(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 108923925 B
(45)授权公告日 2022.11.08

(21)申请号 201810650431.0

(22)申请日 2018.06.22

(65)同一申请的已公布的文献号
申请公布号 CN 108923925 A

(43)申请公布日 2018.11.30

(73)专利权人 北京京东尚科信息技术有限公司
地址 100195 北京市海淀区杏石口路65号西杉创意园四区11号楼东段1-4层西段1-4层
专利权人 北京京东世纪贸易有限公司

(72)发明人 张伟

(74)专利代理机构 北京英赛嘉华知识产权代理有限责任公司 11204
专利代理师 王达佐 马晓亚

(51)Int.Cl.
H04L 9/30(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 9/06(2006.01)
H04L 9/40(2022.01)

(56)对比文件
CN 107292181 A,2017.10.24
CN 107770182 A,2018.03.06
CN 105915520 A,2016.08.31
US 2017373850 A1,2017.12.28

审查员 张攀

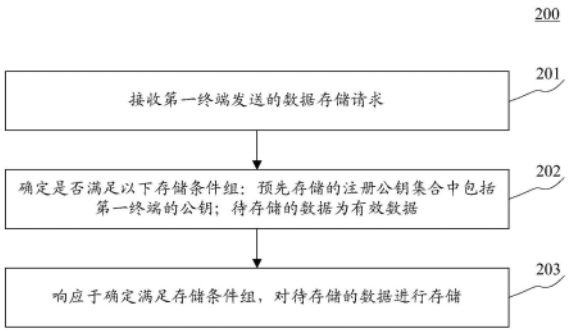
权利要求书3页 说明书12页 附图4页

(54)发明名称

应用于区块链的数据存储方法和装置

(57)摘要

本申请实施例公开了应用于区块链的数据存储方法和装置。应用于区块链的数据存储方法的一具体实施方式包括:接收第一终端发送的数据存储请求,该数据存储请求包括该第一终端的公钥以及待存储的数据;确定是否满足以下存储条件组:预先存储的注册公钥集合中包括该第一终端的公钥;待存储的数据为有效数据;响应于确定满足该存储条件组,对待存储的数据进行存储。该实施方式可以降低所存储的数据中存在异常数据的风险以及数据被篡改的风险,提高所存储的数据的安全性。



CN 108923925 B

1.一种应用于区块链的数据存储方法,包括:

接收第一终端发送的数据存储请求,所述数据存储请求包括所述第一终端的公钥以及待存储的数据;

确定是否满足以下存储条件组:预先存储的注册公钥集合中包括所述第一终端的公钥;待存储的数据为有效数据;

响应于确定满足所述存储条件组,对待存储的数据进行存储;

确定是否满足以下存储条件组,包括:采用预先约定的密钥对所述待存储的数据中的时间戳信息进行解密,并根据解密后的时间戳信息确定所述待存储的数据是否为有效数据;

接收第二终端发送的数据访问请求,其中,所述数据访问请求包括所述第二终端的公钥、所持有的访问公钥以及所请求访问的数据的存储数据标识;

确定是否满足以下访问条件组:所述预先存储的注册公钥集合中包括所述第二终端的公钥;所持有的访问公钥为所述第一终端的公钥;

响应于确定满足所述访问条件组,利用所述第一终端的公钥对所请求访问的数据的存储数据标识加密,确定加密后的所请求访问的数据的存储数据标识与所述第一终端存储的加密后的存储数据标识是否相同;

响应于确定加密后的所请求访问的数据的存储数据标识与所述第一终端存储的加密后的存储数据标识相同,向所述第二终端发送所述第一终端存储的数据。

2.根据权利要求1所述的方法,其中,在接收第一终端发送的数据存储请求之前,所述方法还包括:

接收所述第一终端发送的公钥注册请求,所述公钥注册请求包括所述第一终端的公钥;

对所述第一终端的公钥进行加密;

将加密后的公钥添加至所述注册公钥集合,以及将加密后的公钥发送至第二终端。

3.根据权利要求1所述的方法,其中,在接收第一终端发送的数据存储请求之前,所述方法还包括:

接收所述第一终端发送的公钥注册请求;

基于所述公钥注册请求,生成公钥和私钥密钥对;

将所生成的公钥和私钥密钥对发送至所述第一终端,以及对所生成的公钥进行加密;

将加密后的公钥添加至所述注册公钥集合,以及将加密后的公钥发送至第二终端。

4.根据权利要求1-3之一所述的方法,其中,所述数据存储请求还包括数字签名;以及

所述确定是否满足以下存储条件组,包括:

利用所述第一终端的公钥对所述数字签名进行解密验证,确定所述数字签名是否有效;

响应于确定所述数字签名有效,确定待存储的数据为有效数据。

5.根据权利要求2或3所述的方法,其中,所述数据存储请求还包括存储数据标识;以及

响应于确定满足所述存储条件组,对待存储的数据进行存储,包括:

利用所述第一终端的公钥对所述存储数据标识进行加密;

将加密后的存储数据标识作为待存储的数据的主关键字,对加密后的存储数据标识进

行存储；

响应于确定存储成功，向所述第一终端返回存储成功的信息，以及向所述第二终端发送所述存储数据标识。

6.一种应用于区块链的数据存储装置，包括：

接收单元，被配置成接收第一终端发送的数据存储请求，所述数据存储请求包括所述第一终端的公钥以及待存储的数据；

确定单元，被配置成确定是否满足以下存储条件组：预先存储的注册公钥集合中包括所述第一终端的公钥；待存储的数据为有效数据；

存储单元，被配置成响应于确定满足所述存储条件组，对待存储的数据进行存储；

所述确定单元还被配置：成采用预先约定的密钥对所述待存储的数据中的时间戳信息进行解密，并根据解密后的时间戳信息确定所述待存储的数据是否为有效数据；

所述装置进一步被配置成：

接收第二终端发送的数据访问请求，其中，所述数据访问请求包括所述第二终端的公钥、所持有的访问公钥以及所请求访问的数据的存储数据标识；

确定是否满足以下访问条件组：所述预先存储的注册公钥集合中包括所述第二终端的公钥；所持有的访问公钥为所述第一终端的公钥；

响应于确定满足所述访问条件组，利用所述第一终端的公钥对所请求访问的数据的存储数据标识加密，确定加密后的所请求访问的数据的存储数据标识与所述第一终端存储的加密后的存储数据标识是否匹配；

