

数字证书校验方法、装置、计算机设备和存储介质

本申请要求于2018年07月24日提交的申请号为201810821667.6、发明名称为“数字证书校验方法、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校验方法、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，数字证书校验均由生成数字证书的权威认证中心进行，如果该权威认证中心被劫持，则认证中心对数字证书进行校验得到的校验结果是不可靠的，导致网络安全性低。

发明内容

基于此，有必要针对上述的问题，提供一种数字证书校验方法、装置、计算机设备和存储介质，可通过根据目标数字证书在区块链中记载的交易记录得到对应的目标账户类型，根据对应的目标账户类型确定目标数字证书对应的校验结果，由于数字证书是作为交易资源存储在区块链中的，交易记录不易篡改，而且不同的账户类型对应不同的证书操作状态，因此根据区块链中交易记录的账户类型得到的校验结果可靠度高，网络安全性高。

一种数字证书校验方法，所述方法包括：接收对目标数字证书进行校验的校验请求；从区块链中获取所述目标数字证书对应的目标交易记录，所述目标数字证书是作为交易资源存储在所述区块链中的；获取所述目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态；根据所述目标账户类型确定所述目标数字证书对应的校验结果。

一种数字证书校验装置，所述装置包括：校验请求接收模块，用于接收对目标数字证书进行校验的校验请求；目标交易记录获取模块，用于从区块链中获取所述目标数字证书对应的目标交易记录，所述目标数字证书是作为交易资源存储在所述区块链中的；目标账户类型获取模块，用于获取所述目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态；校验结果确定模块，用于根据所述目标账户类型确定所述目标数字证书对应的校验结果。

在其中一个实施例中，所述装置还包括：操作请求接收模块，用于接收对所述目标数字证书进行的操作请求；接收账户类型确定模块，用于根据所述操作请求的操作类型确定所述目标数字证书对应的目标接收账户类型；证书交易记录生成模块，用于生成所述操作请求对应的证书交易记录，将所述证书交易记录写入至所述区块链，其中，所述证书交易记录的交易资源为所述目标数字证书，所述证书交易记录中的接收账户为所述目标接收账户类型对应的账户。

在其中一个实施例中，所述接收账户类型确定模块用于：当所述操作请求对应的操作类型为更新操作类型或者插入操作类型时，确定所述目标接收账户类型为证书发行账户类型。

在其中一个实施例中，所述接收账户类型确定模块用于：当所述操作请求对应的操作类型为撤销操作类型时，确定所述目标接收账户类型为证书回收账户类型。

在其中一个实施例中，所述目标交易记录为最新交易记录，所述目标账户类型获取模块用于：获取所述最新交易记录对应的接收所述目标数字证书的当前接收账户类型，作为所述目标账户类型；所述校验结果确定模块用于：当所述当前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。

在其中一个实施例中，所述目标账户类型获取模块用于：获取所述最新交易记录对应的接收所述目标数字证书的当前接收账户类型，作为所述目标账户类型；所述校验结果确定模块用于：当所述当前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对应的校验结果为校验失败。

在其中一个实施例中，所述校验请求中携带所述目标数字证书对应的交易标识，所述目标交易记录获取模块用于：根据所述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，所述交易链中的各条交易记录按照交易顺序依次排列。

在其中一个实施例中，所述装置还包括：根证书获取模块，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；根校验结果得到模块，用于根据所述根证书对所述目标数字证书进行校验，得到根校验结果；进入模块，用于当所述根校验结果为校验失败时，确认所述目标数字证书对应的校验结果为校验失败，否则，进入从区块链中获取所述目标数字证书对应的目标交易记录的步骤。

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校验方法的步骤。

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校验方法的步骤。

上述数字证书校验方法、装置、计算机设备和存储介质，通过接收对目标数字证书进行校验的校验请求，从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的，获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态，根据目标账户类型确定目标数字证书对应的校验结果。由于数字证书是作为交易资源存储在区块链中的，交易记录不易篡改，而且不同的账户类型对应不同的证书操作状态，因此根据区块链中交易记录的账户类型得到的校验结果可靠度高，网络安全性高。

