

身份验证方法、系统、存储介质及芯片

技术领域

本申请属于计算机技术领域，尤其涉及一种身份验证方法、系统、存储介质及芯片。

发明背景

5 随着快递业迅猛发展，为了更好地从源头保障快递的安全，我国快递实名制登记正式开始。为了满足实名寄件的需求，收派人员在为用户进行寄件服务时，需要对用户进行身份验证。在当前的快递寄件场景中，如果用户预先在物流公司平台上进行过实名认证，用户通过在线提交寄件订单，收派件人员在为用户进行寄件服务时，可以直接通过物流公司平台完成用户身份的验证；如果用户未在物流公司平台进行过实名认证，则收派件人员需要对用户出示的身份信息进行验证。另外，当用户需要邮寄贵重物品时，即使用户预先在物流公司平台上进行过实名认证，在收件时收派人员还需要对用户出示的身份信息再次进行验证。

10 当收派人员需要对用户出示身份信息进行验证时，收派件人员的时间成本将会大大增加。并且用户无论是在物流公司平台上进行实名认证，或者是向收派件人员出示身份信息，都将增大用户信息泄露的风险。因此，如何在实现用户身份验证的同时提高用户信息的安全性，成为亟待解决的技术问题。

发明内容

本申请实施例提供了一种身份验证方法、系统、存储介质及芯片，能够实现用户的身份认证的同时减少信息泄露的风险。

20 第一方面，本申请实施例提供了一种身份验证方法，应用于身份验证系统，身份验证系统包括物流管理平台、多个收派员终端和分布式身份系统，该方法包括：物流管理平台或者目标收派员终端向分布式身份系统发送身份验证请求，身份验证请求包括第一分布式身份标识（DID）标识符和第一可验证声明（VC）文档，目标收派员终端为多个收派员终端中的一个；分布式身份系统根据身份验证请求，对用户进行身份验证，以获得身份验证结果；在身份验证结果为验证成功的情况下，分布式身份系统对订单信息进行验证，以获得订单验证结果，并向目标收派员终端发送订单验证结果。

25 第二方面，本申请实施例提供了一种身份验证系统，包括物流管理平台、多个收派员终端和分布式身份系统，物流管理平台用于执行如以上第一方面所述的方法中物流管理平台所执行的步骤，多个收派员终端中的一个收派员终端用于执行如以上第一方面所述的方法中目标收派员终端所执行的步骤，分布式身份系统用于执行如以上第一方面所述的方法中分布式身份系统所执行的步骤。

第三方面，本申请实施例提供了一种计算机可读存储介质，计算机可读存储介质中存储有计算机程序或指令，当计算机读取并执行计算机程序或指令时，使得计算机执行如以上第一方面所述的方法。

5 第四方面，本申请实施例提供了一种芯片，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有芯片的计算机设备执行如以上第一方面所述的方法。

在本申请提供的身份验证方法中，利用分布式身份系统进行身份验证和订单信息验证，身份验证用于确定用户是真实的用户，即，用户和现实中的人一一对应；订单信息验证用于确定订单的合法性，即，订单信息是由用户下单的，具备法律属性。由于身份验证和订单信息验证均是由分布式身份系统完成的，因此用户只需在分布式身份系统中完成实名认证，而
10 无需在物流管理平台进行实名认证，也不需要向收派员出示身份信息，可以最大限度的保证用户身份信息的安全性，从而实现用户的身份认证的同时减少信息泄露的风险。。

附图简要说明

为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有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一些实施例，
15 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，还可以根据这些附图获得其他的附图。

图 1 是本申请一实施例提供的身份验证系统的场景示意图。

图 2 是本申请一实施例中提供的应用分布式数字身份的原理图。

20 图 3 是本申请一实施例提供的在分布式身份系统中进行实名注册的过程的示意性交互图。

图 4 是本申请一实施例提供的身份验证方法的示意性交互图。

图 5 是本申请另一实施例提供的身份验证方法的示意性交互图。

图 6 是本申请一实施例提供的计算机设备的内部结构示意图。

图 7 是本申请一实施例提供的存储介质的内部结构示意图。

实施本发明的方式

25 为了满足实名寄件的需求，收派人员在为用户进行寄件服务时，需要对用户进行身份验证。无论是用户在物流公司平台上进行实名认证，或者是用户向收派件人员出示身份信息，都将增大用户信息泄露的风险。因此，如何在实现用户身份验证的同时提高用户信息的安全性（或者在实现用户的身份认证的同时减少信息泄露的风险），成为亟待解决的技术问题。

图 1 为本申请一实施例提供的身份验证系统的场景示意图，如图 1 所示，该场景包括身份
30 验证系统 100 和用户终端 200。身份验证系统 100 包括物流管理平台 110、多个收派员终端 121，122，123...12m 和分布式身份系统 130。物流管理平台 110 分别与用户终端 200、多个收

