(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 111031076 B
(45)授权公告日 2020.07.10

(21)申请号 202010151274.6

(22)申请日 2020.03.06

(65)同一申请的已公布的文献号
申请公布号 CN 111031076 A

(43)申请公布日 2020.04.17

(73)专利权人 南京畅洋科技有限公司
地址 211135 江苏省南京市江宁区创研路266号7号楼3楼

(72)发明人 陈立全 姬磊 唐敏 顾朋鹏 陈垚

(74)专利代理机构 北京汇捷知识产权代理事务所(普通合伙) 11531
代理人 邢文月

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
H04L 12/18(2006.01)

(56)对比文件
CN 110278091 A,2019.09.24

审查员 郝玉香

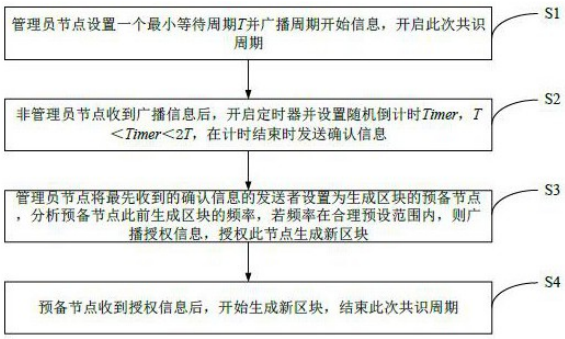
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种基于定时机制的物联网区块链共识方法

(57)摘要

本发明公开了一种基于定时机制的物联网区块链共识方法,包括步骤:S1、管理员节点设置一个最小等待周期*T*后广播共识开始信息,开启此次共识周期;S2、非管理员节点收到广播信息后开启定时器并设置随机倒计时*Timer*,*T*<*Timer*<2*T*,在倒计时结束时发送确认信息;S3、管理员节点将最先收到的确认信息的发送者设置为生成区块的预备节点,分析预备节点此前生成区块的频率,若频率在预设范围内,则广播信息授权此节点生成新区块;S4、预备节点收到授权信息生成新区块,结束此次共识周期。本发明可以实现区块链技术应用于计算和存储能力较弱的物联网中,能够实现高吞吐量区块链的应用,还可以弥补以往区块链应用大量消耗计算、存储、带宽的缺陷。



CN 111031076 B

1.一种基于定时机制的物联网区块链共识方法，其特征在于，该方法包括以下步骤：

S1、管理员节点设置一个最小等待周期T并广播共识开始信息，开启此次共识周期；

S2、非管理员节点收到广播共识开始信息后开启定时器并设置随机倒计时$Timer$，$T<Timer<2T$，并在倒计时结束时发送确认信息；

S3、管理员节点将最先收到的确认信息的发送者设置为生成区块的预备节点，分析该预备节点此前生成区块的频率，若频率在预设范围内，则广播授权信息，授权此节点生成新区块；

S4、预备节点收到授权信息后，开始生成新区块，结束此次共识周期。

2.如权利要求1所述的基于定时机制的物联网区块链共识方法，其特征在于，在步骤S1中，所述最小等待周期T的大小为管理员节点到其他非管理员节点之间的最大端到端通信时延。

3.如权利要求1所述的基于定时机制的物联网区块链共识方法，其特征在于，在步骤S2之后还包括步骤：

S30、若管理员节点在开启共识周期后的4倍最小等待周期后仍未收到确认消息，则广播提前结束此次共识周期，重复步骤S1。

4.如权利要求3所述的基于定时机制的物联网区块链共识方法，其特征在于，在步骤S2之后还包括步骤：

S31、若多个节点消息同时到达，管理员节点根据节点定时器时间Timer和生成区块的频率$freq$选择$Timer*freq$值最小的节点作为预备节点。

5.如权利要求4所述的基于定时机制的物联网区块链共识方法，其特征在于，所述S31之后还包括步骤：

S32、管理员节点根据频率$freq$是否超过设定的阈值f_{Thr}来判断此预备节点是否为恶意节点，如频率$freq>f_{Thr}$则废除其生成区块的权利，并将其从网络中剔除，提前结束此次共识周期，重复步骤S1。

