

(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
2020 年 12 月 17 日 (17.12.2020)



(10) 国际公布号
WO 2020/248981 A1

(51) 国际专利分类号:
H04L 29/08 (2006.01) *H04L 9/32* (2006.01)

(21) 国际申请号: PCT/CN2020/095199

(22) 国际申请日: 2020 年 6 月 9 日 (09.06.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910509596.0 2019年6月13日 (13.06.2019) CN

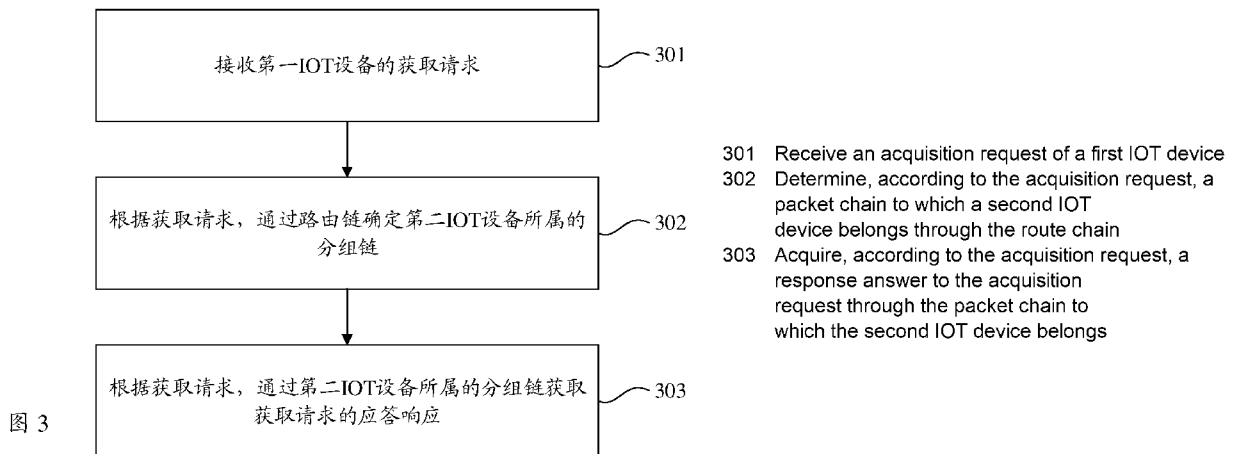
(71) 申请人: 深圳前海微众银行股份有限公司 (WEBANK CO., LTD.) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 西安交通大学(XI'AN

JIAOTONG UNIVERSITY) [CN/CN]; 中国陕西省西安市咸宁西路28号, Shaanxi 710049 (CN)。

(72) 发明人: 王晨旭 (WANG, Chenxu); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 汪雅伟 (WANG, Yawei); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 范瑞彬 (FAN, Ruibin); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 张开翔 (ZHANG, Kaixiang); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 李辉忠 (LI, Huizhong); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。 李成博 (LI,

(54) Title: BLOCKCHAIN-BASED METHOD AND DEVICE FOR COMMUNICATION BETWEEN IOT DEVICES

(54) 发明名称: 一种基于区块链的物联网IOT设备间通信的方法及装置



(57) Abstract: Disclosed are a blockchain-based method and device for communication between internet of things (IOT) devices, applicable for an alliance chain comprising a route chain and at least one packet chain. The method comprises: receiving an acquisition request of a first IOT device; determining, according to the acquisition request, a packet chain to which a second IOT device belongs through the route chain; and acquiring, according to the acquisition request, a response answer to the acquisition request through the packet chain to which the second IOT device belongs. No shared key is required to be distributed during communication between IOT devices, which improves the communication efficiency.

(57) 摘要: 一种基于区块链的物联网IOT设备间通信的方法及装置, 适用于包括路由链和至少一个分组链的联盟链, 其中, 方法包括: 接收第一IOT设备的获取请求, 根据获取请求, 通过路由链确定第二IOT设备所属的分组链, 根据获取请求, 通过第二IOT设备所属的分组链获取获取请求的应答响应。在IOT设备间通信时, 无需分发共享密钥, 提高了通信效率。

Chengbo); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司 (**TDIP & PARTNERS**); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, 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, GH, GM, KE, LR, LS, MW, MZ, NA, RW, 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, MK, MT, NL, NO, 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))。

一种基于区块链的物联网IOT设备间通信的方法及装置

相关申请的交叉引用

本申请要求在2019年06月13日提交中国专利局、申请号为201910509596.0、申请名称为“一种基于区块链的物联网IOT设备间通信的方法及装置”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

本发明实施例涉及金融科技（Fintech）领域，尤其涉及一种基于区块链（BlockChain）的 IOT（Internet of Things，物联网）设备间通信的方法及装置。

背景技术

区块链是由一系列区块组成的一条链，每个区块记录本块的数据及上一块的哈希值，所有区块通过这种方式前后相继组成一条链。区块链所基于的密码学技术和去中心化思想使链上的历史信息无法被篡改。

随着计算机技术的发展，越来越多的技术应用在金融领域，传统金融业正在逐步向金融科技转变，物联网技术也不例外，但由于金融、支付行业的安全性、实时性要求，也对技术提出的更高的要求。

如图1为现有技术中的基于比特币系统组建的物联网系统，该物联网系统中包括智能网关、IOT设备和云存储平台，其中，智能网关为该物联网系统中的矿工节点，当IOT设备之间需要通信时，矿工节点会生成共享密钥并分发至该待通信的IOT设备，以使得该待通信的IOT设备之间可以进行加密通信。

但该种方式中，每次IOT设备之间需要通信时，都需要矿工节点生成共享密钥，并分发至该待通信的IOT设备。该方式中，若物联网系统中存在大量待通信的IOT设备，则矿工节点需要执行大量的生成、分发共享密钥的工作，矿工节点的工作负荷过大。

发明内容

本发明实施例提供一种基于区块链的IOT设备间通信的方法及装置，用以在IOT设备间通信时，无需分发共享密钥，且提高通信效率的方式。

本发明实施例提供的一种基于区块链的IOT设备间通信的方法，适用于包括路由链和至少一个分组链的联盟链；

所述方法包括：

接收第一IOT设备的获取请求；所述获取请求用于获取第二IOT设备的第一数据；

根据所述获取请求，通过所述路由链确定所述第二IOT设备所属的分组链；所述路由链用于在确定所述第一IOT设备通过第一身份验证后返回所述第二IOT设备所属的分组链；

根据所述获取请求，通过所述第二IOT设备所属的分组链获取所述获取请求的应答响应；所述第二IOT设备所属的分组链用于在确定所述第一IOT设备通过第二身份验证后，返回所述获取请求的应答响应；所述应答响应用于获取所述第一数据。

上述技术方案中，第一IOT设备通过联盟链访问第二IOT设备，第一IOT设备向联盟链发送获取第二IOT设备的第一数据的获取请求，并根据获取请求通过路由链确定第二

IOT设备所属的分组链,以及通过第二IOT设备所属的分组链获取应答响应,第一IOT设备与第二IOT设备无需直接通信,则无需分发共享密钥,而是经过路由链和分组链获取第二IOT设备的应答响应,用于获取第一数据,提高了第一IOT设备和第二IOT设备之间的通信效率,该技术方案适用于大规模的物联网系统中大量IOT设备间的通信。进一步的,路由链用于对第一IOT设备进行第一身份验证,分组链用于对第一IOT设备进行第二身份验证,相当于两层数据访问控制,提高了数据访问的安全性。

可选的,所述路由链设置有第一智能合约;

所述根据所述获取请求,通过所述路由链确定所述第二IOT设备所属的分组链,包括:

根据所述获取请求,调用所述第一智能合约,通过所述第一智能合约确定所述第一IOT设备为经过所述路由链认证的IOT设备,并通过所述第一智能合约确定所述第二IOT设备所属的分组链。

上述技术方案中,调用路由链的第一智能合约,相当于采用第一智能合约实现路由链功能的多样化,通过第一智能合约的判断功能,判断第一IOT设备是否为经过路由链认证的IOT设备;以及将第一智能合约作为路由链中的路由表,用于确定第二IOT设备所属的分组链。

可选的,所述分组链设置有归属于所述分组链的各IOT设备的第二智能合约;

所述根据所述获取请求,通过所述第二IOT设备所属的分组链获取所述获取请求的应答响应,包括:

根据所述获取请求,调用所述第二IOT设备的第二智能合约,通过所述第二IOT设备的第二智能合约确定所述第一IOT设备具有访问所述第二IOT设备的权限,并通过所述第二IOT设备的第二智能合约得到所述应答响应。

上述技术方案中,分组链设置有归属于分组链的各IOT设备的第二智能合约,根据获取请求,调用第二IOT设备的第二智能合约,相当于采用第二智能合约实现分组链功能的多样化,通过第二智能合约的判断功能,判断第一IOT设备是否具有访问第二IOT设备的权限;以及根据第二智能合约中的对应关系,确定出第二IOT设备的应答响应。

可选的,所述应答响应为所述第一数据的哈希值;

所述第一数据的哈希值是所述第二IOT设备将所述第一数据存储至分布式存储系统后,所述分布式存储系统返回的哈希值。

上述技术方案中,在确定第一IOT设备通过第一身份验证和第二身份验证之后,可以向第一IOT设备返回第一数据的哈希值,第一IOT设备可以根据该第一数据的哈希值从分布式存储系统中获取第二IOT的第一数据。采用分布式存储系统将第二IOT设备的数据分布存储于各服务器上,保障了数据的安全性,同时采用分布式存储系统,在第一IOT设备通过第一数据的哈希值下载数据时,可以实现数据的完整性以及高速下载第一数据。

可选的,所述方法还包括:

接收所述第二IOT设备发送的上链请求;所述上链请求包括所述第二IOT设备的第二数据的哈希值;

根据所述上链请求,通过所述路由链确定所述第二IOT设备所属的分组链;