派员终端 121, 122, 123...12m 以及分布式身份系统 130 通信连接, 多个收派员终端 121, 122, 123...12m 与分布式身份系统 130 通信连接。

示例性的, 物流管理平台 110 与用户终端 200 交互, 物流管理平台 110 与多个收派员终端 121, 122, 123...12m 交互, 物流管理平台 110 与分布式身份系统 130 交互, 例如, 物流管理平台 110 接收用户终端 200 发送的登录请求, 并根据登录请求, 对用户进行登录验证; 物流管理平台 110 接收用户终端 200 发送的订单信息, 并根据订单信息, 从多个收派员终端 121, 122, 123...12m 中确定目标收派员终端 12x, 并向目标收派员终端 12x 发送订单信息即, 向目标收派员终端 12x 派单。目标收派员终端 12x 在接收到订单信息之后, 目标收派员终端 12x 向分布式身份系统 130 发送身份验证请求, 分布式身份系统 130 根据身份验证请求, 对用户进行身份验证, 以获得身份验证结果, 在身份验证结果为验证成功的情况下, 向分布式身份系统 130 发送订单验证请求。分布式身份系统 130 在接收到订单验证请求之后, 根据订单验证请求, 对订单信息进行验证, 以获得订单验证结果, 并向目标收派员终端 12x 发送订单验证结果。

除了上述提到, 目标收派员终端 12x 向分布式身份系统 130 发送身份验证请求以外, 身份验证请求也可以是物流管理平台 110 向分布式身份系统 130 发送的。

可以理解的是, 物流管理平台 110 为物流公司内部的管理系统, 例如, 可以为物流公司提供物流服务的服务器; 多个收派员终端 121, 122, 123...12m 为物流公司的收派员所使用的终端设备, 例如, 可以为手持设备(例如手机、把枪等)、车载设备或可穿戴设备等; 分布式身份系统 130 为对用户进行实名认证、对用户进行身份验证和订单验证的平台, 例如, 可以包括用于实现分布式数字身份功能的服务器和区块链; 用户终端 200 为想要寄件的用户所使用的终端设备。

应当理解的是, 本申请实施例中用户可以利用用户终端 200 在分布式身份系统 130 中进行实名注册, 而无需在物流管理平台 110 中进行实名注册; 分布式身份系统 130 对用户终端 200 进行身份验证, 从而避免了收派员花费过多时间进行身份验证以及用户身份信息的泄露的问题。

再者, 分布式身份系统 130 采用分布式数字身份(Decentralized Identity, DID), 也称去中心化身份。基于区块链的分布式数字身份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。

为了便于理解, 在本申请实施例中的分布式身份系统 130 进行介绍之前, 下面结合图 2 对分布式数字身份的原理进行示例性的说明。

图 2 为本申请一实施例中提供的应用分布式数字身份的原理图, 其主要示出了注册/验证的流程。如图 2 所示, 在分布式数字身份应用中, 参与的实体包括发行人(Issuer)21、持有人(Holder)22、验证人(Verifier)23、DID 注册系统(例如, 区块链节点)24 和凭证存储平台(例如, 分布式存储节点)25。可验证声明(Verifiable Credential, VC)是在各个实体之间流转的可验证信息, 可验证声明提供了一种规范来描述实体所具有的某些属性, 实现基于证据的信

任。持有人 22 可以通过可验证声明，向其他实体 (如验证人 23) 证明自己的某些属性是可信的。DID 标识符 (即，分布式身份标识符) 是一个特定格式的字符串且全局唯一，用来代表一个持有人的数字身份。

应当理解，发行人 21 拥有用户数据并且能向持有人 22 出具 (或颁布) 相应的可验证声明，
5 如政府部门、公安机关、教育机构等可以作为发行人。持有人 22 则是可验证声明的持有者，任何人都可以充当该实体角色。验证人 23 负责接收持有人 22 出示的可验证声明，并对可验证声明进行核验，在通过核验后，为持有人 22 提供相应的服务。区块链节点 24 负责链上的数据信息的验证维护，例如，发行人 21 和验证人 23 在链上对可验证声明进行核验，或者持有人 22 在链上注册身份；分布式存储节点 25 负责链上链下数据信息的验证维护，例如，发行人 21
10 向分布式存储节点 25 颁布/更新/撤销用户数据，或持有人 22 授权/存储用户数据。

