(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115720137 A
(43)申请公布日 2023.02.28

(21)申请号 202110977568.9

(22)申请日 2021.08.24

(71)申请人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 康鑫 朱成康 王海光 李铁岩

(74)专利代理机构 深圳市深佳知识产权代理事务所(普通合伙) 44285
专利代理师 李杭

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

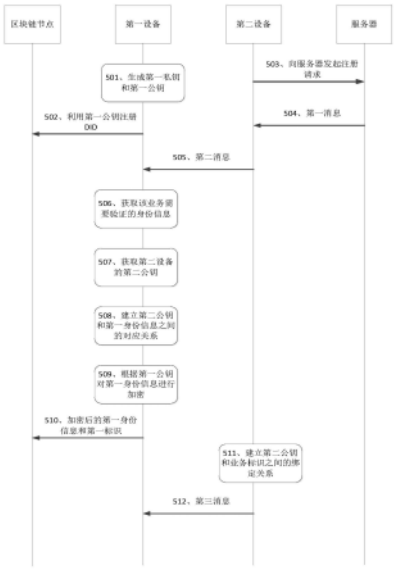
权利要求书8页 说明书28页 附图12页

(54)发明名称

一种信息管理的系统、方法以及装置

(57)摘要

本申请提供一种信息管理的系统，方法以及装置，用户通过第一设备掌握用户的完整的身份信息，第二设备通过不同的第二公钥获取不同业务所需验证的身份信息，加强对用户身份信息的隐私保护。方法包括：第二设备向服务器发起注册请求。服务器向第二设备发送第一业务需要验证的信息的种类和第一业务的标识。第二设备建立第二设备的公钥和第一业务的标识之间的绑定关系。第一设备从第二设备处获取第一业务需要验证的信息的种类，并根据第一业务需要验证的信息的种类，从第一设备本地存储的信息中获取第一业务需要验证的信息，第一业务需要验证的信息和第二设备的公钥之间存在绑定关系。



CN 115720137 A

1.一种身份信息管理的系统,其特征在于,包括:第一设备、第二设备和服务器;

所述第二设备,用于向所述服务器发起注册请求;

所述服务器,用于响应于所述注册请求,向所述第二设备发送第一消息,所述第一消息中携带第一业务需要验证的身份信息的种类和所述第一业务的标识;

所述第二设备,还用于建立所述第二设备的公钥和所述第一业务的标识之间的绑定关系;

所述第一设备,用于从所述第二设备处获取所述第一业务需要验证的身份信息的种类,并根据所述第一业务需要验证的身份信息的种类,从所述第一设备本地存储的身份信息中获取所述第一业务需要验证的身份信息,所述第一业务需要验证的身份信息和所述第二设备的公钥之间存在绑定关系。

2.根据权利要求1所述的系统,其特征在于,所述第一设备,还用于根据所述第一设备的公钥加密所述第一业务需要验证的身份信息。

3.根据权利要求2所述的系统,其特征在于,所述系统还包括区块链节点,

所述第一设备,还用于向所述区块链节点发送加密后的所述第一业务需要验证的身份信息;

所述区块链节点,用于建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

4.根据权利要求2所述的系统,其特征在于,所述第一设备,还用于向所述第二设备发送加密后的所述第一业务需要验证的身份信息;

所述第二设备,还用于建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

5.根据权利要求3或4所述的系统,其特征在于,

所述第一设备,还用于发送了加密后的所述第一业务需要验证的身份信息之后,删除所述第一设备本地存储的加密后的所述第一业务需要验证的身份信息。

6.根据权利要求1至5任一项所述的系统,其特征在于,

所述第一设备,还用于获取用户的生物特征,并根据所述生物特征生成所述第一设备的私钥。

7.根据权利要求1至6任一项所述的系统,其特征在于,

所述第一设备,还用于利用所述第一设备的公钥注册去中心化身份DID。

8.根据权利要求1至7任一项所述的系统,其特征在于,

所述第一设备,还用于生成所述第二设备的私钥和所述第二设备的公钥,并向所述第二设备发送所述第二设备的私钥和所述第二设备的公钥。

9.根据权利要求8所述的系统,其特征在于,

所述第一设备,还用于从所述第二设备处获取所述第一业务的标识;

所述第一设备,具体用于根据所述第一业务的标识、所述第一业务需要验证的身份信息、所述第一设备的私钥生成所述第二设备的私钥。

10.一种身份信息管理的系统,其特征在于,包括:第一设备、第二设备和服务器;

所述第二设备,用于向所述服务器发起访问请求;

所述服务器,用于响应于所述访问请求,向所述第二设备发送身份请求IR消息,所述IR

消息中携带第一业务的标识；

所述第二设备，还用于根据所述第一业务的标识，查找与所述第一业务标识绑定的所述第二设备的公钥；

所述第二设备，还用于利用与所述第二设备的公钥对应的所述第二设备的私钥，生成第二设备的数字签名，并向所述第一设备发送所述第二设备的数字签名以及所述第二设备的公钥；

所述第一设备，用于验证所述第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息；

所述第一设备，还用于根据所述第一设备的私钥生成所述第一设备的数字签名，所述数字签名中携带所述第一业务需要验证的身份信息；

所述服务器，还用于获取所述第一设备的数字签名，验证所述第一设备的数字签名来自所述第一设备后，获取所述第一业务需要验证的身份信息。

11.根据权利要求10所述的系统，其特征在于，所述系统还包括区块链节点；

所述第一设备，具体用于从所述区块链节点处获取与所述第二设备的公钥绑定的加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

12.根据权利要求10所述的系统，其特征在于，

所述第一设备，具体用于从所述第二设备处获取与所述第二设备的公钥绑定的加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

13.根据权利要求10所述的系统，其特征在于，

所述第一设备，具体用于从所述第一设备本地获取加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的身份信息。

14.根据权利要求10至13任一项所述的系统，其特征在于，

所述第一设备，还用于发送了所述第一设备的数字签名后，删除所述第一设备的私钥以及所述第一业务需要验证的身份信息。

15.根据权利要求10至14任一项所述的系统，其特征在于，

所述第一设备，还用于验证所述第二设备的数字签名来自所述第二设备后，获取用户的生物特征，并根据所述生物特征生成所述第一设备的私钥。

16.一种身份信息管理的系统，其特征在于，包括：第一设备、第二设备和服务器；

所述第二设备，用于向所述服务器发起注册请求；

所述服务器，用于响应于所述注册请求，向所述第二设备发送第一消息，所述第一消息中携带第一业务需要验证的身份信息的种类和所述第一业务的标识；

所述第一设备，用于从所述第二设备处获取所述第一业务需要验证的身份信息的种类，并根据所述第一业务需要验证的身份信息的种类，从所述第一设备本地存储的身份信息中获取所述第一业务需要验证的身份信息，所述第一业务需要验证的身份信息和目标密钥绑定，所述目标密钥是基于第一密钥、第二密钥和第三密钥生成的，所述第一密钥是根据所述第一设备获取的用户的生物特征生成的密钥，所述第二密钥是根据所述第一设备的标

识生成的密钥，所述第三密钥是根据第一业务的标识生成的密钥；

所述第一设备，还用于根据所述目标密钥对所述第一业务需要验证的身份信息进行加密处理。

17.根据权利要求16所述的系统，其特征在于，

所述第一设备，还用于删除所述第一密钥、所述第二密钥、所述第三密钥以及所述目标密钥。

18.根据权利要求16或17所述的系统，其特征在于，

所述第二设备，还用于根据所述第一业务的标识生成所述第三密钥，并建立所述第三密钥和所述第一业务的标识之间的绑定关系。

19.一种身份信息管理的系统，其特征在于，包括：第一设备、第二设备和服务器；

所述第二设备，用于向所述服务器发起访问请求；

所述服务器，用于响应于所述访问请求，向所述第二设备发送身份请求IR消息，所述IR消息中携带第一业务的标识；

所述第一设备，用于从所述第二设备处获取所述第一业务的标识；

所述第一设备，还用于根据第一密钥、第二密钥以及第三密钥生成目标密钥，所述第一密钥是根据所述第一设备获取的用户的生物特征生成的密钥，所述第二密钥是根据所述第一设备的标识生成的密钥，所述第三密钥是根据第一业务的标识生成的密钥；

所述第一设备，还用于根据所述目标密钥解密加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的身份信息；

所述第一设备，还用于根据所述服务器的公钥加密所述第一业务需要验证的身份信息，以使所述服务器根据所述服务器的私钥解密后，获取所述第一业务需要验证的身份信息。

20.根据权利要求19所述的系统，其特征在于，

所述第一设备，还用于删除所述第一密钥、所述第二密钥、所述第三密钥以及所述目标密钥。

21.根据权利要求19或20所述的系统，其特征在于，

所述第二设备，还用于获取与所述第一业务的标识绑定的所述第三密钥，并向所述第一设备发送所述第三密钥。

22.一种身份信息管理的方法，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、第二设备和服务器，所述方法包括：

所述第二设备向服务器发起注册请求；

所述第二设备接收所述服务器响应于所述注册请求发送的第一消息，所述第一消息中携带第一业务需要验证的身份信息的种类和所述第一业务的标识；

所述第二设备建立所述第二设备的公钥和所述第一业务的标识之间的绑定关系；

所述第二设备向所述第一设备发送所述第一业务需要验证的身份信息的种类，以使所述第一设备根据所述第一业务需要验证的身份信息的种类，从所述第一设备本地存储的身份信息中获取所述第一业务需要验证的身份信息，所述第一业务需要验证的身份信息和所述第二设备的公钥之间存在绑定关系。

23.根据权利要求22所述的方法，其特征在于，所述方法还包括：

所述第二设备接收所述第一设备发送的加密后的所述第一业务需要验证的身份信息；

所述第二设备建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

24.根据权利要求22或23所述的方法，其特征在于，所述方法还包括：

所述第二设备接收所述第一设备发送的所述第二设备的私钥和所述第二设备的公钥。

25.一种身份信息管理的方法，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、第二设备和服务器，所述方法包括：

所述第一设备从所述第二设备处获取第一业务需要验证的身份信息的种类，并根据所述第一业务需要验证的身份信息的种类，从所述第一设备本地存储的身份信息中获取所述第一业务需要验证的身份信息，所述第一业务需要验证的身份信息和所述第二设备的公钥之间存在绑定关系。

26.根据权利要求25所述的方法，其特征在于，所述方法还包括：

所述第一设备建立所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

27.根据权利要求25所述的方法，其特征在于，所述方法还包括：

所述第一设备根据所述第一设备的公钥加密所述第一业务需要验证的身份信息。

28.根据权利要求27所述的方法，其特征在于，所述系统还包括区块链节点，所述方法还包括：

所述第一设备向所述区块链节点发送加密后的所述第一业务需要验证的身份信息，以使所述区块链节点建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

29.根据权利要求27所述的方法，其特征在于，所述方法还包括：

所述第一设备向所述第二设备发送加密后的所述第一业务需要验证的身份信息，以使所述第二设备建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

30.根据权利要求28或29所述的方法，其特征在于，所述方法还包括：

所述第一设备发送了加密后的所述第一业务需要验证的身份信息之后，删除所述第一设备本地存储的加密后的所述第一业务需要验证的身份信息。

31.根据权利要求25至30任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备获取用户的生物特征，并根据所述生物特征生成所述第一设备的私钥。

32.根据权利要求25至31任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备利用所述第一设备的公钥注册去中心化身份DID。

33.根据权利要求25至32任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备生成所述第二设备的私钥和所述第二设备的公钥，并向所述第二设备发送所述第二设备的私钥和所述第二设备的公钥。

34.根据权利要求25至32任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备从所述第二设备处获取所述第一业务的标识；

所述第一设备生成所述第二设备的私钥，包括：

所述第一设备根据所述第一业务的标识、所述第一业务需要验证的身份信息、所述第

一设备的私钥生成所述第二设备的私钥。

35.一种第二设备，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、所述第二设备和服务器，所述第二设备包括：

收发模块，用于向服务器发起注册请求；

所述收发模块，还用于接收所述服务器响应于所述注册请求发送的第一消息，所述第一消息中携带第一业务需要验证的身份信息的种类和所述第一业务的标识；

处理模块，用于建立所述第二设备的公钥和所述第一业务的标识之间的绑定关系；

所述收发模块，还用于向所述第一设备发送所述第一业务需要验证的身份信息的种类，以使所述第一设备根据所述第一业务需要验证的身份信息的种类，从所述第一设备本地存储的身份信息中获取所述第一业务需要验证的身份信息，所述第一业务需要验证的身份信息和所述第二设备的公钥之间存在绑定关系。

36.根据权利要求35所述的第二设备，其特征在于，

所述收发模块，还用于接收所述第一设备发送的加密后的所述第一业务需要验证的身份信息；

所述处理模块，还用于建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

37.根据权利要求35或36所述的第二设备，其特征在于，

所述收发模块，还用于接收所述第一设备发送的所述第二设备的私钥和所述第二设备的公钥。

38.一种第一设备，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括所述第一设备、第二设备和服务器，所述第一设备包括：

收发模块，用于从所述第二设备处获取第一业务需要验证的身份信息的种类，并根据所述第一业务需要验证的身份信息的种类，从所述第一设备的存储模块中获取所述第一业务需要验证的身份信息，所述第一业务需要验证的身份信息和所述第二设备的公钥之间存在绑定关系。

39.根据权利要求38所述的第一设备，其特征在于，所述设备还包括处理模块，用于：

建立所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

40.根据权利要求39所述的第一设备，其特征在于，所述处理模块，还用于：

根据所述第一设备的公钥加密所述第一业务需要验证的身份信息。

41.根据权利要求40所述的第一设备，其特征在于，所述系统还包括区块链节点，所述收发模块，还用于：

向所述区块链节点发送加密后的所述第一业务需要验证的身份信息，以使所述区块链节点建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

42.根据权利要求40所述的第一设备，其特征在于，所述收发模块，还用于：

所述第一设备向所述第二设备发送加密后的所述第一业务需要验证的身份信息，以使所述第二设备建立所述加密后的所述第一业务需要验证的身份信息和所述第二设备的公钥之间的绑定关系。

43.根据权利要求41或42所述的第一设备，其特征在于，所述处理模块，还用于：

所述第一设备发送了加密后的所述第一业务需要验证的身份信息之后，删除所述第一设备本地存储的加密后的所述第一业务需要验证的身份信息。

44.根据权利要求38至43任一项所述的第一设备，其特征在于，所述处理模块，还用于：

根据用户的生物特征生成所述第一设备的私钥。

45.根据权利要求38至43任一项所述的第一设备，其特征在于，所述处理模块，还用于：

利用所述第一设备的公钥注册去中心化身份DID。

46.根据权利要求38至45任一项所述的第一设备，其特征在于，所述处理模块，还用于：

生成所述第二设备的私钥和所述第二设备的公钥；

所述收发模块，还用于向所述第二设备发送所述第二设备的私钥和所述第二设备的公钥。

47.根据权利要求38至46任一项所述的第一设备，其特征在于，所述收发模块，还用于：

从所述第二设备处获取所述第一业务的标识；

所述处理模块，具体用于根据所述第一业务的标识、所述第一业务需要验证的身份信息、所述第一设备的私钥生成所述第二设备的私钥。

48.一种身份信息管理的方法，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、第二设备和服务器，所述方法包括：

所述第二设备向所述服务器发起访问请求；

所述第二设备接收所述服务器响应于所述访问请求发送的身份请求IR消息，所述IR消息中携带第一业务的标识；

所述第二设备根据所述第一业务的标识，查找与所述第一业务标识绑定的所述第二设备的公钥；

所述第二设备利用与所述第二设备的公钥对应的所述第二设备的私钥，生成第二设备的数字签名，并向所述第一设备发送所述第二设备的数字签名以及所述第二设备的公钥，以使所述第一设备验证所述第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息。

49.一种身份信息管理的方法，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、第二设备和服务器，所述方法包括：

所述第一设备验证第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息；

所述第一设备根据所述第一设备的私钥生成所述第一设备的数字签名，所述数字签名中携带所述第一业务需要验证的身份信息。

50.根据权利要求49所述的方法，其特征在于，所述系统还包括区块链节点，所述第一设备验证第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息，包括：

所述第一设备验证第二设备的数字签名来自所述第二设备后，从所述区块链节点处获取与所述第二设备的公钥绑定的加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

51.根据权利要求49所述的方法，其特征在于，所述第一设备验证第二设备的数字签名

来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息，包括：

所述第一设备验证第二设备的数字签名来自所述第二设备后，从所述第二设备处获取与所述第二设备的公钥绑定的加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

52.根据权利要求49所述的方法，其特征在于，所述第一设备验证第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息，包括：

所述第一设备验证第二设备的数字签名来自所述第二设备后，从所述第一设备本地获取加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

53.根据权利要求49至52任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备发送了所述第一设备的数字签名后，删除所述第一设备的私钥以及所述第一业务需要验证的身份信息。

54.根据权利要求49至53任一项所述的方法，其特征在于，所述方法还包括：

所述第一设备验证所述第二设备的数字签名来自所述第二设备后，获取用户的生物特征，并根据所述生物特征生成所述第一设备的私钥。

55.一种第二设备，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、所述第二设备和服务器，所述第二设备，包括：

收发模块，用于向所述服务器发起访问请求；

所述收发模块，还用于接收所述服务器响应于所述访问请求发送的身份请求IR消息，所述IR消息中携带第一业务的标识；

处理模块，用于根据所述第一业务的标识，查找与所述第一业务标识绑定的所述第二设备的公钥；

所述处理模块，还用于利用与所述第二设备的公钥对应的所述第二设备的私钥，生成第二设备的数字签名；

所述收发模块，还用于向所述第一设备发送所述第二设备的数字签名以及所述第二设备的公钥，以使所述第一设备验证所述第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息。

56.一种第一设备，其特征在于，应用于身份信息管理系统，所述身份信息管理系统包括第一设备、第二设备和服务器，所述第一设备包括：

处理模块，用于验证第二设备的数字签名来自所述第二设备后，获取与所述第二设备的公钥绑定的所述第一业务需要验证的身份信息；

所述处理模块，还用于根据所述第一设备的私钥生成所述第一设备的数字签名，所述数字签名中携带所述第一业务需要验证的身份信息。

57.根据权利要求56所述的第一设备，其特征在于，所述系统还包括区块链节点，所述处理模块，具体用于：

验证第二设备的数字签名来自所述第二设备后，从所述区块链节点处获取与所述第二

设备的公钥绑定的加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

58.根据权利要求56所述的第一设备，其特征在于，所述处理模块，具体用于：

验证第二设备的数字签名来自所述第二设备后，从所述第二设备处获取与所述第二设备的公钥绑定的加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

59.根据权利要求56所述的第一设备，其特征在于，所述处理模块，具体用于：

所述第一设备验证第二设备的数字签名来自所述第二设备后，从所述第一设备本地获取加密后的所述第一业务需要验证的身份信息，根据所述第一设备的私钥解密所述加密后的所述第一业务需要验证的身份信息，以获取所述第一业务需要验证的的身份信息。

60.根据权利要求56至59任一项所述的第一设备，其特征在于，所述处理模块，还用于：

所述收发模块发送了所述第一设备的数字签名后，删除所述第一设备的私钥以及所述第一业务需要验证的身份信息。

61.根据权利要求56至60任一项所述的第一设备，其特征在于，所述处理模块，还用于：

验证所述第二设备的数字签名来自所述第二设备后，获取用户的生物特征，并根据所述生物特征生成所述第一设备的私钥。

62.一种第二设备，其特征在于，包括处理器，所述处理器和存储器耦合，所述存储器存储有程序，当所述存储器存储的程序指令被所述处理器执行时实现权利要求22至24中任一项所述的方法，或者实现权利要求48所述的方法。

63.一种第一设备，其特征在于，包括处理器，所述处理器和存储器耦合，所述存储器存储有程序，当所述存储器存储的程序指令被所述处理器执行时实现权利要求25至34中任一项所述的方法，或者实现权利要求49至54中任一项所述的方法。

64.一种计算机可读存储介质，包括程序，当其被处理单元所执行时，执行如权利要求22至24中任一项所述的方法，或者实现权利要求48所述的方法。

65.一种计算机可读存储介质，包括程序，当其被处理单元所执行时，执行如权利要求25至34中任一项所述的方法，或者实现权利要求49至54中任一项所述的方法。

66.一种计算机程序产品，包括计算机程序/指令，其特征在于，所述计算机程序/指令被处理器执行时实现如权利要求22至24中任一项所述的方法，或者实现权利要求48所述的方法。

