(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 8 月 27 日 (27.08.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/168773 A1

(51) 国际专利分类号:
G06F 21/45 (2013.01)

(21) 国际申请号: PCT/CN2019/121891

(22) 国际申请日: 2019 年 11 月 29 日 (29.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910119332.4 2019年2月18日 (18.02.2019) CN

(71) 申请人: 深圳壹账通智能科技有限公司 (ONE CONNECT SMART TECHNOLOGY CO.,LTD. (SHENZHEN)) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。

(72) 发明人: 霍云 (HUO, Yun); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。 陆陈一帆 (LU, Frank YiFan Chen); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。 冯承勇 (FENG, Chengyong); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518000 (CN)。

(74) 代理人: 深圳中一联合知识产权代理有限公司 (SHENZHEN ZHONGYI UNION INTELLECTUAL PROPERTY AGENCY CO.,LTD.); 中国广东省深圳市福田区园岭街道深南中路1014号报春大厦9楼 (5号信箱), Guangdong 518028 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

(54) **Title:** METHOD FOR ISSUING AND VERIFYING DIGITAL CERTIFICATE ON BLOCKCHAIN, DEVICE AND MEDIUM

(54) 发明名称: 一种区块链上的数字证书签发、验证方法、设备及介质

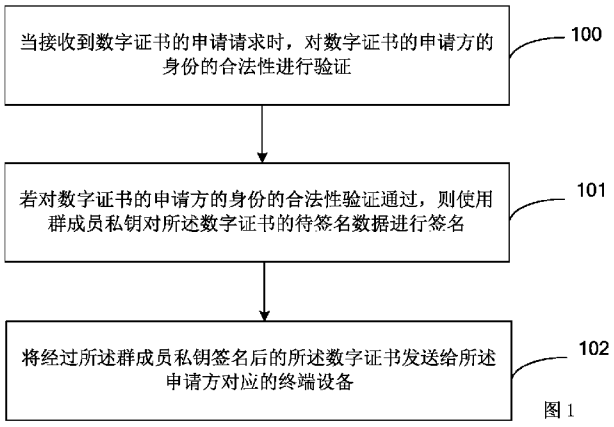

图 1

100 When receiving an application request for a digital certificate, verify the legitimacy of the identity of the applicant for the digital certificate
101 If the verification of the legitimacy of the identity of the applicant for the digital certificate passes, then use a group member private key to sign the data to be signed of the digital certificate
102 Send the digital certificate signed by the group member private key to a terminal device corresponding to the applicant

(57) **Abstract:** The present application relates to a method for issuing and verifying a digital certificate on a blockchain and a device and a medium, the method for issuing a digital certificate on a blockchain comprising: when receiving an application request for a digital certificate, verifying the legitimacy of the identity of the applicant for the digital certificate; if the verification of the legitimacy of the identity of the applicant for the digital certificate passes, then using a group member private key to sign the data to be signed of the digital certificate, an identifier of the issuer of the digital certificate being the identifier of a CA organisation group in a group certificate, the group member private key and the group certificate being issued to the CA organisation in advance by a management

WO 2020/168773 A1

[见续页]

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

server of the CA organisation group; and sending the digital certificate signed by the group member private key to a terminal device corresponding to the applicant. The present application can hide the actual issuer of the digital certificate, avoiding the problem of client channel information leakage, and increasing the client information security.

(57) 摘要：本申请涉及一种区块链上的数字证书签发、验证方法、设备及介质，区块链上的数字证书签发方法包括：当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构；将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。本申请可以隐藏数字证书的实际签发者，避免泄露客户的渠道信息的问题，提高了客户信息的安全性。

一种区块链上的数字证书签发、验证方法、设备及介质

[0001] 本申请要求于2019年02月18日提交中国专利局、申请号为201910119332.4 、发明名称为“区块链上的数字证书签发、验证方法、设备、系统及介质”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

[0002] 本申请属于数据处理技术领域，尤其涉及一种区块链上的数字证书签发、验证方法、设备及介质。

背景技术

[0003] 目前，区块链系统使用CA（Certificate Authority，认证授权）机构签发数字证书来标识节点或用户的身份。不同的节点和用户可能属于不同的机构，机构通常使用自身的CA机构为节点和用户签发数字证书，在区块链系统中具有多个CA机构的场景下，用户的数字证书的签发机构常常会公开用户的渠道信息，例如，用户与数字证书签发机构之间的关系，或在数字证书中公开数字证书的实际签发机构。然而，在一些业务场景中，参与链上交易的机构不希望公开用户的渠道信息。故，如何使得数字证书的签发机构不公开用户的渠道信息，是目前亟待解决的一个问题。

发明概述

技术问题

[0004] 基于此，有必要针对签发机构在签发数字证书时公开数字证书的实际签发机构的问题，提供一种区块链上的数字证书签发、验证方法、设备及介质。

问题的解决方案

技术解决方案

[0005] 本申请实施例的第一方面提供了一种区块链上的数字证书签发方法，应用于认证授权CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，所述方法包括：

[0006] 当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验

证；

[0007] 若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

[0008] 将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[0009] 本申请实施例的第二方面提供了一种区块链上的数字证书验证方法，应用于数字证书的申请方的终端设备，所述方法包括：

[0010] 当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

[0011] 使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

[0012] 在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[0013] 本申请实施例的第三方面提供了一种区块链上的数字证书签发装置，应用于认证授权CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，所述装置包括：

[0014] 第一验证模块，用于当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

[0015] 签名模块，用于对数字证书的申请方的身份的合法性验证通过时，使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构；

[0016] 发送模块，用于将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[0017] 本申请实施例的第四方面提供了一种区块链上的数字证书验证装置，应用于数字证书的申请方的终端设备，其特征在于，所述装置包括：

