

数字证书管理方法、装置、计算机设备和存储介质

本申请要求于 2018 年 7 月 24 日提交的申请号为 201810821687.3、发明名称为“数字证书管理方法、装置、计算机设备和存储介质”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本申请涉及计算机技术领域，特别是涉及数字证书管理方法、装置、计算机设备和存储介质。

背景技术

数字证书是用于在网络上证明网络节点身份的证明文件，为了证明身份，网络节点可以向权威认证中心申请数字证书，权威认证中心在进行身份认证后向该网络节点颁发数字证书。

目前，数字证书的生成以及存储均集中在权威认证中心，如果该权威认证中心被劫持，则权威认证中心生成或存储的数字证书是不可靠的，导致网络安全性低。

发明内容

本申请实施例提供一种数字证书管理方法、装置、计算机设备和存储介质，可用于解决相关技术中网络安全性低的问题。该技术方案包括：

一方面，提供了一种数字证书管理方法，所述方法由计算机设备执行，所述方法包括：接收证书申请节点发送的数字证书生成请求，所述数字证书生成请求携带身份认证信息；将所述身份认证信息发送到各个共识认证中心进行认证，获取各个所述共识认证中心根据所述身份认证信息进行认证得到的认证结果；根据各个所述共识认证中心的认证结果确定所述证书申请节点对应的身份认证结果；当所述身份认证结果为通过认证时，根据所述数字证书生成请求生成所述证书申请节点对应的目标数字证书；将所述目标数字证书作为交易资源写入至所述共识认证中心对应的区块链。

一方面，提供了一种数字证书管理装置，所述装置包括：生成请求接收模块，用于接收证书申请节点发送的数字证书生成请求，所述数字证书生成请求携带身份认证信息；共识认证模块，用于将所述身份认证信息发送到各个共识认证中心进行认证，获取各个所述共识认证中心根据所述身份认证信息进行认证得到的认证结果；身份认证结果得到模块，用于根据各个所述共识认证中心的认证结果确定所述证书申请节点对应的身份认证结果；证书生成模块，用于当所述身份认证结果为通过认证时，根据所述数字证书生成请求生成所述证书申请节点对应的目标数字证书；写入模块，用于将所述目标数字证书作为交易资源写入至所述共识认证中心对应的区块链。

一方面，提供了一种计算机设备，包括存储器和处理器，所述存储器中存储有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器执行上述数字证书管理方法的步骤。

一方面，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上存储有计算机程序，所述计算机程序被处理器执行时，使得所述处理器执行上述数字证书管理方法的步骤。

一方面，提供了一种计算机程序产品，当该计算机程序产品被执行时，其用于执行上述数字证书管理方法。

本申请实施例提供的技术方案带来的有益效果至少包括：

通过多个认证中心来对证书申请节点的身份信息进行校验，之后根据各个共识认证中心对应的认证结果来确定证书申请节点的身份认证结果，并在身份认证结果为通过时生成数字证书，该数字证书被作为交易资源写入各个共识认证中心对应的区块链中，由于身份认证结果是基于多个认证中心的认证结果的，相比于仅通过一个认证中心来进行校验，校验的准确度更高。另外，数字证书被写入区块链而并非存储在某个认证中心中，其它非法节点很难在区块链中对数字证书进行修改或撤销，可以保证数字证书的安全，提高网络安全性。

附图说明

图1为本申请一个实施例提供的应用环境的示意图；

图2为本申请一个实施例提供数字证书管理方法的流程图；

图 3 为本申请一个实施例提供的数字证书的示意图；

图 4 为本申请一个实施例提供将目标数字证书作为交易资源写入至共识认证中心对应的区块链的流程图；

图 5 为本申请一个实施例提供的数字证书管理方法的流程图；

图 6 为本申请一个实施例提供的数字证书管理方法的流程图；

图 7 为本申请一个实施例提供的交易链的示意图；

图 8 为本申请一个实施例提供的数字证书管理方法的流程图；

图 9 为本申请一个实施例中提供的管理数字证书的示意图；

图 10 为本申请一个实施例提供的数字证书管理装置的结构框图；

图 11 为本申请一个实施例提供的写入模块的结构框图；

图 12 为本申请一个实施例提供的数字证书管理装置的结构框图；

图 13 为本申请一个实施例提供的计算机设备的内部结构框图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

可以理解，本申请所使用的术语“第一”、“第二”等可在本文中用于描述各种元件，但除非特别说明，这些元件不受这些术语限制。这些术语仅用于将第一个元件与另一个元件区分。举例来说，在不脱离本申请的范围的情况下，可以将第一账户称为第二账户，且类似地，可将第二账户称为第一账户。

下面对本申请实施例涉及的相关名词进行介绍。

数字证书：用于在网络通讯中标识通讯方的身份信息，其可以由数字、字母、符号中的至少一种的组合。数字证书通常由权威 CA（Certificate Authority、证书授权）机构发行的。示例性地，CA 机构为 CFCA（China Financial Certification Authority，中国金融认证中心）中心。

