(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108648076 B
(45)授权公告日 2021.03.19

(21)申请号 201810356600.X

(22)申请日 2018.04.19

(65)同一申请的已公布的文献号
申请公布号 CN 108648076 A

(43)申请公布日 2018.10.12

(73)专利权人 上海分布信息科技有限公司
地址 200082 上海市杨浦区政学路88号创智天地企业中心5号楼301

(72)发明人 丛宏雷 胡凝

(74)专利代理机构 上海恒锐佳知识产权代理事务所(普通合伙) 31286
代理人 黄海霞

(51)Int.Cl.
G06Q 40/04(2012.01)

(56)对比文件
CN 106952124 A,2017.07.14
CN 107194666 A,2017.09.22
CN 107292735 A,2017.10.24
CN 107341660 A,2017.11.10
CN 107423962 A,2017.12.01
US 2016300234 A1,2016.10.13
US 2016164884 A1,2016.06.09
王晓光.区块链技术共识算法综述.《信息与电脑》.2017,全文.
张永,李晓辉.一种改进的区块链共识机制的研究与实现.《电子设计工程》.2018,全文.

审查员 吕源

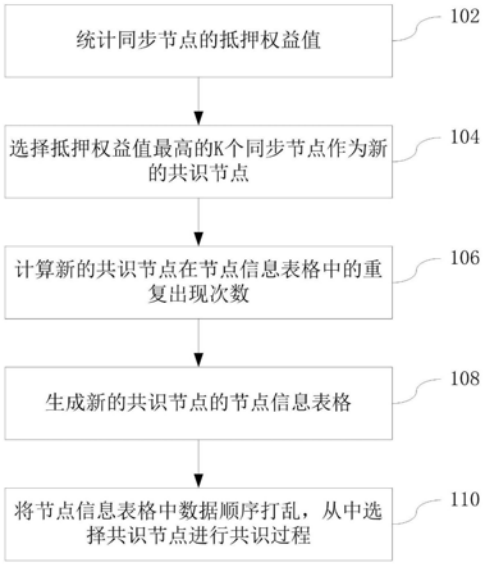
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种选举共识节点及生成节点信息表格的方法及系统

(57)摘要

本申请公开了一种选举共识节点及生成节点信息表格的方法,包括:统计步骤:统计每个同步节点的抵押权益值。选举步骤:选择抵押权益值最高的同步节点成为新的共识节点。计算步骤:计算每个新的共识节点在节点信息表格中重复出现的次数,其与节点的抵押权益值正相关。表格生成步骤:生成新的共识节点的节点信息表格。乱序步骤:将节点信息表格中的数据顺序打乱,形成最终的新的共识节点的节点信息表格用于从中选择共识节点参与共识过程。本申请还公开了一种选举共识节点及生成节点信息表格的系统。本申请可以让具有较高抵押权益值的共识节点较多地参与到共识过程中,这些节点是值得信赖的,因而降低了共识算法出现拜占庭错误的几率。



CN 108648076 B

1.一种选举共识节点及生成节点信息表格的方法,其特征是,包括如下步骤:

统计步骤:统计每个同步节点的抵押权益值;

选举步骤:从所有同步节点中选择抵押权益值最高、且与共识节点的数量相同的同步节点成为新的共识节点;如果所有同步节点中抵押权益值大于零的节点数量小于共识节点的数量,那么选举失败,由现有的共识节点在新的一个周期内再次担任共识节点,等待下一周期选举新的共识节点;

计算步骤:根据每个新的共识节点的抵押权益值以及节点信息表格的长度计算每个新的共识节点在节点信息表格中重复出现的次数;抵押权益值越高的新的共识节点,在节点信息表格中出现的次数就越多;抵押权益值越低的新的共识节点,在节点信息表格中出现的次数就越少;

表格生成步骤:生成新的共识节点的节点信息表格,并将新的共识节点按照重复出现的次数加入到所生成的节点信息表格中;

