(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 107508680 B
(45)授权公告日 2021.02.05

(21)申请号 201710617611.4
(22)申请日 2017.07.26
(65)同一申请的已公布的文献号
申请公布号 CN 107508680 A
(43)申请公布日 2017.12.22
(73)专利权人 创新先进技术有限公司
地址 开曼群岛大开曼岛西湾路802号木槿街大展览馆31119号邮箱
(72)发明人 邱鸿霖
(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 许振新
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 29/06(2006.01)

审查员 郑杰

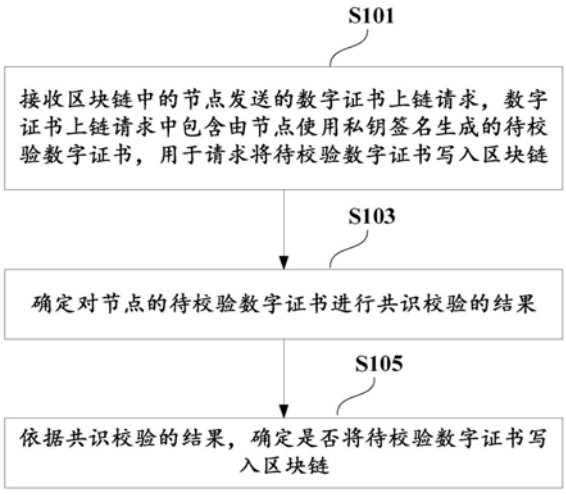
权利要求书5页 说明书15页 附图7页

(54)发明名称

数字证书管理方法、装置及电子设备

(57)摘要

本申请公开了一种数字证书管理方法，包括：接收区块链中的节点发送的数字证书上链请求，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链；确定对所述节点的待校验数字证书进行共识校验的结果；依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链。本申请还公开了相对应的装置和电子设备等。



CN 107508680 B

1.一种数字证书管理方法,包括:

接收区块链中的节点发送的数字证书上链请求,所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书,用于请求将所述待校验数字证书写入所述区块链,其中,所述私钥为所述区块链中公开的私钥;

确定对所述节点的待校验数字证书进行共识校验的结果;

依据共识校验的结果,确定是否将所述待校验数字证书写入所述区块链;

所述确定对所述节点的待校验数字证书进行共识校验的结果,包括:

当参与共识校验的节点的数量达到预设数值时,根据所述参与共识校验的节点的数量以及第一节点的数量,确定对所述节点的待校验数字证书进行共识校验的结果,所述第一节点为校验结果为通过共识校验的节点,所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

2.根据权利要求1所述方法,确定对所述节点的待校验数字证书进行共识校验的结果,包括:

确定所述区块链中参与共识校验的节点的校验结果;

确定所述参与共识校验的节点中第一节点的数量和/或第二节点的数量;其中,所述第一节点的校验结果为通过共识校验,所述第二节点的校验结果为未通过共识校验;

依据所述第一节点的数量和/或第二节点的数量确定共识校验的结果。

3.根据权利要求2所述方法,依据所述第一节点的数量确定共识校验的结果,包括:

当所述第一节点的数量满足第一预设条件时,确定共识校验的结果为通过共识校验;

满足所述第一预设条件包括以下一项或多项:

所述第一节点的数量达到第一预设阈值;

所述第一节点的数量与所述参与共识校验的节点的数量的比值达到第二预设阈值;

所述第一节点的数量与所述区块链的节点的数量的比值达到第三预设阈值。

4.根据权利要求3所述方法,依据共识校验的结果,确定是否将所述待校验数字证书写入所述区块链,包括:

当所述共识校验的结果为通过共识校验时,将所述待校验数字证书写入所述区块链。

5.根据权利要求1～4之任一所述方法,还包括:

接收所述区块链中的节点发送的数字证书吊销请求,所述数字证书吊销请求中包含请求吊销的目标节点的数字证书;

确定对所述目标节点的数字证书进行共识校验的结果;

依据共识校验的结果,确定是否吊销所述目标节点的数字证书。

6.一种数字证书管理方法,包括:

接收区块链中的节点发送的数字证书吊销请求,所述数字证书吊销请求中包含由所述节点使用私钥签名生成的请求吊销的目标节点的数字证书,其中,所述私钥为所述区块链中公开的私钥;所述数字证书是由区块链中的节点使用私钥签名生成并通过共识校验的数字证书;

确定对所述目标节点的数字证书进行共识校验的结果;

依据共识校验的结果,确定是否在所述区块链中吊销所述目标节点的数字证书;

所述确定对所述目标节点的数字证书进行共识校验的结果,包括:

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述目标节点的数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

7.根据权利要求6所述方法，确定对所述目标节点的数字证书进行共识校验的结果，包括：

确定所述区块链中参与共识校验的节点的校验结果；

确定所述参与共识校验的节点中第一节点的数量和/或第二节点的数量；其中，所述第一节点的校验结果为通过共识校验，所述第二节点的校验结果为未通过共识校验；

依据所述第一节点的数量和/或第二节点的数量确定共识校验的结果。

8.根据权利要求7所述方法，依据所述第一节点的数量确定共识校验的结果，包括：

当所述第一节点的数量满足第一预设条件时，确定共识校验的结果为通过共识校验；

满足所述第一预设条件包括以下一项或多项：

所述第一节点的数量达到第一预设阈值；

所述第一节点的数量与所述参与共识校验的节点的数量的比值达到第二预设阈值；

所述第一节点的数量与所述区块链的节点的数量的比值达到第三预设阈值。

9.根据权利要求7所述方法，依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书，包括：

当所述共识校验的结果为通过共识校验时，在所述区块链中吊销所述目标节点的数字证书。

10.一种数字证书管理方法，包括：

区块链中的节点向区块链中发送数字证书上链请求，用于供所述区块链确定对所述节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；

其中，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链，所述私钥为所述区块链中公开的私钥；

所述确定对所述节点的待校验数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述节点的待校验数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

11.一种数字证书管理方法，包括：

区块链中的节点向区块链中发送数字证书吊销请求，用于供所述区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书，所述数字证书是由区块链中的节点使用私钥签名生成并通过共识校验的数字证书，所述私钥为所述区块链中公开的私钥；

其中，所述数字证书吊销请求中包含请求吊销的所述目标节点的数字证书；

所述确定对目标节点的数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对目标节点的数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

12.一种数字证书管理装置，用于区块链，包括：

请求接收模块，接收区块链中的节点发送的数字证书上链请求，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链，其中，所述私钥为所述区块链中公开的私钥；

共识校验结果确定模块，确定对所述节点的待校验数字证书进行共识校验的结果；

证书管理模块，依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；

所述确定对所述节点的待校验数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述节点的待校验数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

13.一种电子设备，用于区块链，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

接收区块链中的节点发送的数字证书上链请求，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链，其中，所述私钥为所述区块链中公开的私钥；

确定对所述节点的待校验数字证书进行共识校验的结果；

依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；

所述确定对所述节点的待校验数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述节点的待校验数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

14.一种数字证书管理装置，用于区块链，包括：

请求接收模块，接收区块链中的节点发送的数字证书吊销请求，所述数字证书吊销请求中包含由所述节点使用私钥签名生成的请求吊销的目标节点的数字证书，其中，所述私钥为所述区块链中公开的私钥；所述数字证书是由区块链中的节点使用私钥签名生成并通过共识校验的数字证书；

共识校验结果确定模块，确定对所述目标节点的数字证书进行共识校验的结果；

证书管理模块，依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书；

所述确定对所述目标节点的数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述目标节点的数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

15.一种电子设备，用于区块链，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

接收区块链中的节点发送的数字证书吊销请求，所述数字证书吊销请求中包含由所述节点使用私钥签名生成的请求吊销的目标节点的数字证书，其中，所述私钥为所述区块链中公开的私钥；所述数字证书是由区块链中的节点使用私钥签名生成并通过共识校验的数字证书；

确定对所述目标节点的数字证书进行共识校验的结果；

依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书；

所述确定对所述目标节点的数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述目标节点的数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

16.一种数字证书管理装置，用于区块链中的节点，包括：

请求发起模块，向区块链中发送数字证书上链请求，用于供所述区块链确定对所述节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；其中，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链，所述私钥为所述区块链中公开的私钥；

所述确定对所述节点的待校验数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述节点的待校验数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

17.一种电子设备，用于区块链中的节点，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

向区块链中发送数字证书上链请求，用于供所述区块链确定对所述节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；其中，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链，所述私钥为所述区块链中公开的私钥；

所述确定对所述节点的待校验数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对所述节点的待校验数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

18.一种数字证书管理装置，用于区块链中的节点，包括：

请求发起模块，向区块链中发送数字证书吊销请求，用于供所述区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书，所述数字证书是由区块链中的节点使用私钥签名生成并通过共识校验的数字证书，所述私钥为所述区块链中公开的私钥；其中，所述数字证书吊销请求中包含请求吊销的所述目标节点的数字证书；

