

数据获取方法、装置、设备及存储介质

相关申请的引用

本公开要求于 2021 年 1 月 13 日向中华人民共和国国家知识产权局提交的申请号为 202110041858.2, 发明名称为“数据获取方法、装置、
5 设备及存储介质”的发明专利申请的全部权益, 并通过引用的方式将其全部内容并入本公开。

领域

本公开大体上涉及区块链技术领域, 更具体地涉及数据获取方法、
10 装置、设备及存储介质。

背景

在数字经济时代, 数据安全和隐私保护的重要性日益凸显, 因此, 诞生了很多的数据安全保护的方案。现有技术通过搭建大数据中心平台, 将需要共享的数据通过大数据中心平台进行授权访问的权限设置, 以实现数据授权访问。
15

可见, 现有的技术方案是中心化的, 数据的导入和导出, 都通过大数据中心平台来进行管理。

20 概述

第一方面, 本公开涉及数据获取方法, 应用于联盟链, 其包括:
获取第一终端发送的数据调用请求, 其中, 所述数据调用请求中携带数据授权用户的第一分布式身份标识, 以及数据调用用户的标识;
根据所述数据调用请求, 对所述第一终端对应的所述数据调用用户进行身份认证;
25

在所述数据调用用户认证合法时, 向所述数据调用用户分配第二分布式身份标识;

根据所述第二分布式身份标识, 利用所述第一分布式身份标识, 查询所述数据授权用户的数据授权凭证;

30 根据所述数据授权凭证, 向所述数据授权用户对应的第二终端发送数据授权请求; 以及

在确定所述数据授权用户确定授权后, 加密所述数据调用请求对应的请求结果, 并将加密后的所述请求结果发送至所述第一终端。

在某些实施方案中，根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证之前，还包括：

5 获取所述第二终端发送的数据存证请求，其中，所述数据存证请求中携带所述数据授权用户的标识；

根据所述数据存证请求，对所述数据授权用户进行身份认证；

在所述数据授权用户认证合法时，向所述数据授权用户分配所述第一分布式身份标识；以及

10 根据所述第一分布式身份标识，向所述数据授权用户分发所述数据授权凭证。

在某些实施方案中，所述数据调用请求包括：所述数据调用用户的身份类型；

根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证，包括：

15 当所述数据调用用户的所述身份类型为个人时，利用人脸识别技术对所述数据调用用户进行身份认证；以及

当所述数据调用用户的所述身份类型为企业时，利用企业认证技术对所述数据调用用户进行身份认证。

20 在某些实施方案中，所述数据存证请求中包括：所述数据授权用户的身份类型；

根据所述数据存证请求，对所述数据授权用户进行身份认证，包括：

当所述数据授权用户的所述身份类型为所述个人时，利用所述人脸识别技术对所述数据授权用户进行身份认证；以及

25 当所述数据授权用户的所述身份类型为所述企业时，利用所述企业认证技术对所述数据授权用户进行身份认证。

在某些实施方案中，根据所述数据授权凭证，向所述数据授权用户对应的第二终端发送数据授权请求，包括：

30 根据所述数据授权凭证，发起所述数据授权请求，并利用预先存储的私钥对所述数据授权请求进行数字签名，生成授权请求验证信息，向所述数据授权用户对应的第二终端发送所述授权请求验证信息。

在某些实施方案中，向所述数据授权用户对应的第二终端发送所述授权请求验证信息之后，还包括：

获取所述第二终端返回的正在运行验证操作的指示信息；

35 验证所述数据授权用户的所述第一分布式身份标识，以及所述数据授权凭证；以及

在验证合法时，向所述第二终端发送执行数据授权操作的指示信息。

在某些实施方案中，所述授权请求验证信息包括二维码、条形码以及验证码中的任意一项；

- 5 生成授权请求验证信息，向所述数据授权用户对应的第二终端发送所述授权请求验证信息，包括：

 生成所述二维码，向所述数据授权用户对应的第二终端发送所述二维码；

- 10 或，生成所述条形码，向所述数据授权用户对应的第二终端发送所述条形码；

 或，生成所述验证码，向所述数据授权用户对应的第二终端发送所述验证码。

在某些实施方案中，所述数据调用请求还包括：数据授权凭证类型；

- 15 根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的所述数据授权凭证，包括：

 根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询与所述数据调用请求中的所述数据授权凭证类型，对应的所述数据授权凭证。

