行说明：

[0132] 步骤41，全节点A通过对等网络(Peer-to-Peer networking，P2P)通信获取全节点集群中其他全节点的节点信息，其中，节点信息比如可以包括IP地址、VRF公钥、转账地址；

[0133] 步骤42，全节点A在出块周期起始时刻到来时，基于私钥以及VRF生成第一随机数，并将生成的第一随机数广播给全节点集群中的其他全节点；

[0134] 步骤42中，全节点A将生成的第一随机数广播给全节点集群中的其他全节点后，还包括：

[0135] 接收全节点集群中的至少两个全节点分别基于各自的私钥以及VRF生成并发送来的随机数(统称第二随机数)。第二随机数的计算方式请参考前文描述。

[0136] 例如，假设全节点集群中除全节点A外，至少还包括全节点B、全节点C，全节点B、全节点C分别基于各自的私钥以及VRF生成第二随机数b、c，并发送给全节点A。

[0137] 步骤43，全节点A基于拜占庭容错算法，对第一随机数和第二随机数进行投票以选出目标随机数，并将目标随机数作为指令发送给矿机，或者承载在指令中发送给矿机；

[0138] 沿用上述实施例1中的例子，假设全节点A生成第一随机数a，全节点B、全节点C分别生成第二随机数b、c，且a<b<c，则全节点A基于拜占庭容错算法，从a、b、c中投票选出目标随机数c。假设预设的选取规则为选取最大的随机数，则全节点A投票选出最大随机数。

[0139] 需要说明的是，选取最大的随机数作为目标随机数仅是一种示例性说明，本发明实施例中，还可以选取最小随机数等其余的可以唯一确定的随机数作为目标随机数。

[0140] 其中，本发明实施例中，采用拜占庭容错算法，可以避免由于网络延迟使得全节点A在预计接收时长内没有接收到某随机数(假设为随机数c)，导致全节点A根据预设的选取规则投票选取的目标随机数b与全节点B、全节点C根据预设的选取规则投票选取的目标随机数c不一致，从而，在后续操作中无法明确根据b或是c生成指令的问题。本发明实施例由于采用拜占庭容错算法，所以当出现上述情况时，会将投票数量在投票总数量中的占比较

高的c确定为最终的目标随机数，保证了投票选出的目标随机数的唯一性。

[0141] 以上即为全节点A在出块周期中准备期进行的全部操作，下面，本发明实施例将从区块链网络中矿机的角度出发，对矿机在出块周期包含的计算期中执行的操作进行描述。

[0142] 如图4b所示，计算期可以包括以下几个步骤：

[0143] 步骤44，矿机接收到全节点发送的目标随机数后，开始进行工作量证明计算；

[0144] 步骤45，矿机判断是否基于设定计算难度计算出符合条件(符合需求)的哈希值；若基于设定计算难度计算出符合需求的哈希值，执行步骤46；若未基于设定计算难度计算出符合需求的哈希值，执行步骤47；

[0145] 步骤46，矿机基于设定计算难度计算出符合需求的哈希值、基于设定计算难度计算出符合条件的哈希值时所用的随机数(第三随机数)，以及接收到的目标随机数，生成携带有基于设定计算难度计算出符合需求的哈希值、目标随机数和第三随机数的区块，并发送区块给包括全节点A在内的全节点集群进行验证，而后执行步骤49；

[0146] 步骤47，矿机判断是否接收到其他节点(矿机或全节点)计算出的经验证符合需求的哈希值或是否达到计算期终止时间(时刻)；若是，执行步骤48；若否，执行步骤45；

[0147] 步骤48，一方面，矿机等待全节点集群对区块的验证结果；另一方面，矿机等待下一轮工作量证明计算任务的开始——即等待下一轮工作量证明计算周期内由全节点发送的指令的到来；

[0148] 其中，以全节点A为例，全节点集群中的全节点对区块进行验证的过程(该过程在出块周期中所属的时间区间，也可称为“验证期”)可以包括以下步骤：

[0149] 步骤49，全节点A判断是否接收到由矿机在本周期内计算得到的符合条件的哈希值(即判断是否接收到区块)；若是，执行步骤410；若否，执行步骤411；

[0150] 步骤410，全节点A基于拜占庭容错算法，对接收到的携带有目标随机数、第三随机数和由矿机在本周期内计算得到的符合条件的哈希值的区块进行合法性验证，当验证通过时，将该区块最为最终区块，进行全网广播，而后执行步骤412；

[0151] 具体验证方式请见实施例1中相关描述，此处不再赘述。

[0152] 步骤411，判断计算期是否结束；若是，执行步骤412；若否，执行步骤49；

[0153] 步骤412，等待当前出块周期的终止时刻到来，也即等待当前出块周期时间耗尽，以便在接收到全节点发送来的指令时，响应于指令，开始下一出块周期的工作量证明计算。

