(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 106656974 A
(43)申请公布日 2017.05.10

(21)申请号 201610901226.8

(22)申请日 2016.10.17

(71)申请人 江苏通付盾科技有限公司
地址 江苏省苏州市工业园区新平街388号腾飞创新园6号楼5楼

(72)发明人 汪德嘉 郭宇 王少凡

(74)专利代理机构 北京市浩天知识产权代理事务所(普通合伙) 11276
代理人 宋菲 刘云贵

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)
G06Q 20/40(2012.01)

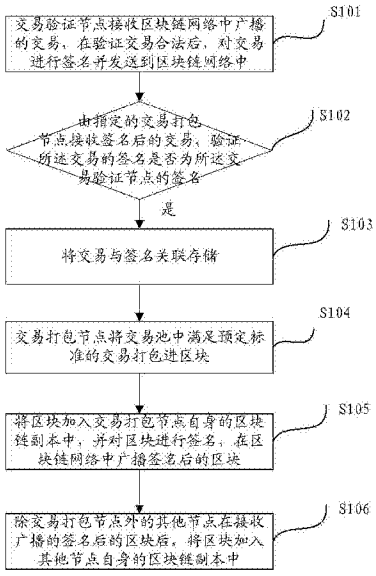
权利要求书2页 说明书11页 附图3页

(54)发明名称

区块链的分组共识方法及系统

(57)摘要

本发明公开了一种区块链的分组共识方法及系统，其中，方法包括：交易验证节点接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中；由指定的交易打包节点接收签名后的交易，验证交易的签名是否为交易验证节点的签名，若是，将交易与签名关联存储；交易打包节点将交易池中满足预设标准的交易打包进区块；将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块；除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中。利用本方案，为节点进行分组，实现不同功能，从而实现权限控制。



CN 106656974 A

1.一种区块链的分组共识方法，其特征在于，包括：

交易验证节点接收区块链网络中广播的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中；

由指定的交易打包节点接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名，若是，将交易与签名关联存储；

所述交易打包节点将交易池中满足预设标准的交易打包进区块；将所述区块加入所述交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块；

除所述交易打包节点外的其他节点在接收广播的签名后的区块后，将所述区块加入所述其他节点自身的区块链副本中；其中，所述其他节点包括交易验证节点、未被指定的交易打包节点和常规节点。

2.根据权利要求1所述的方法，其特征在于，所述交易验证节点接收区块链网络中广播的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中进一步包括：

交易验证节点通过对交易的格式和/或验证交易是否双重花费验证所述交易是否为合法交易。

3.根据权利要求1所述的方法，其特征在于，在交易验证节点接收区块链网络中广播的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中之前，所述方法还包括：

若所述交易为其他交易验证节点签名后的交易，交易验证节点对所述交易进行签名并发送到所述区块链网络中。

4.根据权利要求3所述的方法，其特征在于，所述若所述交易为其他交易验证节点签名后的交易，对所述交易进行签名并发送到所述区块链网络中进一步包括：

交易验证节点将其他交易验证节点的签名替换为该交易验证节点的签名并发送到所述区块链网络中。

5.根据权利要求1所述的方法，其特征在于，在所述由指定的交易打包节点接收签名后的交易，判断所述交易是否已保存在交易池中之前，所述方法还包括：

在多个交易打包节点中利用预设选举算法选举出一个交易打包节点作为指定的交易打包节点。

6.根据权利要求1所述的方法，其特征在于，所述由指定的交易打包节点接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名，若是，将交易与签名关联存储进一步包括：

判断所述交易是否已保存在所述交易打包节点的交易池中；

若否，将所述交易保存在交易池中，并将所述交易的签名与所述交易关联存储；

若是，判断所述交易的签名是否与所述交易已关联存储的签名一致，若不一致，将所述交易的签名与所述交易关联存储。

7.根据权利要求1所述的方法，其特征在于，所述预设标准为交易关联的交易验证节点签名数量超过交易验证节点数量的三分之二。

8.根据权利要求1所述的方法，其特征在于，所述交易验证节点接收区块链网络中广播

的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中进一步包括：

若验证所述交易不合法，将所述交易直接发送到所述区块链网络中。

9.根据权利要求1所述的方法，其特征在于，在所述除所述交易打包节点外的其他节点在接收广播的签名后的区块后，将所述区块加入所述其他节点自身的区块链副本中之前，所述方法还包括：

所述其他节点利用公钥验证所述区块的签名是否为所述交易打包节点的签名；若否，所述方法结束。

10.一种区块链的分组共识系统，其特征在于，包括：多个交易验证节点、多个交易打包节点以及多个常规节点；

所述交易验证节点用于接收区块链网络中广播的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中；

所述交易打包节点用于接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名，若是，将交易与签名关联存储；

所述交易打包节点还用于将交易池中满足预设标准的交易打包进区块；将所述区块加入所述交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块；

