(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 106445711 A
(43)申请公布日 2017.02.22

(21)申请号 201610752879.4

(22)申请日 2016.08.28

(71)申请人 杭州云象网络技术有限公司
地址 310026 浙江省杭州市余杭区仓前街道龙潭路20号4幢475室

(72)发明人 黄步添 王云霄 王从礼 张维赛 毛道明 刘振广 石太彬

(74)专利代理机构 杭州天勤知识产权代理有限公司 33224
代理人 胡红娟

(51)Int.Cl.
G06F 11/07(2006.01)

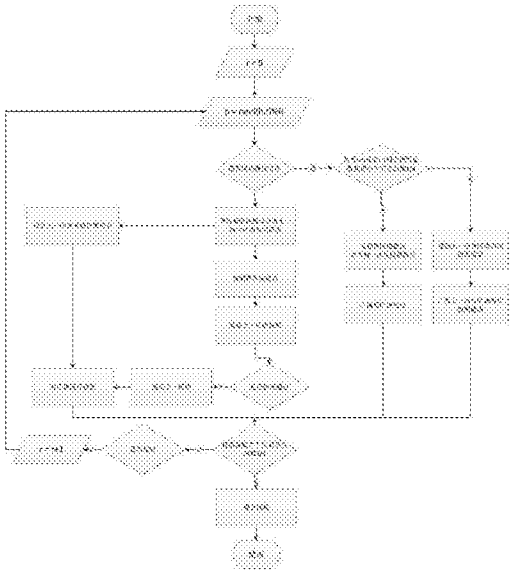
权利要求书2页 说明书4页 附图4页

(54)发明名称

一种应用于区块链的拜占庭容错共识方法

(57)摘要

本发明公开了一种应用于区块链的拜占庭容错共识方法，包括：在区块链创始块中指定一定数量的权益账号和初始共识账号；共识过程开始后，针对当前区块高度h，在共识账号名单中按照固定的随机算法选取一个共识账号发起新区块的提议；其他共识节点收到提议之后并对高度为h区块进行投票；在一段时间之内，如果投票数量超过η_1，表示形成一致共识，开始下一轮h+1高度的区块的共识；如果投票数量未超过η_1，但是超过η_2，表示有可能形成共识，广播上一轮区块的投票请求，继续等待一段时间；如果投票数量未超过η_2，该轮提议作废，重新进行新区块的提议。故本发明能够节省计算资源，可连续产生大量区块，避免了算力竞争。



CN 106445711 A

1.一种应用于区块链的拜占庭容错共识方法，其特征在于：

初始将一定数量的权益账号和共识账号分配给分布式系统中的节点；

各共识节点使用共识账号登录后参与每一区块加入区块链的共识过程，所述的共识节点即为分布式系统中拥有共识账号的节点；

对于当前区块加入区块链的共识过程，首先从共识节点中选举出一节点作为提名节点，由提名节点从交易池中选取若干条交易记录封装至当前区块中，进而发起关于当前区块加入区块链的提议，并向其他共识节点广播所述的提议同时对该提议进行投票，该提议中包含当前区块以及提名节点收到的关于前一区块加入区块链的所有最终轮投票结果信息；

其他共识节点收到所述的提议后，对该提议及其发起者的真实性、可靠性及合法性进行验证，验证通过后对该提议进行投票，验证不通过则忽视该提议；

在一定时间T内，当超过一定比例η_1的共识节点投票通过关于当前区块加入区块链的提议，则各共识节点对当前区块进行提交使其加入本地区块链末尾，并开始关于下一区块加入区块链的共识过程；

在一定时间T内，当超过一定比例η_2但未超过一定比例η_1的共识节点投票通过关于当前区块加入区块链的提议，则进入下一轮重新选举提名节点，由提名节点向其他共识节点广播其收到的关于上一轮的所有投票结果信息，进而使各共识节点对所述的提议重新进行投票，其中η_1和η_2均为实数且$0<\eta_2<\eta_1<1$；

