(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 112700333 A
(43)申请公布日 2021.04.23

(21)申请号 202110033313.7

(22)申请日 2021.01.11

(71)申请人 东北大学
地址 110819 辽宁省沈阳市和平区文化路3号巷11号

(72)发明人 刘园 谭立元 陈俣欣

(74)专利代理机构 沈阳东大知识产权代理有限公司 21109
代理人 梁焱

(51)Int.Cl.
G06Q 40/04(2012.01)
G06F 16/23(2019.01)
G06F 16/27(2019.01)
G06F 11/14(2006.01)

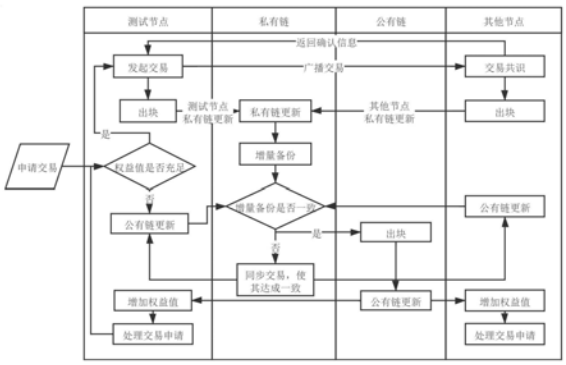
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于区块链的电子档案共识方法

(57)摘要

本发明公开了一种基于区块链的电子档案共识方法，属于电子档案存储技术领域。测试节点收到用户发起的交易申请时，首先判断其权益值是否充足，若否则触发公有链更新；若是则测试节点发起交易，其他节点对测试节点发起的交易进行交易共识，若达成共识则测试节点私有链更新，若未达成共识则驳回交易。公有链更新时需校验增量备份是否一致，不一致则需进行增量备份同步使增量备份达成一致后，测试节点创建区块存储增量备份中的交易数据，需校验区块数据真实，若真实则将区块添加到公有链上，完成公有链更新后，对参与交易共识、校验增量备份是否一致和校验区块数据真实性过程的节点给予权益值奖励。采取义务驱动代替经济激励机制保障共识的真实性。



CN 112700333 A

1.一种基于区块链的电子档案共识方法,其特征在于,包括以下步骤:

步骤1、测试节点接收用户发起的交易申请;

步骤2、测试节点判断权益值是否充足,若是,则执行步骤3,若否,则执行步骤6;

步骤3、测试节点发起交易;

步骤4、其他节点对测试节点发起的交易进行交易共识,若达成共识,则执行步骤5,若未达成共识,则驳回该交易;

区块链系统记录其他节点参与交易共识过程的义务付出,给出义务劳动证明;

步骤5、测试节点私有链更新;

步骤6、公有链更新;

步骤6.1、校验增量备份是否一致,若是,则执行步骤6.3,若否,则执行步骤6.2;

增量备份是指上一次公有链更新到当前时刻,测试节点私有链上所有新增的交易;校验增量备份是否一致是指,校验测试节点的增量备份与其他节点的增量备份是否一致;

步骤6.2、测试节点与其他节点进行增量备份同步,使增量备份达成一致;

区块链系统记录其他节点参与校验增量备份是否一致过程的义务付出,给出义务劳动证明;

步骤6.3、测试节点创建区块,以存储增量备份中的交易数据,且存储到区块中的数据称为区块数据;

步骤6.4、校验区块数据的真实性,若真实,则执行步骤6.5,若不真实,则转至步骤6.3;

区块链系统记录其他节点参与校验区块数据真实性过程的义务付出,给出义务劳动证明;

步骤6.5、电子档案节点将区块添加到公有链上,完成公有链更新;

步骤7、根据区块链系统记录的义务劳动证明,分别给予各电子档案节点一定的权益值。

2.根据权利要求1所述的基于区块链的电子档案共识方法,其特征在于,测试节点每发起一笔交易,都需要消耗一定的权益值。

3.根据权利要求1所述的基于区块链的电子档案共识方法,其特征在于,步骤4中,采用拜占庭容错算法对交易进行共识。

4.根据权利要求1所述的基于区块链的电子档案共识方法,其特征在于,所述步骤5中,测试节点私有链更新的方法为:达成共识的交易可以出块,出块是指将一定时间内达成共识的交易存储在区块中,生成一个区块;测试节点出块后,区块将被链接到测试节点的私有链上,更新测试节点私有链。