[0018] 获取模块，用于当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

[0019] 第二验证模块，用于使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

[0020] 确定模块，用于在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[0021] 本申请实施例的第五方面提供了一种终端设备，所述终端设备为认证授权CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

[0022] 当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

[0023] 若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

[0024] 将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[0025] 本申请实施例的第六方面提供了一种终端设备，所述终端设备为数字证书的申请方的终端设备，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

[0026] 当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

[0027] 使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

[0028] 在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[0029] 本申请实施例的第七方面提供了一种电子交易系统，所述系统包括如上所述的区块链上的数字证书签发装置以及如上所述的区块链上的数字证书验证装置。

[0030] 本申请实施例的第八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存储有计算机可读指令，其特征在于，所述计算机可读指令被至少一个处理器执行时实现如上所述的区块链上的数字证书签发方法的步骤。

[0031] 本申请实施例的第九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存储有计算机可读指令，其特征在于，所述计算机可读指令被至少一个处理器执行时实现如上所述的区块链上的数字证书验证方法的步骤。

发明的有益效果

有益效果

[0032] 通过使用CA机构群的群证书的信息签发数字证书以及使用CA机构群为CA机构分发的群成员私钥对数字证书的待签名数据进行签名，使得数字证书中的签发机构的标识为CA机构群的标识，从而隐藏了数字证书的实际签发者，避免了泄露客户的渠道信息的问题，提高了客户信息的安全性；数字证书的验证方的终端设备使用CA机构群发布的群证书对数字证书的合法性进行验证时，数字证书

中的颁发者的标识为CA机构群的标识，验证方的终端设备不会获知数字证书的实际签发者，保障了客户渠道的隐私性。

对附图的简要说明

附图说明

[0033] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0034] 图1是根据一示例性实施例示出的一种区块链上的数字证书签发方法的流程图；

[0035] 图2是根据一示例性实施例示出的一种区块链上的数字证书验证方法的流程图；

[0036] 图3是根据一示例性实施例示出的一种区块链上的数字证书签发装置的框图；

[0037] 图4是根据一示例性实施例示出的一种区块链上的数字证书验证装置的框图；

[0038] 图5是根据一示例性实施例示出的一种电子交易系统的框图；

[0039] 图6是根据一示例性实施例示出的一种区块链上的数字证书签发装置的框图；

[0040] 图7是根据一示例性实施例示出的一种区块链上的数字证书验证装置的框图。

发明实施例

本发明的实施方式

[0041] 以下描述中，为了说明而不是为了限定，提出了诸如特定系统结构、技术之类的具体细节，以便透彻理解本申请实施例。然而，本领域的技术人员应当清楚，在没有这些具体细节的其它实施例中也可以实现本申请。在其它情况中，省略对众所周知的系统、装置、电路以及方法的详细说明，以免不必要的细节妨碍本申请的描述。

[0042] 为了说明本申请所述的技术方案，下面通过具体实施例来进行说明。

[0043] 图1是根据一示例性实施例示出的一种区块链上的数字证书签发方法的流程图，该方法应用于一CA机构的服务器，即该方法可由CA机构的服务器执行，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，如图1所示，

该方法包括如下步骤：

[0044] 步骤100：当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

[0045] 步骤101：若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

[0046] CA机构的服务器在为用户设备或节点设备（区块链系统中的节点）签发数字证书时，可使用该CA机构的群成员私钥对数字证书的待签名数据进行签名。其中，数字证书的待签名数据可包括：版本、证书序列号、签名算法、颁发者名称、证书效期、主体名称、主体公钥信息以及证书自定义扩展项信息。该群成员私钥可由CA机构群的群管理服务器生成并分发给CA机构群中的各CA机构的服务器，例如，在CA1机构注册到CA机构群后，群管理服务器生成与该CA1机构对应的群成员私钥1，将该群成员私钥1发送给该CA1机构。群管理服务器可记录CA1机构与群成员私钥1之间的对应关系，或者，在群管理服务器上，可用群成员私钥来标识各CA机构。又例如，群管理服务器可在各CA机构均注册到CA机构群后，生成与各CA机构对应的群成员私钥，再将生成的各群成员私钥分发给各CA机构的服务器，群管理服务器可记录各群成员私钥与各CA机构之间的对应关系。其中，每个CA机构对应唯一一个群成员私钥，即各CA机构的群成员私钥不同，该群成员私钥例如可以是一串序列码。

[0047] 在上述步骤101中，对数字证书进行签名可以使用非对称密码体制，以RSA算法体制为例，在产生了RSA公私钥对的情况下，可以使用RSA私钥对待签名的数字证书的待签名数据（可先对数据进行摘要运算）进行签名，得到签名后的数字证书。数字证书的验证方对应的终端设备则可使用RSA公钥验证该数字证书中的签名的合法性。在本实施例的签发数字证书的方法中，群公钥和各CA机构的群成员私钥均构成一对密钥对，故可使用群公钥对各CA机构使用自身的群成员私钥进行签名的数字证书中的签名的合法性进行验证。

[0048] 在一个实施例中，数字证书中的颁发者的名称可以为CA机构群的信息，例如，颁发者的名称可以为CA机构群的唯一标识或CA机构群的名称，基于此，对数字证书的验证方对应的终端设备来说，其获取到数字证书后，根据数字证书中的颁发者的名称仅可获知该数字证书的颁发者为CA机构群，而由于CA机构群中包括多个CA机构，故数字证书的验证方对应的终端设备无从获知该数字证书具体由CA机构群中的哪个CA机构签发，从而可隐藏数字证书的实际签发机构。