在一定时间T内，未超过一定比例η_2的共识节点投票通过关于当前区块加入区块链的提议，则该提议作废且进入下一轮重新选举提名节点，由提名节点从交易池中重新选取若干条交易记录封装至当前区块中，进而发起关于当前区块加入区块链的新提议并向其他共识节点广播所述的新提议，该新提议中包含当前区块以及提名节点收到的关于前一区块加入区块链的所有最终轮投票结果信息，进而使各共识节点对所述的新提议进行投票。

2.根据权利要求1所述的拜占庭容错共识方法，其特征在于：初始化权益账号的数量大于等于1，共识账号的数量大于等于4。

3.根据权利要求1所述的拜占庭容错共识方法，其特征在于：各权益节点不定期地通过投票表决以增加或减少共识账号的数量；当超过一定比例的权益节点投票通过关于增加或减少共识账号的决议，则向所有节点发出关于增加或减少共识账号的请求，该请求中包含增加或减少共识账号后各共识账号的分配信息，所述的权益节点即为分布式系统中拥有权益账号的节点。

4.根据权利要求3所述的拜占庭容错共识方法，其特征在于：在共识过程中，若超过一定比例的共识节点收到权益节点发出的关于增加或减少共识账号的请求，各共识节点暂停共识过程并更新本地共识节点列表以完成共识节点的增减操作；当超过一定比例的共识节点完成共识节点的增减操作，各共识节点继续之前的共识过程。

5.根据权利要求1所述的拜占庭容错共识方法，其特征在于：从共识节点中选举出一节点作为提名节点的具体过程为：若当前共识节点个数为N，则为各共识节点按0,1,2,3,…,N-1进行编号，根据算式$p=rand(h,r)\%N$计算编号p，使编号为p的共识节点作为提名节点；其中rand(h,r)为自变量为h和r的随机函数，h为加入当前区块后区块链的长度，r为共识过程中的当前轮数，%为取余运算符。

6.根据权利要求1所述的拜占庭容错共识方法，其特征在于：若某一共识节点由于网络原因未收全其他共识节点对于前一区块加入区块链的最终轮投票结果信息从而导致其未完成对前一区块的提交，则该共识节点验证通过关于当前区块加入区块链的提议后，将该提议中附带的关于前一区块加入区块链的所有最终轮投票结果信息加入本地投票统计池中，进而对前一区块进行提交使其加入本地区块链末尾。

7.根据权利要求1所述的拜占庭容错共识方法，其特征在于：所述的一定时间T＝Tbase*C^r，其中r为共识过程中的当前轮数，Tbase和C均为预设的常量。

8.根据权利要求1所述的拜占庭容错共识方法，其特征在于：当任一共识节点对所述的提议投票后，则将其投票结果信息广播给其他共识节点，共识节点根据其收到的投票结果信息以决定是否对当前区块进行提交。

9.根据权利要求1所述的拜占庭容错共识方法，其特征在于：当任一共识节点完成对当前区块的提交后，则将其提交成功信息广播给其他共识节点。

10.根据权利要求4所述的拜占庭容错共识方法，其特征在于：当任一共识节点完成共识节点的增减操作后，则将其操作成功信息广播给其他共识节点。

一种应用于区块链的拜占庭容错共识方法

技术领域

[0001] 本发明属于区块链技术领域，具体涉及一种应用于区块链的拜占庭容错共识方法。

背景技术

[0002] 区块链(Blockchain)是比特币的一个重要概念，本质上是一个去中心化、不可篡改的分布式账本，同时作为比特币的底层技术。区块链是一串使用密码学方法相关联产生的区块，每一区块中包含了若干条比特币网络交易信息，用于验证其信息的有效性(防伪)和生成下一个区块。

[0003] 在相互不信任的前提下，需要对区块的有效性形成一致的共识。在实际使用过程中，数据传输面临着网络延时、网络丢包、黑客入侵等各种异常情况。针对这些异常情况，区块链需要有一种方法，当发生这些异常情况时，仍能够达成共识。

[0004] 传统区块链使用的共识方法是工作量证明，即每一个区块链中的区块都包含一个随机字符串，只有通过计算搜索到满足一定条件的字符串，区块才能生成并被加入区块链。工作量证明存在以下缺点：(1)浪费计算资源；(2)区块产生的时间无法确定，可能很快就产生新区块，也可能过很长时间才产生一个新区块；(3)算力强的节点能够对算力弱的节点产生算力攻击，造成区块链节点之间的算力竞争；(4)没有确定性，会产生分叉。