5.根据权利要求1所述的基于区块链的电子档案共识方法,其特征在于,所述步骤6.1的具体方法为:测试节点基于增量备份生成哈希值,将该哈希值广播给其他节点,其他节点接收哈希值,并校验该哈希值和自己基于增量备份生成的哈希值是否一致,如若哈希值不同,则增量备份不一致,其他节点将不一致的交易返回给测试节点,执行步骤6.2,若哈希值相同,则增量备份一致,执行步骤6.3。

6.根据权利要求5所述的基于区块链的电子档案共识方法,其特征在于,所述步骤6.2中,针对测试节点的增量备份中缺少交易的情况,测试节点从其他节点获得增量备份中缺少的交易并逐一广播,其他节点接收后,逐一与自己的增量备份中存储的交易进行对比,若

超过电子档案节点总数1/3的节点无该交易，则认为该交易不存在，判定测试节点的增量备份中不是缺少该交易；反之，该交易存在，判定测试节点的增量备份中缺少该交易，测试节点把该交易记录到私有链上，并增加到增量备份中。

7.根据权利要求5所述的基于区块链的电子档案共识方法，其特征在于，所述步骤6.2中，针对测试节点的增量备份中的交易与其他节点的增量备份中的交易不一致的情况，测试节点从其他节点获得不一致的交易并逐一广播，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则认为该交易不存在，判定测试节点的增量备份与其他节点的增量备份不是该交易不一致；反之，该交易存在，判定测试节点的增量备份与其他节点的增量备份所存储的该交易不一致，测试节点把该交易记录到私有链上，对应修改增量备份。

8.根据权利要求5所述的基于区块链的电子档案共识方法，其特征在于，所述步骤6.2中，针对测试节点的增量备份中有多余交易的情况，测试节点逐一广播多余的交易，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则判定测试节点的增量备份中该交易是多余的，测试节点从增量备份中删除该交易；反之，该交易不是多余交易。

9.根据权利要求1所述的基于区块链的电子档案共识方法，其特征在于，校验区块数据的真实性的方法为：测试节点广播区块数据，其他节点接收区块数据，将区块数据与其他节点的增量备份进行校验，若区块链系统中超过2/3的电子档案节点校验通过，则认为区块数据真实，否则，则认为区块数据不真实。

10.根据权利要求1所述的基于区块链的电子档案共识方法，其特征在于，电子档案节点参与公有链更新的过程分为主动参与和被动参与；主动参与是指电子档案节点主动参与公有链更新，包括参与校验增量备份是否一致的过程和参与校验区块数据真实性的过程；被动参与指的是区块链系统中的电子档案节点被强制参与公有链更新，参与校验区块数据真实性的过程。

一种基于区块链的电子档案共识方法

技术领域

[0001] 本发明属于电子档案的存储技术领域，具体涉及一种基于区块链的电子档案共识方法。

背景技术

[0002] 当前基于区块链有很多共识机制，共识机制是解决区块链系统在去中心化的分布式场景下如何保证互不信任的各个节点诚实记账，对合法交易达成共识的一种机制。当前已有区块链系统通过不同的共识算法实现了这一机制，如工作量证明共识算法(POW)、股权证明共识算法(POS)、授权股权证明共识算法(DPOS)、拜占庭共识算法(PBFT)等。

[0003] 经过研究发现共识算法中的共识机制和激励机制是相辅相成的，共识机制的安全性很大一部分是依赖于激励机制的策略保证。现在的区块链系统和金融行业结合比较紧密，交易的对象主要是电子货币，再由电子货币与现实生活中具有实际价值的货物进行关联，也就是说采用经济推动的激励机制来保障共识的安全可靠。但对于一些公共基础设施的应用场景，比如电子档案在区块链中存储的场景，似乎并不适合使用市场的手段去保证区块链系统的安全性，因为区块链节点的诚实性依赖于经济激励，这将产生巨大的公共资产投入。

发明内容

[0004] 为了解决上述问题，本发明提供一种基于区块链的电子档案共识方法，针对于电子档案的使用场景，提出了使用义务驱动代替经济激励的新机制，对构成区块链网络的每个节点进行了权利和义务的定义与划分，想要获取电子档案的信息化服务就必须履行作为诚实节点的义务，以此保证区块链节点的诚实性以及共识结果的一致性和真实性。