- 20 在某些实施方案中，应用于联盟链的数据获取方法还包括：

 利用哈希算法分别计算所述身份认证对应的身份认证记录、所述数据授权凭证、所述数据授权请求、以及与所述数据授权请求对应的数据授权记录的哈希值，并将所述哈希值存储在所述联盟链中。

 第二方面，本公开涉及数据获取方法，应用于第二终端，其包括：

- 25 接收联盟链发送的数据授权请求；

- 30 其中，所述数据授权请求为：联盟链在获取第一终端发送的数据调用请求；根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证后发送，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；以及

 根据所述数据授权请求进行授权操作。

在某些实施方案中，接收联盟链发送的数据授权请求，包括：

- 35 接收所述联盟链发送的授权请求验证信息；

 根据所述数据授权请求进行授权操作，包括：

验证所述授权请求验证信息，并将正在运行验证操作的指示信息返回给所述联盟链；

接收所述联盟链发送的执行数据授权操作的指示信息；以及

5 根据所述执行数据授权操作的指示信息，执行授权操作，并利用预先存储的私钥对所述授权操作进行数据签名。

在某些实施方案中，所述授权请求验证信息包括二维码、条形码以及验证码中的任意一项；

验证所述授权请求验证信息，并将正在运行验证操作的指示信息返回给所述联盟链，包括：

10 调用扫码功能，扫描所述二维码，并将正在运行验证操作的指示信息返回给所述联盟链；

或，调用扫码功能，扫描所述条形码，并将正在运行验证操作的指示信息返回给所述联盟链；

15 或，调用验证功能，验证所述验证码，并将正在运行验证操作的指示信息返回给所述联盟链。

第三方面，本公开涉及数据获取装置，其包括：

获取模块，配置为第一终端发送的数据调用请求，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；

20 认证模块，配置为根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；

分配模块，配置为在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；

25 查询模块，配置为根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证；

第一发送模块，配置为根据所述数据授权凭证，向所述数据授权用户对应的第二终端发送数据授权请求；以及

30 第二发送模块，配置为在确定所述数据授权用户确定授权后，加密所述数据调用请求对应的请求结果，并将加密后的所述请求结果发送至所述第一终端。

第四方面，本公开涉及数据获取装置，其包括：

接收模块，配置为接收联盟链发送的数据授权请求；

35 其中，所述数据授权请求为：联盟链在获取第一终端发送的数据调用请求；根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；根据所述第二分布式身份标识，

利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证后发送，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；以及

授权模块，配置为根据所述数据授权请求进行授权操作。

5 第五方面，本公开涉及电子设备，其包括：处理器、通信组件、存储器和通信总线，其中，所述处理器、所述通信组件和所述存储器通过所述通信总线完成相互间的通信；所述存储器，配置为存储计算机程序；所述处理器，配置为执行所述存储器中所存储的程序，实现第一方面所述的应用于联盟链的数据获取方法，或，实现第一方面所述的应用于第二终端的数据获取方法。

10 第六方面，本公开涉及计算机可读存储介质，其存储有计算机程序，所述计算机程序被处理器执行时实现本公开的应用于联盟链的数据获取方法，或，实现本公开的应用于第二终端的数据获取方法。

在某些实施方案中，本公开提供的方法，应用于联盟链，利用联盟链的分布式特征，避免了所有数据都存储在一个中心平台；本公开获取第一终端发送的数据调用请求，根据数据调用请求，对第一终端对应的数据调用用户进行身份认证，有效的解决了非法用户入侵的问题，在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识，使得该数据调用用户在联盟链中以第二分布式身份标识作为唯一标识；根据第二分布式身份标识，利用数据调用请求携带的第一分布式身份标识，查询数据授权用户的数据授权凭证，根据该数据授权凭证，向数据授权用户对应的第二终端发送数据授权请求，在确定数据授权用户确定授权后，加密数据调用请求对应的请求结果，并将加密后的请求结果发送至第一终端，有效的提高了数据的安全性。

25

附图简要说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。

30 为了更清楚地说明本公开的技术方案，下面将对本公开中所需要使用的附图作简单地介绍，显而易见地，对于本领域普通技术人员而言，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