所述确定对目标节点的数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对目标节点的数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节。

19.一种电子设备，用于区块链中的节点，包括：

处理器；以及

被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

向区块链中发送数字证书吊销请求，用于供所述区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书，所述数字证书是由区块链中的节点使用私钥签名生成并通过共识校验的数字证书，所述私钥为所述区块链中公开的私钥；其中，所述数字证书吊销请求中包含请求吊销的所述目标节点的数字证书；

所述确定对目标节点的数字证书进行共识校验的结果，包括：

当参与共识校验的节点的数量达到预设数值时，根据所述参与共识校验的节点的数量以及第一节点的数量，确定对目标节点的数字证书进行共识校验的结果，所述第一节点为校验结果为通过共识校验的节点，所述参与共识校验的节点为区块链中接收速度快且响应速度快的节点。

数字证书管理方法、装置及电子设备

技术领域

[0001] 本申请涉及计算机技术领域，尤其涉及数字证书管理的方法、装置及电子设备。

背景技术

[0002] 随着计算机技术的发展，区块链技术(又称分布式账本技术)以其去中心化、公开透明、不可篡改、可信任等优点，备受青睐，在智能合约、证券交易、电子商务、物联网、社交通讯、文件存储、存在性证明、身份验证、股权众筹等众多领域得到广泛应用。

[0003] 目前，区块链系统主要可分为三类，分别是公有链(Public Blockchain)、私有链(Private Blockchain)和联盟链(Consortium Blockchain)。这三类区块链的主要区别在于开放对象的不同。公有链可对所有人开放，私有链仅对单独的个人或实体组织开放，而联盟链介于公有链和私有链之间，对特定的个人或实体组织开放，而对之外的其他个人或实体组织加以限制。

[0004] 在区块链中，尤其是在面向特定组织的联盟链中，为了提高通讯安全，通常会设计证书授权中心(全称Certificate Authority，可简称为CA中心)，为每个参与区块链通讯的节点签发节点证书，使得持有合法证书的节点才能够互相通讯。在现有技术中，会将签发的节点证书以及与证书有效性有关的信息，例如证书吊销列表等，都存储在CA中心的服务器中；区块链的节点间需要通讯时，也将调用并查询CA中心存储的与证书有效性有关的信息，以便确认证书的有效性，完成对通讯过程的验证。这种方式的主要缺陷在于：

[0005] 节点的数字证书以及与证书有效性有关的信息均存储在CA中心，一旦CA中心被黑，黑客可以任意修改与证书有效性有关的信息，例如，可以篡改证书吊销列表，使得已吊销的证书恢复正常。黑客进而可以利用这些原本被吊销的问题证书非法加入区块链，区块链节点在确认证书有效性时也将依据被篡改的信息进行，从而对区块链的安全造成威胁。更有甚者，CA中心的私钥也可能被黑客盗取，进而黑客可以恣意签发数字证书，威胁着区块链网络的安全。

发明内容

[0006] 本申请实施例提供数字证书管理方法、装置及相应的电子设备，旨在提高区块链网络的安全性。

[0007] 本申请实施例采用下述技术方案：

[0008] 第一方面，本申请实施例提供一种数字证书管理方法，包括：

[0009] 接收区块链中的节点发送的数字证书上链请求，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链；

[0010] 确定对所述节点的待校验数字证书进行共识校验的结果；

[0011] 依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链。

[0012] 优选的，在第一方面提供的数字证书管理方法中，确定对所述节点的待校验数字

证书进行共识校验的结果，包括：

[0013] 确定所述区块链中参与共识校验的节点的校验结果；

[0014] 确定所述参与共识校验的节点中第一节点的数量和/或第二节点的数量；其中，所述第一节点的校验结果为通过共识校验，所述第二节点的校验结果为未通过共识校验；

[0015] 依据所述第一节点的数量和/或第二节点的数量确定共识校验的结果。

[0016] 优选的，在第一方面提供的数字证书管理方法中，依据所述第一节点的数量确定共识校验的结果，包括：

[0017] 当所述第一节点的数量满足第一预设条件时，确定共识校验的结果为通过共识校验；

[0018] 满足所述第一预设条件包括以下一项或多项：

[0019] 所述第一节点的数量达到第一预设阈值；

[0020] 所述第一节点的数量与所述参与共识校验的节点的数量的比值达到第二预设阈值；

[0021] 所述第一节点的数量与所述区块链的节点的数量的比值达到第三预设阈值。

[0022] 优选的，在第一方面提供的数字证书管理方法中，依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链，包括：

[0023] 当所述共识校验的结果为通过共识校验时，将所述待校验数字证书写入所述区块链。

[0024] 优选的，在第一方面提供的数字证书管理方法中，所述方法还包括：

[0025] 接收所述区块链中的节点发送的数字证书吊销请求，所述数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0026] 确定对所述目标节点的数字证书进行共识校验的结果；

[0027] 依据共识校验的结果，确定是否吊销所述目标节点的数字证书。

[0028] 第二方面，本申请实施例提供一种数字证书管理方法，包括：

[0029] 接收区块链中的节点发送的数字证书吊销请求，所述数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0030] 确定对所述目标节点的数字证书进行共识校验的结果；

[0031] 依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书。

[0032] 优选的，在第二方面提供的数字证书管理方法中，确定对所述目标节点的数字证书进行共识校验的结果，包括：

[0033] 确定所述区块链中参与共识校验的节点的校验结果；

[0034] 确定所述参与共识校验的节点中第一节点的数量和/或第二节点的数量；其中，所述第一节点的校验结果为通过共识校验，所述第二节点的校验结果为未通过共识校验；

[0035] 依据所述第一节点的数量和/或第二节点的数量确定共识校验的结果。

[0036] 优选的，在第二方面提供的数字证书管理方法中，依据所述第一节点的数量确定共识校验的结果，包括：

[0037] 当所述第一节点的数量满足第一预设条件时，确定共识校验的结果为通过共识校验；

[0038] 满足所述第一预设条件包括以下一项或多项：

[0039] 所述第一节点的数量达到第一预设阈值；

[0040] 所述第一节点的数量与所述参与共识校验的节点的数量的比值达到第二预设阈值；

[0041] 所述第一节点的数量与所述区块链的节点的数量的比值达到第三预设阈值。

[0042] 优选的，在第二方面提供的数字证书管理方法中，依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书，包括：

[0043] 当所述共识校验的结果为通过共识校验时，在所述区块链中吊销所述目标节点的数字证书。

[0044] 第三方面，本申请实施例提供一种数字证书管理方法，包括：

[0045] 区块链中的节点向区块链中发送数字证书上链请求，用于供所述区块链确定对所述节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；

[0046] 其中，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链。

[0047] 第四方面，本申请实施例提供一种数字证书管理方法，包括：

[0048] 区块链中的节点向区块链中发送数字证书吊销请求，用于供所述区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书；

[0049] 其中，所述数字证书吊销请求中包含请求吊销的所述目标节点的数字证书。

[0050] 第五方面，本申请实施例提供一种数字证书管理装置，用于区块链，包括：

[0051] 请求接收模块，接收区块链中的节点发送的数字证书上链请求，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链；

[0052] 共识校验结果确定模块，确定对所述节点的待校验数字证书进行共识校验的结果；

[0053] 证书管理模块，依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链。

[0054] 第六方面，本申请实施例提供一种电子设备，用于区块链，包括：

[0055] 处理器；以及

[0056] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[0057] 接收区块链中的节点发送的数字证书上链请求，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链；

[0058] 确定对所述节点的待校验数字证书进行共识校验的结果；

[0059] 依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链。

[0060] 第七方面，本申请实施例提供一种数字证书管理装置，用于区块链，包括：

[0061] 请求接收模块，接收区块链中的节点发送的数字证书吊销请求，所述数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0062] 共识校验结果确定模块，确定对所述目标节点的数字证书进行共识校验的结果；

[0063] 证书管理模块，依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书。

[0064] 第八方面，本申请实施例提供一种电子设备，用于区块链，包括：

[0065] 处理器；以及

[0066] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[0067] 接收区块链中的节点发送的数字证书吊销请求，所述数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0068] 确定对所述目标节点的数字证书进行共识校验的结果；

[0069] 依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书。

[0070] 第九方面，本申请实施例提供一种数字证书管理装置，用于区块链中的节点，包括：

[0071] 请求发起模块，向区块链中发送数字证书上链请求，用于供所述区块链确定对所述节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；其中，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链。

[0072] 第十方面，本申请实施例提供一种电子设备，用于区块链中的节点，包括：

[0073] 处理器；以及

[0074] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[0075] 向区块链中发送数字证书上链请求，用于供所述区块链确定对所述节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将所述待校验数字证书写入所述区块链；其中，所述数字证书上链请求中包含由所述节点使用私钥签名生成的待校验数字证书，用于请求将所述待校验数字证书写入所述区块链。