67.一种计算机程序产品，包括计算机程序/指令，其特征在于，所述计算机程序/指令被处理器执行时实现如权利要求25至34中任一项所述的方法，或者实现权利要求49至54中任一项所述的方法。

一种信息管理的系统、方法以及装置

技术领域

[0001] 本申请涉及人工智能安全领域，尤其涉及一种图像处理的方法以及装置。

背景技术

[0002] 随着网络活动的普遍化和多样化，各种身份充斥在网络空间中，对网络身份的管理面临很多严峻的问题。

[0003] 网络身份管理不当引起的身份信息泄露、网络欺诈、网络银行资金的窃取等现象频繁发生，给人们的生命、财产安全带来巨大隐患。此外，社会活动的数字化，使得个人敏感的身份数据遍布在多个不同的网络应用中，越来越多的企业兼具身份管理的角色，是否能对身份信息进行安全有效管理，身份管理服务是否值得信赖等问题引起广泛关注。

发明内容

[0004] 本申请实施例提供一种身份信息管理的系统、方法以及装置，针对于每个业务所需验证的身份信息不同，生成不同的业务身份，对用户的数据隐私和安全进行有效保护。

[0005] 有鉴于此，本申请第一方面提供一种身份信息管理的系统，包括：第一设备、第二设备和服务器。第二设备，用于向服务器发起注册请求。服务器，用于响应于注册请求，向第二设备发送第一消息，第一消息中携带第一业务需要验证的身份信息的种类和第一业务的标识。第二设备，还用于建立第二设备的公钥和第一业务的标识之间的绑定关系。第一设备，用于从第二设备处获取第一业务需要验证的身份信息的种类，并根据第一业务需要验证的身份信息的种类，从第一设备本地存储的身份信息中获取第一业务需要验证的身份信息，第一业务需要验证的身份信息和第二设备的公钥之间存在绑定关系。

[0006] 本申请实施例中，用户通过第一设备掌握用户的完整的身份信息，除第一设备之外的其他设备无法获取用户的完整身份信息，加强对用户身份信息的隐私保护。此外，针对于每个业务所需验证的身份信息的不同，通过不同的第二设备的公钥与不同业务所需验证的身份信息进行绑定。相当于，为每一个主身份设置了多个从属身份，每个从属身份对应一个第二设备的公钥，每个从属身份用于访问一种服务。每个服务只能获取其需要验证的身份信息，无法获取用户的完整身份信息，进一步加强对用户身份信息的隐私保护。

[0007] 在第一方面的第一种可能的实施方式中，系统还包括区块链节点。第一设备，还用于向区块链节点发送加密后的第一业务需要验证的身份信息。区块链节点，用于建立加密后的第一业务需要验证的身份信息和第二设备的公钥之间的绑定关系。在这种实施方式中，将第一业务需要验证的身份信息保存在区块链节点上。由区块链节点维护第一业务需要验证的身份信息，保证第一业务需要验证的身份信息不被篡改，增加了方案的稳定性。

[0008] 在第一方面的第一种可能的实施方式中，第一设备，还用于向第二设备发送加密后的第一业务需要验证的身份信息。第二设备，还用于建立加密后的第一业务需要验证的身份信息和第二设备的公钥之间的绑定关系。在这种实施方式中，在第二设备上保存第一业务需要验证的身份信息，节约区块链的存储资源和通信资源，由于第二设备通常是手机，

安全性能更高，将加密后的第一身份信息存储在手机中，可以提升身份信息的安全性。

[0009] 在第一方面的第一种可能的实施方式中，第一设备，还用于发送了加密后的第一业务需要验证的身份信息之后，删除第一设备本地存储的加密后的第一业务需要验证的身份信息。在这种实施方式中，当注册完成后，已经在第二设备或者区块链上保存了加密后的第一业务需要验证的身份信息之后，可以删除第一设备本地存储的加密后的第一业务，以节约第一设备本地的存储资源。

[0010] 在第一方面的第一种可能的实施方式中，第一设备，还用于获取用户的生物特征，并根据生物特征生成第一设备的私钥。在这种实施方式中，可以根据用户的生物特征生成第一设备的私钥，使第一设备无需在本地保存第一设备的私钥，并且当第一设备丢失后，也不会面临私钥随之丢失的风险。

[0011] 在第一方面的第一种可能的实施方式中，第一设备，还用于利用第一设备的公钥注册去中心化身份DID。在这种实施方式中，在本申请实施例中，通过第一公钥注册DID，使第一公钥与唯一的DID进行绑定，当服务器方获取了DID之后，可以根据DID查询到第一公钥，并基于第一公钥验证身份，比如验证接收到的数字签名来自第一设备。如果不同的第一设备采用了相同的第一公钥，可能导致根据该多个不同的第一设备获取的DID是相同的。为了使每一个第一设备都能够具有唯一的DID，所以第一设备获取了DID之后，区块链还会对该获取的DID进行查重，如果当前区块链上没有存储过相同的DID，则认为注册成功，将第一公钥绑定唯一的DID。

[0012] 在第一方面的第一种可能的实施方式中，第一设备，还用于生成第二设备的私钥和第二设备的公钥，并向第二设备发送第二设备的私钥和第二设备的公钥。

[0013] 在第一方面的第一种可能的实施方式中，第一设备，还用于从第二设备处获取第一业务的标识。第一设备，具体用于根据第一业务的标识、第一业务需要验证的身份信息、第一设备的私钥生成第二设备的私钥。

[0014] 第二方面，本申请实施例提供一种身份信息管理的系统，包括：第一设备、第二设备和服务器。第二设备，用于向服务器发起访问请求。服务器，用于响应于访问请求，向第二设备发送身份请求IR消息，IR消息中携带第一业务的标识。第二设备，还用于根据第一业务的标识，查找与第一业务标识绑定的第二设备的公钥。第二设备，还用于利用与第二设备的公钥对应的第二设备的私钥，生成第二设备的数字签名，并向第一设备发送第二设备的数字签名以及第二设备的公钥。第一设备，用于验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的身份信息。第一设备，还用于根据第一设备的私钥生成第一设备的数字签名，数字签名中携带第一业务需要验证的身份信息。服务器，还用于获取第一设备的数字签名，验证第一设备的数字签名来自第一设备后，获取第一业务需要验证的身份信息。

[0015] 在第二方面的第一种可能的实施方式中，系统还包括区块链节点。第一设备，具体用于从区块链节点处获取与第二设备的公钥绑定的加密后的第一业务需要验证的身份信息，根据第一设备的私钥解密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的的身份信息。

[0016] 在第二方面的第一种可能的实施方式中，第一设备，具体用于从第二设备处获取与第二设备的公钥绑定的加密后的第一业务需要验证的身份信息，根据第一设备的私钥解

密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的的身份信息。

[0017] 在第二方面的第一种可能的实施方式中，第一设备，具体用于从第一设备本地获取加密后的第一业务需要验证的身份信息，根据第一设备的私钥解密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的的身份信息。

[0018] 在第二方面的第一种可能的实施方式中，第一设备，还用于发送了第一设备的数字签名后，删除第一设备的私钥以及第一业务需要验证的身份信息。

[0019] 在第二方面的第一种可能的实施方式中，第一设备，还用于验证第二设备的数字签名来自第二设备后，获取用户的生物特征，并根据生物特征生成第一设备的私钥。

[0020] 第三方面本申请实施例提供一种身份信息管理的系统，包括：第一设备、第二设备和服务器。第二设备，用于向服务器发起注册请求。服务器，用于响应于注册请求，向第二设备发送第一消息，第一消息中携带第一业务需要验证的身份信息的种类和第一业务的标识。第一设备，用于从第二设备处获取第一业务需要验证的身份信息的种类，并根据第一业务需要验证的身份信息的种类，从第一设备本地存储的身份信息中获取第一业务需要验证的身份信息，第一业务需要验证的身份信息和目标密钥绑定，目标密钥是基于第一密钥、第二密钥和第三密钥生成的，第一密钥是根据第一设备获取的用户的生物特征生成的密钥，第二密钥是根据第一设备的标识生成的密钥，第三密钥是根据第一业务的标识生成的密钥。第一设备，还用于根据目标密钥对第一业务需要验证的身份信息进行加密处理。

[0021] 在第三方面的第一种可能的实施方式中，第一设备，还用于删除第一密钥、第二密钥、第三密钥以及目标密钥。

[0022] 在第三方面的第一种可能的实施方式中，第二设备，还用于根据第一业务的标识生成第三密钥，并建立第三密钥和第一业务的标识之间的绑定关系。

[0023] 本申请第四方面提供提供一种身份信息管理系统，包括：第一设备、第二设备和服务器。第二设备，用于向服务器发起访问请求。服务器，用于响应于访问请求，向第二设备发送身份请求IR消息，IR消息中携带第一业务的标识。第一设备，用于从第二设备处获取第一业务的标识。第一设备，还用于根据第一密钥、第二密钥以及第三密钥生成目标密钥，第一密钥是根据第一设备获取的用户的生物特征生成的密钥，第二密钥是根据第一设备的标识生成的密钥，第三密钥是根据第一业务的标识生成的密钥。第一设备，还用于根据目标密钥解密加密后的第一业务需要验证的身份信息，一获取第一业务需要验证的身份信息。第一设备，还用根据服务器的公钥加密第一业务需要验证的身份信息，以使服务器根据服务器的私钥解密后，获取第一业务需要验证的身份信息。

[0024] 在第四方面的第一种可能的实施方式中，第一设备，还用于删除第一密钥、第二密钥、第三密钥以及目标密钥。

[0025] 在第四方面的第一种可能的实施方式中，第二设备，还用于获取与第一业务的标识绑定的第三密钥，并向第一设备发送第三密钥。

[0026] 第五方面本申请实施例提供的一种身份信息管理的方法，应用于身份信息管理系统，身份信息管理系统包括第一设备、第二设备和服务器，方法包括：第二设备向服务器发起注册请求。第二设备接收服务器响应于注册请求发送的第一消息，第一消息中携带第一业务需要验证的身份信息的种类和第一业务的标识。第二设备建立第二设备的公钥和第一业务的标识之间的绑定关系。第二设备向第一设备发送第一业务需要验证的身份信息的种

类,以使第一设备根据第一业务需要验证的身份信息的种类,从第一设备本地存储的身份信息中获取第一业务需要验证的身份信息,第一业务需要验证的身份信息和第二设备的公钥之间存在绑定关系。

[0027] 在第五方面的第一种可能的实施方式中,该方法还包括:第二设备接收第一设备发送的加密后的第一业务需要验证的身份信息。第二设备建立加密后的第一业务需要验证的身份信息和第二设备的公钥之间的绑定关系。

[0028] 在第五方面的第一种可能的实施方式中,该方法还包括:第二设备接收第一设备发送的第二设备的私钥和第二设备的公钥。

[0029] 在第五方面的第一种可能的实施方式中,该应用于身份信息管理系统,身份信息管理系统包括第一设备、第二设备和服务器,方法包括:第一设备从第二设备处获取第一业务需要验证的身份信息的种类,并根据第一业务需要验证的身份信息的种类,从第一设备本地存储的身份信息中获取第一业务需要验证的身份信息,第一业务需要验证的身份信息和第二设备的公钥之间存在绑定关系。

[0030] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备建立第一业务需要验证的身份信息和第二设备的公钥之间的绑定关系。

[0031] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备根据第一设备的公钥加密第一业务需要验证的身份信息。

[0032] 在第五方面的第一种可能的实施方式中,该系统还包括区块链节点,该方法还包括:第一设备向区块链节点发送加密后的第一业务需要验证的身份信息,以使区块链节点建立加密后的第一业务需要验证的身份信息和第二设备的公钥之间的绑定关系。

[0033] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备向第二设备发送加密后的第一业务需要验证的身份信息,以使第二设备建立加密后的第一业务需要验证的身份信息和第二设备的公钥之间的绑定关系。

[0034] 在第五方面的第一种可能的实施方式中,该方法还包括:述第一设备发送了加密后的第一业务需要验证的身份信息之后,删除第一设备本地存储的加密后的第一业务需要验证的身份信息。

[0035] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备获取用户的生物特征,并根据生物特征生成第一设备的私钥。

[0036] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备利用第一设备的公钥注册去中心化身份DID。

[0037] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备生成第二设备的私钥和第二设备的公钥,并向第二设备发送第二设备的私钥和第二设备的公钥。

[0038] 在第五方面的第一种可能的实施方式中,该方法还包括:第一设备从第二设备处获取第一业务的标识。第一设备生成第二设备的私钥,包括:第一设备根据第一业务的标识、第一业务需要验证的身份信息、第一设备的私钥生成第二设备的私钥。

[0039] 本申请实施例第六方面提供一种身份信息管理的方法,应用于身份信息管理系统,身份信息管理系统包括第一设备、第二设备和服务器,该方法,包括:第二设备向服务器发起访问请求。第二设备接收服务器响应于访问请求发送的身份请求IR消息,IR消息中携带第一业务的标识。第二设备根据第一业务的标识,查找与第一业务标识绑定的第二设备

的公钥。第二设备利用与第二设备的公钥对应的第二设备的私钥，生成第二设备的数字签名，并向第一设备发送第二设备的数字签名以及第二设备的公钥，以使第一设备验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的身份信息。

[0040] 在第六方面的第一种可能的实施方式中，应用于身份信息管理系统，身份信息管理系统包括第一设备、第二设备和服务器，该方法，包括：第一设备验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的身份信息。第一设备根据第一设备的私钥生成第一设备的数字签名，数字签名中携带第一业务需要验证的身份信息。

[0041] 在第六方面的第一种可能的实施方式中，系统还包括区块链节点，第一设备验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的身份信息，包括：第一设备验证第二设备的数字签名来自第二设备后，从区块链节点处获取与第二设备的公钥绑定的加密后的第一业务需要验证的身份信息，根据第一设备的私钥解密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的的身份信息。

[0042] 在第六方面的第一种可能的实施方式中，第一设备验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的身份信息，包括：第一设备验证第二设备的数字签名来自第二设备后，从第二设备处获取与第二设备的公钥绑定的加密后的第一业务需要验证的身份信息，根据第一设备的私钥解密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的的身份信息。

[0043] 在第六方面的第一种可能的实施方式中，第一设备验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的身份信息，包括：第一设备验证第二设备的数字签名来自第二设备后，从第一设备本地获取加密后的第一业务需要验证的身份信息，根据第一设备的私钥解密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的的身份信息。

[0044] 在第六方面的第一种可能的实施方式中，该方法还包括：第一设备发送了第一设备的数字签名后，删除第一设备的私钥以及第一业务需要验证的身份信息。

[0045] 在第六方面的第一种可能的实施方式中，该方法还包括第一设备验证第二设备的数字签名来自第二设备后，获取用户的生物特征，并根据生物特征生成第一设备的私钥。

[0046] 本申请实施例第七方面提供一种身份信息管理的方法，应用于身份信息管理系统，身份信息管理系统包括第一设备、第二设备和服务器，该方法，包括：第二设备向服务器发起注册请求。第二设备接收服务器发送的第一消息，第一消息中携带第一业务需要验证的身份信息的种类和第一业务的标识。

[0047] 本申请实施例第八方面提供一种身份信息管理的方法，应用于身份信息管理系统，身份信息管理系统包括第一设备、第二设备和服务器，该方法，包括：第一设备从第二设备处获取第一业务需要验证的身份信息的种类，并根据第一业务需要验证的身份信息的种类，从第一设备本地存储的身份信息中获取第一业务需要验证的身份信息，第一业务需要验证的身份信息和目标密钥绑定，目标密钥是基于第一密钥、第二密钥和第三密钥生成的，第一密钥是根据第一设备获取的用户的生物特征生成的密钥，第二密钥是根据第一设备的标识生成的密钥，第三密钥是根据第一业务的标识生成的密钥。第一设备根据目标密钥对

第一业务需要验证的身份信息进行加密处理。

[0048] 本申请实施例第九方面提供一种身份信息管理的方法，应用于身份信息管理系统，身份信息管理系统包括第一设备、第二设备和服务器，该方法包括：第二设备向服务器发起访问请求。第二设备接收服务器发送的身份请求IR消息，IR消息中携带第一业务的标识。第二设备向第一设备发送第一业务的标识。

[0049] 本申请实施例第十方面提供一种身份信息管理的方法，应用于身份信息管理系统，身份信息管理系统包括第一设备、第二设备和服务器，该方法包括：第一设备从第二设备处获取第一业务的标识。第一设备根据第一密钥、第二密钥以及第三密钥生成目标密钥，第一密钥是根据第一设备获取的用户的生物特征生成的密钥，第二密钥是根据第一设备的标识生成的密钥，第三密钥是根据第一业务的标识生成的密钥。第一设备根据目标密钥解密加密后的第一业务需要验证的身份信息，以获取第一业务需要验证的身份信息。第一设备根据服务器的公钥加密第一业务需要验证的身份信息，以使服务器根据服务器的私钥解密后，获取第一业务需要验证的身份信息。

[0050] 第十一方面，本申请实施例提供一种第二设备，该第二设备具有实现上述第五方面或第七方面或第九方面描述的方法中第二设备的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

[0051] 第十二方面，本申请实施例提供一种第一设备，该第二设备具有实现上述第六方面或第八方面或第十方面描述的方法中第一设备的功能。该功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。该硬件或软件包括一个或多个与上述功能相对应的模块。

[0052] 第十三方面，本申请实施例提供一种第二设备，包括：处理器和存储器，其中，处理器和存储器通过线路互联，处理器调用存储器中的程序代码用于执行上述第五方面或第七方面或第九方面任一项所示的方法中与处理相关的功能。可选地，该归属设备可以是芯片。

[0053] 第十四方面，本申请实施例提供一种第一设备，包括：处理器和存储器，其中，处理器和存储器通过线路互联，处理器调用存储器中的程序代码用于执行上述第六方面或第八方面或第十方面任一项所示的方法中与处理相关的功能。可选地，该归属设备可以是芯片。

[0054] 第十五方面，本申请实施例提供了一种装置，该装置也可以称为数字处理芯片或者芯片，芯片包括处理单元和通信接口，处理单元通过通信接口获取程序指令，程序指令被处理单元执行，处理单元用于执行如上述第五方面或第七方面或第九方面任一可选实施方式中与处理相关的功能。

[0055] 第十六方面，本申请实施例提供了一种装置，该装置也可以称为数字处理芯片或者芯片，芯片包括处理单元和通信接口，处理单元通过通信接口获取程序指令，程序指令被处理单元执行，处理单元用于执行如上述第六方面或第八方面或第十方面任一可选实施方式中与处理相关的功能。

[0056] 第十七方面，本申请实施例提供了一种计算机可读存储介质，包括指令，当其在计算机上运行时，使得计算机执行上述第五方面或第七方面或第九方面任一可选实施方式中的方法。

[0057] 第十八方面，本申请实施例提供了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上述第六方面或第八方面或第十方面任一可选实施方式中的方法。

附图说明

[0058] 图1为生成数字签名以及验证数字签名的流程示意图；

[0059] 图2为本申请实施例提供的一种身份管理系统的架构示意图；

[0060] 图3为本申请实施例提供的另一种身份管理系统的架构示意图；

[0061] 图4为本申请实施例提供的一种典型的应用场景的示意图；

[0062] 图5为本申请实施例提供的一种信息管理方法的流程示意图；

[0063] 图6为本申请实施例提供的另一种信息管理方法的流程示意图；

[0064] 图7为本申请实施例提供的另一种信息管理方法的流程示意图；

[0065] 图8为本申请实施例提供的另一种信息管理方法的流程示意图；

[0066] 图9为本申请实施例提供的另一种信息管理方法的流程示意图；

[0067] 图10为本申请实施例提供的另一种信息管理方法的流程示意图；

[0068] 图11为本申请实施例提供的另一种信息管理方法的流程示意图；

[0069] 图12为本申请实施例提供的另一种信息管理方法的流程示意图；

[0070] 图13为本申请实施例提供的一种第二设备的结构示意图；

[0071] 图14为本申请实施例提供的一种第一设备的结构示意图；

[0072] 图15为本申请实施例提供的另一种第二设备的结构示意图；

[0073] 图16为本申请实施例提供的另一种第一设备的结构示意图；

[0074] 图17为本申请实施例提供的一种服务器的结构示意图。

具体实施方式

[0075] 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做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。