所述常规节点用于在接收广播的签名后的区块后，将所述区块加入所述常规节点自身的区块链副本中；

所述交易验证节点还用于在接收广播的签名后的区块后，将所述区块加入所述交易验证节点自身的区块链副本中；

所述未被指定的交易打包节点还用于在接收广播的签名后的区块后，将所述区块加入所述未被指定的交易打包节点自身的区块链副本中。

区块链的分组共识方法及系统

技术领域

[0001] 本发明涉及互联网软件领域，尤其涉及一种区块链的分组共识方法及系统。

背景技术

[0002] 区块链是一种新型去中心化分布式系统协议。信息不可伪造和篡改，无需任何中心化机构的审核。区块链技术解决了拜占庭将军问题，大大降低了现实社会的信任成本，重新定义互联网时代的信任机制。区块链本质上是一个去中心化，开放的数据库，同时作为比特币的底层技术。区块链是一串使用密码学方法相关联产生的数据块链，每一个区块中包含了一定数量的比特币网络交易信息。通过将需要信任背书的数据存入比特币交易账本中，实现可信的，去中心化的信用背书。

[0003] 在去中心化的情况下，区块链并不是一个中心机构创造的，而是由比特币网络中的所有节点各自竞争完成的。比特币网络依靠去中心化的自发共识机制来保证区块链受到各个节点的认可。比特币的去中心化共识包括以下部分：每个节点对每个交易进行独立验证；通过完成工作量证明算法的验算，挖矿节点将交易记录独立打包进新区块；每个节点独立对新区块进行校验并组装进区块链；每个节点对区块链进行独立选择，在工作量证明机制下选择累计工作量最大的区块链。目前的共识机制下，每个节点都可以对交易进行验证和打包，缺少了权限控制。

发明内容

[0004] 本发明的发明目的是针对现有技术的缺陷，提供了一种区块链的分组共识方法及系统，用于解决现有技术中节点缺失权限控制等问题。

[0005] 根据本发明的一个方面，提供了一种区块链的分组共识方法，包括：

[0006] 交易验证节点接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中；

[0007] 由指定的交易打包节点接收签名后的交易，验证交易的签名是否为交易验证节点的签名，若是，将交易与签名关联存储；

[0008] 交易打包节点将交易池中满足预设标准的交易打包进区块；将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块；

[0009] 除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中；其中，其他节点包括交易验证节点、未被指定的交易打包节点和常规节点。

[0010] 根据本发明的另一个方面，还提供了一种区块链的分组共识系统，包括：多个交易验证节点、多个交易打包节点以及多个常规节点；

[0011] 交易验证节点用于接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中；

[0012] 交易打包节点用于接收签名后的交易，验证交易的签名是否为交易验证节点的签

名，若是，将交易与签名关联存储；

[0013] 交易打包节点还用于将交易池中满足预设标准的交易打包进区块；将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块；

[0014] 常规节点用于在接收广播的签名后的区块后，将区块加入常规节点自身的区块链副本中；

[0015] 交易验证节点还用于在接收广播的签名后的区块后，将区块加入交易验证节点自身的区块链副本中；

[0016] 未被指定的交易打包节点还用于在接收广播的签名后的区块后，将区块加入未被指定的交易打包节点自身的区块链副本中。

[0017] 根据本发明提供的区块链的分组共识方法及系统，交易验证节点接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中。由指定的交易打包节点接收签名后的交易，验证交易的签名是否为交易验证节点的签名，若是，将交易与签名关联存储。交易打包节点将交易池中满足预设标准的交易打包进区块，将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块。除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中。对区块链中各不同功能节点进行分类，处理不同的操作，实现对不同节点的权限控制。将操作委托给可信赖的节点如交易验证节点、交易打包节点，由于这些节点是受信任的节点，无需通过工作量证明对交易进行打包，减少了交易打包的时间，提高了区块形成速度。

附图说明

[0018] 通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

[0019] 图1示出了根据本发明一个实施例的区块链的分组共识方法的流程示意图；

[0020] 图2示出了根据本发明另一个实施例的区块链的分组共识方法的流程示意图；

[0021] 图3示出了根据本发明一个实施例的区块链的分组共识系统的功能结构示意图。

具体实施方式

[0022] 下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

[0023] 对区块链网络中存在的多个节点，进行分组。不同组的节点用于实现不同的功能，如交易验证节点用于对在区块链网络中广播的交易进行验证，将验证通过的交易加入自身的交易池并且再次广播到区块链；交易打包节点用于将验证通过的交易加入自身的交易池，将交易池中的交易打包进区块并在区块链网络中广播区块等。这些节点都是受信任的节点。除此之外，还有普通节点，用于广播交易。其中，可以通过如硬编码的方式对节点进行分组，每个节点都知道自己为哪种节点，也知道其他节点为哪种节点，以及节点的公钥，以

便对节点的签名进行验证。所有的节点都可以广播交易，对广播的区块进行验证，将验证通过的区块加入自身的区块链副本。

[0024] 图1示出了根据本发明一个实施例的区块链的分组共识方法的流程示意图。如图1所示，本方法具体包括如下步骤：

[0025] 步骤S101，交易验证节点接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中。

[0026] 通过如硬编码等方式设置区块链网络中的某些节点为交易验证节点。交易验证节点在接收到区块链网络中广播的交易后，对交易进行验证。验证时，交易验证节点通过对交易的格式、交易是否双重花费等多个方面验证交易是否为合法交易。交易的格式、交易是否双重花费等验证条件的设置可采用现有的交易验证条件，此处不做具体限定。

