(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115460019 B
(45)授权公告日 2023.03.24

(21)申请号 202211401670.5
(22)申请日 2022.11.10
(65)同一申请的已公布的文献号
申请公布号 CN 115460019 A
(43)申请公布日 2022.12.09
(73)专利权人 中国信息通信研究院
地址 100191 北京市海淀区学院路40号
(72)发明人 李瑾 郭健 张波
(74)专利代理机构 北京思源智汇知识产权代理有限公司 11657
专利代理师 李林莎
(51)Int.Cl.
H04L 9/40(2022.01)
H04L 67/51(2022.01)

(56)对比文件
CN 113010870 A,2021.06.22
CN 112581126 A,2021.03.30
CN 110826107 A,2020.02.21
US 2015304847 A1,2015.10.22

审查员 刘丽

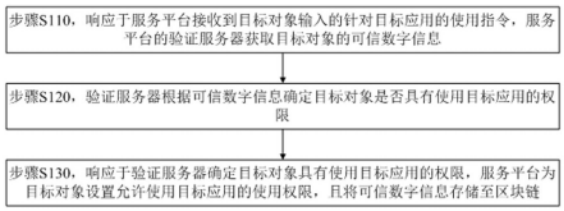
权利要求书3页 说明书15页 附图5页

(54)发明名称

基于数字身份的目标应用提供方法和装置、设备和介质

(57)摘要

本公开实施例公开了一种基于数字身份的目标应用提供方法和装置、设备和介质，其中，方法包括：当服务平台接收到目标对象输入的针对目标应用的使用指令时，服务平台的验证服务器获取目标对象的可信数字信息；验证服务器根据可信数字信息确定目标对象是否具有使用目标应用的权限；当验证服务器确定目标对象具有使用目标应用的权限，服务平台为目标对象设置允许使用目标应用的使用权限，且将可信数字信息存储至区块链。实现了可以利用数字身份标识对应的可验证凭证确定目标对象是否具有使用目标应用的权限，提高了目标对象的使用体验。



CN 115460019 B

1.一种基于数字身份的目标应用提供方法,其特征在于,包括:

响应于服务平台接收到目标对象输入的针对目标应用的使用指令,所述服务平台的验证服务器获取所述目标对象的可信数字信息,其中,所述可信数字信息包括所述目标对象登录所述服务平台的数字身份标识所对应的可验证凭证中的至少一条验证信息;

所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限;

响应于所述验证服务器确定所述目标对象具有使用所述目标应用的权限,所述服务平台为所述目标对象设置允许使用所述目标应用的使用权限,且将所述可信数字信息存储至区块链;

其中,所述服务平台的验证服务器获取所述目标对象的可信数字信息,包括:

所述目标对象的客户端接收出示可信数字信息的出示请求,其中,所述出示请求包括:所述目标应用对应的使用条件;

所述客户端基于所述目标应用对应的使用条件,确定可验证信息,其中,所述可验证信息包括所述数字身份标识所对应的可验证凭证中的至少一条验证信息;

响应于所述客户端发送的所述可验证信息符合所述目标应用对应的使用条件,所述验证服务器根据所述可验证信息,确定所述目标对象的初始可信数字信息,其中,所述初始可信数字信息具有由所述验证服务器的公私密钥对中私钥生成的签名;

所述客户端利用所述验证服务器的公私密钥对中公钥对所述初始可信数字信息的签名进行验证;

响应于所述初始可信数字信息的签名通过验证,所述客户端利用所述目标对象的公私密钥对中私钥对所述初始可信数字信息进行签名处理,得到所述可信数字信息;

所述客户端将所述可信数字信息发送至 所述验证服务器。

2.根据权利要求1所述的方法,其特征在于,所述可信数字信息具有由所述目标对象的公私密钥对中私钥生成的签名;

所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限,包括:

所述验证服务器通过所述目标对象的公私密钥对中公钥对所述可信数字信息的签名进行验证;

响应于所述可信数字信息的签名通过验证,确定所述目标对象具有使用所述目标应用的权限。

3.根据权利要求1所述的方法,其特征在于,所述出示请求还包括:所述验证服务器的授权凭证,其中,所述授权凭证具有由所述验证服务器的公私密钥对中私钥生成的签名;

所述方法还包括:

所述客户端利用所述验证服务器的公私密钥对中公钥对所述授权凭证的签名进行验证;

响应于所述授权凭证的签名通过所述验证服务器的公私密钥对中公钥的验证,所述客户端基于所述授权凭证,确定所述验证服务器是否具有获取所述目标应用对应的使用条件所指示的验证信息的权限;

响应于所述验证服务器具有获取所述目标应用对应的使用条件所指示的验证信息的

权限，所述客户端执行所述客户端基于所述目标应用对应的使用条件，确定所述可验证信息的操作。

4.根据权利要求1或2所述的方法，其特征在于，还包括：

响应于所述服务平台接收所述目标对象输入的登录请求，所述服务平台的登录服务器获取所述数字身份标识；

所述登录服务器确定所述数字身份标识是否符合预设标识条件；

响应于所述数字身份标识符合所述预设标识条件，所述登录服务器生成令牌；

所述目标对象基于所述数字身份标识和所述令牌登录所述服务平台。

5.根据权利要求4所述的方法，其特征在于，所述登录服务器确定所述数字身份标识是否符合预设标识条件，包括：

所述登录服务器确定所述数字身份标识的格式是否符合预设标识格式条件；

响应于所述数字身份标识的格式符合所述预设标识格式条件，所述登录服务器向所述目标对象的客户端发送随机数；

所述客户端利用所述目标对象的公私密钥对中私钥对所述随机数进行签名处理，得到签名随机数；

所述登录服务器利用所述目标对象的公私密钥对中公钥对所述签名随机数的签名进行验证；

响应于所述签名随机数的签名通过所述目标对象的公私密钥对中公钥的验证，所述登录服务器确定所述数字身份标识符合所述预设标识条件。

6.一种基于数字身份的目标应用提供装置，其特征在于，包括：

第一获取模块，用于响应于服务平台接收到目标对象输入的针对目标应用的使用指令，所述服务平台的验证服务器获取所述目标对象的可信数字信息，其中，所述可信数字信息包括所述目标对象登录所述服务平台的数字身份标识所对应的可验证凭证中的至少一条验证信息；

第一判断模块，用于所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限；

应用许可模块，用于响应于所述验证服务器确定所述目标对象具有使用所述目标应用的权限，所述服务平台为所述目标对象设置允许使用所述目标应用的使用权限，且将所述可信数字信息存储至区块链；

其中，所述第一获取模块包括：

接收子模块，用于所述目标对象的客户端接收出示可信数字信息的出示请求，其中，所述出示请求包括：所述目标应用对应的使用条件；

第二确定子模块，用于所述客户端基于所述目标应用对应的使用条件，确定可验证信息，其中，所述可验证信息包括所述数字身份标识所对应的可验证凭证中的至少一条验证信息；

第三确定子模块，用于响应于所述客户端发送的所述可验证信息符合所述目标应用对应的使用条件，所述验证服务器根据所述可验证信息，确定所述目标对象的初始可信数字信息，其中，所述初始可信数字信息具有由所述验证服务器的公私密钥对中私钥生成的签名；

第二签名验证子模块，用于所述客户端利用所述验证服务器的公私密钥对中公钥对所述初始可信数字信息的签名进行验证；

第一签名子模块，用于响应于所述初始可信数字信息的签名通过验证，所述客户端利用所述目标对象的公私密钥对中私钥对所述初始可信数字信息进行签名处理，得到所述可信数字信息；

发送子模块，用于所述客户端将所述可信数字信息发送至 所述验证服务器。

7.根据权利要求6所述的装置，其特征在于，所述可信数字信息具有由所述目标对象的公私密钥对中私钥生成的签名；所述第一判断模块包括：

第一签名验证子模块，用于所述验证服务器通过所述目标对象的公私密钥对中公钥对所述可信数字信息的签名进行验证；

第一确定子模块，用于响应于所述可信数字信息的签名通过验证，确定所述目标对象具有使用所述目标应用的权限。

8.一种电子设备，其特征在于，包括：

存储器，用于存储计算机程序；

处理器，用于执行所述存储器中存储的计算机程序，且所述计算机程序被执行时，实现上述权利要求1-5中任一所述的方法。

9.一种计算机可读存储介质，其上存储有计算机程序，其特征在于，该计算机程序被处理器执行时，实现上述权利要求1-5中任一所述的方法。

基于数字身份的目标应用提供方法和装置、设备和介质

技术领域

[0001] 本公开涉及数字身份技术、应用权限管理技术领域，尤其是一种基于数字身份的目标应用提供方法和装置、设备和介质。

背景技术

[0002] 服务平台是一个将多种应用或功能集合在一起的一个综合性应用平台。现有技术中，服务平台针对不同服务内容以及服务对象，其开发出了多种应用，用户可以通过其数字身份中数字身份标识登录服务平台使用应用。用户的数字身份标识可以对应的多个的可验证凭证，不同的可验证凭证表示用户可以具有不同的属性，如何将数字身份与用户对应用的使用权限结合一个亟待解决的问题。

