(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 111523896 A
(43)申请公布日 2020.08.11

(21)申请号 202010373105.7

(22)申请日 2020.05.06

(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 何玉斌 王志文 吴思进

(51)Int.Cl.
G06Q 20/38(2012.01)
G06F 16/27(2019.01)
G06F 16/2455(2019.01)
G06F 16/22(2019.01)

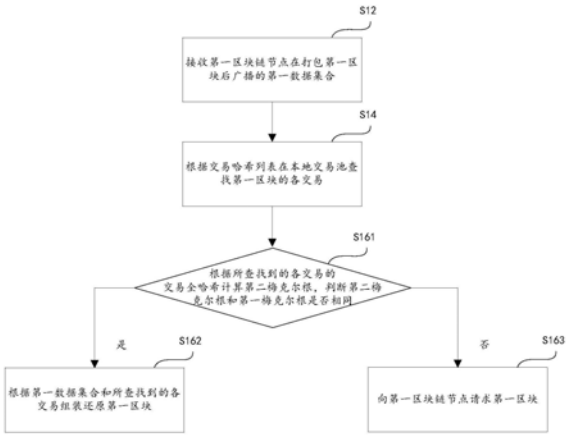
权利要求书1页 说明书6页 附图2页

(54)发明名称

防攻击方法、设备和存储介质

(57)摘要

本发明提供一种防攻击方法、设备和存储介质，该方法包括：接收第一区块链节点在打包第一区块后广播的第一数据集合；其中，第一数据集合包括第一区块的第一区块头信息和交易哈希列表，第一区块头信息包括第一梅克尔根，第一梅克尔根根据第一区块的各交易的交易全哈希计算生成，交易全哈希根据相应交易的交易内容和签名信息生成；根据交易哈希列表在本地交易池查找第一区块的各交易；根据所查找到的各交易的交易全哈希计算第二梅克尔根，在第二梅克尔根和第一梅克尔根相同时，根据第一数据集合和所查找到的各交易组装还原第一区块；在第二梅克尔根和第一梅克尔根不同时，向第一区块链节点请求第一区块。上述方法提高区块链稳定性。



CN 111523896 A

1.一种防攻击方法,其特征在于,所述方法适用于区块链节点,所述方法包括:

接收第一区块链节点在打包第一区块后广播的第一数据集合;其中,所述第一数据集合包括所述第一区块的第一区块头信息和交易哈希列表,所述第一区块头信息包括第一梅克尔根,所述第一梅克尔根根据所述第一区块的各交易的交易全哈希计算生成,所述交易全哈希根据相应交易的交易内容和签名信息生成;

根据所述交易哈希列表在本地交易池查找所述第一区块的各交易;

根据所查找到的各交易的交易全哈希计算第二梅克尔根,判断所述第二梅克尔根和所述第一梅克尔根是否相同:

是,则根据所述第一数据集合和所查找到的各交易组装还原所述第一区块;

否,则向所述第一区块链节点请求所述第一区块。

2.根据权利要求1所述的方法,其特征在于,所述向所述第一区块链节点请求所述第一区块包括:

向所述第一区块链节点请求所述第一区块;

验证所述第一区块的正确性,在验证通过时删除本地交易池中所述第一区块所包括的各交易。

3.一种防攻击方法,其特征在于,所述方法适用于区块链节点,所述方法包括:

打包第一区块并生成所述第一区块的第一数据集合;其中,所述第一数据集合包括所述第一区块的第一区块头信息和交易哈希列表,所述第一区块头信息包括第一梅克尔根,所述第一梅克尔根根据所述第一区块的各交易的交易全哈希计算生成,所述交易全哈希根据相应交易的交易内容和签名信息生成;

将所述第一数据集合广播给其它区块链节点,以供其它区块链节点:

根据所述交易哈希列表在本地交易池查找所述第一区块的各交易;

根据所查找到的各交易的交易全哈希计算第二梅克尔根,判断所述第二梅克尔根和所述第一梅克尔根是否相同:

是,则根据所述第一数据集合和所查找到的各交易组装还原所述第一区块;

否,则向当前节点请求所述第一区块。

4.根据权利要求3所述的方法,其特征在于,所述向当前节点请求所述第一区块包括:

向当前节点请求所述第一区块;

