(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 106603698 A
(43)申请公布日 2017.04.26

(21)申请号 201611238337.1

(22)申请日 2016.12.28

(71)申请人 北京果仁宝科技有限公司
地址 100088 北京市海淀区太月园1号楼3层303室

(72)发明人 李海 唐剑 崔萌 徐伟 孙江涛

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 杨泽 刘芳

(51)Int.Cl.
H04L 29/08(2006.01)
G06Q 40/00(2012.01)

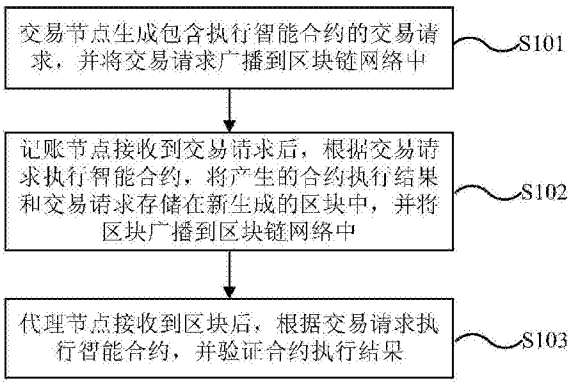
权利要求书1页 说明书6页 附图3页

(54)发明名称

基于DPOS的区块链共识方法和节点

(57)摘要

本发明提供一种基于DPOS的区块链共识方法和节点，其中，该方法包括：交易节点生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中；记账节点接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中；代理节点接收到区块后，根据交易请求执行智能合约，并验证合约执行结果。本发明提供的技术方案不需要普通节点验证合约执行结果，能够有效的提高整个网络的计算能力。



CN 106603698 A

1.一种基于股份授权证明DPOS的区块链共识方法，其特征在于，包括：

交易节点生成包含执行智能合约的交易请求，并将所述交易请求广播到区块链网络中；

记账节点接收到所述交易请求后，根据所述交易请求执行所述智能合约，将产生的合约执行结果和所述交易请求存储在新生成的区块中，并将所述区块广播到所述区块链网络中；

代理节点接收到所述区块后，根据所述交易请求执行所述智能合约，并验证所述合约执行结果。

2.根据权利要求1所述的方法，其特征在于，所述代理节点接收到所述区块数据后，根据所述交易请求执行所述智能合约，并验证所述合约执行结果，包括：

所述代理节点根据所述交易请求执行所述智能合约，判断产生的合约执行结果与所述区块中的合约执行结果是否一致；

若是，则将所述区块存储在区块链中；

若否，则删除所述区块。

3.根据权利要求1所述的方法，其特征在于，所述方法还包括：

普通节点接收到所述区块后，将所述区块存储在区块链中。

4.根据权利要求1-3任一项所述的方法，其特征在于，所述交易请求包括：智能合约标识ID和交易参数。

5.一种节点，其特征在于，包括：

请求生成模块，用于生成包含执行智能合约的交易请求，并将所述交易请求广播到区块链网络中；

记账模块，用于若所述节点为记账节点，则在接收到所述交易请求后，根据所述交易请求执行所述智能合约，将产生的合约执行结果和所述交易请求存储在新生成的区块中，并将所述区块广播到所述区块链网络中；

处理模块，用于若所述节点为代理节点，则在接收到所述区块后，根据所述交易请求执行所述智能合约，并验证所述合约执行结果。

6.根据权利要求5所述的节点，其特征在于，所述处理模块具体用于：

根据所述交易请求执行所述智能合约，判断产生的合约执行结果与所述区块中的合约执行结果是否一致；

若是，则将所述区块存储在区块链中；

若否，则删除所述区块。

7.根据权利要求5所述的节点，其特征在于，所述处理模块还用于：若所述节点为普通节点，则在接收到所述区块后，将所述区块存储在区块链中。

8.根据权利要求5-7任一项所述的节点，其特征在于，所述交易请求包括：智能合约标识ID和交易参数。

基于DPOS的区块链共识方法和节点

技术领域

[0001] 本发明涉及互联网技术领域，尤其涉及一种基于DPOS的区块链共识方法和节点。

背景技术

[0002] 区块链(Blockchain)是随着比特币等数字加密货币的日益普及而逐渐兴起的一种全新的去中心的分布式记账系统。系统中的节点无需互相信任，各节点通过统一的共识机制共同维护一份账本，每个节点都有一份完整的数据记录。区块链中各块(block)的交易通过密码学算法连接在一起，使得整个账本公开透明、可追踪、不可篡改。