[0154] 采用本发明实施例提供的方法，将出块周期按照一定时间比例划分为三部分，分别为准备期、计算期和验证期，整个出块周期中，计算期只占出块周期中的一部分，对于算力相对较弱的矿机而言，可以解决由于受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，从而导致资源耗费较大，可能出现无谓资源浪费的问题。

[0155] 另外，对于区块链网络中既包括新加入的算力相对较强、能耗相对较低的“新矿机”，又包括算力相对较弱、能耗相对较高的“老矿机”的情况，采用本发明实施例的方法，由于资源消耗减少，所以新矿机大算力和能耗低的优势被弱化，使得老矿机可以通过增加数量弥补算力不足，从而可以有效抵制技术垄断，降低算力低下的矿机的报废率。

[0156] 采用本发明实施例提供的方法，首先，矿机在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算，有效控制了矿机在整个出块周期内进行工作量证明计算的时间长度；其次，计算期的终止时刻被设置为早于出块周期的终止时刻，且当计

算期的终止时刻到来时，若矿机未能得出符合计算难度的哈希值所对应的随机数，则停止工作量证明计算。对于算力相对较弱的矿机而言，可以避免矿机受限于其算力相对较弱，在出块周期的全时段内均可能需要进行枚举与哈希值运算，然而，最后可能仍然难以获得出块权利，从而导致无谓的资源耗费较大的问题。

[0157] 实施例4

[0158] 为解决现有出块技术中，对于一些算力相对较弱的矿机而言，由于受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，但最后可能仍然难以获得出块权利，从而导致资源耗费较大的问题，本发明实施例提供一种工作量证明计算的触发装置50，该装置可以是矿机，或者可以设置在矿机中，该装置的具体结构示意图如图5所示，包括计算模块51以及停止模块52。其中，各模块的功能如下：

[0159] 计算模块51，用于在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算；

[0160] 停止模块52，用于在预设的计算期终止时刻到来时，若所述矿机未能基于设定计算难度计算出符合需求的哈希值对应的随机数，则停止所述矿机的所述工作量证明计算。

[0161] 其中，所述起始时刻基于指定事件确定；

[0162] 所述指定事件可以包括但不限于，接收到全节点发送的用于触发工作量证明计算的指令；所述指令中可以包含所述全节点集群基于拜占庭容错算法投票选出的目标随机数；

[0163] 所述计算期的终止时刻，可以被设置为早于所述出块周期的终止时刻；

[0164] 采用将计算期的终止时刻设置为早于出块周期的终止时刻的方式，相当于在已有的两种停止工作量证明计算的触发条件——“计算出符合计算难度的哈希值所对应的随机数”和“接收到符合计算难度的哈希值所对应的随机数的广播”之外，新增了一种新的适时触发矿机停止工作量证明计算的条件。

[0165] 由于计算期的终止时刻可以是一个经验值，在实际应用中可以通过设置，使得计算期的终止时刻在满足早于出块周期的终止时刻的同时，尽量保证算力相对较弱的矿机能够有足够长的时间进行工作量证明计算，从而可以在节省矿机处理资源的同时，对矿机可用的工作量证明计算耗时不会过于缩减。

[0166] 可选地，计算模块51，具体用于：

[0167] 在所述计算期的起始时刻到来后，在所述计算期内进行工作量证明计算；

[0168] 其中，计算期的起始时刻晚于出块周期的起始时刻；或，计算期的起始时刻与出块周期的起始时刻相同。

[0169] 可选地，所述装置还包括：

[0170] 发送模块，用于在预设的计算期终止时刻到来时，若矿机基于设定计算难度计算出符合需求的哈希值对应的随机数，则将所述符合需求的哈希值对应的随机数携带在区块中发送给全节点集群进行验证；所述全节点集群为由全节点构成的集合。

[0171] 所述区块中还可以携带有目标随机数；

[0172] 所述目标随机数，可以作为全节点集群对区块合法性进行验证的验证证据之一，以下进行说明：

[0173] 对于矿机而言，根据全节点集群中各全节点的地址，将第三随机数携带在区块中

发送给全节点集群进行验证；

[0174] 对于全节点而言，若接收到待验证的区块，则根据待验证的区块中是否包含目标随机数，对待验证的区块的合法性进行验证；若待验证的区块中包含目标随机数，则确定该区块合法，进而进一步验证该区块中的第三随机数(验证第三随机数为成熟的相关技术，此处不再赘述)；否则，则确定该区块不合法，从而可以丢弃该区块，或者，不再对该区块中的第三随机数进行验证，而是直接判定发送来该区块的矿机没有出块权利。

