(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 2024/001022 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2022/135244

(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:
202210759288.5 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: 黄祖城 (**HUANG, Zucheng**); 中国浙江省杭州市西湖区西溪路556号8层B段801-11, Zhejiang 310000 (CN)。

(74) 代理人: 北京博思佳知识产权代理有限公司 (**BEIJING BESTIPR INTELLECTUAL PROPERTY LAW CORPORATION**); 中国北京市海淀区上地三街9号嘉华大厦B座409, Beijing 100085 (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:** CROSS-SUBNET CALLING

(54) 发明名称: 跨子网调用

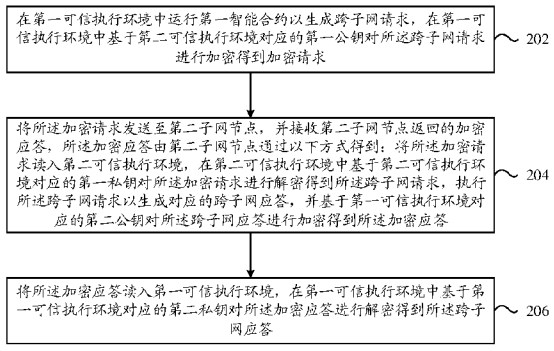

图 2

202 Run a first smart contract in a first trusted execution environment to generate a cross-subnet request, and in the first trusted execution environment, on the basis of a first public key corresponding to a second trusted execution environment, encrypt the cross-subnet request to obtain an encrypted request

204 Send the encrypted request to a second subnet node, and receive an encrypted response returned by the second subnet node, the encrypted response being obtained by the second subnet node by means of the following approach: reading the encrypted request into the second trusted execution environment, decrypting the encrypted request in the second trusted execution environment on the basis of a first private key corresponding to the second trusted execution environment to obtain the cross-subnet request, executing the cross-subnet request to generate a corresponding cross-subnet response, and encrypting the cross-subnet response on the basis of a second public key corresponding to the first trusted execution environment to obtain the encrypted response

206 Read the encrypted response into the first trusted execution environment, and decrypt the encrypted response in the first trusted execution environment on the basis of a second private key corresponding to the first trusted execution environment to obtain the cross-subnet response

(57) **Abstract:** The present description provides a cross-subnet calling method and apparatus, an electronic device, and a storage medium. The method is applied to a first subnet node in a first blockchain subnet managed by a blockchain mainnet; the first subnet node maintains a first trusted execution environment, the blockchain mainnet also manages a second blockchain subnet, and a second subnet node in the second blockchain subnet maintains a second trusted execution environment. The method comprises: running a first smart contract in the first trusted execution environment to generate a cross-subnet request and encrypting same to obtain an encrypted request; sending the encrypted request to the second subnet node, and receiving an encrypted response returned by the second subnet node, the encrypted response being obtained by the second subnet node by means of the following approach: reading the encrypted request into the second trusted execution environment for decryption to obtain the cross-subnet request, executing the cross-subnet request to generate a corresponding cross-subnet response, and encrypting same to obtain the encrypted response; and reading the encrypted response into the first trusted execution environment for decryption to obtain the cross-subnet response.

WO 2024/001022 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))。

(57) 摘要: 本说明书提供一种跨子网调用方法, 装置, 电子设备和存储介质. 其方法应用于由区块链主网所管理的第一区块链子网中的第一子网节点, 第一子网节点维护有第一可信执行环境, 区块链主网还管理有第二区块链子网, 第二区块链子网中的第二子网节点维护有第二可信执行环境; 该方法包括: 在第一可信执行环境中运行第一智能合约以生成跨子网请求并加密得到加密请求; 将加密请求发送至第二子网节点, 并接收第二子网节点返回的加密应答, 加密应答由第二子网节点通过以下方式得到: 将加密请求读入第二可信执行环境解密得到跨子网请求, 执行跨子网请求以生成对应的跨子网应答并加密得到加密应答; 将加密应答读入第一可信执行环境解密得到跨子网应答.

跨子网调用

技术领域

[01]本说明书实施例属于区块链技术领域，尤其涉及一种跨子网调用方法、装置、电子设备和存储介质。

背景技术

[02]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。

[03]在一些区块链网络中，部分节点有时存在实现小范围交易的需求，以避免其他节点获得这些交易及其相关数据，而这可以通过在区块链主网的基础上进一步建立区块链子网来实现。在区块链主网建立有多个区块链子网的场景下，不同的区块链子网之间具有跨子网调用的需求。

发明内容

[04]本发明的目的在于提供一种跨子网调用方法、装置、电子设备和存储介质。

[05]根据本说明书一个或多个实施例的第一方面，提出了一种跨子网调用方法，应用于由区块链主网所管理的第一区块链子网中的第一子网节点，第一子网节点维护有第一可信执行环境，所述区块链主网还管理有第二区块链子网，第二区块链子网中的第二子网节点维护有第二可信执行环境；所述方法包括：在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求；将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答；将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[06]根据本说明书一个或多个实施例的第二方面，提出了一种跨子网调用方法，应用于由区块链主网所管理的第二区块链子网中的第二子网节点，第二子网节点维护有第二可信执行环境，所述区块链主网还管理有第一区块链子网，第一区块链子网中的第一子网节点维护有第一可信执行环境；所述方法包括：接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成；将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应

的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到加密应答；将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[07]根据本说明书一个或多个实施例的第三方面，提出了一种跨子网调用装置，应用于由区块链主网所管理的第一区块链子网中的第一子网节点，第一子网节点维护有第一可信执行环境，所述区块链主网还管理有第二区块链子网，第二区块链子网中的第二子网节点维护有第二可信执行环境；所述装置包括：加密请求获取单元，用于在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求；加密请求发送单元，用于将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答；加密应答解密单元，用于将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[08]根据本说明书一个或多个实施例的第四方面，提出了一种跨子网调用装置，应用于由区块链主网所管理的第二区块链子网中的第二子网节点，第二子网节点维护有第二可信执行环境，所述区块链主网还管理有第一区块链子网，第一区块链子网中的第一子网节点维护有第一可信执行环境；所述装置包括：加密请求接收单元，用于接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成；加密应答获取单元，用于将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到加密应答；加密应答发送单元，用于将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[09]根据本说明书一个或多个实施例的第五方面，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和第二方面中任一项所述的方法。

[10]根据本说明书一个或多个实施例的第六方面，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和第二方面中任一项所述方法的步骤。

[11]在本说明书实施例中，第一子网节点与第二子网节点分别处于不同的区块链子网，在第一子网节点与第二子网节点之间进行跨子网调用的情况下，通过在第一子网节点与

第二子网节点分别维护相应的可信执行环境，能够确保第一子网节点与第二子网节点在节点运行过程中的安全性，而彼此又可以通过对方所处的可信执行环境对应的公钥对跨子网请求或跨子网应答进行加密传输，从而确保跨子网通讯过程的安全性，节点运行过程的安全性与跨子网通讯过程的安全性相互配合，最终实现整个跨子网调用过程的系统级别的安全性。

附图说明

[12]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。

[13]图 1 是一示例性实施例提供的一种基于区块链主网组建区块链子网的示意图。

[14]图 2 是一示例性实施例提供的一种跨子网调用方法的流程图。

[15]图 3 是一示例性实施例提供的一种跨子网调用方法的应用场景图。

[16]图 4 是一示例性实施例提供的另一种跨子网调用方法的应用场景图。

[17]图 5 是一示例性实施例提供的另一种跨子网调用方法的流程图。

[18]图 6 是一示例性实施例提供的一种设备的结构示意图。

[19]图 7 是一示例性实施例提供的一种跨子网调用装置的框图。

[20]图 8 是一示例性实施例提供的另一种跨子网调用装置的框图。

具体实施方式

[21]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。

[22]由于区块链网络的去中心化特性，使得区块链网络中的所有区块链节点均会维护相同的区块数据，无法满足部分节点的特殊需求。以联盟链为例，所有联盟成员（即联盟内的节点成员）可以组成一区块链网络，所有联盟成员在该区块链网络中分别存在对应的区块链节点，并可以通过对应的区块链节点获得该区块链网络上发生的所有交易和相关数据。但在一些情况下，可能存在部分联盟成员希望完成一些具有保密需求的交易，这些联盟成员既希望这些交易能够在区块链上存证或借助于区块链技术的其他优势，又能够避免其他联盟成员查看到这些交易和相关数据。虽然这些联盟成员可以额外组建一新的区块链网络，其建立方式与上述包含所有联盟成员的区块链网络类似，但是从头开始建立一条新的区块链网络需要消耗大量的资源，且无论是该区块链网络的建立过程或是建成后的配置过程都非常耗时。联盟成员之间的需求往往是临时的或者具有一定的时

效性，使得新建的区块链网络很快就会由于需求消失而失去存在的意义，从而进一步增加了上述区块链网络的建链成本。而联盟成员之间的需求经常会变化，而每一需求所对应的联盟成员也往往不同，因而每当联盟成员发生变化时就可能需要组建一新的区块链网络，从而造成资源和时间的大量浪费。

[23]为此，可以将已组建的区块链网络作为区块链主网，并在该区块链主网的基础上组建区块链子网。那么，在诸如上述的联盟链场景下，联盟成员可以在已经参与区块链主网的情况下，基于自身需求而在区块链主网的基础上组建所需的区块链子网。由于区块链子网是在区块链主网的基础上所建立，使得区块链子网的组建过程相比于完全独立地组建一条区块链网络，所消耗的资源和所需的耗时等都极大地降低，灵活性极高。

