(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 113704271 A
(43)申请公布日 2021.11.26

(21)申请号 202111034886.8

(22)申请日 2021.09.03

(71)申请人 杭州复杂美科技有限公司
地址 310000 浙江省杭州市西湖区文三路90号东部软件园6号楼7层702室

(72)发明人 王志文 吴思进

(51)Int.Cl.
G06F 16/22(2019.01)
G06F 16/23(2019.01)
G06F 16/27(2019.01)

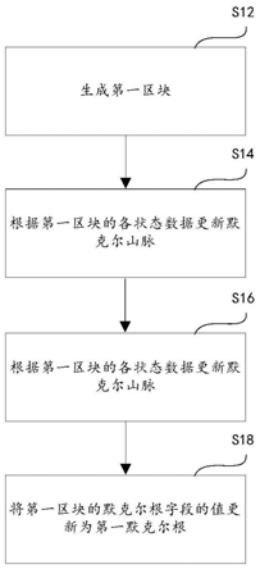
权利要求书4页 说明书9页 附图7页

(54)发明名称

默克尔树生成方法、非法节点识别方法、设备和存储介质

(57)摘要

本发明提供一种默克尔树生成方法、非法节点识别方法、防作弊方法、设备和存储介质，该方法包括：生成第一区块；根据第一区块的各状态数据更新默克尔山脉；根据所更新的默克尔山脉的各根节点生成第一默克尔二叉树和第一默克尔二叉树的第一默克尔根；将第一区块的默克尔根字段的值更新为第一默克尔根。本申请减小证明状态数据的存在性的树形结构。



CN 113704271 A

1.一种默克尔树生成方法,其特征在于,区块链网络的各节点分别存储有所在链的每个区块的默克尔树的全局索引表,状态数据以默克尔山脉的方式进行存储,所述全局索引表以区块高度为版本号,所述方法适用于区块链节点,所述方法包括:

生成第一区块;

根据所述第一区块的各状态数据更新默克尔山脉;

根据所更新的所述默克尔山脉的各根节点生成第一默克尔二叉树和所述第一默克尔二叉树的第一默克尔根;

将所述第一区块的默克尔根字段的值更新为所述第一默克尔根。

2.一种默克尔树生成方法,其特征在于,区块链网络的各节点分别存储有所在链的每个区块的默克尔树的全局索引表,所述全局索引表以区块高度为版本号,所述方法适用于区块链节点,所述方法包括:

生成第一区块;

根据所述第一区块的各状态数据生成第二默克尔二叉树和所述第二默克尔二叉树的第二默克尔根;

将所述第二默克尔根作为默克尔山脉的第一叶子节点;

根据所述第一叶子节点更新默克尔山脉;

根据所更新的所述默克尔山脉的各根节点生成第三默克尔二叉树和所述第三默克尔二叉树的第三默克尔根;

将所述第一区块的默克尔根字段的值更新为所述第三默克尔根。

3.根据权利要求2所述的方法,其特征在于,还包括:

在第一时长后,将所述第二默克尔二叉树分布式存储。

4.一种非法节点识别方法,其特征在于,区块链网络的各节点根据如权利要求1-3任一项所述的方法生成默克尔树,所述方法适用于平行链节点,所述方法包括:

在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时,从当前节点的状态数据库查找出执行第一交易所需的第二状态数据;其中,所述第一状态数据为所述第一共识交易中的执行所述第一交易得到的状态数据;

根据所述第二状态数据所在的第一平行链区块的第一默克尔山脉信息、所述第一交易生成第一举报交易并发送至主链,以供主链节点:

验证所述第二状态数据是否在所述第一默克尔山脉信息中:

在所述第二状态数据在所述第一默克尔山脉信息中时,根据所述第二状态数据执行所述第一交易以得到第三状态数据,并判断所述第三状态数据是否与所述第一状态数据相同:

在所述第三状态数据与所述第一状态数据不同时,识别出当前链的非法共识节点;其中,所述非法共识节点为提交所述第一高度的第二共识交易的共识节点,所述第二共识交易与所述第一共识交易的默克尔山脉相同。

5.根据权利要求4所述的方法,其特征在于,所述在所述第三状态数据与所述第一状态数据不同时,识别出当前链的非法共识节点包括:

在所述第三状态数据与所述第一状态数据不同时,识别出当前链的非法共识节点;

在所述第三状态数据与所述第一状态数据相同时,根据所述第三状态数据计算所述第

一高度的第二平行链区块的第二默克尔山脉，验证所述第一共识交易中的第一默克尔山脉与所述第二默克尔山脉是否相同：

在所述第一默克尔山脉与所述第二默克尔山脉不同时，识别出当前链的非法共识节点。

6.根据权利要求4所述的方法，其特征在于，所述第一默克尔山脉信息包括所述第一平行链区块的第三默克尔山脉，所述验证所述第二状态数据是否在所述第一默克尔山脉信息中包括：

验证所述第二状态数据是否在所述第三默克尔山脉中。

7.根据权利要求4所述的方法，其特征在于，所述第一默克尔山脉信息包括所述第一平行链区块的第二高度、所述第二状态数据、所述第二状态数据的第一默克尔山脉路径；所述验证所述第二状态数据是否在所述第一默克尔山脉信息中包括：

通过所述第二高度找到主链上标识为已正确共识的所述第二高度的第三共识交易；

根据所述第三共识交易中的第三默克尔山脉根、所述第二状态数据、所述第一默克尔山脉路径验证所述第二状态数据是否在所述第三默克尔山脉根中。

8.根据权利要求4-7任一项所述的方法，其特征在于，所述验证所述第二状态数据是否在所述第一默克尔山脉信息包括：

存证所述第一举报交易；

在预配置的第一时长内，接收第一挑战交易；其中，所述第一挑战交易由当前链的其它平行链节点在监测到主链上存证的所述第一举报交易中的所述第二状态数据不是执行所述第一交易所需的最新的状态数据时生成，所述第一挑战交易包括所述第一交易和第四状态数据所在的第三平行链区块的第二默克尔山脉信息，所述第四状态数据为所述其它平行链节点所查找出的执行第一交易所需的状态数据，所述第三平行链区块的区块高度高于所述第一平行链区块的区块高度；

验证所述第四状态数据是否在所述第二默克尔山脉信息中：

在所述第四状态数据不在所述第二默克尔山脉信息中，且到达所述第一时长时，验证所述第二状态数据是否在所述第一默克尔山脉信息中。

9.一种非法节点识别方法，其特征在于，区块链网络的各节点根据如权利要求1-3任一项所述的方法生成默克尔树，所述方法适用于主链节点，所述方法包括：

接收第一举报交易；其中，所述第一举报交易由第一平行链的第一平行链节点生成，所述第一举报交易根据第二状态数据所在的第一平行链区块的第一默克尔山脉信息、第一交易生成，所述第二状态数据为所述第一平行链节点从状态数据库中查找出的执行所述第一交易所需的状态数据，所述第二状态数据由所述第一平行链节点在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时所查找，所述第一状态数据为所述第一共识交易中的执行所述第一交易得到的状态数据；

