

基于区块链的群组交易方法、装置及计算机可读存储介质

技术领域

本申请属于线上交易领域，具体涉及基于区块链的群组交易方法、系统、装置及计算机可读存储介质。

背景技术

本部分旨在为权利要求书中陈述的本申请的实施方式提供背景或上下文。此处的描述不因为包括在本部分中就承认是现有技术。

区块链是将数据以区块的方式按时间顺序相连形成的一种链式数据结构，并以密码学方式保证数据的不可篡改和不可伪造的分布式账本。

目前，数字/加密资产相关技术日益发展完善，基于区块链的线上交易逐渐增多，但基于区块链的线上交易的接入门槛高，相比传统中心化的金融设施交易效率低，交易成本高。

例如，在传统中心化的交易所技术（CEX）中，用户将其数字资产托管到中心化交易所，交易所平台根据订单簿进行交易订单的匹配撮合，交易完成后，用户再将资产从托管平台转移至自有钱包账户，然而，该种方案的交易安全性和隐私性较低。又例如，在去中心化的交易技术（DEX）中，用户依托区块链上的智能合约，而非中心化交易平台，进行数字资产的交易，智能合约中通过实现自动做市商协议或订单簿模型完成交易订单的撮合，交易在链上完成结算，该种方案的安全性和隐私性较高，但交易速度、交易成本及易用性上都较低。

因此，如何提供一种兼顾安全、可信且成本低廉且易用的线上交易方案是一个亟待解决的问题。

申请内容

针对上述现有技术中存在的问题，提出了基于区块链的群组交易方法、系统、装置及计算机可读存储介质，利用这种方法、系统、装置及计算机可读存储介质，能够解决上述问题。

本申请提供了以下方案。

第一方面，基于区块链的群组交易方法，群组包括注册于传输网络的一个或多个传输节点的多个群组参与方以及部署在指定传输节点的群组接收方，方法包括：

各个群组参与方通过传输网络将交易请求发送给群组接收方；

群组接收方对接收到的群组信息进行全局一致性排序，并有序发布到群组中，群组信息包括交易请求和交易匹配结果；

群组参与方中的群组执行方获取发布到群组中的交易请求，有序执行交易匹配程序得到交易匹配结果，并通过传输网络将交易匹配结果发送给群组接收方；

群组参与方获取发布到群组中的交易匹配结果，并根据交易匹配结果在区块链网络上执行交易结算。

在一种实施方式中，所述群组接收方基于向各个群组参与方公开的一致性排序方法，对接收到的群组信息进行全局一致性排序。

在一种实施方式中，所述群组参与方基于所述群组信息携带的时间戳，对所述全局一致性排序进行验证；其中，所述传输网络中根据传输所述群组信息的时间生成所述时间戳。

在一种实施方式中，群组接收方对接收到的群组信息进行全局一致性排序，包括：群组接收方根据群组信息送达指定传输节点的时间点，对接收到的群组信息进行排序。

在一种实施方式中，群组接收方对接收到的群组信息进行全局一致性排序，包括：在群组信息送达指定传输节点的时间一致的情况下，群组接收方通过比较群组信息的哈希值，对群组信息进行排序。

在一种实施方式中，所述群组接收方对接收到的群组信息进行全局一致性排序，还包括：所述群组接收方每间隔一个时间段确定一个区间，针对每个区间内送达到所述群组接收方的交易请求均统一进行哈希计算；并根据每个区间内收到的交易请求的哈希值排序，对每个区间内的群组信息进行全局一致性排序。

在一种实施方式中，方法还包括：传输网络的每个传输节点发送群组信息的信息次序与指定传输节点接收群组信息的信息次序保持一致。

在一种实施方式中，还包括：在区块链上创建发信合约；群组内各方和/或其所注册的传输节点通过传输网络发送群组信息时，将发送的群组信息的摘要提交至发信合约；群组内各方和/或其所注册的传输节点通过传输网络接收群组信息时，根据接收信息的摘要生成接收确认回执，并提交至发信合约。

在一种实施方式中，还包括：群组参与方利用群组参与方私钥对交易请求进行第一签名，通过传输网络将携带第一签名的交易请求发送到群组接收方；群组接收方获取携带第一签名的交易请求，根据群组发送方公钥进行第一验签后，有序发布到群组中；群组执行方获取发布到群组中的携带第一标签的交易请求，利用群组参与方公钥对交易请求的密文进行第一验签后，有序执行交易匹配程序。

在一种实施方式中，还包括：群组参与方将携带第一签名的交易请求发送给可信第三方；可信第三方对交易请求的密文进行第一验签，验证通过后基于可信第三方私钥对交易请求的密文进行第二签名，以使交易请求携带第一签名和第二签名；群组接收方和/或群组执行方获取交易请求后，还利用可信第三方公钥进行交易请求的密文进行第二验签。

在一种实施方式中，还包括：群组执行方利用群组执行方私钥对生成的交易匹配结果进行第三签名，通过传输网络将携带第三签名的交易匹配结果发送

到群组接收方；群组接收方获取携带第三签名的交易匹配结果，根据群组执行方公钥进行第三验签后，有序发布到群组中；群组参与方获取发布到群组中的携带第三签名的交易匹配结果，利用群组执行方公钥对交易匹配结果的密文进行第三验签后，执行交易。

在一种实施方式中，还包括：在区块链上创建可信合约；群组内的一个或多个群组参与方在可信合约中质押可信凭证；群组接收方被配置为：仅支持接收已在可信合约中质押可信凭证的群组参与方发送的群组消息。

在一种实施方式中，还包括：在区块链上创建一个或多个交易凭证合约；群组参与方在交易结算之前，在相应的交易凭证合约中存入用于交易结算的交易凭证，并根据哈希时间锁锁定用于交易结算的交易凭证，并告知交易目标方。

在一种实施方式中，群组执行方注册在群组接收方所部署的指定传输节点上。

在一种实施方式中，群组执行方有序进行交易匹配程序，包括：流式处理：每次接收到发布到群组中的交易请求，即时输入交易匹配程序处理，并将生成的交易匹配结果即时发送到群组接收方。

在一种实施方式中，群组执行方有序进行交易匹配程序，包括：周期性处理：将周期时段内发布在群组的一个或多个交易请求一次性地输入交易匹配程序，将生成的交易匹配结果发送到群组接收方。

