(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 106548397 A
(43)申请公布日 2017.03.29

(21)申请号 201611046082.9

(22)申请日 2016.11.22

(71)申请人 天津米游科技有限公司
地址 301700 天津市武清区黄花镇政府南路22号

(72)发明人 邓迪 孟繁轲 丁江

(74)专利代理机构 北京奥翔领智专利代理有限公司 11518
代理人 李清

(51)Int.Cl.
G06Q 40/00(2012.01)
G06Q 20/38(2012.01)

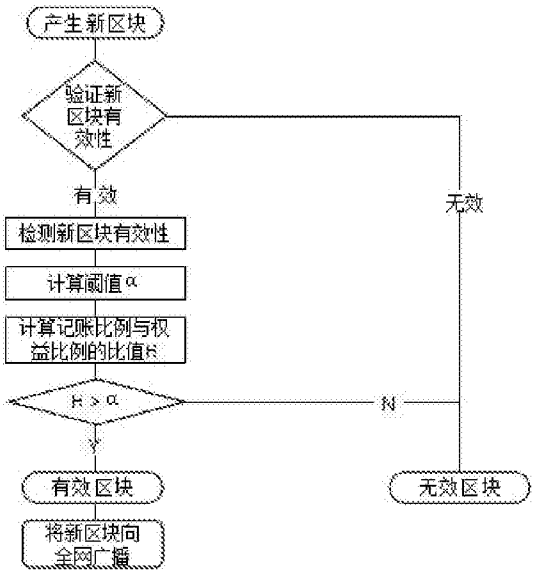
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种区块链共识机制

(57)摘要

本发明属于区块链技术领域，提供一种区块链共识机制。本发明的区块链共识机制基于权益证明共识机制，具体是当一个新区块产生时，检测产生所述新区块的地址的平均权益比例和记账比例，如果所述记账比例高于平均权益比例，则所述新区块被认为无效。采用本发明方法解决了权益证明共识机制中存在的算力攻击问题。



CN 106548397 A

1.一种区块链共识机制，基于权益证明共识机制，其特征在于：当一个新区块产生时，检测产生所述新区块的地址的平均权益比例和记账比例，如果所述记账比例高于平均权益比例，则所述新区块被认为无效。

2.根据权利要求1所述的区块链共识机制，其特征在于：所述平均权益比例与记账比例的比值小于阈值α时，所述新区块被认为无效。

3.根据权利要求1或2所述的区块链共识机制，其特征在于：所述平均权益比例A计算方法如下：

$$A = \frac{\sum_{i=1}^{n} P_i}{n}$$

其中，n为选取产生所述新区块的地址过去一段时间内产生的区块个数；P_i为选取的过去区块中第i个区块上该地址的权益比例。

4.根据权利要求1或2所述的区块链共识机制，其特征在于：所述记账比例B计算方法如下：

$$B = \frac{b}{N}$$

其中，N为选取过去一段时间内所有地址产生的全部区块个数；b为选取的过去一段时间内产生所述新区块的地址产生的区块个数。

5.根据权利要求2所述的区块链共识机制，其特征在于：所述阈值α的确定方法如下：

$$\alpha = \frac{tm}{t_0}$$

其中，t_0为标准出块间隔时间，m为标准冗余度，t为新区块之前两个区块的出块时间间隔。

一种区块链共识机制

技术领域

[0001] 本发明涉及区块链技术领域，具体地说是一种区块链共识机制。

背景技术

[0002] 区块链通俗地说就是一个公开的分布式账簿系统。以比特币的区块链为例，每一个参与交易者都是区块网络的节点，每个节点都有一份完整的公共账簿备份，上面记载着自比特币诞生以来所有的交易信息。任何一个节点发起交易行为都需要将相关信息传递到区块网络中的每一个节点，从而所有节点上的账簿都能验证这一笔交易行为并准确更新。此外，账簿是分区块存储的，随着交易的增加，新的数据块会附加到已存在的链上，形成链状结构。拓展开来，区块链能验证、转移和记载任何可以通过一致数学算法转化成数据的事实。其中交易封装成区块及区块加载到主链上，即记账权分配，是需要共识机制的方式完成。目前通常采用的区块链共识机制包括工作量证明、权益证明等方式。其中工作量证明，就是大家熟悉的挖矿，通过枚举与哈希运算，计算出一个满足规则的随机数，即获得本次记账权，发出本轮需要记录的数据，全网其它节点验证后一起存储。工作量证明方式的共识机制优点是完全去中心化，节点自由进出。缺点是目前比特币已经吸引全球大部分的算力，其它再用Pow共识机制的区块链应用很难获得相同的算力来保障自身的安全；挖矿造成大量的资源浪费；共识达成的周期较长，不适合商业应用。

