(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 110661867 B
(45)授权公告日 2021.07.23

(21)申请号 201910908746.5
(22)申请日 2019.09.25
(65)同一申请的已公布的文献号
申请公布号 CN 110661867 A
(43)申请公布日 2020.01.07
(73)专利权人 东北大学
地址 110819 辽宁省沈阳市和平区文化路3号巷11号
(72)发明人 信俊昌 姚钟铭 郝琨 王之琼 陈金义 范子嘉 罗艺栖 李云飞
(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
代理人 梁焱
(51)Int.Cl.
H04L 29/08(2006.01)
(56)对比文件
CN 109600230 A,2019.04.09
CN 109964242 A,2019.07.02
US 2019251187 A1,2019.08.15
CN 104219291 A,2014.12.17
CN 106921681 A,2017.07.04
CN 108366113 A,2018.08.03
CN 109150972 A,2019.01.04
CN 110011974 A,2019.07.12
CN 107124403 A,2017.09.01
CN 107424066 A,2017.12.01
CN 109214817 A,2019.01.15
CN 110113388 A,2019.08.09
CN 109361661 A,2019.02.19
CN 111010278 A,2020.04.14
US 6471521 B1,2002.10.29
US 10382388 B2,2019.08.13
US 2018096163 A1,2018.04.05 (续)
审查员 文庆

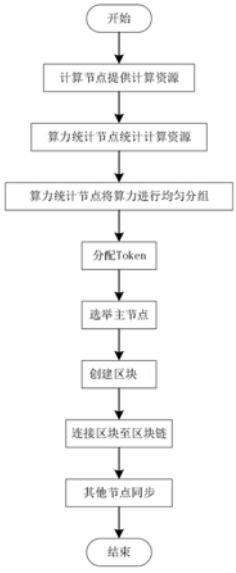
权利要求书1页 说明书4页 附图1页

(54)发明名称

一种基于改进工作量证明与权益证明的区块链共识方法

(57)摘要

本发明涉及计算机区块链技术领域，提供一种基于改进工作量证明与权益证明的区块链共识方法。步骤1：区块链中的算力统计节点统计计算节点的算力；步骤2：算力统计节点对区块链中所有计算节点的算力进行均匀分组，为每个计算组在加入区块链之前分配Token值；步骤3：用户发送存入数据的请求，对所有计算组按照Token值由大到小排序，选择前k个计算组分别对数据进行打包成区块操作，选取最先完成打包成区块操作的计算组为主节点，主节点将区块连接至区块链中，并利用协议向其他节点广播消息，其他节点同步区块链状态。本发明能够节约系统算力、缩短计算周期，且避免对新加入网络的节点和拥有计算资源较少的节点不友好的问题。



CN 110661867 B

[转续页]

[接上页]

(56)对比文件

CN 107450981 A,2017.12.08

Sunny Pahlajani等.“Survey on Private Blockchain Consensus Algorithms”.《IEEE》.2019,

尚新.“一种基于层次化聚类学习的区块链共识方法”.《http://www.cnki.com.cn/Article/CJFDTotal-SDDZ201809035.htm》.2018,

韩爽等.“区块链技术在数字资产安全交易中的应用”.《计算机系统应用》.2018,

郝琨等.“去中心化的分布式存储模型”.《计算机工程与应用》.2017,

贾大宇等.“区块链的存储容量可扩展模型”.《计算机科学与探索》.2017,

1.一种基于改进工作量证明与权益证明的区块链共识方法,所述区块链中存在M个算力统计节点$S_{csn}=\{csn_1,csn_2,...,csn_m,...,csn_M\}$和N个计算节点$S_{cn}=\{cn_1,cn_2,...,cn_n,...,cn_N\}$,所述算力统计节点用于统计计算节点的算力,所述计算节点用于创建区块和连接区块,所述计算节点的算力为计算节点能够提供的计算资源大小,其特征在于,包括下述步骤:

步骤1:区块链中的算力统计节点对每个计算节点的算力进行统计,得到N个计算节点的算力$S_p=\{p_1,p_2,...,p_n,...,p_N\}$;其中,$p_n$为第n个计算节点的算力;

步骤2:算力统计节点对全网计算节点的算力进行平衡:

步骤2.1:算力统计节点对区块链中所有计算节点的算力进行均匀分组:算力统计节点计算所有计算节点的总算力$P=\sum_{n=1}^{N}p_n$,并寻找所有计算节点的算力中的最大值$p_{max}=max\{p_1,p_2,...,p_n,...,p_N\}$,计算分组个数为$L=\lceil P/p_{max}\rceil$,将算力小于$p_{max}$的计算节点随机组合形成总算力最大化且总算力小于或等于p_{max}的分组,将算力为p_{max}的计算节点自成一组,得到计算组集合$S_{group}=\{group_1,group_2,...,group_1,...,group_L\}$;其中,$\lceil\ \rceil$为向上取整运算符,$group_1$为第1个计算组;