[0076] 第十一方面，本申请实施例提供一种数字证书管理装置，用于区块链中的节点，包括：

[0077] 请求发起模块，向区块链中发送数字证书吊销请求，用于供所述区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书；其中，所述数字证书吊销请求中包含请求吊销的所述目标节点的数字证书。

[0078] 第十二方面，本申请实施例提供一种电子设备，用于区块链中的节点，包括：

[0079] 处理器；以及

[0080] 被安排成存储计算机可执行指令的存储器，所述可执行指令在被执行时使所述处理器执行以下操作：

[0081] 向区块链中发送数字证书吊销请求，用于供所述区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在所述区块链中吊销所述目标节点的数字证书；其中，所述数字证书吊销请求中包含请求吊销的所述目标节点的数字证书。

[0082] 本申请实施例采用的上述至少一个技术方案能够达到以下有益效果：

[0083] 采用本申请实施例的方案，将传统的CA中心的功能改由区块链实现，当区块链中的某节点需要申请数字证书时，可以使用区块链内部私钥自行签名，生成待校验的数字证书，进一步经过区块链网络进行共识校验通过之后入链，方才成为合法有效的数字证书。这一系列数字证书签发、验证、存储的过程均在区块链中进行。

[0084] 由于在本申请实施例中，需要经过共识校验的数字证书才能入链，而只有入链的数字证书才是合法的数字证书，因此，即使某一节点被黑客攻击，或者黑客取得了CA私钥可以随意签发数字证书，黑客也无法在区块链中取得合法的数字证书，从而无法加入区块链网络进行非法通讯。因此，基于区块链去中心化、公开透明、不可篡改等优点，采用这种去中心化的架构对数字证书进行管理，提高了区块链网络的安全性。

附图说明

[0085] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0086] 图1为本申请实施例中一种数字证书管理方法的流程示意图；

[0087] 图2为本申请实施例中第二种数字证书管理方法的流程示意图；

[0088] 图3为本申请实施例中第三种数字证书管理方法的流程示意图；

[0089] 图4为本申请实施例的实施场景示意图；

[0090] 图5为本申请实施例中一种数字证书管理装置的流程示意图；

[0091] 图6为本申请实施例中一种电子设备的流程示意图；

[0092] 图7为本申请实施例中第二种数字证书管理装置的流程示意图；

[0093] 图8为本申请实施例中第二种电子设备的流程示意图；

[0094] 图9为本申请实施例中第三种数字证书管理装置的流程示意图；

[0095] 图10为本申请实施例中第三种电子设备的流程示意图；

[0096] 图11为本申请实施例中第四种数字证书管理装置的流程示意图；

[0097] 图12为本申请实施例中第四种电子设备的流程示意图。

具体实施方式

[0098] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例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。

[0099] 以下结合附图，详细说明本申请各实施例提供的技术方案。

[0100] 参见图1所示，本申请实施例提供了一种数字证书管理方法，包括：

[0101] S101：接收区块链中的节点发送的数字证书上链请求，数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书，用于请求将待校验数字证书写入区块链；

[0102] S103：确定对节点的待校验数字证书进行共识校验的结果；

[0103] S105：依据共识校验的结果，确定是否将待校验数字证书写入区块链。

[0104] 可以理解到，上述区块链中发送数字证书上链请求的节点，可以是区块链中希望

申请数字证书的任一节点。在本申请实施例中，该节点可以使用在区块链中公开的私钥自行签名，生成待校验数字证书，进而向区块链发送包含有该待校验数字证书的数字证书上链请求，以便请求区块链将该待校验数字证书写入区块链。在具体实施时，该节点可以采用全网广播的方式发送上述数字证书上链请求。

[0105] 上述节点的自行签发的待校验数字证书，虽然在入链之前并未生效，但其在内容和形式上可以与合法生效的数字证书没有本质区别。在本申请实施例中，可体现为标志通讯节点身份信息的一串数字，可以携带包含证书版本号、证书持有者信息(例如，可以具体体现为证书所对应的节点的身份信息)、证书签发者信息(此处可以与证书持有者信息相同，也可以反映私钥的来源)、证书起止有效期、证书序列号、证书签发者的签名等内容。

[0106] 由于上述节点自行签发的待校验数字证书并未生效，而只有写入了区块链的数字证书才是合法的数字证书，合法的数字证书对应的节点才能够正常的参与区块链的通讯，因此，在本申请实施例中，即使公开了签发证书所需的私钥，也不会造成数字证书管理的混乱，不会影响区块链网络的安全。相反的，合法的数字证书经由区块链执行以下步骤S103进行全网共识校验后产生，提高了区块链网络的安全性。

[0107] 区块链在接收到上述数字证书上链请求后，可以对该请求进行解析，得到该请求中包含的待校验数字证书。而后对该节点的待校验数字证书进行共识校验。所谓共识校验，可以理解为区块链上的各节点都可以参与对待校验数字证书的校验，按照区块链的共识机制确定共识校验的结果。

[0108] 区块链上的各节点在具体实施校验时，可以按照预先约定的校验标准进行。校验的内容可以与待校验数字证书中的信息相关，例如：有效期是否过期，序列号是否符合要求，申请节点的身份信息是否符合要求等等。

[0109] 由于点对点网络下可能存在的网络延迟，区块链中各个节点接收到数字证书上链请求的时间及对该请求的响应速度可能不一样，因此，在区块链中接收速度和响应速度快的节点将有更多的机会参与对待校验数字证书的共识校验。

[0110] 区块链上参与共识校验的节点在完成对待校验数字证书的校验后，可以采用全网广播的方式将校验的结果发送到区块链(可具体为区块链中的各节点)。与之相对应地，区块链在执行步骤S103确定对节点的待校验数字证书进行共识校验的结果时，参见图2所示，可以具体包括：

[0111] S301：确定区块链中参与共识校验的节点的校验结果；

[0112] 可以理解到，校验结果可能为“通过共识校验”，也可能为“未通过共识校验”。除此之外，执行这一步骤的时机，可以是自广播待校验数字证书起算的预设时间之后，可以是共识校验开始后实时进行，也可以是周期性的确定，还可以是当参与共识校验的节点的数量达到预设数值时进行。在本申请实施例中，为得到满足区块链的共识机制的共识校验结果，步骤S301～S305中，各步骤自身、以及组合，都可能会循环执行多次，本申请实施例对此不做限定。

[0113] S303：确定参与共识校验的节点中第一节点的数量和/或第二节点的数量；其中，第一节点的校验结果为通过共识校验，第二节点的校验结果为未通过共识校验；

[0114] 具体地，在参与共识校验的节点将各自的校验结果广播公告之后，可按照校验结果的不同，将这些节点区分为校验结果为“通过共识校验”的第一节点和校验结果为“未通

过共识校验”的第二节点。在此基础上，可以择一或同时统计校验结果不同的两种节点的数量，以便判断是否达到共识机制所约定的确定共识校验结果的条件。

[0115] 在确定节点的数量时，可以统计节点的绝对数量，例如，假设参与共识校验的节点共10个，其中，第一节点有4个，第二节点有6个。也可以按照节点在共识校验过程中的权重不同(具体权重可以由区块链的共识机制确定)，统计节点的加权数量，例如，假设参与共识校验的节点共4个，其中，第一节点和第二节点的绝对数量相同，均为2个；2个第一节点的权重分别为0.5和1.2，2个第二节点的权重分别为2和4；则第一节点的数量的计算表达式为：1*0.5+1*1.2＝1.7，第二节点的数量的计算表达式为1*2+1*4＝6。

[0116] S305：依据第一节点的数量和/或第二节点的数量确定共识校验的结果。

[0117] 可以理解到，依据区块链的共识机制的不同，既可以依据校验结果为“通过共识校验”的第一节点的数量确定共识校验的结果，也可以依据校验结果为“未通过共识校验”的第二节点的数量确定，还可以同时依据这两种节点的数量确定。本申请实施例中对此不做限定。

[0118] 若依据第一节点的数量确定共识校验的结果，可以考察第一节点的数量是否满足以下一项或多项条件：

[0119] 第一节点的数量达到第一预设阈值；

[0120] 第一节点的数量与参与共识校验的节点的数量的比值达到第二预设阈值；

[0121] 第一节点的数量与区块链的节点的数量的比值达到第三预设阈值。

[0122] 可以理解到，根据区块链中共识机制的不同，可以预设不同的条件以确定共识校验的结果。以上例举的三方面判断，都能反映第一节点的数量达到了一定的程度，表示已有足够多(依据共识机制的设计不同，具体的标准可以不同)的区块链节点对待校验数字证书的校验结果为“通过共识校验”。因此，若满足以上条件，则可认为共识校验的结果为“通过共识校验”，这一结果可以理解为区块链中达到足够数量要求的节点认为请求入链的待校验数字证书是合法的，从而可进一步将待校验数字证书写入区块链，以便将这一合法的数字证书存储在区块链中，使得该数字证书对应的节点能够在区块链中正常通讯。

