

资源处理方法、签名私钥获取方法、装置

相关申请

本申请要求 2024 年 01 月 02 日申请的，申请号为 2024100067734，名称为“数字账户创建方法、签名私钥获取方法、装置”的中国专利申请的优先权，在此将其全文引入作为参考。

技术领域

本申请涉及计算机技术领域，特别是涉及一种资源处理方法、签名私钥获取方法、装置。

背景技术

随着科学技术的发展，出现了数字账户。数字账户是指用以存储虚拟资源的容器。对于数字账户而言，其存储的每份虚拟资源均具有不同的资源标识，资源标识是指唯一标识一份虚拟资源的信息。每份虚拟资源所对应的资源量可不同，比如，可将 100 资源量的虚拟资源作为一份资源，也可将 1 资源量的虚拟资源作为一份资源。

目前，在创建数字账户的过程中，会额外创建一对主公私钥对，并将主公钥对与数字账户创建者标识对应存储于数据库中。然而，将主公钥对与数字账户创建者标识对应存储于数据库中，存在主公钥对被攻击窃取的风险，从而降低了数字账户的安全性。

发明内容

本申请提供一种资源处理方法、签名私钥获取方法、装置、计算机设备、计算机可读存储介质和计算机程序产品。

第一方面，本申请提供了一种资源处理方法，由计算机设备执行，所述方法包括：

在接收到数字账户创建请求的情况下，响应于所述数字账户创建请求，从所述数字账户创建请求中提取出数字账户创建者标识；

根据所述数字账户创建者标识创建用于存储虚拟资源的数字账户；

获取预设的主公钥，根据所述主公钥和所述数字账户创建者标识，生成所述数字账户的签名公钥；

获取与所述主公钥相配对的主私钥，根据所述主私钥和所述签名公钥，生成与所述签名公钥相配对的签名私钥；

将所述签名私钥发送至所述数字账户创建者标识所对应的终端；发送的所述签名私钥，用于触发所述终端基于所述签名私钥生成数字签名；

接收所述终端反馈的包括所述数字签名的资源处理请求；及

在基于所述数字账户的所述签名公钥对所述数字签名验证通过后，根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

第二方面，本申请还提供了一种资源处理装置，所述装置包括：

签名公钥生成模块，用于在接收到数字账户创建请求的情况下，响应于所述数字账户创建请求，从所述数字账户创建请求中提取出数字账户创建者标识；根据所述数字账户创建者标识创建用以存储虚拟资源的数字账户；获取预设的主公钥，根据所述主公钥和所述数字账户创建者标识，生成所述数字账户的签名公钥；

签名私钥生成模块，用于获取与所述主公钥相配对的主私钥，根据所述主私钥和所述签名公钥，生成与所述签名公钥相配对的签名私钥；

签名私钥发送模块，用于将所述签名私钥发送至所述数字账户创建者标识所对应的终端；发送的所述签名私钥，用于触发所述终端基于所述签名私钥生成数字签名；

资源处理请求接收模块，用于接收所述终端反馈的包括所述数字签名的资源处理请求；及

资源处理模块，用于在基于所述数字账户的所述签名公钥对所述数字签名验证通过后，根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

第三方面，本申请还提供了一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现本申请实施例提供的任一种资源处理方法中的步骤。

第四方面，本申请还提供了一种计算机可读存储介质，所述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本申请实施例提供的任一种资源处理方法中的步骤。

第五方面，本申请还提供了一种计算机程序产品，所述计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现本申请实施例提供的任一种资源处理方法中的步骤。

第六方面，本申请提供了一种签名私钥获取方法，所述方法包括：

获取数字账户创建者标识，并根据所述数字账户创建者标识生成数字账户创建请求；

发送所述数字账户创建请求；发送的所述数字账户创建请求，用于触发根据所述数字账户创建者标识创建数字账户、签名公钥和签名私钥，以及用于触发生成验证码，基于所述验证码对所述签名私钥进行加密，得到加密私钥；

接收所述加密私钥和所述验证码；

通过所述验证码对所述加密私钥进行解密，获得所述签名私钥；所述签名私钥用于在资源处理的过程中，通过所述签名私钥生成包括数字签名的资源处理请求；所述数字签名，用于在通过与所述数字账户相绑定的所述签名公钥对所述数字签名验证通过后，触发根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

第七方面，本申请还提供了一种签名私钥获取装置，所述装置包括：

请求生成模块，用于获取数字账户创建者标识，并根据所述数字账户创建者标识生成数字账户创建请求。

请求发送模块，用于发送所述数字账户创建请求；发送的所述数字账户创建请求，用于触发根据所述数字账户创建者标识创建数字账户、签名公钥和签名私钥，以及用于触发生成验证码，基于所述验证码对所述签名私钥进行加密，得到加密私钥。

密钥接收模块，用于接收所述加密私钥和所述验证码；通过所述验证码对所述加密私钥进行解密，获得所述签名私钥；所述签名私钥用于在资源处理的过程中，通过所述签名私钥生成包括数字签名的资源处理请求；所述数字签名，用于在通过与所述数字账户相绑定的所述签名公钥对所述数字签名验证通过后，触发根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

第八方面，本申请还提供了一种计算机设备，所述计算机设备包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现本申请实施例提供的任一种签名私钥获取方法中的步骤。

第九方面，本申请还提供了一种计算机可读存储介质，所述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本申请实施例提供的任一种签名私钥获取方法中的步骤。

第十方面，本申请还提供了一种计算机程序产品，所述计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现本申请实施例提供的任一种签名私钥获取方法中的步骤。

本申请的一个或多个实施例的细节在下面的附图和描述中提出。本申请的其它特征、目的和优点将从说明书、附图以及权利要求书变得明显。

附图说明

为了更清楚地说明本申请实施例或传统技术中的技术方案，下面将对实施例或传统技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据公开的附图获得其他的附图。

图 1 为一个实施例中资源处理方法的应用环境图；
图 2 为一个实施例中区块链网络的示意图；
图 3 为一个实施例中资源处理方法的流程示意图；
图 4 为一个实施例中账户创建页面的示意图；
图 5 为一个实施例中签名公钥的生成示意图；
图 6 为另一个实施例中签名公钥的生成示意图；
图 7 为一个实施例中签名公钥的展示示意图；
图 8 为一个实施例中第一加密密钥的生成示意图；
图 9 为一个实施例中签名私钥获取方法的流程示意图；
图 10 为一个实施例中验证码的输入示意图；
图 11 为一个实施例中详情页面的示意图；
图 12 为一个实施例中虚拟资源处理方法的流程示意图；
图 13 为一个实施例中资源处理装置的结构框图；
图 14 为一个实施例中签名私钥获取装置的结构框图；
图 15 为一个实施例中计算机设备的内部结构图；
图 16 为一个实施例中计算机设备的内部结构图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有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。

本申请实施例提供的资源处理方法，可以应用于如图 1 所示的应用环境中。其中，终端 102 通过网络与服务器 104 进行通信。数据存储系统可以存储服务器 104 需要处理的数据。数据存储系统可以集成在服务器 104 上，也可以放在云上或其他服务器上。终端 102 可发送数字账户的创建请求至服务器 104，从而服务器 104 可响应于创建请求，创建数字账户，以及创建与该数字账户相绑定的签名私钥和签名公钥，将签名私钥下发至终端 102，以使终端 102 可基于签名私钥生成包括数字签名的资源处理请求。当服务器 104 接收到包括数字签名的资源处理请求时，可通过与数字账户相绑定的签名公钥对数字签名进行验证，并在验证通过后根据资源处理请求对数字账户中的虚拟资源进行处理。其中，终端 102 可以但不限于各种台式计算机、笔记本电脑、智能手机、平板电脑、物联网设备和便携式可穿戴设备，物联网设备可为智能音箱、智能电视、智能空调、智能车载设备等。便携式可穿戴设备可为智能手表、智能手环、头戴设备等。服务器 104 可以用独立的服务器或者是多个服务器组成的服务器集群来实现，还可以是云服务器。

值得注意的是，本申请涉及区块链技术，比如，本申请中的共享账户为基于区块链设置的共享账户。本发明实施例涉及的区块链网络可以为基于分布式系统而生成的网络。参见图 2，图 2 是本发明实施例提供的分布式系统应用于区块链网络的一个可选的结构示意图，由区块链网络由多个节点（接入网络中的任意形式的计算设备，如服务器、用户终端）形成，节点之间形成组成的点对点（Peer To Peer）网络，点对点协议是一个运行在传输控制协议（TCP，Transmission Control Protocol）协议之上的应用层协议。在分布式系统中，任何机器如服务器、终端都可加入而成为节点，节点包括硬件层、中间层、操作系统层和应用层。区块链网络中各节点的功能包括：

1) 路由，节点具有的基本功能，用于支持节点之间的通信。

节点除具有路由功能外，还可以具有以下功能：

2) 应用，用于部署在区块链中，根据实际业务需求而实现特定业务，记录实现功能相关的数据形成记录数据，在记录数据中携带数字签名以表示任务数据的来源，将记录数据发送到区块链系统中的其他节点，供其他节点在验证记录数据来源以及完整性成功时，将

记录数据添加到临时区块中。

值得注意的是，本申请还涉及云技术，比如，本申请中的智能合约服务器可以为提供云计算服务的云服务器。云技术（Cloud technology）是指在广域网或局域网内将硬件、软件、网络等系列资源统一起来，实现数据的计算、储存、处理和共享的一种托管技术。

需要说明的是，本申请中使用的“第一”、“第二”以及类似的词语并不表示任何顺序、数量或者重要性，而只是用来区分不同的组成部分。除非上下文另外清楚地指出，否则单数形式“一个”、“一”或者“该”等类似词语也不表示数量限制，而是表示存在至少一个。本申请各实施例中提及的“多个”或“多份”等的数量均指代“至少两个”的数量，比如，“多个”指“至少两个”，“多份”指“至少两份”。