发明内容

[0005] 针对现有技术所存在的上述缺陷，本发明提供了一种应用于区块链的拜占庭容错共识方法，能够节省计算资源，避免了算力竞争。

[0006] 一种应用于区块链的拜占庭容错共识方法，如下：

[0007] 初始将一定数量的权益账号和共识账号分配给分布式系统中的节点；

[0008] 各共识节点使用共识账号登录后参与每一区块加入区块链的共识过程，所述的共识节点即为分布式系统中拥有共识账号的节点；

[0009] 对于当前区块加入区块链的共识过程，首先从共识节点中选举出一节点作为提名节点，由提名节点从交易池中选取若干条交易记录封装至当前区块中，进而发起关于当前区块加入区块链的提议，并向其他共识节点广播所述的提议同时对该提议进行投票，该提议中包含当前区块以及提名节点收到的关于前一区块加入区块链的所有最终轮投票结果信息；

[0010] 其他共识节点收到所述的提议后，对该提议及其发起者的真实性、可靠性及合法性进行验证，验证通过后对该提议进行投票，验证不通过则忽视该提议；

[0011] 在一定时间T内，当超过一定比例η_1的共识节点投票通过关于当前区块加入区块链的提议，则各共识节点对当前区块进行提交使其加入本地区块链末尾，并开始关于下一区块加入区块链的共识过程；

[0012] 在一定时间T内，当超过一定比例η_2但未超过一定比例η_1的共识节点投票通过关于

当前区块加入区块链的提议，则进入下一轮重新选举提名节点，由提名节点向其他共识节点广播其收到的关于上一轮的所有投票结果信息，进而使各共识节点对所述的提议重新进行投票，其中η_1和η_2均为实数且$0<\eta_2<\eta_1<1$；

[0013] 在一定时间T内，未超过一定比例η_2的共识节点投票通过关于当前区块加入区块链的提议，则该提议作废且进入下一轮重新选举提名节点，由提名节点从交易池中重新选取若干条交易记录封装至当前区块中，进而发起关于当前区块加入区块链的新提议并向其他共识节点广播所述的新提议，该新提议中包含当前区块以及提名节点收到的关于前一区块加入区块链的所有最终轮投票结果信息，进而使各共识节点对所述的新提议进行投票。

[0014] 进一步地，初始化权益账号的数量大于等于1，共识账号的数量大于等于4。

[0015] 进一步地，各权益节点不定期地通过投票表决以增加或减少共识账号的数量；当超过一定比例的权益节点投票通过关于增加或减少共识账号的决议，则向所有节点发出关于增加或减少共识账号的请求，该请求中包含增加或减少共识账号后各共识账号的分配信息，所述的权益节点即为分布式系统中拥有权益账号的节点。

[0016] 进一步地，在共识过程中，若超过一定比例的共识节点收到权益节点发出的关于增加或减少共识账号的请求，各共识节点暂停共识过程并更新本地共识节点列表以完成共识节点的增减操作；当超过一定比例的共识节点完成共识节点的增减操作，各共识节点继续之前的共识过程。

[0017] 进一步地，从共识节点中选举出一节点作为提名节点的具体过程为：若当前共识节点个数为N，则为各共识节点按0,1,2,3,…,N-1进行编号，根据算式$p=rand(h,r)\%N$计算编号p，使编号为p的共识节点作为提名节点；其中rand(h,r)为自变量为h和r的随机函数，h为加入当前区块后区块链的长度，r为共识过程中的当前轮数，%为取余运算符。

[0018] 进一步地，若某一共识节点由于网络原因未收全其他共识节点对于前一区块加入区块链的最终轮投票结果信息从而导致其未完成对前一区块的提交，则该共识节点验证通过关于当前区块加入区块链的提议后，将该提议中附带的关于前一区块加入区块链的所有最终轮投票结果信息加入本地投票统计池中，进而对前一区块进行提交使其加入本地区块链末尾。

