

在区块链网络中实现安全组播的方法及装置

技术领域

[01] 本说明书一个或多个实施例涉及终端技术领域，尤其涉及在区块链网络中实现安全组播的方法及装置。

背景技术

[02] 在传统的 IP 组播中，中心站点如果要将同一份数据包传送到两个分支站点（例如分支站点 A 和分支站点 B），就需要分别与分支站点 A 和分支站点 B 建立安全关联（Security Association，简称 SA），此时中心站点发送数据到分支站点 A 的流量不能被中心站点 B 所解密，反之亦然。可见，传统 IP 组播场景下如果涉及一对多传输或多对多传输的情况，往往需要建立很多个安全关联，这大大增加了网络的复杂度和维护难度。

[03] 针对上述问题，相关技术中提出了一些解决方案。在这些解决方案中，可以由密钥服务器向需要实现组播的各个成员分发密钥，使得这些成员可以通过分发的密钥对组播消息进行加密传输，以实现安全组播。但是，密钥服务器的引入增加了架构复杂度和管理难度，而且密钥服务器作为中心化管理的角色，与区块链技术的去中心化存在冲突，无法适用于区块链场景下的安全组播。

发明内容

[04] 有鉴于此，本说明书一个或多个实施例提供在区块链网络中实现安全组播的方法及装置。

[05] 为实现上述目的，本说明书一个或多个实施例提供技术方案如下：

[06] 根据本说明书一个或多个实施例的第一方面，提出了一种在区块链网络中实现安全组播的方法，包括：第一区块链节点生成并发送安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；第二区块链节点收到所述安全组创建消息后，从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[07] 根据本说明书一个或多个实施例的第二方面，提出了一种在区块链网络中实现安全组播的方法，包括：第一区块链节点生成安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信

息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；第一区块链节点发送所述安全组创建消息，使各个目标区块链节点分别从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[08]根据本说明书一个或多个实施例的第三方面，提出了一种在区块链网络中实现安全组播的方法，包括：第二区块链节点接收第一区块链节点发送的安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；第二区块链节点从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[09]根据本说明书一个或多个实施例的第四方面，提出了一种在区块链网络中实现安全组播的装置，包括：消息创建单元，使第一区块链节点生成安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；消息发送单元，使第一区块链节点发送所述安全组创建消息，使各个目标区块链节点分别从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[10]根据本说明书一个或多个实施例的第五方面，提出了一种在区块链网络中实现安全组播的装置，包括：消息接收单元，使第二区块链节点接收第一区块链节点发送的安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；消息处理单元，使第二区块链节点从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[11]根据本说明书一个或多个实施例的第六方面，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二方面或第三方面所述的方法。

[12]根据本说明书一个或多个实施例的第七方面，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二方面或第三方面所述的方法。

[13]由上述技术方案可知，本说明书利用了区块链网络中的每个区块链节点均可获得其他区块链节点的公钥这一特性，使得第一区块链节点生成的安全组创建消息中可以包含分别对应于各个目标区块链节点的安全组信息结构体，并且由于每一安全组信息结构体仅包含相应的目标区块链节点的公钥和基于该公钥加密后的密文安全组信息，使得一方面该目标区块链节点可以通过匹配公钥的方式查询到自身对应的安全组信息结构体，另一方面可以确保该密文安全组信息只能由该目标区块链节点通过自身私钥解密、无法被其他区块链节点解密，从而在无需增加中心化的密钥服务器的情况下，实现了安全且精准的密钥分享操作，完成了对组播安全组的创建，使得组播安全组内的区块链节点之间可以通过上述的安全组会话密钥实现安全组播。

附图说明

[14]图1是一示例性实施例提供的一种在区块链网络中实现安全组播的方法的流程图。

[15]图2是一示例性实施例提供的一种创建方侧的在区块链网络中实现安全组播的方法的流程图。

[16]图3是一示例性实施例提供的一种参与方侧的在区块链网络中实现安全组播的方法的流程图。

[17]图4是一示例性实施例提供的一种组播场景的示意图。

[18]图5是一示例性实施例提供的一种设备的结构示意图。

[19]图6是一示例性实施例提供的一种创建方侧的在区块链网络中实现安全组播的装置的框图。

[20]图7是一示例性实施例提供的一种参与方侧的在区块链网络中实现安全组播的装置的框图。

具体实施方式

[21]这里将详细地对示例性实施例进行说明，其示例表示在附图中。下面的描述涉及附图时，除非另有表示，不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本说明书一个或多个实施例相一致的所有实施方式。相反，它们仅是与如所附权利要求书中所详述的、本说明书一个或多个实施例的一些方面相一致的装置和方法的例子。

[22]需要说明的是：在其他实施例中并不一定按照本说明书示出和描述的顺序来执行相应方法的步骤。在一些其他实施例中，其方法所包括的步骤可以比本说明书所描述的更

多或更少。此外，本说明书中所描述的单个步骤，在其他实施例中可能被分解为多个步骤进行描述；而本说明书中所描述的多个步骤，在其他实施例中也可能被合并为单个步骤进行描述。