[24]基于区块链主网快捷组建区块链子网的过程如下：区块链主网中的各区块链节点分别获取组建区块链子网的交易，所述交易包含所述区块链子网的配置信息，所述配置信息包括参与组建所述区块链子网的节点成员的身份信息，所述区块链主网中的各区块链节点分别执行所述交易以透出所述配置信息，当所述配置信息包含第一区块链节点对应的节点成员的身份信息时，部署第一区块链节点的节点设备基于所述包含所述配置信息的创世块启动属于所述区块链子网的第二区块链节点。

[25]以图 1 所示为例，区块链主网为 subnet0，该 subnet0 包含的区块链节点为 nodeA、nodeB、nodeC、nodeD 和 nodeE 等。假定 nodeA、nodeB、nodeC 和 nodeD 希望组建一区块链子网：如果 nodeA 为管理员且仅允许管理员发起组建区块链子网的交易，那么可由 nodeA 向 subnet0 发起上述组建区块链子网的交易；如果 nodeE 为管理员且仅允许管理员发起组建区块链子网的交易，那么 nodeA~nodeD 需要向 nodeE 进行请求，使得 nodeE 向 subnet0 发起上述组建区块链子网的交易；如果 nodeE 为管理员但允许普通用户发起组建区块链子网的交易，那么 nodeA~nodeE 均可以向 subnet0 发起上述组建区块链子网的交易。当然，不论是管理员或者普通用户，发起组建区块链子网的交易的区块链节点并不一定参与所组建的区块链子网，比如虽然最终由 nodeA、nodeB、nodeC 和 nodeD 组建区块链子网，但可由 nodeE 向 subnet0 发起上述组建区块链子网的交易，而并不一定由 nodeA~nodeD 来发起该组建区块链子网的交易。

[26]在区块链主网的基础上组建区块链子网时，容易理解的是，会使得该区块链子网与区块链主网之间存在逻辑上的层次关系。比如在图 1 所示的 subnet0 上组建区块链子网 subnet1 时，可以认为 subnet0 处于第一层、subnet1 处于第二层。一种情况下，本说明书中的区块链主网可以为底层区块链网络，即区块链主网并非在其他区块链网络的基础上组建的区块链子网，比如图 1 中的 subnet0 可以认为属于底层区块链网络类型的区块链主网。另一种情况下，本说明书中的区块链主网也可以为其他区块链网络的子网，比如可以在图 1 中 subnet1 的基础上进一步组建另一区块链子网，此时可以认为 subnet1 为该区块链子网对应的区块链主网，而这并不影响该 subnet1 同时属于 subnet0 上创建的区块链子网。可见，区块链主网与区块链子网实际上是相对概念，同一区块链网络在一些情况下可以为区块链主网、另一些情况下可以为区块链子网。

[27]上述组建区块链子网的交易在被发送至区块链主网后，由区块链主网内的共识节点进行共识，并在通过共识后由各主网节点执行该交易，以完成区块链子网的组建。共识过程取决于所采用的共识机制，本说明书并不对此进行限制。

[28]通过在上述组建区块链子网的交易中包含配置信息，该配置信息可以用于对所组建的区块链子网进行配置，使得组建的区块链子网符合组网需求。例如，通过在配置信息中包含节点成员的身份信息，可以指定组建的区块链子网包含哪些区块链节点。

[29]节点成员的身份信息可以包括节点的公钥，或者采用节点 ID 等其他能够表征节点身份的信息，本说明书并不对此进行限制。以公钥为例，每个区块链节点都存在对应的一组或多组公私钥对，由区块链节点持有私钥而公钥被公开且唯一对应于该私钥，因而可以通过公钥来表征相应区块链节点的身份。因此，对于希望作为区块链子网的节点成员的区块链节点，可以将这些区块链节点的公钥添加至上述组建区块链子网的交易中，以作为上述节点成员的身份信息。上述的公私钥对可以用于签名验证的过程。例如，在采用有签名的共识算法中，譬如 subnet1 上述的 nodeA1 采用自身维护的私钥对消息进行签名后，将经过签名的消息在 subnet1 中广播，而 nodeB1、nodeC1 和 nodeD1 可以用 nodeA1 的公钥对收到的消息进行签名验证，以确认自身收到的消息确实来自 nodeA1 且没有经过篡改。

[30]第一主网节点可以为区块链主网上属于配置信息所指示的节点成员的区块链节点。在组建区块链子网时，并非由第一主网节点直接参与组建区块链子网、成为其节点成员，而是需要由用于部署该第一主网节点的节点设备生成第一子网节点，并由第一子网节点成为区块链子网中的节点成员。第一主网节点和第一子网节点对应于同一个区块链成员，比如在联盟链场景下对应于同一联盟链成员，但第一主网节点属于区块链主网、第一子网节点属于区块链子网，使得该区块链成员可以分别参与到区块链主网和区块链子网的交易中；并且，由于区块链主网和区块链子网属于相互独立的两个区块链网络，使得第一主网节点生成的区块与第一子网节点生成的区块分别存入所述节点设备上的不同存储（采用的存储譬如可以为数据库），实现了第一主网节点与第一子网节点分别使用的存储之间的相互隔离，因而区块链子网所产生的数据仅会在区块链子网的节点成员之间同步，使得仅参与了区块链主网的区块链成员无法获得区块链子网上产生的数据，实现了区块链主网与区块链子网之间的数据隔离，满足了部分区块链成员（即参与区块链子网的区块链成员）之间的交易需求。

[31]可见，第一主网节点和第一子网节点是在逻辑上划分出来的区块链节点，而从物理设备的角度来说，相当于上述部署了第一主网节点和第一子网节点的节点设备同时参与了区块链主网和区块链子网。由于区块链主网与区块链子网之间相互独立，使得这两个区块链网络的身份体系也相互独立，因而即便第一主网节点和第一子网节点可以采用完全相同的公钥，仍然应当将两者视为不同的区块链节点。譬如在图 1 中，subnet0 中的 nodeA 相当于第一主网节点，而部署该 nodeA 的节点设备生成了属于 subnet1 的 nodeA1，该 nodeA1 相当于第一子网节点。可见，由于身份体系相互独立，所以即便第一子网节点所采用的公钥区别于第一主网节点，也不影响本说明书方案的实施。

[32]当然，区块链子网的节点成员并不一定只是区块链主网的部分节点成员。在一些情况下，区块链子网的节点成员可以与区块链主网的节点成员完全一致，此时所有的区块链成员都可以获得区块链主网和区块链子网上的数据，但是区块链主网与区块链子网所产生的数据依然可以相互隔离，比如可以通过在区块链主网上实现一类业务、在区块链子网上实现另一类业务，从而可以使得这两类业务分别产生的业务数据之间相互隔离。

[33]除了上述的节点成员的身份信息之外，配置信息还可以包括下述至少之一：所述区块链子网的网络标识、所述区块链子网的管理员的身份信息、针对区块链平台代码的属性配置等，本说明书并不对此进行限制。网络标识用于唯一表征该区块链子网，因而该区块链子网的网络标识应当区别于区块链主网和该区块链主网上组建的其他区块链子网。区块链子网的管理员的身份信息，譬如可以为作为管理员的节点成员的公钥；其中，区块链主网与区块链子网的管理员可以相同，也可以不同。

[34]通过区块链主网来组建区块链子网的优势之一，就是由于生成第一子网节点的节点设备上已经部署了第一主网节点，因而可以将第一主网节点所使用的区块链平台代码复用在第一子网节点上，免去了区块链平台代码的重复部署，极大地提高了区块链子网的组建效率。那么，如果配置信息中未包含针对区块链平台代码的属性配置，第一子网节点可以复用第一主网节点上采用的属性配置；如果配置信息中包含了针对区块链平台代码的属性配置，第一子网节点可以采用该属性配置，使得第一子网节点所采用的属性配置不受限于第一主网节点的属性配置、与第一主网节点无关。针对区块链平台代码的属性配置可以包括下述至少之一：代码版本号、是否需要共识、共识算法类型、区块大小等，本说明书并不对此进行限制。

[35]组建区块链子网的交易包括调用合约的交易。该交易中可以指明被调用的智能合约的地址、调用的方法和传入的参数。例如，调用的合约可以为前述的创世合约或系统合约，调用的方法可以为组建区块链子网的方法，传入的参数可以包括上述的配置信息。在一实施例中，该交易可以包含如下信息：

from: Administrator

to: Subnet

method: AddSubnet(string)

string: genesis

[36]其中，from 字段为该交易的发起方的信息，譬如 Administrator 表明该发起方为管理员；to 字段为被调用的智能合约的地址，譬如该智能合约可以为 Subnet 合约，则 to 字段具体为该 Subnet 合约的地址；method 字段为调用的方法，譬如在 Subnet 合约中用于组建区块链子网的方法可以为 AddSubnet(string)，而 string 为 AddSubnet()方法中的参数，上述示例中通过 genesis 表征该参数的取值，该 genesis 具体为前述的配置信息。

[37]以 Subnet0 上的节点 nodeA~nodeE 执行调用 Subnet 合约中 AddSubnet()方法的交易为例。在交易通过共识后，nodeA~nodeE 分别执行 AddSubnet()方法并传入配置信息，得到相应的执行结果。

[38]区块链网络中的节点在执行调用智能合约的交易后，会生成相应的收据（receipt），以用于记录与执行该智能合约相关的信息。这样，可以通过查询交易的收据来获得合约执行结果的相关信息。合约执行结果可以表现为收据中的事件（event）。消息机制可以通过收据中的事件实现消息传递，以触发区块链节点执行相应的处理。事件的结构譬如可以为：

Event:

[topic][data]

[topic][data]

.....