本申请实施例中的分布式身份系统 130，是基于图 2 中的分布式数字身份的原理来设置的。如图 1 所示，本申请实施例中的分布式身份系统 130 包括身份认证服务器 132、证书颁发机构 (Certification Authorities, CA) 服务器 131 和区块链 133，并且身份认证服务器 132、CA 服务器 132 和区块链 133 之间两两通信连接。由图 1 可知，分布式身份系统 130 通过身份认证服
15 务器 132 分别与物流管理平台 110 和多个收派员终端 121, 122, 123...12m 通信连接，例如，物流管理平台 110 或目标收派员终端 12x 向身份认证服务器 132 发送身份验证请求。区块链 133 包括多个节点 1, 2, 3...n, 通过多个节点 1, 2, 3...n, 实现去中心化身份，去中心化是将数据分散存储在多个节点 1, 2, 3...n 上，多个节点 1, 2, 3...n 的数量越多，数据的安全性也会越高。图 2 中的区块链节点 24 可以理解为是图 1 的区块链 133 中的任意节点 x。

20 可以理解的是，身份认证服务器 132 可以为单独的服务器，也可以为多个服务器组成的服务器集群；同样的，CA 服务器 131 可以为单独的服务器，也可以为多个服务器组成的服务器集群。

为了使得分布式数字身份系统中各部分的作用能够更清楚地被理解，下面结合附图 1 和 3 对用户在分布式身份系统进行实名注册 (也称实名认证) 的过程进行示例性的说明。图 3 为
25 本申请一实施例中提供的在分布式身份系统中进行实名注册的过程的交互示意图。如图 3 所示，实名认证的过程包括以下步骤 S301 至 S309。步骤 S301 至 S309 中提到的用户终端即为图 1 中的用户终端 200，步骤 S301 至 S309 中提到的身份认证服务器即为图 1 中的身份认证服务器 132，步骤 S301 至 S309 中提到的 CA 服务器即为图 1 中的证书颁发机构服务器 131，步骤 S301 至 S309 中提到的区块链即为图 1 中的区块链 133。

30 S301: 用户在用户终端输入实名注册信息。

实名注册信息也可称为实名认证信息，实名注册信息包括用户的身份信息。例如，用户的身份信息可以为用户的身份证号、指纹信息或面部识别信息等。

S302: 用户终端根据实名注册信息，向身份认证服务器发送实名注册请求。

S303: 身份认证服务器根据实名注册请求, 生成与用户对应的第二 DID 标识符和第二 VC 文档。

第二 DID 标识符和第二 VC 文档是与用户相对应的, 即, 第二 DID 标识符和第二 VC 文档可以作为用户的数字身份信息。后续的订单验证和身份验证, 是通过对第二 DID 标识符和
5 第二 VC 文档进行验证来实现的。

应当理解, 如无特殊声明, 本申请实施例中的 VC 文档即为图 2 中所示的可验证声明。

在一些实施例中, 实名注册信息可以加密存储到身份认证服务器, 另外, 实名注册信息的哈希值(hash 值)可以上传到区块链上保存, 哈希算法可以使用 sha256 和 sm3 等。

S304: 身份认证服务器向 CA 服务器发送密钥请求。

10 S305: CA 服务器根据密钥请求, 生成第二公钥和第二私钥。

第二公钥和第二私钥为与用户对应的公钥和私钥。

应当理解的是, 第二私钥和第二公钥可以用于后续的订单验证和身份验证, 即, 订单验证和身份验证可以采用私钥签名和公钥验签的方式来进行验证, 方法简单, 便于应用。

S306: CA 服务器向身份认证服务器发送第二公钥和第二私钥。

15 S307: 身份认证服务器对第二公钥、第二 DID 标识符和第二 VC 文档进行存储。

S308: 身份认证服务器将第二私钥、第二 DID 标识符和第二 VC 文档返回给用户终端。

S309: 身份认证服务器将第二公钥、第二 DID 标识符和第二 VC 文档上传到区块链。

第二私钥只能由用户终端保存, 同时用户终端也会对第二 DID 标识符和第二 VC 文档进行保存。第二公钥、第二 DID 标识符和第二 VC 文档则由身份认证服务器和/或区块链保存。

20 应当理解, 身份认证服务器和区块链在对第二公钥、第二 DID 标识符和第二 VC 文档进行存储时, 还会对第二 DID 标识符和第二 VC 文档的映射关系, 第二 DID 标识符和第二公钥的映射关系等进行存储。

例如, 在后续进行身份验证或者订单验证时, 身份认证服务器或区块链可以通过第二 DID 标识符查找到第二公钥和/或第二 VC 文档, 从而实现验证。

25 当用户在分布式身份系统中完成实名注册之后, 身份验证系统利用第二公钥、第二私钥、第二 DID 标识符和第二 VC 文档, 实现对用户的身份验证和订单验证, 并且由于全程无需向物流管理平台和收派员终端出示用户的身份信息, 因此可以避免用户身份信息的泄露。

基于本申请上述实施例提供的身份验证系统, 本申请一种身份验证方法, 图 4 为本申请一实施例提供的身份验证方法的示意性交互图。如图 4 所示, 该方法可以包括 S401 至 S411。

