(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 9 月 24 日 (24.09.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/186827 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01)

(21) 国际申请号: PCT/CN2019/122879

(22) 国际申请日: 2019 年 12 月 4 日 (04.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910218385.1 2019年3月21日 (21.03.2019) 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: 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, 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,

WO 2020/186827 A1

(54) **Title:** USER AUTHENTICATION METHOD AND APPARATUS, COMPUTER DEVICE AND COMPUTER-READABLE STORAGE MEDIUM

(54) 发明名称: 用户认证方法、装置、计算机设备及计算机可读存储介质

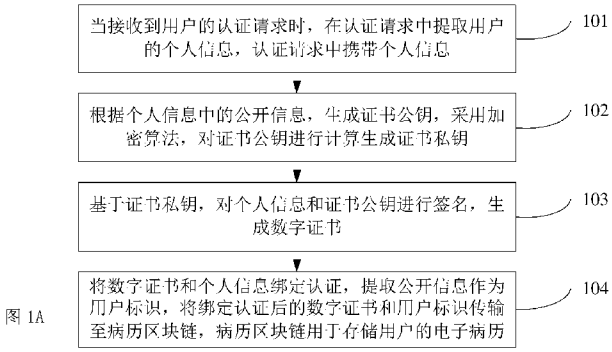

图 1A

101 Extract, upon receiving an authentication request of a user, personal information of the user from the authentication request, wherein the authentication request carries the personal information

102 Generate a certificate public key according to public information in the personal information, and calculate the certificate public key by using an encryption algorithm to generate a certificate private key

103 Sign the personal information and the certificate public key on the basis of the certificate private key to generate a digital certificate

104 Bind and authenticate the digital certificate and the personal information, extract the public information as a user identifier, and transmit the bound and authenticated digital certificate and user identifier to a medical record blockchain, wherein the medical record blockchain is used for storing an electronic medical record of the user

(57) **Abstract:** The present application relates to the technical field of information storage. Disclosed are a user authentication method and apparatus, a computer device and a computer-readable storage medium, capable of generating a digital certificate for a user according to personal information of the user, and implementing the authentication of the user on the basis of the digital certificate without the need to directly use the personal information to perform operations such as information storage, thereby reducing the risk of leakage of the personal information of the user, avoiding serious loss to the user, and achieving better security. The method comprises: extract-

[见续页]

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))。

ing, upon receiving an authentication request of a user, personal information of the user from the authentication request; generating a certificate public key according to public information in the personal information, and calculating the certificate public key by using an encryption algorithm to generate a certificate private key; signing the personal information and the certificate public key on the basis of the certificate private key to generate a digital certificate; and binding and authenticating the digital certificate and the personal information, extracting the public information as a user identifier, and transmitting the bound and authenticated digital certificate and user identifier to a medical record blockchain.

(57) 摘要：本申请公开了一种用户认证方法、装置、计算机设备及计算机可读存储介质，涉及信息存储技术领域，可以根据用户的个人信息为用户生成数字证书，基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。所述方法包括：当接收到用户的认证请求时，在认证请求中提取用户的个人信息；根据个人信息中的公开信息，生成证书公钥，采用加密算法，对证书公钥进行计算，生成证书私钥；基于证书私钥，对个人信息和证书公钥进行签名，生成数字证书；将数字证书和个人信息绑定认证，提取公开信息作为用户标识，将绑定认证后的数字证书和用户标识传输至病历区块链。

用户认证方法、装置、计算机设备及计算机可读存储介质

[0001] 本申请要求于2019年3月21日提交中国专利局、申请号为201910218385.1、发明名称为“用户认证方法、装置、计算机设备及计算机可读存储介质”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

[0002] 本申请涉及信息存储技术领域，特别是涉及一种用户认证方法、装置、计算机设备及计算机可读存储介质。

背景技术

[0003] 随着互联网技术的飞速发展，卫生与健康现代医疗卫生体系的建设规划也越来越成熟，预计到2020年，将建成全面的健康信息平台，实现所在地区各大医院之间信息的互联互通。健康信息平台中采用电子病历的形式存储患者的所有信息以及实时更新的信息，目前已经建立的健康信息平台通常依赖中心化的信息系统所搭载，并基于该中心化的信息系统实现已经认证的用户的电子病历的存储及更新。

[0004] 相关技术中，中心化的信息系统是通过身份认证和授权来保护用户的个人隐私的，也即采用用户的身份证信息、联系方式信息等个人信息对用户的身份进行认证，进而将用户的电子病历与用户的个人信息绑定存储，以便在后续用户治疗时，采用用户提供个人信息的方式来获取用户的电子病历，实现对用户的治疗。

[0005] 在实现本申请的过程中，发明人发现相关技术至少存在以下问题：

[0006] 对用户进行认证使用的个人信息包括了很多用户的私密信息，如果系统出现安全漏洞或管理不善将导致所有的医疗信息泄漏事故，使得用户的私密信息也会被泄露，给用户带来严重的风险和损失，安全性较差。

发明概述

技术问题

[0007] 有鉴于此，本申请提供了一种用户认证方法、装置、计算机设备及计算机可读存储介质，主要目的在于解决目前用户的私密信息也会被泄露，给用户带来严重的风险和损失，安全性较差的问题。

