(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 107743064 A
(43)申请公布日 2018.02.27

(21)申请号 201710903353.6

(22)申请日 2017.09.28

(71)申请人 深圳市易成自动驾驶技术有限公司
地址 518000 广东省深圳市南山区西丽街道高新科技产业园北区朗山路16号华瀚创新园

(72)发明人 刘新 宋朝忠 郭烽 单单

(74)专利代理机构 深圳市世纪恒程知识产权代理事务所 44287
代理人 胡海国 赵爱蓉

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/00(2006.01)
G06Q 20/38(2012.01)

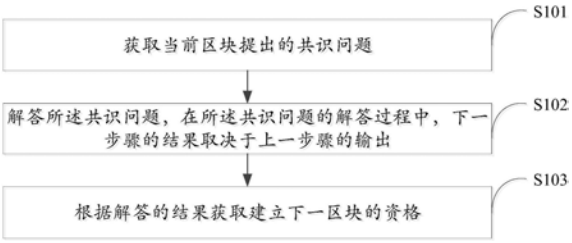
权利要求书1页 说明书4页 附图2页

(54)发明名称

区块链的共识方法和系统

(57)摘要

本发明涉及一种区块链的共识方法和系统，包括获取当前区块提出的共识问题，解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出，根据解答的结果获取建立下一区块的资格；该方法采用单线条算法进行共识问题的计算，抑制共识过程的并行处理方式，简化了共识过程，降低了区块链的运营成本。



CN 107743064 A

1.一种区块链的共识方法,其特征在于,包括:

获取当前区块提出的共识问题;

解答所述共识问题,在所述共识问题的解答过程中,下一步骤的结果取决于上一步骤的输出;

根据解答的结果获取建立下一区块的资格。

2.根据权利要求1所述的方法,其特征在于,解答所述共识问题的步骤具体为:

采用混沌迭代算法解决所述共识问题。

3.根据权利要求1所述的方法,其特征在于,所述获取当前区块提出的共识问题的步骤之前,还包括:

根据需求设定解答所述共识问题所需时长的期望值不低于预设时长。

4.根据权利要求1所述的方法,其特征在于,所述根据解答的结果获取建立下一区块的资格包括:

根据解答的结果选取最先解答的终端作为建立下一区块的对象。

5.根据权利要求1所述的方法,其特征在于,所述根据解答的结果获取建立下一区块的资格的步骤之后,还包括:

建立所述下一区块。

6.根据权利要求1所述的方法,其特征在于,所述获取当前区块提出的共识问题的步骤之前,还包括:

获取当前区块的哈希值,根据所述哈希值建立和所述当前区块的关联性。

7.一种区块链的共识系统,其特征在于,包括:

问题获取模块,用于获取当前区块提出的共识问题;

计算模块,解答所述共识问题,在所述共识问题的解答过程中,下一步骤的结果取决于上一步骤的输出;

资格获取模块,根据解答的结果获取建立下一区块的资格。

8.根据权利要求7所述的系统,其特征在于,所述计算模块具有用于,采用混沌迭代算法解决所述共识问题,在所述共识问题的解答过程中,下一步骤的结果取决于上一步骤的输出。

9.根据权利要求7所述的系统,其特征在于,还包括:

解答时长设定模块,用于根据需求设定解答所述共识问题所需时长的期望值不低于预设时长。

10.根据权利要求7所述的系统,其特征在于,所述资格获取模块具体用于,根据解答的结果选取最先解答的终端作为建立下一区块的对象;

所述系统还包括:

区块建立模块,用于在获取所述资格之后,建立所述下一区块。

关联性建立模块,用于获取当前区块的哈希值,根据所述哈希值建立和所述当前区块的关联性。

区块链的共识方法和系统

技术领域

[0001] 本发明涉及区块链技术领域，特别是涉及一种区块链的共识方法和系统。

背景技术

[0002] 区块链由各个相关联的区块组成，各个区块之间具备不可篡改、可追溯性等特征，区块链技术可以使彼此之间没有建立传统信任关系的经济主体达成合作，无需通过中央权威机构，它是建立信任的机器，具有去中心化、去信用化等诸多优势，受到了银行、金融、证券等行业的追捧。

[0003] 目前，对于公有区块链，世界上任何个体或者团体都可以发送交易，且交易能够获得该区块链的有效确认，任何人都可以参与其共识过程，即增加区块的过程。在这个过程中，个人或团体主要通过复杂的数学运算来实现共识，得到增加区块的所有权，这些复杂的运算可以并行处理，导致区块链的运营依赖于高性能的并行处理器，共识过程十分复杂，消耗了巨大的计算能量，提高了区块链的运营成本。