[0027] 交易验证节点通过多方面的验证条件验证交易为合法交易后，利用其本身的私钥对交易进行签名，将签名后的交易发送到区块链网络中。

[0028] 步骤S102，由指定的交易打包节点接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名。

[0029] 通过如硬编码等方式设置区块链网络中的某些节点为交易打包节点。存在多个交易打包节点时，指定其中一个节点为本次的交易打包节点。

[0030] 由指定的交易打包节点接收签名后的交易，利用签名的交易验证节点的公钥对交易的签名进行验证，验证交易的签名是否为交易验证节点的签名。若是，执行步骤S103。

[0031] 步骤S103，若是，将交易与签名关联存储。

[0032] 在将交易与签名关联存储时，可选地，还可用在将交易与签名关联存储之前，判断交易是否已保存在交易池中。若交易未保存在交易池中，将交易保存在交易池中，并将交易的签名与交易关联存储；若交易已经保存在交易池中，进一步判断交易的签名是否与交易已关联存储的签名一致。若一致，不再再次保存。若不一致，将交易的签名与交易进行关联存储，即将交易当前与已关联存储的签名不一致的签名进行存储，存储时，将交易的签名与交易需关联存储。

[0033] 步骤S104，交易打包节点将交易池中满足预设标准的交易打包进区块。

[0034] 预设标准为拜占庭容错标准。拜占庭容错标准为交易池中保存的交易关联的交易验证节点签名数量大于交易验证节点数量的三分之二。如交易验证节点的数量为10，交易打包节点的交易池中的某一交易关联的交易验证节点签名数量大于等于7，则该交易满足拜占庭容错标准。交易打包节点将交易池中满足预设标准的交易打包进区块。

[0035] 可选地，交易打包节点可以在某预设条件时，将交易池中满足预设标准的交易打包进区块。预设条件可以为如上述的交易打包节点的交易池中保存有一定数量的满足预设标准的交易；或预设条件为时间达到预设的时间间隔，即距离上次打包时间已过去预设的时间间隔时，交易打包节点将交易池中满足上述拜占庭容错标准的交易打包进区块。具体的数量或时间间隔数值可根据实施情况进行设定，此处不做具体限定。

[0036] 步骤S105，将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块。

[0037] 将步骤S104打包的区块加入到交易打包节点自身的区块链副本中，形成新的区块链副本。同时，对打包的区块进行签名，如利用交易打包节点本身的私钥进行签名等。签名

后，将签名后的区块在区块链网络中进行广播。

[0038] 步骤S106，除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中。

[0039] 其他节点包括了交易验证节点、本次未被指定的交易打包节点和区块链网络中存在的常规节点。这些节点在接收广播的签名后的区块后，将区块加入到其自身的区块链副本中，从而整个区块链网络中所有节点都完成了将该区块组装至区块链的过程。

[0040] 根据本发明提供的区块链的分组共识方法，交易验证节点接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中。由指定的交易打包节点接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名；若是，将交易的签名与交易关联存储。交易打包节点将交易池中满足预设标准的交易打包进区块，将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块。除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中。对区块链中各不同功能节点进行分类，处理不同的操作，实现对不同节点的权限控制。将操作委托给可信赖的节点如交易验证节点、交易打包节点，由于这些节点是受信任的节点，无需通过工作量证明对交易进行打包，减少了交易打包的时间，提高了区块形成速度。

[0041] 图2示出了根据本发明另一个实施例的区块链的分组共识方法的流程示意图。如图2所示，本方法包括如下步骤：

[0042] 步骤S201，交易验证节点接收区块链网络中广播的交易。

[0043] 步骤S202，判断交易是否为其他交易验证节点签名后的交易。

[0044] 在交易验证节点接收区块链网络中广播的交易后，判断交易是否已经被其他交易验证节点签名，即交易是否为已经验证后合法的交易，并被其他交易验证节点签名后的交易。若是，即交易为合法交易，且被其他交易验证节点签名，执行步骤S203，否则，即交易还没有被验证，执行步骤S204。

[0045] 步骤S203，若交易为其他交易验证节点签名后的交易，交易验证节点对交易进行签名并发送到区块链网络中。

[0046] 交易验证节点可以直接利用自身的私钥对交易进行签名，签名时，可以在交易原有签名的基础上，再增加本次交易验证节点的签名，也可以将其他交易验证节点的签名替换为本次交易验证节点的签名，具体实施时，可根据实施情况进行设置，此处不做具体限定。

[0047] 签名后，将签名后的交易发送到区块链网络中，继续执行步骤S207。

[0048] 步骤S204，交易验证节点验证交易是否合法。

[0049] 因交易未经验证，交易验证节点通过对交易的格式、交易是否双重花费等多个方面验证交易是否为合法交易。交易的格式、交易是否双重花费等验证条件的设置可采用现有的交易验证条件，此处不做具体限定。