[0076] 集中式身份管理是指由一个机构或者服务器颁发和控制用户的身份。具体流程如下：用户向服务提供商提供一些信息，并基于这些信息申请身份，服务提供商为用户产生身份(一般情况下是用户名和密码)将这些信息保存在服务器上面，然后将身份发放给用户。用户接入服务时，需要提供身份信息(一般情况下是用户名和密码)，服务提供商的服务器对比自身存储的用户身份信息，验证通过后，允许用户使用服务。最常见的场景包括用户注册某项服务，获取了账号和密码，通过该账号和密码登录，并使用该服务。

[0077] 集中式身份管理方案，机构或者中央服务器对于用户的身份具有完全的控制权，包括可以随时撤销、更改用户的身份，导致用户没有控制用户身份的权利，甚至知情权。此外，当机构或者中央服务器出现系统漏洞，可能导致大量用户身份信息泄露，用户的身份信息没有保障。

[0078] 为了解决上述问题，本申请实施例提供一种身份管理的方案，解决集中式身份管理方案带来的用户隐私泄露的潜在安全隐患。由于本申请实施例涉及大量与公钥、证书、加

解密及签名技术的相关知识，为了便于理解本申请实施例提供的方案，首先对这些相关知识进行介绍。

[0079] 单向散列函数，又称单向哈希(hash)函数、杂凑函数，用于把任意长的输入消息串变化成固定长的输出串且由输出串难以得到输入串的一种函数。这个输出串称为该消息的散列值。一般用于产生消息摘要，密钥加密等。单向散列函数包括如下优点：

[0080] 1.加密后密文的长度是定长的(即对任意长度的消息三列，得到的散列值是定长的)。

[0081] 2.如果明文不一样，那么散列后的结果一定不一样。

[0082] 3.如果明文一样，那么加密后的密文一定一样(对相同数据加密，加密后的密文一样)。

[0083] 4.具备单向性，不可以逆推反算。

[0084] 非对称加密(asymmetric cryptography)是一种密码学算法类型，在这种密码学方法中，需要一对密钥，一个是私人密钥(简称为私钥)，另一个则是公开密钥(简称为公钥)。这两个密钥是数学相关，用某用户密钥加密后所得的信息，只能用该用户的解密密钥才能解密。如果知道了其中一个，并不能计算出另外一个。因此如果公开了一对密钥中的一个(公开公钥)，并不会危害到另外一个的秘密性质(不会危害到私钥的私密性质)。如果加密密钥是公钥，这用于客户给私钥所有者上传加密的数据，这被称作为公开密钥加密。如果解密密钥是公钥，用私钥加密的信息，可以用公钥对其解密，用于客户验证持有私钥一方发布的数据或文件是完整准确的，接收者由此可知这条信息确实来自于拥有私钥的某人，这被称作数字签名，公钥的形式就是数字证书。例如，从网上下载的安装程序，一般都带有程序制作者的数字签名，可以证明该程序的确是该作者(公司)发布的而不是第三方伪造的且未被篡改过(身份认证/验证)。

[0085] 下面结合图1对数字签名的过程进行进一步的介绍：数据发送方对需要传输的文本，做一个HASH计算，获取的结果作为需要传输的文本的摘要。使用数据发送方的私钥对需要传输的文本的摘要进行加密，得到的密文即被称为该次传输过程的签名。数据接收端，拿到传输文本，但是需要确认该文本是否就是发送发出的内容，中途是否曾经被篡改。因此拿自己持有的公钥对签名进行解密(密钥对中的一种密钥加密的数据必定能使用另一种密钥解密。)，得到了文本的摘要，然后使用与发送方同样的HASH算法计算摘要值，再与解密得到的摘要做对比，发现二者完全一致，则说明文本没有被篡改过。验证二者是否完全一致的过程即是签名验证的过程。

[0086] 在签名的过程中，收到数据的一方，需要自己保管好公钥，但是由于每一个发送方都有一个公钥，那么接收数据的一方需要保存非常多的公钥，存在管理困难的问题。并且本地保存的公钥有可能被篡改替换，无从发现。为了解决这一问题，可以由一个统一的证书管理机构来管理所有需要发送数据方的公钥，对公钥进行认证和加密。这个机构也就是我们常说的证书颁发方(certificate authority，CA)。认证加密后的公钥，即是证书，又称为CA证书，证书中包含了很多信息，最重要的是申请者的公钥。CA机构在给公钥加密时，用的是一个统一的密钥对，在加密公钥时，用的是其中的私钥。这样，申请者拿到证书后，在发送数据时，用自己的私钥生成签名，将签名、证书和发送内容一起发给对方，对方拿到了证书后，需要对证书解密以获取到证书中的公钥，解密需要用到CA机构的”统一密钥对“中的公钥，

这个公钥也就是我们常说的CA根证书，通常需要我们到证书颁发机构去下载并安装到相应的收取数据的客户端，如浏览器上面。这个公钥只需要安装一次。有了这个公钥之后，就可以解密证书，拿到发送方的公钥，然后解密发送方发过来的签名，获取摘要，重新计算摘要，作对比，以验证数据内容的完整性。

[0087] 本申请实施例提供的方案可以适用于任何一种需要进行身份验证的场景。本申请实施例提供的方案可以使用户有自主身份，即用户具有自主权、控制权的身份体系。自主身份与集中身份管理最大的不同就是用户对身份具体自主权和控制权，而服务提供商不具备对身份的控制权。除此之外，更重要的是，本申请实例提供的方案可以保证每个服务提供商只能获取该服务提供商所需验证的部分身份信息，无法获取用户完整的身份信息，保证用户身份信息的安全性。另外，通过本申请实施例提供的方案，当用户的设备丢失时，用户的身份信息不会轻易泄露，进一步的保障身份信息的安全性。

[0088] 参见图2，为本申请实施例提供的一种身份管理系统的架构示意图。本申请实施例提供的方案至少涉及三方执行主体，包括主身份管理设备，使用服务的设备以及服务器。

[0089] 主身份管理设备，用于管理用户的全部身份信息。本申请实施例提供的方案，用户对身份信息具有自主权和控制权，所有的身份信息由用户自己保管，具体可以保存在主身份管理设备上。在一些可能的实施方式中，主身份管理设备可以是用户可以贴身携带的设备，比如主身份管理设备可以是智能手表、智能眼镜、智能戒指等等，还可以是手机等其他电子设备。

[0090] 使用服务的设备，用于使用服务。比如使用服务的设备上可以安装不同服务对应的客户端，用户可以通过操作客户端使用不同的服务，比如使用购物服务，使用阅读服务，使用社交服务，使用游戏服务，等等。使用服务的设备上可以不保存任何身份信息，并且使用服务的设备可以和主身份管理设备进行交互，以从主身份管理设备上获取部分身份信息。本申请实施例提供的方案，使用服务的设备和主身份管理设备是两个不同的设备，并且对于同一个主身份管理设备，可以对应多个使用服务的设备。在一些可能的实施方式中，使用服务的设备，可以是便于安装服务的设备，比如手机、PAD等等。也可以是智能手表、智能眼镜、智能戒指等其他电子设备。

[0091] 服务器，用于为使用服务的设备提供服务。在一些场景中，服务器允许使用服务的设备访问服务器时，不需要使用服务的设备提供任何身份信息，在另一些场景中，服务器需要使用服务的设备提供相关的身份信息，才会允许使用服务的设备访问该服务器。本申请实施例重点关注服务器需要使用服务的设备提供相关的身份信息的场景。

[0092] 需要说明的是，虽然图2中展示了3个服务器，4个使用服务的设备以及2个主身份管理设备，这并不代表本申请实施例对他们的数目进行限制，在实际应用场景中，包括更多或者更少的服务器、使用服务的设备以及主身份管理设备。

[0093] 参见图3，为本申请实施例提供的另一种身份管理系统的架构示意图。本申请实施例提供的方案还涉及区块链。

[0094] 区块链由一系列不断增长的记录组成，这些记录成为区块(Block)。这些区块通过密码学技术链接再一起，每一个区块包含前一个区块的哈希值，时间戳，和交易数据等。区块链本质上是一个分布式多备份的数据库，但是与数据库最大的不同之处是数据的存储是通过多方共识形成，并使用哈希链对历史数据进行保护，从而使得数据不可篡改。与传统的

数据库技术相比，区块链数据不可以篡改的特征更容易获得用户的信任，因而能够更好地支持多方合作。通常，主身份管理设备生成的公钥是很重要的，并且还需要保证每个主身份管理设备生成的公钥都是唯一的，因此必须保证主身份管理设备生成的公钥是可信的。因此，本申请通过采用区块链的不可篡改特性保证，通过公钥在区块链上注册去中心化身份(decentralized identity,DID)，使每一个公钥对应唯一的DID，并且每个主身份管理设备生成的公钥都是不可篡改的。

[0095] 基于上面图2和图3所描述的架构，图4为本申请实施例提供的一种典型的应用场景的示意图。如图4所示，用户的身份信息是多种多样的，比如姓名、出生日期、地址、教育程度、医疗记录、收入等等。主身份管理设备可以通过多种不同的渠道获取这些身份信息，比如从学校获取教育程度、从医院获取医疗记录，本申请实施例对主身份管理设备如何获取用户的身份信息并不进行限定。主身份管理设备在本地生成主身份管理设备的私钥，以及与该私钥对应的公钥。可以通过私钥对身份进行数字签名，以使拥有了公钥的设备可以验证该数字签名。使用服务的设备上安装了不同的服务，本申请有时也将服务称为业务，再不特意强调二者的区别之时，他们表示相同的意思。每个服务所需要验证的身份信息可能是不相同的，比如游戏类的服务需要验证用户的年龄，金融类的服务需要验证用户的收入等等。所以本申请实施例，使每一种服务只能获取其需要验证的身份信息，无法获取用户的全部信息。具体的，本申请实施例中，针对主身份设置了多个业务身份，本申请实施例通过使使用服务的设备具有多个公私钥对，每一个公私钥对中的公钥绑定一种业务，绑定该业务需要验证的身份信息，以实现使用服务的设备采用业务对应的身份访问业务，在验证阶段只提供该业务所需验证的身份信息，而不会采用主身份访问每一个服务，不会在验证阶段提供全部的身份信息。通过这种方式，使用户对身份具体自主权和控制权，可以保证每个服务提供商只能获取该服务提供商所需验证的部分身份信息，无法获取用户完整的身份信息，保证用户身份信息的安全性。

[0096] 下面对本申请实施例提供的方案进行介绍。本申请实施例提供的方案可以包括身份注册阶段和身份使用阶段，下面将分别从这两个方面对本申请实施例提供的多种方案进行介绍。

[0097] 一、身份注册阶段——方案1

[0098] 参阅图5，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0099] 501、第一设备生成第一私钥(secret key,SK)和第一公钥(public key,PK)。

[0100] 在一种可能的实施方式中，第一设备可以随机生成第一私钥，以及与第一私钥对应的第一公钥。在这种实施方式中，本申请实施例对生成第一私钥的具体方式并不进行限定，任意一种能够生成第一私钥，以及与第一私钥相对应的第一公钥的方式，本申请实施例均可以采用。在这种实施方式中，还可以基于某些信息生成第一私钥和与第一私钥相关的公钥，以便于可以根据该某些信息以及预选择的密钥生成算法，生成第一私钥和第一公钥，比如某些信息包括但不限于用户设定的密码、用户的身份证号、用户的医保账号。在这种实施方式中，第一设备可以始终保存第一私钥，比如将第一私钥存放于第一设备的私密空间，当第一设备需要使用第一私钥时，从该私密空间中获取该第一私钥。或者，在这种实施方式中，第一设备可以不保存第一私钥，当第一设备需要使用第一私钥时，根据用户提供的上述某些信息以及与选择的密钥生成算法，生成第一私钥后再使用。

[0101] 在另一种可能的实施方式中，第一设备获取用户的生物特征，根据用户的生物特征生成第一私钥，以及与第一私钥对应的第一公钥。其中，用户的生物特征包括但不限于指纹信息、虹膜信息。在这种实施方式中，第一设备不需要保存第一私钥，当第一设备需要使用第一私钥时，可以先获取用户的生物特征，然后根据用户的生物特征生成第一私钥。由于第一设备不需要保存第一私钥，增加了第一私钥的安全性，即使第一设备丢失，除了用户之外的其他人也无法获取第一设备的私钥。

[0102] 在一个优选的实施方式中，第一设备可以是智能手表、智能戒指、智能眼镜、智能手环等贴身智能设备。大多数场景中，用户会贴身携带这些贴身智能设备，本申请实施例将用户的主身份信息存储于这些贴身智能设备中，便于用户对主身份信息有更好的掌控。

[0103] 502、第一设备利用第一公钥注册去中心化身份(decentralized IDentity，DID)。

[0104] DID允许个人或组织能够完全拥有对自己数字身份及其数据的所有权、管理权和控制权的身份。相对于传统的基于PKI的身份体系，基于区块链建立的DID数字身份系统具有保证数据真实可信、保护用户隐私安全、可移植性强等特征。

[0105] 在一些实施例中，DID可以是指示真实实体和在线实体之间的映射关系的唯一标识。DID可以包括URL方案标识、用于DID方法的标识以及DID方法专用标识。每个DID可以指向对应的DID文档。DID文档可以包括关于DID和DID的所有者的预设格式(例如，JSON-LD)的描述性文本。DID可以用作用于定位DID文档的统一资源标识(URI)。DID文档可以包括各种属性，例如上下文、DID主题、公钥、认证、授权和委托、服务端点、创建、更新、证明、可扩展性、其他合适的属性或其任意组合。DID文档可以定义或指向定义多个操作的资源，所述操作可以相对于DID执行。

[0106] 可验证声明(VC)可允许不同实体之间进行授权、背书和确认。在商业环境中，服务或产品提供商可以使用其客户的DID和VC来识别并认证客户，并相应地提供服务或产品。

[0107] 在一些实施例中，VC可以提供关于实体的质量、特征、关系和其他相关信息的可验证在线信息。VC可以包含预设格式(例如JSON-LD)的描述性文本，该文本描述有关DID的一个或多个声明(例如，DID所有者的年龄、DID所有者的教育背景)以及实体对声明的背书。VC可以包括各种属性，例如上下文、标识、类型、凭证主题、发布者、发布日期、证明、到期日、状态、表示、其他合适的属性或其任意组合。VC可以指定其声明(claim)的类型，该类型可以指示该声明的结构。这可以促使VC发布者和VC验证者自动进行处理。

[0108] DID的所有者可以以不同的角色参与身份管理系统。例如，个人可能期望使用由商业实体提供的服务，该服务需要证明该个人已超过18岁。该个人可以是DID的所有者，并且可以请求由提供公民年龄验证的政府机构发布的VC。商业实体可以验证VC，以确保该个人符合年龄要求。在这种情况下，个人可以是DID所有者和VC持有者；政府机构可以是VC发布者，而商业实体可以是VC验证者。

[0109] 在本申请实施例中，通过第一公钥注册DID，使第一公钥与唯一的DID进行绑定，当服务器方获取了DID之后，可以根据DID查询到第一公钥，并基于第一公钥验证身份，比如验证接收到的数字签名来自第一设备。

[0110] 如果不同的第一设备采用了相同的第一公钥，可能导致根据该多个不同的第一设备获取的DID是相同的。为了使每一个第一设备都能够具有唯一的DID，所以第一设备获取了DID之后，区块链还会对该获取的DID进行查重，如果当前区块链上没有存储过相同的

DID,则认为注册成功,将第一公钥绑定唯一的DID。

[0111] 503、第二设备向服务器发起注册请求。

[0112] 用户可以通过第二设备访问多种服务,比如访问购物类服务、社交类服务、游戏类服务等等。通常情况下,各类服务需要用户注册后才能够进行访问,或者用户注册后该服务的服务器才会保存该用户在使用服务中产生的相关数据,当用户根据注册的账号访问该服务时,可以获取这些相关数据。

[0113] 在本申请实施例提供的方案中,第二设备向服务器发起注册请求后,不需要等待服务器为用户产生身份(一般情况下是用户名和密码),也不需要服务器将身份发放给用户。在本申请实施例提供的方案中,第二设备向服务器发起注册请求,是为了获取服务器需要验证的身份信息。将在以下步骤进行具体的解释说明。

[0114] 504、第二设备接收服务器发送的第一信息。

[0115] 第二设备向服务器发起注册请求之后,第二设备接收服务器发送的第一消息。在一个可能的实施方式中,第一消息中携带需要验证的身份信息的类别。比如,针对于游戏类服务,当第二设备向游戏类服务器发起注册请求之后,第一消息中携带需要验证的身份信息的类别可能包括年龄。再比如,针对于社交类服务,当第二设备向社交类服务器发起注册请求之后,第一消息中携带需要验证的身份信息的类别可能包括身份证号、学历等。

[0116] 在一个可能的实施方式中,第一消息中还可以携带其他信息,比如还可以携带业务标识(service id),每个业务的业务标识用于表示一个唯一的业务。或者说,业务标识和业务是一一对应的关系。

[0117] 505、第二设备向第一设备发送第二消息。

[0118] 第二设备接收了服务器发送的第一消息后,根据该第一消息获取第二消息,并向第一合并发送第二消息。

[0119] 在一个可能的实施方式中,第二消息携带的内容和第一消息携带的内容完全一致。比如第一消息中携带需要验证的身份信息的类别,第二设备将第一消息携带的内容通过第二消息转发给第一设备,即第二消息中也携带第一消息中携带的需要验证的身份信息的类别。再比如,第一消息中携带需要验证的身份信息的类别以及业务标识,第二设备将第一消息携带的内容通过第二消息转发给第一设备,即第二消息中也携带第一消息中携带的需要验证的身份信息的类别,以及业务标识。

[0120] 在一个可能的实施方式中,第二消息携带的内容可以是第一消息中携带的内容中的部分内容。比如第一消息中携带需要验证的身份信息的类别以及业务标识,第二设备可以只将第第一消息中携带的内容中的部分内容通过第二消息发送给第一设备,比如只将第一消息中携带的需要验证的身份信息的类别通过第二消息发送给第一设备。

[0121] 可以理解为第二消息中必须携带第一消息中携带的需要验证的身份信息的类别,在优选的实施方式中,还可以携带业务标识,此外,第二消息中还可以携带其他信息。

[0122] 在一个可能的实施方式中,第二设备可以通过安全通道想第一设备发送第二消息。任意一种通过安全通道传输的方案,本申请实施例都可以采用,比如,可以使第一设备和第二设备之间建立安全连接,第二设备通过安全网络传输协议(transport layer security,TLS)向第二设备发送第二消息。

[0123] 506、第一设备获取该业务需要验证的身份信息。

[0124] 根据第二消息中携带的需要验证的身份信息的类别，查找每一个类别对应的身份信息，查找到的每一个类型对应的身份信息组成第一身份信息。比如第一设备中存储了用户的全部身份信息，包括但不限于姓名、出生日期、地址、教育程度、医疗记录、收入等等。当第二消息中携带的需要验证的身份信息的类别指示包括姓名和出生日期时，第一设备从全部身份信息中获取姓名以及出生日期对应的信息，假设用户的姓名为张三，出生日期是2000年1月1日，则第一身份信息可能包括张三，2000年1月1日，或者第一身份信息可能包括姓名：张三；出生日期：2000年1月1日。本申请实施例对第一身份信息的具体表现方式并不进行限定。

[0125] 507、第一设备获取第二设备的第二公钥。

[0126] 在一种可能的实施方式中，第一设备可以从其他设备处获取一对公私钥作为第二设备的公私钥。

[0127] 在一个可能的实施方式中，第二设备可以生成第二私钥，以及与第二私钥对应的第二公钥，本申请实施例对生成私钥，以及与私钥对应的公钥的方式并不进行限定，以下对此不再重复说明。在这种实施方式中，第二设备生成了第二私钥和第二公钥之后，可以将第二设备的公钥发送给第一设备。