[0003] 权益证明是目前常用的记账权分配方法，其核心实现如下：记账节点在产生新的区块时，将自己的地址附在区块中，以证明其占有的权益比例，记账节点同时也需要用该地址对应的私钥对部分区块信息签名，以证明其确实拥有该地址的资产。权益证明的出发点是，如果一个人在系统中占有的权益越多，那么他就越倾向于积极地维护这个系统的正常运行，理应更容易的获得记账权。因此长久看来，一个用户期望的记账比例，应当与其所占权益比例相等。然而，目前的权益证明方式均无法抵御算力攻击，即一个权益较少的用户，可通过投入大量的算力，获得远高于其权益比例的记账权。

发明内容

[0004] 本发明的目的是针对区块链权益证明共识机制现有技术的缺点，提出一种区块链共识机制，具体如下：当一个新区块产生时，检测产生所述新区块的地址的平均权益比例和记账比例，如果所述记账比例高于平均权益比例，则所述新区块被认为无效。

[0005] 优选的是，所述平均权益比例与记账比例的比值小于阈值α时，所述新区块被认为无效。

[0006] 优选的是，所述平均权益比例A计算方法如下：

[0007] $$A=\frac{\sum_{i=0}^{n}P_i}{n}$$

[0008] 其中，n为选取产生所述新区块的地址过去一段时间内产生的区块个数；P_i为选取的过去区块中第i个区块上该地址的权益比例。

[0009] 优选的是，所述记账比例B计算方法如下：

[0010] $$B=\frac{b}{N}$$

[0011] 其中，N为选取过去一段时间内所有地址产生的全部区块个数；b为选取的过去一段时间内产生所述新区块的地址产生的区块个数。

[0012] 优选的是，所述阈值α的确定方法如下：

[0013] $$\alpha=\frac{t_{0}m}{t}$$

[0014] 其中，t_0为标准出块间隔时间，m为标准冗余度，t为新区块之前两个区块的出块时间间隔。

[0015] 本发明有益效果如下：

[0016] 1.解决了权益证明中存在的算力攻击问题。

[0017] 2.自动调整记账冗余度，提高了出块的均匀性。

附图说明

[0018] 图1是实施例1中根据本发明的一种区块链共识机制流程图。

[0019] 图2是实施例2中根据本发明的一种区块链共识机制流程图。

具体实施方式

[0020] 下面结合附图对本发明作进一步详细描述，有必要在此指出的是，以下具体实施方式只用于对本发明进行进一步的说明，不能理解为对本发明保护范围的限制，该领域的技术人员可以根据上述发明内容对本发明作出一些非本质的改进和调整。

[0021] 本发明提出的一种区块链共识机制，是对权益证明共识机制的一种改进，解决了权益证明中存在的算力攻击问题。

[0022] 实施例1

[0023] 本发明提出的一种区块链共识机制，如图1所示，具体如下：

[0024] 步骤一、新的区块产生时，验证区块的有效性。

[0025] 验证区块的有效性指现有权益证明共识机制通常采用的区块验证方法。比如验证区块哈希是否有效，验证区块内每一笔交易是否有效，验证区块指向的前一个区块是否有效，验证前一个区块是否处于有效活动的区块链上，验证区块的哈希是否小于目标难度除以消耗的币龄，使用币龄消耗地址的公钥验证签名是否正确等。如果经过上述各个参数验证通过，则确定新区块有效，新区块有效后进行检测新的区块有效性。

[0026] 步骤二、检测新的区块有效性。

[0027] 检测产生所述新区块的地址的平均权益比例和记账比例，如果所述记账比例高于平均权益比例，则所述新区块被认为无效，否则将所述新区块向区块链全网广播。

[0028] 所述记账比例与平均权益比例的比值大于阈值α时，所述新区块被认为无效，否则将所述新区块向区块链全网广播。

[0029] 所述平均权益比例A计算方法如下：

[0030] $$A=\frac{\sum_{i=0}^{n}P_i}{n}$$

[0031] 其中，n为选取产生所述新区块的地址过去一段时间内产生的区块个数；P_i为选取的过去区块中第i个区块上该地址的权益比例。

[0032] 所述记账比例B计算方法如下：

[0033] $$B=\frac{b}{N}$$

[0034] 其中，N为选取过去一段时间内所有地址产生的全部区块个数；b为选取的过去一段时间内产生所述新区块的地址产生的区块个数。

[0035] 所述阈值α的确定方法如下：

[0036] $$\alpha=\frac{tm}{t_0}$$

[0037] 其中，t_0为标准出块间隔时间，m为标准冗余度，t为新区块之前两个区块的出块时间间隔。所述标准冗余度为一个指定的不小于1的系统参数，标准冗余度越大，系统的鲁棒性越好，但也越容易收到攻击。如在过去一段时间内，一个拥有20％权益的节点，最多允许打包全网30％的区块，则冗余度为150％。

