(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 106878071 A
(43)申请公布日 2017.06.20

(21)申请号 201710062689.4

(22)申请日 2017.01.25

(71)申请人 上海钜真金融信息服务有限公司
地址 200127 上海市浦东新区中国(上海)自由贸易试验区峨山路111号4幢129室

(72)发明人 李升林 陈晋飞 姜海涛 寮岩

(74)专利代理机构 上海汉声知识产权代理有限公司 31236
代理人 胡晶

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/08(2006.01)
G06Q 40/00(2012.01)

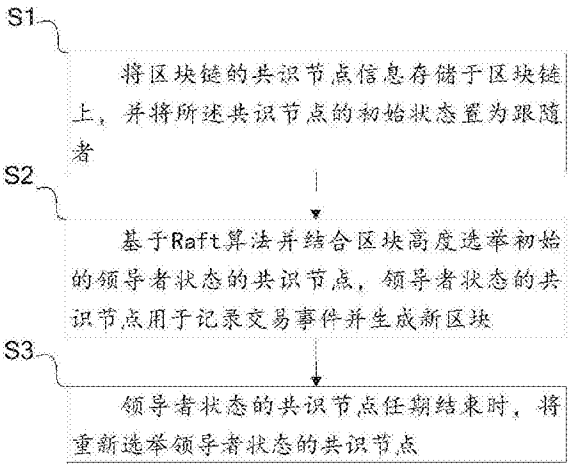
权利要求书1页 说明书5页 附图3页

(54)发明名称

一种基于Raft算法的区块链共识机制

(57)摘要

一种基于Raft算法的区块链共识机制,包括步骤:将区块链的共识节点信息存储于区块链上,并将共识节点的初始状态置为跟随者;基于Raft算法并结合区块高度选举初始领导者状态的共识节点,领导者状态的共识节点用于记录交易事件并生成新区块;领导者状态的共识节点任期结束时,将重新选举领导者状态的共识节点。由于领导者状态的共识节点选举过程中参考其所同步的区块高度,可提高共识效率,缩短交易确认时间,任期结束后重新选举新的共识节点,提高系统容错性,并且,领导者状态的共识节点选举的唯一性,使得每个区块都有最终一致性,不会出现区块链分叉情况,同时,通过智能合约对共识节点的管理机制,能实现共识节点动态加入退出。