乱序步骤:将节点信息表格中的数据顺序打乱,形成最终的新的共识节点的节点信息表格用于从中选择共识节点参与共识过程。

2.根据权利要求1所述的选举共识节点及生成节点信息表格的方法,其特征是,所述计算步骤中,让每个新的共识节点在节点信息表格中重复出现的次数与其抵押权益值成正比。

3.根据权利要求1所述的选举共识节点及生成节点信息表格的方法,其特征是,所述乱序步骤中,采用随机算法打乱表格中的数据顺序。

4.根据权利要求1所述的选举共识节点及生成节点信息表格的方法,其特征是,在所述统计步骤之前还包括集合步骤:将多个物理同步节点组成一个虚拟同步节点;

所述统计步骤中,虚拟同步节点的抵押权益值是组成该虚拟同步节点的所有物理同步节点的抵押权益值之和;

所述统计步骤、计算步骤、表格生成步骤、乱序步骤中,均将虚拟同步节点作为一个同步节点对待,如选举为共识节点则作为一个共识节点对待。

5.一种选举共识节点及生成节点信息表格的系统,其特征是,包括统计单元、选举单元、计算单元、表格生成单元、乱序单元;

所述统计单元用来统计每个同步节点的抵押权益值;

所述选举单元用来从所有同步节点中选择抵押权益值最高的、且与共识节点的数量相同的同步节点成为新的共识节点;所述选举单元还在所有同步节点中抵押权益值大于零的节点数量小于共识节点的数量时放弃本次选举共识节点,而由现有的共识节点在新的一个周期内再次担任共识节点,等待下一周期选举新的共识节点;

所述计算单元用来根据每个新的共识节点的抵押权益值以及节点信息表格的长度计算每个新的共识节点在节点信息表格中重复出现的次数;抵押权益值越高的新的共识节点,在节点信息表格中出现的次数就越多;抵押权益值越低的新的共识节点,在节点信息表格中出现的次数就越少;

所述表格生成单元用来生成新的共识节点的节点信息表格,并将新的共识节点按照重复出现的次数加入到所生成的节点信息表格中;

所述乱序单元用来将节点信息表格中的数据顺序打乱,形成最终的新的共识节点的节

点信息表格用于从中选择共识节点参与共识过程。

6.根据权利要求5所述的选举共识节点及生成节点信息表格的系统，其特征是，所述计算单元还让每个新的共识节点在节点信息表格中重复出现的次数与其抵押权益值成正比。

7.根据权利要求5所述的选举共识节点及生成节点信息表格的系统，其特征是，所述乱序单元还采用随机算法打乱表格中的数据顺序。

8.根据权利要求5所述的选举共识节点及生成节点信息表格的系统，其特征是，还包括集合单元；

所述集合单元用来将多个物理同步节点组成一个虚拟同步节点；

所述统计单元将组成虚拟同步节点的所有物理同步节点的抵押权益值之和作为该虚拟同步节点的抵押权益值；

所述统计单元、计算单元、表格生成单元、乱序单元均将虚拟同步节点作为一个同步节点对待，如选举为共识节点则作为一个共识节点对待。

一种选举共识节点及生成节点信息表格的方法及系统

技术领域

[0001] 本申请涉及一种区块链(Blockchain)网络中的共识机制(consensus mechanism),特别是涉及其中共识节点的选择方法。

背景技术

[0002] 2016年10月18日工业和信息化部发布的《中国区块链技术和应用发展白皮书》中,将区块链定义为一种无须中介参与、亦能在互不信任或弱信任的参与者之间维系一套不可篡改的账本记录的技术。首先,区块链是一种以区块(block)为单位的链(chain)状数据结构,每一个区块都与前续区块通过密码学证明的方式链接在一起。其次,区块链是一种全网共享的分布式账本(distributed ledger)。许多场景中,区块链与分布式账本这两个技术术语具有相同含义。

[0003] 典型地,区块链技术被P2P网络(peer-to-peer network)的全部或部分节点用来根据某种共识算法验证新的区块,通过验证的新区块被新增到区块链数据结构的末尾。采用区块链技术的P2P网络就被称为区块链网络。共识是指多方参与的节点在预设规则下,通过多个节点交互对某些数据、行为或流程达成一致的过程。共识机制是定义共识过程的算法、协议和规则。