[0005] 为解决上述技术问题，本发明提供一种技术方案：

[0006] 一种基于区块链的电子档案共识方法，包括以下步骤：

[0007] 步骤1、测试节点接收用户发起的交易申请；

[0008] 步骤2、测试节点判断权益值是否充足，若是，则执行步骤3，若否，则执行步骤6；

[0009] 步骤3、测试节点发起交易；

[0010] 步骤4、其他节点对测试节点发起的交易进行交易共识，若达成共识，则执行步骤5，若未达成共识，则驳回该交易；

[0011] 区块链系统记录其他节点参与交易共识过程的义务付出，给出义务劳动证明；

[0012] 步骤5、测试节点私有链更新；

[0013] 步骤6、公有链更新；

[0014] 步骤6.1、校验增量备份是否一致，若是，则执行步骤6.3，若否，则执行步骤6.2；

[0015] 增量备份是指上一次公有链更新到当前时刻，测试节点私有链上所有新增的交易；校验增量备份是否一致是指，校验测试节点的增量备份与其他节点的增量备份是否一致；

[0016] 步骤6.2、测试节点与其他节点进行增量备份同步，使增量备份达成一致；

[0017] 区块链系统记录其他节点参与校验增量备份是否一致过程的义务付出，给出义务劳动证明；

[0018] 步骤6.3、测试节点创建区块，以存储增量备份中的交易数据，且存储到区块中的数据称为区块数据；

[0019] 步骤6.4、校验区块数据的真实性，若真实，则执行步骤6.5，若不真实，则转至步骤6.3；

[0020] 区块链系统记录其他节点参与校验区块数据真实性过程的义务付出，给出义务劳动证明；

[0021] 步骤6.5、电子档案节点将区块添加到公有链上，完成公有链更新；

[0022] 步骤7、根据区块链系统记录的义务劳动证明，分别给予各电子档案节点一定的权益值。

[0023] 进一步地，根据所述的基于区块链的电子档案共识方法，测试节点每发起一笔交易，都需要消耗一定的权益值。

[0024] 进一步地，根据所述的基于区块链的电子档案共识方法，步骤4中，采用拜占庭容错算法对交易进行共识。

[0025] 进一步地，根据所述的基于区块链的电子档案共识方法，所述步骤5中，测试节点私有链更新的方法为：达成共识的交易可以出块，出块是指将一定时间内达成共识的交易存储在区块中，生成一个区块；测试节点出块后，区块将被链接到测试节点的私有链上，更新测试节点私有链。

[0026] 进一步地，根据所述的基于区块链的电子档案共识方法，所述步骤6.1的具体方法为：测试节点基于增量备份生成哈希值，将该哈希值广播给其他节点，其他节点接收哈希值，并校验该哈希值和自己基于增量备份生成的哈希值是否一致，如若哈希值不同，则增量备份不一致，其他节点将不一致的交易返回给测试节点，执行步骤6.2，若哈希值相同，则增量备份一致，执行步骤6.3。

[0027] 进一步地，根据所述的基于区块链的电子档案共识方法，所述步骤6.2中，针对测试节点的增量备份中缺少交易的情况，测试节点从其他节点获得增量备份中缺少的交易并逐一广播，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则认为该交易不存在，判定测试节点的增量备份中不是缺少该交易；反之，该交易存在，判定测试节点的增量备份中缺少该交易，测试节点把该交易记录到私有链上，并增加到增量备份中。

[0028] 进一步地，根据所述的基于区块链的电子档案共识方法，所述步骤6.2中，针对测试节点的增量备份中的交易与其他节点的增量备份中的交易不一致的情况，测试节点从其他节点获得不一致的交易并逐一广播，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则认为该交易不存在，判定测试节点的增量备份与其他节点的增量备份不是该交易不一致；反之，该交易存在，判定测试节点的增量备份与其他节点的增量备份所存储的该交易不一致，测试节点把该交易记录到私有链上，对应修改增量备份。

[0029] 进一步地，根据所述的基于区块链的电子档案共识方法，所述步骤6.2中，针对测

试节点的增量备份中有多余交易的情况，测试节点逐一广播多余的交易，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则判定测试节点的增量备份中该交易是多余的，测试节点从增量备份中删除该交易；反之，该交易不是多余交易。

[0030] 进一步地，根据所述的基于区块链的电子档案共识方法，校验区块数据的真实性的方法为：测试节点广播区块数据，其他节点接收区块数据，将区块数据与其他节点的增量备份进行校验，若区块链系统中超过2/3的电子档案节点校验通过，则认为区块数据真实，否则，则认为区块数据不真实。