在一个实施例中，如图3所示，提供了一种资源处理方法，以该方法应用于图1中的服务器为例进行说明，包括以下步骤：

步骤302，响应于数字账户创建请求，从数字账户创建请求中提取出数字账户创建者标识。

具体地，当需要创建一个数字账户时，数字账户创建者可触发终端生成一个数字账户创建请求，并将数字账户创建请求发送至服务器，从而服务器即可接收到该数字账户创建请求。比如，参考图4，数字创建者所对应的终端可显示如图4所示的账户创建页面，从而数字创建者可在账户创建页面中输入创建数字账户所需的信息，比如，可输入数字账户创建者标识。当数字创建者点击账户创建页面中的确定控件时，数字创建者所对应的终端即可生成携带有数字账户创建者标识的数字账户创建请求。其中，数字账户创建者标识是指用以标识数字创建者的信息，比如，数字账户创建者标识可为用户名、手机号或邮箱等等。图4示出了一个实施例中账户创建页面的示意图。

其中，数字账户创建请求用于创建一个数字账户。对于数字账户而言，存储的每份虚拟资源均具有不同的资源标识，资源标识是指唯一标识一份虚拟资源的信息。每份虚拟资源可对应于不同的资源量，比如，可将100资源量的虚拟资源作为一份资源，将1资源量的资源作为另一份虚拟资源。单份虚拟资源在不同的数字账户中流转时，该份虚拟资源的标识并不会随着数字账户的变化而变化。数字账户可为与单个数字账户创建者所拥有的普通账户，也可为多个数字创建者共同拥有的共享账户。且数字账户中存储的虚拟资源，为由中央管理机构统一下发的虚拟资源，并且只有中央管理机构能够对一份虚拟资源进行拆分，得到多份虚拟资源，并为多份虚拟资源赋予不同的标识。数字账户之间，能够将存储的虚拟资源进行交换，比如，数字账户A中的两份50资源量的虚拟资源可以与数字账户B中的1份100资源量的虚拟资源进行交换，当两份50资源量的虚拟资源从数字账户A交换至数字账户B时，这两份50资源量的虚拟资源的标识并不会随着数字账户的改变而改变。虚拟资源是指可被利用或能够被利用的物质的总称。虚拟资源可为计算机资源或者货币。计算机资源可包含CPU资源、时间片资源和GPU资源等。

在其中一个实施例中，当待创建的数字账户为共享账户时，数字账户创建者可点击共享账户创建控件，从而数字账户创建者所对应的终端可显示账户创建页面，进而数字账户创建者可在账户创建页面中输入多个数字账户创建者标识，比如，数字账户创建者（用户A）可输入自身的邮箱和手机号，还可以输入用户B的邮箱和手机号，进而数字创建者所对应的终端可基于输入的多个数字账户创建者标识生成数字账户创建请求。容易理解地，在上述举例中，用户A和用户B即为共同拥有共享账户的用户。

或者，用户A可在账户创建页面中输入自身的数字账户创建者标识，例如，输入自身的邮箱和手机号，并点击账户标识添加控件，以使用户A所对应的终端可生成携带有用户A的数字账户创建者标识的数字账户创建请求，并将数字账户创建请求发送至服务器，例如，生成数字账户创建请求A，将数字账户创建请求A发送至服务器。用户A所对应的终端还可以生成携带数字账户创建请求的请求标识的账户标识添加请求，例如，生成携带数字账户创建请求A的请求标识的账户标识添加请求。用户A可从好友列表中选择下一个

填写数字账户创建者标识的用户，比如，选择用户 B，进而用户 A 所对应的终端可将账户标识添加请求发送至用户 B。当用户 B 所对应的终端在接收到账户标识添加请求时，用户 B 所对应的终端可展示账户创建页面。用户 B 可在账户创建页面中输入自身的数字账户创建者标识，例如，输入自身的邮箱和手机号，进而，用户 B 所对应的终端可生成携带用户 B 的数字账户创建者标识和接收到的数字账户创建请求中的请求标识的数字账户创建请求，比如，生成携带数字账户创建请求 A 的请求标识和用户 B 的数字账户创建者标识的数字账户创建请求 B，并将数字账户创建请求 B 发送至服务器。当然，用户 B 还可触发自身的终端生成账户标识添加请求，并将数字账户标识添加请求发送至其余数字账户创建者（例如，用户 C）。进而，当最后一个数字账户创建者账户在创建页面中输入自身的数字账户创建者标识后，最后一个数字账户创建者即可点击完成控件，最后一个数字账户创建者所对应的终端可根据接收到的账户标识添加请求中的请求标识和最后一个数字账户创建者的标识，生成与最后一个数字账户创建者对应的数字账户创建请求，并在与最后一个数字账户创建者对应的数字账户创建请求中添加结束标识符。当服务器接收到添加有结束标识符的数字账户创建请求时，服务器可以添加有结束标识符的数字账户创建请求为基准，依次寻找与添加有结束标识符的数字账户创建请求相关的数字账户创建请求，并从查找到的数字账户创建请求中提取出数字账户创建者标识，基于提取出的数字账户创建者标识创建共享的数字账户。比如，从数字账户创建请求 C 中可提取出用户 C 的数字账户创建者标识和数字账户创建请求 B 的标识，服务器根据数字账户创建请求 B 的标识查找得到数字账户创建请求 B，并从数字账户创建请求 B 中提取出用户 B 的数字账户创建者标识和数字账户创建请求 A 的标识；服务器根据数字账户创建请求 A 的标识查找得到数字创建请求 A，并从数字账户创建请求 A 中提取出用户 A 的数字账户创建者标识。至此，得到全部数字账户创建者的标识。

步骤 304，根据数字账户创建者标识创建用以存储虚拟资源的数字账户。

具体地，服务器根据数字账户创建者标识，创建数字账户，比如，对数字账户创建者标识进行加密，生成一个加密账号名，该加密账户名即为数字账户的账户名。在其中一个实施例中，服务器还可为创建的数字账号创建一个智能合约，以通过该智能合约对创建的数字账户进行管理。智能合约是一种旨在以信息化方式传播、验证或执行合同的计算机协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可查看且不可逆转。智能合约概念于 1994 年由 Nick Szabo 首次提出。通俗地说，智能合约就是设定好的计算机程序，这个程序能够在没有第三方中间机构参与的情况下，自动执行可信的合约内容，所有操作公开可查且不可逆转。比如，可设置智能合约参数，基于智能合约参数生成数字账户的智能合约。当需要通过智能合约对数字账户中的资源量总数进行管控时，智能合约参数可为资源管控条件、资源管控持续时长等等。

步骤 306，获取预设的主公钥，根据主公钥和数字账户创建者标识，生成数字账户的签名公钥。

具体地，当服务器创建数字账户时，服务器还可根据数字账户创建者标识以及预设的主公钥，生成签名公钥。比如，服务器可获取预设的签名公钥生成算法，通过签名公钥生成算法来基于数字账户创建者标识和主公钥生成签名公钥。其中，预设的主公钥为预先设置的一个公钥。在其中一个实施例中，不同的服务器可预设有不同的主公钥，或者，不同的数字创建者可预设有不同的主公钥。或者，可按照预设时间间隔，更新服务器中预设的主公钥。本实施例对此不作限定。

在其中一个实施例中，参考图 5，服务器中运行有虚拟机，可通过虚拟机来生成签名公钥。比如，可预先设置多个签名公钥生成算法，当需要生成签名公钥时，可从多个签名公钥生成算法中筛选出一个签名公钥算法，并将筛选出的签名公钥算法称作目标签名公钥算法。进一步地，可获取与目标签名公钥算法相对应的算法源代码，基于预设的虚拟机指令集，将算法源代码编译成虚拟机可识别的虚拟算法程序。通过虚拟机运行虚拟算法程

序以通过数字账户创建者标识生成签名公钥。图 5 示出了一个实施例中签名公钥的生成示意图。

在其中一个实施例中，可获取当前服务器的服务器标识，并根据服务器标识从多种加密算法中选择与服务器的运行能力相匹配的目标签名公钥算法；或者，可从多种加密算法中随机选择出目标签名公钥算法。在其中一个实施例中，可基于与服务器的操作系统相匹配的系统指令集，对算法源代码进行编译，得到由系统指令集中预设的系统指令所构成的中间代码；基于预设的虚拟机指令集与系统指令集之间的映射关系，将中间代码转化编译成虚拟机可识别的虚拟算法程序。

本申请实施例中预设虚拟机指令集，该虚拟机指令集非通用的指令集，例如为针对特定的应用程序专门开发的指令集等。而该预设的虚拟机指令集中的各个虚拟机指令均能够与系统指令集中的系统指令相对应。由此，服务器即可基于预设的虚拟机指令集与系统指令集之间的映射关系，将中间代码转化编译成虚拟机可识别的虚拟算法程序。

在其中一个实施例中，服务器也可仅基于数字账户创建者标识来生成签名公钥。比如，参考图 6，服务器可通过数字账户创建者的手机号、邮箱、用户名等信息，并基于签名公钥生成算法来生成签名公钥。图 6 示出了另一个实施例中签名公钥的生成示意图。

在其中一个实施例中，当生成了主公钥，可将主公钥存储于区块链中，并经过区块链中共识节点的共识。

步骤 308，获取与主公钥相配对的主私钥，根据主私钥和签名公钥，生成与签名公钥相配对的签名私钥。

具体地，当需要生成签名公钥时，服务器可获取预设的主私钥，根据主私钥和签名公钥，生成签名私钥。其中，主私钥是与上述的主公钥相配对的私钥，在生成主公钥的同时可生成一个对应的主私钥。

在其中一个实施例中，服务器可通过下述公式来生成签名私钥： $ID_Pri = s * ID_Pub$ ，这里的 s 是主私钥， ID_Pub 是签名公钥。

在其中一个实施例中，服务器也可触发虚拟机来生成主私钥，通过虚拟机来生成主私钥的方式可参照上述通过虚拟机生成主公钥的方式。

在其中一个实施例中，可在服务器的可信执行环境中生成签名私钥。比如，服务器以 TEE（Trusted Execution Environment，受硬件芯片保护的可信执行环境）为硬件基础，将签名私钥的生成逻辑运行于 TEE 中，签名私钥生成组件，用以根据签名公钥和主私钥来生成签名私钥。其中，TEE：受硬件芯片保护的可信执行环境称之为 TEE（Trusted Execution Environment）。TEE 具有固有的签注密钥用于保护数据隐私和认证数据完整性、来源可靠性等；与外部有内存访问控制和内存加密机制，即外部包括操作系统也没有可信计算域内存空间的访问权限；TEE 具有远程认证机制，用于向远端证明一个可信计算域内运行的逻辑等没有受到篡改。使用可信计算达到的效果是，可信计算域内的数据、程序逻辑在没有主动输出的情况下无法被外部环境窥探。