[0003] 智能合约是区块链的一个重要特征，其可以使得区块链更加智能化。目前区块链主要有四大类共识机制：工作量证明(Proof Of Work，POW)机制、权益证明(Proof of Stake，POS)机制、股份授权证明(Delegate Proof of Stake，DPOS)机制和验证池(Pool)机制。其中，基于POW机制的智能合约共识技术较为成熟，其共识过程为：触发交易的节点向区块链网络广播交易请求后，网络中的所有节点竞争获得创建新区块的权利，竞争成功的节点执行智能合约后向全网广播生成的新区块，然后全网所有节点验证该新区块的正确性。

[0004] 上述这种基于POW机制的智能合约共识方法完全去中心化，节点自由进出，但是需要区块链网络中的所有节点验证新区块的正确性，占用了全网大部分的计算能力，从而降低了整个网络的计算能力。

发明内容

[0005] 本发明提供一种基于DPOS的区块链共识方法和节点，用于提高区块链网络的计算能力。

[0006] 一方面。本发明提供一种基于DPOS的区块链共识方法，包括：

[0007] 交易节点生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中；

[0008] 记账节点接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中；

[0009] 代理节点接收到区块后，根据交易请求执行智能合约，并验证合约执行结果。

[0010] 在本发明的一实施例中，代理节点接收到区块数据后，根据交易请求执行智能合约，并验证合约执行结果，具体包括：

[0011] 代理节点根据交易请求执行智能合约，判断产生的合约执行结果与区块中的合约执行结果是否一致；

[0012] 若是，则将区块存储在区块链中；

[0013] 若否，则删除区块。

[0014] 在本发明的一实施例中，该方法还包括：

[0015] 普通节点接收到区块后，将区块存储在区块链中。

[0016] 在本发明的一实施例中，交易请求包括：智能合约标识ID和交易参数。

[0017] 另一方面，本发明还提供一种节点，包括：

[0018] 请求生成模块，用于生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中；

[0019] 记账模块，用于若节点为记账节点，则在接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中；

[0020] 处理模块，用于若节点为代理节点，则在接收到区块后，根据交易请求执行智能合约，并验证合约执行结果。

[0021] 在本发明的一实施例中，处理模块具体用于：

[0022] 根据交易请求执行智能合约，判断产生的合约执行结果与区块中的合约执行结果是否一致；

[0023] 若是，则将区块存储在区块链中；

[0024] 若否，则删除区块。

[0025] 在本发明的一实施例中，处理模块还用于：若节点为普通节点，则在接收到区块后，将区块存储在区块链中。

[0026] 在本发明的一实施例中，交易请求包括：智能合约标识ID和交易参数。

[0027] 本发明实施例提供的基于DPOS的区块链共识方法和节点，交易节点将生成的包含执行智能合约的交易请求广播到区块链网络中后，记账节点根据接收到的交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中，然后由代理节点根据接收到的交易请求执行智能合约，验证合约执行结果，就可以使得正确的智能合约交易结果能被承认，错误的结果被丢弃，该方法不需要普通节点验证合约执行结果，从而有效的提高了整个网络的计算能力。

