(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 106296191 A
(43)申请公布日 2017.01.04

(21)申请号 201610669673.5

(22)申请日 2016.08.13

(71)申请人 深圳市樊溪电子有限公司
地址 518000 广东省深圳市南山区桃园街道龙珠二路龙都名苑4栋405

(72)发明人 张丛

(51)Int.Cl.
G06Q 20/38(2012.01)
G06F 9/50(2006.01)

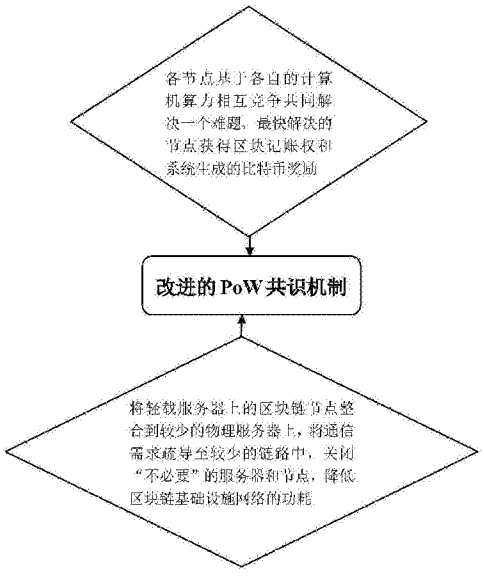
权利要求书2页 说明书4页 附图2页

(54)发明名称

一种区块链功耗感知的PoW共识机制

(57)摘要

本发明提供了一种区块链功耗感知的PoW共识机制，包括如下过程步骤：(1)在比特币系统中，各节点基于各自的计算机算力相互竞争共同解决一个求解复杂但验证容易的SHA数学难题，最快解决该难题的节点获得区块记账权和系统自动生成的比特币奖励；(2)采用WDM网状网将位于不同地理位置的物理服务器互联，构成区块链基础设施网络，响应区块连请求产生功耗，将轻载服务器上的区块链节点整合到较少的物理服务器上，将通信需求疏导至较少的链路中，关闭“不必要”的服务器和节点。采用该功耗感知PoW共识机制，在提高区块链性能的同时进一步挖掘基础设施网络的资源潜力，同时还能感知功耗，降低碳排放和温室效应。



CN 106296191 A

1.一种区块链功耗感知的PoW共识机制,其特征在于该共识机制包括如下过程步骤:

S1在比特币系统中,各节点基于各自的计算机算力相互竞争共同解决一个求解复杂但验证容易的SHA数学难题,最快解决该难题的节点获得区块记账权和系统自动生成的比特币奖励;

S2采用WDM网状网将位于不同地理位置的物理服务器互联,构成区块链基础设施网络,响应区块连请求产生功耗,将轻载服务器上的区块链节点整合到较少的物理服务器上,将通信需求疏导至较少的链路中,关闭"不必要"的服务器和节点。

2.根据权利要求1所述的一种区块链功耗感知的PoW共识机制,其特征在于:所述SHA数学难题可表述为根据当前难度值,通过搜索求解一个合适的随机数使得区块头各元数值的双SHA哈希值小于或者等于目标哈希值。

3.根据权利要求2所述的一种区块链功耗感知的PoW共识机制,其特征在于:所述比特币系统调整随机数搜索的难度值来控制区块的平均生成时间为6分钟。

4.根据权利要求2所述的一种区块链功耗感知的PoW共识机制,其特征在于:所述PoW共识的随机数搜索过程包括如下步骤:

D1搜集当前时间段的全网未确认交易,并增加一个用于发行新比特币奖励的Coinbase交易,形成当前区块体的交易集合;

D2计算区块体交易集合的Merkle根记入区块头,并填写区块头的其他元数据,其中随机数Nonce设置为零;

D3随机数Nonce加1,计算当前区块头的双SHA哈希值,如果小于或等于目标哈希值,则成功搜索到合适的随机数,并获得该区块的记账权;否则继续步骤D3直到任一节点搜索到合适的随机数为止;