[0004] 常用的共识算法包括权益证明(proof-of-stake,PoS)算法、委托权益证明(delegated proof-of-stake,DPoS)算法等。

[0005] 权益证明算法的主要思想是节点记账权的获得难度与节点持有的权益成反比,即节点持有的权益越高则越容易获得记账权,反之亦然。所述记账权主要是指在每一轮共识过程中提出新的备选区块的权限。

[0006] 委托权益证明算法的主要思想是从全部节点中选举产生若干见证人(witness),仅有见证人有记账权。所述记账权也主要是指在每一轮共识过程中提出新的备选区块的权限。

[0007] 在区块链网络的每一轮共识过程中,新的备选区块被提出后还需要进行检查验证,才能最终确认为完成共识的区块。在检查、验证、确认的过程中,无法杜绝拜占庭节点即出错或作恶的节点的参与,因此有可能导致拜占庭错误(Byzantine failure)即共识失败。

发明内容

[0008] 本申请所要解决的技术问题是提供一种在委托权益证明算法中选举共识节点及生成节点信息表格的方法,可以减小出现拜占庭错误的概率。为此,本申请还要提供一种在委托权益证明算法中选举共识节点及生成节点信息表格的系统。

[0009] 为解决上述技术问题,本申请提供了一种选举共识节点及生成节点信息表格的方法,包括如下步骤。统计步骤:统计每个同步节点的抵押权益值。选举步骤:从所有同步节点中选择抵押权益值最高、且与共识节点的数量相同的同步节点成为新的共识节点,如果所有同步节点中抵押权益值大于零的节点数量小于共识节点的数量,那么选举失败,由现有

的共识节点在新的一个周期内再次担任共识节点，等待下一周期选举新的共识节点。计算步骤：根据每个新的共识节点的抵押权益值以及节点信息表格的长度计算每个新的共识节点在节点信息表格中重复出现的次数；抵押权益值越高的新的共识节点，在节点信息表格中出现的次数就越多；抵押权益值越低的新的共识节点，在节点信息表格中出现的次数就越少。表格生成步骤：生成新的共识节点的节点信息表格，并将新的共识节点按照重复出现的次数加入到所生成的节点信息表格中。乱序步骤：将节点信息表格中的数据顺序打乱，形成最终的新的共识节点的节点信息表格用于从中选择共识节点参与共识过程。

[0010] 这样可以避免没有抵押权益值的节点成为共识节点，从而避免没有抵押权益值的节点参与共识过程。没有抵押权益值的节点是不值得信赖的，如参与共识过程可能会增加共识算法出现拜占庭错误的几率。

[0011] 优选地，所述计算步骤中，让每个新的共识节点在节点信息表格中重复出现的次数与其抵押权益值成正比。这提供了一种计算方法的具体实现方式。

[0012] 优选地，所述乱序步骤中，采用随机算法打乱表格中的数据顺序。例如采用费雪耶兹随机置乱(Fisher-Yates Shuffle，也称费雪耶兹洗牌)算法打乱表格中的数据顺序。这提供了一种乱序方法的具体实现方式。

[0013] 进一步地，所述选举共识节点及生成节点信息表格的方法在统计步骤之前还包括集合步骤：将多个物理同步节点组成一个虚拟同步节点。所述统计步骤中，虚拟同步节点的抵押权益值是组成该虚拟同步节点的所有物理同步节点的抵押权益值之和。所述统计步骤、计算步骤、表格生成步骤、乱序步骤中，均将虚拟同步节点作为一个同步节点对待，如选举为共识节点则作为一个共识节点对待。这样可以提高同步节点的运算能力，如选举为共识节点后也能提高共识节点的运算能力，从而提高共识过程的运算效率，缩短共识过程所需时间。