[0175] 采用本发明实施例提供的该装置，矿机可以在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算，其中，计算期的终止时刻被设置为早于出块周期的终止时刻，即矿机可以在小于出块周期的一个时间段内进行工作量证明计算，且当计算期的终止时刻到来时，若矿机未能得出符合计算难度的哈希值所对应的随机数，则停止工作量证明计算。对于算力相对较弱的矿机而言，可以防止矿机受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，然而，最后可能仍然难以获得出块权利，从而导致无谓资源耗费较大的问题。

[0176] 实施例5

[0177] 为解决现有出块技术中，对于一些算力相对较弱的矿机而言，由于受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，但最后可能仍然难以获得出块权利，从而导致资源耗费较大的问题，本发明实施例提供一种工作量证明计算的触发装置60，该装置的具体结构示意图如图6所示，包括指令发送模块61、监控模块62以及指示模块63。其中，各模块的功能如下：

[0178] 指令发送模块61，用于发送用于触发工作量证明计算的指令；

[0179] 监控模块62，用于监控是否存在满足预定条件的矿机；所述预定条件包括：在出块周期的起始时刻到来后，在所述出块周期包含的计算期内进行工作量证明计算，且在预设的计算期终止时刻到来时，未能基于设定计算难度计算出符合需求的哈希值对应的随机数；所述起始时刻基于指定事件确定；所述计算期的终止时刻，被设置为早于所述出块周期的终止时刻；

[0180] 指示模块63，用于指示满足所述预定条件的矿机停止所述工作量证明计算。

[0181] 其中，指令中可以包含全节点集群基于拜占庭容错算法投票选出的目标随机数；所述全节点集群为由全节点构成的集合；

[0182] 所述目标随机数，可以用于对区块的合法性进行验证。

[0183] 所述目标随机数，可以采用下述方式投票选出：

[0184] 第一，可以根据全节点A的节点信息生成第一随机数；

[0185] 例如，全节点A在出块周期起始时刻，执行基于全节点A的私钥以及可验证随机函数(Verifiable Random Function，VRF)生成第一随机数的运算。

[0186] 第二，全节点A接收全节点集群中的至少两个全节点分别基于各自的私钥以及VRF生成并发送来的第二随机数；

[0187] 例如，假设全节点集群中除全节点A外，至少还包括全节点B、全节点C，全节点B、全节点C分别基于各自的私钥以及VRF生成第二随机数b、c，并发送给全节点A。

[0188] 第三，可以基于拜占庭容错算法，从第一随机数和第二随机数中投票选出目标随机数。

[0189] 沿用上例，假设全节点A生成第一随机数a，全节点B、全节点C分别生成第二随机数b、c，且a<b<c，则全节点A基于拜占庭容错算法，从a、b、c中投票选出目标随机数c。假设预设的选取规则为选取最大的随机数，则全节点A投票选出最大随机数。

[0190] 需要说明的是，选取最大的随机数作为目标随机数仅是一种示例性说明，本发明实施例中，还可以选取最小随机数等其余的可以唯一确定的随机数作为目标随机数。

[0191] 其中，本发明实施例中，采用拜占庭容错算法，可以避免上述第一步中由于网络延迟，使得全节点A在预计接收时长内没有接收到某随机数(假设为随机数c)，导致全节点A根据预设的选取规则投票选取的目标随机数b与全节点B、全节点C根据预设的选取规则投票选取的目标随机数c不一致，从而，在后续操作中无法明确根据b或是c生成指令的问题。本发明实施例由于采用拜占庭容错算法，所以当出现上述情况时，会将投票数量在投票总数量中的占比较高的c确定为最终的目标随机数，保证了投票选出的目标随机数的唯一性。

[0192] 此外，本发明实施例采用将计算期的终止时刻设置为早于出块周期的终止时刻的方式，相当于在已有的两种停止工作量证明计算的触发条件——“计算出符合计算难度的哈希值所对应的随机数”和“接收到符合计算难度的哈希值所对应的随机数的广播”之外，新增了一种新的适时触发矿机停止工作量证明计算的条件。

[0193] 由于计算期的终止时刻可以是一个经验值，在实际应用中可以通过设置，使得计算期的终止时刻在满足早于出块周期的终止时刻的同时，尽量保证算力相对较弱的矿机能够有足够长的时间进行工作量证明计算，从而可以在节省矿机处理资源的同时，对矿机可用的工作量证明计算耗时不会过于缩减。

[0194] 采用本发明实施例提供的该装置，矿机可以在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算，其中，计算期的终止时刻被设置为早于出块周期的终止时刻，即矿机可以在小于出块周期的一个时间段内进行工作量证明计算，且当计算期的终止时刻到来时，若矿机未能得出符合计算难度的哈希值所对应的随机数，则停止工作量证明计算。对于算力相对较弱的矿机而言，可以防止矿机受限于其算力相对较弱，在出块周期的全时段内可能均需要进行枚举与哈希值运算，然而，最后可能仍然难以获得出块权利，从而导致资源耗费较大的问题。