认证中心：在网络中承担认证服务、签发数字证书以确认节点身份等工作的具有权威性和公正性的计算机节点。

区块链：用于存储某一交易资源的交易记录。交易记录包括 3 个要素：交

易资源、转出账户、转入账户。在本申请实施例中，上述交易资源也即是数字证书。另外，账户（转出账户或转入账户）也可以称为地址，地址可由公钥经过单向的加密哈希算法得到。哈希算法是一种单向函数，接收任意长度的输入产生指纹摘要。由公钥生成地址时使用的算法是 Secure Hash Algorithm (SHA) 算法或者 the RACE Integrity Primitives Evaluation Message Digest (RIPEMD) 算法，例如可以是 SHA256 或者 RIPEMD160 算法。

区块链技术：简称 BT (Blockchain technology)，也被称之为分布式账本技术，是一种互联网数据库技术，其特点是去中心化、公开透明，让每个人均可参与数据库记录。区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种分布式基础架构与计算方式。

图 1 为本申请一个实施例提供的数字证书管理方法的应用环境图，如图 1 所示，该应用环境包括证书申请节点和至少两个认证中心。

证书申请节点用于申请数字证书。当需要申请数字证书时，由证书申请节点向认证中心发送数字证书申请请求。证书申请节点可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据库、云存储和 CDN 等基础云计算服务的云服务器。

上述至少两个认证中心用于对证书申请节点进行共识认证。上述至少两个认证中心中的任一认证中心具有与证书申请节点进行数据交互的功能，例如接收证书申请节点发送的数字证书申请请求，向证书申请节点返回数字证书等。认证中心的数量可以根据实际需求设定。在本申请实施例中，仅以上述至少两个认证中心包括认证中心 1、认证中心 2、认证中心 3 和认证中心 4 为例进行说明。其中，认证中心 1 用于实现上述与证书申请节点进行数据交互的功能。各个认证中心可以是独立的物理服务器或终端，也可以是多个物理服务器构成的服务器集群，可以是提供云服务器、云数据库、云存储和 CDN 等基础云计算服务的云服务器。

各个认证中心之间可以利用网络进行连接，以进行共识认证。证书申请节点与认证中心可以通过网络进行连接。另外，上述各个认证中心是属于同一区

区块链的节点。可以理解，区块链中还可以包括其他节点，证书申请节点也可以是区块链中的节点。

图 2 为本申请一个实施例提供的数字证书管理方法的流程图，本实施例主要以该方法应用于计算机设备（例如图 1 所示实施环境中的认证中心 1）来举例说明。该方法具体可以包括以下步骤：

S202，接收证书申请节点发送的数字证书生成请求，数字证书生成请求携带身份认证信息。

证书申请节点是指需要申请数字证书的计算机节点。证书申请节点可以是存在通讯需求的实体（个人或组织）所拥有的计算机节点。例如，当企业需要建立一个网站时，需要申请该网站对应的数字证书，此时可以由需要申请数字证书的企业服务器向认证中心发送数字证书生成请求。

数字证书生成请求用于请求生成数字证书。数字证书生成请求中携带证书申请节点的身份信息。身份认证信息用于对证书申请节点的身份进行认证。可选地，身份认证信息是管理证书申请节点的企业对应的营业执照信息或者管理证书申请节点的个人用户对应的身份证信息等。

可选地，数字证书生成请求中还可以携带证书申请节点的公钥。公钥（Public Key）与私钥（Private Key）是通过算法得到的一个密钥对，公钥是密钥对中公开的密钥，私钥则是非公开的密钥。公钥通常用于加密会话密钥或者验证数字签名。当需要申请数字证书时，证书申请节点产生密钥对，存储密钥对的私钥并将公钥发送到认证中心，以使认证中心将公钥写入到数字证书中。这样，证书申请节点可以利用私钥对发送的信息进行签名，接收到签名的信息的节点可以通过数字证书的公钥对证书申请节点发送的信息进行校验，确认接收的信息为证书申请节点发送的信息。

S204，将身份认证信息发送到各个共识认证中心进行认证，获取各个共识认证中心根据身份认证信息进行认证得到的认证结果。

认证中心是在网络中承担认证服务、签发数字证书以确认节点身份等工作的具有权威性和公正性的计算机节点。共识认证中心是用于进行共识认证的认证中心。在本申请实施例中，认证中心 1 也为共识认证中心。共识认证中心的数量可以根据需要设置。进行共识认证时采用的共识算法可以是 PBFT（Practical

Byzantine Fault Tolerance, 实用拜占庭容错算法)。共识是指多方参与的节点在预设规则下, 通过多个节点交互对某些数据、行为或流程达成一致的过程。

在一种可能的实现方式中, 身份认证信息的发送可以通过 P2P (peer-to-peer, 点对点) 技术实现的, 认证中心 1 通过 P2P 方式向各个共识认证中心发送身份认证信息。在另一种可能的实现方式中, 认证中心 1 可以在区块链中广播该身份认证信息, 接收到身份认证信息的共识认证中心也可以继续广播该身份认证信息, 使各个共识认证中心可以接收到身份认证信息。