[0050] 若交易为合法交易，执行步骤S206，否则执行步骤S205。

[0051] 步骤S205，若验证交易不合法，将交易直接发送到区块链网络中。

[0052] 若交易为不合法交易，对交易不做任何处理，将交易直接发送到区块链网络中，执行步骤S217，本次方法的执行结束。

[0053] 步骤S206，验证交易合法后，对交易进行签名并发送到区块链网络中。

[0054] 交易验证节点通过多方面的验证条件验证交易为合法交易后，利用其本身的私钥对交易进行签名，将签名后的交易发送到区块链网络中。

[0055] 步骤S207，在多个交易打包节点中利用预设选举算法选举出一个交易打包节点作为指定的交易打包节点。

[0056] 通过如硬编码等方式设置区块链网络中的某些节点为交易打包节点。存在多个交易打包节点时，指定其中一个节点为本次的交易打包节点。指定时利用预设选举算法选举出一个交易打包节点。每一次执行前选举出一个交易打包节点对交易执行打包，预设选举算法仅在交易打包节点中执行，选举出的交易打包节点为唯一一个指定的交易打包节点。具体的选举算法可采用如随机法、比重法、轮序法等等算法，此处不做具体限定。

[0057] 步骤S208，由指定的交易打包节点接收签名后的交易，利用公钥验证交易的签名是否为交易验证节点的签名。

[0058] 指定的交易打包节点接收签名后的交易后，利用签名的交易验证节点的公钥对交易的签名进行验证，验证交易的签名是否为交易验证节点的签名。若是，执行步骤S209，否则执行步骤S217，本次方法的执行结束。

[0059] 步骤S209，判断交易是否已保存在交易池中。

[0060] 验证交易的签名为交易验证节点的签名后，进一步判断交易是否已保存在交易打包节点的交易池中。若已保存，执行步骤S211，若未保存，执行步骤S210。

[0061] 步骤S210，将交易保存在交易池中，并将交易的签名与交易关联存储。

[0062] 将该交易保存在交易打包节点的交易池中，并将交易的签名和交易本身进行关联存储。存储后，执行步骤S213。

[0063] 步骤S211，若交易已保存在交易池中，判断交易的签名是否与交易已关联存储的签名一致。

[0064] 若交易已保存在交易打包节点的交易池中，还需要判断保存的交易已关联存储的签名与交易当前的签名是否一致，若不一致，执行步骤S212，若一致，执行步骤S213。

[0065] 步骤S212，若不一致，将交易的签名与交易关联存储。

[0066] 将交易的签名与交易进行关联存储，即将交易当前与已关联存储的签名不一致的签名进行存储，存储时，交易的签名与交易需关联存储。

[0067] 步骤S213，交易打包节点将交易池中满足预设标准的交易打包进区块。

[0068] 预设标准为拜占庭容错标准。拜占庭容错标准为交易池中保存的交易关联的交易验证节点签名数量大于交易验证节点数量的三分之二。如交易验证节点的数量为10，交易打包节点的交易池中的某一交易关联的交易验证节点签名数量大于等于7，则该交易满足拜占庭容错标准。交易打包节点将交易池中满足预设标准的交易打包进区块。

[0069] 可选地，交易打包节点可以在某预设条件时，将交易池中满足预设标准的交易打包进区块。预设条件可以为如上述的交易打包节点的交易池中保存有一定数量的满足预设标准的交易；或预设条件为时间达到预设的时间间隔，即距离上次打包时间已过去预设的时间间隔时，交易打包节点将交易池中满足拜占庭容错标准的交易打包进区块。具体的数量或时间间隔数值可根据实施情况进行设定，此处不做具体限定。

[0070] 步骤S214，将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在

区块链网络中广播签名后的区块。

[0071] 将步骤S213打包的区块加入到交易打包节点自身的区块链副本中，形成新的区块链副本。同时，对打包的区块进行签名，如利用交易打包节点本身的私钥进行签名等。签名后，将签名后的区块在区块链网络中进行广播。

[0072] 步骤S215，除交易打包节点外的其他节点在接收广播的签名后的区块后，其他节点利用公钥验证区块的签名是否为交易打包节点的签名。

[0073] 其他节点包括了交易验证节点、本次未被指定的交易打包节点和区块链网络中存在的常规节点。这些节点在接收广播的签名后的区块后，利用公钥来验证区块的签名是否为交易打包节点的签名，若是，执行步骤S216，否则执行步骤S217，本次方法的执行结束。

[0074] 步骤S216，将区块加入其他节点自身的区块链副本中。

[0075] 将验证后的区块加入到其他节点自身的区块链副本中，从而整个区块链网络中所有节点都完成了将该区块组装至区块链的过程。

[0076] 步骤S217，方法结束。

[0077] 根据本发明提供的区块链的分组共识方法，交易验证节点验证交易合法性并对交易进行签名后发送到区块链网络中。指定的交易打包节点接收签名后的交易，保存在交易池中，并将交易的签名与交易关联存储。当满足预设条件时，交易打包节点将交易池中的交易打包进区块，将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块。除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中。通过对区块链中各不同功能节点进行分类，使其专门的处理不同的操作，实现了对节点不同的权限控制。将需要验证合法性、打包等操作委托给可信赖的节点如交易验证节点、交易打包节点，由于这些节点是受信任的节点，无需通过工作量证明对交易进行验证、打包等，减少了交易打包的时间，提高了区块形成速度。

