(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 1 月 4 日 (04.01.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/001037 A1

(51) 国际专利分类号:
H04L 9/40 (2022.01) *H04L 67/10* (2022.01)
H04L 9/08 (2006.01) *H04L 67/104* (2022.01)

(21) 国际申请号: PCT/CN2022/135607

(22) 国际申请日: 2022 年 11 月 30 日 (30.11.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202210760927.X 2022年6月29日 (29.06.2022) CN

(71) 申请人: 蚂蚁区块链科技（上海）有限公司 **(ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.)** [CN/CN]; 中国上海市黄浦区外马路618号8层803室, Shanghai 200010 (CN)。

(72) 发明人: 魏长征 **(WEI, Changzheng)**; 中国上海市黄浦区外马路618号8层803室, Shanghai 200010 (CN)。 闫莺 **(YAN, Ying)**; 中国上海市黄浦区外马路618号8层803室, Shanghai 200010 (CN)。

(74) 代理人: 北京智信禾专利代理有限公司 **(CHISPO ATTORNEYS AT LAW)**; 中国北京市东城区崇文门外大街8号哈德门广场西塔9层901, Beijing 100062 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO,

(54) Title: MESSAGE TRANSMISSION METHOD AND APPARATUS, ELECTRONIC DEVICE AND STORAGE MEDIUM

(54) 发明名称: 一种消息传输方法、装置、电子设备和存储介质

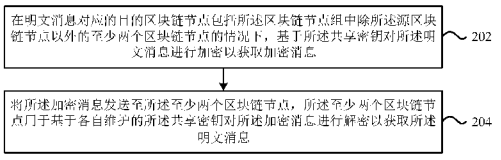

图 2

202 When target blockchain nodes corresponding to a plaintext message comprise at least two blockchain nodes except a source blockchain node in a blockchain node group, encrypt the plaintext message on the basis of a shared key, so as to acquire an encrypted message

204 Transmit the encrypted message to the at least two blockchain nodes, the at least two blockchain nodes being used for decrypting the encrypted message on the basis of the shared key maintained thereby respectively, so as to acquire the plaintext message

(57) Abstract: Provided in present specification are a message transmission method and apparatus, an electronic device and a storage medium, which are applied to a source blockchain node. All blockchain nodes in a blockchain node group to which a source blockchain node belongs maintain a same shared key. The method comprises: when target blockchain nodes corresponding to a plaintext message comprise at least two blockchain nodes except a source blockchain node in the blockchain node group, encrypting the plaintext message on the basis of the shared key, so as to acquire an encrypted message; and transmitting the encrypted message to the at least two blockchain nodes, the at least two blockchain nodes being used for decrypting the encrypted message on the basis of the shared key maintained thereby respectively, so as to acquire the plaintext message.

(57) 摘要: 本说明书提供一种消息传输方法、装置、电子设备和存储介质，应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述方法包括：在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息；将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

WO 2024/001037 A1

[见续页]

PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

一种消息传输方法、装置、电子设备和存储介质

本申请要求于2022年06月29日提交中国专利局、申请号为202210760927.X、发明名称为“一种消息传输方法、装置、电子设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本说明书实施例属于区块链技术领域，尤其涉及一种消息传输方法、装置、电子设备和存储介质。

背景技术

区块链（Blockchain）是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。区块链系统中按照时间顺序将数据区块以顺序相连的方式组合成链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。由于区块链具有去中心化、信息不可篡改、自治性等特性，区块链也受到人们越来越多的重视和应用。

在传统的区块链技术中，各个区块链节点之间直接采用P2P（Peer to Peer，点对点）技术进行通信，以传输交易、区块等，为了确保信息安全，区块链节点之间往往会建立加密信道，由此实现加密通信。而由于每个加密信道都具有独立性，其对应的密钥或加密策略并不相同，因此在对消息进行组播或广播的场景下，源区块链节点需要按照与多个目的区块链节点相连的多个加密信道对应的多个密钥，对同一明文消息进行多次加密后再分别发送至其他区块链节点，由此给源区块链节点带来了极大的计算负担，影响区块链节点之间的加密通信效率。

发明内容

本说明书的目的在于提供一种消息传输方法、装置、电子设备和存储介质。

根据本说明书一个或多个实施例的第一方面，提出了一种消息传输方法，应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述方法包括：

在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息；

将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

根据本说明书一个或多个实施例的第二方面，提出了一种消息传输装置，应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述装置包括：

加密单元，用于在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息；

发送单元，用于将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

根据本说明书一个或多个实施例的第三方面，提出了一种电子设备，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如第一方面所述的方法。

根据本说明书一个或多个实施例的第四方面，提出了一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如第一方面所述方法的步骤。

在本说明书实施例中，源区块链节点在进行广播或组播时，由于源区块链节点与目的区块链节点中至少两个区块链节点共同维护有相同的共享密钥，因此源区块链节点可以使用共享密钥对明文消息进行一次加密后发送给所述至少两个区块链节点，从而降低组播或广播场景中对明文消息的加密次数，在确保通讯安全前提下减少源区块链节点的计算负担，提高区块链节点之间的加密通信效率。

附图说明

为了更清楚地说明本说明书实施例的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本说明书中记载的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 是一示例性实施例提供的一种区块链节点之间进行交互的场景示意图。

图 2 是一示例性实施例提供的一种消息传输方法的流程图。

图 3 是一示例性实施例提供的一种源区块链节点进行广播的场景示意图。

图 4 是一示例性实施例提供的一种设备的结构示意图。

图 5 是一示例性实施例提供的一种消息传输装置的框图。

具体实施方式

为了使本技术领域的人员更好地理解本说明书中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本说明书一部分实施例，而不是全部的实施例。基于本说明书中的实施例，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，都应当属于本说明书保护的范围。

当区块链节点之间在基于 P2P 技术进行端到端直连时，可以使用 SSL（Secure Socket Layer，安全套接字层）链路、TLS(Transport Layer Security，传输层安全协议)、IPsec（Intemet Protocol Security，互联网安全协议）等基于端到端加密协议来实现加密通信。例如，当区块链节点 Node A 需要向区块链节点 Node B 发送区块链消息时，Node A 与 Node B 之间可以基于 SSL 协议进行密钥协商，从而基于协商出的传输密钥在该 Node A 与 Node B 之间建立起 SSL 链路。那么，区块链消息在该 SSL 链路内部传输时都处于密文状态（由上述的传输密钥加密），仅由持有该传输密钥的 Node A 与 Node B 能够解密出相应的消息明文。

然而，区块链节点之间建立的各个加密信道均具有独立性，同一区块链节点与其他不同区块链节点所建立的多个加密信道的密钥或加密策略均不相同，这意味着对于一个需要同时向其他多个目的区块链节点广播或组播同一明文消息的源区块链节点而言，其需要将明文消息分别按照与其他多个目的区块链节点之间建立的多个加密信道对应的密钥和加密策略进行多次独立地加密，从而得到多个加密消息，然后再将这多个加密消息分别通过相应的加密信道发送至对应的其他多个目的区块链节点，这加重了区块链节点执行广播或组播的计算开销，特别是在作为目的区块链节点的数量众多时，将成倍地增加源区块链节点执行加密任务的计算负担，影响区块链节点之间的通信效率。