步骤2.2:在每个计算组加入区块链之前为每个计算组分配相同的Token值初始值;其中,Token值代表计算组在区块链中还可以存活的时间;

步骤3:计算节点创建区块,并选择主节点将区块连接至区块链:

步骤3.1:用户向区块链发送存入数据的请求,对所有计算组按照Token值由大到小进行排序,设定随区块链网络规模正比变化的阈值k,选择排序后的计算组中前k个计算组来响应请求;

步骤3.2:前k个计算组分别对数据进行打包成区块操作,选取最先完成打包成区块操作的计算组为主节点;

步骤3.3:主节点将区块连接至区块链中;

步骤3.4:主节点利用协议向其他节点广播消息,其他节点同步区块链状态。

2.根据权利要求1所述的基于改进工作量证明与权益证明的区块链共识方法,其特征在于,所述步骤1包括下述步骤:

步骤1.1:每个计算节点表明自己能够提供的计算资源大小;

步骤1.2:算力统计节点记录每个计算节点能够提供的计算资源大小。

3.根据权利要求1所述的基于改进工作量证明与权益证明的区块链共识方法,其特征在于,所述步骤3中,所述协议为Gossip协议。

一种基于改进工作量证明与权益证明的区块链共识方法

技术领域

[0001] 本发明涉及计算机区块链技术领域，特别是涉及一种基于改进工作量证明与权益证明的区块链共识方法。

背景技术

[0002] 区块链是一种由互不相信的节点维护同一个全局状态的数据库，具有去中心化、冗余存储以及数据防篡改等优点。区块链技术无需借助第三方可信机构既可以实现互不信任的多方完成数据共享。区块链之所以能够实现数据防篡改的特性，主要是因为以区块为单位的链式结构和合理的共识机制。

[0003] 共识机制是指在没有中心节点控制的情况下，互不信任的节点之间就下一步合法性行为达成共识的机制。区块链中常见的共识机制有工作量证明机制(POW)和权益证明机制(POS)。

[0004] 工作量证明机制即区块链中的节点必须达到一定的工作量才能拥有区块的记录权。在基于工作量证明机制构建的区块链网络中，节点通过计算随机哈希散列的数值解竞争记录权，正确求解的节点具有当前的记录权。工作量证明机制具有完全去中心化的优点，在以工作量证明机制为共识的区块链中，节点可以自由进出。但是，基于工作量证明机制的区块链系统造成了大量的资源浪费，达成共识所需要的周期也较长，另外如果过多强算力节点结合，那么这些节点会控制整条区块链。

[0005] 权益证明机制的运作方式与工作量证明机制相似，但权益证明机制会根据每个节点拥有代币的比例和时间，依据算法等比例地降低节点的挖矿难度，从而加快了寻找随机数的速度，能一定程度地减少资源的浪费。但是，如果有矿工恶意囤币后挖矿，会很容易得到记录权，因此对于新加入的节点和拥有计算资源较少的节点挖矿的难度很大，获得记录权的概率较小。

[0006] 可见，传统基于工作量证明的区块链共识方法会浪费大量的系统算力且计算周期较长，基于权益证明的区块链共识方法对新加入网络的节点和拥有计算资源较少的节点不友好。

发明内容

[0007] 针对现有技术存在的问题，本发明提供一种基于改进工作量证明与权益证明的区块链共识方法，能够节约系统算力、缩短计算周期，且避免对新加入网络的节点和拥有计算资源较少的节点不友好的问题。

[0008] 本发明的技术方案为：

[0009] 一种基于改进工作量证明与权益证明的区块链共识方法，所述区块链中存在M个算力统计节点$S_{csn}=\{csn_1,csn_2,...,csn_m,...,csn_M\}$和N个计算节点$S_{cn}=\{cn_1,cn_2,...,cn_n,...,cn_N\}$，所述算力统计节点用于统计计算节点的算力，所述计算节点用于创建区块和连接区块，所述计算节点的算力为计算节点能够提供的计算资源大小，其特征在于，包括下

述步骤：

[0010] 步骤1：区块链中的算力统计节点对每个计算节点的算力进行统计，得到N个计算节点的算力$S_p=\{p_1,p_2,\ldots,p_n,\cdots,p_N\}$；其中，$p_n$为第n个计算节点的算力；