响应于确定加密后的所请求访问的数据的存储数据标识与所述第一终端存储的加密后的存储数据标识匹配，向所述第二终端发送所述第一终端存储的数据。

7.根据权利要求6所述的装置，其中，所述装置还包括：

公钥注册请求单元，被配置成接收所述第一终端发送的公钥注册请求，所述公钥注册请求包括所述第一终端的公钥；

加密单元，被配置成对所述第一终端的公钥进行加密；

添加单元，被配置成将加密后的公钥添加至所述注册公钥集合，以及将加密后的公钥发送至第二终端。

8.根据权利要求6所述的装置，其中，所述装置还包括：

公钥注册请求单元，被配置成接收所述第一终端发送的公钥注册请求；

生成单元，被配置成基于所述公钥注册请求，生成公钥和私钥密钥对；

加密单元，被配置成将所生成的公钥和私钥密钥对发送至所述第一终端，以及对所生成的公钥进行加密；

添加单元，被配置成将加密后的公钥添加至所述注册公钥集合，以及将加密后的公钥发送至第二终端。

9.根据权利要求6-8之一所述的装置，其中，所述数据存储请求还包括数字签名；以及

所述确定单元被配置成：

利用所述第一终端的公钥对所述数字签名进行解密验证，确定所述数字签名是否有效；

响应于确定所述数字签名有效，确定待存储的数据为有效数据。

10.根据权利要求7或8所述的装置，其中，所述数据存储请求还包括存储数据标识；以及

所述添加单元被配置成：

利用所述第一终端的公钥对所述存储数据标识进行加密；

将加密后的存储数据标识作为待存储的数据的主关键字，对加密后的存储数据标识进行存储；

响应于确定存储成功，向所述第一终端返回存储成功的信息，以及向所述第二终端发送存储数据标识。

11.一种第一终端设备，包括：

一个或多个处理器；

存储装置，其上存储有一个或多个程序；

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1-5中任一所述的方法。

12.一种计算机可读存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1-5中任一所述的方法。

应用于区块链的数据存储方法和装置

技术领域

[0001] 本申请实施例涉及无线通信技术领域，具体涉及数据存储方法和装置。

背景技术

[0002] 随着互联网技术的不断发展，网络已经成为用户获取信息的一种重要方式，同时也给用户带来了极大的便利。

[0003] 现有的信息共享技术中，通常设置局部开放的信息共享平台，用户可以将数据存储到信息共享平台，也可以从信息共享平台读取所需要的数据。

发明内容

[0004] 本申请实施例提出了数据存储方法和装置。

[0005] 第一方面，本申请实施例提供了一种应用于区块链的数据存储方法，包括：接收第一终端发送的数据存储请求，该数据存储请求包括该第一终端的公钥以及待存储的数据；确定是否满足以下存储条件组：预先存储的注册公钥集合中包括该第一终端的公钥；待存储的数据为有效数据；响应于确定满足该存储条件组，对待存储的数据进行存储。

[0006] 在一些实施例中，在接收第一终端发送的数据存储请求之前，该方法还包括：接收该第一终端发送的公钥注册请求，该公钥注册请求包括该第一终端的公钥；对该第一终端的公钥进行加密；将加密后的公钥添加至该注册公钥集合，以及将加密后的公钥发送至第二终端。

[0007] 在一些实施例中，在接收第一终端发送的数据存储请求之前，该方法还包括：接收第一终端发送的公钥注册请求；基于公钥注册请求，生成公钥和私钥密钥对；将所生成的公钥和私钥密钥对发送至第一终端，以及对所生成的公钥进行加密；将加密后的公钥添加至所述注册公钥集合，以及将加密后的公钥发送至第二终端。

[0008] 在一些实施例中，该数据存储请求还包括数字签名；以及该确定是否满足以下存储条件组，包括：利用该第一终端的公钥对该数字签名进行解密验证，确定该数字签名是否有效；响应于确定该数字签名有效，确定待存储的数据为有效数据。

[0009] 在一些实施例中，该数据存储请求还包括存储数据标识；以及响应于确定满足该存储条件组，对待存储的数据进行存储，包括：利用该第一终端的公钥对该存储数据标识进行加密；将加密后的存储数据标识作为待存储的数据的主关键字，对加密后的存储数据标识进行存储；响应于确定存储成功，向该第一终端返回存储成功的信息，以及向该第二终端发送该存储数据标识。

[0010] 在一些实施例中，该方法还包括：接收该第二终端发送的数据访问请求，其中，该数据访问请求包括该第二终端的公钥、所持有的访问公钥以及所请求访问的数据的存储数据标识；确定是否满足以下访问条件组：该预先存储的注册公钥集合中包括该第二终端的公钥；所持有的访问公钥为该第一终端的公钥；响应于确定满足该访问条件组，利用该第一终端的公钥对所请求访问的数据的存储数据标识加密，确定加密后的所请求访问的数据的

存储数据标识与该第一终端存储的加密后的存储数据标识是否相同;响应于确定加密后的所请求访问的数据的存储数据标识与该第一终端存储的加密后的存储数据标识相同,向该第二终端发送该第一终端存储的数据。

[0011] 第二方面,本申请实施例提供了一种应用于区块链的数据存储装置,包括:接收单元,被配置成接收第一终端发送的数据存储请求,该数据存储请求包括该第一终端的公钥以及待存储的数据;确定单元,被配置成确定是否满足以下存储条件组:预先存储的注册公钥集合中包括该第一终端的公钥;待存储的数据为有效数据;存储单元,被配置成响应于确定满足该存储条件组,对待存储的数据进行存储。

[0012] 在一些实施例中,该装置还包括:公钥注册请求单元,被配置成接收该第一终端发送的公钥注册请求,该公钥注册请求包括该第一终端的公钥;加密单元,被配置成对该第一终端的公钥进行加密;添加单元,被配置成将加密后的公钥添加至该注册公钥集合,以及将加密后的公钥发送至第二终端。

[0013] 在一些实施例中,该装置还包括:公钥注册请求单元,被配置成接收第一终端发送的公钥注册请求;生成单元,被配置成基于公钥注册请求,生成公钥和私钥密钥对;加密单元,被配置成将所生成的公钥和私钥密钥对对发送至所述第一终端,以及对所生成的公钥进行加密;添加单元,被配置成将加密后的公钥添加至注册公钥集合,以及将加密后的公钥发送至第二终端。

[0014] 在一些实施例中,该数据存储请求还包括数字签名;以及该确定单元进一步被配置成:利用该第一终端的公钥对该数字签名进行解密验证,确定该数字签名是否有效;响应于确定该数字签名有效,确定待存储的数据为有效数据。

[0015] 在一些实施例中,该数据存储请求还包括存储数据标识;以及该添加单元进一步被配置成:利用该第一终端的公钥对该存储数据标识进行加密;将加密后的存储数据标识作为待存储的数据的主关键字,对加密后的存储数据标识进行存储;响应于确定存储成功,向该第一终端返回存储成功的信息,以及向该第二终端发送该存储数据标识。

[0016] 在一些实施例中,该装置进一步被配置成:接收该第二终端发送的数据访问请求,其中,该数据访问请求包括该第二终端的公钥、所持有的访问公钥以及所请求访问的数据的存储数据标识;确定是否满足以下访问条件组:该预先存储的注册公钥集合中包括该第二终端的公钥;所持有的访问公钥为该第一终端的公钥;响应于确定满足该访问条件组,利用该第一终端的公钥对所请求访问的数据的存储数据标识加密,确定加密后的所请求访问的数据的存储数据标识与该第一终端存储的加密后的存储数据标识是否相同;响应于确定加密后的所请求访问的数据的存储数据标识与该第一终端存储的加密后的存储数据标识相同,向该第二终端发送该第一终端存储的数据。

[0017] 第三方面,本申请实施例提供了一种第一终端设备,该第一终端设备包括:一个或多个处理器;存储装置,其上存储有一个或多个程序;当一个或多个程序被一个或多个处理器执行,使得一个或多个处理器实现如第一方面中任一实现方式描述的方法。

[0018] 第四方面,本申请实施例提供了一种计算机可读介质,其上存储有计算机程序,该计算机程序被处理器执行时实现如第一方面中任一实现方式描述的方法。

[0019] 本申请实施例提供的数据存储方法和装置,首先接收第一终端发送的数据存储请求,然后确定第一终端的数据存储请求是否满足存储条件组,最后在第一终端的数据存储

请求满足存储条件组的情况下，对待存储的数据进行存储。该数据存储方法，可以降低所存储的数据中存在异常数据(例如病毒数据)的风险以及数据被篡改的风险，提高所存储的数据的安全性。