根据所述上链请求,通过所述第二IOT设备所属的分组链存储所述第二数据的哈希值。

上述技术方案中,第二IOT设备将第二数据的哈希值记录在上链请求中发送至联盟链,联盟链根据上链请求、路由链确定第二IOT设备所属的分组链以及根据第二IOT设备所属

的分组链存储第二数据的哈希值，相当于根据联盟链和分组链，将第二 IOT 设备的第二数据的哈希值存储至所属的分组链中，实现将不同类型的 IOT 设备进行分组，以及将不同类型的 IOT 设备的数据存储至所属的分组链中，从而高效的管理物联网系统中的各 IOT 设备。

可选的，在所述接收第一 IOT 设备的获取请求之前，还包括：

接收所述第一 IOT 设备发送的注册请求；

根据所述注册请求，通过所述路由链对所述第一 IOT 设备的 IOT 设备 ID 进行认证，并在认证通过后，确定所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链；

通过所述第一 IOT 设备所属的分组链确定所述第一 IOT 设备的第二智能合约；

将所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链的信息存储至所述第一智能合约中；所述第一 IOT 设备所属的分组链的信息中记录有所述第一 IOT 设备的第二智能合约在所属的分组链中的地址。

上述技术方案中，第一 IOT 设备可以向联盟链发送注册请求，路由链对第一 IOT 设备的 IOT 设备 ID 进行认证，并在认证通过后，生成第一 IOT 设备的身份证书；路由链确定第一 IOT 设备所属的分组链，并通过分组链确定第一 IOT 设备的第二智能合约；将第一 IOT 设备的身份证书及第一 IOT 设备所属的分组链的信息存储至第一智能合约中，用于在注册完成后，第一 IOT 设备的数据上链以及访问其他被访问 IOT 设备时的第一身份验证和第二身份验证。

可选的，所述第一智能合约中记录有 IOT 设备的服务类型、IOT 设备所属网络 ID、IOT 设备所属的分组链 ID 的对应关系，以及 IOT 设备所属的分组链 ID、IOT 设备 ID 与 IOT 设备的第二智能合约在所属的分组链中的地址的对应关系；

所述第二智能合约中记录有 IOT 设备 ID、时间戳和 IOT 设备的数据的哈希值的对应关系。

上述技术方案中，第一智能合约中记录有预设的对应关系，用于确定物联网系统中各 IOT 设备的完整路径，该对应关系中，第一个对应关系为 IOT 设备的服务类型、IOT 设备所属网络 ID、IOT 设备所属的分组链 ID 的对应关系；第二个对应关系为 IOT 设备所属的分组链 ID、IOT 设备 ID 与 IOT 设备的第二智能合约在所属的分组链中的地址的对应关系，通过第一智能合约中预设的对应关系，可以在获取到被访问 IOT 设备的信息时，确定出被访问 IOT 设备所属的分组链，以及该被访问 IOT 设备的第二智能合约在所属分组链中的地址，从而可以调用该被访问 IOT 设备的第二智能合约。进一步的，第二智能合约中同样记录有预设的对应关系，用于确定该被访问 IOT 设备的数据的哈希值，该对应关系为被访问 IOT 设备 ID、时间戳和被访问 IOT 设备的数据的哈希值，通过第二智能合约中预设的对应关系，可以在获取到时间信息和被访问 IOT 设备 ID 后，确定出被访问 IOT 设备的数据的哈希值，从而将被访问 IOT 设备的数据的哈希值返回访问 IOT 设备，实现访问 IOT 设备获取被访问 IOT 设备的数据。

相应的，本发明实施例还提供了一种基于区块链的 IOT 设备间通信的装置，适用于包括路由链和至少一个分组链的联盟链；

所述装置包括：

接收单元，用于接收第一 IOT 设备的获取请求；所述获取请求用于获取第二 IOT 设备的第一数据；

处理单元，用于根据所述获取请求，通过所述路由链确定所述第二 IOT 设备所属的分

组链；所述路由链用于在确定所述第一 IOT 设备通过第一身份验证后返回所述第二 IOT 设备所属的分组链；

所述处理单元，还用于根据所述获取请求，通过所述第二 IOT 设备所属的分组链获取所述获取请求的应答响应；所述第二 IOT 设备所属的分组链用于在确定所述第一 IOT 设备通过第二身份验证后，返回所述获取请求的应答响应；所述应答响应用于获取所述第一数据。

可选的，所述路由链设置有第一智能合约；

所述处理单元，具体用于：

根据所述获取请求，调用所述第一智能合约，通过所述第一智能合约确定所述第一 IOT 设备为经过所述路由链认证的 IOT 设备，并通过所述第一智能合约确定所述第二 IOT 设备所属的分组链。

可选的，所述分组链设置有归属于所述分组链的各 IOT 设备的第二智能合约；

所述处理单元，具体用于：

根据所述获取请求，调用所述第二 IOT 设备的第二智能合约，通过所述第二 IOT 设备的第二智能合约确定所述第一 IOT 设备具有访问所述第二 IOT 设备的权限，并通过所述第二 IOT 设备的第二智能合约得到所述应答响应。

可选的，所述应答响应为所述第一数据的哈希值；

所述第一数据的哈希值是所述第二 IOT 设备将所述第一数据存储至分布式存储系统后，所述分布式存储系统返回的哈希值。

可选的，所述处理单元，还用于：

控制所述接收单元接收所述第二 IOT 设备发送的上链请求；所述上链请求包括所述第二 IOT 设备的第二数据的哈希值；

根据所述上链请求，通过所述路由链确定所述第二 IOT 设备所属的分组链；

根据所述上链请求，通过所述第二 IOT 设备所属的分组链存储所述第二数据的哈希值。

可选的，所述处理单元，还用于：

在控制所述接收单元接收第一 IOT 设备的获取请求之前，接收所述第一 IOT 设备发送的注册请求；

根据所述注册请求，通过所述路由链对所述第一 IOT 设备的 IOT 设备 ID 进行认证，并在认证通过后，确定所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链；

通过所述第一 IOT 设备所属的分组链确定所述第一 IOT 设备的第二智能合约；

将所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链的信息存储至所述第一智能合约中；所述第一 IOT 设备所属的分组链的信息中记录有所述第一 IOT 设备的第二智能合约在所属的分组链中的地址。

可选的，所述第一智能合约中记录有 IOT 设备的服务类型、IOT 设备所属网络 ID、IOT 设备所属的分组链 ID 的对应关系，以及 IOT 设备所属的分组链 ID、IOT 设备 ID 与 IOT 设备的第二智能合约在所属的分组链中的地址的对应关系；

所述第二智能合约中记录有 IOT 设备 ID、时间戳和 IOT 设备的数据的哈希值的对应关系。

相应的，本发明实施例还提供了一种计算设备，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行上述基于区块链的 IOT 设备间通信的方法。

相应的，本发明实施例还提供了一种计算机可读非易失性存储介质，包括计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行上述基于区块链的 IOT 设备间通信的方法。

相应的，本申请提供一种包含指令的计算机程序产品，当其在计算机上运行时，使得计算机执行上述基于区块链的 IOT 设备间通信的方法。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 为现有技术中的基于比特币系统组建的物联网系统；

图 2 为本发明实施例提供的一种系统架构的示意图；

图 3 为本发明实施例提供的一种基于区块链的 IOT 设备间通信的方法的流程示意图；

图 4 为本发明实施例提供的路由链对第一 IOT 设备进行身份认证；

图 5 为本发明实施例提供的第一 IOT 设备注册的流程示意图；

图 6 为本发明实施例提供的第二 IOT 设备的数据哈希值上链的流程示意图；

图 7 为本发明实施例提供的另一种基于区块链的 IOT 设备间通信的方法的流程示意图；

图 8 为本发明实施例提供的另一种系统架构的示意图；

图 9 为本发明实施例提供的一种基于区块链的 IOT 设备间通信的装置的结构示意图；

图 10 为本申请提供的一种计算设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案和优点更加清楚，下面将结合附图对本发明作进一步地详细描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其它实施例，都属于本发明保护的范围。

金融领域中通常涉及到多个系统，比如办公系统、生产系统、运维系统等，办公系统可以用于执行金融领域内部的各项事务，而生产系统可以用于执行金融领域中产生的业务；相应地，运维系统可以对办公系统和生产系统进行监督，从而保证办公系统和生产系统的正常运行。通过多个系统的协同运作，可以保证金融领域快速、健康地发展。基于此，将办公系统、生产系统、运维系统中各设备组成物联网系统，并结合本发明实施例提供的基于区块链的 IOT 设备间通信的方法，可实现金融领域内各 IOT 设备之间的高效通信以及保障数据的安全性。

图 2 示例性的示出了本发明实施例提供的基于区块链的 IOT 设备间通信的方法所适用的物联网系统的系统架构，该系统架构包括联盟链、分布式存储系统、IOT 设备集群、应用程序服务器。

联盟链包括路由链和至少一个分组链；IOT 设备集群中包括多个 IOT 设备，IOT 设备

通过应用程序服务器将数据保存至分布式存储系统中，且将存储数据的信息存储至联盟链中，IOT设备之间通过应用程序服务器、联盟链进行通信；应用程序服务器可以作为单独的服务器，也可以集成于联盟链中，为方便下述描述，可以将应用程序服务器集成于联盟链中，IOT设备与联盟链直接通信；分布式存储系统可以是IPFS(InterPlanetary File System, 星际文件系统)系统。

为方便描述，IOT设备间通信的方法中，以两个IOT设备为例进行说明，分别为第一IOT设备和第二IOT设备。其中，第一IOT设备为访问IOT设备或主动访问IOT设备，第二IOT设备为待访问IOT设备或被访问IOT设备。在第一IOT设备通过联盟链访问第二IOT设备时，联盟链接收第一IOT设备的获取请求，联盟链中路由链用于对第一IOT设备进行第一身份验证以及确定第二IOT设备所属的分组链；联盟链中分组链用于对第一IOT设备进行第二身份验证以及确定上述获取请求的应答响应。