步骤 310，将签名私钥发送至数字账户创建者标识所对应的终端；发送的签名私钥，用于触发终端基于签名私钥生成数字签名；接收终端反馈的包括数字签名的资源处理请求；及在基于数字账户的签名公钥对数字签名验证通过后，根据资源处理请求对数字账户中的虚拟资源进行处理。

具体地，当生成与签名公钥相匹配的签名私钥后，服务器可将生成的签名私钥以安全的方式发送至数字账户创建者标识所对应的终端，从而终端可将接收到的签名私钥安全存储。在其中一个实施例中，当生成签名私钥后，即表明数字账户已创建完毕，此时，服务器可将数字账户创建成功信息和签名私钥一起发送至终端，进而终端可向数字账户创建者展示数字账户创建成功消息，以及将签名私钥安全存储。

在其中一个实施例中，当数字账户创建者期望对数字账户中的虚拟资源进行处理时，比如，当数字账户创建者期望增加数字账户中的虚拟资源时，数字账户创建者可触发终端

展示虚拟资源信息采集页面，从而数字账户创建者可在虚拟资源信息采集页面输入相关信息，比如，输入期望增加的虚拟资源量和虚拟资源，进而终端可基于签名私钥对数字账户创建者输入的信息进行签名，生成数字签名，并根据数字签名生成资源处理请求，将资源处理请求发送至服务器。当服务器接收到资源处理请求时，服务器可通过与下发的签名私钥相配对的签名公钥对数字签名进行验证，并在验证通过后，响应于资源处理请求，对数字账户中的虚拟资源进行处理，比如，服务器可将期望增加的虚拟资源量的资源，从虚拟资源源转入数字账户。

在其中一个实施例中，参考图 7，数字账户创建者还可在终端中输入数字账户创建者标识，比如，输入手机号或者邮箱，进而终端可将数字账户创建者标识发送至服务器，服务器可基于接收到的数字账户创建者标识确定对应的签名公钥，比如，服务器可获取预设的签名公钥生成算法，通过签名公钥生成算法并基于接收到的数字账户创建者标识，来生成签名公钥，并将签名公钥返回至终端，以使终端展示接收到的签名公钥。进一步地，终端在接收到签名公钥后，还可通过存储的签名私钥对接收到的签名公钥进行验证，并展示验证结果。图 7 示出了一个实施例中签名公钥的展示示意图。数字账户创建者可输入一个数字账户创建者标识，也可输入多个数字账户创建者标识，当仅输入一个数字账户创建者标识时，服务器可根据输入的数字账户创建者标识，找到创建数字账户时使用的其余数字账户创建者标识。

上述资源处理方法中，在接收到数字账户创建请求时，通过从数字账户创建请求中提取出数字账户创建者标识，可基于数字账户创建者标识生成数字账户和数字账户的签名公钥。通过生成签名公钥，可基于签名公钥生成签名私钥，进而可将签名私钥发送至数字账户创建者标识所对应的终端，以使数字账户创建者标识所对应的终端可通过接收到的签名私钥生成包括数字签名的资源处理请求，并使得当通过签名公钥对数字签名验证通过时，服务器可响应于资源处理请求以对数字账户中的虚拟资源进行处理。由于签名公钥是根据签名公钥生成算法和数字账户标识生成得到的，因此，本申请无需额外维护数字账户创建者标识与签名公私钥之间的对应关系，也即无需通过中心化的数据库来对应存储数字账户创建者标识和签名公私钥，当需要确定与数字账户创建者标识对应的签名公钥时，本申请可基于签名公钥生成算法对数字账户创建者标识进行处理来反推出签名公钥。相比于传统的需要在中心化的数据库中存储数字账户创建者标识与公私钥，由于本申请无需通过中心化的数据库将数字账户创建者标识与签名公私钥对应存储，因此，减少了因中心化的数据库被攻击窃取信息而导致数字账户存在安全性的问题，进而提升了数字账户的安全性。

此外，通过主公私钥额外生成一对签名公私钥，可在后续基于签名公私钥对数字账户中的虚拟资源进行处理，而非通过主公私钥对数字账户中的虚拟资源进行处理，这样，即使主公私钥被泄露，也不会影响数字账户的安全性，如此，进一步提升了数字账户的安全性。

在其中一个实施例中，上述方法还包括主公私钥生成步骤，主公私钥生成步骤包括：产生随机数，并将随机数作为主私钥；获取第一椭圆曲线，并在第一椭圆曲线上确定第一基点；将第一基点与主私钥进行倍点运算，获得与主私钥相配对的主公钥。

具体地，在生成签名公钥和签名私钥之前，可生成一对主公私钥。当需要生成主公私钥时，服务器可产生一个随机数，并将该随机数作为主私钥。进一步地，服务器可获取一条椭圆曲线，将该椭圆曲线称作第一椭圆曲线。服务器可确定第一椭圆曲线的基点（又称作生成元），将第一椭圆曲线的基点称作第一基点，将第一基点与主私钥进行倍点运算，得到主私钥倍点，将该主私钥倍点作为与主私钥相配对的主公钥。

在其中一个实施例中，服务器产生随机数 $s \in [1, N-1]$ 作为主私钥，计算第一椭圆曲线中的元素 $P = [s] * G$ 作为主公钥，其中，第一椭圆曲线为阶为素数的 N 的加法循环群。 G 为第一椭圆曲线的基点。 $[s] * G$ 代表 G 的 s 倍点。其中，随机数可以是正整数。

基点是椭圆曲线上的点，是用于确定椭圆曲线上倍点的基础。假设坐标系（ X 轴和 Y

轴)中有椭圆曲线,其上有一个基点,该基点的切线与该椭圆曲线相交,则该相交的交点相对于坐标系的X轴对称的点为该基点的2倍点。一条经过基点的2倍点与基点的直线又与椭圆曲线相交,该相交的点相对于坐标系的X轴对称的点为3倍点,依此类推。倍点运算,是计算倍点的计算方式,可以采用快速幂算法和秦九韶算法进行倍点运算。

上述实施例中,通过生成主公钥和主私钥,使得后续可基于主公钥和主私钥生成签名公钥和签名私钥。

在其中一个实施例中,根据主公钥和数字账户创建者标识,生成数字账户的签名公钥,包括:在从数字账户创建请求中提取出多个数字账户创建者标识的情况下,对多个数字账户创建者标识和主公钥进行拼接处理,得到拼接标识;对拼接标识进行哈希运算,得到哈希标识;根据哈希标识生成签名公钥。

具体地,数字账户创建者可在账户创建页面中输入多个数字账户创建者标识,比如,输入邮箱、手机号和用户名等,进而数字账户创建者所对应的终端可生成携带有多个数字账户创建者标识的数字账户创建请求。当服务器接收到该数字账户创建请求时,服务器即可从该数字账户创建请求中提取出多个数字账户创建者标识,比如,提取出邮箱、手机号和用户名,进而服务器可将主公钥和提取出的多个数字账户创建者标识进行拼接,比如,将邮箱、手机号、用户名以及主公钥进行拼接,得到拼接标识。

进一步地,服务器对拼接标识进行哈希运算,得到哈希标识,比如,服务器可通过预设的哈希算法对拼接标识进行哈希运算,得到哈希标识,之后,基于哈希标识生成签名公钥。

本实施例中,在具有多个数字账户创建者标识的情况下,通过将多个数字账户创建者标识进行拼接,可得到拼接标识,从而后续可基于拼接标识来得到签名公钥,如此,便实现了签名公钥的生成。相比于仅能通过一个数字账户创建者标识来生成得到签名公钥,本实施例即使在接收到多个数字账户创建者标识,也可以基于多个数字账户创建者标识来得到签名公钥,从而大大提升了签名公钥的生成灵活性。

在其中一个实施例中,根据拼接标识生成签名公钥,包括:获取第二椭圆曲线,并确定第二椭圆曲线上的第二基点;根据第二椭圆曲线将第二基点与哈希标识进行融合,得到签名公钥。

具体地,当需要基于拼接标识生成签名公钥时,服务器可获取第二椭圆曲线,并确定第二椭圆曲线的基点(又称作生成元),将第二椭圆曲线的基点称作第二基点。进一步地,服务器根据第二椭圆曲线将第二基点与哈希标识进行融合,得到签名公钥。比如,服务器可通过公式: $ID_PUB = H(ID)*G$ 得到签名公钥。其中,H是哈希函数,ID是拼接标识,G是第二椭圆曲线上的第二基点,即生成元,ID_PUB为签名公钥。

上述实施例中,通过确定第二基点,可基于第二基点快速得到签名公钥,从而提升了签名公钥的生成效率。

在其中一个实施例中,根据主私钥和签名公钥,生成与签名公钥相配对的签名私钥,包括:将主私钥与签名公钥相乘,得到与签名公钥配对的签名私钥。

在其中一个实施例中,发送签名私钥包括:获取验证码,并确定加密密钥生成算法;通过加密密钥生成算法对验证码进行处理,得到第一加密密钥;根据第一加密密钥对签名私钥进行加密,得到加密私钥;将加密私钥和验证码发送至与数字账户创建者标识相对应的终端;发送的加密私钥和验证码,用于触发终端通过验证码对加密私钥进行解密,得到签名私钥。

具体地,为了能够安全地下发签名私钥,服务器可生成一个验证码,比如,服务器可基于验证码生成算法,生成一个随机的验证码。进一步地,服务器可确定预设的加密密钥生成算法,通过加密密钥生成算法对验证码进行处理,以得到第一加密密钥,通过第一加密密钥对签名私钥进行加密,得到加密私钥。加密密钥生成算法可根据需求自由设置,本实施例在此不做限定。

进一步地，服务器将第一加密密钥发送至数字账户创建者标识所对应的终端。比如，服务器通过安全链接（例如，HTTPS，Hypertext Transfer Protocol Secure，超文本传输协议），将第一加密密钥以及验证码发送至数字账户创建者标识所对应的终端。当该终端接收到第一加密密钥和验证码时，该终端可通过验证码对第一加密密钥进行解密，以得到签名私钥。

本实施例中，由于验证码的具体内容具有一定的随机性，因此，通过验证码来对签名私钥进行加密，可提升加密的随机性，进而提升加密效果。通过将加密后的签名私钥发送至终端，可提升签名私钥的发送安全性，减少在发送的过程中签名私钥被盗取的风险。