附图说明

[0020] 通过阅读参照以下附图所作的对非限制性实施例所作的详细描述，本申请的其它特征、目的和优点将会变得更明显：

[0021] 图1是本申请的一个实施例可以应用于其中的示例性系统架构图；

[0022] 图2是根据本申请的应用于区块链的数据存储方法的一个实施例的流程图；

[0023] 图3是图2所提供的应用于区块链的数据存储方法的一个应用场景的示意图；

[0024] 图4是根据本申请的应用于区块链的数据存储方法的又一个实施例的流程图；

[0025] 图5是根据本申请的应用于区块链的数据存储装置的一个实施例的流程图；

[0026] 图6是适于用来实现本申请实施例的计算机系统的结构示意图。

具体实施方式

[0027] 下面结合附图和实施例对本申请作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释相关发明，而非对该发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与有关发明相关的部分。

[0028] 需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。下面将参考附图并结合实施例来详细说明本申请。

[0029] 图1示出了可以应用本申请的应用于区块链的数据存储方法的实施例的示例性系统架构100。

[0030] 如图1所示，系统架构100可以包括第一终端设备101、网络102、104、区块链103以及第二终端设备105。网络102可以用以在第一终端设备101和区块链103之间提供通信链路的介质，网络104可以用以在区块链103以及第二终端设备105之间提供通信链路介质。网络102、104可以包括各种连接类型，例如有线、无线通信链路或者光纤电缆等等。用户可以使用第一终端设备101以及第二终端设备105分别通过网络102、104与区块链103交互，以接收或发送消息等。第一终端设备101以及第二终端设备105上可以安装有各种通讯客户端应用，例如无线接入点连接类应用、搜索类应用、数据存储类应用、数据读取类应用等等。

[0031] 第一终端设备101、第二终端设备105可以是硬件，也可以是软件。当第一终端设备101、第二终端设备105为硬件时，可以是支持连接无线接入点的各种电子设备，包括但不限于智能手机、平板电脑、膝上型便携计算机和台式计算机等等。当第一终端设备101、第二终端设备105为软件时，可以安装在上述所列举的电子设备中。其可以实现成多个软件或软件模块，也可以实现成单个软件或软件模块。在此不做具体限定。

[0032] 上述第一终端设备101、第二终端设备104可以通过有线连接或者无线连接的方式作为区块链节点接入区块链。同时，当第一终端设备101为存储数据至区块链的节点设备，第二终端设备105为从区块链中获取第一终端设备101中存储的数据的节点设备时，第二终端设备105可以通过区块链从第一终端设备101中获取数据。

[0033] 区块链103可以提供各种服务，例如可以对第一终端设备101接收到的数据存储请

求进行验证，在确定第一终端设备101以及所请求存储的数据满足存储条件后，对所请求存储的数据进行存储。再例如，区块链103还可以对接收到的第二终端设备104数据访问请求进行验证后，在满足访问条件组的情况下，将第二终端设备104所请求访问的数据发送给第二终端设备104。

[0034] 需要说明的是，区块链103可以是硬件，也可以是软件。当区块链103为硬件时，可以实现集群式服务，也可以实现单个服务。当服务器为软件时，可以实现成多个软件或软件模块(例如用来提供分布式服务)，也可以实现成单个软件或软件模块。在此不做具体限定。

[0035] 需要说明的是，本申请实施例所提供的数据存储方法可以由区块链103执行。相应地，数据存储装置一般设置于区块链103中。

[0036] 此时，

[0037] 应该理解，图1中的第一终端设备、第二终端设备、网络和区块链的数目仅仅是示意性的。根据实现需要，可以具有任意数目的第一终端设备、第二终端设备、网络和区块链。

[0038] 继续参考图2，其示出了根据本申请的应用于区块链的数据存储方法的一个实施例的流程200。包括以下步骤：

[0039] 步骤201，接收第一终端发送的数据存储请求。

[0040] 在本实施例中，数据存储方法的执行主体(例如图1所示的区块链103)可以通过有线连接或无线连接的方式接收第一终端发送的数据存储请求。上述执行主体可以为数据存储服务器，该数据存储服务器可以存储至少一个第一终端的数据。在这里，可以将第一终端作为向上述执行主体发送数据存储请求的终端。由此，上述执行主体可以接收一个第一终端发送的数据存储请求，也可以同时接收两个、三个第一终端发送的数据存储请求，在此不做限定，根据应用场景的需要设定。

[0041] 在本实施例中，上述执行主体可以接收包括第一终端的公钥以及待存储的数据的数据存储请求。该第一终端的公钥既可以为第一终端本地生成的，也可以为第一终端从上述执行主体中获取的。该待存储的数据既可以为数据内容本身，也可以为对该数据内容进行哈希计算后生成的数据摘要。

[0042] 作为示例，上述第一终端可以首先利用加密算法(例如JAVA RSA加密算法)本地生成公钥和私钥密钥对。然后，基于预先设置的协议(例如第一终端与上述执行主体的连接协议、传输协议等)，第一终端可以将本地生成的公钥发送至上述执行主体中以便执行主体存储。当上述执行主体确定上述预先设置的协议正确、公钥满足预设格式(例如预设公钥字符长度、预设生成公钥的算法)，可以将第一终端的公钥存储至注册公钥集合中。当上述执行主体存储成功后，则表明第一终端的公钥已经在上述执行主体中注册过。在进行数据存储时，上述第一终端可以将在上述执行主体中注册过的公钥以及待存储的数据发送至上述执行主体。

[0043] 作为示例，当用于存储第一终端所请求存储的数据为区块链中的区块时，上述执行主体可以为区块链。在这里，区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型数据存储装置。该区块链可以包括但不限于以下至少一项：私有链、联盟链、许可链。以联盟链为例进行阐述。

[0044] 联盟链为只针对特定群体成员开放的区块链，联盟链中指定多个预选第一终端作为联盟链的节点向联盟链中存储数据。在这里，第一终端可以通过联盟链中的API

(Application Programming Interface,应用程序编程接口)根据其预先设置的授权许可机制以授权许可的方式加入联盟链,从而可以向联盟链中存储的数据。因此,上述第一终端即为可以向联盟链中存储数据的节点。在这里,上述授权许可的方式例如可以包括根据预先设置的条件(例如达到某一行业共识标准,获得行业证书等)来对第一终端进行授权许可。当第一终端被授权许可后,上述联盟链可以利用加密算法生成公钥和私钥,将生成的公钥存储至注册公钥集合,将生成的公钥和私钥密钥对发送至被授权许可的第一终端。第一终端在向联盟链中的区块存储数据时,需要向联盟链发送联盟链授权许可的公钥以及待存储的数据。

[0045] 步骤202,确定是否满足以下存储条件组:预先存储的注册公钥集合中包括第一终端的公钥;待存储的数据为有效数据。

[0046] 在本实施例中,上述执行主体接收到第一终端的公钥时,可以将该第一终端的公钥与预先存储的注册公钥集合中的公钥进行比较,从而确定注册公钥集合中是否包括上述第一终端的公钥。