具体的，路由链中可以设置有两个智能合约，分别实现上述两种功能，如路由链调用第一个智能合约对第一IOT设备的进行第一身份验证，以及调用第二个智能合约确定第二IOT设备所属的分组链。路由链中还可以设置一个智能合约，可以叫做第一智能合约，路由链调用该第一智能合约用于对第一IOT设备进行第一身份验证以及确定第二IOT设备所属的分组链。

本发明实施例中，第一智能合约在对第一IOT设备进行第一身份验证时，相当于判断该第一IOT设备是否为该物联网系统中的已注册设备，或判断该第一IOT设备是否为经过路由链认证的IOT设备，若是，则确定该第一IOT设备通过第一智能合约的第一身份验证。第一IOT设备的注册过程在下述实施例中进行具体描述。

第一智能合约在确定第二IOT设备所属的分组链时，可以根据第一智能合约中记录的该物联网系统中各IOT设备的完整路径进行确定，该完整路径可以通过预设的对应关系实现，该预设的对应关系可以理解为一组路由表。具体的，第一个对应关系为IOT设备的服务类型、IOT设备所属网络ID、IOT设备所属的分组链ID的对应关系；第二个对应关系为IOT设备所属的分组链ID、IOT设备ID与IOT设备的第二智能合约在所属的分组链中的地址的对应关系。

具体实现中，路由链的第一智能合约可以通过两个Map(Map1和Map2)来记录IOT设备的路径信息，Map1的结构为Map1[servicetype][netID]，其中，第一个key为IOT设备的服务类型，第二个key为IOT设备所属网络ID，value值为set chainID，即IOT设备所属的分组链ID；Map2的结构为Map2[set chainID][deviceID]，其中，第一个key为IOT设备所属的分组链ID，第二个key为IOT设备ID，value值为IOT设备的第二智能合约在所属的分组链中的地址。

分组链用于对第一IOT设备进行第二身份验证以及确定获取请求的应答响应，其中，应答响应用于获取第二IOT设备的数据。具体的，分组链设置有归属于分组链的各IOT设备的智能合约，即各IOT设备对应自己的智能合约，每个IOT设备可以设置两个智能合约，分别实现对第一IOT设备的第二身份验证以及确定应答响应两种功能，也可以设置一个智能合约，可以叫做第二智能合约，路由链调用该第二智能合约用于对第一IOT设备进行第二身份验证以及确定应答响应。

路由链调用第二IOT设备的第二智能合约对第一IOT设备进行第二身份验证，相当于判断第一IOT设备是否有权限访问第一IOT设备的数据，若是，则确定该第一IOT设备

通过第二智能合约的第二身份验证。

第二 IOT 设备的数据可以为第二 IOT 设备的运行数据、参数信息等。第二智能合约中可以记录有该第二 IOT 设备的设备 ID、时间戳和数据存储位置三者的对应关系，则此时应答响应为数据存储位置；第二智能合约中也可以记录有该第二 IOT 设备的设备 ID、时间戳和数据的哈希值三者的对应关系，则此时应答响应为数据的哈希值，其中，数据的哈希值是第二 IOT 设备将数据存储至分布式存储系统时，分布式存储系统返回给该数据的哈希值。

具体实现中，路由链可以通过一个 Map（Map3）来记录 IOT 设备的数据的哈希值，Map3 的结构为 Map[deviceID][timestamp]，第一个 key 为 IOT 设备 ID，第二个 key 为 IOT 设备上传数据时的时间戳，value 值为 IPFS 返回的数据的哈希值。

基于上述描述，图 3 示例性的示出了本发明实施例提供的一种基于区块链的 IOT 设备间通信的方法的流程，该流程可以由基于区块链的 IOT 设备间通信的装置执行。

如图 3 所示，该流程具体包括：

步骤 301，接收第一 IOT 设备的获取请求。

本发明实施例中，获取请求用于获取第二 IOT 设备的第一数据，获取请求中可以记录有第一 IOT 设备的参数信息、第二 IOT 设备的参数信息，参数信息可以包括 IOT 设备的设备 ID，当然，参数信息还可以包括 IOT 设备的设备序列号、服务类型、所属网络 ID、所属服务类型等。

步骤 302，根据获取请求，通过路由链确定第二 IOT 设备所属的分组链。

可选的，根据获取请求，调用路由链中的第一智能合约判断第一 IOT 设备是否通过第一身份验证，相当于调用第一智能合约确定第一 IOT 设备是否为经过路由链认证的 IOT 设备，若是，则通过第一智能合约确定第二 IOT 设备所属的分组链；否则，向该第一 IOT 设备返回拒绝消息。该技术方案中，在第一 IOT 设备通过联盟链访问第二 IOT 设备的数据时，先要对第一 IOT 设备进行第一身份验证，确保只有被路由链认证通过的 IOT 设备才能访问第二 IOT 设备，保障了第二 IOT 设备的数据的安全性。

也就是说，路由链在对第一 IOT 设备进行第一身份验证之前，可以存在路由链对第一 IOT 设备进行认证，相当于将第一 IOT 设备注册进联盟链，具体的，接收第一 IOT 设备发送的注册请求，根据注册请求，通过路由链对第一 IOT 设备的 IOT 设备 ID 进行认证，并在认证通过后，确定第一 IOT 设备的身份证书及第一 IOT 设备所属的分组链，通过第一 IOT 设备所属的分组链确定第一 IOT 设备的第二智能合约，将第一 IOT 设备的身份证书及第一 IOT 设备所属的分组链的信息存储至第一智能合约中；其中，第一 IOT 设备所属的分组链的信息中记录有第一 IOT 设备的第二智能合约在所属的分组链中的地址。

在一种可以实现的方式中，可以对第一 IOT 设备进行注册，接收第一 IOT 设备发送的注册请求，该注册请求中可以包括第一 IOT 设备的参数信息，如设备 ID、设备序列号、服务类型、所属网络 ID、所属组织等，如图 4 所示，路由链中具有仲裁性质的节点可以对该第一 IOT 设备进行身份认证，并分别在确定该第一 IOT 设备通过身份认证后签名，将签名的存证作为该第一 IOT 设备的身份证书，身份证书中记录该第一 IOT 设备的设备 ID、设备序列号、服务类型、所属网络 ID、所属组织等，将第一 IOT 设备的身份证书存储至第一智能合约中。也就是说，在调用第一智能合约确定第一 IOT 设备是否是经过路由链认证的 IOT 设备时，可以判断第一智能合约中是否存在有第一 IOT 设备的身份证书，若是，则确定第一 IOT 设备经过第一身份验证。在路由链生成该第一 IOT 设备的身份证书之后，还可

以根据第一 IOT 设备的服务类型、所属网络 ID 等信息,确定第一 IOT 设备所属的分组链,将第一 IOT 设备的身份证书、第一 IOT 设备所属的分组链信息一起存储至第一智能合约中。通过第一 IOT 设备所属的分组链确定第一 IOT 设备的第二智能合约,第一 IOT 设备所属的分组链将第一 IOT 设备的第二智能合约的地址返回至路由链,路由链将该第二智能合约的地址作为所属的分组链信息一起存储至第一智能合约中,从而第一智能合约可以根据第一 IOT 设备所属的分组链的信息生成第一 IOT 设备的完整路径。

结合图 5,第一 IOT 设备注册的具体流程如下:

步骤 501,第一 IOT 设备向路由链发送注册请求。

步骤 502,路由链中具有仲裁性质的节点对第一 IOT 设备进行签名,签名后的存证作为第一 IOT 设备的身份证书;

步骤 503,路由链确定第一 IOT 设备所属的分组链;

步骤 504,路由链向分组链发送部署第二智能合约的交易;

步骤 505,分组链部署第一 IOT 设备的第二智能合约;

步骤 506,分组链向路由链发送第二智能合约的地址;

步骤 507,路由链通过两个 Map 来记录第一 IOT 设备的路径信息;

步骤 508,路由链将第一 IOT 设备的身份证书和路径信息存储至第一智能合约中;

步骤 509,路由链发送注册成功消息至第一 IOT 设备。

本发明实施例中,路由链中具有仲裁性质的节点可以包括三类节点,分别是组织节点、仲裁节点、存证节点,在第一 IOT 设备发送注册请求后,该三类节点分别对该第一 IOT 设备的参数信息进行验证,并在验证通过后进行签名,路由链将具有该三类节点签名的存证作为该第一 IOT 设备的身份证书。此外,路由链中具有仲裁性质的节点不仅可以包括组织节点、仲裁节点、存证节点,还可以包括如监管节点等其他节点。

需要说明的是,第二 IOT 设备为联盟链进行注册后的设备,路由链的第一智能合约中记录有第二 IOT 设备的完整路径,即可以根据第二 IOT 设备的设备信息,如第二 IOT 设备的服务类型、IOT 设备所属网络 ID、设备 ID 确定出第二 IOT 设备的完整路径,即确定出第二 IOT 设备所属的分组链 ID 和第二 IOT 设备的第二智能合约在所属的分组链中的地址。

步骤 303,根据获取请求,通过第二 IOT 设备所属的分组链获取获取请求的应答响应。

第二 IOT 设备所属的分组链先对第一 IOT 设备进行第二身份验证,相当于调用第二 IOT 设备的第二智能合约确定第一 IOT 设备是否具有访问第二 IOT 设备的数据的权限,若是,则通过第一 IOT 设备的第二智能合约确定应答响应;否则,向该第一 IOT 设备返回拒绝消息。

此处,第一 IOT 设备是否具有访问第二 IOT 设备的数据的权限,理解为,第一 IOT 设备可以提供访问第二 IOT 设备的数据的 Token 值,或者向第二 IOT 设备支付相应的金钱。