在一种实施方式中，交易请求包括：用于指示己方交易需求的源交易信息，和用于指示目标方交易条件的目标交易信息；群组执行方有序进行交易匹配程序包括：根据至少两条交易请求的源交易信息和目标交易信息进行撮合匹配。

在一种实施方式中，交易请求还包括：交易请求的交易限制信息，包括交易请求的有效时间和/或交易匹配的截止时间；群组执行方执行交易匹配程序还包括：验证是否满足交易请求的交易限制条件。

在一种实施方式中，方法还包括：群组接收方在指定交易请求未被匹配成功前，接收到指定交易请求对应的群组参与方发送的交易撤销请求，将指定交易请求从匹配队列中清除。

在一种实施方式中，根据交易匹配结果在区块链网络上执行交易结算方法，还包括：群组参与方上部署交易匹配程序；群组参与方在发出第一交易请求之后，获取发布到群组中的一个或多个交易请求并输入交易匹配程序，得到验证匹配结果；群组参与方获取发布到群组中的第一交易请求对应的交易匹配结果，并基于验证匹配结果对交易匹配结果进行匹配验证。

第二方面，提供一种基于区块链的群组交易系统，被配置为执行第一方面的方法，系统包括：传输网络，包括通信连接的多个传输节点；区块链网络，被配置为用于执行交易结算；群组包括注册于传输网络的一个或多个传输节点的多个群组参与方以及部署在指定传输节点的群组接收方；群组参与方包含一个或多个群组执行方。

第三方面，提供一种基于区块链的群组交易装置，包括：至少一个处理器；以及，与至少一个处理器通信连接的存储器；其中，存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个处理器能够执行：第一方面的方法。。

第四方面，提供一种计算机可读存储介质，计算机可读存储介质存储有程序，当程序被多核处理器执行时，使得多核处理器执行第一方面的方法。

上述实施例的优点之一，能够提供一种兼顾安全、可信且成本低廉且易用的线上交易方案。

本申请的其他优点将配合以下的说明和附图进行更详细的解说。

应当理解，上述说明仅是本申请技术方案的概述，以便能够更清楚地了解本申请的技术手段，从而可依照说明书的内容予以实施。为了让本申请的上述和其它目的、特征和优点能够更明显易懂，以下特举例说明本申请的具体实施方式。

附图说明

通过阅读下文的示例性实施例的详细描述，本领域普通技术人员将明白本文所述的优点和益处以及其他优点和益处。附图仅用于示出示例性实施例的目

的，而并不认为是对本申请的限制。而且在整个附图中，用相同的标号表示相同的部件。在附图中：

图 1 为本申请实施例提供的一种基于区块链的群组交易系统的示意图；

图 2 为本申请实施例提供的一种基于区块链的群组交易方法的流程示意图；

图 3 为本申请实施例提供的一种基于区块链的群组交易系统的群组内交互示意图；

图 4 为本申请实施例提供的一种基于区块链的群组交易系统的群组内交互示意图；

图 5 为本申请实施例提供的一种基于区块链的群组交易方法的流程示意图；

图 6 为本申请实施例提供的一种基于区块链的群组交易系统的信息上链示意图。

在附图中，相同或对应的标号表示相同或对应的部分。

具体实施方式

下面将参照附图更详细地描述本申请的示例性实施方式。虽然附图中显示了本申请的示例性实施方式，然而应当理解，本申请可以以各种形式实现，而不应被这里阐述的实施方式所限制。相反，提供这些实施方式是为了能够更透彻地理解本申请，并且能够将本申请的范围完整传达给本领域的技术人员。

在本申请实施方式的描述中，应理解，诸如“包括”或“具有”等术语旨在指示本说明书中存在所公开的特征、数字、步骤、行为、部件、部分或其组合，并且并不排除存在一个或多个其他特征、数字、步骤、行为、部件、部分或其组合的可能性。

除非另有说明，“/”表示或的意思，例如，A/B 可以表示 A 或 B；本文中的“和/或”仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B 可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。

术语“第一”、“第二”等仅为了便于描述而用于区分相同或相似的技术特征，而不能理解为指示或暗示这些技术特征的相对重要性或者数量。由此，由“第一”、“第二”等限定的特征可以明示或者隐含地包括一个或者更多个这一特征。在本申请实施方式的描述中，除非另有说明，术语“多个”的含义是两个或多于两个。

另外还需要说明的是，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。

图1是本申请一实施例提供的基于区块链网络的群组交易系统。该系统主要包括用于高效率公平传输信息的传输网络N，以及用于对群组信息进行记录存证的区块链网络BT，该区块链网络BT上的智能合约可以用于管理交易费用。

传输网络N包括通信连接的多个传输节点；传输网络N具体可以是点对点传输网络，由N1、N2、...等负责传输网络中信息的接收传递和路由分发的传输节点构成。

区块链网络BT中存储的信息具有“不可伪造”、“全程留痕”、“可追溯”、“公开透明”、“集体维护”等特征。该区块链网络上的资产合约中存有各个群组参与方用于交易结算的交易凭证，如代币；该区块链上存有传输节点列表和收发地址列表，传输节点列表用于记录公开该传输网络中每个传输节点的地址。

群组包括注册于传输网络N的一个或多个传输节点（如N1、N2等）的多个群组参与方（如A、B、C等）以及部署在指定传输节点的群组接收方G。

群组接收方G，设于传输网络N的指定传输节点，如图1中的N2，被配置为用于接收各个群组参与方（如A、B、C等）发送的群组信息，对接收到群组信息进行全局一致性排序，随后发布在群组中；

群组参与方，注册于传输网络N的传输节点，如群组参与方A注册于传输节点N1，群组参与方B、C注册于传输节点N2，各个群组参与方（如A、B、C）用于将交易请求 Q_U 通过传输网络N发送给群组接收方G。