[0014] 为解决上述技术问题，本申请还提供了一种选举共识节点及生成节点信息表格的系统，包括统计单元、选举单元、计算单元、表格生成单元、乱序单元。所述统计单元用来统计每个同步节点的抵押权益值。所述选举单元用来从所有同步节点中选择抵押权益值最高的、且与共识节点的数量相同的同步节点成为新的共识节点，所述选举单元还在所有同步节点中抵押权益值大于零的节点数量小于共识节点的数量时放弃本次选举共识节点，而由现有的共识节点在新的一个周期内再次担任共识节点，等待下一周期选举新的共识节点。所述计算单元用来根据每个新的共识节点的抵押权益值以及节点信息表格的长度计算每个新的共识节点在节点信息表格中重复出现的次数；抵押权益值越高的新的共识节点，在节点信息表格中出现的次数就越多；抵押权益值越低的新的共识节点，在节点信息表格中出现的次数就越少。所述表格生成单元用来生成新的共识节点的节点信息表格，并将新的共识节点按照重复出现的次数加入到所生成的节点信息表格中。所述乱序单元用来将节点信息表格中的数据顺序打乱，形成最终的新的共识节点的节点信息表格用于从中选择共识节点参与共识过程。

[0015] 这样可以避免没有抵押权益值的节点成为共识节点，从而避免没有抵押权益值的节点参与共识过程。没有抵押权益值的节点是不值得信赖的，如参与共识过程可能会增加共识算法出现拜占庭错误的几率。

[0016] 优选地，所述计算单元还让每个新的共识节点在节点信息表格中重复出现的次数

与其抵押权益值成正比。这提供了一种计算方法的具体实现方式。

[0017] 优选地，所述乱序单元还采用随机算法打乱表格中的数据顺序。例如采用费雪耶兹随机置乱算法打乱表格中的数据顺序。这提供了一种乱序方法的具体实现方式。

[0018] 进一步地，所述选举共识节点及生成节点信息表格的系统还包括集合单元。所述集合单元用来将多个物理同步节点组成一个虚拟同步节点。所述统计单元将组成虚拟同步节点的所有物理同步节点的抵押权益值之和作为该虚拟同步节点的抵押权益值。所述统计单元、计算单元、表格生成单元、乱序单元均将虚拟同步节点作为一个同步节点对待，如选举为共识节点则作为一个共识节点对待。这样可以提高同步节点的运算能力，如选举为共识节点后也能提高共识节点的运算能力，从而提高共识过程的运算效率，缩短共识过程所需时间。

[0019] 本申请提供了一种选举共识节点及生成节点信息表格的方法及系统，通过设置每一周期新的共识节点生成节点信息表格，可以让具有较高的抵押权益值的共识节点较多地参与到共识过程中，这些节点是值得信赖的，因而降低了共识算法出现拜占庭错误的几率。

附图说明

[0020] 图1是本申请的选举共识节点及生成节点信息表格的方法的实施例一的流程示意图。

[0021] 图2是本申请的选举共识节点及生成节点信息表格的方法的实施例二的流程示意图。

具体实施方式

[0022] 本申请适用的区块链网络中，全部节点根据是否参与共识可以分为两大类，参与共识的节点称为共识节点，不参与共识的节点称为非共识节点。

[0023] 所述共识节点用来对区块链网络中的数据、行为或流程进行共识，将完成共识的数据生成为区块，还将完成共识的区块分发给同步节点。共识节点还维护区块链网络的分布式账本，即在自身保存的区块链数据结构中添加并保存完成共识的区块。

[0024] 所述非共识节点用来对共识节点进行状态监控，对完成共识的区块进行验证，并协助仲裁管理共识节点。非共识节点主要包括同步节点。同步节点不参与共识，但保持与共识节点相同的同步状态。当共识节点达成一轮新的共识以后，就会将完成共识的区块分发给同步节点。同步节点也维护区块链网络的分布式账本，即在自身保存的区块链数据结构中添加并保存完成共识的区块。非共识节点还可以包括除同步节点以外的非共识节点。