验证所述第二状态数据是否在所述第一默克尔山脉信息中：

在所述第二状态数据在所述第一默克尔山脉信息中时，根据所述第二状态数据执行所述第一交易以得到第三状态数据，并判断所述第三状态数据是否与所述第一状态数据相同：

在所述第三状态数据与所述第一状态数据不同时，识别出所述第一平行链的非法共识

节点;其中,所述非法共识节点为提交所述第一高度的第二共识交易的共识节点,所述第二共识交易与所述第一共识交易的默克尔山脉相同。

10.根据权利要求9所述的方法,其特征在于,所述在所述第三状态数据与所述第一状态数据不同时,识别出所述第一平行链的非法共识节点包括:

在所述第三状态数据与所述第一状态数据不同时,识别出所述第一平行链的非法共识节点;

在所述第三状态数据与所述第一状态数据相同时,根据所述第三状态数据计算所述第一高度的第二平行链区块的第二默克尔山脉,验证所述第一共识交易中的第一默克尔山脉与所述第二默克尔山脉是否相同:

在所述第一默克尔山脉与所述第二默克尔山脉不同时,识别出所述第一平行链的非法共识节点。

11.根据权利要求9所述的方法,其特征在于,所述第一默克尔山脉信息包括所述第一平行链区块的第三默克尔山脉,所述验证所述第二状态数据是否在所述第一默克尔山脉信息中包括:

验证所述第二状态数据是否在所述第三默克尔山脉中。

12.根据权利要求9所述的方法,其特征在于,所述第一默克尔山脉信息包括所述第一平行链区块的第二高度、所述第二状态数据、所述第二状态数据的第一默克尔山脉路径;所述验证所述第二状态数据是否在所述第一默克尔山脉信息中包括:

通过所述第二高度找到主链上标识为已正确共识的所述第二高度的第三共识交易;

根据所述第三共识交易中的第三默克尔山脉根、所述第二状态数据、所述第一默克尔山脉路径验证所述第二状态数据是否在所述第三默克尔山脉根中。

13.根据权利要求9-12任一项所述的方法,其特征在于,所述验证所述第二状态数据是否在所述第一默克尔山脉信息包括:

存证所述第一举报交易;

在预配置的第一时长内,接收第一挑战交易;其中,所述第一挑战交易由当前链的其它平行链节点在监测到主链上存证的所述第一举报交易中的所述第二状态数据不是执行所述第一交易所需的最新的状态数据时生成,所述第一挑战交易包括所述第一交易和第四状态数据所在的第三平行链区块的第二默克尔山脉信息,所述第四状态数据为所述其它平行链节点所查找出的执行第一交易所需的状态数据,所述第三平行链区块的区块高度高于所述第一平行链区块的区块高度;

验证所述第四状态数据是否在所述第二默克尔山脉信息中:

在所述第四状态数据不在所述第二默克尔山脉信息中,且到达所述第一时长时,验证所述第二状态数据是否在所述第一默克尔山脉信息中。

14.一种防作弊方法,其特征在于,适用于主链节点,所述方法包括:

惩罚第一平行链的非法共识节点;其中,所述第一平行链的非法共识节点根据如权利要求9-13任一项所述的方法识别得到。

15.一种计算机设备,其特征在于,所述设备包括:

一个或多个处理器;

存储器,用于存储一个或多个程序,

当所述一个或多个程序被所述一个或多个处理器执行时，使得所述一个或多个处理器执行如权利要求1-14中任一项所述的方法。

16.一种存储有计算机程序的存储介质，其特征在于，该程序被处理器执行时实现如权利要求1-14中任一项所述的方法。

默克尔树生成方法、非法节点识别方法、设备和存储介质

技术领域

[0001] 本申请涉及区块链技术领域，具体涉及一种默克尔树生成方法、非法节点识别方法、防作弊方法、设备和存储介质。

背景技术

[0002] 在现有技术中，区块链采用mpt结构来证明状态数据的存在性。

[0003] 上述机制使得证明状态数据的存在性的树形结构非常庞大。

发明内容

[0004] 鉴于现有技术中的上述缺陷或不足，期望提供一种减小证明状态数据的存在性的树形结构的默克尔树生成方法、非法节点识别方法、防作弊方法、设备和存储介质。

[0005] 第一方面，本发明提供一种适用于区块链节点的默克尔树生成方法，区块链网络的各节点分别存储有所在链的每个区块的默克尔树的全局索引表，状态数据以默克尔山脉的方式进行存储，全局索引表以区块高度为版本号，上述方法包括：

[0006] 生成第一区块；

[0007] 根据第一区块的各状态数据更新默克尔山脉；

[0008] 根据所更新的默克尔山脉的各根节点生成第一默克尔二叉树和第一默克尔二叉树的第一默克尔根；

[0009] 将第一区块的默克尔根字段的值更新为第一默克尔根。

[0010] 第二方面，本发明提供一种适用于区块链节点的默克尔树生成方法，区块链网络的各节点分别存储有所在链的每个区块的默克尔树的全局索引表，全局索引表以区块高度为版本号，上述方法包括：

[0011] 生成第一区块；

[0012] 根据第一区块的各状态数据生成第二默克尔二叉树和第二默克尔二叉树的第二默克尔根；

[0013] 将第二默克尔根作为默克尔山脉的第一叶子节点；

[0014] 根据第一叶子节点更新默克尔山脉；

[0015] 根据所更新的默克尔山脉的各根节点生成第三默克尔二叉树和第三默克尔二叉树的第三默克尔根；

[0016] 将第一区块的默克尔根字段的值更新为第三默克尔根。

[0017] 第三方面，本发明提供一种适用于平行链节点的非法节点识别方法，区块链网络的各节点根据如上述第一方面或第二方面的方法生成默克尔树，上述方法包括：

[0018] 在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时，从当前节点的状态数据库查找出执行第一交易所需的第二状态数据；其中，第一状态数据为第一共识交易中的执行第一交易得到的状态数据；

[0019] 根据第二状态数据所在的第一平行链区块的第一默克尔山脉信息、第一交易生成

第一举报交易并发送至主链，以供主链节点：

[0020] 验证第二状态数据是否在第一默克尔山脉信息中：

[0021] 在第二状态数据在第一默克尔山脉信息中时，根据第二状态数据执行第一交易以得到第三状态数据，并判断第三状态数据是否与第一状态数据相同：

[0022] 在第三状态数据与第一状态数据不同时，识别出当前链的非法共识节点；其中，非法共识节点为提交第一高度的第二共识交易的共识节点，第二共识交易与第一共识交易的默克尔山脉相同。

[0023] 第四方面，本发明提供一种适用于主链节点的非法节点识别方法，区块链网络的各节点根据如上述第一方面或第二方面的方法生成默克尔树，上述方法包括：

[0024] 接收第一举报交易；其中，第一举报交易由第一平行链的第一平行链节点生成，第一举报交易根据第二状态数据所在的第一平行链区块的第一默克尔山脉信息、第一交易生成，第二状态数据为第一平行链节点从状态数据库中查找出的执行第一交易所需的状态数据，第二状态数据由第一平行链节点在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时所查找，第一状态数据为第一共识交易中的执行第一交易得到的状态数据；

[0025] 验证第二状态数据是否在第一默克尔山脉信息中：

[0026] 在第二状态数据在第一默克尔山脉信息中时，根据第二状态数据执行第一交易以得到第三状态数据，并判断第三状态数据是否与第一状态数据相同：

[0027] 在第三状态数据与第一状态数据不同时，识别出第一平行链的非法共识节点；其中，非法共识节点为提交第一高度的第二共识交易的共识节点，第二共识交易与第一共识交易的默克尔山脉相同。