群组执行方MPE，属于群组参与方中的其中一个或多个，比如图1中的群组参与方C即作为群组执行方，其注册于传输节点N2，用于从群组接收方G

发布到群组的信息中获取经排序的交易请求，并有序执行交易匹配程序得到交易匹配结果，并将交易匹配结果发送给群组接收方 G。

各个群组参与方（如 A、B、C）还用于从群组接收方 G 发布到群组的信息中获取交易匹配结果，并在区块链网络 BT 上执行交易结算。

本申请各个实施例以基于区块链技术的交易匹配方法应用于图 1 中的基于区块链技术的交易匹配系统为例进行说明。

图 2 为根据本申请一实施例的基于区块链技术的交易匹配方法的流程示意图，在该流程中，从设备角度而言，执行主体可以是一个或者多个电子设备；从程序角度而言，执行主体相应地可以是搭载于这些电子设备上的程序。

如图 2 所示，本实施例提供的方法可以包括以下步骤：

步骤 210、各个群组参与方（如 A、B、C）通过传输网络将交易请求发送给群组接收方 G；

各个群组参与方（如 A、B、C）均记录群组接收方 G 的地址，从而得以通过传输网络将交易请求发送给群组接收方 G 所部署的指定传输节点上。

各个群组参与方（如 A、B、C）生成的交易请求可以包括：用于指示己方交易需求的源交易信息，和用于指示目标方交易条件的目标交易信息。比如，源交易信息可以是：所持资产的合约地址，所持资产的待交易金额，资产持有方的地址等用于指示己方资产及地址的交易信息；目标交易信息可以是：目标交易资产的合约地址，目标交易资产的金额，目标交易资产的承接地址等用于指示目标资产及地址的交易信息；还可以包括交易请求的唯一序列号；交易限制信息：如限定交易时间，哈希时间锁等。

例如，群组参与方 A 发出的一条交易请求 Q_{U_A} 可以包括

交易唯一序列号：

0x36a3a4c617302067359e8f614058564dcef309b767337343990d03a90d2b24bd

所持资产合约地址：0x70C78FC35ae0756CA95Bb3D95016edeFbDA8a6A4

所持资产待交易金额：800

目标资产合约地址：0x43cdcb84d6217de595049c762f2687223307e015

目标交易资产金额：200

目标交易资产承接地址：0x7ed58b3621fb0b462cf9c21069904d1a08decfdd

交易截止时间：1695318031464

哈希时间锁：

[0x97fc46276c172633607a331542609db1e3da793fca183d594ed5a61803a1079

2, 1d];

与之相对的，群组参与方 B 发出的一条交易请求 Q_{U_B} 可以包括

交易唯一序列号：

0x13af62fe9d5dd3d5d83b933d1fb1907c38d170b37119c2eda66b26881e5644f3

所持资产合约地址：0x43cdcb84d6217de595049c762f2687223307e015

所持资产待交易金额：200

目标资产合约地址：0x70C78FC35ae0756CA95Bb3D95016edeFbDA8a6A4

目标交易资产金额：800

目标交易资产承接地址：

0x6421C9c87F57833b02d33324d2D1A298fA5F96d2

交易截止时间：1695318051464

应当理解，各个群组参与方（如 A、B、C）生成的交易请求之前或者之后，应当向区块链的交易凭证合约中存入数字资产，也即发行资产。资产的发行或持有，可以在交易结算交割前的任一时间点完成。

步骤 220、群组接收方 G 对接收到的群组信息进行全局一致性排序，并发布到群组中；

该群组信息包括群组参与方（如 A、B、C）发送的全部群组信息，包括各个群组参与方发送的交易请求，也包括群组参与方中的群组执行方 MPE 发送的交易匹配结果。

在群组接收方 G 所部署的指定传输节点上，各个群组参与方（如 A、B、C）均注册为群组的发布信息接收方，也即群组接收方 G 在指定传输节点上记

录群组中各个群组参与方的地址,从而群组接收方 G 发布到群组中的群组信息,可以自动发布到各个群组参与方(如 A、B、C)。简言之,群组内各方均可向群组接收方发送信息,且群组接收方 G 接收的群组信息,可被群组内各方读取。

参考图 3 和图 4 对群组接收方 G 与群组参与方(A、B、C)之间的交互进行说明。参考图 3,群组参与方 B 向群组接收方 G 发送信息时,群组参与方 B 通过第一传输节点将群组信息发送至第二传输节点,第二传输节点根据群组接收方 G 上注册的发布信息接收方地址,再将群组参与方 B 发送的信息分别发送给第二传输节点的群组参与方 C 和第一传输节点的群组参与方 A。参考图 4,群组参与方 C 向群组接收方 G 发送信息的流程与此类似。

群组接收方 G 与群组内各群组参与方的交互,可以仅依赖单传输节点(所有群组成员在同一个节点),也可以是多传输节点(群组成员分布在不同的节点上)。

为了保证交易的公平,需要维持群组内消息次序的全局公平,进而本申请实施例在信息传输网络中开设群组接收方 G 作为群组信息中转渠道,负责群组消息的分发并确保消息次序的全局公平一致。群组接收方 G 以各个群组参与方都同意的全局一致性排序规则对接收到的群组信息进行排序。

步骤 230、群组执行方获取发布到群组中的交易请求,有序执行交易匹配程序得到交易匹配结果,并通过传输网络将交易匹配结果发送给群组接收方;

具体地,群组执行方属于群组参与方。优选地,群组执行方由群组参与方选举确定。

例如,如前,群组参与方 A 发出如上述的一条交易请求 Q_{U_A} ;与之相对的,群组参与方 B 发出如上述的一条交易请求 Q_{U_B} ,进而可以根据至少两条交易请求的源交易信息和目标交易信息进行撮合匹配,可以看出交易请求 Q_{U_A} 和交易请求 Q_{U_B} 的交易信息完全匹配,可以得到交易匹配结果 $M_{Q_A Q_B}$ 。

可选地，在交易请求包含交易限制条件的情况下，群组执行方可以首先验证是否满足交易请求的交易限制条件，比如当前时间是否满足交易请求的有效时间和/或交易匹配的截止时间。如不满足，则直接拒绝匹配。

步骤 240、群组参与方获取发布到群组中的交易匹配结果，并根据交易匹配结果在区块链网络上执行交易结算。

例如，群组参与方 A 和群组参与方 B 在获取交易匹配结果 $M_{Q_A Q_B}$ 之后，可在区块链上采用原子交换的方法，完成交易结算。

为实现区块链网络上的交易结算，还可以在区块链上创建一个或多个交易凭证合约，如群组参与方 A 创建的交易凭证合约 C_1 和群组参与方 B 创建的交易凭证合约 C_2 ；各个群组参与方在交易结算之前，应在相应的交易凭证合约中存入用于交易结算的交易凭证，根据哈希时间锁锁定用于交易结算的交易凭证，并告知交易目标方。