[0123] 若依据第二节点的数量确定共识校验的结果，则若有足够多(类似地，依据共识机制的设计不同，具体的标准可以不同)的节点对待校验数字证书的校验结果为“未通过共识校验”，表示区块链中达到足够数量要求的节点认为请求入链的待校验数字证书是不合法的。因此，该待校验数字证书不能写入区块链成为合法的数字证书，相应地，该待校验数字证书所对应的节点也无法参与区块链网络的通讯。可以理解到，依据第二节点的数量确定共识校验的结果的具体标准可以与前述举例类似，由区块链的共识机制的设计决定，此处不再赘述。

[0124] 与以上区块链一侧执行的实施例相对应地，本申请实施例还提供了一种数字证书管理方法，由申请数字证书的节点一侧执行，具体可包括：

[0125] 区块链中的节点向区块链中发送数字证书上链请求，用于供区块链确定对节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将待校验数字证书写入区块链；

[0126] 其中，数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书，用于请求将待校验数字证书写入区块链。

[0127] 以上区块链一侧执行的实施例中的相关阐述均适用于此处，不再赘述。

[0128] 采用本申请实施例对数字证书的管理，除了体现在数字证书的签发、校验和入链的过程之外，还可以进行数字证书的吊销。具体地，本申请实施例还提供了一种数字证书管理方法，可以采用以下步骤实现对已经入链的合法的数字证书进行吊销，参见图3所示：

[0129] S201：接收区块链中的节点发送的数字证书吊销请求，数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0130] S203：确定对目标节点的数字证书进行共识校验的结果；

[0131] S205：依据共识校验的结果，确定是否吊销目标节点的数字证书。

[0132] 具体地，步骤S203确定对目标节点的数字证书进行共识校验的结果，可以具体包括：

[0133] 确定区块链中参与共识校验的节点的校验结果；

[0134] 确定参与共识校验的节点中第一节点的数量和/或第二节点的数量；其中，第一节点的校验结果为通过共识校验，第二节点的校验结果为未通过共识校验；

[0135] 依据第一节点的数量和/或第二节点的数量确定共识校验的结果。

[0136] 更进一步地，依据第一节点的数量确定共识校验的结果，可以包括：

[0137] 当第一节点的数量满足第一预设条件时，确定共识校验的结果为通过共识校验；

[0138] 满足第一预设条件包括以下一项或多项：

[0139] 第一节点的数量达到第一预设阈值；

[0140] 第一节点的数量与参与共识校验的节点的数量的比值达到第二预设阈值；

[0141] 第一节点的数量与区块链的节点的数量的比值达到第三预设阈值。

[0142] 当以上共识校验的结果为通过共识校验时，在区块链中吊销目标节点的数字证书。

[0143] 可以理解到，对于区块链中各节点而言，均可发起数字证书吊销请求，既可以请求吊销自己的数字证书，也可以请求吊销其他问题节点的数字证书，此处无需限定。并且，不难理解到，数字证书吊销请求中，除包含请求吊销的目标节点的数字证书之外，还可以包含吊销该目标节点的数字证书的原因，以便区块链中各节点参与共识校验时判断是否通过共识校验。

[0144] 需要说明的是，在针对数字证书吊销请求进行共识校验时，发起数字证书吊销请求的节点与上述目标节点，均可能参与共识校验的过程。而在针对数字证书上链请求进行共识校验时，发起该请求的节点将无法参与共识校验的过程，因为该节点尚未取得合法的数字证书，无法加入区块链网络。

[0145] 还需要说明的是，在针对数字证书吊销请求进行共识校验时，第一节点的校验结果为“通过共识校验”，表示第一节点同意吊销目标节点的数字证书；第二节点的校验结果为“未通过共识校验”，表示第二节点不同意吊销目标节点的数字证书。上述实施例可以在此基础上，依据第一节点的数量和/或第二节点的数量确定共识校验的结果，以便确定是否吊销目标节点的数字证书。具体地确定共识校验的结果的过程，与对待校验数字证书的共识校验类似，具体的标准由共识机制确定，此处不再赘述。

[0146] 与图3所示区块链一侧执行的实施例相对应地，本申请实施例还提供了一种数字证书管理方法，由申请数字证书的节点一侧执行，具体可包括：

[0147] 区块链中的节点向区块链中发送数字证书吊销请求，用于供区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在区块链中吊销目标节点的数字证书；

[0148] 其中，数字证书吊销请求中包含请求吊销的目标节点的数字证书。

[0149] 以上区块链一侧执行的实施例中的相关阐述均适用于此处，不再赘述。

[0150] 图4简化的呈现出了区块链网络中在数字证书管理中的信息交互过程。以签发、校验、上链数字证书的过程为例，具体包括以下步骤：

[0151] S11：节点4作为发起节点，使用公开的私钥为自己签名，生成待校验的数字证书；

[0152] S12：节点4将生成的待校验数字证书广播到区块链中；

[0153] S13：节点1、节点2和节点3先后参与对待校验数字证书的共识校验；若共识校验的结果为“通过共识校验”，则区块链中各节点(不限于节点1～4)将节点4的待校验数字证书作为合法有效的数字证书入链。至此，节点4取得合法有效的数字证书，能够正常的参与区块链网络的通讯。

[0154] 可以理解到，对数字证书进行吊销的过程与之类似，主要区别在于，发起的节点发送的请求由数字证书上链请求改变为数字证书吊销请求。此处不再赘述。

[0155] 采用本申请实施例的方案，将传统的CA中心的功能改由区块链实现，当区块链中的某节点需要申请数字证书时，可以使用区块链内部私钥自行签名，生成待校验的数字证书，进一步经过区块链网络进行共识校验通过之后入链，方才成为合法有效的数字证书。这一系列数字证书签发、验证、存储的过程均在区块链中进行。数字证书的吊销过程也可在区块链中进行。

[0156] 由于在本申请实施例中，需要经过共识校验的数字证书才能入链，而只有入链的数字证书才是合法的数字证书，因此，即使某一节点被黑客攻击，或者黑客取得了CA私钥可以随意签发数字证书，黑客也无法在区块链中取得合法的数字证书，从而无法加入区块链网络进行非法通讯。因此，基于区块链去中心化、公开透明、不可篡改等优点，采用这种去中心化的架构对数字证书进行管理，提高了区块链网络的安全性。

[0157] 参见图5所示，本申请实施例还提供一种数字证书管理装置，用于区块链，包括：

[0158] 请求接收模块101，接收区块链中的节点发送的数字证书上链请求，数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书，用于请求将待校验数字证书写入区块链；

[0159] 共识校验结果确定模块103，确定对节点的待校验数字证书进行共识校验的结果；

[0160] 证书管理模块105，依据共识校验的结果，确定是否将待校验数字证书写入区块链。

[0161] 图6是本申请的一个实施例电子设备的结构示意图。请参考图6，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少1个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[0162] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是ISA(Industry Standard Architecture，工业标准体系结构)总线、PCI(Peripheral

Component Interconnect,外设部件互连标准)总线或EISA(Extended Industry Standard Architecture,扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图6中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0163] 存储器,用于存放程序。具体地,程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[0164] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成数字证书管理装置。处理器,执行存储器所存放的程序,并具体用于执行以下操作:

[0165] 接收区块链中的节点发送的数字证书上链请求,数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书,用于请求将待校验数字证书写入区块链;

[0166] 确定对节点的待校验数字证书进行共识校验的结果;

[0167] 依据共识校验的结果,确定是否将待校验数字证书写入区块链。

[0168] 上述如本申请图1所示实施例揭示的数字证书管理装置执行的方法可以应用于处理器中,或者由处理器实现。处理器可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器,包括中央处理器(Central Processing Unit,CPU)、网络处理器(Network Processor,NP)等;还可以是数字信号处理器(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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

[0169] 该电子设备还可执行图1中数字证书管理装置执行的方法,并实现数字证书管理装置在图1所示实施例的功能,本申请实施例在此不再赘述。

[0170] 本申请实施例还提出了一种计算机可读存储介质,该计算机可读存储介质存储一个或多个程序,该一个或多个程序包括指令,该指令当被包括多个应用程序的电子设备执行时,能够使该电子设备执行图1所示实施例中数字证书管理装置执行的方法,并具体用于执行:

[0171] 接收区块链中的节点发送的数字证书上链请求,数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书,用于请求将待校验数字证书写入区块链;

[0172] 确定对节点的待校验数字证书进行共识校验的结果;