[0028] 第五方面，本发明提供一种适用于主链节点的防作弊方法，上述方法包括：

[0029] 惩罚第一平行链的非法共识节点；其中，第一平行链的非法共识节点根据上述第四方面的方法识别得到。

[0030] 第六方面，本发明还提供一种设备，包括一个或多个处理器和存储器，其中存储器包含可由该一个或多个处理器执行的指令以使得该一个或多个处理器执行根据本发明各实施例提供的默克尔树生成方法、非法节点识别方法和防作弊方法。

[0031] 第四方面，本发明还提供一种存储有计算机程序的存储介质，该计算机程序使计算机执行根据本发明各实施例提供的默克尔树生成方法、非法节点识别方法和防作弊方法。

[0032] 本发明诸多实施例提供的默克尔树生成方法、非法节点识别方法、防作弊方法、设备和存储介质通过生成第一区块；根据第一区块的各状态数据更新默克尔山脉；根据所更新的默克尔山脉的各根节点生成第一默克尔二叉树和第一默克尔二叉树的第一默克尔根；将第一区块的默克尔根字段的值更新为第一默克尔根的方法，减小证明状态数据的存在性的树形结构。

附图说明

[0033] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0034] 图1为本发明一实施例提供的默克尔山脉的示意图。

[0035] 图2为本发明一实施例提供的一种默克尔树生成方法的流程图。

[0036] 图3为根据图2所示方法所构建的默克尔树的示意图。

[0037] 图4为本发明一实施例提供的一种默克尔树生成方法的流程图。

[0038] 图5为根据图4所示方法所构建的部分默克尔树的示意图。

[0039] 图6为根据图4所示方法所构建的完整默克尔树的示意图。

[0040] 图7为本发明一实施例提供的一种非法节点识别方法的流程图。

[0041] 图8为本发明一实施例提供的另一种非法节点识别方法的流程图。

[0042] 图9为本发明一实施例提供的一种防作弊方法的流程图。

[0043] 图10为本发明一实施例提供的一种计算机设备的结构示意图。

具体实施方式

[0044] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与发明相关的部分。

[0045] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0046] 图1为默克尔山脉的示意图。默克尔山脉(MMR)相对于默克尔二叉树的优点是，当有新数据到来的时候(新数据，指的是叶子节点)，中间节点的值不需要改变，数据永远都是追加。在现有技术中，MMR一般用于验证交易的存在性，而在本申请中，MMR用于验证状态信息的存在性。如图1所示，假设当前图中的默克尔山脉根为root1；如果要验证15的状态数据是否存在，需要提供默克尔山脉路径(16、18、14)，具体为，根据15和16生成17，根据14、17、18生成默克尔山脉根root1'，如果root1＝root1'，则代表15的状态数据存在。

[0047] 图2为本发明一实施例提供的一种默克尔树生成方法的流程图。如图2所示，在本实施例中，本发明提供一种适用于区块链节点的默克尔树生成方法，区块链网络的各节点分别存储有所在链的每个区块的默克尔树的全局索引表，状态数据以默克尔山脉的方式进行存储，全局索引表以区块高度为版本号，上述方法包括：

[0048] S12：生成第一区块；

[0049] S14：根据第一区块的各状态数据更新默克尔山脉；

[0050] S16：根据所更新的默克尔山脉的各根节点生成第一默克尔二叉树和第一默克尔二叉树的第一默克尔根；

[0051] S18：将第一区块的默克尔根字段的值更新为第一默克尔根。

[0052] 以图1所示的MMR为例；假设生成block(10)后的MMR由图1的0～17构成，假设区块链网络中有node1～node7；

[0053] node1～node7执行步骤S12，生成区块block(11)；假设执行block(11)的各交易后，只改变了一个状态数据，所改变的状态数据为18；

[0054] node1～node7执行步骤S14，根据block(11)的状态数据18更新MMR，更新后的MMR由图1的0～18构成；

[0055] node1～node7执行步骤S16，根据14、17、18、18'(由18复制得到)生成默克尔二叉

树,以及该默克尔二叉树的默克尔根;本领域技术人员应当理解,此时是默克尔二叉树是奇数个点,所以计算merkeltree的时候,18会复制一个18';

[0056] 此时,构建了如图3所示的默克尔树;

[0057] node1～node7执行步骤S18,将block(11)的默克尔根字段的值更新为上述默克尔二叉树的默克尔根。

[0058] 本领域技术人员应当理解,此时要验证18的存在性,可以至少有一种方案,具体为,根据14、17、18、18'计算出root2',如果block(11)的默克尔根＝root2',则代表18的状态数据存在。

[0059] 在现有技术中,是直接根据14、17、18生成block(11)的默克尔根字段的值;图1所示的MMR只有3个根节点,假设现在一共有4亿的数据(大概有32个根节点,),则MMR非常大,至少需要(32+32)*32,大约为2k的数据;通过上述实施例所示的方法构造MMR,则只需要(32+5)*32,所构造的MMR高度降低,数据减小。

[0060] 图4为本发明一实施例提供的一种默克尔树生成方法的流程图。如图4所示,在本实施例中,本发明提供一种适用于区块链节点的默克尔树生成方法,区块链网络的各节点分别存储有所在链的每个区块的默克尔树的全局索引表,全局索引表以区块高度为版本号,上述方法包括:

[0061] S21:生成第一区块;

[0062] S22:根据第一区块的各状态数据生成第二默克尔二叉树和第二默克尔二叉树的第二默克尔根;

[0063] S23:将第二默克尔根作为默克尔山脉的第一叶子节点;

[0064] S24:根据第一叶子节点更新默克尔山脉;

[0065] S25:根据所更新的默克尔山脉的各根节点生成第三默克尔二叉树和第三默克尔二叉树的第三默克尔根;

[0066] S26:将第一区块的默克尔根字段的值更新为第三默克尔根。

[0067] 以图1所示的MMR为例;假设生成block(10)后的MMR由图1的0～17构成;

[0068] node1～node7执行步骤S21,生成区块block(11);假设执行block(11)的各交易后,生成了四个状态数据state1～state4(对应于图中的s1～s4);

[0069] node1～node7执行步骤S22,根据上述state1～state4生成默克尔二叉树和默克尔二叉树的默克尔根s1234;

[0070] node1～node7执行步骤S23,将s1234作为MMR的叶子节点,此时,构建了如图5所示的部分默克尔树;s1234即图5所示的18;

[0071] node1～node7执行步骤S24,根据18更新MMR,更新后的MMR由图5的0～18构成;

[0072] node1～node7执行步骤S25,根据14、17、18、18'(由18复制得到)生成默克尔二叉树',以及该默克尔二叉树的默克尔根';

[0073] 此时,构建了如图6所示的完整默克尔树;本领域技术人员应当理解,此时是默克尔二叉树是奇数个点,所以计算merkel tree的时候,18会复制一个18';