附图说明

图1为一个实施例中提供的数字证书校验方法的应用环境图；

图2为一个实施例中数字证书校验方法的流程图；

图3为一个实施例中数字证书校验方法的流程图；

图4为一个实施例中数字证书校验方法的流程图；

图5为一个实施例中数字证书的示意图；

图6为一个实施例中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 7 为一个实施例中交易链的示意图；
图 8 为一个实施例中数字证书校验方法的流程图；
图 9 为一个实施例中提供的数字证书校验方法的应用环境图；
图 10 为一个实施例中数字证书校验装置的结构框图；
图 11 为一个实施例中数字证书校验装置的结构框图；
图 12 为一个实施例中数字证书校验装置的结构框图；
图 13 为一个实施例中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，可以将第一交易记录称为第二交易记录，且类似地，可将第二交易记录称为第一交易记录。

图 1 为一个实施例中提供的数字证书校验方法的应用环境图，如图 1 所示，该应用环境包括证书申请节点、交互节点以及认证中心。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，证书申请节点向交互节点返回目标数字证书以及交易标识。交互节点可以向认证中心发送校验请求，校验请求中携带交易标识以及目标数字证书。认证中心执行本申请实施例提供的数字证书校验方法，得到校验结果，并向交互节点返回校验结果。

交互节点与证书申请节点、交互节点与认证中心之间可以通过网络进行连接。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（Content Delivery Network，内容分发网络）等基础云计算服务的云服务器。证书申请节点以及交互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。

如图 2 所示，在一个实施例中，提出了一种数字证书校验方法，本实施例

主要以该方法应用于上述图 1 中的认证中心来举例说明。具体可以包括以下步骤：

步骤 S202，接收对目标数字证书进行校验的校验请求。

具体地，数字证书是网络通讯中标志通讯方身份信息的一串数字，用于识别通讯方的身份。数字证书提供了一种在 Internet（互联网）上验证通信实体身份的方式，因此数字证书一般是由权威 CA（Certificate Authority、证书授权）机构发行的。CA 机构例如可以为 CFCA（China Financial Certification Authority，中国金融认证中心）中心。校验请求用于请求对目标数字证书进行校验，以确认数字证书的有效性以及真实性。目标数字证书是需要被验证身份的节点的数字证书，例如图 1 的证书申请节点对应的数字证书。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。

步骤 S204，从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的。

具体地，交易资源是可以用于交易的资源。区块链是运行区块链技术的载体和组织方式。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。交易记录是对交易资源对应的所达成交易的记载。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。交易记录中可以包括数字证书本身或者数字证书对应的标识。在区块链中，交易资源是以交易记录的形式表现的。证书的交易记录相当于一个 UTXO（Unspent Transaction Output，未花费交易输出）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。目标交易记录可以是目标数字证书对应的最新交易记录。

在一个实施中，校验请求携带目标数字证书对应的交易标识。当生成证书

交易时，认证中心生成交易记录对应的交易标识，将交易标识发送至证书申请节点，以使证书申请节点将交易标识发送至校验请求发送节点，这里的校验请求发送节点即为与证书申请节点进行交互的交互节点。

步骤 S206，获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态。

具体地，区块链中存储的目标数字证书通过不同的账户类型体现证书的操作状态。目标账户类型可以是接收账户类型，即接收目标数字证书的账户的类型。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的。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的，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。各个认证中心的账户可以包括证书回收账户类型以及证书发行状态类型。对于撤销状态的数字证书，对应的最新交易记录的接收账户类型为证书回收账户类型，当交易记录中接收账户为证书回收账户类型时，表示数字证书处于撤销状态，即已被撤销。对于处于插入状态以及更新状态的数字证书，则对应的最新交易记录的接收账户类型为证书发行账户类型，当交易记录中接收账户为证书发行账户类型时，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。