在其中一个实施例中，通过加密密钥生成算法对验证码进行处理，得到第一加密密钥，包括：获取盐值，并根据验证码和盐值，生成当前轮次的初始密钥块；获取上一个轮次的密钥块，并将当前轮次的初始密钥块与上一个轮次的密钥块进行拼接，得到当前轮次的密钥块；当当前轮次的密钥块的字节长度不满足预设长度条件时，进入一个轮次，将下一个作为当前轮次，并返回根据验证码和盐值，生成当前轮次的初始密钥块的步骤继续执行，直至当前轮次的密钥块的字节长度满足预设长度条件；将最后一个轮次的密钥块，作为第一加密密钥。

在密码学中，通过在密码任意固定位置插入特定的字符串，让散列后的结果和使用原始密码的散列结果不相符，这种过程称之为“加盐”，该特定的字符串即盐值。

本实施例中，当需要通过加密密钥算法对验证码进行处理，以生成第一加密密钥时，服务器可获取预设的盐值，该盐值可为一个字符串，进而服务器根据验证码和盐值，生成当前轮次的初始密钥块。

服务器可获取上一个轮次生成的密钥块，将上一个轮次生成的密钥块与当前轮次生成的初始密钥块进行拼接，得到当前轮次的密钥块。比如，参考图 8，服务器可将当前轮次（例如，第 5 轮次）生成的初始密钥块置于上一轮次（例如，第 4 轮次）生成的密钥块之后，得到当前轮次生成的密钥块。进一步地，可预先设置待生成的第一加密密钥的字节长度，将当前轮次生成的密钥块的字节长度与待生成的第一加密密钥的字节长度进行对比，在当前轮次生成的密钥块的字节长度小于待生成的第一加密密钥的字节长度时，确定当前轮次的密钥块的字节长度不满足预设长度条件，此时需要执行下一轮次的密钥块生成过程，服务器进入下一个轮次（例如，第 6 轮次），将下一个轮次作为当前轮次，返回根据验证码和盐值，生成当前轮次的初始密钥块的步骤继续执行，直至当前轮次的密钥块的字节长度满足预设长度条件。比如，服务器生成第 6 轮次的初始密钥块，将第 6 轮次的初始密钥块与第 5 轮次的密钥块进行拼接，得到第 6 轮次的密钥块，若第 6 轮次的密钥块的字节长度等于待生成的第一加密密钥的字节长度时，则确定当前轮次的密钥块的字节长度满足预设长度条件，此时结束密钥块的生成。

进一步地，当结束密钥块的生成过程时，服务器可将最后一个轮次的密钥块作为第一加密密钥，比如，将第 6 轮次的密钥块作为第一加密密钥。图 8 示出了一个实施例中第一加密密钥的生成示意图。

在其中一个实施例中，服务器可获取预设的字节长度，作为待生成的第一加密密钥的字节长度，并确定单个轮次生成的初始密钥块的字节长度，将待生成的第一加密密钥的字节长度除以单个轮次生成的初始密钥块的字节长度，得到应进行的轮次，服务器执行应进行的轮次后，即可得到第一加密密钥。当待生成的第一加密密钥的字节长度除以单个轮次生成的初始密钥块的字节长度，所得到的相除结果不为整数时，服务器可调整待生成的第一加密密钥的字节长度，或者，调整单个轮次生成的初始密钥块的字节长度，以使得这两者的相除结果为正整数。如此，便提升了第一加密密钥的生成灵活性。

上述实施例中，通过执行多轮次的密钥块生成过程，可增加第一加密密钥的复杂性，从而通过复杂的第一加密密钥得到复杂的加密私钥，进而减少了加密私钥被破解的概率，提升了加密私钥的安全性。

在其中一个实施例中，根据验证码和盐值，生成当前轮次的初始密钥块，包括：获取

编码数据，将盐值与编码数据进行拼接，得到目标盐值；对验证码和目标盐值进行散列哈希运算，得到首个散列密钥块；在从第二个散列密钥块生成过程起的当前散列密钥块生成过程中，根据验证码和上一个散列密钥块，生成当前散列密钥块；将下一个散列密钥块生成过程作为当前散列密钥块生成过程，返回根据验证码和上一个散列密钥块，确定当前散列密钥块的步骤继续执行，直至生成预设数量个散列密钥块时停止；将最后一个散列密钥块，作为当前轮次的初始密钥块。

具体地，在单个轮次中，服务器可获取预设的编码数据，并将盐值与预设的编码数据进行拼接，得到目标盐值。其中，编码数据为对预设数进行编码得到的预设字节长度的数据，比如，为对 i 进行编码成的 32 位数。服务器对目标盐值进行散列哈希运算，得到首个散列密钥块。

对于从第二个散列密钥块生成过程起的当前散列块密钥生成过程中，服务器可根据验证码和上一个散列密钥块生成当前散列密钥块。比如，对于第二个散列密钥块生成过程，服务器根据验证码和首个散列密钥块，生成第二个散列密钥块，对于第三个散列密钥块生成过程，服务器根据验证码和第二个散列密钥块，生成第三个散列密钥块。进一步地，服务器判断是否已生成预设数量个散列密钥块，若未生成预设数量个散列密钥块，则服务器进入下一个散列密钥块生成过程，返回根据验证码和上一个散列密钥块，确定当前散列密钥块的步骤继续执行，直至生成预设数量个散列密钥块时停止。

当生成了预设数量个散列密钥块，则服务器将最后一个散列密钥块作为当前轮次的初始密钥块。比如，在预设数量为 10，且生成了 10 个散列密钥块后，服务器则继续生成散列密钥块，将第 10 个散列密钥块作为当前轮次的初始密钥块，从而后续服务器可基于当前轮次的初始密钥块生成当前轮次的密钥块。

在其中一个实施例中，根据验证码和上一个散列密钥块生成当前散列密钥块的步骤包括：对验证码和上一个散列密钥块进行散列哈希运算，以得到当前散列密钥块。

在其中一个实施例中，生成第一加密密钥的步骤包括：

把验证码 (Code) 和一个盐值 (Salt) 作为一个输入参数，然后重复进行运算，并最终产生第一加密密钥 Key。

可通过以下公式生成第一加密密钥：Key=F1 (Code, Salt,C,kLen)

其中，C 为迭代次数，kLen 为第一加密密钥的字节长度。F1 为用以生成第一加密密钥的函数。

第一加密密钥 Key 的值由一个以上的初始密钥块拼接而成。初始密钥块的数量是 $kLen/hLen$ ，其中，hLen 为初始密钥块的字节长度。就是说，函数 F1 输出的结果比期望得到的第一加密密钥要短，则要通过拼接多个结果以满足第一加密密钥的长度，如下公式所示：

Key=T1||T2.....||T (kLen/hLen)，其中，T1、T2...均为初始密钥块。其中，每个初始密钥块则通过函数 F2 得到。

函数 F2 得到初始密钥块的步骤包括可通过以下公式实现：Ti=F2(Code,Salt,R,i)。函数 F2 里，会进行 R 次运算，以得到初始密钥块。i 为预设数，对 i 进行编码可得到编码数据。其中，第一次，函数 F2 会将盐值 Salt 与将 i 编码成的 32 位数进行拼接，得到目标盐值，通过目标盐值和验证码，得到首个散列密钥块，即 $P1=H(\text{Code}, \text{Salt}||\text{INT_32_BE}(i))$ ，H 是将 Code 和 Salt||INT_32_BE (i) 作为输入进行散列哈希运算，以得到输出 P1。

而在后续的 R-1 个散列密钥块生成过程，则会使用上次得到的散列密钥得到当前散列密钥块，即：P2= H (Code, P1)，U3= H (Code, P2)

当得到最后一个散列密钥块时，则将最后一个散列密钥块作为初始密钥块，比如，将 PR 作为在某个轮次中生成的初始密钥块。

上述实施例中，通过多轮次的生成散列密钥块，可使得生成的散列密钥块更为复杂，从而基于更为复杂的散列米密钥块得到更为复杂的初始密钥块，进而基于更为复杂的初始

密钥块得到更为复杂的第一加密密钥。

在其中一个实施例中，上述方法还包括：接收包括数字签名的资源处理请求；通过签名公钥对数字签名进行验证；在验证通过后，通过与数字账户相绑定的智能合约响应资源处理请求，以对数字账户中的资源进行处理，得到资源处理结果；将资源处理结果存储于区块链中。存储于区块链的资源处理结果可经过区块链中各共识节点的共识。

具体地，当数字账户创建者标识所对应的终端获取到签名私钥后，当数字账户创建者期望对数字账户中的虚拟资源进行处理时，数字账户创建者所对应的终端可获取到资源处理信息，进而该终端可对资源处理信息进行签名，得到数字签名，基于数字签名和数字账户创建者标识生成资源处理请求，并将资源处理请求发送至服务器。当服务器接收到携带有数字签名和数字账户创建者标识的资源处理请求时，服务器可通过数字账户创建者标识反推出签名公钥，比如，获取预设的主公钥，基于主公钥和数字账户创建者标识，按照生成签名公钥的方式来计算一个签名公钥，该计算得到的签名公钥即为反推出的签名公告，从而通过反推出的签名公钥对数字签名进行验证。当验证通过后，服务器可响应于资源处理请求，确定与数字账户创建者标识对应的数字账户，通过与该数字账户相绑定的智能合约，对该数字账户中的虚拟资源进行处理。

在其中一个实施例中，假设希望对资源处理信息 m 进行签名，所采用的第三椭圆曲线参数为 $D=(p,a,b,G,n,h)$ ，其中， G 为基点，对应签名私钥 $KeyS$ ；产生一个随机整数数 k ， $1 \leq k \leq n-1$ ；计算点 $P=k*G=(x_1,y_1)$ ，其中， (x_1,y_1) 为融合点；令 $e=x_1 \bmod n$ ，若 $e=0$ ，则返回产生一个随机整数数 k 的步骤继续执行，其中， e 为第一余数， n 为椭圆曲线的阶；计算 $z=hash(m)$ ，哈希函数可选择 UHA-2 计算；计算 $u=k^{-1}(z+eEa) \pmod n$ ，若 u 为 0，则返回产生一个随机整数数 k 的步骤继续执行，其中， u 为第二余数；综合第一余数和第二余数得到数字签名 (e,u) 。