问题的解决方案

技术解决方案

[0008] 本申请第一方面，提供了一种用户认证方法，该方法包括：

[0009] 当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息，所述认证请求中携带所述个人信息；

[0010] 根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

[0011] 基于所述证书私钥，对所述个人信息和所述证书公钥进行签名，生成数字证书；

[0012] 将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[0013] 在另一个实施例中，所述当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息之后，所述方法还包括：

[0014] 对所述个人信息进行验证，判断所述个人信息是否为真实的个人信息；

[0015] 如果确定所述个人信息是真实的个人信息，则继续执行上述获取证书公钥并生成数字证书的过程；

[0016] 如果确定所述个人信息不是真实的个人信息，则生成失败响应，将所述失败响应返回至所述用户。

[0017] 在另一个实施例中，所述根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥，包括：

[0018] 获取公开信息模板，按照所述公开信息模板，在所述个人信息中提取符合所述公开信息模板的公开信息，将所述公开信息作为所述证书公钥；

[0019] 确定所述加密算法，采用所述加密算法，对所述证书公钥进行计算，生成证书私钥，所述加密算法至少为高级加密标准AES算法。

[0020] 本申请第二方面，提供了一种用户认证方法，该方法包括：

[0021] 接收所述认证中心传输的绑定认证的数字证书和用户标识，所述数字证书由所述认证中心对所述用户标识指示的用户进行认证后，并根据所述用户标识指示的用户的个人信息生成；

[0022] 检测病历区块链中至少一个用户信息区块的可用数据量，统计所述绑定认证的数字证书和用户标识的目标数据量，根据所述目标数据量，在所述至少一个用户信息区块中确定目标用户信息区块，所述目标用户信息区块的可用数据量大于等于所述目标数据量；

[0023] 将所述绑定认证的数字证书和用户标识添加至所述目标用户信息区块中进行存储。

[0024] 在另一个实施例中，所述方法还包括：

[0025] 当接收到电子病历存储请求时，确定所述电子病历存储请求中携带的用户标识指示的目标数字证书；

[0026] 对所述目标数字证书进行数据读取，提取所述目标数字证书包括的证书公钥，基于所述证书公钥，对待存储电子病历进行加密，生成病历密文；

[0027] 基于所述病历密文，生成病历区块，将所述病历区块添加至所述病历区块链中存储。

[0028] 在另一个实施例中，所述方法还包括：

[0029] 当接收到电子病历查询请求时，在所述电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名；

[0030] 对所述待查询用户标识、待查询数字证书和所述待查询证书签名进行验证；

[0031] 如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功，则在所述至少一个用户信息区块中查询所述待查询数字证书指示的待查询病历密文，将所述待查询病历密文返回；

[0032] 如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败，则生成失败响应，并返回所述失败响应。

[0033] 在另一个实施例中，所述对所述待查询用户标识、待查询数字证书和所述待查询证书签名进行验证，包括：

[0034] 在所述待查询数字证书中提取待查询证书公钥，采用所述待查询证书公钥对所述待查询证书签名解密，判断所述待查询证书公钥是否成功对所述待查询证书签名解密；

[0035] 在所述病历区块链中查询所述待查询用户标识对应的数字证书与所述待查询数字证书是否一致；

[0036] 相应地，当采用所述待查询证书公钥对所述待查询证书签名解密成功，且确定所述待查询用户标识对应的数字证书与所述待查询数字证书一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功；

[0037] 当采用所述待查询证书公钥对所述待查询证书签名解密失败，或确定所述待查询用户标识对应的数字证书与所述待查询数字证书不一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败。

[0038] 依据本申请第三方面，提供了一种用户认证装置，该装置包括：

[0039] 提取模块，用于当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息，所述认证请求中携带所述个人信息；

[0040] 生成模块，用于根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

[0041] 签名模块，用于基于所述证书私钥，对所述个人信息和所述证书公钥进行签名，生成数字证书；

[0042] 传输模块，用于将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[0043] 在另一个实施例中，所述装置还包括：

[0044] 验证模块，用于对所述个人信息进行验证，判断所述个人信息是否为真实的个人信息；

[0045] 所述生成模块，还用于如果确定所述个人信息是真实的个人信息，则继续执行上述获取证书公钥并生成数字证书的过程；

[0046] 返回模块，用于如果确定所述个人信息不是真实的个人信息，则生成失败响应，将所述失败响应返回至所述用户。

[0047] 在另一个实施例中，所述生成模块，包括：

[0048] 提取子模块，用于获取公开信息模板，按照所述公开信息模板，在所述个人信息中提取符合所述公开信息模板的公开信息，将所述公开信息作为所述证书公钥；

[0049] 计算子模块，用于确定所述加密算法，采用所述加密算法，对所述证书公钥进行计算，生成证书私钥，所述加密算法至少为高级加密标准AES算法。

[0050] 本申请第四方面，提供了一种用户认证装置，该装置包括：

[0051] 接收模块，用于接收所述认证中心传输的绑定认证的数字证书和用户标识，所述数字证书由所述认证中心对所述用户标识指示的用户进行认证后，并根据所述用户标识指示的用户的个人信息生成；

[0052] 统计模块，用于检测病历区块链中至少一个用户信息区块的可用数据量，统计所述绑定认证的数字证书和用户标识的目标数据量，根据所述目标数据量，在所述至少一个用户信息区块中确定目标用户信息区块，所述目标用户信息区块的可用数据量大于等于所述目标数据量；