[39]在上述示例中，事件的数量可以为一个或多个；其中，每个事件分别包括主题（topic）和数据（data）等字段。区块链节点可以通过监听事件的 topic，从而在监听到预定义的 topic 的情况下，执行预设处理，或者从相应事件的 data 字段读取相关内容，以及可以基于读取的内容执行预设处理。

[40]上述的事件机制中，相当于在监听方（比如存在监听需求的用户）处存在具有监听功能的客户端，譬如该客户端上运行了用于实现监听功能的 SDK 等，由该客户端对区块链节点产生的事件进行监听，而区块链节点只需要正常生成收据即可。除了上述的事件机制之外，还可以通过其他方式实现交易信息的透出。例如，可以通过在区块链节点运行的区块链平台代码中嵌入监听代码，使得该监听代码可以监听区块链交易的交易内容、智能合约的合约状态、合约产生的收据等其中的一种或多种数据，并将监听到的数据发送至预定义的监听方。由于监听代码部署于区块链平台代码中，而非监听方的客户端处，因而相比于事件机制而言，这种基于监听代码的实现方式相对更加的主动。其中，上述的监听代码可以由区块链平台的开发人员在开发过程中加入区块链平台代码，也可以由监听方基于自身的需求而嵌入，本说明书并不对此进行限制。

[41]可见，上述 Subnet 合约的执行结果可以包括所述配置信息，该执行结果可以处于前文所述的收据中，该收据中可以包含与执行 AddSubnet()方法相关的 event，即组网事件。组网事件的 topic 可以包含预定义的组网事件标识，以区别于其他的事件。譬如在与执行 AddSubnet()方法相关的 event 中，topic 的内容为关键词 subnet，且该关键词区别于其他方法所产生 event 中的 topic。那么，nodeA~nodeE 通过监听生成的收据中各个 event 所含的 topic，可以在监听到包含关键词 subnet 的 topic 的情况下，确定监听到与执行 AddSubnet()方法相关的 event，即组网事件。例如，收据中的 event 如下：

Event:

[topic:other][data]

[topic:subnet][data]

.....

[42]那么，nodeA~nodeE 在监听到第 1 条 event 时，由于所含 topic 的内容为 other，确定该 event 与 AddSubnet()方法无关；以及，nodeA~nodeE 在监听到第 2 条 event 时，由于所含 topic 的内容为 subnet，确定该 event 与 AddSubnet()方法相关，并进而读取该 event 对应的 data 字段，该 data 字段包含上述的配置信息。以配置信息包括区块链子网的节点成员的公钥为例，data 字段的内容例如可以包括：

{subnet1;

nodeA 的公钥，nodeA 的 IP、nodeA 的端口号…;

nodeB 的公钥，nodeB 的 IP、nodeB 的端口号…;

nodeC 的公钥，nodeC 的 IP、nodeC 的端口号…；

nodeD 的公钥，nodeD 的 IP、nodeD 的端口号…；

}

[43]其中，subnet1 为希望创建的区块链子网的网络标识。区块链主网中的各个区块链节点可以记录该区块链主网上已创建的所有区块链子网的网络标识，或者与这些区块链子网相关的其他信息，这些信息譬如可以维护在上述的 Subnet 合约中，具体可以对应于该 Subnet 合约所含的一个或多个合约状态的取值。那么，nodeA~nodeE 可以根据记录的已创建的所有区块链子网的网络标识，确定上述的 subnet1 是否已经存在；如果不存在，说明 subnet1 是当前需要创建的新区块链子网，如果存在则说明 subnet1 已经存在。

[44]除了采用希望创建的新的区块链子网的网络标识之外，还可以采用预定义的新建网络标识，该新建网络标识表明相应的组网事件用于组建新的区块链子网。例如，可以将上述的 subnet1 替换为 newsubnet，该 newsubnet 为预定义的新建网络标识，nodeA~nodeE 在识别到 data 字段包含 newsubnet 时，即可确定包含该 newsubnet 的 event 为组网事件，需要创建新的区块链子网。

[45]除了网络标识 subnet1 之外，上述 data 字段中还包含各个节点成员的身份信息等内容。部署第一主网节点的节点设备可以监听生成的收据，并在监听到所述组网事件且所述组网事件的内容表明第一主网节点属于所述节点成员的情况下，由部署第一主网节点的节点设备获取所述组网事件包含的配置信息或创世块。或者，第一区块链节点可以监听生成的收据，并在监听到所述组网事件且所述组网事件的内容表明第一区块链节点属于所述节点成员的情况下，触发部署第一区块链节点的节点设备获取所述组网事件包含的所述配置信息或所述创世块。

[46]如前所述，节点设备可以直接监听收据。假定 nodeA~nodeE 分别部署在节点设备 1~5 上，节点设备 1~5 可以监听 nodeA~nodeE 分别生成的收据，那么在监听到 subnet1 是需要新组建的区块链子网的情况下，节点设备 1~5 会进一步识别 data 字段中包含的节点成员的身份信息，以确定自身的处理方式。以 nodeA 和节点设备 1 为例：如果节点设备 1 发现 data 字段包含 nodeA 的公钥、IP 地址和端口号等身份信息，那么节点设备 1 在基于上述的消息机制从 data 字段获得配置信息的情况下，生成包含该配置信息的创世块，且节点设备 1 会在本地部署 nodeA1，进而由 nodeA1 加载生成的创世块，从而成为 subnet1 的子网节点；类似地，节点设备 2 可以生成 nodeB1、节点设备 3 可以生成 nodeC1、节点设备 4 可以生成 nodeD1。以及，节点设备 5 会发现 data 字段包含的身份信息与自身均不匹配，则该节点设备 5 不会根据 data 字段中的配置信息生成创世块，也不会生成 subnet1 中的区块链节点。

[47]如前所述，区块链主网中的区块链节点可以监听收据，并根据监听结果触发节点设备执行相关处理。例如，nodeA~nodeE 在确定 subnet1 是需要新组建的区块链子网的情况下，会进一步识别 data 字段中包含的节点成员的身份信息，以确定自身的处理方式。比如，nodeA~nodeD 会发现在 data 字段包含自身的公钥、IP 地址和端口号等身份信息，假定 nodeA~nodeD 分别部署在节点设备 1~4 上，以 nodeA 和节点设备 1 为例： nodeA 会触发节点设备 1，使得节点设备 1 基于上述的消息机制从 data 字段获得配置信息并生

成包含该配置信息的创世块，且节点设备 1 会在本地部署 nodeA1，该 nodeA1 加载生成的创世块，从而成为 subnet1 中的 1 个子网节点；类似地，nodeB 会触发节点设备 2 生成 nodeB1、nodeC 会触发节点设备 3 生成 nodeC1、nodeD 会触发节点设备 4 生成 nodeD1。以及，nodeE 会发现 data 字段包含的身份信息与自身均不匹配，假定 nodeE 部署在节点设备 5 上，那么该节点设备 5 不会根据 data 字段中的配置信息生成创世块，也不会生成 subnet1 中的节点。

[48]如前所述，第一主网节点与第一子网节点并不一定采用相同的身份信息。因此，在上述实施例中，data 字段中可以包含预先为 nodeA1~nodeD1 生成的身份信息，且区别于 nodeA~nodeD 的身份信息。仍以 nodeA 和节点设备 1 为例：节点设备 1 如果在 data 字段中发现了 nodeA1 的身份信息，可以生成创世块、部署 nodeA1，并由 nodeA1 加载该创世块；或者，nodeA 如果在 data 字段中发现了 nodeA1 的身份信息，那么 nodeA 会触发节点设备 1 生成创世块、部署 nodeA1，并由 nodeA1 加载该创世块。其他区块链节点或节点设备的处理方式类似，此处不再一一赘述。

[49]除了配置信息之外，合约的执行结果可以包括创世块。换言之，除了可以在 data 字段中包含配置信息，还可以直接在执行合约调用的过程中生成包含配置信息的创世块，从而将创世块包含于 data 字段中，那么对于上述的 nodeA~nodeD 而言，相应的节点设备 1~4 可以通过消息机制直接从 data 字段获得创世块，而无需自行生成，可以提升对 nodeA1~nodeD1 的部署效率。

[50]节点设备通过在该进程中创建一个运行区块链平台代码的实例，实现在该节点设备上部署一区块链节点。对于第一主网节点而言，由节点设备在上述进程中创建第一实例，并由该第一实例运行区块链平台代码而形成。类似地，对于第一子网节点而言，由节点设备在上述进程中创建区别于第一实例的第二实例，并由该第二实例运行区块链平台代码而形成。例如，节点设备可以首先在进程中创建第一实例，以形成区块链主网中的第一区块链节点；而当该节点设备对应的节点成员希望参与组建区块链子网时，可以在上述进程中创建第二实例，该第二实例区别于上述的第一实例，并由该第二实例形成区块链子网中的第二区块链节点。当第一实例与第二实例位于同一进程时，由于不涉及跨进程交互，可以降低对第一子网节点的部署难度、提高部署效率；当然，第二实例也可能与第一实例分别处于节点设备上的不同进程中，本说明书并不对此进行限制；例如，节点设备可以在第一进程中创建第一实例，以形成区块链主网中的第一区块链节点；而当该节点设备对应的节点成员希望参与组建区块链子网时，可以启动区别于第一进程的第二进程，并在该第二进程中创建第二实例，该第二实例区别于上述的第一实例，进而由该第二实例形成区块链子网中的第二区块链节点。事实上，本说明书实施例中涉及的任一节点设备上部署的各区块链节点均为运行在所述任一节点设备上的不同的区块链实例，任一节点设备上部署的各区块链节点生成的区块分别存入所述任一节点设备上的不同存储（例如数据库），且任一节点设备部署的各区块链节点分别使用的存储之间相互隔离。