[0031] 进一步地，根据所述的基于区块链的电子档案共识方法，电子档案节点参与公有链更新的过程分为主动参与和被动参与；主动参与是指电子档案节点主动参与公有链更新，包括参与校验增量备份是否一致的过程和参与校验区块数据真实性的过程；被动参与指的是区块链系统中的电子档案节点被强制参与公有链更新，参与校验区块数据真实性的过程。

[0032] 本发明的有益效果：本发明的基于区块链的电子档案共识方法采取义务驱动电子档案节点参与共识，代替了金钱驱动电子档案节点参与共识的方法，克服了电子档案没有经济体推动的问题，且采取义务驱动代替经济激励机制，更加适用于电子档案的共识，来保障共识的真实性。

附图说明

[0033] 图1是本发明基于区块链的电子档案共识方法流程图；

[0034] 图2是本发明基测试节点增量备份校验与同步过程流程图；

[0035] 图3是本发明测试节点与其他节点进行增量备份同步的三种情况示意图。

具体实施方式

[0036] 为了便于理解本申请，下面将参照相关附图对本申请进行更全面的描述。附图中给出了本申请的较佳实施方式。但是，本申请可以以许多不同的形式来实现，并不限于本文所描述的实施方式。相反地，提供这些实施方式的目的是使对本申请的公开内容理解的更加透彻全面。

[0037] 本实施方式的基于区块链的电子档案共识方法，如图1所示，包括以下步骤：

[0038] 步骤1、测试节点接收用户发起的交易申请；

[0039] 在本实施方式中，将发起交易的电子档案节点称为测试节点，将其他电子档案节点称为其他节点。

[0040] 步骤2、测试节点判断权益值是否充足，若否，则执行步骤6，若是，则执行步骤3；

[0041] 本实施方式中，测试节点每发起一笔交易，都需要消耗一定的权益值。权益值相当于代币，测试节点具有足够的权益值才能被允许发起交易。若测试节点权益值不足，则执行步骤6，若测试节点权益值充足，则执行步骤3。

[0042] 步骤3、测试节点发起交易；

[0043] 若测试节点权益值充足，则允许测试节点发起交易。

[0044] 步骤4、其他节点对测试节点发起的交易进行交易共识；

[0045] 测试节点发起的交易广播给其他节点，其他节点对该交易进行交易共识。本实施方式采用拜占庭容错算法对交易进行共识，若电子档案节点中有2/3的电子档案节点同意该交易，则交易达成共识，测试节点和其他节点都对该交易进行记录，执行步骤5；反之，则交易未达成共识，驳回该交易，交易结束。

[0046] 其他节点参与交易共识过程时，其他节点需要记录测试节点广播的交易并进行投票，且耗费自己的存储空间存储测试节点的交易，这些都属于义务劳动，区块链系统将记录其他节点的义务付出，给出义务劳动证明。

[0047] 步骤5、测试节点私有链更新；

[0048] 达成共识的交易可以出块，出块是指将一定时间内达成共识的交易存储在区块中，生成一个区块。一个区块中可以存储多个交易。测试节点出块，区块将被链接到测试节点的私有链上，更新测试节点私有链。

[0049] 步骤6、公有链更新；

[0050] 测试节点权益值不足时，触发公有链更新。

[0051] 步骤6.1、如图2所示，校验增量备份是否一致，若是，则执行步骤6.3，若否，则执行步骤6.2

[0052] 增量备份是指上一次公有链更新到当前时刻，测试节点私有链上所有新增的交易。校验增量备份是否一致是指，校验测试节点的增量备份与其他节点的增量备份是否一致。测试节点基于增量备份生成哈希值，将该哈希值广播给其他节点，其他节点接收哈希值，并校验该哈希值和自己的增量备份生成的哈希值是否一致。如若哈希值不同，则增量备份不一致，其他节点将不一致的交易返回给测试节点，执行步骤6.2。若哈希值相同，则增量备份一致，执行步骤6.3。