本发明实施例中,第二 IOT 设备经联盟链进行注册后,可以将生成的第二数据存储至分布式存储系统中,并接收分布式存储系统返回的该第二数据的哈希值,第二 IOT 设备将该第二数据的哈希值记录在上链请求中发送至路由链以请求上链,第二数据的哈希值可以是经第二 IOT 设备的密钥加密后的数据。相应的,联盟链系统接收第二 IOT 设备发送的上链请求,根据上链请求,通过路由链确定第二 IOT 设备所属的分组链,再根据上链请求,通过第二 IOT 设备所属的分组链存储该第二数据的哈希值。可选的,第二 IOT 设备所属的

分组链调用第二 IOT 设备的第二智能合约，将第二数据的哈希值存储至第二智能合约中。

结合图 6，第二 IOT 设备的数据的哈希值上链的具体流程如下：

步骤 601，第二 IOT 设备将第二数据发送至分布式存储系统；

步骤 602，分布式存储系统存储第二数据，并生成第二数据的哈希值；

步骤 603，分布式存储系统将第二数据的哈希值发送至第二 IOT 设备；

步骤 604，第二 IOT 设备将第二数据的哈希值加密，生成上链请求；

步骤 605，第二 IOT 设备将上链请求发送至路由链；

步骤 606，路由链根据上链请求确定第二 IOT 设备的身份证书；

步骤 607，路由链根据第二 IOT 设备的身份证书中的服务类型和网络 ID 在第一智能合约中确定第二 IOT 设备所属的分组链；

步骤 608，路由链根据第二 IOT 设备所属的分组链 ID、第二 IOT 设备的设备 ID 在第一智能合约中确定第二 IOT 设备的第二智能合约的地址；

步骤 609，路由链将加密后的第二数据的哈希值发送至分组链；

步骤 610，分组链将该加密后的第二数据的哈希值存储至第二智能合约中。

基于上述描述，第一 IOT 设备向联盟链系统发送获取第二 IOT 设备的第一数据的哈希值的请求，在确定第一 IOT 设备通过第一身份验证和第二身份验证之后，可以向第一 IOT 设备返回第一数据的哈希值，第一 IOT 设备可以根据该第一数据的哈希值从分布式存储系统中获取第二 IOT 的第一数据。

为了更好的解释本发明实施例，下面将在具体的实施场景下描述该基于区块链的 IOT 设备间通信的流程，如图 7 所示，具体如下：

步骤 701，第一 IOT 设备向路由链发送获取请求；

步骤 702，路由链根据第一智能合约对第一 IOT 设备进行第一身份验证；

步骤 703，路由链确定第一 IOT 设备通过第一身份验证，从第一智能合约中确定第二 IOT 设备的第二智能合约的地址；

步骤 704，路由链将第二智能合约的地址发送至分组链；

步骤 705，分组链根据第二智能合约对第一 IOT 设备进行第二身份验证；

步骤 706，分组链确定第一 IOT 设备通过第二身份验证，从第二智能合约中确定第一数据的哈希值；

步骤 707，分组链将第一数据的哈希值发送至第一 IOT 设备；

步骤 708，第一 IOT 设备将第一数据的哈希值发送至分布式存储系统；

步骤 709，分布式存储系统返回第一数据至第一 IOT 设备。

此外，上述实施例中不仅可以第二 IOT 设备的第二数据存储至分布式存储系统中，当然，还可以将第二 IOT 设备的第二数据存储至云存储系统上，如采用第三方的云存储系统来存储数据，相应的，本发明实施例还提供一种系统架构的示意图，可以如图 8 所示。相比于云存储系统，分布式存储系统将第二 IOT 设备的第二数据分布存储于各服务器上，保障了第二数据的安全性，同时采用分布式存储系统，在第一 IOT 设备通过第二数据的哈希值下载数据时，可以实现第二数据的完整性以及高速下载第二数据。

上述技术方案中，第一 IOT 设备通过联盟链访问第二 IOT 设备，第一 IOT 设备向联盟链发送获取第二 IOT 设备的第一数据的获取请求，并根据获取请求通过路由链确定第二 IOT 设备所属的分组链，以及通过第二 IOT 设备所属的分组链获取应答响应，第一 IOT 设

备与第二 IOT 设备无需直接通信,则无需分发共享密钥,而是经过路由链和分组链获取第二 IOT 设备的应答响应,用于获取第一数据,提高了第一 IOT 设备和第二 IOT 设备之间的通信效率,该技术方案适用于大规模的物联网系统中大量 IOT 设备间的通信。进一步的,路由链用于对第一 IOT 设备进行第一身份验证,分组链用于对第一 IOT 设备进行第二身份验证,相当于两层数据访问控制,提高了数据访问的安全性。

基于同一发明构思,图 9 示例性的示出了本发明实施例提供的一种基于区块链的 IOT 设备间通信的装置的结构,该装置可以执行基于区块链的 IOT 设备间通信的方法的流程。

该装置适用于包括路由链和至少一个分组链的联盟链;该装置包括:

接收单元 901,用于接收第一 IOT 设备的获取请求;所述获取请求用于获取第二 IOT 设备的第一数据;

处理单元 902,用于根据所述获取请求,通过所述路由链确定所述第二 IOT 设备所属的分组链;所述路由链用于在确定所述第一 IOT 设备通过第一身份验证后返回所述第二 IOT 设备所属的分组链;

所述处理单元 902,还用于根据所述获取请求,通过所述第二 IOT 设备所属的分组链获取所述获取请求的应答响应;所述第二 IOT 设备所属的分组链用于在确定所述第一 IOT 设备通过第二身份验证后,返回所述获取请求的应答响应;所述应答响应用于获取所述第一数据。

可选的,所述路由链设置有第一智能合约;

所述处理单元 902,具体用于:

根据所述获取请求,调用所述第一智能合约,通过所述第一智能合约确定所述第一 IOT 设备为经过所述路由链认证的 IOT 设备,并通过所述第一智能合约确定所述第二 IOT 设备所属的分组链。

可选的,所述分组链设置有归属于所述分组链的各 IOT 设备的第二智能合约;

所述处理单元 902,具体用于:

根据所述获取请求,调用所述第二 IOT 设备的第二智能合约,通过所述第二 IOT 设备的第二智能合约确定所述第一 IOT 设备具有访问所述第二 IOT 设备的权限,并通过所述第二 IOT 设备的第二智能合约得到所述应答响应。

可选的,所述应答响应为所述第一数据的哈希值;

所述第一数据的哈希值是所述第二 IOT 设备将所述第一数据存储至分布式存储系统后,所述分布式存储系统返回的哈希值。

可选的,所述处理单元 902,还用于:

控制所述接收单元 901 接收所述第二 IOT 设备发送的上链请求;所述上链请求包括所述第二 IOT 设备的第二数据的哈希值;

根据所述上链请求,通过所述路由链确定所述第二 IOT 设备所属的分组链;

根据所述上链请求,通过所述第二 IOT 设备所属的分组链存储所述第二数据的哈希值。

可选的,所述处理单元 902,还用于:

在控制所述接收单元 901 接收第一 IOT 设备的获取请求之前,接收所述第一 IOT 设备发送的注册请求;

根据所述注册请求,通过所述路由链对所述第一 IOT 设备的 IOT 设备 ID 进行认证,并在认证通过后,确定所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链;

通过所述第一 IOT 设备所属的分组链确定所述第一 IOT 设备的第二智能合约；

将所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链的信息存储至所述第一智能合约中；所述第一 IOT 设备所属的分组链的信息中记录有所述第一 IOT 设备的第二智能合约在所属的分组链中的地址。

可选的，所述第一智能合约中记录有 IOT 设备的服务类型、IOT 设备所属网络 ID、IOT 设备所属的分组链 ID 的对应关系，以及 IOT 设备所属的分组链 ID、IOT 设备 ID 与 IOT 设备的第二智能合约在所属的分组链中的地址的对应关系；

所述第二智能合约中记录有 IOT 设备 ID、时间戳和 IOT 设备的数据的哈希值的对应关系。

基于与上述图 3 所示的方法相同的构思，本申请还提供一种计算设备，如图 10 所示，该计算设备包括至少一个处理器 1020，用于实现本申请实施例提供的图 3 中任一方法。

计算设备 1000 还可以包括至少一个存储器 1030，用于存储程序指令和/或数据。存储器 1030 和处理器 1020 耦合。本申请实施例中的耦合是装置、单元或模块之间的间接耦合或通信连接，可以是电性，机械或其它的形式，用于装置、单元或模块之间的信息交互。处理器 1020 可能和存储器 1030 协同操作。处理器 1020 可能执行存储器 1030 中存储的程序指令。所述至少一个存储器中的至少一个可以包括于处理器中。

在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。结合本申请实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。为避免重复，这里不再详细描述。

应注意，本申请实施例中的处理器可以是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法实施例的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器、数字信号处理电路（digital signal processor, DSP）、专用集成芯片（application specific integrated circuit, ASIC）、现场可编程门阵列（field programmable gate array, FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

可以理解，本申请实施例中的存储器可以是易失性存储器或非易失性存储器，或可包括易失性和非易失性存储器两者。其中，非易失性存储器可以是只读存储器（read-only memory, ROM）、可编程只读存储器（programmable ROM, PROM）、可擦除可编程只读存储器（erasable PROM, EPROM）、电可擦除可编程只读存储器（electrically EPROM, EEPROM）或闪存。易失性存储器可以是随机存取存储器（random access memory, RAM），其用作外部高速缓存。通过示例性但不是限制性说明，许多形式的 RAM 可用，例如静态

随机存取存储器 (static RAM, SRAM)、动态随机存取存储器 (dynamic RAM, DRAM)、同步动态随机存取存储器 (synchronous DRAM, SDRAM)、双倍数据速率同步动态随机存取存储器 (double data rate SDRAM, DDR SDRAM)、增强型同步动态随机存取存储器 (enhanced SDRAM, ESDRAM)、同步连接动态随机存取存储器 (synchlink DRAM, SLDRAM) 和直接内存总线随机存取存储器 (direct rambus RAM, DR RAM)。应注意, 本文描述的系统和方法的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