[0049] 在一个实施例中，上述群证书的格式可同X.509证书的格式一致或类似，群证书可包含证书信息和签名。其中，证书信息可包括：版本、证书序列号、签名算法、颁发者名称、证书有效期、主体名称、主体公钥信息以及证书的自定义扩展项信息。

[0050] 步骤102：将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[0051] 在本实施例的区块链上的签发数字证书的方法中，CA机构的服务器使用CA机构群为其分发的群成员私钥对数字证书的待签名的数据进行签名，以及使用CA机构群的群证书的信息签发数字证书，使得数字证书中的签发者为CA机构群的标识，从而隐藏了数字证书的实际签发者，避免了泄露客户渠道信息的问题，提高了客户信息的安全性。

[0052] 在一种可实现方式中，区块链上的签发数字证书的方法还可包括：向所述CA机构群的服务器发送注册请求；注册到所述CA机构群后可向CA机构群的群管理服务器提交本CA机构的身份信息等，用以标识该CA机构的身份。接收所述CA机构群的管理服务器发送的所述群成员私钥以及所述群证书，其中，所述群成员私钥与所述CA机构唯一对应，该群成员私钥例如可以是一串序列码；所述群证书被所述CA机构群中的各CA机构共用，即，CA机构群中的各CA机构的服务器在为用户设备或节点设备签发数字证书时，均可使用群证书中的信息进行签发，例如，各CA机构的服务器签发的数字证书中的签发者可均为CA机构群的名称，或CA机构群的标识。CA机构群的管理服务器可对CA机构群中的CA机构统一进行管理，为各CA机构分配群成员私钥，各CA机构的服务器可直接使用被分配的该私钥对数字证书中待签名的数据进行签名，各CA机构的服务器无需再额

外生成私钥，减少了CA机构端在签发数字证书过程中的操作。

[0053] 在一种可实现方式中，所述数字证书中的签发机构的密钥标识为所述群公钥的密钥标识。群公钥的密钥标识例如可以是通过摘要算法对群公钥进行摘要运算获得的一串序列码。

[0054] 在一种可实现方式中，所述至少两个CA机构可包括所述区块链系统中所有的CA机构，这样可使得该区块链系统中所有的CA机构能够被CA机构群的群管理员统一管理。

[0055] 图2是根据一示例性实施例示出的一种区块链上的数字证书验证方法的流程图，该方法可应用于数字证书的申请方的终端设备，或者，该方法也可应用于数字证书的验证方的终端设备，数字证书的验证方的终端设备例如可以是区块链系统中的客户端设备或节点设备。例如，在业务交易中，两个客户端设备之间进行交易，双方在业务过程中会对自身的数据或交易行为进行签名，则双方需要互相验证对方签名的合法性。在客户端设备与节点设备交互时，节点设备会验证客户端设备的数字证书的合法性，在这种情况下，节点设备为数字证书的验证方的终端设备；而在节点设备之间相互连接时，各节点设备之间会互相验证对方的数字证书的合法性，在这种情况下，各节点设备为数字证书的验证方的终端设备；此外，区块链系统会记录各种交易的数据，节点设备会验证交易中的签名及数字证书的合法性，在这种情况下，各节点设备是数字证书的验证方的终端设备。如图2所示，该方法可包括如下步骤：

[0056] 步骤201：当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

[0057] 步骤202：使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群颁发给所述CA机构。

[0058] 步骤203：在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到

的摘要信息一致，则确定所述签名的合法性验证通过。

[0059] 在本实施例的区块链上的数字证书验证方法中，由于数字证书的验证方对应的终端设备使用CA机构群发布的群证书中的群公钥对数字证书的合法性进行验证，数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，验证方对应的终端设备不会获知数字证书的实际签发者，从而隐藏了数字证书的实际签发机构，保障了客户渠道的隐私性。

[0060] 在一种可实现方式中，获取CA机构群预先发布的群证书可包括：从区块链系统获取所述群证书。例如，在数字证书的验证方对应的终端设备需对数字证书进行验证时，该终端设备可从区块链系统上获取群证书，例如，可从区块链系统上下载该群证书，从而使用该群证书中的群公钥验证客户端设备或节点设备的数字证书中的签名的合法性。该终端设备还可保存下载的群证书，以便后续可直接使用该群证书中的群公钥验证所述CA机构群中其他CA机构签发的数字证书，基于此，在验证同一CA机构群中的CA机构签发的数字证书时，可仅从区块链系统下载一次群证书即可，简化了证书验证方的操作。或者，数字证书的验证方对应的终端设备也可以在获知区块链系统上发布了其所需的群证书后，预先从区块链系统上下载并保存该群证书，以便在需要对客户端设备或节点设备的数字证书进行验证时，可直接从验证方对应的终端设备的本地获取并使用该群证书，可提高数字证书的验证效率。

[0061] 在一种可实现方式中，所述群成员私钥与所述CA机构唯一对应，也即，CA机构群中的各CA机构的群成员私钥不同。所述群证书被所述CA机构群中的各CA机构共用。例如，各CA机构的服务器可使用群证书中的信息为用户或节点签发数字证书，签发的数字证书中，证书的颁发者标识可为CA机构群的唯一标识。

[0062] 基于本申请的区块链上的数字证书的验证方法，各CA机构的群成员私钥与群公钥构成密钥对，而节点设备以及用户设备的数字证书使用了群成员私钥进行签名，故数字证书的验证方对应的终端设备可直接从区块链系统获取群证书，使用群证书中的群公钥对数字证书中的签名进行验证，简化了数字证书验证方的操作，提高了数字证书验证效率。