[0074] node1～node7执行步骤S26,将block(11)的默克尔根字段的值更新为上述默克尔二叉树的默克尔根'。

[0075] 本领域技术人员应当理解,此时要验证s4的存在性,可以至少有两种方案;方案一

为,根据第一默克尔路径s3、s12验证s4是否存在于18中;方案二为,根据第一默克尔路径s3、s12,第二默克尔路径14、17验证s4是否存在,具体为,根据s3、s12计算出18,再根据14、17、18、18'计算出root2',如果block(11)的默克尔根=root2',则代表s4的状态数据存在。

[0076] 上述实施例同样可以使得所构造的MMR高度降低,数据减小。

[0077] 图4所示的实施例与图2所示的实施例的不同之处在于,根据图4所示的实施例的方法所构造的MMR的根节点更少,MMR更小。

[0078] 优选地,上述方法还包括:

[0079] 在第一时长后,将第二默克尔二叉树分布式存储。

[0080] 图7为本发明一实施例提供的一种非法节点识别方法的流程图。如图7所示,在本实施例中,本发明提供一种适用于平行链节点的非法节点识别方法,区块链网络的各节点(包括主链节点和平行链节点,主链节点根据上述默克尔树生成方法生成主链区块的默克尔树,平行链节点根据上述默克尔树生成方法生成平行链区块的默克尔树)根据如上述默克尔树生成方法生成默克尔树,上述方法包括:

[0081] S32:在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时,从当前节点的状态数据库查找出执行第一交易所需的第二状态数据;其中,第一状态数据为第一共识交易中的执行第一交易得到的状态数据;

[0082] S34:根据第二状态数据所在的第一平行链区块的第一默克尔山脉信息、第一交易生成第一举报交易并发送至主链,以供主链节点:

[0083] 验证第二状态数据是否在第一默克尔山脉信息中:

[0084] 在第二状态数据在第一默克尔山脉信息中时,根据第二状态数据执行第一交易以得到第三状态数据,并判断第三状态数据是否与第一状态数据相同:

[0085] 在第三状态数据与第一状态数据不同时,识别出当前链的非法共识节点;其中,非法共识节点为提交第一高度的第二共识交易的共识节点,第二共识交易与第一共识交易的默克尔山脉相同。

[0086] 具体的,以第一默克尔山脉信息包括第一平行链区块的第二高度、第二状态数据、第二状态数据的第一默克尔山脉路径;验证第二状态数据是否在第一默克尔山脉信息中包括"通过第二高度找到主链上标识为已正确共识的第二高度的第三共识交易;根据第三共识交易中的第三默克尔山脉根、第二状态数据、第一默克尔山脉路径验证第二状态数据是否在第三默克尔山脉根中"为例;

[0087] 假设有主链mainchain和平行链pc1,pc1有平行链节点node1～node7,node1～node4是共识节点,node1～node4在主链上冻结有若干押金;假设当前addr(a)的状态数据为1万(该状态数据为在执行block(8)时生成),有一笔pc1的转账交易tx1(将10万coins从addr(a)转至addr(b));node1～node3联合作弊,node1～node3的tx1的执行状态为执行成功,并分别生成block(10)_node1～block(10)_node3;node4～node7的tx1的执行状态为执行失败,并分别生成block(10)_node4～block(10)_node7;node1根据block(10)_node1生成共识交易tx_consensus(10)_node1并发送至主链……node4根据block(10)_node4生成共识交易tx_consensus(10)_node4并发送至主链;主链节点根据tx_consensus(10)_node1～tx_consensus(10)_node4来完成主链侧的block(10)的平行链共识;主链上标识为已正确共识的block(10)的共识交易为tx_consensus(10)_node1～tx_consensus(10)_node3,

即主链侧tx1执行成功通过共识；

[0088] node4判断出主链上标识为已正确共识的block(10)的共识交易(以tx_consensus(10)_node1为例)的执行tx1的状态数据不正确，执行步骤S32，从node4的状态数据库查找出执行tx1所需的状态数据，即，addr(a)的状态数据为1万(该状态数据为在执行block(8)时生成)；

[0089] node4执行步骤S34，根据高度8、addr(a):1万、addr(a):1万的默克尔山脉路径、tx1生成举报交易tx2并发送至主链；本领域技术人员应当理解，还可以根据实际需求将tx2中的tx1替换为hash(tx1)等可以找到tx1的区块数据，可实现相同的技术效果；

[0090] 主链节点根据高度8找到主链上标识为已正确共识的共识交易(假设为tx_consensus(8)_node1)，根据tx_consensus(8)_node1的默克尔山脉根、addr(a):1万、addr(a):1万的默克尔山脉路径验证addr(a):1万是否在tx_consensus(8)_node1的默克尔山脉根中；

[0091] 假设addr(a):1万确实在tx_consensus(8)_node1的默克尔山脉根中，则主链节点根据addr(a):1万执行tx1；

[0092] 由于addr(a)的余额只剩1万，执行tx1失败，执行状态为执行失败，而tx_consensus(10)_node1的执行状态为执行成功，且tx_consensus(10)_node2～tx_consensus(10)_node3的默克尔山脉与tx_consensus(10)_node1的默克尔山脉相同，则主链节点识别出pc1的非法节点为node1～node3。

[0093] 在更多实施例中，默克尔山脉信息所包括的具体内容还可以根据实际需求进行配置，例如配置为，默克尔山脉信息包括第一平行链区块的第三默克尔山脉；相应的，验证第二状态数据是否在第一默克尔山脉信息中的步骤则配置为“验证第二状态数据是否在第三默克尔山脉中”，可实现相同的技术效果。

[0094] 在更多实施例中，主链节点还可以根据实际需求惩罚所识别出的非法共识节点，例如，如果各平行链的共识节点在主链上冻结有若干押金，则可以罚没非法共识节点的部分押金；或者配置为，将当前链的非法共识节点加入黑名单，主链节点将屏蔽黑名单中的共识节点所发送的共识交易等。

[0095] 本领域技术人员应当理解，还可以根据实际需求配置可以生成举报交易的角色，例如配置为，只有共识节点可以生成举报交易，或所有平行链节点均可以生成举报交易，可实现相同的技术效果。

[0096] 上述实施例用更少的时间和更少的算力识别出联合作弊的平行链共识节点。

[0097] 假设有如下第一场景：

[0098] node1～node3在运行v1.0的区块链代码，而node4～node7运行了v1.1的区块链代码则node1～node3虽然执行得到了正确的状态数据(即第三状态数据与第一状态数据相同)，但是计算出的默克尔山脉仍然是错误的。

[0099] 上述第一场景产生的问题可由如下实施例所示的方法解决；

[0100] 优选地，在第三状态数据与第一状态数据不同时，识别出当前链的非法共识节点包括：

[0101] 在第三状态数据与第一状态数据不同时，识别出当前链的非法共识节点；

[0102] 在第三状态数据与第一状态数据相同时，根据第三状态数据计算第一高度的第二

平行链区块的第二默克尔山脉，验证第一共识交易中的第一默克尔山脉与第二默克尔山脉是否相同：

[0103] 在第一默克尔山脉与第二默克尔山脉不同时，识别出当前链的非法共识节点。

[0104] 在上述第一场景中，node1～node3仍然应当被识别为非法节点。

[0105] 假设有如下第二场景：

[0106] node4所提交的第一默克尔山脉信息是正确的，但其实正确的block(9)中，存在另一笔执行成功的交易tx2，该tx2执行成功后，addr(a)的状态数据更新为addr(a):11万；此时block(10)中的tx1其实是可以执行成功的。引起该种场景的原因可能有多种，例如node4的block(9)是不正确的，或者，node4故意作恶等。