[0195] 实施例6

[0196] 图7为本发明实施例6提供的一种计算设备的结构示意图70，图7展示的设备仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0197] 图7显示的计算设备70仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0198] 如图7所示，计算设备70以通用计算设备的形式表现。计算设备70的组件可以包括但不限于：一个或者多个处理器71，系统存储器75，连接不同系统组件(包括系统存储器75和处理器71的总线72。

[0199] 总线72表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0200] 计算设备70典型地包括多种计算机系统可读介质。这些介质可以是任何能够被计

算设备访问的可用介质,包括易失性和非易失性介质,可移动的和不可移动的介质。

[0201] 系统存储器75可以包括易失性存储器形式的计算机系统可读介质,例如随机存取存储器(RAM)751和/或高速缓存存储器752。计算设备70可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例,存储系统753可以用于读写不可移动的、非易失性磁介质(图7未显示,通常称为“硬盘驱动器”)。尽管图7中未示出,可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器754,以及对可移动非易失性光盘(例如CD-ROM,DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下,每个驱动器可以通过一个或者多个数据介质接口与总线72相连。系统存储器85可以包括至少一个程序产品,该程序产品具有一组(例如至少一个)程序模块,这些程序模块被配置以执行本发明实施例各实施例的功能。

[0202] 计算设备70也可以与一个或多个外部设备76(例如键盘、指向设备、显示器77等)通信,还可与一个或者多个使得用户能与该设备72交互的设备通信,和/或与使得该计算设备70能与一个或多个其它计算设备进行通信的任何设备(例如网卡,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73进行。并且,设备70还可以通过网络适配器74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74通过总线72与设备70的其它模块通信。应当明白,尽管图中未示出,可以结合设备70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、冗余处理器、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。

[0203] 处理器71通过运行存储在系统存储器75中的多个程序中的至少一个程序,从而执行各种功能应用以及数据处理,例如实现本发明上述提供的工作量证明计算的触发方法中的任意一种方法。

[0204] 本发明实施例还提供一种计算机可读存储介质,计算机可读存储介质上存储有计算机程序,该计算机程序被处理器执行时实现上述工作量证明计算的触发方法实施例的各个过程,且能达到相同的技术效果,为避免重复,这里不再赘述。其中,所述的计算机可读存储介质,如只读存储器(Read-Only Memory,简称ROM)、随机存取存储器(Random Access Memory,简称RAM)、磁碟或者光盘等。

[0205] 本领域内的技术人员应明白,本发明的实施例可提供为方法、系统、或计算机程序产品。因此,本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0206] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0207] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指

令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0208] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0209] 在一个典型的配置中，计算设备包括一个或多个处理器 (CPU)、输入/输出接口、网络接口和内存。

[0210] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器 (RAM) 和/或非易失性内存等形式，如只读存储器 (ROM) 或闪存(flash RAM)。内存是计算机可读介质的示例。

[0211] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器 (RAM)、只读存储器 (ROM)、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器 (CD-ROM)、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体 (transitory media)，如调制的数据信号和载波。

[0212] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0213] 以上所述仅为本发明的实施例而已，并不用于限制本发明。对于本领域技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本发明的权利要求范围之内。


出块周期T
T0
出块周期起始时刻
T1
出块周期终止时刻

图1

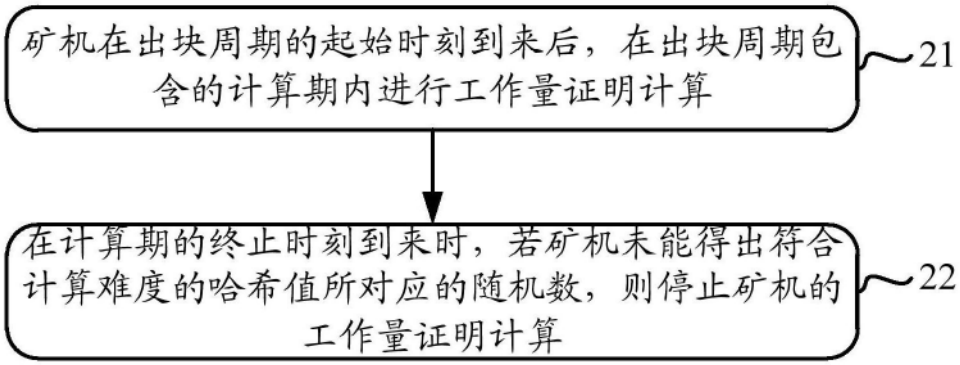

矿机在出块周期的起始时刻到来后，在出块周期包含的计算期内进行工作量证明计算
21
在计算期的终止时刻到来时，若矿机未能得出符合计算难度的哈希值所对应的随机数，则停止矿机的工作量证明计算
22

