

一种基于区块链的数据处理方法、装置、电子设备、计算机可读存储介质及计算机程序产品

相关申请的交叉引用

本申请基于申请号为 202211259133.1、申请日为 2022 年 10 月 14 日的中国专利申请提出，并要求中国专利申请的优先权，中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及互联网技术领域，尤其涉及一种基于区块链的数据处理方法、装置、电子设备、计算机可读存储介质及计算机程序产品。

背景技术

随着移动互联网技术以及各种新兴技术的快速发展，平台应用好像雨后春笋。随着大量平台应用的出现，用户有了更广泛的选择。为了提升活跃留存，平台应用需要不断地推广自己的平台。

在现有技术中，平台应用为了推广自己，会与具有强大的平台推广能力的广告商合作。具体为，平台应用提供自己的第一业务数据至广告商，广告商确定自己拥有的第二业务数据与第一业务数据之间共同的业务数据，即业务交集数据，然后进行与业务交集数据相关联的推广处理。明显地，现有技术存在如下缺陷：1、平台应用将自己的原始数据（即第一业务数据）传输至广告商，故降低了数据的安全性；2、平台应用与广告商之间直接的数据流转，致使无法准确地追溯数据获取状态。

发明内容

本申请实施例提供一种基于区块链的数据处理方法、装置、电子设备、计算机可读存储介质及计算机程序产品，可以提高数据的安全性以及准确地追溯数据获取状态。

本申请实施例提供了一种基于区块链的数据处理方法，所述方法由第一设备执行，所述方法包括：

当第一业务数据满足数据上传条件时，生成第一业务数据对应的第一位数组；

通过数据密钥，对第一位数组进行加密处理，得到密文位数组；其中，所述数据密钥是第二设备在数据交集应用中生成的，数据交集应用运行于第二设备的可信执行环境 a 中；

将密文位数组传输至区块链中的区块链节点，以使区块链节点存储密文位数组；其中，存储在区块链节点的密文位数组用于由区块链节点转发至第二设备；第二设备用于在数据交集应用中，通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理，得到第一位数组；第一位数组用于指示第二设备在数据交集应用中，生成第二业务数据对应的第二位数组；第二位数组以及第一位数组用于指示第二设备在数据交集应用中，确定第一业务数据以及第二业务数据之间的业务交集数据；业务交集数据用于指示第二设备进行与业务交集数据相关联的业务处理。

本申请实施例提供了一种基于区块链的数据处理方法，所述方法由第二设备执行，所述方法包括：

获取由区块链中的区块链节点转发的密文位数组；其中，密文位数组是第一设备传输至区块链节点的，且密文位数组是第一设备通过数据密钥，对第一位数组进行加密处理所得到的，数据密钥是第二设备在数据交集应用中生成的；数据交集应用运行于第二设备的可信执行环境 a 中；第一位数组是第一设备在第一业务数据满足数据上传条件时，针对第一业务数据所生成的；

在数据交集应用中，通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理，得到第一位数组；

在数据交集应用中，生成第二业务数据对应的第二位数组，根据第二位数组以及第一位数组，确定第一业务数据以及第二业务数据之间的业务交集数据；

对业务交集数据进行业务处理。

本申请实施例提供了一种基于区块链的数据处理装置，所述装置运行于第一设备，所述装置包括：

第一生成模块，配置为当第一业务数据满足数据上传条件时，生成第一业务数据对应的第一位数组；

第一处理模块，配置为通过数据密钥，对第一位数组进行加密处理，得到密文位数组；其中，数据密钥是第二设备在数据交集应用中生成的，数据交集应用运行于第二设备的可信执行环境 a 中；

密文传输模块，配置为将密文位数组传输至区块链中的区块链节点，以使区块链节点存储密文位数组；其中，存储在区块链节点的密文位数组用于由区块链节点转发至第二设备；第二设备用于在数据交集应用中，通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理，得到第一位数组；第一位数组用于指示第二设备在数据交集应用中，生成第二业务数据对应的第二位数组；第二位数组以及第一位数组用于指示第二设备在数据交集应用中，确定第一业务数据以及第二业务数据之间的业务交集数据；业务交集数据用于指示第二设备进行与业务交集数据相关联的业务处理。

还配置为还配置为还配置为还配置为还配置为还配置为还配置为还配置为还配置为本申请实施例提供了一种基于区块链的数据处理装置，所述装置运行于第二设备，所述装置包括：

密文获取模块，配置为获取由区块链中的区块链节点转发的密文位数组；其中，密文位数组是第一设备传输至区块链节点的，且密文位数组是第一设备通过数据密钥，对第一位数组进行加密处理所得到的，数据密钥是第二设备在数据交集应用中生成的；数据交集应用运行于第二设备的可信执行环境 a 中；第一位数组是第一设备在第一业务数据满足数据上传条件时，针对第一业务数据所生成的；

第一处理模块，配置为在数据交集应用中，通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理，得到第一位数组；

第一生成模块，配置为在数据交集应用中，生成第二业务数据对应的第二位数组，根据第二位数组以及第一位数组，确定第一业务数据以及第二业务数据之间的业务交集数据；

第二处理模块，配置为对业务交集数据进行业务处理。

本申请提供了一种电子设备，包括：处理器、存储器、网络接口；

上述处理器与上述存储器、上述网络接口相连，其中，上述网络接口用于提供数据通信功能，上述存储器用于存储计算机程序，上述处理器用于调用上述计算机程序，以使得电子设备执行本申请实施例中的基于区块链的数据处理方法。

本申请实施例提供了一种计算机可读存储介质，上述计算机可读存储介质中存储有计算机程序，上述计算机程序适于由处理器加载并执行本申请实施例中的基于区块链的数据处理方法。

本申请实施例提供了一种计算机程序产品，该计算机程序产品包括计算机程序，该计算机程序存储在计算机可读存储介质中；电子设备的处理器从计算机可读存储介质读取该计算机程序，处理器执行该计算机程序，使得该电子设备执行本申请实施例中的基于区块链的数据处理方法。

在本申请实施例中，通过生成第一业务数据对应的第一位数组，可以确保第一业务数据可用不可见，故可以提高第一业务数据的安全性；进一步地，由于数据密钥是通过可信执行环境 a 中的数据交集应用

所生成的，故其生成环境安全、应用环境安全以及存储环境安全，故通过数据密钥对第一位数组进行加密处理，可以提高第一位数组的安全性；进一步地，通过将密文位数组传输至区块链，可以准确地追溯第二设备针对密文位数组的获取状态；此外，本申请实施例是通过第一位数组以及第二业务数据对应的第二位数组，确定第一业务数据以及第二业务数据之间的业务交集数据，故不仅可以进行与业务交集数据相关联的业务处理，还进一步提高了第一业务数据的安全性。上述可知，采用本申请实施例，可以提高数据（包括第一业务数据以及第一位数组）的安全性，以及准确地追溯数据获取状态。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有技术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申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 是本申请实施例提供的一种系统架构示意图；

图 2a 是本申请实施例提供的一种基于区块链的数据处理的场景示意图一；

图 2b 是本申请实施例提供的一种基于区块链的对象注册方法的流程示意图；

图 2c 是本申请实施例提供的一种基于区块链的数据处理的场景示意图二；

图 3 是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图一；

图 4a 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图一；

图 4b 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图二；

图 4c 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图三；

图 4d 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图四；

图 4e 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图五；

图 5 是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图二；

图 6a 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图六；

图 6b 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图七；

图 6c 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图八；

图 7 是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图三；

图 8 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图九；

图 9 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图十；

图 10 是本申请实施例提供的一种基于区块链的数据处理装置的结构示意图一；

图 11 是本申请实施例提供的一种基于区块链的数据处理装置的结构示意图二；

图 12 是本申请实施例提供的一种电子设备的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请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申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，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，都属于本申请保护的范围。

为了便于理解，首先对部分名词进行以下简单解释：

1、区块链：区块链是一种以区块为基本单位的链式数据结构，区块中利用数字摘要对之前获取的交易历史进行校验，适合分布式记账场景下防篡改和可扩展性的需求；区块链还指代区块链结构实现的分布式记账技术，包括分布式共识、隐私与安全保护、点对点通信技术、网络协议、智能合约等。区块链的目标是实现一个分布的数据记录账本，此账本只允许添加，不允许删除。账本底层的基本结构是一个线性的链表。链表由一个个“区块”串联组成，后继区块中记录前继区块的哈希（Hash）值，每个区块（以及区块中的交易）是否合法，可通过计算哈希值的方式进行快速检验。若网络中的节点发出添加一个新的区块的请求，必须经过共识机制对区块达成共识确认。

2、哈希值（hash）：也称作信息特征值或特征值，哈希值是通过哈希算法将任意长度的输入数据转换为密码并进行固定输出而生成的，不能通过解密哈希值来检索原始输入数据，它是一个单向的加密函数。在区块链中，每个区块（除了初始区块）都包含前继区块的哈希值，哈希值是区块链技术中的潜力核心基础和最重要的方面，它保留了记录和查看数据的真实性，以及区块链作为一个整体的完整性。

3、区块链节点：区块链网络将节点区分为共识节点（也可以称作核心节点）以及同步节点（可以包括数据节点以及轻节点）。其中，共识节点负责区块链全网的共识业务；同步节点负责同步共识节点的账本信息，即同步最新的区块数据。无论是共识节点还是同步节点，其内部构造都包括网络通信组件，因为区块链网络本质是一个点对点（Peer to Peer, P2P）网络，需通过 P2P 组件与区块链网络中的其他节点进行通信。区块链网络中的资源和服务都分散在各个节点上，信息的传输和服务的实现都直接在节点之间进行，无需中间环节或中心化的服务器（第三方）介入。

4、公钥（public key）与私钥（private key）：公钥与私钥是通过一种算法得到的一个密钥对（即一个公钥和一个私钥），公钥是密钥对中公开的部分，私钥则是非公开的部分。公钥通常用于加密数据、验证数字签名等。通过这种算法能够确保得到的密钥对是唯一的，使用这种密钥对的时候，如果用其中一个密钥加密一段数据，必须用另一个密钥解密，例如，用公钥加密数据就必须用私钥解密，如果用私钥加密也必须用公钥解密，否则解密将不会成功。

5、非对称签名：签名算法包括两个密钥，公开密钥（简称公钥，public key）和私有密钥（简称私钥，private key）。公钥与私钥是一对，如果用私钥对数据进行签名，只有用对应的公钥才能验签。因为签名过程和验签过程分别使用两个不同的密钥，所以这种算法称作非对称签名。非对称签名实现机密信息交换的基本过程可以是：甲方生成一对密钥并将公钥公开，甲方需要向其他角色（乙方）发送消息时，使用自己的私钥对机密消息进行签名后再发送给乙方；乙方再用甲方的公钥对签名后的消息进行验签。

6、智能合约（Smart Contract）：是一种旨在以信息化方式传播、验证或执行合同的计算机协议。在区块链系统当中，智能合约（简称合约）是一种区块链各节点可以理解并执行的代码，可以执行任意逻辑并得到结果。在实际应用中，智能合约通过区块链上的交易来管理与试用。每条交易相当于对区块链系统的一个远程过程调用（Remote Procedure Call, RPC）请求。如果说智能合约相当于可执行程序，区块链就相当于提供运行环境的操作系统。区块链可以包含多个合约（如本申请中的资源融合函数、资源发行函数等），以合约账号（Identity, ID）、标识号或名称来区分。在本申请实施例中，发布主题合约以及订阅主题合约均属于智能合约。

7、可信执行环境（Trusted Execution Environment, TEE）：可信执行环境是计算平台上由软硬件方法构建的一个安全区域，可以保证在安全区域内加载的代码和数据在机密性和完整性方面得到保护。可信执行环境的目标是确保一个任务按照预期执行，保证初始状态的机密性、完整性，以及运行时状态的机