在其中一个实施例中，当需要对数字签名进行验证时，服务器计算 $z=hash(m)$ ，其中， m 为资源处理信息， $hash()$ 为哈希运算；计算 $P_1=zu^{-1} \bmod n$ ， $P_2=eu^{-1} \bmod n$ ，其中， n 为第三椭圆曲线的阶， u 为数字签名中的第二余数， P_1 为第三余数， P_2 为第四余数；计算点 $(x_1,y_1)=P_1G+P_2Qa$ ，其中， Qa 为签名公钥， G 为第三椭圆曲线的基点；验证等式： e 是否等于 $x_1 \bmod n$ ，其中， e 为数字签名中的第一余数；若等于，则确定数字签名验证通过，此时可通过智能合约响应于资源处理请求，以对数字账户中的虚拟资源进行处理。

在其中一个实施例中，当需要通过智能合约响应于资源处理请求时，智能合约可判断资源处理请求是否为合法请求，并根据资源处理请求中的资源处理信息，确定资源处理请求是否满足智能合约所约定的条件，若满足智能合约所约定的条件，则根据资源处理请求中的资源处理信息对数字账户中的虚拟资源进行处理。比如，智能合约约定，每天最多向数字账户中转入 1000 资源量的虚拟资源，若资源处理信息表征数字账户创建者期望向数字账户转入 10000 资源量的虚拟资源时，则确定资源处理请求不满足智能合约所约定的条件，此时服务器返回资源处理失败的消息。若资源处理信息表征数字账户创建者期望向数字账户转入 500 资源量的虚拟资源时，则确定资源处理请求满足智能合约所约定的条件，此时服务器向数字账户转入 500 资源量的虚拟资源，且服务器返回资源处理成功的消息。进一步地，当对数字账户中的虚拟资源进行处理后，可将资源处理结果存储于区块链中。存储于区块链中的资源处理结果可经过区块链中各共识节点的共识。

在其中一个实施例中，对数字账户中的虚拟资源进行处理的方式可包括增减数字账户中虚拟资源的资源量。比如，将向该数字账户冲入虚拟资源，以增加该数字账户中的虚拟资源的资源量，或者，扣除该数字账户中的虚拟资源，以减少该数字账户中的虚拟资源的资源量。

上述实施例中，通过在验证通过后，再响应于资源处理请求，可大大提升虚拟资源处理的安全性。

在一个实施例中，如图 9 所示，提供了一种签名私钥获取方法，以该方法应用于图 1

中与数字账户创建者标识所对应的终端为例进行说明，包括以下步骤：

步骤 902，获取数字账户创建者标识，并根据数字账户创建者标识生成数字账户创建请求。

具体地，当需要创建数字账户时，数字账户创建者可触发终端展示账户创建页面，并在账户创建页面中输入数字账户创建者标识，比如，输入自身的手机号、邮箱和账户名等，如此，终端便可响应于数字账户创建者标识输入操作，获取数字账户创建者标识，并根据数字账户创建者标识生成数字账户创建请求。

步骤 904，发送数字账户创建请求；发送的数字账户创建请求，用于触发根据数字账户创建者标识创建数字账户、签名公钥和签名私钥，以及用于触发生成验证码，基于验证码对签名私钥进行加密，得到加密私钥。

具体地，当终端生成数字账户创建请求时，终端可将数字账户创建请求发送至服务器，以使服务器基于接收到的数字账户创建请求中的数字账户创建者标识创建数字账户、签名公钥和签名私钥。当服务器生成签名私钥后，服务器还可生成验证码，并通过验证码对签名私钥进行加密，得到加密私钥，将加密私钥和验证码发送至终端。

步骤 906，接收加密私钥和验证码。

步骤 908，通过验证码对加密私钥进行解密，获得签名私钥；签名私钥用于在资源处理的过程中，通过签名私钥生成包括数字签名的资源处理请求；数字签名，用于在通过与数字账户相绑定的签名公钥对数字签名验证通过后，触发根据资源处理请求对数字账户中的虚拟资源进行处理。

具体地，当服务器生成加密私钥后，服务器可将加密私钥和验证码一起发送至终端，从而终端可接收服务器发送的加密私钥和验证码。当终端接收到加密私钥和验证码时，终端可通过验证码对加密私钥进行解密，得到签名私钥，并在对资源处理的过程中，通过签名私钥生成数字签名，并通过数字签名生成资源处理请求，将资源处理请求发送至服务器。从而当服务器接收到资源处理请求时，服务器可通过签名公钥对数字签名进行验证，并在验证通过后，响应于资源处理请求，对数字账户中的虚拟资源进行处理。

上述签名私钥获取方法中，通过响应于数字账户创建者标识输入操作，可获取得到数字账户创建者标识，通过发送数字账户创建者标识，可触发服务器创建数字账户、签名公钥和签名私钥，以及触发服务器通过验证码对签名私钥进行加密，得到加密私钥。通过获取服务器生成的加密私钥和验证码，可通过验证码对加密私钥进行解密，以得到签名私钥，进而在资源处理的过程中，通过签名私钥来保证资源处理的安全性。由于签名公私钥是根据签名公钥生成算法和数字账户标识生成得到的，因此，本申请无需额外维护数字账户创建者标识与签名公私钥之间的对应关系，减少了因用于存储数字账户创建者标识与签名公私钥之间的对应关系的数据库被攻击窃取信息，而导致数字账户存在安全性的问题。由于本申请是将加密私钥下发至终端，相比于直接将签名私钥下发至终端，减少了签名私钥在下发过程中被窃取的风险，进一步提升了数字账户的安全性。

在其中一个实施例中，通过验证码对加密私钥进行解密，并在解密成功的情况下，获得签名私钥，包括：通过加密密钥生成算法对验证码进行处理，得到第二加密密钥；通过第二加密密钥对加密私钥进行解密，并在解密成功时，获得签名私钥。

具体地，由于服务器是通过加密密钥生成算法来对验证码进行处理，以得到第一加密密钥，并通过第一加密密钥对签名私钥进行处理的，因此，当终端接收到服务器发送的加密私钥和验证码后，终端可通过同样的加密密钥生成算法来对验证码进行处理，以得到第二加密密钥，并通过第二加密密钥来对加密私钥进行解密，在解密成功后，得到签名私钥。容易理解地，通过加密密钥生成算法来对验证码进行处理，以得到第二加密密钥的过程，可参照上述的通过加密密钥生成对验证码进行处理，以得到第一加密密钥的过程。在其中一个实施例中，加密密钥生成算法可为对称密钥生成算法，因此，生成的第一加密密钥和第二加密密钥，均为对称密钥。对称密钥是指在加密和解密时使用相同的密钥，也即，在

正确的情况下，第一加密密钥与第二加密密钥是一致的，其即可用于加密，也可用于解密。

上述实施例中，通过获取得到验证码，可基于验证码生成第二加密密钥，如此，便可基于第二加密密钥对加密私钥进行解密，以得到签名私钥。

在其中一个实施例中，上述方法还包括：当接收到服务器发送的验证码的情况下，展示验证码和验证码填写框；响应于针对验证码填写框的填写操作，展示填写的验证码；发送填写的验证码至服务器，发送的填写的验证码，用于触发服务器将填写的验证码与发送的验证码进行一致性比对，并在填写的验证码与发送的验证码一致时，确定成功下发签名私钥。

具体地，当终端接收到服务器发送的验证码时，终端还可展示验证码以及展示验证码填写框。在其中一个实施例中，该验证码具体可为短信验证码。进一步地，当数字账户创建者查看到验证码后，数字账户创建者可将验证码输入至验证码填写框中，终端可响应于针对验证码填写框的填写操作，展示数字账户创建者填写的验证码。比如，参考图 10，数字账户创建者可在验证码填写框 1001 中填写验证码。图 10 示出了一个实施例中验证码的输入示意图。

与此同时，终端还可将数字账户创建者填写的验证码发送至服务器，以使服务器将填写的验证码与之前发送的验证码进行一致性对比。当填写的验证码与发送的验证码一致时，则确定成功下发签名私钥，否则，确定下发签名私钥的过程有误。比如，服务器可将验证码“1234”发送至终端，当终端接收到“1234”时，可展示“1234”，进而数字账户创建者可将“1234”输入至验证码填写框中。当数字账户创建者将“1234”输入至验证码填写框后，终端可将“1234”发送至服务器，从而服务器可将接收到的“1234”与之前发送的“1234”进行一致性对比，由于服务器接收到的验证码与之前发送的验证码均为“1234”，则服务器可确定签名私钥已成功下发至终端。若服务器接收到的验证码为“1111”与之前发送的验证码“1234”不一致时，则确定签名私钥的下发过程有误，此时服务器可生成验证码验证失败消息，并将验证码验证失败消息发送至终端，以使终端展示验证码验证失败消息，进而数字账户创建者可通过展示的验证码验证失败消息，确定终端接收到的签名私钥有误。

本实施例中，通过在验证码输入框中输入验证码，并将输入的验证码发送至服务器，可使得服务器对接收到的验证码与发送的验证码进行一致性比对，从而基于比对结果快速确定签名私钥是否已成功下发至终端。比如，便实现了签名私钥的下发验证，提升了下发至终端的签名私钥的准确性。

在其中一个实施例中，签名私钥用于在资源处理的过程中，触发通过签名私钥生成包括数字签名的资源处理请求，包括：展示多个物品，响应于针对多个物品的选择操作，展示选择操作选中的物品的详情页面；详情页面显示有物品获取控件和获取选择操作选中的物品的所需付出的资源量；响应于针对物品获取控件的触发操作，根据获取选择操作选中的物品的所需付出的资源量生成资源处理报文；通过签名私钥对资源处理报文进行签名，得到数字签名，并根据数字签名生成资源处理请求。

具体地，当成功创建数字账户，以及当成功获取得到签名私钥后，数字账户创建者可对数字账户中的虚拟资源进行处理。比如，数字账户创建者可触发终端展示多个物品，数字账户创建者可通过选择操作在多个物品中选择一个物品，将选择的物品作为目标物品，进而终端可响应于数字账户创建者的选择操作，展示目标物品的详情页面。在目标物品的详情页面中，可显示有目标物品获取控件和获取目标物品的所需付出的资源量。比如，参考图 11，可显示确定控件 1101，该确定控件即为上述的目标物品获取控件，图 11 中的“资源量：328” 1102，即为上述的获取目标物品的所需付出的资源量。图 11 示出了一个实施例中详情页面的示意图。