验证所述第一区块的正确性,在验证通过时删除本地交易池中所述第一区块所包括的各交易。

5.一种设备,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1-4中任一项所述的方法。

6.一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1-4中任一项所述的方法。

防攻击方法、设备和存储介质

技术领域

[0001] 本申请涉及区块链技术领域，具体涉及一种防攻击方法、设备和存储介质。

背景技术

[0002] 在申请人先前所提出的交易广播机制(具体可参考申请人所申请的各项交易广播或区块广播等专利文本)中，交易哈希由交易的交易内容生成，区块的区块头信息中的梅克尔根由区块的各交易的交易哈希计算生成，区块链节点在收到一笔交易，假设该交易内容为content(X)，区块链节点先判断本地是否已存有与content(X)相同的另一笔交易：若存有，则丢弃新接收的交易；若未存有，则将新接收的交易存入本地交易池。在申请人先前所提出的区块验证机制(具体可参考申请人所申请的各项区块生成、区块广播或区块验证等专利文本)中，生成区块的区块链节点将所生成的区块的数据集合(包括所生成的区块的区块头信息和交易哈希列表)发送给其它区块链节点；其它区块链节点在接收区块时，根据交易哈希列表在本地交易池查找所接收区块的各交易，根据所查找到的各交易的交易哈希计算梅克尔根，在判断所计算的梅克尔根与区块头信息中的梅克尔根相同时，再根据所接收的数据集合和所查找到的各交易组装还原第一区块，执行所还原的第一区块得到执行结果，在执行结果与区块头信息中的执行结果不一致时，区块链节点认为该问题(梅克尔根相同，执行结果不同)是版本不一致导致的，区块链节点停止运行并等待版本更新。

[0003] 假设区块链中有ABCD四个区块链节点，用户a为恶意用户，用户a用两个账户的私钥对同一笔交易内容进行签名生成两笔不同的交易tx1(sig_a1(content(M)))和tx2(sig_a2(content(M)))；假设A、B先收到tx1，C、D先收到tx2；A、B收到tx1后，再收到tx2时，由于tx1和tx2的交易内容相同，A、B不会将tx2存入本地交易池；同理，C、D不会将tx1存入本地交易池；假设A生成了包括tx1的区块block(N)，并将blockheader(N)和block(N)的交易哈希列表广播给B、C、D；由于交易哈希由交易的交易内容生成，因此A、B、C、D的梅克尔根均相同；在梅克尔根相同的情况下，B、C、D根据所查找到的交易组装还原block(N)；B根据hash(content(M))从本地查找到tx1，而C、D根据hash(content(M))从本地查找到tx2；因此，A、B执行block(N)所生成的第一执行结果相同，C、D执行block(N)所生成的第二执行结果相同，而第一执行结果与第二执行结果不同。C、D认为该问题是版本不一致导致的，C、D停止运行并等待版本更新。可见，在上述交易广播机制中，一笔交易可以让很多区块链节点无法正常工作，降低了区块链运行的稳定性。

发明内容

[0004] 鉴于现有技术中的上述缺陷或不足，期望提供一种提高区块链稳定性的防攻击方法、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防攻击方法，上述方法包括：

[0006] 接收第一区块链节点在打包第一区块后广播的第一数据集合；其中，第一数据集合包括第一区块的第一区块头信息和交易哈希列表，第一区块头信息包括第一梅克尔根，

第一梅克尔根根据第一区块的各交易的交易全哈希计算生成，交易全哈希根据相应交易的交易内容和签名信息生成；

[0007] 根据交易哈希列表在本地交易池查找第一区块的各交易；

[0008] 根据所查找到的各交易的交易全哈希计算第二梅克尔根，判断第二梅克尔根和第一梅克尔根是否相同：

[0009] 是，则根据第一数据集合和所查找到的各交易组装还原第一区块；

[0010] 否，则向第一区块链节点请求第一区块。

[0011] 第二方面，本发明提供一种适用于区块链节点的防攻击方法，上述方法包括：

[0012] 打包第一区块并生成第一区块的第一数据集合；其中，第一数据集合包括第一区块的第一区块头信息和交易哈希列表，第一区块头信息包括第一梅克尔根，第一梅克尔根根据第一区块的各交易的交易全哈希计算生成，交易全哈希根据相应交易的交易内容和签名信息生成；

