(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 107171829 A
(43)申请公布日 2017.09.15

(21)申请号 201710272177.0

(22)申请日 2017.04.24

(71)申请人 杭州趣链科技有限公司
地址 310012 浙江省杭州市西湖区文三路199号13幢南楼501室

(72)发明人 邱炜伟 李启雷 李伟 梁秀波 尹可挺

(74)专利代理机构 杭州求是专利事务所有限公司 33200
代理人 邱启旺

(51)Int.Cl.
H04L 12/24(2006.01)
H04L 29/08(2006.01)
H04L 29/06(2006.01)
H04L 9/32(2006.01)

权利要求书1页 说明书4页 附图3页

(54)发明名称

一种基于BFT共识算法实现的动态节点管理方法

(57)摘要

本发明公开了一种基于BFT共识算法实现的动态节点管理方法。在一个区块链网络上,新节点通过线下获取证书得到区块链网络的准入及参与共识资格,向全网现有节点请求连接后并验证通过后成功加入共识;而当一个节点请求退出区块链网络时,向全网请求退出,经各节点管理员同意后成功退出区块链网络。新增节点的步骤具体为:新节点拿CA证书通过介绍人节点连接后获取全网的连接信息,经全网共识且新节点完成同步后加入区块链网络。删除节点的步骤具体为:选择退出的节点向全网广播退出请求,各节点管理员选择同意其退出则向全网广播删除退出节点;当全网共识同意节点退出后更新各自的连接信息并与选择退出节点断开连接,将该节点清出区块链网络中。

CN 107171829 A

1.一种基于BFT共识算法实现的动态节点管理方法，其特征在于，包括如下步骤：

1)ECert和RCert的获取：线下由第三方认证中心生成新节点加入区块链网络的CA证书，所述CA证书包括Ecert证书和Rcert证书；其中，ECert为节点准入证书，只有拥有ECert证书的节点才能进入区块链网络，RCert为节点参与投票共识的证书，只有拥有RCert证书才能参与区块链网络的共识投票。

2)介绍人机制：新节点通过选择一个现有节点作为介绍人拿到全网的网络连接信息，介绍人节点验证CA证书，证书通过后才将全网的网络连接信息发送给新节点。

3)现有节点需要有2f+1个节点同意通过新节点的CA认证：新节点拿到全网的网络连接信息需要继续带上CA证书和全部节点请求连接，现有节点确认全网2f+1个节点同意新节点的认证后和新节点建立反向连接。

4)新节点进入Recovery恢复：在新节点确认全网N-f个节点都与自己相连后触发，新节点的Recovery完成时则与区块链网络上的其他节点保持同步。

5)新节点正式加入共识投票：在新节点完成Recovery后向全网广播申请加入共识，全网共识同意后真正更新共识算法的参数，新节点完成加入过程。

6)退出节点的认证需要通过各节点管理员的确认：退出节点需要向区块链网络中的所有节点提交退出申请，由各节点的管理员认证确认同意后发起全网共识确认退出节点的信息；

7)现有节点与退出节点断开连接：现有节点确认2f+1节点同意申请退出节点的请求后与退出节点断开网络连接，更新自己的全网连接信息。

8)区块链网络更新共识参数：现有节点确认自己更新完连接信息后全网广播更新共识参数，当确认全网2f+1节点同意更新后完成更新，退出节点才真正退出区块链网络。

2.如权利要求1所述的一种基于BFT共识算法实现的动态节点管理方法，其特征在于，所述的步骤1)中，ECert证书保证了参与投票的共识节点和不参与投票的记账节点能顺利进入区块链网络中；RCert证书保证了节点拥有参与投票的权限，一个共识节点的加入需要同时拥有这两种证书才能加入成功；新节点创建之初，由第三方认证中心保存根证书，每个申请加入区块链网络的节点都需要线下向第三方认证中心申请证书，而在退出后则由第三方认证中心注销证书。

一种基于BFT共识算法实现的动态节点管理方法

技术领域

[0001] 本发明涉及去中心化的区块链CA证书体系，尤其涉及一种基于BFT共识算法实现的动态节点管理方法。

背景技术

[0002] 区块链技术，区块链是一种新型去中心化协议，能安全地存储数字货币交易或其他数据，信息不可伪造和篡改，区块链上的交易确认由区块链上的所有节点共同完成，由共识算法保证其一致性，区块链上维护一个公共的账本，公共账本位于存储区块上任何节点可见，从而保证其不可伪造和篡改。