发明内容

[0003] 本公开实施例提供一种基于数字身份的目标应用提供方法和装置、设备和介质，以解决上述问题。

[0004] 本公开实施例的一个方面，提供了一种基于数字身份的目标应用提供方法，包括：响应于服务平台接收到目标对象输入的针对目标应用的使用指令，所述服务平台的验证服务器获取所述目标对象的可信数字信息，其中，所述可信数字信息包括所述目标对象登录所述服务平台的数字身份标识所对应的可验证凭证中的至少一条验证信息；所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限；响应于所述验证服务器确定所述目标对象具有使用所述目标应用的权限，所述服务平台为所述目标对象设置允许使用所述目标应用的使用权限，且将所述可信数字信息存储至区块链。

[0005] 可选地，在本公开上述任一实施例的方法中，所述可信数字信息具有由所述目标对象的公私密钥对中私钥生成的签名；所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限，包括：所述验证服务器通过所述目标对象的公私密钥对中公钥对所述可信数字信息的签名进行验证；响应于所述可信数字信息的签名通过验证，确定所述目标对象具有使用所述目标应用的权限。

[0006] 可选地，在本公开上述任一实施例的方法中，所述服务平台的验证服务器获取所述目标对象的可信数字信息，包括：所述目标对象的客户端接收出示可信数字信息的出示请求，其中，所述出示请求包括：所述目标应用对应的使用条件；所述客户端基于所述目标应用对应的使用条件，确定可验证信息，其中，所述可验证信息包括所述数字身份标识所对应的可验证凭证中的至少一条验证信息；响应于所述客户端发送的所述可验证信息符合所述目标应用对应的使用条件，所述验证服务器根据所述可验证信息，确定所述目标对象的初始可信数字信息，其中，所述初始可信数字信息具有由所述验证服务器的公私密钥对中私钥签生成的签名；所述客户端利用所述验证服务器的公私密钥对中公钥对所述初始可信数字信息的签名进行验证；响应于所述初始可信数字信息的签名通过验证，所述客户端利用所述目标对象的公私密钥对中私钥对所述初始可信数字信息进行签名处理，得到所述可

信数字信息;所述客户端将所述可信数字信息发送所述验证服务器。

[0007] 可选地,在本公开上述任一实施例的方法中,所述出示请求还包括:所述验证服务器的授权凭证,其中,所述授权凭证具有由所述验证服务器的公私密钥对中私钥生成的签名;所述方法还包括:所述客户端利用所述验证服务器的公私密钥对中公钥对所述授权凭证的签名进行验证;响应于所述授权凭证的签名通过所述验证服务器的公私密钥对中公钥的验证,所述客户端基于所述授权凭证,确定所述验证服务器是否具有获取所述目标应用对应的使用条件所指示的验证信息的权限;响应于所述验证服务器具有获取所述目标应用对应的使用条件所指示的验证信息的权限,所述客户端执行所述客户端基于所述目标应用对应的使用条件,确定所述可验证信息的操作。

[0008] 可选地,在本公开上述任一实施例的方法中,还包括:响应于所述服务平台接收所述目标对象输入的登录请求,所述服务平台的登录服务器获取所述数字身份标识;所述登录服务器确定所述数字身份标识是否符合预设标识条件;响应于所述数字身份标识符合所述预设标识条件,所述登录服务器生成令牌;所述目标对象基于所述数字身份标识和所述令牌登录所述服务平台。

[0009] 可选地,在本公开上述任一实施例的方法中,所述登录服务器确定所述数字身份标识是否符合预设标识条件,包括:所述登录服务器确定所述数字身份标识的格式是否符合预设标识格式条件;响应于所述数字身份标识的格式符合所述预设标识格式条件,所述登录服务器向所述目标对象的客户端发送随机数;所述客户端利用所述目标对象的公私密钥对中私钥对所述随机数进行签名处理,得到签名随机数;所述登录服务器利用所述目标对象的公私密钥对中公钥对所述签名随机数的签名进行验证;响应于所述签名随机数的签名通过所述目标对象的公私密钥对中公钥的验证,所述登录服务器确定所述数字身份标识符合所述预设标识条件。

[0010] 本公开实施例的一个方面,提供了一种基于数字身份的目标应用提供装置,包括:第一获取模块,用于响应于服务平台接收到目标对象输入的针对目标应用的使用指令,所述服务平台的验证服务器获取所述目标对象的可信数字信息,其中,所述可信数字信息包括所述目标对象登录所述服务平台的数字身份标识所对应的可验证凭证中的至少一条验证信息;第一判断模块,用于所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限;应用许可模块,用于响应于所述验证服务器确定所述目标对象具有使用所述目标应用的权限,所述服务平台为所述目标对象设置允许使用所述目标应用的使用权限,且将所述可信数字信息存储至区块链。

[0011] 可选地,在本公开上述任一实施例的装置中,所述可信数字信息具有由所述目标对象的公私密钥对中私钥生成的签名;所述第一判断模块包括:第一签名验证子模块,用于所述验证服务器通过所述目标对象的公私密钥对中公钥对所述可信数字信息的签名进行验证;第一确定子模块,用于响应于所述可信数字信息的签名通过验证,确定所述目标对象具有使用所述目标应用的权限。

[0012] 本公开实施例的一个方面,提供了一种电子设备,包括:存储器,用于存储计算机程序;处理器,用于执行所述存储器中存储的计算机程序,且所述计算机程序被执行时,实现基于数字身份的目标应用提供方法。

[0013] 本公开实施例的一个方面,提供了一种计算机可读存储介质,其上存储有计算机

程序，该计算机程序被处理器执行时，实现上述基于数字身份的目标应用提供方法。

[0014] 本公开实施例提供了一种基于数字身份的目标应用提供方法和装置、设备和介质，包括：当服务平台接收到目标对象输入的针对目标应用的使用指令时，服务平台的验证服务器获取目标对象的可信数字信息；验证服务器根据可信数字信息确定目标对象是否具有使用目标应用的权限；当验证服务器确定目标对象具有使用目标应用的权限，服务平台为所述目标对象设置允许使用目标应用的使用权限，且将可信数字信息存储至区块链。由此，本公开实施例中，验证服务器的通过确定包括目标对象登录服务平台的数字身份标识对应的可验证凭证中的至少一条验证信息的可信数字信息，确定服务平台是否允许目标对象使用目标应用，实现了可以利用数字身份标识对应的可验证凭证确定目标对象是否具有使用目标应用的权限，提高了目标对象的使用体验。同时，由于可信数字信息中包括可验证凭证中的至少一条验证信息，用户可以根据自身需要使用的目标应用选择不同的可验证凭证以及数字身份标识，实现了目标对象对其数字身份以及数字身份的先关信息的自主选择、管理和应用。

[0015] 另外，本公开实施例中，无需目标对象主动发送可信数字信息，由验证服务器依据目标应用获取目标对象的可信数字信息，减少了用户操作，进一步提高了用户体验。

[0016] 下面通过附图和实施例，对本公开的技术方案做进一步的详细描述。

附图说明

[0017] 构成说明书的一部分的附图描述了本公开的实施例，并且连同描述一起用于解释本公开的原理。

[0018] 参照附图，根据下面的详细描述，可以更加清楚地理解本公开，其中：

[0019] 图1示出本公开实施例的基于数字身份的目标应用提供方法一个实施例的流程图；

[0020] 图2示出本公开实施例的步骤S120的流程图；

[0021] 图3示出本公开实施例的步骤S110的流程图；

[0022] 图4示出本公开实施例的基于数字身份的目标应用提供方法一个实施例的流程图；

[0023] 图5示出本公开实施例的基于数字身份的目标应用提供方法一个实施例的流程图；

[0024] 图6示出本公开实施例的步骤S320的流程图；

[0025] 图7示出本公开实施例的登录服务平台的时序图；

[0026] 图8示出本公开实施例的提供目标应用的时序图；

[0027] 图9为本公开实施例基于数字身份的目标应用提供装置一个实施例的结构示意图；

[0028] 图10为本公开电子设备一个应用实施例的结构示意图。

具体实施方式

[0029] 现在将参照附图来详细描述本公开的各种示例性实施例。应注意到：除非另外具体说明，否则在这些实施例中阐述的部件和步骤的相对布置、数字表达式和数值不限制本

公开的范围。

[0030] 本领域技术人员可以理解，本公开实施例中的“第一”、“第二”等术语仅用于区别不同步骤、设备或模块等，既不代表任何特定技术含义，也不表示它们之间的必然逻辑顺序。

[0031] 还应理解，在本公开实施例中，“多个”可以指两个或两个以上，“至少一个”可以指一个、两个或两个以上。

[0032] 还应理解，对于本公开实施例中提及的任一部件、数据或结构，在没有明确限定或者在前后文给出相反启示的情况下，一般可以理解为一个或多个。

[0033] 另外，本公开中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A和/或B，可以表示：单独存在A，同时存在A和B，单独存在B这三种情况。另外，本公开中字符“/”，一般表示前后关联对象是一种“或”的关系。