[0019] 进一步地，所述的一定时间$T=Tbase*C^r$，其中r为共识过程中的当前轮数，Tbase和C均为预设的常量。

[0020] 进一步地，当任一共识节点对所述的提议投票后，则将其投票结果信息广播给其他共识节点，共识节点根据其收到的投票结果信息以决定是否对当前区块进行提交；当任一共识节点完成对当前区块的提交后，则将其提交成功信息广播给其他共识节点；当任一共识节点完成共识节点的增减操作后，则将其操作成功信息广播给其他共识节点。

[0021] 本发明的有益技术效果如下：

[0022] 1.节省计算资源。

[0023] 2.可连续产生区块，短时间内可以产生大量区块，在没有交易的情形下不产生区块。

[0024] 3.只有授权节点才参与共识过程，避免了算力竞争。

[0025] 4.具有确定性，区块一旦确定即是最终状态。

附图说明

[0026] 图1为本发明共识过程的流程示意图。

[0027] 图2为本发明共识过程中的状态转移示意图。

[0028] 图3为本发明共识节点增减操作的流程示意图。

[0029] 图4为本发明共识节点增减操作的状态转移示意图。

具体实施方式

[0030] 为了更为具体地描述本发明，下面结合附图及具体实施方式对本发明的技术方案进行详细说明。

[0031] 本发明应用于区块链的拜占庭容错共识方法，具体过程如下：

[0032] 首先，在区块链创始块中指定数量为M的权益账号和数量为N的初始共识账号，M>=1，N>=4；本实施方式在区块链创始块中指定3个权益账号(记为Q1，Q2，Q3)和4个初始共识账号(记为G1，G2，G3，G4)。

[0033] 每一个参与共识的节点使用共识账号登录，本实施方式有4个节点参与共识，分别用G1，G2，G3，G4登录。共识节点之间的通信采用P2P对等网络，共识节点在后续提出新区块的提议、对区块进行投票，需要使用共识账号的私钥对提议、投票进行签名，从而解决共识节点的身份认证问题。

[0034] 如图1所示，共识过程开始，当前区块高度h为1000，当前回合r为0。高度为0～999的区块已完成共识。节点G1，G2，G3，G4分别用随机算法公式p=rand(h，r)%N计算高度为1000回合为0的区块提名节点，p=rand(1000，0)%4，假设p计算后的结果是1。因为p可能的结果是0，1，2，3，分别对应G1，G2，G3，G4。因此p=1代表区块提名节点为G2。因为G1，G2，G3，G4各自计算了区块提名节点，当有非诚实节点企图对高度为1000，回合为0的区块产生提名时，其余所有诚实节点都将拒绝非诚实节点的提名。G2节点选择交易池中符合条件的交易，同时附带上高度为999区块的投票信息，发起并广播新区块的提议BlockProposal[1000]，同时，G2对新区块提议BlockProposal[1000]进行投票。

[0035] 其他节点收到BlockProposal[1000]之后，首先验证提名节点是否是G2，如果不是G2，则忽略BlockProposal[1000]；接着对其包含的高度为999的区块的投票信息进行验证，如果验证不通过，忽略BlockProposal[1000]；然后对BlockProposal[1000]中包含的交易进行验证，验证其中的交易是否都是正确合法的交易。BlockProposal[1000]验证通过之后，如果有节点尚未提交区块高度为999的区块(由于网络原因导致未收到部分高度为999区块投票)，将BlockProposal[1000]附带的投票加入到高度为999的投票统计池中，并提交高度为999的区块。然后节点对BlockProposal[1000]进行投票，并将投票广播给其他的节点。

[0036] 每个节点各自记录所有节点的投票信息。如图2所示，在T=3秒(T=Tbase*C^r，令Tbase=3，C=1.5，r=0)之内，如果有3个及以上节点(超过N*η_1)对BlockProposal[1000]进行了投票，整个区块链网络对高度为1000的区块提名达成了共识，各个节点通过BlockProposal[1000]生成第1000号区块，并提交到本地区块链数据库中，之后开始高度为1001的区块共识过程。