[0173] 依据共识校验的结果,确定是否将待校验数字证书写入区块链。

[0174] 本申请实施例还提供一种数字证书管理装置,用于区块链,参见图7所示,包括:

[0175] 请求接收模块201,接收区块链中的节点发送的数字证书吊销请求,数字证书吊销

请求中包含请求吊销的目标节点的数字证书；

[0176] 共识校验结果确定模块203，确定对目标节点的数字证书进行共识校验的结果；

[0177] 证书管理模块205，依据共识校验的结果，确定是否在区块链中吊销目标节点的数字证书。

[0178] 图8是本申请的一个实施例电子设备的结构示意图。请参考图8，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少1个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[0179] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是ISA(Industry Standard Architecture，工业标准体系结构)总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或EISA(Extended Industry Standard Architecture，扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图8中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[0180] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[0181] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成数字证书管理装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

[0182] 接收区块链中的节点发送的数字证书吊销请求，数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0183] 确定对目标节点的数字证书进行共识校验的结果；

[0184] 依据共识校验的结果，确定是否在区块链中吊销目标节点的数字证书。上述如本申请图3所示实施例揭示的数字证书管理装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，CPU)、网络处理器(Network Processor，NP)等；还可以是数字信号处理器(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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[0185] 该电子设备还可执行图3中数字证书管理装置执行的方法，并实现数字证书管理装置在图3所示实施例的功能，本申请实施例在此不再赘述。

[0186] 本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的电子设备执行时，能够使该电子设备执行图1所示实施例中应用页面截图上报装置执行的方法，并具体用于执行：

[0187] 接收区块链中的节点发送的数字证书吊销请求，数字证书吊销请求中包含请求吊销的目标节点的数字证书；

[0188] 确定对目标节点的数字证书进行共识校验的结果；

[0189] 依据共识校验的结果，确定是否在区块链中吊销目标节点的数字证书。

[0190] 本申请实施例提供一种数字证书管理装置，用于区块链中的节点，参见图9所示，包括：

[0191] 请求发起模块401，向区块链中发送数字证书上链请求，用于供区块链确定对节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将待校验数字证书写入区块链；其中，数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书，用于请求将待校验数字证书写入区块链。

[0192] 图10是本申请的一个实施例电子设备的结构示意图。请参考图10，在硬件层面，该电子设备包括处理器，可选地还包括内部总线、网络接口、存储器。其中，存储器可能包含内存，例如高速随机存取存储器(Random-Access Memory，RAM)，也可能还包括非易失性存储器(non-volatile memory)，例如至少1个磁盘存储器等。当然，该电子设备还可能包括其他业务所需要的硬件。

[0193] 处理器、网络接口和存储器可以通过内部总线相互连接，该内部总线可以是ISA(Industry Standard Architecture，工业标准体系结构)总线、PCI(Peripheral Component Interconnect，外设部件互连标准)总线或EISA(Extended Industry Standard Architecture，扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示，图10中仅用一个双向箭头表示，但并不表示仅有一根总线或一种类型的总线。

[0194] 存储器，用于存放程序。具体地，程序可以包括程序代码，所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器，并向处理器提供指令和数据。

[0195] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成数字证书管理装置。处理器，执行存储器所存放的程序，并具体用于执行以下操作：

[0196] 向区块链中发送数字证书上链请求，用于供区块链确定对节点的待校验数字证书进行共识校验的结果，并依据共识校验的结果，确定是否将待校验数字证书写入区块链；其中，数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书，用于请求将待校验数字证书写入区块链。

[0197] 上述如本申请前述实施例揭示的数字证书管理装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，CPU)、网络处理器(Network Processor，NP)等；还可以是数字信号处理器(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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器,闪存、只读存储器,可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器,处理器读取存储器中的信息,结合其硬件完成上述方法的步骤。

[0198] 该电子设备还可执行前述数字证书管理装置执行的方法,并实现数字证书管理装置在前述实施例的功能,本申请实施例在此不再赘述。

[0199] 本申请实施例还提出了一种计算机可读存储介质,该计算机可读存储介质存储一个或多个程序,该一个或多个程序包括指令,该指令当被包括多个应用程序的电子设备执行时,能够使该电子设备执行前述实施例中数字证书管理装置执行的方法,并具体用于执行:

[0200] 向区块链中发送数字证书上链请求,用于供区块链确定对节点的待校验数字证书进行共识校验的结果,并依据共识校验的结果,确定是否将待校验数字证书写入区块链;其中,数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书,用于请求将待校验数字证书写入区块链。

[0201] 本申请实施例还提供一种数字证书管理装置,用于区块链中的节点,参见图11所示,包括:

[0202] 请求发起模块501,向区块链中发送数字证书吊销请求,用于供区块链确定对目标节点的数字证书进行共识校验的结果,并依据共识校验的结果,确定是否在区块链中吊销目标节点的数字证书;其中,数字证书吊销请求中包含请求吊销的目标节点的数字证书。

[0203] 图12是本申请的一个实施例电子设备的结构示意图。请参考图12,在硬件层面,该电子设备包括处理器,可选地还包括内部总线、网络接口、存储器。其中,存储器可能包含内存,例如高速随机存取存储器(Random-Access Memory,RAM),也可能还包括非易失性存储器(non-volatile memory),例如至少1个磁盘存储器等。当然,该电子设备还可能包括其他业务所需要的硬件。

[0204] 处理器、网络接口和存储器可以通过内部总线相互连接,该内部总线可以是ISA(Industry Standard Architecture,工业标准体系结构)总线、PCI(Peripheral Component Interconnect,外设部件互连标准)总线或EISA(Extended Industry Standard Architecture,扩展工业标准结构)总线等。所述总线可以分为地址总线、数据总线、控制总线等。为便于表示,图12中仅用一个双向箭头表示,但并不表示仅有一根总线或一种类型的总线。

[0205] 存储器,用于存放程序。具体地,程序可以包括程序代码,所述程序代码包括计算机操作指令。存储器可以包括内存和非易失性存储器,并向处理器提供指令和数据。

[0206] 处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行,在逻辑层面上形成数字证书管理装置。处理器,执行存储器所存放的程序,并具体用于执行以下操

作：

[0207] 向区块链中发送数字证书吊销请求，用于供区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在区块链中吊销目标节点的数字证书；其中，数字证书吊销请求中包含请求吊销的目标节点的数字证书。

[0208] 上述如本申请前述实施例揭示的数字证书管理装置执行的方法可以应用于处理器中，或者由处理器实现。处理器可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过处理器中的硬件的集成逻辑电路或者软件形式的指令完成。上述的处理器可以是通用处理器，包括中央处理器(Central Processing Unit，CPU)、网络处理器(Network Processor，NP)等；还可以是数字信号处理器(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。可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。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。结合本申请实施例所公开的方法的步骤可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于随机存储器，闪存、只读存储器，可编程只读存储器或者电可擦写可编程存储器、寄存器等本领域成熟的存储介质中。该存储介质位于存储器，处理器读取存储器中的信息，结合其硬件完成上述方法的步骤。

[0209] 该电子设备还可执行前述数字证书管理装置执行的方法，并实现数字证书管理在前述实施例的功能，本申请实施例在此不再赘述。

[0210] 本申请实施例还提出了一种计算机可读存储介质，该计算机可读存储介质存储一个或多个程序，该一个或多个程序包括指令，该指令当被包括多个应用程序的电子设备执行时，能够使该电子设备执行前述实施例中数字证书管理装置执行的方法，并具体用于执行：

[0211] 向区块链中发送数字证书吊销请求，用于供区块链确定对目标节点的数字证书进行共识校验的结果，并依据共识校验的结果，确定是否在区块链中吊销目标节点的数字证书；其中，数字证书吊销请求中包含请求吊销的目标节点的数字证书。

[0212] 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0213] 本发明是参照根据本发明实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0214] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特

定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0215] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0216] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0217] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0218] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0219] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0220] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0221] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