[0034] 还应理解，本公开对各个实施例的描述着重强调各个实施例之间的不同之处，其相同或相似之处可以相互参考，为了简洁，不再一一赘述。

[0035] 同时，应当明白，为了便于描述，附图中所示出的各个部分的尺寸并不是按照实际的比例关系绘制的。

[0036] 以下对至少一个示例性实施例的描述实际上仅仅是说明性的，决不作为对本公开及其应用或使用的任何限制。

[0037] 对于相关领域普通技术人员已知的技术、方法和设备可能不作详细讨论，但在适当情况下，所述技术、方法和设备应当被视为说明书的一部分。

[0038] 应注意到：相似的标号和字母在下面的附图中表示类似项，因此，一旦某一项在一个附图中被定义，则在随后的附图中不需要对其进行进一步讨论。

[0039] 本公开实施例可以应用于终端设备、计算机系统、服务器等电子设备，其可与众多其它通用或专用计算系统环境或配置一起操作。适于与终端设备、计算机系统、服务器等电子设备一起使用的众所周知的终端设备、计算系统、环境和/或配置的例子包括但不限于：个人计算机系统、服务器计算机系统、瘦客户机、厚客户机、手持或膝上设备、基于微处理器的系统、机顶盒、可编程消费电子产品、网络个人电脑、小型计算机系统、大型计算机系统和包括上述任何系统的分布式云计算技术环境，等等。

[0040] 终端设备、计算机系统、服务器等电子设备可以在由计算机系统执行的计算机系统可执行指令(诸如程序模块)的一般语境下描述。通常，程序模块可以包括例程、程序、目标程序、组件、逻辑、数据结构等等，它们执行特定的任务或者实现特定的抽象数据类型。计算机系统/服务器可以在分布式云计算环境中实施，分布式云计算环境中，任务是由通过通信网络链接的远程处理设备执行的。在分布式云计算环境中，程序模块可以位于包括存储设备的本地或远程计算系统存储介质上。

[0041] 图1示出本公开实施例中基于数字身份的目标应用提供方法的流程示意图。本实施例可应用在电子设备上，如图1所示，本实施例的基于数字身份的目标应用提供方法包括如下步骤：

[0042] 步骤S110，响应于服务平台接收到目标对象输入的针对目标应用的使用指令，服务平台的验证服务器获取目标对象的可信数字信息。

[0043] 其中，该可信数字信息包括目标对象登录服务平台的数字身份标识所对应的可验

证凭证中的至少一条验证信息。

[0044] 服务平台可以设置在计算机或服务器上,服务平台可以包括多个应用。每个应用可以实现至少一个服务功能,例如,应用可以为证书存储的应用、标识管理的应用等。目标对象可以通过鼠标单击或双击目标应用以触发输入针对目标应用的使用指令。目标对象可以为企业、组织、团体或个人等。验证服务器用于审核目标对象是否具有使用目标应用的权限,验证服务器可以为计算机或服务器等。

[0045] 数字身份可以包括数字身份标识和可验证凭证(Verifiable Credentials,VC)。数字身份标识用于标识目标对象,例如,数字身份标识可以为DID标识(Decentralized Identity,分布式数字身份)标识或BID(Blockchain-based Identity区块链基础身份)标识等,其中,BID标识是基于W3C的DID标准开发的分布式标识,BID标识支持39-57位变长编码方式,其可以有效适应各种业务场景,兼容各类设备。目的对象可以通过其数字身份标识登录服务平台。

[0046] 数字身份标识可以对应至少一个可验证凭证。可验证凭证用于背书或证明与其对应的数字身份标识所标识的目标主体具有某种属性。可验证凭证可以包括目标对象名称、目标对象的数字身份标识、目标对象具有的属性、凭证有效日期、凭证ID(Identity document,标识号)、颁发该可验证凭证的机构名称等。可以根据使用目标应用所需的条件,将可验证凭证中的相关字段作为验证信息,例如,可以将可验证凭证中的目标对象的数字身份标识、目标对象具有的属性或凭证有效日期作为一条验证信息。可信数字信息可以包括多条验证信息。

[0047] 在一种实现方式中,目标对象可以在其客户端中创建数字身份标识和目标对象的公私密钥对,目标对象通过其客户端向第三方机构发送凭证申请请求。目标对象的公私密钥对包括公钥和私钥。目标对象的公私密钥对中公钥用于对目标对象的公私密钥对中私钥生成的签名进行验证,目标对象的公私密钥对中私钥用于对数据或信息进行签名。目标对象可以利用国密SM2算法、对称加密算法或非对称加密算法的生成目标对象的公私密钥对。该凭证申请请求包括:目标对象的数字身份标识、目标对象的公私密钥对,以及目标对象的审核信息;其中,审核信息包括目标对象所申请的可验证凭证所需要具备的信息,例如,审核信息可以包括目标对象的营业执照、组织机构代码等。第三方机构为具有颁发可验证凭证资格的认证机构。目标对象的客户端可以为插件钱包等。插件钱包是基于浏览器开发的插件,插件钱包可以用于数字身份标识、可验证凭证等的存储、管理和构建等。

[0048] 第三方机构对审核信息进行审核,当审核通过后,第三方机构基于目标对象的公私密钥对和数字身份标识生成可验证凭证,第三方机构将可验证凭证与数字身份标识绑定以形成数字身份标识与可验证凭证的对应关系。第三方机构将可验证凭证和数字身份标识发送目标对象的客户端。

[0049] 需要说明的是,目标对象可以是需要使用目标应用的任一对象,目标应用可以是目标对象要使用服务平台中的应用,目标对象和目标应用中的“目标”并不构成对目标对象和目标应用的任何限定。

[0050] 步骤S120,验证服务器根据可信数字信息确定目标对象是否具有使用目标应用的权限。

[0051] 其中,验证服务器可以基于预设审核规则对可信数字信息进行审核,确定目标对

象是否具有使用目标应用的权限。预设审核规则可以根据实际需求设定。

[0052] 步骤S130,响应于验证服务器确定目标对象具有使用目标应用的权限,服务平台为目标对象设置允许使用目标应用的使用权限,且将可信数字信息存储至区块链。

[0053] 其中,当验证服务器确定目标对象具有使用目标应用的权限时,验证服务器向服务平台发送目标对象具有使用权限的消息,以及目标对象的可信数字信息;服务平台为目标对象设置允许使用目标应用的权限,当目标对象具有使用是目标应用的权限后便可以使用目标应用,同时服务平台将目标对象的可信数字信息存储到区块链。

[0054] 区块链(Block Chain)是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构,并以密码学方式保证数据不可篡改和不可伪造的分布式账本。

[0055] 在一种实现方式中,当验证服务器确定目标对象不具有使用目标应用的权限时,验证服务器向服务平台发送目标对象不具有使用权限的消息,服务平台拒绝目标对象使用目标应用。

[0056] 本公开实施例中,验证服务器的通过包括用于登录服务平台的数字身份标识所对应的可验证凭证中的至少一条验证信息的可信数字信息,确定服务平台是否允许目标对象使用目标应用,实现了可以利用数字身份标识对应的可验证凭证确定目标对象是否具有使用目标应用的权限,提高了目标对象的使用体验。同时,由于可信数字信息中包括可验证凭证中的至少一条验证信息,目标对象可以根据其需要使用的目标应用选择不同的可验证凭证,实现了目标对象对其可验证凭证的自主选择、管理和应用。另外,本公开实施例中,无需目标对象主动发送可信数字信息,由验证服务器依据目标应用获取目标对象的可信数字信息,减少了目标对象操作,进一步提高了目标对象的使用体验。

[0057] 在一个可选实施例中,本公开实施例中的可信数字信息具有由目标对象的公私密钥对中私钥生成的签名;如图2所示,步骤S120可以包括如下步骤:

[0058] 步骤S121,验证服务器通过目标对象的公私密钥对中公钥对可信数字信息的签名进行验证。

[0059] 其中,验证服务器可以从目标对象公布的存储地址处获取目标对象的公私密钥对中公钥,或者,验证服务器可以从目标对象的客户端获取目标对象的公私密钥对中公钥。

[0060] 步骤S122,响应于可信数字信息的签名通过验证,确定目标对象具有使用目标应用的权限。

[0061] 在一种实现方式中,当可信数字信息的签名通过目标对象的公私密钥对中公钥的验证时,确定目标对象具有使用目标应用的权限;当可信数字信息的签名未通过目标对象的公私密钥对中公钥的验证时,确定目标对象不具有使用目标应用的权限,验证服务器向服务平台发送目标对象不具有使用权限的消息,服务平台拒绝目标对象使用目标应用。

[0062] 在一个可选实施例中,如图3所示,本公开实施例中的步骤S110可以包括如下步骤:

[0063] 步骤S111,目标对象的客户端接收出示可信数字信息的出示请求。

[0064] 其中,该出示请求包括:目标应用对应的使用条件。可以预先设置目标应用与使用目标应用所需的使用条件的对应关系。例如,使用条件可以包括:需要提供的字段(验证信息)等。

[0065] 客户端可以为插件钱包,该插件钱包中存储目标对象的数字身份标识和与数字身

份标识对应的可验证凭证。在一种实现方式中，验证服务器可以调用插件钱包的SDK(Software Development Kit，软件开发工具包)接口实现与插件钱包之间的数据交互。服务平台或验证服务器向目标对象的客户端发送出示请求。