计算设备 1000 还可以包括通信接口 1010, 用于通过传输介质和其它设备进行通信, 从而用于计算设备 1000 中的装置可以和其它设备进行通信。在本申请实施例中, 通信接口可以是收发器、电路、总线、模块或其它类型的通信接口。在本申请实施例中, 通信接口为收发器时, 收发器可以包括独立的接收器、独立的发射器; 也可以集成收发功能的收发器、或者是接口电路。

计算设备 1000 还可以包括通信线路 1040。其中, 通信接口 1010、处理器 1020 以及存储器 1030 可以通过通信线路 1040 相互连接; 通信线路 1040 可以是外设部件互连标准 (peripheral component interconnect, 简称 PCI) 总线或扩展工业标准结构 (extended industry standard architecture, 简称 EISA) 总线等。所述通信线路 1040 可以分为地址总线、数据总线、控制总线等。为便于表示, 图 10 中仅用一条粗线表示, 但并不表示仅有一根总线或一种类型的总线。

基于同一发明构思, 本发明实施例还提供了一种计算机可读非易失性存储介质, 包括计算机可读指令, 当计算机读取并执行所述计算机可读指令时, 使得计算机执行上述基于区块链的 IOT 设备间通信的方法。

基于同一发明构思, 本申请实施例提供一种包含指令的计算机程序产品, 当其在计算机上运行时, 使得计算机执行上述基于区块链的 IOT 设备间通信的方法。

本发明是参照根据本发明实施例的方法、设备 (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。

尽管已描述了本发明的优选实施例, 但本领域内的技术人员一旦得知了基本创造性概念, 则可对这些实施例作出另外的变更和修改。所以, 所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

权利要求

1、一种基于区块链的物联网 IOT 设备间通信的方法，其特征在于，适用于包括路由链和至少一个分组链的联盟链；所述方法包括：

接收第一 IOT 设备的获取请求；所述获取请求用于获取第二 IOT 设备的第一数据；

根据所述获取请求，通过所述路由链确定所述第二 IOT 设备所属的分组链；所述路由链用于在确定所述第一 IOT 设备通过第一身份验证后返回所述第二 IOT 设备所属的分组链；

根据所述获取请求，通过所述第二 IOT 设备所属的分组链获取所述获取请求的应答响应；所述第二 IOT 设备所属的分组链用于在确定所述第一 IOT 设备通过第二身份验证后，返回所述获取请求的应答响应；所述应答响应用于获取所述第一数据。

2、如权利要求 1 所述的方法，其特征在于，所述路由链设置有第一智能合约；

所述根据所述获取请求，通过所述路由链确定所述第二 IOT 设备所属的分组链，包括：

根据所述获取请求，调用所述第一智能合约，通过所述第一智能合约确定所述第一 IOT 设备为经过所述路由链认证的 IOT 设备，并通过所述第一智能合约确定所述第二 IOT 设备所属的分组链。

3、如权利要求 1 所述的方法，其特征在于，所述分组链设置有归属于所述分组链的各 IOT 设备的第二智能合约；

所述根据所述获取请求，通过所述第二 IOT 设备所属的分组链获取所述获取请求的应答响应，包括：

根据所述获取请求，调用所述第二 IOT 设备的第二智能合约，通过所述第二 IOT 设备的第二智能合约确定所述第一 IOT 设备具有访问所述第二 IOT 设备的权限，并通过所述第二 IOT 设备的第二智能合约得到所述应答响应。

4、如权利要求 1 至 3 任一项所述的方法，其特征在于，所述应答响应为所述第一数据的哈希值；

所述第一数据的哈希值是所述第二 IOT 设备将所述第一数据存储至分布式存储系统后，所述分布式存储系统返回的哈希值。

5、如权利要求 4 所述的方法，其特征在于，所述方法还包括：

接收所述第二 IOT 设备发送的上链请求；所述上链请求包括所述第二 IOT 设备的第二数据的哈希值；

根据所述上链请求，通过所述路由链确定所述第二 IOT 设备所属的分组链；

根据所述上链请求，通过所述第二 IOT 设备所属的分组链存储所述第二数据的哈希值。

6、如权利要求 4 所述的方法，其特征在于，在所述接收第一 IOT 设备的获取请求之前，还包括：

接收所述第一 IOT 设备发送的注册请求；

根据所述注册请求，通过所述路由链对所述第一 IOT 设备的 IOT 设备 ID 进行认证，并在认证通过后，确定所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链；

通过所述第一 IOT 设备所属的分组链确定所述第一 IOT 设备的第二智能合约；

将所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链的信息存储至所述第一智能合约中；所述第一 IOT 设备所属的分组链的信息中记录有所述第一 IOT 设备的第二智能合约在所属的分组链中的地址。

7、如权利要求 6 所述的方法，其特征在于，所述第一智能合约中记录有 IOT 设备的服务类型、IOT 设备所属网络 ID、IOT 设备所属的分组链 ID 的对应关系，以及 IOT 设备所属的分组链 ID、IOT 设备 ID 与 IOT 设备的第二智能合约在所属的分组链中的地址的对应关系；

所述第二智能合约中记录有 IOT 设备 ID、时间戳和 IOT 设备的数据的哈希值的对应关系。

8、一种基于区块链的物联网 IOT 设备间通信的装置，其特征在于，适用于包括路由链和至少一个分组链的联盟链；所述装置包括：

接收单元，用于接收第一 IOT 设备的获取请求；所述获取请求用于获取第二 IOT 设备的第一数据；

处理单元，用于根据所述获取请求，通过所述路由链确定所述第二 IOT 设备所属的分组链；所述路由链用于在确定所述第一 IOT 设备通过第一身份验证后返回所述第二 IOT 设备所属的分组链；

所述处理单元，还用于根据所述获取请求，通过所述第二 IOT 设备所属的分组链获取所述获取请求的应答响应；所述第二 IOT 设备所属的分组链用于在确定所述第一 IOT 设备通过第二身份验证后，返回所述获取请求的应答响应；所述应答响应用于获取所述第一数据。

9、如权利要求 8 所述的装置，其特征在于，所述路由链设置有第一智能合约；

所述处理单元，具体用于：

根据所述获取请求，调用所述第一智能合约，通过所述第一智能合约确定所述第一 IOT 设备为经过所述路由链认证的 IOT 设备，并通过所述第一智能合约确定所述第二 IOT 设备所属的分组链。

10、如权利要求 8 所述的装置，其特征在于，所述分组链设置有归属于所述分组链的各 IOT 设备的第二智能合约；

所述处理单元，具体用于：

根据所述获取请求，调用所述第二 IOT 设备的第二智能合约，通过所述第二 IOT 设备的第二智能合约确定所述第一 IOT 设备具有访问所述第二 IOT 设备的权限，并通过所述第二 IOT 设备的第二智能合约得到所述应答响应。

11、如权利要求 8 至 10 任一项所述的装置，其特征在于，所述应答响应为所述第一数据的哈希值；

所述第一数据的哈希值是所述第二 IOT 设备将所述第一数据存储至分布式存储系统后，所述分布式存储系统返回的哈希值。

12、如权利要求 11 所述的装置，其特征在于，所述处理单元，还用于：

控制所述接收单元接收所述第二 IOT 设备发送的上链请求；所述上链请求包括所述第二 IOT 设备的第二数据的哈希值；

根据所述上链请求，通过所述路由链确定所述第二 IOT 设备所属的分组链；

根据所述上链请求，通过所述第二 IOT 设备所属的分组链存储所述第二数据的哈希值。

13、如权利要求 11 所述的装置，其特征在于，所述处理单元，还用于：

在控制所述接收单元接收第一 IOT 设备的获取请求之前，接收所述第一 IOT 设备发送的注册请求；

根据所述注册请求，通过所述路由链对所述第一 IOT 设备的 IOT 设备 ID 进行认证，并在认证通过后，确定所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链；

通过所述第一 IOT 设备所属的分组链确定所述第一 IOT 设备的第二智能合约；

将所述第一 IOT 设备的身份证书及所述第一 IOT 设备所属的分组链的信息存储至所述第一智能合约中；所述第一 IOT 设备所属的分组链的信息中记录有所述第一 IOT 设备的第二智能合约在所属的分组链中的地址。

14、如权利要求 13 所述的装置，其特征在于，所述第一智能合约中记录有 IOT 设备的服务类型、IOT 设备所属网络 ID、IOT 设备所属的分组链 ID 的对应关系，以及 IOT 设备所属的分组链 ID、IOT 设备 ID 与 IOT 设备的第二智能合约在所属的分组链中的地址的对应关系；