密性、完整性。

请参见图 1，图 1 是本申请实施例提供的一种系统架构示意图。如图 1 所示，该系统架构可以包括第一设备集群、第二设备集群、证书设备集群以及区块链网络。

上述系统可以包括一个或多个第一设备，本申请实施例不对第一设备的数量进行限制。如图 1 所示，第一设备集群包括第一设备 100a。第一设备 100a 是指安装有平台应用的设备。其中，平台应用可以为视频应用、直播应用、社交应用、即时通信应用、游戏应用、音乐应用、购物应用、小说应用、浏览器等具有提供平台功能的应用。其中，平台应用对应的应用客户端可以为独立的客户端，也可以为集成在某客户端（例如，社交客户端、教育客户端以及多媒体客户端等）中的嵌入式子客户端，在此不做限定。本申请实施例中的第一设备 100a 可以提供上述平台应用的第一业务数据，基于隐私保护需求，可以使用相关技术手段（例如布隆过滤器），隐匿原始数据（即第一业务数据），生成第一位数组，确保第一业务数据的可用性。

上述系统可以包括一个或多个第二设备，本申请实施例不对第二设备的数量进行限制。如图 1 所示，第二设备集群包括第二设备 100b，第二设备 100b 可以提供可信执行环境，例如指令集扩展（Software Guard Extensions, SGX）。基于其硬件技术，第二设备 100b 可以在可信执行环境中运行数据交集应用，在数据交集应用中生成数据密钥，并将数据密钥存储于安全飞地，故可以确保数据密钥的安全。此外，第二设备 100b 可以在区块链网络中下载第一设备 100a 所提供的第一位数组，在可信执行环境中运行数据交集应用，以进行数据求交运算，即通过第一位数组以及自己的第二业务数据，确定第一业务数据以及第二业务数据之间的共同业务数据，本申请实施例称为业务交集数据。此外，第二设备 100b 可以进行与业务交集数据相关联的业务处理，例如业务交集数据用于表征交集用户，则可以对交集用户投放针对上述平台应用的广告，吸引交集用户回归平台应用。其中，数据交集应用可以为短视频应用、直播应用、社交应用、即时通信应用、游戏应用、音乐应用、购物应用、小说应用、浏览器等具有提供业务交集数据确定功能的应用。其中，数据交集应用对应的应用客户端可以为独立的客户端，也可以为集成在某客户端（例如，社交客户端、教育客户端以及多媒体客户端等）中的嵌入式子客户端，在此不做限定。

上述系统可以包括一个或多个证书设备，本申请实施例不对证书设备的数量进行限制。如图 1 所示，证书设备集群包括证书设备 100c。本申请实施例中的证书设备 100c 是指具有提供对象信息背书功能的设备，例如证书颁发机构（Certificate Authority, CA）对应的设备。证书设备集群可以为第一设备集群对应的第一对象以及第二设备集群对应的第二对象分别提供对象认证，且为第一对象以及第二对象分别提供对象信息背书，并将对象公钥与其对象信息绑定起来，用于验签，确保对象信息的完整性及不可伪造，并确保信息发送方的不可抵赖性。

图 1 中的任意设备（包括第一设备 100a、第二设备 100b 以及证书设备 100c）包括但不限于终端设备或业务服务器。其中，业务服务器可以是独立的物理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云数据库、云服务、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、CDN、以及大数据和人工智能平台等基础云计算服务的云服务器。终端设备包括但不限于手机、电脑、智能语音交互设备、智能家电、车载终端、飞行器等。

区块链网络可以包括区块链节点集群 10，区块链节点集群 10 可以包括区块链节点 10A、区块链节点 10B、区块链节点 10C 以及区块链节点 10N。同理，本申请实施例不对区块链节点集群 10 中的区块链节点的数量进行限制。图 1 中的区块链节点包括但不限于移动终端或服务器。上述服务器可以是独立的物

理服务器，也可以是多个物理服务器构成的服务器集群或者分布式系统，还可以是提供云服务、云数据库、云计算、云函数、云存储、网络服务、云通信、中间件服务、域名服务、安全服务、内容分发网络（Content Delivery Network，简称 CDN）、以及大数据和人工智能平台等基础云计算服务的云服务器。上述移动终端包括但不限于手机、电脑、智能语音交互设备、智能家电、车载终端、飞行器等。其中，移动终端和服务器可以通过有线或无线方式进行直接或间接地连接，本申请实施例对此不做限制。

第一设备集群之间可以存在通信连接。同时，第一设备集群中的第一设备可以与第二设备集群中的第二设备存在通信连接，例如第一设备 100a 与第二设备 100b 之间存在通信连接。同时，第一设备集群中的第一设备可以与证书设备集群中的证书设备存在通信连接，例如第一设备 100a 与证书设备 100c 之间存在通信连接。同时，第一设备集群中的第一设备可以与区块链节点集群 10 中的区块链节点存在通信连接，例如第一设备 100a 可以与区块链节点 10A 之间存在通信连接。

第二设备集群之间可以存在通信连接。同时，第二设备集群中的第二设备可以与证书设备集群中的证书设备存在通信连接，例如第二设备 100b 与证书设备 100c 之间存在通信连接。同时，第二设备集群中的第二设备可以与区块链节点集群 10 中的区块链节点存在通信连接，例如第二设备 100b 可以与区块链节点 10A 之间存在通信连接。

证书设备集群之间可以存在通信连接。同时，证书设备集群中的证书设备可以与区块链节点集群 10 中的区块链节点存在通信连接，例如证书设备 100c 可以与区块链节点 10A 之间存在通信连接。

区块链节点集群 10 之间可以存在通信连接，例如区块链节点 10A 与区块链节点 10C 之间存在通信连接，区块链节点 10A 与区块链节点 10N 之间存在通信连接。

上述的通信连接不限定连接方式，可以通过有线通信方式进行直接或间接地连接，也可以通过无线通信方式进行直接或间接地连接，还可以通过其他方式，本申请在此不做限制。

在本申请的具体实施方式中，涉及到用户信息（例如主题发布对象信息以及主题订阅对象信息）等相关的数据，当本申请中的实施例运用到具体产品或技术中时，需要获得用户许可或者同意，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

本申请实施例提供的基于区块链的数据处理方法的流程可以概述如下。

步骤 1、第一对象（例如平台方）对应的第一设备 100a 生成用于业务消息签名的第一非对称密钥对；第二对象（例如广告商，不同于第一对象的另一个平台方）对应的第二设备 100b 生成用于业务消息签名的第二非对称密钥对，以及生成用于数据交集应用签名的第三非对称密钥对，第三非对称密钥对可以用于确定应用开发者为第二对象的开发人员。请一并参见图 2a，图 2a 是本申请实施例提供的一种基于区块链的数据处理的场景示意图一。第一非对称密钥对包括图 2a 中的第一私钥以及第一私钥对应的第一公钥；第二非对称密钥对包括图 2a 中的第二私钥以及第二私钥对应的第二公钥；第三非对称密钥对包括图 2a 中的第三私钥以及第三私钥对应的第三公钥。

步骤 2、如图 2a 所示，第一设备 100a 将第一公钥以及用于表征第一对象的第一对象信息作为参数，生成第一证书申请请求；第一设备 100a 通过第一私钥，对第一证书申请请求进行签名处理，得到第一签名消息，将携带第一签名消息的第一证书申请请求发送至证书设备 100c。第二设备 100b 将第二公钥以及用于表征第二对象的第二对象信息作为参数，生成第二证书申请请求；第二设备 100b 通过第二私钥，对第二证书申请请求进行签名处理，得到第二签名消息，将携带第二签名消息的第二证书申请请求发送至证书设备 100c。第二设备 100b 将第三公钥以及用于表征第二对象的第二对象信息作为参数，生成第三证

书申请请求；第二设备 100b 通过第三私钥，对第三证书申请请求进行签名处理，得到第三签名消息，将携带第三签名消息的第三证书申请请求发送至证书设备 100c。第二设备 100b 向证书设备 100c 申请两方证书。

步骤 3、如图 2a 所示，证书设备 100c 收到第一证书申请请求时，先通过第一公钥对第一签名消息进行验签处理，若验签成功，则审核第一对象信息，若证书设备 100c 确认第一对象信息无误后，则向第一设备 100a 颁发第一业务证书，该第一业务证书包括第一公钥。同样地，收到第二证书申请请求时，先通过第二公钥对第二签名消息进行验签处理，若验签成功，则审核第二对象信息，若证书设备 100c 确认第二对象信息无误后，则向第二设备 100b 颁发第二业务证书，该第二业务证书包括第二公钥。同样地，收到第三证书申请请求时，先通过第三公钥对第三签名消息进行验签处理，若验签成功，则审核第二对象信息，若证书设备 100c 确认第二对象信息无误后，则向第二设备 100b 颁发应用开发者证书，该应用开发者证书包括第三公钥。

步骤 4、如图 2a 所示，第一设备 100a 将第一业务证书作为参数，向区块链网络发起第一对象注册请求；该第一对象注册请求也携带一个签名消息，其生成过程可以参见第一签名消息的生成过程，此处不再进行赘述，为了区别上述提及的签名消息，将第一对象注册请求所携带的签名消息称为第四签名消息，同理，下文提及的第二对象注册请求携带第五签名消息，第三对象注册请求携带第六签名消息。

区块链网络中的区块链节点收到第一对象注册请求时，先通过第一公钥对第四签名消息进行验签处理，若验签成功，则审核第一业务证书，若区块链节点审核通过第一业务证书，则调用智能合约中的对象合约，对象合约基于第一业务证书中的第一公钥，生成第一对象信息对应的第一地址，并将该第一地址作为第一对象标识，然后将第一对象标识、第一业务证书以及第一对象信息进行关联存储，对象合约的结构体参数以及合约方法可以参见图 2b 所示的对象合约。

同样地，区块链网络中的区块链节点收到第二对象注册请求时，先通过第二公钥对第五签名消息进行验签处理，若验签成功，则审核第二业务证书，若区块链节点审核通过第二业务证书，则调用智能合约中的对象合约，对象合约基于第二业务证书中的第二公钥，生成第二对象信息对应的第二地址，并将该第二地址作为第二对象标识，然后将第二对象标识、第二业务证书以及第二对象信息进行关联存储。同样地，区块链节点收到第三对象注册请求时，先通过第三公钥对第六签名消息进行验签处理，若验签成功，则审核应用开发者证书，若区块链节点审核通过应用开发者证书，则调用智能合约中的对象合约，对象合约基于应用开发者证书中的第三公钥，生成第二对象信息对应的第三地址，并将该第三地址作为第三对象标识，然后将第三对象标识、应用开发者证书以及第二对象信息进行关联存储。

上述步骤 1-步骤 4 过程请一并参见图 2b，图 2b 是本申请实施例提供的一种基于区块链的对象注册方法的流程示意图。如图 2b 所示，步骤 1a，第一设备生成第一非对称密钥对；步骤 1b，第二设备生成第二非对称密钥对以及第三非对称密钥对；步骤 2a，第一设备向证书设备申请证书；步骤 2b，第二设备向证书设备申请证书；步骤 3a，证书设备向第一设备颁发证书；步骤 3b，证书设备向第二设备颁发证书；步骤 4a，第一设备向区块链节点进行对象注册；步骤 4b，第二设备向区块链节点进行对象注册。上述可知，本申请实施例的参与方（包括第一对象以及第二对象）信息由 CA 认证，并将密钥与对象信息挂钩，协作过程均由私钥签名，确保每个流程均能关联到发起方，故可以防止篡改与抵赖，便于溯源，利于监管，减少作恶。

步骤 5、第一设备需要确定第一业务数据满足数据上传条件，确定过程可以概述如下：请一并参见图

2c, 图 2c 是本申请实施例提供的一种基于区块链的数据处理的场景示意图二。如图 2c 所示, 第一设备 100a 通过远程认证, 对第二设备 100b 进行对象信息、执行环境以及应用的安全性检测, 该过程的具体实现, 此处暂不展开描述, 请参见下文图 3 所对应的实施例中步骤 S101 的描述, 以及下文图 5 所对应的实施例中的描述。通过上述的安全性检测, 若第一设备 100a 确定第一业务数据满足数据上传条件, 则获取第一业务数据对应的第一位数组 20a。第一位数组 20a 可以使原始数据, 即第一业务数据, 可用不可见, 故可以提高第一业务数据的安全性。其中, 第一位数组 20a 的具体实现过程, 请参见下文图 3 所对应的实施例中步骤 S101 的描述, 此处暂不展开描述。