附图说明

[0028] 图1为本发明提供的基于DPOS的区块链共识方法实施例一的流程示意图；

[0029] 图2-图4为本发明提供的基于DPOS的区块链共识方法的一种应用示例图；

[0030] 图5为本发明提供的基于DPOS的区块链共识方法实施例二的流程示意图；

[0031] 图6为本发明提供的节点的结构示意图。

具体实施方式

[0032] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0033] 本发明实施例涉及的方法可以适用于区块链网络，所述区块链网络本质上是一个去中心化的分布式账本数据库，区块链本身是一串使用密码学技术相关联所产生的数据区块，每个区块中包含了多次区块链网络交易有效确认的信息。区块链网络是基于对等网络(Peer to Peer，P2P)而构建的，在P2P网络中，各节点之间可以互相直接通信，一个节点所产生的数据可以同时向该网络中的其它多个节点发送广播，也可以向该网络中其他任意节

点查询和获取数据。其中，该节点特指参与到所述区块链网络中进行资产交易和数据交换的节点，每个节点是一组物理网络、计算机、数据库等的组合。

[0034] 区块链共识机制中的DPOS机制，类似于董事会投票，由股份持有人通过投票选出受托人(即代理节点)，由受托人按照特定的顺序进行区块的生成。在DPOS系统中，各节点(包括代理节点和普通节点)选取受托人产生的区块构成的不同分支中最长的一支作为被认可的区块链。

[0035] 本发明实施例提供的方法，旨在解决现有技术中基于POW机制的智能合约共识方式，需要区块链网络中的所有节点验证新区块的正确性，占用了全网大部分的计算能力，降低了整个网络的计算能力的技术问题。

[0036] 下面以具体地实施例对本发明的技术方案进行详细说明。下面这几个具体的实施例可以相互结合，对于相同或相似的概念或过程可能在某些实施例不再赘述。

[0037] 图1为本发明提供的基于DPOS的区块链共识方法实施例一的流程示意图，如图1所示，本实施例提供的方法包括以下步骤：

[0038] S101、交易节点生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中。

[0039] 其中，智能合约是一套以数字形式定义和实现的契约，表现为一段可运行的计算机代码，这些代码能够实现交易过程，例如：资产的发行、申购、转让、赎回等。当一个预先编好的合约的某一条件被触发时，就自动在区块链网络中执行合约相应的合同条款，而不需人为干预。

[0040] 本实施例中，所有代理节点中都保存有一个或多个智能合约，且所有代理节点上保存的智能合约的个数及种类是相同的，且对于每一种智能合约，都具有唯一的标识ID。

[0041] 具体的，在区块链网络中任意一个节点都可以触发交易的过程，即上述交易节点可以是区块链网络中的任意一个节点。触发交易的交易节点会生成交易请求，并在整个区块链网络中广播该交易请求，以使其他节点都可以接收到该交易请求。其中，交易节点生成的交易请求中可以包括：智能合约ID和交易参数。当然，该交易请求中还可以包括其他参数，此处不做特别限定。

[0042] S102、记账节点接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中。

[0043] 具体的，在DPOS区块链网络中，由股份持有人通过投票选出的受托人对应的节点为代理节点，其他非代理节点即为普通节点。任意一个代理节点都可以作为记账节点使用，该记账节点用于进行交易确认及生成区块数据。同一时刻，区块链网络中仅有一个记账节点。具体的记账节点是基于预先设置的记账节点的确认逻辑及机制确定的。

[0044] 本发明实施例中，区块链网络中的所有节点都可以接收到交易节点广播的交易请求，其中，记账节点接收到交易请求后，取出交易请求中的智能合约ID和交易参数，执行对应的智能合约，然后将原始的交易请求和合约执行结果一同存储到新生成的区块中，然后在全网广播该区块数据，以使其他节点可以接收到该区块数据。

[0045] S103、代理节点接收到区块后，根据交易请求执行智能合约，并验证合约执行结果。

[0046] 具体的，代理节点接收到区块后，取出交易请求和合约执行结果，根据交易请求执

行智能合约，将产生的结果与区块中的合约执行结果对比，验证合约执行结果的正确性，若正确则接受该区块，否则丢弃该区块。

[0047] 图2-图4为本发明提供的基于DPOS的区块链共识方法的一种应用示例图，其主要体现代理节点作弊被否决的过程。

[0048] 如图2所示，代理节点1在生成区块时作弊，打包不正确的结果，将生成的错误块(Wrong Block)广播到网络中，代理节点2和代理节点3验证不正确，丢弃该区块，普通节点接受错误块。