[0066] 步骤S112，客户端基于目标应用对应的使用条件，确定可验证信息。

[0067] 其中，该可验证信息包括数字身份标识所对应的可验证凭证中的至少一条验证信息。

[0068] 客户端从用于登录服务平台的数字身份标识对应的可验证凭证中获取使用条件指示的验证信息。

[0069] 在一种实现方式中，出示请求还可以包括：凭证ID、客户端的地址、登录应用平台的账户(目标对象的数字身份标识)key(键)值等。

[0070] 客户端接收验证服务器或服务平台发送的出示请求，查看用于登录服务平台的数字身份标识是否对应有与出示请求中的凭证ID所指示的可验证凭证，当具有与出示请求中的凭证ID所指示的可验证凭证时，从该可验证凭证中获取使用条件指示的验证信息，得到可验证信息，客户端还可以利用目标对象的公私密钥对中私钥对可验证信息进行签名处理，客户端将可验证信息发送验证服务器。当用于登录服务平台的数字身份标识未对应有与出示请求中的凭证ID所指示的可验证凭证时，客户端向验证服务器发送失败消息，验证服务器接收失败消息并向服务平台发送目标对象不具有使用权限的消息，服务平台拒绝目标对象使用目标应用。

[0071] 步骤S113，响应于客户端发送的可验证信息符合目标应用对应的使用条件，验证服务器根据可验证信息，确定目标对象的初始可信数字信息。

[0072] 其中，该初始可信数字信息具有由验证服务器的公私密钥对中私钥签生成的签名。该初始可信数字信息包括至少一条验证信息。

[0073] 验证服务器的公私密钥对包括：公钥和私钥。验证服务器的公私密钥对中公钥用于对验证服务器的公私密钥对中私钥生成的签名进行验证，验证服务器的公私密钥对中私钥用于对数据或信息进行签名。验证服务器可以利用国密SM2算法、对称加密算法或非对称加密算法等生成验证服务器的公私密钥对。

[0074] 客户端将可验证信息发送验证服务器。验证服务器接收可验证信息，并将可验证信息中的验证信息与目标应用对应的使用条件指示的验证信息比较，当可验证信息中的验证信息与目标应用对应的使用条件指示的验证信息相同，确定客户端向验证服务器发送的可验证信息符合目标应用对应的使用条件。

[0075] 可以通过可验证信息中的所有验证信息构建未签名的初始可信数字信息，利用验证服务器的公私密钥对中私钥对未签名的初始可信数字信息进行签名处理，得到初始可信数字信息。

[0076] 验证服务器将初始可信数字信息发送目标对象的客户端。

[0077] 在一种实现方式中，当可验证信息具有由目标对象的公私密钥对中私钥生成的签名时，验证服务器利用目标对象的公私密钥对中公钥对可验证信息的签名进行验证，在可验证信息的签名通过验证，且可验证信息中的验证信息与目标应用对应的使用条件指示的验证信息相同时，确定客户端向验证服务器发送的可验证信息符合目标应用对应的使用条件。

[0078] 在一种实现方式中，当客户端向验证服务器发送的可验证信息不符合目标应用对应的使用条件时，验证服务器向服务平台发送目标对象不具有使用权限的消息，服务平台拒绝目标对象使用目标应用。

[0079] 步骤S114，客户端利用验证服务器的公私密钥对中公钥对初始可信数字信息的签名进行验证。

[0080] 其中，客户端接收验证服务器发送的初始可信数字信息。客户端可以从验证服务器公布的存储地址处获取验证服务器的公私密钥对中公钥，或者，客户端可以从验证服务器中获取验证服务器的公私密钥对中公钥。

[0081] 步骤S115，响应于初始可信数字信息的签名通过验证，客户端利用目标对象的公私密钥对中私钥对初始可信数字信息进行签名处理，得到可信数字信息。

[0082] 在一种实现方式中，当初始可信数字信息的签名未通过验证，客户端向验证服务器发送失败消息，验证服务器接收失败消息并向服务平台发送目标对象不具有使用权限的消息，服务平台拒绝目标对象使用目标应用。

[0083] 步骤S116，客户端将可信数字信息发送验证服务器。

[0084] 在一种实现方式中，验证服务器接收可信数字信息，并根据可信数字信息确定目标对象是否具有使用目标应用的权限。

[0085] 在一个可选实施例中，本公开实施例中的出示请求还包括：验证服务器的授权凭证。其中，该授权凭证具有由验证服务器的公私密钥对中私钥生成的签名；如图4所示，本公开实施例中的基于数字身份的目标应用提供方法还包括如下步骤：

[0086] 步骤S210，客户端利用验证服务器的公私密钥对中公钥对授权凭证的签名进行验证。

[0087] 其中，授权凭证可以为用于证明验证服务器的身份的数字证书，授权凭证可以包括：凭证编号、有效日期、标识验证服务器的标识等。

[0088] 步骤S220，响应于授权凭证的签名通过验证服务器的公私密钥对中公钥的验证，客户端基于授权凭证，确定验证服务器是否具有获取目标应用对应的使用条件所指示的验证信息的权限。

[0089] 其中，客户端中可以预先设置授权凭证与权限对应关系，以及权限与可获取的验证信息的对应关系；

[0090] 根据授权凭证与权限对应关系确定授权凭证的权限，根据授权凭证的权限和权限与可获取的验证信息的对应关系，确定授权凭证是否可以获取目标应用对应的使用条件所指示的验证信息，当授权凭证可以获取目标应用对应的使用条件所指示的验证信息时，确定验证服务器具有获取目标应用对应的使用条件所指示的验证信息的权限。

[0091] 步骤S230，响应于验证服务器具有获取目标应用对应的使用条件所指示的验证信息的权限，客户端执行客户端基于目标应用对应的使用条件，确定可验证信息的操作。

[0092] 在一种实现方式中，当验证服务器不具有获取目标应用对应的使用条指示的验证信息的权限时，客户端向验证服务器发送失败消息，验证服务器接收失败消息并向服务平台发送目标对象不具有使用权限的消息，服务平台拒绝目标对象使用目标应用。

[0093] 本公开实施例中，客户端通过对授权凭证的签名进行验证，以及通过授权凭证确定验证服务器是否具有获取目标应用对应的使用条件所指示的验证信息的权限，有效确保

了客户端数据的安全。

[0094] 在一个可选实施例中，如图5所示，本公开实施例中基于数字身份的目标应用提供方法还包括如下步骤：

[0095] 步骤S310，响应于服务平台接收目标对象输入的登录请求，服务平台的登录服务器获取数字身份标识。

[0096] 其中，登录请求可以包括目标对象的客户端的地址或接口。登录服务器可以为计算或服务器等。登录服务器与服务平台和目标对象的客户端通信连接。

[0097] 在一种实现方式中，当服务平台接收目标对象输入的登录请求，服务平台的登录服务器可以根据登录请求中包括目标对象的客户端的地址或接口获取目标对象的数字身份标识。

[0098] 步骤S320，登录服务器确定数字身份标识是否符合预设标识条件。

[0099] 其中，预设标识条件可以根据实际需求设定。例如，预设标识条件可以包括标识格式，登录服务器可以确定数字身份标识的格式是否符合预设标识条件中包括的标识格式。

[0100] 步骤S330，响应于数字身份标识符合预设标识条件，登录服务器生成令牌。

[0101] 其中，令牌(token)相当于临时密码，其用于登录服务平台。例如，登录服务器可以通过令牌生成器生成令牌。

[0102] 在一种实现方式中，登录服务器可以将令牌发送目标对象的客户端。

[0103] 步骤S340，目标对象基于数字身份标识和令牌登录服务平台。

[0104] 其中，目标对象的客户端可以通过数字身份标识和令牌登录服务平台。

[0105] 本公开实施例中，当服务平台接收目标对象输入的登录请求，服务平台的登录服务器获取数字身份标识，并在数字身份标识通过验证后生产令牌，目标对象可以通过令牌和数字身份标识登录服务平台。不仅保证了目标对象的身份的真实性，而且无需目标对象主动输入用于登录服务平台的密码和数字身份标识，提高了目标对象的使用体验。