[0053] 存储模块，用于将所述绑定认证的数字证书和用户标识添加至所述目标用户信息区块中进行存储。

[0054] 在另一个实施例中，所述装置还包括：

[0055] 确定模块，用于当接收到电子病历存储请求时，确定所述电子病历存储请求中携带的用户标识指示的目标数字证书；

[0056] 加密模块，用于对所述目标数字证书进行数据读取，提取所述目标数字证书包括的证书公钥，基于所述证书公钥，对待存储电子病历进行加密，生成病历密文；

[0057] 生成模块，用于基于所述病历密文，生成病历区块，将所述病历区块添加至所述病历区块链中存储。

[0058] 在另一个实施例中，所述装置还包括：

[0059] 提取模块，用于当接收到电子病历查询请求时，在所述电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名；

[0060] 验证模块，用于对所述待查询用户标识、待查询数字证书和所述待查询证书签

名进行验证；

[0061] 第一返回模块，用于如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功，则在所述至少一个用户信息区块中查询所述待查询数字证书指示的待查询病历密文，将所述待查询病历密文返回；

[0062] 第二返回模块，用于如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败，则生成失败响应，并返回所述失败响应。

[0063] 在另一个实施例中，所述验证模块，用于在所述待查询数字证书中提取待查询证书公钥，采用所述待查询证书公钥对所述待查询证书签名解密，判断所述待查询证书公钥是否成功对所述待查询证书签名解密；在所述病历区块链中查询所述待查询用户标识对应的数字证书与所述待查询数字证书是否一致；

[0064] 相应地，所述第一返回模块，用于当采用所述待查询证书公钥对所述待查询证书签名解密成功，且确定所述待查询用户标识对应的数字证书与所述待查询数字证书一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功；

[0065] 所述第二返回模块，用于当采用所述待查询证书公钥对所述待查询证书签名解密失败，或确定所述待查询用户标识对应的数字证书与所述待查询数字证书不一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败。

[0066] 本申请第五方面，提供了一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，所述处理器执行所述计算机可读指令时实现上述第一方面或第二方面所述方法的步骤。

[0067] 本申请第六方面，提供了一种计算机可读存储介质，其上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现上述第一方面或第二方面所述的方法的步骤。

发明的有益效果

有益效果

[0068] 本申请提供的一种用户认证方法、装置、计算机设备及计算机可读存储介质，与目前对用户进行认证使用的个人信息的方式相比，本申请当接收到用户的认

证请求时，在认证请求中提取用户的个人信息，并根据个人信息中的公开信息生成证书公钥以及证书私钥，进而基于证书私钥，生成数字证书，使得根据用户的公开信息为用户生成数字证书，基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。

对附图的简要说明

附图说明

[0069] 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。

[0070] 图1A示出了本申请实施例提供的一种用户认证方法流程示意图；

[0071] 图1B示出了本申请实施例提供的一种用户认证方法流程示意图；

[0072] 图2A示出了本申请实施例提供的一种用户认证方法流程示意图；

[0073] 图2B示出了本申请实施例提供的一种用户认证方法流程示意图；

[0074] 图2C示出了本申请实施例提供的一种用户认证方法流程示意图；

[0075] 图3A示出了本申请实施例提供的一种用户认证装置的结构示意图；

[0076] 图3B示出了本申请实施例提供的一种用户认证装置的结构示意图；

[0077] 图3C示出了本申请实施例提供的一种用户认证装置的结构示意图；

[0078] 图4A示出了本申请实施例提供的一种用户认证装置的结构示意图；

[0079] 图4B示出了本申请实施例提供的一种用户认证装置的结构示意图；

[0080] 图4C示出了本申请实施例提供的一种用户认证装置的结构示意图；

[0081] 图5示出了本申请实施例提供的一种计算机设备的装置结构示意图。

发明实施例

本发明的实施方式

[0082] 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。

[0083] 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。

[0084] 本申请一实施例提供了一种用户认证方法，可以根据用户的个人信息为用户生成数字证书，基于数字证书实现对用户的认证，达到了无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好的目的，如图1A所示，该方法应用于认证中心中，包括：

[0085] 101、当接收到用户的认证请求时，在认证请求中提取用户的个人信息，认证请求中携带个人信息。

[0086] 在本申请实施例中，当接收到用户的认证请求时，为了使认证中心可以获知当前为哪一个用户进行认证，并帮助认证中心对用户进行认证，认证请求中通常会携带个人信息，因此，认证中心可以在认证请求中提取用户的个人信息。

[0087] 102、根据个人信息中的公开信息，生成证书公钥，采用加密算法，对证书公钥进行计算，生成证书私钥。

[0088] 在本申请实施例中，为了使给用户生成的数字证书与用户息息相关，且后续生成的数字证书中需要包括证书公钥和证书私钥，因此，在个人信息中获取证书公钥，并采用加密算法，对证书公钥进行计算，从而生成证书私钥，以便后续基于证书公钥和证书私钥为用户生成数字证书。

[0089] 103、基于证书私钥，对个人信息和证书公钥进行签名，生成数字证书。

[0090] 在本申请实施例中，当确定了证书公钥和证书私钥后，由于下发给病历区块链的数字证书是不能包括证书私钥的，也即该证书私钥是用户自行保管的，因此，基于证书私钥，对个人信息和证书公钥进行签名，生成数字证书。