D4如果一定时间内未成功,则更新时间戳和未确认交易集合、重新计算Merkle根后继续搜索。

5.根据权利要求1所述的一种区块链功耗感知的PoW共识机制,其特征在于:所述功耗包括与业务载荷相关的功耗和与业务载荷无关的功耗。

6.根据权利要求1所述的一种区块链功耗感知的PoW共识机制,其特征在于:使用混合整数规划(MIP)算法对功耗感知区块链建模。

7.根据权利要求6所述的一种区块链功耗感知的PoW共识机制,其特征在于:将功耗感知的区块连问题建模成数学优化问题求解,以最小化总的功耗为如下优化目标函数(1):

$$\text{Minimize}\{\eta \cdot P_{network}+\zeta \cdot P_{server}\} \quad (1)$$

目标函数试图最小化PoW共识机制下区块链的总功耗,包括网络功耗和服务器功耗,其中$\eta+\xi=1$,两者分别用来平衡网络功耗和服务器功耗的权重。

8.根据权利要求7所述的一种区块链功耗感知的PoW共识机制,其特征在于:求解所述优化目标函数(1)满足资源容量约束,位置约束条件为:节点"流量守恒";节点提供给区块连的资源量不超过自身可用资源量;用户低速率业务状态下每条链路所承载业务带宽总量不能超过容忍限度;以及底层物理网络长期总功耗最低。

9.根据权利要求6-8所述的一种区块链功耗感知的PoW共识机制,其特征在于:区块链节点映射和链路映射是协同考虑节点资源需求和邻近链路的带宽资源需求,根据资源需求量对节点进行将序排列后,计算区块链资源利用效率和接纳率,利用最低功耗路径有限原

则选择不同的功耗实施路径完成的，其中所述资源需求量为如下公式(2)：

$$RES(v) = req(v) + \sum_{e \in Adj(v)} b(e) \quad (2),$$

其中req(v)表示节点v的服务器资源需求量，b(e)表示链路e的链路带宽资源需求量，Adj(v)表示节点v的邻近链路集合。

10.根据权利要求9所述的一种区块链功耗感知的PoW共识机制，其特征在于：采用规一化惩罚因子算法计算所述资源需求量，获得节点和链路的分配机制。

一种区块链功耗感知的PoW共识机制

技术领域

[0001] 本发明涉及区块链PoW共识机制，特别是一种可功耗感知的区块链PoW共识机制。

背景技术

[0002] 2009年比特币的出现带来了一种颠覆性的成果--区块链技术，区块链是一个安全的帐簿类数据库，由一个个数据区块组成，使用者可以在这个不断更新升级的平台查找数据，对于金融机构来说，区块链能加快交易处理过程、降低成本、减少中间人、提高市场洞察力，增加业务透明度。

[0003] 如何在分布式系统中高效达成共识是分布式计算领域的重要研究问题，区块链的优势之一就在于能够在决策权高度分散的去中心化系统中使得各个节点高效的针对区块数据的有效性达成共识。早期的比特币区块链采用高度依赖节点算力的工作量证明，即Proof of work，也就是PoW机制保证比特币网络分布式记账的一致性，其核心思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性，其近乎完美的整合了比特币系统的货币发行、交易支付和验证功能，通过算力竞争保障系统的安全性和去中心性，PoW共识机制也存在非常显著的缺陷，其强大算力造成资源浪费，比如电力，长达10分钟的交易确认时间使其相对不适合小额交易的商业应用。

[0004] 目前提出PoS共识机制来解决资源浪费和安全性缺陷问题，其本质上是采用权益证明替代PoW中的基于哈希算力的工作量证明，是由系统中具有最高权益而非最高算力的节点获得区块记账权，然而其共识过程仅仅靠内部币龄和权益，而不需要消耗外部算力和资源，解决了算力浪费问题，但是算力却大打折扣。

[0005] 我们知道，区块链是和云计算完全不同的计算方式，从某种意义上来说，两者是对立的，然而基于网络虚拟化技术的云计算却可以在满足服务水平协议SLAs的前提下进行功耗感知，在提高网络性能的同时进一步挖掘基础设施网络的资源潜力，同时还能感知功耗，降低碳排放和温室效应。