[0053] 步骤6.2、测试节点与其他节点进行增量备份同步，使增量备份达成一致；

[0054] 若增量备份不一致，如图3所示，可能是以下三种情况，测试节点与其他节点分别就这三种情况进行相应处理使增量备份达成一致。

[0055] a)测试节点的增量备份中缺少交易

[0056] 测试节点从其他节点获得增量备份中缺少的交易并逐一广播，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则认为该交易不存在，判定测试节点的增量备份中不是缺少该交易；反之，该交易存在，判定测试节点的增量备份中缺少该交易，测试节点把该交易记录到私有链上，并增加到增量备份中。

[0057] b)测试节点的增量备份中的交易与其他节点的增量备份中的交易不一致

[0058] 测试节点从其他节点获得不一致的交易并逐一广播，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则认为该交易不存在，判定测试节点的增量备份与其他节点的增量备份不是该交易不一致；反之，该交易存在，判定测试节点的增量备份与其他节点的增量备份所存储的该交易不一致，测试节点把该交易记录到私有链上，对应修改增量备份。

[0059] c)测试节点的增量备份中有多余交易

[0060] 测试节点逐一广播多余的交易，其他节点接收后，逐一与自己的增量备份中存储的交易进行对比，若超过电子档案节点总数1/3的节点无该交易，则判定测试节点的增量备

份中该交易是多余的，测试节点从增量备份中删除该交易；反之，该交易不是多余交易。

[0061] 其他节点参与校验增量备份是否一致的过程，属于义务劳动过程，区块链系统将记录其他节点的义务付出，给出义务劳动证明。

[0062] 步骤6.3、测试节点创建区块，以存储增量备份中的交易数据；

[0063] 测试节点创建区块，区块中存储增量备份中的交易数据，将存储到区块中的数据称为区块数据。创建区块，是为了将区块添加到公有链上，以更新公有链。

[0064] 步骤6.4、校验区块数据的真实性，若真实，则执行步骤6.5，若不真实，则转至步骤6.3；

[0065] 该步骤的具体内容包括：测试节点广播区块数据，其他节点接收区块数据，将区块数据与其他节点的增量备份进行校验。若区块链系统中超过2/3的电子档案节点校验通过，则认为区块数据真实，执行步骤6.5，否则，则认为区块数据不真实，需重新创建区块，执行步骤6.3；

[0066] 其他节点参与校验区块数据的真实性的过程，属于义务劳动过程，区块链系统将记录其他节点的义务付出，给出义务劳动证明。

[0067] 步骤6.5、电子档案节点将区块添加到公有链上，完成公有链更新；

[0068] 电子档案节点参与公有链更新的过程分为主动参与和被动参与。主动参与是指电子档案节点主动参与公有链更新，包括参与校验增量备份是否一致的过程和参与校验区块数据真实性的过程。被动参与指的是区块链系统中的电子档案节点被强制参与公有链更新，参与校验区块数据真实性的过程。

[0069] 步骤7、根据区块链系统记录的义务劳动证明，分别给予各电子档案节点一定的权益值。

[0070] 公有链更新后，将根据电子档案节点参与交易共识时，区块链系统记录的义务劳动证明，相应地给予一定权益值奖励；将根据电子档案节点参与公有链更新时，区块链系统记录的义务劳动证明，给予一定的权益值奖励。

[0071] 应当理解的是，本领域技术人员在本发明技术构思的启发下，在不脱离本发明内容的基础上，可以根据上述说明做出各种改进或变换，这仍落在本发明的保护范围之内。