步骤 S208，根据目标账户类型确定目标数字证书对应的校验结果。

具体地，校验结果可以为校验成功或者校验失败。得到目标交易记录后，根据目标交易记录的目标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，可以通过最新交易记录对应的目标账户类型确定目标数字证书的操作状态。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。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，由于此时数字证书可以是插入的数字证书或者更新的数字证书，因此确认数字证书为有效的，确定目标数字证书对应的校验结果为校验成功。或者，可以获取最新交易记录对应的转出账户类型，如果转出账户为预设的初始账户，则确认该数字证书是新插入的数字证书，校验结果为成功。

在一个实施例中，目标交易记录为最新交易记录，获取目标交易记录对应的目标账户类型包括：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型。根据目标账户类型确定目标数字证书对应的校

验结果包括：当当前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。当当前接收账户类型为证书回收账户类型时，确定目标数字证书对应的校验结果为校验失败。其中，当前账户类型是指最新交易记录中的接收账户的类型。

上述数字证书校验方法，通过接收对目标数字证书进行校验的校验请求，从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的，获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态，根据目标账户类型确定目标数字证书对应的校验结果。由于数字证书是作为交易资源存储在区块链中的，交易记录不易篡改，而且不同的账户类型对应不同的证书操作状态，因此根据区块链中交易记录的账户类型得到的校验结果可靠度高，网络安全性高。

在一个实施例中，如图3所示，数字证书校验可以包括以下步骤：

步骤 S302，接收对目标数字证书进行操作的操作请求。

具体地，操作可以为插入操作、撤销操作以及更新操作中的一个。插入操作是指首次将数字证书存储到区块链中对应的操作，更新操作则是对已存储的目标数字证书进行更新对应的操作。撤销操作是对目标数字证书进行撤销对应的操作。对目标数字证书进行操作的操作请求可以是证书申请节点、认证中心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。或者，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。或者，当认证中心节点生成了目标数字证书，需要将目标数字证书存储到区块链中时，也可以触发对目标数字证书进行操作的操作请求。

步骤 S304，根据操作请求的操作类型确定目标数字证书对应的目标接收账户类型。

其中，目标数字证书对应的目标接收账户类型，可以是指接收目标数字证书的账户对应的目标接收账户类型。

具体地，不同的操作类型对应的接收账户类型不同。各个认证中心的账户可以包括证书回收账户类型以及证书发行状态类型。对于撤销操作类型，则对应的接收账户类型为证书回收账户类型，当交易记录中接收账户为证书回收账

户类型时，表示数字证书处于撤销状态，即已被撤销。对于更新操作类型以及插入操作类型，则对应的账户类型为证书发行账户类型，当交易记录中接收账户为证书发行账户类型时，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。

在一个实施例中，当操作请求对应的操作类型为更新操作类型或者插入操作类型时，确定目标接收账户类型为证书发行账户类型。

在一个实施例中，当操作请求对应的操作类型为撤销操作类型时，确定目标接收账户类型为证书回收账户类型。其中，证书回收账户以及证书发行账户可以是生成数字证书的认证节点对应的账户。

步骤 S306，生成操作请求对应的证书交易记录，将证书交易记录写入至区块链，其中，证书交易记录的交易资源为目标数字证书，证书交易记录中的接收账户为目标接收账户类型对应的账户。

具体地，在交易中，接收账户是指拥有交易资源的账户。转出账户是指将交易资源转出到接收账户的账户。将目标数字证书作为可以交易的资源，区块链中存储的是该数字证书的交易记录。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。得到目标接收账户类型后，获取目标接收账户类型对应的账户，作为证书交易记录对应的接收账户。得到证书交易记录后，将证书交易记录写入至区块链的区块中，以使区块中存储该证书交易记录。可以理解，在将证书交易记录写入到区块时，广播证书交易记录，以使得区块链中的节点也在区块中存储证书交易记录。在广播证书交易记录前，可以利用私钥对证书交易记录进行签名，将签名后的证书交易记录进行广播。在生成证书交易记录时，可以生成对应的交易标识，以用于标识证书交易。

