

数字证书的处理方法及相关装置

本申请要求于 2018 年 10 月 9 日提交中国专利局、申请号为 201811175201.X、申请名称为“数字证书的处理方法及相关装置”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

本申请涉及区块链技术领域，尤其涉及一种数字证书的处理方法及相关装置。

背景技术

目前很多联盟链应用都开始引入数字证书颁发机构 (Certificate Authority, CA) 为区块链上的参与方颁发数字证书。由于很多参与方 (例如大多数银行) 都有自己的 CA, 因此都会要求可以通过自己的 CA 为自己的客户来颁发数字证书。例如, 银行 A 有自己的 CA (例如 CA-A), 银行 B 有自己的 CA (比如 CA-B), 银行 C 有自己的 CA (比如 CA-C) 等等, 各个银行均可通过自己的 CA 为自己的客户颁发数字证书。在联盟链网络中, 银行 A、银行 B 以及银行 C 等任一参与方均会认同其他参与方的 CA 给其客户颁发的数字证书。然而, 由于所有联盟链上的参与方也都可以通过一个客户的数字证书来判断该客户的哪个参与方的客户, 比如银行 B 可以通过一个企业的数字证书的签发方来判断这个企业是哪个银行的客户。比如说, 该企业的数字证书是由银行 A 颁发, 银行 B 则可确定该企业是银行 A 的客户等等。目前联盟链上的这种数字证书的颁发方式导致联盟链交易的交易信息对于联盟链上的各个参与方是完全公开的, 交易双方的身份暴露无遗, 难以满足各个参与方的交易需求, 适用性差。

发明内容

本申请实施例提供一种数字证书的处理方法及相关装置, 可实现数字证书的匿名签发, 增强数字证书的签发方的身份私密性, 适用性强。

第一方面, 本申请实施例提供了一种数字证书的签发方法, 上述方法适用于数字证书的签发方, 上述方法包括:

区块链网络中的第一参与方的证书颁发机构 CA 将上述第一参与方的 CA 公钥记录至区块链网络中, 上述第一参与方为上述区块链网络中数字证书的签发方, 上述区块链网络中还记录了至少一个第二参与方的 CA 公钥, 上述第二参与方为上述区块链网络中除上述第一参与方之外的参与方;

当上述第一参与方的 CA 接收到任一用户的证书授权请求时, 根据上述证书授权请求中携带的用户身份信息确认上述用户是否为上述第一参与方的 CA 的用户;

若上述签发方的 CA 确认上述用户是上述第一参与方的 CA 的用户, 则从上述证书授权请求中获取上述用户的公钥, 并根据预先设定的环签名证书签发规则, 从上述区块链网络中获取任意 N 个上述第二参与方的 CA 公钥, 其中, N 等于上述环签名证书签发规则中设定的公钥数量;

上述签发方的 CA 根据上述第一参与方的 CA 的公钥、私钥和上述 N 个上述第二参与方的 CA 公钥对上述用户的用户身份信息和公钥进行环签名并形成数字证书，并向上述用户发送上述数字证书。

第二方面，本申请实施例提供了一种数字证书的验证方法，上述方法适用于数字证书的验证方，上述方法包括：

当验证方获得区块链网络中的任一签名交易时，上述验证方获取上述签名交易的发起方的数字证书；上述签名交易的发起方可为上述区块链网络中的参与方之一，上述区块链网络中记录了包括上述交易的发起方在内的各个参与方的证书颁发机构 CA 公钥；

上述验证方基于预设的环签名证书签发规则从上述数字证书中获取上述数字证书的环签名的公钥信息，并根据上述公钥信息确定上述数字证书的环签名对应的所有公钥，上述环签名对应的所有公钥为上述区块链网络中的多个参与方的 CA 公钥，且上述环签名对应的公钥数量等于上述环签名证书签发规则中设定的公钥数量；

上述验证方根据上述环签名对应的所有公钥对上述签名交易的签名进行验证。

第三方面，本申请实施例提供了一种数字证书的签发装置，上述装置适用于数字证书的签发方的证书颁发机构 CA，上述装置包括：

记录单元，用于将上述第一参与方的 CA 公钥记录至区块链网络中，上述第一参与方为上述区块链网络中数字证书的签发方，上述区块链网络中还记录了至少一个第二参与方的 CA 公钥，上述第二参与方为上述区块链网络中除上述第一参与方之外的参与方；

确认单元，用于在接收到任一用户的证书授权请求时，根据上述证书授权请求中携带的用户身份信息确认上述用户是否为上述第一参与方的 CA 的用户；

获取单元，用于在上述确认单元确认上述用户是上述第一参与方的 CA 的用户时，从上述证书授权请求中获取上述用户的公钥，并根据预先设定的环签名证书签发规则，从上述区块链网络中获取任意 N 个上述第二参与方的 CA 公钥，其中，N 等于上述环签名证书签发规则中设定的公钥数量；

签发单元，用于根据上述第一参与方的 CA 的公钥、私钥和上述 N 个上述第二参与方的 CA 公钥对上述用户的用户身份信息和公钥进行环签名并形成数字证书，并向上述用户发送上述数字证书。

第四方面，本申请实施例提供了一种数字证书的验证装置，上述装置适用于数字证书的验证方，上述装置包括：

获取单元，用于在获得区块链网络中的任一签名交易时，获取上述签名交易的发起方的数字证书；上述签名交易的发起方可以为上述区块链网络中的参与方之一，上述区块链网络中记录了包括上述交易的发起方在内的各个参与方的证书颁发机构 CA 公钥；

确定单元，用于基于预设的环签名证书签发规则从上述数字证书中获取上述数字证书的环签名的公钥信息，并根据上述公钥信息确定上述数字证书的环签名对应的所有公钥，上述环签名对应的所有公钥为上述区块链网络中的多个参与方的 CA 公钥，且上述环签名对应的公钥数量等于上述环签名证书签发规则中设定的公钥数量；

验证单元，用于根据上述确定单元确定的上述环签名对应的所有公钥对上述签名交易的签名进行验证。

第五方面，本申请实施例提供了一种终端，该终端包括处理器、存储器和/或收发器，上述处理器、存储器和/或收发器相互连接，其中，上述存储器用于存储计算机程序，上述计算机程序包括程序指令，上述处理器和/或上述收发器被配置用于调用上述程序指令，执行上述第一方面中提供的方法或第二方面中提供的方法。

第六方面，本申请实施例提供了一种计算机可读存储介质，上述计算机可读存储介质存储有计算机程序，上述计算机程序包括程序指令，上述程序指令当被处理器执行时使上述处理器执行上述第一方面中提供的方法或第二方面中提供的方法。

基于本申请实施例，可实现作为数字证书的签发机构的任一参与方的无条件匿名，实现数字证书签发机构向其用户匿名签发数字证书，可避免数字证书的签发机构的身份泄露，避免区块链网络中的其他参与方获知数字证书的签发机构的信息，从而可增强数字证书的签发机构的身份私密性，保障数字证书的签发机构的交易信息的私密性，适用性强。