CN 106878071 A

1.一种基于Raft算法的区块链共识机制，其特征在于，包括步骤：

将区块链的共识节点信息存储于区块链上，所述共识节点的状态包括：领导者、跟随者和候选者，并将所述共识节点的初始状态置为跟随者；

基于Raft算法并结合区块高度选举初始领导者状态的共识节点，所述领导者状态的共识节点用于记录交易事件并生成新区块；

所述领导者状态的共识节点任期结束时，将重新选举领导者状态的共识节点。

2.如权利要求1所述的区块链共识机制，其特征在于，选举初始领导者状态的共识节点之前，还包括初始化各个所述共识节点的选举定时器的步骤。

3.如权利要求2所述的区块链共识机制，其特征在于，所述基于Raft算法并结合区块高度选举初始领导者状态的共识节点，包括步骤：

所述共识节点的选举定时器被触发时，被触发的所述共识节点由跟随者状态转换为候选者状态；

所述候选者状态的共识节点向跟随者状态的共识节点发送邀票信息，所述邀票信息包含其所拥有的区块高度；

所述跟随者状态的共识节点判断所述邀票信息中的区块高度是否大于或等于自身区块高度，若是，向所述候选者状态的共识节点投票；

判断所述候选者状态的共识节点所得票数是否大于或等于N/2+1，若是，将所述共识节点由候选者状态转换为领导者状态，N为共识节点的个数。

4.如权利要求1所述的区块链共识机制，其特征在于，重新选举领导者状态的共识节点，包括步骤：

当前领导者状态的共识节点向跟随者状态的共识节点广播新区块的区块高度，并随机推荐一个跟随者状态的共识节点，所述被推荐的共识节点由跟随者状态转换为候选者状态；

所述候选者状态的共识节点向跟随者状态的共识节点发送邀票信息，所述邀票信息包含其所拥有的区块高度；

所述跟随者状态的共识节点判断所述邀票信息中的区块高度是否大于或等于自身区块高度，若是，向所述候选者状态的共识节点投票；

判断所述候选者状态的共识节点所得票数是否大于或等于N/2+1，若是，将所述共识节点由候选者状态转换为领导者状态，N为共识节点的个数。

5.如权利要求1所述的区块链共识机制，其特征在于，所述领导者状态的共识节点任期结束时，其由领导者状态转换为跟随者状态。

6.如权利要求1所述的区块链共识机制，其特征在于，所述领导者状态的共识节点还用于将新区块广播至跟随者状态的共识节点。

7.如权利要求1所述的区块链共识机制，其特征在于，还包括通过智能合约的调用以更新所述共识节点信息的步骤。

8.如权利要求7所述的区块链共识机制，其特征在于，还包括将所述共识节点的更改后的信息通过区块的同步机制进行全网广播的步骤。

9.如权利要求7所述的区块链共识机制，其特征在于，所述共识节点信息包括节点名称、IP、端口和状态。

一种基于Raft算法的区块链共识机制

技术领域

[0001] 本发明涉及区块链共识机制技术领域，具体涉及一种基于Raft算法的区块链共识机制。

背景技术

[0002] 目前，业界广泛使用的共识机制是PoW算法(包括其扩展算法PoS和DPoS)、PBFT算法、Paxos算法和Raft算法。

[0003] PoW算法(Proof Of Work)：工作量证明，用来确认某个节点做过一定量的工作。是一种应对拒绝服务攻击和其它服务滥用的经济对策。它要求发起者进行一定量的运算，也就意味着需要消耗计算机一定的计算时间。

[0004] PBFT算法(Practical Byzantine Fault Tolerance)：PBFT意为实用拜占庭容错算法，其解决了原始拜占庭容错算法效率不高的问题，使得拜占庭容错算法在实际系统应用中变得可行。可容错节点数为N/3-1。

[0005] Raft算法：Raft是由Stanford发布的分布式一致性算法，由Paxos算法改进而来，更注重协议的可理解性和落地性，其特点是任何时刻最多只有1个合法Leader，可容错节点数为N/2-1。

[0006] 上述各算法具有以下缺点。

[0007] PoW算法：依赖机器进行数学运算来获取记账权，资源消耗相比其它共识机制高、可监管性弱，同时每次达成共识需要全网共同参与运算，性能效率比较低，容错性方面允许全网50％节点出错。

[0008] PoS算法：主要思想是节点记账权的获得难度与节点持有的权益成反比，相对于PoW，一定程度减少了数学运算带来的资源消耗，性能也得到了相应的提升，但依然是基于哈希运算竞争获取记账权的方式，可监管性弱。该共识机制容错性和PoW相同。

[0009] DPoS算法：与PoS的主要区别在于节点选举若干代理人，由代理人验证和记账。其合规监管、性能、资源消耗和容错性与PoS相似。

[0010] Paxos算法：是一种基于选举领导者的共识机制，领导者状态的共识节点拥有绝对权限，并允许强监管节点参与，性能高，资源消耗低。所有节点一般有线下准入机制，但选举过程中不允许有作恶节点，不具备容错性。

[0011] PBFT算法：与Paxos类似，也是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制，但该共识机制允许拜占庭容错。该共识机制允许强监管节点参与，具备权限分级能力，性能更高，耗能更低，该算法每轮记账都会由全网节点共同选举领导者，允许33％的节点作恶，容错性为33％。

[0012] Raft算法：Raft算法是Paxos算法的一个简化实现。其合规监管、性能、资源消耗和容错性与Paxos相似。Raft算法应用于联盟链，相对于Paxos和PBFT算法更高效，但是目前业界将Raft应用于区块链，主要是选举一个共识节点并由此节点持续记账。这种方案存在以下的问题：

[0013] 1)选举共识节点未参考节点的区块高度,不能跟区块链有效结合;

[0014] 2)选举一个共识节点并由此节点持续记账,容错性较差;

[0015] 3)目前很多方案对共识节点的监管不够,不能实现共识节点的动态加入退出。

发明内容

[0016] 针对上述算法的缺陷,本申请提供一种基于Raft算法的区块链共识机制,包括步骤:

[0017] 将区块链的共识节点存储于区块链上,共识节点的状态包括:领导者、跟随者和候选者,并将共识节点的初始状态置为跟随者状态;

[0018] 基于raft算法并结合区块高度选举初始领导者状态的共识节点,领导者状态的共识节点用于记录交易事件并生成新区块;

[0019] 领导者状态的共识节点任期结束时,将重新选举领导者状态的共识节点。

[0020] 一种实施例中,选举初始领导者状态的共识节点之前,还包括初始化各个共识节点的选举定时器的步骤。

[0021] 一种实施例中,基于Raft算法并结合区块高度选举初始领导者状态的共识节点,包括步骤:

[0022] 共识节点的选举定时器被触发时,被触发的共识节点由跟随者状态转换为候选者状态;

[0023] 候选者状态的共识节点向跟随者状态的共识节点发送邀票信息,邀票信息包含其所拥有的区块高度;

[0024] 跟随者状态的共识节点判断邀票信息中的区块高度是否大于或等于自身区块高度,若是,向候选者状态的共识节点投票;

[0025] 判断候选者状态的共识节点所得票数是否大于或等于N/2+1,若是,将共识节点由候选者状态转换为领导者状态,N为共识节点的个数。

[0026] 一种实施例中,重新选举领导者状态的共识节点,包括步骤:

[0027] 当前领导者状态的共识节点向跟随者状态的共识节点广播新区块的区块高度,并随机推荐一个跟随者状态的共识节点,被推荐的共识节点由跟随者状态转换为候选者状态;

[0028] 候选者状态的共识节点向跟随者状态的共识节点发送邀票信息,邀票信息包含其所拥有的区块高度;

[0029] 跟随者状态的共识节点判断邀票信息中的区块高度是否大于或等于自身区块高度,若是,向候选者状态的共识节点投票;

[0030] 判断候选者状态的共识节点所得票数是否大于或等于N/2+1,若是,将共识节点由候选者状态转换为领导者状态,N为共识节点的个数。

[0031] 一种实施例中,领导者状态的共识节点任期结束时,其由领导者状态转换为跟随者状态。

[0032] 一种实施例中,领导者状态的共识节点还用于将新区块广播至跟随者状态的共识节点。

[0033] 一种实施例中,还包括通过智能合约的调用以更新共识节点信息的步骤。

[0034] 一种实施例中，还包括将共识节点的更新后信息通过区块的同步机制进行全网广播的步骤。

[0035] 一种实施例中，共识节点信息包括节点名称、IP、端口和状态。

[0036] 依据上述实施例的区块链共识机制，由于领导者状态的共识节点选举过程中参考其所同步的区块高度，提高共识效率，缩短交易确认时间，任期结束后重新选举新的共识节点，提高系统容错性，并且，领导者状态的共识节点选举的唯一性，使得每个区块都有最终一致性，不会出现区块链分叉情况，同时，通过智能合约的共识节点的管理机制，能实现共识节点动态加入退出，通过同步机制实现更新后的共识节点信息的同步，区块链数据的不可篡改性保证了共识节点信息的安全可靠。

附图说明

[0037] 图1为区块链共识机制流程图；

[0038] 图2为共识节点状态转换示意图；

[0039] 图3为初始选举领导者状态的共识节点的过程示意图；

[0040] 图4为共识节点信息同步机制的示意图；

[0041] 图5为重新选举领导者状态的共识节点的过程示意图。

具体实施方式

[0042] 下面通过具体实施方式结合附图对本发明作进一步详细说明。

[0043] 本申请中用到的术语定义：区块链(Block chain)：源于比特币的底层技术，是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造，实现去中心化的分布式账本。公有链(Public block chain)：对任何个人或组织开放的区块链网络。共识节点的进出完全自由。联盟链(Consortiumblock chain)：仅对特定的个人或组织开放的区块链网络。共识节点的进出受到严格管控。智能合约：是一种运行在区块链的一段代码(智能合约)，它可以维持自己的状态，控制自己的资产和对接收到的外界信息或者资产进行回应。共识机制：由于区块链系统是去中心化的分布式账本系统，不依赖于任何的可信第三方，所以需要一种无需依赖第三方机构来鉴定和验证某一数值或交易的机制，即共识机制。共识机制是所有区块链和分布式账本应用的基础。共识节点：共识节点是组成区块链网络的基本单元，一般一个节点对应一台计算机，保存账本的副本，可担任不同角色，如发出交易、验证交易、记账等等。