[0107] 上述第二场景产生的问题可由如下实施例所示的方法解决；

[0108] 优选地，验证第二状态数据是否在第一默克尔山脉信息包括：

[0109] 存证第一举报交易；

[0110] 在预配置的第一时长内，接收第一挑战交易；其中，第一挑战交易由当前链的其它平行链节点在监测到主链上存证的第一举报交易中的第二状态数据不是执行第一交易所需的最新的状态数据时生成，第一挑战交易包括第一交易和第四状态数据所在的第三平行链区块的第二默克尔山脉信息，第四状态数据为其它平行链节点所查找出的执行第一交易所需的状态数据，第三平行链区块的区块高度高于第一平行链区块的区块高度；

[0111] 验证第四状态数据是否在第二默克尔山脉信息中：

[0112] 在第四状态数据不在第二默克尔山脉信息中，且到达第一时长时，验证第二状态数据是否在第一默克尔山脉信息。

[0113] 假设在第一时长内，node5生成了挑战交易tx3，tx3包括tx1、bl ock(9)的默克尔山脉信息(假设为tx1、addr(a):11万、addr(a):11万的默克尔山脉路径)；

[0114] 如果主链节点验证出addr(a):11万不在block(9)的默克尔山脉中，则应当在到达第一时长时，验证第二状态数据是否在第一默克尔山脉信息，即，验证addr(a):1万是否在tx_consensus(8)_node1的默克尔山脉根中；

[0115] 本领域技术人员应当理解，还可以根据实际需求配置主链节点在验证出addr(a):11万在block(9)的默克尔山脉中时的操作，例如配置为结束；或，罚没node4的若干押金等。

[0116] 图8为本发明一实施例提供的另一种非法节点识别方法的流程图。图8所示的方法可与图7所示的方法配合使用。如图8所示，在本实施例中，本发明提供一种适用于主链节点的非法节点识别方法，区块链网络的各节点根据如上述第一方面或第二方面的方法生成默克尔树，上述方法包括：

[0117] S42:接收第一举报交易；其中，第一举报交易由第一平行链的第一平行链节点生成，第一举报交易根据第二状态数据所在的第一平行链区块的第一默克尔山脉信息、第一交易生成，第二状态数据为第一平行链节点从状态数据库中查找出的执行第一交易所需的状态数据，第二状态数据由第一平行链节点在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时所查找，第一状态数据为第一共识交易中的执行第一交易得到的状态数据；

[0118] S441:验证第二状态数据是否在第一默克尔山脉信息中：

[0119] 在第二状态数据在第一默克尔山脉信息中时，执行步骤S4421:根据第二状态数据

执行第一交易以得到第三状态数据，并判断第三状态数据是否与第一状态数据相同：

[0120] 在第三状态数据与第一状态数据不同时，执行步骤S4422：识别出第一平行链的非法共识节点；其中，非法共识节点为提交第一高度的第二共识交易的共识节点，第二共识交易与第一共识交易的默克尔山脉相同。

[0121] 上述实施例的非法节点识别原理可参考图7所示的方法，此处不再赘述。

[0122] 图9为本发明一实施例提供的一种防作弊方法的流程图。如图9所示，在本实施例中，本发明提供一种适用于主链节点的防作弊方法，上述方法包括：

[0123] S52：惩罚第一平行链的非法共识节点；其中，第一平行链的非法共识节点根据上述非法节点识别方法识别得到。

[0124] 在更多实施例中，主链节点还可以根据实际需求惩罚所识别出的非法共识节点，例如，如果各平行链的共识节点在主链上冻结有若干押金，则可以罚没非法共识节点的部分押金；或者配置为，将第一平行链的非法共识节点加入黑名单，主链节点将屏蔽黑名单中的共识节点所发送的共识交易等。

[0125] 针对图7所示的一种优选实施方式所识别到的非法共识节点，主链节点也可以根据实际需求配置不同情况下惩罚所识别出的非法共识节点的方法，例如，在第三状态数据与第一状态数据不同时，罚没非法共识节点的部分押金；在第三状态数据与第一状态数据相同，但第一默克尔山脉与第二默克尔山脉不同时，将第一平行链的非法共识节点加入黑名单并在主链上记录报错信息。

[0126] 图10为本发明一实施例提供的一种计算机设备的结构示意图。

[0127] 如图10所示，作为另一方面，本申请还提供了一种计算机设备，包括一个或多个中央处理单元(CPU)1001，其可以根据存储在只读存储器(ROM)1002中的程序或者从存储部分1008加载到随机访问存储器(RAM)1003中的程序而执行各种适当的动作和处理。在RAM1003中，还存储有计算机设备操作所需的各种程序和数据。CPU1001、ROM1002以及RAM1003通过总线1004彼此相连。输入/输出(I/O)接口1005也连接至总线1004。

[0128] 以下部件连接至I/O接口1005：包括键盘、鼠标等的输入部分1006；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分1007；包括硬盘等的存储部分1008；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分1009。通信部分1009经由诸如因特网的网络执行通信处理。驱动器1010也根据需要连接至I/O接口1005。可拆卸介质1011，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器1010上，以便于从其上读出的计算机程序根据需要被安装入存储部分1008。

[0129] 特别地，根据本公开的实施例，上述任一实施例描述的方法可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括有形地包含在机器可读介质上的计算机程序，所述计算机程序包含用于执行上述任一方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分1009从网络上被下载和安装，和/或从可拆卸介质1011被安装。

[0130] 作为又一方面，本申请还提供了一种计算机可读存储介质，该计算机可读存储介质可以是上述实施例的装置中所包含的计算机可读存储介质；也可以是单独存在，未装配入计算机设备中的计算机可读存储介质。计算机可读存储介质存储有一个或者一个以上程序，该程序被一个或者一个以上的处理器用来执行描述于本申请提供的方法。

[0131] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这根据所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以通过执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以通过专用硬件与计算机指令的组合来实现。

[0132] 描述于本申请实施例中所涉及到的单元或模块可以通过软件的方式实现，也可以通过硬件的方式来实现。所描述的单元或模块也可以设置在处理器中，例如，各所述单元可以是设置在计算机或移动智能设备中的软件程序，也可以是单独配置的硬件装置。其中，这些单元或模块的名称在某种情况下并不构成对该单元或模块本身的限定。

[0133] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离本申请构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