[0037] 如果在3秒之内，有2个节点(未超过$N*\eta_1$，但是超过$N*\eta_2$)对BlockProposal[1000]进行投票，表示有可能形成共识，则进入下一回合r＝1。计算高度为1000回合为1的区块提名人，p＝rand(1000,1)％4，假设p的计算结果是G3，则G3广播上一回合的投票提名，请求各节点再次进行投票。如果在T＝4.5秒(T＝Tbase*C^r，令Tbase＝3，C＝1.5，r＝1)之内，有超过3个节点进行了投票，则表示达成共识，提交第1000号区块，开始高度为1001区块的共识过程；否则按投票数量进行再次投票的请求或者重新进行高度为1000区块的提名。

[0038] 如果在3秒之内，只有2个以下节点(未超过$N*\eta_2$)对BlockProposal[1000]进行投票，该轮回合提议作废，则进入下一回合r＝1。计算高度为1000回合为1的区块提名人，p＝rand(1000,1)％4，按照上一步骤的假设，p的计算结果是G3。G3发现BlockProposal[1000]的投票未超过$N*\eta_2$，忽略BlockProposal[1000]，重新生成新的区块提名BlockProposal[1000]*。G3节点重新选择交易池中符合条件的交易，同时附带上高度为999区块的投票信息，发起并广播新区块的提议BlockProposal[1000]*。同时，G3对新区块提议BlockProposal[1000]*进行投票。

[0039] 我们假设整个区块链网络中的诚实节点的数量是超过$N*\eta_1$的，在合理的网络状况下，总是能够达成区块的共识。

[0040] 此外，权益账号可通过投票动态增加/减少共识账号；当投票数量大于$M*\eta_1$，表明投票通过增加/减少共识账号。如图3所示，在进行高度为1500区块的共识过程中，超过半数的权益账号发出增加共识节点的请求，各个记账节点广播自己收到增加节点请求，并统计其他节点收到增加节点请求的情况。一旦有超过$N*\eta_1$个节点表明自己收到增加节点请求，各个节点暂停共识过程，在本地的共识节点列表中增加新的共识节点账号，然后广播自己已完成增加节点操作，并统计其他节点是否完成增加节点操作；当有超过$N*\eta_1$个节点表明自己已完成增加节点操作，各个节点重新开始高度为1500的共识过程，如图4所示。减少共识节点的操作与增加共识节点的操作类似。

[0041] 本实施方式中，设定$\eta_1＝2/3$，$\eta_2＝1/3$。

[0042] 上述对实施例的描述是为便于本技术领域的普通技术人员能理解和应用本发明。熟悉本领域技术的人员显然可以容易地对上述实施例做出各种修改，并把在此说明的一般原理应用到其他实施例中而不必经过创造性的劳动。因此，本发明不限于上述实施例，本领域技术人员根据本发明的揭示，对于本发明做出的改进和修改都应该在本发明的保护范围之内。