[0044] 本例提出一种基于Raft算法的区块链共识机制，更适用于联盟链的共识机制，该共识机制在合规监管、性能、资源消耗和容错性方面更均衡高效，其流程图如图1所示，具体包括如下步骤。

[0045] S1：将区块链的共识节点信息存储于区块链上，并将共识节点的初始状态置为跟随者状态。

[0046] 其中，共识节点信息包括节点名称、IP、端口和状态等等，通过智能合约对共识节点进行管理，并保存在区块链上。

[0047] 另外，共识节点的状态包括：领导者状态(Leader)、跟随者状态(Follower)和候选者状态(Candidate)；如图2所示，共识节点在某一时刻仅有一个节点处于领导者状态，其他

节点为跟随者状态，领导者状态的共识节点异常或任期结束后，其转换为跟随者状态。

[0048] 进一步，可以通过智能合约的调用以更新共识节点信息，如，包括共识节点的状态变更、共识节点的加入、退出等修改。

[0049] 将更新后共识节点信息打包在区块数据中，并通过P2P区块的同步机制进行全网广播。

[0050] S2：基于Raft算法并结合区块高度选举初始领导者状态的共识节点，领导者状态的共识节点用于记录交易事件并生成新区块。

[0051] 由于在步骤S1中将区块链中的所有共识节点的状态均初始化为跟随者状态，在选举初始领导者状态的共识节点之前，还需要初始化各个共识节点的选举定时器，即，本例的初始选举由定时器来触发，且，各个共识节点的选举定时器时间不尽相同。

[0052] 如图3所示，选举初始领导者状态的共识节点的过程是：

[0053] 1)共识节点的选举定时器被触发时，被触发的共识节点由跟随者状态转换为候选者状态；

[0054] 具体的，当某个共识节点的定时器到时时触发选举。

[0055] 2)候选者状态的共识节点向跟随者状态的共识节点发送邀票信息，邀票信息包含其所拥有的区块高度；

[0056] 本例的区块高度均是指区块在区块链中的位置编号。

[0057] 3)跟随者状态的共识节点判断邀票信息中的区块高度是否大于或等于自身区块高度，若是，向候选者状态的共识节点投票；

[0058] 由于候选者状态的共识节点通过全网广播的方式向跟随者状态的共识节点发送邀票信息，根据竞争机制，慢速度的共识节点与快速度的共识节点相比，其区块高度不一，如，快速度的共识节点所属的区块高度往往大于慢速度的共识节点所属的区块高度，因此，跟随者状态的共识节点仅向大于或等于自身区块高度的候选者状态的共识节点投票。

[0059] 4)候选者状态的共识节点判断所得票数是否大于或等于N/2+1，若是，所述共识节点由候选者状态转换为领导者状态，N为共识节点的个数；

[0060] 领导者状态的共识节点向所有跟随者状态的共识节点发送通知，以确立其领导者身份，并负责记录交易事件，及生成新区块，如负责记账，及将新区块广播至跟随者状态的共识节点，以实现共识节点间区块同步的机制，具体如图4所示，节点1为领导者状态的共识节点，节点2、节点3和节点4分别为跟随者状态的共识节点，节点1将新区块全网广播至节点2、节点3和节点4。

[0061] 由于选举过程中参考共识节点所同步区块高度，可以提高共识效率，缩短交易确认时间。

[0062] S3：领导者状态的共识节点任期结束时，将重新选举领导者状态的共识节点。

[0063] 当领导者状态的共识节点任期结束时，其由领导者状态转换为跟随者状态，然后，重新选举其他共识节点作为领导者，如图5所示，重新选举领导者状态的共识节点的步骤如下：

[0064] 1)当前领导者状态的共识节点向跟随者状态的共识节点广播新区块的区块高度，并随机推荐一个跟随者状态的共识节点，被推荐的共识节点由跟随者状态转换为候选者状态；