6.如权利要求1所述的基于定时机制的物联网区块链共识方法，其特征在于，在步骤S3之后还包括步骤：

S5、其他非授权节点根据广播的授权信息，对该授权节点拥有生成新区块的权利达成共识。

一种基于定时机制的物联网区块链共识方法

技术领域

[0001] 本发明属于区块链关键技术领域，尤其涉及一种基于定时机制的物联网区块链共识方法。

背景技术

[0002] 目前在物联网领域中，应用区块链技术构建的系统还处于发展时期，目前的研究主要集中在理论层面，包括以下几个方面：身份认证系统，供应链溯源，小额交易，数据存储管理等。然而，区块链中如何在不同应用场景下使得不可信节点间达成共识是一个由来已久的重要问题。早在1980年，这个问题被描述为拜占庭将军问题：有一队将军想要攻陷一座城，但这队军队中，有一部分军人打算进攻，另一部分打算撤退，如何在这支军队中达成共识的问题。现阶段常用的共识方法有：工作量证明(PoW)、权益证明(PoS)和实用拜占庭容错(PBFT)。PoW的做法是通过让节点不停地进行Hash运算来得到大家认可的Hash值，进而在节点间达成共识，需要消耗大量资源用于争夺记账权，效率低下，而且物联网设备并不适合做大量的运算；PoS解决了工作量证明过于浪费资源的问题，但是引入了新的安全问题，权益证明即持币越多被选为生成区块的节点概率越大，但是拥有少量财产的节点进行恶意操作的成本低，可能导致区块链分叉，PoS也不适合充当物联网区块链的共识方法。PBFT可以授权节点动态加入，相对来说较为适用于物联网应用场景，但是共识过程中有两次平方级别复杂度的数据量传输，物联网设备之间通信带宽有限，导致整个共识过程效率低，因此PBFT也不能直接用作物联网区块链的共识方法。因此，找到一种可以适用到物联网区块链中的共识方法非常重要。

发明内容

[0003] 本发明针对现有区块链共识方法不适用物联网系统的问题，提供一种基于定时机制的物联网区块链共识方法，利用节点自带的定时器来实现在一个共识周期内，在非管理员节点中随机选取且仅选取一个节点获得生成区块的权利。

[0004] 本发明是这样实现的，本发明公开了一种基于定时机制的物联网区块链共识方法，该方法包括以下步骤：

[0005] S1、管理员节点设置一个最小等待周期T并广播共识开始信息，开启此次共识周期；

[0006] S2、非管理员节点收到广播共识开始信息后开启定时器并设置随机倒计时Timer，T＜Timer＜2T，并在倒计时结束时发送确认信息；

[0007] S3、管理员节点将最先收到的确认信息的发送者设置为生成区块的预备节点，分析该预备节点此前生成区块的频率，若频率在预设范围内，则广播授权信息，授权此节点生成新区块；

[0008] S4、预备节点收到授权信息后，开始生成新区块，结束此次共识周期。

[0009] 优选地，在步骤S1中，所述最小等待周期T的大小为管理员节点到其他非管理员节

点之间的最大端到端通信时延。

[0010] 优选地，在步骤S2之后还包括步骤：S30、若管理员节点在开启共识周期后的4倍最小等待周期后仍未收到确认消息，则广播提前结束此次共识周期，重复步骤S1。

[0011] 优选地，在步骤S2之后还包括步骤：S31、若多个节点消息同时到达，管理员节点根据节点定时器时间Timer和生成区块的频率freq选择Timer*freq值最小的节点作为预备节点。

[0012] 优选地，所述S31之后还包括步骤：S32、管理员节点根据频率freq是否超过设定的阈值f_{Thr}来判断此预备节点是否为恶意节点，如频率freq＞f_{Thr}则废除其生成区块的权利，并将其从网络中剔除，提前结束此次共识周期，重复步骤S1。