发明内容

[0004] 基于此，有必要提供一种区块链的共识方法和系统，抑制共识过程的并行处理方式，简化了共识过程，降低了区块链的运营成本。

[0005] 一方面，本发明提出一种区块链的共识方法，包括：

[0006] 获取当前区块提出的共识问题；

[0007] 解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出；

[0008] 根据解答的结果获取建立下一区块的资格。

[0009] 上述区块链的共识方法，包括获取当前区块提出的共识问题，解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出，根据解答的结果获取建立下一区块的资格；该方法采用单线条算法进行共识问题的计算，抑制共识过程的并行处理方式，简化了共识过程，降低了区块链的运营成本。

[0010] 在其中一个实施例中，解答所述共识问题的步骤具体为：

[0011] 采用混沌迭代算法解决所述共识问题。

[0012] 在其中一个实施例中，所述获取当前区块提出的共识问题的步骤之前，还包括：

[0013] 根据需求设定解答所述共识问题所需时长的期望值不低于预设时长。

[0014] 在其中一个实施例中，所述根据解答的结果获取建立下一区块的资格包括：

[0015] 根据解答的结果选取最先解答的终端作为建立下一区块的对象。

[0016] 在其中一个实施例中，所述根据解答的结果获取建立下一区块的资格的步骤之后，还包括：

[0017] 建立所述下一区块。

[0018] 在其中一个实施例中，所述获取当前区块提出的共识问题的步骤之前，还包括：

[0019] 获取当前区块的哈希值，根据所述哈希值建立和所述当前区块的关联性。

[0020] 另一方面，本发明还提出一种区块链的共识系统，包括：

[0021] 问题获取模块，用于获取当前区块提出的共识问题；

[0022] 计算模块，解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出；

[0023] 资格获取模块，根据解答的结果获取建立下一区块的资格。

[0024] 在其中一个实施例中，所述计算模块具有用于，采用混沌迭代算法解决所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出。

[0025] 在其中一个实施例中，还包括：

[0026] 解答时长设定模块，用于根据需求设定解答所述共识问题所需时长的期望值不低于预设时长。

[0027] 在其中一个实施例中，所述资格获取模块具体用于，根据解答的结果选取最先解答的终端作为建立下一区块的对象；

[0028] 所述系统还包括：

[0029] 区块建立模块，用于在获取所述资格之后，建立所述下一区块。

[0030] 关联性建立模块，用于获取当前区块的哈希值，根据所述哈希值建立和所述当前区块的关联性。

附图说明

[0031] 图1为一实施例中区块链的共识方法的方法流程图；

[0032] 图2为另一实施例中区块链的共识方法的方法流程图；

[0033] 图3为一实施例中区块链的共识系统的系统方框图；

[0034] 图4为另一实施例中区块链的共识系统的系统方框图。

具体实施方式

[0035] 参见图1，图1为一实施例中区块链的共识方法的方法流程图。

[0036] 在本实施例中，该区块链的共识方法包括如下步骤：

[0037] S101，获取当前区块提出的共识问题。

[0038] 区块链由多个区块组成，每个区块对应唯一的哈希值，区块与区块之间通过哈希值形成相互的关联性，该哈希值可以理解为区块的身份。

[0039] 在公有区块链中，任何个人或团体都可以参与共识过程，在区块链上建立新的区块。但是，在同一时间，只能选择一个对象来建立这个区块，一般的，由当前区块给出一个共识问题，参与者，即挖矿者，谁先解答这个共识问题，就可以获得建立下一区块的权利，即挖矿成功。

[0040] S102，解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出。

[0041] 在公有区块链中，由于参与者众多，挖矿竞争十分激烈，本实施例在共识问题的设置上，只能通过单线条算法对该共识问题进行计算，在计算的过程中，每一步的计算结果都取决于上一步的输出。

[0042] 该单线条算法不能通过并行方式进行计算，不需要通过昂贵的计算设备，如并行处理器、特有的挖矿芯片，或者多个FPGA(Field-Programmable GateArray，现场可编程门阵列)等来处理这个计算过程。将挖矿过程变得简单，减少了竞争者们在共识过程中为了挖矿成功而造成的资源消耗，如计算能量的巨大消耗、能源的消耗、硬件设备的消耗、生产这些硬件设备的过程中人力资源的消耗等，降低了区块链的运营成本，同时抑制了恶性竞争。

