(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 108377206 B
(45)授权公告日 2021.04.06

(21)申请号 201810199178.1

(22)申请日 2018.03.12

(65)同一申请的已公布的文献号
申请公布号 CN 108377206 A

(43)申请公布日 2018.08.07

(73)专利权人 众安信息技术服务有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室

(72)发明人 杜君君

(74)专利代理机构 北京永新同创知识产权代理有限公司 11376
代理人 钟胜光

(51)Int.Cl.
H04L 12/24(2006.01)
G06Q 40/04(2012.01)
G06F 9/50(2006.01)

(56)对比文件
CN 107231299 A,2017.10.03
CN 107341660 A,2017.11.10
CN 107579848 A,2018.01.12
CN 107563754 A,2018.01.09
CN 107590738 A,2018.01.16
US 2018039667 A1,2018.02.08
Vijay K. Garg等.TheWeighted Byzantine Agreement Problem.《2011 IEEE International Parallel & Distributed Processing Symposium》.2011,

审查员 李文娟

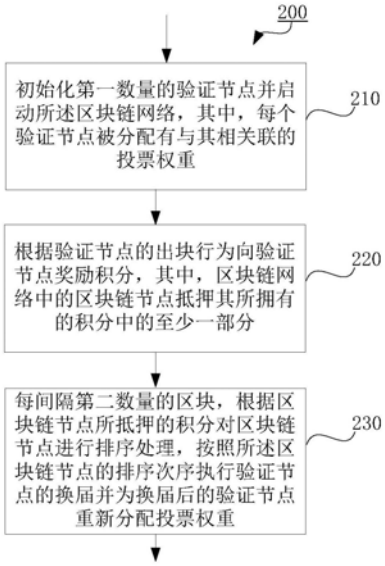
权利要求书2页 说明书10页 附图2页

(54)发明名称

用于配置共识算法的方法、装置及计算机可读存储介质

(57)摘要

本公开内容公开了用于配置区块链中的共识算法的方法，其包括：初始化第一数量的验证节点并启动区块链网络，每个验证节点被分配有与其相关联的投票权重；根据验证节点的出块行为向验证节点奖励积分，所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分；以及每间隔第二数量的区块，根据区块链节点所抵押的积分对区块链节点进行排序处理，按照区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。在该方法中，参与共识的验证节点可以拥有不同的权重，从而能够降低机器资源的消耗；此外，投票权重的分配与权益有关但又不完全依赖于权益来生成，从而能够降低巨头出现的可能性。



CN 108377206 B

1.一种用于配置区块链网络中的共识算法的方法,所述方法包括:

初始化第一数量的验证节点并启动所述区块链网络,其中,每个验证节点被分配有与其相关联的投票权重;

根据所述验证节点的出块行为向所述验证节点奖励积分,其中,所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分;以及

每间隔第二数量的区块,根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理,按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

2.根据权利要求1所述的方法,其中,所述第一数量的验证节点中的每个验证节点具有不同的投票权重。

3.根据权利要求1所述的方法,其中,为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。

4.根据权利要求3所述的方法,其中,每个投票节点的投票权重均不超过投票权重总和的三分之一。

5.根据权利要求1所述的方法,其中,所述第二数量大于等于投票权重总和。

6.根据权利要求1所述的方法,其中,在所述验证节点未参与共识的情况下,相应地扣除所述区块链节点所抵押的积分。

7.根据权利要求6所述的方法,其中,所述验证节点未参与共识包括所述验证节点不投票或不出块。

8.一种计算机可读存储介质,所述存储介质包括指令,当所述指令被执行时,使得所述计算机的处理器至少用于:

初始化第一数量的验证节点并启动区块链网络,其中,每个验证节点被分配有与其相关联的投票权重;

根据所述验证节点的出块行为向所述验证节点奖励积分,其中,所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分;以及

每间隔第二数量的区块,根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理,按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

9.根据权利要求8所述的计算机可读存储介质,其中,所述第一数量的验证节点中的每个验证节点具有不同的投票权重。

10.根据权利要求8所述的计算机可读存储介质,其中,为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。

11.根据权利要求10所述的计算机可读存储介质,其中,每个投票节点的投票权重均不超过投票权重总和的三分之一。

12.根据权利要求8所述的计算机可读存储介质,其中,所述第二数量大于等于投票权重总和。

13.根据权利要求8所述的计算机可读存储介质,其中,在所述验证节点未参与共识的情况下,相应地扣除所述区块链节点所抵押的积分。

14.一种用于配置区块链网络中的共识算法的装置,所述装置包括:

初始化模块，所述初始化模块被配置为初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重；

积分管理模块，所述积分管理模块被配置为根据所述验证节点的出块行为向所述验证节点奖励积分，其中，所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分；以及

投票权重再分配模块，所述投票权重再分配模块被配置为每间隔第二数量的区块，根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理，按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