[0091] 104、将数字证书和个人信息绑定认证，提取公开信息作为用户标识，将绑定认证后的数字证书和用户标识传输至病历区块链，病历区块链用于存储用户的电子病历。

[0092] 在本申请实施例中，为了使病历区块链在接收到数字证书时，可以将数字证书与用户关联起来，以便后续对数字证书进行利用，认证中心在将数字证书传输

至病历区块链之前，可在数字证书中提取用户标识，将数字证书和用户标识传输至病历区块链，病历区块链用于存储用户的电子病历。

[0093] 本申请实施例提供的方法，当接收到用户的认证请求时，在认证请求中提取用户的个人信息，并根据个人信息中的公开信息生成证书公钥以及证书私钥，进而基于证书私钥，生成数字证书，使得根据用户的公开信息为用户生成数字证书，基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。

[0094] 本申请一实施例提供了一种用户认证方法，可以接收认证中心传输的数字证书，基于数字证书实现对用户的认证，达到了无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好的目的，如图1B所示，该方法包括：

[0095] 105、接收认证中心传输的绑定认证的数字证书和用户标识，数字证书由认证中心对用户标识指示的用户进行认证后，并根据用户标识指示的用户的个人信息生成。

[0096] 在本申请实施例中，由于认证中心在生成了数字证书后，会将数字证书和用户标识传输给病历区块链，因此，病历区块链会接收到认证中心传输的数字证书和用户标识。

[0097] 106、检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，目标用户信息区块的可用数据量大于等于目标数据量。

[0098] 在本申请实施例中，由于病历区块链基于区块存储数据，因此，在接收到数字证书和用户标识后，为了避免浪费病历区块链中的存储空间，需要对病历区块链中的至少一个用户信息区块的可用数据量进行检测，找到一个可以容纳绑定认证的数字证书和用户标识的目标数据量的目标用户信息区块，以便可以基于该目标用户信息区块存储绑定认证的数字证书和用户标识的目标数据量。107、将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储。

[0099] 在本申请实施例中，当生成了用户信息区块后，便可以将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储，完成用户的认证以及注册。

[0100] 本申请实施例提供的方法，接收认证中心传输的绑定认证的数字证书和用户标识，并检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储，使得基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。

[0101] 本申请一实施例提供了一种用户认证方法，可以根据用户的个人信息为用户生成数字证书，基于数字证书实现对用户的认证，达到了无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好的目的，如图2A所示，该方法应用于认证中心和病历区块链中，涉及到认证中心和病历区块链之间的交互，具体包括：

[0102] 201、当接收到用户的认证请求时，认证中心在认证请求中提取用户的个人信息，认证请求中携带个人信息。

[0103] 在本申请实施例中，为了避免不法分子随意的在病历区块链中上传并下载数据，认证中心为用户提供认证服务，基于用户的个人信息为用户进行认证，使得后续只有通过认证的用户才可以使用病历区块链所提供的各种服务，从而避免不法分子进行恶意操作。认证中心可以为用户提供客户端，用户通过下载客户端来享受认证中心提供的用户认证服务。客户端中为用户提供注册入口，当检测到用户触发该注册入口时，确定检测到用户请求注册，显示注册页面。在检测到用户对注册页面的确认时，确定接收到用户的认证请求，认证中心获取用户在注册页面中填写的个人信息，从而获取到用户的个人信息，也即在认证请求中提取用户的个人信息，以便在后续可以基于用户的个人信息对用户进行认证。具体地，用户提供的个人信息可以包括用户的身份证号码、社保账号、姓名等信息。

[0104] 在实际应用的过程中，由于每个人的身份证号码与姓名是具有唯一对应关系的

，考虑到有些不法分子为了在认证中心中认证，可能提供假的身份证号码或者假的姓名等，因此，在提取到用户的个人信息后，可以对用户的个人信息的真实性进行验证，并在确定个人信息是真实的时，再继续为用户提供认证服务。具体地，在对个人信息进行验证时，获取数据库中预设的身份证号码与姓名之间的对应关系，判断用户提供的个人信息中的身份证号码以及姓名的对应关系是否可与数据库中存储的对应关系匹配，也即判断个人信息是否为真实的个人信息。如果确定个人信息是真实的个人信息，则表示当前用户提供的个人信息是真实的，可以继续执行上述获取证书公钥并生成数字证书的过程；如果确定个人信息不是真实的个人信息，则表示当前用户提供的个人信息是虚假的，或者用户提供的个人信息发生了错误，需要用户重新提供，因此，生成失败响应，将失败响应返回至用户。需要说明的是，为了使用户可以明确哪一些信息发生了错误，生成的失败响应中可以显示发生错误的那一项信息，以便用户对信息进行修改，并重新提供正确的个人信息。

[0105] 202、认证中心获取公开信息模板，按照公开信息模板，在个人信息中提取符合公开信息模板的公开信息，将公开信息作为证书公钥。

[0106] 在本申请实施例中，由于后续生成的数字证书是具有证书公钥和证书私钥的，证书私钥和证书公钥可以相互解密和加密，且证书公钥是公开的，而证书私钥是用户自己持有的，为了使后续给用户生成的数字证书与用户是相关的，从而在保证数字证书的唯一性的同时，还可以将数字证书与用户关联起来，可以在个人信息中提取公开信息，并将公开信息作为证书公钥，进而基于该公开信息为用户生成数字证书。