[0128] 在一个可能的实施方式中，第一设备可以随机生成一对公私钥，作为第二设备的第二私钥和第二公钥。

[0129] 在一个可能的实施方式中，第一设备可以根据相关信息推演出第二私钥，进一步的可以根据第二私钥获取第二公钥。在这种实施方式中，使第一设备可以根据已经获取的信息推演出第二私钥，进而可以使第一设备中无需保存第二私钥。比如，在一个可能的实施方式中，可以根据通过上述步骤获取的第一身份信息、第一公钥以及业务标识推演出第一私钥。具体的，可以将第一身份信息、第一公钥以及业务标识分别作为密钥推演函数(key derivation function，KDF)的参数，根据KDF的取值获取第二私钥，进一步的根据第二私钥获取与第二私钥对应的第二公钥。

[0130] 508、第一设备建立第二公钥和第一身份信息之间的对应关系。

[0131] 第一设备获取了第二公钥，和第一身份信息之后，建立第二公钥和第一身份信息之间的绑定关系，使一个第二公钥对应唯一的第一身份信息。

[0132] 在一个可能的实施方式中，如果第一设备获取了业务标识，比如，在步骤505中，第一设备既获取了业务标识，则还可以建立业务标识和第一身份信息之间的对应关系。当第一设备建立了业务标识和第一身份信息之间的对应关系时，也可以不再建立第二公钥和第一身份信息之间的对应的关系。

[0133] 509、第一设备根据第一公钥对第一身份信息进行加密。

[0134] 为了增加第一身份信息的安全，使保存在第一设备上的第一身份信息不会被轻易泄露，还可以通过第一公钥对第一身份信息进行加密。

[0135] 在一个可能的实施方式中，可以根据第一公钥对第一身份信息和业务标识进行加密处理。

[0136] 510、第一设备将加密后的第一身份信息和第一标识发送至区块链。

[0137] 其中，第一标识可以是第二公钥，还可以是业务标识。

[0138] 第一设备可以向区块链发送数字签名，该数字签名中携带加密后的第一身份信息

和第一标识。当区块链根据第一设备的公钥验证该数字签名来自第一设备后，区块链将加密后的第一身份信息存储在该第一设备注册的DID对应的DID文档(DID Document)中。每一个DID标识都会对应一个DID文档(DID Document)。

[0139] 区块链中建立第一标识和加密后的第一身份信息之间的绑定关系。比如，建立第二公钥和加密后的第一身份信息之间的绑定关系，或者建立业务标识和加密后的第一身份信息之间的绑定关系。

[0140] 511、第二设备建立第二公钥和业务标识之间的绑定关系。

[0141] 在一个可能的实施方式中，可以是第二设备生成了第二私钥和第二公钥，则在第二设备获取的第一消息之后，就可以建立第二公钥和业务标识之间的绑定关系。

[0142] 在一个可能的实施方式中，如果是第一设备生成了第二私钥和第二公钥，则第二设备接收第一设备发送的第二公钥和第二私钥。在一个可能的实施方式中，第一设备可以通过安全通道向第二设备发送第二私钥和第二公钥，其中，安全通道参照步骤505中描述的安全通道进行理解，这里不再重复赘述。在这个实施方式中，第二设备接收了第一设备发送的第二公钥和第二私钥后，建立第二公钥和业务标识之间的绑定关系，由于第二公钥和第二私钥是一一对应的关系，相当于根据业务标识也可以查询到唯一的第二私钥。

[0143] 第二设备获取了第二私钥和第二公钥后，存储该第二公钥和第二私钥，以及第二公钥和业务标识之间的绑定关系。

[0144] 512、第二设备向第一设备发送第三消息。

[0145] 第二设备建立了第二公钥和业务标识之间的绑定关系后，可以向第一设备发送第三消息，使第一设备获取第二设备的状态。在一个可能的实施方式中，该第三消息可以用于指示注册成功。

[0146] 在一个可能的实施方式中，第一设备获取了第二设备发送的第三消息之后，可以将第一设备本地存储的第一身份信息，或者第一身份信息进行删除处理。

[0147] 在一个可能的实施方式中，如果第一设备是根据用户的生物特征生成的第一私钥，则第一设备获取了第三消息之后，可以将本地存储的第一私钥进行删除处理。

[0148] 在一个可能的实施方式中，如果第一设备生成了第二私钥以及第二公钥，则第一设备获取了第三消息之后，可以将本地存储的第二私钥进行删除处理。

[0149] 需要说明的是，在上述图5所描述的实施例的基础上，本申请实施例可以包括更多或者更少的步骤。比如，在一个可能的实施方式中，还可以包括步骤：第一设备提示注册成功。第一设备获取了第二设备发送的第三消息后，可以提示用户注册成功，本申请实施例对注册成功的提示方式并不进行限定。比如，可以提示用户上述步骤中描述的服务/业务注册成功。再比如，有些步骤可以不执行，比如在一个可能的实施方式中，可以不执行步骤502，或者步骤508。实际上，本申请实例描述的每个实施例中包括的步骤都可能更多或者更少，以下对此不再重复赘述。

[0150] 此外，需要说明的是，在上述图5所描述的实施例的基础上，上述描述的各个步骤之间的顺序可以发生调换，比如步骤511可以先于步骤506至步骤510执行，或者可以和步骤506至步骤510同步执行。实际上，本申请实例描述的每个实施例中各个步骤之间的顺序都可能发生调换或者各个步骤同步执行，以下对此不再重复赘述。

[0151] 由图5对应的实施例可知，在注册阶段，针对于每个业务所需验证的身份信息的不

同,生成不同的身份信息(第一身份信息),并将该不同的身份信息绑定不同的第二公钥,相当于本申请实施例中为每一个主身份设置了多个从属身份,每个从属身份用于访问一种服务。使得用户通过第一设备掌握用户的完整的身份信息,除第一设备之外的其他设备无法获取用户的完整身份信息,加强对用户身份信息的隐私保护。

[0152] 下面再对与上述图5所描述的注册过程对应的登录过程进行介绍。

[0153] 二、身份使用阶段(本申请也称之为登录阶段)——方案1

[0154] 参阅图6,为本申请实施例提供的一种信息管理方法的流程示意图,如下所述。

[0155] 601、第二设备向服务器发起访问请求。

[0156] 当第二设备向服务器发起访问请求之后,服务器向第二设备发送身份请求(identity request,IR)消息。

[0157] 在一个可能的实施方式中,IR消息中携带业务标识。在一个可能的实施方式中,IR消息中携带业务标识和服务器的证书。在一个可能的实施方式中,IR消息中携带业务标识、服务器的证书、以及防重放验证参数,比如,该防重放验证参数可以是一个随机数(Nonce)本申请实施例对防重放验证参数的具体方式并不进行限定。在一个可能的实施方式中,防重放参数为用于表征访问请求的生成时间的时间戳和/或序列号。举例说明,假设,服务器发送给第二设备的IR消息中包括服务器的唯一标识123,以及时间戳10:00,则第二设备在获取IR消息后,先验证IR消息中的服务器的所述唯一标识123以及所述时间戳10:00的有效性:若第二设备通过查询对应的唯一标识数据库确定所述唯一标识123真实存在,且所述时间戳11:30在当前时间之前且在预设时间范围内,则第二设备确定IR消息的服务器的唯一标识123以及所述时间戳10:00的有效,即第二设备确定IR消息为有效的IR消息。然后,第二设备继续执行后续步骤,比如执行步骤602。

[0158] 602、第二设备根据业务标识获取第二私钥。

[0159] 上文介绍到,在注册阶段,第二设备获取了第二私钥以及第二公钥,并且第二设备建立了第二公钥和业务标识之间的绑定关系。当第二设备根据IR消息获取了业务标识后,可以根据第二设备存储的业务标识和第二公钥之间的绑定关系,获取与该业务标识唯一对应的第二公钥。然后,由于一个第二公钥对应唯一的第二私钥,所以可以根据该业务标识唯一对应的第二公钥获取第二私钥。

[0160] 603、第二设备向第一设备发送数字签名和第二公钥。

[0161] 第二设备根据步骤602中获取的第二私钥生成数字签名。

[0162] 在一个可能的实施方式中,该数字签名中携带IR消息。此外,第二设备还向第一设备发送第二设备的公钥。

[0163] 在一个可能的实施方式中,可以通过同一条消息向第一设备发送数字签名和第二公钥。在一个可能的实施方式中,可以通过不同消息向第一设备发送数字签名和第二公钥。

[0164] 在一个可能的实施方式中,可以通过安全通道向第一设备发送数字签名和第二公钥。

[0165] 604、第一设备验证数字签名。

[0166] 第一设备接收第二设备发送的数字签名,以及第二设备发送的公钥。第一设备根据接收到的第二设备的公钥验证第二设备发送的数字签名。关于如何验证数字签名的过程已经在上文进行了介绍,这里不再重复赘述。

[0167] 若验证通过，则继续执行后续的步骤，比如执行步骤605，若验证未通过，则不再执行后续的步骤。

[0168] 605、第一设备获取第一私钥。

[0169] 在一个可能的实施方式中，如果在注册的阶段采用了在第一设备本地存储第一私钥的方式，则在第一设备验证第二设备的数字签名通过后，从第一设备本地获取第一私钥。

[0170] 在一个可能的实施方式中，如果在注册的阶段采用了通过用户的生物特征生成第一私钥的方式，则在第一设备验证第二设备的数字签名通过后，获取用户的生物特征。第一设备根据获取到的用户的生物特征生成第一私钥，还可以采用与注册阶段相同的方式生成与第一私钥对应的第一公钥。

[0171] 606、第一设备从区块链中获取加密后的第一身份信息。

[0172] 第一设备可以向区块链发送数字签名，该数字签名中携带第一标识。在登录阶段中的第一标识和注册阶段中的第一标识相同。比如，如果在注册阶段，该第一标识是业务标识，则在登录阶段，第一设备向区块链发送数字签名，该数字签名中携带业务标识，当区块链根据第一设备的公钥验证该数字签名来自第一设备后，根据该业务标识，查询与该业务标识对应的加密后的第一身份信息。再比如，如果在注册阶段，该第一标识是第二公钥，则在登录阶段，第一设备向区块链发送数字签名，该数字签名中携带第二公钥，当区块链根据第一设备的公钥验证该数字签名来自第一设备后，根据该第二公钥，查询与该第二公钥对应的加密后的第一身份信息。

[0173] 区块链根据第一标识查询到加密后的第一身份信息后，将该加密后的第一身份信息向第一设备发送，以使第一设备获取加密后的第一身份信息。

[0174] 607、第一设备利用第一私钥解密出第一身份信息。

[0175] 第一设备从区块链中获取了加密后的第一身份信息后，由于在注册阶段采用了第一公钥对该第一身份信息进行了加密处理，所以在登录阶段，第一设备可以利用与第一公钥对应的第一私钥对加密后的第一身份信息进行解密处理，以获取第一身份信息。

[0176] 608、第一设备向第二设备发送数字签名。

[0177] 第一设备利用第一私钥生成数字签名，该数字签名中携带第一身份信息。在一个可能的实施方式中，该数字签名中还可以携带业务标识。在一个可能的实施方式中，该数字签名中还可以携带防重放参数。

[0178] 第一设备向第二设备发送该数字签名，在一个可能的实施方式中，当第一设备向第二设备发送了该数字签名，将第一身份信息发送给第二设备后，可以删除第一设备本地保存的第一身份信息、第一公钥以及业务标识。

[0179] 609、第二设备向服务器转发该数字签名。

[0180] 在一个可能的实施方式中，第二设备可以不对该数字签名进行验证，只将获取到的数字签名转发至服务器。

[0181] 在一个可能的实施方式中，第二设备获取了第一设备发送的数字签名后，可以通过第一设备的公钥验证该第一数字签名，在验证通过后，即证实该数字签名是来自第一设备后，向服务器发送该数字签名。

[0182] 610、服务器通过第一公钥验证数字签名。

[0183] 服务器通过第一设备的公钥验证接收到的数字签名，关于如何验证数字签名已经

在上文进行了介绍，这里不再重复赘述。

[0184] 在一个可能的实施方式中，服务器可以从区块链中查询第一设备的DID，根据该第一设备唯一对应的DID获取第一设备的公钥。

[0185] 611、服务器验证成功后，允许第二设备访问服务器。

[0186] 服务器验证成功后，确定该数字签名确实是第一设备发出的，则允许第二设备访问服务器，即允许第二设备使用对应的服务/业务。

[0187] 在一个可能的实施方式中，服务器还可以向第二设备或者第一设备发送身份验证成功的通知消息。

[0188] 在一个可能的实施方式中，如果验证未通过，则不允许第二设备访问服务器。

[0189] 由图6对应的实施例可知，在身份使用阶段，每个服务器只能获取该服务器所需要验证的身份信息，而无法获取用户的全部身份信息，增加了用户身份的隐私性和安全性。并且，本申请实施例提供的方案可以很方便的撤销第二公钥，确保用户身份信息的安全性。比如，第二设备丢失后，第一设备可以设置第二设备的公钥失效，第二设备不能再基于之前第二设备的公钥，请求第一设备发送身份信息。并且，第一设备可以重新生成生成新的第二公钥，与新的第二设备建立绑定关系。此外，本申请实施例提供的方案可以根据用户的生物特征生成第一私钥，第一设备中无需保存第一私钥，进一步的增加了身份信息的安全性。另外，第二设备的公钥存储在第二设备上，方便随时认证使用。

[0190] 需要说明的是，在上述图6所描述的实施例的基础上，可以包括更多或者更少的步骤。此外，需要说明的是，在上述图6所描述的实施例的基础上，上述描述的各个步骤之间的顺序可以发生调换，或者可以同步执行。

[0191] 在上述图5和图6描述的方案中，加密后的第一身份信息存储于区块链中，在一些其他的实施方式中，该加密后的第一身份信息也可以存储在第一设备中或者第二设备中，下面结合具体的实施方式对此进行介绍。

[0192] 一、身份注册阶段——方案2

[0193] 参阅图7，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0194] 701、第一设备生成第一私钥和第一公钥。

[0195] 702、第一设备利用第一公钥注册DID。

[0196] 703、第二设备向服务器发起注册请求。

[0197] 704、第二设备接收服务器发送的第一信息。

[0198] 705、第二设备向第一设备发送第二消息。

[0199] 706、第一设备获取该业务需要验证的身份信息。

[0200] 707、第一设备获取第二设备的第二公钥。

[0201] 708、第一设备建立第二公钥和第一身份信息之间的对应关系。

[0202] 709、第一设备根据第一公钥对第一身份信息进行加密。

[0203] 步骤701至步骤709可以参照图5对应的实施例中的步骤501至步骤509进行理解，这里不再重复赘述。

[0204] 710、第一设备存储加密后的第一身份信息。

[0205] 不同于图5所描述的实施方式中，在区块链中存储加密后的第一身份信息，在图7所描述的实施方式中，第一设备在本地存储加密后的第一身份信息，节约区块链的存储资

源和通信资源。

[0206] 第一设备建立第一标识和加密后的第一身份信息之间的绑定关系。其中，第一标识可以是第二公钥，还可以是业务标识。比如，建立第二公钥和加密后的第一身份信息之间的绑定关系，或者建立业务标识和加密后的第一身份信息之间的绑定关系。

[0207] 711、第一设备利用第二公钥注册DID。

[0208] 如果不同的第二设备采用了相同的第二公钥，或者第二设备的多个不同的业务都绑定了相同的公钥，则可能导致同一个第二公钥绑定了不同的第一身份信息，在登录阶段也会造成混乱，比如可能导致第一设备错误的向第二设备发送第一身份信息，进而导致服务器验证失败。比如，第一设备有对应的两个第二设备，分别是第二设备A和第二设备B。如果第二设备A的公钥是第二公钥A，第二设备B的公钥是第二公钥B。其中，第二公钥A绑定的第一身份信息是第一身份信息A，第二公钥B绑定的第一身份信息是第一身份信息B。在登录阶段，第一设备根据第二公钥A验证数字签名通过后，第一设备将与第二公钥A绑定的第一身份信息发送给第二设备A。但是，如果第二公钥A和第二公钥B相同，第一设备可能将与第二公钥B绑定的第一身份信息发送给第二设备A，如果与第二公钥A绑定的第一身份信息和与第二公钥B绑定的第一身份信息并不相同，当第二设备A将与第二公钥B绑定的第一身份信息发送给服务器后，可能导致验证失败。再比如，第二设备上注册了两个不同的服务，分别是服务A和服务B，假设服务A对应的公钥是第二公钥A，服务B对应的公钥是第二公钥B。其中，第二公钥A绑定的第一身份信息是第一身份信息A，第二公钥B绑定的第一身份信息是第一身份信息B。在登录阶段，第一设备根据第二公钥A验证数字签名通过后，第一设备将与第二公钥A绑定的第一身份信息发送给第二设备。但是，如果第二公钥A和第二公钥B相同，第一设备可能将与第二公钥B绑定的第一身份信息发送给第二设备A，如果与第二公钥A绑定的第一身份信息和与第二公钥B绑定的第一身份信息并不相同，当第二设备A将与第二公钥B绑定的第一身份信息发送给服务器后，可能导致验证失败。比如，服务A是游戏类服务，与第二公钥A绑定的第一身份信息包括年龄，服务B是金融类服务，与第二公钥B绑定的第一身份信息包括收入情况。如果将收入情况发送至服务A的服务器，有可能导致验证失败。

[0209] 为了解决上述问题，第一设备利用第二公钥注册DID，区块链还会对该获取的DID进行查重，如果当前区块链上没有存储过相同的DID，则认为注册成功，将第二公钥绑定唯一的DID。

[0210] 712、第二设备建立第二公钥和业务标识之间的绑定关系。

[0211] 713、第二设备向第一设备发送第三消息。

[0212] 步骤712和步骤713可以参照图5对应的实施例中的步骤511和步骤512进行理解，这里不再重复赘述。

[0213] 二、身份使用阶段(本申请也称之为登录阶段)——方案2

[0214] 参阅图8，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0215] 801、第二设备向服务器发起访问请求。

[0216] 802、第二设备根据业务标识获取第二私钥。

[0217] 803、第二设备向第一设备发送数字签名和第二公钥。

[0218] 804、第一设备验证数字签名。

[0219] 805、第一设备获取第一私钥。

[0220] 步骤801至步骤805可以参照图6对应的实施例中的步骤601至步骤605进行理解，这里不再重复赘述。

[0221] 806、第一设备从本地获取加密后的第一身份信息。

[0222] 第一设备根据第一标识查询本地存储，以获取加密后的第一身份信息。

[0223] 在登录阶段中的第一标识和注册阶段中的第一标识相同。比如，如果在注册阶段，该第一标识是业务标识，则在登录阶段，第一设备根据该业务标识，查询与该业务标识对应的加密后的第一身份信息。再比如，如果在注册阶段，该第一标识是第二公钥，则在登录阶段，第一设备根据该第二公钥，查询与该第二公钥对应的加密后的第一身份信息。

[0224] 807、第一设备利用第一私钥解密出第一身份信息。

[0225] 808、第一设备向第二设备发送数字签名。

[0226] 809、第二设备向服务器转发该数字签名。

[0227] 810、服务器通过第一公钥验证数字签名。

[0228] 811、服务器验证成功后，允许第二设备访问服务器。

[0229] 步骤807至步骤811可以参照图6对应的实施例中的步骤607至步骤611进行理解，这里不再重复赘述。

[0230] 需要说明的是，在上述图7和图8所描述的实施例的基础上，可以包括更多或者更少的步骤。此外，需要说明的是，在上述图7和图8所描述的实施例的基础上，上述描述的各个步骤之间的顺序可以发生调换，或者可以同步执行。

[0231] 在上述图7和图8描述的方案中，除了具有图5和图6所描述的实施例所描述的优势之外，加密后的第一身份信息存储于第一设备中，节约区块链的存储资源和通信资源。在一些可能的实施方式中，该加密后的第一身份信息还可以存储于第二设备中，下面结合具体的实施方式对此进行介绍。

[0232] 一、身份注册阶段——方案3

[0233] 参阅图9，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0234] 901、第一设备生成第一私钥和第一公钥。