当各个共识认证中心接收到身份认证信息后, 可以将接收到的身份认证信息与预先存储的该证书申请节点的身份认证信息进行对比或者将身份认证信息发送到存储有身份认证信息的信任源中进行对比, 以确认接收到的身份信息与存储的身份信息是否一致, 当一致时, 确认接收到的身份信息是真实的, 则共识认证中心对应的认证结果为通过, 否则, 认证结果为不通过。信任源可以是颁发身份认证信息的节点例如公安机关颁发个人身份证对应的节点。

S206, 根据各个共识认证中心的认证结果确定证书申请节点对应的身份认证结果。

身份认证结果可以为通过认证或者未通过认证。在本申请实施例中, 身份认证结果是结合各个共识认证中心的认证结果计算得到的。可选地, 计算机设备根据第一数量和第二数量中的至少一个来确定身份认证结果。其中, 第一数量是指认证结果为通过的共识认证中心的数量。第二数量为是指认证结果为不通过的共识认证中心的数量。

具体地, 计算机设备在第一数量以及第二数量满足以下条件中的至少一个时确定身份认证结果为通过认证: 第一数量大于第二数量、第一数量达到第一预设阈值、第一数量与共识认证中心总数量的比值达到第二预设阈值、第一数量与区块链中的节点总数量的比值达到第三预设阈值。第一预设阈值、第二预设阈值以及第三预设阈值对应的具体数值可以根据需要设置。

示例性地, 假设身份认证结果为通过认证的条件为第一数量占共识认证中心总数量的比例大于等于 $3/4$, 假设认证中心 1~4 对应的认证结果分别为通过、通过、通过以及不通过, 则第一数量为 3, 第二数量为 1, 则第一数量占共识认证中心总数量的比例等于 $3/4$, 满足上述条件, 此时身份认证结果为通过认证。

S208, 当身份认证结果为通过认证时, 根据数字证书生成请求生成证书申

请节点对应的目标数字证书。

数字证书用于在网络通讯中标识通讯方的身份信息。可选地，数字证书是经过认证中心数字签名的文件。数字证书内可以包含证书申请节点的身份信息。可选地，数字证书还可以包括以下至少一项信息：证书颁发者的信息、证书申请节点的公钥、数字证书的有效期信息、进行数字签名的签名哈希算法以及数字签名。其中，数字签名是将数字证书按双方约定的签名哈希算法计算得到的报文摘要。当数字证书中的任意一位被改动时，其对应的数字签名也会相应变动，从而可以识别数字证书是否被更改。

结合参考图 3，其示出了本申请一个实施例提供的数字证书的示意图，该数字证书包括证书颁发者的信息、证书申请节点的公钥、证书申请节点即证书拥有者的信息、有效期信息、进行数字签名的签名哈希算法以及数字签名。

S210，将目标数字证书作为交易资源写入至各个共识认证中心对应的区块链。

在本申请实施例中，计算机设备将目标数字证书作为交易资源写入到各个共识认证中心对应的区块链中，该区块链中存储的是该数字证书的交易记录。

可选地，结合参考图 4，S210 可以包括如下几个子步骤：

S402，生成第一证书交易记录，其中，第一证书交易记录的交易资源为目标数字证书，第一证书交易记录中的转出账户为预设初始账户，第一证书交易记录中的接收账户为数字证书生成请求接收节点对应的证书发行账户。

交易记录是对交易资源对应的所达成交易的记载。证书交易记录中可以包含此次交易中转出交易资源的转出账户以及接收交易资源的接收账户。交易记录中包括数字证书本身或者数字证书对应的标识。

预设初始账户是预先设置的，用于表示在进行当前交易之前，交易资源是初始的、未进行过交易的资源。预设初始账户具体的值可以根据需要进行设置，例如可以是一个全为 0 的字符串，字符串中字符的个数可以根据需要设置。在本申请实施例中，由于目标数字证书是首次存入的目标数字证书，因此，转出账户可以是一个预设初始账户，表示该交易资源是初始的交易资源。

数字证书生成请求接收节点也即是本申请实施例各个步骤的执行主体，也即认证中心 1。数字证书生成请求接收节点对应的证书发行账户可以是认证中心 1 所拥有的任意一个账户，该账户的类型为证书发行账户类型。当接收账户的类

型为证书发行账户类型时，表示数字证书处于发行状态中，为有效的数字证书。

在本申请实施例中，生成的第一证书交易记录相当于一个 UTXO（Unspent Transaction Output，未花费交易输出）交易。在生成第一证书交易记录时，生成对应的第一交易标识，以用于标识第一证书交易。在 UTXO 交易中，包括交易输入（input）以及交易输出（output）。每笔交易都有交易输入，也就是交易资源的来源，也都有交易输出，也就是交易资源的去向，在本申请实施例中，将交易输入对应的账户称为转出账户，将交易输出对应的账户称为接收账户。

可选地，计算机设备在生成第一证书交易记录时，还可以生成第一证书交易记录对应的第一交易标识，计算机设备可以向证书申请节点反馈该第一交易标识，以便证书申请节点对目标数字证书进行校验。