图 1 为本公开一实施例中的应用于联盟链的数据获取方法的流程示意图；

35 图 2 为本公开一实施例中的获取数据授权凭证的流程示意图；

图 3 为本公开一实施例中的应用于第二终端的数据获取方法的流程图示意图；

图 4 为本公开一实施例中的第一数据获取装置的结构示意图；

图 5 为本公开一实施例中的第二数据获取装置的结构示意图；以及

图 6 为本公开一实施例中的电子设备的结构示意图。

详述

为使本公开实施例的目的、技术方案和优点更加清楚，下面将结合本公开实施例中的附图，对本公开实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本公开的一部分实施例，而不是全部的实施例。基于本公开中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本公开保护的范围。

本公开涉及数据获取方法，该方法应用在联盟链，该方法的实现如图 1 所示：

步骤 101，获取第一终端发送的数据调用请求；

步骤 102，根据数据调用请求，对第一终端对应的数据调用用户进行身份认证；

步骤 103，在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识；

步骤 104，根据第二分布式身份标识，利用第一分布式身份标识，查询数据授权用户的数据授权凭证；

步骤 105，根据数据授权凭证，向数据授权用户对应的第二终端发送数据授权请求；以及

步骤 106，在确定数据授权用户确定授权后，加密数据调用请求对应的请求结果，并将加密后的请求结果发送至第一终端。

在某些实施方案中，数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识。

在某些实施方案中，联盟链只针对某个特定群体的成员和有限的第三方，其内部指定多个预选节点为记账人，每个块的生成由所有的预选节点共同决定。

利用区块链技术，建立联盟链。为了能够将授权相关数据和身份相关数据分开存储，进一步的保证数据的安全性，可以采用建立数据授权验证联盟链，和分布式身份联盟链的方式建立联盟链，其中，数

据授权验证联盟链用于存证服务，分布式身份联盟链用于身份验证服务。当然，也可以建立数据授权验证及分布式身份联盟链，该数据授权验证及分布式身份联盟链既用于存证服务，又用于身份验证服务。

5 下面，以建立数据授权验证联盟链，和分布式身份联盟链为例进行说明，当然，此处仅是举例说明，并不用于对本公开的保护范围进行限制。并且，本公开中的一些其他举例说明，也不用于对本公开的保护范围的限制，便不在一一说明。

在某些实施方案中，数据授权验证联盟链的参与方包括：法院、公证处、第三方鉴定机构、监管部门、教育部、数据保管机构以及参与联盟链节点维护运营的其他企事业单位。其中，数据授权验证联盟链旨在提供一种去中心化的区块链哈希散列证据存证服务，确保数据授权访问的整个生命周期的授权访问记录，对应的哈希散列信息能够实现链上存储和链上验证。

15 分布式身份联盟链参与方包括：证书颁发机构(Certificate Authority, 简称 CA)、法院、公证处、第三方鉴定机构、监管部门、教育部以及参与联盟链节点维护运营的其他企事业单位。其中，分布式身份联盟链旨在提供一种去中心化的移动式身份验证服务。

在某些实施方案中，小程序是一种不需要下载安装即可使用的应用，用户扫一扫或者搜一下即可打开应用。用户不用关心是否安装太多应用的问题，该应用随时可用，但又无需安装卸载。可见，采用小程序的方式即方便快捷，又能够为用户节省终端的内存空间。

在某些实施方案中，分布式身份联盟链接收第一终端上运行的小程序发送的数据调用请求。数据调用用户根据数据调用用户的标识，登录第一终端上的小程序，查找数据授权用户的第一分布式身份标识，并发起数据调用请求。当分布式身份联盟链认证数据调用用户合法时，为数据调用请求分配链上的第二分布式身份标识，作为数据调用用户在链上的唯一标识。

在某些实施方案中，本公开的小程序为基于分布式身份的移动端的小程序。采用移动端的小程序，能够在移动互联网下随时发起申请，使得用户不受地域或时间的限制。

在某些实施方案中，数据调用请求包括：数据调用用户的身份类型。

在某些实施方案中，分布式身份联盟链接收第一终端上运行的小程序发送的数据调用请求，获取数据调用请求中的数据调用用户的身份类型，当数据调用用户的身份类型为个人时，利用人脸识别技术对数据调用用户进行身份认证；当数据调用用户的身份类型为企业时，