[0047] 在本实施例中,上述执行主体还需要对接收到的第一终端发送的待存储的数据进行验证,从而确定待存储的数据是否为有效数据。在这里,该有效数据例如可以包括上述待存储的数据在在有效期内的数据。具体的,上述执行主体可以对第一终端发送的预设时间段内的数据进行存储。上述待存储数据中通常包括加密的时间戳信息。上述执行主体可以利用第一终端的公钥或者与第一终端约定的密钥对加密的时间戳信息进行解密,并根据解密后的时间戳信息确定待存储的数据是否为有效数据。在这里,该加密的密钥例如可以为与第一终端的公钥对应的私钥,也可以为与上述执行主体约定的其他方式的密钥。

[0048] 在本实施例中,当确定预先存储的注册公钥集合中包括第一终端的公钥以及待存储的数据为有效数据时,可以确定第一终端以及第一终端存储的数据满足预设存储条件。

[0049] 在本实施例的一些可选的实现方式中,上述第一终端的数据存储请求还包括数字签名。上述执行主体可以利用第一终端的公钥对数字签名进行解密验证,从而确定数字签名是否有效。在数字签名有效时,确定待存储的数据为有效数据。

[0050] 具体的,数字签名通常为第一终端利用哈希函数(例如SHA-256算法)对待存储的数据进行哈希计算后生成的待存储的数据的摘要,然后利用其私钥对所生成的摘要进行加密而得到。因此,上述执行主体可以利用与第一终端相同的计算方法对第一终端发送的待存储数据进行哈希计算,生成第一终端发送的待存储的数据的摘要。然后,上述执行主体利用第一终端的公钥对第一终端发送的数据签名进行解密,得到待存储的数据的摘要。最后,上述执行主体可以将解密第一终端的数字签名后得到的摘要与计算的摘要进行比较,确定二者是否相同。当二者相同时,可以确定第一终端发送的数字签名有效。从而,上述执行主体可以确定待存储的数据为有效数据。

[0051] 在本实施例的一些可选的实现方式中,该注册公钥集合中还包括与第一终端的公钥对应存储的第一终端的标识。为了便于确认第一终端是否拥有存储数据的权限,上述主体还可以将所述第一终端的标识与预设标识集合中的标识进行比较,以确定上述第一终端是否具有存储数据的权限。

[0052] 步骤203,响应于确定满足存储条件组,对待存储的数据进行存储。

[0053] 在本实施例中,当上述执行主体在确定预先存储的注册公钥集合中包括第一终端

的公钥以及待存储的数据为有效数据时，可以对待存储的数据进行存储。在这里，上述执行主体既可以存储数据内容本身，也可以存储对数据内容进行哈希计算后的数据摘要。

[0054] 继续参考图3，图3是图2所提供的应用于区块链的数据存储方法的一个应用场景300的示意图。在图3的应用场景中，用户通过手机301向服务器302发送“财务报告”的数据存储请求。该“财务报告”存储请求包括用户通过手机301进行密钥计算后生成的公钥303以及“财务报告”数据304。接着，服务器302将手机301发送的公钥303与预先存储的注册公钥集合中的公钥进行比较，确定注册公钥集合中包括公钥303。服务器302还需要对“财务报告”数据304进行验证，确定该“财务报告”数据304为有效数据。最后，服务器302在确定预先存储的注册公钥集合中包括手机301发送的公钥303以及“财务报告”数据304为有效数据时，对“财务报告”数据进行存储。

[0055] 本申请实施例提供的数据存储方法，首先接收第一终端发送的数据存储请求，然后确定第一终端的数据存储请求是否满足存储条件组，最后在第一终端的数据存储请求满足存储条件组的情况下，对待存储的数据进行存储。该数据存储方法，可以降低所存储的数据中存在异常数据(例如病毒数据)的风险以及数据被篡改的风险，提高所存储的数据的安全性，从而为数据共享平台提供安全保障。

[0056] 进一步参考图4，其示出了根据本申请的应用于区块链的数据存储方法的又一个实施例的流程400。包括以下步骤：

[0057] 步骤401，接收第一终端发送的公钥注册请求。

[0058] 在本实施例中，数据存储方法的执行主体(例如图1所示的区块链103)可以通过有线连接或无线连接的方式接收第一终端发送的公钥注册请求。在这里，上述执行主体可以为数据存储服务器，该数据存储服务器可以存储至少一个第一终端的数据。该公钥注册请求中请求注册的公钥可以为第一终端(例如图1所示的第一终端设备101)本地生成的，也可以为上述执行主体生成的。

[0059] 作为一种实现方式，上述第一终端可以首先利用加密算法(例如JAVA RSA加密算法)本地生成公钥和私钥密钥对。然后，基于预先设置的协议(例如第一终端与上述执行主体的连接协议、传输协议等)，上述执行主体可以接收第一终端本地生成的公钥以便在上述执行主体上注册。

[0060] 作为另一种实现方式，当数据存储方法的执行主体为区块链时，上述第一终端可以通过区块链中预先设置的授权许可机制以授权许可的方式加入区块链，从而可以向区块链中存储数据。该授权许可的方式例如可以包括根据预先设置的条件(例如达到某一行业共识标准，获得行业证书等)来对第一终端进行授权许可。当第一终端被授权许可后，上述区块链可以利用加密算法生成公钥和私钥密钥对。然后，将生成的公钥存储至注册公钥集合，将生成的公钥以及私钥一起发送至被授权许可的第一终端。由此，第一终端请求加入区块链可以作为向区块链发送公钥注册请求。

[0061] 步骤402，对第一终端的公钥进行加密。

[0062] 在本实施例中，上述执行主体接收到第一终端发送的公钥注册请求后，可以对第一终端发送的公钥或者本地生成的公钥利用其预先设置的现有技术的加密算法对该公钥进行加密。

[0063] 步骤403，将加密后的公钥添加至注册公钥集合，以及将加密后的公钥发送至第二

终端。

[0064] 在本实施例中，上述执行主体可以将加密后的公钥添加至注册公钥集合，然后将第一终端的公钥发送至第二终端。从而，第二终端向上述执行主体访问第一终端存储的数据时，可以携带第一终端的公钥。

[0065] 步骤404，接收第一终端发送的数据存储请求。

[0066] 在本实施例中，数据存储方法的执行主体(例如图1所示的区块链103)可以通过有线连接或无线连接的方式接收第一终端发送的数据存储请求。在这里，可以将第一终端作为向上述执行主体发送数据存储请求的终端。由此，上述执行主体可以接收一个第一终端发送的数据存储请求，也可以同时接收两个、三个第一终端发送的数据存储请求，在此不做限定，根据应用场景的需要设定。

[0067] 在本实施例中，上述执行主体可以接收包括第一终端的公钥、待存储的数据以及待存储的数据的存储数据标识的数据存储请求。该第一终端的公钥即可以为第一终端本地生成的，也可以为第一终端从上述执行主体中获取的。该待存储的数据既可以为数据内容本身，也可以为对该数据内容进行哈希计算后生成的数据摘要。

[0068] 步骤405，确定是否满足以下存储条件组：预先存储的注册公钥集合中包括第一终端的公钥；待存储的数据为有效数据。

[0069] 在本实施例中，上述执行主体接收到第一终端的公钥时，可以将该第一终端的公钥与预先存储的注册公钥集合中的公钥进行比较，从而确定注册公钥集合中是否包括上述第一终端的公钥。

[0070] 在本实施例中，上述执行主体还需要对接收到的第一终端发送的待存储的数据进行验证，从而确定待存储的数据是否为有效数据。在这里，该有效数据例如可以包括上述待存储的数据在有效期内的数据。具体的，上述执行主体可以对第一终端发送的预设时间段内的数据进行存储。上述待存储数据中通常包括加密的时间戳信息。上述执行主体可以利用第一终端的公钥或者与第一终端约定的密钥对加密的时间戳信息进行解密，并根据解密后的时间戳信息确定待存储的数据是否为有效数据。在这里，该加密的密钥例如可以为与第一终端的公钥对应的私钥，也可以为与上述执行主体约定的其他方式的密钥。