[0011] 步骤2：算力统计节点对全网计算节点的算力进行平衡：

[0012] 步骤2.1：算力统计节点对区块链中所有计算节点的算力进行均匀分组：算力统计节点计算所有计算节点的总算力$P=\sum_{n=1}^{N}p_n$，并寻找所有计算节点的算力中的最大值$p_{max}=\max\{p_1,p_2,\cdots,p_n,\cdots,p_N\}$，计算分组个数为$L=\lceil P/p_{max}\rceil$，将算力小于$p_{max}$的计算节点随机组合形成总算力最大化且总算力小于或等于p_{max}的分组，将算力为p_{max}的计算节点自成一组，得到计算组集合$S_{group}=\{group_1,group_2,\cdots,group_l,\cdots,group_L\}$；其中，$\lceil\ \rceil$为向上取整运算符，$group_l$为第l个计算组；

[0013] 步骤2.2：在每个计算组加入区块链之前为每个计算组分配相同的Token值初始值；其中，Token值代表计算组在区块链中还可以存活的时间；

[0014] 步骤3：计算节点创建区块，并选择主节点将区块连接至区块链：

[0015] 步骤3.1：用户向区块链发送存入数据的请求，对所有计算组按照Token值由大到小进行排序，设定随区块链网络规模正比变化的阈值k，选择排序后的计算组中前k个计算组来响应请求；

[0016] 步骤3.2：前k个计算组分别对数据进行打包成区块操作，选取最先完成打包成区块操作的计算组为主节点；

[0017] 步骤3.3：主节点将区块连接至区块链中；

[0018] 步骤3.4：主节点利用协议向其他节点广播消息，其他节点同步区块链状态。

[0019] 所述步骤1包括下述步骤：

[0020] 步骤1.1：每个计算节点表明自己能够提供的计算资源大小；

[0021] 步骤1.2：算力统计节点记录每个计算节点能够提供的计算资源大小。

[0022] 所述步骤3中，所述协议为Gossip协议。

[0023] 本发明的有益效果为：

[0024] 本发明通过算力统计节点对区块链中所有计算节点的算力进行均匀分组并为每个计算组分配Token值，根据Token值选取主节点将区块连接至区块链中，相比于基于工作量证明的区块链共识方法，不需要额外计算随机哈希散列的数值解来竞争记录权，有效节约了系统算力，缩短了计算周期；相比于基于权益证明的区块链共识方法，避免了对新加入网络的节点和拥有计算资源较少的节点不友好的问题。

附图说明

[0025] 图1为本发明的基于改进工作量证明与权益证明的区块链共识方法的流程图。

具体实施方式

[0026] 下面将结合附图和具体实施方式，对本发明作进一步描述。

[0027] 本实施例中，区块链中存在M＝5个算力统计节点$S_{csn}=\{csn_1,csn_2,csn_3,csn_4,$

$csn_5\}$和N＝10个计算节点$S_{cn}=\{cn_1,cn_2,\cdots,cn_n,\cdots,cn_{10}\}$，算力统计节点用于统计计算节点的算力，计算节点用于创建区块和连接区块，计算节点的算力为计算节点能够提供的计算资源大小。

[0028] 如图1所示，本发明的基于改进工作量证明与权益证明的区块链共识方法，包括下述步骤：

[0029] 步骤1：区块链中的算力统计节点$S_{csn}=\{csn_1,csn_2,csn_3,csn_4,csn_5\}$对每个计算节点的算力进行统计，得到10个计算节点的算力$S_p=\{p_1,p_2,\ldots,p_n,\ldots,p_{10}\}$；其中，$p_n$为第n个计算节点的算力：

[0030] 步骤1.1：每个计算节点表明自己能够提供的计算资源大小；

[0031] 步骤1.2：算力统计节点记录每个计算节点能够提供的计算资源大小。

[0032] 本实施例中，$S_p=\{p_1,p_2,\ldots,p_n,\ldots,p_{10}\}=\{1T,2T,3T,5T,5T,5T,9T,10T,10T,10T\}$。

[0033] 步骤2：算力统计节点对全网计算节点的算力进行平衡：

[0034] 步骤2.1：算力统计节点对区块链中所有计算节点的算力进行均匀分组：算力统计节点计算所有计算节点的总算力$P=\sum_{n=1}^{N}p_n=60T$，并寻找所有计算节点的算力中的最大值$p_{max}=\max\{p_1,p_2,\ldots,p_n,\ldots,p_N\}=10T$，计算分组个数为$L=\lceil P/p_{max}\rceil=6$；将算力小于$p_{max}$的计算节点随机组合形成总算力最大化且总算力小于或等于p_{max}的分组，将cn_1和cn_7组合成第1个计算组$group_1$，将cn_2、cn_3、cn_4组成第2个计算组$group_2$，将cn_5和cn_6组成第3个计算组$group_3$；将算力为p_{max}的计算节点自成一组，即将cn_8单独组成$group_4$、cn_9单独组成$group_5$、cn_{10}单独组成$group_6$；得到计算组集合$S_{group}=\{group_1,group_2,\ldots,group_1,\ldots,group_6\}$；其中，$\lceil\ \rceil$为向上取整运算符，$group_1$为第1个计算组；