发明内容

[0006] 本发明的目的在于提供一种区块链功耗感知的PoW共识机制，该共识机制包括如下过程步骤：(1)在比特币系统中，各节点基于各自的计算机算力相互竞争共同解决一个求解复杂但验证容易的SHA数学难题，最快解决该难题的节点获得区块记账权和系统自动生成的比特币奖励；(2)采用WDM网状网将位于不同地理位置的物理服务器互联，构成区块链基础设施网络，响应区块链请求产生功耗，将轻载服务器上的区块链节点整合到较少的物理服务器上，将通信需求疏导至较少的链路中，关闭“不必要”的服务器和节点。

[0007] 优选的，所述SHA数学难题可表述为根据当前难度值，通过搜索求解一个合适的随机数使得区块头各元数值的双SHA哈希值小于或者等于目标哈希值。

[0008] 优选的，所述比特币系统调整随机数搜索的难度值来控制区块的平均生成时间为6分钟。

[0009] 优选的，所述PoW共识的随机数搜索过程包括如下步骤：(1)搜集当前时间段的全网未确认交易，并增加一个用于发行新比特币奖励的Coinbase交易，形成当前区块体的交易集合；(2)计算区块体交易集合的Merkle根记入区块头，并填写区块头的其他元数据，其中随机数Nonce设置为零；(3)随机数Nonce加1，计算当前区块头的双SHA哈希值，如果小于或等于目标哈希值，则成功搜索到合适的随机数，并获得该区块的记账权；否则继续步骤(3)直到任一节点搜索到合适的随机数为止；(4)如果一定时间内未成功，则更新时间戳和未确认交易集合、重新计算Merkle根后继续搜索。

[0010] 优选的，所述功耗包括与业务载荷相关的功耗和与业务载荷无关的功耗。

[0011] 优选的，使用混合整数规划(MIP)算法对功耗感知区块链建模。

[0012] 采用该功耗感知PoW共识机制，在提高区块链性能的同时进一步挖掘基础设施网络的资源潜力，同时还能感知功耗，降低碳排放和温室效应。

[0013] 根据下文结合附图对本发明具体实施例的详细描述，本领域技术人员将会更加明了本发明的上述以及其他目的、优点和特征。

附图说明

[0014] 后文将参照附图以示例性而非限制性的方式详细描述本发明的一些具体实施例。附图中相同的附图标记标示了相同或类似的部件或部分。本领域技术人员应该理解，这些附图未必是按比例绘制的。本发明的目标及特征考虑到如下结合附图的描述将更加明显，附图中：

[0015] 图1为根据本发明实施例的区块链功耗感知的PoW共识机制示意图。

[0016] 图2为根据本发明实施例的PoW共识机制随机数搜索流程图

具体实施方式

[0017] 在进行具体实施方式的说明之前，为了更为清楚的表达所论述的内容，首先定义一些非常重要的概念。

[0018] 交易：交易的实质是个关系数据结构，这个数据结构中包含交易参与者价值转移的相关信息。这些交易信息被称为记账总账簿。交易需经过三个创建、验证、写入区块链。交易必须经过数字签名，保证交易的合法性。

[0019] 区块：所有的交易信息存放于区块中，一条交易信息就是一条记录，作为一个独立的记录存放于区块链中。区块由区块头部和数据部分组成，区块头字段包含区块本身的各种特性，例如前一区块信息，merkle值及时间戳等。其中区块头哈希值和区块高度是标识区块最主要的两个指标。区块主标识符是它的加密哈希值，一个通过SHA算法对区块头进行二次哈希计算而得到的数字指纹。产生的32字节哈希值被称为区块哈希值，或者区块头哈希值，只有区块头被用于计算。区块哈希值可以唯一、明确地标识一个区块，并且任何节点通过简单地对区块头进行哈希计算都可以独立地获取该区块哈希值。

[0020] 区块链：由区块按照链式结构有序链接起来的数据结构。区块链就像一个垂直的堆栈，第一个区块作为栈底的首区块，随后每个区块都被放置在其他区块之上。当区块写入区块链后将永远不会改变，并且备份到其他的区块链服务器上。