步骤 6、如图 2c 所示, 第一设备 100a 使用数据密钥 20b 对第一位数组 20a 进行加密处理, 得到密文位数组 20c。其中, 数据密钥 20b 是第二设备 100b 在可信执行环境 20e 中的数据交集应用中所生成的。由于数据密钥 20b 在 TEE 中生成, 其生成环境安全, 因此数据密钥 20b 不会泄露, 用它来加密第一位数组 20a 安全性高, 仅生成它的飞地(即数据交集应用)可以通过数据密钥 20b 解密密文位数组 20c, 故可以确保第一位数组 20a 的安全。

步骤 7、第一设备 100a 通过上述的第一私钥, 对密文位数组 20c 进行签名处理, 得到第七签名消息, 如图 2c 所示, 第一设备 100a 将携带第七签名消息的密文位数组 20c 传输至区块链网络。区块链网络中的区块链节点接收密文位数组 20c 后, 首先通过第一非对称密钥对中的第一公钥, 对第七签名消息进行验签处理, 若验签通过, 则区块链节点确保密文位数组 20c 完整未经篡改, 故对密文位数组 20c 进行上链处理, 即进行存储。

步骤 8、第二设备 100b 向区块链网络发送用于获取密文位数组 20c 的数据下载请求, 区块链节点获取到数据下载请求后, 根据第二对象信息(等同于本申请的主题订阅对象信息)对应的当前订阅状态, 决定返回密文位数组 20c 或拒绝处理数据下载请求, 并将此过程上链留痕, 便于追溯。若针对第二对象信息的当前订阅状态表征第二设备 100b 具有获取该密文位数组 20c 的权限, 则将密文位数组 20c 返回至第二设备 100b。由区块链网络见证第二设备 100b 获取密文位数组 100c 的过程, 确保数据可溯源, 防止第二设备 100b 不提供业务服务。

步骤 9、如图 2c 所示, 第二设备 100b 具有普通执行环境 20d 以及可信执行环境 20e, 普通执行环境 20d 可以运行第二对象对应的第二对象平台(其不同于第一设备 100a 对应的平台), 例如广告商平台; 数据交集应用运行于可信执行环境中 20e。在运行于普通执行环境 20d 的第二对象平台中, 第二设备 100b 将密文位数组 20c 以及第二业务数据作为参数, 生成交集数据查找请求; 将交集数据查找请求发送至运行于可信执行环境 20e 中的数据交集应用。

步骤 10、如图 2c 所示, 在数据交集应用中, 第二设备 100b 通过数据密钥 20b, 对密文位数组 20c 进行解密处理, 得到第一位数组 20a。进一步, 第二设备 100b 生成第二业务数据对应的第二位数组 20f, 通过第一位数组 20a 以及第二位数组 20f, 第二设备 100b 可以确定第一业务数据以及第二业务数据之间的共有的业务数据, 本申请实施例称为业务交集数据。

步骤 11、如图 2c 所示, 第二设备 100b 将在可信执行环境 20e 中所确定的业务交集数据传输至第二对象平台, 进一步, 第二设备 100b 进行与业务交集数据相关联的业务处理。

本申请实施例可应用于各种场景, 包括但不限于云技术、人工智能、智慧交通、辅助驾驶等。本申请实施例可适用于平台之间业务交集数据确定场景, 平台推荐场景, 平台测评场景等, 这里将不对具体的业务场景进行一一列举。

参见图 3, 图 3 是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图一。该基于区块链的数据处理方法可以由第一设备执行, 也可以由第二设备执行, 也可以由区块链节点执行, 还可以由第一设备、第二设备以及区块链节点中的至少两个主体交互执行, 此处不做限制。为了便于叙述以及理解, 本申请实施例以在第一设备中进行为例进行叙述, 其中, 第一设备可以为上述图 1 所对应实施例的第一设备 100a。如图 3 所示, 该基于区块链的数据处理方法至少可以包括以下步骤 S101-步骤 S103。

步骤 S101, 当第一业务数据满足数据上传条件时, 生成第一业务数据对应的第一位数组。

具体的, 生成针对第一业务数据的主题, 生成包括主题以及主题发布对象信息的主题发布请求; 通过第一设备对应的设备私钥, 对主题发布请求进行签名处理, 得到签名消息 z 。基于主题发布请求, 调用区块链节点的发布主题合约; 通过发布主题合约, 将携带签名消息 z 的主题发布请求发送至区块链节点, 以使区块链节点在通过主题发布请求的合法性验证时, 调用发布主题合约; 发布主题合约用于指示区块链节点在验证主题发布对象信息属于注册对象信息, 且确定主题具有待发布属性时, 存储主题; 存储在区块链节点的主题, 用于指示第二设备向区块链节点发送主题订阅请求; 签名消息 z 用于指示区块链节点对主题发布请求进行合法性验证; 获取区块链节点在确定主题订阅请求具有请求有效属性时, 所转发的主题订阅请求; 根据区块链节点所转发的主题订阅请求, 确定第一业务数据与数据上传条件之间的关系; 第一业务数据与数据上传条件之间的关系包括第一业务数据满足数据上传条件, 或第一业务数据不满足数据上传条件。

在一些实施例中, 根据区块链节点所转发的主题订阅请求, 确定第一业务数据与数据上传条件之间的关系的具体过程可以包括: 根据区块链节点所转发的主题订阅请求, 生成远程认证请求; 将远程认证请求发送至第二设备, 以使第二设备根据远程认证请求生成包括中间公钥 f 的中间密钥对 g ; 中间公钥 f 用于指示第二设备调用可信执行环境 a , 生成针对数据交集应用的远程认证报告; 获取第二设备返回的远程认证报告, 根据远程认证报告, 确定第一业务数据与数据上传条件之间的关系。

在一些实施例中, 根据区块链节点所转发的主题订阅请求, 生成远程认证请求的具体过程可以包括: 根据区块链节点所转发的主题订阅请求, 生成认证挑战随机数, 以及包括中间私钥 h 以及中间公钥 i 的中间密钥对 j ; 根据中间公钥 i 以及认证挑战随机数, 生成远程认证请求; 中间公钥 i 用于指示第二设备根据中间公钥 i 、认证挑战随机数以及中间密钥对 g 中的中间私钥 k , 生成通信密钥; 通信密钥用于对数据密钥进行加密处理, 得到加密数据密钥; 则还可以包括: 获取远程认证报告中的中间公钥 f , 根据中间公钥 f 、认证挑战随机数以及中间私钥 h , 生成通信密钥; 获取第二设备返回的加密数据密钥, 通过通信密钥, 对加密数据密钥进行解密处理, 得到数据密钥。

具体的, 获取映射有第一随机数的初始位数组以及随机映射函数, 将第一业务数据输入至随机映射函数; 通过随机映射函数, 生成第一业务数据对应的第二随机数; 第一随机数包括第二随机数; 在初始位数组中确定待更新位数组; 待更新位数组映射有第二随机数; 对初始位数组中的待更新位数组更新, 并将更新之后的初始位数组确定为第一位数组。

在本申请实施例中, 第一设备在发布密文位数组之前, 先发布第一业务数据对应的主题, 以使数据接收方 (包括第二设备) 订阅该主题, 故第一设备可以审核第二设备对应的主题订阅请求, 并将审核结果返回至区块链网络; 若审核结果为审核通过结果, 则确定第一业务数据满足数据上传条件。请一并参见图 4a, 图 4a 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图一。如图 4a 所示, 步骤 4a1, 第一设备生成主题; 本申请实施例不对第一设备对应的平台进行限制, 故不对第一业务数据

的类型进行限制。步骤 4a2, 第一设备生成主题发布请求; 其中, 该主题发布请求包括主题以及主题发布对象信息 (等同于上文提及的第一对象信息); 步骤 4a3, 第一设备生成签名消息 z ; 第一设备通过第一设备对应的设备私钥 (等同于上文提及的第一私钥), 对主题发布请求进行签名处理, 得到签名消息 z ; 步骤 4a4, 第一设备发送携带签名消息 z 的主题发布请求至区块链节点; 具体地, 第一设备调用区块链上的主题合约的发布主题方法 (即发布主题合约), 向区块链网络发布主题; 主题合约的结构体参数以及合约方法 (包括发布主题方法) 可以参见图 4a 所示的主题合约。步骤 4a5, 区块链节点验证主题; 具体地, 区块链节点接收到主题发布请求后, 通过第一设备对应的设备公钥 (等同于上述的第一公钥), 对签名消息 z 进行验签处理, 若验证通过, 则确保主题发布请求未被篡改, 进一步, 调用发布主题方法, 通过发布主题方法, 区块链节点可以核对发布者 (即主题发布对象信息) 属于链上注册对象信息, 等同于图 4a 中加粗表示的有效对象, 其次可以确保主题尚未被注册, 即链上是否已存在主题; 以上验证通过后执行步骤 4a6。步骤 4a6, 区块链节点存储主题。步骤 4a7, 区块链节点返回结果至第一设备; 结果可以为用于表征区块链节点存储主题的信息。本申请实施例暂不展开描述第二设备发送主题订阅请求至区块链节点的过程, 请参见下文图 7 所对应的实施例中的描述。

在确定主题订阅请求具有请求有效属性时, 区块链节点转发主题订阅请求至第一设备, 或第一设备向区块链节点查询待处理的主题订阅请求, 如图 4b 所示, 图 4b 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图二。步骤 4b1, 第一设备向区块链节点查询待处理的主题订阅请求; 步骤 4b2, 区块链节点返回最新有效的主题订阅请求至第一设备; 区块链节点可以将主题 (等同于主题名) 作为参数, 调用主题合约中的方法, 如图 4b 中加粗表示的“获取最新有效的订阅请求”, 获取待处理的主题订阅请求。

第一设备根据区块链节点所转发的主题订阅请求, 可以确定第一业务数据与数据上传条件之间的关系, 请一并参见图 4c, 图 4c 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图三。如图 4c 所示, 步骤 4c1, 第一设备生成认证挑战随机数, 以及中间密钥对 $j(h, i)$, 其中, h 表示中间密钥对 j 中的中间公钥, i 表示中间密钥对 j 中的中间私钥, 其为一对非对称密钥对。步骤 4c2, 第一设备生成远程认证请求; 具体地, 第一设备将中间公钥 h 以及认证挑战随机数作为参数, 生成远程认证请求。步骤 4c3, 第一设备发送远程认证请求。步骤 4c4, 第二设备生成中间密钥对 $g(f, k)$, 其中, f 表示中间密钥对 g 中的中间公钥, k 表示中间密钥对 g 中的中间私钥, 其也是一对非对称密钥对。步骤 4c5, 第二设备生成远程认证报告; 具体地, 第二设备将中间公钥 f 作为参数, 调用可信执行环境 a , 生成远程认证报告。步骤 4c6, 第二设备生成通信密钥; 具体地, 第二设备根据远程认证请求中的中间公钥 i 、认证挑战随机数以及中间私钥 k , 生成通信密钥, 将其保存下来, 一种可行方式为通过密钥交换算法, 生成通信密钥。其中, 中间密钥对 j 的中间私钥 h 以及中间公钥 i , 可以通过如下公式 (1) 表示。

$$i = (G^h) \bmod p \quad (1)$$

其中, 公式 (1) 中的 G 为底数, p 为素数, G 以及 P 均属于认证挑战随机数。

中间密钥对 g 的中间私钥 k 以及中间公钥 f , 可以通过如下公式 (2) 表示。

$$f = (G^k) \bmod p \quad (2)$$

第一设备以及第二设备分别生成的通信密钥, 可以通过如下公式 (3) 表示。

$$S = (i^k) \bmod p = (f^h) \bmod p \quad (3)$$

步骤 4c7, 第二设备返回远程认证报告至第一设备。步骤 4c8, 第一设备验证远程认证报告; 第一设备调用认证服务 (Provisioning Certification Service, PCS), 对远程认证报告进行验证, 若验证通过, 即第一业务数据满足数据上传条件, 则执行步骤 4c9。步骤 4c9, 第一设备生成通信密钥。具体的, 第一设备根据远程认证报告中的中间公钥 f 、认证挑战随机数以及中间私钥 h , 生成通信密钥, 可以参见上述公式 (3), 之后第一设备保存通信密钥。