[0038] 实施例2

[0039] 本发明提出的一种区块链共识机制，如图2所示，具体如下：

[0040] 步骤一、新的区块产生时，检测新的区块有效性。

[0041] 检测产生所述新区块的地址的平均权益比例和记账比例，如果所述记账比例高于平均权益比例，则所述新区块被认为无效。

[0042] 所述记账比例与平均权益比例的比值大于阈值α时，所述新区块被认为无效。

[0043] 所述平均权益比例A计算方法如下：

[0044] $$A=\frac{\sum_{i=0}^{n}P_i}{n}$$

[0045] 其中，n为选取产生所述新区块的地址过去一段时间内产生的区块个数；P_i为选取的过去区块中第i个区块上该地址的权益比例。比如，对于产生新区快的地址在过去产生的10个区块中，权益分别占比为10％，10％，10％，10％，10％，20％，20％，20％，20％，20％，则该地址的对于过去10个区块的平均区块占比为15％。

[0046] 所述记账比例B计算方法如下：

[0047] $$B=\frac{b}{N}$$

[0048] 其中，N为选取过去一段时间内所有地址产生的全部区块个数；b为选取的过去一段时间内产生所述新区块的地址产生的区块个数。

[0049] 所述阈值α的确定方法如下：

[0050] $$\alpha=\frac{tm}{t_0}$$

[0051] 其中，t_0为标准出块间隔时间，m为标准冗余度，t为新区块之前两个区块的出块时间间隔。所述标准冗余度为一个指定的不小于1的系统参数，标准冗余度越大，系统的鲁棒性越好，但也越容易受到攻击。比如在过去一段时间内，一个拥有20％权益的节点，最多允

许打包全网30％的区块，则冗余度为150％。

[0052] 步骤二、检测新区块有效后，验证新区块的有效性。

[0053] 验证区块的有效性指现有权益证明共识机制通常采用的区块验证方法。比如验证区块哈希是否有效，验证区块内每一笔交易是否有效，验证区块指向的前一个区块是否有效，验证前一个区块是否处于有效活动的区块链上，验证区块的哈希是否小于目标难度除以消耗的币龄，使用币龄消耗地址的公钥验证签名是否正确等。