S404，将第一证书交易记录写入至共识认证中心对应的区块链。

计算机设备生成第一证书交易记录后，将第一证书交易记录写入至共识认证中心对应的区块链的区块中，以使区块中存储该第一证书交易记录。

可选地，计算机设备在将第一证书交易记录写入到区块时，广播第一证书交易记录，以使得区块链中的节点也在区块中存储第一证书交易记录。另外，在广播第一证书交易记录前，可以利用私钥对第一证书交易记录进行签名，将签名后的第一证书交易记录进行广播。

综上所述，本申请实施例提供的技术方案，通过多个认证中心来对证书申请节点的身份信息进行校验，之后根据各个共识认证中心对应的认证结果来确定证书申请节点的身份认证结果，并在身份认证结果为通过时生成数字证书，该数字证书被作为交易资源写入各个共识认证中心对应的区块链中，由于身份认证结果是基于多个认证中心的认证结果的，相比于仅通过一个认证中心来进行校验，校验的准确度更高。另外，数字证书被写入区块链而并非存储在某个认证中心中，其它非法节点很难在区块链中对数字证书进行修改或撤销，可以保证数字证书的安全，提高网络安全性。

目标数字证书被写入区块链之后，其它用户或者组织还可以对目标数字证书进行操作。在基于图 2 所示实施例提供的一个可选实施例中，如图 5 所示，该数字证书管理方法还包括以下步骤：

S502，接收用于对目标数字证书进行的操作请求。

在本申请实施例中，对目标数字证书进行的操作可以为撤销操作或者更新操作。操作请求用于请求对目标数字证书进行操作，对应地，操作请求可以包括数字证书更新请求或者数字证书撤销请求。

可选地，操作请求由证书申请节点或者其他节点触发的。例如，如果目标数字证书需要进行更新，则证书申请节点可以发送数字证书更新请求。如果目标数字证书需要进行撤销，则证书申请节点可以发送数字证书撤销请求。再例如，当认证中心发现证书申请节点在获取目标数字证书时存在欺骗行为时，则认证中心的工作人员可以在认证中心发起撤销操作，认证中心根据撤销操作触发数字证书撤销请求，请求撤销该数字证书。

S504，根据操作请求的操作类型确定接收数字证书的接收账户类型。

接收账户类型是指根据对数字证书所进行的操作而生成的交易记录中的接收账户的类型。接收账户的类型可以是证书回收账户类型，也可以是账户发行账户类型。其中，证书回收账户类型表示数字证书处于撤销状态，即已被撤销，为无效的数字证书。证书发行账户类型表示数字证书已发行，即处于发行状态中，为有效的数字证书。

在本申请实施例中，不同的操作类型对应的接收账户的类型不相同。在一个实施例中，当操作请求的操作类型为更新操作类型时，确定目标类型为证书发行账户类型。在一个实施例中，当操作请求的操作类型为撤销操作类型时，确定目标类型为证书回收账户类型。

S506，生成第二证书交易记录，将第二交易记录写入至区块链，其中，第二证书交易记录的交易资源为目标数字证书，第二证书交易记录中的接收账户为接收账户类型对应的第二账户。

计算机设备预先设置了账户类型与账户之间的对应关系，例如，对于证书发行账户类型，对应的账户为 00001，对于证书回收账户类型，对应的账户为 00002。得到接收账户类型后，计算机设备通过上述对应关系确定类型为接收账户类型的账户，作为第二证书交易记录中的接收账户。

另外，第二证书交易记录中的转出账户可以是第二证书交易记录的上一个交易记录中的接收账户，例如，当第二证书交易记录的上一个交易记录为第一证书交易记录时，则第二证书交易记录中的转出账户是第一账户。或者，也可以利用第二证书交易记录的上一个交易记录对应的交易标识来标识交易的输

入，即转出账户可以用上一个交易记录对应的交易标识表示。

在区块链中，第一次将数字证书写入区块链的操作称为插入操作，将插入操作作为一种交易，形成交易记录写入区块链中，由于存储的交易记录一般情况下是不可篡改的，因此后续要对数字证书进行更新或者撤销时，也可以将对数字证书的操作作为交易，根据操作的类型形成对应的交易记录，存储到区块链中。这样，如果要查询数字证书的状态，则可以根据最新交易记录对应的账户类型确定数字证书是否已被更新或者撤销。

可选地，计算机设备在生成第一证书交易记录时，还可以生成第一证书交易记录对应的第一交易标识，计算机设备可以向证书申请节点反馈该第一交易标识，以便证书申请节点对目标数字证书进行校验。

综上所述，本申请实施例提供的技术方案，还通过在某一节点对数字证书进行操作时，根据该操作生成交易记录，并将交易记录记录在区块链中。其中，该交易记录中的接收账户的类型与操作类型一一对应，后续可以根据接收账户的类型来对数字证书进行校验。