[0049] 如图3所示，由于错误块被丢弃，代理节点2基于Block2生成正确的区块Block3广播到网络中，普通节点接受Block2，代理节点3验证通过后也接受。此时，普通节点的区块链生成两个分支Wrong Block和Block3。

[0050] 如图4所示，代理节点3生成正确的区块Block4广播到网络中，普通节点接受该区块。在DPOS系统中，各节点选取代理节点生成的区块构成的不同分支中最长的一支作为被认可的区块链。此时，普通节点中Block3分支较长，选择Block3分支为正确分支，错误块中的数据失效。

[0051] 结合上述代理节点作弊被否决的过程，本实施例提供的共识方法，由代理节点执行智能合约来验证合约执行结果的正确性，再基于DPOS区块链网络根据分支长度来选择链的共识机制，能够保证普通节点认可被大多数代理认可的结果，使得正确的智能合约交易结果能被承认，而错误的结果被丢弃。该方法只需代理节点执行智能合约验证合约执行结果，而不需要普通节点验证合约执行结果，从而大幅的解放了整个网络的计算能力。同时，相对于现有的DPOS区块链共识方法，本实施例提供的共识方法采用智能合约方式，有效的提高了交易速度，且用户可以将自己编写的代码提交到区块链系统中，从而能够拓展系统的交易类型。

[0052] 本实施例提供的基于DPOS的区块链共识方法，交易节点将生成的包含执行智能合约的交易请求广播到区块链网络中后，记账节点根据接收到的交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中，然后由代理节点根据接收到的交易请求执行智能合约，验证合约执行结果，就可以使得正确的智能合约交易结果能被承认，错误的结果被丢弃，该方法不需要普通节点验证合约执行结果，从而有效的提高了整个网络的计算能力。

[0053] 图5为本发明提供的基于DPOS的区块链共识方法实施例二的流程示意图，本实施例是上述图1所示实施例中步骤S103的一种具体的实施方式。如图5所示，在上述图1所示实施例的基础上，本实施例中，步骤S103代理节点接收到区块后，根据交易请求执行智能合约，并验证合约执行结果具体包括如下步骤：

[0054] S201、代理节点根据交易请求执行智能合约，判断产生的合约执行结果与区块中的合约执行结果是否一致；若是，则执行步骤S202，否则执行步骤S203。

[0055] 具体的，代理节点接收到区块后，取出交易请求和合约执行结果，根据交易请求执行智能合约，判断产生的合约执行结果与区块中的合约执行结果是否一致，以验证合约执行结果正确与否。

[0056] S202、将区块存储在区块链中。

[0057] 若代理节点判断产生的合约执行结果与区块中的合约执行结果一致，则认为该区

块正确，接受该区块，将该区块存储在区块链中

[0058] S203、删除区块。

[0059] 若代理节点判断产生的合约执行结果与区块中的合约执行结果不一致，则认为该区块不正确，此时丢弃该区块。

[0060] 可选的，本实施例提供的方法还可以包括：

[0061] S104、普通节点接收到区块后，将区块存储在区块链中。

[0062] 本实施例中，普通节点不验证合约执行结果的正确性，普通节点接收到区块后，直接将区块存储在区块链中，在后续的交易过程中，基于DPOS区块链网络根据分支长度来选择链的共识机制，普通节点会认可被大多数代理认可的结果，删除错误的区块分支。

[0063] 需要说明的是，步骤S104与步骤S103之间没有严格的时序关系，步骤S104可以在步骤S103之前执行，也可以在步骤S103之后执行，还可以与步骤S103同时执行，本实施例不做特别限定。

[0064] 图6为本发明提供的节点的结构示意图，该节点应用于区块链网络，如图6所示，本实施例提供的节点100包括：请求生成模块10、记账模块20和处理模块30。其中：

[0065] 请求生成模块10，用于生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中；

[0066] 记账模块20，用于若节点为记账节点，则在接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中；