综上，本发明构建了一种公平可信且易用的群组交易方法，结合了传输网络的快速且公平的匹配性能优势和区块链可追溯、不可篡改、高强度可信共识的优势。其中，利用传输网络实现高效率的群组信息传递和公平的交易请求的匹配。交易参与方在交易结算前，无需与区块链发生直接或间接交互，极大降低普通用户对于数字资产所在区块链的学习成本。而在交易结算阶段使用区块链技术，则保证了资产安全性。

在一种实施方式中，上述步骤 220 中，群组接收方 G 基于向各个群组参与方公开的一致性排序方法，对接收到的群组信息进行全局一致性排序。可以理解，全局一致性排序方法对所有群组成员公开，从而群组成员可基于该全局一致性排序方法进行排序验证。

在一种实施方式中，上述步骤 220 中的全局一致性排序，群组参与方可以基于所述群组信息携带的时间戳，对所述全局一致性排序进行验证；其中，所述传输网络中根据传输所述群组信息的时间生成所述时间戳。例如，传输网络中的传输节点在传输该群组信息的时候，可以根据传输时间点进行时间戳打标，可以理解，一致性排序后的群组信息顺序应该和群组信息上的时间戳排序吻合，

从而群组参与方可以对发布到群组中的经过一致性排序的群组信息进行排序验证。

在一种实施方式中，上述步骤 220 中的全局一致性排序，可以包括：群组接收方 G 根据群组信息送达指定传输节点 N2 的时间点，对接收到的群组信息进行排序。

可选地，各个群组参与方所注册的传输节点可根据接收到群组参与方发送的群组信息的时间点，对该群组信息打上时间戳标记，从而后续群组接收方 G 根据群组信息的时间戳，对接收到的群组信息进行排序。

可选地，各个群组参与方所注册的传输节点可将接收到群组参与方发送的群组信息上传到区块链网络，并根据上链时间点对该群组信息打上时间戳标记，从而后续群组接收方 G 根据群组信息的时间戳，对接收到的群组信息进行排序。

可以理解，可以采用多种一致性排序方案对群组信息进行排序，只要全局规则一致可信即可。

进一步地，如两个或更多群组信息送达指定传输节点的时间一致或者群组信息的时间戳指示的时间一致，则群组接收方 G 可以通过比较群组信息的哈希值，对群组信息进行排序。例如，哈希值更大的排序靠前。

在另一种实施方式中，上述步骤 220 中的全局一致性排序，还可以包括：群组接收方 G 每间隔一个时间段确定一个区间，针对每个区间内送达到所述群组接收方的交易请求均统一进行哈希计算；并根据每个区间内收到的交易请求的哈希值排序，对每个区间内的群组信息进行全局一致性排序。如此，可以节省排序工作量。

可选地，还可以通过比较群组信息的其他参数进行排序比较，本申请对此不作具体限制。

在一种实施方式中，为确保传输节点对信息的无差别收发，避免其对特定地址的信息进行恶意拒绝和过滤；上述步骤 220 中的全局一致性排序，还包括：

传输网络的每个传输节点发送群组信息的信息次序与指定传输节点接收群组信息的信息次序保持一致。

例如，当群组参与方 A 按照发送顺序依次发送信息编号 ($T_1, T_2, \dots, T_n$; $T_1 < T_2 < \dots < T_n$) 到所注册的传输节点 N1；在群组接收方 G 所处的指定传输节点 N2 处，也遵循上述次序对消息进行接收。总之，可以由传输节点进行协调信息的收发次序，以确保各传输节点信息的收发次序一致。

在一种实施方式中，为了保证传输网络 N 中传输的群组消息不被篡改，保证交易安全，还可以利用区块链网络的可追溯、不可篡改特性，对群组信息的传输过程进行安全保护。

参考图 5，包括如下步骤：

步骤 510、在区块链上创建发信合约；

具体地，可以由群组推选出的任意方在区块链上创建该发信合约。也可以由群组外的交易管理方创建该发信合约，本申请对此不作具体限制。该发信合约是一种链上智能合约，其定义一组具有特定规则的数字化协议，且该协议能够在满足既定条件时在链上被强制执行。

步骤 520、群组内各方和/或其所注册的传输节点通过传输网络发送群组信息时，将发送的群组信息的摘要提交至发信合约；

具体地，群组内各方包括各个群组参与方和该群组接收方；群组内各方所注册的传输节点包括各个群组参与方注册的传输节点，也包括群组接收方所部署的传输节点。需要强调的是，群组执行方属于群组参与方，自然也属于该群组内各方的范畴内。

具体地，该摘要是对群组信息进行哈希运算得到。群组信息的摘要的数据量较小，上传区块链的成本较小。

例如，参考图 6，示出了图 1 所示网络的发信合约，其中，群组参与方 A 将交易请求发送至群组接收方 G 的过程中，群组参与方 A 将交易请求的摘要上传发信合约后发送给传输节点 N1，随后传输节点 N1 将交易请求通过传输网络

N 发送至传输节点 N2 并向发信合约上传发送确认回执，以证明 N1 完成了信息发送。

步骤 530、群组内各方和/或其所注册的传输节点通过传输网络接收群组信息时，根据接收信息的摘要生成接收确认回执，并提交至发信合约。

例如，参考图 6，其中，传输网络 N2 接收到传输网络 N1 发来的交易请求之后，根据所接受群组信息的摘要向区块链的发信合约上传接收确认回执，以证明 N2 完成了信息接收。

在一种实施方式中，为了进一步保证群组消息不被篡改，保证交易安全，上述步骤 210-230 可以进一步包括如下步骤：

步骤 210 进一步包括：群组参与方利用群组参与方私钥对交易请求进行第一签名，通过传输网络将携带第一签名的交易请求发送到群组接收方；

步骤 220 进一步包括：群组接收方获取携带第一签名的交易请求，根据群组发送方公钥进行第一验签后，有序发布到群组中；

步骤 230 进一步包括：群组执行方获取发布到群组中的携带第一标签的交易请求，利用群组参与方公钥对交易请求的密文进行第一验签后，有序执行交易匹配程序。

可以预先设置群组参与方（A、B、C）、群组接收方 G 和传输网络的各个传输节点（N1、N2、...）的公钥和私钥，其中，可以基于非对称加密算法获得该若干对公钥和私钥，公钥公开在区块链上或者在群组中共享，私钥由各方各自保管。