在一个实施例中，生成证书交易记录对应的交易标识后，将交易标识发送至证书申请节点。这样，与证书申请节点通信的交互节点可以获取该证书申请节点对应的交易标识以及目标数字证书，并根据交易标识在区块链中获取目标数字证书在区块链存储的交易记录，以进行证书校验。

可以理解，步骤 S302~S306 可以是在步骤 S202~S208 之前执行的，也可以是在步骤 S202~S208 之后执行的。

在一个实施例中，对目标数字证书的操作为插入操作，如图 4 所示，数字证书校验方法具体还可以包括以下步骤：

步骤 S402, 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。

具体地, 身份认证信息用于对证书申请节点的身份进行认证, 身份认证信息例如可以是证书申请节点的企业对应的营业执照信息或者证书申请节点的个人用户对应的身份证信息等。证书申请节点是指需要申请数字证书的节点。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。

在一个实施例中, 数字证书生成请求中还可以携带公钥。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签名认证, 确认接收的信息为证书申请节点发送的信息。

步骤 S404, 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。

具体地, 共识认证中心的数量可以根据需要设置。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 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。共识认证中心是用于进行共识认证的认证中心, 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。进行共识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)。认证中心可以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。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。

步骤 S406, 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。

具体地, 身份认证结果可以为通过身份认证或者未通过身份认证。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。在确定身份认证结果时, 可以获取认证结果为认证通过的共识认证中心对应的第一数量以及认证结果为认证未通过的共识认证中心对应的第二数量中的至少一个, 根据第一数量以及第二数量中的至少一个确定身份认证结果。例如, 可以是当满足以下条件中的至少一个时身份认证结果为通过: 第一数量大于第二数量、第一数量达到第一预设阈值、第一数量与参与共识校验的认证中心的数量的比值达到第二预设阈值以及第一数量与区块链的节点的数量的比值达到第三预设阈值。可以理解, 认证中心 1 也是共识认证中心。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。例如, 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, 假设身份认证结果为通过的条件为大于第一数量占共识认证中心总数量的比例大于等于 $3/4$, 则身份认证结果为通过。

步骤 S408, 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。

具体地, 数字证书是一个经认证中心数字签名的文件, 用于证明网络节点的身份。数字证书内可以包含证书申请点的身份信息和公钥信息, 同时还附有认证中心的签名信息。当然也还可以包括数字证书的有效日期等信息。目标数字证书可以是确认身份认证结果为通过认证后生成的, 也可以是在未确认身份认证结果为通过认证时生成目标数字证书。在未确认身份认证结果为通过认证时生成目标数字证书可以在身份认证结果为通过时, 快速地将目标数字证书写入至区块链中。而确认身份认证结果为通过认证后生成目标数字证书则可以避免身份认证结果为未通过认证时也需要生成目标数字证书的情况发生。

如图 5 所示, 图 5 为数字证书的示意图, 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, 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。在数学上可以保证只要改动数字证书中任何一位, 重新计算出的报文摘要值就会与原先的值不相符。这样就保证了可以识别出数字证书是否被更改。

步骤 S410, 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, 其中, 目标数字证书对应的接收账户为数字证书生成请求接收节点对应的第一账户。

具体地, 目标数字证书所写入的区块链是共识认证中心所对应的区块链。数字证书生成请求接收节点是指接收数字证书生成请求的节点。在交易中, 接收账户是指拥有交易资源的账户。转出账户是指将交易资源转出到接收账户的账户。在将目标数字证书写入到区块链中时, 将目标数字证书作为可以交易的资源, 区块链中存储的是该数字证书的交易记录。在将目标数字证书存入到区块链中时, 目标数字证书的交易记录中的接收账户是接收数字证书生成请求的节点所对应的账户。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的账户。例如可以为全为 0 的字符串, 表示该交易资源是初始的交易资源。在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时, 可以创建新的区块, 将目标数字证书写入创建的新区块中。