[0067] 处理模块30，用于若节点为代理节点，则在接收到区块后，根据交易请求执行智能合约，并验证合约执行结果。

[0068] 作为本发明实施例一种可选的实施方式，处理模块30具体用于：

[0069] 根据交易请求执行智能合约，判断产生的合约执行结果与区块中的合约执行结果是否一致；

[0070] 若是，则将区块存储在区块链中；

[0071] 若否，则删除区块。

[0072] 在本发明的一实施例中，处理模块30还用于：若节点为普通节点，则在接收到区块后，将区块存储在区块链中。

[0073] 可选的，交易请求包括：智能合约标识ID和交易参数。

[0074] 本实施例提供的节点装置可以执行上述方法实施例，其实现原理和技术效果类似，此处不再赘述。

[0075] 本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0076] 最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术

方案的范围。

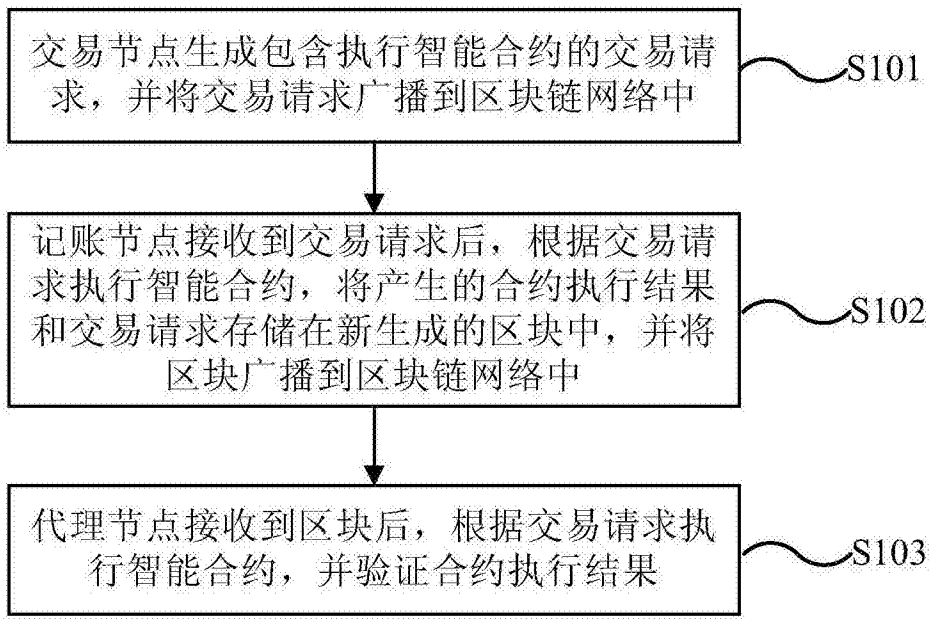

交易节点生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中
S101
记账节点接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中
S102
代理节点接收到区块后，根据交易请求执行智能合约，并验证合约执行结果
S103