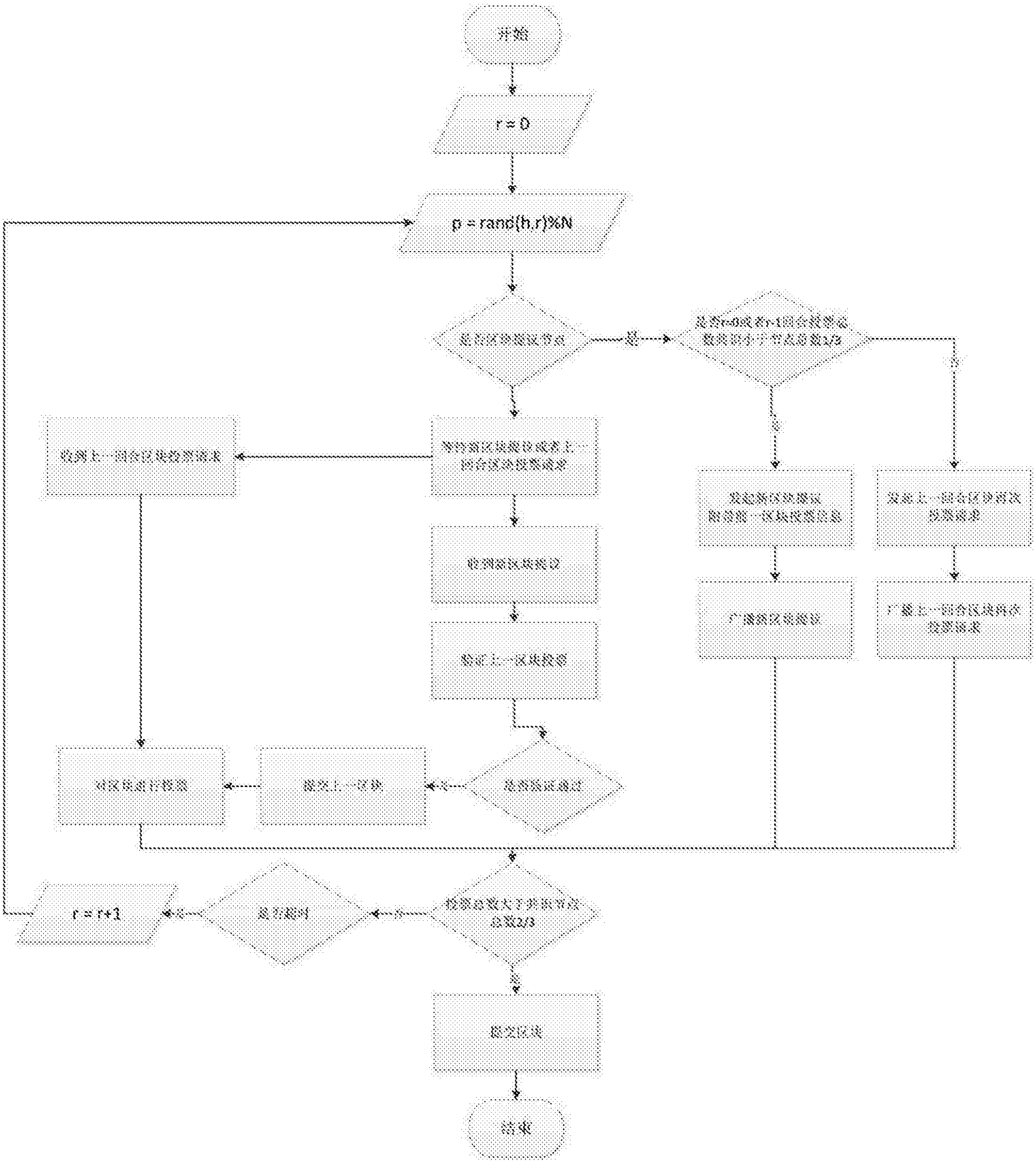


图1

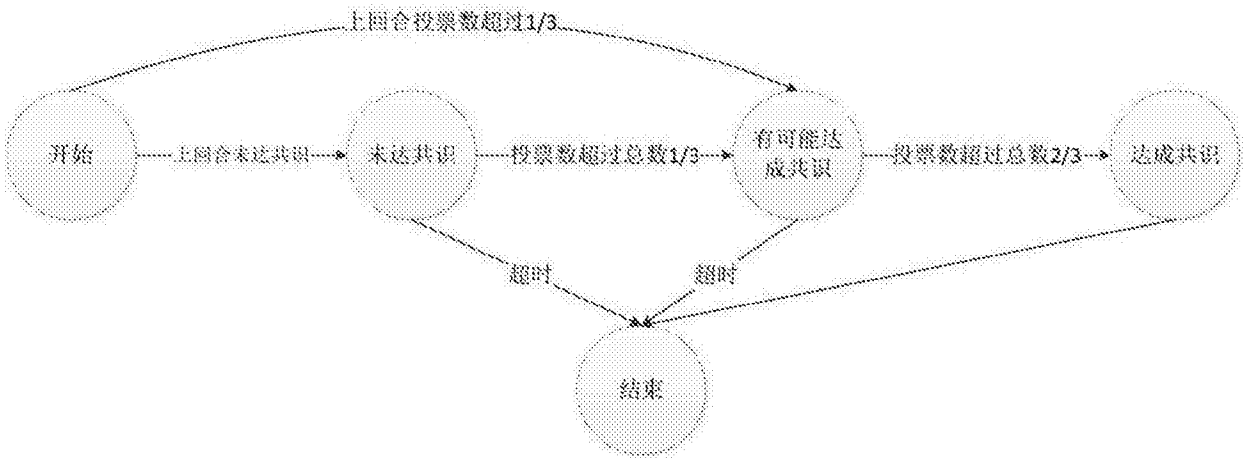

上回合投票数超过1/3
开始
上回合未达共识
未达共识
投票数超过总数1/3
有可能达成共识
投票数超过总数2/3
达成共识
超时
超时