[0013] 优选地，在步骤S3之后还包括步骤：S5、其他非授权节点根据广播的授权信息对该授权节点拥有生成新区块的权利达成共识。

[0014] 本发明克服现有技术的不足，提供一种基于定时机制的物联网区块链共识方法，该共识方法是一种基于节点设置的定时器时间，随机选择合适的节点负责新区块的生成；其中，每个节点都设有一个定时器，在每个共识周期开启时，管理员节点将广播一条消息，其中包括确定的最小等待周期；每个节点在接收到这条消息后将自己的定时器重置为一个大于最小等待周期小于两倍最小等待周期的值，定时器停止时立即向管理员节点发送确认消息，管理员节点判断最先收到的确认消息的发送节点生成区块的频率合理后，广播授权其获得生成新区块的权利。为防止网络中存在恶意节点无限制的广播区块，管理员节点在收到确认消息时需要对该节点产生区块的频率进行检测，如果发现有节点产生区块的频率超过了一个限定的阈值，该节点会被移出网络，直到该节点重新生成新的身份标识积累可信赖度。

[0015] 相比于现有技术的缺点和不足，本发明具有以下有益效果：

[0016] (1)本发明可以实现区块链技术应用于计算和存储能力较弱的物联网中；

[0017] (2)本发明能够实现高吞吐量区块链的应用，满足物联网设备通信效率要求；

[0018] (3)本发明可以在一定程度上弥补以往区块链应用大量消耗计算、存储、带宽的缺陷，使得区块链技术真正在物联网中实现。

附图说明

[0019] 图1是本发明基于定时机制的物联网区块链共识方法实施方式的步骤流程图；

[0020] 图2是本发明基于定时机制的物联网区块链共识方法实施方式的运算流程图。

具体实施方式

[0021] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0022] 本发明公开了一种基于定时机制的物联网区块链共识方法，如图1所示，该方法包括以下步骤：

[0023] S1、管理员节点设置一个最小等待周期T并广播周期开始信息，开启此次共识周期

[0024] 在步骤S1中，所述最小等待周期T的大小为管理员节点到其他非管理员节点之间

的最大端到端通信时延。

[0025] S2、非管理员节点收到广播信息后，开启定时器并设置随机倒计时Timer，T＜Timer＜2T，在计时结束时发送确认信息

[0026] S3、管理员节点将最先收到的确认信息的发送者设置为生成区块的预备节点，分析预备节点此前生成区块的频率，若频率在预设范围内，则广播授权信息，授权此节点生成新区块

[0027] S4、预备节点收到授权信息后，开始生成新区块，结束此次共识周期。

[0028] 在本发明实施例中，为避免步骤S2中管理员节点不能收到确认信息的问题，在步骤S2之后还包括步骤：

[0029] S30、若管理员节点在开启共识周期后的4倍最小等待周期后仍未收到确认消息，则广播提前结束此次共识周期，重复步骤S1。

[0030] 在本发明实施例中，为解决多个节点消息同时到达的问题，在步骤S2之后还包括步骤：

[0031] S31、若多个节点消息同时到达，管理员节点根据节点定时器时间Timer和生成区块的频率freq选择Timer*freq值最小的节点的作为预备节点。

[0032] 在本发明实施例中，根据实际应用情况，所述S31之后还包括步骤：

[0033] S32、管理员节点根据频率freq是否超过设定的阈值f_{Thr}来判断此预备节点是否为恶意节点，如频率freq＞f_{Thr}则废除其生成区块的权利，并将其从网络中剔除，提前结束此次共识周期，重复步骤S1。