图2a

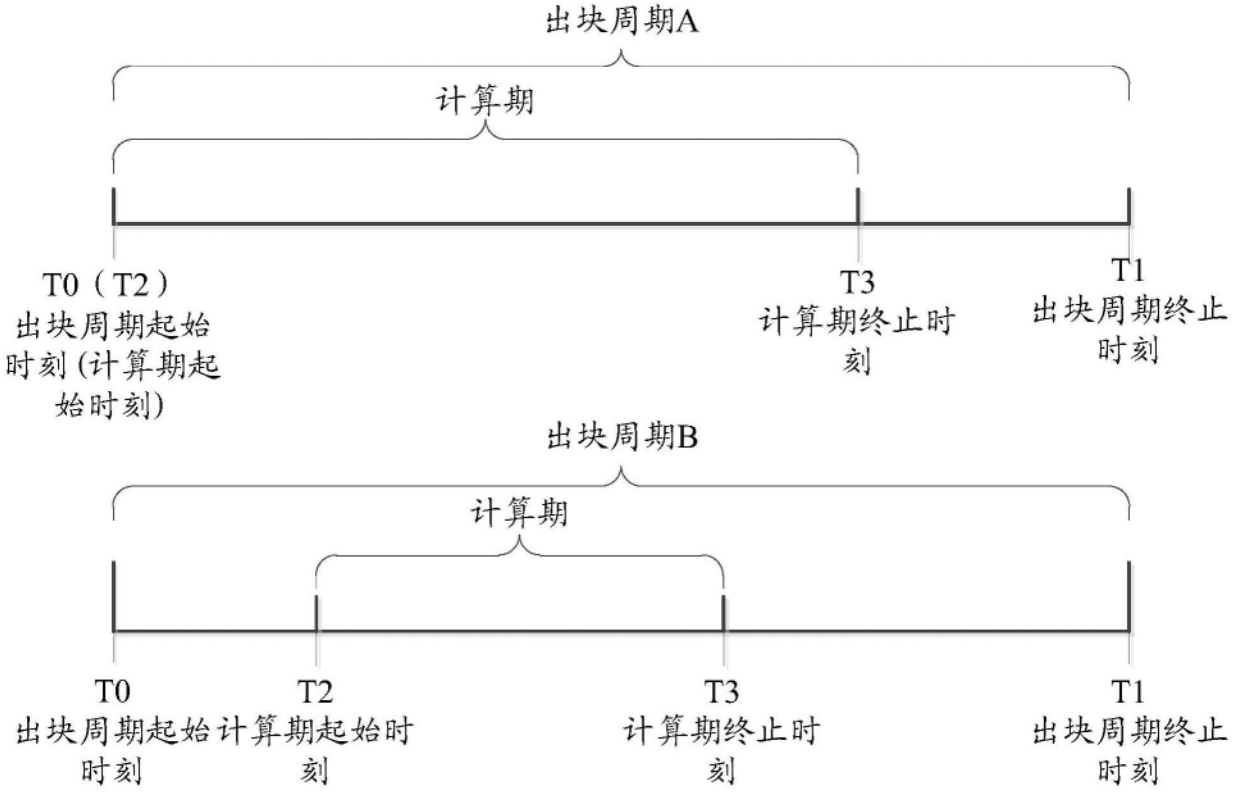

出块周期A
计算期
T0（T2）
出块周期起始时刻(计算期起始时刻)
T3
计算期终止时刻
T1
出块周期终止时刻
出块周期B
计算期
T0
出块周期起始时刻
T2
计算期起始时刻
T3
计算期终止时刻
T1
出块周期终止时刻