[0078] 图3示出了根据本发明一个实施例的区块链的分组共识系统的功能结构示意图。如图3所示，本系统包括如下各种节点：多个交易验证节点310、多个交易打包节点320以及多个常规节点330。

[0079] 交易验证节点310用于接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中。

[0080] 交易验证节点310进一步用于：通过对交易的格式和/或验证交易是否双重花费验证交易是否为合法交易。

[0081] 交易验证节点310进一步用于：若验证交易不合法，将交易直接发送到区块链网络中。

[0082] 交易验证节点310进一步用于：若交易为其他交易验证节点签名后的交易，对交易进行签名并发送到区块链网络中。

[0083] 交易验证节点310进一步用于：将其他交易验证节点的签名替换为该交易验证节点的签名并发送到区块链网络中。

[0084] 交易验证节点310还用于在接收广播的签名后的区块后，将区块加入交易验证节点自身的区块链副本中。

[0085] 交易验证节点310进一步用于：利用公钥验证区块的签名是否为交易打包节点的

签名;若否,系统执行结束。

[0086] 交易打包节点320用于接收签名后的交易,验证交易的签名是否为交易验证节点的签名,若是,将交易与签名关联存储。

[0087] 交易打包节点320进一步用于:在多个交易打包节点中利用预设选举算法选举出一个交易打包节点作为指定的交易打包节点。

[0088] 交易打包节点320进一步用于:判断交易是否已保存在交易打包节点的交易池中;若否,将交易保存在交易池中,并将交易的签名与交易关联存储;若是,判断交易的签名是否与交易已关联存储的签名一致,若不一致,将交易的签名与交易关联存储。

[0089] 交易打包节点320还用于将交易池中满足预设标准的交易打包进区块;将区块加入交易打包节点自身的区块链副本中,并对区块进行签名,在区块链网络中广播签名后的区块。

[0090] 未被指定的交易打包节点320还用于在接收广播的签名后的区块后,将区块加入未被指定的交易打包节点自身的区块链副本中。

[0091] 未被指定的交易打包节点320进一步用于:利用公钥验证区块的签名是否为交易打包节点的签名;若否,系统执行结束。

[0092] 常规节点330用于在接收广播的签名后的区块后,将区块加入常规节点自身的区块链副本中。

[0093] 常规节点330进一步用于:利用公钥验证区块的签名是否为交易打包节点的签名;若否,系统执行结束。

[0094] 以上各节点的具体描述可参考各方法实施例中对应的步骤的具体描述,在此不再赘述。

[0095] 根据本发明提供的区块链的分组共识系统,交易验证节点接收区块链网络中广播的交易,在验证交易合法后,对交易进行签名并发送到区块链网络中。由指定的交易打包节点接收签名后的交易,判断交易是否已保存在交易池中,若否,将交易保存在交易池中,并将交易的签名与交易关联存储。当满足预设条件时,交易打包节点将交易池中的交易打包进区块,将区块加入交易打包节点自身的区块链副本中,并对区块进行签名,在区块链网络中广播签名后的区块。除交易打包节点外的其他节点在接收广播的签名后的区块后,将区块加入其他节点自身的区块链副本中。对区块链中各不同功能节点进行分类,处理不同的操作,实现对不同节点的权限控制。将操作委托给可信赖的节点如交易验证节点、交易打包节点,由于这些节点是受信任的节点,无需通过工作量证明对交易进行打包,减少了交易打包的时间,提高了区块形成速度。

[0096] 在此提供的算法和显示不与任何特定计算机、虚拟系统或者其它设备固有相关。各种通用系统也可以与基于在此的示教一起使用。根据上面的描述,构造这类系统所要求的结构是显而易见的。此外,本发明也不针对任何特定编程语言。应当明白,可以利用各种编程语言实现在此描述的本发明的内容,并且上面对特定语言所做的描述是为了披露本发明的最佳实施方式。

[0097] 在此处所提供的说明书中,说明了大量具体细节。然而,能够理解,本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中,并未详细示出公知的方法、结构和技术,以便不模糊对本说明书的理解。

[0098] 类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

[0099] 本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书(包括伴随的权利要求、摘要和附图)中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书(包括伴随的权利要求、摘要和附图)中公开的每个特征可以由提供相同、等同或相似目的的替代特征来代替。

[0100] 此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

[0101] 本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器(DSP)来实现根据本发明实施例中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序(例如，计算机程序和计算机程序产品)。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

[0102] 应该注意的是上述实施例对本发明进行说明而不是对本发明进行限制，并且本领域技术人员在不脱离所附权利要求的范围的情况下可设计出替换实施例。在权利要求中，不应将位于括号之间的任何参考符号构造成对权利要求的限制。单词“包含”不排除存在未列在权利要求中的元件或步骤。位于元件之前的单词“一”或“一个”不排除存在多个这样的元件。本发明可以借助于包括有若干不同元件的硬件以及借助于适当编程的计算机来实现。在列举了若干装置的单元权利要求中，这些装置中的若干个可以是通过同一个硬件项来具体体现。单词第一、第二、以及第三等的使用不表示任何顺序。可将这些单词解释为名称。