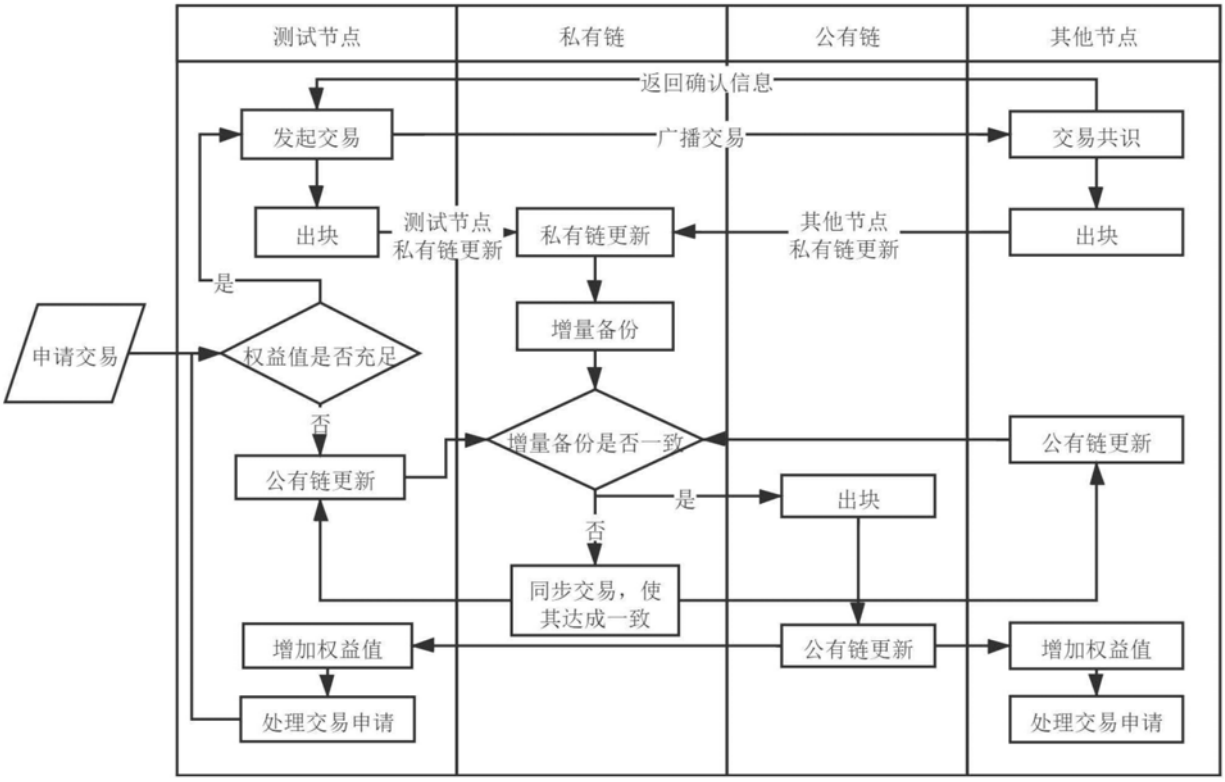

测试节点
私有链
公有链
其他节点
返回确认信息
发起交易
广播交易
交易共识
出块
测试节点
私有链更新
私有链更新
其他节点
私有链更新
出块
是
申请交易
权益值是否充足
增量备份
否
公有链更新
增量备份是否一致
公有链更新
是
出块
否
同步交易，使
其达成一致
增加权益值
公有链更新
增加权益值
处理交易申请
处理交易申请