所述第二智能合约中记录有 IOT 设备 ID、时间戳和 IOT 设备的数据的哈希值的对应关系。

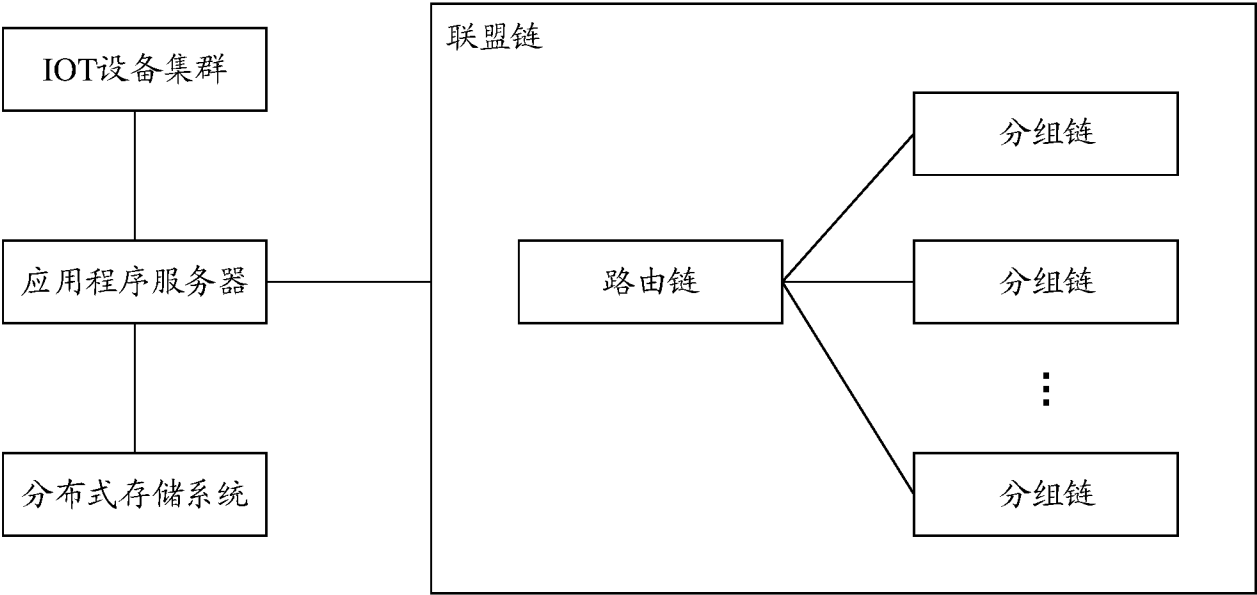
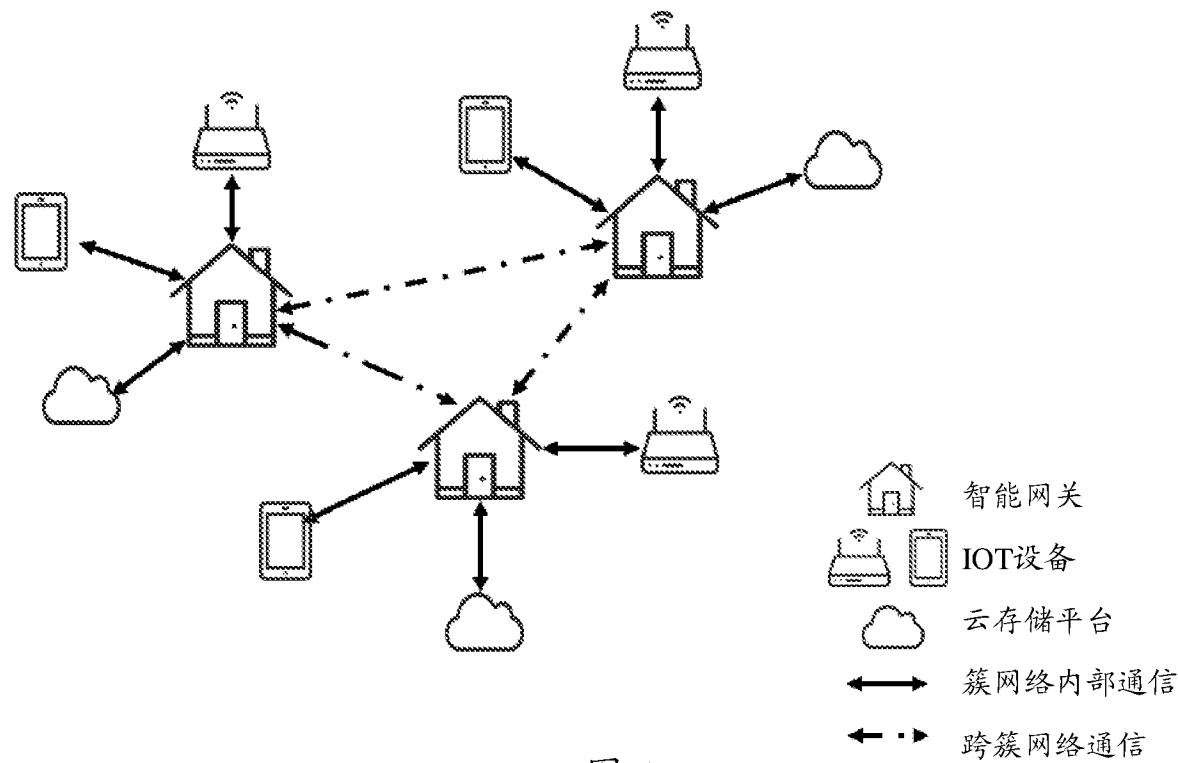
15、一种计算设备，其特征在于，包括：

存储器，用于存储程序指令；

处理器，用于调用所述存储器中存储的程序指令，按照获得的程序执行权利要求 1 至 7 任一项所述的方法。

16、一种计算机可读非易失性存储介质，其特征在于，包括计算机可读指令，当计算机读取并执行所述计算机可读指令时，使得计算机执行如权利要求 1 至 7 任一项所述的方法。

17、一种计算机程序产品，其特征在于，所述计算机程序产品包括存储在非暂态计算机可读存储介质上的计算程序，所述计算机程序包括程序指令，当所述程序指令被计算机执行时，使所述计算机执行权利要求 1 至 7 任一所述方法。