利用企业认证技术对数据调用用户进行身份认证。

在某些实施方案中，当数据调用用户的身份类型为个人时，分布式身份联盟链对输入的人脸图像，判断其是否存在人脸，如果存在人脸，则进一步的给出每个脸的位置、大小和各个主要面部器官的位置信息。并依据这些信息，进一步提取每个人脸中所蕴涵的身份特征，
5 并将提取的身份特征和预保存的人脸特征进行对比，得到第一匹配度，当第一匹配度大于第一预设值时，确定该数据调用用户认证成功，否则，确定该数据调用用户认证失败。

在某些实施方案中，当数据调用用户的身份类型为企业时，分布式身份联盟链对输入的企业信息和预保存的企业信息进行对比，得到
10 第二匹配度，当第二匹配度大于第二预设值时，确定该数据调用用户认证成功，否则，确定该数据调用用户认证失败。

在某些实施方案中，在数据调用用户进行身份认证时，通过 CA 机构提供的秘钥托管服务对数据调用用户在数据调用时进行签名的私钥进行安全存储。
15

在某些实施方案中，分布式身份联盟链在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识，该数据调用用户在分布式身份联盟链和数据授权验证联盟链中，以第二分布式身份标识作为唯一标识。

在某些实施方案中，数据授权用户通过基于分布式身份的移动端的小程序，申请第一分布式身份标识，并根据第一分布式身份标识获得数据授权凭证，如图 2 所示：
20

步骤 201，获取第二终端发送的数据存证请求，

其中，数据存证请求中携带所述数据授权用户的标识；

25 步骤 202，根据数据存证请求，对数据授权用户进行身份认证；

步骤 203，在数据授权用户认证合法时，向数据授权用户分配第一分布式身份标识；以及

步骤 204，根据第一分布式身份标识，向数据授权用户分发数据授权凭证。

在某些实施方案中，分布式身份联盟链获取第二终端上运行的小程序发送的数据存证请求。
30

在某些实施方案中，数据存证请求中包括：数据授权用户的身份类型。

在某些实施方案中，分布式身份联盟链获取数据存证请求中数据授权用户的身份类型，当数据授权用户的身份类型为个人时，利用人脸识别技术对数据授权用户进行身份认证；当数据授权用户的身份类
35

型企业时，利用企业认证技术对数据授权用户进行身份认证。

在某些实施方案中，在数据授权用户进行身份认证时，通过 CA 机构提供的秘钥托管服务对数据授权用户在进行用户授权签名时的私钥进行安全存储。

- 5 在某些实施方案中，分布式身份联盟链在数据授权用户认证合法时，向数据授权用户分配第一分布式身份标识，该数据授权用户在分布式身份联盟链和数据授权验证联盟链中，以第一分布式身份标识作为唯一标识。

- 10 在某些实施方案中，数据授权验证联盟链中的数据保管机构，根据第一分布式身份标识，向数据授权用户分发数据授权凭证。此时，数据授权用户可以在小程序中查看数据授权凭证。

- 15 在某些实施方案中，向数据授权用户分发数据授权凭证后，数据授权验证联盟链分别将身份认证记录、数据授权凭证通过哈希算法，得到哈希散列值，并将该哈希散列值存储。其中，身份认证记录为数据授权用户发起数据存证请求，直至数据授权用户认证合法的过程。

在某些实施方案中，数据调用请求还包括：数据授权凭证类型。当然，一个数据授权用户至少具有一种类型的数据授权凭证。分布式身份联盟链根据第二分布式身份标识，利用第一分布式身份标识，查询与数据调用请求中的数据授权凭证类型，对应的数据授权凭证。

- 20 在某些实施方案中，以数据授权凭证为学历证书为例进行说明：公司 A 想要获取用户 B 的学历证书，公司 A 在小程序中发起数据调用请求，该数据调用请求包括：用户 B 的学历证书，当分布式身份联盟链认证公司 A 合法时，为公司 A 分配第二分布式身份标识。分布式身份联盟链根据第二分布式身份标识，利用用户 B 的第一分布式身份标识，向数据授权验证联盟链请求查询用户 B 的学历证书。