当数字账户创建者点击了物品获取控件时，终端即可响应于针对物品获取控件的点击操作，将目标物品的获取数量、获取目标物品所需付出的资源量、资源接收账户等信息作为资源处理信息，并根据资源处理信息生成资源处理报文。比如，终端可按照预设的报文

格式，对资源处理信息进行转换，以得到资源处理报文，或者，终端可直接将资源处理信息作为资源处理报文。进一步地，终端通过签名私钥对资源处理报文进行签名，得到数字签名，其中，通过签名私钥对资源处理报文进行签名的方式，可参照上述的通过签名私钥对资源处理信息进行签名的方式。本实施例在此不作赘述。

进一步地，当得数字签名后，终端可通过数字账户创建者标识、数字签名、资源处理报文生成资源处理请求，也即，终端生成携带有数字账户创建者标识、数字签名和资源处理报文的资源处理请求，并将该资源处理请求发送至服务器。当服务器接收到资源处理请求后，服务器可通过数字账户创建者标识反推出签名公钥，通过签名公钥对数字签名进行验证，在验证通过后，从与数字账户创建者标识相对应的数字账户中提取出一定资源量的虚拟资源，将提取出的虚拟资源流入至资源接收账户中。该一定资源量，为基于获取选择操作选中的物品的所需付出的资源量确定得到的资源量。比如，当数字账户创建者期望获取得到两个目标物品，且获取单个目标物品所需付出的资源量为 100，则服务器从数字账户中提取出 200 资源量的虚拟资源，并将提取出的 200 资源量的虚拟资源存入资源接收账户中。当资源接收账户接收到虚拟资源后，资源接收账户所对应的用户即可将目标物品发送至数字账户创建者。

在其中一个实施例中，当数字账户中的虚拟资源的资源量发生了变化时，可将变化结果存储至区块链中，比如，当数字账户中的虚拟资源减少了 200 时，则可将数字账户剩余的资源量存储至区块链中。存储至区块链中的资源量可经过区块链中各共识节点的共识。

上述实施例中，通过获取得到签名私钥，可通过签名私钥对资源处理报文进行签名，得到数字签名。通过得到数字签名，可在数字签名验证通过后，再对数字账户中的虚拟资源进行处理，从而提升了虚拟资源处理的安全性。

在其中一个实施例中，在创建了数字账户之后，服务器还用于接收资源处理请求，资源处理请求携带有账户创建者标识、资源处理信息和通过数字账户创建者标识所对应的签名私钥生成的资源处理请求数字签名；根据数字账户创建者标识确定对应的签名公钥，并通过签名公钥对资源处理请求数字签名进行验证；在验证通过的情况下，根据数字账户创建者标识和资源处理信息，生成与资源处理请求对应的临时标识；根据临时标识，生成与资源处理请求对应的临时公钥和临时私钥；发送临时私钥，发送的临时私钥，用于在响应于针对资源处理请求触发的请求确认操作时，触发通过临时私钥生成请求确认数字签名；接收请求确认数字签名，并在通过临时公钥对请求确认数字签名验证通过的情况下，响应于资源处理请求，对数字账户创建者标识所对应的数字账户中的虚拟资源进行处理。

具体地，当数字账户创建者期望对数字账户中的虚拟资源进行处理时，数字账户创建者标识可触发终端生成资源处理请求，并将资源处理请求发送至服务器。在服务器通过签名公钥对资源处理请求携带的资源处理请求数字签名验证通过后，服务器可根据数字账户创建者标识和资源处理信息生成与资源处理请求相对应的临时标识。比如，可将数字账户创建者标识与资源处理订单号进行拼接，以得到临时标识。之后，服务器可通过该临时标识生成与该资源处理请求相对应的临时公钥和临时私钥。通过临时标识生成临时公钥和临时私钥的方式，可参照上述生成签名公钥和签名私钥的方式。将生成的临时私钥下发至数字账户创建者标识所对应的终端，当数字账户创建者触发了针对资源处理请求触发的请求确认操作时，终端可通过临时私钥对确认报文进行签名，生成请求确认数字签名，并将请求确认数字签名发送至服务器，以使服务器通过临时公钥对请求确认数字签名进行验证，并在验证通过时，响应于资源处理请求，对数字账户创建者标识所对应的数字账户中的虚拟资源进行处理。通过针对每个资源处理请求均生成一个临时公钥和临时私钥，这样即使临时公钥和临时私钥被泄露，也仅会影响一个资源处理请求，而不会影响其他的资源处理请求，大大提升了资源处理的安全性。

在其中一个具体实施例中，参考图 12，提供了一种虚拟资源处理方法，包括：

步骤 1202，通过终端响应于数字账户创建者标识输入操作，获取数字账户创建者标识，

并根据数字账户创建者标识生成数字账户创建请求，并将数字账户创建请求发送至服务器。

步骤 1204，通过服务器响应于数字账户创建请求，从数字账户创建请求中提取出数字账户创建者标识，根据数字账户创建者标识创建用以存储虚拟资源的数字账户。

步骤 1206，在从数字账户创建请求中提取出多个数字账户创建者标识的情况下，通过服务器对多个数字账户创建者标识和预设的主公钥进行拼接处理，得到拼接标识，对拼接标识进行哈希运算，得到哈希标识。

步骤 1208，通过服务器获取第二椭圆曲线，并确定第二椭圆曲线上的第二基点；根据第二椭圆曲线将第二基点与哈希标识进行融合，得到签名公钥，将签名公钥与预设的主私钥相乘，得到签名私钥。

步骤 1210，通过服务器获取验证码，并确定加密密钥生成算法，并通过加密密钥生成算法对验证码进行处理，得到第一加密密钥；根据第一加密密钥对签名私钥进行加密，得到加密私钥；将加密私钥和验证码发送至相应终端。

步骤 1212，通过终端接收加密私钥和验证码；通过加密密钥生成算法对验证码进行处理，得到第二加密密钥；通过第二加密密钥对加密私钥进行解密，并在解密成功时，获得签名私钥。

步骤 1214，通过终端展示验证码和验证码填写框；响应于针对验证码填写框的填写操作，展示填写的验证码；发送填写的验证码至服务器。

步骤 1216，通过服务器接收在数字账户创建者在终端中填写的验证码，将填写的验证码与发送的验证码进行一致性比对，并在填写的验证码与发送的验证码一致时，确定成功下发签名私钥。

步骤 1218，通过终端展示多个物品，响应于针对多个物品的选择操作，展示选择操作选中的物品的详情页面；详情页面显示有物品获取控件和获取选择操作选中的物品的所需付出的资源量。

步骤 1220，通过终端响应于针对物品获取控件的触发操作，根据获取选择操作选中的物品的所需付出的资源量生成资源处理报文，并通过签名私钥对资源处理报文进行签名，得到数字签名，并根据数字签名生成资源处理请求，将资源处理请求发送至服务器。

步骤 1222，通过服务器接收资源处理请求，通过对应的签名公钥对资源处理请求中的数字签名进行验证，在验证通过后，对数字账户中的虚拟资源进行处理。

应该理解的是，虽然如上所述的各实施例所涉及的流程图中的各个步骤按照箭头的指示依次显示，但是这些步骤并不是必然按照箭头指示的顺序依次执行。除非本文中有明确的说明，这些步骤的执行并没有严格的顺序限制，这些步骤可以以其它的顺序执行。而且，如上所述的各实施例所涉及的流程图中的至少一部分步骤可以包括多个步骤或者多个阶段，这些步骤或者阶段并不必然是在同一时刻执行完成，而是可以在不同的时刻执行，这些步骤或者阶段的执行顺序也不必然是依次进行，而是可以与其它步骤或者其它步骤中的步骤或者阶段的至少一部分轮流或者交替地执行。

本申请还提供一种应用场景，该应用场景应用上述的资源处理方法。具体地，该资源处理方法在该应用场景的应用如下：

当多个数字账户创建者期望创建一个共享账户时，多个数字账户创建者可分别在自身的终端中输入自身的数字账户创建者标识，多个数字账户创建者也可在一个终端中输入自身的数字账户创建者标识。当服务器获取到各数字账户创建者标识后，服务器即可基于获取到的数字账户创建者标识，并通过预设的主公私钥，创建一个共享账户，以及与共享账户对应的签名私钥和签名公钥。服务器将签名私钥进行分片，得到多个签名私钥分片，将各签名私钥分片下发至数字账户创建者，以使每个数字账户创建者均可拿到一个签名私钥分片。当某个数字账户创建者期望对共享账户中的虚拟资源进行处理时，服务器可生成一个虚拟资源处理授权请求，并将虚拟资源处理授权请求下发至各数字账户创建者，数字账户创建者可根据需求，确定是否授权对共享账户中的虚拟资源进行处理。若某个数字账

户创建者授权对共享账户中的虚拟资源进行处理，则终端会将该数字账户创建者的签名私钥分片发送至管理者所对应的终端。比如，当数字账户创建者 B 授权数字账户创建者 A 对共享账户中的虚拟资源进行处理，则数字账户创建者 B 所对应的终端会将数字账户创建者 B 接收到的签名私钥分片发送至管理者所对应的终端。管理者所对应的终端可基于接收到的签名私钥分片对签名私钥进行还原，当接收到越多的签名私钥分片时，则越有可能还原出签名私钥。当管理者所对应的终端还原出签名私钥后，管理者所对应的终端可通过还原出的签名私钥对资源处理信息进行签名，以生成包括数字签名的资源处理请求，并将资源处理请求发送至服务器，以使服务器基于签名公钥响应于该资源处理请求，对共享账户中的虚拟资源进行处理。

本申请还另外提供一种应用场景，该应用场景应用上述的资源处理方法。具体地，该资源处理方法在该应用场景的应用如下：

数字账户具体可为数字钱包，针对数字钱包，可绑定有智能合约，用于约束用户对数字钱包的使用。用户可通过数字钱包来进行物品的购买。

上述应用场景仅为示意性的说明，可以理解，本申请各实施例所提供的资源处理方法的应用不局限于上述场景。

基于同样的发明构思，本申请实施例还提供了一种用于实现上述所涉及的资源处理方法的资源处理装置。该装置所提供的解决问题的实现方案与上述方法中所记载的实现方案相似，故下面所提供的一个或多个资源处理装置实施例中的具体限定可以参见上文中对于资源处理方法的限定，在此不再赘述。