[0103] 本发明公开了：A1、一种区块链的分组共识方法，其中，包括：

[0104] 交易验证节点接收区块链网络中广播的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中；

[0105] 由指定的交易打包节点接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名，若是，将交易与签名关联存储；

[0106] 所述交易打包节点将交易池中满足预设标准的交易打包进区块;将所述区块加入所述交易打包节点自身的区块链副本中,并对区块进行签名,在区块链网络中广播签名后的区块;

[0107] 除所述交易打包节点外的其他节点在接收广播的签名后的区块后,将所述区块加入所述其他节点自身的区块链副本中;其中,所述其他节点包括交易验证节点、未被指定的交易打包节点和常规节点。

[0108] A2、根据A1所述的方法,其中,所述交易验证节点接收区块链网络中广播的交易,在验证所述交易合法后,对所述交易进行签名并发送到所述区块链网络中进一步包括:

[0109] 交易验证节点通过对交易的格式和/或验证交易是否双重花费验证所述交易是否为合法交易。

[0110] A3、根据A1所述的方法,其中,在交易验证节点接收区块链网络中广播的交易,在验证所述交易合法后,对所述交易进行签名并发送到所述区块链网络中之前,所述方法还包括:

[0111] 若所述交易为其他交易验证节点签名后的交易,交易验证节点对所述交易进行签名并发送到所述区块链网络中。

[0112] A4、根据A3所述的方法,其中,所述若所述交易为其他交易验证节点签名后的交易,对所述交易进行签名并发送到所述区块链网络中进一步包括:

[0113] 交易验证节点将其他交易验证节点的签名替换为该交易验证节点的签名并发送到所述区块链网络中。

[0114] A5、根据A1所述的方法,其中,在所述由指定的交易打包节点接收签名后的交易,判断所述交易是否已保存在交易池中之前,所述方法还包括:

[0115] 在多个交易打包节点中利用预设选举算法选举出一个交易打包节点作为指定的交易打包节点。

[0116] A6、根据A1所述的方法,其中,所述由指定的交易打包节点接收签名后的交易,验证所述交易的签名是否为所述交易验证节点的签名,若是,将交易与签名关联存储进一步包括:

[0117] 判断所述交易是否已保存在所述交易打包节点的交易池中;

[0118] 若否,将所述交易保存在交易池中,并将所述交易的签名与所述交易关联存储;

[0119] 若是,判断所述交易的签名是否与所述交易已关联存储的签名一致,若不一致,将所述交易的签名与所述交易关联存储。

[0120] A7、根据A1所述的方法,其中,所述预设标准为交易关联的交易验证节点签名数量超过交易验证节点数量的三分之二。

[0121] A8、根据A1所述的方法,其中,所述交易验证节点接收区块链网络中广播的交易,在验证所述交易合法后,对所述交易进行签名并发送到所述区块链网络中进一步包括:

[0122] 若验证所述交易不合法,将所述交易直接发送到所述区块链网络中。

[0123] A9、根据A1所述的方法,其中,在所述除所述交易打包节点外的其他节点在接收广播的签名后的区块后,将所述区块加入所述其他节点自身的区块链副本中之前,所述方法还包括:

[0124] 所述其他节点利用公钥验证所述区块的签名是否为所述交易打包节点的签名;若

否，所述方法结束。

[0125] 本发明还公开了：B10、一种区块链的分组共识系统，其中，包括：多个交易验证节点、多个交易打包节点以及多个常规节点；

[0126] 所述交易验证节点用于接收区块链网络中广播的交易，在验证所述交易合法后，对所述交易进行签名并发送到所述区块链网络中；

[0127] 所述交易打包节点用于接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名，若是，将交易与签名关联存储；

[0128] 所述交易打包节点还用于将交易池中满足预设标准的交易打包进区块；将所述区块加入所述交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块；