区块链中的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 SHA (Secure Hash Algorithm, 安全哈希算法) 或者 RIPEMD (the RACE Integrity Primitives Evaluation Message Digest, 原始完整性校验消息摘要) 算法, 例如可以是 SHA256 或者 RIPEMD160 算法。

本申请实施例中, 由于可通过对身份认证信息进行共识认证, 得到的身份认证结果为通过认证时将目标数字证书写入至区块链中, 如果认证中心被劫持, 很难在区块链中写入数字证书, 而且, 数字证书是作为交易资源写入至区块链中的, 接收账户为数字证书生成请求接收节点对应的账户, 其他节点无法随意对数字证书进行修改或者撤销, 保证了数字证书的安全, 提高了数字证书的可信度, 也提高了网络安全性。

在一个实施例中, 如图 6 所示, 步骤 S410 即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步骤具体可以包括以下步骤:

步骤 S602, 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。

具体地, 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，相当于比特币交易的挖矿所得对应的 Coinbase 交易，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。证书发行账户是用于发行证书的账户。当接收账户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。证书交易记录也可以包括证书交易的时间等信息。

在一个实施例中，证书交易记录中的转出账户可以是该证书交易记录的上一个交易记录中的接收账户，或者，也可以利用该证书交易记录的上一个证书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。

步骤 S604，将第一证书交易记录写入至共识认证中心对应的区块链。

具体地，得到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。可以理解，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。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。

在一个实施例中，生成第一证书交易记录对应的第一交易标识后，将第一交易标识发送至证书申请节点。这样，与证书申请节点通信的节点可以获取该证书申请节点对应的第一交易标识以及目标数字证书，并根据第一交易标识在区块链中获取目标数字证书在区块链存储的交易记录，以进行证书校验。

在一个实施例中，当将目标数字证书插入到区块链后，可以对目标数字证书进行撤销或者更新，当认证中心对目标数字证书的操作为更新操作或者撤销操作时，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。当对目标数字证书的操作为更新操作时，第二证书交易记录中的接收账户为更新操作对应的目标接收账户类型对应的第二账户，当对目标数字证书的操作为撤销操作时，第二证书交易记录中的接收账户为撤销操作对应的目标接收账户类型对应的第二账户。

可以理解，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，其中第一账户是指第一交易记录中的接收账户。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，将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，通过根据操作请求的操作类型确定接收目标数字证书的目标接收账户类型，并生成第二交易记录，第二证书交易记录中的接收账户为目标接收账户类型对应的第二账户，因此可以利用不同的账户类型表示数字证书是否已被撤销或者更新。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。

在一个实施例中，认证中心可以向证书申请节点返回第二证书交易记录对应的第二交易标识，以使证书申请节点向交互节点发送第二交易标识，校验请求中携带的可以是第二交易标识。

在一个实施中，目标交易记录为最新交易记录，校验请求中携带目标数字证书对应的交易标识，从区块链中获取目标数字证书对应的目标交易记录包括：根据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，交易链中的各条交易记录按照交易顺序依次排列。交易链可以为存储数字证书对应的交易记录的区块链。

具体地，最新交易记录是目标数字证书对应的交易记录中，交易记录时间最新的交易记录。由于在区块链中，对目标数字证书的操作视为对目标数字证书的交易，因此，区块链中存储了目标数字证书的交易记录，可以从目标数字证书的交易记录中，获取交易时间最新的交易记录作为最新交易记录。