[0034] 此外，在步骤S3之后还包括步骤：

[0035] S5、其他非授权节点根据广播的授权信息，对该授权节点拥有生成区块的权利达成共识。

[0036] 本发明在实际应用过程中，如图2所示，该方法的实际运算流程更具体包括以下步骤：

[0037] 步骤101：设置一个最小等待周期T；

[0038] 本实施例中，采用N＝20个节点的网络组建物联网区块链，设置最小共识周期为1s；

[0039] 步骤102：管理员节点广播信息，信息中包含步骤101中确定最小等待周期，开启共识周期；

[0040] 步骤103：其他所有非管理员节点收到管理员广播的开启共识周期的信息后开启定时器；

[0041] 步骤103中，节点定时器时间Timer为随机产生的一个大于最小等待周期小于2倍最小等待周期，在本实例中即1～2s的随机数；

[0042] 步骤104：定时器停止时，则节点立即向管理员节点发送确认消息；

[0043] 步骤105：管理员节点在共识周期开启的4倍最小等待周期内仍未收到任何节点发送确认消息，在本实例中即自广播信息后的4s中仍未收到确认消息，则提前结束此次共识周期，即跳转到步骤110，否则进入步骤106；

[0044] 步骤106：管理员节点将最先收到的确认消息的发送者设置为生成区块的预备节点，若同时收到多个节点发送的确认消息，则选择Timer*freq最小的节点为唯一预备节点；

[0045] 步骤107:管理员节点分析此预备节点生成区块的频率是否合理,若频率freq高于设定的阈值$f_{Thr}=\sqrt{2\pi}*N_{\text{blocks}}/N_{\text{nodes}}$,则取消其生成区块的权利,并将其从区块链网络中剔除,提前结束此次共识周期,即进入步骤110,否则进入步骤108(N_{blocks}为当前共识周期内区块链账本中的区块数量,N_{nodes}为当前共识周期内区块链网络中节点数量);

[0046] 步骤108:管理员节点广播授权信息,授权此预备节点生成新区块的权利;

[0047] 步骤109:节点收到管理员节点广播的授权信息后,预备节点开始生成新的区块;

[0048] 步骤110:共识周期结束。

[0049] 以上所述仅为本发明的较佳实施例而已,并不用以限制本发明,凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等,均应包含在本发明的保护范围之内。

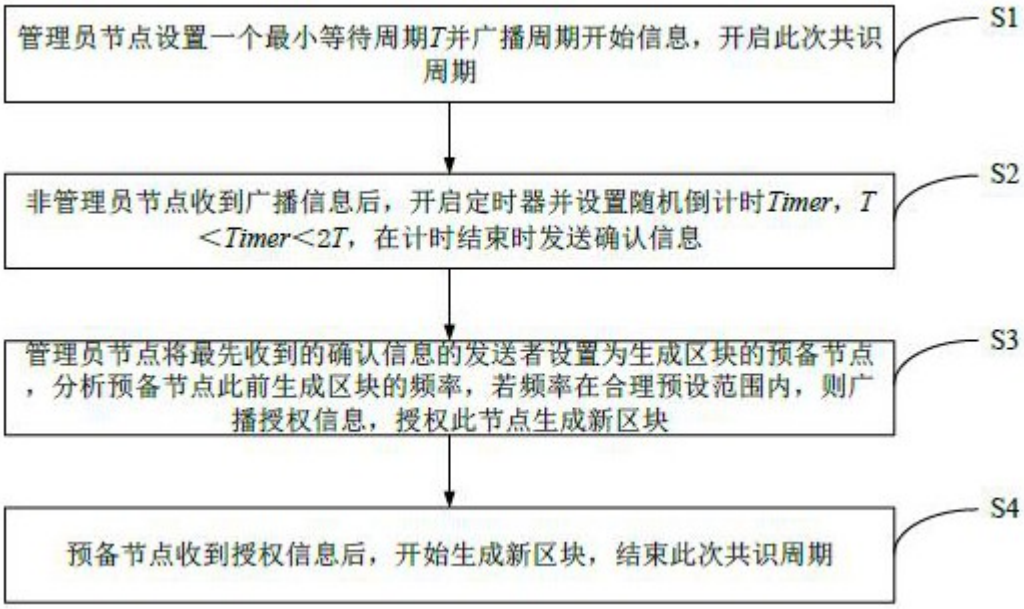

管理员节点设置一个最小等待周期T并广播周期开始信息，开启此次共识周期
S1
非管理员节点收到广播信息后，开启定时器并设置随机倒计时Timer，T＜Timer＜2T，在计时结束时发送确认信息
S2
管理员节点将最先收到的确认信息的发送者设置为生成区块的预备节点，分析预备节点此前生成区块的频率，若频率在合理预设范围内，则广播授权信息，授权此节点生成新区块
S3
预备节点收到授权信息后，开始生成新区块，结束此次共识周期
S4