也即，可以通过各方的数字签名，保障交易的安全性。

可选地，在群组参与方在进行数字签名之前，还可以根据群组执行方公钥对交易请求进行加密，以使得交易请求得以在传输网络中加密传输，且在群组执行方能够基于群组执行方私钥进行解密。

在一种实施方式中，为了进一步保证交易安全，可以引入可信第三方进行安全验证。具体来说，

在上述步骤 210 之后，群组参与方将交易请求的密文发送给可信第三方，可信第三方根据群组参与方公钥对交易请求文进行第一验签，验证通过后基于可信第三方私钥对交易请求进行第二签名，以使交易请求的密文携带第一签名和第二签名。群组参与方将携带群组参与方的第一签名、可信第三方的第二签名的交易请求的密文，作为完整、合法的交易请求，由信息传输网络中的任一方发送至群组信息接收方。

在上述步骤 220 和步骤 230，群组接收方和/或群组执行方获取交易请求后，还利用可信第三方公钥进行交易请求的密文进行第二验签。

可以预先设置可信第三方的公钥和私钥，其中，可以基于非对称加密算法获得该若公钥和私钥，公钥公开在区块链上或者在群组中共享，私钥由可信第三方保管。

也即，通过引入可信第三方的签名，进一步保证了交易的安全性。

在一种实施方式中，为了进一步保证交易安全，可以在区块链上创建可信合约，约定参与交易的群组内的一个或多个群组参与方在可信合约中质押可信凭证；且将群组接收方配置为：仅支持接收已在可信合约中质押可信凭证的群组参与方的群组消息。

例如，参考图 1，可以在区块链上创建可信合约 ζ ，群组参与方 A、B 在可信合约 ζ 中质押可信凭证，比如设定额度的代币，可信身份信息等。且群组接收方在接收到群组消息时，会首先到可信合约 ζ 中检查发送该群组消息的群组参与方是否在该可信合约 ζ 中质押了可信凭证，如未质押，则拒绝接受该群组参与方发来的群组信息，该群组参与方失去参与交易匹配的资格。

在一种实施方式中，为了保证交易匹配结果不被篡改，在群组执行方生成交易匹配结果之后，可以利用所述群组执行方私钥对生成的交易匹配结果进行第三签名，通过传输网络将携带所述第三签名的所述交易匹配结果发送到所述群组接收方；所述群组接收方获取携带所述第三签名的所述交易匹配结果，根据所述群组执行方公钥进行第三验签后，有序发布到群组中；所述群组参与方

获取发布到群组中的携带所述第三签名的所述交易匹配结果，利用所述群组执行方公钥对所述交易匹配结果的密文进行第三验签后，执行交易。

在一种实施方式中，为了缩短传输网络上的信息传输路径，群组执行方 MPE 注册在群组接收方 G 所部署的指定传输节点上。

可以理解，群组执行方 MPE 需要不断从群组接收方获取其发布到群组的交易请求，并需要不断地执行交易匹配并将交易匹配结果发送到群组接收方 G 上，二者的信息传输十分频繁，因此将群组执行方 MPE 注册到群组接收方 G 所部署的指定传输节点上，能减少传输网络中的信息传输次数。

在一种实施方式中，步骤 230 中，所述群组执行方有序进行交易匹配程序，可以采用以下两种处理方：

流式处理：每次接收到发布到群组中的所述交易请求，即时输入交易匹配程序处理，并将生成的交易匹配结果即时发送到所述群组接收方；或者，

周期性处理：将周期时段内发布在群组的一个或多个交易请求一次性地输入交易匹配程序，将生成的交易匹配结果发送到所述群组接收方。

例如，假设群组参与方 A 在时间点 t_0 送达群组接收方一条交易请求 Q_{At_0} ，群组参与方 B 在时间点 t_0 送达群组接收方一条交易请求 Q_{Bt_0} ，且交易请求 Q_{At_0} 和 Q_{Bt_0} 恰好完全匹配，生成交易匹配结果 M_{C1} ；假设群组参与方 A 在时间点 t_1 送达群组接收方一条交易请求 Q_{At_1} ，群组参与方 C 在时间点 t_2 送达群组接收方一条交易请求 Q_{Ct_2} ，且交易请求 Q_{At_1} 、 Q_{Ct_2} 完全匹配，对应匹配结果 M_{C2} 。若 $\Delta t = t_2 - t_0$ ，以下是几种群组内的可能出现的合法消息次序：

流式处理：

$\{Q_{At_0}, Q_{Bt_0}, M_{C1}, Q_{At_1}, Q_{Ct_2}, M_{C2}\}$ 或 $\{Q_{At_0}, Q_{Bt_0}, Q_{At_1}, M_{C1}, Q_{Ct_2}, M_{C2}\}$ 或 $\{Q_{At_0}, Q_{Bt_0}, Q_{At_1}, Q_{Ct_2}, M_{C1}, M_{C2}\}$ ；

周期性处理： $\{Q_{At_0}, Q_{Bt_0}, Q_{At_1}, Q_{Ct_2}, M_{C1}, M_{C2}\}$ 。

在一种实施方式中，步骤 230 还可以包括：

所述群组接收方在指定交易请求未被匹配成功前，接收到所述指定交易请求对应的群组参与方发送的交易撤销请求，将所述指定交易请求从匹配队列中清除。

在一种实施方式中，步骤 240 中根据所述交易匹配结果在区块链网络上执行交易结算方法还可以包括：

所述群组参与方上部署所述交易匹配程序；

所述群组参与方在发出第一交易请求之后，获取发布到群组中的一个或多个所述交易请求并输入所述交易匹配程序，得到验证匹配结果；

所述群组参与方获取发布到群组中的所述第一交易请求对应的交易匹配结果，并基于所述验证匹配结果对所述交易匹配结果进行匹配验证。

步骤 240 中根据所述交易匹配结果在区块链网络上执行交易结算方法还可以包括如下原子交换步骤：

1、群组参与方 A、B 两方交易时，群组参与方 A 生成哈希时间锁 $HTL = (h, T)$ ，其中 $h = \text{Hash}(s)$ ，使用 HTL 在 ζ_1 中将其持有的 a 个 \$X 锁定；