结束

图2

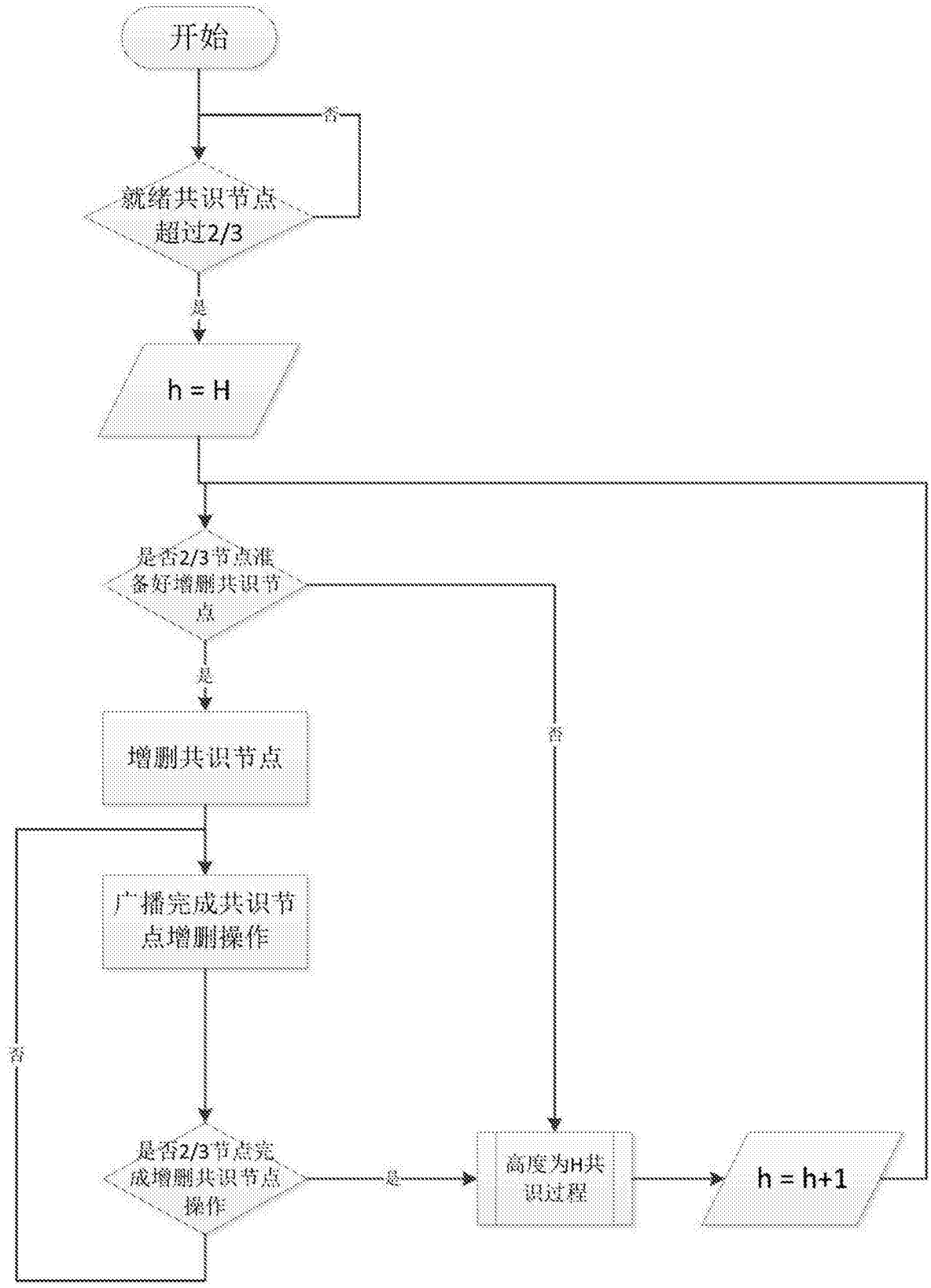

开始
否
就绪共识节点超过2/3
是
h = H
是否2/3节点准备好增删共识节点
是
否
增删共识节点
广播完成共识节点增删操作
否
是否2/3节点完成增删共识节点操作
是
高度为H共识过程
h = h+1