[51]通过上述方式，可以在区块链主网上创建出区块链子网。以图 1 为例，subnet0 原本包含 nodeA~nodeE，而在 subnet0 的基础上可以组建出 subnet1，该 subnet1 包含 nodeA1~nodeD1，且 nodeA 与 nodeA1、nodeB 与 nodeB1、nodeC 与 nodeC1、nodeD 与

nodeD1 分别部署在同一节点设备上。类似地，还可以在 subnet0 上组建出 subnet2 或更多的区块链子网，其中 subnet2 包含 nodeA2、nodeB2、nodeC2 和 nodeE2，且 nodeA 与 nodeA1、nodeA2，nodeB 与 nodeB1、nodeB2，nodeC、nodeC1 与 nodeC2，nodeD 与 nodeD1，nodeE 与 nodeE2 分别部署在同一节点设备上。以及，可以将 subnet1、subnet2 等作为新的区块链主网，并在此基础上进一步组建出区块链子网，其过程与 subnet1 或 subnet2 的组建相似，此处不再赘述。可见，上述在区块链主网上发起交易选取节点成员以创建区块链子网的方式，可以使得新创建的区块链子网的子网节点均部署在区块链主网的主网节点所在的节点设备上，也就是从节点设备的角度上来说，区块链子网的子网节点所在的节点设备属于主网节点所在节点设备的子集，换言之，部署有区块链子网的子网节点所处的节点设备上部署有区块链主网中的主网节点。

[52]除了通过上述在区块链主网上发起交易选取节点成员以创建区块链子网的方式，还可以通过其他手段创建区块链子网，并使得其受到区块链主网的管理。例如，可以通过注册方式在区块链主网上组建区块链子网（后续简称注册组网方式），将现有区块链网络直接注册至区块链主网，使新注册的区块链网络受到区块链主网的管理，从而使得新注册的区块链网络成为区块链主网的区块链子网。通过注册组网方式，待组建区块链子网的子网信息被直接注册至区块链主网，使得区块链主网获取待组建区块链子网的相关信息（通过接收并执行待组建区块链网络发出的、用于将其身份信息与分配至该待组建区块链网络的子网标识进行关联存证的交易），例如待组建区块链子网的子网标识和运行状态，其中各节点成员的公钥和插件配置信息、各节点设备的 IP 地址和端口信息等，这些信息会被写入区块链主网对应的系统合约的合约状态中，由此区块链主网将获取该待组建区块链子网的管理权，在完成注册后，便意味着区块链子网组建完成。由于注册组网方式并不需要通过交易在区块链主网上指定节点成员构成区块链子网，因此通过注册组网方式组建的区块链子网中的子网节点可以与部署在区块链主网中各节点的节点设备完全不同或部分不同，例如图 1 中 subnet0 以注册组网方式创建了一个 subnet4（图 1 中未示出），假设 subnet0 自身所包含的主网节点 nodeA~nodeE 分别部署于节点设备 1~5，那么 subnet4 对应的子网节点可以部署于除节点设备 1~5 外的其他任意节点设备上，或者，subnet4 中的其中一个或多个子网节点分别部署于节点设备 1~5 内的任意节点设备（但仍需要保证一个节点设备上仅部署 subnet4 中的一个子网节点），而 subnet4 中的其他的子网节点部署于除节点设备 1~5 外的其他任意节点设备上，当然，subnet4 中的子网节点也可以均部署于节点设备 1~5 之中。

[53]下面结合图 2 对本说明书涉及的跨子网调用方法进行详细说明。图 2 是一示例性实施例提供的一种跨子网调用方法的流程图。该方法应用于由区块链主网所管理的第一区块链子网中的第一子网节点，第一子网节点维护有第一可信执行环境，所述区块链主网还管理有第二区块链子网，第二区块链子网中的第二子网节点维护有第二可信执行环境；所述方法包括：

[54]S202：在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求。

[55]在本说明书实施例中，第一区块链子网与第二区块链子网均是按照前述创建区块链

子网的方式在区块链主网的基础上所创建，其中，任一区块链子网均受到区块链主网的管理，具体可以表现为：区块链主网可以通过调用区块链主网所部署的子网管理合约来实现对各区块链子网的节点启停、网络结构调整等管理功能。

[56]第一子网节点维护有第一可信执行环境，其可以将节点运行过程中的交易执行、共识过程、合约运行等计算任务置入第一可信执行环境中再进行执行，在这个过程中，第一子网节点会将第一可信执行环境外部的密文数据读入第一可信执行环境后解密为明文数据再进行操作，因此，第一子网节点可以利用第一可信执行环境的机密性来确定第一子网节点在节点运行层面的安全性。同理，第二子网节点也维护有第二可信执行环境，其同样可以通过上述方式以利用第二可信执行环境来实现第二子网节点在节点运行层面的安全性。

[57]在本说明书实施例中，第一区块链子网或第二区块链子网中的任一子网节点均可以部署有相应的可信执行环境，并按照上述方式实现各自节点运行层面的安全性，在这种场景下，第一区块链子网与第二区块链子网称之为TEE(Trusted Execution Environment，可信执行环境）链。

[58]第一子网节点在第一可信执行环境中运行第一智能合约时，第一智能合约可能产生针对其他区块链子网的跨子网调用需求，例如生成指向第二区块链子网中的第二子网节点的跨子网请求，此时就要求将跨子网请求传输至第二子网节点并被响应执行，同时接收第二子网节点执行跨子网请求所生成的跨子网响应。然而，为了确保跨子网请求和跨子网应答在可信执行环境外部的传输过程（跨子网通讯）中的安全性，有必要对它们事先在可信执行环境中进行加密处理后再进行跨子网通讯。因此，第一子网节点不会直接将第一可信执行环境中运行的第一智能合约所生成的跨子网请求直接发送至第二子网节点，而是首先在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求，然后再将该加密请求发送至第二子网节点。为了确保加密请求能够被正确路由至第二子网节点，在加密过程中会保留原跨子网请求中特定的字段不进行加密，例如第二子网节点的身份信息（IP 地址、节点公钥或其他身份标识）第二区块链子网的标识信息等。

[59]在本说明书实施例中，第一可信执行环境维护有对应的公私钥对（第二公钥和第二私钥）以实现第一可信执行环境内外部数据的加解密过程，其中，第二私钥由第一可信执行环境独自持有，第二公钥则对外公开。同理，第二可信执行环境也维护有对应的公私钥对（第一公钥和第一私钥）以实现第二可信执行环境内外部数据的加解密过程，其中，第一私钥由第二可信执行环境独自持有，第一公钥对外公开。

[60]因此，当在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求后，该加密请求理论上只能在唯一持有第一私钥的第二子网节点所维护的第二可信执行环境中解密，从而使得加密请求在可信执行环境外部的传输过程中即使被第三方捕获，第三方也会因为缺少第一私钥而将其无法解密还原得到明文状态的跨子网请求，从而确保跨子网通讯过程的安全性，而这种加密请求由于同时具有区块链交易的性质和机密性因此属于一种隐私交易。

[61]在本说明书实施例中，第一智能合约由第一子网节点通过在第一可信执行环境中加

载第一智能合约程序而运行于第一可信执行环境中，其中，第一智能合约程序由第一子网节点将从第一可信执行环境外部读入的第一智能合约程序密文在第一可信执行环境中解密得到。第一智能合约运行在第一可信执行环境中，实际上是第一子网节点在第一可信执行环境中加载第一智能合约程序的结果，由于第一可信执行环境本质上是一段物理隔离的执行环境，其中运行的程序均被加载在隔离的内存上，因此对于暂时不需要运行在第一可信执行环境中的程序，需要进行持久化存储。而为了确保信息安全，对于在第一可信执行环境中运行的任何程序，均遵循“可信执行环境内部解密加载，可选执行环境外部加密存储”的原则，因此，第一智能合约程序本质上是从第一可信执行环境外部读取到的第一智能合约程序密文在第一可信执行环境内部解密的结果，例如，第一智能程序密文是由第一智能合约程序通过第二公钥被加密存储在第一可信执行环境外部，同时在第一可信执行环境内部可以通过第二私钥被解密为第一智能合约程序，而类似第一智能合约这种在可信执行环境内部明文执行但在可信执行环境外部加密存储的智能合约被称为隐私合约。

[62]S204: 将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答。

[63]第一子网节点在第一可信执行环境中对跨子网请求进行加密得到加密请求后，可以通过跨子网通讯将加密请求发送至第二子网节点。

[64]不同区块链子网中子网节点之间的跨子网通讯主要是通过各自所处节点设备上部署的主网节点之间预先建立的网络连接链路所实现。以图 1 为例，第一区块链子网 subnet1 中的第一子网节点 nodeC1 所处的节点设备 3 上还部署有区块链主网 subnet0 中的主网节点 nodeC，而第二区块链子网 subnet2 中的第二子网节点 nodeE2 所处的节点设备 5 上还部署有 subnet0 中的主网节点 nodeE。假设 nodeC1 希望向第 nodeE2 发送加密请求，虽然 subnet1 和 subnet2 之间（nodeC 和 nodeE 之间）不存在直接的网络连接链路，但由于节点设备 3 上部署的 nodeC 和节点设备 5 上部署的 nodeE 之间已经预先建立有形成 subnet0 时所实现的网络连接链路，且该网络连接链路可以使节点设备 3 与节点设备 5 进行相互通讯，因此，nodeC1 可以通过 nodeC 与 nodeE 之间建立的网络连接链路，从而将加密请求发送至从节点设备 3 发送至节点设备 5，并最终由节点设备 5 路由至其本地部署的 nodeE2。在一实施例中，形成 subnet0 时所实现的网络连接链路即为 subnet0 中各主网节点之间建立的用于对交易进行共识的共识链路和/或用于对区块进行同步的同步链路。