[0129] 所述常规节点用于在接收广播的签名后的区块后，将所述区块加入所述常规节点自身的区块链副本中；

[0130] 所述交易验证节点还用于在接收广播的签名后的区块后，将所述区块加入所述交易验证节点自身的区块链副本中；

[0131] 所述未被指定的交易打包节点还用于在接收广播的签名后的区块后，将所述区块加入所述未被指定的交易打包节点自身的区块链副本中。

[0132] B11、根据B10所述的系统，其中，所述交易验证节点进一步用于：

[0133] 通过对交易的格式和/或验证交易是否双重花费验证所述交易是否为合法交易。

[0134] B12、根据B11所述的系统，其中，所述交易验证节点进一步用于：

[0135] 若所述交易为其他交易验证节点签名后的交易，对所述交易进行签名并发送到所述区块链网络中。

[0136] B13、根据B12所述的系统，其中，所述交易验证节点进一步用于：

[0137] 将其他交易验证节点的签名替换为该交易验证节点的签名并发送到所述区块链网络中。

[0138] B14、根据B10所述的系统，其中，所述交易打包节点进一步用于：

[0139] 在多个交易打包节点中利用预设选举算法选举出一个交易打包节点作为指定的交易打包节点。

[0140] B15、根据B14所述的系统，其中，所述交易打包节点进一步用于：

[0141] 判断所述交易是否已保存在所述交易打包节点的交易池中；

[0142] 若否，将所述交易保存在交易池中，并将所述交易的签名与所述交易关联存储；

[0143] 若是，判断所述交易的签名是否与所述交易已关联存储的签名一致，若不一致，将所述交易的签名与所述交易关联存储。

[0144] B16、根据B15所述的系统，其中，所述预设标准为交易关联的交易验证节点签名数量超过交易验证节点数量的三分之二。

[0145] B17、根据B10所述的系统，其中，所述交易验证节点进一步用于：

[0146] 若验证所述交易不合法，将所述交易直接发送到所述区块链网络中。

[0147] B18、根据B10所述的系统，其中，所述常规节点进一步用于：

[0148] 利用公钥验证所述区块的签名是否为所述交易打包节点的签名；若否，所述系统执行结束。

[0149] B19、根据B10所述的系统，其中，所述交易验证节点进一步用于：

[0150] 利用公钥验证所述区块的签名是否为所述交易打包节点的签名；若否，所述系统执行结束。

[0151] B20、根据B10所述的系统，其中，所述未被指定的交易打包节点进一步用于：

[0152] 利用公钥验证所述区块的签名是否为所述交易打包节点的签名；若否，所述系统执行结束。

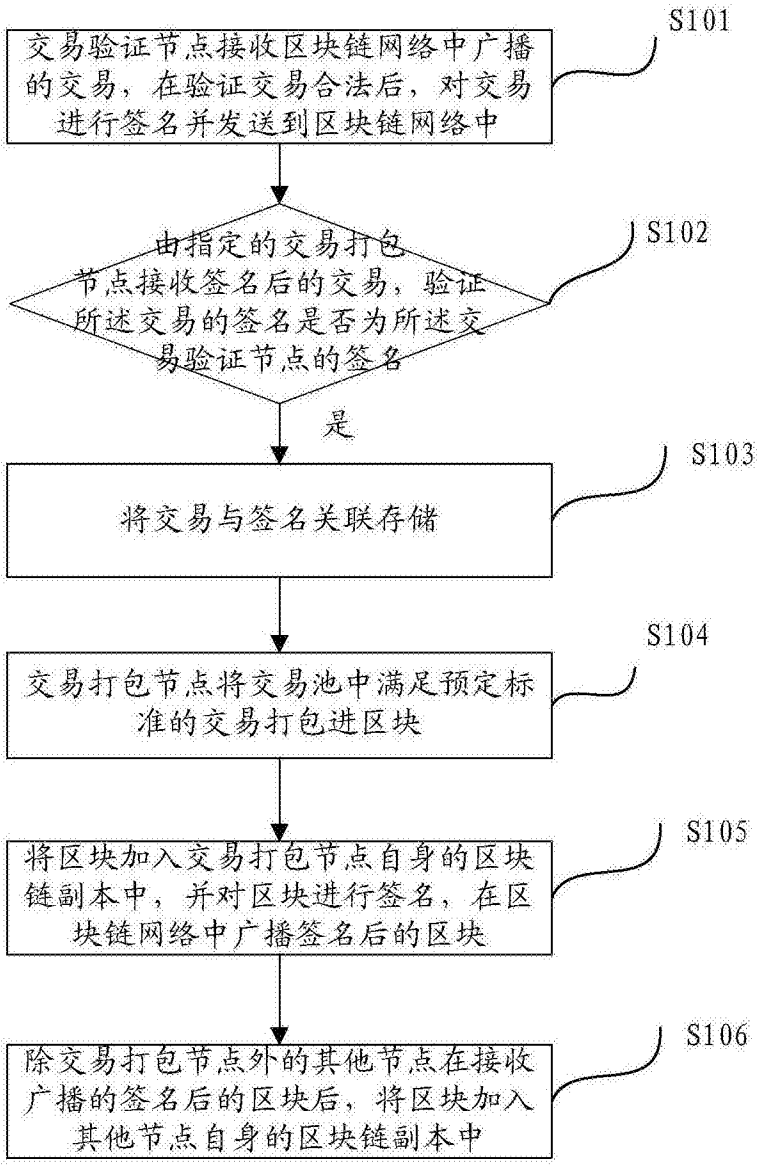

S101
交易验证节点接收区块链网络中广播的交易，在验证交易合法后，对交易进行签名并发送到区块链网络中
S102
由指定的交易打包节点接收签名后的交易，验证所述交易的签名是否为所述交易验证节点的签名
是
S103
将交易与签名关联存储
S104
交易打包节点将交易池中满足预定标准的交易打包进区块
S105
将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块
S106
除交易打包节点外的其他节点在接收广播的签名后的区块后，将区块加入其他节点自身的区块链副本中