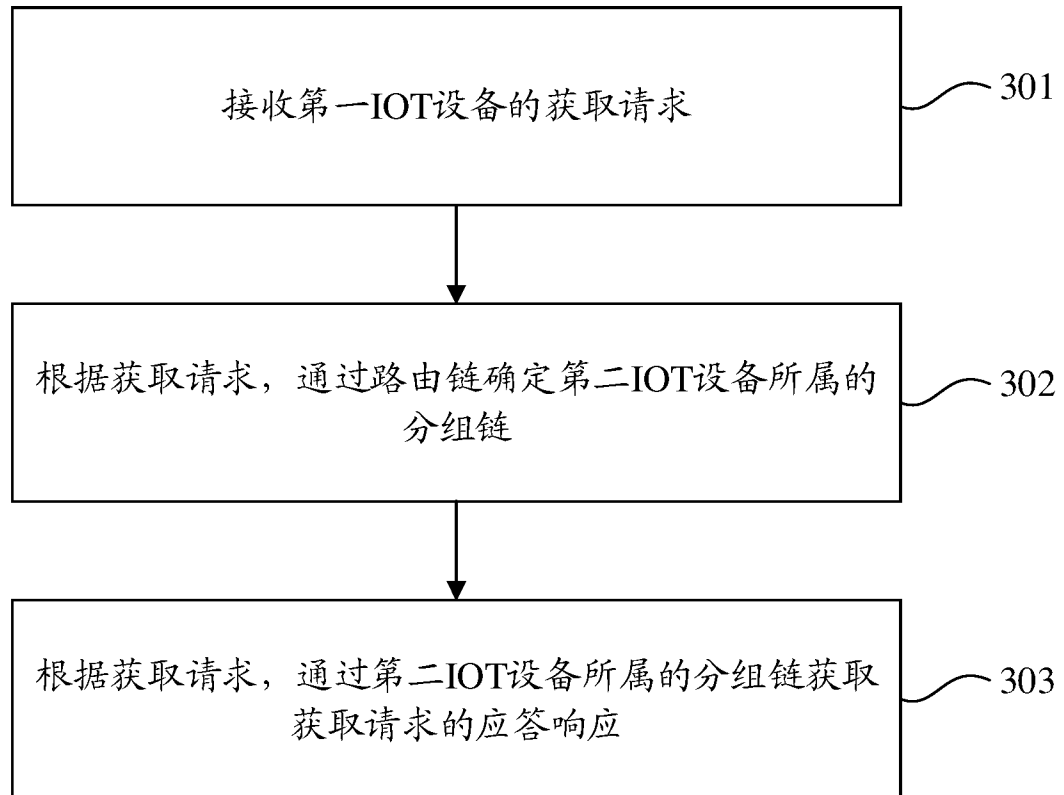


图 3

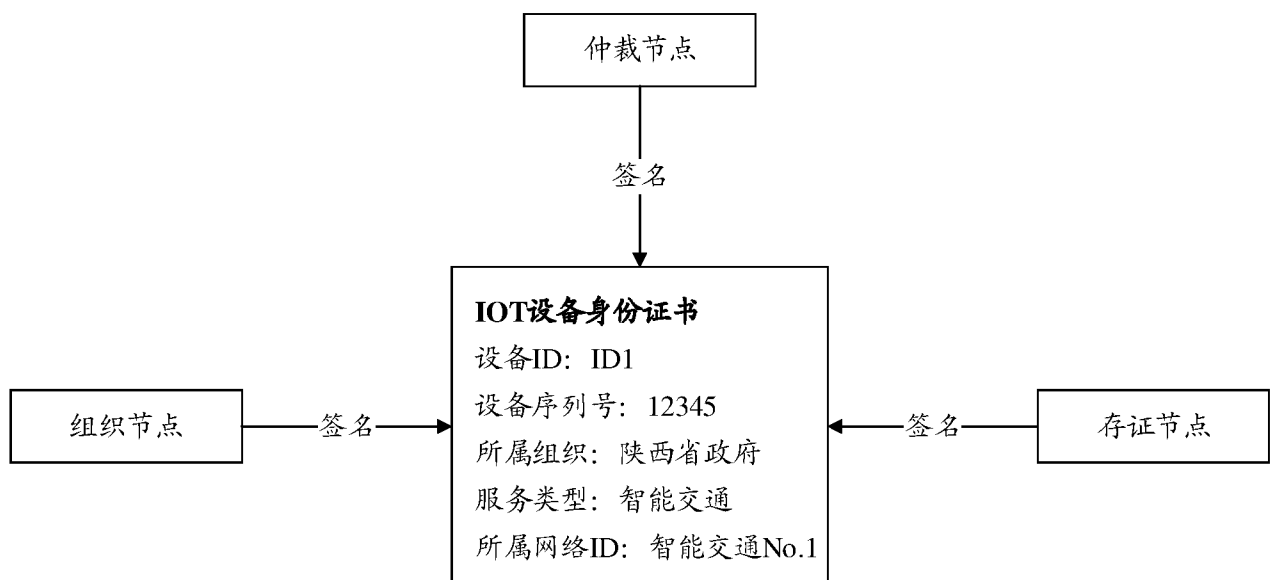


图 4

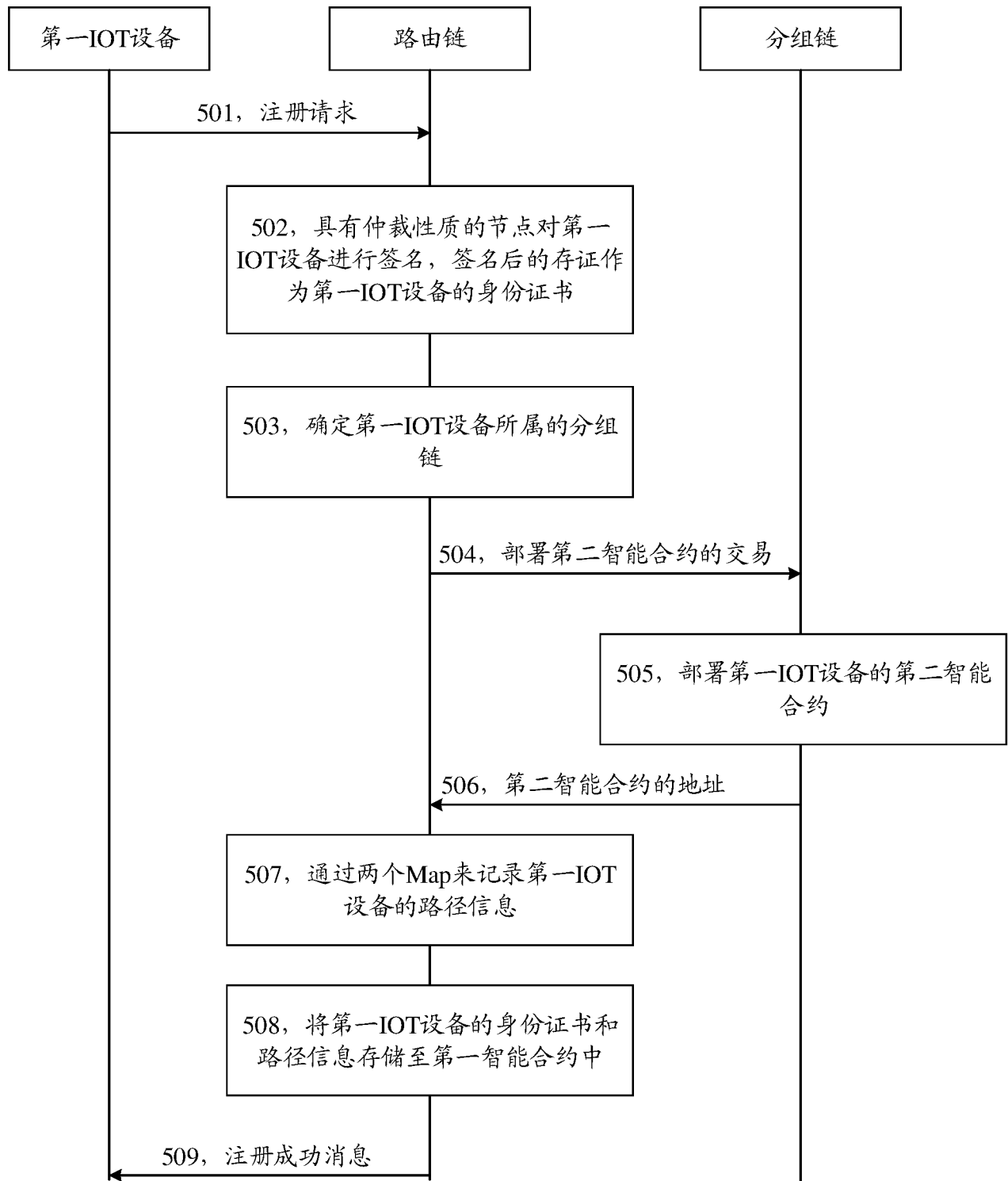


图 5

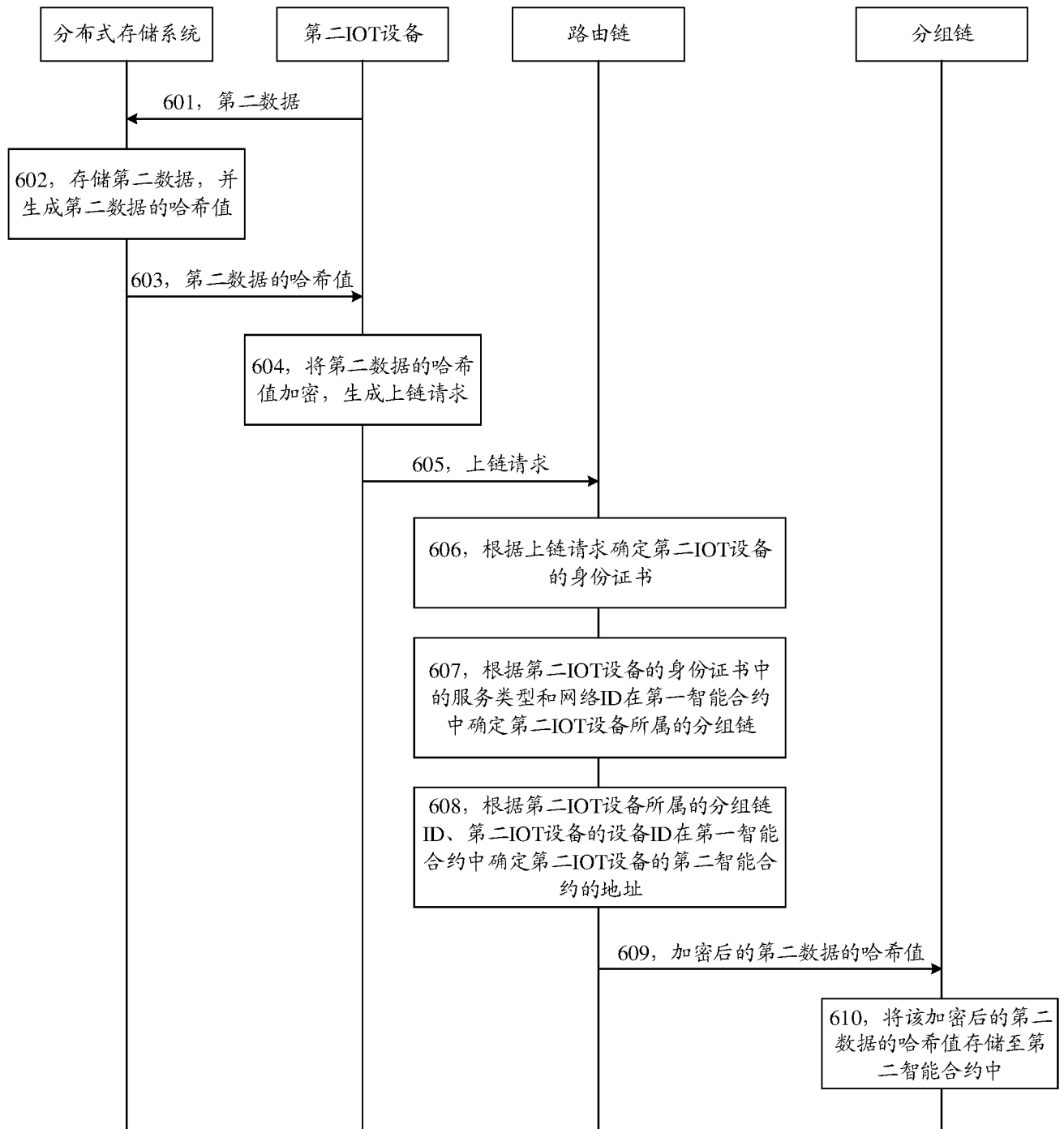


图 6

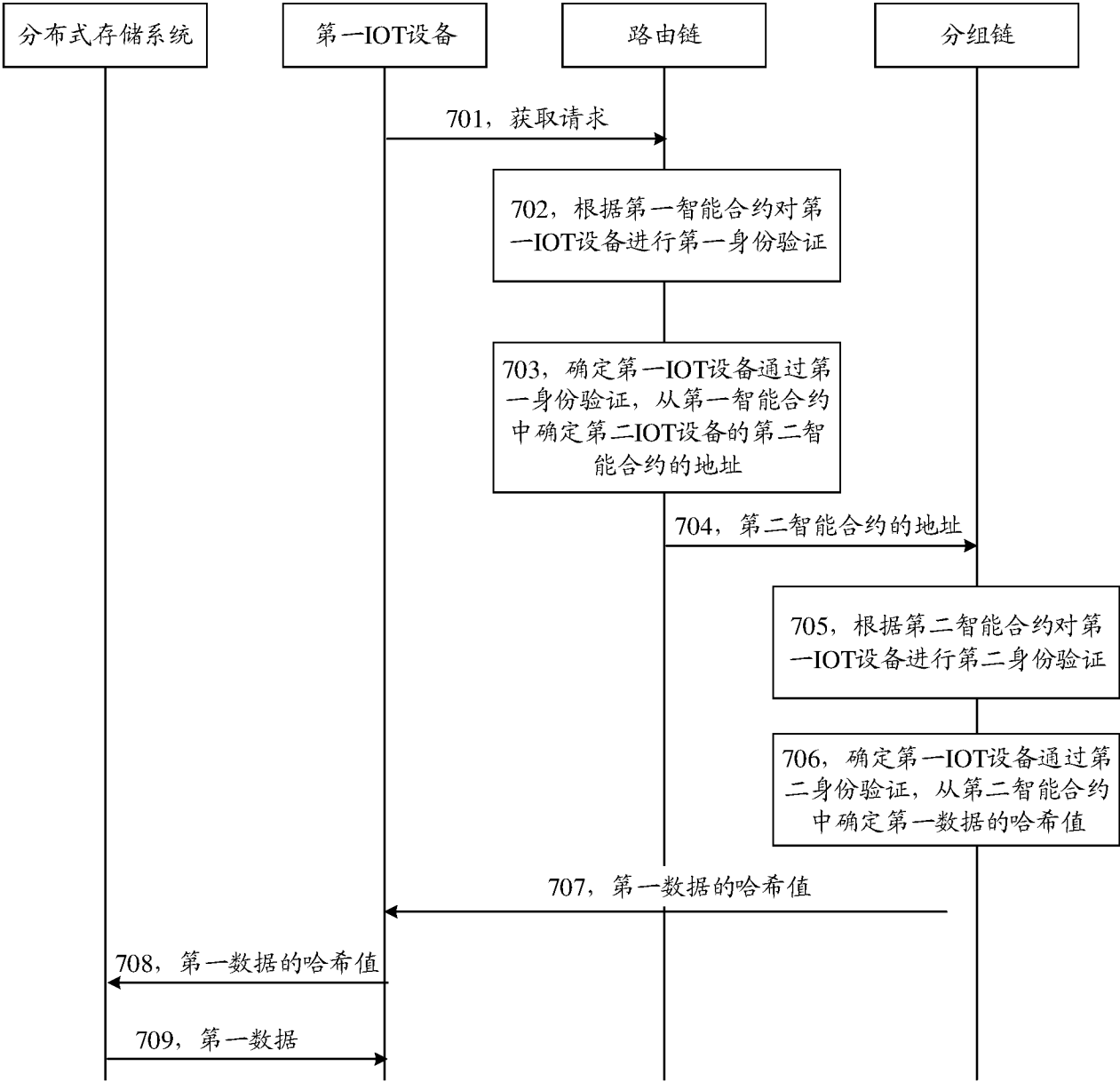


图 7

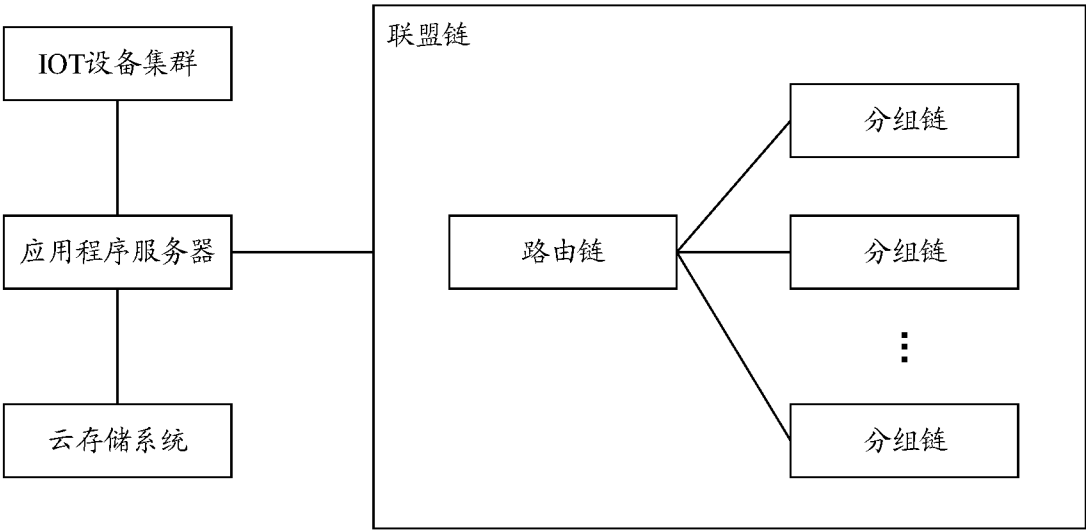


图 8

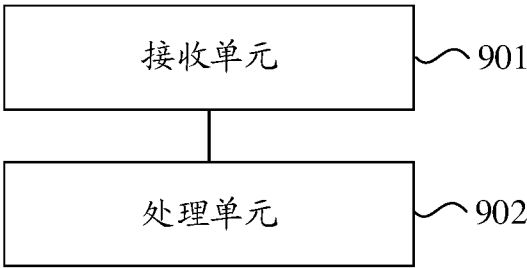


图 9

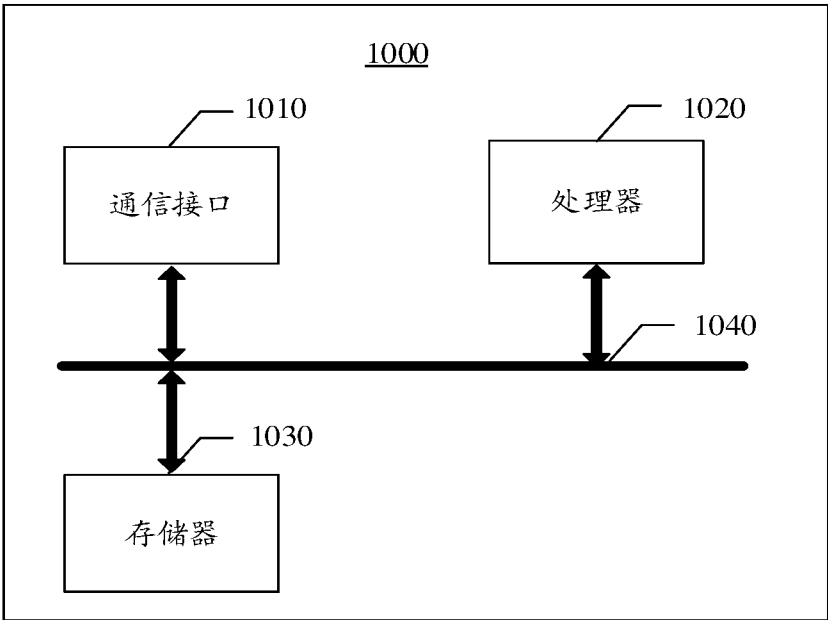


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/095199

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/08(2006.01)i; H04L 9/32(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)

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)

CNABS; CNTXT; VEN; USTXT; WOTXT; EPTXT; CNKI: 区块链, 联盟, 链, 分组, 多链, 多个, 请求, 获取, 访问, 物联网, 路由, 验证, 对应, 合约, blockchain, block chain, consortium, chain, group, multiple, request, access, get, IOT, rout+, corresponding, contract

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110278255 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 24 September 2019 (2019-09-24) description, paragraphs [0067]-[0167]	1-17
Y	CN 108540536 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 14 September 2018 (2018-09-14) description paragraphs [0041]-[0124], figure 4	1-17
Y	CN 109446830 A (SINOCHAIN TECHNOLOGY CO., LTD.) 08 March 2019 (2019-03-08) description, paragraphs [0042]-[0082]	1-17
A	CN 109492380 A (PANOVASIC TECHNOLOGY CO., LTD. et al.) 19 March 2019 (2019-03-19) entire document	1-17
A	US 2018254905 A1 (CHUN SAM GU) 06 September 2018 (2018-09-06) entire document	1-17



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

29 July 2020

Date of mailing of the international search report

02 September 2020

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

International application No.

PCT/CN2020/095199

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	周微 (ZHOU, Wei). "面向物联网的安全认证方法研究 (Research on Security Authentication Method for Internet of Things)" 中国优秀硕士学位论文全文数据库 信息科技辑 (<i>Information Science and Technology, Chinese Master's Theses Full-Text Database</i>), No. 05, 15 May 2019 (2019-05-15), ISSN: 1674-0246, chapter 5	1-17

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/095199