[23] 基于开放程度的不同，区块链网络可以分为公有链、私有链和联盟链等。其中，公有链的开放程度最高、私有链的开放程度最低，而联盟链则介于这两者之间。区块链网络中包含若干区块链节点，区块链节点之间的需要实现诸如共识、交易传输、区块同步等通信操作。各个区块链节点之间可以通过 P2P (Peer to Peer, 点对点) 技术进行通信。或者，各个区块链节点可以借助于区块链中继通信网络中的中继节点，譬如需要通信的区块链节点分别接入中继节点，这样区块链节点之间就可以通过区块链中继通信网络来实现通信。相比于采用 P2P 技术进行通信，由于区块链中继通信网络是面向区块链实时传输的骨干中继通信网络，各个中继节点之间能够通过高 QoS 保障的优质带宽进行通信交互，因而由区块链中继通信网络接管区块链节点之间通信的中间链路，能够降低通信时延、提高稳定性，从而显著提升区块链节点之间的通信质量。相关技术中的区块链中继通信网络譬如可以包括：应用于公有链的区块链中继通信网络主要包括 Falcon、Fast Bitcoin Relay Network (FBRN)、Fast Internet Bitcoin Relay Engine (FIBRE) 等，而应用于联盟链的区块链中继通信网络主要包括 BloXRoute、Blockchain Transmission Network (BTN) 等。

[24] 无论是基于 P2P 技术或者通过区块链中继通信网络，区块链节点之间均可能存在组播需求。比如，区块链网络中的部分区块链节点可能基于业务需求或其他需求而需要实现安全通信，并且不希望区块链网络中的其他区块链节点获知通信内容，那么可以通过本说明书的技术方案在该部分区块链节点之间建立组播安全组，从而既可以通过组播来提升通讯效率、无需在各个区块链节点之间进行一对一形式的低效通信，又可以避免其他区块链节点获知通信内容。

[25] 图 1 是一示例性实施例提供的一种在区块链网络中实现安全组播的方法的流程图。如图 1 所示，该方法可以包括：步骤 102，第一区块链节点生成并发送安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输。

[26] 第一区块链节点可以为区块链网络中的任意一个区块链节点，该第一区块链节点通过安全组创建消息来创建组播安全组，相当于该组播安全组的创建方。当然，在一些管理较为严格的区块链网络中，可以对组播安全组的创建方进行一定限制，比如仅允许区块链网络中指定的一个或多个区块链节点成为创建方，例如在区块链的创世块中可以记录有这些区块链节点的信息（如公钥），而其他区块链节点可以据此验证接收到的安全组创建消息是否来自这些指定的区块链节点，如果是则正常处理收到的安全组创建消息，

如果不是则丢弃收到的安全组创建消息。

[27] 目标区块链节点可以为区块链网络中的任意一个或多个区块链节点。第一区块链节点可以通过链下协商、线下协商等方式, 从区块链网络中确定出上述的目标区块链节点, 并由第一区块链节点与确定出的目标区块链节点组成上述的组播安全组, 从而在这些区块链节点之间实现安全组播, 避免区块链网络中的其他区块链节点获知组播消息的内容。

[28] 为了实现安全组播, 第一区块链节点与目标区块链节点均需维护相同的会话密钥, 并且确保该会话密钥仅由第一区块链节点和目标区块链节点所维护、不被区块链网络中的其他区块链节点获知, 这样第一区块链节点与目标区块链节点之间才能够通过该会话密钥对组播消息进行加密传输, 并且确保只有第一区块链节点和目标区块链节点能够对收到的组播消息进行解密。这里所描述的会话密钥, 譬如可以为本说明书中的安全组会话密钥。

[29] 第一区块链节点可以通过任意方式获得安全组会话密钥, 譬如由第一区块链节点接收用户配置的安全组会话密钥, 或者由第一区块链节点通过密钥生成规则生成该安全组会话密钥, 或者由第一区块链节点从链外的密钥服务器处获得该安全组会话密钥等, 本说明书并不对此进行限制。由第一区块链节点获得安全组会话密钥, 并进而通过安全组创建消息分发至目标区块链节点, 而无需在区块链网络内添加相关技术中的密钥服务器, 有助于简化网络架构, 并且这种密钥分发方式能够适用于各个区块链节点、符合区块链网络的去中心化特性。

[30] 每个区块链节点可以同时加入多个组播安全组, 只要该区块链节点能够获得相应组播安全组内分发的安全组会话密钥即可。

[31] 步骤 104, 第二区块链节点收到所述安全组创建消息后, 从所述安全组创建消息中查找携带自身公钥的安全组信息结构体, 并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[32] 在区块链网络中, 每个区块链节点均存在相应的公私钥对, 以代表自身的身份。其中, 公私钥对中的私钥由各个区块链节点自行维护、避免泄露, 而公钥则可以对外公开。鉴于区块链技术的特点, 每个区块链节点都可以获得区块链网络中的各个区块链节点的公钥, 而本说明书的技术方案利用这一特点实现了对安全组会话密钥的安全分发。

[33] 在密钥分发的过程中, 公钥起到的作用分为两部分: 第一部分, 在生成分别对应于各个目标区块链节点的安全组信息结构体时, 通过在安全组信息结构体内包含相应的目标区块链节点的公钥, 使得各个区块链节点在收到安全组创建消息后, 均可以将自身的公钥作为标识进行匹配, 以准确查找到对应于自身的安全组信息结构体, 当然如果未匹配到则表明自身并不属于相应的组播安全组, 从而确保了对安全组会话密钥的精准分发; 第二部分, 在生成分别对应于各个目标区块链节点的安全组信息结构体时, 采用相应的目标区块链节点的公钥进行非对称加密、以生成上述的密文安全组信息, 确保只有该安