区块链的中交易资源的交易记录是前后连接的，交易链的形式是一笔交易消耗了父交易的输出，并为随后的交易（子交易）创造了输入。交易链中的各条交易记录按照交易顺序依次连接，因此，可以根据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，交易链末端是指交易时间最新的交易记录所处的端点。各个交易记录中记录了父交易对应的交易标识。如图7所示，为一个交易链的图示。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。由图 7 可得，交易输入为上一次交易对应的交易标识。交易输出为用户对应的账户，也可以称为地址。一笔交易记录中可以存在多个交易输出，一笔交易记录中可以包括多个交易资源。

在一个实施例中，校验请求中携带的是第二交易标识，可以根据第二交易标识获取目标数字证书对应的交易链。第二交易标识是第二证书交易记录对应的标识。认证中心在生成第二证书交易记录时，可以向证书申请节点发送第二交易标识，以使证书申请节点向对应的交互节点发送第二交易标识。

在一个实施例中，校验请求中携带的是第一交易标识，通过交易链，可以根据目标数字证书的第一交易标识获取得到最新交易记录，这样，即使第二交易记录对应的第二交易标识未及时发送到证书申请节点，证书申请节点向交互节点发送的是第一交易标识，也可以通过第一交易标识获取得到最新交易记录。

如图 8 所示，在一个实施例中，数字证书管理方法还可以包括以下步骤：

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。

具体地，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。可以将根证书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。

步骤 S804，根据根证书对目标数字证书进行校验，得到根校验结果。

具体地，根校验结果可以为校验成功或者校验失败。得到根证书后，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。

步骤 S806，判断根校验结果是否为校验失败。

具体地，如果根校验结果为校验失败，则进入步骤 S808。如果根校验结果为校验成功，则进入步骤 S204。

步骤 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。

在一个实施例中，根证书、证书发行账户以及证书回收账号可以存储在认证中心中，也可以存储在区块链中，例如根证书、证书发行账户以及证书回收账号可以存储在区块链的创世区块中。可以理解，接收校验请求的认证中心与接收数字证书生成请求的认证中心可以相同也可以不同。例如，根证书、证书发行账户以及证书回收账号可以存储在接收数字证书生成请求的认证中心，这样，只有接收数字证书生成请求的认证中心才可以对目标数字证书进行校验。各个认证中心也可以存储根证书以及接收数字证书生成请求的节点对应的证书发行账户以及证书回收账号，或者区块链上的根证书、证书发行账户、账户回收账户对参与共识的认证中心公开可查。这样，各个认证中心均可以接收对目标数字证书进行校验的校验请求，对目标数字证书进行校验，即使颁发证书的认证中心被劫持或者崩溃，也可以利用其他的认证中心进行校验。即不同的认证中心之间可以相互信任，一个认证中心可以对多个认证中心颁发的数字证书进行校验，不受只能通过颁发证书的认证中心校验目标数字证书的限制。

在一个实施例中，也可以确认区块链中是否存在目标数字证书，如果存在，则确认目标数字证书校验通过。由于区块链的数字不容易被篡改，若区块链中存在一致的数字证书，则表示该数字证书是可信的。

图 9 为一个实施例中提供的数字证书校验方法的应用环境图，该应用环境包括证书申请节点、属于同一区块链的认证中心 1、认证中心 2、认证中心 3 以及认证中心 4。以下结合如图 9，对本申请实施例提供的证书校验方法进行说明：

1、当需要申请数字证书时，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 接收数字证书生成请求，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。

8、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。

如图10所示，在一个实施例中，提供了一种数字证书校验装置，该数字证书校验装置可以集成于上述的认证节点4中，具体可以包括校验请求接收模块1002、目标交易记录获取模块1004、目标账户类型获取模块1006以及校验结果确定模块1008。