[0013] 将第一数据集合广播给其它区块链节点，以供其它区块链节点：

[0014] 根据交易哈希列表在本地交易池查找第一区块的各交易；

[0015] 根据所查找到的各交易的交易全哈希计算第二梅克尔根，判断第二梅克尔根和第一梅克尔根是否相同：

[0016] 是，则根据第一数据集合和所查找到的各交易组装还原第一区块；

[0017] 否，则向当前节点请求第一区块。

[0018] 第三方面，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防攻击方法。

[0019] 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防攻击方法。

[0020] 本发明诸多实施例提供的防攻击方法、设备和存储介质通过接收第一区块链节点在打包第一区块后广播的第一数据集合；其中，第一数据集合包括第一区块的第一区块头信息和交易哈希列表，第一区块头信息包括第一梅克尔根，第一梅克尔根根据第一区块的各交易的交易全哈希计算生成，交易全哈希根据相应交易的交易内容和签名信息生成；根据交易哈希列表在本地交易池查找第一区块的各交易；根据所查找到的各交易的交易全哈希计算第二梅克尔根，在第二梅克尔根和第一梅克尔根相同时，根据第一数据集合和所查找到的各交易组装还原第一区块；在第二梅克尔根和第一梅克尔根不同时，向第一区块链节点请求第一区块的方法，提高区块链稳定性。

附图说明

[0021] 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：

[0022] 图1为本发明一实施例提供的一种防攻击方法的流程图。

[0023] 图2为本发明一实施例提供的另一种防攻击方法的流程图。

[0024] 图3为本发明一实施例提供的一种设备的结构示意图。

具体实施方式

[0025] 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。

[0026] 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。

[0027] 图1为本发明一实施例提供的一种防攻击方法的流程图。如图1所示，在本实施例中，本发明提供一种适用于区块链节点的防攻击方法，上述方法包括：

[0028] S12：接收第一区块链节点在打包第一区块后广播的第一数据集合；其中，第一数据集合包括第一区块的第一区块头信息和交易哈希列表，第一区块头信息包括第一梅克尔根，第一梅克尔根根据第一区块的各交易的交易全哈希计算生成，交易全哈希根据相应交易的交易内容和签名信息生成；

[0029] S14：根据交易哈希列表在本地交易池查找第一区块的各交易；

[0030] S161：根据所查找到的各交易的交易全哈希计算第二梅克尔根，判断第二梅克尔根和第一梅克尔根是否相同：

[0031] 是，则执行步骤S162：根据第一数据集合和所查找到的各交易组装还原第一区块；

[0032] 否，则执行步骤S163：向第一区块链节点请求第一区块。

[0033] 具体地，假设区块链中有ABCD四个区块链节点，用户a为恶意用户，用户a用两个账户的私钥对同一笔交易内容进行签名生成两笔不同的交易tx1(sig_a1(content(M)))和tx2(sig_a2(content(M)))；A、B先收到tx1，C、D先收到tx2；假设A生成了block(N)，block(N)包括tx1(sig_a1(content(M)))、tx3(sig_b(content(R)))、tx4(sig_c(content(S)))，A将blockheader(N)和block(N)的交易哈希列表广播给B、C、D；

[0034] 在申请人先前所提出的交易广播机制(具体可参考申请人所申请的各项交易广播或区块广播专利文本)中，交易哈希由交易的交易内容生成，区块的区块头信息中的梅克尔根由区块的各交易的交易哈希计算生成，区块链节点在收到一笔交易，假设该交易内容为content(X)，区块链节点先判断本地是否已存有与content(X)相同的另一笔交易：若存有，则丢弃新接收的交易；若未存有，则将新接收的交易存入本地交易池。在申请人先前所提出的区块验证机制(具体可参考申请人所申请的各项区块生成、区块广播或区块验证等专利文本)中，生成区块的区块链节点将所生成的区块的数据集合(包括所生成的区块的区块头信息和交易哈希列表)发送给其它区块链节点；其它区块链节点在接收区块时，根据交易哈希列表在本地交易池查找所接收区块的各交易，根据所查找到的各交易的交易哈希计算梅克尔根，在判断所计算的梅克尔根与区块头信息中的梅克尔根相同时，再根据所接收的数据集合和所查找到的各交易组装还原第一区块，执行所还原的第一区块得到执行结果，在执行结果与区块头信息中的执行结果不一致时，区块链节点认为该问题(梅克尔根相同，执行结果不同)是版本不一致导致的，区块链节点停止运行并等待版本更新。

[0035] A、B收到tx1后，再收到tx2时，由于tx1和tx2的交易内容相同，A、B不会将tx2存入本地交易池；同理，C、D不会将tx1存入本地交易池；A将blockheader(N)(包括梅克尔根(根据hash(content(M))、hash(content(R))、hash(content(S))生成)、交易哈希列表(hash(content(M))、hash(content(R))、hash(content(S)))广播给B、C、D；