2、群组参与方 A 将 HTL 发送给群组参与方 B，群组参与方 B 可在 ζ_1 中查询确认群组参与方 A 的 HTL 锁定额度，之后使用 HTL 在 ζ_2 中将其持有的 b 个 \$Y 锁定，并告知群组参与方 A；

3、群组参与方 A 在 T 之前使用 $(s, M_{Q_A Q_B})$ 在 ζ_2 中提取群组参与方 B 锁定的 b 个 \$Y，从而公开 s；

4、群组参与方 B 在 T 之前使用 $(s, M_{Q_A Q_B})$ 在 ζ_1 中提取群组参与方 A 锁定的 a 个 \$X，交易完成。

为帮助理解，结合图 1 对本申请的一个具体示例进行阐述，但应当理解，本申请实施例的方案并不限于此。

- a) 参与交易的群组参与方 A、B 分别向不同交易凭证合约 ζ_1, ζ_2 （也可以是在同一合约）中持有不同的加密资产 a 个 \$X、b 个 \$Y；
- b) 群组参与方 A、B 各自在可信合约 ζ 中质押可信凭证 10 USDT；

- c) 群组参与方 A、B 使用各自的资产管理私钥对己方的交易请求签名，约定交易限制信息，例如，在 T 时刻之前交易请求有效，需要在 T-t 之前完成匹配，得到交易请求 Q_{U_A} 和 Q_{U_B} ；
- d) 群组参与方 A、B 分别将交易请求 Q_{U_A} 和 Q_{U_B} 通过信息传输网络 N 发送给约定的群组接收方 G；基于传输网络 N 的特点， Q_{U_A} 和 Q_{U_B} 按对应消息的发送次序送达；即，若送达时间 $t_{Q_{U_A}} < t_{Q_{U_B}}$ ，G 内各方在接收到的所有发送至 G 的消息中，都满足 $t_{Q_{U_A}} < t_{Q_{U_B}}$ ；
- e) 群组接收方 G 中约定由群组执行方 MPE 作为交易请求的匹配程序执行方，P 为 G 中约定的交易匹配程序；群组接收方 G 中约定只有在可信合约 ζ 中质押可信凭证后，才能向群组接收方 G 发送信息；
- f) 群组执行方 MPE 将 Q_{U_A} 和 Q_{U_B} 依次输入 P，P 检查交易限定条件（交易请求的有效时间，匹配的截止时间）是否满足，满足时，得到匹配结果 $M_{Q_A Q_B}$ ；群组执行方 MPE 使用其资产管理私钥，对匹配结果进行签名，将并通过 N 发送至群组接收方 G；
- g) 群组接收方 G 内，包括 A、B 在内的各方接收到 $M_{Q_A Q_B}$ ，验证 MPE 的签名，并将 $M_{Q_A Q_B}$ 之前的所有消息输入 P，验证是否输出结果与 $M_{Q_A Q_B}$ 一致；
- h) 若上一步匹配结果验证无误，A 和 B 可利用 $M_{Q_A Q_B}$ 采用原子交换的方法，完成 a 个 \$X 和 b 个 \$Y 的交易。
- i) 交易凭证合约 ζ_1, ζ_2 中约定，在引用 $M_{Q_A Q_B}$ 达成交易时，由 A 和 B 自主选择是否释放在 ζ 中质押的保证金，如 A 选择释放，则 A 在 ζ_2 中提取 \$Y 资产后， ζ_2 合约自动调用 ζ 中的押金释放方法，释放 A 的交易保证金。

本申请实施例可广泛应用于各类数字资产的线上交易场景，包括但不限于以下典型示例所列举的情形。

1、加密资产的交易：本申请实施例可用于单一链上各类加密资产的交易，也支持跨链间的资产交易。包括符合 ERC-20 标准、ERC721 标准（NFT）、ERC1155 标准等各类加密资产标准类型的资产，都可以在将上述类型的加密资

产充值到本发明所述的交易凭证合约后，按本发明所述方法进行交易。交易参与方将质押资产质押在群组内各参与方约定的合约内，如上述交易凭证合约。

2、传统金融资产与加密资产的交易场景：基于本申请实施例，可实现传统金融资产与加密资产的高效交易。以法定货币为例，可以引入银行作为可信第三方，为其借记客户在链上合约发行借记账户等额的代币，并锁定其借记账户内的法币资产；即银行以其信用和借记客户的法币资产作为担保，借记客户可在基于本发明方法下的系统内，进行法币资产对应代币与其他数字资产的交易。类似地，该方法适用于股票、期权、债权等传统金融产品的交易。

3、商品的交易场景：基于本申请实施例，可实现商品与加密资产、商品与商品之间的高效交易，可用于普通商品贸易、大宗商品交易、期货交易等。以商品的标准化监管仓为可信第三方，为商品的所有方在链上合约发行与商品对应的代币，并在监管仓锁定对应数量的商品；即标准化监管仓以其信用和锁定在监管仓的商品作为担保，商品所有方可在基于本发明的系统内，进行商品与其他数字资产的交易。

4、标准化虚拟产品的交易场景：基于本申请实施例，可实现虚拟产品、数字权益、数字产品、数据资产、虚拟资产（如游戏道具、数字票券、数字卡、数字版权、音视频媒体文件、算法等）与其他数字资产的高效交易。虚拟产品的平台方或发行方作为可信第三方，通过质押数字资产，为其平台上的虚拟产品所有者担保；虚拟产品的所有者可在基于本发明的系统内，进行虚拟产品与其他数字资产的交易。

在本说明书的描述中，参考术语“一些可能的实施方式”、“一些实施方式”、“示例”、“具体示例”、或“一些示例”等进行的描述意指结合该实施方式或示例所描述的具体特征、结构、材料或者特点包含于本申请的至少一个实施方式或示例中，而且上述术语未必表示相同的实施方式或示例。而且，所描述的具体特征、结构、材料或者特点可以在任一个或多个实施方式或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施方式或示例以及不同实施方式或示例的特征进行结合和组合。