图2b

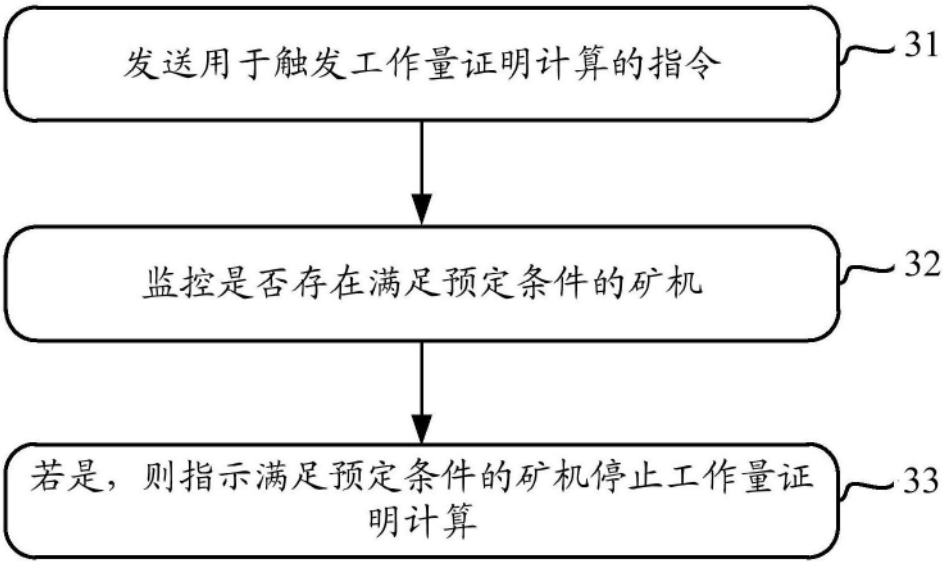

发送用于触发工作量证明计算的指令
31
监控是否存在满足预定条件的矿机
32
若是，则指示满足预定条件的矿机停止工作量证明计算
33

图3

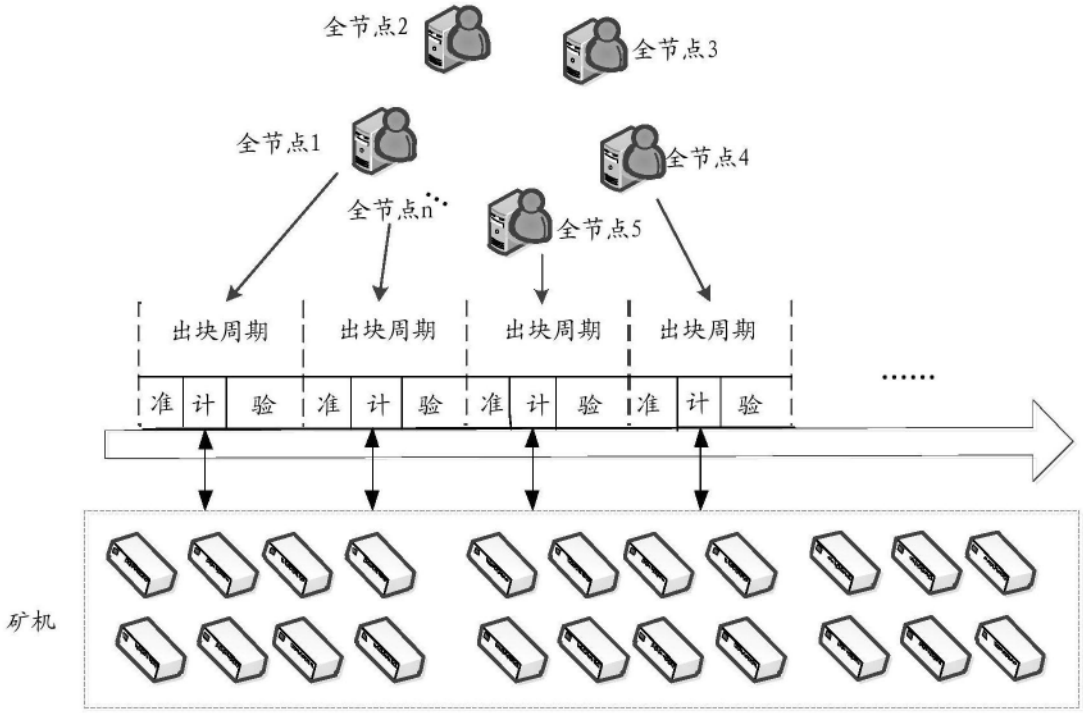

全节点2
全节点3
全节点1
全节点4
全节点n
全节点5
出块周期
出块周期
出块周期
出块周期
准
计
验
准
计
验
准
计
验
准
计
验
.....
矿机