[0043] S103，根据解答的结果获取建立下一区块的资格。

[0044] 先解答共识问题的参与者可以获得建立下一区块的权限。

[0045] 上述区块链的共识方法，获取当前区块提出的共识问题，解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出，根据解答的结果获取建立下一区块的资格；该方法采用单线条算法进行共识问题的计算，在计算的过程中，每一步的计算结果都取决于上一步的输出，不能采用并行处理方式，简化了共识过程，降低了区块链的运营成本，同时抑制了恶性竞争。

[0046] 参见图2，图2为另一实施例中区块链的共识方法的方法流程图。

[0047] 在本实施例中，该区块链的共识方法包括如下步骤：

[0048] S201，获取当前区块的哈希值，根据所述哈希值建立和所述当前区块的关联性。

[0049] 在共识过程中，参与者在当前区块的基础上建立新的区块之前，需要先通过区块唯一的哈希值找到该当前区块，并建立和当前区块的关联性。

[0050] S202，获取当前区块提出的共识问题。

[0051] S203，根据混沌迭代算法解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出。

[0052] 该共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出。混沌迭代算法是一种单线条算法，根据混沌迭代算法解答该共识问题时，不能通过多个终端并行计算，抑制了在区块链共识过程中的恶性竞争，节约了人力资源。

[0053] S204，根据解答的结果选取最先解答的终端作为建立下一区块的对象。

[0054] 在公有区块链中，多个终端同时参与共识过程，一个终端可以视为一个参与者，每个终端在解答该共识问题的过程中彼此公开，信息共享，在共识过程结束后自动将最先解答出共识问题的终端选取为下建立下一区块的对象。

[0055] 此外，各终端还可以根据需求设定解答共识问题所需时长的期望值不低于预设时长。

[0056] S205，建立下一区块。

[0057] 上述区块链的共识方法，获取当前区块提出的共识问题，根据单线条的混沌迭代算法解答该共识问题，每一步的计算结果都取决于上一步的输出，不能采用并行处理方式，简化了共识过程，降低了区块链的运营成本，同时抑制了恶性竞争。

[0058] 此外，本申请实施例还提供一种计算机处理设备，该计算机处理设备包括存储器和处理器，所述存储器存储有实现上述区块链的共识方法的计算机程序，该处理器用于执行该计算机程序。

[0059] 由于解决共识问题的算法为单线条算法，计算过程简单，使得实现该方法的计算机程序可以在普通的计算机设备上运行，如X86处理器、X64处理器等，不限于这两种处理器。这些处理器比较常规，价格较并行处理器低廉，减少了区块链的运营成本。

[0060] 参见图3,图3为一实施例中区块链的共识系统的系统方框图。

[0061] 在本实施例中,一种区块链的共识系统,包括:

[0062] 问题获取模块10,用于获取当前区块提出的共识问题。

[0063] 计算模块11,用于解答所述共识问题,在所述共识问题的解答过程中,下一步骤的结果取决于上一步骤的输出。

[0064] 资格获取模块12,用于根据解答的结果获取建立下一区块的资格。

[0065] 参见图4,在其中一个实施例中,所述计算模块11具有用于,采用混沌迭代算法解决所述共识问题,在所述共识问题的解答过程中,下一步骤的结果取决于上一步骤的输出。

[0066] 在其中一个实施例中,该系统还包括:

[0067] 解答时长设定模块13,用于根据需求设定解答所述共识问题所需时长的期望值不低于预设时长。

[0068] 在其中一个实施例中,上述资格获取模块12具体用于,根据解答的结果选取最先解答的终端作为建立下一区块的对象。

[0069] 在其中一个实施例中,所述系统还包括:区块建立模块14,用于在获取所述资格之后,建立所述下一区块。

[0070] 在其中一个实施例中,所述系统还包括:关联性建立模块15,用于获取当前区块的哈希值,根据所述哈希值建立和所述当前区块的关联性。

[0071] 上述区块链的共识系统,获取当前区块提出的共识问题,根据单线条的混沌迭代算法解答该共识问题,每一步的计算结果都取决于上一步的输出,不能采用并行处理方式,简化了共识过程,降低了区块链的运营成本,同时抑制了恶性竞争。

[0072] 以上所述实施例的各技术特征可以进行任意的组合,为使描述简洁,未对上述实施例中的各个技术特征所有可能的组合都进行描述,然而,只要这些技术特征的组合不存在矛盾,都应当认为是本说明书记载的范围。

[0073] 以上所述实施例仅表达了本发明的几种实施方式,其描述较为具体和详细,但并不能因此而理解为对发明专利范围的限制。应当指出的是,对于本领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干变形和改进,这些都属于本发明的保护范围。因此,本发明专利的保护范围应以所附权利要求为准。