附图说明

为了更清楚地说明本申请实施例技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍。

图1是本申请实施例提供的数字证书签发通用流程的示意图；

图2是本申请实施例提供的数字证书的处理方法的流程示意图；

图3是本申请实施例提供的数字证书的签发装置的结构示意图；

图4是本申请实施例提供的数字证书的验证装置的结构示意图；

图5是本申请实施例提供的终端的一结构示意图；

图6是本申请实施例提供的终端的另一结构示意图。

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。

本申请实施例提供的数字证书的处理方法（包括数字证书的签发方法和数字证书的验证方法，为方便描述，以下简称本申请实施例提供的方法）及相关装置可适用于是银行、保险、证券、商业协会、集团企业及上下游企业等机构的业务交易和/或企业信息处理等应用场景中，具体可根据实际应用场景确定，在此不做限制。可选的，上述银行、保险、证券、商业协会、集团企业及上下游企业等机构可作为同一个联盟链网络中的多个参与方。可选的，上述银行、保险、证券、商业协会、集团企业及上下游企业等机构也可以有各自的联盟链网络，在上述银行、保险、证券、商业协会、集团企业及上下游企业等机构各自的联盟链网络中，各个机构的客户和/或员工可以是联盟链网络中的参与方，具体可根据实际应用场景确定，在此不做限制。为方便描述，下面将以上述银行、保险、证券、商业协会、集团企业及上下游企业等机构可作为同一个联盟链网络中的多个参与方为例进行说明。为方便理解，下面将对本申请实施例提供的方法所涉及的联盟链以及数字证书进行简要说明。

一、联盟链

区块链诞生于移动互联网时代，上述银行、保险、证券、商业协会、集团企业及上下游

企业等机构普遍已经是 IT 化和互联网化的组织和/或机构，区块链对于进一步提升这些机构圈子的产业链条中的公证、结算清算业务和价值交换等业务的处理效率很有帮助。然而，传统区块链（比如公有链）的处理性能、隐私保护、合规性等都不能满足这些机构的业务需求，采用公有链来处理公证、结算清算业务或者价值交换等业务，会颠覆这些机构的现有商业模式和固有利益，风险较大。因此，基于上述各个机构的业务需求，具备更好的隐私保护的区块链体系——联盟链，应运而生。联盟链，只针对特定某个群体的成员和有限的第三方，内部指定多个预选的节点为记账人，每个区块的生成由所有的预选节点共同决定，其他接入节点可以参与交易，但不过问记账过程，其他第三方可以通过该联盟链开放的应用程序编程接口（Application Programming Interface, API）进行限定查询。有了准入机制，可以使得联盟链网络中各个参与方之间的交易性能得到提高，私密性更强。

二、数字证书

数字证书是互联网通讯中用于标识各个通讯方身份信息的一串数字，数字证书的出现为互联网通讯提供了一种在互联网上验证各个通讯方的通信实体身份的方式。数字证书不是数字身份证，而是各个通信实体的身份认证机构盖在各个通信实体的数字身份证上的一个章或印（或者说加在各个通信实体的数字身份证上的一个签名）。数字证书是由权威机构——CA 发行的，可以在互联网上用数字证书来识别各个通信实体的身份。数字证书是一个经 CA 数字签名的文件，其中包含公开密钥（简称公钥）的持有者信息以及公开密钥的文件。最简单的数字证书中可以包含一个公钥、公钥的持有者名称以及证书授权中心的数字签名，且数字证书只在特定的时间段内有效。

数字证书是一种权威性的电子文档，可以由权威公正的第三方机构，即 CA（例如中国各地方的 CA 公司）签发的证书，也可以由企业级的 CA（比如银行 A 的 CA-A）进行签发。数字证书可用于：发送安全电子邮件、访问安全站点、网上证券交易、网上招标采购、网上办公、网上保险、网上税务、网上签约和网上银行等安全电子事务处理和安全电子交易签名。数字证书里存有很多数字和英文，当使用数字证书进行身份认证时，它将随机生成 128 位的身份码，每份数字证书都能生成相应但每次都不可能相同的数码，从而保证数据传输的保密性，即相当于生成一个复杂的密码。数字证书绑定了公钥以及公钥持有者的真实身份，它类似于现实生活中的居民身份证，所不同的是数字证书不再是纸质的证照，而是一段含有数字证书的持有者身份信息并经过认证中心审核签发的电子数据，可以更加方便灵活地运用在电子商务和电子政务中。

参见图 1，图 1 是本申请实施例提供的数字证书签发通用流程的示意图。本申请实施例提供的数字证书的签发过程一般包括如下步骤 S11 和 S12：

S11，用户向机构的 CA 发送证书授权请求。

在一些可行的实施方式中，当用户（比如银行、保险或者企业等机构的客户）请求与机构（比如银行、保险或者企业等）进行交易时，可首先产生自己的密钥对，该密钥对中包括公钥和私钥，并通过向机构的 CA 发送证书授权请求的方式将公钥以及部分用户身份信息传送给机构的 CA。换句话说，用户向机构的 CA 发送的证书授权请求中可包括部分的用户身份信息和用户的公钥，以向机构的 CA 请求对用户的用户身份信息和公钥进行签名并颁发数字证书。

S12, 机构的 CA 验证用户身份并签发数字证书。

在一些可行的实施方式中, 用户请求签名交易的机构, 可通过机构的 CA 核实用户的身份。机构的 CA 核实用户的身份 (即用户为自己的客户) 时, 可对用户发送的证书授权请求中包括的用户身份信息进行确定, 以确认证书授权请求确实由自己的客户 (即用户) 发送而来。机构的 CA 确认证书授权请求由用户发送而来时, 向用户发送一个数字证书, 该数字证书内包含用户的用户身份信息和用户的公钥, 同时还附有机机构的 CA 的签名信息。用户就可以使用机构的 CA 签发的数字证书进行相关的交易签名。各个机构的 CA 给其客户颁发的数字证书由各个机构独立的证书发行机构 (即 CA) 发布。数字证书各不相同, 每种证书可提供不同级别的可信度, 各个机构的各个客户用户 (即用户) 可以从各个机构的 CA 获得自己的数字证书。

数字证书采用公钥体制, 即利用一对互相匹配的密钥进行数字签名和验签。每个用户自己设定一把特定的且仅为本人所知的私有密钥 (即私钥), 基于该私钥可进行与机构交易的交易信息的数字签名。同时, 用户可设定一把对应的公共密钥 (即公钥) 并由本人公开, 为一组用户所共享, 用于对交易信息进行签名验证。公钥技术解决了密钥发布的管理问题, 用户可以公开其所持有的公钥, 而保留其所持有的私钥。用户也可以采用自己的私钥对交易信息加以处理, 由于私钥仅为本人所有, 这样就产生了别人无法生成的文件, 也就形成了数字签名。采用数字签名, 可以保证交易信息是由发送方自己签名发送的, 发送方不能否认或难以否认, 同时也可保证交易信息自发送方签发后至接收方收到为止未曾作过任何修改, 签发的文件是真实文件, 保证了交易信息的不可篡改性。

基于上述联盟链的特性以及数字证书的特性, 本申请实施例提供了一种基于分布式数字证书的数字证书的处理方法及相关装置, 包括数字证书的签发方法及装置、和数字证书的验证方法及装置, 可实现对联盟链网络中的任一参与方的客户签发数字证书, 并可实现基于任一签名交易的发起方的数字证书确定数字证书的环签名对应的所有公钥以基于数字证书的环签名对应的所有公钥对该交易的签名进行验证。联盟链中的各个参与方的 CA 可基于本申请实施例提供的数字证书签发方法为与自己的客户签发数字证书, 实现作为签名者 (即数字证书的签发方) 的任一参与方的 CA 的无条件匿名, 从而可避免数字证书的签发方的 CA 的身份泄露, 避免联盟链网络中的其他参与方获知数字证书的签发方的 CA 的客户信息, 从而可保障数字证书的签发方的交易信息的私密性, 保证签发方的客户信息的安全性, 适用性更强, 具体可参见如下各个实施例所提供的实现方式。具体的, 本申请实施例提供的方法可通过联盟链网络记录联盟链网络中所有可以被认可参与方 (或非参与方) 的 CA 的公钥 (例如银行 A 的 CA-A, 银行 B 的 CA-B, ……)。当任一机构的 CA 要为自己的一个客户 (或以用户进行说明) 颁发数字证书时, 该机构的 CA 会用环签名来对该客户签发数字证书 (传统方式是 CA 用自己的私钥对其颁发给其客户的数字证书进行签名), 这样使得第三方无法判断这个数字证书究竟是哪一个机构的 CA 签发。也就是说其他第三方无法判断该客户是联盟链网络中哪一个被认可参与方的 CA 的客户, 从而可实现各个被认可参与方的 CA 的数字证书匿名发送, 从而保护了联盟链网络中各个被认可参与方的 CA 为其客户颁发数字证书的私密性, 可提高数字证书签发方的 CA 的身份私密性, 从而可增强数据证书的签发方式的适用性。