[0071] 在本实施例中，当确定预先存储的注册公钥集合中包括第一终端的公钥以及待存储的数据为有效数据时，可以确定第一终端以及第一终端存储的数据满足预设条件。

[0072] 步骤406，利用第一终端的公钥对存储数据标识进行加密。

[0073] 在本实施例中，存储数据标识用于标识待存储的数据，可以包括但不限于：第一终端的版本号与数据存储编号的组合，所存储的数据的报文头等。数据存储标识的具体的格式可以包括但不限于以下至少一项：字母、符号、字母与符号的组合等。

[0074] 在本实施例中，判断步骤405确定的第一终端以及第一终端所请求存储的数据是否满足存储条件，在确定第一终端以及第一终端所请求存储的数据满足存储条件时，上述执行主体可以利用第一终端的公钥通过公钥加密算法(例如哈希加密算法、RSA非对称加密算法)对存储数据标识进行加密。

[0075] 步骤407，将加密后的存储数据标识作为待存储的数据的主关键字，对加密后的存储数据标识进行存储。

[0076] 在本实施例中，主关键字是一个或多个字段，用于唯一标识某一条记录或某一个

数据内容。在这里，该主关键字可以用于唯一标识第一终端待存储的数据。由于存储数据标识可用于唯一标识待存储的数据，因此，可以将加密后的存储数据标识作为待存储的数据的主关键字。从而，通过查找到加密后的存储数据标识，并进行解密后，即可查找到所存储的数据。

[0077] 在本实施例中，上述执行主体既可以对待存储的数据本身直接进行存储。也可以对待存储的数据经过哈希计算后的数据摘要进行存储。也可以不直接存储待存储的数据，当有其他终端需要访问第一终端存储的数据时，上述执行主体可以建立第一终端与其他终端的连接，从而使得其他终端直接从第一终端获取该数据。

[0078] 步骤408，响应于确定存储成功，向第一终端返回存储成功的信息，以及向第二终端发送存储数据标识。

[0079] 在本实施例中，根据步骤407对加密后的存储数据进行存储后，上述执行主体可以在响应于确定存储成功的条件下，向第一终端返回存储成功的信息。同时，上述执行主体还可以向第二终端发送加密后的存储数据标识。

[0080] 在本实施例中，当上述执行主体为区块链时，上述第一终端所请求存储的数据也即为在区块链中共享的数据。因此，上述区块链仅存储上述加密后的存储数据标识即可。同时将加密后的存储数据标识发送给第二终端。当第二终端需要访问第一终端所存储的数据时，可以将所携带的存储数据标识提供给区块链。区块链可以根据存储数据标识查找到第一终端，从而可以直接从第一终端获取数据。

[0081] 步骤409，接收第二终端发送的数据访问请求。

[0082] 在本实施例中，根据步骤408所存储的第一终端所请求存储的数据以及向第二终端发送的加密后的存储数据标识，上述执行主体还可以接收第二终端发送的数据访问请求。在这里，该数据访问请求可以包括第二终端的公钥、所持有的访问公钥以及所请求访问的数据的存储数据标识。

[0083] 在本实施例中，上述第二终端的公钥可以为第二终端通过本地生成的，也可以为上述执行主体生成并发送给第二终端的。所持有的访问公钥以及所请求访问的数据的存储数据标识均为上述执行主体在步骤403与步骤408中发送给第二终端的。

[0084] 步骤410，确定是否满足以下访问条件组：预先存储的注册公钥集合中包括第二终端的公钥；第二终端所持有的访问公钥为所存储的数据的第一终端的公钥。

[0085] 在本实施例中，上述执行主体接收到第二终端的公钥时，可以将该第二终端的公钥与预先存储的注册公钥集合中的公钥进行比较，从而确定注册公钥集合中是否包括上述第二终端的公钥。在这里，第二终端的公钥的生成方法可以参考步骤401中所示的第一终端生成公钥、私钥的方法，在此不再赘述。

[0086] 在本实施中，上述执行主体还需要对第二终端所持有的访问公钥进行验证，确定第二终端所持有的访问公钥是否为存储第二终端所访问的数据的第一终端的公钥。在这里，上述执行主体可以对第二终端所持有的访问公钥进行解密。然后将解密后的公钥与存储数据标识对应的公钥进行比较，确定解密后的公钥与存储数据标识对应的公钥是否相同。响应于确定解密后的公钥与存储数据标识对应的公钥相同，则确定第二终端所持有的访问公钥为存储第二终端所访问的数据的第一终端的公钥。

[0087] 在本实施中，当上述执行主体确定注册公钥集合中包括第二终端的公钥以及确定

第二终端所持有的访问公钥为存储第二终端所访问的数据的第一终端的公钥时，确定第二终端满足访问条件组。

[0088] 步骤411，响应于确定满足访问条件组，利用第一终端的公钥对所请求访问的数据的存储数据标识加密，确定加密后的所请求访问的数据的存储数据标识与第一终端存储的加密后的存储数据标识是否相同。

[0089] 在本实施例中，根据步骤410确定的第二终端是否满足访问条件组，上述执行主体确定满足访问条件组时，可以利用第一终端的公钥通过现有的公钥加密算法对所请求访问的数据的存储数据标识加密计算。然后，将加密计算后的存储数据标识与步骤407中存储的加密后的存储数据标识进行比较，确定二者是否相同。

[0090] 步骤412，响应于确定加密后的所请求访问的数据的存储数据标识与第一终端存储的加密后的存储数据标识相同，向第二终端发送所述第一终端存储的数据。

[0091] 在本实施例中，当上述执行主体确定所请求访问的数据的存储标识与第一终端存储的数据的存储数据标识相同后，可以直接向第二终端发送第一终端存储的数据。

[0092] 从图4中可以看出，与图2所示的实施例不同的是，本实施例增加了第一终端的公钥注册的步骤以及第二终端访问第一终端存储的数据的步骤，从而提高了终端之间以及终端与执行主体之间的交互的灵活性，进一步提高了数据存储以及数据访问的安全性。

[0093] 进一步参考图5，作为对上述各图所示方法的实现，本申请提供了一种应用于区块链的数据存储装置的一个实施例，该装置实施例与图2所示的方法实施例相对应，该装置具体可以应用于各种电子设备中。

[0094] 如图5所示，本实施例的应用于区块链的数据存储装置500包括：接收单元501、确定单元502以及存储单元503。其中，接收单元501，被配置成接收第一终端发送的数据存储请求，该数据存储请求包括该第一终端的公钥以及待存储的数据。确定单元502，被配置成确定是否满足以下存储条件组：预先存储的注册公钥集合中包括该第一终端的公钥；待存储的数据为有效数据。存储单元503，被配置成响应于确定满足该存储条件组，对待存储的数据进行存储。

[0095] 在本实施例中，应用于区块链的数据存储装置500中：接收单元501、确定单元502以及存储单元503具体实现及其所带来的技术效果可分别参考图2对应实施例中的步骤201、步骤202以及步骤203的相关说明，在此不再赘述。