全组信息结构体对应的目标区块链节点才能够对该密文安全组信息进行解密以得到安全组会话密钥，因为正如前文所述，只有该目标区块链节点持有自身的私钥，从而确保了对安全组会话密钥的安全分发。因此，如果第一区块链节点希望将第二区块链节点添加为组播安全组的成员，第一区块链节点可以在安全组创建消息中包含对应于第二区块链节点的安全组信息结构体，该安全组信息结构体包含第二区块链节点的公钥以及由该公钥加密生成的密文安全组信息，使得第二区块链节点能够通过自身公钥查找到该安全组信息结构体、解密得到安全组会话密钥。

[34]对安全组会话密钥分发完毕后，相当于区块链网络中获得该安全组会话密钥的所有区块链节点组成了组播安全组，这些区块链节点成为该组播安全组的成员。组播安全组的成员之间可以实现安全组播：各个成员之间发送的组播消息都会采用上述的安全组会话密钥进行加密传输，使得这些组播消息只能被这些成员解密，即便这些组播消息被区块链网络中的其他区块链节点接收也无法被解密，从而确保组播消息的消息内容必然仅能够被组播安全组的成员获得，故而实现了安全组播。

[35]在通过安全组会话密钥对组播消息进行加密时，组播安全组的成员之间可以预先配置或协商（例如链下协商或线下协商等）所采用的加密算法，该加密算法还用于对组播消息进行解密操作。或者，明文安全组信息可以包含：加密算法指示信息，该加密算法指示信息用于表征采用上述安全组会话密钥对组播消息进行加密传输时使用的加密算法，相当于由第一区块链节点来指定所采用的加密算法；当然，该加密算法也可以是由第一区块链节点与目标区块链节点预先协商确定的，并由第一区块链节点标记在明文安全组信息中。

[36]当安全组会话密钥为对称密钥时，所采用的加密算法可以为任意对称加密算法，譬如 AES128-GCM 、 AES128-CCM 、 AES256-GCM 、 AES256-CCM 、 AEAD_CHACHA20_POLY1305、SM4-GCM、SM4-CCM 等，本说明书并不对此进行限制。当安全组会话密钥为非对称密钥时，该安全组会话密钥包括公私钥对，其中公钥用于对组播消息进行加密、私钥用于对组播消息进行解密。相应地，所采用的加密算法可以为任意非对称加密算法，譬如 RSA、Elgamal、背包算法、Rabin、D-H、ECC (椭圆曲线加密算法)等，本说明书并不对此进行限制。

[37]如果一个区块链节点仅同时加入一个组播安全组，那么该区块链节点只会在这个组播安全组内收发组播消息，只需要采用这个组播安全组内分发的安全组会话密钥进行解密，不会产生组播或安全组会话密钥的混淆。而如前所述，同一区块链节点可以同时加入多个组播安全组，此时该区块链节点需要对各个组播安全组进行区分，比如各个组播安全组分别使用的安全组会话密钥、所采用的加密算法等，再比如收到的组播消息属于哪个组播安全组、自己是否属于该组播安全组等。因此，明文安全组信息还可以包含安全组标识，该安全组标识对应于组播安全组，譬如安全组标识与组播安全组之间一一对应。相应的，对于组播安全组内的组播消息（即组播安全组的成员之间传输的组播消

息)，可以包含该组播安全组对应的安全组标识，以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。组播消息的接收方可以通过该组播消息所含的安全组标识，确定该组播消息所属的组播安全组，而如果该接收方属于该组播安全组，该接收方就维护有通过如上述步骤 102-104 获得的、包含该安全组标识的明文安全组信息，并进而通过该明文安全组信息所含的安全组会话密钥对该组播消息进行解密。类似地，当某一区块链节点希望发送组播消息时，该区块链节点可以确定在哪个组播安全组内进行通信，就可以根据确定出的组播安全组对应的安全组标识，从而包含该安全组标识的明文安全组信息中获得安全组会话密钥，并通过该安全组会话密钥对组播消息进行加密发送。

[38] 上述的安全组创建消息还可以包含由第一区块链节点的私钥生成的消息签名。那么，第二区块链节点在收到安全组创建消息后，还可以首先通过第一区块链节点的公钥对该消息签名进行验签，并在验签成功的情况下确定：安全组创建消息确实来自第一区块链节点，并且该安全组创建消息在传输过程中并未发生篡改，第一区块链节点可以在确认验签成功后才执行步骤 104 和其他操作，否则可以丢弃或不处理该安全组创建消息。