15.根据权利要求14所述的装置，其中，所述第一数量的验证节点中的每个验证节点具有不同的投票权重。

16.根据权利要求14所述的装置，其中，为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。

17.根据权利要求16所述的装置，其中，每个投票节点的投票权重均不超过投票权重总和的三分之一。

18.根据权利要求14所述的装置，其中，所述第二数量大于等于投票权重总和。

19.根据权利要求14所述的装置，其中，在所述验证节点未参与共识的情况下，相应地扣除所述区块链节点所抵押的积分。

20.根据权利要求19所述的装置，其中，所述验证节点未参与共识包括所述验证节点不投票或不出块。

用于配置共识算法的方法、装置及计算机可读存储介质

技术领域

[0001] 本公开内容属于区块链技术领域，尤其涉及一种用于配置区块链中的共识算法的方法、一种用于配置区块链中的共识算法的装置以及一种相应的有形的计算机可读存储介质。

背景技术

[0002] 区块链(Block Chain)技术是一种基于去中心化的对等网络的技术，其将密码学原理与共识机制相结合来保障分布式各节点的数据连贯和持续，从而实现信息即时验证、可追溯、难篡改和无法屏蔽之目的，进而创造了一套隐私、高效、安全的分布式信任体系。

[0003] 区块链根据访问权限通常分为公有链、联盟链和私有链。其中，公有链是指任何人都可以根据协议接入并且参与共识的区块链；联盟链是指其共识过程受到预选节点控制的区块链；私有链是指所有权限都在一个组织中，并受该组织任意控制的区块链。

[0004] 共识算法是指由参与区块链的多个节点之间共同运行、遵守的一套协议，用来保证提交到区块链的请求操作(有时也包括执行结果)能在区块链的多个节点间达成一致。

[0005] 在现有的区块链技术中，不同的区块链平台选择的共识算法也各有千秋，不尽相同，从技术指标来看，不同的共识算法在系统可用性，可扩展性以及共识确认速度等指标上也有较大差异，没有一个十全十美满足所有场景的共识算法。因此在实际的区块链实践中，往往是需要根据实际的使用场景和技术指标要求来选择一个合适的共识算法。

[0006] 目前为止，区块链技术采用的共识算法有工作量证明(Proof Of Work:PoW)共识算法、权益证明(Proof Of Stake:PoS)共识算法、委托权益证明(Delegated Proof of Stake::dPoS)共识算法、实用拜占庭容错(Practical Byzantine Fault Tolerance:PBFT)共识算法，Paxos共识算法、Raft共识算法等。其中，工作量证明共识算法，例如由比特币使用，多在公有链使用；权益证明共识算法，目前用权益证明的区块链比较有名的例子是量子链，以太坊在尝试使用，多在公有链使用；委托权益证明共识算法是权益证明共识算法的变种，多在公有链使用；实用拜占庭容错共识算法，多在联盟链使用。换句话说，PoW和PoS、dPoS适用于公有链；PBFT，Paxos，Raft等较多地应用在联盟链和私有链中。

[0007] 在权益证明共识算法中，权益可以有不同的表现方式，在传统的权益证明共识算法中，有以代币(token)来表现的，也有以币龄(coin-age)来表现的。

[0008] 一般而言，工作量证明共识算法特别消耗计算资源，造成极大的电力浪费。权益证明共识算法及由其衍生的算法的出现是为了减少计算资源的消耗，一定程度上弥补了工作量证明共识算法的不足之处，但权益证明共识算法容易形成巨头，进而会打破区块链去中心化的特性。

发明内容

[0009] 针对上述问题，即现有技术中的共识算法有的会消耗特别大的计算资源进而造成极大的电力浪费，有的则会容易形成巨头进而会打破区块链去中心化的特性，本公开内容

的任务在于克服现有技术中形成区块链共识的上述缺陷。

[0010] 本公开内容的发明构思在于将权益证明共识算法和实用拜占庭容错共识算法进行结合，即结合权益证明共识算法和实用拜占庭容错共识算法的各自优点，从而形成一种新的用于配置区块链中的共识算法的方法，该用于配置区块链中的共识算法的方法能够在保证区块链激励机制的同时，还能够提供防巨头、不分叉的特性。

[0011] 更为具体而言，该用于形成区块链共识算法的方法对于实用拜占庭容错共识算法进行了改造，把实用拜占庭容错共识算法中“一个节点一张票”的特点改造为“节点拥有不同权重的投票权”，可以称之为带权重的实用拜占庭容错共识算法(Weighted Practical Byzantine Fault Tolerance，简称为WPBFT)。在该用于配置区块链中的共识算法的方法中，节点投票权可以按需进行修改，修改可以通过特权节点修改、节点达成共识修改、配置文件初始化修改等方式。在本公开内容中，主要使用节点达成共识修改这种方式。