[0106] 在一个可选实施例中，如图6所示，本公开实施例中的步骤S320还包括如下步骤：

[0107] 步骤S321，登录服务器确定数字身份标识的格式是否符合预设标识格式条件。

[0108] 其中，预设标识格式条件可包括标识的格式要求，预设标识格式条件可以根据实际需求设定。例如，预设标识格式条件可以包括标识的编码位数、编码是否完整等。

[0109] 步骤S322，响应于数字身份标识的格式符合预设标识格式条件，登录服务器向目标对象的客户端发送随机数。

[0110] 其中，登录服务器可以生成随机数，并将随机数与数字身份标识绑定，以使随机数和数字身份标识形成对应关系，同时登录服务器还将随机数发送目标对象的客户端。

[0111] 步骤S323，客户端利用目标对象的公私密钥对中私钥对随机数进行签名处理，得到签名随机数。

[0112] 其中，目标对象的客户端将签名随机数发送登录服务器。

[0113] 步骤S324，登录服务器利用目标对象的公私密钥对中公钥对签名随机数的签名进行验证。

[0114] 其中，登录服务器接收目标对象的客户端发送的签名随机数，并利用目标对象的公私密钥对中公钥对签名随机数的签名进行验证。

[0115] 步骤S325，响应于签名随机数的签名通过目标对象的公私密钥对中公钥的验证，

登录服务器确定数字身份标识符合预设标识条件。

[0116] 在一种实现方式中，登录服务器还可以确定目标对象的公私密钥对中公钥的地址是否存在，以及客户端反馈的签名随机数中包括的随机数是否与登录服务器生成的随机数相同(即与数字身份标识对应的随机数是否相同)，当确定目标对象的公私密钥对中公钥的地址存在、客户端反馈的签名随机数中包括的随机数与登录服务器生成的随机数相同、且签名随机数的签名通过目标对象的公私密钥对中公钥验证，登录服务器确定数字身份标识符合预设标识条件。其中，公钥对应的地址是通过对目标对象的公私密钥对中公钥做哈希计算，然后从该哈希计算得到的哈希值中取最后的40位16进制字符得到的。公钥对应的地址是一个有效的以太坊地址。

[0117] 以下为本公开实施例中基于数字身份的目标应用提供方法的一个应用实施例。在本应用实施例中，目标对象的客户端以插件钱包为例，数字身份标识以BID标识为例。

[0118] 如图7所示，登录服务平台的流程包括如下步骤：

[0119] A1，目标对象可以通过点击服务平台上的授权登录按键发送登录请求；

[0120] A2，服务平台调用插件钱包的SDK.auth(SDK授权)接口向插件钱包发送请求授权登录服务器获取BID标识的授权请求，插件钱包选择BID标识授权，即插件钱包选择用于登录服务平台的BID标识，被授权的BID标识即为用于登录服务平台的BID标识，插件钱包授权的BID标识以下称为目标BID标识；

[0121] A3，插件钱包向服务平台的登录服务器发送目标BID标识，同时调用请求随机数接口向登录服务器请求随机数；

[0122] A4，登录服务器确定目标BID标识的格式是否合法，即登录服务器确定目标BID标识的格式是否符合预设标识格式条件，当确定目标BID标识的格式合法，即确定目标BID标识的格式符合预设标识格式条件，登录服务器生成随机数，并将随机数与目标BID标识绑定形成随机数和目标BID标识的对应关系，向插件钱包发送随机数；

[0123] A5，插件钱包利用目标对象的公私密钥对中私钥对随机数进行签名，得到签名随机数，并调用授权接口向登录服务器发送签名随机数和目标对象的公私密钥对中公钥；

[0124] A6，登录服务器利用目标对象的公私密钥对中公钥对签名随机数的签名进行验证，确定目标对象的公私密钥对中公钥的地址是否存在，以及确定签名随机数中包括的随机数是否正确，即确定签名随机数中包括的随机数是否与登录服务器生成的随机数相同，当确定目标对象的公私密钥对中公钥的地址存在、签名随机数中包括的随机数正确，即签名随机数中包括的随机数与登录服务器生成的随机数相同，且签名随机数的签名通过目标对象的公私密钥对中公钥验证，登录服务器生成令牌，并将令牌发送插件钱包；

[0125] A7，插件钱包向服务平台发送目标BID标识和令牌，以使用目标BID标识和令牌登录服务平台。

[0126] 如图8所示，提供目标应用包括如下步骤：

[0127] B1，目标对象输入的针对目标应用的使用指令，服务平台调用插件钱包的SDK接口发送出示请求，该出示请求可以包括：目标应用对应的使用条件、凭证ID、客户端的地址和目标BID标识的key值；

[0128] B2，插件钱包确定目标BID标识是否对应有凭证ID对应的可验证凭证，当目标BID标识对应有凭证ID对应的可验证凭证时，从与凭证ID对应的可验证凭证中获取目标应用对

应的使用条件指示的验证信息，插件钱包根据其获取的验证信息组成可验证信息，插件钱包向验证服务器发送可验证信息；

[0129] B3，验证服务器对插件钱包发送的可验证信息进行审核，当可验证信息中的验证信息与目标应用对应的使用条件指示的验证信息相同，确定客户端向验证服务器发送的可验证信息符合目标应用对应的使用条件，确定可验证信息通过审核，验证服务器根据可验证信息中的验证信息构建初始可信数字信息，利用验证服务器的公私密钥对中私钥签对初始可信验证信息进行签名，并将签名后的初始可信验证信息发送插件钱包；

[0130] B4，插件钱包利用验证服务器的公私密钥对中公钥对初始可信数字信息的签名进行验证，当验证通过，插件钱包利用目标对象的公私密钥对中私钥对初始可信数字信息进行签名处理，得到可信数字信息，将可信数字信息发送验证服务器；

[0131] B5，验证服务器利用目标对象的公私密钥对中公钥对可信数字信息的签名进行验证，当可信数字信息的签名通过目标对象的公私密钥对中公钥的验证时，确定目标对象具有使用目标应用的权限，验证服务器生成验证通过证明，该该验证通过证明包括：目标对象具有使用权限的消息和目标对象的可信数字信息；向插件钱包发送验证通过证明；

[0132] B6，插件钱包向登录服务器发送验证通过证明，服务平台为目标对象设置使用目标应用的使用权限，当目标对象具有目标应用的使用权限后，可以使用目标应用，同时，服务平台解析验证通过证明以获取可信数字信息，并将获取的可信数字信息作为目标对象的通过验证的数据，对通过验证的数据添加收到验证通过证明时的时间戳，然后存储至区块链。

[0133] 图9示出本公开实施例中基于数字身份的目标应用提供装置的框图。如图9所示，该实施例基于数字身份的目标应用提供装置包括：

[0134] 第一获取模块410，用于响应于服务平台接收到目标对象输入的针对目标应用的使用指令，所述服务平台的验证服务器获取所述目标对象的可信数字信息，其中，所述可信数字信息包括所述目标对象登录所述服务平台的数字身份标识所对应的可验证凭证中的至少一条验证信息；

[0135] 第一判断模块420，用于所述验证服务器根据所述可信数字信息确定所述目标对象是否具有使用所述目标应用的权限；

[0136] 应用许可模块430，用于响应于所述验证服务器确定所述目标对象具有使用所述目标应用的权限，所述服务平台为所述目标对象设置使用所述目标应用的使用权限，且将所述可信数字信息存储至区块链。

[0137] 在一个可选实施例方式中，本公开实施例中所述可信数字信息具有由所述目标对象的公私密钥对中私钥生成的签名；所述第一判断模块420包括：

[0138] 第一签名验证子模块，用于所述验证服务器通过所述目标对象的公私密钥对中公钥对所述可信数字信息的签名进行验证；

[0139] 第一确定子模块，用于响应于所述可信数字信息的签名通过验证，确定所述目标对象具有使用所述目标应用的权限。

[0140] 在一个可选实施例方式中，本公开实施例中所述第一获取模块410包括：

[0141] 接收子模块，用于所述目标对象的客户端接收出示可信数字信息的出示请求，其中，所述出示请求包括：所述目标应用对应的使用条件；

[0142] 第二确定子模块，用于所述客户端基于所述目标应用对应的使用条件，确定可验证信息，其中，所述可验证信息包括所述数字身份标识所对应的可验证凭证中的至少一条验证信息；

[0143] 第三确定子模块，用于响应于所述客户端发送的所述可验证信息符合所述目标应用对应的使用条件，所述验证服务器根据所述可验证信息，确定所述目标对象的初始可信数字信息，其中，所述初始可信数字信息具有由所述验证服务器的公私密钥对中私钥签生成的签名；

[0144] 第二签名验证子模块，用于所述客户端利用所述验证服务器的公私密钥对中公钥对所述初始可信数字信息的签名进行验证；

[0145] 第一签名子模块，用于响应于所述初始可信数字信息的签名通过验证，所述客户端利用所述目标对象的公私密钥对中私钥对所述初始可信数字信息进行签名处理，得到所述可信数字信息；

[0146] 发送子模块，用于所述客户端将所述可信数字信息发送所述验证服务器。

[0147] 在一个可选实施例方式中，本公开实施例中所述出示请求还包括：所述验证服务器的授权凭证，其中，所述授权凭证具有由所述验证服务器的公私密钥对中私钥生成的签名；所述装置还包括：

[0148] 第三签名验证子模块，用于所述客户端利用所述验证服务器的公私密钥对中公钥对所述授权凭证的签名进行验证；

[0149] 第四确定子模块，用于响应于所述授权凭证的签名通过所述验证服务器的公私密钥对中公钥的验证，所述客户端基于所述授权凭证，确定所述验证服务器是否具有获取所述目标应用对应的使用条件所指示的验证信息的权限；

[0150] 第五确定子模块，用于响应于所述验证服务器具有获取所述目标应用对应的使用条件所指示的验证信息的权限，所述客户端执行所述客户端基于所述目标应用对应的使用条件，确定所述可验证信息的操作。