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110278255	A	24 September 2019	None			
CN	108540536	A	14 September 2018	None			
CN	109446830	A	08 March 2019	None			
CN	109492380	A	19 March 2019	None			
US	2018254905	A1	06 September 2018	EP	3386142	B1	04 March 2020
				WO	2017095036	A1	08 June 2017
				JP	6601828	B2	06 November 2019
				KR	101678795	B1	22 November 2016
				EP	3386142	A4	10 April 2019
				JP	2018525952	A	06 September 2018
				EP	3386142	A1	10 October 2018

国际检索报告

国际申请号

PCT/CN2020/095199

A. 主题的分类

H04L 29/08 (2006.01) i; H04L 9/32 (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)

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))

CNABS; CNTXT; VEN; USTXT; WOTXT; EPTXT; CNKI: 区块链, 联盟, 链, 分组, 多链, 多个, 请求, 获取, 访问, 物联网, 路由, 验证, 对应, 合约, blockchain, block chain, consortium, chain, group, multiple, request, access, get, IoT, rout+, corresponding, contract

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 110278255 A (深圳前海微众银行股份有限公司) 2019年 9月 24日 (2019 - 09 - 24) 说明书第[0067]-[0167]段	1-17
Y	CN 108540536 A (深圳前海微众银行股份有限公司) 2018年 9月 14日 (2018 - 09 - 14) 说明书第[0041]-[0124]段, 图4	1-17
Y	CN 109446830 A (中链科技有限公司) 2019年 3月 8日 (2019 - 03 - 08) 说明书第[0042]-[0082]段	1-17
A	CN 109492380 A (四川虹微技术有限公司 等) 2019年 3月 19日 (2019 - 03 - 19) 全文	1-17
A	US 2018254905 A1 (CHUN SAM GU) 2018年 9月 6日 (2018 - 09 - 06) 全文	1-17
A	周微. “面向物联网的安全认证方法研究” 中国优秀硕士学位论文全文数据库 信息科技辑, 第05期, 2019年 5月 15日 (2019 - 05 - 15), ISSN: 1674-0246, 第五章	1-17

☐ 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

2020年 7月 29日

国际检索报告邮寄日期

2020年 9月 2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

授权官员

吕梅利

电话号码 86-(512)-88996099

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/095199

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	110278255	A	2019年 9月 24日	无			
CN	108540536	A	2018年 9月 14日	无			
CN	109446830	A	2019年 3月 8日	无			
CN	109492380	A	2019年 3月 19日	无			
US	2018254905	A1	2018年 9月 6日	EP	3386142	B1	2020年 3月 4日
				WO	2017095036	A1	2017年 6月 8日
				JP	6601828	B2	2019年 11月 6日
				KR	101678795	B1	2016年 11月 22日
				EP	3386142	A4	2019年 4月 10日
				JP	2018525952	A	2018年 9月 6日
				EP	3386142	A1	2018年 10月 10日