[0021] 实施例：参见图1，一种区块链功耗感知的PoW共识机制，该共识机制包括如下过程

步骤：(1)在比特币系统中，各节点基于各自的计算机算力相互竞争共同解决一个求解复杂但验证容易的SHA数学难题，最快解决该难题的节点获得区块记账权和系统自动生成的比特币奖励；(2)采用WDM网状网将位于不同地理位置的物理服务器互联，构成区块链基础设施网络，响应区块链请求产生功耗，将轻载服务器上的区块链节点整合到较少的物理服务器上，将通信需求疏导至较少的链路中，关闭“不必要”的服务器和节点。

[0022] SHA数学难题可表述为根据当前难度值，通过搜索求解一个合适的随机数使得区块头各元数值的双SHA哈希值小于或者等于目标哈希值。比特币系统调整随机数搜索的难度值来控制区块的平均生成时间为小于10分钟，最好是6分钟以内，以满足快速处理交易的需求。

[0023] 参见图2，PoW共识的随机数搜索过程包括如下步骤：(1)搜集当前时间段的全网未确认交易，并增加一个用于发行新比特币奖励的Coinbase交易，形成当前区块体的交易集合；(2)计算区块体交易集合的Merkle根记入区块头，并填写区块头的其他元数据，其中随机数Nonce设置为零；(3)随机数Nonce加1，计算当前区块头的双SHA哈希值，如果小于或等于目标哈希值，则成功搜索到合适的随机数，并获得该区块的记账权；否则继续步骤(3)直到任一节点搜索到合适的随机数为止；(4)如果一定时间内未成功，则更新时间戳和未确认交易集合、重新计算Merkle根后继续搜索。功耗包括与业务载荷相关的功耗和与业务载荷无关的功耗，与业务载荷无关的功耗称为无用功耗，在功耗感知的PoW共识机制中，可以通过降低不必要的基本功耗来达到节能的目的，将工作状态分为激活模式和关闭模式。本实施例中，区块链的两个节点a和d被映射到物理服务器S1上，而其余的两个节点b和e被整合到物理服务器S2上，另外两个基点c和f整合到物理服务器S3上，而链路(a-b)和(d-e)均被映射到物理路径(A-B)上，链路(b-c)和(e-f)映射到物理路径(B-C)上，链路(c-a)和(f-d)被映射到物理路径(C-A)上，在该功耗感知的区块链映射中，通过业务载荷的整合和疏导，关闭不必要的服务器和节点，降低功耗大约50％。在映射服务器的算法中，使用混合整数规划(MIP)算法对功耗感知区块链建模，将功耗感知的区块连问题建模成数学优化问题求解，以最小化总的功耗为优化目标函数，定义如下：

[0024] $\text{Minimize}\{\eta \cdot P_{network}+\zeta \cdot P_{server}\}$ (1)

[0025] 目标函数试图最小化PoW共识机制下区块链的总功耗，包括网络功耗和服务器功耗，其中$\eta+\zeta=1$，两者分别用来平衡网络功耗和服务器功耗的权重。同时，需要满足一些特定的约束条件，包括资源容量约束，位置约束等，约束条件为：

[0026] (1)节点“流量守恒”；

[0027] (2)节点提供给区块连的资源量不超过自身可用资源量；

[0028] (3)用户低速率业务状态下每条链路所承载业务带宽总量不能超过容忍限度

[0029] (4)底层物理网络长期总功耗最低。

[0030] 当求解目标函数完成后，需要完成剩余的两个重要工作，区块链节点映射和链路映射，协同考虑节点资源需求和邻近链路的带宽资源需求，根据资源需求量对节点进行将序排列后，计算区块链资源利用效率和接纳率，利用最低功耗路径有限原则选择不同的功耗实施路径。其中资源需求量定义为：

[0031] $$RES(v) = req(v) + \sum_{e \in Adj(v)} b(e) \quad (2),$$

[0032] 其中req(v)表示节点v的服务器资源需求量，b(e)表示链路e的链路带宽资源需求量，Adj(v)表示节点v的邻近链路集合。

[0033] 采用规一化惩罚因子算法计算上述资源需求量即可获得节点和链路的分配机制。

[0034] 虽然本发明已经参考特定的说明性实施例进行了描述，但是不会受到这些实施例的限定而仅仅受到附加权利要求的限定。本领域技术人员应当理解可以在不偏离本发明的保护范围和精神的情况下对本发明的实施例能够进行改动和修改。