30 下面结合图 4 对各个步骤进行详细说明。

S401: 物流管理平台接收用户终端发送的登录请求, 登录请求包括第一 DID 标识符和第一 VC 文档。

用户终端发送的登录请求是用户终端根据用户输入的第一 DID 标识符和第一 VC 文档生成的。

S402: 物流管理平台根据第一 DID 标识符和第一 VC 文档, 生成身份验证请求。

S403: 物流管理平台向分布式身份系统发送身份验证请求, 身份验证请求包括第一 DID 标识符和第一 VC 文档。

S404: 分布式身份系统根据身份验证请求, 对用户进行身份验证, 以获得身份验证结果。

5 在一些实施例中, 分布式身份系统根据身份验证请求, 对用户进行身份验证可以包括以下步骤: 分布式身份系统根据第一 DID 标识符, 确定与第一 DID 标识符对应的目标 VC 文档; 分布式身份系统将目标 VC 文档与第一 VC 文档进行比较, 确定身份验证结果。

应当理解, 分布式身份系统中存储的 DID 标识符和 VC 文档是一一对应的, 并且该 DID 标识符和 VC 文档对应的用户是在分布式身份系统中实名注册过的用户。因此, 分布式身份系统 10 在获得第一 DID 标识符之后, 若查找到与第一 DID 标识符对应的目标 VC 文档, 并且目标 VC 文档与第一 VC 文档相同, 则用户身份验证成功; 若未查找到与第一 DID 标识符对应的目标 VC 文档, 或者查找的目标 VC 文档与第一 VC 文档不同, 则用户身份验证失败。

在另外一些实施例中, 分布式身份系统根据身份验证请求, 对用户进行身份验证可以包括以下步骤: 分布式身份系统利用自身的公钥, 对第一 VC 文档进行验签, 以获得身份验证结果。分布式身份系统在生成与用户对应的 VC 文档时, 会利用自己的私钥对其进行电子签名, 15 当分布式身份系统接收到第一 VC 文档时, 利用自己的公钥对第一 VC 文档进行验签, 如果验签通过, 则证明第一 VC 文档是分布式身份系统生成的 VC 文档, 即, 用户的身份验证成功; 如果验签失败, 则证明第一 VC 文档不是分布式身份系统生成的, 即, 用户的身份验证失败。

S405: 分布式身份系统将身份验证结果作为登录验证结果发送至物流管理平台。

20 S406: 在登录验证成功的情况下, 物流管理平台接收用户终端发送的订单信息。

应当理解, 用户终端发送的订单信息是由用户在该用户终端进行订单信息填写得到的。用户终端向物流管理平台发送的订单信息, 是采用该用户终端中存储的用户的第一私钥进行电子签名之后的订单信息。电子签名技术为成熟的相关技术, 在此不做具体阐述。

S407: 物流管理平台根据订单信息, 从多个收派员终端中确定出目标收派员终端。

25 S408: 物流管理平台将订单信息发送至目标收派员终端。

应当理解, 目标收派员终端为可以接收该订单的收派员所使用的终端设备。一般来说, 订单信息中可以包括寄件地址, 物流管理平台根据寄件地址, 确定该寄件地址所对应的收派员, 进而确定目标收派员终端。

示例性的, 每个收派员都有自己的服务范围, 通过判断寄件地址处于哪个收派员的服务 30 范围内, 从而确定该收派员为目标收派员, 该目标收派员所使用的收派员终端为目标收派员终端。

S409: 目标收派员终端向分布式身份系统发送订单验证请求, 订单验证请求包括订单信息。

可以理解的是, 订单验证请求是由目标收派员终端根据订单信息生成的。

示例性的，收派员携带终端设备（即，目标收派员终端）为用户进行寄件服务，当收派员在到达与用户约定的收件位置后，为了对用户进行验证（即，订单验证），收派员点击终端设备显示的验证控件，以使得目标收派员终端向分布式身份系统发送订单验证请求。

S410：分布式身份系统对订单信息进行验证，以获得订单验证结果。

5 在一些实施例中，物流管理平台接收到订单信息为用户终端利用私钥进行电子签名后的订单信息，分布式身份系统在对订单信息进行验证，以获得订单验证结果可以包括以下步骤：分布式身份系统根据订单验证请求中的第一 DID 标识符，确定目标公钥，目标公钥为分布式身份系统存储的与第一 DID 标识符对应的公钥；分布式身份系统利用目标公钥，对订单信息进行验签，以获得订单验证结果。采用私钥签名和公钥验签的方式，对订单信息进行验证，
10 方法简单，便于实现。

S411：分布式身份系统向目标收派员终端发送订单验证结果。

物流管理平台和分布式身份系统，利用用户在用户终端中填写的第一 DID 标识符和第一 VC 文档，对用户进行登录验证，登录验证结果即为身份验证结果。通过将登录验证和身份验证合二为一，简化了验证过程，且方法简单，身份验证效率较高。并且由于在登录过程中完
15 成了身份验证，因此，后续流程无需再进行身份验证，即，用户终端后续的下单过程均可只对订单信息进行验证，提高了验证效率，并提升了物流订单的处理效率。