[0235] 902、第一设备利用第一公钥注册DID。

[0236] 903、第二设备向服务器发起注册请求。

[0237] 904、第二设备接收服务器发送的第一信息。

[0238] 905、第二设备向第一设备发送第二消息。

[0239] 906、第一设备获取该业务需要验证的身份信息。

[0240] 907、第一设备获取第二设备的第二公钥。

[0241] 908、第一设备建立第二公钥和第一身份信息之间的对应关系。

[0242] 909、第一设备根据第一公钥对第一身份信息进行加密。

[0243] 步骤901至步骤909可以参照图7对应的实施例中的步骤701至步骤709进行理解，这里不再重复赘述。

[0244] 910、第一设备利用第二公钥注册DID。

[0245] 步骤910可以参照图7对应的实施例中的步骤711进行理解，这里不再重复赘述。

[0246] 911、第二设备获取加密后的第一身份信息以及第二公钥。

[0247] 在一个可能的实施方式中，可以是第二设备生成了第二私钥和第二公钥。在一个

可能的实施凡是中，如果是第一设备生成了第二私钥和第二公钥，则第二设备接收第一设备发送的第二公钥和第二私钥。在一个可能的实施方式中，第一设备可以通过安全通道向第二设备发送第二私钥和第二公钥，其中，安全通道参照步骤505中描述的安全通道进行理解，这里不再重复赘述。

[0248] 第二设备从第一设备处获取加密后的第一身份信息。在一个可能的实施方式中，第一设备可以通过安全通道向第二设备发送加密后的第一身份信息。在一个可能的实施方式中，第一设备可以通过同一个消息向第二设备发送加密后的第一身份信息，以及第二私钥以及第二公钥。在一个可能的实施方式中，第一设备可以通过不同消息向第二设备发送加密后的第一身份信息，以及第二私钥以及第二公钥。

[0249] 第二设备或了加密后的第一身份信息以及第二公钥后，保存该加密后的第一身份信息以及第二公钥、第二私钥。

[0250] 912、第二设备建立第二设备建立第二公钥和业务标识之间的绑定关系，建立第二公钥和第一身份信息之间的绑定关系。

[0251] 第二设备建立第二公钥和业务标识之间的绑定关系后，由于第二公钥和第二私钥是一一对应的关系，相当于根据业务标识也可以查询到唯一的第二私钥。

[0252] 第二设备获取与该业务标识绑定的第二公钥，进而可以获取与该第二公钥绑定的第一身份信息。

[0253] 在一个可能的实施方式中，也可以建立业务标识和第一身份信息之间的绑定关系。当第二设备获取了业务标识后，可以直接获取与该业务标识绑定的加密后的第一身份信息。

[0254] 在图9所描述的实施方式中，第二设备在本地存储加密后的第一身份信息，由于第二设备通常是手机，安全性能更高，将加密后的第一身份信息存储在手机中，可以提升身份信息的安全性。

[0255] 913、第二设备向第一设备发送第三消息。

[0256] 步骤913可以参照图5对应的实施例中的步骤512进行理解，这里不再重复赘述。

[0257] 二、身份使用阶段(本申请也称之为登录阶段)——方案3

[0258] 参阅图10，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0259] 1001、第二设备向服务器发起访问请求。

[0260] 1002、第二设备根据业务标识获取第二私钥。

[0261] 步骤1001至步骤1002可以参照图6对应的实施例中的步骤601和步骤602进行理解，这里不再重复赘述。

[0262] 1003、第二设备向第一设备发送数字签名和第二公钥。

[0263] 第二设备根据步骤602中获取的第二私钥生成数字签名，该数字签名中携带IR消息和加密后的第一身份信息。此外，第二设备还向第一设备发送第二设备的公钥。

[0264] 具体的，第二设备获取了业务标识后，可以根据与该业务标识绑定的第二公钥，进而可以获取与该公钥绑定的加密后的第一身份信息。如果在注册阶段建立了业务标识和加密后的第一身份信息之间的绑定关系，则第二设备获取了业务标识后，可以根据该业务标识直接获取与该业务标识绑定的加密后的第一身份信息。

[0265] 在一个可能的实施方式中，可以通过同一条消息向第一设备发送数字签名和第二

公钥。在一个可能的实施方式中，可以通过不同消息向第一设备发送数字签名和第二公钥。

[0266] 在一个可能的实施方式中，可以通过安全通道向第一设备发送数字签名和第二公钥。

[0267] 1004、第一设备验证数字签名。

[0268] 1005、第一设备获取第一私钥。

[0269] 步骤1004和步骤1005可以参照图6对应的实施例中的步骤604和步骤605进行理解，这里不再重复赘述。

[0270] 1006、第一设备通过第一私钥解密出第一身份信息。

[0271] 第一设备从第二设备处获取了加密后的第一身份信息后，通过第一私钥对加密后得到的第一身份信息进行解密，以获取第一身份信息。

[0272] 1007、第一设备向第二设备发送数字签名。

[0273] 1008、第二设备向服务器转发该数字签名。

[0274] 1009、服务器通过第一公钥验证数字签名。

[0275] 1010、服务器验证成功后，允许第二设备访问服务器。

[0276] 步骤1007至步骤1010可以参照图6对应的实施例中的步骤608至步骤611进行理解，这里不再重复赘述。

[0277] 在上述图9和图10描述的方案中，除了具有图5和图6所描述的实施例所描述的优势之外，加密后的第一身份信息存储于第二设备中，由于第二设备通常是手机，安全性能更高，将加密后的第一身份信息存储在手机中，可以提升身份信息的安全性。

[0278] 上述图5至图10描述的实施例中，在身份注册阶段和身份使用阶段利用了公私钥对，比如引入了第一私钥，与第一私钥对应的第一公钥，第二私钥，以及与第二私钥对应的第二公钥。在一些实施例中，也可以不采用非对称加密技术，采用对称加密技术也是可以的。下面结合具体的实施方式进行介绍。

[0279] 一、身份注册阶段——方案4

[0280] 参阅图11，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0281] 1101、第一设备生成第一密钥。

[0282] 在一种可能的实施方式中，第一设备可以随机生成第一密钥。在这种实施方式中，第一设备可以始终保存第一私钥，比如将第一私钥存放于第一设备的私密空间，当第一设备需要使用第一私钥时，从该私密空间中获取该第一私钥。

[0283] 在一种可能的实施方式中，第一设备获取用户的生物特征，根据用户的生物特征生成第一密钥。其中，用户的生物特征包括但不限于指纹信息、虹膜信息。在这种实施方式中，第一设备不需要保存第一密钥，当第一设备需要使用第一密钥时，可以先获取用户的生物特征，然后根据用户的生物特征生成第一密钥。由于第一设备不需要保存第一密钥，增加了第一私钥的安全性，即使第一设备丢失，除了用户之外的其他人也无法获取第一设备的私钥。

[0284] 1102、第一设备根据第一设备的标识生成第二密钥。

[0285] 每个设备都有唯一对应对应的标识，本申请实施例对第一设备的标识的具体表现方式并不进行限定。比如根据国际移动设备识别码(international mobile equipment identity，IMEI)和媒体存取控制位址(media access control address，MAC)地址作为第

一设备的标识。再比如根据接入网标识作为第一设备的标识。

[0286] 根据第一设备唯一对应的标识生成第二密钥。

[0287] 1103、第二设备向服务器发起注册请求。

[0288] 1104、第二设备接收服务器发送的第一信息。

[0289] 步骤1103和步骤1104可以参照图5对应的实施例中的步骤503和步骤504进行理解，这里不再重复赘述。

[0290] 1105、第二设备根据业务标识生成第三密钥。

[0291] 如果第二设备根据业务标识生成的第三密钥，则第二设备建立业务标识和第三密钥之间的绑定关系。

[0292] 1106、第二设备向第一设备发送目标消息。

[0293] 目标消息中携带需要验证的身份信息的类别和第三密钥。比如，针对于游戏类服务，当第二设备向游戏类服务器发起注册请求之后，第一消息中携带需要验证的身份信息的类别可能包括年龄。再比如，针对于社交类服务，当第二设备向社交类服务器发起注册请求之后，第一消息中携带需要验证的身份信息的类别可能包括身份证号、学历等。

[0294] 在一个可能的实施方式中，目标消息中携带需要验证的身份信息的类别和业务标识。在这种实施方式中，可以不执行步骤1105，由第一设备根据业务标识生成第三密钥。如果由第一设备根据业务标识生成的第三密钥，则第一设备建立业务标识和第三密钥之间的绑定关系。

[0295] 在一个可能的实施方式中，目标消息中可以携带需要验证的身份信息的类别、业务标识以及第三密钥。

[0296] 1107、第一设备获取目标密钥。

[0297] 第一设备根据第一密钥、第二密钥以及第三密钥合成目标密钥。本申请实施例对具体采用何种方式何从目标密钥并不进行限定，只需要保证根据第一密钥、第二密钥以及第三密钥这三种密钥共同合成目标密钥。

[0298] 1108、第一设备获取第一身份信息。

[0299] 第一设备获取该业务需要验证的身份信息，步骤1108可以参照图5对应的实施例中的步骤506进行理解，这里不再重复赘述。

[0300] 1109、第一设备根据目标密钥加密第一身份信息。

[0301] 1110、第一设备建立绑定关系。

[0302] 在一个可能的实施方式中，第一设备建立第三密钥和加密后的第一身份信息之间的绑定关系。

[0303] 在一个可能的实施方式中，第一设备建立目标密钥和加密后的第一身份信息之间的绑定关系。

[0304] 在一个可能的实施方式中，第一设备建立业务标识和加密后的第一身份信息之间的绑定关系。

[0305] 1111、第一设备通知第二设备已经通过目标密钥对第一身份信息进行了加密。

[0306] 1112、第二设备向第一设备发送反馈信息。

[0307] 第二设备获取了第一设备已经通过目标密钥对第一身份信息进行了加密后，可以向第一设备发送反馈消息，通知第二设备已经接受到第一设备发送的消息(步骤1110)。

[0308] 在一个可能的实施方式中，第一设备获取了第二设备发送的反馈消息后，可以对第一密钥、第二密钥、第三密钥以及目标密钥进行删除处理。

[0309] 在一个可能的实施方式中，第一设备可以提示用户注册成功。

[0310] 二、身份使用阶段(本申请也称之为登录阶段)——方案4

[0311] 参阅图12，为本申请实施例提供的一种信息管理方法的流程示意图，如下所述。

[0312] 1201、第二设备向服务器发起访问请求。

[0313] 步骤1201可以参照图6对应的实施例中的步骤601进行理解，这里不再重复赘述。

[0314] 1202、第二设备根据业务标识获取第三密钥。

[0315] 图11对应的实施例介绍到，在注册阶段，第二设备建立了第三密钥和业务标识之间的绑定关系，所以第二设备获取了业务标识后，可以获取和该业务标识绑定的第三密钥。

[0316] 1203、第二设备向第一设备发送IR消息以及第三密钥。

[0317] 在一个可能的实施方式中，如果在注册阶段，由第一设备生成的第三密钥，则第二设备可以只向第一设备发送IR消息，由第一设备根据业务标识生成第三密钥。

[0318] 在一个可能的实施方式中，第二设备可以通过安全通道向第一设备发送IR消息以及第三密钥。

[0319] 1204、第一设备获取第一密钥和第二密钥。

[0320] 第一设备获取用户的生物特征，根据用户的生物特征生成第一密钥。第一设备获取第一设备的标识，第一设备根据第一设备的标识获取第二密钥。显然，用户的生物特征与注册阶段采用的生物特征相同，该标识与注册阶段采用的标识相同，本申请实施例对此不再重复解释说明。

[0321] 1205、第一设备获取目标密钥。

[0322] 第一设备根据与注册阶段相同的方式，根据第一密钥、第二密钥以及第三密钥合成目标密钥。

[0323] 其中，在一个可能的实施方式中，第三密钥可能由第一设备根据业务标识获取，或者第三密钥可能由第二设备根据业务标识生成后，向第一设备发送。

[0324] 1206、第一设备获取加密后的第一身份信息。

[0325] 在一个可能的实施方式中，如果在注册阶段，第一设备建立第三密钥和加密后的第一身份信息之间的绑定关系。则在登录阶段，第一设备可以根据获取的第三密钥，查找与该第三密钥绑定的加密后的第一身份信息。

[0326] 在一个可能的实施方式中，如果在注册阶段，第一设备建立目标密钥和加密后的第一身份信息之间的绑定关系。则在登录阶段，第一设备可以根据目标密钥，查找与该目标密钥绑定的加密后的第一身份信息。

[0327] 在一个可能的实施方式中，如果在注册阶段，第一设备建立业务标识和加密后的第一身份信息之间的绑定关系。则在登录阶段，第一设备可以根据业务标识，查找与该业务标识绑定的加密后的第一身份信息。

[0328] 1207、第一设备通过目标密钥解密出第一身份信息。

[0329] 1208、第一设备向第二设备发送通过服务器的公钥加密的第一身份信息。

[0330] 在一个可能的实施方式中，第一设备完成了步骤1207或者步骤1208后，可以对第一密钥、第二密钥、第三密钥以及目标密钥进行删除处理。

[0331] 1209、第二设备向服务器发送通过服务器的公钥加密后的第一身份信息。

[0332] 1210、服务器通过服务器的私钥解密通过服务器的公钥加密后的第一身份信息，并验证。

[0333] 1211、服务器验证成功后，允许第二设备访问服务器。

[0334] 图5至图10所描述的实施例，都是基于公钥体系设计的方案，在应用的时候，可能对设备的计算能力要求比较高，功耗也相对大一些。图11和图12所描述的实施例使用的是基于对称钥的方案，对设备的计算要求能力比较低，同时功能比较小。另外，图11和图12所描述的实施例将第一设备的本身的标识做为部分密钥，来合成对称钥，完成了设备与用户密钥的强绑定，安全性也比较好。同时，对称钥实施简单，技术成熟。

[0335] 前述对本申请提供的系统以及方法进行了详细介绍，下面对本申请提供的装置进行介绍。

[0336] 参阅图13，本申请提供的一种第二设备的结构示意图。

[0337] 该第二设备包括：

[0338] 收发模块1301，用于向服务器发起注册请求。

[0339] 收发模块1301，还用于接收服务器响应于注册请求发送的第一消息，第一消息中携带第一业务需要验证的信息的种类和第一业务的标识。

[0340] 处理模块1303，用于建立第二设备的公钥和第一业务的标识之间的绑定关系。

[0341] 收发模块1301，还用于向第一设备发送第一业务需要验证的信息的种类，以使第一设备根据第一业务需要验证的信息的种类，从第一设备本地存储的信息中获取第一业务需要验证的信息，第一业务需要验证的信息和第二设备的公钥之间存在绑定关系。

[0342] 在一个可能的实施方式中，收发模块1301，还用于接收第一设备发送的加密后的第一业务需要验证的信息。处理模块1303，还用于建立加密后的第一业务需要验证的信息和第二设备的公钥之间的绑定关系。

[0343] 在一个可能的实施方式中，收发模块1301，还用于接收第一设备发送的第二设备的私钥和第二设备的公钥。收发模块1301，用于向服务器发起访问请求。收发模块1301，还用于接收服务器响应于访问请求发送的身份请求IR消息，IR消息中携带第一业务的标识。处理模块1303，用于根据第一业务的标识，查找与第一业务标识绑定的第二设备的公钥。处理模块1303，还用于利用与第二设备的公钥对应的第二设备的私钥，生成第二设备的数字签名。收发模块1301，还用于向第一设备发送第二设备的数字签名以及第二设备的公钥，以使第一设备验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的信息。

[0344] 在一个可能的实施方式中，收发模块1301，用于向服务器发起注册请求。收发模块1301接收服务器发送的第一消息，第一消息中携带第一业务需要验证的信息的种类和第一业务的标识。收发模块1301，还用于向第二设备发送第一业务需要验证的信息的种类。

[0345] 在一个可能的实施方式中，处理模块1303，还用于根据第一业务的标识生成第三密钥，并建立第三密钥和第一业务的标识之间的绑定关系。

[0346] 在一个可能的实施方式中，还包括存储模块1302，用于保存收发模块获取的数据。

[0347] 参阅图14，本申请提供的一种第一设备的结构示意图。

[0348] 该第一设备包括：

[0349] 收发模块1401，用于从第二设备处获取第一业务需要验证的信息的种类，并根据第一业务需要验证的信息的种类，从第一设备的存储模块1402中获取第一业务需要验证的信息，第一业务需要验证的信息和第二设备的公钥之间存在绑定关系。

[0350] 在一个可能的实施方式中，设备还包括处理模块1403，用于建立第一业务需要验证的信息和第二设备的公钥之间的绑定关系。

[0351] 在一个可能的实施方式中，处理模块1403，还用于根据第一设备的公钥加密第一业务需要验证的信息。

[0352] 在一个可能的实施方式中，收发模块1401，还用于：向区块链节点发送加密后的第一业务需要验证的信息，以使区块链节点建立加密后的第一业务需要验证的信息和第二设备的公钥之间的绑定关系。

[0353] 在一个可能的实施方式中，收发模块1401，还用于向第二设备发送加密后的第一业务需要验证的信息，以使第二设备建立加密后的第一业务需要验证的信息和第二设备的公钥之间的绑定关系。

[0354] 在一个可能的实施方式中，处理模块1403，还用于：第一设备发送了加密后的第一业务需要验证的信息之后，删除第一设备本地存储的加密后的第一业务需要验证的信息。

[0355] 在一个可能的实施方式中，处理模块1403，还用于：根据用户的生物特征生成第一设备的私钥。

[0356] 在一个可能的实施方式中，处理模块1403，还用于：利用第一设备的公钥注册去中心化身份DID。

[0357] 在一个可能的实施方式中，处理模块1403，还用于：生成第二设备的私钥和第二设备的公钥。收发模块1401，还用于向第二设备发送第二设备的私钥和第二设备的公钥。

[0358] 在一个可能的实施方式中，收发模块1401，还用于：从第二设备处获取第一业务的标识。处理模块1403，具体用于根据第一业务的标识、第一业务需要验证的信息、第一设备的私钥生成第二设备的私钥。

[0359] 在一个可能的实施方式中，处理模块1403，还用于验证第二设备的数字签名来自第二设备后，获取与第二设备的公钥绑定的第一业务需要验证的信息。处理模块1403，还用于根据第一设备的私钥生成第一设备的数字签名，数字签名中携带第一业务需要验证的信息。

[0360] 在一个可能的实施方式中，处理模块1403，具体用于：验证第二设备的数字签名来自第二设备后，从区块链节点处获取与第二设备的公钥绑定的加密后的第一业务需要验证的信息，根据第一设备的私钥解密加密后的第一业务需要验证的信息，以获取第一业务需要验证的的信息。

[0361] 在一个可能的实施方式中，处理模块1403，具体用于验证第二设备的数字签名来自第二设备后，从第二设备处获取与第二设备的公钥绑定的加密后的第一业务需要验证的信息，根据第一设备的私钥解密加密后的第一业务需要验证的信息，以获取第一业务需要验证的的信息。

[0362] 在一个可能的实施方式中，处理模块1403，具体用于第一设备验证第二设备的数字签名来自第二设备后，从第一设备本地获取加密后的第一业务需要验证的信息，根据第一设备的私钥解密加密后的第一业务需要验证的信息，以获取第一业务需要验证的的信

息。

[0363] 在一个可能的实施方式中，处理模块1403，还用于收发模块1401发送了第一设备的数字签名后，删除第一设备的私钥以及第一业务需要验证的信息。

[0364] 在一个可能的实施方式中，处理模块1403，还用于验证第二设备的数字签名来自第二设备后，获取用户的生物特征，并根据生物特征生成第一设备的私钥。

[0365] 在一个可能的实施方式中，收发模块1401，还用于从第二设备处获取第一业务需要验证的信息的种类，并根据第一业务需要验证的信息的种类，从第一设备本地存储的信息中获取第一业务需要验证的信息，第一业务需要验证的信息和目标密钥绑定，目标密钥是基于第一密钥、第二密钥和第三密钥生成的，第一密钥是根据第一设备获取的用户的生物特征生成的密钥，第二密钥是根据第一设备的标识生成的密钥，第三密钥是根据第一业务的标识生成的密钥。处理模块1403，还用于根据目标密钥对第一业务需要验证的信息进行加密处理。