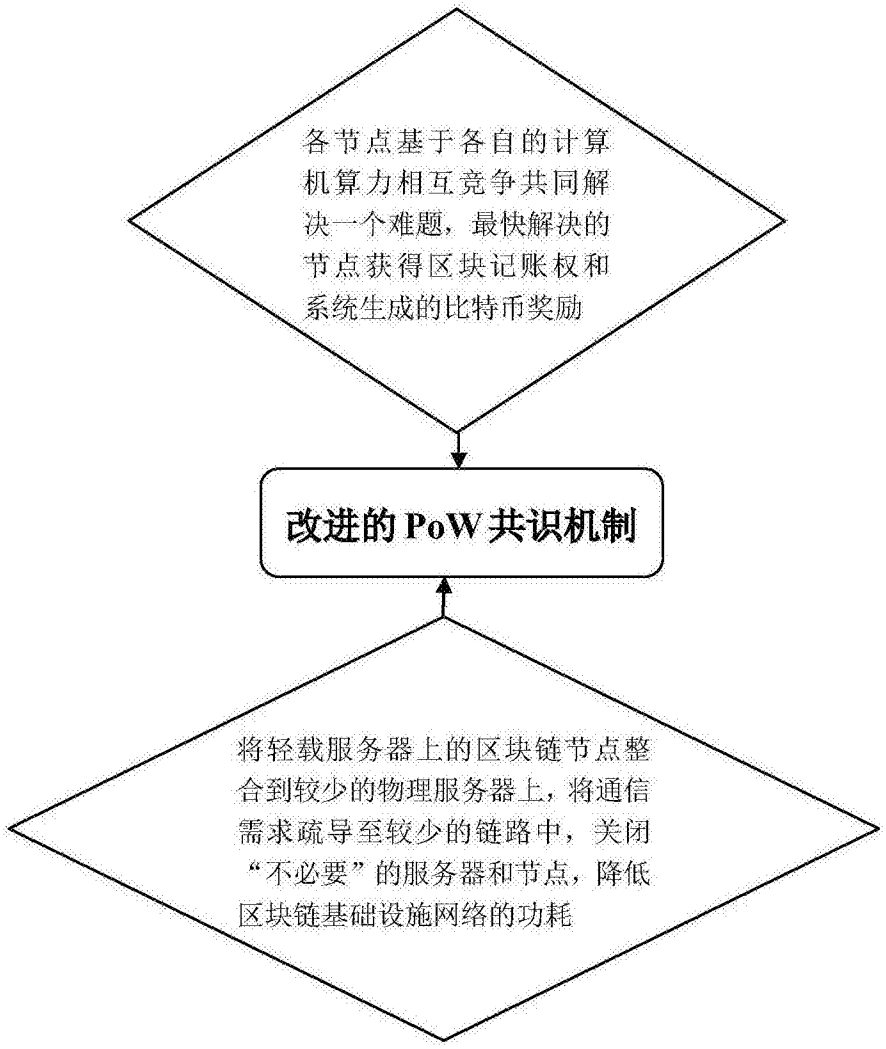

各节点基于各自的计算机算力相互竞争共同解决一个难题，最快解决的节点获得区块记账权和系统生成的比特币奖励
改进的PoW共识机制
将轻载服务器上的区块链节点整合到较少的物理服务器上，将通信需求疏导至较少的链路中，关闭“不必要”的服务器和节点，降低区块链基础设施网络的功耗