在一些实施例中，分布式身份系统进行订单验证或者身份验证时，可以利用身份认证服务器来进行验证，也可以为利用区块链进行智能合约验证。

下面以订单验证为例，对身份认证服务器验证和区块链的智能合约验证进行示例性的说
20 明。

在利用身份认证服务器进行验证时，身份认证服务器根据订单验证请求中的第一 DID 标识符，确定与用户对应的目标公钥，并利用目标公钥，对订单信息进行验签，以获得订单验证结果。

在利用区块链进行智能合约验证时，目标收派员终端根据订单验证请求中的第一 DID 标识符，确定区块链合约接口，从而使得区块链完成订单验证。区块链进行订单验证可以包括
25 以下步骤：区块链根据订单验证请求中的第一 DID 标识符，确定与用户对应的目标公钥，并利用目标公钥，对订单信息进行验签，以获得订单验证结果。

应当理解的是，私钥签名和公钥验签为本领域技术人员容易理解的技术内容，本申请实施例对此不做赘述。

30 下面以根据身份验证请求，对用户进行身份验证为例，对身份认证服务器验证和区块链的智能合约验证进行示例性的说明。

在一些实施例中，在利用身份认证服务器进行验证时，身份认证服务器根据身份验证请求中的第一 DID 标识符，确定身份认证服务器中存储的与第一 DID 标识符对应的目标 VC 文档，并将确定的目标 VC 文档与第一 VC 文档进行比较，以获得身份验证结果。

可以理解的是，将确定的目标 VC 文档与第一 VC 文档进行比较时，如果目标 VC 文档与第一 VC 文档相同，则确定身份验证结果为验证成功；如果目标 VC 文档与第一 VC 文档不同，则确定身份验证结果为验证失败。

在另一些实施例中，在利用身份认证服务器进行验证时，身份认证服务器利用第一公钥，
5 对第一 VC 文档进行验签，以获得身份验证结果。第一公钥为身份认证服务器的公钥。

可以理解的是，身份认证服务器在为用户生成第二 VC 文档时，身份认证服务器利用自身的私钥，对第二 VC 文档进行了电子签名，因此，在进行身份验证时，身份认证服务器利用自己的第一公钥对第一 VC 文档进行验签，如果验签成功，说明第一 VC 文档是身份认证服务器颁发的，因此，确定身份验证结果为验证成功；如果验签失败，说明第一 VC 文档不是身份认
10 证服务器颁发的，因此，确定身份验证结果为验证失败。

在一些实施例中，在利用区块链进行智能合约验证时，目标收派员终端根据身份验证请求中的第一 DID 标识符，确定区块链合约接口，从而使得区块链完成身份验证。区块链进行身份验证可以包括以下步骤：区块链根据第一 DID 标识符，确定区块链存储的与第一 DID 标识符对应的目标 VC 文档，并将目标 VC 文档与第一 VC 文档进行比较，以获得身份验证结果。
15 可以理解的是，如果目标 VC 文档与第一 VC 文档相同，则确定身份验证结果为验证成功；如果目标 VC 文档与第一 VC 文档不同，则确定身份验证结果为验证失败。

在另外一些实施例中，区块链根据第一 VC 文档中的身份认证服务器的标识信息，确定身份认证服务器的公钥，并利用身份认证服务器的公钥，对第一 VC 文档进行验签，以获得身份验证结果。采用公钥验签，确定身份验证结果时，如果验签成功，则确定身份验证结果为验证成功，如果验签失败，则确定身份验证结果为验证失败。
20

在一些实施例中，目标收派员终端在接收到订单验证结果之后，若订单验证结果为验证成功，则目标收派员终端向收派员提示验证成功，目标收派员终端向物流管理平台发送运单生成指示信息，物流管理平台根据运单生成指示信息，生成基于订单信息的运单；若订单验证结果为验证失败，则目标收派员终端向物流平台发送终止下单请求，物流管理平台向用户
25 终端发送下单失败提醒。在验证成功的情况下，物流管理平台生成基于订单信息的运单，即，用户成功下单，方法简单，便于实现；在验证失败的情况下，物流管理平台向用户终端发送下单失败提醒，以提高用户体验。

在一些实施例中，登录请求包括用户终端在物流管理平台注册的用户名和密码，应当理解，由于用户无需在物流管理平台进行实名认证，因此，基于用户名和密码的登录验证无法
30 实现对用户的身份验证。由于用户在登录物流管理平台的过程中，物流管理平台未对用户进行身份验证，所以可以在进行订单信息验证之前进行身份验证。下面结合附图 5 对这种情况下的身份验证方法进行示例性的说明。