[65]在本说明书实施例中，同一节点设备上的主网节点和子网节点共享该节点设备上运行的区块链通讯插件，例如 P2P（Peer to Peer，对等网络通讯）插件，而上述形成 subnet0 时所实现的网络连接链路具体是通过 nodeC 和 nodeE 分别采用节点设备 3 和节点设备 5 上的 P2P 插件所建立，由于节点设备上的 P2P 插件可以被该节点设备上各个区块链节点所共享，因此 subnet1 中的 nodeC1 可以通过调用节点设备 3 本地运行的 P2P 插件，借助形成 subnet0 时所实现的节点设备 3 与节点设备 5 之间基于 P2P 插件的网络连接，建

立与 nodeE2 所属节点设备 5 上运行的 P2P 插件之间的网络连接，由此将加密请求发送至节点设备 5，从而进一步实现与 nodeE2 之间的网络通讯。因此，第一区块链子网与第二区块链子网之间无需建立新的网络连接链路，而是通过底层区块链主网预先建立的网络连接链路，实现第一区块链子网中第一子网节点与第二区块链子网中第二子网节点之间的跨子网通讯。

[66]在第二子网节点接收到加密应答后，第二子网节点会将该加密应答读入其所维护的第二可信执行环境，并在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密已获取跨子网请求。在获取跨子网请求后，第二子网节点进一步在第二可信执行环境中执行跨子网请求以生成对应的跨子网应答，例如，调用第二可信执行环境中运行的第二智能合约执行所述跨子网请求以生成跨子网应答，即所述跨子网应答由第二可信执行环境中运行的第二智能合约执行所述跨子网请求所生成，在跨子网请求为查询第二智能合约中特定区块高度下的特定合约状态的情况下，跨子网应答中便包含对应的特定合约状态。在第二子网节点获取到跨子网应答后，同样出于跨子网通讯安全性的考虑，会在第二可信执行环境中基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答，然后再将所述加密应答输出第二可信执行环境并回调至第一子网节点，此时加密应答在可信执行环境外部的传输过程即使被第三方捕获，第三方也会因为缺少第二私钥而将其无法解密还原得到明文状态的跨子网应答，从而确保跨子网通讯过程的安全性，而这种加密应答同样属于一种隐私交易。

[67]在本说明书实施例中，第二智能合约由第二子网节点通过在第二可信执行环境中加载第二智能合约程序而运行于第二可信执行环境中，其中，第二智能合约程序由第二子网节点将从第二可信执行环境外部读入的第二智能合约程序密文在第二可信执行环境中解密得到。第二智能合约运行在第二可信执行环境中，实际上是第二子网节点在第二可信执行环境中加载第二智能合约程序的结果，由于第二可信执行环境本质上是一段物理隔离的执行环境，其中运行的程序均被加载在隔离的内存上，因此对于暂时不需要运行在第二可信执行环境中的程序，需要进行持久化存储。而为了确保信息安全，对于在第二可信执行环境中运行的任何程序，均遵循“可信执行环境内部解密加载，可选执行环境外部加密存储”的原则，因此，第二智能合约程序本质上是从第二可信执行环境外部读取到的第二智能合约程序密文在第二可信执行环境内部解密的结果。例如，在第二子网节点接收到加密消息并在第二可信执行环境中解密得到跨子网请求的情况下，进一步发现该跨子网请求是用于调用第二智能合约的跨子网请求，于是第二子网节点可以直接调用第二可信执行环境中正在运行的第二智能合约执行该跨子网请求，或者将第二智能程序密文从第二可信执行环境外部读入第二可信执行环境内部并通过第一私钥解密为第二智能合约程序后，临时在第二可信执行环境中通过加载第二智能合约程序，从而实现在第二可信执行环境中运行第二智能合约，最后再调用运行状态下的第二智能合约执行该跨子网请求。与第一智能合约类似，第二智能合约同样也属于一种隐私合约。

[68]第二子网节点向第一子网节点发送加密应答的过程，与第一子网节点向第二子网节点发送加密请求的过程类似，均是基于跨子网通讯所实现的，其详细过程这里不再赘述。

[69]S206：将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[70]在第一子网节点接收到加密应答后，可以将其读入第一可信执行环境中，并在第一可信执行环境中使用第一可信执行环境所唯一持有的第二私钥对加密应答进行解密以获取跨子网应答。至此，本说明书实施例完整地实现了第一子网节点向第二子网节点发起跨子网调用的过程。

[71]在本说明书实施例中，第一子网节点与第二子网节点分别处于不同的区块链子网，在第一子网节点与第二子网节点之间进行跨子网调用的情况下，通过在第一子网节点与第二子网节点分别维护相应的可信执行环境，能够确保第一子网节点与第二子网节点在节点运行过程中的安全性，而彼此又可以通过对方所处的可信执行环境对应的公钥对跨子网请求或跨子网应答进行加密传输，从而确保跨子网通讯过程的安全性，节点运行过程的安全性与跨子网通讯过程的安全性相互配合，最终实现整个跨子网调用过程的系统级别的安全性。

[72]可选的，所述跨子网请求包括：由第二区块链子网中各子网节点共同参与执行的共识交易，或者仅由第二子网节点独立执行的本地交易。

[73]在本说明书实施例中，跨子网请求可以为共识交易或本地交易。其中，在跨子网请求为共识交易的情况下，当第二子网节点接收到跨子网请求后，跨子网请求会像普通的区块链交易那样在第二区块链子网中进行共识、执行、成块并上链至区块链账本，这意味着第二区块链子网中的所有子网节点（包括第二子网节点）均会执行该跨子网请求以生成对应的跨子网应答，同时改变第二区块链子网的世界状态，并通过其中一个选举出的子网节点（例如第二子网节点）返回相应的跨子网应答。

[74]本说明书实施例所涉及的本地交易是指不参与区块链共识、成块、上链的交易，其仅作为一种内部的调用媒介；在跨子网请求为本地交易的情况下，当第二子网节点接收到跨子网请求后，第二子网节点将独立执行跨子网请求以生成对应的跨子网应答，不会共识也不会改变世界状态，而只是在本地完成执行后将跨子网应答以回调方式返回至第一子网节点。由于作为本地交易的跨子网请求不需要进行共识、成块与上链，因此，本说明书实施例可以将计算量限制在第二子网节点内部，减少第二区块链网络整体响应于跨子网请求的计算负担，提高跨子网请求的执行效率。

[75]可选的，第一子网节点与第二子网节点部署于相同或不同的节点设备。

[76]如图 3 所示，图 3 是在图 1 的基础上将 nodeC1 作为第一子网节点而 nodeE2 作为第二子网节点的应用场景图，作为一个第一子网节点与第二子网节点部署于不同的节点设备的实施例，节点设备 3 上同时部署有属于 subnet0 的 nodeC、属于 subnet1 的 nodeC1 以及属于 subnet2 中的 nodeC2，其中，nodeC、nodeC1 和 nodeC2 具体为节点设备 3 在本地部署的虚拟机中运行预先部署的区块链平台代码所形成的区块链节点实例（下称区块链节点），而 nodeC 作为区块链节点在运行过程中的相关数据保存在 nodeC 对应的数据库中，nodeC1 和 nodeC2 作为其他区块链节点在运行过程中的相关数据则分部保存在 nodeC1 和 nodeC2 对应的数据库中。类似的，节点设备 5 上同时部署有属于 subnet0 的 nodeE 和属于 subnet2 的 nodeE2。另外，任一节点设备中可以部署有区块链共识代码，节点设备可以运行该共识代码以在本地形成共识组件实例；以及，节点设备中还可以部署有以插件形式管理的 P2P（Peer to Peer，对等网络通讯）组件代码，节点设备可以运

行该 P2P 组件代码以在本地形成 P2P 组件实例，也即 P2P 插件，例如图 3 中节点设备 3 和节点设备 5 就均在本地运行有 P2P 插件，该 P2P 插件可以被同一节点设备上的不同区块链节点所共享使用，例如节点设备 3 中 nodeC、nodeC1 和 nodeC2 可以调用节点设备 3 上运行的同一个 P2P 插件，以共享其功能和数据，例如实现跨子网通讯。nodeC1 维护有第一可信执行环境，nodeC1 所部署的第一智能合约就能够以明文形式运行在第一可信执行环境中，类似的，nodeE2 也维护有第二可信执行环境，nodeE2 所部署的第二智能合约也能够以明文形式运行在第二可信执行环境中。在本说明书实施例中，第一子网节点与第二子网节点之间的跨子网通讯具体是跨节点设备的通讯，其传输数据在路由过程可能会途径第一子网节点和第二子网节点分别所处的节点设备以外的其他节点设备。

[77]如图 4 所示，图 4 是在图 1 的基础上将 nodeC1 作为第一子网节点而 nodeC2 作为第二子网节点的应用场景图，作为一个第一子网节点与第二子网节点部署于相同的节点设备的实施例，节点设备 3 上同时部署有属于 subnet0 的 nodeC、属于 subnet1 的 nodeC1 以及属于 subnet2 中的 nodeC2，节点设备 3 在本地运行有 P2P 插件，该 P2P 插件可以被节点设备 3 中 nodeC、nodeC1 和 nodeC2 共享数据和功能。在本说明书实施例中，同一节点设备（节点设备 3）中维护有多个可信执行环境（第一可信执行环境和第二可信执行环境），nodeC1 维护有第一可信执行环境，nodeC1 所部署的第一智能合约就能够以明文形式运行在第一可信执行环境中，nodeC2 也维护有第二可信执行环境，nodeC2 所部署的第二智能合约也能够以明文形式运行在第二可信执行环境中。在本说明书实施例中，第一子网节点与第二子网节点之间的跨子网通讯具体是节点设备内部的跨进程通讯，其传输数据不会经由第一子网节点和第二子网节点共同所处的节点设备以外的其他节点设备，而只会途径节点设备本地运行的 P2P 插件，在第一子网节点与第二子网节点之间进行流转。