- 25 在某些实施方案中，用户 B 可以只有学历证书这一种数据授权凭证，也可以有多种类型的数据授权凭证，比如还有：用户 B 的学位证书等。

- 30 在某些实施方案中，分布式身份联盟链在数据调用用户认证合法后，向数据授权联盟链发送查询数据授权用户的数据授权凭证的查询请求。数据授权联盟链根据查询请求，向分布式身份联盟链返回数据授权用户的数据授权凭证。分布式身份联盟链根据数据授权凭证，发起数据授权请求，并利用预先存储的私钥对数据授权请求进行数字签名，生成授权请求验证信息，向数据授权用户对应的第二终端上的小程序发送授权请求验证信息。

- 35 在某些实施方案中，授权请求验证信息包括二维码、条形码以及

验证码中的任意一项。分布式身份联盟链根据数据授权凭证，发起数据授权请求，并利用预先存储的私钥对数据授权请求进行数字签名，生成二维码，并向数据授权用户对应的第二终端上的小程序发送二维码；或，分布式身份联盟链根据数据授权凭证，发起数据授权请求，
5 并利用预先存储的私钥对数据授权请求进行数字签名，生成条形码，并向数据授权用户对应的第二终端上的小程序发送条形码；或，分布式身份联盟链根据数据授权凭证，发起数据授权请求，并利用预先存储的私钥对数据授权请求进行数字签名，生成验证码，并向数据授权用户对应的第二终端上的小程序发送验证码。

10 在某些实施方案中，验证码可以为图片、字母或数字等多种形式。
本公开以生成二维码为例进行说明，但并不用于限制本公开的保护范围。

在某些实施方案中，分布式身份联盟链向数据授权用户对应的第二终端发送授权请求验证信息之后，获取第二终端上的小程序返回的
15 正在运行验证操作的指示信息，根据正在运行验证操作的指示信息，验证数据授权用户的第一分布式身份标识，以及数据授权凭证，在验证合法时，向第二终端上的小程序发送执行数据授权操作的指示信息。

在某些实施方案中，在确定数据授权用户确定授权后，使用公钥加密数据调用请求对应的请求结果，并将加密后的请求结果发送至第一
20 终端对应的小程序。

在某些实施方案中，利用哈希算法分别计算身份认证对应的身份认证记录、数据授权凭证、数据授权请求、以及与数据授权请求对应的数据授权记录的哈希值，并将哈希值存储在数据授权验证联盟链中。

在某些实施方案中，身份认证记录为数据授权用户发起数据存证
25 请求，直至数据授权用户认证合法的过程，或，数据调用用户发起数据调用请求，直至数据调用用户认证合法的过程；数据授权记录为发起数据授权请求直至确定数据授权用户确定授权的过程。

本公开实施例提供的方法，应用于联盟链，利用联盟链的分布式特征，避免了所有数据都存储在一个中心平台；本公开获取第一终端
30 发送的数据调用请求，根据数据调用请求，对第一终端对于的数据调用用户进行身份认证，有效的解决了非法用户入侵的问题，在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识，使得该数据调用用户在联盟链中以第二分布式身份标识作为唯一标识；根据第二分布式身份标识，利用数据调用请求携带的第一分布式身份标识，
35 查询数据授权用户的数据授权凭证，根据该数据授权凭证，向数据授权用户对应的第二终端发送数据授权请求，在确定数据授权用户

确定授权后，加密数据调用请求对应的请求结果，并将加密后的请求结果发送至第一终端，有效的提高了数据的安全性。

本公开涉及数据获取方法，该方法应用在第二终端中，该方法的实现如图3所示：

5 步骤301，接收联盟链发送的数据授权请求；

其中，数据授权请求为：联盟链在获取第一终端发送的数据调用请求；根据数据调用请求，对第一终端对应的数据调用用户进行身份认证；在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识；根据第二分布式身份标识，利用第一分布式身份标识，查
10 询数据授权用户的数据授权凭证后发送，其中，数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；以及

步骤302，根据数据授权请求进行授权操作。

在某些实施方案中，第二终端的小程序接收分布式身份联盟链发送的授权请求验证信息，验证该授权请求验证信息，并将正在运行验证操作的指示信息返回给分布式身份联盟链；等待接收分布式身份联盟链发送的执行数据授权操作的指示信息，根据执行数据授权操作的指示信息，执行授权操作，并利用预先存储的私钥对授权操作进行数据
15 签名。