[0063] 图3是根据一示例性实施例示出的一种区块链上的数字证书签发装置的框图，

该装置可用于实现上述区块链上的签发数字证书的方法，所述装置应用于CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，如图3所示，所述装置30包括如下组成部分：

[0064] 第一验证模块31，用于当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

[0065] 签名模块32，用于对数字证书的申请方的身份的合法性验证通过时，使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

[0066] 发送模块33，用于将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[0067] 在一种可实现方式中，区块链上的数字证书签发装置还可包括：接收模块，用于在注册到所述CA机构群后，接收所述CA机构群的管理服务器发送的所述群成员私钥以及所述群证书，其中，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[0068] 在一种可实现方式中，所述至少两个CA机构包括所述区块链系统中所有的CA机构。

[0069] 图4是根据一示例性实施例示出的一种区块链上的数字证书验证装置的框图，该装置可应用于数字证书的申请方的终端设备，如图4所示，该装置40包括如下组成部分：

[0070] 获取模块41，用于当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

[0071] 验证模块42，用于使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

[0072] 确定模块43，用于在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[0073] 在一种可实现方式中，所述获取模块可用于：从区块链系统获取所述群证书。

[0074] 在一种可实现方式中，所述数字证书中的颁发机构的密钥标识为所述群公钥的密钥标识。

[0075] 在一种可实现方式中，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[0076] 本申请还提供了一种电子交易系统，该系统可包括上述区块链上的数字证书签发装置30以及区块链上的数字证书验证装置40，图5是根据一示例性实施例示出一种电子交易系统的框图，在图5中，数字证书签发装置以CA机构的服务器51为例，数字证书验证装置以终端设备52为例，更进一步的该电子交易系统50还可包括，群管理员服务器53，需要说明的是，该系统中可包括多个CA机构的服务器，图5中仅以服务器51进行示例，同时，该系统中也可包括多个终端设备，图5中仅以终端设备52进行示例。区块链系统上所有的CA机构（CA机构1至CA机构N）可构成一个CA机构群，群管理服务器53可管理该CA机构群内的各CA机构，各CA机构可通过各自的服务器为用户设备或区块链中的节点设备签发数字证书（CA机构签发数据证书的方法参考图1所示的方法）。监管机构的服务器可充当该CA机构群中的群管理服务器53的角色，根据区块链系统使用场景的不同，监管机构可以是政府机构、行业协会或联盟的管理机构等，群管理服务器53可打开数字证书的签名，查看数字证书的签发机构，以对各数字证书的签发机构进行监管。群管理服务器53可以是通过群管理员账号登录的一个可用于管理上述CA机构群中的群成员，该服务器并非仅能使用固定的某一服务器，可通过在不同的服务器上登录群管理账号来实现对CA机构群中各群成员的管理。在各CA机构注册到CA机构群后，CA机构群的群管理服务器53可为CA机构群中的每个CA机构颁发群证书以及群成员私钥。各CA机构的服务器可使用该群证书的证书信息来进行数字证书的签发，例如，签发的数字证书中颁发者的标识等信息需与群证书中的信息一致，以及CA机构的服务器51可使用群成员私钥对数字证书

的待签名数据进行签名。群管理服务器53可将群证书发布到区块链系统上，以便于在交易过程中，数字证书的验证方的终端设备52在需要验证数字证书中签名的合法性时，可从区块链系统获取该群证书，从而使用该群证书中的群公钥对数字证书中的签名进行验证（验证数字证书的方法可参考图2所示的方法）。其中，群管理服务器53颁发给各CA机构的群证书为同一群证书，各CA机构的服务器均可使用该群证书进行数字证书的签发。

[0077] 图6是根据一示例性实施例示出的一种终端设备的框图。如图6所示，该设备600可以包括：处理器601，存储器602，多媒体组件603，输入/输出（I/O）接口604，以及通信组件605。

[0078] 其中，处理器601用于控制该设备600的整体操作，以完成上述的数字证书验证方法中的全部或部分步骤。存储器602用于存储各种类型的数据以支持在该设备600的操作，这些数据例如可以包括用于在该设备600上操作的任何应用程序或方法的指令，以及应用程序相关的数据，例如联系人数据、收发的消息、图片、音频、视频等等。多媒体组件603可以包括屏幕和音频组件。其中屏幕例如可以是触摸屏，音频组件用于输出和/或输入音频信号。例如，音频组件可以包括一个麦克风，麦克风用于接收外部音频信号。所接收的音频信号可以被进一步存储在存储器602或通过通信组件605发送。音频组件还包括至少一个扬声器，用于输出音频信号。I/O接口604为处理器601和其他接口模块之间提供接口，上述其他接口模块可以是键盘，鼠标，按钮等。这些按钮可以是虚拟按钮或者实体按钮。通信组件605用于该设备600与其他设备之间进行有线或无线通信。无线通信，例如Wi-Fi，蓝牙，近场通信（Near Field Communication，简称NFC），2G、3G或4G，或它们中的一种或几种的组合，因此相应的该通信组件605可以包括：Wi-Fi模块，蓝牙模块，NFC模块。

[0079] 在一示例性实施例中，上述设备600可以被一个或多个应用专用集成电路（Application Specific Integrated Circuit，简称ASIC）、数字信号处理器（Digital Signal Processor，简称DSP）、数字信号处理设备（Digital Signal Processing Device，简称DSPD）、可编程逻辑器件（Programmable Logic Device，简称PLD）、现场可编程门阵列（Field Programmable Gate Array，简称FPGA）、控制器、微控制

器、微处理器或其他电子元件实现，用于执行上述的数字证书签发方法。

[0080] 在另一示例性实施例中，还提供了一种包括程序指令的非临时性计算机可读存储介质，例如包括程序指令的存储器602，上述程序指令可由设备600的处理器601执行以完成上述的区块链上的数字证书签发方法。