[78]可选的，还包括：将跨子网交易密文读入第一可信执行环境，在第一可信执行环境中对所述跨子网交易密文进行解密得到跨子网交易，并调用第一智能合约执行所述跨子网交易以生成所述跨子网请求。

[79]在本说明书实施例中，第一智能合约是在执行跨子网交易的情况下生成的所述跨子网请求，而所述跨子网请求是通过将从第一可信执行环境外部读入的跨子网交易密文在第一可信执行环境内部解密得到的。具体而言，交易发起方可以向第一区块链网络发起跨子网交易密文，该跨子网交易密文由第一区块链网络中的各子网节点（包括第一子网节点）进行共识并执行，第一子网节点在需要执行跨子网交易密文时，需要首先将跨子网交易密文读入第一可信执行环境中解密（例如基于第二私钥进行解密）得到跨子网交易，然后可以直接调用第一可信执行环境中正在运行的第一智能合约执行该跨子网交易，或者将第一智能程序密文从第一可信执行环境外部读入第一可信执行环境内部并通过第一私钥解密为第一智能合约程序后，临时在第一可信执行环境中通过加载第一智能合约程序，从而实现在第一可信执行环境中运行第一智能合约，最后再调用运行状态下的第一智能合约执行该跨子网交易以生成跨子网请求。本说明书实施例所涉及的跨子网交易属于隐私交易。

[80]图 5 是一示例性实施例提供的另一种跨子网调用方法的流程图。该方法应用于由区块链主网所管理的第二区块链子网中的第二子网节点，第二子网节点维护有第二可信执

行环境，所述区块链主网还管理有第一区块链子网，第一区块链子网中的第一子网节点维护有第一可信执行环境；所述方法包括 S502 至 S506。

[81]S502：接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成。

[82]S504：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到加密应答。

[83]S506：将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[84]图 6 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 6，在硬件层面，该设备包括处理器 602、内部总线 604、网络接口 606、内存 608 以及非易失性存储器 610，当然还可能包括其他业务所需要的硬件。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 602 从非易失性存储器 610 中读取对应的计算机程序到内存 608 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。

[85]如图 7 所示，图 6 是本说明书根据一示例性实施例提供的一种跨子网调用装置的框图，该装置可以应用于如图 6 所示的设备中，以实现本说明书的技术方案；所述装置应用于由区块链主网所管理的第一区块链子网中的第一子网节点，第一子网节点维护有第一可信执行环境，所述区块链主网还管理有第二区块链子网，第二区块链子网中的第二子网节点维护有第二可信执行环境；所述装置包括：加密请求获取单元 701，用于在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求；加密请求发送单元 702，用于将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答；加密应答解密单元 703，用于将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[86]可选的，第一智能合约由第一子网节点通过在第一可信执行环境中加载第一智能合约程序而运行于第一可信执行环境中，其中，第一智能合约程序由第一子网节点将从第一可信执行环境外部读入的第一智能合约程序密文在第一可信执行环境中解密得到。

[87]可选的，所述跨子网应答由第二可信执行环境中运行的第二智能合约执行所述跨子

网请求所生成。

[88]可选的，第二智能合约由第二子网节点通过在第二可信执行环境中加载第二智能合约程序而运行于第二可信执行环境中，其中，第二智能合约程序由第二子网节点将从第二可信执行环境外部读入的第二智能合约程序密文在第二可信执行环境中解密得到。

[89]可选的，所述跨子网请求包括：由第二区块链子网中各子网节点共同参与执行的共识交易，或者仅由第二子网节点独立执行的本地交易。

[90]可选的，第一子网节点与第二子网节点部署于相同或不同的节点设备。

[91]可选的，还包括：跨子网交易执行单元 704，用于将跨子网交易密文读入第一可信执行环境，在第一可信执行环境中对所述跨子网交易密文进行解密得到跨子网交易，并调用第一智能合约执行所述跨子网交易以生成所述跨子网请求。

[92]如图 8 所示，图 8 是本说明书根据一示例性实施例提供的另一种跨子网调用装置的框图，该装置可以应用于如图 6 所示的设备中，以实现本说明书的技术方案；所述装置应用于由区块链主网所管理的第二区块链子网中的第二子网节点，第二子网节点维护有第二可信执行环境，所述区块链主网还管理有第一区块链子网，第一区块链子网中的第一子网节点维护有第一可信执行环境；所述装置包括：加密请求接收单元 801，用于接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成；加密应答获取单元 802，用于将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到加密应答；加密应答发送单元 803，用于将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

[93]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。

[94]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。

[95]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。

[96]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。

[97]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。

[98]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。

[99]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。

[100]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。

[101]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。

[102]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。

[103]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。

[104]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。

[105]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。

[106]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。

[107]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。

权利要求书

1. 一种跨子网调用方法，应用于由区块链主网所管理的第一区块链子网中的第一子网节点，第一子网节点维护有第一可信执行环境，所述区块链主网还管理有第二区块链子网，第二区块链子网中的第二子网节点维护有第二可信执行环境；所述方法包括：

在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求；

将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答；

将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

2. 根据权利要求 1 所述的方法，第一智能合约由第一子网节点通过在第一可信执行环境中加载第一智能合约程序而运行于第一可信执行环境中，其中，第一智能合约程序由第一子网节点将从第一可信执行环境外部读入的第一智能合约程序密文在第一可信执行环境中解密得到。

3. 根据权利要求 1 所述的方法，所述跨子网应答由第二可信执行环境中运行的第二智能合约执行所述跨子网请求所生成。

4. 根据权利要求 3 所述的方法，第二智能合约由第二子网节点通过在第二可信执行环境中加载第二智能合约程序而运行于第二可信执行环境中，其中，第二智能合约程序由第二子网节点将从第二可信执行环境外部读入的第二智能合约程序密文在第二可信执行环境中解密得到。

5. 根据权利要求 1 所述的方法，所述跨子网请求包括：由第二区块链子网中各子网节点共同参与执行的共识交易，或者仅由第二子网节点独立执行的本地交易。

6. 根据权利要求 1 所述的方法，第一子网节点与第二子网节点部署于相同或不同的节点设备。

7. 根据权利要求 1 所述的方法，还包括：

将跨子网交易密文读入第一可信执行环境，在第一可信执行环境中对所述跨子网交易密文进行解密得到跨子网交易，并调用第一智能合约执行所述跨子网交易以生成所述跨子网请求。

8. 一种跨子网调用方法，应用于由区块链主网所管理的第二区块链子网中的第二子网节点，第二子网节点维护有第二可信执行环境，所述区块链主网还管理有第一区块链子网，第一区块链子网中的第一子网节点维护有第一可信执行环境；所述方法包括：

接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成；

将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应

答进行加密得到加密应答;

将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

9. 一种跨子网调用装置，应用于由区块链主网所管理的第一区块链子网中的第一子网节点，第一子网节点维护有第一可信执行环境，所述区块链主网还管理有第二区块链子网，第二区块链子网中的第二子网节点维护有第二可信执行环境；所述装置包括:

加密请求获取单元，用于在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求;

加密请求发送单元，用于将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答;

加密应答解密单元，用于将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

10. 一种跨子网调用装置，应用于由区块链主网所管理的第二区块链子网中的第二子网节点，第二子网节点维护有第二可信执行环境，所述区块链主网还管理有第一区块链子网，第一区块链子网中的第一子网节点维护有第一可信执行环境；所述装置包括:

加密请求接收单元，用于接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成;

加密应答获取单元，用于将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到加密应答;

加密应答发送单元，用于将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答。

11. 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 1-8 中任一项所述的方法。

12. 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 1-8 中任一项所述方法的步骤。

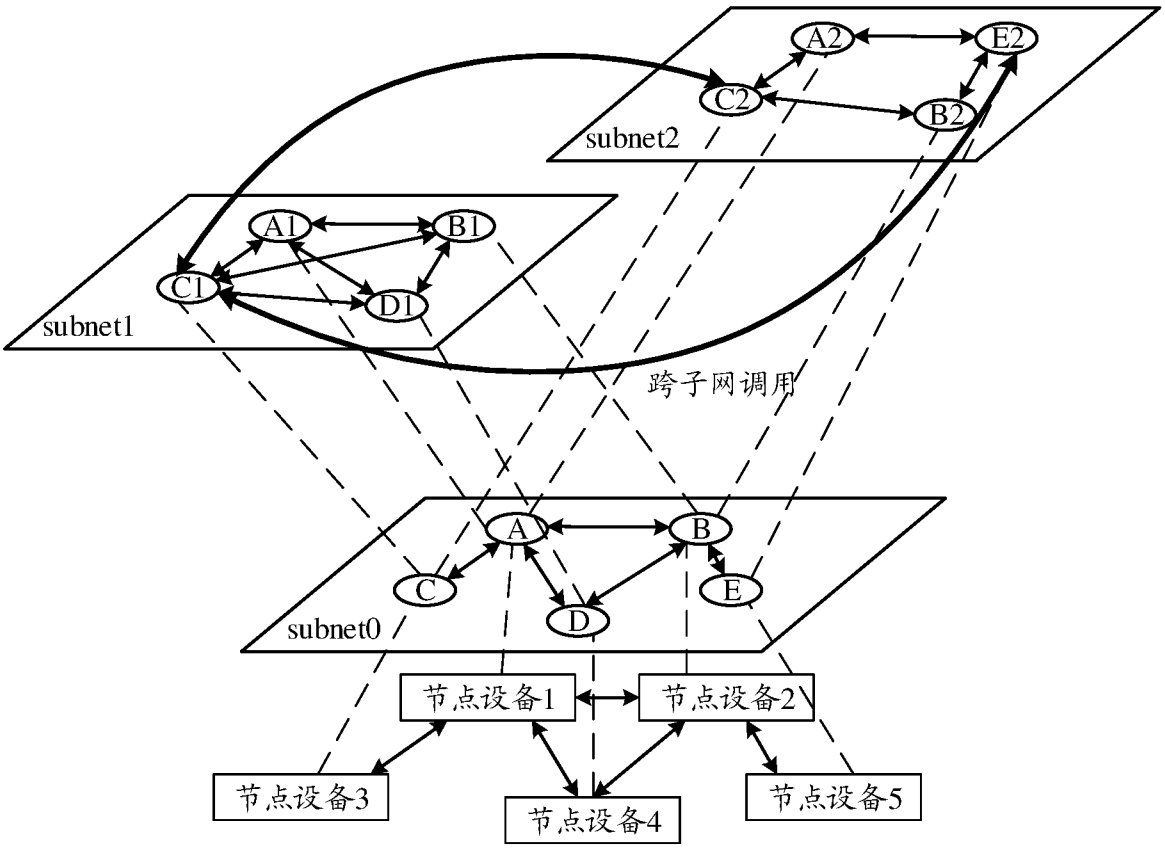
A2
E2
C2
B2
subnet2
A1
B1
C1
D1
subnet1
跨子网调用
A
B
C
E
D
subnet0
节点设备1
节点设备2
节点设备3
节点设备4
节点设备5