[39] 上述的消息签名可以由第一区块链节点的私钥对安全组创建消息中的关键信息进行签名而生成，使得验签成功的情况下具体可以证明该关键信息没有被篡改。例如，关键信息可以包括：对应于各个目标区块链节点的安全组信息结构体。再例如，关键信息除了上述的安全组信息结构体之外，还可以包含以下至少之一：防重放随机数，第一区块链节点的公钥或数字证书等，本说明书并不对此进行限制。第一区块链节点发送的不同安全组创建消息可以分别包含不同的防重放随机数，那么第二区块链节点可以在当前接收到的安全组创建消息与历史上接收到的安全组创建消息包含相同的防重放随机数的情况下，确认当前接收到的安全组创建消息为重放消息、需要丢弃或不处理，而只有当前接收到的安全组创建消息与历史上接收到的安全组创建消息包含的防重放随机数均不同的情况下，才会正常处理收到的安全组创建消息。第一区块链节点的数字证书由 CA 中心发放，该数字证书中包含第一区块链节点的公钥，第二区块链节点可以在数字证书通过验证的情况下，确定该数字证书包含的公钥确实属于第一区块链节点。

[40] 组播安全组可以是长期有效的安全组，也可以是短期或临时性的。对于短期或临时性的组播安全组，具有一定的时效性；比如，这类组播安全组可以存在一有效期，使得相应的组播安全组仅在有效期内能够实现安全组播。例如，上述任一实施例的明文安全组信息还可以包含：会话有效期，该会话有效期用于表征明文安全组信息的有效期，使得：当处于有效期内时，明文安全组信息被已加入相应的组播安全组的各个区块链节点存储；当未处于有效期内时，明文安全组信息被已加入相应的组播安全组的各个区块链节点丢弃或标记为无效。虽然这里描述的会话有效期用于管理明文安全组信息的有效期，但是由于组播安全组内的安全组播需要利用明文安全组信息所含的安全组会话密钥、会话组标识等信息，因而对明文安全组信息的管理实际上就是对组播安全组的管理，而明

文安全组信息的有效期即为组播安全组的有效期。由于同一明文安全组信息的使用时间越长，该明文安全组信息发生泄露的风险就越大，因而通过设置上述的会话有效期可以避免长期使用同一明文安全组信息所带来的潜在安全性风险，迫使相应组播安全组的成员对明文安全组信息进行更新，以提升组播安全性。

[41] 图 2 是一示例性实施例提供的一种创建方侧的在区块链网络中实现安全组播的方法的流程图。如图 2 所示，该方法可以包括：步骤 202，第一区块链节点生成安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输。

[42] 在第一区块链节点用于生成安全组创建消息的情况下，相当于由第一区块链节点发起了对相应的组播会话组的创建，因而可以将第一区块链节点视为该组播会话组的创建方。相应地，对于其他从第一区块链节点处接收该安全组创建消息、获得安全组会话密钥等的区块链节点，相当于参与了相应的组播会话组，因而可以将这些区块链节点视为该组播会话组的参与方。同一区块链节点在一些组播安全组内可以属于创建方这一角色，同时在另一些组播安全组内也可以属于参与方这一角色。

[43] 步骤 204，第一区块链节点发送所述安全组创建消息，使各个目标区块链节点分别从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[44] 如前所述，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

[45] 如前所述，所述明文安全组信息还包含会话有效期，所述会话有效期用于表征所述明文安全组信息的有效期；其中，当处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储；当未处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

[46] 如前所述，所述明文安全组信息还包含安全组标识，所述安全组标识对应于所述组播安全组；其中，所述组播安全组内的组播消息包含所述安全组标识，以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

[47] 如前所述，所述安全组创建消息还包含：由第一区块链节点的私钥生成的消息签名。

[48] 如前所述，所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成；其中，所述关键信息包括：对应于各个目标区块链节点的安全组信息结构体。

[49]如前所述，所述关键信息还包含以下至少之一：防重放随机数；第一区块链节点的公钥或数字证书。

[50]图3是一示例性实施例提供的一种参与方侧的在区块链网络中实现安全组播的方法的流程图。如图3所示，该方法可以包括：步骤302，第二区块链节点接收第一区块链节点发送的安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输。

[51]步骤304，第二区块链节点从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[52]如前所述，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

[53]如前所述，所述明文安全组信息还包含会话有效期，所述会话有效期用于表征所述明文安全组信息的有效期；其中，当处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储；当未处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

[54]如前所述，所述明文安全组信息还包含安全组标识，所述安全组标识对应于所述组播安全组；其中，所述组播安全组内的组播消息包含所述安全组标识，以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

[55]如前所述，所述安全组创建消息还包含由第一区块链节点的私钥生成的消息签名；所述方法还包括：第二区块链节点通过第一区块链节点的公钥对所述消息签名进行验签。

[56]如前所述，所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成；其中，所述关键信息包括：对应于各个目标区块链节点的安全组信息结构体。

[57]如前所述，所述关键信息还包含以下至少之一：防重放随机数；第一区块链节点的公钥或数字证书。

[58]在上述图1所示的实施例中，已经结合第一区块链节点、第二区块链节点分别执行的处理操作，对组播安全组的创建方、参与方侧的技术方案予以描述，因而上述图2和图3所示的实施例中，相关特征或方案的描述可以参考图1所示的实施例，此处不再赘述。

[59]图4是一示例性实施例提供的一种组播场景的示意图。如图4所示，区块链网络中存在节点A、节点B、节点C和节点D等若干区块链节点；其中，假定节点A、节点B和节点C之间需要建立一组播安全组，使得在节点A、节点B和节点C之间可以对一些敏感内容进行传输，而避免节点D等其他区块链节点获得这些敏感内容。那么，节点A、节点B和节点C可以通过基于本说明书实施例的BSGGP(Blockchain Security Group Generate Protocol，区块链安全组生成协议)进行密钥协商，以建立组播安全组，并进而通过基于本说明书实施例的BSGMP(Blockchain Security Group Multicast Protocol，区块链安全组组播协议)实现安全组播。