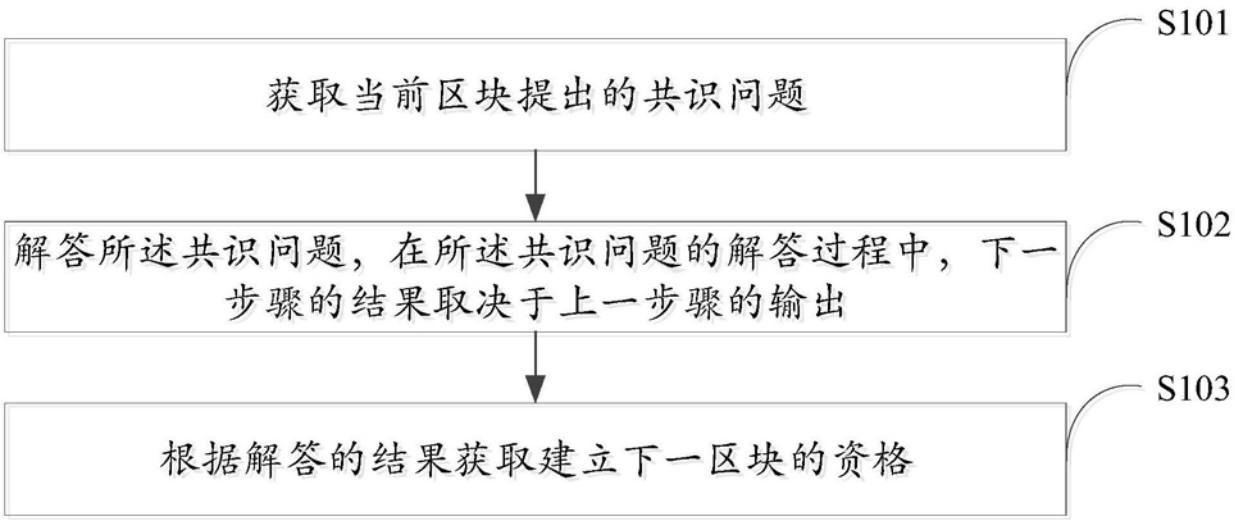

S101
获取当前区块提出的共识问题
S102
解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出
S103
根据解答的结果获取建立下一区块的资格