[0003] 传统区块链的BFT共识算法没有动态节点管理的功能，尽管BFT现在已经有了很多改进和变种版本，大多都是对于共识一致性的保障和可用性增强上，对于如何动态管理节点的探索却一直都是空白的状态。就拿PBFT算法来说，增删节点的过程就需要将所有节点全部停机，然后更新配置文件，再全部重启。但是这样的做法在实际生产中则显得不可接受，如何解决BFT共识算法的动态成员管理问题是将区块链技术运用于实际的一项挑战。

[0004] 正是面对这一棘手的亟待解决问题，我们提出了动态成员管理机制。使整个区块链系统能在不停机情况下，进行动态的增删节点。

发明内容

[0005] 本发明的目的是针对现有技术的不足，提供一种基于BFT共识算法实现的动态节点管理方法。

[0006] 本发明的目的是通过以下技术方案来实现的：一种基于BFT共识算法实现的动态节点管理方法，包括如下步骤：

[0007] 1)ECert和RCert的获取：线下由第三方认证中心生成新节点加入区块链网络的CA证书，所述CA证书包括Ecert证书和Rcert证书；其中，ECert为节点准入证书，只有拥有ECert证书的节点才能进入区块链网络，RCert为节点参与投票共识的证书，只有拥有RCert证书才能参与区块链网络的共识投票；

[0008] 2)介绍人机制：新节点通过选择一个现有节点作为介绍人拿到全网的网络连接信息，介绍人节点验证CA证书，证书通过后才将全网的网络连接信息发送给新节点；

[0009] 3)现有节点需要有2f+1个节点同意通过新节点的CA认证：新节点拿到全网的网络连接信息需要继续带上CA证书和全部节点请求连接，现有节点确认全网2f+1个节点同意新节点的认证后和新节点建立反向连接；

[0010] 4)新节点进入Recovery恢复：在新节点确认全网N-f个节点都与自己相连后触发，新节点的Recovery完成时则与区块链网络上的其他节点保持同步；

[0011] 5)新节点正式加入共识投票：在新节点完成Recovery后向全网广播申请加入共识，全网共识同意后真正更新共识算法的参数，新节点完成加入过程；

[0012] 6)退出节点的认证需要通过各节点管理员的确认：退出节点需要向区块链网络中

的所有节点提交退出申请，由各节点的管理员认证确认同意后发起全网共识确认退出节点的信息；

[0013] 7)现有节点与退出节点断开连接：现有节点确认2f+1节点同意申请退出节点的请求后与退出节点断开网络连接，更新自己的全网连接信息；

[0014] 8)区块链网络更新共识参数：现有节点确认自己更新完连接信息后全网广播更新共识参数，当确认全网2f+1节点同意更新后完成更新，退出节点才真正退出区块链网络。

[0015] 进一步的，所述的步骤1)中，ECert证书保证了参与投票的共识节点和不参与投票的记账节点能顺利进入区块链网络中；RCert证书保证了节点拥有参与投票的权限，一个共识节点的加入需要同时拥有这两种证书才能加入成功；新节点创建之初，由第三方认证中心保存根证书，每个申请加入区块链网络的节点都需要线下向第三方认证心中申请证书，而在退出后则由第三方认证中心注销证书。

[0016] 本发明的有益效果是：本发明应用于联盟链背景下的区块链网络上，即保证了BFT算法的有效性，同时又解决了BFT对于动态节点支持不友好的问题，是BFT共识体系下区块链技术的大突破。对于传统区块链上BFT类算法，增删节点的过程需要将所有节点全部停机，然后更新配置文件，再全部重启。这在区块链技术的实际应用中存在大量的问题，不仅不能保证系统的可用性，还要耗费大量人力配置重启，是区块链应用的一大痛点。而我们提出的动态节点管理功能则解决了这一问题，使整个在增删节点的过程中时依然保证有效性。

附图说明

[0017] 图1是新节点动态接入状态图；

[0018] 图2是退出节点动态退出状态图；

[0019] 图3是新节点动态加入流程图；

[0020] 图4是退出节点动态退出流程图。

具体实施方式

[0021] 下面根据附图和具体实施例详细描述本发明，本发明的目的和效果将变得更加明显。

[0022] 本发明的一种基于BFT共识算法实现的动态节点管理方法，包括如下步骤：

[0023] 1)ECert和RCert的获取：线下获取由第三方认证中心生成新节点加入区块链网络的CA证书，所述CA证书包括Ecert证书和Rcert证书；其中，ECert为节点准入证书，只有拥有ECert证书的节点才能进入区块链网络，RCert为节点参与投票共识的证书，只有拥有RCert证书才能参与区块链网络的共识投票；