[60]假定由节点A作为创建方，则节点A需要首先生成符合BSGGP的安全组创建消息BSGGP_GroupInfo，该BSGGP_GroupInfo的消息结构可以为：

```
Struct{
    Version                version //协议版本号
    String                  Nonce //随机数，用于防止重放攻击
    Cert                    cert //节点A的公钥
    Encrypt_Session_chain   sess_chain //保存组播安全组相关信息的结构体
    String                  Verify //对Nonce, cert 和 sess_chain 的签名
}BSGGP_GroupInfo
```

[61]在上述BSGGP_GroupInfo的消息结构中，Encrypt_Session_chain用于保存组播安全组相关信息，该组播安全组相关信息可以为前述实施例中对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体。该Encrypt_Session_chain的结构可以为：

```
Struct{
    BSG_Encrypt_Session    sess[Group_member_num-1];
}Encrypt_Session_chain
```

[62]其中，BSG_Encrypt_Session即为上述的安全组信息结构体，且对应于节点B、节点C等各个目标区块链节点的安全组信息结构体之间可以串成一条链后，以链式结构被添加于上述的Encrypt_Session_chain中。这些安全组信息结构体在构成链式结构时，可以按照预设顺序（如IP地址的大小顺序、节点公钥的大小顺序等，本说明书并不对此进行限制）依次拼接；也可以无序拼接，拼接顺序并不会影响协商效果。

[63]BSG_Encrypt_Session的结构可以为：

```
Struct{
    PublicKey              key; //目标区块链节点的公钥
```

Enc_Session sess; //使用目标区块链节点的公钥对 BSG_Session 进行加密后生成的密文安全组信息

}BSG_Encrypt_Session

[64]由上述 BSG_Encrypt_Session 的结构可见：由于需要针对各个目标区块链节点分别生成相应的 BSG_Encrypt_Session，且每个 BSG_Encrypt_Session 均会包含相应目标区块链节点的公钥，使得不论这些 BSG_Encrypt_Session 之间采用何种顺序进行拼接，每个目标区块链节点总是能够通过匹配自身的公钥来找到自身对应的 BSG_Encrypt_Session，故而这些 BSG_Encrypt_Session 之间的拼接顺序不会影响协商效果。

[65]Enc_Session 相当于前文所述的密文安全组信息，Enc_Session 由所属 BSG_Encrypt_Session 对应的目标区块链节点的公钥对 BSG_Session 进行加密得到，该 BSG_Session 相当于前文所述的明文安全组信息。比如节点 B 对应的 BSG_Encrypt_Session 中，所含的 Enc_Session 由节点 B 的公钥对 BSG_Session 进行加密得到，而节点 C 对应的 BSG_Encrypt_Session 中，所含的 Enc_Session 由节点 C 的公钥对 BSG_Session 进行加密得到。可见，只有 BSG_Encrypt_Session 对应的目标区块链节点能够通过自身维护的私钥对该 Enc_Session 进行解密以得到 BSG_Session，而其他区块链节点即便可以获得该 BSG_Encrypt_Session，也由于无法获得私钥而不能完成解密，从而实现了 BSG_Session 的安全传递，确保了协商过程的安全性。

[66]各个节点对应的 BSG_Encrypt_Session 中，Enc_Session 对应的 BSG_Session 均相同。BSG_Session 可以包含节点 A 希望传递给节点 B、节点 C 的任何内容，当然这些内容通常与需要创建的组播会话组相关。例如，BSG_Session 的结构可以为：

```
Struct{
    uint32 session_lifetime_hint; //会话有效期
    String BSG_ID; //安全组标识
    uint32 cipher_id; //用于使用的加密算法
    String Master_key; //安全组会话密钥
}BSG_Session
```

[67]每个目标区块链节点解密得到 BSG_Session 后，会对该 BSG_Session 进行保存。而每个 BSG_Session 中包含的 session_lifetime_hint，用于表明相应的组播会话组的有效期或者相应会话的有效期，那么目标区块链节点可以在确定某个 BSG_Session 所含的 session_lifetime_hint 超期时，删除该 BSG_Session 或者将该 BSG_Session 标记为无效，或者在需要发送组播消息之前查看到相应 BSG_Session 所含的 session_lifetime_hint 超期时避免使用该 BSG_Session 中的 Master_key 进行加密；换言之，只有当 BSG_Session 所含的 session_lifetime_hint 未超期时，该 BSG_Session 中的 Master_key 才会被用于对组

播消息进行加密传输。

[68]BSG_ID 用于标记组播会话组或该组播会话组所对应的会话，使得该组播会话组的成员之间传输的组播消息均会包含该 BSG_ID，这样当某一区块链节点在收到组播消息后，能够根据该组播消息所含的 BSG_ID 来匹配自身维护的 BSG_Session，并通过包含该 BSG_ID 的 BSG_Session 中的 Master_key 来解密收到的组播消息。Master_key 用于对组播消息进行加解密处理。而 cipher_id 用于指示组播会话组的成员，在执行加解密处理时所采用的算法。