图1

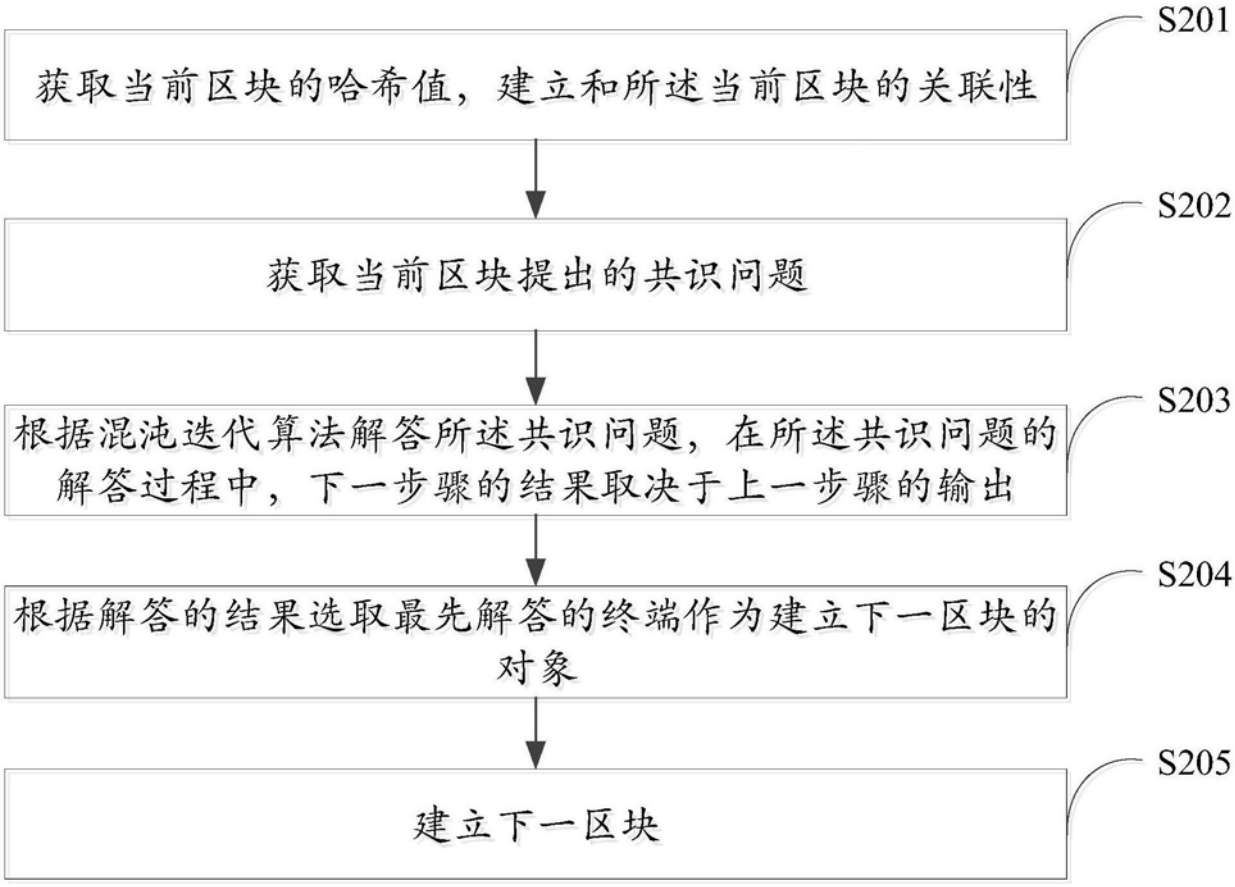

S201
获取当前区块的哈希值，建立和所述当前区块的关联性
S202
获取当前区块提出的共识问题
S203
根据混沌迭代算法解答所述共识问题，在所述共识问题的解答过程中，下一步骤的结果取决于上一步骤的输出
S204
根据解答的结果选取最先解答的终端作为建立下一区块的对象
S205
建立下一区块

图2

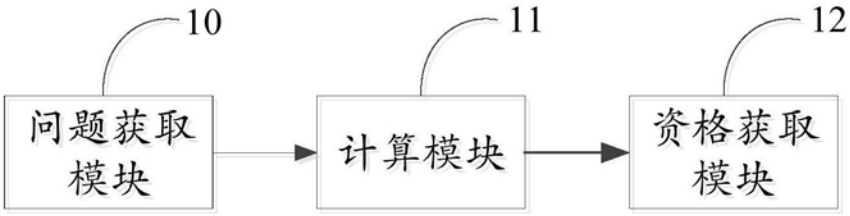

10
11
12
问题获取模块
计算模块
资格获取模块

图3

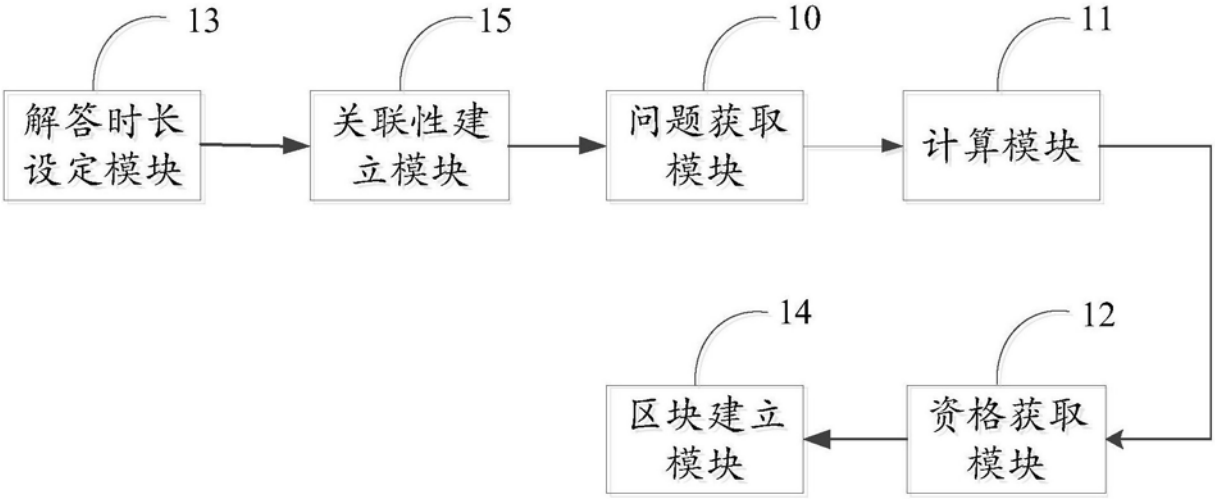

13
15
10
11
解答时长设定模块
关联性建立模块
问题获取模块
计算模块
14
12
区块建立模块
资格获取模块

图4