[0151] 在一个可选实施例方式中，本公开实施例中的基于数字身份的目标应用提供装置还包括：

[0152] 第二获取模块，用于响应于所述服务平台接收所述目标对象输入的登录请求，所述服务平台的登录服务器获取所述数字身份标识；

[0153] 第二判断模块，用于所述登录服务器确定所述数字身份标识是否符合预设标识条件；

[0154] 令牌生成模块，用于响应于所述数字身份标识符合所述预设标识条件，所述登录服务器生成令牌；

[0155] 登录模块，用于所述目标对象基于所述数字身份标识和所述令牌登录所述服务平台。

[0156] 在一个可选实施例方式中，本公开实施例中所述第二判断模块包括：

[0157] 第一判断子模块，用于所述登录服务器确定所述数字身份标识的格式是否符合预设标识格式条件；

[0158] 随机数发送子模块，用于响应于所述数字身份标识的格式符合所述预设标识格式条件，所述登录服务器向所述目标对象的客户端发送随机数；

[0159] 第二签名子模块，用于所述客户端利用所述目标对象的公私密钥对中私钥对所述随机数进行签名处理，得到签名随机数；

[0160] 第四签名验证子模块，用于所述登录服务器利用所述目标对象的公私密钥对中公钥对所述签名随机数的签名进行验证；

[0161] 第二判断子模块，用于响应于所述签名随机数的签名通过所述目标对象的公私密钥对中公钥的验证，所述登录服务器确定所述数字身份标识符合所述预设标识条件。

[0162] 另外，本公开实施例还提供了一种电子设备，包括：

[0163] 存储器，用于存储计算机程序；

[0164] 处理器，用于执行所述存储器中存储的计算机程序，且所述计算机程序被执行时，实现本公开上述任一实施例所述的基于数字身份的目标应用提供方法。

[0165] 图10为本公开电子设备一个应用实施例的结构示意图。下面，参考图10来描述根据本公开实施例的电子设备。该电子设备可以是第一设备和第二设备中的任一个或两者、或与它们独立的单机设备，该单机设备可以与第一设备和第二设备进行通信，以从它们接收所采集到的输入信号。

[0166] 如图10所示，电子设备包括一个或多个处理器510和存储器520。

[0167] 处理器510可以是中央处理单元(CPU)或者具有数据处理能力和/或指令执行能力的其他形式的处理单元，并且可以控制电子设备中的其他组件以执行期望的功能。

[0168] 存储器520可以包括一个或多个计算机程序产品，所述计算机程序产品可以包括各种形式的计算机可读存储介质，例如易失性存储器和/或非易失性存储器。所述易失性存储器例如可以包括随机存取存储器(RAM)和/或高速缓冲存储器(cache)等。所述非易失性存储器例如可以包括只读存储器(ROM)、硬盘、闪存等。在所述计算机可读存储介质上可以存储一个或多个计算机程序指令，处理器可以运行所述程序指令，以实现上文所述的本公开的各个实施例的基于数字身份的目标应用提供方法以及/或者其他期望的功能。

[0169] 在一个示例中，电子设备还可以包括：输入装置530和输出装置540，这些组件通过总线系统和/或其他形式的连接机构(未示出)互连。

[0170] 此外，该输入装置530还可以包括例如键盘、鼠标等等。

[0171] 该输出装置540可以向外部输出各种信息，包括确定出的距离信息、方向信息等。该输出装置可以包括例如显示器、扬声器、打印机、以及通信网络及其所连接的远程输出设备等等。

[0172] 当然，为了简化，图10中仅示出了该电子设备中与本公开有关的组件中的一些，省略了诸如总线、输入/输出接口等等的组件。除此之外，根据具体应用情况，电子设备还可以包括任何其他适当的组件。

[0173] 除了上述方法和设备以外，本公开的实施例还可以是计算机程序产品，其包括计算机程序指令，所述计算机程序指令在被处理器运行时使得所述处理器执行本说明书上述部分中描述的根据本公开各种实施例的基于数字身份的目标应用提供方法中的步骤。

[0174] 所述计算机程序产品可以以一种或多种程序设计语言的任意组合来编写用于执行本公开实施例操作的程序代码，所述程序设计语言包括面向对象的程序设计语言，诸如Java、C++等，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设备上执行、部分地在用户设备上执行、作为一个独立的软

件包执行、部分在用户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。

[0175] 此外，本公开的实施例还可以是计算机可读存储介质，其上存储有计算机程序指令，所述计算机程序指令在被处理器运行时使得所述处理器执行本说明书上述部分中描述的根据本公开各种实施例的基于数字身份的目标应用提供方法中的步骤。

[0176] 所述计算机可读存储介质可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以包括但不限于电、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。可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器(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。

[0177] 本领域普通技术人员可以理解：实现上述方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成，前述的程序可以存储于一计算机可读取存储介质中，该程序在执行时，执行包括上述方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

[0178] 以上结合具体实施例描述了本公开的基本原理，但是，需要指出的是，在本公开中提及的优点、优势、效果等仅是示例而非限制，不能认为这些优点、优势、效果等是本公开的各个实施例必须具备的。另外，上述公开的具体细节仅是为了示例的作用和便于理解的作用，而非限制，上述细节并不限制本公开为必须采用上述具体的细节来实现。

[0179] 本说明书中各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其它实施例的不同之处，各个实施例之间相同或相似的部分相互参见即可。对于系统实施例而言，由于其与方法实施例基本对应，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0180] 本公开中涉及的器件、装置、设备、系统的方框图仅作为例示性的例子并且不意图要求或暗示必须按照方框图示出的方式进行连接、布置、配置。如本领域技术人员将认识到的，可以按任意方式连接、布置、配置这些器件、装置、设备、系统。诸如“包括”、“包含”、“具有”等等的词语是开放性词汇，指“包括但不限于”，且可与其互换使用。这里所使用的词汇“或”和“和”指词汇“和/或”，且可与其互换使用，除非上下文明确指示不是如此。这里所使用的词汇“诸如”指词组“诸如但不限于”，且可与其互换使用。

[0181] 可能以许多方式来实现本公开的方法和装置。例如，可通过软件、硬件、固件或者软件、硬件、固件的任何组合来实现本公开的方法和装置。用于所述方法的步骤的上述顺序仅是为了进行说明，本公开的方法的步骤不限于以上具体描述的顺序，除非以其它方式特别说明。此外，在一些实施例中，还可将本公开实施为记录在记录介质中的程序，这些程序包括用于实现根据本公开的方法的机器可读指令。因而，本公开还覆盖存储用于执行根据本公开的方法的程序的记录介质。

[0182] 还需要指出的是，在本公开的装置、设备和方法中，各部件或各步骤是可以分解和/或重新组合的。这些分解和/或重新组合应视为本公开的等效方案。

[0183] 提供所公开的方面的以上描述以使本领域的任何技术人员能够做出或者使用本公开。对这些方面的各种修改对于本领域技术人员而言是非常显而易见的，并且在此定义

的一般原理可以应用于其他方面而不脱离本公开的范围。因此，本公开不意图被限制到在此示出的方面，而是按照与在此公开的原理和新颖的特征一致的最宽范围。

[0184] 为了例示和描述的目的已经给出了以上描述。此外，此描述不意图将本公开的实施例限制到在此公开的形式。尽管以上已经讨论了多个示例方面和实施例，但是本领域技术人员将认识到其某些变型、修改、改变、添加和子组合。

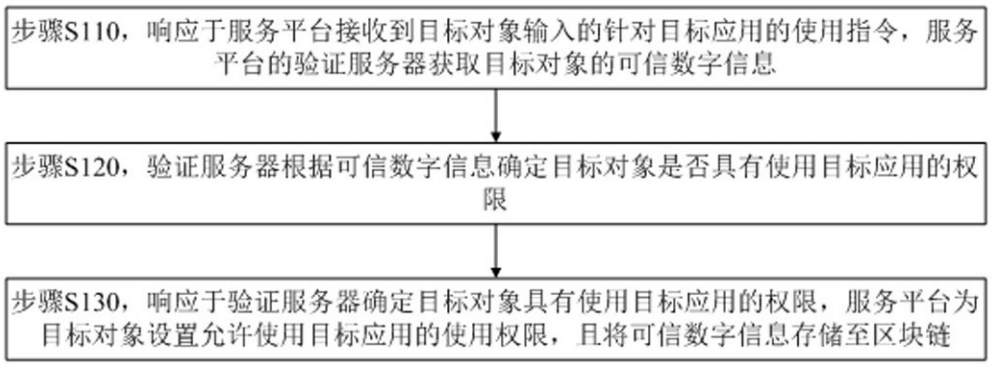

步骤S110，响应于服务平台接收到目标对象输入的针对目标应用的使用指令，服务平台的验证服务器获取目标对象的可信数字信息
步骤S120，验证服务器根据可信数字信息确定目标对象是否具有使用目标应用的权限
步骤S130，响应于验证服务器确定目标对象具有使用目标应用的权限，服务平台为目标对象设置允许使用目标应用的使用权限，且将可信数字信息存储至区块链

图1


步骤S121，验证服务器通过目标对象的公私密钥对中公钥对可信数字信息的签名进行验证
步骤S122，响应于可信数字信息的签名通过验证，确定目标对象具有使用目标应用的权限