[0096] 在本实施例的一些可选的实现方式中，应用于区块链的数据存储装置500还包括：公钥注册请求单元(未示出)，被配置成接收该第一终端发送的公钥注册请求，该公钥注册请求包括该第一终端的公钥；加密单元(未示出)，被配置成对该第一终端的公钥进行加密；添加单元(未示出)，被配置成将加密后的公钥添加至该注册公钥集合，以及将加密后的公钥发送至第二终端。

[0097] 在本实施例的一些可选的实现方式中，应用于区块链的数据存储装置500还包括：公钥注册请求单元(未示出)，被配置成接收第一终端发送的公钥注册请求；生成单元(未示出)，被配置成基于公钥注册请求，生成公钥和私钥密钥对；加密单元(未示出)，被配置成将所生成的公钥和私钥密钥对对发送至所述第一终端，以及对所生成的公钥进行加密；添加单元(未示出)，被配置成将加密后的公钥添加至注册公钥集合，以及将加密后的公钥发送至第二终端。

[0098] 在本实施例的一些可选的实现方式中，数据存储请求还包括数字签名；以及确定单元502被配置成：利用该第一终端的公钥对该数字签名进行解密验证，确定该数字签名是否有效；响应于确定该数字签名有效，确定待存储的数据为有效数据。

[0099] 在本实施例的一些可选的实现方式中，数据存储请求还包括存储数据标识；以及添加单元503进一步被配置成：利用该第一终端的公钥对该存储数据标识进行加密；将加密后的存储数据标识作为待存储的数据的主关键字，对加密后的存储数据标识进行存储；响应于确定存储成功，向该第一终端返回存储成功的信息，以及向该第二终端发送存储数据标识。

[0100] 在本实施例的一些可选的实现方式中，应用于区块链的数据存储装置500进一步被配置成：接收该第二终端发送的数据访问请求，其中，该数据访问请求包括该第二终端的公钥、所持有的访问公钥以及所请求访问的数据的存储数据标识；确定是否满足以下访问条件组：该预先存储的注册公钥集合中包括该第二终端的公钥；所持有的访问公钥为该第一终端的公钥；响应于确定满足该访问条件组，利用该第一终端的公钥对所请求访问的数据的存储数据标识加密，确定加密后的所请求访问的数据的存储数据标识与该第一终端存储的加密后的存储数据标识是否相同；响应于确定加密后的所请求访问的数据的存储数据标识与该第一终端存储的加密后的存储数据标识相同，向该第二终端发送该第一终端存储的数据。

[0101] 下面参考图6，其示出了适于用来实现本申请实施例的第一终端设备的计算机系统600的结构示意图。图6示出的第一终端设备仅仅是一个示例，不应对本申请实施例的功能和使用范围带来任何限制。

[0102] 如图6所示，计算机系统600包括中央处理单元(CPU)601，其可以根据存储在只读存储器(ROM)602中的程序或者从存储部分608加载到随机访问存储器(RAM)603中的程序而执行各种适当的动作和处理。在RAM 603中，还存储有系统600操作所需的各种程序和数据。CPU 601、ROM 602以及RAM 603通过总线604彼此相连。输入/输出(I/O)接口605也连接至总线604。

[0103] 以下部件连接至I/O接口605：包括键盘、鼠标等的输入部分606；包括诸如阴极射线管(CRT)、液晶显示器(LCD)等以及扬声器等的输出部分607；包括硬盘等的存储部分608；以及包括诸如LAN卡、调制解调器等的网络接口卡的通信部分609。通信部分609经由诸如因特网的网络执行通信处理。驱动器610也根据需要连接至I/O接口605。可拆卸介质611，诸如磁盘、光盘、磁光盘、半导体存储器等等，根据需要安装在驱动器610上，以便于从其上读出的计算机程序根据需要被安装入存储部分608。

[0104] 特别地，根据本公开的实施例，上文参考流程图描述的过程可以被实现为计算机软件程序。例如，本公开的实施例包括一种计算机程序产品，其包括承载在计算机可读介质上的计算机程序，该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中，该计算机程序可以通过通信部分609从网络上被下载和安装，和/或从可拆卸介质611被安装。在该计算机程序被中央处理单元(CPU)601执行时，执行本申请的方法中限定的上述功能。需要说明的是，本申请所述的计算机可读介质可以是计算机可读信号介质或者计算机可读介质或者是上述两者的任意组合。计算机可读介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算

机可读介质的更具体的例子可以包括但不限于:具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中,计算机可读介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中,计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读介质以外的任何计算机可读介质,该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输,包括但不限于:无线、电线、光缆、RF等等,或者上述的任意合适的组合。

[0105] 可以以一种或多种程序设计语言或其组合来编写用于执行本申请的操作的计算机程序代码,所述程序设计语言包括面向目标的程序设计语言—诸如Java、Smalltalk、C++,还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0106] 附图中的流程图和框图,图示了按照本申请各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上,流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分,该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意,在有些作为替换的实现中,方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如,两个接连地表示的方框实际上可以基本并行地执行,它们有时也可以按相反的顺序执行,这依所涉及的功能而定。也要注意的是,框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合,可以用执行规定的功能或操作的专用的基于硬件的系统来实现,或者可以用专用硬件与计算机指令的组合来实现。

[0107] 描述于本申请实施例中所涉及到的单元可以通过软件的方式实现,也可以通过硬件的方式来实现。所描述的单元也可以设置在处理器中,例如,可以描述为:一种处理器包括接收单元、确定单元和存储单元。其中,这些单元的名称在某种情况下并不构成对该单元本身的限定,例如,接收单元还可以被描述为“接收第一终端发送的数据存储请求的单元”。

[0108] 作为另一方面,本申请还提供了一种计算机可读介质,该计算机可读介质可以是上述实施例中描述的第一终端设备中所包含的;也可以是单独存在,而未装配入该第一终端设备中。上述计算机可读介质承载有一个或者多个程序,当上述一个或者多个程序被该第一终端设备执行时,使得该第一终端设备:接收第一终端发送的数据存储请求,该数据存储请求包括该第一终端的公钥以及待存储的数据;确定是否满足以下存储条件组:预先存储的注册公钥集合中包括该第一终端的公钥;待存储的数据为有效数据;响应于确定满足

该存储条件组，对待存储的数据进行存储。

[0109] 以上描述仅为本申请的较佳实施例以及对所运用技术原理的说明。本领域技术人员应当理解，本申请中所涉及的发明范围，并不限于上述技术特征的特定组合而成的技术方案，同时也应涵盖在不脱离上述发明构思的情况下，由上述技术特征或其等同特征进行任意组合而形成的其它技术方案。例如上述特征与本申请中公开的(但不限于)具有类似功能的技术特征进行互相替换而形成的技术方案。