[0054] 步骤三、验证通过后，将所述新区块向区块链全网广播。

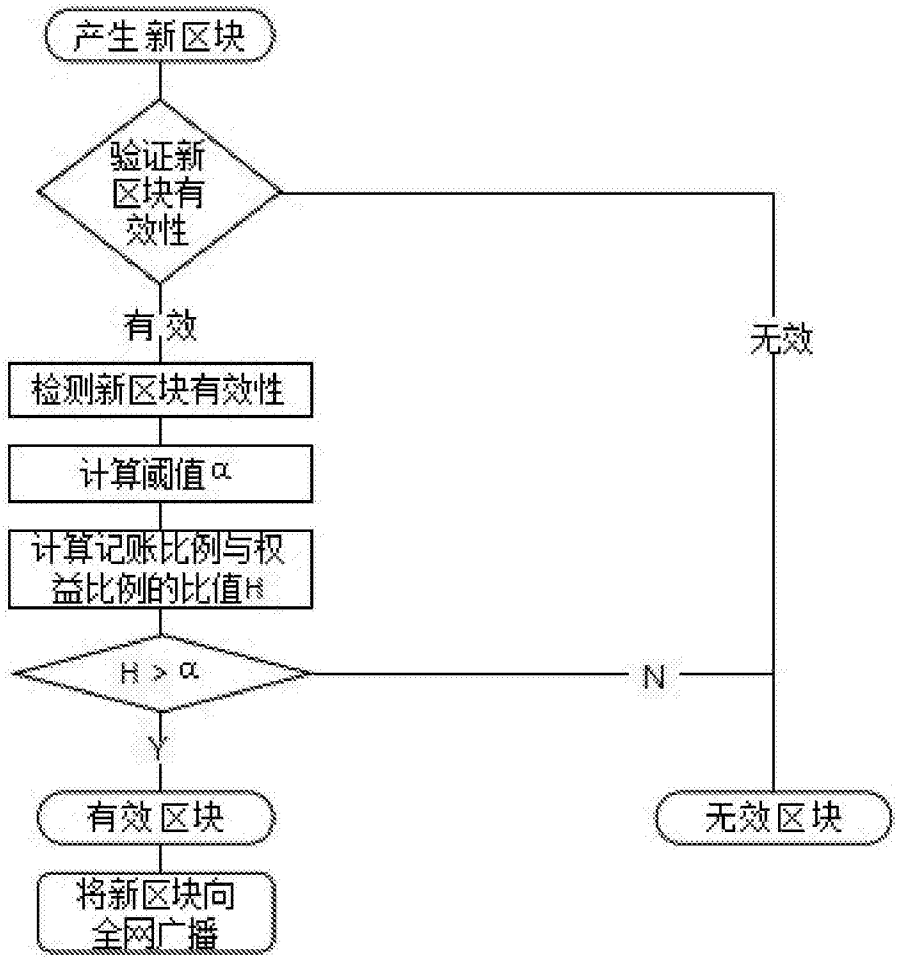

产生新区块
验证新区块有效性
有效
无效
检测新区块有效性
计算阈值α
计算记账比例与权益比例的比值H
H > α
N
Y
有效区块
无效区块
将新区块向全网广播

图1

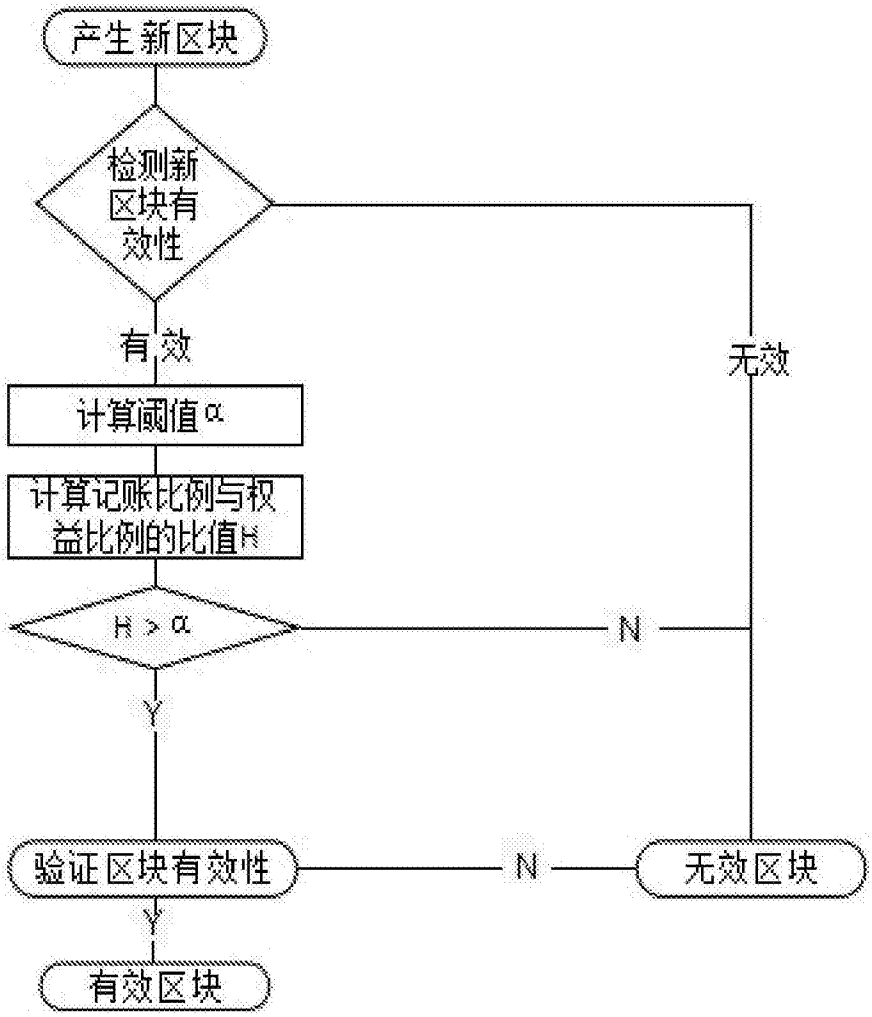

产生新区块
检测新区块有效性
有效
无效
计算阈值α
计算记账比例与权益比例的比值H
H > α
N
Y
验证区块有效性
N
无效区块
Y
有效区块

图2