图 5 为本申请另一实施例提供的身份验证方法的示意性交互图。如图 5 所示，该方法可以包括 S501 至 S510。下面结合图 5 对各个步骤进行详细说明。

S501: 物流管理平台接收用户终端发送的登录请求, 登录请求包括用户在物流管理平台注册的用户名和密码。

S502: 物流管理平台根据登录请求, 对用户进行登录验证。

5 S503: 在登录成功的情况下, 物流管理平台接收用户终端发送的第一 DID 标识符、第一 VC 文档和订单信息。

S504: 物流管理平台根据订单信息, 从多个收派员终端中确定出目标收派员终端。

S505: 物流管理平台向目标收派员终端发送第一 DID 标识符、第一 VC 文档和订单信息。

应当理解, 第一 DID 标识符和第一 VC 文档的传输与订单信息的传输也可以分开进行, 本申请实施例对此不做限制。

10 S506: 目标收派员终端根据第一 DID 标识符和第一 VC 文档, 生成身份验证请求。

S507: 目标收派员终端将身份验证请求发送至分布式身份系统。

S508: 分布式身份系统根据身份验证请求, 对用户进行身份验证, 以获得身份验证结果。

应当理解, 分布式身份系统根据身份验证请求, 对用户进行身份验证的过程, 与图 4 所示的实施例中的分布式身份系统根据身份验证请求, 对用户进行身份验证的过程基本相同。

15 在此不做赘述。

S509: 在身份验证结果为验证成功的情况下, 分布式身份系统对订单信息进行验证, 以获得订单验证结果。

S510: 分布式身份系统向目标收派员终端发送订单验证结果。

用户可以通过在物流管理平台注册的用户名和密码, 登录物流管理平台, 因此, 该登录
20 过程对用户较为友好。并且在进行订单信息验证之前, 分布式身份系统根据用户终端发送的第一 DID 标识符和第一 VC 文档, 对用户进行身份验证, 只有在身份验证成功的情况下, 才进行订单信息的验证, 在身份验证失败的情况下, 无需进行订单验证, 因此, 可以减少分布式身份系统的数据处理量。身份验证可以确定使用用户终端的用户为真实的用户 (即用户与现实中的用户一一对应), 订单信息验证则可以确定订单的合法性, 即, 该订单确实是用户所
25 下的订单, 具备法律属性。

在一些实施例中, 目标收派员终端将第一 DID 标识符、第一 VC 文档、订单信息和运单上传至区块链存储。通过对生成运单所使用的数据以及运单上链存储, 可以起到证据保存的作用, 当用户对订单产生质疑时, 可以用作证据, 并且可以避免用户事后否认生成的运单, 以保证目标收派员终端的利益 (或者收派员的合法权益)。

30 应理解, 上述实施例中各步骤的序号的大小并不意味着执行顺序的先后, 各过程的执行顺序应以其功能和内在逻辑确定, 而不应对本申请实施例的实施过程构成任何限定。本申请一实施例还提供了一种计算机设备 600。该计算机设备可以为用户终端、收派员终端、物流管理平台以及分布式身份系统中的至少一个。如图 6 所示, 计算机设备 600 包括: 处理器 601、存储器 602 以及存储在存储器 602 中并在处理器 601 上运行的计算机程序 604。计算机程序

604 可被处理器 601 运行，生成指令 603，处理器 601 根据指令 603 实现上述各个实施例所述的方法。

示例性的，计算机程序 604 可以被分割成一个或多个模块/单元，一个或者多个模块/单元被存储在存储器 602 中，并由处理器 601 执行，以完成上述各个实施例所述的方法。一个或多个模块/单元可以是能够完成特定功能的一系列计算机程序指令段，该指令段用于描述计算机程序 604 在计算机设备 600 中的执行过程。

本领域技术人员可以理解，图 6 仅仅是计算机设备 600 的示例，并不构成对计算机设备 600 的限定，计算机设备 600 可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如计算机设备 600 还可以包括输入输出设备、网络接入设备或总线等。

10 处理器 601 可以是中央处理单元（Central Processing Unit, CPU），还可以是其它通用处理器、数字信号处理器（Digital Signal Processor, DSP）、专用集成电路（Application Specific Integrated Circuit, ASIC）、现场可编程门阵列（Field-Programmable Gate Array, FPGA）或者其它可编程逻辑器件、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该处理器也可以是任何常规的处理器等。

15 存储器 602 可以是计算机设备 600 的内部存储单元，例如，计算机设备 600 的硬盘或内存。存储器 602 也可以是计算机设备 600 的外部存储设备，例如，计算机设备 600 上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等。进一步地，存储器 602 还可以既包括计算机设备 600 的内部存储单元也包括外部存储设备。存储器 602 用于存储计算机程序以及计算机设备 600 所需的其它程序和数据。