图1

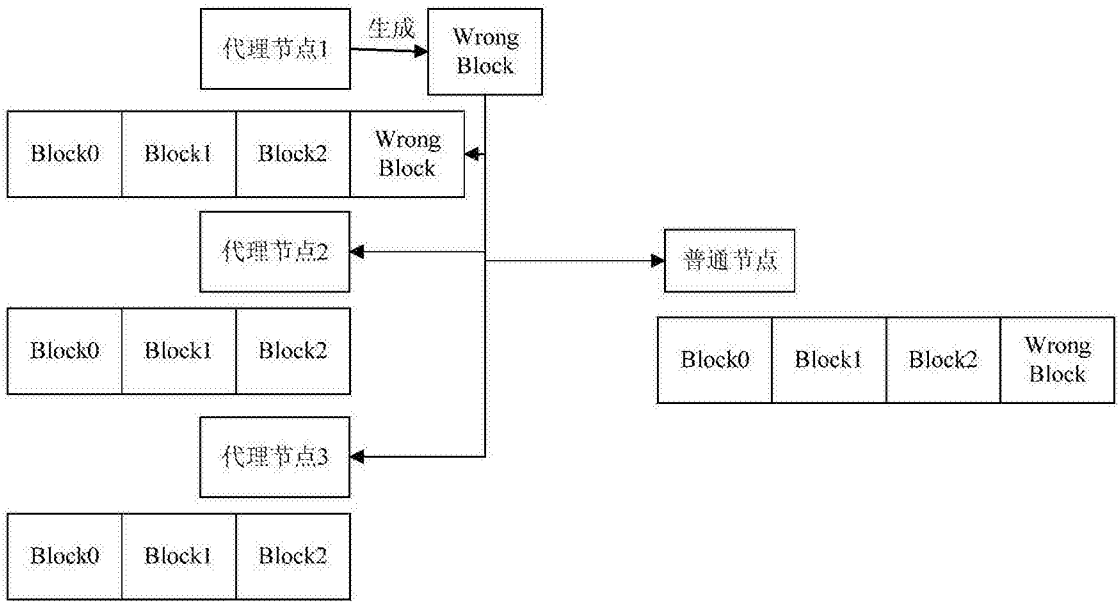

代理节点1
生成
Wrong Block
Block0
Block1
Block2
Wrong Block
代理节点2
普通节点
Block0
Block1
Block2
Wrong Block
Block0
Block1
Block2
代理节点3
Block0
Block1
Block2

图2

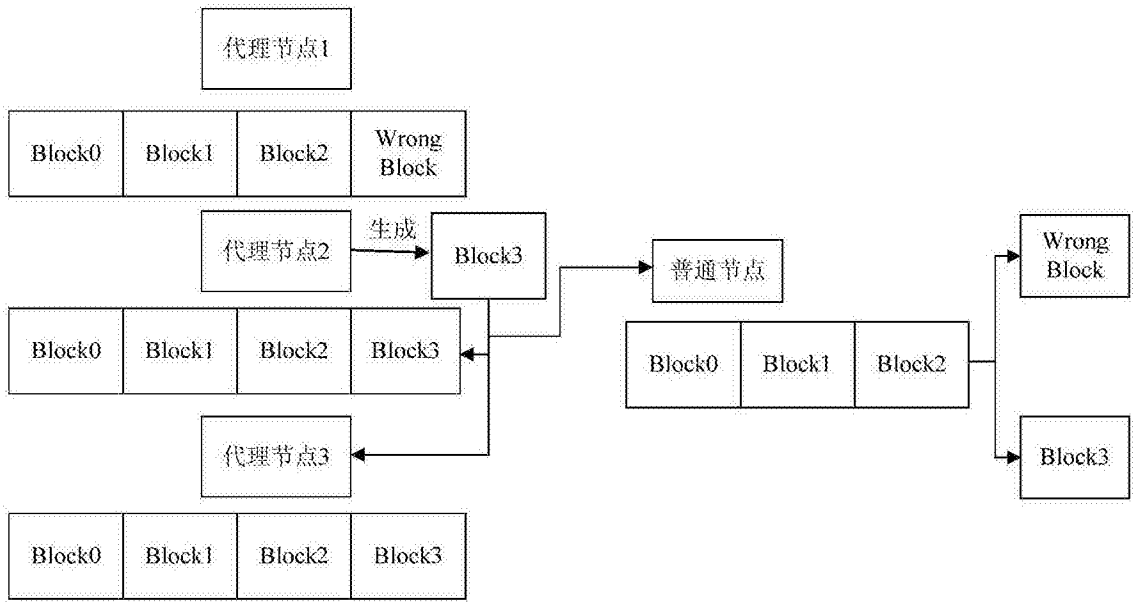

代理节点1
Block0
Block1
Block2
Wrong Block
代理节点2
生成
Block3
普通节点
Wrong Block
Block0
Block1
Block2
Block3
代理节点3
Block0
Block1
Block2
Block3