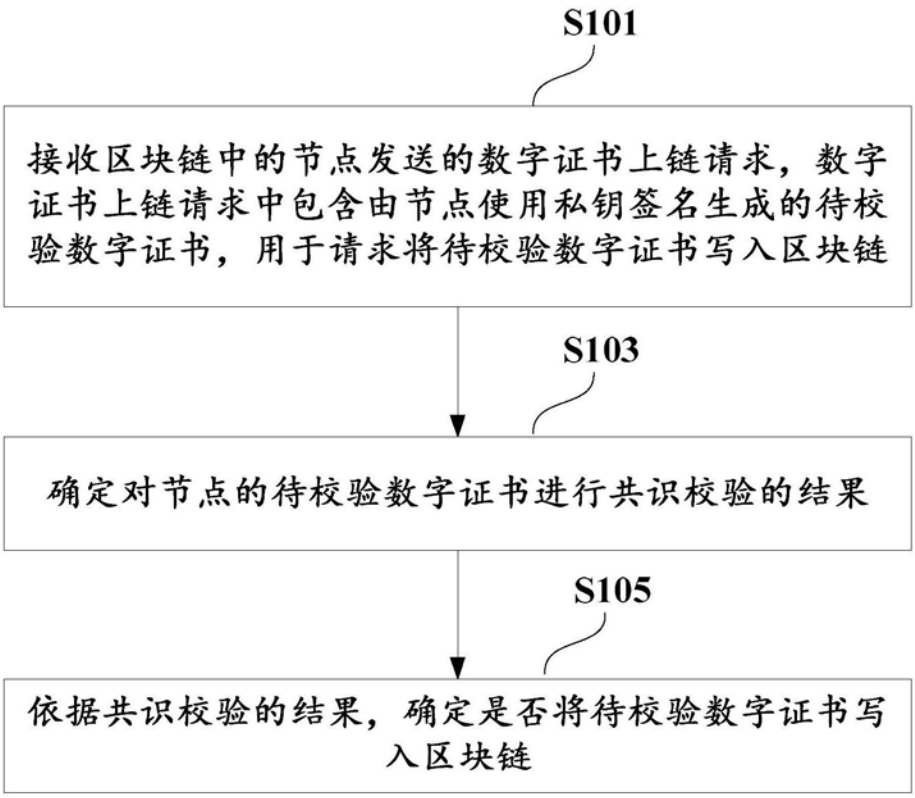

S101
接收区块链中的节点发送的数字证书上链请求，数字证书上链请求中包含由节点使用私钥签名生成的待校验数字证书，用于请求将待校验数字证书写入区块链
S103
确定对节点的待校验数字证书进行共识校验的结果
S105
依据共识校验的结果，确定是否将待校验数字证书写入区块链

图1

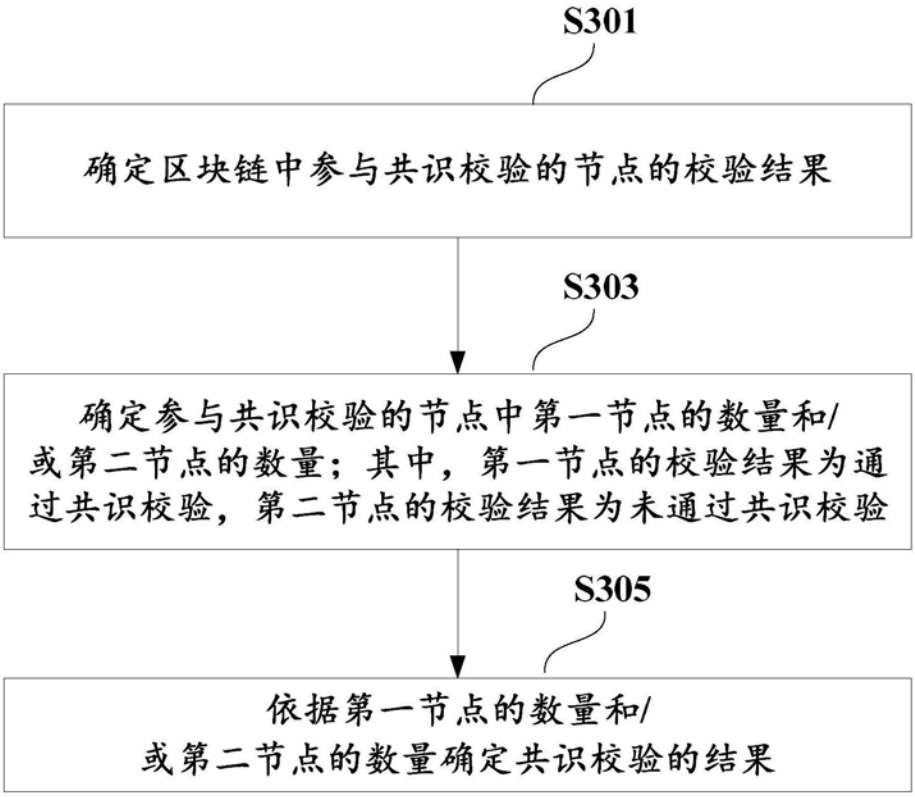

S301
确定区块链中参与共识校验的节点的校验结果
S303
确定参与共识校验的节点中第一节点的数量和/或第二节点的数量；其中，第一节点的校验结果为通过共识校验，第二节点的校验结果为未通过共识校验
S305
依据第一节点的数量和/或第二节点的数量确定共识校验的结果

图2

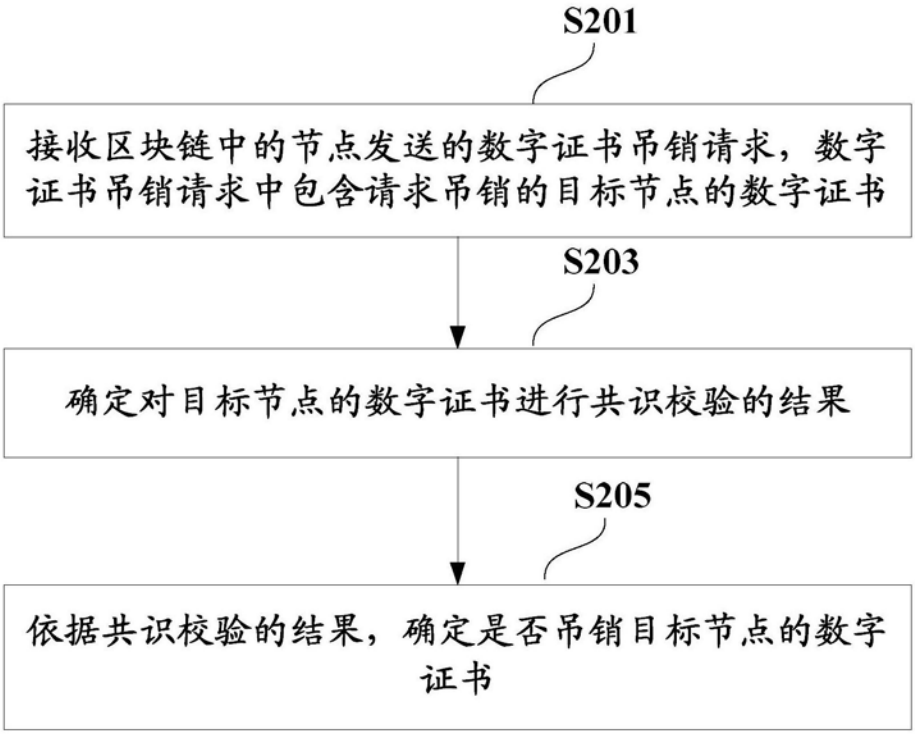

S201
接收区块链中的节点发送的数字证书吊销请求，数字证书吊销请求中包含请求吊销的目标节点的数字证书
S203
确定对目标节点的数字证书进行共识校验的结果
S205
依据共识校验的结果，确定是否吊销目标节点的数字证书