[0024] 2)介绍人机制：新节点通过选择一个现有节点作为介绍人拿到全网的网络连接信息，介绍人节点验证CA证书，证书通过后才将全网的网络连接信息发送给新节点；

[0025] 3)现有节点需要有2f+1个节点同意通过新节点的CA认证：如图1的第一步，新节点拿到全网的网络连接信息需要继续带上CA证书和全部节点请求连接，现有节点确认全网2f+1个节点同意新节点的认证后和新节点建立反向连接；

[0026] 4)新节点进入Recovery恢复：如图1的分界线所示，在新节点确认全网N-f个节点

都与自己相连后触发，新节点的Recovery完成时则与区块链网络上的其他节点保持同步；

[0027] 5)新节点正式加入共识投票：如图1的最后三步所示，在新节点完成Recovery后向全网广播申请加入共识，全网共识同意后真正更新共识算法的参数，新节点完成加入过程；

[0028] 6)退出节点的认证需要通过各节点管理员的确认：如图2所示，退出节点需要向区块链网络中的所有节点提交退出申请，由各节点的管理员认证确认同意后发起全网共识确认退出节点的信息；

[0029] 7)现有节点与退出节点断开连接：如图2的第二步所示，现有节点确认2f+1节点同意申请退出节点的请求后与退出节点断开网络连接，更新自己的全网连接信息；

[0030] 8)区块链网络更新共识参数：如图2的最后三步所示，现有节点确认自己更新完连接信息后全网广播更新共识参数，当确认全网2f+1节点同意更新后完成更新，退出节点才真正退出区块链网络。

[0031] 进一步地，所述的步骤1)中，区块链网络的动态节点管理是基于CA证书体系的，ECert保证了参与投票的共识节点和不参与投票的记账节点能顺利进入区块链网络中；RCert保证了节点拥有参与投票的权限。一个共识节点的加入需要同时拥有两种证书才能加入成功，CA体系也是整个区块链网络实现动态节点管理的前提。创建之初，可由第三方认证中心保存根证书，每个申请加入区块链网络的节点都需要线下向第三方认证中心申请证书，而在退出后则由第三方认证中心注销证书。

[0032] 进一步地，所述的步骤2)中，新节点加入区块链网络需要全网的连接信息，同时根据BFT算法思想得到全网连接信息需要全网共识，这本是一个悖论，但基于联盟链的应用场景我们引入了介绍人机制，新节点可选取信任的现有节点作为介绍人得到全网的网络连接信息。

[0033] 进一步地，所述步骤3)中，现有节点需要确认全网2f+1个节点通过新节点的CA认证后才会和新节点建立反连，避免新节点只和部分节点连接，造成小范围共识的可能性。

[0034] 进一步地，所述的步骤4)中，新节点确认全网N-f个节点和自己建立反连后并不是立马起到共识作用，因为新节点没有区块链网络中的历史数据，如果这时候立马加入共识反而是作为一个拜占庭加点加入的，会影响整个系统的容错性，所以需要进入Recovery流程，正如所述步骤5)中只有当新节点与区块链网络中的节点数据完全同步后，整个系统才真正更新共识参数，新节点正式加入共识。

[0035] 进一步地，所述的步骤6)中，节点退出区块链网络需要节点管理员人工参与，就是为了避免有节点伪造或窃取节点信息恶意退出，仅当节点管理员确认同意该节点退出区块链网络后方可进行全网共识删除该节点。

[0036] 下面用一个区块链交易实例来说明具体实施方式：

[0037] 区块链网络存在A,B,C,D四个节点，模拟E节点在线下获取CA证书后加入区块链网络。

[0038] 如图3所示：首先，E节点在线下获取ECert和RCert，然后选择A节点作为介绍人，配置好配置文件后启动，A节点验证通过E节点的CA证书后将全网连接信息传回，E节点然后与全网节点申请建立连接加入共识网络，现有四个节点通过2f+1共识认证后与E节点进行反连，E节点在确认N-f个现有节点和自己建立连接后开始Recovery，待Recovery完成则可全网广播申请加入区块链网络。

[0039] 区块链网络存在A,B,C,D,E四个节点,模拟节点E申请退出区块链网络。

[0040] 如图4所示:首先,E节向全网广播申请退出区块链网络(需要注意的是,仅支持在5个及以上节点存在时进行删节点,因为4为保证拜占庭问题的最小数字),各节点将管理员同意退出后全网广播删除E节点,经2f+1共识验证后各节点断开与E节点的连接,并在接下来再经过一轮共识更新共识参数,E节点正式退出区块链网络。