参见图 2，是本申请实施例提供的数字证书的处理方法的流程示意图。参见图 2，联盟链网络中包括的任一参与方的 CA 采用环签名为自己的客户签发数字证书签名以及任一验证方对任一签名交易进行验签的实现方式可参见如下步骤 S21 至 S25 所提供的实现方式。为方便描述，下面将以任一参与方的 CA 为自己的客户（或称用户）签发数字证书的实现方式为例进行说明，其中该任一参与方可以签发方（即第一参与方）为例进行说明。换句话说，这里的签发方指代联盟链网络中任一需要为自己的用户签发数字证书的参与方，对应的，对数字证书进行验证的任一机构可以验证方为例进行说明，具体可根据实际应用场景确定，在此不做限制。

S21，签发方的 CA 将自己的公钥记录至区块链网络中。

在一些可行的实施方式中，联盟链网络（即区块链网络）中的任一被认可参与方（为方便描述下面简称参与方）的 CA（或简称参与方 CA）产生一个公钥和一个私钥，并可通过智能加密合约（Smart Crypto Contract, SCC）将自己（即参与方 CA）的信息和公钥记录到联盟链网络中。比如说，对于被认可的多个银行，每个银行的 CA 可产生一个公钥和一个私钥，并且每个银行的 CA 产生的公钥可由每个银行的 CA 自己公开，并由联盟链网络记录每个银行的 CA 的公钥（即每个银行的 CA 的公钥），每个银行的 CA 的私钥由每个银行的 CA 自己所知。换句话说，假设签发方为联盟链网络中的参与方之一（假设为第一参与方），联盟链网络中记录了签发方（为方便描述，区块链网络中的数字证书的签发方可以第一参与方为例进行说明）的 CA 的公钥（或简称 CA 公钥）之外，还记录了签发方之外的其他各个参与方（为方便描述，区块链网络中除了数字证书的签发方之外的其他任意参与方可以第二参与方为例进行说明）的 CA 公钥。

可以理解，这里各个参与方的 CA 公钥都记录在联盟链网络中，因此联盟链中的任一参与方均可知道联盟链网络中其他各个参与方的 CA 公钥。在任一参与方（比如第一参与方，即签发方）的 CA 需要为自己的客户（签发方的 CA 的客户，同时也为签发方的客户，为方便描述，下面以签发方的 CA 的客户为例进行说明）的数字证书进行签名时，可以采用环签名的方式，从联盟链网络中获取其他一个或者多个参与方的 CA 公钥，结合自己的公钥和私钥（即签发方的 CA 的公钥和私钥）为自己的客户签发数字证书，具体可参见如下步骤说明。

S22，当签发方的 CA 接收到任一用户的证书授权请求时，根据证书授权请求中携带的用户身份信息确认用户是否为自己的用户。

在一些可行的实施方式中，当任一用户（比如银行 A 的任一客户）请求与机构（比如银行 A）进行交易时，可通过向银行 A 的 CA（为方便描述，将以签发方的 CA 作为银行 A 的 CA 的示例进行说明）发送证书授权请求（或称认证请求）的方式将公钥以及用户身份信息传送给签发方的 CA。换句话说，用户向签发方的 CA 发送的证书授权请求中可包括用户身份信息和用户的公钥，以向签发方的 CA 请求对用户的用户身份信息和公钥进行签名并颁发数字证书给用户。签发方的 CA 可根据证书授权请求中包括的用户身份信息核实用户的身份（即核实用户是否为自己的客户），即签发方的 CA 可对用户发送的证书授权请求中包括的用户身份信息进行确定，以确认证书授权请求确实由自己的客户发送而来。签发方的 CA 确定发送证书授权请求的用户为自己的用户（即签发方的 CA 的用户，也就是第一参与方的 CA 的用户）之后，则可向用户签发数字证书。

S23, 若签发方的 CA 确认上述用户是自己的用户, 则从证书授权请求中获取用户的公钥, 并根据预先设定的环签名证书签发规则, 从区块链网络中获取其他任意 N 个参与方的 CA 公钥。

在一些可行的实施方式中, 各个参与方的环签名证书签发规则 (即采用环签名的方式签发数字证书的规则) 可由各个参与方的 CA 自行制定, 每个参与方的 CA 均可以根据自身需求, 任意选择一个或者多个 (为方便描述可假设为 N 个) 第三方公钥, 结合自身的公钥和私钥来完成环签名。这里, 对应任一联盟链网络中的任一参与方的 CA 来说, 其所任意选择的 N 个第三方公钥可以是联盟链网络中除了该参与方之外的任意 N 个参与方的 CA 记录在联盟链网络中的 CA 公钥。换句话说, 任一参与方自行制定的环签名证书签发规则中, 该参与方的 CA 给用户签发数字证书所使用的公钥数量可由该参与方的 CA 自行设定。可选的, 联盟链网络中的各个参与方的 CA 可以共同制定的环签名证书签发规则并写入联盟链网络中, 包括但不限于环签名所需公钥数量以及规范, 可以提前在联盟链网络范围设置, 在此不做限制。

可选的, 在一些可行的实施方式中, 各个参与方自行制定的环签名证书签发规则可写入联盟链网络中, 包括但不限于环签名所需公钥数量以及规范 (即由 X509 格式的数字证书构成的规范, 比如数字证书格式 (X509) 和/或 X509 中用于记录环签名的公钥信息的预设字段), 可以提前在联盟链网络范围设置。举例来说, 联盟链网络中的各个参与方的 CA (比如签发方的 CA) 采用环签名为自己的用户签发数字证书时所需的公钥数量, 以及 X509 格式的数字证书构成的规范 (或称环签名证书签发规范) 等, 可以提前在联盟链网络范围设置, 从而可帮助验证方基于上述规范等信息对联盟链网络中的交易进行验签验证。其中, 上述 X509 中用于记录环签名的公钥信息的预设字段包括但不限于数字证书格式中的签发方标注字段和/或扩展字段, 具体可根据实际应用场景确定, 在此不做限制。

可选的, 上述 X509 中包括扩展字段 (Extension), 该扩展字段可用于记录数字证书的环签名对应的所有公钥 (比如环签名对应的 N 个参与方的 CA 公钥), 和/或该环签名对应的所有公钥 (比如环签名对应的 N 个参与方的 CA 公钥) 的标识等公钥信息。验证方基于上述 X509 中包括的扩展字段中所记录的所有公钥确定环签名对应的所有公钥, 和/或所有公钥的标识从联盟链网络中查找对应的公钥, 以基于环签名对应的所有公钥对交易的签名进行验证。