在本申请实施例中, 为了保障第一位数组的安全性, 第一设备会对第一位数组进行加密, 且对第一位数组进行加密的数据密钥, 是第二设备在可信执行环境中所生成的。请一并参见图 4d, 图 4d 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图四。如图 4d 所示, 步骤 4d1, 第二设备生成数据密钥; 第二设备可以在获取到远程认证请求时, 在可信执行环境中生成数据密钥, 并将其运行以及存储于可信执行环境。步骤 4d2, 第二设备生成加密数据密钥; 具体地, 第二设备通过通信密钥, 对数据密钥进行加密处理, 得到加密数据密钥。步骤 4d3, 第二设备发送加密数据密钥至第一设备。步骤 4d4, 第一设备通过通信密钥, 解密加密数据密钥, 得到数据密钥。除了第一设备以及第二设备之外的其他设备, 无法生成通信密钥, 因为不具有中间私钥 k 或中间私钥 h 。

当第一业务数据满足数据上传条件时, 第一设备生成第一业务数据对应的第一位数组, 一种可行地生成第一位数组的方法为采用布隆过滤器 (Bloom Filter), 布隆过滤器是由一个很长的二进制向量 (可以等同于初始位数组, 原始的二进制向量的每个点均为 0), 和一系列随机映射函数构成。布隆过滤器可以用于检索一个元素 (例如本申请实施例的第二业务数据), 是否在一个集合 (例如本申请实施例中的第一业务数据) 中, 其原理是, 当一个元素被加入集合时, 通过 L 个随机映射函数 (通常 L 大于 1), 将这个元素映射成初始位数组中的 L 个点, 将 L 个点置为 1。检索时, 确认第一位数组中这 L 个点是否为 1, 如果第一位数组中这 L 个点中存在任意一个点不为 1, 可以确定该元素不属于集合, 如果第一位数组中这 L 个点均为 1, 则这个元素可能在该集合中, 在本申请实施例中, 将该元素确定为业务交集数据。

请一并参见图 4e, 图 4e 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图五。如图 4e 所示, 步骤 4e1, 第一设备获取第一业务数据。步骤 4e2, 第一设备生成第一位数组; 第一设备生成布隆过滤器, 将第一业务数据存入布隆过滤器, 此时第一位数组为存入有第一业务数据的布隆过滤器。在本申请实施例中, 第一设备不提供明文数据 (第一业务数据), 而是将第一业务数据从数据库中读取出来, 并存入布隆过滤器, 在不泄漏数据的情况下, 又能保证第二设备可以从中过滤出业务交集数据, 达到数据可用不可见的目的。

步骤 S102, 通过数据密钥, 对第一位数组进行加密处理, 得到密文位数组; 数据密钥是第二设备在数据交集应用中生成的, 数据交集应用运行于第二设备的可信执行环境 a 中。

具体的, 请再参见图 4e, 步骤 4e3, 第一设备生成加密位数组; 第一设备通过数据密钥, 对第一位数组进行加密处理, 得到加密位数组。

步骤 S103, 将密文位数组传输至区块链中的区块链节点, 以使区块链节点存储密文位数组; 存储在区块链节点的密文位数组用于由区块链节点转发至第二设备; 第二设备用于在数据交集应用中, 通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理, 得到第一位数组; 第一位数组用于指示第二设备在数据交集应用中, 生成第二业务数据对应的第二位数组; 第二位数组以及第一位数组用于指示

第二设备在数据交集应用中，确定第一业务数据以及第二业务数据之间的业务交集数据；业务交集数据用于指示第二设备进行与业务交集数据相关联的业务处理。

具体的，步骤 4e4，第一设备发送加密位数组至区块链节点。步骤 4e5，区块链节点存储加密位数组。

本申请实施例暂不对第二设备获取加密位数组的过程，以及确定业务交集数据的过程展开描述，第二设备获取加密位数组的过程，以及确定业务交集数据的过程可以参见下文图 7 所对应的实施例中的描述。

在本申请实施例中，通过生成第一业务数据对应的第一位数组，可以确保第一业务数据可用不可见，故可以提高第一业务数据的安全性；进一步地，由于数据密钥是通过可信执行环境 a 中的数据交集应用所生成的，故其生成环境安全、应用环境安全以及存储环境安全，故通过数据密钥对第一位数组进行加密处理，可以提高第一位数组的安全性；进一步地，通过将密文位数组传输至区块链，可以准确地追溯第二设备针对密文位数组的获取状态；此外，本申请实施例是通过第一位数组以及第二业务数据对应的第二位数组，确定第一业务数据以及第二业务数据之间的业务交集数据，故不仅可以进行与业务交集数据相关联的业务处理，还进一步提高了第一业务数据的安全性。上述可知，采用本申请实施例，可以提高数据（包括第一业务数据以及第一位数组）的安全性，以及准确地追溯数据获取状态。

参见图 5，图 5 是本申请实施例提供的一种数据处理方法的流程示意图二。如图 5 所示，该数据处理方法的过程包括如下步骤 S1011-步骤 S1013，且步骤 S1011-步骤 S1013 为图 3 所对应实施例中步骤 S101 的一个具体实施例。

步骤 S1011，调用认证服务，通过认证服务对远程认证报告进行验证处理，得到第一验证结果，

作为示例，远程认证发生在第一设备将密文位数组发送至区块链网络之前，主要验证第二设备的数据运行环境、应用程序安全性，以及开发者信息（即订阅方）的正确性，从而保证密文位数组提供给了正确的使用者，并且密文位数组使用过程安全。

作为示例，本申请实施例不对数据运行环境的验证、应用程序的验证，以及开发者信息的验证顺序进行限定，可以并行验证，也可以串行验证，若串行验证，可以最先进行数据运行环境的验证，也可以最后进行数据运行环境的验证。

步骤 S1012，当第一验证结果指示远程认证报告验证失败时，确定第一业务数据不满足数据上传条件。

作为示例，当第一验证结果指示远程认证报告验证失败时，确定可信执行环境 a 不具有环境安全属性；生成用于指示可信执行环境 a 不具有环境安全属性的第一更新订阅状态，将第一更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第一更新订阅状态。

第一设备调用认证服务，通过认证服务，验证远程认证报告的有效性，当验证失败时，说明第二设备的可信执行环境不可靠，需忽略订阅请求，此时，第一设备更新订阅状态为“环境不安全”，即第一更新订阅状态，并终止后续流程。

步骤 S1013，当第一验证结果指示远程认证报告验证通过时，获取数据交集应用的源码，根据源码，确定第一业务数据与数据上传条件之间的关系。

作为示例，对源码进行验证处理，得到第二验证结果；当第二验证结果指示源码验证通过时，获取远程认证报告中针对数据交集应用的主题订阅对象信息，对主题订阅对象信息进行验证处理，得到第三验证结果；获取远程认证报告中针对源码的远程度量值，对远程度量值进行验证处理，得到第四验证结果；根据第三验证结果以及第四验证结果，确定第一业务数据与数据上传条件之间的关系；当第二验证

结果指示源码验证失败时，确定第一业务数据不满足数据上传条件；还可以执行以下技术方案：当第二验证结果指示源码验证失败时，确定源码不具有代码安全属性；生成用于指示源码不具有代码安全属性的第二更新订阅状态，将第二更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第二更新订阅状态。

在一些实施例中，对主题订阅对象信息进行验证处理，得到第三验证结果的具体过程可以包括：获取针对数据交集应用的应用开发对象证书，从应用开发对象证书中获取应用开发对象信息，将主题订阅对象信息与应用开发对象信息进行对比；当主题订阅对象信息与应用开发对象信息不同时，生成用于指示主题订阅对象信息验证失败的第三验证结果；当主题订阅对象信息与应用开发对象信息相同时，生成用于指示主题订阅对象信息验证通过的第三验证结果；还可以执行以下技术方案：当第三验证结果指示主题订阅对象信息验证失败时，生成用于指示主题订阅对象信息为未授权对象信息的第三更新订阅状态；将第三更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第三更新订阅状态。

在一些实施例中，对远程度量值进行验证处理，得到第四验证结果的具体过程可以包括：在第一设备的可信执行环境 b 中对源码进行编译处理，得到可信度量值；将远程度量值与可信度量值进行对比，当远程度量值与可信度量值不同时，生成用于指示远程度量值验证失败的第四验证结果；当远程度量值与可信度量值相同时，生成用于指示远程度量值验证通过的第四验证结果；还可以执行以下技术方案：当第四验证结果指示远程度量值验证失败时，生成用于指示源码与运行代码不匹配的第四更新订阅状态；将第四更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第四更新订阅状态。

在一些实施例中，根据第三验证结果以及第四验证结果，确定第一业务数据与数据上传条件之间的关系的具体过程可以包括：当第三验证结果指示主题订阅对象信息验证通过，且第四验证结果指示远程度量值验证通过时，确定第一业务数据满足数据上传条件；还可以执行以下技术方案：当第一业务数据满足数据上传条件时，生成用于指示主题订阅请求通过验证的第五更新订阅状态；将第五更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第五更新订阅状态。

当存在未处理的远程认证报告时，第一设备会验证该远程认证报告对应的订阅者的身份，确保它为合作方，请一并参见图 6a，图 6a 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图六。如图 6a 所示，步骤 6a1，第一设备向区块链节点请求获取应用开发者证书；当第一设备还未缓存订阅方的应用开发者证书时，从链上下载订阅方的应用开发者证书，并将订阅方的应用开发者证书缓存；当本地已缓存订阅方的应用开发者证书时，跳过步骤 6a1，执行步骤 6a2。步骤 6a2，区块链节点返回应用开发者证书至第一设备；区块链节点可以根据第一设备发送的对象标识，调用对象合约中的获取对象信息方法，进而获取第一设备请求获取的应用开发者证书。步骤 6a3，第一设备对主题订阅对象信息进行验证，得到第三验证结果；具体地，第一设备将应用开发者证书中的应用开发对象信息，与远程认证报告中的主题订阅对象信息进行对比，得到第三验证结果。步骤 6a4，当验证失败时，第一设备返回第三更新订阅状态至区块链节点。当验证通过时，第一设备不执行该步骤，此时可以执行其他验证步骤，也可以返回第五更新订阅状态至区块链节点。

第二设备提供数据交集应用的源码（代码）给第一设备，由第一设备进行人工审核，当源码存在不安全因素时，例如漏洞或恶意使用数据，更新订阅状态为“程序不符预期”（第二更新订阅状态），并终止后续流程。

此外，请一并参见图 6b，图 6b 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图

七。如图 6b 所示，步骤 6b1，第一设备可信执行环境中编译源码生成可信度量值；步骤 6b2，第一设备将可信度量值以及远程度量值进行对比；当可信度量值以及远程度量值相同时，返回第五更新订阅状态，或进行后续过程。步骤 6b3，当不同，则第一设备返回第四更新订阅状态；当可信度量值以及远程度量值不一致，说明第二设备提供的审核代码与在第二设备在 TEE 环境中正在运行的代码不一致，有潜在的风险，因此更新订阅状态为“审核代码与运行代码不一致”，并终止后续流程。