图 1

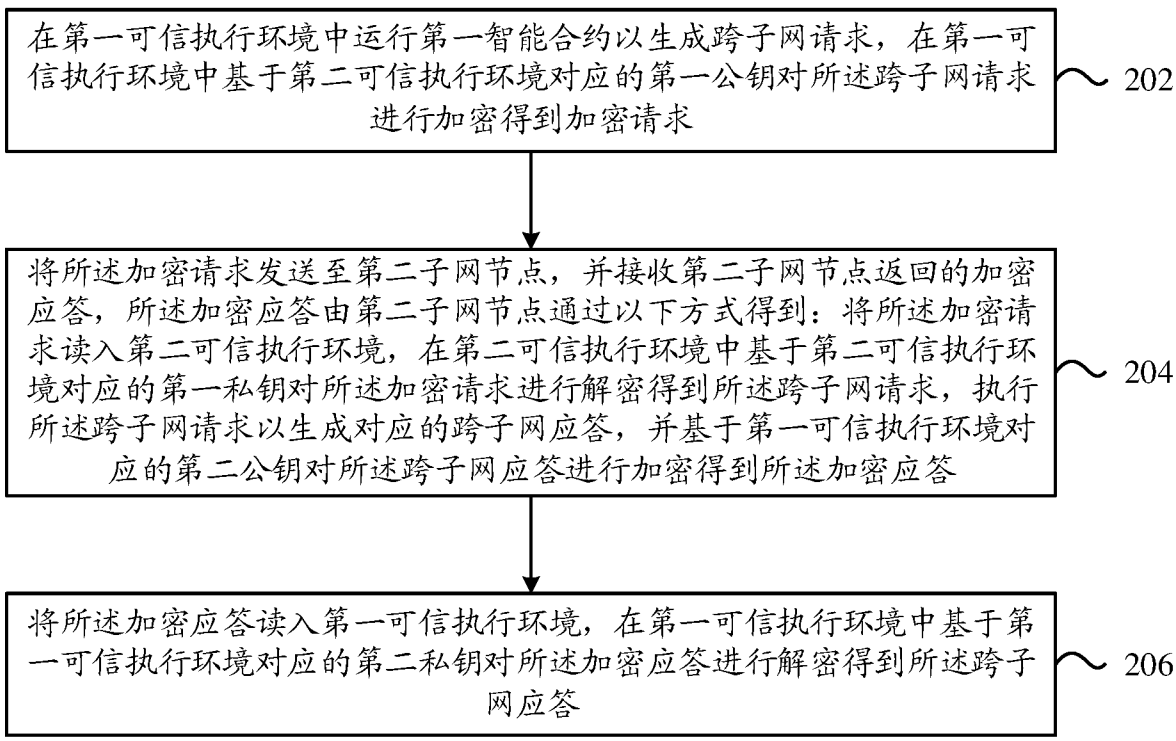
在第一可信执行环境中运行第一智能合约以生成跨子网请求，在第一可信执行环境中基于第二可信执行环境对应的第一公钥对所述跨子网请求进行加密得到加密请求
202
将所述加密请求发送至第二子网节点，并接收第二子网节点返回的加密应答，所述加密应答由第二子网节点通过以下方式得到：将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到所述加密应答
204
将所述加密应答读入第一可信执行环境，在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答
206

图 2

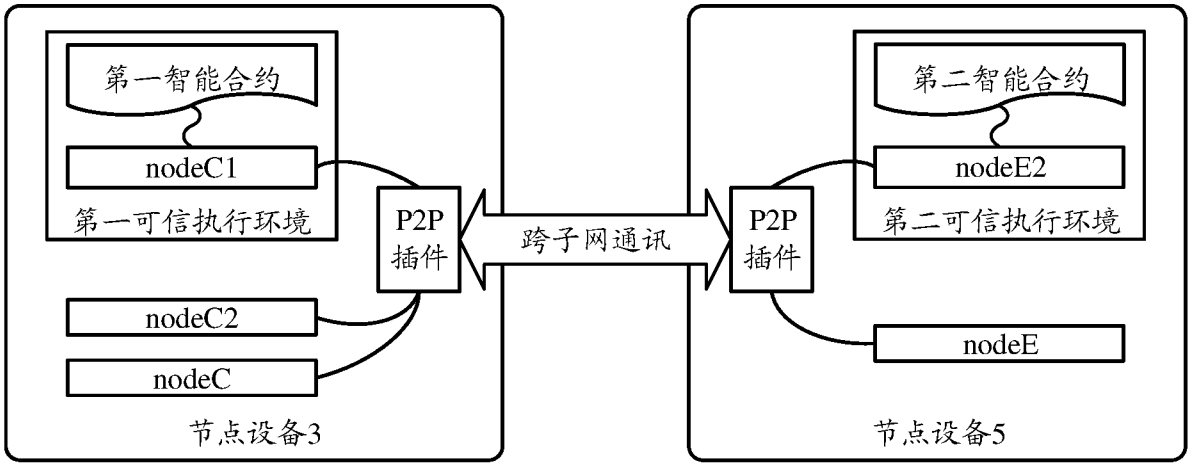
第一智能合约
nodeC1
第一可信执行环境
P2P
插件
跨子网通讯
P2P
插件
第二智能合约
nodeE2
第二可信执行环境
nodeC2
nodeC
nodeE
节点设备3
节点设备5

图 3

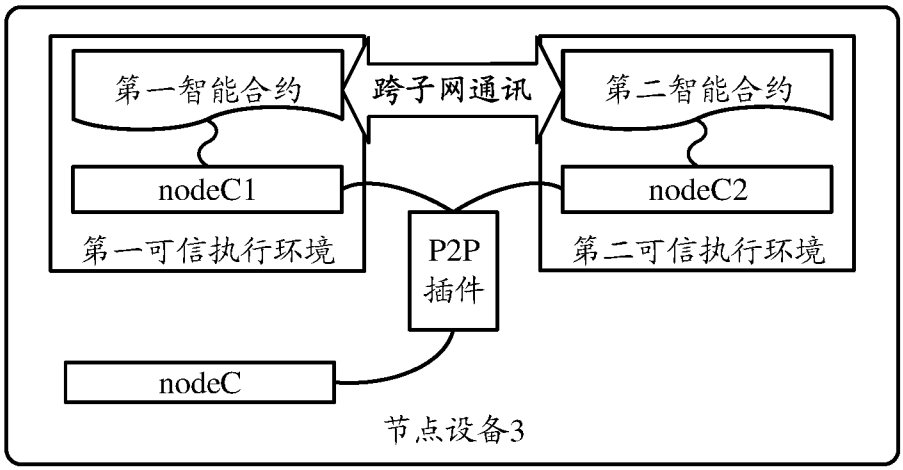
第一智能合约
跨子网通讯
第二智能合约
nodeC1
nodeC2
第一可信执行环境
P2P
插件
第二可信执行环境
nodeC
节点设备3