以图 1 为例，图 1 是一示例性实施例提供的一种区块链节点之间进行交互的场景示意图。如图 1 所

示，该场景中共包含4个区块链节点Node A、Node B、Node C和Node D，它们彼此之间均建立有加密信道，以实现加密通信。然而，在传统架构中，区块链节点之间所建立的加密信道互相具有独立性，例如Node A与Node B、Node C、Node D分别建立有三个互不相关的加密信道tunnel_AB、tunnel_AC、tunnel_AD，在Node A需要同时向Node B、Node C、Node D广播消息时，Node A会分别基于tunnel_AB、tunnel_AC、tunnel_AD对应的密钥对待广播的明文消息进行加密以获取三个不同的加密消息msg_AB、msg_AC、msg_AD，再将msg_AB通过tunnel_AB发送至Node B，将msg_AC通过tunnel_AC发送至Node C，将msg_AD通过tunnel_AD发送至Node D。不难发现，Node A为了向其他三个区块链节点广播同一明文消息，需要对该明文消息独立地进行三次加密。特别是在场景中的区块链节点例如Node A、Node B、Node C和Node D处于同一区块链网络中时，由于交易共识、区块同步等需求，区块链网络中的每个区块链节点都会承担大量消息广播任务，这使得随着区块链网络规模逐渐增大，区块链节点数量越来愈多，其通信开销会以二次函数增长。

为解决上述问题，本说明书提出了一种消息传输方案，通过在区块链节点中建立区块链节点组并维护相同的共享密钥，从而降低组播或广播场景中对明文消息的加密次数，同时还能够确保通讯安全。

下面结合图2对本说明书涉及的消息传输方法进行详细说明。图2是一示例性实施例提供的一种消息传输方法的流程图，其中，所述方法应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述方法包括：

S202：在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息。

在本说明书实施例中，源区块链节点指的是在一次区块链节点之间的交互中处于消息发送方地位的区块链节点，因此源区块链节点一般只有一个，而目的区块链节点则指的是在一次区块链节点之间的交互中处于消息接收方地位的区块链节点，显然消息的接收方并不唯一，因此目的区块链节点的数量也不唯一，可以为一个，也可以为多个。

在本说明书实施例中，可以将能够互相通信的区块链节点按照区块链节点组的群组管理方式进行管理，从而使得处于同一区块链节点组中的各个区块链节点维护有相同的共享密钥。例如，若干个区块链节点可以事先通过组密钥协商来维护共同的共享密钥，从而基于线上协商的方式共同组织成为一个区块链节点组；或者，若干个区块链节点在线下被手动录入了相同的密钥作为共享密钥，从而基于线下录入的方式共同组织成为一个区块链节点组；或者，若干个区块链节点所处的节点设备绑定有相同的密钥，那么这若干个区块链节点会从自身所处节点设备上读取得到该相同的密钥并作为共享密钥，从而基于设备绑定的方式共同组织成为一个区块链节点组。区块链节点组内的区块链节点在进行相互通信的过程中，首先会根据共同维护的共享密钥对明文消息进行加密以获得加密消息，然后再对加密消息进行传输，由此以来，无论加密消息在传输过程中经过任何处理、或者被攻击者所窃取，由于共享密钥仅被同一区块链节点组内的区块链节点所维护，因此从理论上排除了明文消息在传输过程中被暴露的可能性。本说明书实施例所涉及的共享密钥为对称密钥，因此，在区块链节点接收到来自与其属于同一区块链节点组内的其他区块链节点的加密消息时，可以直接基于共享密钥进行解密以获取明文消息。

在本说明书实施例中，所述区块链节点组中的各区块链节点处于相同的区块链网络或不同的区块链网络，例如，所述源区块链节点与所述目的区块链节点可以处于相同的区块链网络或不同的区块链网络。需要指出的是，区块链节点组与区块链网络之间并非同一概念，这意味着，同属于一个区块链节点组中

的区块链节点成员并非一定处于同一区块链网络中，同一区块链网络中的各区块链节点也不一定处于同一区块链节点组中，本说明书实施例所涉及的区块链节点组其初衷在于实现区块链节点组内成员的安全通信，这不仅可以适应区块链网络内部各区块链节点针对交易共识、区块同步的链内交互需求（通过将统同一区块链网络中的所有区块链节点设置为同一区块链节点组），也可以适应不同区块链网络中的区块链节点之间的跨链交互需求（通过将处于不同区块链网络中的区块链节点设置为同一区块链节点组）。区块链网络组中的各区块链节点同处于不同区块链网络的情况下，所述不同的区块链网络之间彼此同构或异构，例如，在所述源区块链节点与所述目的区块链节点处于不同的区块链网络的情况下，所述源区块链节点所处的源区块链网络与所述目的区块链节点所处的目的区块链网络同构或异构，区块链节点组中的区块链节点并不被要求需要具有相同的区块链架构，即一个区块链节点组中各区块链节点所涉及的多个区块链网络并非一定要求同构，具有相同的区块链协议、共识协议等，涉及的多个区块链网络之间也可以是异构的。

需要说明的是，狭义上的异构区块链，通常是指在区块链上流通的价值存在明显差异；也即，所流通的价值存在明显差异的两个区块链之间，通常可以称之为异构区块链。比如，比特币网络和以太坊就是狭义上的异构区块链。

而广义上的异构区块链，是指区块链的类型和/或采用的区块链协议存在明显差异；也即，区块链的类型和/或采用的区块链协议存在明显的两个区块链之间，通常也可以称之为异构区块链。比如，蚂蚁区块链（ANT CHAIN）和 hyperledger fabric 区块链就是广义上的异构区块链。

在本说明书实施例中，同一个区块链节点可以同时隶属于多个不同的区块链节点组，因而对于任一区块链节点而言，其本地可以分别维护有自身共同所属的多个区块链节点组的成员列表及其对应的共享密钥。而在源区块链节点需要向目的区块链节点发送明文消息的情况下，源区块链节点首先通过在本地查找预先维护的至少一个区块链节点组，并确定自身与目的区块链节点共同所属的区块链节点组（可能有多个），然后基于本地维护的该区块链节点组对应的共享密钥对明文消息进行加密以获取加密消息，从而使得目的区块链节点在接收到该加密消息后能够基于该区块链节点组的共享密钥解密得到明文消息。显然，在目的区块链节点包括至少两个区块链节点时的情况下，需要在本地查找出源区块链节点与作为目的区块链节点的至少两个区块链节点所共同所属的区块链节点组，然后再基于对应的共享密钥进行加密。

在源区块链节点响应于组播或者广播任务时，不一定会触发执行本说明书实施例涉及的消息传输方法，这是由于组播和广播任务虽然都是将同一消息发送至至少两个区块链节点，符合明文消息对应的目的区块链节点包括至少两个区块链节点的条件，但本案的触发条件实际上为明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点，也就是说，本说明书实施所涉及的消息传输方法不仅依赖于执行组播或者广播任务的场景，还需要确保作为目的区块链节点的至少两个区块链节点与源区块链节点同属于一个区块链节点组，均为同一区块链节点组内的节点成员。因此，针对一个组播或者广播任务，源区块链节点首先会确定待发送的明文消息以及待发往的目的区块链节点，通过查找本地维护的区块链节点组的成员列表以在确定与目的区块链节点共同所属的一个区块链节点组后，才会根据确定得到的区块链节点组对应的共享密钥对明文消息进行加密以得到加密消息，最终将加密消息发送至包含至少两个区块链节点的目的区块链节点。