[0081] 图7是根据一示例性实施例示出的一种终端设备的框图。例如，设备700可以被提供为一服务器。参照图7，设备700包括处理器722，其数量可以为一个或多个，以及存储器732，用于存储可由处理器722执行的计算机可读指令。存储器732中存储的计算机可读指令可以包括一个或一个以上的每一个对应于一组指令的模块。此外，处理器722可以被配置为执行该计算机可读指令，以执行上述区块链上的数字证书验证方法。

[0082] 另外，设备700还可以包括电源组件726和通信组件750，该电源组件726可以被配置为执行设备700的电源管理，该通信组件750可以被配置为实现设备700的通信，例如，有线或无线通信。此外，该设备700还可以包括输入/输出（I/O）接口758。设备700可以操作基于存储在存储器732的操作系统，例如Windows ServerTM，Mac OS XTM，UnixTM, LinuxTM等等。

[0083] 在另一示例性实施例中，还提供了一种存储有计算机可读指令的存储介质，例如包括程序指令的存储器732，上述程序指令可由设备700的处理器722执行以完成上述的区块链上的数字证书验证方法。

[0084] 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，是可以通过计算机可读指令来指令相关的硬件来完成，所述的计算机可读指令可存储于一非易失性计算机可读取存储介质中，该计算机可读指令在执行时，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。

[0085] 以上结合附图详细描述了本申请的优选实施方式，但是，本申请并不限于上述实施方式中的具体细节，在本申请的技术构思范围内，可以对本申请的技术方案进行多种简单变型，这些简单变型均属于本申请的保护范围。

[0086] 另外需要说明的是，在上述具体实施方式中所描述的各个具体技术特征，在不矛盾的情况下，可以通过任何合适的方式进行组合。为了避免不必要的重复，本申请对各种可能的组合方式不再另行说明。

[0087] 此外，本申请的各种不同的实施方式之间也可以进行任意组合，只要其不违背本申请的思想，其同样应当视为本申请所公开的内容。

权利要求书

[权利要求 1] 一种区块链上的数字证书签发方法，其特征在于，所述方法应用于认证授权CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，所述方法包括：

当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[权利要求 2] 如权利要求1所述的方法，其特征在于，所述方法还包括：

向所述CA机构群的服务器发送注册请求；

在注册到所述CA机构群后，接收所述CA机构群的管理服务器发送的所述群成员私钥以及所述群证书，其中，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[权利要求 3] 如权利要求1所述的方法，其特征在于，所述至少两个CA机构包括所述区块链系统中所有的CA机构。

[权利要求 4] 如权利要求1至3任一项所述的方法，其特征在于，所述数字证书中的签发机构的密钥标识为所述群公钥的密钥标识。

[权利要求 5] 一种区块链上的数字证书验证方法，其特征在于，应用于数字证书的申请方的终端设备，所述方法包括：

当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[权利要求 6] 如权利要求5所述的方法，其特征在于，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[权利要求 7] 一种区块链上的数字证书签发装置，其特征在于，所述装置应用于认证授权CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，所述装置包括：

第一验证模块，用于当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

签名模块，用于对数字证书的申请方的身份的合法性验证通过时，使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构；

发送模块，用于将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[权利要求 8] 一种区块链上的数字证书验证装置，应用于数字证书的申请方的终端设备，其特征在于，所述装置包括：

获取模块，用于当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

第二验证模块，用于使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私

钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

确定模块，用于在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[权利要求 9] 一种终端设备，其特征在于，所述终端设备为认证授权CA机构的服务器，所述CA机构属于一CA机构群，所述CA机构群包括至少两个CA机构，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的标识为群证书中的所述CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给所述CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[权利要求 10] 如权利要求9所述的终端设备，其特征在于，还实现如下步骤：

向所述CA机构群的服务器发送注册请求；

在注册到所述CA机构群后，接收所述CA机构群的管理服务器发送的所述群成员私钥以及所述群证书，其中，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[权利要求 11] 如权利要求9所述的终端设备，其特征在于，所述至少两个CA机构包括所述区块链系统中所有的CA机构。

[权利要求 12] 如权利要求9至11任意一项所述的终端设备，其特征在于，所述数字

证书中的签发机构的密钥标识为所述群公钥的密钥标识。

[权利要求 13] 一种终端设备，其特征在于，所述终端设备为数字证书的申请方的终端设备，所述终端设备包括存储器、处理器，所述存储器上存储有可在所述处理器上运行的计算机可读指令，所述处理器执行所述计算机可读指令时实现如下步骤：

当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[权利要求 14] 如权利要求13所述的终端设备，其特征在于，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[权利要求 15] 一种电子交易系统，其特征在于，所述系统包括权利要求7所述的区块链上的数字证书签发装置以及权利要求8所述的区块链上的数字证书验证装置。

[权利要求 16] 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被至少一个处理器执行时实现如下步骤：

当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证；

若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名，所述数字证书中的颁发者的

标识为群证书中的CA机构群的标识，所述群成员私钥以及所述群证书由所述CA机构群的管理服务器预先颁发给CA机构，所述群证书中包括群公钥，所述群公钥与所述群成员私钥为一对密钥对；

将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备。

[权利要求 17] 如权利要求16所述的计算机可读存储介质，其特征在于，还实现如下步骤：

向所述CA机构群的服务器发送注册请求；

在注册到所述CA机构群后，接收所述CA机构群的管理服务器发送的所述群成员私钥以及所述群证书，其中，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各CA机构共用。