[0366] 在一个可能的实施方式中，处理模块1403，还用于删除第一密钥、第二密钥、第三密钥以及目标密钥。

[0367] 在一个可能的实施方式中，处理模块1403，还用于根据第一业务的标识生成第三密钥，并建立第三密钥和第一业务的标识之间的绑定关系。

[0368] 在一个可能的实施方式中，收发模块1401，还用于从第二设备处获取第一业务的标识。处理模块1403，还用于根据第一密钥、第二密钥以及第三密钥生成目标密钥，第一密钥是根据第一设备获取的用户的生物特征生成的密钥，第二密钥是根据第一设备的标识生成的密钥，第三密钥是根据第一业务的标识生成的密钥。处理模块1403，还用于根据目标密钥解密加密后的第一业务需要验证的信息，一获取第一业务需要验证的信息。处理模块1403，还用于根据服务器的公钥加密第一业务需要验证的信息，以使服务器根据服务器的私钥解密后，获取第一业务需要验证的信息。

[0369] 请参阅图15，本申请提供的另一种第二设备的结构示意图，如下所述。

[0370] 该第二设备可以包括处理器1501和存储器1502。该处理器1501和存储器1502通过线路互联。其中，存储器1502中存储有程序指令和数据。

[0371] 存储器1502中存储了前述图5-图12中的步骤对应的程序指令以及数据。

[0372] 处理器1501用于执行前述图5-图12中任一实施例所示的第二设备执行的方法步骤。

[0373] 收发器1503，用于接收或者发送数据。

[0374] 可选地，前述的图15中所示的归属设备可以为芯片。

[0375] 请参阅图16，本申请提供的另一种第一设备的结构示意图，如下所述。

[0376] 该第一设备可以包括处理器1601和存储器1602。该处理器1601和存储器1602通过线路互联。其中，存储器1602中存储有程序指令和数据。

[0377] 存储器1602中存储了前述图5-图12中的步骤对应的程序指令以及数据。

[0378] 处理器1601用于执行前述图5-图12中任一实施例所示的第一设备执行的方法步骤。

[0379] 收发器1603，用于接收或者发送数据。

[0380] 可选地，前述的图16中所示的访问控制节点可以为芯片。

[0381] 请参阅图17,本申请提供的服务器的结构示意图,如下所述。

[0382] 该服务器可以包括处理器1701和存储器1702。该处理器1701和存储器1702通过线路互联。其中,存储器1702中存储有程序指令和数据。

[0383] 存储器1702中存储了前述图5-图12中的步骤对应的程序指令以及数据。

[0384] 处理器1701用于执行前述图5-图12中任一实施例所示的服务器执行的方法步骤。

[0385] 收发器1703,用于接收或者发送数据。

[0386] 可选地,前述的图17中所示的访问控制节点可以为芯片。

[0387] 本申请实施例中还提供一种计算机可读存储介质,该计算机可读存储介质中存储有程序,当其在计算机上运行时,使得计算机执行如前述图5-图12所示实施例描述的方法中的步骤。

[0388] 本申请实施例还提供了一种信息管理设备,该信息管理设备也可以称为数字处理芯片或者芯片,芯片包括处理单元和通信接口,处理单元通过通信接口获取程序指令,程序指令被处理单元执行,处理单元用于执行前述图5-图12中任一实施例所示的方法步骤。

[0389] 本申请实施例还提供一种数字处理芯片。该数字处理芯片中集成了用于实现上述处理器,或者处理器的功能的电路和一个或者多个接口。当该数字处理芯片中集成了存储器时,该数字处理芯片可以完成前述实施例中的任一个或多个实施例的方法步骤。当该数字处理芯片中未集成存储器时,可以通过通信接口与外置的存储器连接。该数字处理芯片根据外置的存储器中存储的程序代码来实现上述图5-图12中任一实施例所示的方法步骤。

[0390] 本申请实施例中还提供一种包括计算机程序产品,当其在计算机上行驶时,使得计算机执行如前述图5-图12所示实施例描述的方法中的步骤。

[0391] 本申请实施例提供的信息管理设备可以为芯片,芯片包括:处理单元和通信单元,所述处理单元例如可以是处理器,所述通信单元例如可以是输入/输出接口、管脚或电路等。该处理单元可执行存储单元存储的计算机执行指令,以使服务器内的芯片执行上述图5-图12所示实施例描述的方法。可选地,所述存储单元为所述芯片内的存储单元,如寄存器、缓存等,所述存储单元还可以是所述无线接入设备端内的位于所述芯片外部的存储单元,如只读存储器(read-only memory,ROM)或可存储静态信息和指令的其他类型的静态存储设备,随机存取存储器(random access memory,RAM)等。

[0392] 具体地,前述的处理单元或者处理器可以是中央处理器(central processing unit,CPU)、网络处理器(neural-network processing unit,NPU)、图形处理器(graphics processing unit,GPU)、数字信号处理器(digital signal processor,DSP)、专用集成电路(application specific integrated circuit,ASIC)或现场可编程逻辑门阵列(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、分立硬件组件等。通用处理器可以是微处理器或者也可以是任何常规的处理器等。

[0393] 另外需说明的是,以上所描述的装置实施例仅仅是示意性的,其中所述作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。另外,本申请提供的装置实施例附图中,模块之间的连接关系表示它们之间具有通信连接,具体可以实现为一条或多条通信总线或信号线。

[0394] 通过以上的实施方式的描述,所属领域的技术人员可以清楚地了解到本申请可借助软件加必需的通用硬件的方式来实现,当然也可以通过专用硬件包括专用集成电路、专用CPU、专用存储器、专用元器件等来实现。一般情况下,凡由计算机程序完成的功能都可以很容易地用相应的硬件来实现,而且,用来实现同一功能的具体硬件结构也可以是多种多样的,例如模拟电路、数字电路或专用电路等。但是,对本申请而言更多情况下软件程序实现是更佳的实施方式。基于这样的理解,本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来,该计算机软件产品存储在可读取的存储介质中,如计算机的软盘、U盘、移动硬盘、只读存储器(read only memory,ROM)、随机存取存储器(random access memory,RAM)、磁碟或者光盘等,包括若干指令用以使得一台计算机设备(可以是个人计算机,服务器,或者网络设备等)执行本申请各个实施例所述的方法。

[0395] 在上述实施例中,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。

[0396] 所述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所述计算机程序指令时,全部或部分地产生按照本申请实施例所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述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计算机可读存储介质传输,例如,所述计算机指令可以从一个网站站点、计算机、服务器或数据中心通过有线(例如同轴电缆、光纤、数字用户线(DSL))或无线(例如红外、无线、微波等)方式向另一个网站站点、计算机、服务器或数据中心进行传输。所述计算机可读存储介质可以是计算机能够存储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。所述可用介质可以是磁性介质,(例如,软盘、硬盘、磁带)、光介质(例如,DVD)、或者半导体介质(例如固态硬盘(solid state disk,SSD))等。

[0397] 本申请的说明书和权利要求书及上述附图中的术语“第一”、“第二”、“第三”、“第四”等(如果存在)是用于区别类似的对象,而不必用于描述特定的顺序或先后次序。应该理解这样使用的数据在适当情况下可以互换,以便这里描述的实施例能够以除了在这里图示或描述的内容以外的顺序实施。此外,术语“包括”和“具有”以及他们的任何变形,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、系统、产品或设备不必限于清楚地列出的那些步骤或单元,而是可包括没有清楚地列出的或对于这些过程、方法、产品或设备固有的其它步骤或单元。

[0398] 最后应说明的是:以上,仅为本申请的具体实施方式,但本申请的保护范围并不局限于此,任何熟悉本技术领域的技术人员在本申请揭露的技术范围内,可轻易想到变化或替换,都应涵盖在本申请的保护范围之内。

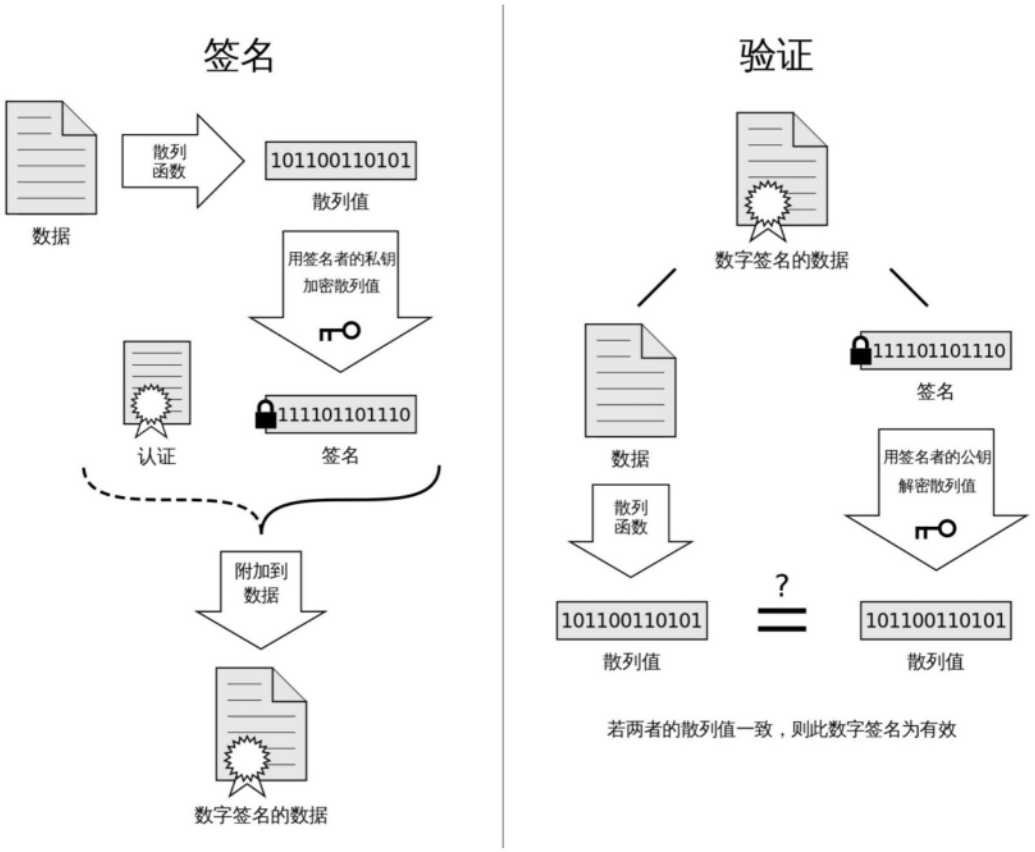

签名
数据
散列
函数
101100110101
散列值
用签名者的私钥
加密散列值
111101101110
签名
认证
附加到
数据
数字签名的数据
验证
数字签名的数据
数据
111101101110
签名
用签名者的公钥
解密散列值
散列
函数
?
101100110101
散列值
101100110101
散列值
若两者的散列值一致，则此数字签名为有效

图1

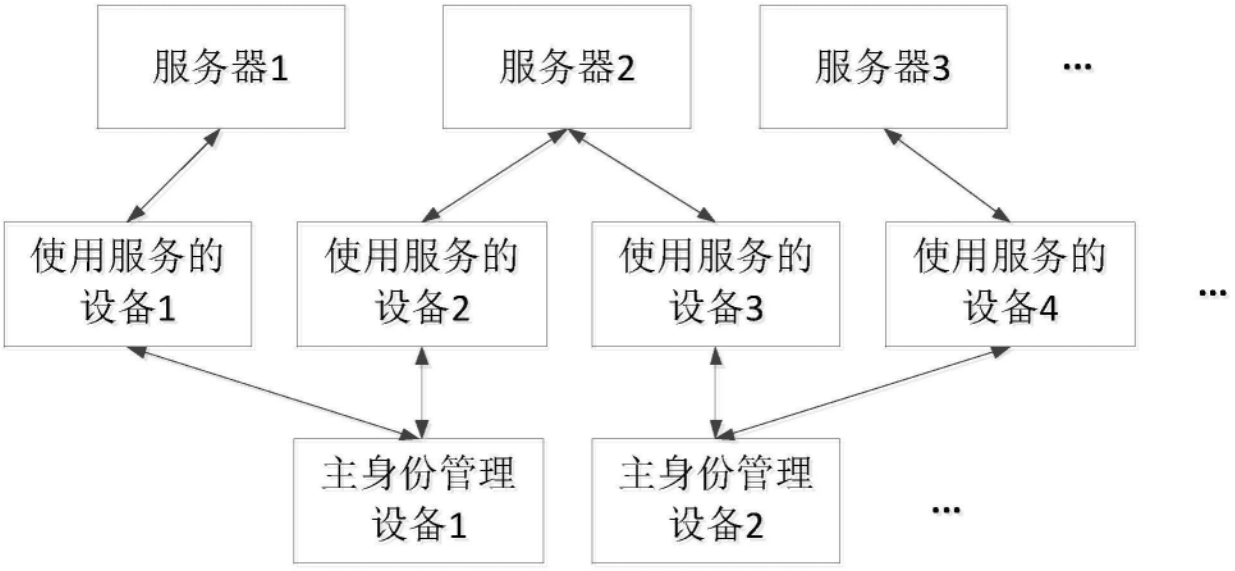

服务器1
服务器2
服务器3
...
使用服务的
设备1
使用服务的
设备2
使用服务的
设备3
使用服务的
设备4
...
主身份管理
设备1
主身份管理
设备2
...

图2

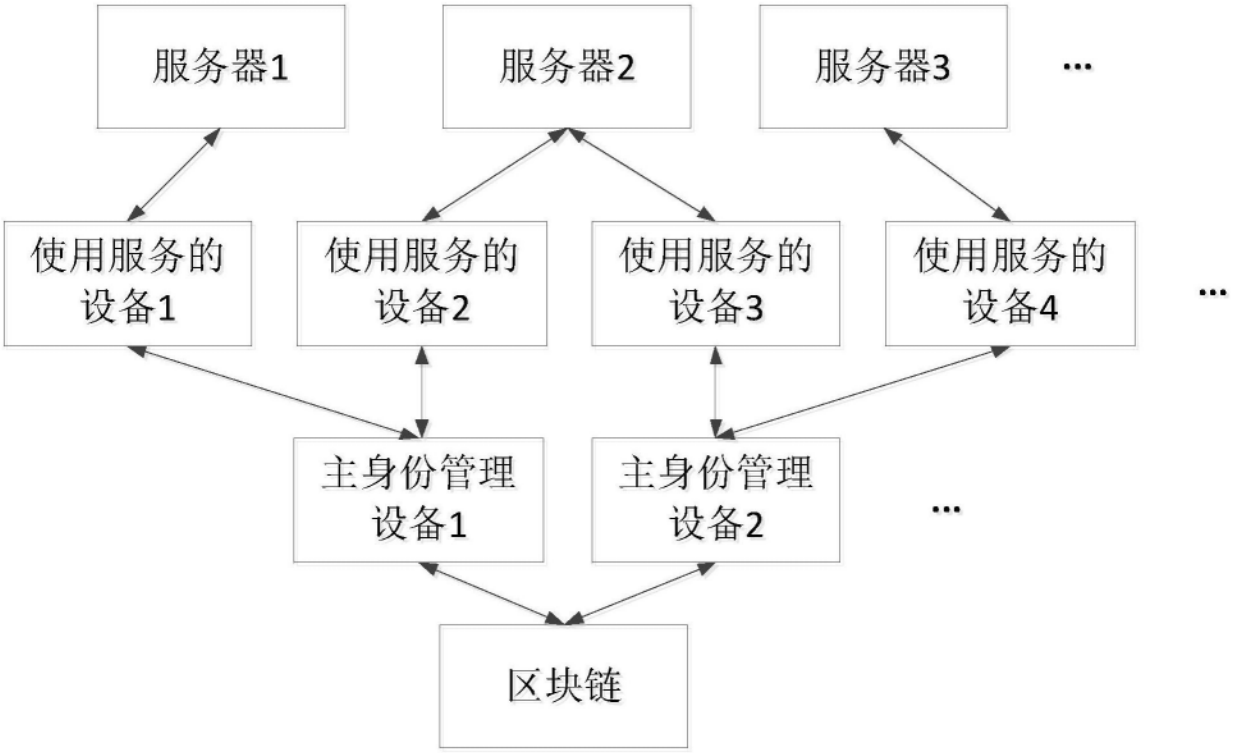

服务器1
服务器2
服务器3
...
使用服务的设备1
使用服务的设备2
使用服务的设备3
使用服务的设备4
...
主身份管理设备1
主身份管理设备2
...
区块链

图3

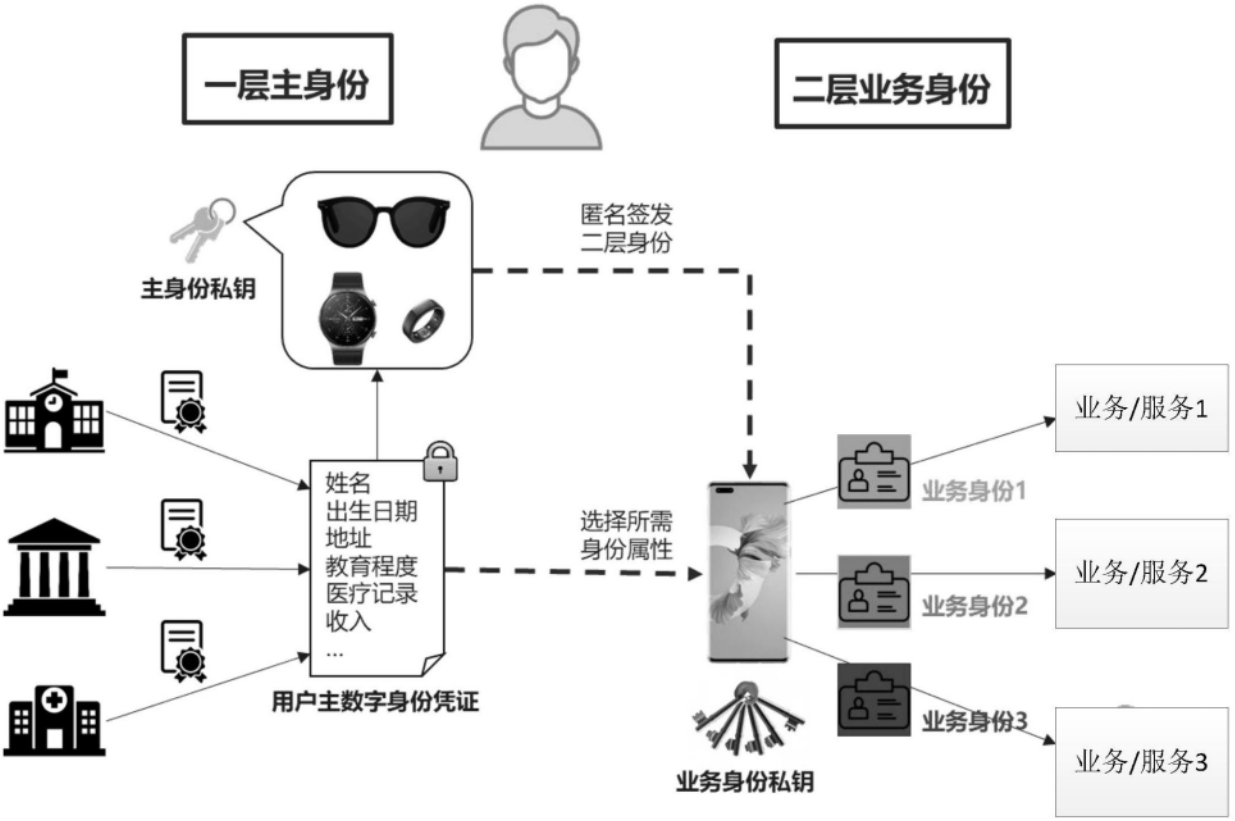

一层主身份
二层业务身份
主身份私钥
匿名签发二层身份
姓名
出生日期
地址
教育程度
医疗记录
收入
...
用户主数字身份凭证
选择所需身份属性
业务身份1
业务身份2
业务身份3
业务身份私钥
业务/服务1
业务/服务2
业务/服务3