[0107] 其中，由于用户提供的个人信息中有些信息是可以公开的，有些是私密信息不便于公开，因此，认证中心中可以设置一个确定哪些信息是可以公开的标准，也即设置一个公开信息模板，并按照公开信息模板在用户提供的个人信息中提取公开信息，将提取到的公开信息作为证书公钥。具体地，公开信息可为用户的个人信息中的社保账号。本申请实施例对公开信息包括的内容不进行具体限定。

[0108] 203、认证中心确定加密算法，采用加密算法，对证书公钥进行计算，生成证

书私钥。

[0109] 在本申请实施例中，当确定了证书公钥后，为了使证书公钥与证书私钥是对应的，从而实现证书公钥和证书私钥之间可以相互加密或者解密，认证中心确定加密算法，并采用该加密算法，对证书公钥进行计算，从而生成证书私钥，以便后续基于证书私钥和证书公钥生成数字证书。其中，加密算法可以为高级加密标准（Advanced Encryption Standard，AES）算法。本申请实施例对加密算法为哪一种算法不进行具体限定。

[0110] 204、基于证书私钥，认证中心对个人信息和证书公钥进行签名，生成数字证书。

[0111] 在本申请实施例中，当生成了证书私钥后，便可以基于证书私钥、证书公钥和个人信息为该用户生成数字证书。为了使生成的数字证书与用户是相关的，且生成的数字证书具有唯一性，在生成数字证书时，认证中心可以基于证书私钥，对个人信息和证书公钥进行签名，将签名得到的结果作为数字证书。其中，由于数字证书是需要上传至病历区块链中，由病历区块链在存储电子病历时使用的，因此，数字证书中仅包括证书公钥，并没有包括证书私钥，证书私钥是需要认证中心下发给用户自行保存的，以便用户基于该证书私钥可以在病历区块链中请求电子病历查询、电子病历存储等操作。

[0112] 205、认证中心将数字证书和个人信息绑定认证，提取公开信息作为用户标识，将绑定认证后的数字证书和用户标识传输至病历区块链。

[0113] 在本申请实施例中，病历区块链用于存储用户的电子病历。为了使病历区块链可以基于数字证书为用户提供病历存储、病历查询等服务，认证中心在生成了数字证书后，将该数字证书和个人信息绑定认证，并将该数字证书传输给病历区块链，以便病历区块链将该数字证书存储。

[0114] 考虑到病历区块链在同一时间可能会接收到大量的数字证书，很容易造成数字证书与用户之间对应关系的混淆，因此，认证中心在将数字证书传输给病历区块链之前，先在个人信息中提取用户的用户标识，并将数字证书和用户标识对应传输至病历区块链。其中，认证中心在将数字证书和用户标识对应传输至病历区块链中时，可以采用用户标识对数字证书进行标记，实现将数字证书与用

户标识一一对应。具体地，用户标识可为姓名、社保账号等，或者还可直接将个人信息中的公开信息作为用户标识，本申请实施例对用户标识不进行具体限定。

[0115] 需要说明的是，在将数字证书和用户标识传输至病历区块链后，由于用户也需要获知在认证中心中认证得到的数字证书，且需要用户将证书私钥自行保存，因此，认证中心还将数字证书和证书私钥下发给用户，以便用户将数字证书和证书私钥存储。

[0116] 206、病历区块链接收认证中心传输的绑定认证的数字证书和用户标识，检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储。

[0117] 在本申请实施例中，当病历区块链接收到认证中心传输的数字证书和用户标识后，便确定该用户在认证中心中认证成功了。由于病历区块链是采用区块的形式存储数据的，考虑到有一些用户信息区块还没有饱和，因此，病历区块链在存储绑定认证的数字证书和用户标识时，首先，检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量；随后，将至少一个用户信息区块的可用数据量与目标数据量进行比对，将可用数据量大于等于目标数据量的用户信息区块作为目标用户区块，将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储。需要说明的是，在确定目标用户区块时，可能有多个用户信息区块的可用数据量均大于等于目标数据量，则此时可以在多个用户信息区块中选取可用数据量最小的来存储绑定认证的数字证书和用户标识，或者随机选取一个用户信息区块存储绑定认证的数字证书和用户标识。本申请实施例对选取目标用户信息区块的方式不进行具体限定。

[0118] 通过执行上述步骤201至步骤206中所示的过程，用户便可以完成在认证中心中的认证，使得认证中心为用户生成并下发数字证书，这样，用户便可以继续在病历区块链中请求存储电子病历，该方法应用于病历区块链中，参见图2B，具

体包括：

[0119] 207、当接收到电子病历存储请求时，病历区块链确定电子病历存储请求中携带的用户标识指示的目标数字证书。

[0120] 在本申请实施例中，由于病历区块链中存储有每一个在认证中心中注册过的用户的数字证书，因此，在接收到携带有用户标识的电子病历存储请求时，病历区块链可基于该用户标识进行查找，查找与该用户标识对应的数字证书作为目标数字证书，以便在后续基于该目标数字证书对接收到的待存储电子病历进行加密，保证电子病历存储的安全性。需要说明的是，确定用户标识指示的目标电子证书的过程也是对用户身份进行检测的过程，如果未能确定用户标识指示的目标电子证书，也即病历区块链中没有存储用户标识指示的目标电子证书，则表明用户尚未在区块链中进行注册，需要用户在认证中心中进行注册后才可以将电子病历存储在病历区块链中，这样，便不能继续执行下述操作。