[0065] 具体的，本例的领导者状态的共识节点任期结束是由新区块生成完成而结束，实现轮流生成区块的共识机制，跟随者状态的共识节点收到领导者状态的共识节点广播的新区块高度后保存该新区块高度。

[0066] 2)候选者状态的共识节点向跟随者状态的共识节点发送邀票信息，邀票信息包含其所拥有的区块高度；

[0067] 3)跟随者状态的共识节点判断邀票信息中的区块高度是否大于或等于自身区块高度，若是，向候选者状态的共识节点投票；

[0068] 4)判断候选者状态的共识节点所得票数是否大于或等于N/2+1，若是，将共识节点由候选者状态转换为领导者状态，N为共识节点的个数。

[0069] 同样的，更新后的领导者状态的共识节点负责本次交易事件的记账和产生下一下新区块，并将该新区块广播至其他跟随者状态的共识节点。

[0070] 与业界现有共识机制相比，本例在选举领导者状态的共识节点的过程中结合了区块高度，及共识节点轮流记账，将本例的共识机制应用于联盟链后将具有以下优势：

[0071] 合规监管：支持超级权限节点对全网节点、数据进行监管；

[0072] 性能效率更高：交易达成共识被确认的效率更高；

[0073] 资源消耗更低：共识过程中耗费的CPU、网络输入输出、存储等计算机资源更少；

[0074] 容错性更强：容易性、防攻击、防欺诈的能力更强。

[0075] 以上应用了具体个例对本发明进行阐述，只是用于帮助理解本发明，并不用以限制本发明。对于本发明所属技术领域的技术人员，依据本发明的思想，还可以做出若干简单推演、变形或替换。

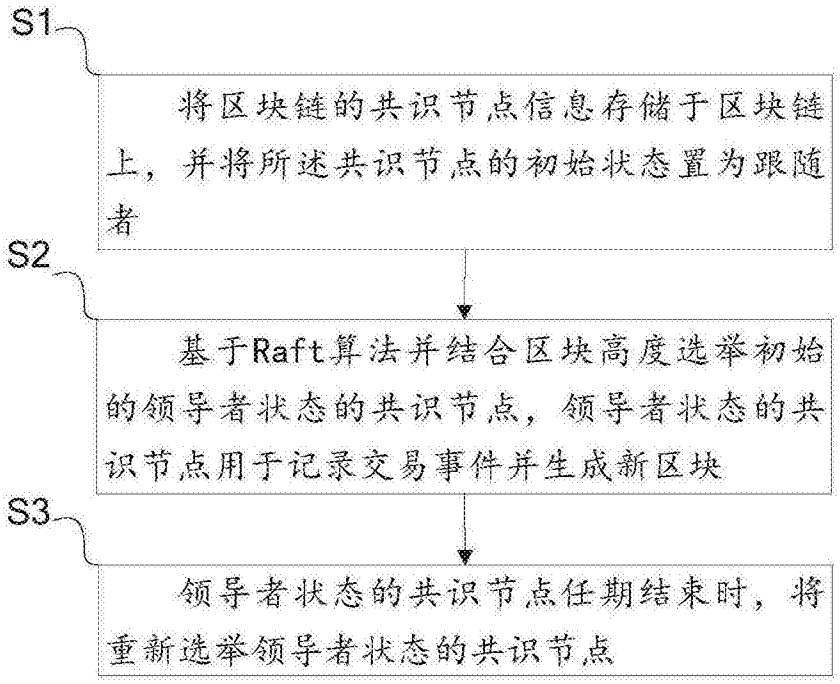

S1
将区块链的共识节点信息存储于区块链上，并将所述共识节点的初始状态置为跟随者
S2
基于Raft算法并结合区块高度选举初始的领导者状态的共识节点，领导者状态的共识节点用于记录交易事件并生成新区块
S3
领导者状态的共识节点任期结束时，将重新选举领导者状态的共识节点