关于本申请实施方式的方法流程图，将某些操作描述为以一定顺序执行的不同步骤。这样的流程图属于说明性的而非限制性的。可以将本文中所描述的某些步骤分组在一起并且在单个操作中执行、或者可以将某些步骤分割成多个子步骤、并且可以以不同于本文中所示的顺序来执行某些步骤。可以由任何电路结构和/或有形机制(例如，由在计算机设备上运行的软件、硬件(例如，处理器或芯片实现的逻辑功能)等、和/或其任何组合)以任何方式来实现流程图所示出的各个步骤。

本领域技术人员可以理解，在上述具体实施方式中描述的方法中，各步骤的撰写顺序并不意味着严格的执行顺序，各步骤的具体执行顺序应当以其功能和可能的内在逻辑确定。

根据本申请的一些实施例，图 1 提供了根据本申请一实施例的基于区块链网络的群组交易系统，用于执行如上实施例所述的群组交易方法。

该系统主要包括用于高效率公平传输信息的传输网络 N，以及用于对群组信息进行记录存证的区块链网络 BT，该区块链网络 BT 上的智能合约可以用于管理交易费用。

传输网络 N 包括通信连接的多个传输节点；传输网络 N 具体可以是点对点传输网络，由 N1、N2、...等负责传输网络中信息的接收传递和路由分发的传输节点构成。

区块链网络 BT 中存储的信息具有“不可伪造”、“全程留痕”、“可追溯”、“公开透明”、“集体维护”等特征。该区块链网络上的资产合约中存有各个群组参与方用于交易结算的交易凭证，如代币；该区块链上存有传输节点列表和收发地址列表，传输节点列表用于记录公开该传输网络中每个传输节点的地址。

群组包括注册于传输网络 N 的一个或多个传输节点（如 N1、N2 等）的多个群组参与方（如 A、B、C 等）以及部署在指定传输节点的群组接收方 G。

群组接收方 G，设于所述传输网络 N 的指定传输节点，如图 1 中的 N2，被配置为用于接收各个所述群组参与方（如 A、B、C 等）发送的群组信息，对接收到群组信息进行全局一致性排序，随后发布在群组中；

群组参与方，注册于传输网络 N 的传输节点，如群组参与方 A 注册于传输节点 N1，群组参与方 B、C 注册于传输节点 N2，各个群组参与方（如 A、B、C）用于将交易请求 Q_U 通过传输网络 N 发送给群组接收方 G。

群组执行方 MPE，属于群组参与方中的其中一个或多个，比如图 1 中的群组参与方 C 即作为群组执行方，其注册于传输节点 N2，用于从群组接收方 G 发布到群组的信息中获取经排序的所述交易请求，并有序执行交易匹配程序得到交易匹配结果，并将所述交易匹配结果发送给所述群组接收方 G。

各个群组参与方（如 A、B、C）还用于从群组接收方 G 发布到群组的信息中获取交易匹配结果，并在区块链网络 BT 上执行交易结算。

根据本申请的一些实施例，提供了根据本申请一实施例的基于区块链网络的群组交易装置，用于执行图 2 所示出的基于区块链网络的群组交易方法，该装置包括：至少一个处理器；以及，与至少一个处理器通信连接的存储器；其中，存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个处理器能够执行上述实施例所述的方法。

根据本申请的一些实施例，提供了基于区块链网络的群组交易方法的非易失性计算机存储介质，其上存储有计算机可执行指令，该计算机可执行指令设置为在由处理器运行时执行：上述实施例所述的方法。

计算机可读介质包括永久性和非永久性、可移动和非可移动媒体，可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机可读存储介质的例子包括但不限于相变内存 (PRAM)、静态随机存取存储器 (SRAM)、动态随机存取存储器 (DRAM)、其他类型的随机存取存储器、只读存储器、电可擦除可编程只读存储器 (EEPROM)、快闪记忆体或其他内存技术、CD-ROM、数字多功能光盘 (DVD) 或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。此外，尽管在附图中以特定顺序描述了本申请方法的操作，但是，这并非要求或者暗示必须按照该特定顺序来执行这些操作，或是必须执行全部所示操作才能实现期望的结果。另外，也可

以省略某些步骤，将多个步骤合并为一个步骤执行，和/或将一个步骤分解为多个子步骤执行。

以上虽然已经参考若干具体实施方式描述了本申请的精神和原理，但是应该理解，本申请并不限于所公开的具体实施方式，对各方面的划分也不意味着这些方面中的特征不能组合。本申请旨在涵盖所附权利要求的精神和范围内所包括的各种修改和等同布置。

权 利 要 求 书

1、一种基于区块链的群组交易方法，其特征在于，所述群组包括注册于传输网络的一个或多个传输节点的多个群组参与方以及部署在指定传输节点的群组接收方，所述方法包括：

各个群组参与方通过传输网络将交易请求发送给所述群组接收方；

所述群组接收方对接收到的群组信息进行全局一致性排序，并有序发布到群组中，所述群组信息包括所述交易请求和交易匹配结果；

所述群组参与方中的群组执行方获取发布到群组中的所述交易请求，有序执行交易匹配程序得到所述交易匹配结果，并通过所述传输网络将所述交易匹配结果发送给所述群组接收方；

所述群组参与方获取发布到群组中的所述交易匹配结果，并根据所述交易匹配结果在区块链网络上执行交易结算。

2、根据权利要求1所述的方法，其特征在于，所述群组接收方对接收到的群组信息进行全局一致性排序，还包括：

所述群组接收方基于向各个群组参与方公开的一致性排序方法，对接收到的群组信息进行全局一致性排序。

3、根据权利要求1所述的方法，其特征在于，还包括：

所述群组参与方基于所述群组信息携带的时间戳，对所述全局一致性排序进行验证；

其中，所述传输网络中根据传输所述群组信息的时间生成所述时间戳。

4、根据权利要求1所述的方法，其特征在于，所述群组接收方对接收到的群组信息进行全局一致性排序，包括：

所述群组接收方根据所述群组信息送达所述指定传输节点的时间点，对接收到的所述群组信息进行排序。

5、根据权利要求4所述的方法，其特征在于，所述群组接收方对接收到的群组信息进行全局一致性排序，包括：

在所述群组信息送达所述指定传输节点的时间一致的情况下，所述群组接收方通过比较所述群组信息的哈希值，对所述群组信息进行排序。

6、根据权利要求1所述的方法，其特征在于，所述群组接收方对接收到的群组信息进行全局一致性排序，还包括：

所述群组接收方每间隔一个时间段确定一个区间，针对每个区间内送达到所述群组接收方的交易请求均统一进行哈希计算；并根据每个区间内收到的交易请求的哈希值排序，对每个区间内的群组信息进行全局一致性排序。