上述可知，针对源码的验证包括两方面，一是对源码进行验证，二是对源码进行编译，请一并参见图 6c，图 6c 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图八。如图 6c 所示，步骤 6c1，第二设备生成数据交集应用的源码；步骤 6c2，第二设备在可信执行环境中编译源码，得到数据交集应用；步骤 6c3，第二设备在可信执行环境中运行数据交集应用；步骤 6c4，第二设备向第一设备传输源码；本申请实施例不对源码传输方式进行限定，可以第二设备与第一设备之间点对点传输，也可以第二设备将源码传输至区块链网络，然后第一设备从区块链网络中获取；此外，在第二设备对源码进行更新的场景下，第二设备会再次传输更新后的源码至第一设备。本申请实施例不对步骤 6c4 与步骤 6c2 的执行顺序进行限定，可以同时执行。步骤 6c5，第二设备审核源码；若审核没通过，则将第二更新订阅状态发送至区块链节点；若审核通过，则执行步骤 6c6，第一设备在可信执行环境中编译源码，得到数据交集应用。步骤 6c7，第一设备生成数据交集应用的可信度量值；后续过程与上文一致，故不再进行赘述。

当以上认证（即订阅方认证、数据运行环境认证以及应用安全认证）均通过时，第一设备更新主题合约中的订阅者，并更新合约订阅请求的状态为“已完成”（第五更新订阅状态）。同时，第一设备保存远程认证结果。

结合本申请实施例以及上文图 3 所对应的实施例中的步骤 S101，可知在获取到待处理的主题订阅请求后，第一设备会根据主题订阅请求，向订阅方（即第二设备）发送远程认证请求，远程认证请求不仅提示第二设备返回远程认证报告，还可以提示第二设备生成通信密钥，以及返回加密数据密钥。

本申请实施例融合区块链、可信执行环境以及布隆过滤器技术，提供加密数据求交集的软硬件结合解决方案。通过区块链提供对象信息认证，确保流程透明，过程可信；通过 TEE 远程认证，确保执行环境安全及应用程序安全；通过布隆过滤器，实现数据可用不可见功能。本方案大幅降低了程序的时间复杂度及空间复杂度，确保了数据在存储、传输、运行过程的全生命周期的安全，在不泄漏业务数据的情况下，可以快速找出多方公共样本，故可以达成联合业务处理。

请参见图 7，图 7 是本申请实施例提供的一种基于区块链的数据处理方法的流程示意图三。该基于区块链的数据处理方法可以由第一设备执行，也可以由第二设备执行，也可以由区块链节点执行，还可以由第一设备、第二设备以及区块链节点中的至少两个主体交互执行，此处不做限制。为了便于叙述以及理解，本申请实施例以在第二设备中执行为例进行叙述，第二设备可以为上述图 1 所对应实施例的第二设备 100b。如图 7 所示，该方法至少可以包括以下步骤 S201 至步骤 S204。

步骤 S201，获取由区块链中的区块链节点转发的密文位数组；密文位数组是第一设备传输至区块链节点的，且密文位数组是第一设备通过数据密钥，对第一位数组进行加密处理所得到的，数据密钥是第二设备在数据交集应用中生成的；数据交集应用运行于第二设备的可信执行环境 a 中；第一位数组是第一设备在第一业务数据满足数据上传条件时，针对第一业务数据所生成的。

在一些实施例中，根据主题订阅对象信息，生成用于订阅主题的主题订阅请求；主题是第一设备针对第一业务数据所生成的；基于主题订阅请求，调用区块链节点的订阅主题合约；通过订阅主题合约，

将主题订阅请求发送至区块链节点,以使区块链节点在通过订阅主题合约验证主题具有待订阅属性,且主题订阅对象信息属于注册对象信息时,储存主题订阅请求,且为主题订阅请求设置请求待验证状态;请求待验证状态用于指示区块链节点将主题订阅请求转发至第一设备。

在一些实施例中,根据主题订阅对象信息,生成用于获取密文位数组的数据下载请求;将数据下载请求发送至区块链节点,以使区块链节点根据数据下载请求查询主题订阅对象信息对应的当前订阅状态;获取区块链节点在确定当前订阅状态为第五更新订阅状态时,所返回的密文位数组;第五更新订阅状态用于指示第一设备对主题订阅请求通过验证;主题订阅请求是在区块链节点存储针对第一业务数据的主题时所发送的。

请一并参见图 8,图 8 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图九。如图 8 所示,步骤 81、第二设备发送主题订阅请求至区块链节点;其中,主题订阅请求包括主题订阅对象信息。步骤 82、区块链节点核对主题订阅请求;具体地,区块链节点会调用订阅主题方法(等同于订阅主题合约),通过订阅主题方法,确保主题还没有被其它方订阅(此类主题仅供一方订阅,因为主题的消息是加密的,通信密钥以及数据密钥不能在多方间共享,防止数据泄密),同时确保订阅者是链上已注册的对象。步骤 83、区块链节点保存主题订阅请求;区块链节点基于主题名,订阅者(即主题订阅对象信息),区块高度及交易索引(index)生成订阅请求标识,保存主题订阅请求,并根据上述验证情况,标记主题订阅请求的请求处理状态为"对象未注册/已被其它对象订阅/待授权"。若主题订阅请求有效,则更新主题的最新有效订阅请求的请求标识为最新订阅请求标识。步骤 84、区块链节点返回结果至第二设备;结果可以用于表征区块链网络针对主题订阅请求的处理结果。

步骤 S202,在数据交集应用中,通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理,得到第一位数组。

请一并参见图 9,图 9 是本申请实施例提供的一种基于区块链的数据处理方法的时序示意图十。如图 9 所示,步骤 91、第二设备从区块链节点下载密文位数组。步骤 92、第二设备通过数据密钥对密文位数组进行解密处理,得到第一位数组。

步骤 S203,在数据交集应用中,生成第二业务数据对应的第二位数组,根据第二位数组以及第一位数组,确定第一业务数据以及第二业务数据之间的业务交集数据。

具体的,第二业务数据包括第二业务数据 C_d , d 为正整数,且 d 小于或等于第二业务数据的总数量;第二位数组包括第二业务数据 C_d 对应的第二位数组 E_d ;当第一位数组包括第二位数组 E_d 时,确定第二业务数据 C_d 为第一业务数据以及第二业务数据之间的业务交集数据。

请再参见图 9,步骤 93、第二设备生成第二业务数据的第二位数组。具体地,第一设备生成第一位数组的过程,与第二设备生成第二位数组的过程是相同的,故此处不再赘述。步骤 94、第二设备对比第二位数组以及第一位数组,确定业务交集数据。图 9 中的步骤 92-步骤 94 均在可信执行环境中执行。本申请实施例不对第二业务数据的数量进行限制,可以为一个或多个。当存在多个第二业务数据时,第二设备是遍历每个第二业务数据,以确定一个第二业务数据对应的一个第二位数组在第一位数组中的存在性,当一个第二业务数据对应的一个第二位数组在第一位数组中存在时,确定该第二业务数据为业务交集数据。步骤 95、第二设备进行与业务交集数据相关联的业务处理。

作为示例,第一业务数据为第一设备对应的平台应用所持有的手机号,该手机号可以是平台应用的静默对象的联系方式,平台应用想对静默对象进行推广,以吸引静默对象回顾平台。故与具有强大推广

能力的推广商合作,但为了保障静默对象的手机号的安全性,第一设备不能将手机号对外,此时第一设备可以采用本申请提供的方法,即先生成手机号(即第一业务数据)对应的第一位数组,具体可以为将手机号存入布隆过滤器;然后通过第二设备在可信执行环境中所生成的数据密钥,对存入有手机号的布隆过滤器进行加密处理,得到加密布隆过滤器;然后将加密布隆过滤器传输至区块链。

区块链先对加密布隆过滤器进行相关审核,审核通过时,存储加密布隆过滤器;在获取到第二设备发送的数据下载请求时,先对第二设备相近相关审核,审核通过时,将加密布隆过滤器转发至第二设备。

在运行于可信执行环境的数据交集应用中,第二设备先通过数据密钥对加密布隆过滤器进行解密处理,得到存入有手机号的布隆过滤器(为了区分,称为第一布隆过滤器)。然后将自己持有的手机号传输至可信执行环境,将每个手机号单独存入布隆过滤器(为了区分,称为第二布隆过滤器),当第二布隆过滤器与第一布隆过滤器匹配时,确定第二布隆过滤器中的手机号属于推广商以及平台应用共同持有的手机号(业务交集数据)。后续,第二设备将第一设备提供的具有推广效果的广告,推送给业务交集数据,业务交集数据属于平台应用的静默对象的联系方式。

本申请实施例为了保护明文数据(第一业务数据),结合了隐私集合求交技术,隐私集合求交技术全称为隐私保护集合交集(Private Set Intersection, PSI),是指持有数据的两方能够计算得到双方数据集合的交集部分,而不暴露交集以外的任何数据集合信息。PSI 通常具有以下三个特点:

- (1) 半可信场景:数据双方不愿意暴露所有数据,仅希望求得数据集合交集;
- (2) 数据最小化:除了数据集合交集以外的数据不能泄露给任意一方;
- (3) 安全双方计算:参与计算的双方需要共同实现一套安全的计算协议,以保证数据的安全性。

步骤 S204,对业务交集数据进行业务处理。

具体的,获取第一设备提供的具有应用推荐功能的媒体数据,将媒体数据推送至第二业务数据 C_d 。

通过布隆过滤器存储第一业务数据,本申请实施例不仅能保护对象隐私,还能减少数据量,降低通信次数,降低系统的时间及空间复杂度。

通过在 TEE 中生成、管理数据密钥,本申请实施例能确保数据密钥在存储、传递及使用过程中的安全性,从而保证数据的安全。

通过使用区块链,本申请实施例将代码上链,提高了应用程序的可信度,当数据使用方(即第二设备)未经数据提供方(即第一设备)同意,更新代码时,数据提供方可停止提供第一业务数据,并将这个过程上链,为服务状态变更存证。此外,参与方(包括数据使用方以及数据提供方)可以为每次提供的服务/数据上链,为后继服务提供依据。另外,将对象身份信息上链,可以验证数据完整性;工作流程上链,可以确保流程透明,便于监管。

在本申请实施例中,通过生成第一业务数据对应的第一位数组,可以确保第一业务数据可用不可见,故可以提高第一业务数据的安全性;进一步地,由于数据密钥是通过可信执行环境 a 中的数据交集应用所生成的,故其生成环境安全、应用环境安全以及存储环境安全,故通过数据密钥对第一位数组进行加密处理,可以提高第一位数组的安全性;进一步地,通过将密文位数组传输至区块链,可以准确地追溯第二设备针对密文位数组的获取状态;此外,本申请实施例是通过第一位数组以及第二业务数据对应的第二位数组,确定第一业务数据以及第二业务数据之间的业务交集数据,故不仅可以进行与业务交集数据相关联的业务处理,还进一步提高了第一业务数据的安全性。上述可知,采用本申请实施例,可以提高数据(包括第一业务数据以及第一位数组)的安全性,以及准确地追溯数据获取状态。

参见图 10, 图 10 是本申请实施例提供的一种基于区块链的数据处理装置的结构示意图一。该基于区块链的数据处理装置 1 可以运行于第一设备, 上述基于区块链的数据处理装置 1 可以用于执行本申请实施例提供的方法中的相应步骤。如图 10 所示, 该基于区块链的数据处理装置 1 可以包括: 第一生成模块 11、第一处理模块 12 以及密文传输模块 13。第一生成模块 11, 配置为当第一业务数据满足数据上传条件时, 生成第一业务数据对应的第一位数组; 第一处理模块 12, 配置为通过数据密钥, 对第一位数组进行加密处理, 得到密文位数组; 其中, 数据密钥是第二设备在数据交集应用中生成的, 数据交集应用运行于第二设备的可信执行环境 a 中; 密文传输模块 13, 配置为将密文位数组传输至区块链中的区块链节点, 以使区块链节点存储密文位数组; 其中, 存储在区块链节点的密文位数组用于由区块链节点转发至第二设备; 第二设备用于在数据交集应用中, 通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理, 得到第一位数组; 第一位数组用于指示第二设备在数据交集应用中, 生成第二业务数据对应的第二位数组; 第二位数组以及第一位数组用于指示第二设备在数据交集应用中, 确定第一业务数据以及第二业务数据之间的业务交集数据; 业务交集数据用于指示第二设备进行与业务交集数据相关联的业务处理。