图1

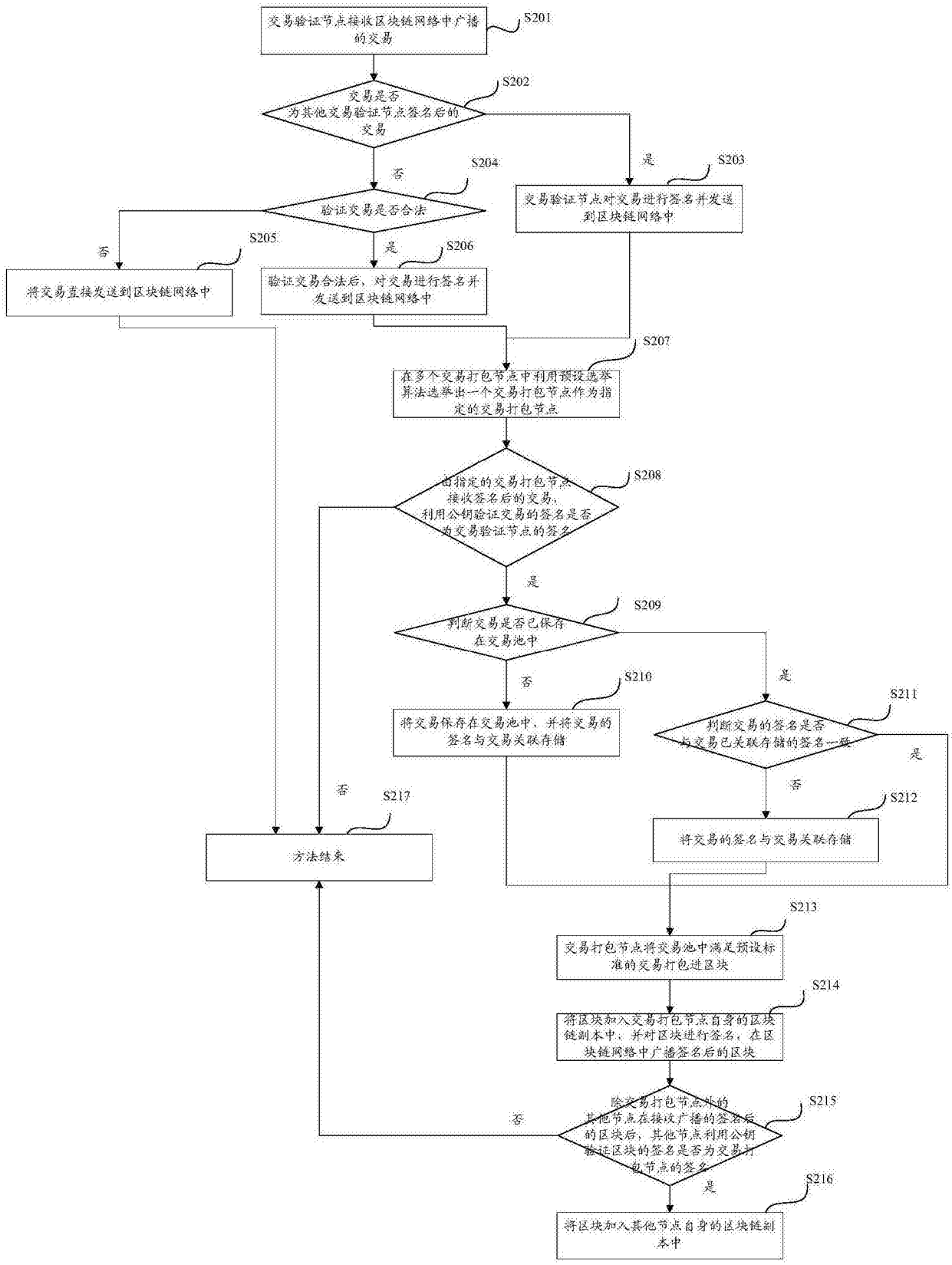

交易验证节点接收区块链网络中广播的交易
S201
交易是否为其他交易验证节点签名后的交易
S202
是
S203
交易验证节点对交易进行签名并发送到区块链网络中
否
S204
验证交易是否合法
否
S205
将交易直接发送到区块链网络中
是
S206
验证交易合法后，对交易进行签名并发送到区块链网络中
S207
在多个交易打包节点中利用预设选举算法选举出一个交易打包节点作为指定的交易打包节点
S208
由指定的交易打包节点接收签名后的交易，利用公钥验证交易的签名是否为交易验证节点的签名
是
S209
判断交易是否已保存在交易池中
否
S210
将交易保存在交易池中，并将交易的签名与交易关联存储
是
S211
判断交易的签名是否与交易已关联存储的签名一致
否
S212
将交易的签名与交易关联存储
是
否
S217
方法结束
S213
交易打包节点将交易池中满足预设标准的交易打包进区块
S214
将区块加入交易打包节点自身的区块链副本中，并对区块进行签名，在区块链网络中广播签名后的区块
S215
除交易打包节点外的其他节点在接收广播的签名后的区块后，其他节点利用公钥验证区块的签名是否为交易打包节点的签名
否
是
S216
将区块加入其他节点自身的区块链副本中

图2

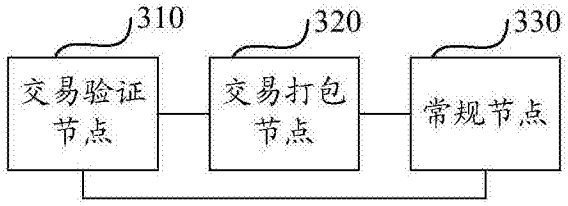


图3