[0025] 每个节点在加入区块链网络时，都设定该节点的抵押权益值。设定方式是将新加入的节点自身的权益值选取部分或全部作为抵押权益值。

[0026] 本申请提供的选举共识节点及生成节点信息表格的方法适用于委托权益证明算法，是呈周期性地进行的。例如，每进行100轮共识过程后，选举新的共识节点并生成新的共识节点的节点信息表格。所述周期性可以根据需要而进行调整。

[0027] 请参阅图1，这是本申请提供的选举共识节点及生成节点信息表格的方法的实施例一，包括如下步骤。

[0028] 统计步骤102：统计每个同步节点的抵押权益值。

[0029] 选举步骤104:从所有同步节点中,选择抵押权益值最高的K个同步节点成为新的共识节点。其中K是共识节点的数量。例如将同步节点按照抵押权益值由高到低排序,选择排在最前方的K个同步节点作为新的共识节点。

[0030] 计算步骤106:根据每个新的共识节点的抵押权益值以及节点信息表格的长度L计算每个新的共识节点在节点信息表格中重复出现的次数。计算的原则是:抵押权益值越高的新的共识节点,在节点信息表格中出现的次数就越多;抵押权益值越低的新的共识节点,在节点信息表格中出现的次数就越少。可选地,让每个新的共识节点在节点信息表格中重复出现的次数与其抵押权益值成正比。例如有两个新的共识节点A和B,节点A、节点B的抵押权益值分别为100、10,那么可以通过某种计算使节点A、节点B在节点信息表格中分别重复出现500次、50次。

[0031] 表格生成步骤108:生成新的共识节点的节点信息表格,并将新的共识节点按照重复出现的次数加入到所生成的节点信息表格中。节点信息表格的长度L是指其中包含的数据的项数,L远大于K,因此每个新的共识节点均可在所述节点信息表格中重复出现多次。

[0032] 乱序步骤110:将节点信息表格中的数据顺序打乱,形成最终的新的共识节点的节点信息表格用于从中选择共识节点参与共识过程。例如采用某种随机算法打乱表格中的数据顺序。可选地,采用费雪耶兹随机置乱算法打乱表格中的数据顺序。所述参与共识过程包括在每一轮共识过程中提出新的备选区块、对新的备选区块进行检查和/或验证、将新的备选区块确认为完成共识的区块等操作。

[0033] 进一步地,在选举步骤104中,限定新的共识节点的抵押权益值必须大于零。如果所有同步节点中抵押权益值大于零的节点数量小于K,那么选举失败,由现有的共识节点在新的一个周期内再次担任共识节点,等待下一周期选举新的共识节点。

[0034] 与图1相对应的,本申请提供的选举共识节点及生成节点信息表格的系统的实施例一包括统计单元、选举单元、计算单元、表格生成单元、乱序单元。

[0035] 所述统计单元用来统计每个同步节点的抵押权益值。

[0036] 所述选举单元用来从所有同步节点中选择抵押权益值最高的K个同步节点成为新的共识节点。其中K是共识节点的数量。

[0037] 所述计算单元用来根据每个新的共识节点的抵押权益值以及节点信息表格的长度L计算每个新的共识节点在节点信息表格中重复出现的次数。计算的原则是:抵押权益值越高的新的共识节点,在节点信息表格中出现的次数就越多;抵押权益值越低的新的共识节点,在节点信息表格中出现的次数就越少。可选地,让每个新的共识节点在节点信息表格中重复出现的次数与其抵押权益值成正比。

[0038] 所述表格生成单元用来生成新的共识节点的节点信息表格,并将新的共识节点按照重复出现的次数加入到所生成的节点信息表格中。节点信息表格的长度L是指其中包含的数据的项数,L远大于K,因此每个新的共识节点均可在所述节点信息表格中重复出现多次。

[0039] 所述乱序单元用来将节点信息表格中的数据顺序打乱,形成最终的新的共识节点的节点信息表格用于从中选择共识节点参与共识过程。例如采用某种随机算法打乱表格中的数据顺序。所述参与共识过程包括提出新的备选区块、对新的备选区块进行检查和/或验证、将新的备选区块确认为完成共识的区块等操作。