[0121] 208、病历区块链对目标数字证书进行数据读取，提取目标数字证书包括的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文。

[0122] 在本申请实施例中，当根据电子病历存储请求中携带的用户标识确定了目标数字证书后，由于目标数字证书中包括证书公钥，为了保证待存储电子病历的存储安全，可以在目标数字证书中提取证书公钥，基于该证书公钥，对该待存储电子病历进行加密，生成包括待存储电子病历的病历密文，并在后续将该病历密文进行存储，以便保证待存储电子病历的安全性。

[0123] 209、病历区块链基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储。

[0124] 在本申请实施例中，由于在存储病历密文时，是由病历区块链存储的，因此，在生成病历密文后，为了将病历密文存储，基于病历密文，生成包括病历密文的病历区块，将该病历区块添加至病历区块链中存储，从而完成待存储电子病历的存储。

[0125] 需要说明的是，由于每一个用户端中都存储有与一个相同且同步的病历区块链，为了保证每一个用户端中的病历区块链的数据是一致的，从而使得在哪一个用户端中均可以实现对电子病历的查询，因此，在将病历区块添加至病历区块

链中存储后，将生成的病历区块广播给每一个用户端，以便每一个用户端均将该病历区块添加至自身存储的病历区块链中，从而保证数据的一致性。

[0126] 在实际应用的过程中，用户在医院中看病时，需要医院在病历区块链中获取用户之前的电子病历，因此，病历区块链还为用户提供电子病历查询服务，参见图2C，该方法包括：

[0127] 210、当病历区块链接收到电子病历查询请求时，在电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名。

[0128] 在本申请实施例中，用户端为用户提供查询入口，当检测到用户触发该查询入口时，确定检测到用户请求查询。由于病历区块链中存储电子病历与用户标识是一一对应的，因此，需要用户提供待查询用户标识，以便按照该待查询用户标识查询指定的电子病历；另外，为了保证电子病历的安全性，避免电子病历被不法分子获取，造成电子病历中信息的泄露，在需要用户提供待查询用户标识的同时，还需要用户提供待查询数字证书，以便通过对该待查询数字证书进行验证来实现对请求进行电子病历查询的用户的身份的验证。而且，为了进一步保证后续传输的查询请求的安全性，避免查询请求在传输的过程中被篡改，病历区块链接收到的电子病历查询请求中还可能会携带用户端采用待查询证书私钥对待查询数字证书进行签名生成的待查询证书签名，这样，病历区块链还需要将该待查询证书签名提取出来，以便后续通过对该待查询证书签名进行验证来确定生成的查询请求是否被篡改。

[0129] 211、病历区块链对待查询用户标识、待查询数字证书和待查询证书签名进行验证，如果对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则执行下述步骤212；如果对待查询用户标识、待查询数字证书和待查询证书签名验证失败，则执行下述步骤213。

[0130] 在本申请实施例中，在本申请实施例中，当病历区块链提取到待查询用户标识、待查询数字证书以及待查询证书签名后，便通过对待查询用户标识、待查询数字证书和待查询证书签名进行验证，实现对用户的身份进行验证。具体地，在对待查询用户标识、待查询数字证书和待查询证书签名进行验证时，首先，在待查询数字证书中提取待查询证书公钥，采用待查询证书公钥对待查询证书

签名解密，判断待查询证书公钥是否成功对待查询证书签名解密。待验证证书签名是基于待验证数字证书的待验证证书私钥对待验证证书进行签名得到的，因此，基于公私钥对可以相互加密和解密的属性，可以采用待验证证书公钥对待验证证书签名解密，并根据是否签名成功来确定待验证证书签名的真实性。随后，为了验证该用户是否在病历区块链中注册过，避免未能在病历区块链中注册的不法分子将恶意信息混入病历区块链中，因此，需要根据待查询用户标识验证用户是否在病历区块链中注册过，也即在病历区块链中查询待查询用户标识对应的数字证书与待查询数字证书是否一致。

[0131] 这样，当采用待查询证书公钥对待查询证书签名解密成功，且确定病历区块链中存储有与待查询用户标识对应的待查询用户信息时，确定对待查询用户标识、待查询数字证书和待查询证书签名验证成功，这时，便可以为用户返回请求查询的电子病历，也即执行下述步骤212；当采用待查询证书公钥对待查询证书签名解密失败，或确定病历区块链中未存储有与待查询用户标识对应的待查询用户信息时，确定对待查询用户标识、待查询数字证书和待查询证书签名验证失败，这时，表示用户的身份无法确定，或者用户未在认证中心中认证过，此时，便需要用户重新发送查询请求，也即执行下述步骤213。

[0132] 212、如果对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则病历区块链确定待查询数字证书指示的待查询病历密文，将待查询病历密文返回。

[0133] 在本申请实施例中，如果病历区块链对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则表示待查询用户标识指示的用户在认证中心中认证过，且身份已经通过了验证，此时，便可以向用户返回其想要查询的电子病历。

[0134] 需要说明的是，由于病历区块链中在存储电子病历时，是生成了包括电子病历的病历密文进行存储的，因此，病历区块链根据待查询用户标识获取到的也是病历密文，这样，病历区块链便将获取到的待查询病历密文返回至用户端，以便用户端通过对该病历密文进行解密实现对电子病历的查看。