图1

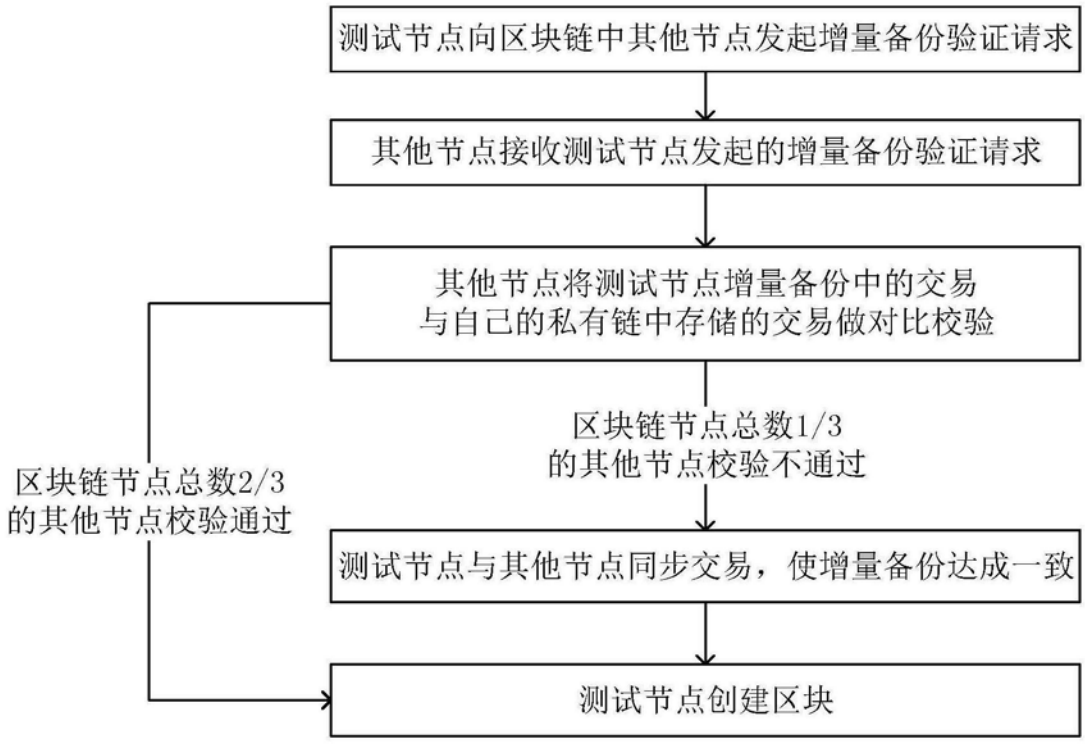

测试节点向区块链中其他节点发起增量备份验证请求
其他节点接收测试节点发起的增量备份验证请求
其他节点将测试节点增量备份中的交易
与自己的私有链中存储的交易做对比校验
区块链节点总数1/3
的其他节点校验不通过
区块链节点总数2/3
的其他节点校验通过
测试节点与其他节点同步交易，使增量备份达成一致
测试节点创建区块

图2

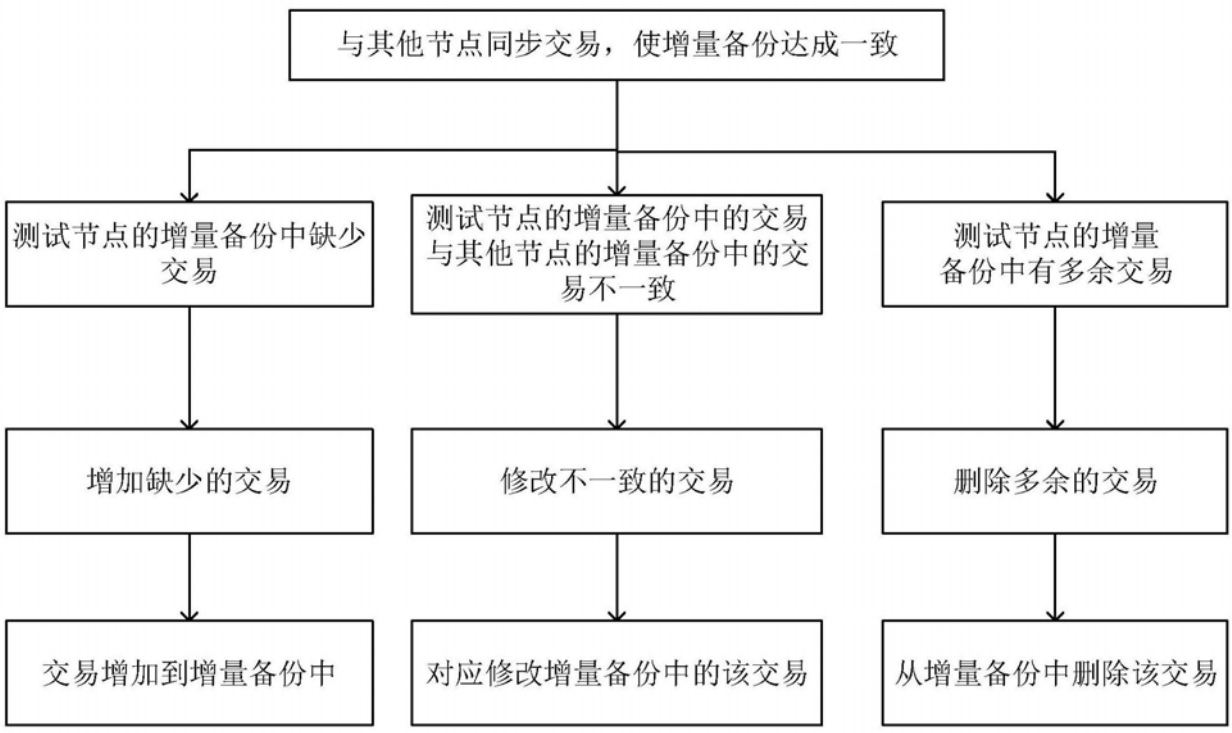

与其他节点同步交易，使增量备份达成一致
测试节点的增量备份中缺少交易
测试节点的增量备份中的交易与其他节点的增量备份中的交易不一致
测试节点的增量备份中有多余交易
增加缺少的交易
修改不一致的交易
删除多余的交易
交易增加到增量备份中
对应修改增量备份中的该交易
从增量备份中删除该交易

图3