图2

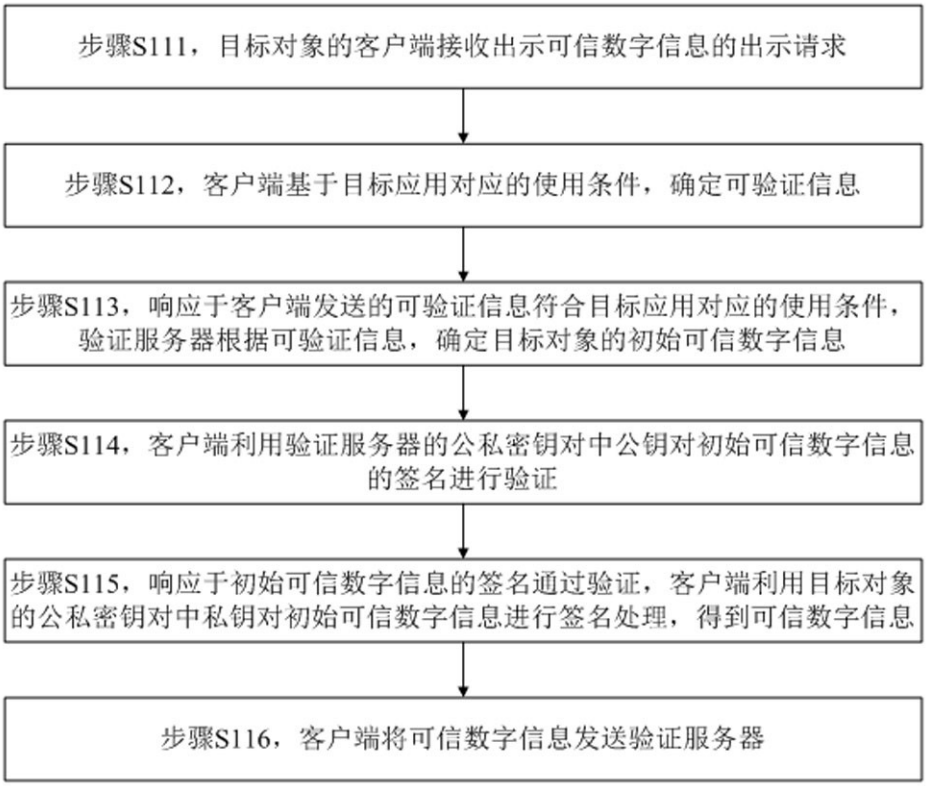

步骤S111，目标对象的客户端接收出示可信数字信息的出示请求
步骤S112，客户端基于目标应用对应的使用条件，确定可验证信息
步骤S113，响应于客户端发送的可验证信息符合目标应用对应的使用条件，验证服务器根据可验证信息，确定目标对象的初始可信数字信息
步骤S114，客户端利用验证服务器的公私密钥对中公钥对初始可信数字信息的签名进行验证
步骤S115，响应于初始可信数字信息的签名通过验证，客户端利用目标对象的公私密钥对中私钥对初始可信数字信息进行签名处理，得到可信数字信息
步骤S116，客户端将可信数字信息发送验证服务器

图3

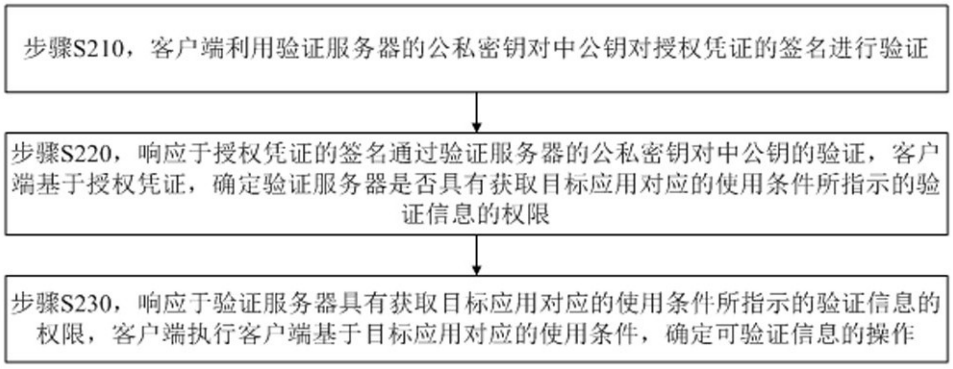

步骤S210，客户端利用验证服务器的公私密钥对中公钥对授权凭证的签名进行验证
步骤S220，响应于授权凭证的签名通过验证服务器的公私密钥对中公钥的验证，客户端基于授权凭证，确定验证服务器是否具有获取目标应用对应的使用条件所指示的验证信息的权限
步骤S230，响应于验证服务器具有获取目标应用对应的使用条件所指示的验证信息的权限，客户端执行客户端基于目标应用对应的使用条件，确定可验证信息的操作

图4

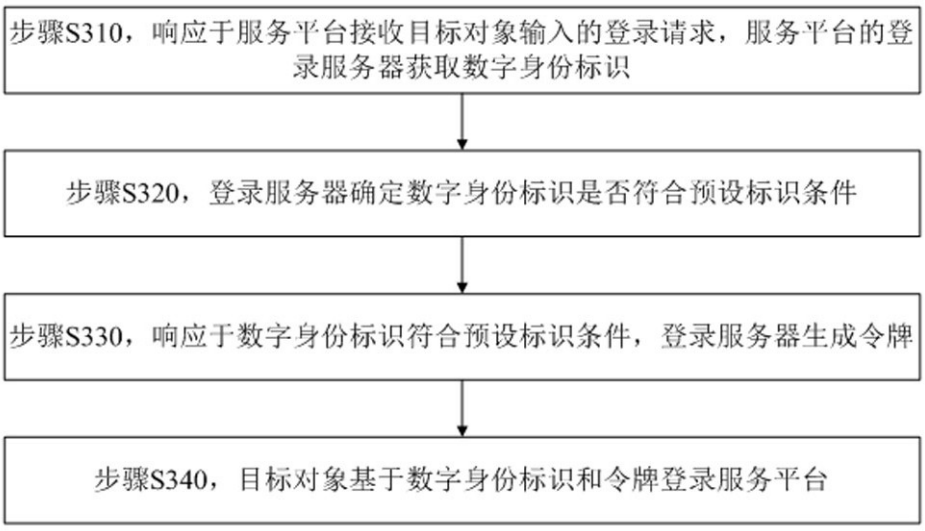

步骤S310，响应于服务平台接收目标对象输入的登录请求，服务平台的登录服务器获取数字身份标识
步骤S320，登录服务器确定数字身份标识是否符合预设标识条件
步骤S330，响应于数字身份标识符合预设标识条件，登录服务器生成令牌
步骤S340，目标对象基于数字身份标识和令牌登录服务平台

图5

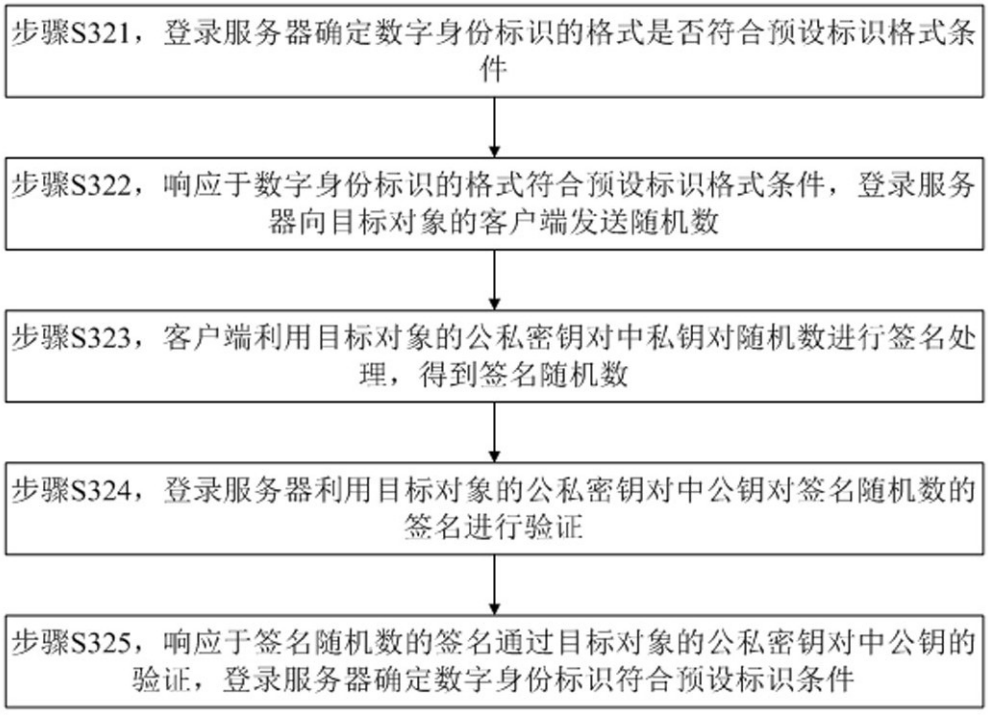

步骤S321，登录服务器确定数字身份标识的格式是否符合预设标识格式条件
步骤S322，响应于数字身份标识的格式符合预设标识格式条件，登录服务器向目标对象的客户端发送随机数
步骤S323，客户端利用目标对象的公私密钥对中私钥对随机数进行签名处理，得到签名随机数
步骤S324，登录服务器利用目标对象的公私密钥对中公钥对签名随机数的签名进行验证
步骤S325，响应于签名随机数的签名通过目标对象的公私密钥对中公钥的验证，登录服务器确定数字身份标识符合预设标识条件