[0040] 进一步地，所述选举单元还在所有同步节点中抵押权益值大于零的节点数量小于K时放弃本次选举共识节点，而由现有的共识节点在新的一个周期内再次担任共识节点，等待下一周期选举新的共识节点。

[0041] 请参阅图2，这是本申请提供的选举共识节点及生成节点信息表格的方法的实施例二，包括如下步骤。

[0042] 集合步骤101：将多个物理同步节点组成一个虚拟同步节点。例如采用分片(Sharding)技术、分布式计算技术等予以实现。这样操作的主要目的是将多个物理同步节点的运算能力集合起来对外形成统一的较为强大的运算能力。如果共识节点对于运算能力有一定要求，而单个的物理同步节点无法满足该运算能力的要求，则可将多个物理同步节点组成一个虚拟同步节点以满足该运算能力的要求。

[0043] 后续步骤均与实施例一相同，并且均将虚拟同步节点作为一个同步节点对待，如选举为共识节点则作为一个共识节点对待。在统计步骤102中，对于虚拟同步节点，则将组成该虚拟同步节点的所有物理同步节点的抵押权益值之和作为该虚拟同步节点的抵押权益值。

[0044] 与图1相对应的，本申请提供的选举共识节点及生成节点信息表格的系统的实施例二包括集合单元、统计单元、选举单元、计算单元、表格生成单元、乱序单元。

[0045] 所述集合单元用来将多个物理同步节点组成一个虚拟同步节点。

[0046] 其余单元均与实施例一相同，并且均将虚拟同步节点作为一个同步节点对待，如选举为共识节点则作为一个共识节点对待。所述统计单元对于虚拟同步节点，是将组成该虚拟同步节点的所有物理同步节点的抵押权益值之和作为该虚拟同步节点的抵押权益值。

[0047] 本申请在现有的委托权益证明算法的基础上提出了一种新的选举共识节点及生成节点信息表格的方法及系统，主要创新之处在于为每一周期新的共识节点生成节点信息表格，该节点信息表格的长度L远大于共识节点的数量K。每个新的共识节点都在该节点信息表格中重复出现，重复出现的次数与每个新的共识节点的抵押权益值正相关。后续的共识算法正是从该节点信息表格中选择共识节点进行共识过程。因此本申请可以让具有较高的抵押权益值的共识节点较多地参与到共识过程中，并认为这些节点是值得信赖的，从而降低了共识算法出现拜占庭错误的几率。

[0048] 以上仅为本申请的优选实施例，并不用于限定本申请。对于本领域的技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本申请的保护范围之内。