[0012] 本公开内容的第一方面提出了一种用于配置区块链中的共识算法的方法，所述方法包括：

[0013] 初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重；

[0014] 根据所述验证节点的出块行为向所述验证节点奖励积分，其中，所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分；以及

[0015] 每间隔第二数量的区块，根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理，按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

[0016] 在依据本公开内容的用于配置区块链中的共识算法的方法中，参与共识的验证节点可以拥有不同的权重，从而能够降低机器资源的消耗；此外，投票权重的分配与权益有关但又不完全依赖于权益生成，从而能够降低巨头出现的可能性。

[0017] 在本公开内容的一种实现方式中，所述第一数量的验证节点中的每个验证节点具有不同的投票权重。以这样的方式，能够在初始化时便为不同的验证节点分配不同的投票权重，从而更好地实现依据本公开内容所公开的用于配置区块链中的共识算法的方法。

[0018] 在本公开内容的一种实现方式中，为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。以这样的方式，能够以所抵押的积分代替权益，减小整个区块链网络的计算负担。

[0019] 在本公开内容的一种实现方式中，每个投票节点的投票权重均不超过投票权重总和的三分之一。以这样的方式能够在减小整个区块链网络的计算负担的同时降低寡头节点的产生。

[0020] 在本公开内容的一种实现方式中，所述第二数量的区块大于等于投票权重总和。以这样的方式能够保证每个验证节点均出过块，从而保证区块链网络的功能的正常实现。

[0021] 在本公开内容的一种实现方式中，在所述验证节点未参与共识的情况下，相应地扣除所述区块链节点所抵押的积分。以这样的方式能够实现奖惩并举，从而使得验证节点的权利与义务的匹配。

[0022] 在本公开内容的一种实现方式中，所述验证节点未参与共识包括所述验证节点不投票或不出块。以这样的方式能够在验证节点不投票或不出块的情况下，相应地扣除所述

区块链节点所抵押的积分，从而实现奖惩并举，从而使得验证节点的权利与义务的匹配。

[0023] 此外，本公开内容的第二方面提出了一种计算机可读存储介质，所述存储介质包括指令，当所述指令被执行时，使得所述计算机的处理器至少用于：

[0024] 初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重；

[0025] 根据所述验证节点的出块行为向所述验证节点奖励积分，其中，所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分；以及

[0026] 每间隔第二数量的区块，根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理，按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

[0027] 在本公开内容的一种实现方式中，所述第一数量的验证节点中的每个验证节点具有不同的投票权重。

[0028] 在本公开内容的一种实现方式中，为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。

[0029] 在本公开内容的一种实现方式中，每个投票节点的投票权重均不超过投票权重总和的三分之一。

[0030] 在本公开内容的一种实现方式中，所述第二数量的区块大于等于投票权重总和。

[0031] 在本公开内容的一种实现方式中，在所述验证节点未参与共识的情况下，相应地扣除所述区块链节点所抵押的积分。

[0032] 再者，本公开内容的第三方面还提供了一种用于配置区块链中的共识算法的装置，所述装置包括：

[0033] 初始化模块，所述初始化模块被配置为初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重；

[0034] 积分管理模块，所述积分管理模块被配置为根据所述验证节点的出块行为向所述验证节点奖励积分，其中，所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分；以及

[0035] 投票权重再分配模块，所述投票权重再分配模块被配置为每间隔第二数量的区块，根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理，按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

[0036] 在本公开内容的一种实现方式中，所述第一数量的验证节点中的每个验证节点具有不同的投票权重。

[0037] 在本公开内容的一种实现方式中，为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。

[0038] 在本公开内容的一种实现方式中，每个投票节点的投票权重均不超过投票权重总和的三分之一。

[0039] 在本公开内容的一种实现方式中，所述第二数量的区块大于等于投票权重总和。

[0040] 在本公开内容的一种实现方式中，在所述验证节点未参与共识的情况下，相应地扣除所述区块链节点所抵押的积分。

[0041] 在本公开内容的一种实现方式中，所述验证节点未参与共识包括所述验证节点不

投票或不出块。

[0042] 综上所述，本公开内容公开了一种基于权益证明共识算法思想的、用于带权重的拜占庭容错共识算法的投票权重再分配的方法。在本公开内容中，该方法的权益以积分形式存在，积分可用于换取投票权。基于该算法，能够避免带权重的拜占庭容错共识算法中的投票权重过度集中，可以有效地降低巨头出现的可能性。

[0043] 概括地讲，本公开内容所提出的用于配置区块链中的共识算法的方法、装置及计算机可读存储介质的优点在于：算法整体基于拜占庭容错共识算法的思想，从而能够实现拜占庭容错；此外，参与共识的验证节点可以拥有不同的权重，从而能够降低机器资源的消耗；再者，投票权重的分配与权益有关但是又不完全依赖于权益生成，从而能够降低巨头出现的可能性，进而使得该用于配置区块链中的共识算法的方法、装置及计算机可读存储介质在工程上是能够实现。