可选的, 在一些可行的实施方式中, 联盟链网络也可以将联盟链网络中各个参与方的 CA 公钥分为不同的公钥分组, 并可为每个公钥分组制定分组标识符。其中, 上述每个分组的分组标识符可以帮助验证方找到环签名对应的公钥分组 (为方便描述可以目标分组为例进行说明), 进而可将环签名对应的公钥分组中的公钥确定为环签名对应的公钥, 从而可获取各个公钥所属的 CA 的信息。验证方基于上述 X509 的扩展字段中确定出环签名的公钥信息, 其中该环签名的公钥信息包括分组标识, 进而可基于数字证书中包括的该分组标识符从联盟链网络中记录的多个公钥分组中确定出目标分组, 从而可将目标分组中包括的所有公钥确定为环签名对应的所有公钥, 以基于环签名对应的所有公钥对交易的签名进行验证。

S24, 签发方的 CA 根据自己的公钥、私钥和其他任意 N 个参与方的 CA 公钥对用户的用

户身份信息和公钥进行环签名并形成数字证书，并向用户发送上述数字证书。

其中，N 等于上述步骤 S23 中预先设定的环签名证书签发规则中设定的公钥数量。

在一些可行的实施方式中，当联盟链网络中的任一参与方（即签发方，比如银行 A）的 CA 准备给自己的客户（即用户，比如企业 1）签发数字证书时，该签发方的 CA 会用自己的公钥和私钥（比如银行 A 的 CA 的公钥和私钥），以及联盟链网络中其他任意多个参与方的 CA 公钥（比如其他银行的 CA 公钥，假设是 N 个公钥，可以理解，上述多个参与方的 CA 公钥都记录在联盟链网络中）为企业 1 的身份信息和公钥签名并形成数字证书，且该数字证书的 X509 中的预设字段中携带该数字证书的环签名的公钥信息。例如，假设银行 A 的 CA 收到其客户的证书授权请求（假设客户为 m），其中包括部分用户身份信息以及用户需要被验证的公钥。银行 A 的 CA 核实证书授权请求中携带的用户身份信息对应的用户的身份且确认 m 确实是自己的客户之后，银行 A 的 CA 可以使用联盟链中 N 个环成员的 CA 公钥、以及银行 A 的 CA 自己的公钥和私钥作为输入，对客户 m 的公钥和身份信息申请产生一个签名 R。银行 A 的 CA 可将通过上述 R 签名的数字证书颁发给该客户（该证书包含客户的基本信息和客户的公钥），客户就可以使用银行 A 的 CA 签发给自己的数字证书进行交易签名。

在一些可行的实施方式中，联盟链网络中的签发方的 CA 给自己的客户签发数字证书采用传统的 X509 格式，签发的数字证书符合 ITU-TX. 509 国际标准。需要说明的是，这里签发数字证书采用 X509，但是在 X509 中对证书签发方（Issuer）的标注不再是一个机构的名称，而是与证书签发方的 CA 对应的区块链网络（比如联盟链网络）的标识。这里，假设 X509 中对证书签发方 CA 的标注是 X509 中的某一个字段，在该字段中记录与证书签发方的 CA 对应的区块链网络的标识，为方便描述，可将该字段假设为签发方标注字段。换句话说，X509 中的签发方标注字段可以是 X509 中任一用于记录与证书签发方的 CA 对应的区块链网络的标识的字段，具体可根据实际应用场景确定，在此不做限制。

可选的，在 X509 中对证书签发方（Issuer）的标注中记录与证书签发方的 CA 对应的公钥指示信息。其中，上述公钥指示信息包括但不限于：该数字证书的环签名对应的所有公钥信息，该数字证书的环签名对应的所有公钥的标识符。换句话说，可以在 X509 的签发方标注字段中记录与证书签发方的 CA 对应的公钥指示信息，该公钥指示信息包括但不限于：该数字证书的环签名对应的所有公钥信息，该数字证书的环签名对应的所有公钥的标识符，在此不做限制。

可选的，可以在 X509 的扩展（Extension）字段中记录与证书签发方的 CA 对应的公钥信息。其中，上述公钥信息包括但不限于：该数字证书的环签名对应的所有公钥，该数字证书的环签名对应的所有公钥的标识符。可选的，可以在 X509 的扩展字段中记录数字证书的环签名对应的公钥分组标识符，该公钥分组标识符用于指示数字证书的环签名对应的公钥的所属分组，以帮助数字证书的验证方基于公钥的所属分组找到环签名对应的公钥。

可选的，在一些可行的实施方式中，如果联盟链网络中有规范制定（例如统一制定，或者约定）的环签名证书签发规则，则 X509 的扩展字段不需要更多的记录，具体可根据实际应用场景确定，在此不做限制。

S25，当验证方获得区块链网络中的任一签名交易时，验证方获取上述交易的发起方的数字证书，基于预设的环签名证书签发规则从上述数字证书中获取环签名的公钥信息，并

根据上述公钥信息确定环签名对应的所有公钥，根据环签名对应的所有公钥对上述交易的签名进行验证。

在一些可行的实施方式中，这里验证方可以是任意机构，在此不做限制。下面以联盟链网络中的任一参与方为例进行说明，具体不做限制。上述环签名证书签发规则记录于区块链网络中，环签名证书签发规则中包括环签名的公钥数量和环签名证书签发规范，环签名证书签发规范中包括数字证书格式 X509 中用于记录环签名的公钥信息的预设字段。上述数字证书中包括的公钥信息包括数字证书格式 X509 的预设字段中所包括的区块链网络的标识、数字证书的环签名对应的所有参与方的 CA 公钥，和/或数字证书的环签名对应的所有参与方的 CA 公钥的标识。其中，上述预设字段包括签发方标注字段和/或扩展字段。可选的，若联盟链网络中记录的各个参与方的 CA 公钥为多个分组，且一个分组对应一个分组标识符，则上述公钥信息可包括数字证书中包括的分组标识符，该分组标识符用于确定区块链网络中所包括的目标分组，以基于目标分组中包括的公钥确定数字证书的环签名对应的所有参与方的 CA 公钥。具体可参见上述步骤 S24 中数字证书的签名对应的验证方操作方式，在此不做限制。

在一些可行的实施方式中，当联盟链网络中收到任意一个签名交易时，联盟链网络中的验证方获得该签名交易时，可获取该签名交易的发起方的数字证书。数据证书格式为 X509，验证方可以通过写在 X509 中的标识符从联盟链网络中找到该发起方的数字证书的环签名对应的所有公钥。换句话说，验证方对任一签名交易的签名进行验证时，可以通过该交易的发起方签发数字证书时写在 X509 中的标识符从联盟链网络中找到该数字证书的环签名对应的所有公钥。可选的，验证方还可通过交易发起方的数字证书找到写在 X509 的签发方（Issuer）的标注中的公钥信息（比如 X509 中签发方标注字段中包括的公钥信息），该公钥信息包括但不限于数字证书的环签名对应的所有公钥，和/或该数字证书的环签名对应的所有公钥的标识符。可选的，验证方还可通过交易发起方的数字证书找到写在 X509 的扩展字段中公钥信息，该公钥信息包括但不限于数字证书的环签名对应的所有公钥，和/或该数字证书的环签名对应的所有公钥的标识符。可选的，验证方还可通过交易发起方的数字证书找到写在 x509 的扩展字段中的公钥分组标识符，基于该公钥分组标识符从联盟链网络中包括的各个公钥分组中找到数字证书的环签名对应的公钥所属分组，进而可基于找到的公钥所属分组确定该数字证书的环签名对应的所有公钥。具体实现中，验证方基于何种方式找到环签名对应的公钥具体可根据 X509 中的信息确定，在此不做限制。验证方找到交易发起方的数字证书的环签名对应的所有公钥之后，则可基于找到的所有公钥对该交易的签名进行验证，具体验证过程在此不做限制。换句话说，数字证书的环签名的公钥信息具体由数字证书中的何种信息来携带和/或指示，在此不做限制。或者说，数字证书的环签名的公钥信息具体由数字证书格式（X509）中的何字段来携带和/或指示，在此不做限制。具体可参见上述步骤 S24 中数字证书的签名对应的验证方操作方式，在此不做限制。