图3

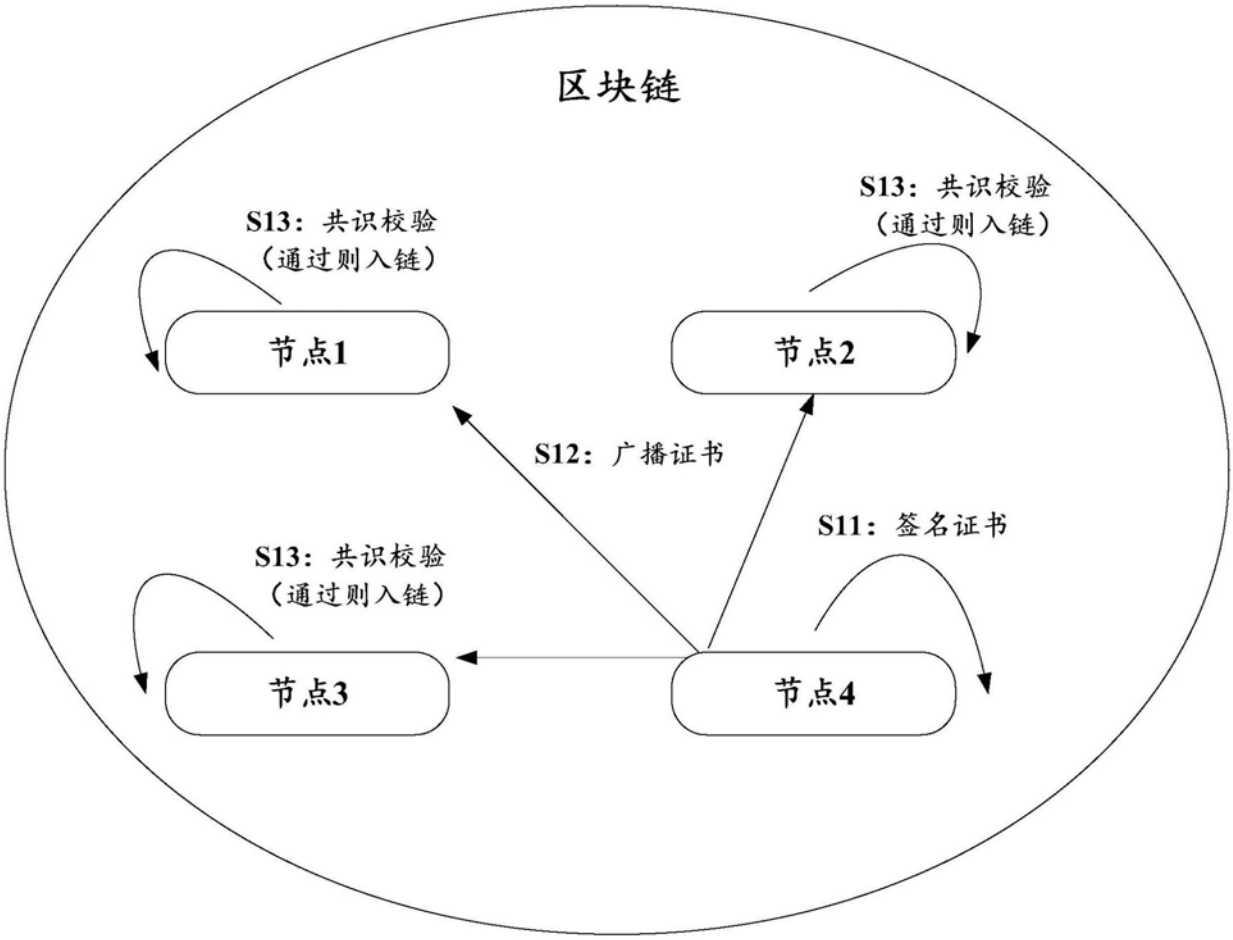

区块链
S13：共识校验
（通过则入链）
S13：共识校验
（通过则入链）
节点1
节点2
S12：广播证书
S11：签名证书
S13：共识校验
（通过则入链）
节点3
节点4