附图说明

[0044] 结合附图并参考以下详细说明，本公开的各实施例的特征、优点及其他方面将变得更加明显，在此以示例性而非限制性的方式示出了本公开的若干实施例，在附图中：

[0045] 图1为本公开内容所提出的用于配置区块链中的共识算法的方法、用于配置区块链中的共识算法的装置及计算机可读存储介质所基于的网络结构100的示意图；

[0046] 图2为依据本公开内容的用于配置区块链中的共识算法的方法200的流程图；

[0047] 图3示出了重新分配投票权重的过程300的示意图；以及

[0048] 图4示出了本公开内容所提出的用于配置区块链中的共识算法的装置400的示意图。

具体实施方式

[0049] 以下参考附图详细描述本公开的各个示例性实施例。附图中的流程图和框图示出了根据本公开的各种实施例的方法和系统的可能实现的体系架构、功能和操作。应当注意，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，所述模块、程序段、或代码的一部分可以包括一个或多个用于实现各个实施例中所规定的逻辑功能的可执行指令。也应当注意，在有些作为备选的实现中，方框中所标注的功能也可以按照不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，或者它们有时也可以按照相反的顺序执行，这取决于所涉及的功能。同样应当注意的是，流程图和/或框图中的每个方框、以及流程图和/或框图中的方框的组合，可以使用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以使用专用硬件与计算机指令的组合来实现。

[0050] 本文所使用的术语“包括”、“包含”及类似术语应该被理解为是开放性的术语，即“包括/包含但不限于”，表示还可以包括其他内容。术语“基于”是“至少部分地基于”。术语“一个实施例”表示“至少一个实施例”；术语“另一实施例”表示“至少一个另外的实施例”，等等。

[0051] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为说明书的一部分。对于附图中的各单元之间的

连线，仅仅是为了便于说明，其表示至少连线两端的单元是相互通信的，并非旨在限制未连线的单元之间无法通信。

[0052] 图1为本公开内容所提出的用于配置区块链中的共识算法的方法、用于配置区块链中的共识算法的装置及计算机可读存储介质所基于的网络结构100的示意图。从图1中可以看出，该区块链平台100包括但不限于通过网络连接起来的终端(或者区块链节点)101、102、103、104、105、106、107以及终端108至199，其中，终端101、103、104通过无线网络与其他区块链终端连接，而终端102、105、106、107、108至199通过有线网络和其他区块链终端连接。换句话说，图中所示出的区块链网络共有99个终端节点，为了清楚简明起见，图中用终端108和终端199之间的点示意省略了终端109至198。本领域的技术人员应当了解，此处所举例说明的99个终端节点仅仅是示例性的，而非限制性的，更多或者更少个区块链终端节点也是可行的。只要不脱离本公开内容的发明构思均应该落入本公开内容的权利要求书所要求的保护范围之内。

[0053] 在具体介绍本公开内容所提出的用于配置区块链中的共识算法的方法、用于配置区块链中的共识算法的装置及计算机可读存储介质之前，本公开内容的申请人首先将阐述以下在介绍过程中将用到的术语的含义。

[0054] 出块:区块链网络中产生区块的动作；

[0055] 积分:出块过程中，对出块节点的奖励；

[0056] 拜占庭节点:在分布式网络中，会带有恶意地对网络共识过程进行干扰的节点；

[0057] PBFT、实用拜占庭容错算法:一种分布式系统常用的共识算法，在有3F+1个共识节点的情况下，可以容忍F个拜占庭节点的存在；

[0058] 投票权重:在PBFT算法中，投票节点占据的权重，假设某一节点X拥有的权重是2，其他节点的权重都是1，那么节点X投票的时候，相当于两票；

[0059] WPBFT、带权重的使用拜占庭容错算法:一种改造过的PBFT算法，在该算法中，节点的投票按权重计算，而非每个节点一票；

[0060] 验证节点:在PBFT算法中，负责参与共识的节点；

[0061] 换届:在PBFT算法中，更换验证节点的操作；

[0062] 抵押:在本算法中，抵押积分，换取投票权重的操作。

[0063] 在阐述清楚上述术语概念的基础上，接下来将结合图2来描述本公开内容所公开的用于配置区块链中的共识算法的方法。

[0064] 图2示出了依据本公开内容的用于配置区块链中的共识算法的方法200的流程图。从图中可以看出，依据本公开内容的用于配置区块链中的共识算法的方法200包括以下三个步骤，即：