图4

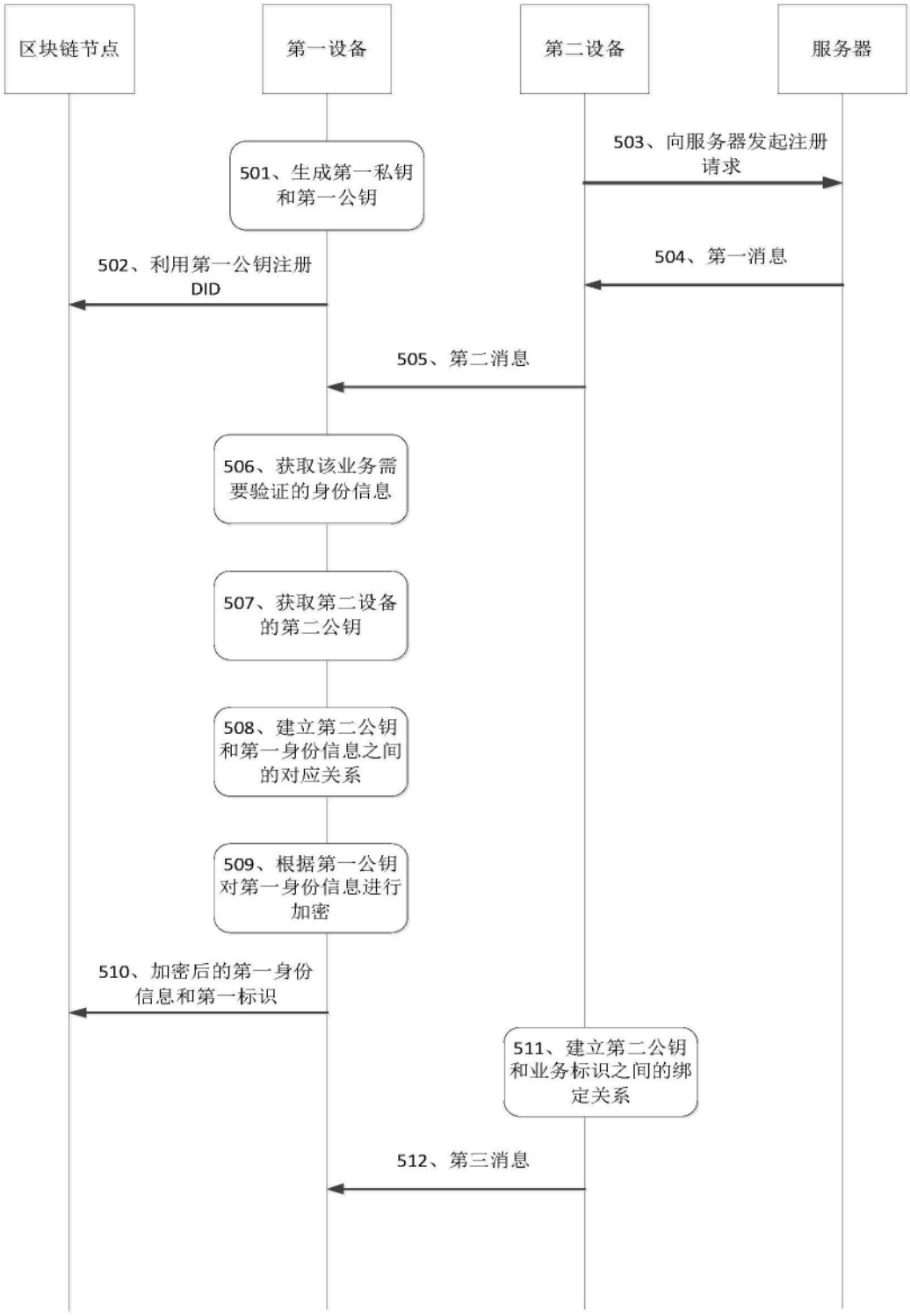

区块链节点
第一设备
第二设备
服务器
501、生成第一私钥和第一公钥
503、向服务器发起注册请求
502、利用第一公钥注册DID
504、第一消息
505、第二消息
506、获取该业务需要验证的身份信息
507、获取第二设备的第二公钥
508、建立第二公钥和第一身份信息之间的对应关系
509、根据第一公钥对第一身份信息进行加密
510、加密后的第一身份信息和第一标识
511、建立第二公钥和业务标识之间的绑定关系
512、第三消息

图5

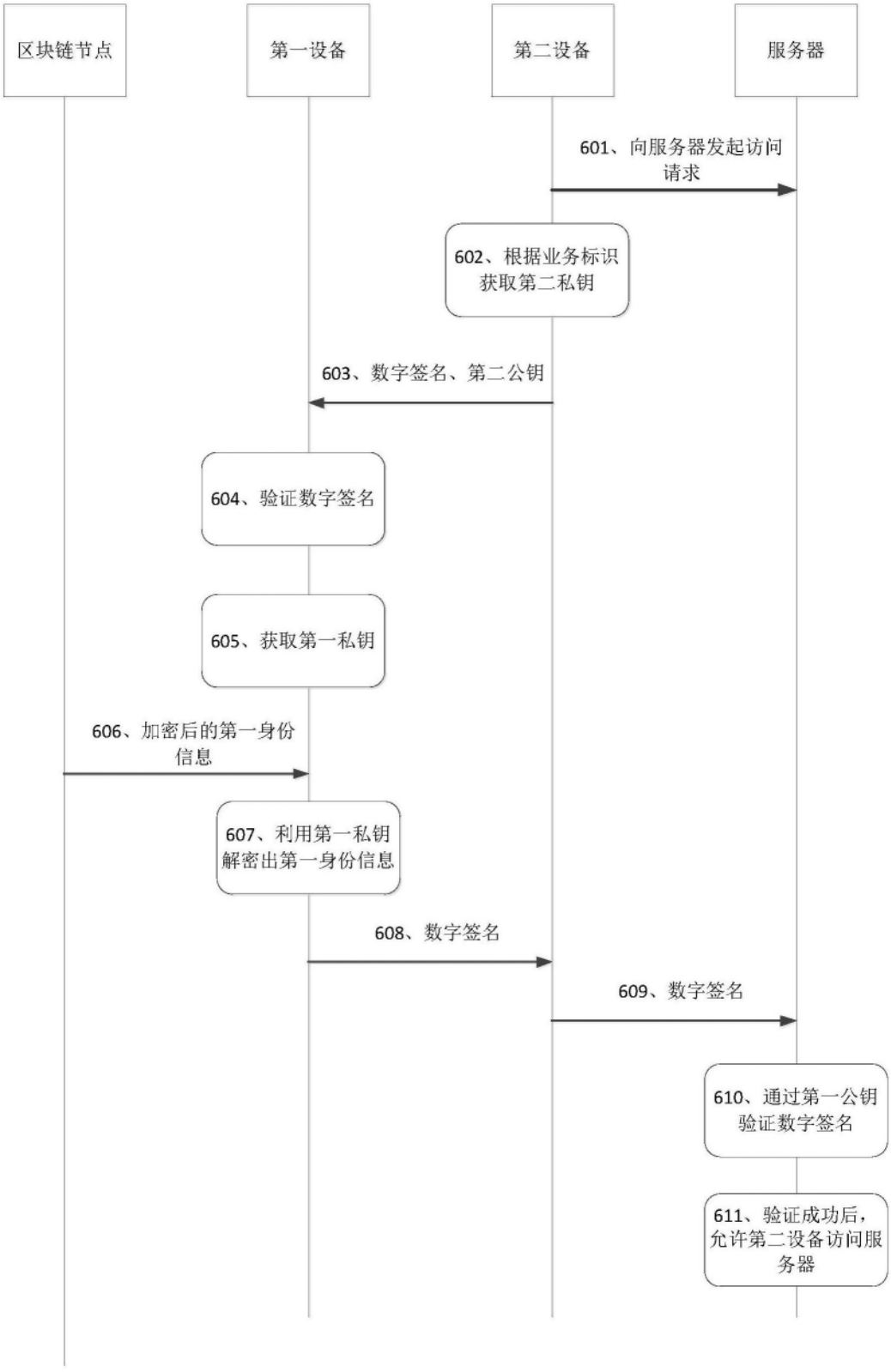

区块链节点
第一设备
第二设备
服务器
601、向服务器发起访问请求
602、根据业务标识获取第二私钥
603、数字签名、第二公钥
604、验证数字签名
605、获取第一私钥
606、加密后的第一身份信息
607、利用第一私钥解密出第一身份信息
608、数字签名
609、数字签名
610、通过第一公钥验证数字签名
611、验证成功后，允许第二设备访问服务器

图6

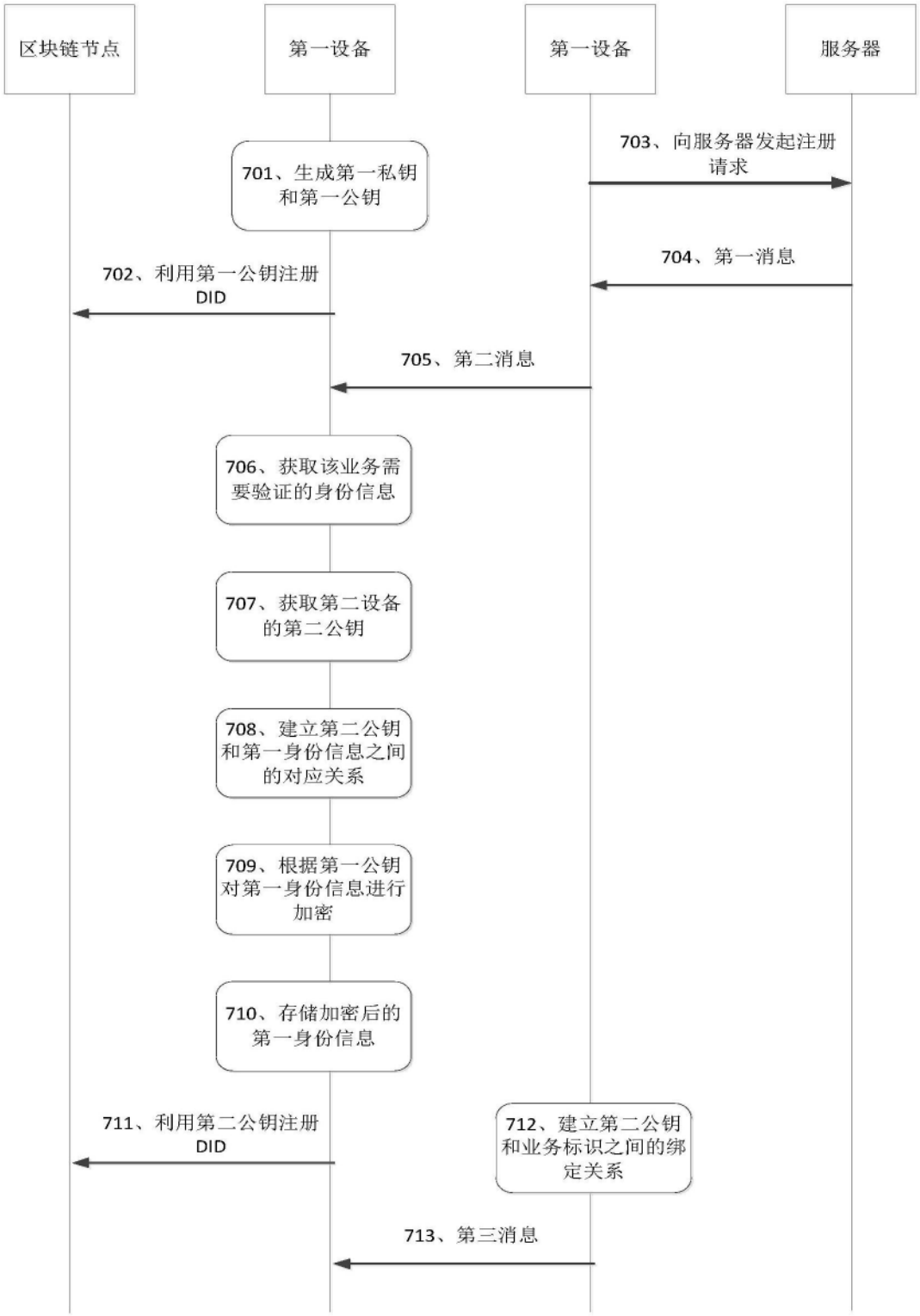

区块链节点
第一设备
第一设备
服务器
703、向服务器发起注册请求
701、生成第一私钥和第一公钥
704、第一消息
702、利用第一公钥注册DID
705、第二消息
706、获取该业务需要验证的身份信息
707、获取第二设备的第二公钥
708、建立第二公钥和第一身份信息之间的对应关系
709、根据第一公钥对第一身份信息进行加密
710、存储加密后的第一身份信息
711、利用第二公钥注册DID
712、建立第二公钥和业务标识之间的绑定关系
713、第三消息

图7

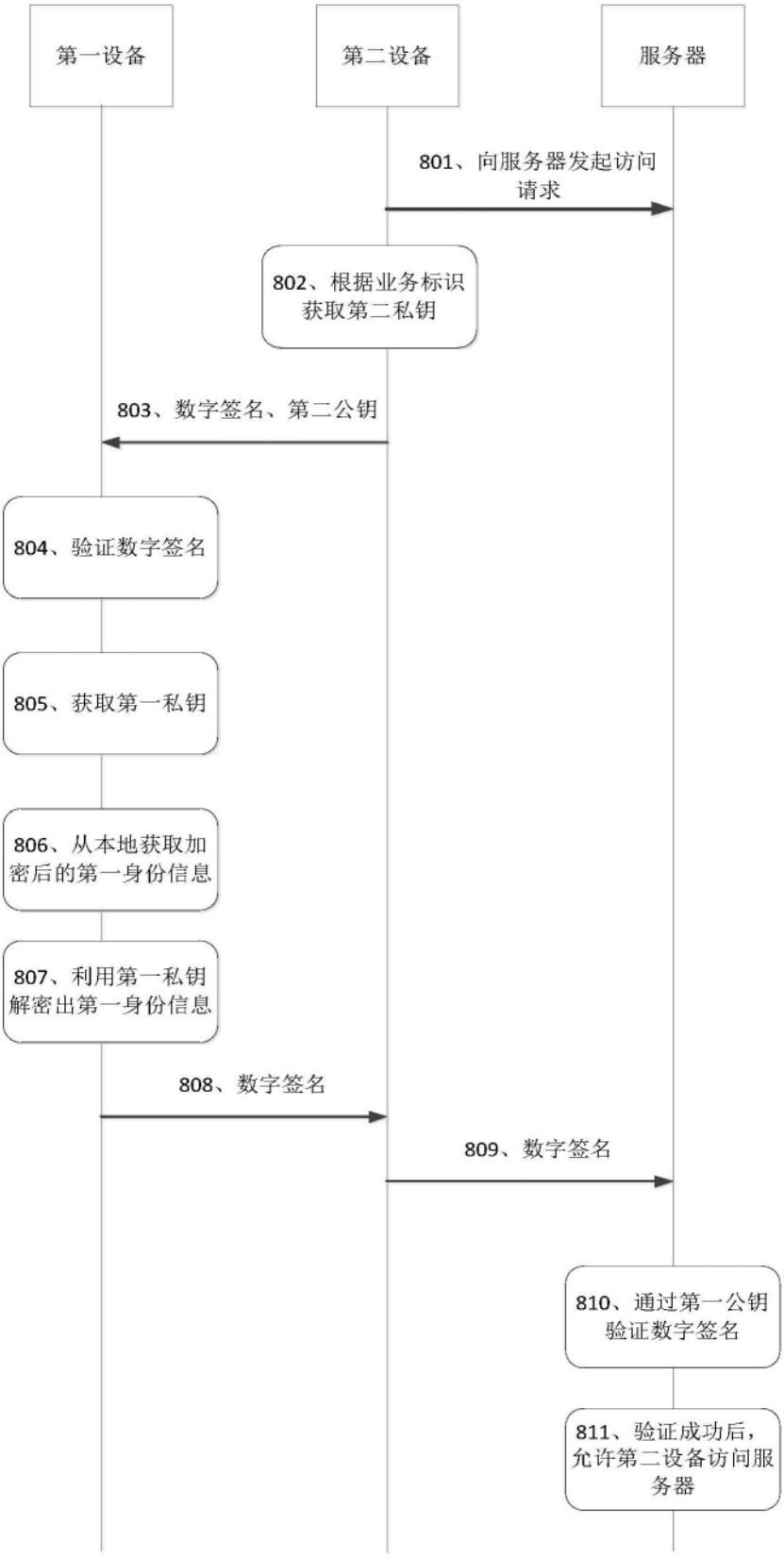

第一设备
第二设备
服务器
801、向服务器发起访问请求
802、根据业务标识获取第二私钥
803、数字签名、第二公钥
804、验证数字签名
805、获取第一私钥
806、从本地获取加密后的第一身份信息
807、利用第一私钥解密出第一身份信息
808、数字签名
809、数字签名
810、通过第一公钥验证数字签名
811、验证成功后，允许第二设备访问服务器

图8

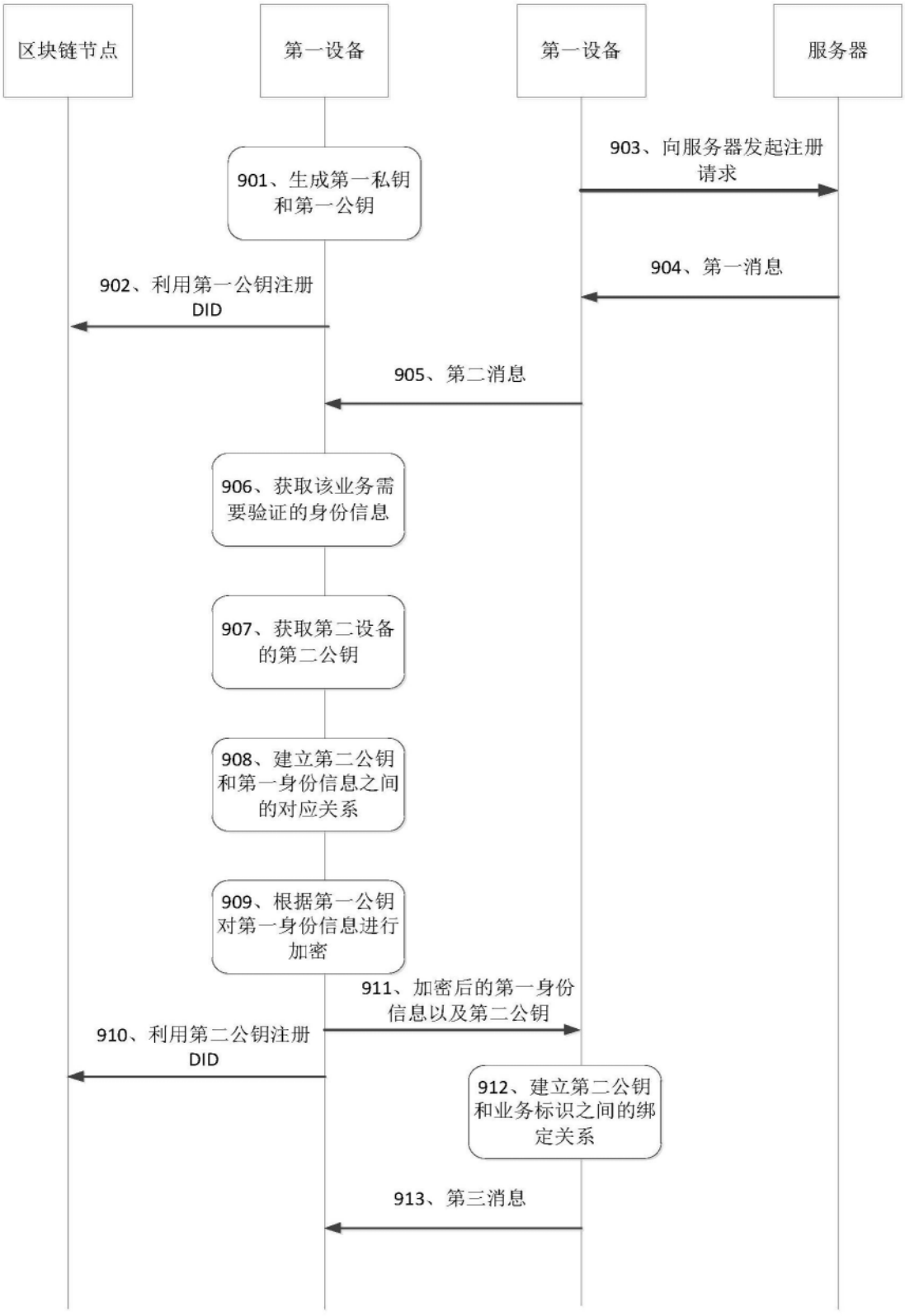

区块链节点
第一设备
第一设备
服务器
901、生成第一私钥和第一公钥
903、向服务器发起注册请求
902、利用第一公钥注册DID
904、第一消息
905、第二消息
906、获取该业务需要验证的身份信息
907、获取第二设备的第二公钥
908、建立第二公钥和第一身份信息之间的对应关系
909、根据第一公钥对第一身份信息进行加密
911、加密后的第一身份信息以及第二公钥
910、利用第二公钥注册DID
912、建立第二公钥和业务标识之间的绑定关系
913、第三消息