需要说明的是，目的区块链节点中包含的所有区块链节点不一定全都与源区块链节点同属一个区块

链节点组，目的区块链节点中的各区块链节点完全有可能同时涉及多个区块链节点组，或者不属于任何区块链节点组。以图 3 为例，图 3 是一示例性实施例提供的一种源区块链节点进行广播的场景示意图，其中源区块链节点为图中的区块链节点 A，目的区块链节点包含区块链节点 B~H 共 7 个区块链节点，可以发现，目的区块链节点中的区块链节点 B、C、D 与区块链节点 A 同属于区块链节点组 1，这意味着区块链节点 A、B、C、D 共同维护有区块链节点组 1 对应的共享密钥，而目的区块链中的区块链节点 E 不属于任何区块链节点组，区块链节点组 F 则虽然属于区块链节点组 3，但区块链节点组 3 的节点成员中并不包含至少两个目的区块链节点，也没有包含区块链节点 A，因此这部分不会触发执行本说明书所涉及的消息传输方法，而区块链节点 G、H 则与区块链节点 A 同属于区块链节点组 2，共同维护有区块链节点组 2 对应的共享密钥，于是，区块链节点 A 在执行向区块链节点 B~H 广播消息过程中，会基于目的区块链节点首先检索自身维护的区块链节点组的成员列表，并在确定区块链节点 B、C、D 与区块链节点 A 同属于区块链节点组 1，而区块链节点 G、H 与区块链节点 A 同属于区块链节点组 2 后，将明文消息分别基于区块链节点组 1 对应的共享密钥进行加密后发送至区块链节点 B、C、D，并将明文消息再基于区块链节点组 2 对应的共享密钥进行加密后发送至区块链节点 G、H，至于区块链节点 E 和 F，则需要利用区块链节点 A 与它们单独建立的加密信道对明文消息进行加密传输，因此，区块链节点 A 对明文消息一共进行了 4 次加密计算，相较于传统方法中分别根据与每个目的区块链节点所建立的加密信道来分别加密传输相比（需要对明文消息进行 7 次加密计算）明显具有更低的计算消耗。

可选的，所述基于所述共享密钥对所述明文消息进行加密以获取加密消息，包括：基于所述明文消息包含的安全参数索引，确定对应于所述安全参数索引的安全关联策略；基于所述安全关联策略中包含的所述共享密钥对所述明文消息进行加密以获取所述加密消息。在本说明书实施例中，如果源区块链节点确定明文消息对应的目的区块链节点包括至少两个区块链节点且所述至少两个区块链节点与源区块链节点同属于一个区块链节点组，此时源区块链节点将按照预设的协议例如 IPsec 协议对待发送的明文消息进行封装，为其添加 SPI（security parameters index，安全参数索引）字段后交付源区块链节点中的加密计算模组进行进一步加密处理，加密计算模组在接收到携带有 SPI 的明文消息后，会根据该 SPI 检索本地预先维护的 SA（security assist，安全关联策略），然后根据检索得到的 SA 中包含的共享密钥（即确定的区块链节点组对应的共享密钥）对明文消息进行加密以获取加密消息并将携带有 SPI 的加密消息发送至目的区块链节点，目的区块链接收到携带有 SPI 的加密消息后，可以通过加密消息所携带的 SPI 字段检索本地预先维护的 SA，然后根据检索得到的 SA 中包含的共享密钥（即确定的区块链节点组对应的共享密钥）对密文消息进行解密以获取明文消息。本说明书实施例相当于在源区块链节点与目的区块链节点之间建立了新的加密信道以实现本说明书实施例所涉及的消息传输方法。

可选的，所述源区块链节点维护的与所述至少两个区块链节点之间分别建立的至少两个点对点加密信道对应的至少两个专用密钥均为所述共享密钥；所述基于所述共享密钥对明文消息进行加密以获取加密消息，包括：基于所述至少两个专用密钥中的任一密钥，对明文消息进行加密以获取所述加密消息；所述将所述加密消息发送至所述至少两个区块链节点，包括：分别确定与所述至少两个区块链节点之间建立的点对点加密信道，将所述加密消息基于相应的点对点加密信道分别发送至所述至少两个区块链节点。在本说明书实施例中，源区块链节点与所述至少两个区块链节点之间分别单独建立有点对点加密信道，如前所述，这些点对点加密信道彼此之间是独立的，具有不同的专用密钥，然而，本说明书实施例通过使得源区块链节点所属区块链节点组中的各区块链节点进行密钥协商，而使得各区块链节点维护有

相同的共享密钥后，每个区块链节点都会将其维护的与同区块链节点组内其他区块链节点建立的点对点加密信道对应的专用密钥替换为共享密钥，从而使得区块链节点组内各区块链节点之间的通讯将仅使用共享密钥进行加解密，从而实现了区块链节点组内加密信道的密钥关联，同时，为了避免重复加密，本说明书实施例还提供了新的加密策略，即在检测到作为目的区块链节点的至少两个区块链节点与源区块链节点同属一个区块链节点组的情况下，虽然会按照原始的加密信道对进行明文消息进行加密后传输，但是多个加密信道对应的独立的加密过程将被合并，例如图 1 中 Node A 向与 Node A 同属于一个区块链节点组的 Node B 和 Node C 发送消息时，传统方案需要将明文消息先通过 Node A 与 Node B 之间的加密信道 tunnel_AB 对明文消息进行一次加密，然后还需要通过 Node A 与 Node C 之间的加密信道 tunnel_AC 对明文消息再进行一次加密，然而在本说明书实施例中，由于 tunnel_AB 与 tunnel_AC 对应的密钥已经关联，其对应的密钥相同均为 Node A、Node B 和 Node C 所属的区块链节点组对应的共享密钥，因此不需要进行两次重复加密过程，而是将加密过程合并为一次，得到的加密消息再分别通过于 tunnel_AB 与 tunnel_AC 发送至 Node B 和 Node C。本说明书实施例通过对原本彼此独立的多个加密信道进行密钥关联和加密过程合并，从而基于传统加密信道的架构实现了本说明书实施例所涉及的消息传输方法，而无需重新建立新的加密信道。

可选的，所述至少两个专用密钥于所述源区块链节点的密钥存储地址均为所述共享密钥于所述源区块链节点的密钥存储地址。在传统的密钥存储策略中，不同点对点加密信道中的专用密钥会独占一份存储空间，而由于本说明书实施例已经将源区块链节点与所述至少两个区块链节点之间的点对点加密信道中的专用密钥均替换为相同的共享密钥，因此对于源区块链节点而言，如果依然采用传统高的存储策略将造成信息冗余。因此，可以在将专用密钥替换为共享密钥时，仅对不同点对点加密信道的密钥存储地址进行修改，以将它们统一为共享密钥所在的密钥存储地址，然后将原本独立存储的各点对点加密信道对应的各专用密钥进行删除以释放存储空间，降低源区块链节点的存储消耗。

S204：将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

如前所述，由于所述至少两个区块链节点与源区块链节点处于同一区块链节点组，同时维护有相同的共享密钥，因此，任一目的区块链节点在接收到加密消息后，都将基于所述共享密钥对加密消息进行解密以最终获取明文消息，至此实现本说明书实施例锁所涉及的消息传输方案的全流程。

在本说明书实施例中，源区块链节点在进行广播或组播时，由于源区块链节点与目的区块链节点中至少两个区块链节点共同维护有相同的共享密钥，因此源区块链节点可以使用共享密钥对明文消息进行一次加密后发送给所述至少两个区块链节点，从而降低组播或广播场景中对明文消息的加密次数，在确保通讯安全前提下减少源区块链节点的计算负担，提高区块链节点之间的加密通信效率。

如前所述，源区块链节点需要通过查找本地维护的区块链节点组的成员列表来确定目的区块链节点中是否存在至少两个区块链节点与源区块链节点同属于一个区块链节点组，然而，源区块链节点或目的区块链节点都有可能暂时缺失区块链节点组的成员列表，这使得虽然源区块链节点或目的区块链节点在客观上同属于一个区块链节点组，但源区块链节点和目的区块链节点却无从知晓，从而导致无法适用本说明书实施例所涉及的消息传输方法。为此，有必要设计一种消息交互方式来使得源区块链节点能够在区块链节点组残缺的情况下依然可以确认目的区块链节点是否与源区块链节点是否同属于一个区块链节点组。