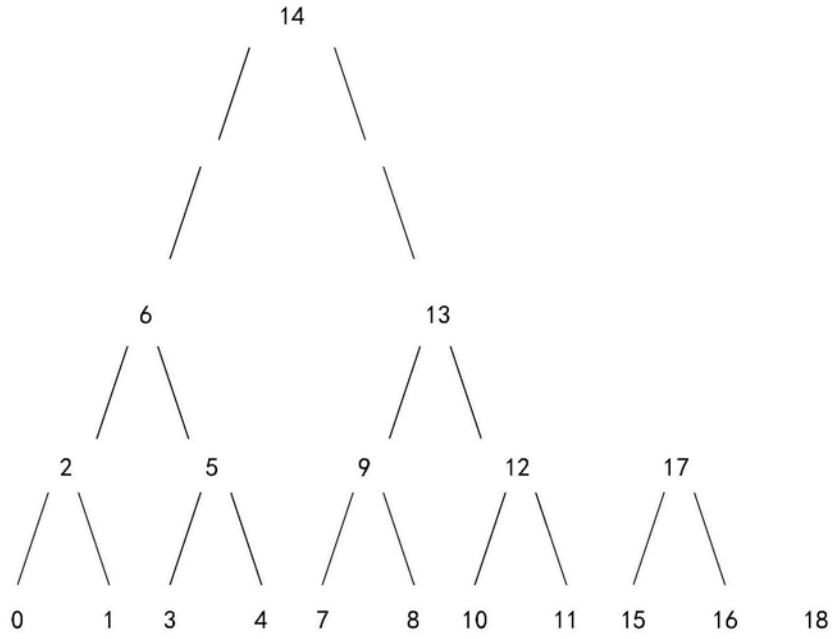

14
6
13
2
5
9
12
17
0
1
3
4
7
8
10
11
15
16
18

图1

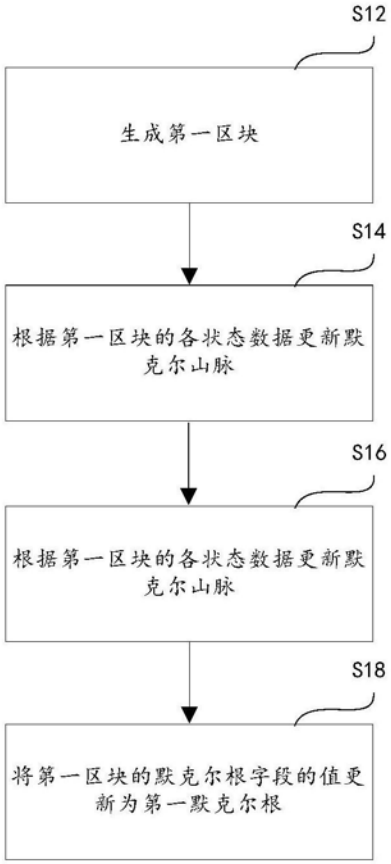

S12
生成第一区块
S14
根据第一区块的各状态数据更新默克尔山脉
S16
根据第一区块的各状态数据更新默克尔山脉
S18
将第一区块的默克尔根字段的值更新为第一默克尔根

图2

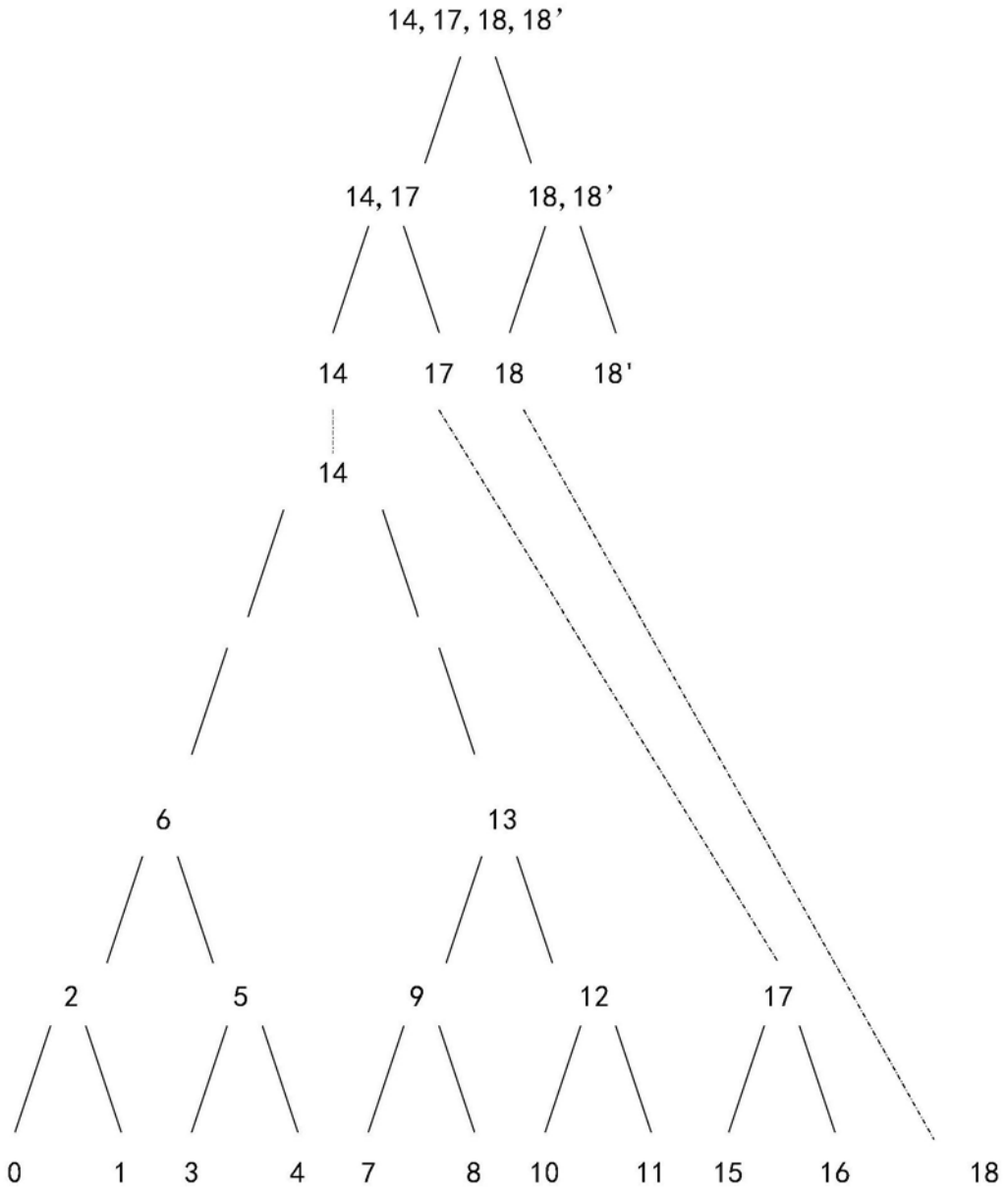

14, 17, 18, 18'
14, 17
18, 18'
14
17
18
18'
14
6
13
2
5
9
12
17
0
1
3
4
7
8
10
11
15
16
18