在生成数字证书后，个人用户可以对该数字证书进行校验。在基于图 2 所示实施例提供的一个可选实施例中，在一个实施例中，该数字证书管理方法还可以包括以下步骤：

S602，接收用于对目标数字证书进行校验的校验请求。

具体地，校验请求用于请求对目标数字证书进行校验，校验请求可以是与证书申请节点进行交互的交互节点发送的。例如，当交互节点需要登录证书申请节点对应的网站时，可以从证书申请节点获取目标数字证书，并向认证中心发送校验请求。

在一个实施例中，校验请求携带第一证书交易记录对应的第一交易标识。当生成第一证书交易记录时，认证中心生成第一证书交易记录对应的第一交易标识，将第一交易标识发送至证书申请节点，后续若某一节点需要对目标数字证书进行校验时，可以从证书申请节点中获取该第一交易标识。

在另一个实施例中，校验请求携带第二证书交易记录对应的第二交易标识。当生成第二证书交易记录时，认证中心生成第二证书交易记录对应的第二交易标识，将第二交易标识发送至证书申请节点，后续若某一节点需要对目标数字

证书进行校验时，可以从证书申请节点中获取该第二交易标识。

S604，从区块链中获取目标数字证书对应的最新交易记录。

最新交易记录是目标数字证书对应的交易记录中，交易记录时间最晚的交易记录。当校验请求中携带第一校验标识时，计算机设备可以根据第一交易标识获取目标数字证书对应的交易链，之后将交易链末端的交易记录作为最新交易记录。

在区块链中，目标数字证书对应的交易记录前后连接，形成交易链。交易链中的交易记录按照交易时间的先后顺序依次排列。也即，交易记录对应的交易时间越早，则该交易记录在交易链中的位置越靠前；交易记录对应的交易时间越晚，则该交易记录在交易链中的位置越靠后。交易链末端的交易记录也即是交易时间最晚的交易记录。

在其它可能的实现方式中，校验请求中携带的还可以是第二交易标识，可以根据第二交易标识获取目标数字证书对应的交易链，之后将交易链末端的交易记录作为最新交易记录。

结合参考图 7，其示出了本申请一个实施例提供的交易链的示意图。图 7 中，交易标识为 1001#的交易记录为将数字证书写入区块链中的操作对应的记录，1001#为 2001#的父交易，2001#为 3001#的父交易。交易记录中可以包括数字证书本身或者数字证书对应的标识。

S606，根据最新交易记录中的接收账户类型确定目标数字证书对应的校验结果。

在本申请实施例中，计算机设备得到最新交易记录后，根据最新交易记录中的接收账户类型确定目标数字证书对应的校验结果是校验通过还是校验失败。可选地，计算机设备可以通过最新交易记录中的接收账户类型确定目标数字证书的操作状态，之后根据操作状态判断目标数字证书对应的校验结果是校验通过还是校验失败。

区块链中数字证书的操作状态可以为插入状态、更新状态以及撤销状态中的一种。插入状态对应的数字证书是作为新生成的初始数字证书插入到区块链中。更新状态对应的数字证书是初始数字证书进行更新后得到的数字证书，即证书已被更新。撤销状态对应的数字证书是已经被撤销的数字证书。

当最新交易记录对应的接收账户类型为证书回收账户类型时，确定区块链

中数字证书的操作状态为撤销状态，也即目标数字证书已被撤销，此时目标数字证书对应的校验结果为校验失败。当最新交易记录对应的接收账户类型为证书发行账户类型时，确定区块链中数字证书的操作状态为插入状态或更新状态，此时数字证书为有效的，确定目标数字证书对应的校验结果为校验成功。

可选地，其它节点还可以对数字证书生成请求接收节点的身份信息进行验证。当验证出数字证书生成请求接收节点为不可靠时，其办法的数字证书必然不会有效；当验证出数字证书生成请求接收节点为可靠时，则还需要进一步验证数字证书是否有效。下面对验证数字证书生成请求接收节点的身份信息的验证过程进行讲解。

在基于图 6 所示实施例提供的一个可选实施例中，如图 8 所示，在一个实施例中，该数字证书管理方法还可以包括以下步骤：

S802，根据校验请求从区块链中获取目标数字证书对应的根证书。

根证书是认证中心给自己颁发的证书，是信任链的起始点。根证书被存储在区块链的创世区块中，创世区块是区块链的第一个区块，以降低根证书被篡改的可能性。

根证书用于对认证中心颁发的数字证书进行校验，可以利用根证书中的公钥对数字证书中的数字签名进行验证，以确认数字证书的合法及有效性，即验证目标数字证书是否确实为 CA 机构签发。根证书也可以是存储在区块链中。

S804，根据根证书对目标数字证书进行校验，得到根校验结果。

根校验结果可以为校验成功或者校验失败。可选地，计算机设备可以获取根证书中的公钥，对目标数字证书的数字签名进行验证，如果确认数字签名验证通过，则校验成功，如果确认数字签名验证不通过，则校验失败。