在一实施例中，源区块链节点仅维护有自身所属的多个区块链节点组对应的多个共享密钥，而未维护这些区块链节点组的成员列表，或者虽然维护有成员列表但这些成员列表中不包含目的区块链节点的身份标识信息，需要指出的是，区块链节点组的成员列表中未包含某区块链节点不代表该区块链节点一定不属于该区块链节点组，因为有可能是暂时未确定到导致的，这意味着如果源区块链节点需要向目的区块链节点发送明文消息，则无法通过节点ID、节点公钥、网络地址等目的区块链节点的身份标识信息确定自身与目的区块链节点共同所属的区块链节点组，因此，在这种情况下，源区块链节点仅能确定目的区块链节点的网络地址而无法确定是否存在与目的区块链节点共同所属的区块链节点组，源区块链节点会将自身维护的全部区块链节点组对应的多个共享密钥分别对明文消息进行加密以获取多个加密消息，然后将这多个加密消息按照目的区块链节点的网络地址一同发送至目的区块链节点，目的区块链节点的数量可以为多个，例如为了配合前述的消息传输方法，这里的目的区块链节点可以为所述明文消息对应的所有目的区块链节点。由此，目的区块链节点如果也无法判断源区块链节点与其所同属的区块链节点，就可以按照自身维护的至少一个区块链节点组对应的共享密钥逐一解密接收到的多个加密消息，例如，目的区块链节点共维护有两个区块链节点组，对应的共享密钥分别为key_1和key_2，同时目的区块链节点共接收到3个加密消息，分别为msg_1、msg_2和msg_3，那么目的区块链节点就会先后使用key_1和key_2分别尝试对msg_1、msg_2和msg_3进行解密，即最多需要进行六次解密，而在上述解密过程中如果有至少一个加密消息被成功解密，例如msg_2通过key_2成功解密得到明文消息，那么目的区块链节点就会知晓自身与源区块链节点同属于key_2对应的区块链节点组，因此可以在本地维护的key_2对应的区块链节点组的成员列表中写入源区块链节点的身份标识信息。

而为了进一步方便后续与源区块链节点之间进行通信，当目的区块链节点成功识别与源区块链节点共同所属的区块链节点组后，还会进一步向源区块链节点告知该区块链节点组，从而使源区块链节点能够确定目的区块链节点与其同属的区块链节点组，由此源区块链节点后续在需要向目的区块链节点发送明文消息时，就可以直接查询到与其同属的区块链节点组并基于该区块链节点组对应的共享密钥对明文消息进行加密以获取加密消息，而无需进行多次加密以生成多个加密消息，避免浪费计算和网络资源。

目的区块链节点可以采取多种方式向源区块链节点告知与其共同所属的区块链节点组。例如，目的区块链节点可以直接向源区块链节点返回对应区块链节点组的组ID，其中，任一区块链节点组的组ID可以包括：事先约定或公开的该任一区块链节点组的标识信息、该任一区块链节点组对应的共享密钥或基于该共享密钥生成的密钥标识簇中的任一密钥标识，密钥标识簇中的每一个密钥标识都是通过共享密钥对共享密钥进行有限次的加密或解密得到的。但这种方式可能会泄露区块链节点组的组ID，因此存在安全隐患；

或者，目的区块链节点可以向源区块链节点返回基于共同所属区块链节点组对应共享密钥加密后的该区块链节点组的组ID；

或者，目的区块链节点可以向源区块链节点返回之前从源区块链节点接收的多个加密消息中解密成功的加密消息，例如目的区块链节点向源区块链节点返回msg_2,此时源区块链节点就能够因此确定当初加密得到msg_2所使用的共享密钥key_2，同时确定得到key_2对应的区块链节点组，由此将目的区块链节点的身份标识信息加入该区块链节点组的成员列表，该方式虽然不会在传输层泄露信息明文，但是假设攻击者同时捕获了源区块链节点之前向目的区块链节点发送的多个加密消息以及目的区块链节点返回的加密消息，就能够因此确定源区块链节点与目的区块链节点至少同属于一个区块链节点组；

或者，目的区块链节点可以先对之前从源区块链节点接收的多个加密消息中解密成功的加密消息按照与源区块链节点共同所属区块链节点组对应共享密钥进行重加密以获取二重加密消息，然后将该二重加密消息返回源区块链节点，而假如从源区块链节点接收的多个加密消息都无法解密，仍然向源区块链节点返回与上述二重加密消息具有相同数据格式但内容随机生成的乱码消息，这样一来，对于源区块链节点而言，其可以预先分别计算出其之前向目的区块链节点发送的多个加密消息对应的二重加密消息（通过计算出某一加密消息的共享密钥对该某一加密消息再进行加密以获得），从而维护得到一个“区块链节点组-共享密钥-加密消息-二重加密消息”四者之间的对应关系，这使得源区块链节点可以基于从目的区块链节点所接收到的二重加密消息来直接确定出对应的区块链节点组，从而将其认定为共同所属的区块链节点组，而当源区块链节点无法从已有的对应关系中匹配出目的区块链节点所发出的二重加密消息的情况下，就可以认定该二重加密消息实则是目的区块链节点随机生成的乱码消息，于是可以得出目的区块链节点与源区块链节点不同属于任何一个区块链节点组。而对于攻击者而言，由于该二重加密消息并未出现在源区块链节点发送的多个加密消息中，用于表征“源区块链节点与目的区块链节点至少同属于一个区块链节点组”的二重加密与用于表征“源区块链节点与目的区块链节点不同属于任何一个区块链节点组”的乱码消息二者之间是无法区分的，因此攻击者无法基于截获的消息本身推断出任何结论，从而保护了传输过程的理论安全性，以对抗针对密文结构进行分析的侧信道攻击。

如前所述，源区块链节在无法确定是否存在与目的区块链节点共同所属的区块链节点组的情况下，源区块链节点会将自身维护的全部区块链节点组对应的多个共享密钥分别对明文消息进行加密以获取多个加密消息，然后将多个加密消息发送至目的区块链节点，然而，这种方式依然会泄露信息：攻击者通过截获包含多个加密消息的报文，虽然攻击者无法通过多个加密消息反推出明文消息，但却可以根据多个加密消息的数量来反推出源区块链节点所属的区块链节点组的数量（等于多个加密消息的数量），这构成了还原区块链节点组的成员列表的参考信息，客观上也会带来安全隐患。而为了避免上述问题，源区块链节点除了发送通过自身维护的所有共享密钥对明文消息分别进行加密得到的加密消息外，还会发送额外随机生成的乱码消息，这样一来，源区块链节点发送至目的区块链节点的所有消息中就不仅包含正常通过共享密钥加密得到的多个加密消息，还会混入有随机数量的乱码消息，由于对于攻击者而言无法区分乱码消息与加密消息，因此这种做法可以对攻击者掩盖多个加密消息的数量，以对抗针对加密消息数量的侧信道攻击。

在一实施例中，目的区块链节点会进一步将自身维护的更新后的该区块链节点组的成员列表通过该区块链节点组对应的共享密钥加密后返回源区块链节点，以指示源区块链节点更新对应区块链节点组的成员列表，虽然源区块链节点所接收到的成员列表是通过共享密钥加密后的密文列表，但源区块链节点可以通过前述方法获知其与目的区块链节点所同属的区块链节点组，这意味着源区块链节点无需按照自身所维护的多个区块链节点组对应的共享密钥逐一对该密文列表进行解密以获取成员列表，而是可以直接基于确定得到的与目的区块链节点同属的区块链节点组对应的共享密钥对密文列表进行解密，节省了计算资源的消耗。