[0135] 213、如果对待查询用户标识、待查询数字证书和待查询证书签名验证失败，

则病历区块链生成失败响应，并返回失败响应。

[0136] 在本申请实施例中，如果病历区块链对待查询用户标识、待查询数字证书和待查询证书签名验证失败，则表示对用户的身份验证失败了，或者用户没有在认证中心中认证，因此，生成失败响应，并返回失败响应。

[0137] 本申请实施例提供的方法，当接收到用户的认证请求时，在认证请求中提取用户的个人信息，并根据个人信息中的公开信息生成证书公钥以及证书私钥，进而基于证书私钥，生成数字证书，使得根据用户的公开信息为用户生成数字证书，基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。

[0138] 应理解，上述实施例中各步骤的序号的大小并不意味着执行顺序的先后，各过程的执行顺序应以其功能和内在逻辑确定，而不应对本申请实施例的实施过程构成任何限定。

[0139] 对应于上文实施例所述的用户认证方法，本申请实施例还提供了一种用户认证装置，为了便于说明，仅示出了与本申请实施例相关的部分。

[0140] 进一步地，作为图1A所述方法的具体实现，本申请实施例提供了一种用户认证装置，如图3A所示，所述装置包括：提取模块301，生成模块302，签名模块303和传输模块304。

[0141] 该提取模块301，用于当接收到用户的认证请求时，在认证请求中提取用户的个人信息，认证请求中携带个人信息；

[0142] 该生成模块302，用于根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

[0143] 该签名模块303，用于基于证书私钥，对个人信息和证书公钥进行签名，生成数字证书；

[0144] 该传输模块304，用于将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[0145] 在具体的应用场景中，如图3B所示，该装置还包括验证模块305和返回模块306

。

[0146] 该验证模块305，用于对个人信息进行验证，判断个人信息是否为真实的个人信息；

[0147] 该生成模块302，还用于如果确定个人信息是真实的个人信息，则继续执行上述获取证书公钥并生成数字证书的过程；

[0148] 该返回模块306，用于如果确定个人信息不是真实的个人信息，则生成失败响应，将失败响应返回至用户。

[0149] 在具体的应用场景中，如图3C所示，该生成模块302，包括提取子模块3021和计算子模块3022。

[0150] 该提取子模块3021，用于获取公开信息模板，按照公开信息模板，在个人信息中提取符合公开信息模板的公开信息，将公开信息作为证书公钥；

[0151] 该计算子模块3022，用于确定加密算法，采用加密算法，对证书公钥进行计算，生成证书私钥，加密算法至少为高级加密标准AES算法。

[0152] 本申请实施例提供的装置，可以当接收到用户的认证请求时，在认证请求中提取用户的个人信息，并根据个人信息中的公开信息生成证书公钥以及证书私钥，进而基于证书私钥，生成数字证书，使得根据用户的公开信息为用户生成数字证书，基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。

[0153] 进一步地，作为图1B所述方法的具体实现，本申请实施例提供了一种用户认证装置，如图4A所示，所述装置包括：接收模块401，统计模块402和存储模块403。

[0154] 该接收模块401，用于接收认证中心传输的绑定认证的数字证书和用户标识，数字证书由认证中心对用户标识指示的用户进行认证后，并根据用户标识指示的用户的个人信息生成；

[0155] 该统计模块402，用于检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，目标用户信息区块的可用数据

量大于等于目标数据量；

[0156] 该存储模块403，用于将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储。

[0157] 在具体的应用场景中，如图4B所示，该装置还包括确定模块404，加密模块405和生成模块406。

[0158] 该确定模块404，用于当接收到电子病历存储请求时，确定电子病历存储请求中携带的用户标识指示的目标数字证书；

[0159] 该加密模块405，用于对目标数字证书进行数据读取，提取目标数字证书包括的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文；

[0160] 该生成模块406，用于基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储。

[0161] 在具体的应用场景中，如图4C所示，该装置还包括提取模块407，验证模块408，第一返回模块409和第二返回模块410。

[0162] 该提取模块407，用于当接收到电子病历查询请求时，在电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名；

[0163] 该验证模块408，用于对待查询用户标识、待查询数字证书和待查询证书签名进行验证；

[0164] 该第一返回模块409，用于如果对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则在至少一个用户信息区块中查询待查询数字证书指示的待查询病历密文，将待查询病历密文返回；

[0165] 该第二返回模块410，用于如果对待查询用户标识、待查询数字证书和待查询证书签名验证失败，则生成失败响应，并返回失败响应。

[0166] 在具体的应用场景中，该验证模块408，用于在待查询数字证书中提取待查询证书公钥，采用待查询证书公钥对待查询证书签名解密，判断待查询证书公钥是否成功对待查询证书签名解密；在病历区块链中查询待查询用户标识对应的数字证书与待查询数字证书是否一致；

[0167] 相应地，该第一返回模块409，用于当采用待查询证书公钥对待查询证书签名解密成功，且确定待查询用户标识对应的数字证书与待查询数字证书一致时，

确定对待查询用户标识、待查询数字证书和待查询证书签名验证成功；

[0168] 该第二返回模块410，用于当采用待查询证书公钥对所述待查询证书签名解密失败，或确定所述待查询用户标识对应的数字证书与所述待查询数字证书不一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败。