图4a

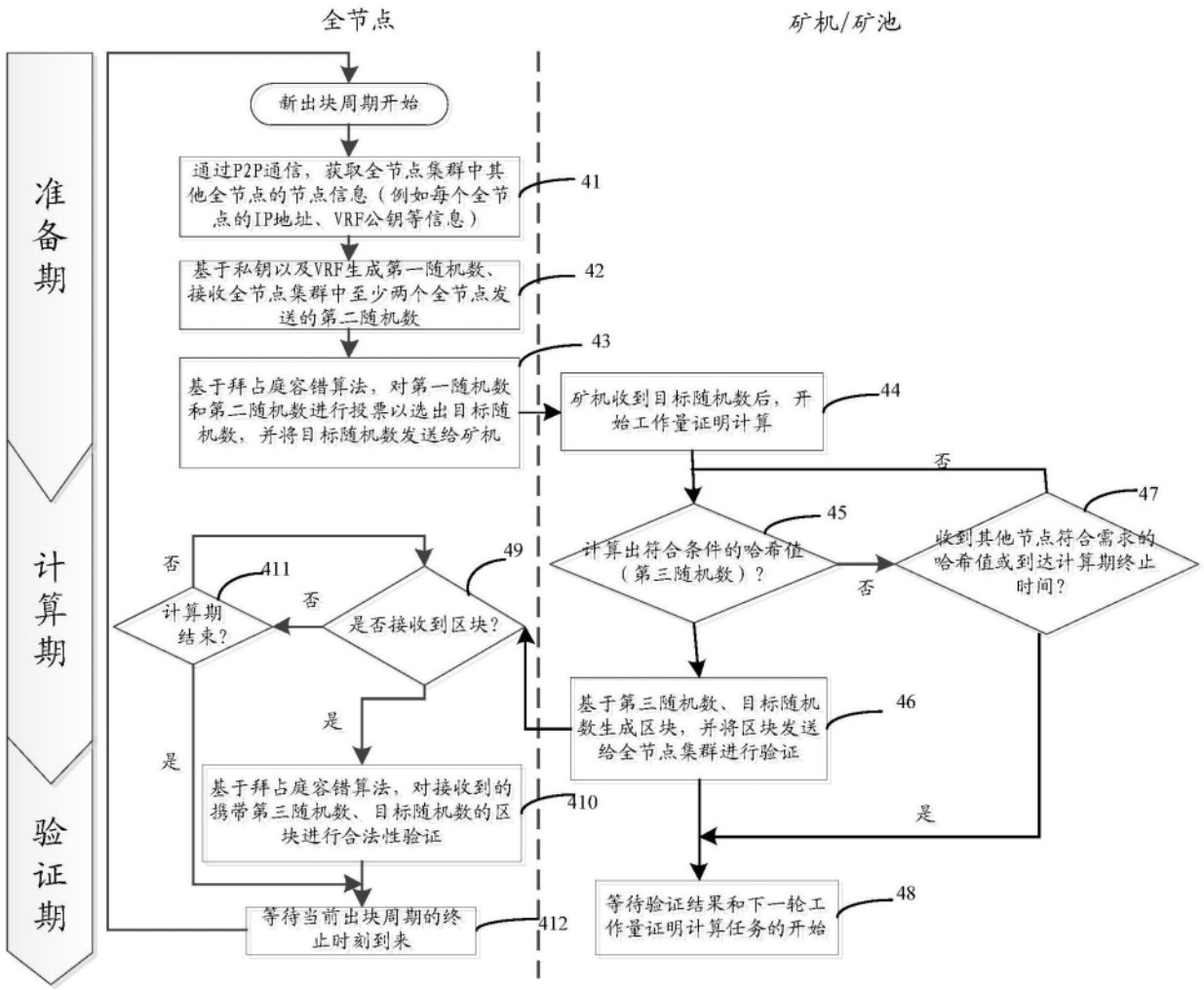

全节点
矿机/矿池
准备期
计算期
验证期
新出块周期开始
通过P2P通信，获取全节点集群中其他全节点的节点信息（例如每个全节点的IP地址、VRF公钥等信息）
41
基于私钥以及VRF生成第一随机数、接收全节点集群中至少两个全节点发送的第二随机数
42
基于拜占庭容错算法，对第一随机数和第二随机数进行投票以选出目标随机数，并将目标随机数发送给矿机
43
矿机收到目标随机数后，开始工作量证明计算
44
否
计算出符合条件的哈希值（第三随机数）？
45
否
收到其他节点符合需求的哈希值或到达计算期终止时间？
47
是
基于第三随机数、目标随机数生成区块，并将区块发送给全节点集群进行验证
46
否
是否接收到区块？
49
否
计算期结束？
411
是
基于拜占庭容错算法，对接收到的携带第三随机数、目标随机数的区块进行合法性验证
410
是
等待验证结果和下一轮工作量证明计算任务的开始
48
等待当前出块周期的终止时刻到来
412