20 在某些实施方案中，授权记录可以在小程序中查看。

在某些实施方案中，授权请求验证信息包括二维码、条形码以及验证码中的任意一项。当第二终端的小程序接收分布式身份联盟链发送的授权请求验证信息为二维码时，小程序调用扫码功能，扫描二维码，并将正在运行验证操作的指示信息返回给分布式身份联盟链；当
25 第二终端的小程序接收分布式身份联盟链发送的授权请求验证信息为条形码时，小程序调用扫码功能，扫描条形码，并将正在运行验证操作的指示信息返回给分布式身份联盟链；当第二终端的小程序接收分布式身份联盟链发送的授权请求验证信息为验证码时，调用验证功能，输入验证码以验证该验证码，并将正在运行验证操作的指示信息返回
30 给所述联盟链。

在某些实施方案中，验证码可以为图片、字母或数字等多种形式。

本公开涉及第一数据获取装置4，该装置的实施可参见数据获取方法实施例部分的描述，重复之处不再赘述，如图4所示：

获取模块401，配置为第一终端发送的数据调用请求，其中，数据
35 调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；

认证模块 401，配置为根据数据调用请求，对第一终端对应的数据调用用户进行身份认证；

分配模块 403，配置为在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识；

5 查询模块 404，配置为根据第二分布式身份标识，利用第一分布式身份标识，查询数据授权用户的数据授权凭证；

 第一发送模块 405，配置为根据数据授权凭证，向数据授权用户对应的第二终端发送数据授权请求；以及

 第二发送模块 406，配置为在确定数据授权用户确定授权后，加密数据调用请求对应的请求结果，并将加密后的请求结果发送至第一终端。

 本公开涉及第二数据获取装置 5，该装置的实施可参见数据获取方法实施例部分的描述，重复之处不再赘述，如图 5 所示：

 接收模块 501，配置为接收联盟链发送的数据授权请求；

15 其中，数据授权请求为：联盟链在获取第一终端发送的数据调用请求；根据数据调用请求，对第一终端对应的数据调用用户进行身份认证；在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识；根据第二分布式身份标识，利用第一分布式身份标识，查询数据授权用户的数据授权凭证后发送，其中，数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；以及

 授权模块 502，配置为根据数据授权请求进行授权操作。

 基于同一构思，本公开还涉及电子设备 6，如图 6 所示，该电子设备主要包括：处理器 601、通信组件 602、存储器 603 和通信总线 604，

25 其中，处理器 601、通信组件 602 和存储器 603 通过通信总线 604 完成相互间的通信。其中，存储器 603 中存储有可被处理器 601 执行的程序，处理器 601 执行存储器 603 中存储的程序，实现如下步骤：获取第一终端发送的数据调用请求，其中，数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；根据数据调用请求，对第一终端对应的数据调用用户进行身份认证；在数据调用用户认证合法时，向数据调用用户分配第二分布式身份标识；根据第二分布式身份标识，利用第一分布式身份标识，查询数据授权用户的数据授权凭证；根据数据授权凭证，向数据授权用户对应的第二终端发送数据授权请求；在确定数据授权用户确定授权后，加密数据调用请求对应的请求结果，并将加密后的请求结果发送至第一终端，或，

30 接收联盟链发送的数据授权请求，根据数据授权请求进行授权操作。

35

上述电子设备中提到的通信总线 604 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。该通信总线 604 可以分为地址总线、数据总线、控制总线等。为便于表示, 图 6 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。

通信组件 602 用于上述电子设备与其他设备之间的通信。

存储器 603 可以包括随机存取存储器(Random Access Memory, 简称 RAM), 也可以包括非易失性存储器(non-volatile memory), 至少一个磁盘存储器。在某些实施方案中, 存储器还可以是至少一个位于远离前述处理器 601 的存储装置。

上述的处理器 601 可以是通用处理器, 包括中央处理器(Central Processing Unit, 简称 CPU)、网络处理器(Network Processor, 简称 NP)等, 还可以是数字信号处理器(Digital Signal Processing, 简称 DSP)、专用集成电路(Application Specific Integrated Circuit, 简称 ASIC)、现场可编程门阵列(Field-Programmable Gate Array, 简称 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。