[0036] B根据hash(content(M))从本地查找到tx1，而C、D根据hash(content(M))从本地查找到tx2；由于交易哈希由交易的交易内容生成，因此A、B、C、D的梅克尔根均相同；在梅克尔根相同的情况下，B、C、D根据查找到的交易组装还原block(N)，但是A、B执行block(N)所生成的第一执行结果相同(实际执行的是tx1、tx3、tx4)，C、D执行block(N)所生成的第二执行结果相同(实际执行的是tx2、tx3、tx4)，第一执行结果与第二执行结果不同。C、D认为该问题是版本不一致导致的，C、D停止运行并等待版本更新。可见，在上述交易广播机制中，一笔交易可以让很多区块链节点无法正常工作，降低了区块链运行的稳定性。

[0037] 针对上述场景所产生的问题，可以通过步骤S12至步骤S163解决；

[0038] A将tx1、tx3、tx4打包入block(N)，并生成block(N)的数据集合；block(N)的数据集合包括blockheader(N)(包括梅克尔根(根据hash(content(M)+sig_a1)、hash(content(R)+sig_b)、hash(content(S)+sig_c)生成)和交易哈希列表(hash(content(M))、hash(content(R))、hash(content(S)))；

[0039] B、C、D执行步骤S12，接收block(N)的数据集合；

[0040] B、C、D执行步骤S14，根据交易哈希列表在本地交易池查找第一区块的各交易；B在本地查找到tx1、tx3、tx4；C、D在本地查找到tx2、tx3、tx4；

[0041] B、C、D执行步骤S161：

[0042] B根据tx1、tx3、tx4的交易全哈希计算梅克尔根blockheader(N)_B(根据hash(content(M)+sig_a1)、hash(content(R)+sig_b)、hash(content(S)+sig_c)生成)，判断blockheader(N)_B和blockheader(N)相同，则执行步骤S162：根据block(N)的数据集合和tx1、tx3、tx4组装还原block(N)。

[0043] C根据tx2、tx3、tx4的交易全哈希计算梅克尔根blockheader(N)_C(根据hash(content(M)+sig_a2)、hash(content(R)+sig_b)、hash(content(S)+sig_c)生成)，判断blockheader(N)_C和blockheader(N)不同，则执行步骤S163：向A请求block(N)。

[0044] D根据tx2、tx3、tx4的交易全哈希计算梅克尔根blockheader(N)_D(根据hash(content(M)+sig_a2)、hash(content(R)+sig_b)、hash(content(S)+sig_c)生成)，判断blockheader(N)_D和blockheader(N)不同，则执行步骤S163：向A请求block(N)。

[0045] 在上述实施例中，C、D不会停止运行，增加了区块链运行的稳定性。

[0046] 优选地，向第一区块链节点请求第一区块包括：

[0047] 向第一区块链节点请求第一区块；

[0048] 验证第一区块的正确性，在验证通过时删除本地交易池中第一区块所包括的各交易。

[0049] 图2为本发明一实施例提供的另一种防攻击方法的流程图。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防攻击方法，上述方法包括：

[0050] S22：打包第一区块并生成第一区块的第一数据集合；其中，第一数据集合包括第一区块的第一区块头信息和交易哈希列表，第一区块头信息包括第一梅克尔根，第一梅克尔根根据第一区块的各交易的交易全哈希计算生成，交易全哈希根据相应交易的交易内容和签名信息生成；

[0051] S24：将第一数据集合广播给其它区块链节点，以供其它区块链节点：

[0052] 根据交易哈希列表在本地交易池查找第一区块的各交易；

[0053] 根据所查找到的各交易的交易全哈希计算第二梅克尔根，判断第二梅克尔根和第一梅克尔根是否相同：

[0054] 是，则根据第一数据集合和所查找到的各交易组装还原第一区块；

[0055] 否，则向当前节点请求第一区块。

[0056] 上述实施例的防攻击原理可参考图1所示的方法，此处不再赘述。

[0057] 优选地，向第一区块链节点请求第一区块包括：

[0058] 向第一区块链节点请求第一区块；

[0059] 验证第一区块的正确性，在验证通过时删除本地交易池中第一区块所包括的各交易。

[0060] 图3为本发明一实施例提供的一种设备的结构示意图。

[0061] 如图3所示，作为另一方面，本申请还提供了一种设备300，包括一个或多个中央处理单元(CPU)301，其可以根据存储在只读存储器(ROM)302中的程序或者从存储部分308加载到随机访问存储器(RAM)303中的程序而执行各种适当的动作和处理。在RAM303中，还存储有设备300操作所需的各种程序和数据。CPU301、ROM302以及RAM303通过总线304彼此相连。输入/输出(I/O)接口305也连接至总线304。