图4b

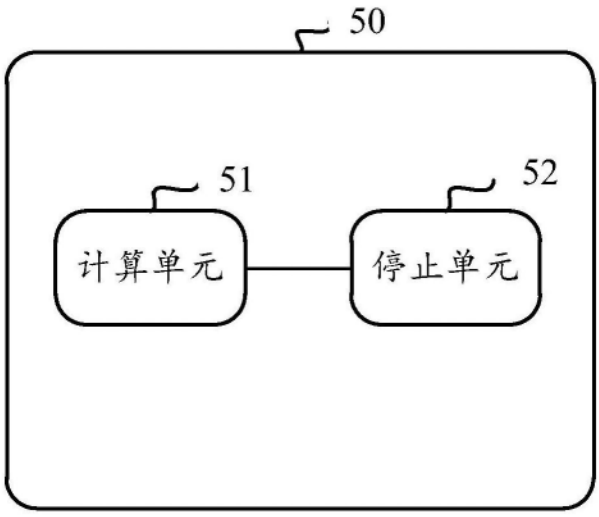

50
51
计算单元
52
停止单元

图5

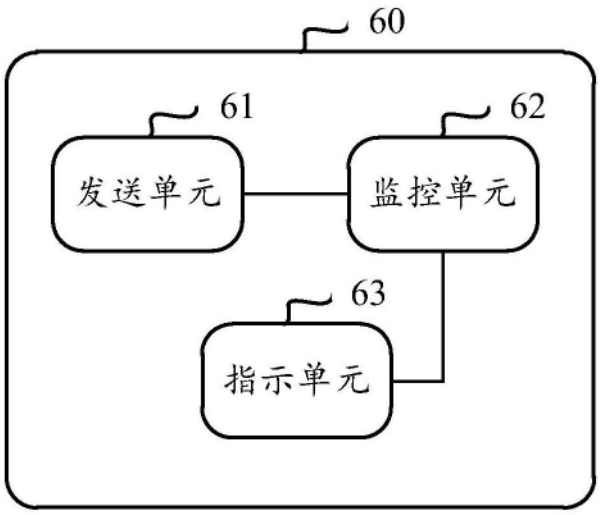

60
61
62
发送单元
监控单元
63
指示单元

图6

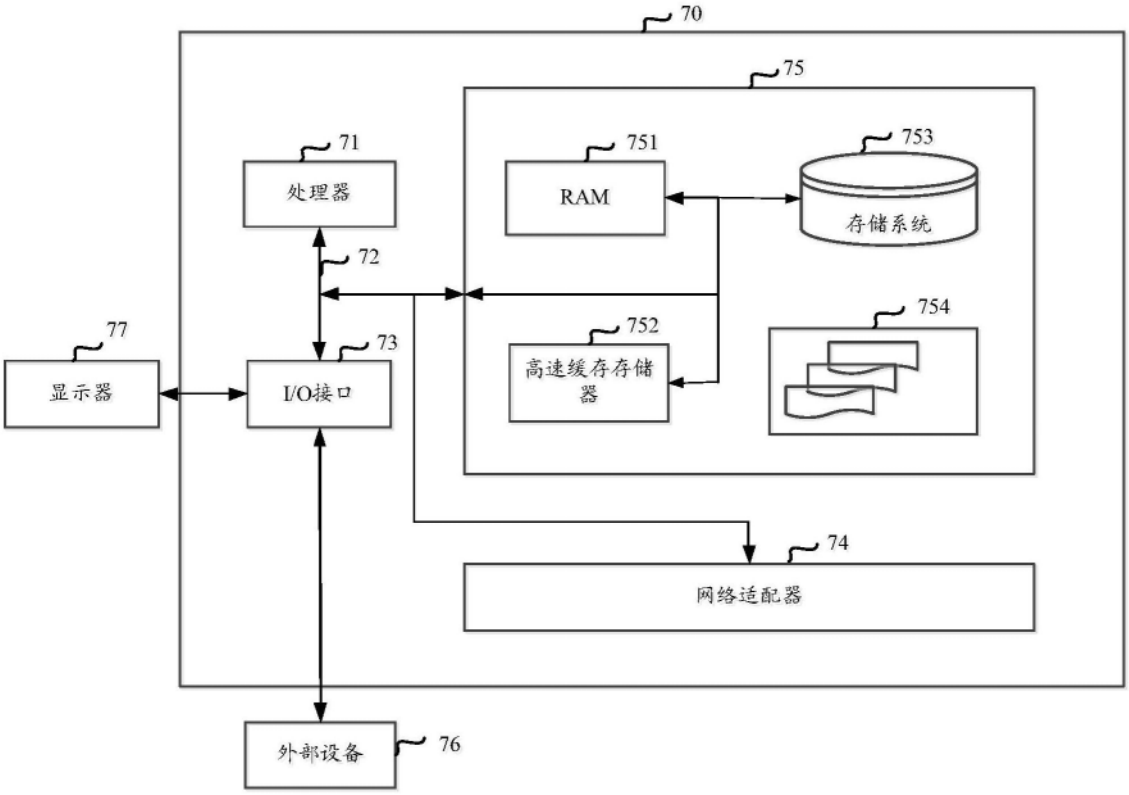

70
75
71
处理器
751
RAM
753
存储系统
72
77
73
显示器
I/O接口
752
高速缓存存储器
754
74
网络适配器
外部设备
76

图7