由上可知，基于本申请实施例提供的方法实现对数字证书的环签名，可实现数字证书的签发方的无条件匿名，对于验证方来说，签发方是完全正确匿名的。基于本申请实施例提供的方法实现对数字证书的环签名包括但不限于如下安全性属性：

- 1) 无条件匿名性。攻击者即使非法获取了所有可能签名者的私钥，能确定出真正的签

名者的概率不超过 $1/n$ ，这里 n 为环成员（即可能签名者）的个数；

2) 不可伪造性。攻击者在不知道任何环成员的私钥的情况下，即使能够从一个产生环签名的随机预言者那里得到任何用户的签名，可以成功伪造该用户的合法签名的概率几乎可以忽略；

3) 环签名具有良好的特性。可以实现签名者的无条件匿名，签名者可以自由指定自己的匿名范围，可以实现群签名的主要功能但无需可信第三方或群管理员等。

在本申请实施例中，基于数字证书的签发方的 CA 自行制定的环签名证书签发规则，对签发方的 CA 的用户签发数字证书，可保证数字证书的签发方的 CA 之外的其他任意参与方的 CA 无法判断数字证书由哪个参与方的 CA 签发。也就是说联盟链网络中除了数字证书的签发方的 CA 之外的其他任意参与方的 CA 均无法判断该数字证书的接收方是联盟链中哪一个参与方的 CA 的客户，从而可实现联盟链中各个参与方的 CA 为其用户签发数字证书的私密性，实现各个参与方的 CA 向其用户匿名发送数字证书，保证数字证书的签发方的 CA 的身份私密性，增强联盟链网络中各个参与方的 CA 与其用户之间的交易的信息安全性，可满足联盟链网络中各个参与方的更多业务需求，适用性更强。

参见图 3，是本申请实施例提供的数字证书的签发装置的结构示意图。该数字证书签发装置适用于数字证书的签发方，可以是联盟链网络中任一需要为自己的用户签发数字证书的参与方，在此不做限制。该数字证书签发装置可包括：

记录单元 31，用于将上述第一参与方的 CA 公钥记录至区块链网络中，上述第一参与方为上述区块链网络中数字证书的签发方，上述区块链网络中还记录了至少一个第二参与方的 CA 公钥，上述第二参与方为上述区块链网络中除上述第一参与方之外的参与方。

确认单元 32，用于在接收到任一用户的证书授权请求时，根据上述证书授权请求中携带的用户身份信息确认上述用户是否为上述第一参与方的 CA 的用户。

获取单元 33，用于在上述确认单元 32 确认上述用户是上述第一参与方的 CA 的用户时，从上述证书授权请求中获取上述用户的公钥，并根据预先设定的环签名证书签发规则，从上述区块链网络中获取其他任意 N 个上述第二参与方的 CA 公钥，其中， N 等于上述环签名证书签发规则中设定的公钥数量。

签发单元 34，用于根据上述第一参与方的 CA 的公钥、私钥和上述 N 个上述第二参与方的 CA 公钥对上述用户的用户身份信息和公钥进行环签名并形成数字证书，并向上述用户发送上述数字证书。

在一些可行的实施方式中，上述环签名证书签发规则由上述第一参与方的 CA 自行制定，或者由上述区块链网络中的各个参与方的 CA 共同制定；上述环签名证书签发规则被记录于上述区块链网络中。

在一些可行的实施方式中，上述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；上述 X509 中包括用于记录环签名的公钥信息的预设字段；

上述签发单元 34 用于：

基于上述规范，使用上述第一参与方的 CA 的公钥、私钥和上述 N 个上述第二参与方的 CA 公钥对上述用户的用户身份信息和公钥进行环签名并形成数字证书，上述数字证书的上述预设字段中携带上述数字证书的环签名的公钥信息。

在一些可行的实施方式中，上述 X509 中包括签发方标注字段，上述签发方标注字段中包括上述第一参与方的 CA 对应的区块链网络标识和/或上述数字证书的环签名的公钥信息；

其中，上述公钥信息包括上述数字证书的环签名对应的上述 N 个上述第二参与方的 CA 公钥，和/或上述环签名对应的上述 N 个上述第二参与方的 CA 公钥的标识。

在一些可行的实施方式中，上述预设字段包括上述 X509 中的扩展字段，上述扩展字段中携带的上述环签名的公钥信息包括上述数字证书的环签名对应的上述 N 个上述第二参与方的 CA 公钥，和/或上述环签名对应的上述 N 个上述第二参与方的 CA 公钥的标识。

在一些可行的实施方式中，上述区块链网络中记录的各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

上述预设字段包括上述 X509 中的扩展字段，上述扩展字段中携带的上述环签名的公钥信息包括分组标识符，上述分组标识符用于指示上述环签名对应的上述 N 个上述第二参与方的 CA 公钥的所属分组，以帮助上述数字证书的验证方基于上述 N 个上述第二参与方的 CA 公钥的所属分组找到上述 N 个上述第二参与方的 CA 公钥。

具体实现中，作为数字证书签发方的数字证书签发装置可通过其内置的各个功能单元执行上述实施例中各个步骤所提供的实施方式。可选的，上述记录单元 31 用于执行上述实施例中步骤 S21 所提供的实施方式，具体可参见上述步骤 S21 中数字证书签发装置所执行的操作，在此不做限制。上述确认单元 32 用于执行上述实施例中步骤 S22 所提供的实施方式，具体可参见上述步骤 S22 中数字证书签发装置所执行的操作，在此不做限制。上述获取单元 33 用于执行上述实施例中步骤 S23 所提供的实施方式，具体可参见上述步骤 S23 中数字证书签发装置所执行的操作，在此不做限制。上述签发单元 34 用于执行上述实施例中步骤 S24 所提供的实施方式，具体可参见上述步骤 S24 中数字证书签发装置所执行的操作，在此不做限制。

在本申请实施例中，数字证书的签发方的 CA 可自行制定环签名证书签发规则，包括环签名所需的公钥数量以及环签名证书签发规范等。基于数字证书的签发方的 CA 自行制定的环签名证书签发规则，对签发方的 CA 的用户签发数字证书，可保证数字证书的签发方的 CA 之外的其他任意参与方的 CA 无法判断数字证书由哪个参与方的 CA 签发。也就是说联盟链网络中除了数字证书的签发方的 CA 之外的其他任意参与方的 CA 均无法判断该数字证书的接收方是联盟链中哪一个参与方的 CA 的客户，从而可实现联盟链中各个参与方的 CA 为其用户颁发数字证书的私密性，实现各个参与方的 CA 向其用户匿名发送数字证书，保证数字证书的签发方的 CA 的身份私密性，增强联盟链网络中各个参与方的 CA 与其用户之间的交易的信息安全性，可满足联盟链网络中各个参与方的更多业务需求，适用性更强。