本公开还涉及计算机可读存储介质, 该计算机可读存储介质中存储有计算机程序, 当该计算机程序在计算机上运行时, 使得计算机执行第一实施例中所描述的应用于联盟链的数据获取方法, 或, 第二实施例中所描述的应用于第二终端的数据获取方法。

在某些实施方案中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。该计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行该计算机指令时, 全部或部分地产生按照本公开实施例所述的流程或功能。该计算机可以时通用计算机、专用计算机、计算机网络或者其他可编程装置。该计算机指令可以存储在计算机可读存储介质中, 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 计算机指令从一个网站站点、计算机、服务器或者数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、微波等)方式向另外一个网站站点、计算机、服务器或数据中心进行传输。该计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、数据中心等数据存储设备。该可用介质可以是磁性介质(例如软盘、硬盘、磁带等)、光介质(例如 DVD)或者半导体介质(例如固态硬盘)等。

需要说明的是, 在本文中, 诸如“第一”和“第二”等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来,

而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，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、物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5 者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

10 以上所述仅是本公开的具体实施方式，使本领域技术人员能够理解或实现本公开。对这些实施例的多种修改对本领域的技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本公开的精神或范围的情况下，在其它实施例中实现。因此，本公开将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

权利要求书

1. 数据获取方法，应用于联盟链，所述数据获取方法包括：

获取第一终端发送的数据调用请求，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；

5 根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；

在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；

10 根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证；

根据所述数据授权凭证，向所述数据授权用户对应的第二终端发送数据授权请求；以及

在确定所述数据授权用户确定授权后，加密所述数据调用请求对应的请求结果，并将加密后的所述请求结果发送至所述第一终端。

15

2. 如权利要求1所述的数据获取方法，其中，根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证之前，所述方法还包括：

20 获取所述第二终端发送的数据存证请求，其中，所述数据存证请求中携带所述数据授权用户的标识；

根据所述数据存证请求，对所述数据授权用户进行身份认证；

在所述数据授权用户认证合法时，向所述数据授权用户分配所述第一分布式身份标识；以及

25 根据所述第一分布式身份标识，向所述数据授权用户分发所述数据授权凭证。

3. 如权利要求1或2所述的数据获取方法，其中，所述数据调用请求包括：所述数据调用用户的身份类型；

30 根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证，包括：

当所述数据调用用户的所述身份类型为个人时，利用人脸识别技术对所述数据调用用户进行身份认证；以及

当所述数据调用用户的所述身份类型为企业时，利用企业认证技术对所述数据调用用户进行身份认证。

35

4. 如权利要求 2 或 3 所述的数据获取方法, 其中, 所述数据存证请求中包括: 所述数据授权用户的身份类型;

根据所述数据存证请求, 对所述数据授权用户进行身份认证, 包括:

5 当所述数据授权用户的所述身份类型为所述个人时, 利用所述人脸识别技术对所述数据授权用户进行身份认证; 以及

当所述数据授权用户的所述身份类型为所述企业时, 利用所述企业认证技术对所述数据授权用户进行身份认证。

10 5. 如权利要求 1 至 4 中任一权利要求所述的数据获取方法, 其中, 根据所述数据授权凭证, 向所述数据授权用户对应的第二终端发送数据授权请求, 包括:

根据所述数据授权凭证, 发起所述数据授权请求, 并利用预先存储的私钥对所述数据授权请求进行数字签名, 生成授权请求验证信息,
15 向所述数据授权用户对应的第二终端发送所述授权请求验证信息。

6. 如权利要求 5 所述的数据获取方法, 其中, 所述方法还包括: 获取所述第二终端返回的正在运行验证操作的指示信息;

20 验证所述数据授权用户的所述第一分布式身份标识, 以及所述数据授权凭证; 以及

在验证合法时, 向所述第二终端发送执行数据授权操作的指示信息。

25 7. 如权利要求 5 或 6 所述的数据获取方法, 其中, 所述授权请求验证信息包括二维码、条形码以及验证码中的任意一项;

生成授权请求验证信息, 向所述数据授权用户对应的第二终端发送所述授权请求验证信息, 包括:

生成所述二维码, 向所述数据授权用户对应的第二终端发送所述二维码;