图3

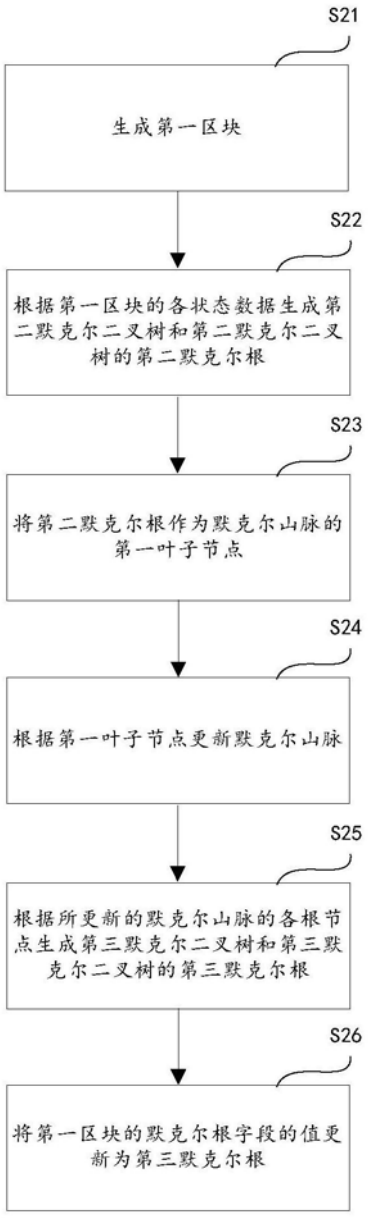

S21
生成第一区块
S22
根据第一区块的各状态数据生成第二默克尔二叉树和第二默克尔二叉树的第二默克尔根
S23
将第二默克尔根作为默克尔山脉的第一叶子节点
S24
根据第一叶子节点更新默克尔山脉
S25
根据所更新的默克尔山脉的各根节点生成第三默克尔二叉树和第三默克尔二叉树的第三默克尔根
S26
将第一区块的默克尔根字段的值更新为第三默克尔根

图4

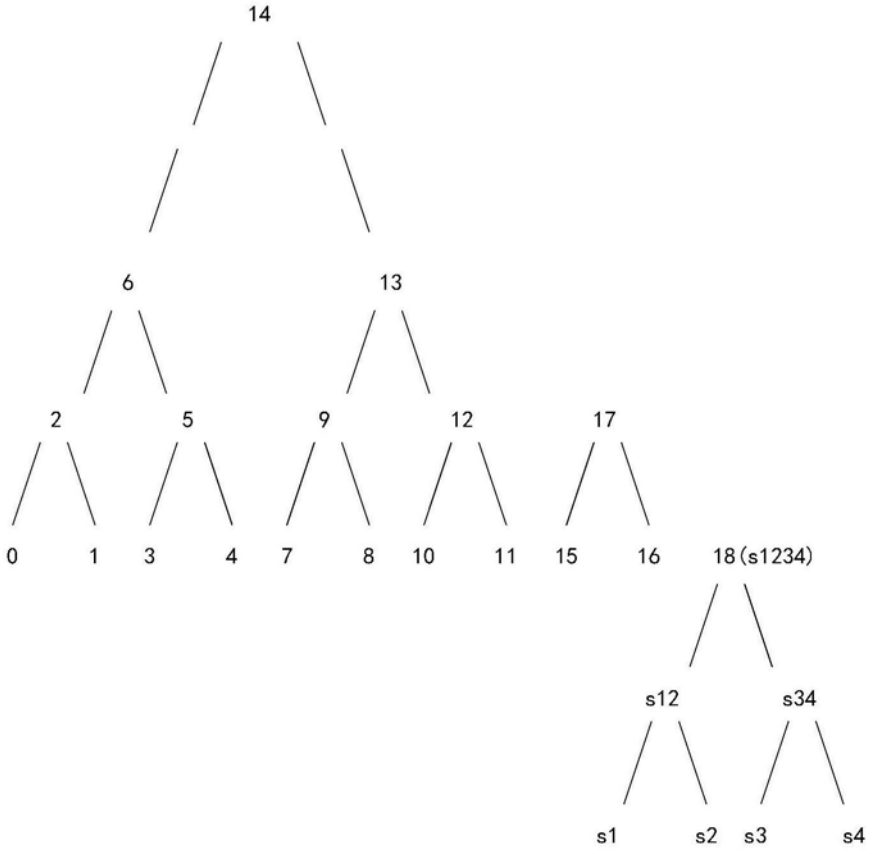


图5

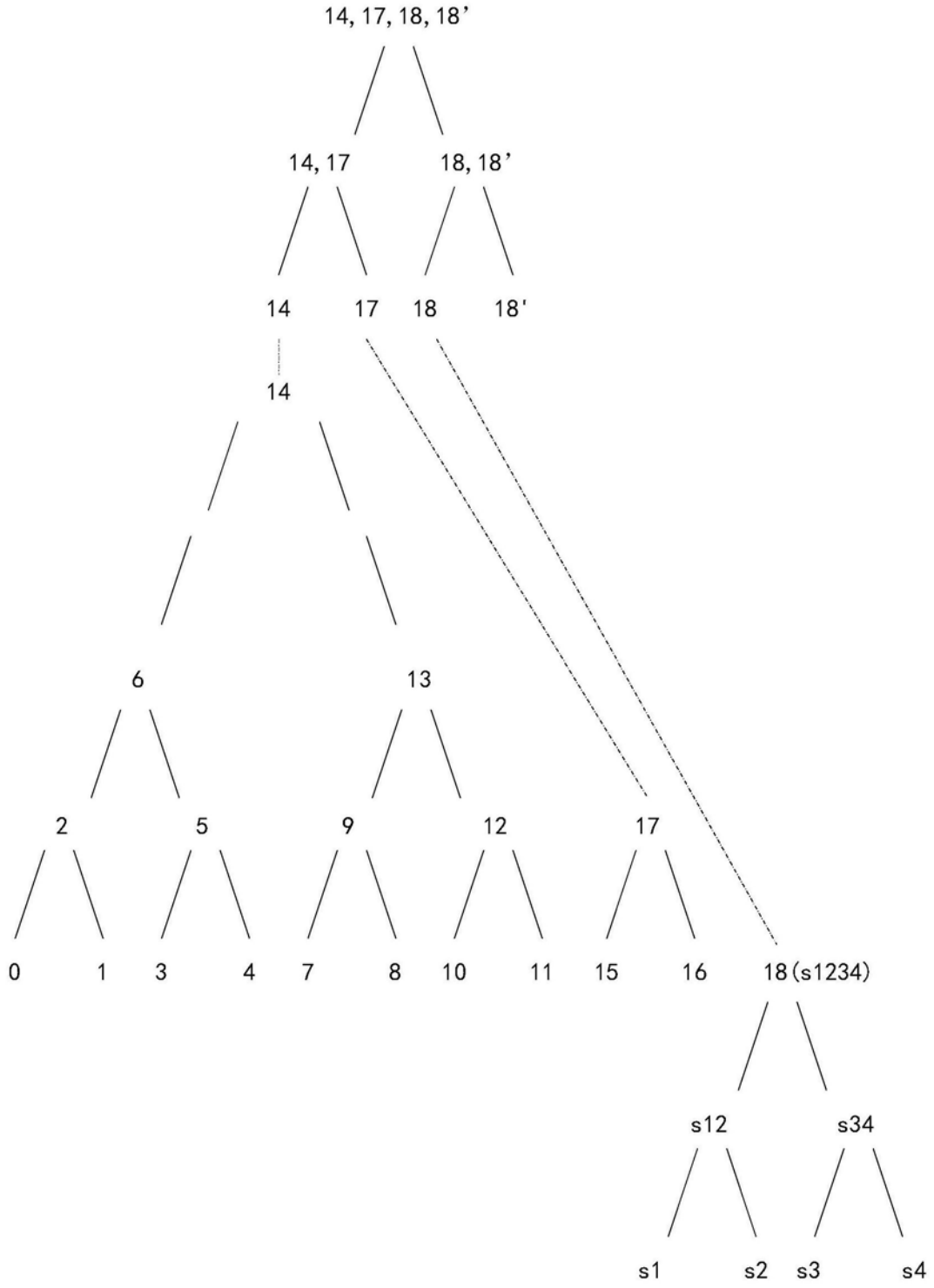

14, 17, 18, 18'
14, 17
18, 18'
14
17
18
18'
14
6
13
2
5
9
12
17
0
1
3
4
7
8
10
11
15
16
18(s1234)
s12
s34
s1
s2
s3
s4