7、根据权利要求1所述的方法，其特征在于，所述方法还包括：

所述传输网络的每个传输节点发送所述群组信息的信息次序与所述指定传输节点接收所述群组信息的信息次序保持一致。

8、根据权利要求1所述的方法，其特征在于，还包括：

在区块链上创建发信合约；

群组内各方和/或其所注册的传输节点通过所述传输网络发送所述群组信息时，将发送的群组信息的摘要提交至所述发信合约；

群组内各方和/或其所注册的传输节点通过所述传输网络接收所述群组信息时，根据接收信息的摘要生成接收确认回执，并提交至所述发信合约。

9、根据权利要求1所述的方法，其特征在于，还包括：

所述群组参与方利用所述群组参与方私钥对所述交易请求进行第一签名，通过传输网络将携带所述第一签名的所述交易请求发送到所述群组接收方；

所述群组接收方获取携带所述第一签名的所述交易请求，根据所述群组发送方公钥进行第一验签后，有序发布到群组中；

所述群组执行方获取发布到群组中的携带第一标签的所述交易请求，利用所述群组参与方公钥对所述交易请求的密文进行第一验签后，有序执行交易匹配程序。

10、根据权利要求9所述的方法，其特征在于，还包括：

所述群组参与方将携带所述第一签名的所述交易请求发送给可信第三方；

所述可信第三方对所述交易请求的密文进行第一验签，验证通过后基于可信第三方私钥对所述交易请求的密文进行第二签名，以使所述交易请求携带所述第一签名和所述第二签名；

所述群组接收方和/或所述群组执行方获取所述交易请求后，还利用所述可信第三方公钥进行所述交易请求的密文进行第二验签。

11、根据权利要求1所述的方法，其特征在于，还包括：

所述群组执行方利用所述群组执行方私钥对生成的交易匹配结果进行第三签名，通过传输网络将携带所述第三签名的所述交易匹配结果发送到所述群组接收方；

所述群组接收方获取携带所述第三签名的所述交易匹配结果，根据所述群组执行方公钥进行第三验签后，有序发布到群组中；

所述群组参与方获取发布到群组中的携带所述第三签名的所述交易匹配结果，利用所述群组执行方公钥对所述交易匹配结果的密文进行第三验签后，执行交易。

12、根据权利要求1所述的方法，其特征在于，还包括：

在区块链上创建可信合约；

群组内的一个或多个群组参与方在所述可信合约中质押可信凭证；

所述群组接收方被配置为：仅支持接收已在所述可信合约中质押可信凭证的群组参与方发送的群组消息。

13、根据权利要求1所述的方法，其特征在于，还包括：

在区块链上创建一个或多个交易凭证合约；

所述群组参与方在交易结算之前，在相应的所述交易凭证合约中存入用于交易结算的交易凭证，并根据哈希时间锁锁定用于交易结算的交易凭证，并告知交易目标方。

14、根据权利要求1所述的方法，其特征在于，所述群组执行方注册在所述群组接收方所部署的指定传输节点上。

15、根据权利要求 4 或 5 所述的方法，其特征在于，所述群组执行方有序进行交易匹配程序，包括：

流式处理：每次接收到发布到群组中的所述交易请求，即时输入交易匹配程序处理，并将生成的交易匹配结果即时发送到所述群组接收方。

16、根据权利要求 6 所述的方法，其特征在于，所述群组执行方有序进行交易匹配程序，包括：

周期性处理：将周期时段内发布在群组的一个或多个交易请求一次性地输入交易匹配程序，将生成的交易匹配结果发送到所述群组接收方。

17、根据权利要求 1 所述的方法，其特征在于，所述交易请求包括：用于指示己方交易需求的源交易信息，和用于指示目标方交易条件的目标交易信息；

所述群组执行方有序进行交易匹配程序包括：

根据至少两条交易请求的源交易信息和目标交易信息进行撮合匹配。

18、根据权利要求 1 所述的方法，其特征在于，所述交易请求还包括：

所述交易请求的交易限制信息，包括所述交易请求的有效时间和/或交易匹配的截止时间；

所述群组执行方执行交易匹配程序还包括：验证是否满足所述交易请求的交易限制条件。

19、根据权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述群组接收方在指定交易请求未被匹配成功前，接收到所述指定交易请求对应的群组参与方发送的交易撤销请求，将所述指定交易请求从匹配队列中清除。

20、根据权利要求 1 所述的方法，其特征在于，根据所述交易匹配结果在区块链网络上执行交易结算方法，还包括：

所述群组参与方上部署所述交易匹配程序；

所述群组参与方在发出第一交易请求之后，获取发布到群组中的一个或多个所述交易请求并输入所述交易匹配程序，得到验证匹配结果；

所述群组参与方获取发布到群组中的所述第一交易请求对应的交易匹配结果，并基于所述验证匹配结果对所述交易匹配结果进行匹配验证。

21、一种基于区块链的群组交易系统，其特征在于，被配置为执行如权利要求 1-20 中任一项所述的方法，所述系统包括：

传输网络，包括通信连接的多个传输节点；

区块链网络，被配置为用于执行交易结算；

所述群组包括注册于传输网络的一个或多个传输节点的多个群组参与方以及部署在指定传输节点的群组接收方；所述群组参与方包含一个或多个群组执行方。

22、一种基于区块链的群组交易装置，其特征在于，包括：

至少一个处理器；以及，与至少一个处理器通信连接的存储器；其中，存储器存储有可被至少一个处理器执行的指令，指令被至少一个处理器执行，以使至少一个处理器能够执行：如权利要求 1-20 中任一项所述的方法。。

23、一种计算机可读存储介质，所述计算机可读存储介质存储有程序，当所述程序被多核处理器执行时，使得所述多核处理器执行如权利要求 1-20 中任一项所述的方法。