参见图 4，是本申请实施例提供的数字证书的验证装置的结构示意图。该数字证书的验证装置适用于数字证书的验证方，在此不做限制。该数字证书验证装置可包括：

获取单元 41，用于在获得区块链网络中的任一签名交易时，获取上述签名交易的发起方的数字证书，上述签名交易的发起方可以为上述区块链网络中的参与方之一，上述区块链网络中记录了包括上述交易的发起方在内的各个参与方的证书颁发机构 CA 公钥。

确定单元 42，用于基于预设的环签名证书签发规则从上述数字证书中获取上述数字证书的环签名的公钥信息，并根据上述公钥信息确定上述数字证书的环签名对应的所有公钥，

上述环签名对应的所有公钥为上述区块链网络中的多个参与方的 CA 公钥，且上述环签名对应的公钥数量等于上述环签名证书签发规则中设定的公钥数量。

验证单元 43，用于根据上述确定单元 42 确定的上述环签名对应的所有公钥对上述签名交易的签名进行验证。

在一些可行的实施方式中，上述环签名证书签发规则被记录于上述区块链网络中，上述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；上述 X509 中包括用于记录环签名的公钥信息的预设字段；

上述公钥信息包括上述预设字段中所包括的区块链网络的标识，和/或数字证书的环签名对应的所有参与方的 CA 公钥，和/或上述所有参与方的 CA 公钥的标识；

其中，上述预设字段包括签发方标注字段和/或扩展字段。

在一些可行的实施方式中，上述环签名证书签发规则被记录于上述区块链网络中，上述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；上述 X509 中包括用于记录环签名的公钥信息的预设字段；

上述区块链网络中记录的上述各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

上述公钥信息包括上述预设字段中所包括的分组标识符，上述分组标识符用于确定上述区块链网络中所包括的目标分组，以基于上述目标分组中包括的 CA 公钥确定上述数字证书的环签名对应的所有参与方的 CA 公钥。

具体实现中，上述作为验证方的数字证书签发装置可通过其内置的各个功能单元执行上述各个实施例中验证方所执行的实现方式，包括但不限于上述步骤 S25 所提供的实现方式中验证方所执行的操作，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。

在本申请实施例中，验证方可根据联盟链网络中各个参与方制定的环签名证书签发规则确定环签名所需的公钥数量和环签名证书签发规范，并可基于联盟链网络中记录的各个参与方的 CA 公钥确定该数字证书的环签名对应的所有公钥。基于环签名对应的所有公钥实现对数字证书持有者发起的交易的验证，操作简单，完成交易的验证的同时也增强了数字证书的签发方的 CA 身份的私密性，可满足更多参与方的业务需求，适用性更强。

参见图 5，图 5 是本申请实施例提供的终端的一结构示意图。该终端适用于数字证书的签发方，该签发方可以是联盟链网络中的任一需要为自己的用户签发数字证书的参与方，具体可根据实际应用场景确定，在此不做限制。

如图 5 所示，本实施例中的终端可以包括：一个或多个处理器 501、存储器 502 和一个或多个收发器 503。上述处理器 501、存储器 502 和收发器 503 通过总线 504 连接。存储器 502 用于存储计算机程序，该计算机程序包括程序指令，处理器 501 和收发器 503 用于执行存储器 502 存储的程序指令。其中，上述处理器 501 和收发器 503 被配置用于调用该程序指令执行如下操作：

收发器 503，用于将第一参与方的 CA 公钥发送并记录至区块链网络中，上述第一参与方为上述区块链网络中数字证书的签发方，上述区块链网络中还记录了至少一个第二参与方的 CA 公钥，上述第二参与方为上述区块链网络中除上述第二参与方之外的参与方。

处理器 501，用于当上述收发器 503 接收到任一用户的证书授权请求时，根据上述证

书授权请求中携带的用户身份信息确认上述用户是否为上述第一参与方的 CA 的用户；若确认上述用户是上述第一参与方的 CA 的用户，则从上述证书授权请求中获取上述用户的公钥，并根据预先设定的环签名证书签发规则，从上述区块链网络中获取任意 N 个上述第二参与方的 CA 公钥，其中，N 等于上述环签名证书签发规则中设定的公钥数量。

处理器 501，还用于根据上述第一参与方的 CA 的公钥、私钥和上述 N 个上述第二参与方的 CA 公钥对上述用户的用户身份信息和公钥进行环签名并形成数字证书。

收发器 503，还用于向上述用户发送上述数字证书。

在一些可行的实施方式中，上述环签名证书签发规则由上述第一参与方的 CA 自行制定，或者由上述区块链网络中的各个参与方的 CA 共同制定；上述环签名证书签发规则被记录于上述区块链网络中。

在一些可行的实施方式中，上述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；上述 X509 中包括用于记录环签名的公钥信息的预设字段；

上述处理器 501 用于：

基于上述规范，使用上述第一参与方的 CA 的公钥、私钥和上述 N 个上述第二参与方的 CA 公钥对上述用户的用户身份信息和公钥进行环签名并形成数字证书，上述数字证书的上述预设字段中携带上述数字证书的环签名的公钥信息。

在一些可行的实施方式中，上述 X509 中包括签发方标注字段，上述签发方标注字段中包括上述第一参与方的 CA 对应的区块链网络标识和/或上述数字证书的环签名的公钥信息；

其中，上述公钥信息包括上述数字证书的环签名对应的上述 N 个上述第二参与方的 CA 公钥，和/或上述环签名对应的上述 N 个上述第二参与方的 CA 公钥的标识。

在一些可行的实施方式中，上述预设字段包括上述 X509 中的扩展字段，上述扩展字段中携带的上述环签名的公钥信息包括上述数字证书的环签名对应的上述 N 个上述第二参与方的 CA 公钥，和/或上述环签名对应的上述 N 个上述第二参与方的 CA 公钥的标识。

在一些可行的实施方式中，上述区块链网络中记录的各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

上述预设字段包括上述 X509 中的扩展字段，上述扩展字段中携带的上述环签名的公钥信息包括分组标识符，上述分组标识符用于指示上述环签名对应的上述 N 个上述第二参与方的 CA 公钥的所属分组，以帮助上述数字证书的验证方基于上述 N 个第二参与方的 CA 公钥的所属分组找到上述 N 个上述第二参与方的 CA 公钥。

在一些可行的实施方式中，上述处理器 501 可以是中央处理单元（central processing unit, CPU），该处理器还可以是其他通用处理器、数字信号处理器（digital signal processor, DSP）、专用集成电路（application specific integrated circuit, ASIC）、现成可编程门阵列（field-programmable gate array, FPGA）或者其他可编程逻辑器件、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。

该存储器 502 可以包括只读存储器和随机存取存储器，并向处理器 501 和收发器 503 提供指令和数据。存储器 502 的一部分还可以包括非易失性随机存取存储器。例如，存储器 502 还可以存储设备类型的信息。

在一些可行的实施方式中，上述终端可通过其内置的处理器 501 和收发器 503 各个功能模块执行如上述实施例中各个步骤所提供的实现方式中签发方的 CA 所执行的操作，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。

在本申请实施例中，作为数字证书签发方 CA 的终端可自行制定环签名证书签发规则，包括环签名所需的公钥数量以及环签名证书签发规范等。基于数字证书的签发方的 CA 自行制定的环签名证书签发规则，对签发方的 CA 的用户签发数字证书，可保证数字证书的签发方的 CA 之外的其他任意参与方的 CA 无法判断数字证书由哪个参与方的 CA 签发。也就是说联盟链网络中除了数字证书的签发方的 CA 之外的其他任意参与方的 CA 均无法判断该数字证书的接收方是联盟链中哪一个参与方的 CA 的客户，从而可实现联盟链中各个参与方的 CA 为其用户颁发数字证书的私密性，实现各个参与方的 CA 向其用户匿名发送数字证书，保证数字证书的签发方的 CA 的身份私密性，增强联盟链网络中各个参与方的 CA 与其用户之间的交易的信息安全性，可满足联盟链网络中各个参与方的更多业务需求，适用性更强。