图6

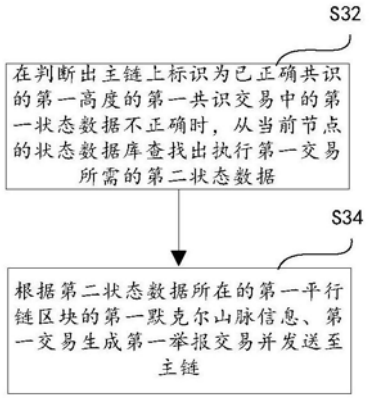

S32
在判断出主链上标识为已正确共识的第一高度的第一共识交易中的第一状态数据不正确时，从当前节点的状态数据库查找出执行第一交易所需的第二状态数据
S34
根据第二状态数据所在的第一平行链区块的第一默克尔山脉信息、第一交易生成第一举报交易并发送至主链

图7

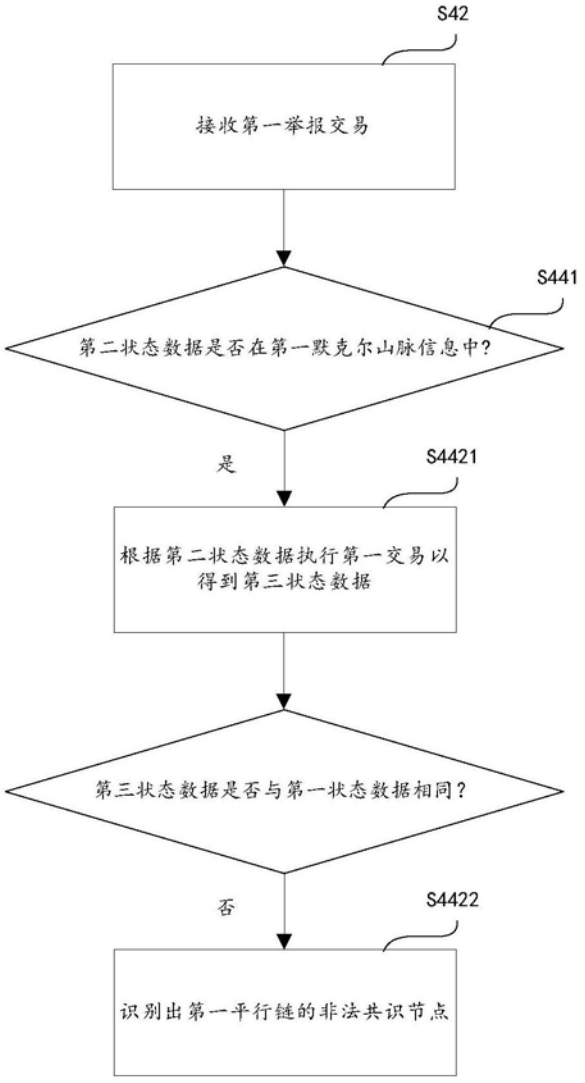

S42
接收第一举报交易
S441
第二状态数据是否在第一默克尔山脉信息中？
是
S4421
根据第二状态数据执行第一交易以得到第三状态数据
第三状态数据是否与第一状态数据相同？
否
S4422
识别出第一平行链的非法共识节点

图8

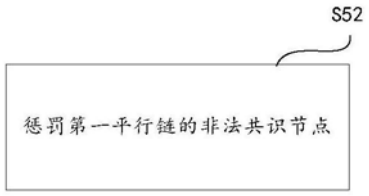

S52
惩罚第一平行链的非法共识节点

图9

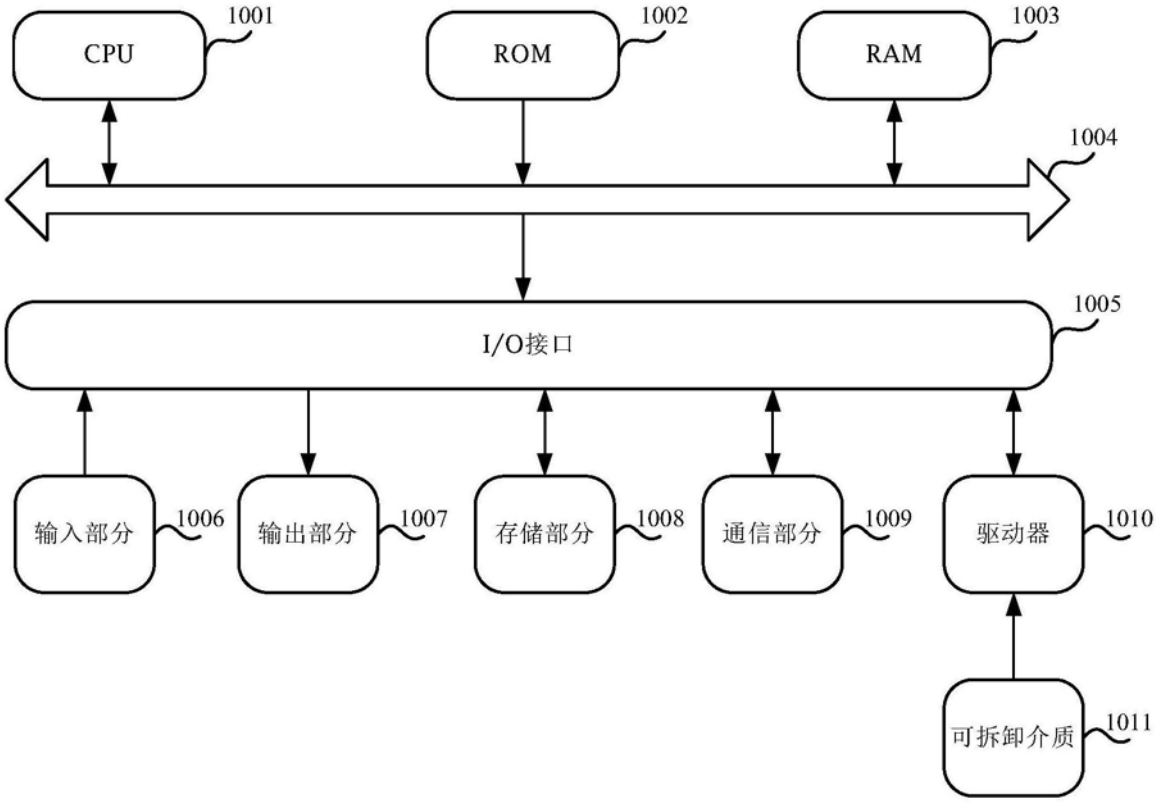

CPU
1001
ROM
1002
RAM
1003
1004
I/O接口
1005
输入部分
1006
输出部分
1007
存储部分
1008
通信部分
1009
驱动器
1010
可拆卸介质
1011

图10