图1

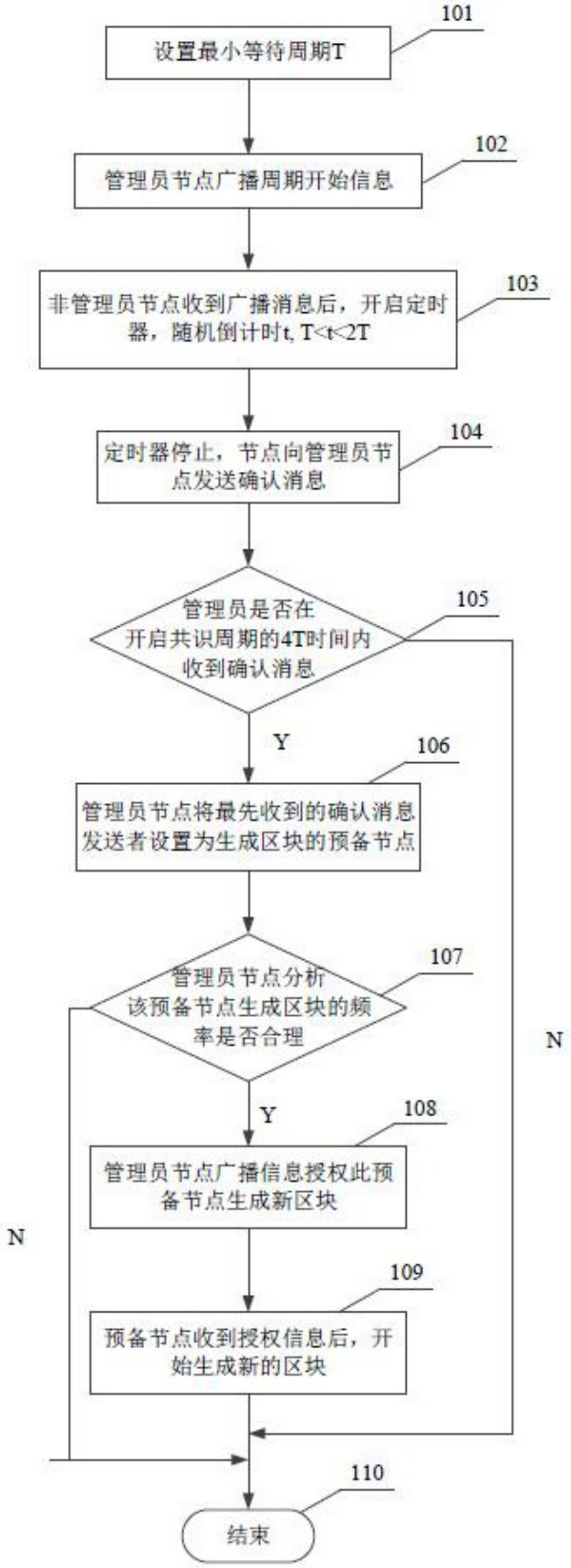

101
设置最小等待周期T
102
管理员节点广播周期开始信息
103
非管理员节点收到广播消息后，开启定时器，随机倒计时t, T<t<2T
104
定时器停止，节点向管理员节点发送确认消息
105
管理员是否在开启共识周期的4T时间内收到确认消息
Y
N
106
管理员节点将最先收到的确认消息发送者设置为生成区块的预备节点
107
管理员节点分析该预备节点生成区块的频率是否合理
Y
N
108
管理员节点广播信息授权此预备节点生成新区块
109
预备节点收到授权信息后，开始生成新的区块
110
结束

图2