20 存储器 602 还可以用于暂时地存储已经输出或者将要输出的数据。

本申请实施例还提供了一种物流管理平台，所述物流管理平台用于执行本申请实施例提供的任一种身份验证方法中物流管理平台所执行的步骤。

本申请实施例还提供了一种分布式身份系统，所述分布式身份系统用于执行本申请实施例提供的任一种身份验证方法中分布式身份系统所执行的步骤。

25 参见图 7，本申请实施例还提供了一种计算机可读存储介质 700，计算机可读存储介质 700 中存储有计算机程序或指令 710，当计算机读取并执行计算机程序或指令 710 时，使得计算机执行上述各个方法实施例所述的方法。

本申请实施例提供了一种计算机程序产品，当计算机程序产品在服务器上运行时，使得服务器执行时，实现本申请实施例提供的任一种身份验证方法。

30 本申请实施例还提供了一种芯片，该芯片包括：处理单元和通信单元。该处理单元例如可以是处理器，该通信单元例如可以是输入/输出接口、管脚或电路等。该处理单元用于从存储器中调用并运行计算机程序或计算机指令，以使安装有芯片的计算机设备执行本申请实施例提供的任一种身份验证方法。

可选地，该计算机程序或计算机指令被存储在存储单元中。

可选地，该存储单元为该芯片内的存储单元，如寄存器、缓存等，该存储单元还可以是位于该芯片外部的存储单元，如 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 RAM 等。上述任一处提到的处理器，可以是一个 CPU，微处理器，ASIC，或一个或多个集成电路。该处理单元和该存储单元可以解耦，分别设置在不同的物理设备上，通过有线或者无线的方式连接，实现该处理单元和该存储单元的各自的功能，以支持该、芯片实现上述实施例中的各种功能。或者，该处理单元和该存储器也可以耦合在同一个设备上。

可以理解的是，本申请实施例提供的芯片可以为用于实现上述任一种身份验证方法的集成电路，该芯片的主要作用是用于执行本申请实施例中的身份验证方法所限定的步骤或者流程，即通过硬件的方式来实现本申请实施例中的身份验证方法。以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

1、一种身份验证方法，其特征在于，应用于身份验证系统，所述身份验证系统包括物流管理平台、多个收派员终端和分布式身份系统，所述方法包括：

所述物流管理平台或者目标收派员终端向所述分布式身份系统发送身份验证请求，所述身份验证请求包括第一分布式身份标识（DID）标识符和第一可验证声明（VC）文档，所述目标收派员终端为所述多个收派员终端中的一个；

所述分布式身份系统根据所述身份验证请求，对用户进行身份验证，以获得身份验证结果；

在所述身份验证结果为验证成功的情况下，所述分布式身份系统对订单信息进行验证，以获得订单验证结果，并向所述目标收派员终端发送所述订单验证结果。

2、根据权利要求1所述的方法，其特征在于，还包括：

所述物流管理平台接收用户终端发送的登录请求，所述登录请求包括所述第一 DID 标识符和所述第一 VC 文档；

所述物流管理平台根据所述第一 DID 标识符和所述第一 VC 文档，生成所述身份验证请求；

在身份验证成功的情况下，所述分布式身份系统向所述物流管理平台发送登录成功的信息。

3、根据权利要求2所述的方法，其特征在于，还包括：

在登录成功的情况下，所述物流管理平台接收所述用户终端发送的所述订单信息；

所述物流管理平台根据所述订单信息，从所述多个收派员终端中确定所述目标收派员终端，并向所述目标收派员终端发送所述订单信息；

所述目标收派员终端向所述分布式身份系统发送订单验证请求，所述订单验证请求包括所述订单信息。

4、根据权利要求1所述的方法，其特征在于，还包括：

所述物流管理平台接收用户终端发送的登录请求，并根据所述登录请求，对所述用户进行登录验证，所述登录请求包括所述用户在所述物流管理平台注册的用户名和密码；

在登录成功的情况下，所述物流管理平台接收所述用户终端发送的所述第一 DID 标识符、所述第一 VC 文档和所述订单信息，并根据所述订单信息，从所述多个收派员终端中确定所述目标收派员终端；

所述物流管理平台向所述目标收派员终端发送所述第一 DID 标识符、所述

第一 VC 文档和所述订单信息；

所述目标收派员终端根据所述第一 DID 标识符和所述第一 VC 文档，生成所述身份验证请求；

所述目标收派员终端向所述分布式身份系统发送所述订单信息。

- 5 5、根据权利要求 1 至 4 中任一项所述的方法，其特征在于，所述分布式身份系统根据所述身份验证请求，对所述用户进行身份验证，以获得身份验证结果，包括：

10 所述分布式身份系统根据所述第一 DID 标识符，确定与所述第一 DID 标识符对应的目标 VC 文档，并将所述目标 VC 文档与所述第一 VC 文档进行比较，以获得所述身份验证结果，