[0062] 以下部件连接至I/O接口305：包括键盘、鼠标等的输入部分306；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307；包括硬盘等的存储部分308；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309。通信部分309经由诸如因特网的网络执行通信处理。驱动器310也根据需要连接至I/O接口305。可拆卸介质311，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310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308。

[0063] 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309从网络上被下载和安装，和/或从可拆卸介质311被安装。

[0064] 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。

[0065] 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。

[0066] 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。

[0067] 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。

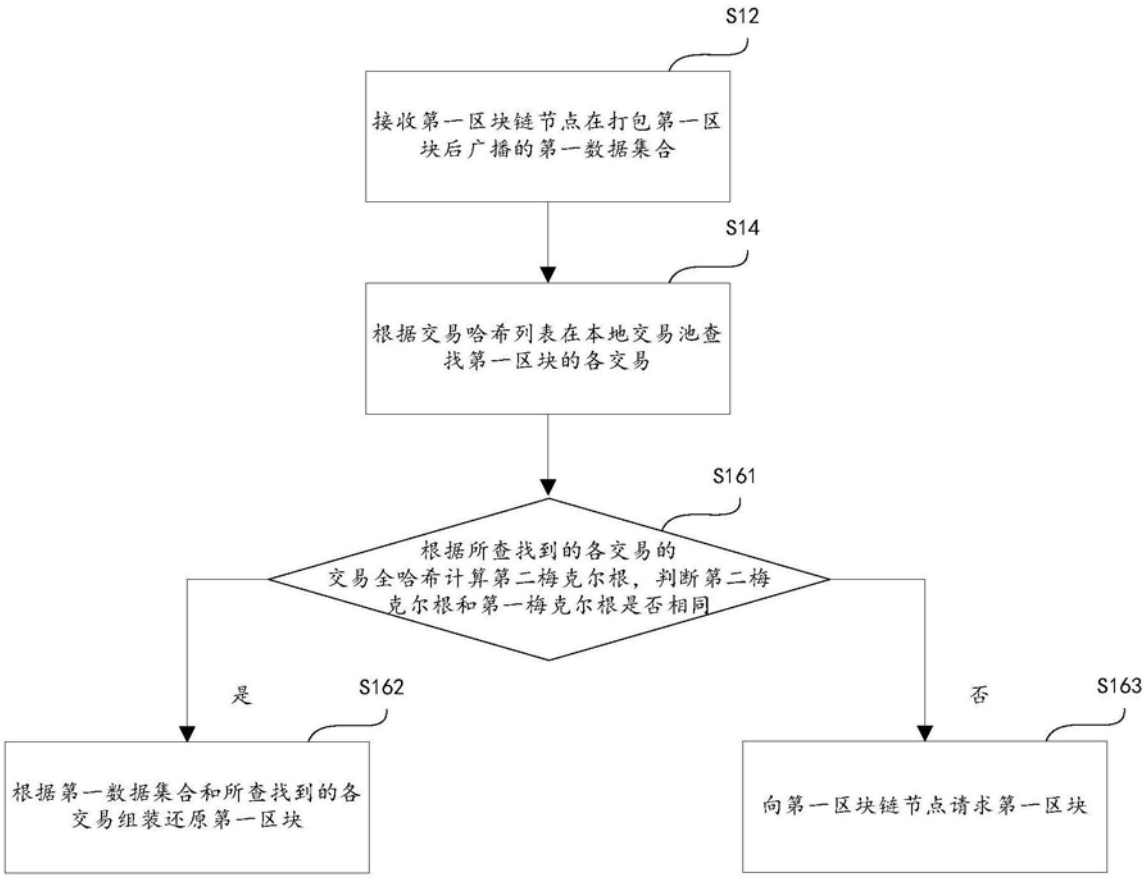

S12
接收第一区块链节点在打包第一区块后广播的第一数据集合
S14
根据交易哈希列表在本地交易池查找第一区块的各交易
S161
根据所查找到的各交易的交易全哈希计算第二梅克尔根，判断第二梅克尔根和第一梅克尔根是否相同
是
S162
根据第一数据集合和所查找到的各交易组装还原第一区块
否
S163
向第一区块链节点请求第一区块