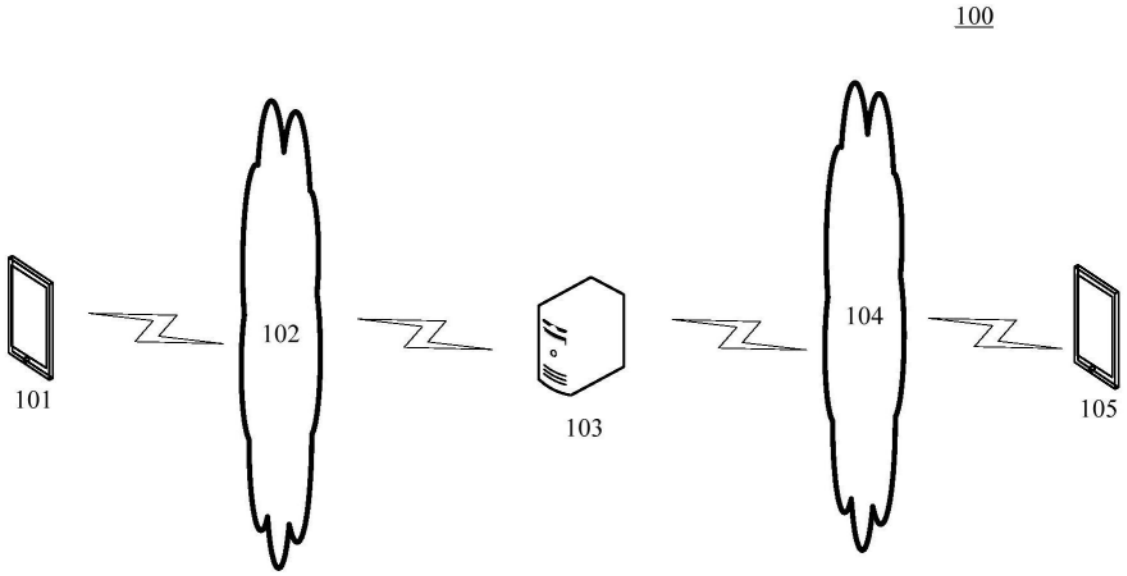

100
101
102
103
104
105

图1

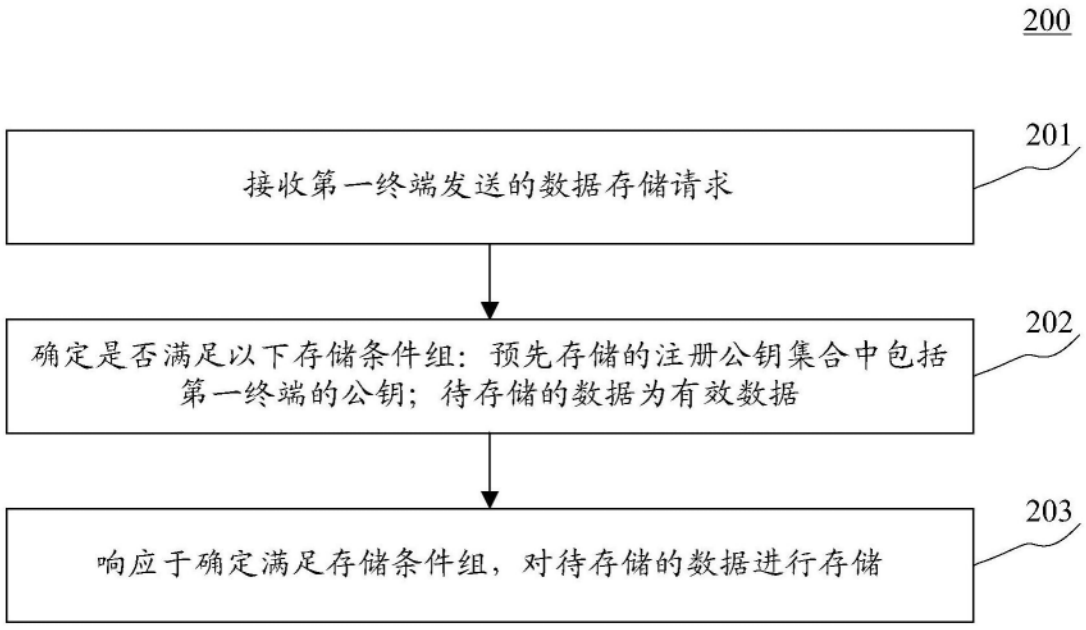

200
接收第一终端发送的数据存储请求
201
确定是否满足以下存储条件组：预先存储的注册公钥集合中包括第一终端的公钥；待存储的数据为有效数据
202
响应于确定满足存储条件组，对待存储的数据进行存储
203