[69]在节点 A、节点 B 和节点 C 之间通过上述方式完成协商后，节点 A、节点 B 和节点 C 在本地均会维护有 BSG_Session，使得节点 A、节点 B 和节点 C 组成一组播安全组，这些节点之间可以基于共同维护的 BSG_Session 实现安全组播。

[70]假定节点 B 希望向节点 A 和节点 C 发送组播消息，节点 B 首先生成符合 BSGMP 的消息结构体 BSG_Plaintext，该 BSG_Plaintext 的结构可以为：

```
Struct{
    String  content; //明文消息内容

    uint8   zeros[length_of_padding-1]; //明文消息内容的最后分块不足 128bit 时，以全 0 填充

    uint8   length_of_padding; //用于描述 padding 的长度
}BSG_Plaintext
```

[71]在上述的消息结构体 BSG_Plaintext 中，节点 B 需要传输的消息内容以明文形式记录于 content 中。在一些情况下，BSG_Plaintext 可以仅包含 content。而在上述实施例 1 中，由于采用块结构来组织 BSG_Plaintext，譬如每个块的长度为 128bit，那么当 content 的长度恰好为 128bit 的整数倍时，content 恰好可以填充相应的若干个块，那么 BSG_Plaintext 同样可以不包含 zeros[length_of_padding-1]和 length_of_padding；但是，当 content 的长度并非恰好为 128bit 的整数倍时，就会造成最后一个分块的 128bit 无法被填满，这些未填满的部分可以全部采用 0 来填充，上述的 zeros[length_of_padding-1]即对应于这些填充为 0 的部分（即 padding），而 length_of_padding 则用于描述 padding 的长度。

[72]进一步地，节点 B 可以对上述的 BSG_Plaintext 进行构造，从而生成组播消息 BSG_Message，其消息结构可以为：

```
Struct{
    Int      BSG_Message.length; //消息长度

    String   BSG_ID; //安全组标识
```

```

        64bit    seq_num; //对称加密的 iv, 每条应用层消息自增

        String.  BSG_Ciphertext; //用 BSG_key 加密的 BSG_Plaintext 消息

    }BSG_Message

```

[73] 节点 B 在生成 BSG_Message 时, 需要使用前述过程获得的 BSG_Session。实际上, 当节点 B 希望在哪个组播会话组发送 BSG_Message 时, 就应当使用该组播会话组对应的 BSG_Session, 并通过该 BSG_Session 所含的 BSG_ID 和 Master_key 生成上述的 BSG_Message。

[74] BSG_Ciphertext 由节点 B 采用 Master_key 对 BSG_Plaintext 进行加密而生成。当采用诸如 AES128-GCM 等加密算法时, 该加密算法还要求使用随机数 iv 以增加对称加密的安全性, 因而 BSG_Message 的结构中包含上述的 seq_num。当然, 节点 B 可以单独将节点 A 和节点 C 发送 seq_num, 而非将其集成在 BSG_Message 的结构中进行发送, 这样即便 Master_key 和 BSG_Message 都暴露的情况下, 也可能由于 seq_num 未暴露而使得 BSG_Ciphertext 无法被正确解密, 从而有助于提升安全性。而上述实施例中, 通过将 seq_num 集成在 BSG_Message 的结构中进行发送, 则考虑到避免单独发送 seq_num 而造成的交互次数增加, 有助于提升通讯效率。

[75] 以 AES128-GCM 为例, 则可以通过下述方式对 BSG_Plaintext 加密生成 BSG_Ciphertext:

```

BSG_Ciphertext=AES128-GCM-Encrypt(Master_key,seq_num,          additional_data,
BSG_Plaintext)

```

[76] 其中, additional_data = BSG_Message.length || BSG_Message

[77] 那么, 如果譬如节点 C 收到节点 B 发送的上述 BSG_Message, 节点 C 可以根据该 BSG_Message 所含的 BSG_ID, 从自身维护的所有 BSG_Session 中进行匹配, 以确定包含该 BSG_ID 的 BSG_Session。进而, 节点 C 可以根据确定出的 BSG_Session 中读取 cipher_id 和 Master_key, 并据此对收到的 BSG_Message 中的 BSG_Ciphertext 进行解密, 以得到明文的 BSG_Plaintext。仍以 AES128-GCM 为例, 则可以通过下述方式对 BSG_Ciphertext 解密得到 BSG_Plaintext:

```

BSG_Plaintext  =  AES128-GCM-Decrypt(Master_key,  seq_num,  additional_data,
BSG_Ciphertext)

```

[78] 在针对组播消息进行传输时, 作为发送方的区块链节点可以在相应的消息报文中指定作为接收方的区块链节点的信息, 譬如在报文头添加这些区块链节点的 IP 地址, 以使得组播消息可以定向发送至被指定为接收方的这些区块链节点, 而不会发送给其他的区块链节点, 以节省网络资源。当然, 实现定向发送的方式还有很多, 比如当区块链节点之间通过区块链中继通信网络进行通信时, 可以通过在消息报文中添加这些区块链节

点对应的标识信息,使得区块链中继通信网络可以将组播消息定向发送至被指定为接收方的这些区块链节点,而不会发送给其他的区块链节点。

[79]当然,不属于组播会话组的区块链节点也可能收到组播消息。例如,如果节点D收到节点B发送的上述BSG_Message,节点D也可以根据该BSG_Message所含的BSG_ID,从自身维护的所有BSG_Session中进行匹配,但节点D无法匹配到包含该BSG_ID的BSG_Session,因而无法对收到的BSG_Message中的BSG_Ciphertext进行解密,那么从安全性的角度而言,无异于节点D未收到组播消息。