[权利要求 18] 如权利要求16或17所述的计算机可读存储介质，其特征在于，所述数字证书中的签发机构的密钥标识为所述群公钥的密钥标识。

[权利要求 19] 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机可读指令，其特征在于，所述计算机可读指令被至少一个处理器执行时实现如下步骤：

当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书，所述CA机构群中至少包括两个CA机构，其中，所述数字证书中的颁发者的标识为所述群证书中的所述CA机构群的标识；

使用所述群证书中的群公钥验证所述签名的合法性，其中，所述数字证书由所述CA机构群中的CA机构使用群成员私钥进行签名，所述群成员私钥由所述CA机构群的管理服务器颁发给所述CA机构；

在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的与所述摘要信息对应的原文产生一个摘要信息，若该摘要信息与解密得到的摘要信息一致，则确定所述签名的合法性验证通过。

[权利要求 20] 如权利要求19所述的计算机可读存储介质，其特征在于，所述群成员私钥与所述CA机构唯一对应，所述群证书被所述CA机构群中的各C

A机构共用。

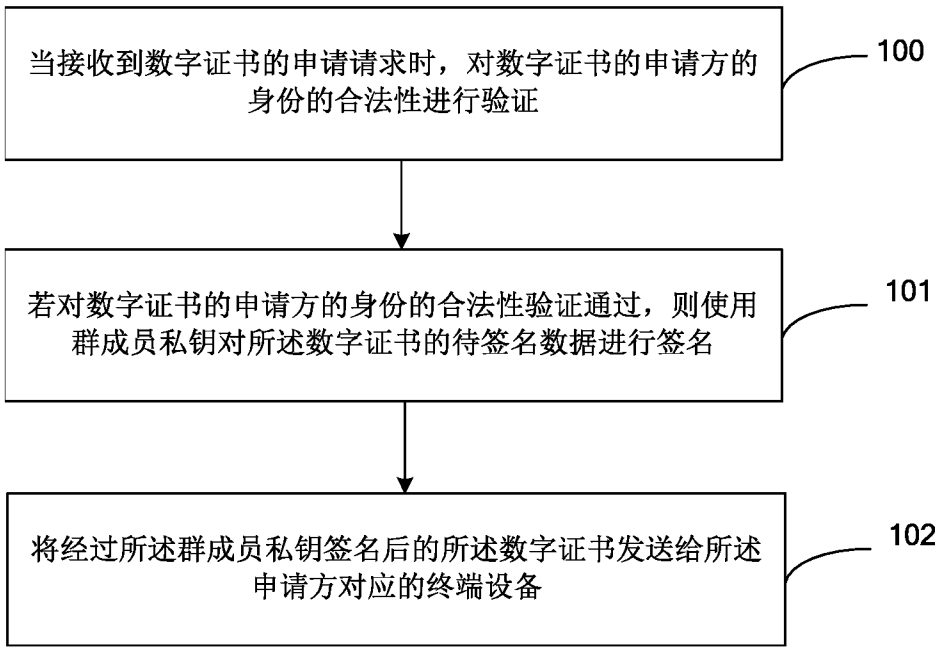
当接收到数字证书的申请请求时，对数字证书的申请方的身份的合法性进行验证
100
若对数字证书的申请方的身份的合法性验证通过，则使用群成员私钥对所述数字证书的待签名数据进行签名
101
将经过所述群成员私钥签名后的所述数字证书发送给所述申请方对应的终端设备
102

图 1

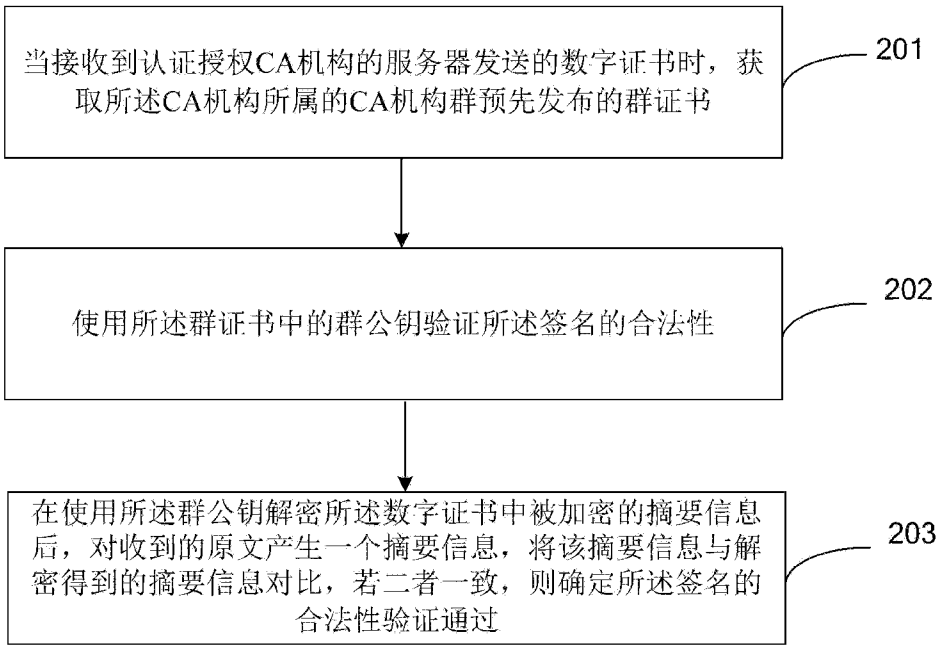
当接收到认证授权CA机构的服务器发送的数字证书时，获取所述CA机构所属的CA机构群预先发布的群证书
201
使用所述群证书中的群公钥验证所述签名的合法性
202
在使用所述群公钥解密所述数字证书中被加密的摘要信息后，对收到的原文产生一个摘要信息，将该摘要信息与解密得到的摘要信息对比，若二者一致，则确定所述签名的合法性验证通过
203