图1

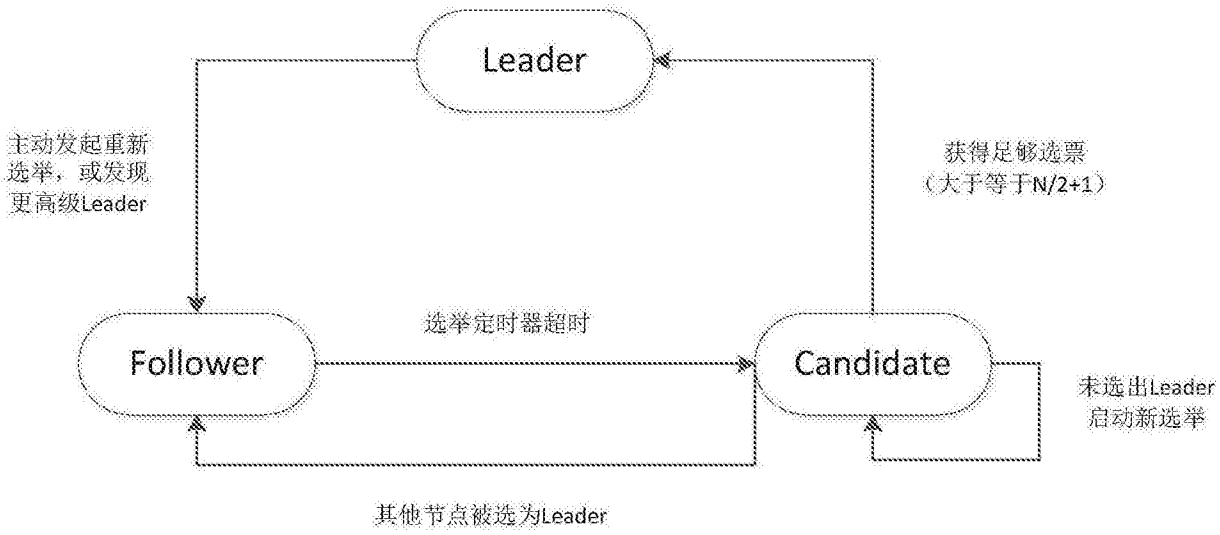

Leader
主动发起重新选举，或发现更高级Leader
获得足够选票（大于等于N/2+1）
选举定时器超时
Follower
Candidate
未选出Leader启动新选举
其他节点被选为Leader

图2

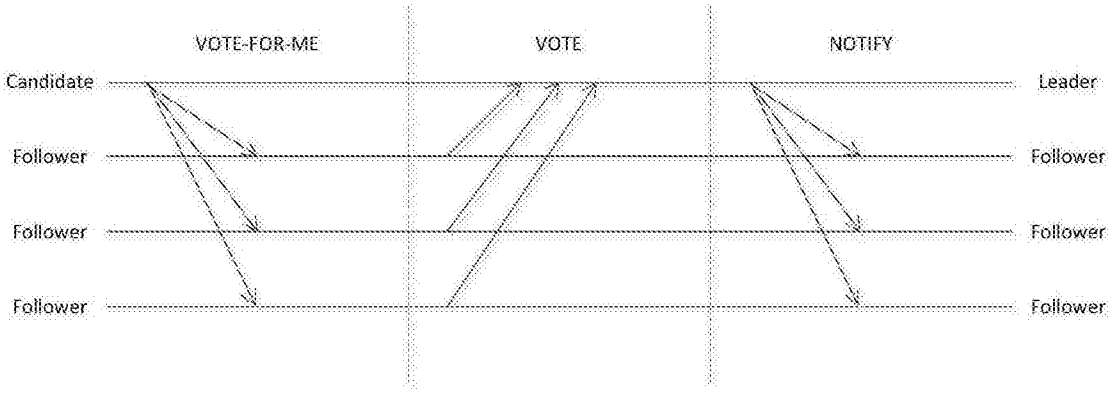

VOTE-FOR-ME
VOTE
NOTIFY
Candidate
Leader
Follower
Follower
Follower
Follower
Follower
Follower
Follower
Follower