[0065] 首先，在方法步骤210之中将会初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重；例如，在如图1所示的99个节点中选择21个节点作为验证节点，本领域的技术人员应当了解，此处所选择的21个验证节点的数量仅仅是示例性的而非限制性的。在符合本公开内容的发明构思的前提下，也可以选择多于21个或者少于21个验证节点，例如选择30个验证节点或者选择10个验证节点。

[0066] 在验证节点选择好之后，在方法步骤220中，将会根据所述验证节点的出块行为向所述验证节点奖励积分，例如每出一次块获得一个积分奖励。其中，所述区块链网络中的区

块链节点抵押其所拥有的积分中的至少一部分;在此,验证节点抵押积分换取更大的投票权重,相当于获得了更多的出块概率。例如,当前区块链网络的节点101具有220个积分,其既可以将220个积分全部抵押,也能够抵押这220个积分中的一部分,例如抵押118个积分。当然,当前区块链网络的节点101所抵押的积分将会影响其在换届时所处于的排队序列中的位置,进而影响其在换届后所分配到的投票权重。

[0067] 最后,该方法还包括方法步骤230,在方法步骤230中,每间隔第二数量的区块,根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理,按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。

[0068] 由以上论述可知,在依据本公开内容的用于配置区块链中的共识算法的方法中,参与共识的验证节点可以拥有不同的权重,从而能够降低机器资源的消耗;此外,投票权重的分配与权益有关但又不完全依赖于权益生成,从而能够降低巨头出现的可能性。

[0069] 可选地,所述第一数量的验证节点中的每个验证节点具有不同的投票权重。例如,从图1的99个节点中选择10个节点为验证节点,对其进行初始化,此时,为第一节点101分配2的投票权重,为第二节点102分配5的投票权重,而为其他节点分配1的投票权重。以这样的方式,能够在初始化时便为不同的验证节点分配不同的投票权重,从而更好地实现依据本公开内容所公开的用于配置区块链中的共识算法的方法。本领域的技术人员应当了解,为所述第一数量的验证节点中的每个验证节点具有不同的投票权重是优选的实现方式。当然,为所述第一数量的验证节点中的每个验证节点具有相同的投票权重也是可行的。

[0070] 可选地,为方法步骤230中重新排序后的各个节点中排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。以这样的方式,能够以所抵押的积分代替权益,减小整个区块链网络的计算负担。进一步可选地,每个投票节点的投票权重均不超过投票权重总和的三分之一。以这样的方式能够在减小整个区块链网络的计算负担的同时降低寡头节点的产生。再者,所述第二数量的区块大于等于投票权重总和。例如在上述的例子中,从图1的99个节点中选择10个节点为验证节点,对其进行初始化,此时,为第一节点101分配2的投票权重,为第二节点102分配5的投票权重,而为其他节点分配1的投票权重,这样一来,投票权重总和便是15,也就是说,在区块链网络上至少有15个区块后再进行节点的排序。以这样的方式能够保证每个验证节点均出过块,从而保证区块链网络的功能的正常实现。

[0071] 可选地,在所述验证节点未参与共识的情况下,相应地扣除所述区块链节点所抵押的积分。以这样的方式能够实现奖惩并举,从而使得验证节点的权利与义务的匹配。在本公开内容的一种实现方式中,所述验证节点未参与共识包括所述验证节点不投票或不出块。以这样的方式能够在验证节点不投票或不出块的情况下,相应地扣除所述区块链节点所抵押的积分,从而实现奖惩并举,从而使得验证节点的权利与义务的匹配。也就是说通过抵押积分获取更大投票权的节点相应地就承担了更多的责任,如果当它不能够正常地参与共识(如不投票,不出块等),应当按比例扣除抵押的积分。

[0072] 上述的方法步骤230中的节点重新排序以及投票权重的再分配过程所采用的规则可以如以下伪代码描述:

[0073]

```
1
2   // tokenMap 记录了节点抵押的积分数量
3   // 例：{node1:100token, node2:200token}
4   // 函数返回节点的权重分配
5   // 例：{node1:100, node2:200}
6   cal_weight(tokenMap) {
7       // sortByToken 函数，根据抵押的积分数量
8       // 将键值对中的组合进行排序，积分数量多的在前
9       tokenMap = sortByToken(tokenMap)
10
11      pos = 0
12      weightMap = {}
13      for node in tokenMap {
14          pos += 1
15          weight = cal_weight_by_pos(pos)
16          weightMap.put(node, weight)
17      }
18      return weightMap
19  }
20
21  cal_weight_by_pos(pos) {
22      if pos == 1 {
23          return 36
24      } else if pos in (2, 3) {
```

```
        return 25
    } else if pos in (4, 5, 6) {
        return 16
    } else if pos in (7, 8, 9, 10) {
        return 9
    } else if pos in (11,12,13,14,15) {
        return 4
    } else if pos in (16,17,18,19,20,21) {
        return 1
    }
}
```