[80]综上所述,本说明书利用了区块链网络中的每个区块链节点均可获得其他区块链节点的公钥这一特性,使得第一区块链节点生成的安全组创建消息中可以包含分别对应于各个目标区块链节点的安全组信息结构体,并且由于每一安全组信息结构体仅包含相应的目标区块链节点的公钥和基于该公钥加密后的密文安全组信息,使得一方面该目标区块链节点可以通过匹配公钥的方式查询到自身对应的安全组信息结构体,另一方面可以确保该密文安全组信息只能由该目标区块链节点通过自身私钥解密、无法被其他区块链节点解密,从而在无需增加中心化的密钥服务器的情况下,实现了安全且精准的密钥分享操作,完成了对组播安全组的创建,使得组播安全组内的区块链节点之间可以通过上述的安全组会话密钥实现安全组播。

[81]图5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5,在硬件层面,该设备包括处理器502、内部总线504、网络接口506、内存508以及非易失性存储器510,当然还可能包括其他业务所需要的硬件。处理器502从非易失性存储器510中读取对应的计算机程序到内存508中然后运行,在逻辑层面上形成在区块链网络中实现安全组播的装置。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。

[82]请参考图6,在软件实施方式中,创建方侧的在区块链网络中实现安全组播的装置可以包括:

[83]消息创建单元61,使第一区块链节点生成安全组创建消息,所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体,每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息,所述明文安全组信息包含安全组会话密钥,所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输;

[84]消息发送单元62,使第一区块链节点发送所述安全组创建消息,使各个目标区块链节点分别从所述安全组创建消息中查找携带自身公钥的安全组信息结构体,并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[85]可选的，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

[86]可选的，所述明文安全组信息还包含会话有效期，所述会话有效期用于表征所述明文安全组信息的有效期；其中，当处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储；当未处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

[87]可选的，所述明文安全组信息还包含安全组标识，所述安全组标识对应于所述组播安全组；其中，所述组播安全组内的组播消息包含所述安全组标识，以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

[88]可选的，所述安全组创建消息还包含由第一区块链节点的私钥生成的消息签名。

[89]可选的，所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成；其中，所述关键信息包括：对应于各个目标区块链节点的安全组信息结构体。

[90]可选的，所述关键信息还包含以下至少之一：防重放随机数；第一区块链节点的公钥或数字证书。

[91]请参考图 7，在软件实施方式中，参与方侧的在区块链网络中实现安全组播的装置可以包括：消息接收单元 71，使第二区块链节点接收第一区块链节点发送的安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；消息处理单元 72，使第二区块链节点从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

[92]可选的，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

[93]可选的，所述明文安全组信息还包含会话有效期，所述会话有效期用于表征所述明文安全组信息的有效期；其中，当处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储；当未处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

[94]可选的，所述明文安全组信息还包含安全组标识，所述安全组标识对应于所述组播安全组；其中，所述组播安全组内的组播消息包含所述安全组标识，以指示所述组播消

息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

[95] 可选的，所述安全组创建消息还包含由第一区块链节点的私钥生成的消息签名；所述方法还包括：第二区块链节点通过第一区块链节点的公钥对所述消息签名进行验签。

[96] 可选的，所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成；其中，所述关键信息包括对应于各个目标区块链节点的安全组信息结构体。

[97] 可选的，所述关键信息还包含以下至少之一：防重放随机数；第一区块链节点的公钥或数字证书。

[98] 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计算机，计算机的具体形式可以是个人计算机、膝上型计算机、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、电子邮件收发设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任意几种设备的组合。

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

[100] 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。

[101] 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、磁盘存储、量子存储器、基于石墨烯的存储介质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。

[102] 还需要说明的是，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、商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、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[103] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[104] 在本说明书一个或多个实施例使用的术语是仅仅出于描述特定实施例的目的，而非旨在限制本说明书一个或多个实施例。在本说明书一个或多个实施例和所附权利要求书中所使用的单数形式的“一种”、“所述”和“该”也旨在包括多数形式，除非上下文清楚地表示其他含义。还应当理解，本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。

[105] 应当理解，尽管在本说明书一个或多个实施例可能采用术语第一、第二、第三等来描述各种信息，但这些信息不应限于这些术语。这些术语仅用来将同一类型的信息彼此区分开。例如，在不脱离本说明书一个或多个实施例范围的情况下，第一信息也可以被称为第二信息，类似地，第二信息也可以被称为第一信息。取决于语境，如在此所使用的词语“如果”可以被解释成为“在……时”或“当……时”或“响应于确定”。

[106] 以上所述仅为本说明书一个或多个实施例的较佳实施例而已，并不用以限制本说明书一个或多个实施例，凡在本说明书一个或多个实施例的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本说明书一个或多个实施例保护的范围之内。

权利要求书

1. 一种在区块链网络中实现安全组播的方法，包括：

第一区块链节点生成并发送安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；

第二区块链节点收到所述安全组创建消息后，从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

2. 根据权利要求 1 所述的方法，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

3. 根据权利要求 1 所述的方法，所述明文安全组信息还包含会话有效期，所述会话有效期用于表征所述明文安全组信息的有效期限；

其中，当处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储；当未处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