S806，判断根校验结果是否为校验失败。

如果根校验结果为校验失败，则进入 S808。如果根校验结果为校验成功，则进入 S604。

S808，当根校验结果为校验失败时，确认目标数字证书对应的校验结果为校验失败。

具体地，如果根校验结果为校验失败，则确认目标数字证书对应的校验结果为校验失败，无需再继续对目标数字证书进行校验，如果根校验结果为校验成功，则进入从区块链中获取目标数字证书对应的最新交易记录的步骤，继续

对目标数字证书进行校验。

在一个具体的例子中，结合参考图 9，其示出了本申请一个实施例提供的数字证书管理方法的流程图。该方法可以包括如下步骤：

1、证书申请节点向认证中心 1 发送数字证书生成请求，数字证书生成请求中携带身份认证信息。

2、认证中心 1 向认证中心 2、认证中心 3 以及认证中心 4 发送身份认证信息到，以进行共识认证。

4、当根据共识认证的结果得到身份认证结果为通过时，认证中心 1 生成目标数字证书以及对应的第一交易记录，将第一交易记录存入区块链中的最新区块中，将目标数字证书以及第一交易标识返回给证书申请节点。

5、交互节点在与证书申请节点进行交互时，发送数字证书获取请求到证书申请节点中，

6、证书申请节点向交互节点返回目标数字证书以及第一交易标识。

7、交互节点向认证中心 4 发送校验请求，校验请求中携带第一交易标识以及目标数字证书。

8、认证中心 4 从创世区块中获取根证书，根据根证书对目标数字证书校验，得到根校验结果。

9、当根校验结果为校验通过时，认证中心 4 根据第一交易标识获取目标数字证书对应的交易链中的最新交易记录的接收账户类型，根据最新交易记录的接收账户类型确定校验结果。例如如果为回收账户类型，则表示目标数字证书已被撤销，校验结果为失败。

可以理解，接收校验请求并进行校验的也可以是区块链的其他节点，只要交互节点认为是可信任的即可。或者交互节点也可以是区块链中的节点，这样，交互节点也从本地存储的区块链数据中获取根证书以及交易记录，进行校验。

下述为本申请装置实施例，可以用于执行本申请方法实施例。对于本申请装置实施例中未披露的细节，请参照本申请方法实施例。

请参考图 10，其示出了本申请一个实施例提供的数字证书管理装置的框图。该装置具有实现上述方法示例中的功能，所述功能可以由硬件实现，也可以由

硬件执行相应的软件实现。该装置可以包括：生成请求接收模块 1002、共识认证模块 1004、身份认证结果得到模块 1006、证书生成模块 1008 以及写入模块 1010。

生成请求接收模块 1002，用于接收证书申请节点发送的数字证书生成请求，数字证书生成请求携带身份认证信息。

共识认证模块 1004，用于将身份认证信息发送到各个共识认证中心进行认证，获取各个共识认证中心根据身份认证信息进行认证得到的认证结果。

身份认证结果得到模块 1006，用于根据各个共识认证中心的认证结果确定证书申请节点对应的身份认证结果。

证书生成模块 1008，用于当身份认证结果为通过认证时，根据数字证书生成请求生成证书申请节点对应的目标数字证书。

写入模块 1010，用于当身份认证结果为通过认证时，将目标数字证书作为交易资源写入至共识认证中心对应的区块链。

综上所述，本申请实施例提供的技术方案，通过多个认证中心来对证书申请节点的身份信息进行校验，之后根据各个共识认证中心对应的认证结果来确定证书申请节点的身份认证结果，并在身份认证结果为通过时生成数字证书，该数字证书被作为交易资源写入各个共识认证中心对应的区块链中，由于身份认证结果是基于多个认证中心的认证结果的，相比于仅通过一个认证中心来进行校验，校验的准确度更高。另外，数字证书被写入区块链而并非存储在某个认证中心中，其它非法节点很难在区块链中对数字证书进行修改或撤销，可以保证数字证书的安全，提高网络安全性。

在基于图 10 所示实施例提供的一个可选实施例中，如图 11 所示，写入模块 1010 包括：

第一记录生成单元 1010A，用于生成第一证书交易记录，其中，第一证书交易记录的交易资源为目标数字证书，第一证书交易记录中的转出账户为预设初始账户，第一证书交易记录中的接收账户为数字证书生成请求接收节点对应的证书发行账户。

第一写入单元 1010B，用于将第一证书交易记录写入至共识认证中心对应的区块链。

在基于图 10 所示实施例提供的一个可选实施例中，如图 12 所示，数字证

书管理装置还包括：

操作请求接收模块 1202，用于接收用于对目标数字证书进行操作的操作请求。

账户类型确定模块 1204，用于根据操作请求的操作类型确定接收目标数字证书的接收账户类型。

第二交易记录生成模块 1206，用于生成第二证书交易记录，将第二证书交易记录写入至区块链，其中，第二证书交易记录的交易资源为目标数字证书，第二证书交易记录中的接收账户为接收账户类型对应的第二账户。