[0075] 也就是说，上述的配置方法能够通过有形的计算机可读存储介质的方式来实现，该存储介质包括指令，当所述指令被执行时，使得计算机的处理器至少用于初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重；根据所述验证节点的出块行为向所述验证节点奖励积分，其中，所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分；以及每间隔第二数量的区块，根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理，按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。即上述的配置方法能够通过计算机程序产品来实现。计算机程序产品可以包括计算机可读存储介质，其上载有用于执行本公开的各个方面的计算机可读程序指令。计算机可读存储介质可以是可以保持和存储由指令执行设备使用的指令的有形设备。计算机可读存储介质例如可以是但不限于电存储设备、磁存储设备、光存储设备、电磁存储设备、半导体存储设备或者上述的任意合适的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括:便携式计算机盘、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)、静态随机存取存储器(SRAM)、便携式压缩盘只读存储器(CD-ROM)、数字多功能盘(DVD)、记忆棒、软盘、机械编码设备、例如其上存储有指令的打孔卡或凹槽内凸起结构、以及上述的任意合适的组合。这里所使用的计算机可读存储介质不被解释为瞬时信号本身，诸如无线电波或者其他自由传播的电磁波、通过波导或其他传输媒介传播的电磁波(例如，通过光纤电缆的光脉冲)、或者通过电线传输的电信号。

[0076] 以下将参照上述伪代码以及图3来描述重新分配投票权重的过程。图3示出了重新分配投票权重的过程300的示意图。从图3中可以看出，在按照所抵押的积分排序之后，按照排序的次序依次将对应的节点按照从上往下从左往右的顺序填充到图3所示出的图形中。其中，在最上面的第1号位置填充进36，即第1位可以获得36的投票权重；第2号位置和第3号位置填充进25，即第2号位置和第3号位置可以获得25的投票权重；第4号位置、第5号位置和第6号位置填充进16，即第4号位置、第5号位置和第6号位置可以获得16的投票权重；第7号位置、第8号位置、第9号位置和第10号位置填充进9，即第7号位置、第8号位置、第9号位置和

第10号位置可以获得9的投票权重;第11号位置、第12号位置、第13号位置、第14号位置和第15号位置填充进4,即第11号位置、第12号位置、第13号位置、第14号位置和第15号位置可以获得4的投票权重;第16号位置、第17号位置、第18号位置、第19号位置、第20号位置和第21号位置填充进1,即第16号位置、第17号位置、第18号位置、第19号位置、第20号位置和第21号位置可以获得1的投票权重。

[0077] 采用这个算法,能够避免巨头的产生。达成这一效果的理论依据为:无论单一个节点抵押多少积分,它最多只能够获得一定数量的投票权重,这个权重能够让他获得比其他节点更多一点的积分奖励,但并不能让他对整个网络占据完全的主导权,从而抑制其对整个区块链网络的影响。需要注意的是,本实施例中,采用的权重分配算法(包括伪代码和图示)仅用于描述实施方法,在具体的应用中,本发明提出的算法可兼容不同的节点数量和不同的权重分配方式,采用不同的节点数量、不同的计算分配方法,都应当视为本发明的变种版本。

[0078] 除了以上的实现形式以外,依据本公开内容所公开的发明构思也能够通过用于配置区块链中的共识算法的装置400来实现,所述装置400包括:初始化模块410,所述初始化模块410被配置为初始化第一数量的验证节点并启动所述区块链网络,其中,每个验证节点被分配有与其相关联的投票权重;积分管理模块420,所述积分管理模块420被配置为根据所述验证节点的出块行为向所述验证节点奖励积分,其中,所述区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分;以及投票权重再分配模块430,所述投票权重再分配模块430被配置为每间隔第二数量的区块,根据所述区块链节点所抵押的积分对所述区块链节点进行排序处理,按照所述区块链节点的排序次序执行验证节点的换届并且为换届后的验证节点重新分配投票权重。可选地,所述第一数量的验证节点中的每个验证节点具有不同的投票权重。优选地,为排序在前的验证节点所分配的投票权重大于为排序在后的验证节点所分配的投票权重。更为优选地,每个投票节点的投票权重均不超过投票权重总和的三分之一。优选地,所述第二数量的区块大于等于投票权重总和。优选地,在所述验证节点未参与共识的情况下,相应地扣除所述区块链节点所抵押的积分,其中,所述验证节点未参与共识包括所述验证节点不投票或不出块。

[0079] 综上所述,本公开内容公开了一种基于权益证明共识算法思想的、用于带权重的拜占庭容错共识算法的投票权重再分配的方法。在本公开内容中,该方法的权益以积分形式存在,积分可用于换取投票权。基于该算法,能够避免带权重的拜占庭容错共识算法中的投票权重过度集中,可以有效地降低巨头出现的可能性。