图4

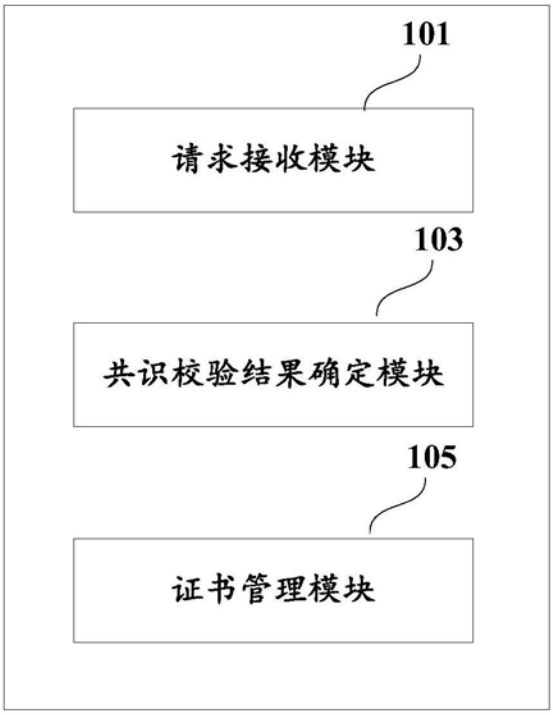

101
请求接收模块
103
共识校验结果确定模块
105
证书管理模块

图5

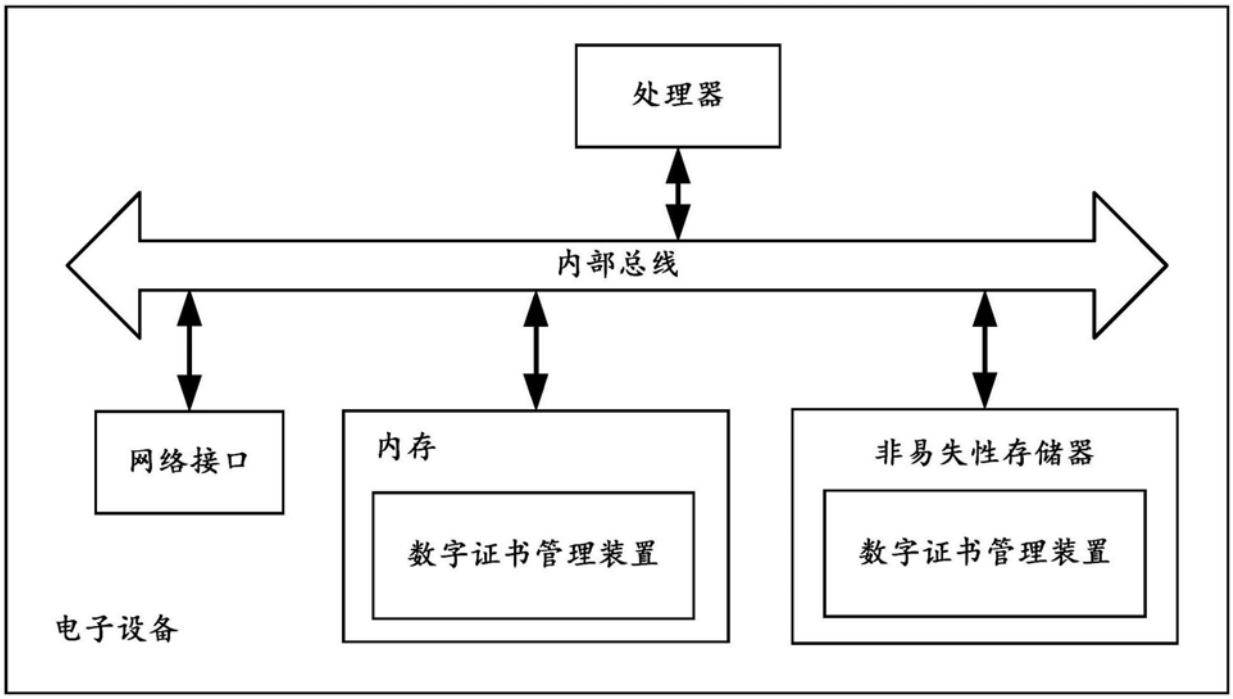

处理器
内部总线
网络接口
内存
数字证书管理装置
非易失性存储器
数字证书管理装置
电子设备

图6

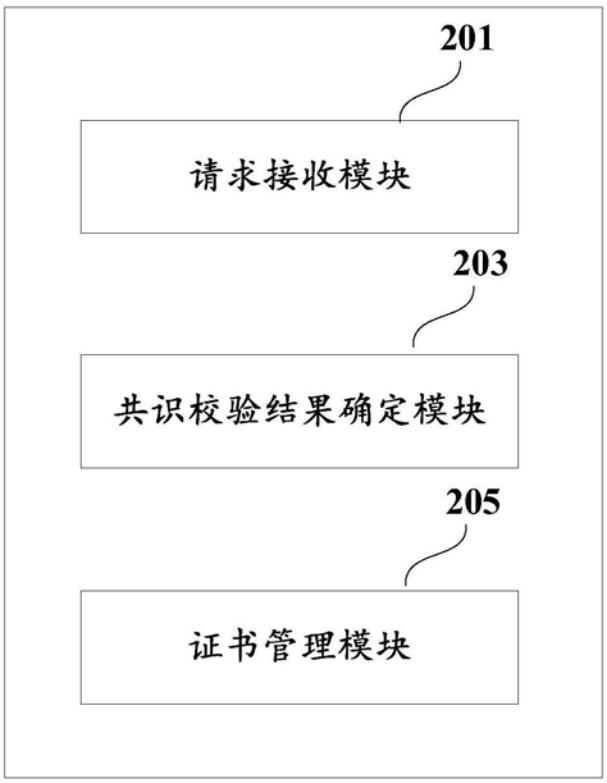

201
请求接收模块
203
共识校验结果确定模块
205
证书管理模块

图7

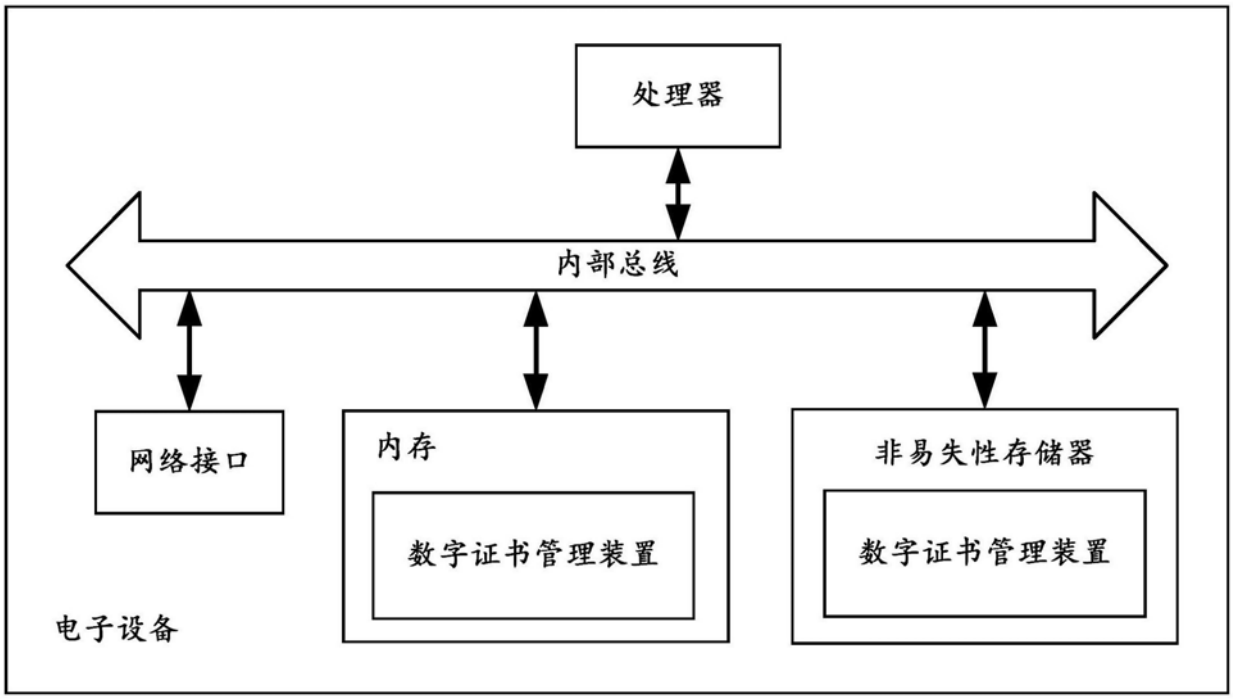

处理器
内部总线
网络接口
内存
数字证书管理装置
非易失性存储器
数字证书管理装置
电子设备

图8

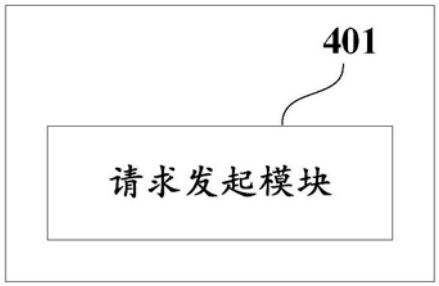

401
请求发起模块

图9

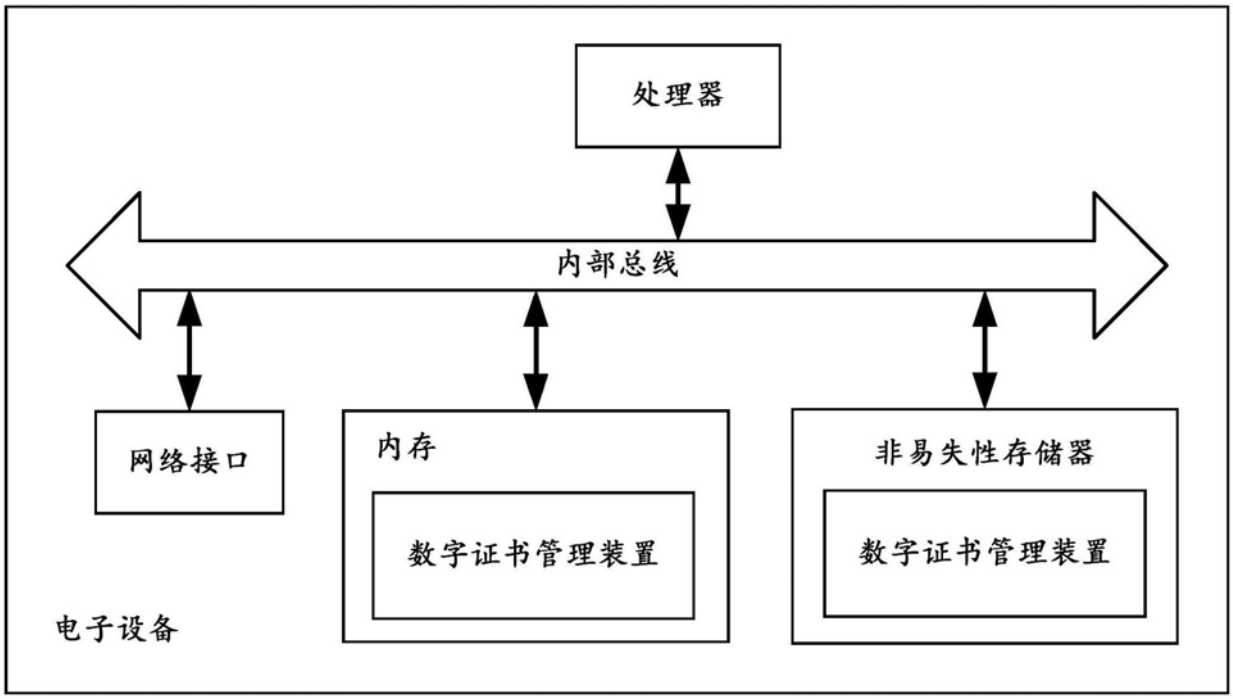

处理器
内部总线
网络接口
内存
数字证书管理装置
非易失性存储器
数字证书管理装置
电子设备

图10

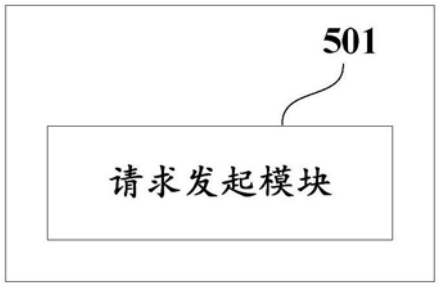

501
请求发起模块

图11

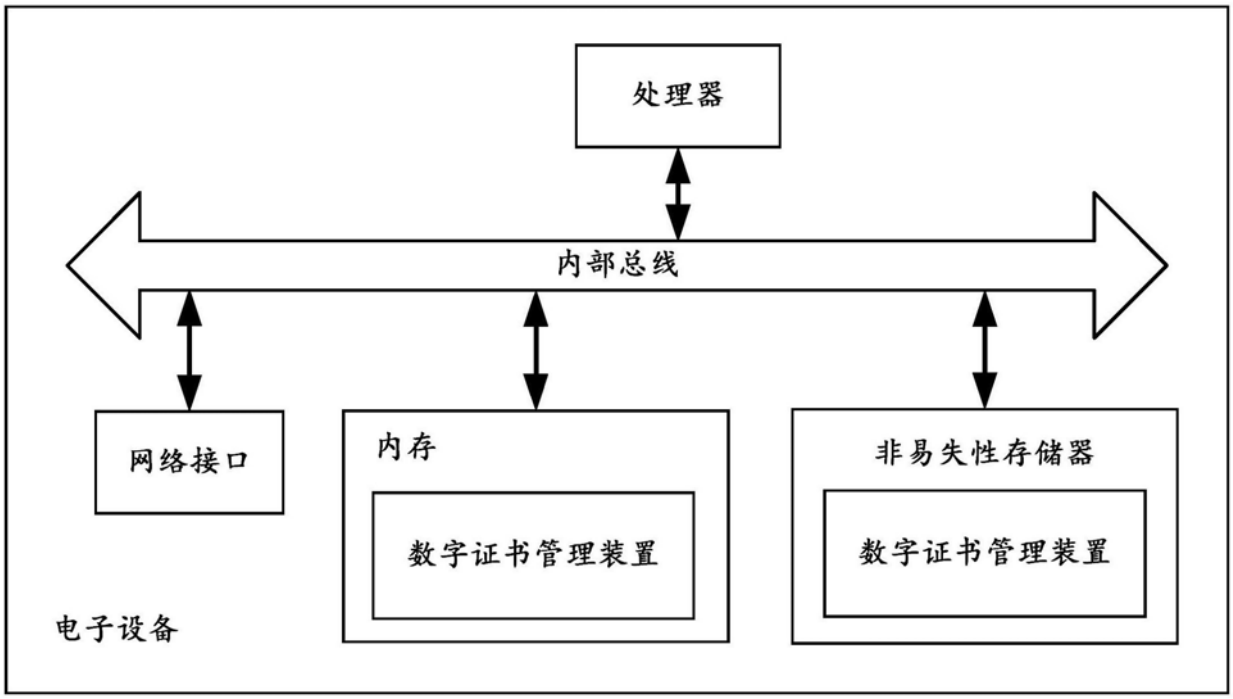


图12