或者，所述分布式身份系统利用第一公钥，对所述第一 VC 文档进行验签，以获得所述身份验证结果，所述第一 VC 文档为所述分布式身份系统利用所述分布式身份系统的私钥进行电子签名后得到的，所述第一公钥为所述分布式身份系统的公钥。

- 15 6、根据权利要求 1 至 5 中任一项所述的方法，其特征在于，所述订单信息为所述用户终端利用第一私钥进行电子签名后得到的，所述第一私钥为所述用户终端存储的与所述用户对应的私钥；

所述分布式身份系统对订单信息进行验证，以获得订单验证结果，包括：

20 所述分布式身份系统根据所述第一 DID 标识符，确定目标公钥，所述目标公钥为所述分布式身份系统存储的与所述第一 DID 标识符对应的公钥；

所述分布式身份系统利用所述目标公钥，对所述订单信息进行验签，以获得所述订单验证结果。

- 25 7、根据权利要求 1 至 6 中任一项所述的方法，其特征在于，所述分布式身份系统包括身份认证服务器、证书颁发机构（CA）服务器和区块链，所述方法还包括：

所述身份认证服务器接收所述用户终端发送的实名注册请求，所述实名注册请求包括所述用户的身份信息；

所述身份认证服务器根据所述实名注册请求，生成与所述用户对应的第二 DID 标识符和第二 VC 文档，并向所述 CA 服务器发送密钥请求；

- 30 所述 CA 服务器根据所述密钥请求，生成与所述用户对应的第二公钥和第二私钥，并向所述身份认证服务发送所述第二公钥和所述第二私钥；

所述身份认证服务器向所述用户终端发送所述第二私钥、所述第二 DID 标识符和所述第二 VC 文档；

所述身份认证服务器存储所述第二公钥、所述第二 DID 标识符和所述第二

VC 文档。

8、根据权利要求 1 至 7 中任一项所述的方法，其特征在于，所述分布式身份系统包括身份认证服务器、证书颁发机构（CA）服务器和区块链，所述方法还包括：

- 5 所述身份认证服务器接收所述用户终端发送的实名注册请求，所述实名注册请求包括所述用户的身份信息；

 所述身份认证服务器根据所述实名注册请求，生成与所述用户对应的第二 DID 标识符和第二 VC 文档，并向所述 CA 服务器发送密钥请求；

- 10 所述 CA 服务器根据所述密钥请求，生成与所述用户对应的第二公钥和第二私钥，并向所述身份认证服务发送所述第二公钥和所述第二私钥；

 所述身份认证服务器向所述用户终端发送所述第二私钥、所述第二 DID 标识符和所述第二 VC 文档；

 所述身份认证服务器将所述第二公钥、所述第二 DID 标识符和所述第二 VC 文档上传到所述区块链。

- 15 9、根据权利要求 7 或 8 所述的方法，其特征在于，所述分布式身份系统根据所述身份验证请求，对所述用户进行身份验证，包括：

 所述身份认证服务器或所述区块链根据所述身份验证请求，对所述用户进行身份验证。

- 20 10、根据权利要求 7 至 9 中任一项所述的方法，其特征在于，所述分布式身份系统对订单信息进行验证，包括：

 所述身份认证服务器或所述区块链对所述订单信息进行验证。

11、根据权利要求 1 至 10 中任一项所述的方法，其特征在于，包括：

 若所述订单验证结果为验证成功，则所述目标收派员终端向所述物流管理平台发送运单生成指示信息；

- 25 所述物流管理平台根据所述运单生成指示信息，生成基于所述订单信息的运单。

12、根据权利要求 11 所述的方法，其特征在于，还包括：

 所述目标收派员终端将所述第一 DID 标识符、所述第一 VC 文档、所述订单信息和所述运单上传至所述区块链存储。

- 30 13、一种身份验证系统，其特征在于，包括物流管理平台、多个收派员终端和分布式身份系统，所述物流管理平台用于执行权利要求 1 至 12 中任一项所述的方法中所述物流管理平台所执行的步骤，所述多个收派员终端中的一个收派员终端用于执行权利要求 1 至 12 中任一项所述的方法中所述目标收派员终端所执行的步骤，所述分布式身份系统用于执行权利要求 1 至 12 中任一项所述的方法

中所述分布式身份系统所执行的步骤。

14、一种计算机可读存储介质，其特征在于，所述计算机可读存储介质中存储有计算机程序或指令，当计算机读取并执行所述计算机程序或指令时，使得所述计算机执行如权利要求 1 至 12 中任一项所述的方法。

- 5 15、一种芯片，其特征在于，包括：处理器，用于从存储器中调用并运行计算机程序，使得安装有所述芯片的计算机设备执行如权利要求 1 至 12 中任一项所述的方法。