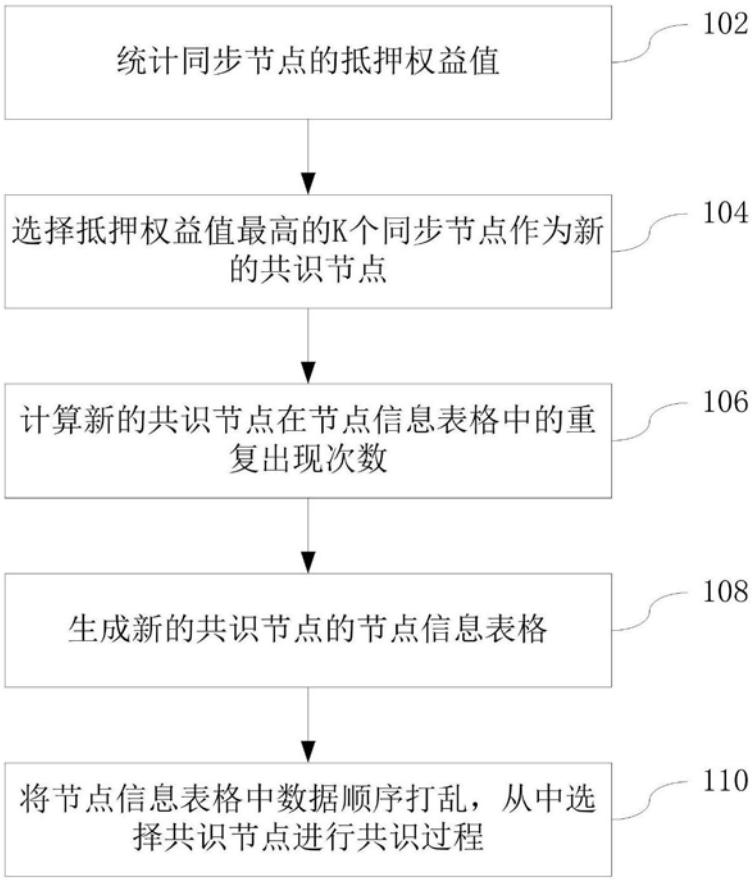

统计同步节点的抵押权益值
102
选择抵押权益值最高的K个同步节点作为新的共识节点
104
计算新的共识节点在节点信息表格中的重复出现次数
106
生成新的共识节点的节点信息表格
108
将节点信息表格中数据顺序打乱，从中选择共识节点进行共识过程
110

图1

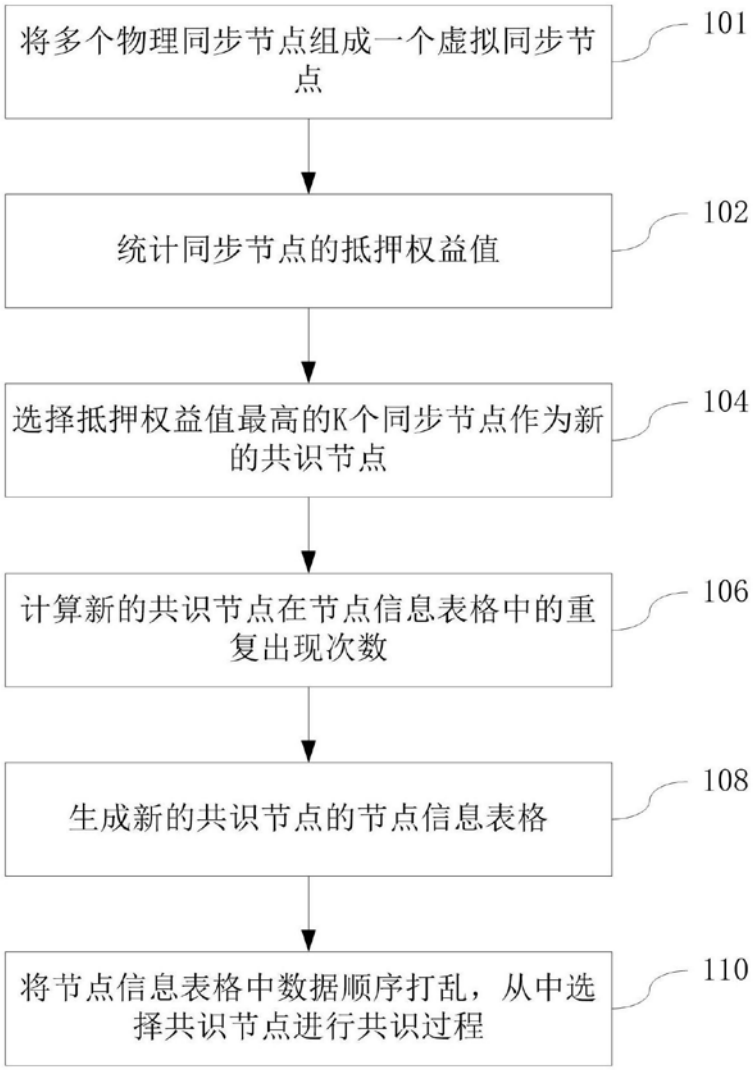

将多个物理同步节点组成一个虚拟同步节点
101
统计同步节点的抵押权益值
102
选择抵押权益值最高的K个同步节点作为新的共识节点
104
计算新的共识节点在节点信息表格中的重复出现次数
106
生成新的共识节点的节点信息表格
108
将节点信息表格中数据顺序打乱，从中选择共识节点进行共识过程
110

图2