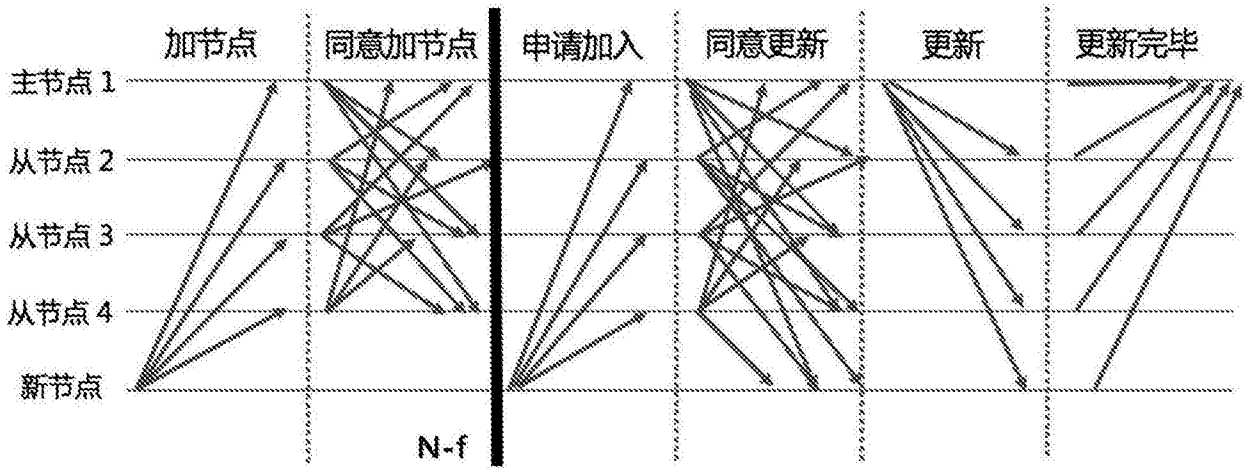
加节点
同意加节点
申请加入
同意更新
更新
更新完毕
主节点 1
从节点 2
从节点 3
从节点 4
新节点
N-f

图1

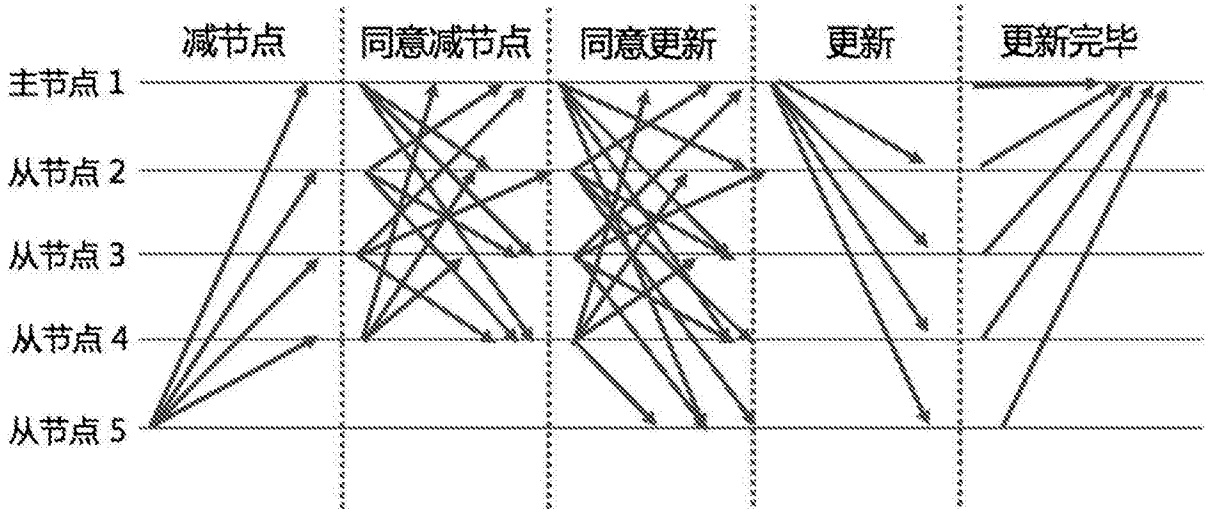
减节点
同意减节点
同意更新
更新
更新完毕
主节点 1
从节点 2
从节点 3
从节点 4
从节点 5