30 或, 生成所述条形码, 向所述数据授权用户对应的第二终端发送所述条形码;

或, 生成所述验证码, 向所述数据授权用户对应的第二终端发送所述验证码。

35 8. 如权利要求 1 至 7 中任一权利要求所述的数据获取方法, 其中,

所述数据调用请求还包括：数据授权凭证类型；以及

根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的所述数据授权凭证，包括：

- 5 根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询与所述数据调用请求中的所述数据授权凭证类型，对应的所述数据授权凭证。

9. 如权利要求 1 至 8 任一权利要求所述的数据获取方法，其还包括：

- 10 利用哈希算法分别计算所述身份认证对应的身份认证记录、所述数据授权凭证、所述数据授权请求、以及与所述数据授权请求对应的数据授权记录的哈希值，并将所述哈希值存储在所述联盟链中。

10. 数据获取方法，应用于第二终端，所述数据获取方法包括：

- 15 接收联盟链发送的数据授权请求；

- 其中，所述数据授权请求为：联盟链在获取第一终端发送的数据调用请求；根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；根据所述第二分布式身份标识，
20 利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证后发送，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；以及

根据所述数据授权请求进行授权操作。

- 25 11. 如权利要求 10 所述的数据获取方法，其中，接收联盟链发送的数据授权请求，包括：

接收所述联盟链发送的授权请求验证信息；

根据所述数据授权请求进行授权操作，包括：

- 30 验证所述授权请求验证信息，并将正在运行验证操作的指示信息返回给所述联盟链；

接收所述联盟链发送的执行数据授权操作的指示信息；以及

根据所述执行数据授权操作的指示信息，执行授权操作，并利用预先存储的私钥对所述授权操作进行数据签名。

- 35 12. 如权利要求 11 所述的数据获取方法，其中，所述授权请求验

证信息包括二维码、条形码以及验证码中的任意一项；

验证所述授权请求验证信息，并将正在运行验证操作的指示信息返回给所述联盟链，包括：

5 调用扫码功能，扫描所述二维码，并将正在运行验证操作的指示信息返回给所述联盟链；

或，调用扫码功能，扫描所述条形码，并将正在运行验证操作的指示信息返回给所述联盟链；

或，调用验证功能，验证所述验证码，并将正在运行验证操作的指示信息返回给所述联盟链。

10

13. 第一数据获取装置，其包括：

获取模块，配置为第一终端发送的数据调用请求，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；

15 认证模块，配置为根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；

分配模块，配置为在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；

20 查询模块，配置为根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证；

第一发送模块，配置为根据所述数据授权凭证，向所述数据授权用户对应的第二终端发送数据授权请求；以及

25 第二发送模块，配置为在确定所述数据授权用户确定授权后，加密所述数据调用请求对应的请求结果，并将加密后的所述请求结果发送至所述第一终端。

14. 第二数据获取装置，其包括：

接收模块，配置为接收联盟链发送的数据授权请求；

30 其中，所述数据授权请求为：联盟链在获取第一终端发送的数据调用请求；根据所述数据调用请求，对所述第一终端对应的所述数据调用用户进行身份认证；在所述数据调用用户认证合法时，向所述数据调用用户分配第二分布式身份标识；根据所述第二分布式身份标识，利用所述第一分布式身份标识，查询所述数据授权用户的数据授权凭证后发送，其中，所述数据调用请求中携带数据授权用户的第一分布式身份标识，以及数据调用用户的标识；以及

35 授权模块，配置为根据所述数据授权请求进行授权操作。

15. 电子设备，包括：处理器、通信组件、存储器和通信总线，其中，所述处理器、所述通信组件和所述存储器通过所述通信总线完成相互间的通信；

5 所述存储器，配置为存储计算机程序；

 所述处理器，配置为执行所述存储器中所存储的程序，实现权利要求 1 至 9 中任一权利要求所述的应用于联盟链的数据获取方法，或，实现权利要求 10 至 12 中任一权利要求所述的应用于第二终端的数据获取方法。

10

16. 计算机可读存储介质，存储有计算机程序，其中，所述计算机程序被处理器执行时实现权利要求 1 至 9 中任一权利要求所述的应用于联盟链的数据获取方法，或，实现权利要求 10 至 12 中任一权利要求所述的应用于第二终端的数据获取方法。

15