图6

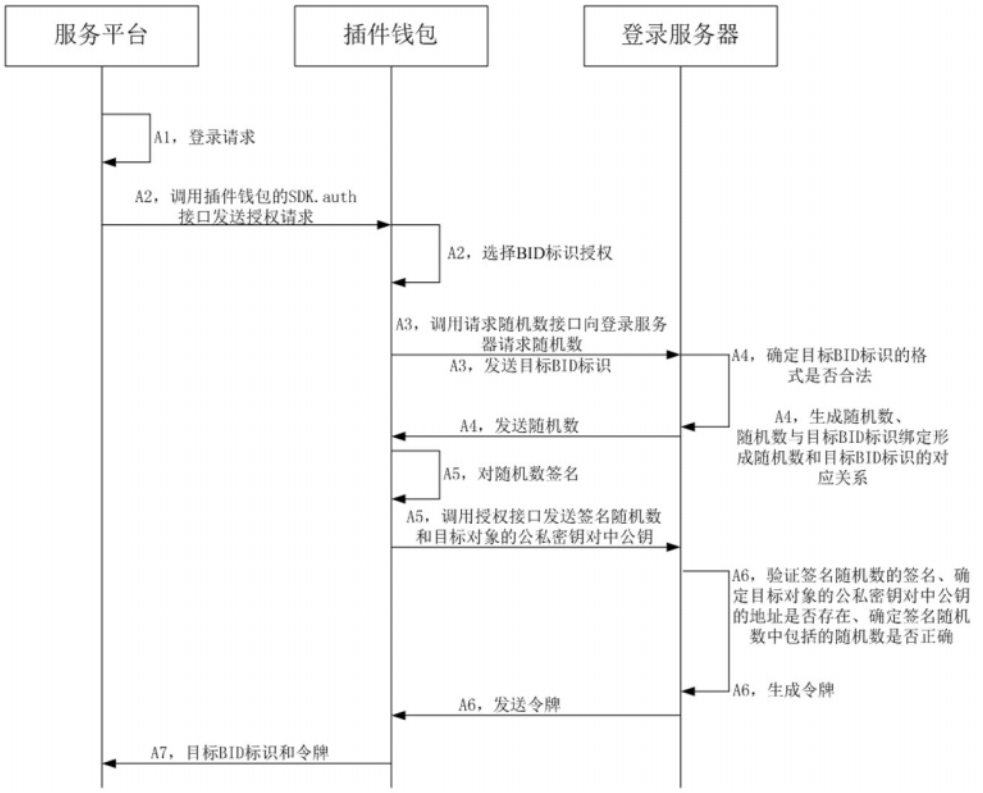

服务平台
插件钱包
登录服务器
A1，登录请求
A2，调用插件钱包的SDK.auth接口发送授权请求
A2，选择BID标识授权
A3，调用请求随机数接口向登录服务器请求随机数
A3，发送目标BID标识
A4，确定目标BID标识的格式是否合法
A4，发送随机数
A4，生成随机数、随机数与目标BID标识绑定形成随机数和目标BID标识的对应关系
A5，对随机数签名
A5，调用授权接口发送签名随机数和目标对象的公私密钥对中公钥
A6，验证签名随机数的签名、确定目标对象的公私密钥对中公钥的地址是否存在、确定签名随机数中包括的随机数是否正确
A6，生成令牌
A6，发送令牌
A7，目标BID标识和令牌

图7

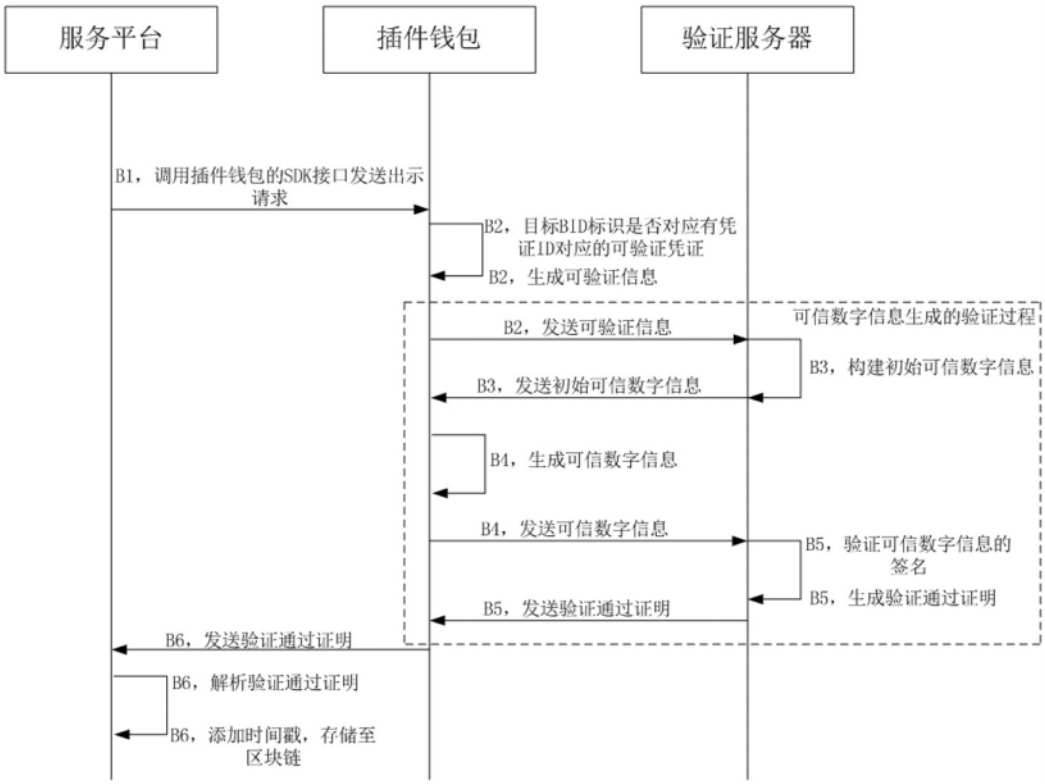

服务平台
插件钱包
验证服务器
B1，调用插件钱包的SDK接口发送出示请求
B2，目标BID标识是否对应有凭证ID对应的可验证凭证
B2，生成可验证信息
可信数字信息生成的验证过程
B2，发送可验证信息
B3，构建初始可信数字信息
B3，发送初始可信数字信息
B4，生成可信数字信息
B4，发送可信数字信息
B5，验证可信数字信息的签名
B5，生成验证通过证明
B5，发送验证通过证明
B6，发送验证通过证明
B6，解析验证通过证明
B6，添加时间戳，存储至区块链

图8


第一获取模块410
第一判断模块420
应用许可模块430

图9

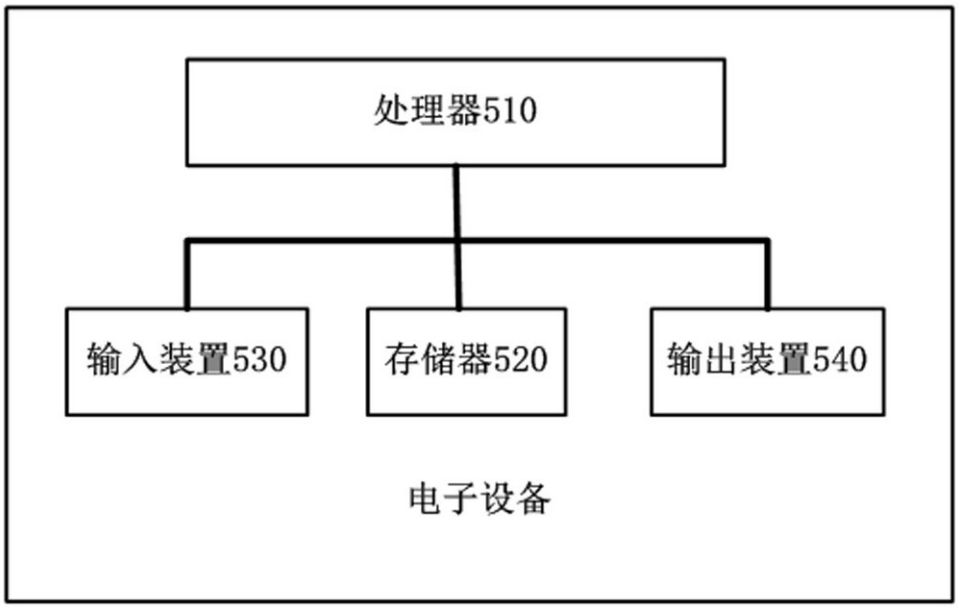


图10