图3

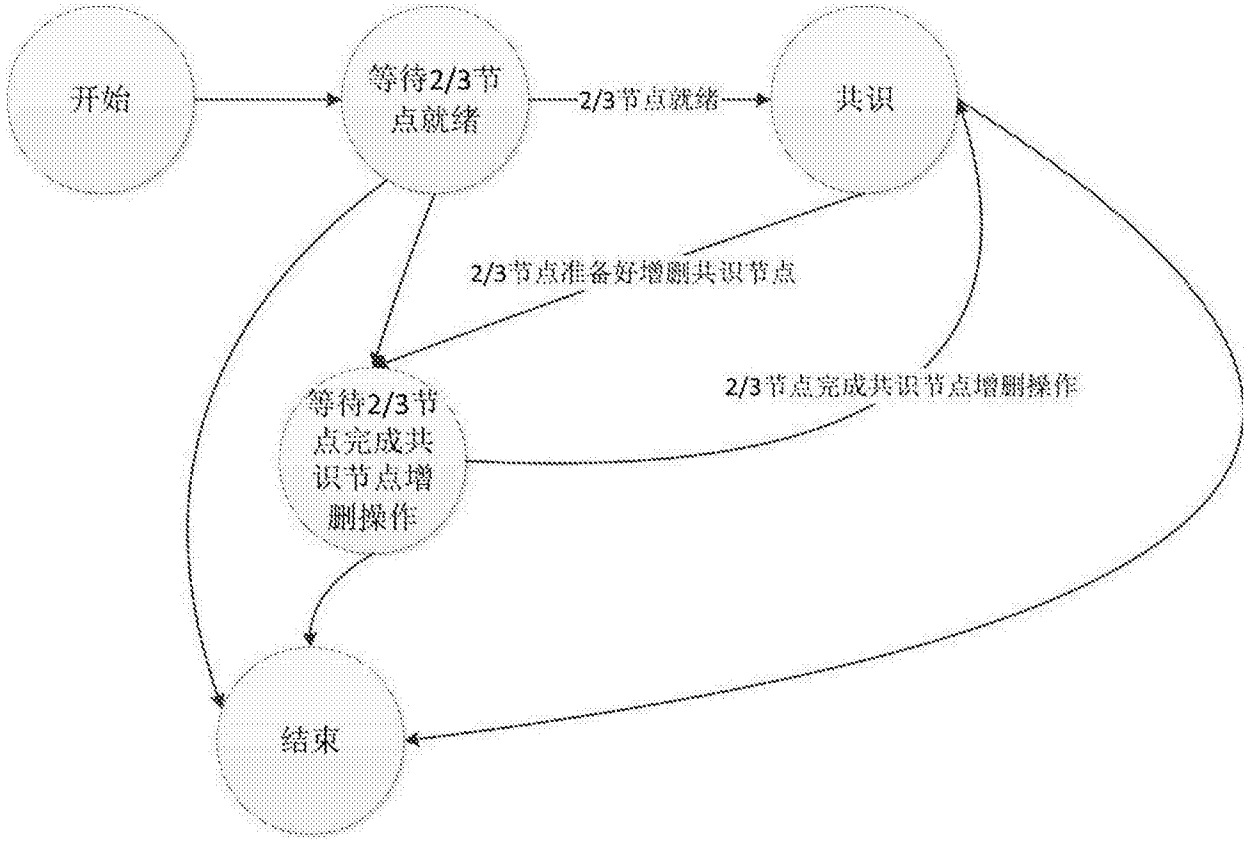

开始
等待2/3节点就绪
2/3节点就绪
共识
2/3节点准备好增删共识节点
等待2/3节点完成共识节点增删操作
2/3节点完成共识节点增删操作
结束

图4