目的区块链节点在利用共享密钥加密得到加密消息后，还会进一步根据与区块链中继通信网络系统之间建立的第一加密信道对应的第一密钥进行加密以获取第一重加密消息，再通过第一加密信道向区块链中继通信网络系统发送该第一重加密消息，从而使得外部攻击者不仅受到基于区块链节点组对应的共享密钥的加密策略的制约，还会进一步受到基于源区块链节点与区块链网络通信系统之间特定加密信道

的加密策略的制约（第一加密信道对应的相关密钥仅由源区块链节点与区块链中继通信网络系统所掌握），因此，即使攻击者通过外部手段获取了源区块链节点与目的区块链节点共同所属区块链节点组的共享密钥，只要没有进一步控制源区块链节点或区块链中继通信网络系统中的关键中继节点，也依然无法通过截获第一重加密消息来还原得到明文消息，从而能够确保系统的安全性。

可选的，所述共享密钥通过所述区块链节点组中的各区块链节点进行组密钥协商以维护于所述各区块链节点。在本说明书实施例中，同属于一个区块链节点组中的各区块链节点通过事先进行组密钥协商实现共同维护有共享密钥。组密钥协商不同于两个对等体之间的端到端的密钥协商，而是指至少三个对等体之间的密钥协商，其目的在于通过线上交互的方式，使至少三个对等体共同维护有相同的共享密钥，同时避免该共享密钥泄露给除是所述至少三个对等体以外的第三方。本说明书实施例所涉及的端到端的密钥协商对应的协议可以包括 TLS 协议、IKE（Internet key exchange，网络密钥交换协议）协议、DH（Diffie-Hellman）密钥交换协议等，本说明书对此并不做限制。

可选的，所述区块链节点组中的各区块链节点进行组密钥协商，包括：所述区块链节点组中的主节点分别与所述区块链节点组中除所述主节点以外的其他区块链节点通过密钥协商以共同维护所述共享密钥。在本说明书实施例中，提供了一种组密钥协商的方法，在该方法中，首先需要在区块链节点组中确定一个主节点作为组密钥协商的主持者，然后，主节点会与所述区块链节点组中除所述主节点以外的其他区块链节点（从节点）分别进行端到端的密钥协商。例如在图 1 所示的场景，假设 Node A 作为主节点且希望组建一个包含 Node A、Node B 与 Node C 的区块链节点组，那么 Node A 可以依次或同时分别与 Node B 和 Node C 进行密钥协商，并且使 Node B 在密钥协商后所维护的共享密钥与 Node C 在密钥协商后所维护的共享密钥相同，同时 Node A 自身也会维护有该共享密钥，从而最终使得 Node A、Node B 与 Node C 维护有相同的共享密钥，从而共同参与组成一个新的区块链节点组。

可选的，所述主节点与所述其他区块链节点中的任一区块链节点（从节点）进行组密钥协商，包括：所述主节点与所述任一区块链节点通过 DH 密钥交换协议生成并维护所述共享密钥；或者，所述主节点与所述任一区块链节点通过 DH 密钥交换协议共同维护会话密钥，并将所述主节点生成的所述共享密钥基于所述会话密钥加密后发送至所述任一区块链节点，所述任一区块链节点用于将加密后的所述共享密钥基于所述会话密钥进行解密以获取所述共享密钥。在本说明书实施例中，主节点在与任一从节点进行密钥协商时，都可以直接或间接基于 DH 密钥交换协议来实现共同维护相同的共享密钥，DH 密钥交换协议是一类在不安全网络中生成对称密钥的方案，其主要通过两个密钥协商方之间相互公开生成元和可公开计算值的方式，使每一密钥协商方都能计算出只有密钥协商方才能获知的相同的密钥种子，从而进一步基于相同的密钥种子生成并维护相同的对称密钥。

在一实施例中，主节点与从节点之间可以将彼此之间通过 DH 密钥交换协议直接生成的密钥作为共享密钥，从而使得主节点与该从节点之间维护相同的共享密钥，但由于每次通过 DH 密钥交换协议得到的共享密钥是不确定的，因此为了确保主节点与其他所有从节点均维护有相同的共享密钥，这种直接通过 DH 密钥协商协议来直接生成共享密钥的做法通常只会用在主节点进行组密钥协商过程中与第一个从节点进行密钥协商时，而后续则需要采用其他方式来确保所有从节点均能维护相同的共享密钥。

在另一实施例中，主节点与从节点之间可以首先将 DH 密钥交换协议直接生成的密钥作为会话密钥，以用于后续进行加密通信，此时主节点就能够将随机生成的对称密钥作为共享密钥（或与第一个从节点通过密钥协商生成的共享密钥）并通过会话密钥加密后发送给从节点，从而使得从节点根据自身维护的

会话密钥解密得到共享密钥，并且由于 DH 密钥交换协议直接生成的会话密钥并不直接作为共享密钥，而是作为构建加密通信的基础，这使得区块链节点组中的每个从节点均可通过该方式维护相同的共享密钥，从而最终实现组密钥协商。

可选的，所述共享密钥和/或所述会话密钥记录在所述主节点与所述任一区块链节点维护的安全关联策略中。为了区分不同的加密策略，同时有效地安排密钥协商的流程，因此需要对不同类型的消息施加以不同的安全关联策略，以使其按照规定的方式进行加密，本说明书实施例所涉及的安全关联策略具体是指 IKE 协议中的 SA(security assist)，不同 SA 可以通过待处理消息上的 SPI(security parameters index，安全参数索引）字段进行索引。例如，用于进行密钥协商的消息（如 DH 密钥协商过程中发送的消息）就可以被设置为通过会话密钥进行加密，因此这类消息对应的报文上的相关索引字段将指向使用会话密钥进行加解密的安全关联策略；而用于进行普通通讯的消息就可以被设置为通过共享密钥进行加密，因此这类消息对应的报文上的相关索引字段将指向使用共享密钥进行加解密的安全关联策略。

可选的，所述主节点与所述其他区块链节点中的任一区块链节点（从节点）进行组密钥协商，包括：所述主节点生成所述共享密钥，并将所述共享密钥基于所述任一区块链节点的公钥加密得到的密文密钥发送至所述任一区块链节点；所述任一区块链节点将所述密文密钥基于所述任一区块链节点的私钥进行解密以获取所述共享密钥。在本说明书实施例中，通过非对称加密特性来实现主节点与从节点之间密钥协商的工作，同时避免在密钥协商的过程中向其他第三方泄露共享密钥，从而在进一步实现组密钥协商。

可选的，还包括：所述其他任一区块链节点将所述共享密钥基于所述主节点公钥加密后返回所述主节点；所述主节点在基于所述主节点的私钥对从所述其他任一区块链节点获取的加密后的所述共享密钥进行解密得到所述共享密钥的情况下，确定与所述其他任一区块链节点的密钥协商已完成。在从节点解密得到共享密钥后，虽然客观上主节点与从节点此刻均已维护有相同的共享密钥，但主节点其实在未接收到相关证明的情况下无法确定从节点已经维护有共享密钥，因此为了使主节点能够确定参与某一次密钥协商的从节点确实已经获取了共享密钥，可以让从节点在解密得到共享密钥后，进一步使用主节点的公钥进行加密后返回至主节点，而主节点解密得到共享密钥后，便可以确定该从节点已经成功获取共享密钥，从而方便安排进行后续的密钥协商任务，或确定组密钥协商已经完成（在确定区块链节点组中所有从节点均维护有共享密钥的情况下）。