图1

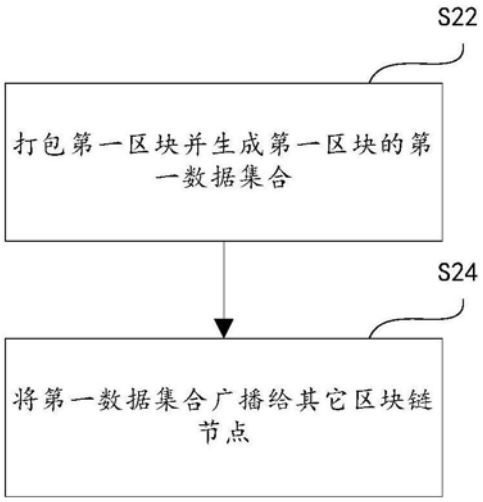

S22
打包第一区块并生成第一区块的第一数据集合
S24
将第一数据集合广播给其它区块链节点

图2

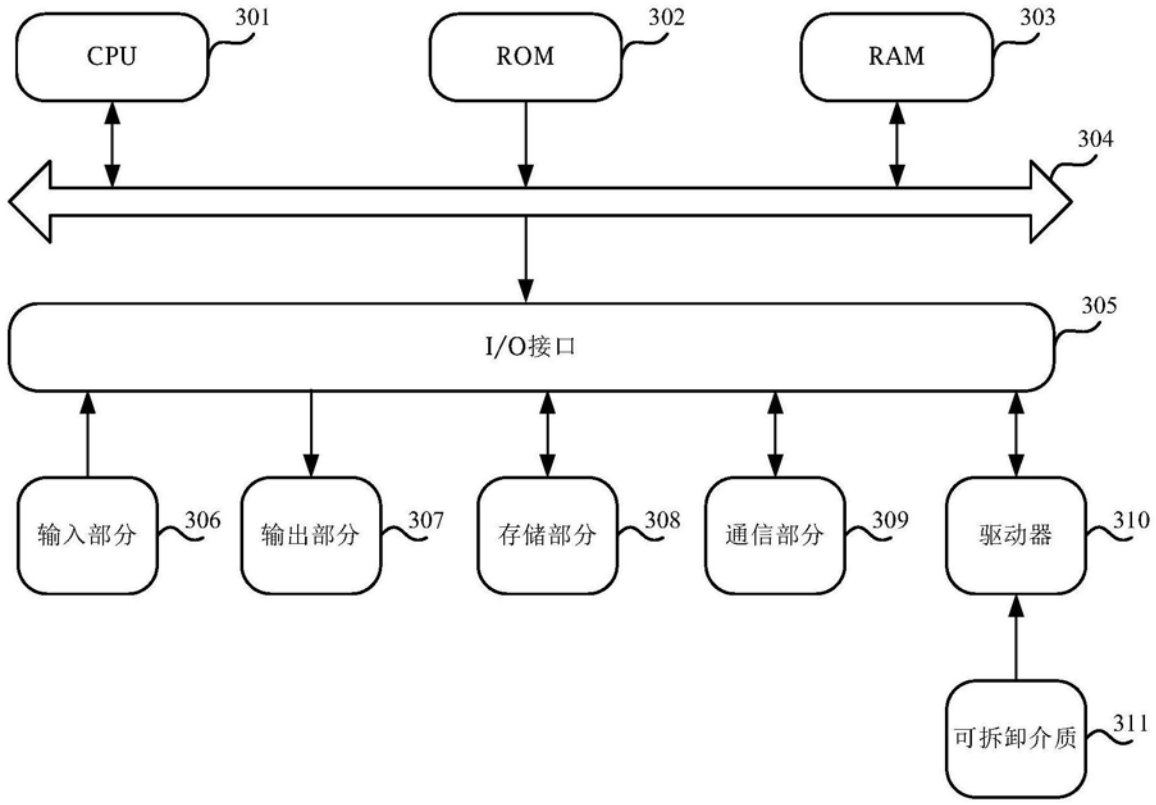

CPU
301
ROM
302
RAM
303
304
I/O接口
305
输入部分
306
输出部分
307
存储部分
308
通信部分
309
驱动器
310
可拆卸介质
311

图3