可选地，账户类型确定模块 1204 用于：当操作请求的操作类型为更新操作类型时，确定接收账户类型为证书发行账户类型。

可选地，账户类型确定模块 1204 用于：当操作请求的操作类型为撤销操作类型时，确定接收账户类型为证书回收账户类型。

在基于图 10 所示实施例提供的一个可选实施例中，该数字证书管理装置还包括：

校验请求接收模块，用于接收用于对目标数字证书进行校验的校验请求。

交易记录获取模块，用于从区块链中获取目标数字证书对应的最新交易记录。

校验结果确定模块，用于根据最新交易记录对应的接收账户类型确定目标数字证书对应的校验结果。

可选地，校验结果确定模块用于：当最新交易记录对应的接收账户类型为证书回收账户类型时，确定目标数字证书已被撤销，目标数字证书对应的校验结果为校验失败。

可选地，校验结果确定模块用于：当最新交易记录对应的接收账户类型为证书发行账户类型时，确定目标数字证书对应的校验结果为校验成功。

可选地，所述校验请求携带所述第一证书交易记录对应的第一交易标识，所述第一交易标识是由数字证书生成请求接收节点发送至所述证书申请节点，再由所述证书申请节点发送至校验请求发送节点的。

可选地，交易记录获取模块，用于：根据第一交易标识获取目标数字证书对应的交易链，将交易链末端的交易记录作为最新交易记录，其中，交易链按照交易时间依次排列。

可选地，所述装置还包括：

证书获取模块，用于根据所述校验请求从所述区块链中获取所述目标数字证书对应的根证书，所述根证书用于校验数字证书生成请求接收节点的身份信息。

校验模块，用于根据所述根证书对所述目标数字证书进行校验，得到根验证结果。

所述交易记录获取模块，还用于当所述根校验结果为校验成功时，执行所述从所述区块链中获取所述目标数字证书对应的最新交易记录的步骤。

请参考图 13，其示出了本申请一个实施例提供的计算机设备的内部结构图。该计算机设备具体可以是图 1 中的认证中心。如图 13 所示，该计算机设备包括该计算机设备包括通过系统总线连接的处理器、存储器、网络接口以及输入装置。其中，存储器包括非易失性存储介质和内存储器。该计算机设备的非易失性存储介质存储有操作系统，还可存储有计算机程序，该计算机程序被处理器执行时，可使得处理器实现数字证书管理方法。该内存储器中也可储存有计算机程序，该计算机程序被处理器执行时，可使得处理器执行数字证书管理方法。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 13 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。

在示例性实施例中，存储器中存储有计算机程序，所述计算机程序由所述处理器加载并执行以实现上述方法实施例中的数字证书管理方法。

在示例性实施例中，还提供了一种计算机可读存储介质，所述存储介质中存储有计算机程序，所述计算机程序由计算机设备的处理器加载并执行以实现上述方法实施例中的数字证书管理方法。

其中，本申请所提供的各实施例中所使用的对存储器、存储、数据库或其它介质的任何引用，均可包括非易失性和/或易失性存储器。

非易失性存储器可包括只读存储器（ROM）、可编程 ROM（PROM）、电可

编程 ROM (EPROM)、电可擦除可编程 ROM (EEPROM) 或闪存。易失性存储器可包括随机存取存储器 (RAM) 或者外部高速缓冲存储器。作为说明而非局限, RAM 以多种形式可得, 诸如静态 RAM (SRAM)、动态 RAM (DRAM)、同步 DRAM (SDRAM)、双数据率 SDRAM (DDRSDRAM)、增强型 SDRAM (ESDRAM)、同步链路 (Synchlink) DRAM (SLDRAM)、存储器总线 (Rambus) 直接 RAM (RDRAM)、直接存储器总线动态 RAM (DRDRAM)、以及存储器总线动态 RAM (RDRAM) 等。

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本申请专利范围的限制。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 书

1、一种数字证书管理方法，所述方法由计算机设备执行，所述方法包括：
接收证书申请节点发送的数字证书生成请求，所述数字证书生成请求携带身份认证信息；

将所述身份认证信息发送到各个共识认证中心进行认证，获取各个所述共识认证中心根据所述身份认证信息进行认证得到的认证结果；

根据各个所述共识认证中心的认证结果确定所述证书申请节点对应的身份认证结果；

当所述身份认证结果为通过认证时，根据所述数字证书生成请求生成所述证书申请节点对应的目标数字证书；

将所述目标数字证书作为交易资源写入至所述共识认证中心对应的区块链。

2、根据权利要求1所述的方法，其中，所述将所述目标数字证书作为交易资源写入至所述共识认证中心对应的区块链包括：

生成第一证书交易记录，其中，所述第一证书交易记录的交易资源为所述目标数字证书，所述第一证书交易记录中的转出账户为预设初始账户，所述第一证书交易记录中的接收账户为数字证书生成请求接收节点对应的证书发行账户；

将所述第一证书交易记录写入至所述共识认证中心对应的区块链。

3、根据权利要求1所述的方法，其中，所述将所述目标数字证书作为交易资源写入至所述共识认证中心对应的区块链之后，还包括：

接收用于对所述目标数字证书进行操作的操作请求；

根据所述操作请求的操作类型，确定接收所述目标数字证书的接收账户类型；

生成第二证书交易记录，将所述第二证书交易记录写入至所述区块链，其中，所述第二证书交易记录的交易资源为所述目标数字证书，所述第二证书交易记录中的接收账户为所述接收账户类型对应的第二账户。