可选的，还包括：所述主节点基于所述主节点的私钥为所述密文密钥生成数字签名，并将所述数字签名发送至所述任一区块链节点；所述任一区块链节点基于所述主节点的公钥对所述数字签名进行验签，在验签成功的情况下确定所述密文密钥来源于所述主节点。在本说明书实施例中，为了使从节点能够验证主节点的身份，防止其他第三方假冒主节点与从节点进行密钥验证，可以利用数字签名技术，使主节点对密文密钥进行数字签名，而后从节点对数字签名进行验签，并在验签成功的情况下确定密文密钥来源的合法性，同时还可以确保密文密钥在传输过程中未被篡改。

本说明书实施例所涉及的消息传输方法可以基于网络层协议实现，也可以基于应用层协议实现，本说明书对此并不做任何限制。而当基于网络层协议实现时，该网络层协议可以是 IPsec（Internet Protocol Security，互联网安全协议），此时基于共享密钥的加解密过程和相应的解密过程均发生在网络层，其对转发效率具有较小的性能损耗，这是由于网络层中加密的对象为 IP 报文，而应用层中加密的对象为应用程序定义的数据结构体，因此网络层加密相较于应用层加密而言，由于 IP 报文属于轻量级的信息载体，因此加密任务的细粒度更小，不需要消耗大量的计算资源，同时基于网络层协议实现的加密方案

在信息传递的环节上更少，具有更高的执行效率，另外网络层加密能够适配不同的上层架构，例如被不同的应用所共同享有和利用，从而体现为一种高适配性。

图 4 是一示例性实施例提供的一种设备的示意结构图。请参考图 4，在硬件层面，该设备包括处理器 402、内部总线 404、网络接口 406、内存 408 以及非易失性存储器 410，当然还可能包括其他功能所需要的硬件。本说明书一个或多个实施例可以基于软件方式来实现，比如由处理器 402 从非易失性存储器 410 中读取对应的计算机程序到内存 408 中然后运行。当然，除了软件实现方式之外，本说明书一个或多个实施例并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

如图 5 所示，图 5 是一示例性实施例提供的一种消息传输装置的框图，该装置可以应用于如图 4 所示的设备中，以实现本说明书的技术方案；所述装置应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述装置包括：

加密单元 501，用于在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息。

发送单元 502，用于将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

可选的，所述加密单元 501 具体用于：

基于所述明文消息包含的安全参数索引，确定对应于所述安全参数索引的安全关联策略；

基于所述安全关联策略中包含的所述共享密钥对所述明文消息进行加密以获取所述加密消息。

可选的，所述源区块链节点维护的与所述至少两个区块链节点之间分别建立的至少两个点对点加密信道对应的至少两个专用密钥均为所述共享密钥；

所述加密单元 501 具体用于：

基于所述至少两个专用密钥中的任一密钥，对明文消息进行加密以获取所述加密消息；

所述发送单元 502 具体用于：

分别确定与所述至少两个区块链节点之间建立的点对点加密信道，将所述加密消息基于相应的点对点加密信道分别发送至所述至少两个区块链节点。

可选的，所述至少两个专用密钥于所述源区块链节点的密钥存储地址均为所述共享密钥于所述源区块链节点的密钥存储地址。

可选的，所述共享密钥通过所述区块链节点组中的各区块链节点进行组密钥协商以维护于所述各区块链节点。

可选的，所述区块链节点组中的各区块链节点进行组密钥协商，包括：

所述区块链节点组中的主节点分别与所述区块链节点组中除所述主节点以外的其他区块链节点通过密钥协商以共同维护所述共享密钥。

可选的，所述主节点与所述其他区块链节点中的任一区块链节点进行密钥协商，包括：

所述主节点与所述任一区块链节点通过 DH 密钥交换协议生成并维护所述共享密钥；或者，

所述主节点与所述任一区块链节点通过 DH 密钥交换协议共同维护会话密钥，并将所述主节点生成

的所述共享密钥基于所述会话密钥加密后发送至所述任一区块链节点，所述任一区块链节点用于将加密后的所述共享密钥基于所述会话密钥进行解密以获取所述共享密钥。

可选的，所述共享密钥和/或所述会话密钥记录在所述主节点与所述任一区块链节点维护的安全关联策略中。

可选的，所述主节点与所述其他区块链节点中的任一区块链节点进行密钥协商，包括：

所述主节点生成所述共享密钥，并将所述共享密钥基于所述任一区块链节点的公钥加密得到的密文密钥发送至所述任一区块链节点；

所述任一区块链节点将所述密文密钥基于所述任一区块链节点的私钥进行解密以获取所述共享密钥。

可选的，还包括：

所述主节点基于所述主节点的私钥为所述密文密钥生成数字签名，并将所述数字签名发送至所述任一区块链节点；

所述任一区块链节点基于所述主节点的公钥对所述数字签名进行验签，在验签成功的情况下确定所述密文密钥来源于所述主节点。

可选的，所述区块链节点组中的各区块链节点处于相同的区块链网络或不同的区块链网络。

可选的，所述不同的区块链网络之间彼此同构或异构。

可选的，所述装置基于网络层协议实现。

在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进（例如，对二极管、晶体管、开关等电路结构的改进）还是软件上的改进（对于方法流程的改进）。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件（Programmable Logic Device, PLD）（例如现场可编程门阵列（Field Programmable Gate Array，FPGA））就是这样一种集成电路，其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上，而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且，如今，取代手工地制作集成电路芯片，这种编程也多半改用“逻辑编译器（logic compiler）”软件来实现，它与程序开发撰写时所用的软件编译器相类似，而要编译之前的原始代码也得用特定的编程语言来撰写，此称之为硬件描述语言（Hardware Description Language，HDL），而HDL也并非仅有一种，而是有许多种，如ABEL（Advanced Boolean Expression Language）、AHDL（Altera Hardware Description Language）、Confluence、CUPL（Cornell University Programming Language）、HDCal、JHDL（Java Hardware Description Language）、Lava、Lola、MyHDL、PALASM、RHDL（Ruby Hardware Description Language）等，目前最普遍使用的是VHDL（Very-High-Speed Integrated Circuit Hardware Description Language）与Verilog。本领域技术人员也应该清楚，只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中，就可以很容易得到实现该逻辑方法流程的硬件电路。

控制器可以按任何适当的方式实现，例如，控制器可以采取例如微处理器或处理器以及存储可由该（微）处理器执行的计算机可读程序代码（例如软件或固件）的计算机可读介质、逻辑门、开关、专用集成电路（Application Specific Integrated Circuit，ASIC）、可编程逻辑控制器和嵌入微控制器的形式，

控制器的例子包括但不限于以下微控制器：ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20 以及 Silicone Labs C8051F320，存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道，除了以纯计算机可读程序代码方式实现控制器以外，完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件，而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至，可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

上述实施例阐明的系统、装置、模块或单元，具体可以由计算机芯片或实体实现，或者由具有某种功能的产品来实现。一种典型的实现设备为服务器系统。当然，本发明不排除随着未来计算机技术的发展，实现上述实施例功能的计算机例如可以为个人计算机、膝上型计算机、车载人机交互设备、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

虽然本说明书一个或多个实施例提供了如实施例或流程图所述的方法操作步骤，但基于常规或者无创造性的手段可以包括更多或者更少的操作步骤。实施例中列举的步骤顺序仅仅为众多步骤执行顺序中的一种方式，不代表唯一的执行顺序。在实际中的装置或终端产品执行时，可以按照实施例或者附图所示的方法顺序执行或者并行执行(例如并行处理器或者多线程处理的环境，甚至为分布式数据处理环境)。术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、产品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、产品或者设备所固有的要素。在没有更多限制的情况下，并不排除在包括所述要素的过程、方法、产品或者设备中还存在另外的相同或等同要素。例如若使用到第一，第二等词语用来表示名称，而并不表示任何特定的顺序。