图9

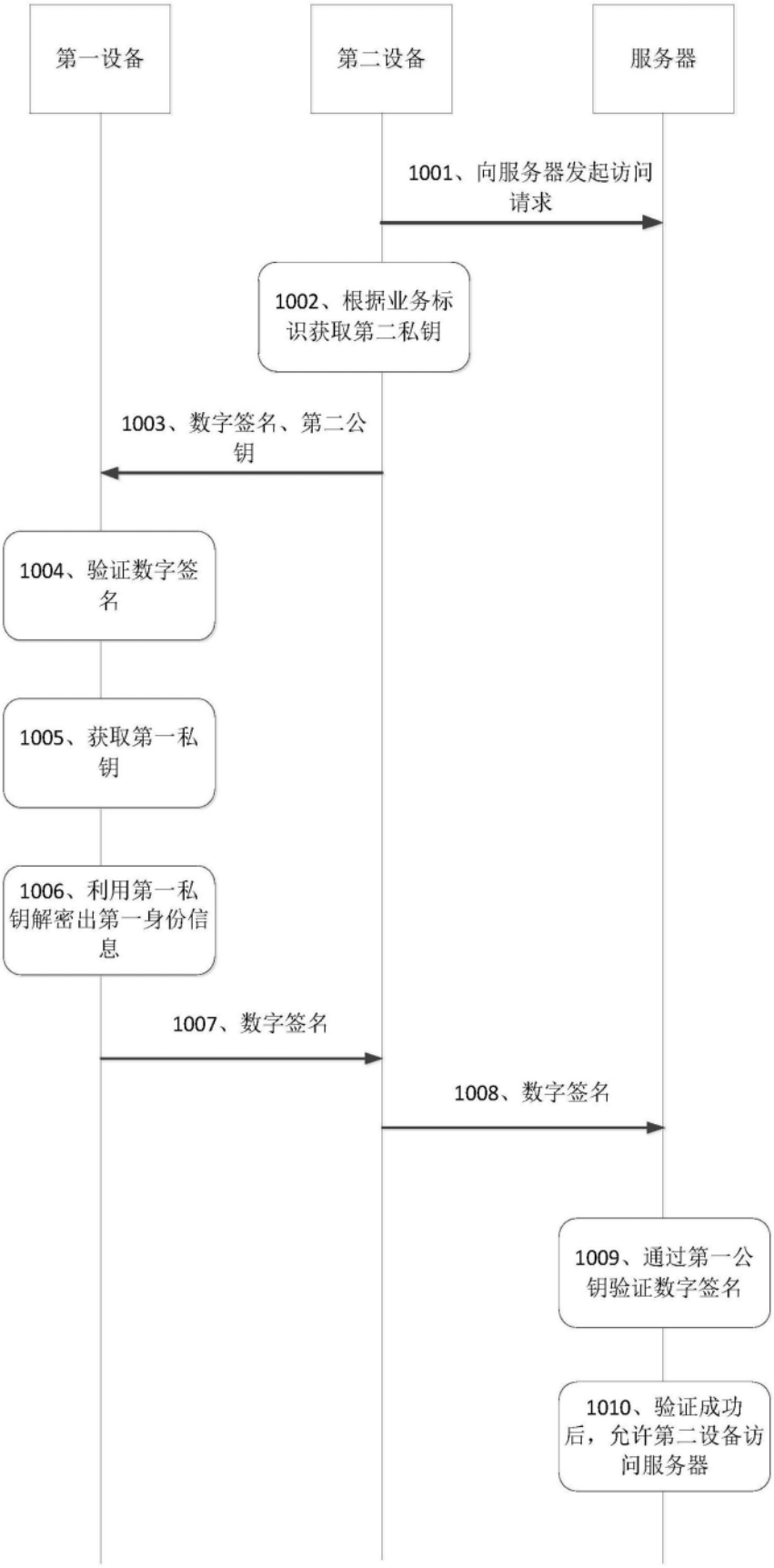

第一设备
第二设备
服务器
1001、向服务器发起访问请求
1002、根据业务标识获取第二私钥
1003、数字签名、第二公钥
1004、验证数字签名
1005、获取第一私钥
1006、利用第一私钥解密出第一身份信息
1007、数字签名
1008、数字签名
1009、通过第一公钥验证数字签名
1010、验证成功后，允许第二设备访问服务器

图10

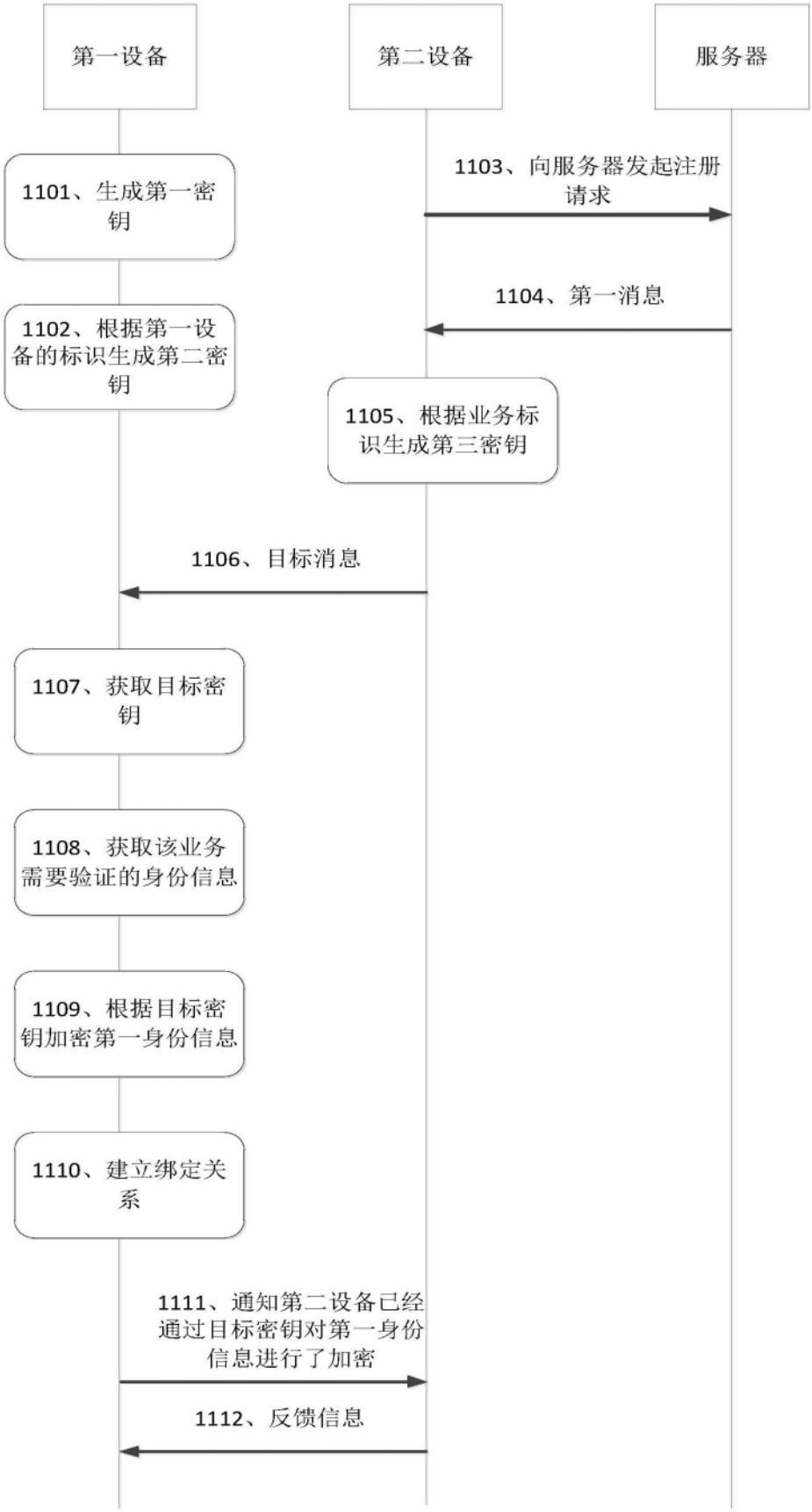

第一设备
第二设备
服务器
1101、生成第一密钥
1103、向服务器发起注册请求
1104、第一消息
1102、根据第一设备的标识生成第二密钥
1105、根据业务标识生成第三密钥
1106、目标消息
1107、获取目标密钥
1108、获取该业务需要验证的身份信息
1109、根据目标密钥加密第一身份信息
1110、建立绑定关系
1111、通知第二设备已经通过目标密钥对第一身份信息进行了加密
1112、反馈信息

图11

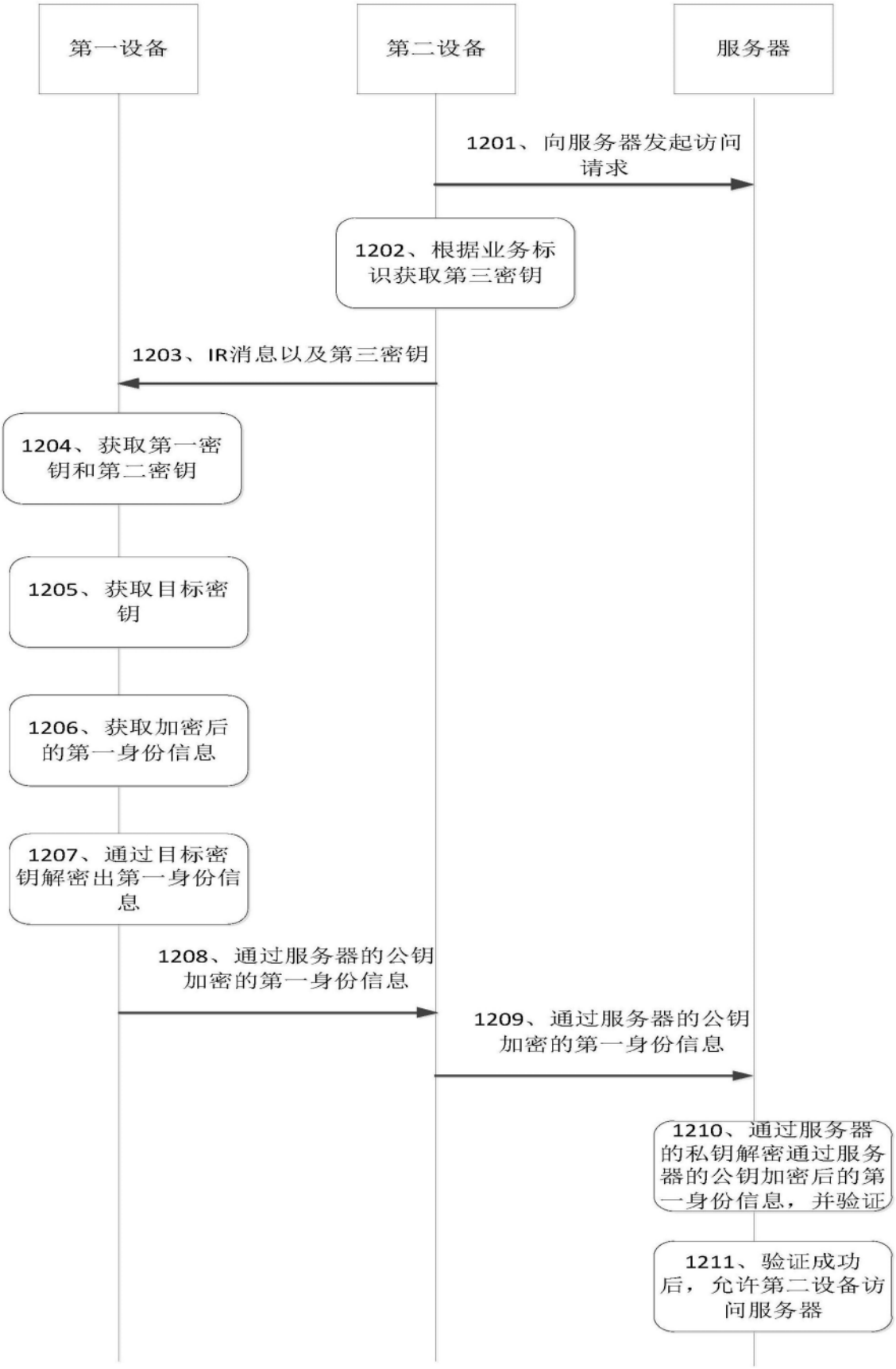

第一设备
第二设备
服务器
1201、向服务器发起访问请求
1202、根据业务标识获取第三密钥
1203、IR消息以及第三密钥
1204、获取第一密钥和第二密钥
1205、获取目标密钥
1206、获取加密后的第一身份信息
1207、通过目标密钥解密出第一身份信息
1208、通过服务器的公钥加密的第一身份信息
1209、通过服务器的公钥加密的第一身份信息
1210、通过服务器的私钥解密通过服务器的公钥加密后的第一身份信息，并验证
1211、验证成功后，允许第二设备访问服务器

图12

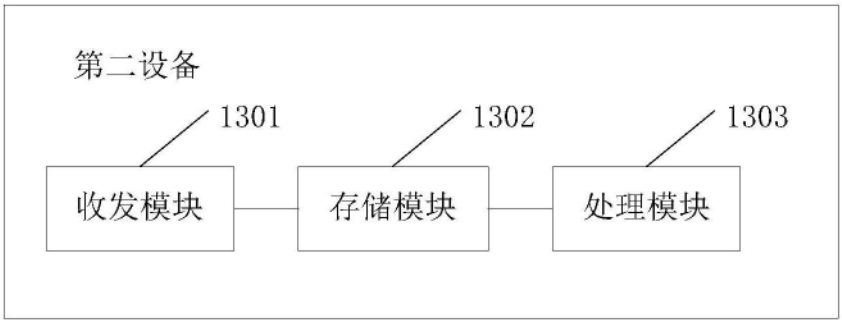

第二设备
1301
1302
1303
收发模块
存储模块
处理模块

图13

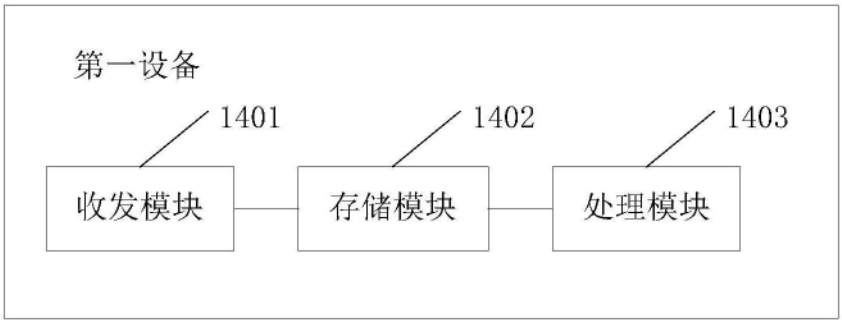

第一设备
1401
1402
1403
收发模块
存储模块
处理模块

图14

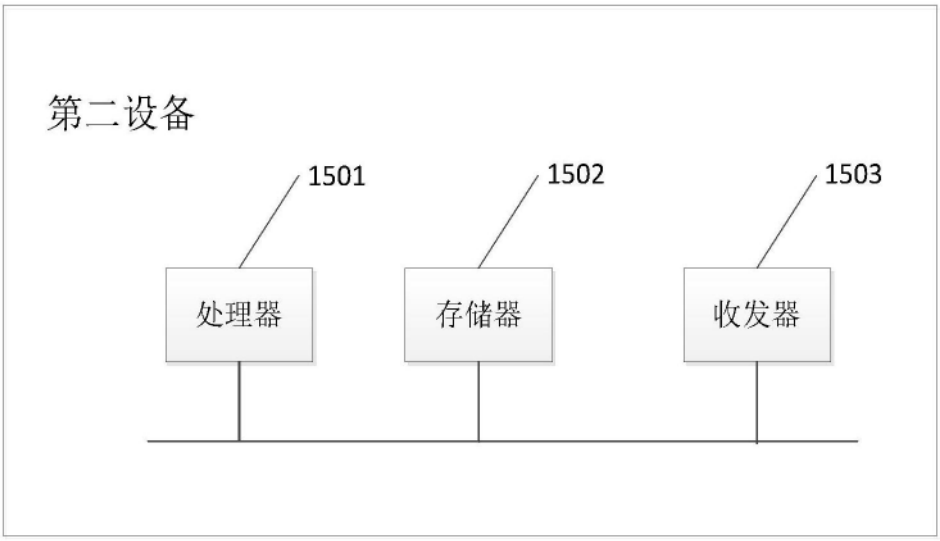

第二设备
1501
1502
1503
处理器
存储器
收发器

图15

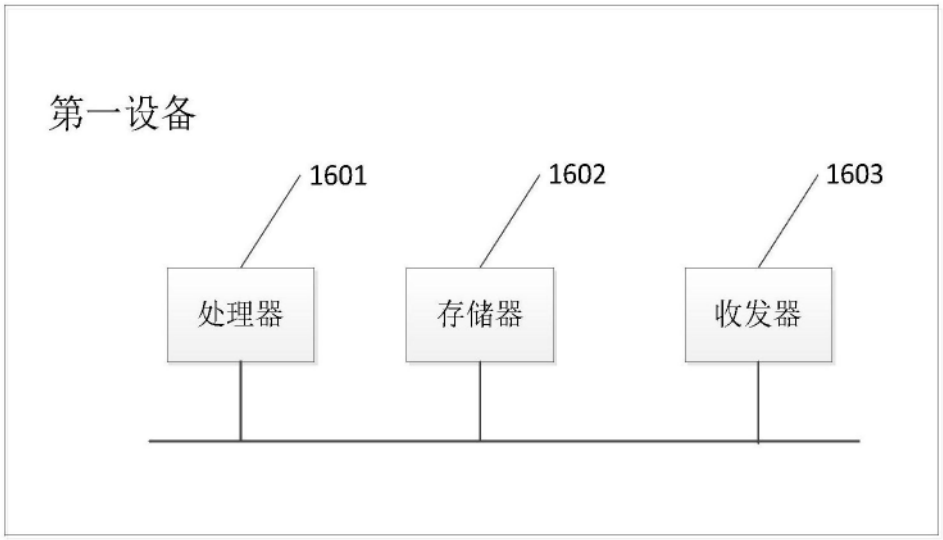


图16

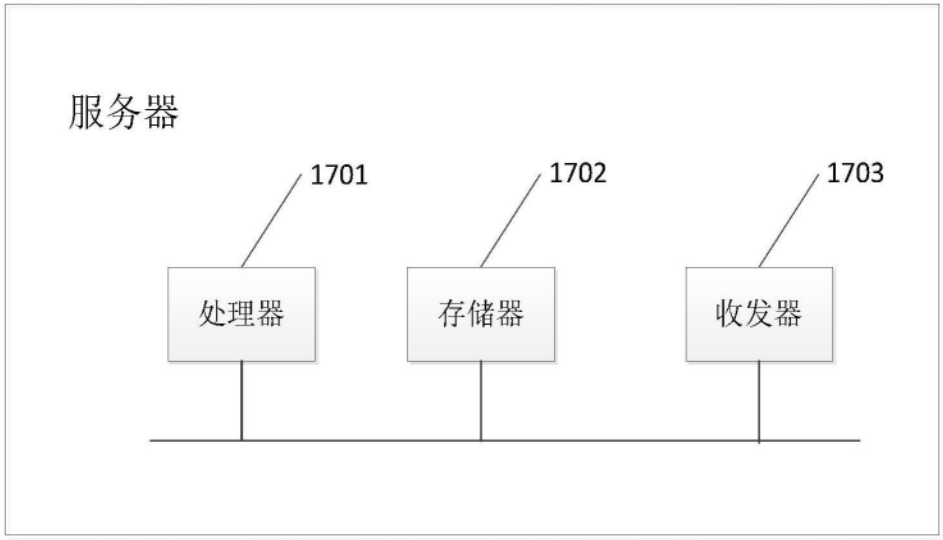


图17