图2

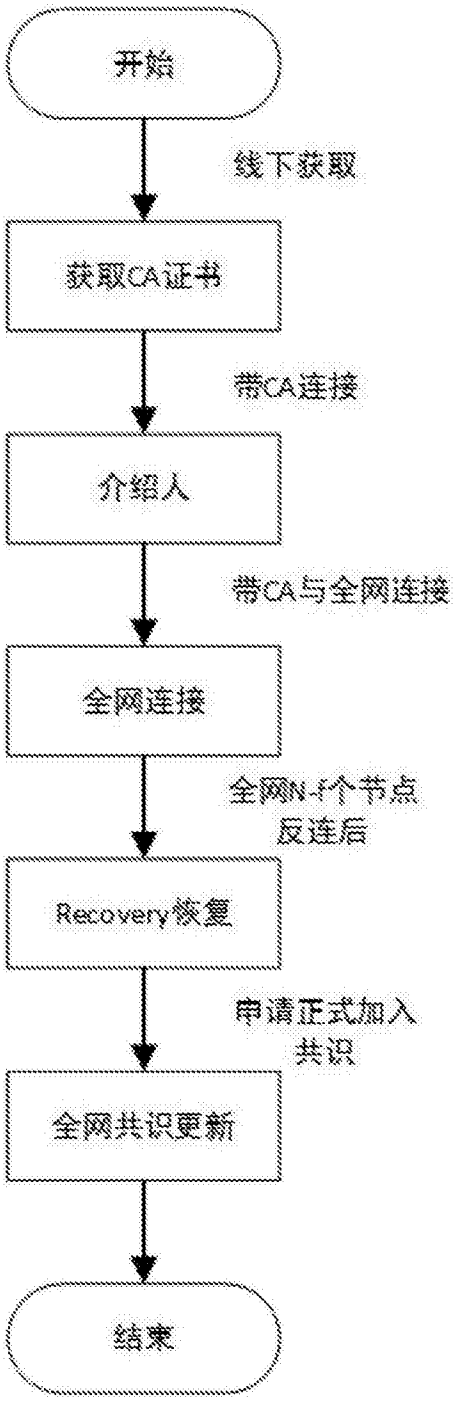
开始
线下获取
获取CA证书
带CA连接
介绍人
带CA与全网连接
全网连接
全网N-f个节点
反连后
Recovery恢复
申请正式加入
共识
全网共识更新
结束

图3

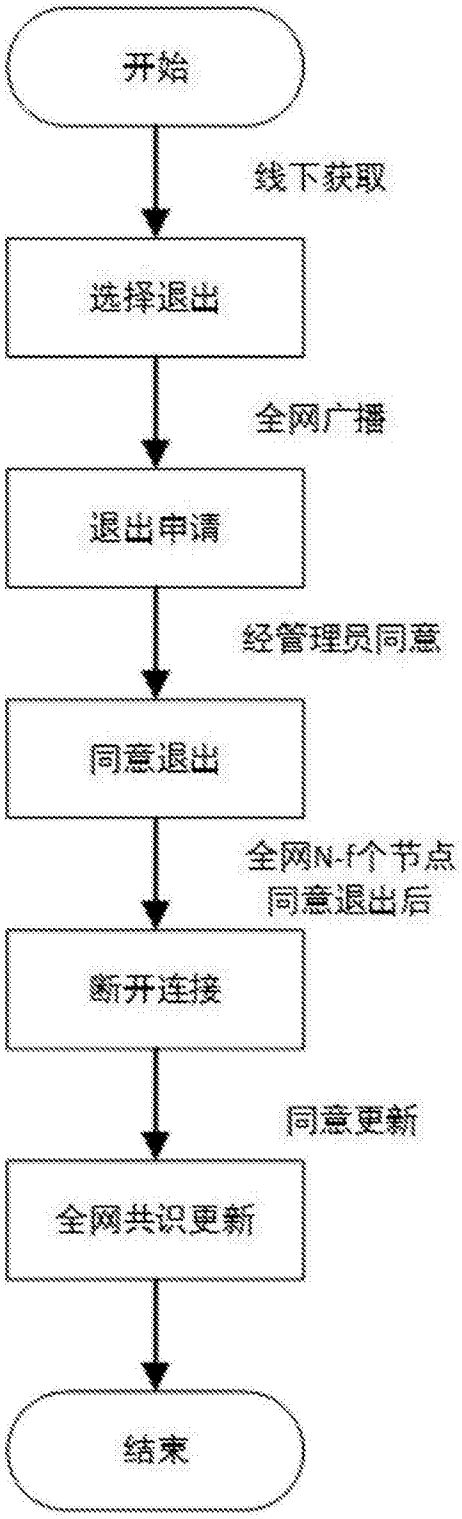
开始
线下获取
选择退出
全网广播
退出申请
经管理员同意
同意退出
全网N-f个节点
同意退出后
断开连接
同意更新
全网共识更新
结束

图4