在一个实施例中，如图 13 所示，提供了一种资源处理装置 1300，包括：签名公钥生成模块 1302、签名私钥生成模块 1304、签名私钥发送模块 1306、资源处理请求接收模块 1308 和资源处理模块 1310，其中：

签名公钥生成模块 1302，用于在接收到数字账户创建请求的情况下，响应于数字账户创建请求，从数字账户创建请求中提取出数字账户创建者标识；根据数字账户创建者标识创建用以存储虚拟资源的数字账户；获取预设的主公钥，根据主公钥和数字账户创建者标识，生成数字账户的签名公钥。

签名私钥生成模块 1304，用于获取与主公钥相配对的主私钥，根据主私钥和签名公钥，生成与签名公钥相配对的签名私钥。

签名私钥发送模块 1306，用于将签名私钥发送至数字账户创建者标识所对应的终端；发送的签名私钥，用于触发终端基于签名私钥生成数字签名；

资源处理请求接收模块 1308，用于接收终端反馈的包括数字签名的资源处理请求；及资源处理模块 1310，用于在基于数字账户的签名公钥对数字签名验证通过后，根据资源处理请求对数字账户中的虚拟资源进行处理。

在其中一个实施例中，资源处理装置 1300 还包括主公私钥生成模块，用于产生随机数，并将随机数作为主私钥；获取第一椭圆曲线，并在第一椭圆曲线上确定第一基点；将第一基点与主私钥进行倍点运算，获得与主私钥相配对的主公钥。

在其中一个实施例中，签名公钥生成模块 1302 还用于在从数字账户创建请求中提取出多个数字账户创建者标识的情况下，对多个数字账户创建者标识以及主公钥进行拼接处理，得到拼接标识；对拼接标识进行哈希运算，得到哈希标识；根据哈希标识生成签名公钥。

在其中一个实施例中，签名公钥生成模块 1302 还用于获取第二椭圆曲线，并确定第二椭圆曲线上的第二基点；根据第二椭圆曲线将第二基点与哈希标识进行融合，得到签名公钥。

在其中一个实施例中，签名私钥发送模块 1306 还用于获取验证码，并确定加密密钥生成算法；通过加密密钥生成算法对验证码进行处理，得到第一加密密钥；根据第一加密密钥对签名私钥进行加密，得到加密私钥；将加密私钥和验证码发送至与数字账户创建者标

识相对应的终端；发送的加密私钥和验证码，用于触发终端通过验证码对加密私钥进行解密，得到签名私钥。

在其中一个实施例中，签名私钥发送模块 1306 还用于获取盐值，并根据验证码和盐值，生成当前轮次的初始密钥块；获取上一个轮次的密钥块，并将当前轮次的初始密钥块与上一个轮次的密钥块进行拼接，得到当前轮次的密钥块；当当前轮次的密钥块的字节长度不满足预设长度条件时，进入一个轮次，将下一个作为当前轮次，并返回根据验证码和盐值，生成当前轮次的初始密钥块的步骤继续执行，直至当前轮次的密钥块的字节长度满足预设长度条件；将最后一个轮次的密钥块，作为第一加密密钥。

在其中一个实施例中，签名私钥发送模块 1306 还用于获取编码数据，将盐值与编码数据进行拼接，得到目标盐值；对验证码和目标盐值进行散列哈希运算，得到首个散列密钥块；在从第二个散列密钥块生成过程起的当前散列密钥块生成过程中，根据验证码和上一个散列密钥块，生成当前散列密钥块；下一个散列密钥块生成过程作为当前散列密钥块生成过程，返回根据验证码和上一个散列密钥块，确定当前散列密钥块的步骤继续执行，直至生成预设数量个散列密钥块时停止；将最后一个散列密钥块，作为当前轮次的初始密钥块。

在其中一个实施例中，资源处理装置 1300 还包括资源处理模块，用于接收包括数字签名的资源处理请求；通过签名公钥对数字签名进行验证；在验证通过后，通过与数字账户相绑定的智能合约响应资源处理请求，以对数字账户中的资源进行处理，得到资源处理结果；将资源处理结果存储于区块链中，并经过区块链中各共识节点的共识。

在一个实施例中，如图 14 所示，提供了一种签名私钥获取装置 1400，包括：请求生成模块 1402、请求发送模块 1404 和密钥接收模块 1406，其中：

请求生成模块 1402，用于获取数字账户创建者标识，并根据数字账户创建者标识生成数字账户创建请求。

请求发送模块 1404，用于发送数字账户创建请求；发送的数字账户创建请求，用于触发根据数字账户创建者标识创建数字账户、签名公钥和签名私钥，以及用于触发生成验证码，基于验证码对签名私钥进行加密，得到加密私钥。

密钥接收模块 1406，用于接收加密私钥和验证码；通过验证码对加密私钥进行解密，获得签名私钥；签名私钥用于在资源处理的过程中，通过签名私钥生成包括数字签名的资源处理请求；数字签名，用于在通过与数字账户相绑定的签名公钥对数字签名验证通过后，触发根据资源处理请求对数字账户中的虚拟资源进行处理。

在其中一个实施例中，密钥接收模块 1406 还用于通过加密密钥生成算法对验证码进行处理，得到第二加密密钥；通过第二加密密钥对加密私钥进行解密，并在解密成功时，获得签名私钥。

在其中一个实施例中，密钥接收模块 1406 还用于当接收到服务器发送的验证码的情况下，展示验证码和验证码填写框；响应于针对验证码填写框的填写操作，展示填写的验证码；发送填写的验证码至服务器，发送的填写的验证码，用于触发服务器将填写的验证码与发送的验证码进行一致性比对，并在填写的验证码与发送的验证码一致时，确定成功下发签名私钥。

在其中一个实施例中，签名私钥获取装置 1400 还包括物品获取模块，用于展示多个物品，响应于针对多个物品的选择操作，展示选择操作选中的物品的详情页面；详情页面显示有物品获取控件和获取选择操作选中的物品的所需付出的资源量；响应于针对物品获取控件的触发操作，根据获取选择操作选中的物品的所需付出的资源量生成资源处理报文；通过签名私钥对资源处理报文进行签名，得到数字签名，并根据数字签名生成资源处理请求。

上述资源处理装置以及签名私钥获取装置中的各个模块可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于计算机设备中的处理器中，也

可以以软件形式存储于计算机设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

在一个实施例中，提供了一种计算机设备，该计算机设备可以是服务器，其内部结构图可以如图 15 所示。该计算机设备包括处理器、存储器、输入/输出接口(Input/Output，简称 I/O)和通信接口。其中，处理器、存储器和输入/输出接口通过系统总线连接，通信接口通过输入/输出接口连接到系统总线。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质和内存存储器。该非易失性存储介质存储有操作系统、计算机程序和数据库。该内存存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的数据库用于存储数字账户创建数据。该计算机设备的输入/输出接口用于处理器与外部设备之间交换信息。该计算机设备的通信接口用于与外部的终端通过网络连接通信。该计算机程序被处理器执行时以实现一种资源处理方法。

在一个实施例中，提供了一种计算机设备，该计算机设备可以是终端，其内部结构图可以如图 16 所示。该计算机设备包括处理器、存储器、输入/输出接口、通信接口、显示单元和输入装置。其中，处理器、存储器和输入/输出接口通过系统总线连接，通信接口、显示单元和输入装置通过输入/输出接口连接到系统总线。其中，该计算机设备的处理器用于提供计算和控制能力。该计算机设备的存储器包括非易失性存储介质、内存存储器。该非易失性存储介质存储有操作系统和计算机程序。该内存存储器为非易失性存储介质中的操作系统和计算机程序的运行提供环境。该计算机设备的输入/输出接口用于处理器与外部设备之间交换信息。该计算机设备的通信接口用于与外部的终端进行有线或无线方式的通信，无线方式可通过 WIFI、移动蜂窝网络、NFC（近场通信）或其他技术实现。该计算机程序被处理器执行时以实现一种签名私钥获取方法。该计算机设备的显示单元用于形成视觉可见的画面，可以是显示屏、投影装置或虚拟现实成像装置，显示屏可以是液晶显示屏或电子墨水显示屏，该计算机设备的输入装置可以是显示屏上覆盖的触摸层，也可以是计算机设备外壳上设置的按键、轨迹球或触控板，还可以是外接的键盘、触控板或鼠标等。

本领域技术人员可以理解，图 15 至图 16 中示出的结构，仅仅是与本申请方案相关的部分结构的框图，并不构成对本申请方案所应用于其上的计算机设备的限定，具体的计算机设备可以包括比图中所示更多或更少的部件，或者组合某些部件，或者具有不同的部件布置。

在一个实施例中，还提供了一种计算机设备，包括存储器和处理器，存储器中存储有计算机程序，该处理器执行计算机程序时实现上述各方法实施例中的步骤。

在一个实施例中，提供了一种计算机可读存储介质，存储有计算机程序，该计算机程序被处理器执行时实现上述各方法实施例中的步骤。

在一个实施例中，提供了一种计算机程序产品或计算机程序，该计算机程序产品或计算机程序包括计算机指令，该计算机指令存储在计算机可读存储介质中。计算机设备的处理器从计算机可读存储介质读取该计算机指令，处理器执行该计算机指令，使得该计算机设备执行上述各方法实施例中的步骤。

需要说明的是，本申请所涉及的用户信息（包括但不限于用户设备信息、用户个人信息等）和数据（包括但不限于用于分析的数据、存储的数据、展示的数据等），均为经用户授权或者经过各方充分授权的信息和数据，且相关数据的收集、使用和处理需要遵守相关国家和地区的相关法律法规和标准。

本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的计算机程序可存储于一非易失性计算机可读存储介质中，该计算机程序在执行时，可包括如上述各方法的实施例的流程。其中，本申请所提供的各实施例中所使用的对存储器、数据库或其它介质的任何引用，均可包括非易失性和易失性存储器中的至少一种。非易失性存储器可包括只读存储器（Read-Only Memory, ROM）、磁带、软盘、闪存、光存储器、高密度嵌入式非易失性存储器、阻变存