图3

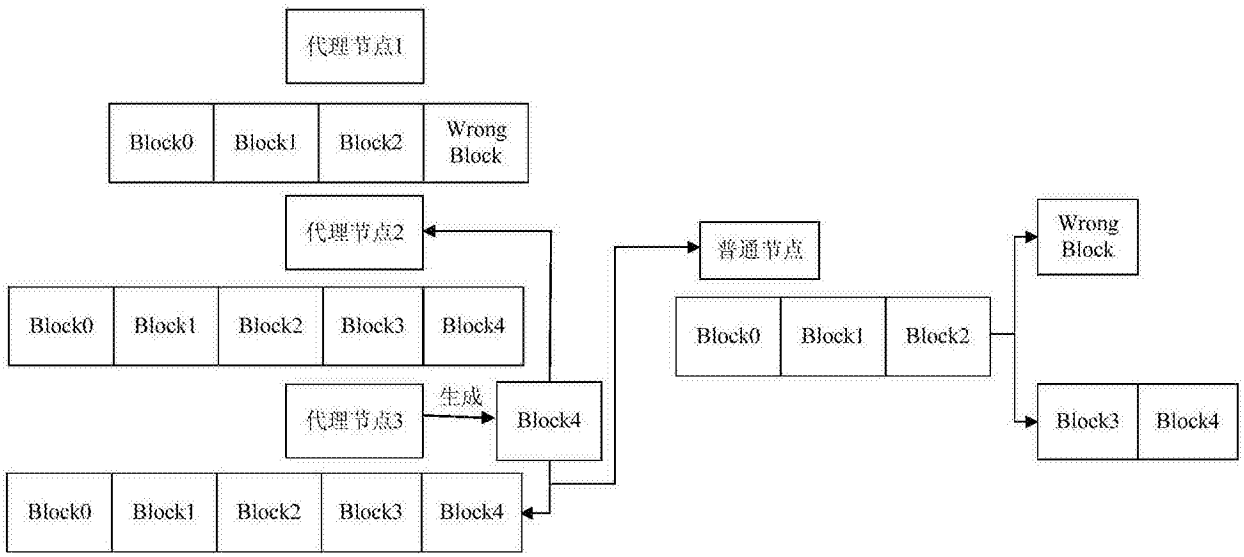

代理节点1
Block0
Block1
Block2
Wrong Block
代理节点2
普通节点
Wrong Block
Block0
Block1
Block2
Block0
Block1
Block2
Block3
Block4
代理节点3
生成
Block4
Block3
Block4
Block0
Block1
Block2
Block3
Block4