图2

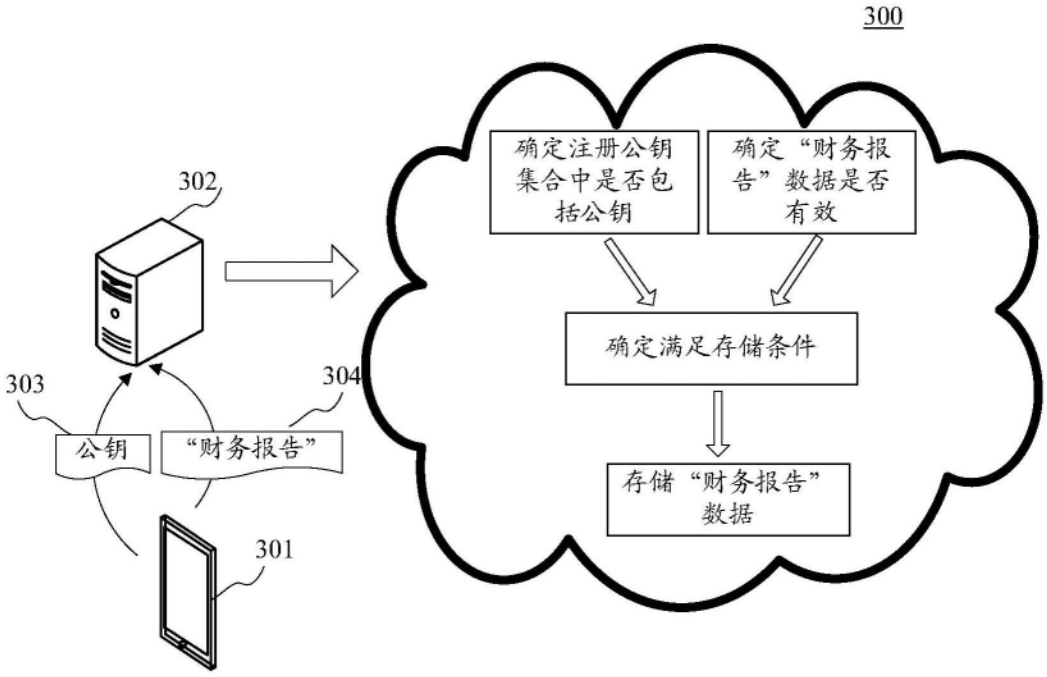

300
确定注册公钥集合中是否包括公钥
确定“财务报告”数据是否有效
确定满足存储条件
存储“财务报告”数据
302
303
304
公钥
“财务报告”
301

图3

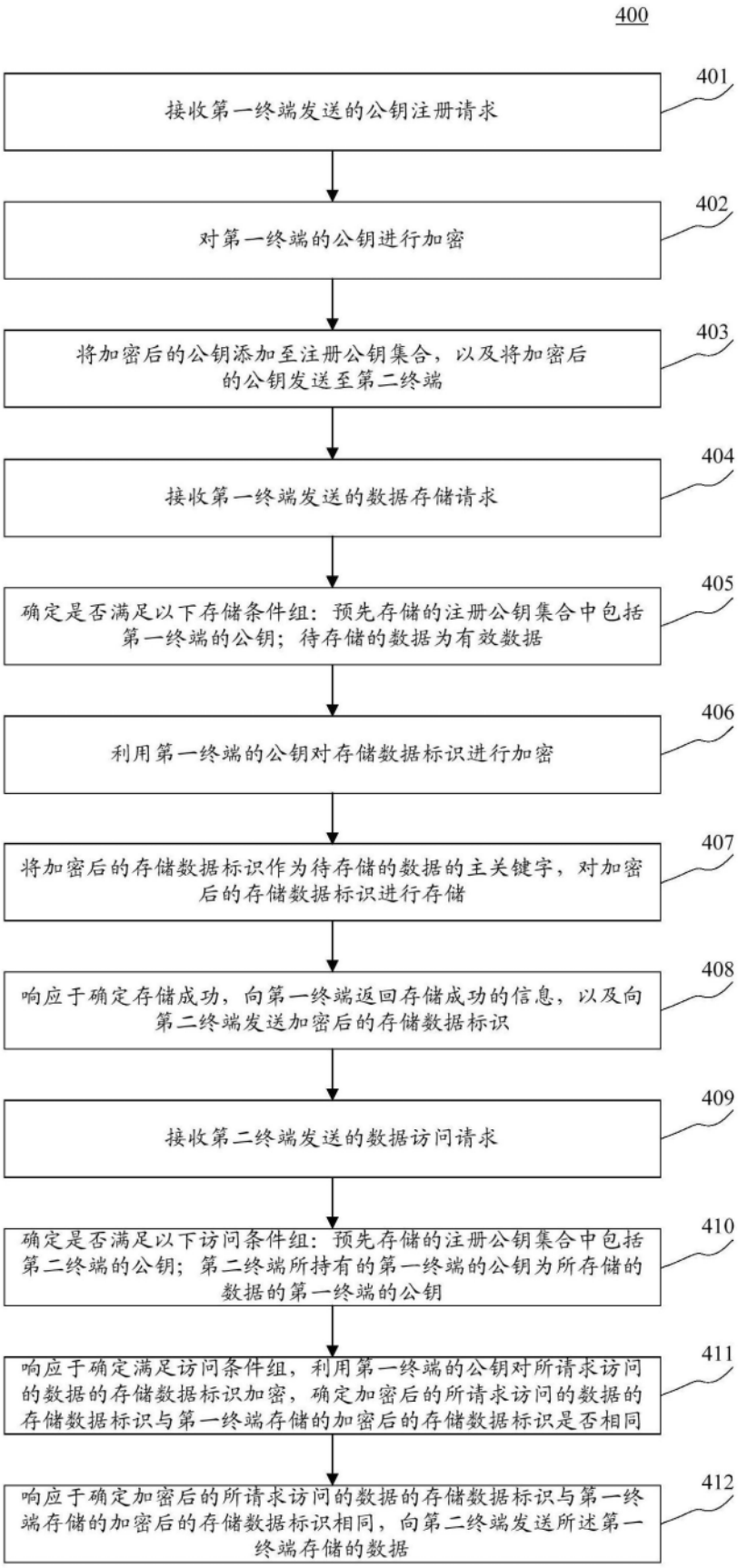

400
401
接收第一终端发送的公钥注册请求
402
对第一终端的公钥进行加密
403
将加密后的公钥添加至注册公钥集合，以及将加密后的公钥发送至第二终端
404
接收第一终端发送的数据存储请求
405
确定是否满足以下存储条件组：预先存储的注册公钥集合中包括第一终端的公钥；待存储的数据为有效数据
406
利用第一终端的公钥对存储数据标识进行加密
407
将加密后的存储数据标识作为待存储的数据的主关键字，对加密后的存储数据标识进行存储
408
响应于确定存储成功，向第一终端返回存储成功的信息，以及向第二终端发送加密后的存储数据标识
409
接收第二终端发送的数据访问请求
410
确定是否满足以下访问条件组：预先存储的注册公钥集合中包括第二终端的公钥；第二终端所持有的第一终端的公钥为所存储的数据的第一终端的公钥
411
响应于确定满足访问条件组，利用第一终端的公钥对所请求访问的数据的存储数据标识加密，确定加密后的所请求访问的数据的存储数据标识与第一终端存储的加密后的存储数据标识是否相同
412
响应于确定加密后的所请求访问的数据的存储数据标识与第一终端存储的加密后的存储数据标识相同，向第二终端发送所述第一终端存储的数据

图4

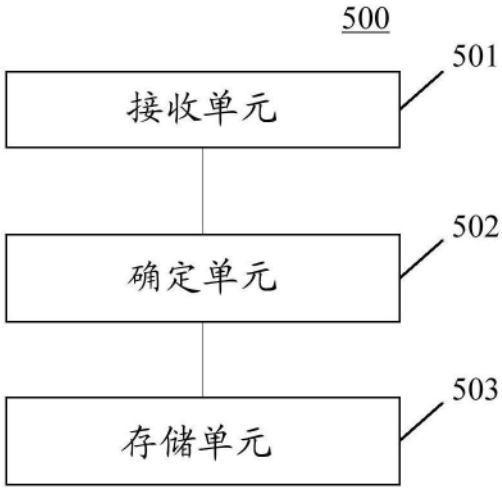

500
501
接收单元
502
确定单元
503
存储单元

图5

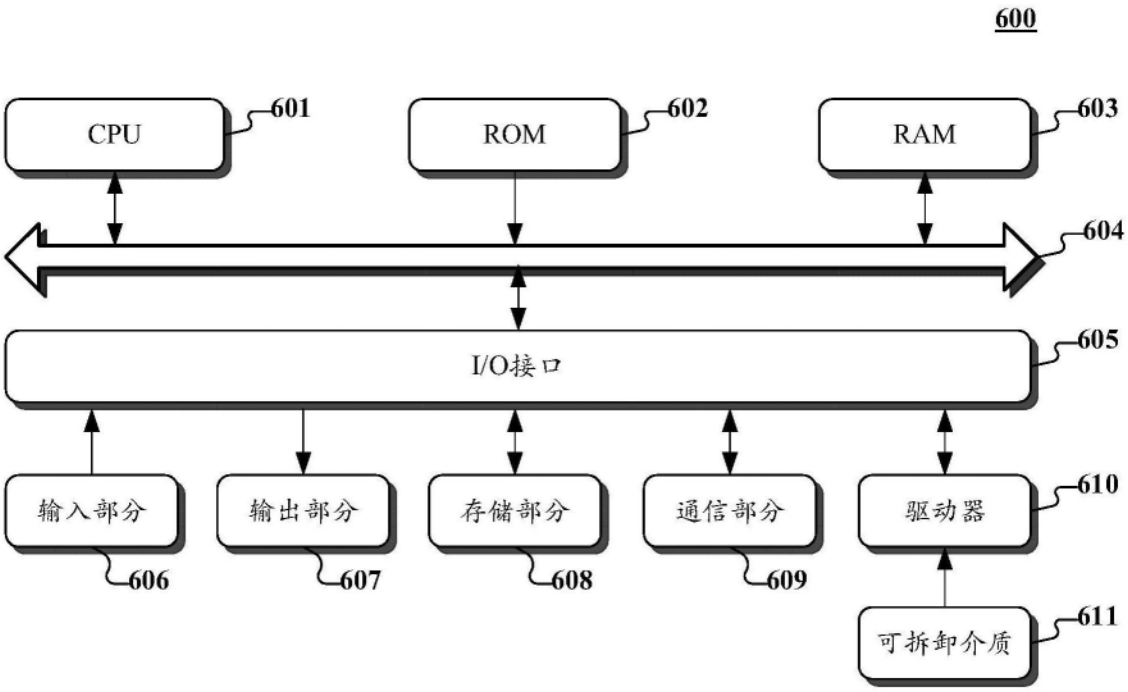

600
CPU
601
ROM
602
RAM
603
604
I/O接口
605
输入部分
606
输出部分
607
存储部分
608
通信部分
609
驱动器
610
可拆卸介质
611

图6