为了描述的方便，描述以上装置时以功能分为各种模块分别描述。当然，在实施本说明书一个或多个时可以把各模块的功能在同一个或多个软件和/或硬件中实现，也可以将实现同一功能的模块由多个子模块或子单元的组合实现等。以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

本发明是参照根据本发明实施例的方法、装置（系统）、和计算机程序产品的流程图和／或方框图来描述的。应理解可由计算机程序指令实现流程图和／或方框图中的每一流程和／或方框、以及流程图和／或方框图中的流程和／或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和／或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程

设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

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。计算机的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(RAM)、只读存储器(ROM)、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、只读光盘只读存储器(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、石墨烯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。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

本领域技术人员应明白，本说明书一个或多个实施例可提供为方法、系统或计算机程序产品。因此，本说明书一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本说明书一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本说明书一个或多个实施例可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本本说明书一个或多个实施例，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本说明书的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，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例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例或示例以及不同实施例或示例的特征进行结合和组合。

以上所述仅为本说明书一个或多个实施例的实施例而已，并不用于限制本本说明书一个或多个实施例。对于本领域技术人员来说，本说明书一个或多个实施例可以有各种更改和变化。凡在本说明书的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在权利要求范围之内。

权 利 要 求

1、一种消息传输方法，应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述方法包括：

在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息；

将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

2、根据权利要求 1 所述的方法，所述基于所述共享密钥对所述明文消息进行加密以获取加密消息，包括：

基于所述明文消息包含的安全参数索引，确定对应于所述安全参数索引的安全关联策略；

基于所述安全关联策略中包含的所述共享密钥对所述明文消息进行加密以获取所述加密消息。

3、根据权利要求 1 所述的方法，所述源区块链节点维护的与所述至少两个区块链节点之间分别建立的至少两个点对点加密信道对应的至少两个专用密钥均为所述共享密钥；

所述基于所述共享密钥对明文消息进行加密以获取加密消息，包括：

基于所述至少两个专用密钥中的任一密钥，对明文消息进行加密以获取所述加密消息；

所述将所述加密消息发送至所述至少两个区块链节点，包括：

分别确定与所述至少两个区块链节点之间建立的点对点加密信道，将所述加密消息基于相应的点对点加密信道分别发送至所述至少两个区块链节点。

4、根据权利要求 3 所述的方法，所述至少两个专用密钥于所述源区块链节点的密钥存储地址均为所述共享密钥于所述源区块链节点的密钥存储地址。

5、根据权利要求 1 所述的方法，所述共享密钥通过所述区块链节点组中的各区块链节点进行组密钥协商以维护于所述各区块链节点。

6、根据权利要求 5 所述的方法，所述区块链节点组中的各区块链节点进行组密钥协商，包括：

所述区块链节点组中的主节点分别与所述区块链节点组中除所述主节点以外的其他区块链节点通过密钥协商以共同维护所述共享密钥。

7、根据权利要求 6 所述的方法，所述主节点与所述其他区块链节点中的任一区块链节点进行密钥协商，包括：

所述主节点与所述任一区块链节点通过 DH 密钥交换协议生成并维护所述共享密钥；或者，

所述主节点与所述任一区块链节点通过 DH 密钥交换协议共同维护会话密钥，并将所述主节点生成的所述共享密钥基于所述会话密钥加密后发送至所述任一区块链节点，所述任一区块链节点用于将加密后的所述共享密钥基于所述会话密钥进行解密以获取所述共享密钥。