图3

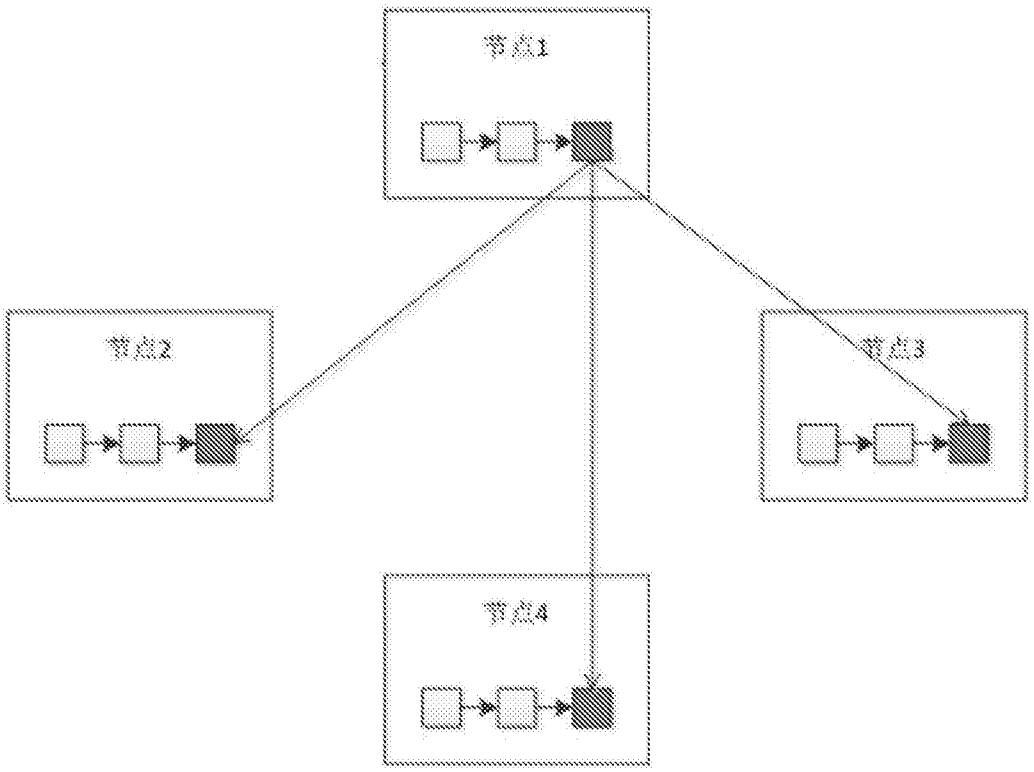

节点1
节点2
节点3
节点4

图4

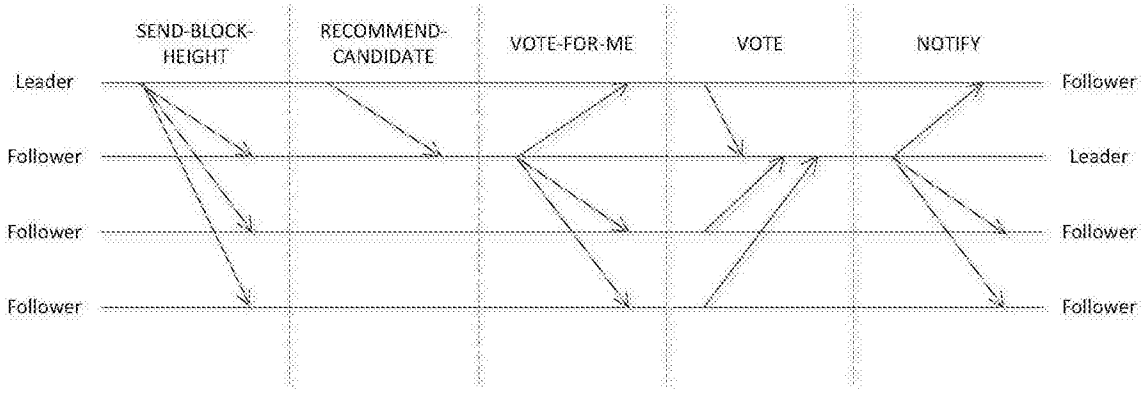

SEND-BLOCK-HEIGHT
RECOMMEND-CANDIDATE
VOTE-FOR-ME
VOTE
NOTIFY
Leader
Follower
Follower
Follower
Follower
Leader
Follower
Follower

图5