参见图 6，图 6 是本申请实施例提供的终端的另一结构示意图。该终端适用于数字证书的验证方。如图 6 所示，本实施例中的终端可以包括：一个或多个处理器 601 和存储器 602。上述处理器 601 和存储器 602 通过总线 603 连接。存储器 602 用于存储计算机程序，该计算机程序包括程序指令，处理器 601 用于执行存储器 602 存储的程序指令。其中，上述处理器 601 被配置用于调用该程序指令执行如下操作：

当验证方获得区块链网络中的任一签名交易时，获取上述签名交易的发起方的数字证书，上述签名交易的发起方可以为上述区块链网络中的参与方之一，上述区块链网络中记录了包括上述交易的发起方在内的各个参与方的证书颁发机构 CA 公钥；

基于预设的环签名证书签发规则从上述数字证书中获取上述数字证书的环签名的公钥信息，并根据上述公钥信息确定上述数字证书的环签名对应的所有公钥，上述环签名对应的所有公钥为上述区块链网络中的多个参与方的 CA 公钥，上述多个参与方的参与方数量等于上述环签名证书签发规则中设定的公钥数量；

根据上述环签名对应的所有公钥对上述签名交易的签名进行验证。

在一些可行的实施方式中，上述环签名证书签发规则被记录于上述区块链网络中，上述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；上述 X509 中包括用于记录环签名的公钥信息的预设字段；

上述公钥信息包括上述预设字段中所包括的区块链网络的标识，和/或数字证书的环签名对应的所有参与方的 CA 公钥，和/或上述所有参与方的 CA 公钥的标识；

其中，上述预设字段包括签发方标注字段和/或扩展字段。

在一些可行的实施方式中，上述环签名证书签发规则被记录于上述区块链网络中，上述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；上述 X509 中包括用于记录环签名的公钥信息的预设字段；

上述区块链网络中记录的上述各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

上述公钥信息包括上述预设字段中所包括的分组标识符，上述分组标识符用于确定上述区块链网络中所包括的目标分组，以基于上述目标分组中包括的 CA 公钥确定上述数字证

书的环签名对应的所有参与方的 CA 公钥。

在一些可行的实施方式中，上述终端可通过其内置的处理器 601 等各个功能器件执行如上述实施例中各个步骤所提供的实现方式中验证方所执行的操作，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。

在本申请实施例中，作为数字证书验证方的终端，可根据联盟链网络中各个参与方的 CA 制定的环签名证书签发规则确定环签名所需的公钥数量和环签名证书签发规范，并可基于联盟链网络中记录的各个参与方的 CA 公钥确定该数字证书的环签名对应的所有公钥。基于环签名对应的所有公钥实现对数字证书持有者发起的交易验证，操作简单，完成交易验证的同时也增强了数字证书的签发方的 CA 的身份私密性，可满足更多参与方的业务需求，适用性更强。

本申请实施例还提供一种计算机可读存储介质，该计算机可读存储介质存储有计算机程序，该计算机程序包括程序指令，该程序指令被处理器执行时实现图 2 中各个步骤所提供的方法，具体可参见上述各个步骤所提供的实现方式，在此不再赘述。

上述计算机可读存储介质可以是前述任一实施例提供的数字证书签发装置或者上述终端的内部存储单元，例如电子设备的硬盘或内存。该计算机可读存储介质也可以是该电子设备的外部存储设备，例如该电子设备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，该计算机可读存储介质还可以既包括该电子设备的内部存储单元也包括外部存储设备。该计算机可读存储介质用于存储该计算机程序以及该电子设备所需的其他程序和数据。该计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

本申请的权利要求书和说明书及附图中的术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置展示该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。在本申请说明书和所附权利要求书中使用的术语“和/或”是指相关联列出的项中的一个或多个的任何组合以及所有可能组合，并且包括这些组合。

权利要求

1. 一种数字证书的签发方法，其特征在于，所述方法适用于数字证书的签发方，所述方法包括：

区块链网络的第一参与方的证书颁发机构 CA 将所述第一参与方的 CA 公钥记录至区块链网络中，所述第一参与方为所述区块链网络中数字证书的签发方，所述区块链网络中还记录了至少一个第二参与方的 CA 公钥，所述第二参与方为所述区块链网络中除所述第一参与方之外的参与方；

当所述第一参与方的 CA 接收到任一用户的证书授权请求时，根据所述证书授权请求中携带的用户身份信息确认所述用户是否为目标用户，所述目标用户为所述第一参与方的 CA 的用户；

若所述第一参与方的 CA 确认所述用户是目标用户，则从所述证书授权请求中获取所述用户的公钥，并根据预先设定的环签名证书签发规则，从所述区块链网络中获取任意 N 个所述第二参与方的 CA 公钥，其中，N 等于所述环签名证书签发规则中设定的公钥数量；

所述第一参与方的 CA 根据所述第一参与方的 CA 的公钥、私钥和所述 N 个所述第二参与方的 CA 公钥对所述用户的用户身份信息和公钥进行环签名并形成数字证书，并向所述用户发送所述数字证书。

2. 根据权利要求 1 所述的方法，其特征在于，所述环签名证书签发规则由所述第一参与方的 CA 自行制定，或者由所述区块链网络中的各个参与方的 CA 共同制定；所述环签名证书签发规则被记录于所述区块链网络中。

3. 根据权利要求 2 所述的方法，其特征在于，所述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；所述 X509 中包括用于记录环签名的公钥信息的预设字段；

所述第一参与方的 CA 根据所述第一参与方的 CA 的公钥、私钥和所述 N 个第二参与方的 CA 公钥对所述用户的用户身份信息和公钥进行环签名并形成数字证书包括：

所述第一参与方的 CA 基于所述规范，使用所述第一参与方的 CA 的公钥、私钥和所述 N 个所述第二参与方的 CA 公钥对所述用户的用户身份信息和公钥进行环签名并形成数字证书，所述数字证书的所述预设字段中携带所述数字证书的环签名的公钥信息。

4. 根据权利要求 3 所述的方法，其特征在于，所述 X509 中包括签发方标注字段，所述签发方标注字段中包括所述第一参与方的 CA 对应的区块链网络标识和/或所述数字证书的环签名的公钥信息；

其中，所述公钥信息包括所述数字证书的环签名对应的所述 N 个所述第二参与方的 CA 公钥，和/或所述环签名对应的所述 N 个所述第二参与方的 CA 公钥的标识。

5. 根据权利要求 3 所述的方法，其特征在于，所述预设字段包括所述 X509 中的扩展字段，所述扩展字段中携带的所述环签名的公钥信息包括所述数字证书的环签名对应的所述 N 个所述第二参与方的 CA 公钥，和/或所述环签名对应的所述 N 个所述第二参与方的 CA 公钥的标识。

6. 根据权利要求 3 所述的方法，其特征在于，所述区块链网络中记录的各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

所述预设字段包括所述 X509 中的扩展字段, 所述扩展字段中携带的所述环签名的公钥信息包括分组标识符, 所述分组标识符用于指示所述环签名对应的所述 N 个所述第二参与方的 CA 公钥的所属分组, 以帮助所述数字证书的验证方基于所述 N 个所述第二参与方的 CA 公钥的所属分组找到所述 N 个所述第二参与方的 CA 公钥。