图1

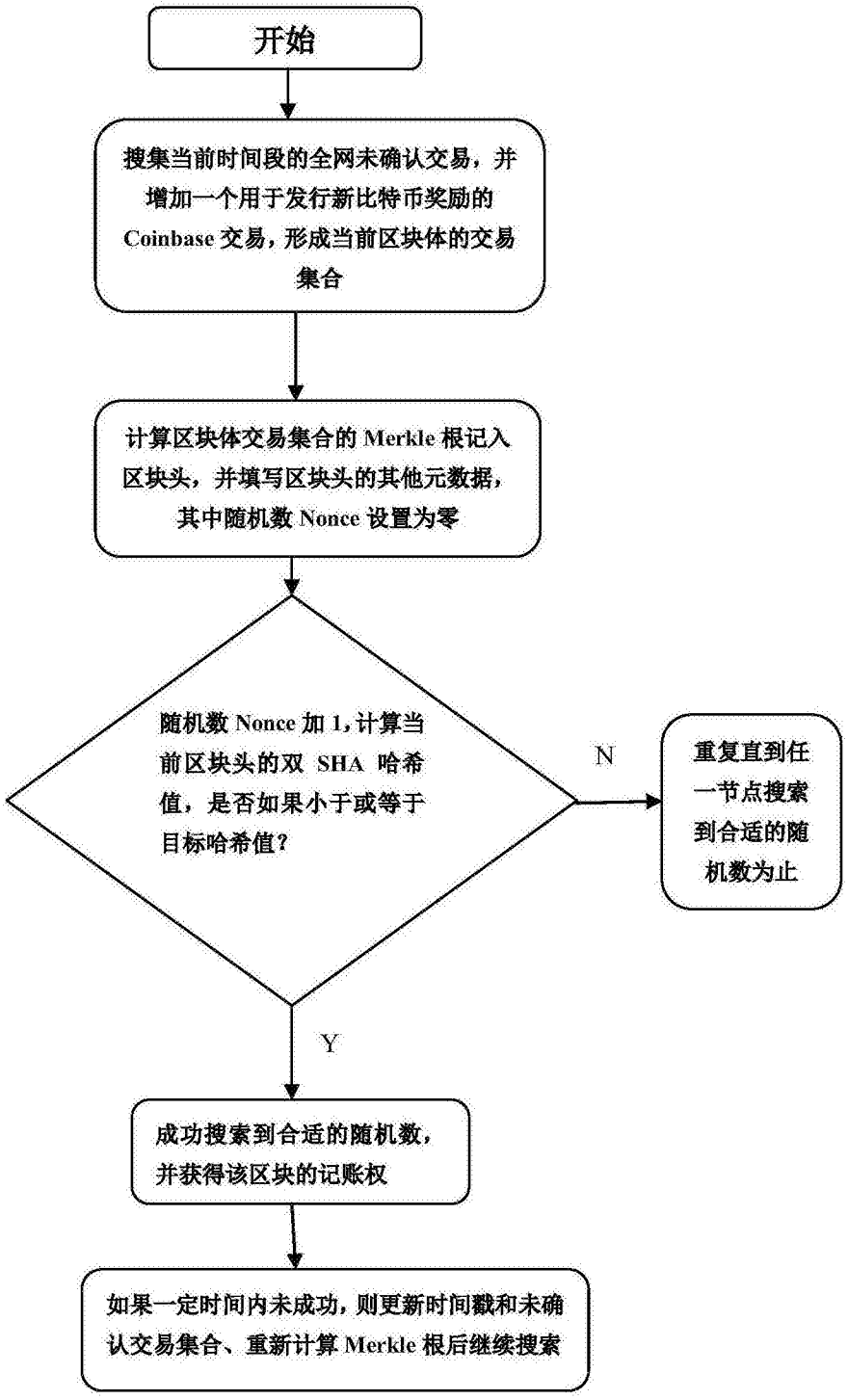

开始
搜集当前时间段的全网未确认交易，并增加一个用于发行新比特币奖励的 Coinbase 交易，形成当前区块体的交易集合
计算区块体交易集合的 Merkle 根记入区块头，并填写区块头的其他元数据，其中随机数 Nonce 设置为零
随机数 Nonce 加 1，计算当前区块头的双 SHA 哈希值，是否如果小于或等于目标哈希值？
N
重复直到任一节点搜索到合适的随机数为止
Y
成功搜索到合适的随机数，并获得该区块的记账权
如果一定时间内未成功，则更新时间戳和未确认交易集合、重新计算 Merkle 根后继续搜索

图2