4、根据权利要求3所述的方法，其中，所述根据所述操作请求的操作类型确定接收所述目标数字证书的接收账户类型，包括：

当所述操作请求的操作类型为更新操作类型时，确定所述接收账户类型为

证书发行账户类型。

5、根据权利要求3所述的方法，其中，所述根据所述操作请求的操作类型确定接收所述目标数字证书的接收账户类型包括：

当所述操作请求的操作类型为撤销操作类型时，确定所述接收账户类型为证书回收账户类型。

6、根据权利要求1至5任一项所述的方法，其中，所述将所述目标数字证书作为交易资源写入至所述各个共识认证中心对应的区块链之后，还包括：

接收用于对所述目标数字证书进行校验的校验请求；

从所述区块链中获取所述目标数字证书对应的最新交易记录；

根据所述最新交易记录中的接收账户类型，确定所述目标数字证书对应的校验结果。

7、根据权利要求6所述的方法，其中，所述根据所述最新交易记录中的接收账户类型确定所述目标数字证书对应的校验结果，包括：

当所述最新交易记录中的接收账户类型为证书回收账户类型时，确定所述目标数字证书已被撤销，所述目标数字证书对应的校验结果为校验失败。

8、根据权利要求6所述的方法，其中，所述根据所述最新交易记录中的接收账户类型确定所述目标数字证书对应的校验结果，包括：

当所述最新交易记录中的接收账户类型为证书发行账户类型时，确定所述目标数字证书对应的校验结果为校验成功。

9、根据权利要求6所述的方法，其中，所述校验请求携带所述第一证书交易记录对应的第一交易标识，所述第一交易标识是由数字证书生成请求接收节点发送至所述证书申请节点，再由所述证书申请节点发送至校验请求发送节点的。

10、根据权利要求9所述的方法，其中，所述从所述区块链中获取所述目标数字证书对应的最新交易记录，包括：

根据所述第一交易标识获取所述目标数字证书对应的交易链，将所述交易链末端的交易记录作为所述最新交易记录，其中，所述交易链按照交易时间依次排列。

11、根据权利要求6所述的方法，其中，所述从所述区块链中获取所述目标数字证书对应的最新交易记录之前，还包括：

根据所述校验请求从所述区块链中获取所述目标数字证书对应的根证书，所述根证书用于校验所述数字证书生成请求接收节点的身份信息；

根据所述根证书对所述目标数字证书进行校验，得到根验证结果；

当所述根校验结果为校验成功时，执行所述从所述区块链中获取所述目标数字证书对应的最新交易记录的步骤。

12、一种数字证书管理装置，所述装置包括：

生成请求接收模块，用于接收证书申请节点发送的数字证书生成请求，所述数字证书生成请求携带身份认证信息；

共识认证模块，用于将所述身份认证信息发送到各个所述共识认证中心进行认证，获取各个所述共识认证中心根据所述身份认证信息进行认证得到的认证结果；

身份认证结果得到模块，用于根据各个所述共识认证中心的认证结果确定所述证书申请节点对应的身份认证结果；

证书生成模块，用于当所述身份认证结果为通过认证时，根据所述数字证书生成请求生成所述证书申请节点对应的目标数字证书；

写入模块，用于当所述身份认证结果为通过认证时，将所述目标数字证书作为交易资源写入至所述共识认证中心对应的区块链。

13、根据权利要求12所述的装置，其中，所述写入模块包括：

第一记录生成单元，用于生成第一证书交易记录，其中，所述第一证书交易记录的交易资源为所述目标数字证书，所述第一证书交易记录中的转出账户为预设初始账户，所述第一证书交易记录中的接收账户为数字证书生成请求接收节点对应的证书发行账户；

第一写入单元，用于将所述第一证书交易记录写入至所述共识认证中心对应的区块链。

14、根据权利要求12所述的装置，其特征在于，所述装置还包括：

操作请求接收模块，用于接收用于对所述目标数字证书进行操作的操作请求；

账户类型确定模块，用于根据所述操作请求的操作类型确定接收所述目标数字证书的接收账户类型；

第二交易记录生成模块，用于生成第二证书交易记录，将所述第二交易记

录写入至所述区块链，其中，所述第二证书交易记录的交易资源为所述目标数字证书，所述第二证书交易记录中的接收账户为所述接收账户类型对应的第二账户。

15、一种计算机设备，其特征在于，包括存储器和处理器，所述存储器中存储有计算机程序，所述计算机程序被所述处理器执行时，使得所述处理器执行权利要求 1 至 11 中任一项权利要求所述数字证书管理方法的步骤。

16、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上存储有计算机程序，所述计算机程序被处理器执行时，使得所述处理器执行权利要求 1 至 11 中任一项权利要求所述数字证书管理方法的步骤。