图 4

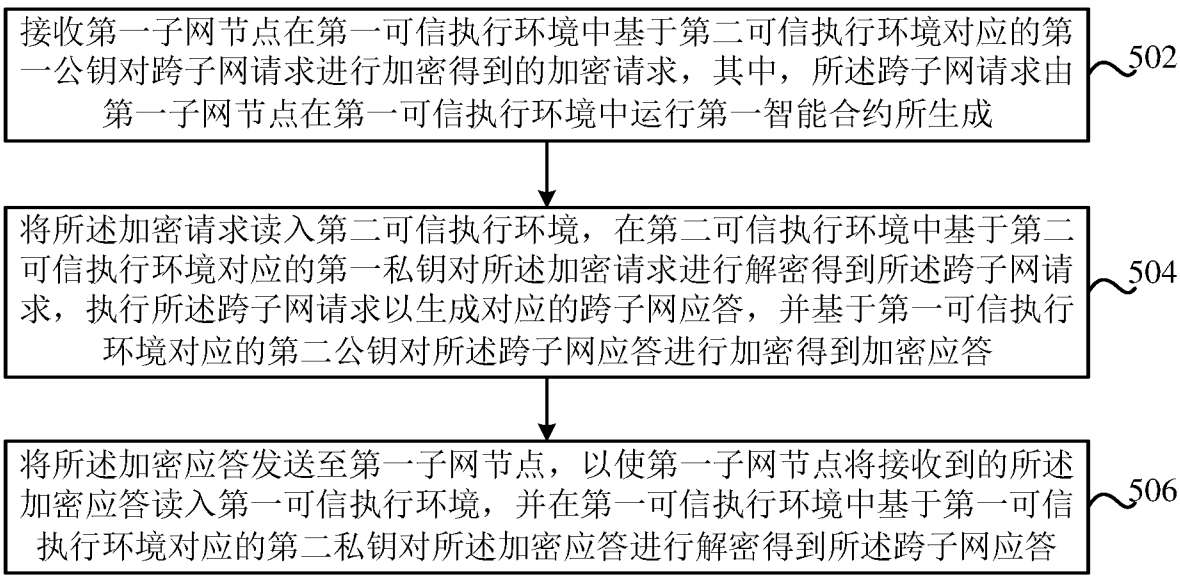
接收第一子网节点在第一可信执行环境中基于第二可信执行环境对应的第一公钥对跨子网请求进行加密得到的加密请求，其中，所述跨子网请求由第一子网节点在第一可信执行环境中运行第一智能合约所生成
502
将所述加密请求读入第二可信执行环境，在第二可信执行环境中基于第二可信执行环境对应的第一私钥对所述加密请求进行解密得到所述跨子网请求，执行所述跨子网请求以生成对应的跨子网应答，并基于第一可信执行环境对应的第二公钥对所述跨子网应答进行加密得到加密应答
504
将所述加密应答发送至第一子网节点，以使第一子网节点将接收到的所述加密应答读入第一可信执行环境，并在第一可信执行环境中基于第一可信执行环境对应的第二私钥对所述加密应答进行解密得到所述跨子网应答
506

图 5

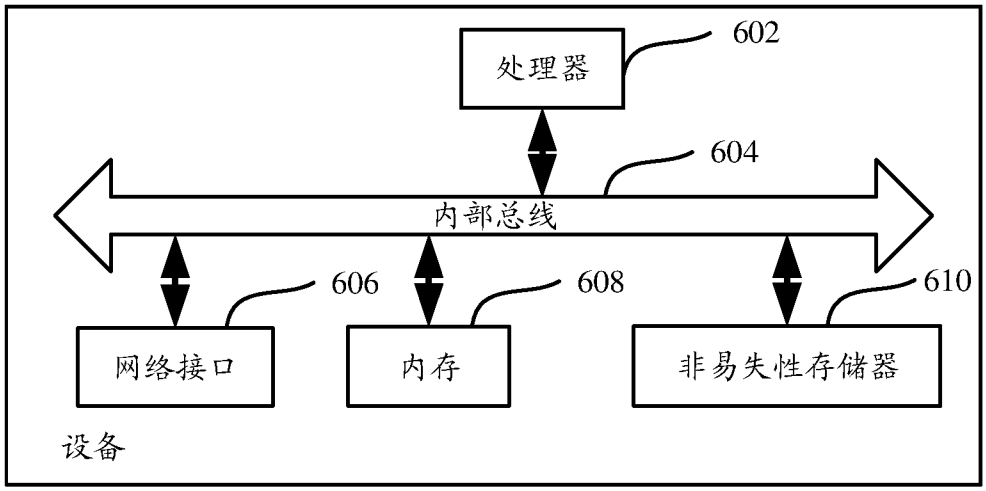
处理器
602
604
内部总线
606
608
610
网络接口
内存
非易失性存储器
设备

图 6

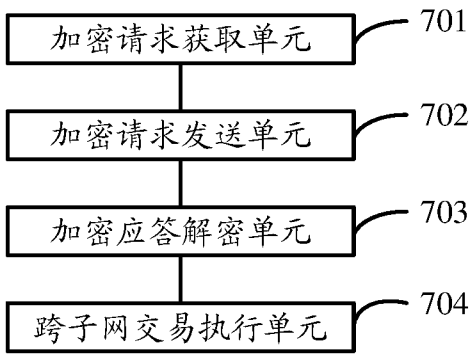
加密请求获取单元
701
加密请求发送单元
702
加密应答解密单元
703
跨子网交易执行单元
704

图 7

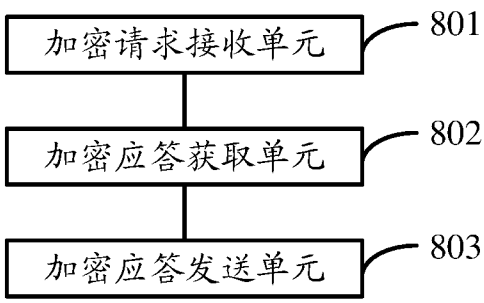
加密请求接收单元
801
加密应答获取单元
802
加密应答发送单元
803

图 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2022/135244

A. CLASSIFICATION OF SUBJECT MATTER

H04L9/08(2006.01)i;H04L9/32(2006.01)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)

IPC: 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)

CNTXT, ENTXTC, WPABSC, VEN, CNKI: 调用, 公钥, 环境, 加密, 交互, 交易, 可信, 跨子网, 跨链, 联盟链, 请求, 区块链, 子网, call, public key, encryption, transaction, TEE, request, cross sub-network

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 115134075 A (ANT BLOCKCHAIN TECHNOLOGY (SHANGHAI) CO., LTD.) 30 September 2022 (2022-09-30) description, paragraphs 4-146	1-12
Y	CN 114255031 A (HUAWEI TECHNOLOGIES CO., LTD.) 29 March 2022 (2022-03-29) description, paragraphs 4-500	1-12
Y	CN 114679274 A (ALIPAY HANGZHOU INFORMATION TECHNOLOGY CO., LTD.; ANT BLOCKCHAIN TECHNOLOGY SHANGHAI CO., LTD.) 28 June 2022 (2022-06-28) description, paragraphs 4-220	1-12
Y	CN 111095256 A (ALIBABA GROUP HOLDING LTD.) 01 May 2020 (2020-05-01) description, paragraphs 5-109	1-12
A	CN 112948153 A (ALIPAY HANGZHOU INFORMATION TECHNOLOGY CO., LTD.; ANT BLOCKCHAIN TECHNOLOGY SHANGHAI CO., LTD.) 11 June 2021 (2021-06-11) entire document	1-12

☐ 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
"D" document cited by the applicant in the international application
"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
01 March 2023	**10 March 2023**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2022/135244

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	115134075	A	30 September 2022	None			
CN	114255031	A	29 March 2022	None			
CN	114679274	A	28 June 2022	None			
CN	111095256	A	01 May 2020	AU	2019207311	A1	18 July 2019
				AU	2019207311	B2	29 October 2020
				JP	2020528224	A	17 September 2020
				KR	20200126321	A	06 November 2020
				KR	102263325	B1	15 June 2021
				WO	2019137564	A2	18 July 2019
				WO	2019137564	A3	12 March 2020
				CA	3061808	A1	18 July 2019
				CA	3061808	C	19 July 2022
				US	2020342092	A1	29 October 2020
				US	10839070	B1	17 November 2020
				SG	11201910054	WA	28 November 2019
				EP	3642753	A2	29 April 2020
				EP	3642753	A4	03 June 2020
				EP	3642753	B1	15 June 2022
CN	112948153	A	11 June 2021	None			

国际检索报告

国际申请号
PCT/CN2022/135244

A. 主题的分类

H04L9/08(2006.01)i;H04L9/32(2006.01)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)

IPC: 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））

CNTXT,ENTXTC,WPABSC,VEN,CNKI:调用,公钥,环境,加密,交互,交易,可信,跨子网,跨链,联盟链,请求,区块链,子网,call,public key,encryption,transaction,TEE,request,cross sub-network

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 115134075 A (蚂蚁区块链科技（上海）有限公司) 2022年9月30日 (2022-09-30) 说明书第4-146段	1-12
Y	CN 114255031 A (华为技术有限公司) 2022年3月29日 (2022-03-29) 说明书第4-500段	1-12
Y	CN 114679274 A (支付宝（杭州）信息技术有限公司 蚂蚁区块链科技（上海）有限公司) 2022年6月28日 (2022-06-28) 说明书第4-220段	1-12
Y	CN 111095256 A (阿里巴巴集团控股有限公司) 2020年5月1日 (2020-05-01) 说明书第5-109段	1-12
A	CN 112948153 A (支付宝（杭州）信息技术有限公司 蚂蚁区块链科技（上海）有限公司) 2021年6月11日 (2021-06-11) 全文	1-12

☐ 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

“D” 申请人在国际申请中引证的文件

“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3月1日	2023年3月10日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	代悦宁
传真号 (86-10)62019451	电话号码 (+86) 010-62411527

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2022/135244

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	115134075	A	2022年9月30日	无			
CN	114255031	A	2022年3月29日	无			
CN	114679274	A	2022年6月28日	无			
CN	111095256	A	2020年5月1日	AU	2019207311	A1	2019年7月18日
				AU	2019207311	B2	2020年10月29日
				JP	2020528224	A	2020年9月17日
				KR	20200126321	A	2020年11月6日
				KR	102263325	B1	2021年6月15日
				WO	2019137564	A2	2019年7月18日
				WO	2019137564	A3	2020年3月12日
				CA	3061808	A1	2019年7月18日
				CA	3061808	C	2022年7月19日
				US	2020342092	A1	2020年10月29日
				US	10839070	B1	2020年11月17日
				SG	11201910054	WA	2019年11月28日
				EP	3642753	A2	2020年4月29日
				EP	3642753	A4	2020年6月3日
				EP	3642753	B1	2022年6月15日
CN	112948153	A	2021年6月11日	无			