[0080] 概括地讲,本公开内容所提出的用于配置区块链中的共识算法的方法、装置及计算机可读存储介质的优点在于:算法整体基于拜占庭容错共识算法的思想,从而能够实现拜占庭容错;此外,参与共识的验证节点可以拥有不同的权重,从而能够降低机器资源的消耗;再者,投票权重的分配与权益有关但是又不完全依赖于权益生成,从而能够降低巨头出现的可能性,进而使得该用于配置区块链中的共识算法的方法、装置及计算机可读存储介质在工程上是能够实现。

[0081] 应当注意,尽管在上文的详细描述中提及了设备的若干装置或子装置,但是这种划分仅仅是示例性而非强制性的。实际上,根据本公开的实施例,上文描述的两个或更多装置的特征和功能可以在一个装置中具体化。反之,上文描述的一个装置的特征和功能可以

进一步划分为由多个装置来具体化。

[0082] 以上所述仅为本公开的实施例可选实施例，并不用于限制本公开的实施例，对于本领域的技术人员来说，本公开的实施例可以有各种更改和变化。凡在本公开的实施例的精神和原则之内，所作的任何修改、等效替换、改进等，均应包含在本公开的实施例的保护范围之内。

[0083] 虽然已经参考若干具体实施例描述了本公开的实施例，但是应该理解，本公开的实施例并不限于所公开的具体实施例。本公开的实施例旨在涵盖在所附权利要求的精神和范围内所包括的各种修改和等同布置。所附权利要求的范围符合最宽泛的解释，从而包含所有这样的修改及等同结构和功能。

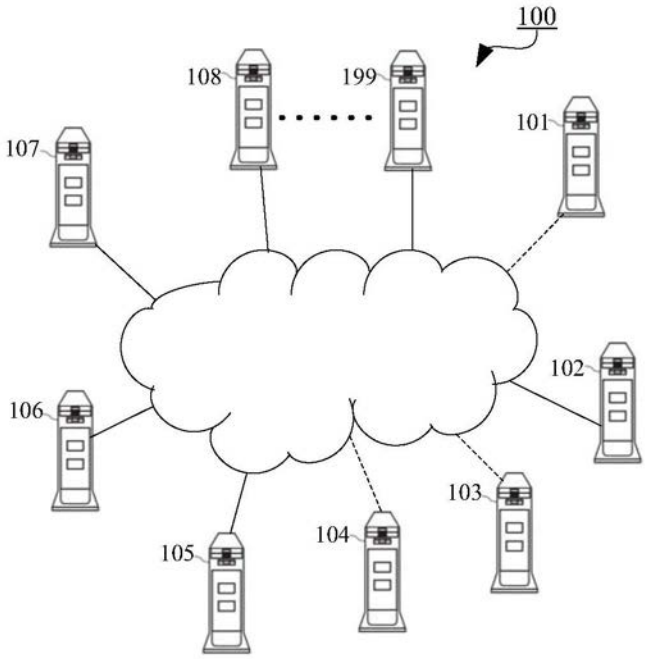

100
108
199
101
107
102
106
103
104
105

图1

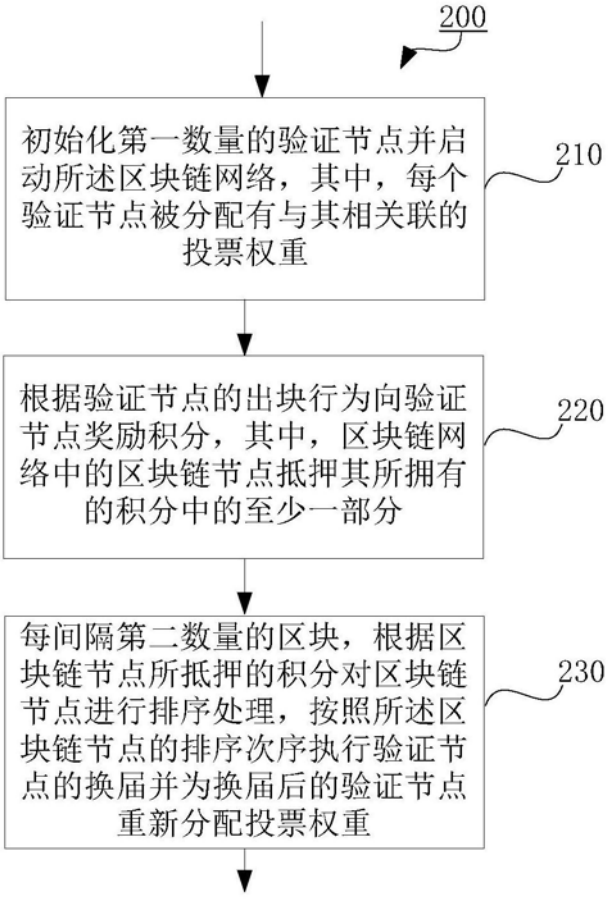

200
初始化第一数量的验证节点并启动所述区块链网络，其中，每个验证节点被分配有与其相关联的投票权重
210
根据验证节点的出块行为向验证节点奖励积分，其中，区块链网络中的区块链节点抵押其所拥有的积分中的至少一部分
220
每间隔第二数量的区块，根据区块链节点所抵押的积分对区块链节点进行排序处理，按照所述区块链节点的排序次序执行验证节点的换届并为换届后的验证节点重新分配投票权重
230