图4

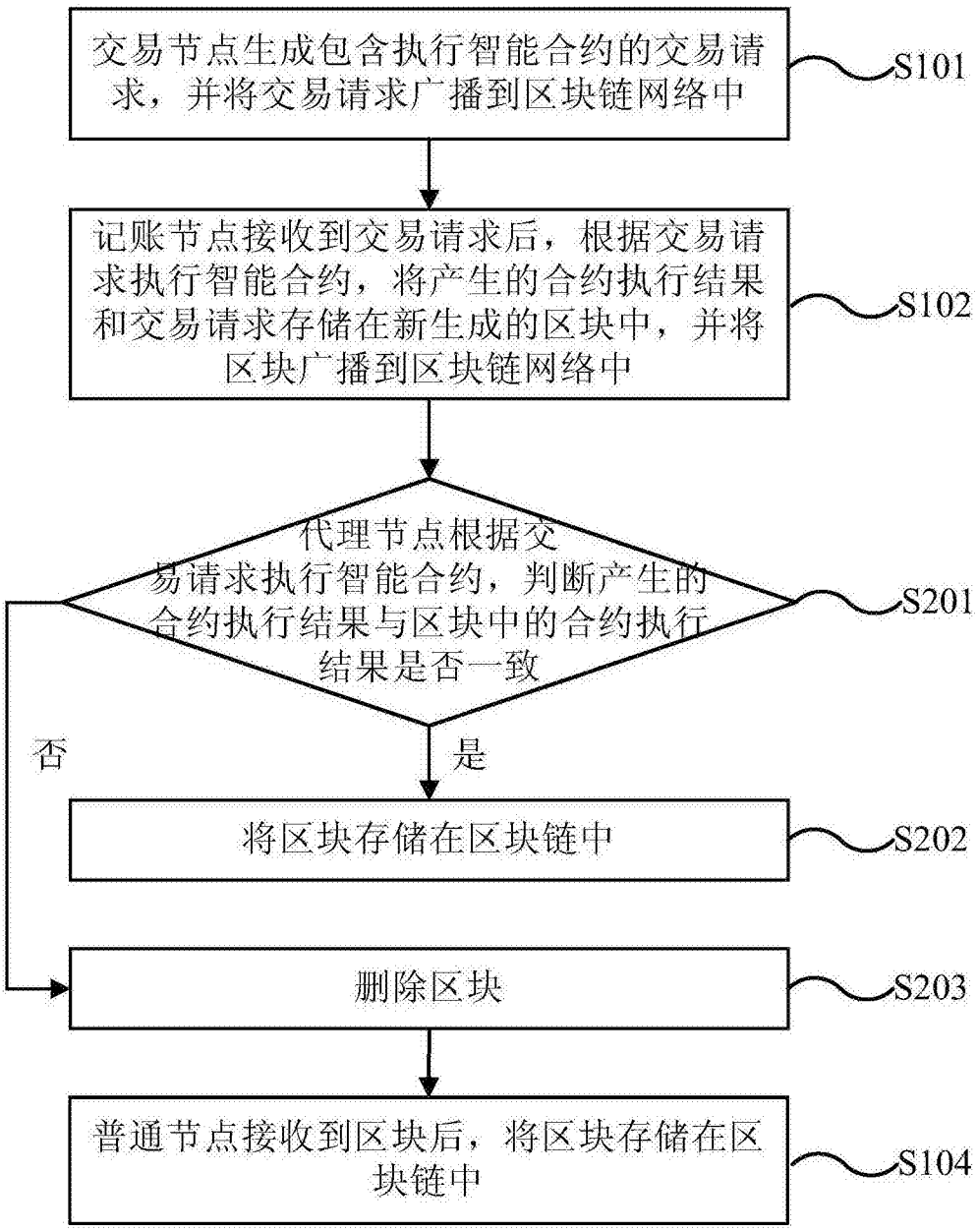

交易节点生成包含执行智能合约的交易请求，并将交易请求广播到区块链网络中
S101
记账节点接收到交易请求后，根据交易请求执行智能合约，将产生的合约执行结果和交易请求存储在新生成的区块中，并将区块广播到区块链网络中
S102
代理节点根据交易请求执行智能合约，判断产生的合约执行结果与区块中的合约执行结果是否一致
S201
否
是
将区块存储在区块链中
S202
删除区块
S203
普通节点接收到区块后，将区块存储在区块链中
S104

图5

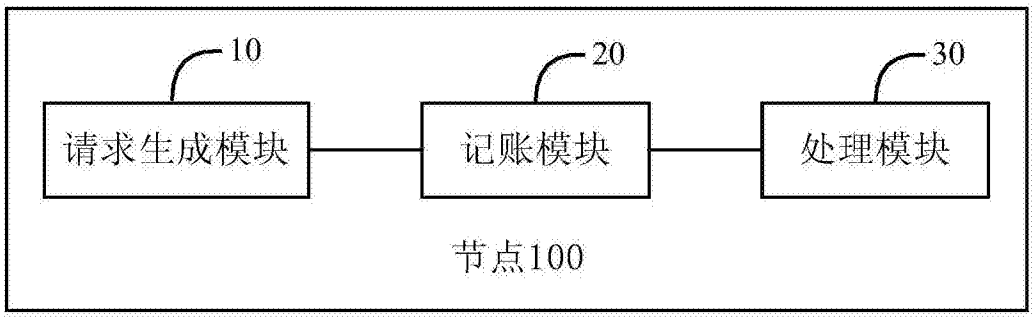

10
20
30
请求生成模块
记账模块
处理模块
节点100

图6