图 2

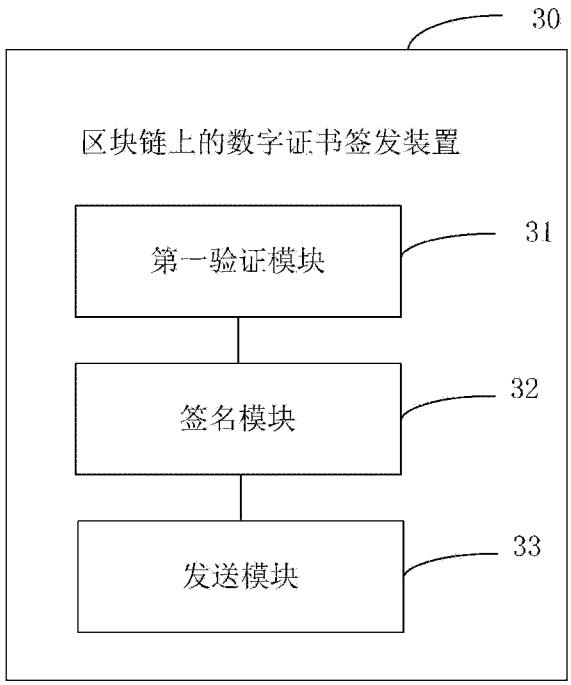
30
区块链上的数字证书签发装置
第一验证模块
31
签名模块
32
发送模块
33

图 3

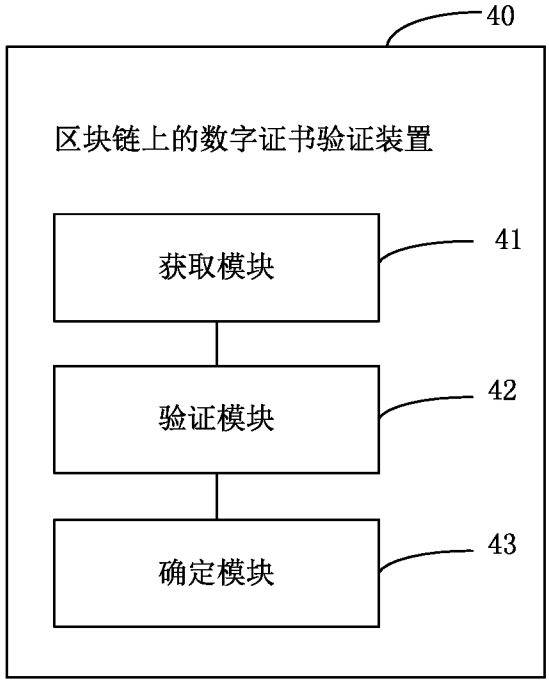
40
区块链上的数字证书验证装置
获取模块
41
验证模块
42
确定模块
43

图 4

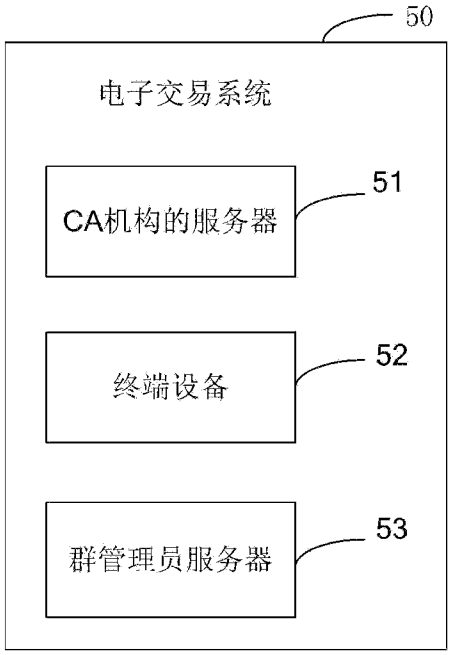
50
电子交易系统
CA机构的服务器
51
终端设备
52
群管理员服务器
53

图 5

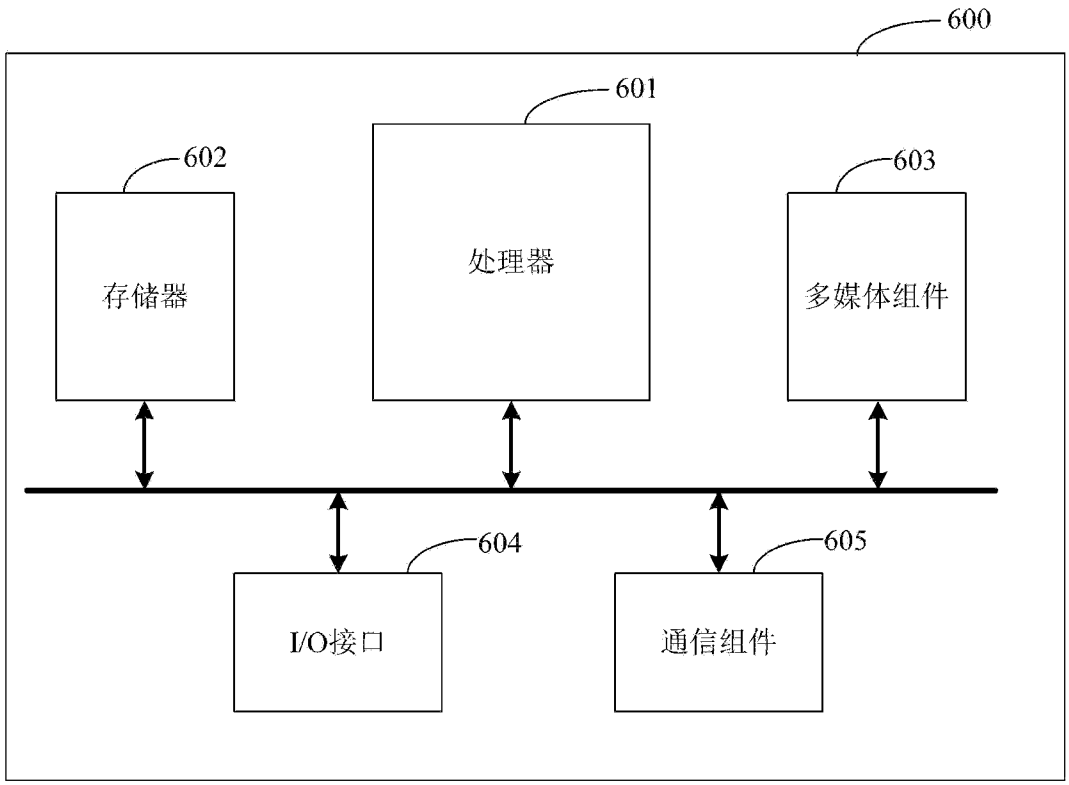
600
601
602
603
存储器
处理器
多媒体组件
604
605
I/O接口
通信组件