第一生成模块 11、第一处理模块 12 以及密文传输模块 13 的具体功能实现方式, 可以参见上述图 3 对应实施例中的步骤 S101-步骤 S103, 这里不再进行赘述。

参见图 10, 基于区块链的数据处理装置 1 还可以包括: 第二处理模块 15、请求发送模块 16、请求获取模块 17 以及关系确定模块 18。第二生成模块 14, 配置为生成针对第一业务数据的主题, 生成包括主题以及主题发布对象信息的主题发布请求; 第二处理模块 15, 配置为通过第一设备对应的设备私钥, 对主题发布请求进行签名处理, 得到签名消息 z, 基于主题发布请求, 调用区块链节点的发布主题合约; 请求发送模块 16, 配置为通过发布主题合约, 将携带签名消息 z 的主题发布请求发送至区块链节点, 以使区块链节点在通过主题发布请求的合法性验证时, 调用发布主题合约; 发布主题合约用于指示区块链节点在验证主题发布对象信息属于注册对象信息, 且确定主题具有待发布属性时, 存储主题; 存储在区块链节点的主题, 用于指示第二设备向区块链节点发送主题订阅请求; 签名消息 z 用于指示区块链节点对主题发布请求进行合法性验证; 请求获取模块 17, 配置为获取区块链节点在确定主题订阅请求具有请求有效属性时, 所转发的主题订阅请求; 关系确定模块 18, 配置为根据区块链节点所转发的主题订阅请求, 确定第一业务数据与数据上传条件之间的关系; 第一业务数据与数据上传条件之间的关系包括第一业务数据满足数据上传条件, 或第一业务数据不满足数据上传条件。

第二处理模块 15、请求发送模块 16、请求获取模块 17 以及关系确定模块 18 的具体功能实现方式, 可以参见上述图 3 对应实施例中的步骤 S101, 这里不再进行赘述。

参见图 10, 关系确定模块 18 可以包括: 第一生成单元 181、请求发送单元 182 以及第一获取单元 183。第一生成单元 181, 配置为根据区块链节点所转发的主题订阅请求, 生成远程认证请求; 请求发送单元 182, 配置为将远程认证请求发送至第二设备, 以使第二设备根据远程认证请求生成包括中间公钥 f 的中间密钥对 g; 其中, 中间公钥 f 用于指示第二设备调用可信执行环境 a, 生成针对数据交集应用的远程认证报告; 第一获取单元 183, 配置为获取第二设备返回的远程认证报告, 根据远程认证报告, 确定第一业务数据与数据上传条件之间的关系。

第一生成单元 181、请求发送单元 182 以及第一获取单元 183 的具体功能实现方式, 可以参见上述图 3 对应实施例中的步骤 S101, 这里不再进行赘述。

参见图 10, 第一获取单元 183 可以包括: 报告验证子单元 1831、第一确定子单元 1832 以及第二确定子单元 1833。报告验证子单元 1831, 配置为调用认证服务, 通过认证服务对远程认证报告进行验证处理, 得到第一验证结果; 第一确定子单元 1832, 配置为当第一验证结果指示远程认证报告验证失败时, 确定第一业务数据不满足数据上传条件; 第二确定子单元 1833, 配置为当第一验证结果指示远程认证报告验证通过时, 获取数据交集应用的源码, 根据源码, 确定第一业务数据与数据上传条件之间的关系; 第一获取单元 183 还可以包括: 第三确定子单元 1834 以及状态发送子单元 1835。第三确定子单元 1834, 配置为当第一验证结果指示远程认证报告验证失败时, 确定可信执行环境 a 不具有环境安全属性; 状态发送子单元 1835, 配置为生成用于指示可信执行环境 a 不具有环境安全属性的第一更新订阅状态, 将第一更新订阅状态发送至区块链节点, 以使区块链节点为主题订阅请求设置第一更新订阅状态。

报告验证子单元 1831、第一确定子单元 1832、第二确定子单元 1833、第三确定子单元 1834 以及状态发送子单元 1835 的具体功能实现方式, 可以参见上述图 5 对应实施例中的步骤 S1013, 这里不再进行赘述。

参见图 10, 第二确定子单元 1833 可以包括: 第一处理子单元 18331、第二处理子单元 18332、第三处理子单元 18333 以及关系确定子单元 18334。第一处理子单元 18331, 配置为对源码进行验证处理, 得到第二验证结果; 第二处理子单元 18332, 配置为当第二验证结果指示源码验证通过时, 获取远程认证报告中针对数据交集应用的主题订阅对象信息, 对主题订阅对象信息进行验证处理, 得到第三验证结果; 第三处理子单元 18333, 配置为获取远程认证报告中针对源码的远程度量值, 对远程度量值进行验证处理, 得到第四验证结果; 关系确定子单元 18334, 配置为根据第三验证结果以及第四验证结果, 确定第一业务数据与数据上传条件之间的关系; 第二处理子单元 18332, 还配置为当第二验证结果指示源码验证失败时, 确定第一业务数据不满足数据上传条件; 第二确定子单元 1833 还可以包括: 状态生成子单元 18335。第二处理子单元 18332, 还配置为当第二验证结果指示源码验证失败时, 确定源码不具有代码安全属性; 状态生成子单元 18335, 配置为生成用于指示源码不具有代码安全属性的第二更新订阅状态, 将第二更新订阅状态发送至区块链节点, 以使区块链节点为主题订阅请求设置第二更新订阅状态。

第一处理子单元 18331、第二处理子单元 18332、第三处理子单元 18333、关系确定子单元 18334 以及状态生成子单元 18335 的具体功能实现方式, 可以参见上述图 5 对应实施例中的步骤 S1013, 这里不再进行赘述。

参见图 10, 第二处理子单元 18332, 具体用于获取针对数据交集应用的应用开发对象证书, 从应用开发对象证书中获取应用开发对象信息, 将主题订阅对象信息与应用开发对象信息进行对比; 第二处理子单元 18332, 还配置为当主题订阅对象信息与应用开发对象信息不同时, 生成用于指示主题订阅对象信息验证失败的第三验证结果; 第二处理子单元 18332, 还配置为当主题订阅对象信息与应用开发对象信息相同时, 生成用于指示主题订阅对象信息验证通过的第三验证结果; 第二处理子单元 18332, 还配置为当第三验证结果指示主题订阅对象信息验证失败时, 生成用于指示主题订阅对象信息为未授权对象信息的第三更新订阅状态; 第二处理子单元 18332, 还配置为将第三更新订阅状态发送至区块链节点, 以使区块链节点为主题订阅请求设置第三更新订阅状态。

第二处理子单元 18332 的具体功能实现方式, 可以参见上述图 5 对应实施例中的步骤 S1013, 这里不再进行赘述。

参见图 10, 第三处理子单元 18333, 还配置为在第一设备的可信执行环境 b 中对源码进行编译处理,

得到可信度量值；第三处理子单元 18333，还配置为将远程度量值与可信度量值进行对比，若远程度量值与可信度量值不同，则生成用于指示远程度量值验证失败的第四验证结果；第三处理子单元 18333，还配置为当远程度量值与可信度量值相同时，生成用于指示远程度量值验证通过的第四验证结果；第三处理子单元 18333，还配置为当第四验证结果指示远程度量值验证失败时，生成用于指示源码与运行代码不匹配的第四更新订阅状态；第三处理子单元 18333，还配置为将第四更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第四更新订阅状态。

第三处理子单元 18333 的具体功能实现方式，可以参见上述图 5 对应实施例中的步骤 S1013，这里不再进行赘述。

参见图 10，关系确定子单元 18334，配置为当第三验证结果指示主题订阅对象信息验证通过，且第四验证结果指示远程度量值验证通过时，确定第一业务数据满足数据上传条件；关系确定子单元 18334，还配置为当第一业务数据满足数据上传条件时，生成用于指示主题订阅请求通过验证的第五更新订阅状态；关系确定子单元 18334，还配置为将第五更新订阅状态发送至区块链节点，以使区块链节点为主题订阅请求设置第五更新订阅状态。

关系确定子单元 18334 的具体功能实现方式，可以参见上述图 5 对应实施例中的步骤 S1013，这里不再进行赘述。

参见图 10，第一生成单元 181 可以包括：第一生成子单元 1811 以及第二生成子单元 1812。第一生成子单元 1811，配置为根据区块链节点所转发的主题订阅请求，生成认证挑战随机数，以及包括中间私钥 h 以及中间公钥 i 的中间密钥对 j；第二生成子单元 1812，配置为根据中间公钥 i 以及认证挑战随机数，生成远程认证请求；中间公钥 i 用于指示第二设备根据中间公钥 i、认证挑战随机数以及中间密钥对 g 中的中间私钥 k，生成通信密钥；通信密钥用于对数据密钥进行加密处理，得到加密数据密钥。

在一些实施例中，第一生成单元 181 可以包括：第一获取子单元 1813 以及第二获取子单元 1814。第一获取子单元 1813，配置为获取远程认证报告中的中间公钥 f，根据中间公钥 f、认证挑战随机数以及中间私钥 h，生成通信密钥；第二获取子单元 1814，配置为获取第二设备返回的加密数据密钥，通过通信密钥，对加密数据密钥进行解密处理，得到数据密钥。

第一生成子单元 1811、第二生成子单元 1812、第一获取子单元 1813 以及第二获取子单元 1814 的具体功能实现方式，可以参见上述图 3 对应实施例中的步骤 S101，这里不再进行赘述。

参见图 10，第一生成模块 11 可以包括：第二获取单元 111、第二生成单元 112、第一确定单元 113 以及第二确定单元 114。第二获取单元 111，配置为获取映射有第一随机数的初始位数组以及随机映射函数，将第一业务数据输入至随机映射函数；第二生成单元 112，配置为通过随机映射函数，生成第一业务数据对应的第二随机数，其中，第一随机数包括第二随机数；第一确定单元 113，配置为在初始位数组中确定待更新位数组，其中，待更新位数组映射有第二随机数；第二确定单元 114，配置为对初始位数组中的待更新位数组更新，并将更新之后的初始位数组确定为第一位数组。

第二获取单元 111、第二生成单元 112、第一确定单元 113 以及第二确定单元 114 的具体功能实现方式，可以参见上述图 3 对应实施例中的步骤 S101，这里不再进行赘述。

在本申请实施例中，通过生成第一业务数据对应的第一位数组，可以确保第一业务数据可用不可见，故可以提高第一业务数据的安全性；进一步地，由于数据密钥是通过可信执行环境 a 中的数据交集应用所生成的，故其生成环境安全、应用环境安全以及存储环境安全，故通过数据密钥对第一位数组进行加

密处理,可以提高第一位数组的安全性;进一步地,通过将密文位数组传输至区块链,可以准确地追溯第二设备针对密文位数组的获取状态;此外,本申请实施例是通过第一位数组以及第二业务数据对应的第二位数组,确定第一业务数据以及第二业务数据之间的业务交集数据,故不仅可以进行与业务交集数据相关联的业务处理,还进一步提高了第一业务数据的安全性。上述可知,采用本申请实施例,可以提高数据(包括第一业务数据以及第一位数组)的安全性,以及准确地追溯数据获取状态。

参见图 11,图 11 是本申请实施例提供的一种基于区块链的数据处理装置的结构示意图二。上述基于区块链的数据处理装置 2 可以运行于第二设备,该装置可以用于执行本申请实施例提供的方法中的相应步骤。如图 11 所示,该基于区块链的数据处理装置 2 可以包括:密文获取模块 21、第一处理模块 22、第一生成模块 23 以及第二处理模块 24。密文获取模块 21,配置为获取由区块链中的区块链节点转发的密文位数组;密文位数组是第一设备传输至区块链节点的,且密文位数组是第一设备通过数据密钥,对第一位数组进行加密处理所得到的,数据密钥是第二设备在数据交集应用中生成的,;数据交集应用运行于第二设备的可信执行环境 a 中;第一位数组是第一设备在第一业务数据满足数据上传条件时,针对第一业务数据所生成的;第一处理模块 22,配置为在数据交集应用中,通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理,得到第一位数组;第一生成模块 23,配置为在数据交集应用中,生成第二业务数据对应的第二位数组,根据第二位数组以及第一位数组,确定第一业务数据以及第二业务数据之间的业务交集数据;第二处理模块 24,配置为对业务交集数据进行业务处理。