8、根据权利要求 7 所述的方法，所述共享密钥和/或所述会话密钥记录在所述主节点与所述任一区块链节点维护的安全关联策略中。

9、根据权利要求 6 所述的方法，所述主节点与所述其他区块链节点中的任一区块链节点进行密钥协商，包括：

所述主节点生成所述共享密钥，并将所述共享密钥基于所述任一区块链节点的公钥加密得到的密文密钥发送至所述任一区块链节点；

所述任一区块链节点将所述密文密钥基于所述任一区块链节点的私钥进行解密以获取所述共享密钥。

10、根据权利要求 9 所述的方法，还包括：

所述主节点基于所述主节点的私钥为所述密文密钥生成数字签名，并将所述数字签名发送至所述任一区块链节点；

所述任一区块链节点基于所述主节点的公钥对所述数字签名进行验签，在验签成功的情况下确定所述密文密钥来源于所述主节点。

11、根据权利要求 1 所述的方法，所述区块链节点组中的各区块链节点处于相同的区块链网络或不同的区块链网络。

12、根据权利要求 10 所述的方法，所述不同的区块链网络之间彼此同构或异构。

13、根据权利要求 1 所述的方法，所述方法基于网络层协议实现。

14、一种消息传输装置，应用于源区块链节点，所述源区块链节点所属的区块链节点组中的各区块链节点均维护有相同的共享密钥；所述装置包括：

加密单元，用于在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息；

发送单元，用于将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息。

15、一种电子设备，包括：

处理器；

用于存储处理器可执行指令的存储器；

其中，所述处理器通过运行所述可执行指令以实现如权利要求 1-13 中任一项所述的方法。

16、一种计算机可读存储介质，其上存储有计算机指令，该指令被处理器执行时实现如权利要求 1-13 中任一项所述方法的步骤。

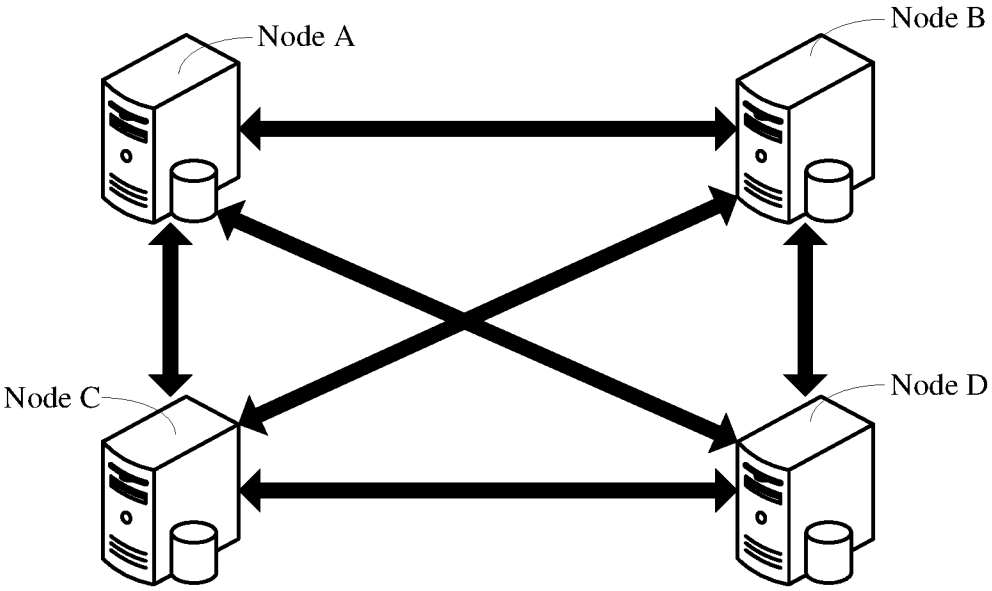
Node A
Node B
Node C
Node D

图 1

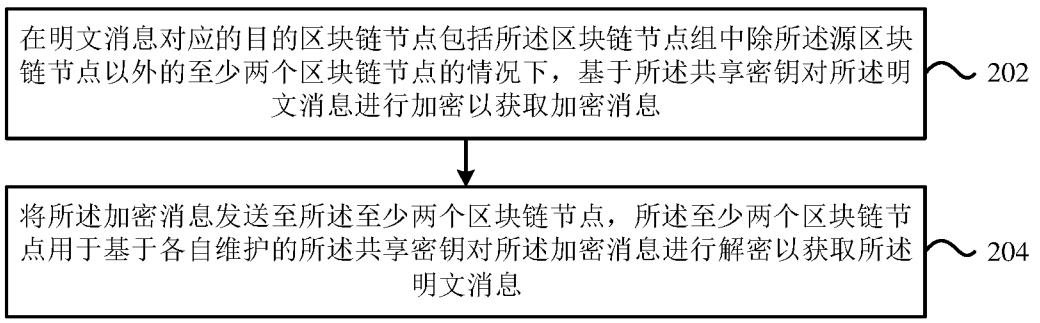
在明文消息对应的目的区块链节点包括所述区块链节点组中除所述源区块链节点以外的至少两个区块链节点的情况下，基于所述共享密钥对所述明文消息进行加密以获取加密消息
202
将所述加密消息发送至所述至少两个区块链节点，所述至少两个区块链节点用于基于各自维护的所述共享密钥对所述加密消息进行解密以获取所述明文消息
204

图 2

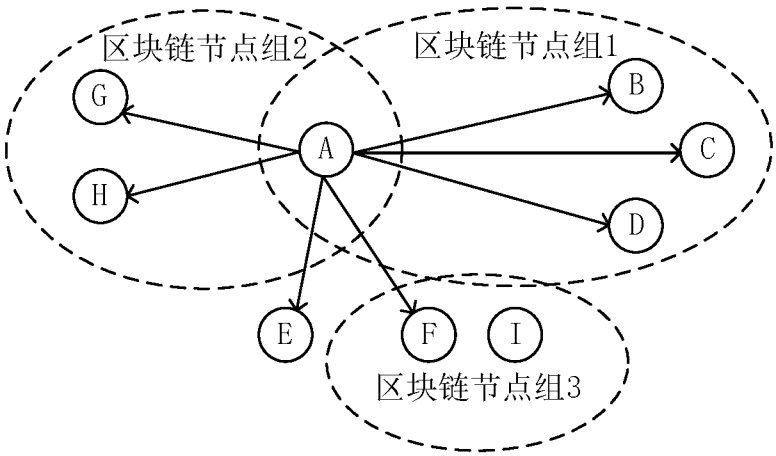
区块链节点组2
区块链节点组1
G
B
A
C
H
D
E
F
I
区块链节点组3

图 3

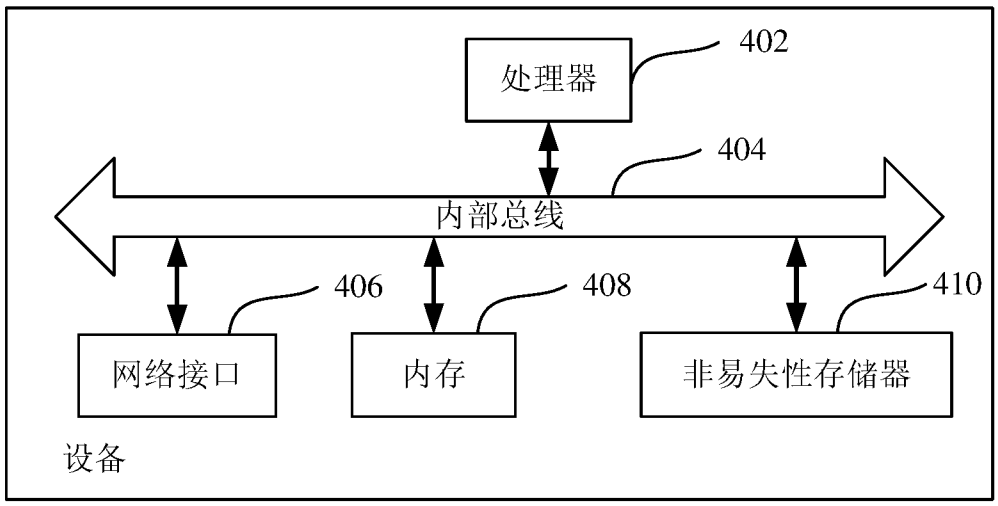
处理器
402
404
内部总线
406
408
410
网络接口
内存
非易失性存储器
设备

图 4


加密单元
501
发送单元
502

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/135607

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/40(2022.01)i; H04L 9/08(2006.01)i; H04L 67/10(2022.01)i; H04L 67/104(2022.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNPAT, CNKI, WPI, EPODOC, 3GPP: 区块链 组 组播 加密 目标 目的 源 block chain blockchain key group+ groupcast+ source destinat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115174188 A (ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.) 11 October 2022 (2022-10-11) claims 1-16	1-16
X	CN 114285555 A (ALIPAY (HANGZHOU) INFORMATION TECHNOLOGY CO., LTD. et al.) 05 April 2022 (2022-04-05) description, paragraphs [0028]-[0108]	1-16
X	CN 113992418 A (NANJING LIANLIAOMO INFORMATION TECHNOLOGY CO., LTD.) 28 January 2022 (2022-01-28) description, paragraphs [0015]-[0027]	1-16
A	CN 108712261 A (HANGZHOU ZHIKUAI NETWORK TECHNOLOGY CO., LTD.) 26 October 2018 (2018-10-26) entire document	1-16
A	KR 20200048722 A (MONEYBRAIN INC.) 08 May 2020 (2020-05-08) entire document	1-16

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 January 2023	**28 January 2023**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/135607

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 115174188 A	11 October 2022	None	
CN 114285555 A	05 April 2022	None	
CN 113992418 A	28 January 2022	None	
CN 108712261 A	26 October 2018	None	
KR 20200048722 A	08 May 2020	None	

国际检索报告

国际申请号
PCT/CN2022/135607

A. 主题的分类

H04L 9/40(2022.01)i; H04L 9/08(2006.01)i; H04L 67/10(2022.01)i; H04L 67/104(2022.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNPAT,CNKI,WPI,EPODOC,3GPP:区块链 组 组播 加密 目标 目的 源 block chain blockchain key group+ groupcast + source destinat+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 115174188 A (蚂蚁区块链科技上海有限公司) 2022年10月11日 (2022-10-11) 权利要求1-16	1-16
X	CN 114285555 A (支付宝杭州信息技术有限公司等) 2022年4月5日 (2022-04-05) 说明书第[0028]-[0108]段	1-16
X	CN 113992418 A (南京联了么信息技术有限公司) 2022年1月28日 (2022-01-28) 说明书第[0015]-[0027]段	1-16
A	CN 108712261 A (杭州智块网络科技有限公司) 2018年10月26日 (2018-10-26) 全文	1-16
A	KR 20200048722 A (MONEY BRAIN INC.) 2020年5月8日 (2020-05-08) 全文	1-16

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：
“A” 认为不特别相关的表示了现有技术一般状态的文件
“E” 在国际申请日的当天或之后公布的在先申请或专利
“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）
“O” 涉及口头公开、使用、展览或其他方式公开的文件
“P” 公布日先于国际申请日但迟于所要求的优先权日的文件
“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件
“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性
“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性
“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2023年1月13日	2023年1月28日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 田琳琳 电话号码 86-(10)-53961736

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/135607

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 115174188 A	2022年10月11日	无	
CN 114285555 A	2022年4月5日	无	
CN 113992418 A	2022年1月28日	无	
CN 108712261 A	2018年10月26日	无	
KR 20200048722 A	2020年5月8日	无	