图 6

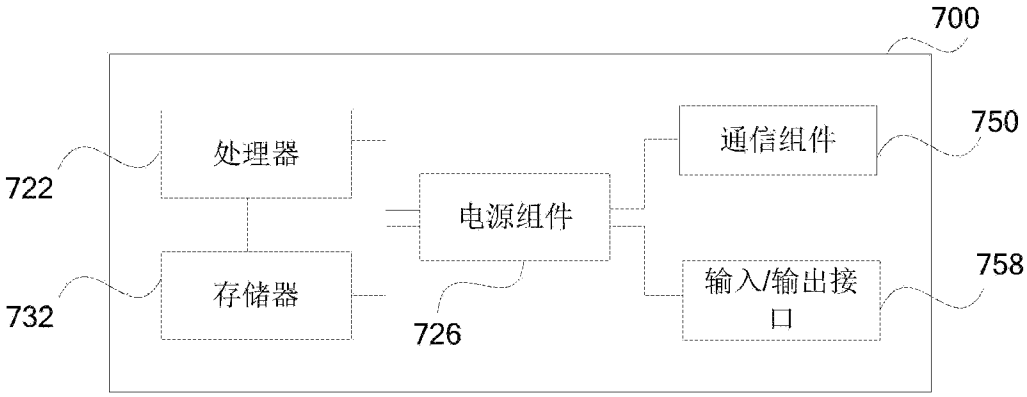

图 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/121891

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/45(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: 区块链, 数字证书, 签名, 标识, 第一, 两个, 多个, CA, 机构, 群, 合法性, 验证, 私钥, 公钥, 签名, 注册, 摘要, blockchain, certificate, authority, digital, identification, public key, private key, register, check, verify

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109992953 A (ONECONNECT FINANCIAL TECHNOLOGY CO., PTE. LTD.) 09 July 2019 (2019-07-09) description, paragraphs [0023]-[0063]	1-20
A	CN 109003083 A (SHANDONG FISHERMAN INFORMATION TECHNOLOGY CO., LTD.) 14 December 2018 (2018-12-14) description, paragraphs [0043]-[0094]	1-20
A	CN 1585326 A (SOUTH CHINA UNIVERSITY OF TECHNOLOGY) 23 February 2005 (2005-02-23) entire document	1-20
A	WO 2018032890 A1 (HUAWEI TECHNOLOGIES CO., LTD.) 22 February 2018 (2018-02-22) entire document	1-20

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 February 2020	**26 February 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/121891

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 109992953 A	09 July 2019	None	
CN 109003083 A	14 December 2018	None	
CN 1585326 A	23 February 2005	None	
WO 2018032890 A1	22 February 2018	EP 3404891 A1	21 November 2018
		CN 107770115 A	06 March 2018
		US 2019057115 A1	21 February 2019

国际检索报告

国际申请号
PCT/CN2019/121891

A. 主题的分类

G06F 21/45(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F; H04L; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

WPI,EPODOC,CNPAT,CNKI； 区块链，数字证书，签名，标识，第一，两个，多个，CA，机构，群，合法性，验证，私钥，公钥，签名，注册，摘要，blockchain，certificate，authority，digital，identification，public key，private key，register，check，verify

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 109992953 A (深圳壹账通智能科技有限公司) 2019年 7月 9日 (2019-07-09) 说明书第[0023]-[0063]段	1-20
A	CN 109003083 A (山东渔翁信息技术股份有限公司) 2018年 12月 14日 (2018-12-14) 说明书第[0043]-[0094]段	1-20
A	CN 1585326 A (华南理工大学) 2005年 2月 23日 (2005-02-23) 全文	1-20
A	WO 2018032890 A1 (华为技术有限公司) 2018年 2月 22日 (2018-02-22) 全文	1-20

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2020年 2月 16日	2020年 2月 26日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	杜少凤
传真号 (86-10)62019451	电话号码 86-(10)-53961593

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/121891

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 109992953 A	2019年 7月 9日	无	
CN 109003083 A	2018年 12月 14日	无	
CN 1585326 A	2005年 2月 23日	无	
WO 2018032890 A1	2018年 2月 22日	EP 3404891 A1	2018年 11月 21日
		CN 107770115 A	2018年 3月 6日
		US 2019057115 A1	2019年 2月 21日