密文获取模块 21、第一处理模块 22、第一生成模块 23 以及第二处理模块 24 的具体功能实现方式,可以参见上述图 7 对应实施例中的步骤 S201-步骤 S204,这里不再进行赘述。

参见图 11,密文获取模块 21 可以包括:请求生成单元 211、请求发送单元 212 以及密文获取单元 213。请求生成单元 211,配置为根据主题订阅对象信息,生成用于获取密文位数组的数据下载请求;请求发送单元 212,配置为将数据下载请求发送至区块链节点,以使区块链节点根据数据下载请求查询主题订阅对象信息对应的当前订阅状态;密文获取单元 213,配置为获取区块链节点在确定当前订阅状态为第五更新订阅状态时,所返回的密文位数组;第五更新订阅状态用于指示第一设备对主题订阅请求通过验证;主题订阅请求是在区块链节点存储针对第一业务数据的主题时所发送的。

请求生成单元 211、请求发送单元 212 以及密文获取单元 213 的具体功能实现方式,可以参见上述图 7 对应实施例中的步骤 S201,这里不再进行赘述。

参见图 11,第二业务数据包括第二业务数据 C_d , d 为正整数,且 d 小于或等于第二业务数据的总数量;第二位数组包括第二业务数据 C_d 对应的第二位数组 E_d ;第一生成模块 23,还配置为当第一位数组包括第二位数组 E_d 时,确定第二业务数据 C_d 为第一业务数据以及第二业务数据之间的业务交集数据;第二处理模块 24,还配置为获取第一设备提供的具有应用推荐功能的媒体数据,将媒体数据推送至第二业务数据 C_d 。

第一生成模块 23 以及第二处理模块 24 的具体功能实现方式,可以参见上述图 7 对应实施例中的步骤 S203-步骤 S204,这里不再进行赘述。

参见图 11,基于区块链的数据处理装置 2 还可以包括:第二生成模块 25、合约调用模块 26 以及请求发送模块 27。第二生成模块 25,配置为根据主题订阅对象信息,生成用于订阅主题的主题订阅请求;主题是第一设备针对第一业务数据所生成的;合约调用模块 26,配置为基于主题订阅请求,调用区块链节点的订阅主题合约;请求发送模块 27,配置为通过订阅主题合约,将主题订阅请求发送至区块链节点,

以使区块链节点在通过订阅主题合约验证主题具有待订阅属性，且主题订阅对象信息属于注册对象信息时，储存主题订阅请求，且为主题订阅请求设置请求待验证状态；请求待验证状态用于指示区块链节点将主题订阅请求转发至第一设备。

第二生成模块 25、合约调用模块 26 以及请求发送模块 27 的具体功能实现方式，可以参见上述图 7 对应实施例中的步骤 S201，这里不再进行赘述。

在本申请实施例中，通过生成第一业务数据对应的第一位数组，可以确保第一业务数据可用不可见，故可以提高第一业务数据的安全性；进一步地，由于数据密钥是通过可信执行环境 a 中的数据交集应用所生成的，故其生成环境安全、应用环境安全以及存储环境安全，故通过数据密钥对第一位数组进行加密处理，可以提高第一位数组的安全性；进一步地，通过将密文位数组传输至区块链，可以准确地追溯第二设备针对密文位数组的获取状态；此外，本申请实施例是通过第一位数组以及第二业务数据对应的第二位数组，确定第一业务数据以及第二业务数据之间的业务交集数据，故不仅可以进行与业务交集数据相关联的业务处理，还进一步提高了第一业务数据的安全性。上述可知，采用本申请实施例，可以提高数据（包括第一业务数据以及第一位数组）的安全性，以及准确地追溯数据获取状态。

参见图 12，图 12 是本申请实施例提供的一种电子设备的结构示意图。如图 12 所示，该电子设备 1000 可以包括：至少一个处理器 1001，例如 CPU，至少一个网络接口 1004，用户接口 1003，存储器 1005，至少一个通信总线 1002。其中，通信总线 1002 用于实现这些组件之间的连接通信。其中，在一些实施例中，用户接口 1003 可以包括显示屏（Display）、键盘（Keyboard），网络接口 1004 可选地可以包括标准的有线接口、无线接口（如 WI-FI 接口）。存储器 1005 可以是高速 RAM 存储器，也可以是非不稳定的存储器（non-volatile memory），例如至少一个磁盘存储器。存储器 1005 可选地还可以是至少一个位于远离前述处理器 1001 的存储装置。如图 12 所示，作为一种计算机存储介质的存储器 1005 可以包括操作系统、网络通信模块、用户接口模块以及设备控制应用程序。

在图 12 所示的电子设备 1000 中，网络接口 1004 可提供网络通讯功能；而用户接口 1003 主要用于为用户提供输入的接口；而处理器 1001 可以用于调用存储器 1005 中存储的设备控制应用程序，以实现以下技术方案：若第一业务数据满足数据上传条件，则生成第一业务数据对应的第一位数组；通过第二设备在数据交集应用中所生成的数据密钥，对第一位数组进行加密处理，得到密文位数组；数据交集应用运行于第二设备的可信执行环境 a 中；将密文位数组传输至区块链中的区块链节点，以使区块链节点存储密文位数组；存储在区块链节点的密文位数组用于由区块链节点转发至第二设备；第二设备用于在数据交集应用中，通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理，得到第一位数组；第一位数组用于指示第二设备在数据交集应用中，生成第二业务数据对应的第二位数组；第二位数组以及第一位数组用于指示第二设备在数据交集应用中，确定第一业务数据以及第二业务数据之间的业务交集数据；业务交集数据用于指示第二设备进行与业务交集数据相关联的业务处理。

在一些实施例中，处理器 1001 可以用于调用存储器 1005 中存储的设备控制应用程序，以实现以下技术方案：获取由区块链中的区块链节点转发的密文位数组；密文位数组是第一设备传输至区块链节点的，且密文位数组是第一设备通过第二设备在数据交集应用中所生成的数据密钥，对第一位数组进行加密处理所得到的；数据交集应用运行于第二设备的可信执行环境 a 中；第一位数组是第一设备在第一业务数据满足数据上传条件时，针对第一业务数据所生成的；在数据交集应用中，通过数据密钥对从区块链节点中所获取的密文位数组进行解密处理，得到第一位数组；在数据交集应用中，生成第二业务数据

对应的第二位数组，根据第二位数组以及第一位数组，确定第一业务数据以及第二业务数据之间的业务交集数据；对业务交集数据进行业务处理。

应当理解，本申请实施例中所描述的电子设备 1000 可执行前文各实施例中对基于区块链的数据处理方法或装置的描述，在此不再赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。

本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，该计算机程序被处理器执行时实现前文各实施例中对基于区块链的数据处理方法或装置的描述，在此不再赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。

上述计算机可读存储介质可以是前述任一实施例提供的基于区块链的数据处理装置或者上述电子设备的内部存储单元，例如电子设备的硬盘或内存。该计算机可读存储介质也可以是该电子设备的外部存储设备，例如该电子设备上配备的插接式硬盘，智能存储卡（smart media card, SMC），安全数字（secure digital, SD）卡，闪存卡（flash card）等。进一步地，该计算机可读存储介质还可以既包括该电子设备的内部存储单元也包括外部存储设备。该计算机可读存储介质用于存储该计算机程序以及该电子设备所需的其他程序和数据。该计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

本申请实施例还提供了一种计算机程序产品，该计算机程序产品包括计算机程序，该计算机程序存储在计算机可读存储介质中。电子设备的处理器从计算机可读存储介质读取该计算机程序，处理器执行该计算机程序，使得该电子设备可执行前文各实施例中对基于区块链的数据处理方法或装置的描述，在此不再赘述。另外，对采用相同方法的有益效果描述，也不再进行赘述。

本申请实施例的说明书和权利要求书及附图中的术语“第一”、“第二”等是用于区别不同对象，而非用于描述特定顺序。此外，术语“包括”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、装置、产品或设备没有限定于已列出的步骤或模块，而是可选地还包括没有列出的步骤或模块，或可选地还包括对于这些过程、方法、装置、产品或设备固有的其他步骤单元。

本领域普通技术人员可以意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

以上所揭露的仅为本申请较佳实施例而已，当然不能以此来限定本申请之权利范围，因此依本申请权利要求所作的等同变化，仍属本申请所涵盖的范围。

权利要求书

1、一种基于区块链的数据处理方法，所述方法由第一设备执行，所述方法包括：

当第一业务数据满足数据上传条件时，生成所述第一业务数据对应的第一位数组；

通过数据密钥，对所述第一位数组进行加密处理，得到密文位数组；其中，所述数据密钥是第二设备在数据交集应用中生成的，所述数据交集应用运行于所述第二设备的可信执行环境a中；

将所述密文位数组传输至所述区块链中的区块链节点，以使所述区块链节点存储所述密文位数组；

其中，存储在所述区块链节点的所述密文位数组用于由所述区块链节点转发至所述第二设备；所述第二设备用于在所述数据交集应用中，通过所述数据密钥对从所述区块链节点中所获取的所述密文位数组进行解密处理，得到所述第一位数组；所述第一位数组用于指示所述第二设备在所述数据交集应用中，生成第二业务数据对应的第二位数组；所述第二位数组以及所述第一位数组用于指示所述第二设备在所述数据交集应用中，确定所述第一业务数据以及所述第二业务数据之间的业务交集数据；所述业务交集数据用于指示所述第二设备进行与所述业务交集数据相关联的业务处理。

2、根据权利要求1所述的方法，其中，所述方法还包括：

生成针对所述第一业务数据的主题；

生成包括所述主题以及主题发布对象信息的主题发布请求；

通过所述第一设备对应的设备私钥，对所述主题发布请求进行签名处理，得到签名消息z；

基于所述主题发布请求，调用所述区块链节点的发布主题合约，并通过所述发布主题合约，将携带所述签名消息z的所述主题发布请求发送至所述区块链节点，以使所述区块链节点在通过所述主题发布请求的合法性验证时，调用所述发布主题合约；

其中，所述发布主题合约用于指示所述区块链节点在验证所述主题发布对象信息属于注册对象信息，且确定所述主题具有待发布属性时，存储所述主题；存储在所述区块链节点的所述主题，用于指示所述第二设备向所述区块链节点发送主题订阅请求；所述签名消息z用于指示所述区块链节点对所述主题发布请求进行合法性验证；

获取所述区块链节点在确定所述主题订阅请求具有请求有效属性时，所转发的所述主题订阅请求；

根据所述区块链节点所转发的所述主题订阅请求，确定所述第一业务数据与所述数据上传条件之间的关系；

其中，所述第一业务数据与所述数据上传条件之间的关系包括所述第一业务数据满足所述数据上传条件，或所述第一业务数据不满足所述数据上传条件。

3、根据权利要求2所述的方法，其中，所述根据所述区块链节点所转发的所述主题订阅请求，确定所述第一业务数据与所述数据上传条件之间的关系，包括：

根据所述区块链节点所转发的所述主题订阅请求，生成远程认证请求；

将所述远程认证请求发送至所述第二设备，以使所述第二设备根据所述远程认证请求生成中间密钥对g；所述中间密钥对g中的中间公钥f用于指示所述第二设备调用所述可信执行环境a，生成针对所述数据交集应用的远程认证报告；