图2

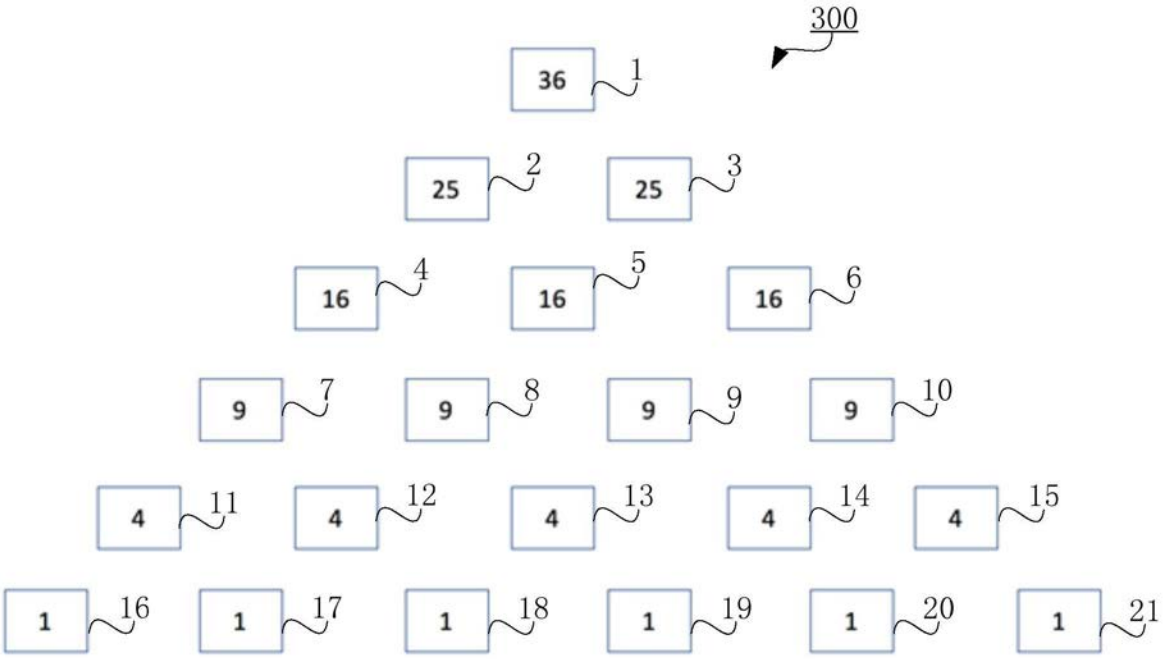

300
36
1
25
2
25
3
16
4
16
5
16
6
9
7
9
8
9
9
9
10
4
11
4
12
4
13
4
14
4
15
1
16
1
17
1
18
1
19
1
20
1
21

图3

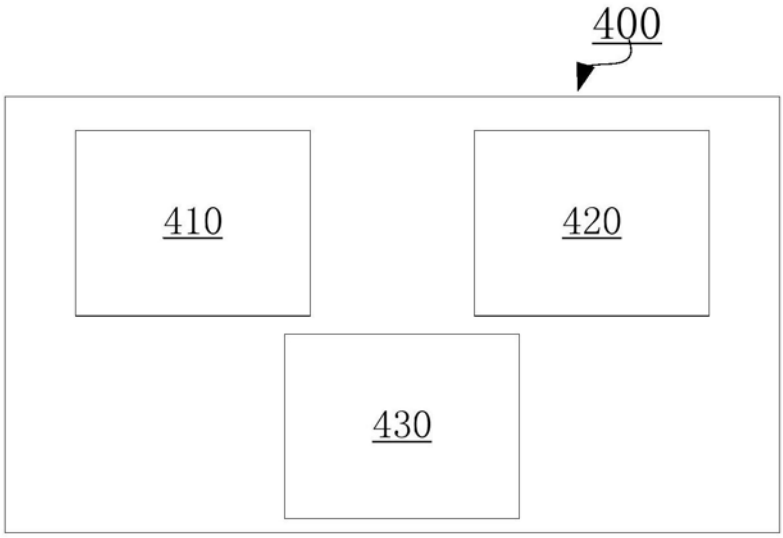

400
410
420
430

图4