4. 根据权利要求 1 所述的方法，所述明文安全组信息还包含安全组标识，所述安全组标识对应于所述组播安全组；

其中，所述组播安全组内的组播消息包含所述安全组标识，以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

5. 根据权利要求 1 所述的方法，所述安全组创建消息还包含：由第一区块链节点的私钥生成的消息签名；第二区块链节点还通过第一区块链节点的公钥对所述消息签名进行验签。

6. 根据权利要求 5 所述的方法，所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成；

其中，所述关键信息包括：对应于各个目标区块链节点的安全组信息结构体。

7. 根据权利要求 6 所述的方法，所述关键信息还包含以下至少之一：

防重放随机数；

第一区块链节点的公钥或数字证书。

8. 一种在区块链网络中实现安全组播的方法，包括：

第一区块链节点生成安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组

内的组播消息进行加密传输；

第一区块链节点发送所述安全组创建消息，使各个目标区块链节点分别从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

9. 根据权利要求 8 所述的方法，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

10. 根据权利要求 8 所述的方法，所述明文安全组信息还包含会话有效期，所述会话有效期用于表征所述明文安全组信息的有效期；

其中，当处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储；当未处于有效期内时，所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

11. 根据权利要求 8 所述的方法，所述明文安全组信息还包含安全组标识，所述安全组标识对应于所述组播安全组；

其中，所述组播安全组内的组播消息包含所述安全组标识，以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

12. 根据权利要求 8 所述的方法，所述安全组创建消息还包含：由第一区块链节点的私钥生成的消息签名。

13. 根据权利要求 12 所述的方法，所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成；

其中，所述关键信息包括：对应于各个目标区块链节点的安全组信息结构体。

14. 根据权利要求 13 所述的方法，所述关键信息还包含以下至少之一：

防重放随机数；

第一区块链节点的公钥或数字证书。

15. 一种在区块链网络中实现安全组播的方法，包括：

第二区块链节点接收第一区块链节点发送的安全组创建消息，所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体，每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息，所述明文安全组信息包含安全组会话密钥，所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输；

第二区块链节点从所述安全组创建消息中查找携带自身公钥的安全组信息结构体，并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

16. 根据权利要求 15 所述的方法，所述明文安全组信息还包含加密算法指示信息，所述加密算法指示信息用于表征采用所述安全组会话密钥对所述组播消息进行加密传输时使用的加密算法。

17. 根据权利要求 15 所述的方法, 所述明文安全组信息还包含会话有效期, 所述会话有效期用于表征所述明文安全组信息的有效期;

其中, 当处于有效期内时, 所述明文安全组信息被已加入所述组播安全组的各个区块链节点存储; 当未处于有效期内时, 所述明文安全组信息被已加入所述组播安全组的各个区块链节点丢弃或标记为无效。

18. 根据权利要求 15 所述的方法, 所述明文安全组信息还包含安全组标识, 所述安全组标识对应于所述组播安全组;

其中, 所述组播安全组内的组播消息包含所述安全组标识, 以指示所述组播消息的接收方通过包含所述安全组标识的明文安全组信息中的安全组会话密钥进行解密操作。

19. 根据权利要求 15 所述的方法, 所述安全组创建消息还包含: 由第一区块链节点的私钥生成的消息签名; 所述方法还包括:

第二区块链节点通过第一区块链节点的公钥对所述消息签名进行验签。

20. 根据权利要求 19 所述的方法, 所述消息签名由第一区块链节点的私钥对所述安全组创建消息中的关键信息进行签名而生成;

其中, 所述关键信息包括: 对应于各个目标区块链节点的安全组信息结构体。

21. 根据权利要求 20 所述的方法, 所述关键信息还包含以下至少之一:

防重放随机数;

第一区块链节点的公钥或数字证书。

22. 一种在区块链网络中实现安全组播的装置, 包括:

消息创建单元, 使第一区块链节点生成安全组创建消息, 所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体, 每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息, 所述明文安全组信息包含安全组会话密钥, 所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输;

消息发送单元, 使第一区块链节点发送所述安全组创建消息, 使各个目标区块链节点分别从所述安全组创建消息中查找携带自身公钥的安全组信息结构体, 并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进行解密以得到所述安全组会话密钥。

23. 一种在区块链网络中实现安全组播的装置, 包括:

消息接收单元, 使第二区块链节点接收第一区块链节点发送的安全组创建消息, 所述安全组创建消息包含分别对应于待加入组播安全组的各个目标区块链节点的安全组信息结构体, 每一安全组信息结构体包含相应的目标区块链节点的公钥和由该公钥对明文安全组信息加密得到的密文安全组信息, 所述明文安全组信息包含安全组会话密钥, 所述安全组会话密钥用于对所述组播安全组内的组播消息进行加密传输;

消息处理单元, 使第二区块链节点从所述安全组创建消息中查找携带自身公钥的安全组信息结构体, 并通过自身私钥对查找到的安全组信息结构体内的密文安全组信息进

行解密以得到所述安全组会话密钥。

24. 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 8 至 21 中任一项所述的方法。

25. 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 8 至 21 中任一项所述的方法。