[0035] 步骤2.2：在每个计算组加入区块链之前为每个计算组分配相同的Token值初始值；其中，Token值代表计算组在区块链中还可以存活的时间。

[0036] 本实施例中，设定每个计算组的存活时间为1小时，计算组相隔5分钟加入区块链网络。

[0037] 步骤3：计算节点创建区块，并选择主节点将区块连接至区块链：

[0038] 步骤3.1：用户向区块链发送存入数据的请求，对所有计算组按照Token值由大到小进行排序，设定随区块链网络规模正比变化的阈值k＝3，选择排序后的计算组中前3个计算组$\{group_4,group_5,group_6\}$来响应请求；

[0039] 步骤3.2：前3个计算组分别对数据进行打包成区块操作，选取最先完成打包成区块操作的计算组$group_4$为主节点；

[0040] 步骤3.3：主节点将区块连接至区块链中；

[0041] 步骤3.4：主节点利用协议向其他节点广播消息，其他节点同步区块链状态。

[0042] 本实施例中，所述协议为Gossip协议。

[0043] 显然，上述实施例仅仅是本发明的一部分实施例，而不是全部的实施例。上述实施例仅用于解释本发明，并不构成对本发明保护范围的限定。基于上述实施例，本领域技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，也即凡在本申请的精神和原

理之内所作的所有修改、等同替换和改进等,均落在本发明要求的保护范围内。

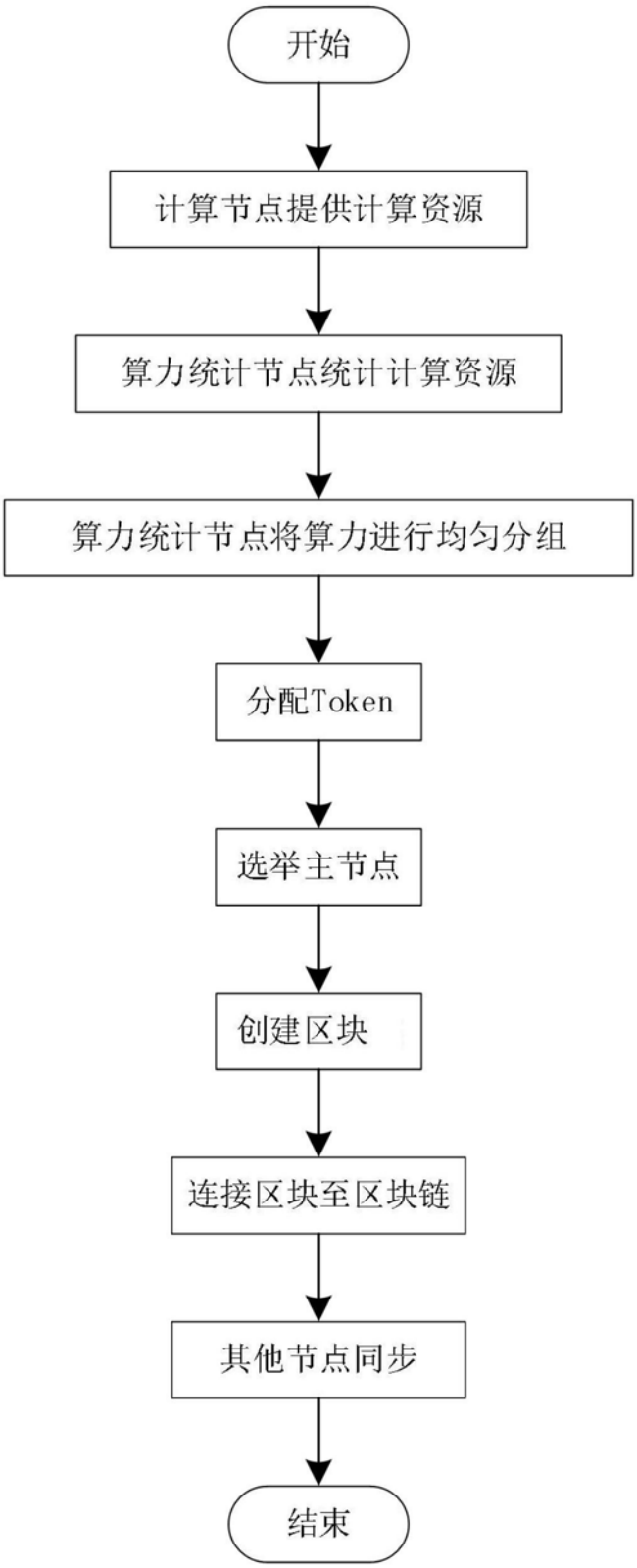

开始
计算节点提供计算资源
算力统计节点统计计算资源
算力统计节点将算力进行均匀分组
分配Token
选举主节点
创建区块
连接区块至区块链
其他节点同步
结束

图1