存储器 (ReRAM)、磁变存储器 (Magnetoresistive Random Access Memory, MRAM)、铁电存储器 (Ferroelectric Random Access Memory, FRAM)、相变存储器 (Phase Change Memory, PCM)、石墨烯存储器等。易失性存储器可包括随机存取存储器 (Random Access Memory, RAM) 或外部高速缓冲存储器等。作为说明而非局限, RAM 可以是多种形式, 比如静态随机存取存储器 (Static Random Access Memory, SRAM) 或动态随机存取存储器 (Dynamic Random Access Memory, DRAM) 等。本申请所提供的各实施例中所涉及的数据库可包括关系型数据库和非关系型数据库中至少一种。非关系型数据库可包括基于区块链的分布式数据库等, 不限于此。本申请所提供的各实施例中所涉及的处理器可为通用处理器、中央处理器、图形处理器、数字信号处理器、可编程逻辑器、基于量子计算的数据处理逻辑器等, 不限于此。

以上实施例的各技术特征可以进行任意的组合, 为使描述简洁, 未对上述实施例中的各个技术特征所有可能的组合都进行描述, 然而, 只要这些技术特征的组合不存在矛盾, 都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式, 其描述较为具体和详细, 但并不能因此而理解为对发明专利范围的限制。应当指出的是, 对于本领域的普通技术人员来说, 在不脱离本申请构思的前提下, 还可以做出若干变形和改进, 这些都属于本申请的保护范围。因此, 本申请专利的保护范围应以所附权利要求为准。

权利要求

- 1、一种资源处理方法，由服务器执行，所述方法包括：
响应于数字账户创建请求，从所述数字账户创建请求中提取出数字账户创建者标识；
根据所述数字账户创建者标识创建用于存储虚拟资源的数字账户；
获取预设的主公钥，根据所述主公钥和所述数字账户创建者标识，生成所述数字账户的签名公钥；
获取与所述主公钥相配对的主私钥，根据所述主私钥和所述签名公钥，生成与所述签名公钥相配对的签名私钥；
将所述签名私钥发送至所述数字账户创建者标识所对应的终端；发送的所述签名私钥，用于触发所述终端基于所述签名私钥生成数字签名；
接收所述终端反馈的包括所述数字签名的资源处理请求；及
在基于所述数字账户的所述签名公钥对所述数字签名验证通过后，根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。
- 2、根据权利要求1所述的方法，所述方法还包括：
产生随机数，并将所述随机数作为主私钥；
获取第一椭圆曲线，并在所述第一椭圆曲线上确定第一基点；
将所述第一基点与所述主私钥进行倍点运算，获得与所述主私钥相配对的主公钥。
- 3、根据权利要求1或2所述的方法，所述根据所述主公钥和所述数字账户创建者标识，生成所述数字账户的签名公钥，包括：
在从所述数字账户创建请求中提取出多个数字账户创建者标识的情况下，对所述多个数字账户创建者标识以及所述主公钥进行拼接处理，得到拼接标识；
对所述拼接标识进行哈希运算，得到哈希标识；
根据所述哈希标识生成签名公钥。
- 4、根据权利要求3所述的方法，所述根据所述哈希标识生成签名公钥，包括：
获取第二椭圆曲线，并确定所述第二椭圆曲线上的第二基点；
根据所述第二椭圆曲线将所述第二基点与所述哈希标识进行融合，得到签名公钥。
- 5、根据权利要求1至4任一项所述的方法，所述根据所述主私钥和所述签名公钥，生成与所述签名公钥相配对的签名私钥，包括：
将所述主私钥与所述签名公钥相乘，得到与所述签名公钥配对的签名私钥。
- 6、根据权利要求1至5任一项所述的方法，所述发送所述签名私钥包括：
获取验证码，并确定加密密钥生成算法；
通过所述加密密钥生成算法对所述验证码进行处理，得到第一加密密钥；
根据所述第一加密密钥对所述签名私钥进行加密，得到加密私钥；
将所述加密私钥和所述验证码发送至与所述数字账户创建者标识相对应的终端；发送的所述加密私钥和所述验证码，用于触发所述终端通过所述验证码对所述加密私钥进行解密，得到所述签名私钥。
- 7、根据权利要求6所述的方法，所述通过所述加密密钥生成算法对所述验证码进行处理，得到第一加密密钥，包括：
获取盐值，并根据所述验证码和所述盐值，生成当前轮次的初始密钥块；
获取上一个轮次的密钥块，并将所述当前轮次的初始密钥块与所述上一个轮次的密钥块进行拼接，得到当前轮次的密钥块；
当所述当前轮次的密钥块的字节长度不满足预设长度条件时，进入下一个轮次，将下一个轮次作为当前轮次，并返回根据所述验证码和所述盐值，生成当前轮次的初始密钥块的步骤继续执行，直至所述当前轮次的密钥块的字节长度满足所述预设长度条件；
将最后一个轮次的密钥块，作为第一加密密钥。

8、根据权利要求 7 所述的方法，所述根据所述验证码和所述盐值，生成当前轮次的初始密钥块，包括：

获取编码数据，将所述盐值与所述编码数据进行拼接，得到目标盐值；

对所述验证码和所述目标盐值进行散列哈希运算，得到首个散列密钥块；

在从第二个散列密钥块生成过程起的当前散列密钥块生成过程中，根据所述验证码和上一个散列密钥块，生成当前散列密钥块；

进入下一个散列密钥块生成过程，将下一个散列密钥块生成过程作为当前散列密钥块生成过程，返回根据所述验证码和上一个散列密钥块，生成当前散列密钥块的步骤继续执行，直至生成预设数量个散列密钥块时停止；

将最后一个散列密钥块，作为当前轮次的初始密钥块。

9、根据权利要求 1 至 8 任意一项所述的方法，所述方法还包括：

接收包括数字签名的资源处理请求；

通过所述签名公钥对所述数字签名进行验证；

在验证通过后，基于与所述数字账户相绑定的智能合约响应所述资源处理请求，以对所述数字账户中的资源进行处理，得到资源处理结果；

将所述资源处理结果存储于区块链中。

10、一种签名私钥获取方法，由终端执行，所述方法包括：

获取数字账户创建者标识，并根据所述数字账户创建者标识生成数字账户创建请求；

发送所述数字账户创建请求，发送的所述数字账户创建请求，用于触发根据所述数字账户创建者标识创建数字账户、签名公钥和签名私钥，以及用于触发生成验证码，根据所述验证码对所述签名私钥进行加密，得到加密私钥；

接收所述加密私钥和所述验证码；

通过所述验证码对所述加密私钥进行解密，获得所述签名私钥，所述签名私钥用于在资源处理的过程中，基于所述签名私钥生成包括数字签名的资源处理请求，所述数字签名，用于在基于与所述数字账户相绑定的所述签名公钥对所述数字签名验证通过后，触发根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

11、根据权利要求 10 所述的方法，所述通过所述验证码对所述加密私钥进行解密，获得所述签名私钥，包括：

通过所述加密密钥生成算法对所述验证码进行处理，得到第二加密密钥；

通过所述第二加密密钥对所述加密私钥进行解密，并在解密成功时，获得所述签名私钥。

12、根据权利要求 11 所述的方法，所述方法还包括：

当接收到服务器发送的验证码的情况下，展示验证码和验证码填写框；

响应于针对所述验证码填写框的填写操作，展示填写的验证码；

发送所述填写的验证码至所述服务器，发送的所述填写的验证码，用于触发所述服务器将所述填写的验证码与发送的验证码进行一致性比对，并在所述填写的验证码与所述发送的验证码一致时，确定成功下发所述签名私钥。

13、根据权利要求 10 至 12 任一项所述的方法，所述资源处理请求的生成步骤包括：

展示多个物品，响应于针对所述多个物品的选择操作，展示所述选择操作选中的物品的详情页面；所述详情页面显示有物品获取控件和获取所述选择操作选中的物品的所需付出的资源量；

响应于针对所述物品获取控件的触发操作，根据所述获取所述选择操作选中的物品的所需付出的资源量生成资源处理报文；

通过所述签名私钥对所述资源处理报文进行签名，得到数字签名，并根据所述数字签名生成资源处理请求。

14、一种资源处理装置，所述装置包括：

签名公钥生成模块，用于在接收到数字账户创建请求的情况下，响应于所述数字账户创建请求，从所述数字账户创建请求中提取出数字账户创建者标识；根据所述数字账户创建者标识创建用于存储虚拟资源的数字账户；获取预设的主公钥，根据所述主公钥和所述数字账户创建者标识，生成所述数字账户的签名公钥；

签名私钥生成模块，用于获取与所述主公钥相配对的主私钥，根据所述主私钥和所述签名公钥，生成与所述签名公钥相配对的签名私钥；

签名私钥发送模块，用于将所述签名私钥发送至所述数字账户创建者标识所对应的终端；发送的所述签名私钥，用于触发所述终端基于所述签名私钥生成数字签名；

资源处理请求接收模块，用于接收所述终端反馈的包括所述数字签名的资源处理请求；及

资源处理模块，用于在基于所述数字账户的所述签名公钥对所述数字签名验证通过后，根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

15、一种签名私钥获取装置，所述装置包括：

请求生成模块，用于获取数字账户创建者标识，并根据所述数字账户创建者标识生成数字账户创建请求；

请求发送模块，用于发送所述数字账户创建请求；发送的所述数字账户创建请求，用于触发根据所述数字账户创建者标识创建数字账户、签名公钥和签名私钥，以及用于触发生成验证码，基于所述验证码对所述签名私钥进行加密，得到加密私钥；

密钥接收模块，用于接收所述加密私钥和所述验证码；通过所述验证码对所述加密私钥进行解密，获得所述签名私钥，所述签名私钥用于在资源处理的过程中，基于所述签名私钥生成包括数字签名的资源处理请求，所述数字签名，用于在基于与所述数字账户相绑定的所述签名公钥对所述数字签名验证通过后，触发根据所述资源处理请求对所述数字账户中的虚拟资源进行处理。

16、一种计算机设备，包括存储器和处理器，所述存储器存储有计算机程序，所述处理器执行所述计算机程序时实现权利要求1至13中任一项所述的方法的步骤。

17、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权利要求1至13中任一项所述的方法的步骤。

18、一种计算机程序产品，包括计算机程序，该计算机程序被处理器执行时实现权利要求1至13中任一项所述的方法的步骤。