获取所述第二设备返回的所述远程认证报告，根据所述远程认证报告，确定所述第一业务数据与所

述数据上传条件之间的关系。

4、根据权利要求3所述的方法，其中，所述根据所述区块链节点所转发的所述主题订阅请求，生成远程认证请求，包括：

根据所述区块链节点所转发的所述主题订阅请求，生成认证挑战随机数，以及包括中间私钥 h 以及中间公钥 i 的中间密钥对 j；

根据所述中间公钥 i 以及所述认证挑战随机数，生成远程认证请求；

其中，所述中间公钥 i 用于指示所述第二设备根据所述中间公钥 i、所述认证挑战随机数以及所述中间密钥对 g 中的中间私钥 k，生成通信密钥；所述通信密钥用于对所述数据密钥进行加密处理，得到加密数据密钥；

所述方法还包括：

获取所述远程认证报告中的所述中间公钥 f，根据所述中间公钥 f、所述认证挑战随机数以及所述中间私钥 h，生成所述通信密钥；

获取所述第二设备返回的加密数据密钥，通过所述通信密钥，对所述加密数据密钥进行解密处理，得到所述数据密钥。

5、根据权利要求3所述的方法，其中，所述根据所述远程认证报告，确定所述第一业务数据与所述数据上传条件之间的关系，包括：

调用认证服务，通过所述认证服务对所述远程认证报告进行验证处理，得到第一验证结果；

当所述第一验证结果指示所述远程认证报告验证失败时，确定所述第一业务数据不满足所述数据上传条件；

当所述第一验证结果指示所述远程认证报告验证通过时，获取所述数据交集应用的源码，根据所述源码，确定所述第一业务数据与所述数据上传条件之间的关系；

所述方法还包括：

当所述第一验证结果指示所述远程认证报告验证失败时，确定所述可信执行环境 a 不具有环境安全属性；

生成用于指示所述可信执行环境 a 不具有所述环境安全属性的第一更新订阅状态，将所述第一更新订阅状态发送至所述区块链节点，以使所述区块链节点为所述主题订阅请求设置所述第一更新订阅状态。

6、根据权利要求5所述的方法，其中，所述根据所述源码，确定所述第一业务数据与所述数据上传条件之间的关系，包括：

对所述源码进行验证处理，得到第二验证结果；

当所述第二验证结果指示所述源码验证通过时，获取所述远程认证报告中针对所述数据交集应用的主题订阅对象信息，对所述主题订阅对象信息进行验证处理，得到第三验证结果；

获取所述远程认证报告中针对所述源码的远程度量值，对所述远程度量值进行验证处理，得到第四验证结果；

根据所述第三验证结果以及所述第四验证结果，确定所述第一业务数据与所述数据上传条件之间的

关系;

当所述第二验证结果指示所述源码验证失败时,确定所述第一业务数据不满足所述数据上传条件;

所述方法还包括:

当所述第二验证结果指示所述源码验证失败时,确定所述源码不具有代码安全属性;

生成用于指示所述源码不具有所述代码安全属性的第二更新订阅状态,将所述第二更新订阅状态发送至所述区块链节点,以使所述区块链节点为所述主题订阅请求设置所述第二更新订阅状态。

7、根据权利要求 6 所述的方法,其中,所述对所述主题订阅对象信息进行验证处理,得到第三验证结果,包括:

获取针对所述数据交集应用的应用开发对象证书,从所述应用开发对象证书中获取应用开发对象信息;

当所述主题订阅对象信息与所述应用开发对象信息不同时,生成用于指示所述主题订阅对象信息验证失败的第三验证结果;

当所述主题订阅对象信息与所述应用开发对象信息相同时,生成用于指示所述主题订阅对象信息验证通过的第三验证结果;

所述方法还包括:

当所述第三验证结果指示所述主题订阅对象信息验证失败时,生成用于指示所述主题订阅对象信息为未授权对象信息的第三更新订阅状态;

将所述第三更新订阅状态发送至所述区块链节点,以使所述区块链节点为所述主题订阅请求设置所述第三更新订阅状态。

8、根据权利要求 6 所述的方法,其中,所述对所述远程度量值进行验证处理,得到第四验证结果,包括:

在所述第一设备的可信执行环境 b 中对所述源码进行编译处理,得到可信度量值;

当所述远程度量值与所述可信度量值不同时,生成用于指示所述远程度量值验证失败的第四验证结果;

当所述远程度量值与所述可信度量值相同时,生成用于指示所述远程度量值验证通过的第四验证结果;

所述方法还包括:

当所述第四验证结果指示所述远程度量值验证失败时,生成用于指示所述源码与运行代码不匹配的第四更新订阅状态;

将所述第四更新订阅状态发送至所述区块链节点,以使所述区块链节点为所述主题订阅请求设置所述第四更新订阅状态。

9、根据权利要求 6 所述的方法,其中,所述根据所述第三验证结果以及所述第四验证结果,确定所述第一业务数据与所述数据上传条件之间的关系,包括:

当所述第三验证结果指示所述主题订阅对象信息验证通过,且所述第四验证结果指示所述远程度量

值验证通过时，确定所述第一业务数据满足所述数据上传条件；

所述方法还包括：

当所述第一业务数据满足所述数据上传条件时，生成用于指示所述主题订阅请求通过验证的第五更新订阅状态；

将所述第五更新订阅状态发送至所述区块链节点，以使所述区块链节点为所述主题订阅请求设置所述第五更新订阅状态。

10、根据权利要求 1 至 9 中任一项所述的方法，其中，所述生成所述第一业务数据对应的第一位数组，包括：

获取映射有第一随机数的初始位数组以及随机映射函数，将所述第一业务数据输入至所述随机映射函数；

通过所述随机映射函数，生成所述第一业务数据对应的第二随机数，其中，所述第一随机数包括所述第二随机数；

在所述初始位数组中确定待更新位数组，其中，所述待更新位数组映射有所所述第二随机数；

对所述初始位数组中的所述待更新位数组更新，并将更新之后的初始位数组确定为第一位数组。

11、一种基于区块链的数据处理方法，所述方法由第二设备执行，所述方法包括：

获取由所述区块链中的区块链节点转发的密文位数组；

其中，所述密文位数组是第一设备传输至所述区块链节点的，且所述密文位数组是所述第一设备通过数据密钥，对第一位数组进行加密处理所得到的，所述数据密钥是所述第二设备在数据交集应用中生成的；所述数据交集应用运行于所述第二设备的可信执行环境 a 中；所述第一位数组是所述第一设备在第一业务数据满足数据上传条件时，针对所述第一业务数据所生成的；

在所述数据交集应用中，通过所述数据密钥对从所述区块链节点中所获取的所述密文位数组进行解密处理，得到所述第一位数组；

在所述数据交集应用中，生成第二业务数据对应的第二位数组，根据所述第二位数组以及所述第一位数组，确定所述第一业务数据以及所述第二业务数据之间的业务交集数据；

对所述业务交集数据进行业务处理。

12、根据权利要求 11 所述的方法，其中，所述获取由所述区块链节点转发的密文位数组，包括：

根据主题订阅对象信息，生成用于获取所述密文位数组的数据下载请求；

将所述数据下载请求发送至所述区块链节点，以使所述区块链节点根据所述数据下载请求查询所述主题订阅对象信息对应的当前订阅状态；

获取所述区块链节点在确定所述当前订阅状态为第五更新订阅状态时，所返回的密文位数组；

其中，所述第五更新订阅状态用于指示所述第一设备对主题订阅请求通过验证；所述主题订阅请求是在所述区块链节点存储针对所述第一业务数据的主题时所发送的。

13、根据权利要求 11 所述的方法，其中，所述第二业务数据包括第二业务数据 C_d ，d 为正整数，且

d 小于或等于所述第二业务数据的总数量；所述第二位数组包括所述第二业务数据 C_d 对应的第二位数组 E_d ；

所述根据所述第二位数组以及所述第一位数组，确定所述第一业务数据以及所述第二业务数据之间的业务交集数据，包括：

当所述第一位数组包括所述第二位数组 E_d 时，确定所述第二业务数据 C_d 为所述第一业务数据以及所述第二业务数据之间的业务交集数据；

所述对所述业务交集数据进行业务处理，包括：

获取所述第一设备提供的具有应用推荐功能的媒体数据，将所述媒体数据推送至所述第二业务数据 C_d 表征的对象。

14、根据权利要求 11 所述的方法，其中，所述方法还包括：

根据主题订阅对象信息，生成用于订阅主题的主题订阅请求；所述主题是所述第一设备针对所述第一业务数据所生成的；

基于所述主题订阅请求，调用所述区块链节点的订阅主题合约；

通过所述订阅主题合约，将所述主题订阅请求发送至所述区块链节点，以使所述区块链节点在通过所述订阅主题合约验证所述主题具有待订阅属性，且所述主题订阅对象信息属于注册对象信息时，储存所述主题订阅请求，且为所述主题订阅请求设置请求待验证状态；所述请求待验证状态用于指示所述区块链节点将所述主题订阅请求转发至所述第一设备。

15、一种基于区块链的数据处理装置，所述装置运行于第一设备，所述装置包括：

第一生成模块，配置为当第一业务数据满足数据上传条件时，生成所述第一业务数据对应的第一位数组；

第一处理模块，配置为通过数据密钥，对所述第一位数组进行加密处理，得到密文位数组；其中，所述数据密钥是第二设备在数据交集应用中生成的，所述数据交集应用运行于所述第二设备的可信执行环境 a 中；

密文传输模块，配置为将所述密文位数组传输至所述区块链中的区块链节点，以使所述区块链节点存储所述密文位数组；其中，存储在所述区块链节点的所述密文位数组用于由所述区块链节点转发至所述第二设备；所述第二设备用于在所述数据交集应用中，通过所述数据密钥对从所述区块链节点中所获取的所述密文位数组进行解密处理，得到所述第一位数组；所述第一位数组用于指示所述第二设备在所述数据交集应用中，生成第二业务数据对应的第二位数组；所述第二位数组以及所述第一位数组用于指示所述第二设备在所述数据交集应用中，确定所述第一业务数据以及所述第二业务数据之间的业务交集数据；所述业务交集数据用于指示所述第二设备进行与所述业务交集数据相关联的业务处理。

16、一种基于区块链的数据处理装置，所述装置运行于第二设备，所述装置包括：

密文获取模块，配置为获取由所述区块链中的区块链节点转发的密文位数组；其中，所述密文位数组是第一设备传输至所述区块链节点的，且所述密文位数组是所述第一设备通过数据密钥，对第一位数组进行加密处理所得到的，所述数据密钥是所述第二设备在数据交集应用中生成的；所述数据交集应用

运行于所述第二设备的可信执行环境 a 中；所述第一位数组是所述第一设备在第一业务数据满足数据上传条件时，针对所述第一业务数据所生成的；

第一处理模块，配置为在所述数据交集应用中，通过所述数据密钥对从所述区块链节点中所获取的所述密文位数组进行解密处理，得到所述第一位数组；

第一生成模块，配置为在所述数据交集应用中，生成第二业务数据对应的第二位数组，根据所述第二位数组以及所述第一位数组，确定所述第一业务数据以及所述第二业务数据之间的业务交集数据；

第二处理模块，配置为对所述业务交集数据进行业务处理。

17、一种电子设备，包括：处理器、存储器以及网络接口；

所述处理器与所述存储器、所述网络接口相连，其中，所述网络接口用于提供数据通信功能，所述存储器用于存储计算机程序，所述处理器用于调用所述计算机程序，以使得所述电子设备执行权利要求 1 至 10 或权利要求 11 至 14 任一项所述的基于区块链的数据处理方法。

18、一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机程序，所述计算机程序适于由处理器加载并执行，以使得具有所述处理器的电子设备执行权利要求 1 至 10 或权利要求 11 至 14 任一项所述的基于区块链的数据处理方法。

19、一种计算机程序产品，所述计算机程序产品包括计算机程序，所述计算机程序存储在计算机可读存储介质中，所述计算机程序适于由处理器读取并执行，以使得具有所述处理器的电子设备执行权利要求 1 至 10 或权利要求 11 至 14 任一项所述的基于区块链的数据处理方法。