校验请求接收模块1002，用于接收对目标数字证书进行校验的校验请求；

目标交易记录获取模块1004，用于从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的；

目标账户类型获取模块1006，用于获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态；

校验结果确定模块1008，用于根据目标账户类型确定目标数字证书对应的校验结果。

在其中一个实施例中，如图11所示，数字证书校验装置还包括：

操作请求接收模块1102，用于接收对目标数字证书进行操作的操作请求；

接收账户类型确定模块1104，用于根据操作请求的操作类型确定目标数字证书对应的目标接收账户类型；

证书交易记录生成模块1106，用于生成操作请求对应的证书交易记录，将证书交易记录写入至区块链，其中，证书交易记录的交易资源为目标数字证书，证书交易记录中的接收账户为目标接收账户类型对应的账户。

在其中一个实施例中，接收账户类型确定模块1104用于：当操作请求对应

的操作类型为更新操作类型或者插入操作类型时，确定目标接收账户类型为证书发行账户类型。

在其中一个实施例中，接收账户类型确定模块 1104 用于：当操作请求对应的操作类型为撤销操作类型时，确定目标接收账户类型为证书回收账户类型。

在其中一个实施例中，目标交易记录为最新交易记录，目标账户类型获取模块 1006 用于：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型；校验结果确定模块 1008 用于：当当前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。

在其中一个实施例中，目标账户类型获取模块 1006 用于：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型；校验结果确定模块 1008 用于：当当前接收账户类型为证书回收账户类型时，确定目标数字证书对应的校验结果为校验失败。

在其中一个实施例中，校验请求中携带目标数字证书对应的交易标识，目标交易记录获取模块 1004 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，交易链中的各条交易记录按照交易顺序依次排列。

在一个实施例中，如图 12 所示，证书校验装置还包括：

证书生成请求接收模块 1202，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。

认证模块 1204，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。

身份认证结果确定模块 1206，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 1208，用于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，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，其中，目标数字证书对应的接收账户为数字证书生成请求接收节点对应的第一账户。

在其中一个实施例中，证书校验装置还包括：

根证书获取模块，用于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；

根校验结果得到模块，用于根据根证书对目标数字证书进行校验，得到根校验结果；

进入模块，用于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，否则，进入从区块链中获取目标数字证书对应的目标交易记录的步骤。

图 13 示出了一个实施例中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校验方法。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校验方法。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。

在一个实施例中，本申请提供的数字证书校验装置可以实现为一种计算机程序的形式，计算机程序可在如图 13 所示的计算机设备上运行。计算机设备的存储器中可存储组成该数字证书校验装置的各个程序模块，比如，图 10 所示的校验请求接收模块 1002、目标交易记录获取模块 1004、目标账户类型获取模块 1006 以及校验结果确定模块 1008。各个程序模块构成的计算机程序使得处理器执行本说明书中描述的本申请各个实施例的数字证书校验方法中的步骤。

例如，图 13 所示的计算机设备可以通过如图 10 所示的数字证书校验装置中的校验请求接收模块 1002 接收对目标数字证书进行校验的校验请求，通过记录获取模块 1004 从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的；通过目标账户类型获取模块 1006 获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态；通过校验结果确定模块 1008，用于根据目标账户类型确定目标数字证

书对应的校验结果。

在一个实施例中，提出了一种计算机设备，计算机设备包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，处理器执行计算机程序时实现以下步骤：接收对目标数字证书进行校验的校验请求；从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的；获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态；根据目标账户类型确定目标数字证书对应的校验结果。

在一个实施例中，计算机程序还使得处理器执行如下步骤：接收对目标数字证书进行的操作请求；根据操作请求的操作类型确定接收目标数字证书对应的目标接收账户类型；生成操作请求对应的证书交易记录，将证书交易记录写入至区块链，其中，证书交易记录的交易资源为目标数字证书，证书交易记录中的接收账户为目标接收账户类型对应的账户。

在一个实施例中，处理器所执行的根据操作请求的操作类型确定接收目标数字证书对应的目标接收账户类型包括：当操作请求对应的操作类型为更新操作类型或者插入操作类型时，确定目标接收账户类型为证书发行账户类型。