7. 一种数字证书的验证方法, 其特征在于, 所述方法适用于数字证书的验证方, 所述方法包括:

当验证方获得区块链网络中的任一签名交易时, 所述验证方获取所述签名交易的发起方的数字证书;

所述验证方基于预设的环签名证书签发规则从所述数字证书中获取所述数字证书的环签名的公钥信息, 并根据所述公钥信息确定所述数字证书的环签名对应的所有公钥, 所述环签名对应的所有公钥为所述区块链网络中的多个参与方的 CA 公钥, 且所述环签名对应的公钥数量等于所述环签名证书签发规则中设定的公钥数量;

所述验证方根据所述环签名对应的所有公钥对所述签名交易的签名进行验证。

8. 根据权利要求 7 所述的方法, 其特征在于, 所述环签名证书签发规则被记录于所述区块链网络中, 所述环签名证书签发规则中还包括由 X509 的数字证书构成的规范; 所述 X509 中包括用于记录环签名的公钥信息的预设字段;

所述公钥信息包括所述预设字段中所包括的区块链网络的标识, 和/或数字证书的环签名对应的所有参与方的 CA 公钥, 和/或所述所有参与方的 CA 公钥的标识;

其中, 所述预设字段包括签发方标注字段和/或扩展字段。

9. 根据权利要求 7 所述的方法, 其特征在于, 所述环签名证书签发规则被记录于所述区块链网络中, 所述环签名证书签发规则中还包括由 X509 的数字证书构成的规范; 所述 X509 中包括用于记录环签名的公钥信息的预设字段;

所述区块链网络中记录的所述各个参与方的 CA 公钥分为多个分组, 且一个分组对应一个分组标识符;

所述公钥信息包括所述预设字段中所包括的分组标识符, 所述分组标识符用于确定所述区块链网络中所包括的目标分组, 以基于所述目标分组中包括的 CA 公钥确定所述数字证书的环签名对应的所有参与方的 CA 公钥。

10. 一种数字证书的签发装置, 其特征在于, 所述装置适用于数字证书的签发方的证书颁发机构 CA, 所述装置包括:

记录单元, 用于将第一参与方的 CA 公钥记录至区块链网络中, 所述第一参与方为所述区块链网络中数字证书的签发方, 所述区块链网络中还记录了至少一个第二参与方的 CA 公钥, 所述第二参与方为所述区块链网络中除所述第一参与方之外的参与方;

确认单元, 用于在接收到任一用户的证书授权请求时, 根据所述证书授权请求中携带的用户身份信息确认所述用户是否为所述第一参与方的 CA 的用户;

获取单元, 用于在所述确认单元确认所述用户是所述第一参与方的 CA 的用户时, 从所述证书授权请求中获取所述用户的公钥, 并根据预先设定的环签名证书签发规则, 从所述区块链网络中获取任意 N 个所述第二参与方的 CA 公钥, 其中, N 等于所述环签名证书签发规则中设定的公钥数量;

签发单元，用于根据所述第一参与方的 CA 的公钥、私钥和所述 N 个所述第二参与方的 CA 公钥对所述用户的用户身份信息和公钥进行环签名并形成数字证书，并向所述用户发送所述数字证书。

11. 根据权利要求 10 所述的装置，其特征在于，所述环签名证书签发规则由所述第一参与方的 CA 自行制定，或者由所述区块链网络中的各个参与方的 CA 共同制定；所述环签名证书签发规则被记录于所述区块链网络中。

12. 根据权利要求 11 所述的装置，其特征在于，所述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；所述 X509 中包括用于记录环签名的公钥信息的预设字段；

所述签发单元用于：

基于所述规范，使用所述第一参与方的 CA 的公钥、私钥和所述 N 个所述第二参与方的 CA 公钥对所述用户的用户身份信息和公钥进行环签名并形成数字证书，所述数字证书的所述预设字段中携带所述数字证书的环签名的公钥信息。

13. 根据权利要求 12 所述的装置，其特征在于，所述 X509 中包括签发方标注字段，所述签发方标注字段中包括所述第一参与方的 CA 对应的区块链网络标识和/或所述数字证书的环签名的公钥信息；

其中，所述公钥信息包括所述数字证书的环签名对应的所述 N 个所述第二参与方的 CA 公钥，和/或所述环签名对应的所述 N 个所述第二参与方的 CA 公钥的标识。

14. 根据权利要求 12 所述的装置，其特征在于，所述预设字段包括所述 X509 中的扩展字段，所述扩展字段中携带的所述环签名的公钥信息包括所述数字证书的环签名对应的所述 N 个所述第二参与方的 CA 公钥，和/或所述环签名对应的所述 N 个所述第二参与方的 CA 公钥的标识。

15. 根据权利要求 12 所述的装置，其特征在于，所述区块链网络中记录的各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

所述预设字段包括所述 X509 中的扩展字段，所述扩展字段中携带的所述环签名的公钥信息包括分组标识符，所述分组标识符用于指示所述环签名对应的所述 N 个所述第二参与方的 CA 公钥的所属分组，以帮助所述数字证书的验证方基于所述 N 个所述第二参与方的 CA 公钥的所属分组找到所述 N 个所述第二参与方的 CA 公钥。

16. 一种数字证书的验证装置，其特征在于，所述装置适用于数字证书的验证方，所述装置包括：

获取单元，用于在获得区块链网络中的任一签名交易时，获取所述交易的发起方的数字证书；

确定单元，用于基于预设的环签名证书签发规则从所述数字证书中获取所述数字证书的环签名的公钥信息，并根据所述公钥信息确定所述数字证书的环签名对应的所有公钥，所述环签名对应的所有公钥为所述区块链网络中的多个参与方的 CA 公钥，且所述环签名对应的公钥数量等于所述环签名证书签发规则中设定的公钥数量；

验证单元，用于根据所述确定单元确定的所述环签名对应的所有公钥对所述交易的签名进行验证。

17. 根据权利要求 16 所述的装置，其特征在于，所述环签名证书签发规则被记录于所

述区块链网络中，所述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；所述 X509 中包括用于记录环签名的公钥信息的预设字段；

所述公钥信息包括所述预设字段中所包括的区块链网络的标识，和/或数字证书的环签名对应的所有参与方的 CA 公钥，和/或所述所有参与方的 CA 公钥的标识；

其中，所述预设字段包括签发方标注字段和/或扩展字段。

18. 根据权利要求 16 所述的装置，其特征在于，所述环签名证书签发规则被记录于所述区块链网络中，所述环签名证书签发规则中还包括由 X509 的数字证书构成的规范；所述 X509 中包括用于记录环签名的公钥信息的预设字段；

所述区块链网络中记录的所述各个参与方的 CA 公钥分为多个分组，且一个分组对应一个分组标识符；

所述公钥信息包括所述预设字段中所包括的分组标识符，所述分组标识符用于确定所述区块链网络中所包括的目标分组，以基于所述目标分组中包括的 CA 公钥确定所述数字证书的环签名对应的所有参与方的 CA 公钥。

19. 一种终端，其特征在于，包括处理器和存储器，所述处理器、收发器和存储器相互连接，其中，所述存储器用于存储计算机程序，所述计算机程序包括程序指令，所述处理器和所述收发器被配置用于调用所述程序指令，执行如权利要求 1-6 任一项所述的方法，或者如权利要求 7-9 任一项所述的方法。

20. 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存储有计算机程序，所述计算机程序包括程序指令，所述程序指令当被处理器执行时使所述处理器执行如权利要求 1-6 任一项所述的方法，或者如权利要求 7-9 任一项所述的方法。