在一个实施例中，处理器所执行的根据操作请求的操作类型确定接收目标数字证书对应的接收账户类型包括：

当操作请求对应的操作类型为撤销操作类型时，确定目标接收账户类型为证书回收账户类型。

在一个实施例中，处理器所执行的目标交易记录为最新交易记录，获取目标交易记录对应的目标账户类型包括：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型；根据目标账户类型确定目标数字证书对应的校验结果包括：当当前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。

在一个实施例中，目标交易记录为最新交易记录，处理器所执行的获取目标交易记录对应的目标账户类型包括：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型；根据目标账户类型确定目标数字证书对应的校验结果包括：当当前接收账户类型为证书回收账户类型时，确定目标数字证书对应的校验结果为校验失败。

在一个实施例中，校验请求中携带目标数字证书对应的交易标识，处理器所执行的从区块链中获取目标数字证书对应的目标交易记录包括：根据交易标

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，交易链中的各条交易记录按照交易顺序依次排列。

在一个实施例中，计算机程序还使得处理器执行如下步骤：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；根据根证书对目标数字证书进行校验，得到根校验结果；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，否则，进入从区块链中获取目标数字证书对应的目标交易记录的步骤。

在一个实施例中，提供一种计算机可读存储介质，计算机可读存储介质上存储有计算机程序，计算机程序被处理器执行时，使得处理器执行以下步骤：接收对目标数字证书进行校验的校验请求；从区块链中获取目标数字证书对应的目标交易记录，目标数字证书是作为交易资源存储在区块链中的；获取目标交易记录对应的目标账户类型，其中，不同的账户类型对应不同的证书操作状态；根据目标账户类型确定目标数字证书对应的校验结果。

在一个实施例中，计算机程序还使得处理器执行如下步骤：接收对目标数字证书进行操作的操作请求；根据操作请求的操作类型确定接收目标数字证书对应的目标接收账户类型；生成操作请求对应的证书交易记录，将证书交易记录写入至区块链，其中，证书交易记录的交易资源为目标数字证书，证书交易记录中的接收账户为目标接收账户类型对应的账户。

在一个实施例中，处理器所执行的根据操作请求的操作类型确定接收目标数字证书对应的目标接收账户类型包括：当操作请求对应的操作类型为更新操作类型或者插入操作类型时，确定目标接收账户类型为证书发行账户类型。

在一个实施例中，处理器所执行的根据操作请求的操作类型确定接收目标数字证书对应的接收账户类型包括：

当操作请求对应的操作类型为撤销操作类型时，确定目标接收账户类型为证书回收账户类型。

在一个实施例中，处理器所执行的目标交易记录为最新交易记录，获取目标交易记录对应的目标账户类型包括：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型；根据目标账户类型确定目标数字证书对应的校验结果包括：当当前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。

在一个实施例中，目标交易记录为最新交易记录，处理器所执行的获取目

标交易记录对应的目标账户类型包括：获取最新交易记录对应的接收目标数字证书的当前接收账户类型，作为目标账户类型；根据目标账户类型确定目标数字证书对应的校验结果包括：当当前接收账户类型为证书回收账户类型时，确定目标数字证书对应的校验结果为校验失败。

在一个实施例中，校验请求中携带目标数字证书对应的交易标识，处理器所执行的从区块链中获取目标数字证书对应的目标交易记录包括：根据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，交易链中的各条交易记录按照交易顺序依次排列。

在一个实施例中，计算机程序还使得处理器执行如下步骤：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；根据根证书对目标数字证书进行校验，得到根校验结果；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，否则，进入从区块链中获取目标数字证书对应的目标交易记录的步骤。

应该理解的是，虽然本申请各实施例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，各实施例中的至少一部分步骤可以包括多个子步骤或者多个阶段，这些子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，这些子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的子步骤或者阶段的至少一部分轮流或者交替地执行。

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，的程序可存储于一非易失性计算机可读取存储介质中，该程序在执行时，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、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