[0169] 本申请实施例提供的装置，接收认证中心传输的绑定认证的数字证书和用户标识，并检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储，使得基于数字证书实现对用户的认证，无需直接使用个人信息进行信息存储等操作，降低用户的个人信息被泄露的风险，避免给用户带来严重的损失，安全性较好。

[0170] 需要说明的是，本申请实施例提供的一种用户认证装置所涉及各功能单元的其他相应描述，可以参考图1A至图1B和图2A至图2C中的对应描述，在此不再赘述。

[0171] 在示例性实施例中，参见图5，本申请还提供了一种设备，该设备500包括通信总线、处理器、存储器和通信接口，还可以包括、输入输出接口和显示设备，其中，各个功能单元之间可以通过总线完成相互间的通信。该存储器存储有计算机可读指令，处理器，用于执行存储器上所存放的程序，执行上述实施例中任一实施例的用户认证方法。

[0172] 本申请还提供一种计算机可读存储介质，其上存储有计算机可读指令，所述计算机可读指令被处理器执行时实现所述实施例中任一实施例的用户认证方法的步骤。

[0173] 示例性的，所述计算机可读指令可以被分割成一个或多个模块/单元，所述一个或者多个模块/单元被存储在所述存储器中，并由所述处理器执行，以完成本申请。所述一个或多个模块/单元可以是能够完成特定功能的一系列计算机可读指令指令段，该指令段用于描述所述计算机可读指令在所述设备中的执行过程。

[0174] 所述设备可以是智能电话、电脑、平板、服务器等。所述设备可包括，但不仅限于，处理器、存储器。本领域技术人员可以理解，图5仅仅是设备500的示例，并不构成对设备500的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件，例如所述设备还可以包括输入输出设备、网络接入设备、总线等。

[0175] 所称处理器可以是中央处理单元(Central Processing Unit，CPU)，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。

[0176] 所述存储器可以是所述设备的内部存储单元，例如设备的硬盘或内存。所述存储器也可以是所述设备的外部存储设备，例如所述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，所述存储器还可以既包括所述设备的内部存储单元也包括外部存储设备。所述存储器用于存储所述计算机可读指令以及所述设备所需的其他程序和数据。所述存储器还可以用于暂时地存储已经输出或者将要输出的数据。

[0177] 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。

[0178] 所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，仅以上述各功能单元、模块的划分进行举例说明，实际应用中，可以根据需要而将上述功能分配由不同的功能单元、模块完成，即将所述装置的内部结构划分成不同的功能单元或模块，以完成以上描述的全部或者部分功能。实施例中的各功能单元、模块可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中，上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。另外，各功能单元、模块的具体名称也只是为了便于相互区分，并不用于限制本申请的保护范围。上述系统中单元、模块的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。

[0179] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述或记载的部分，可以参见其它实施例的相关描述。

[0180] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0181] 另外，在本申请各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。

[0182] 所述集成的模块/单元如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本申请实现上述实施例方法中的全部或部分流程，也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计算机可读存储介质中，该计算机可读指令在被处理器执行时，可实现上述各个方法实施例的步骤

。

[0183] 以上所述实施例仅用以说明本申请的技术方案，而非对其限制；尽管参照前述实施例对本申请进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本申请各实施例技术方案的精神和范围，均应包含在本申请的保护范围之内。

权利要求书

[权利要求 1] 一种用户认证方法，其特征在于，包括：

当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息，所述认证请求中携带所述个人信息；

根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

基于所述证书私钥，对所述个人信息和所述证书公钥进行签名，生成数字证书；

将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[权利要求 2] 根据权利要求1所述的方法，其特征在于，所述当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息之后，所述方法还包括：

对所述个人信息进行验证，判断所述个人信息是否为真实的个人信息；

如果确定所述个人信息是真实的个人信息，则继续执行上述获取证书公钥并生成数字证书的过程；

如果确定所述个人信息不是真实的个人信息，则生成失败响应，将所述失败响应返回至所述用户。

[权利要求 3] 根据权利要求1所述的方法，其特征在于，所述根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥，包括：

获取公开信息模板，按照所述公开信息模板，在所述个人信息中提取符合所述公开信息模板的公开信息，将所述公开信息作为所述证书公钥；

确定所述加密算法，采用所述加密算法，对所述证书公钥进行计算，生成证书私钥，所述加密算法至少为高级加密标准AES算法。

[权利要求 4] 一种用户认证方法，其特征在于，包括：

接收所述认证中心传输的绑定认证的数字证书和用户标识，所述数字证书由所述认证中心对所述用户标识指示的用户进行认证后，并根据所述用户标识指示的用户的个人信息生成；

检测病历区块链中至少一个用户信息区块的可用数据量，统计所述绑定认证的数字证书和用户标识的目标数据量，根据所述目标数据量，在所述至少一个用户信息区块中确定目标用户信息区块，所述目标用户信息区块的可用数据量大于等于所述目标数据量；

将所述绑定认证的数字证书和用户标识添加至所述目标用户信息区块中进行存储。

[权利要求 5] 根据权利要求4所述的方法，其特征在于，所述方法还包括：

当接收到电子病历存储请求时，确定所述电子病历存储请求中携带的用户标识指示的目标数字证书；

对所述目标数字证书进行数据读取，提取所述目标数字证书包括的证书公钥，基于所述证书公钥，对待存储电子病历进行加密，生成病历密文；

基于所述病历密文，生成病历区块，将所述病历区块添加至所述病历区块链中存储。

[权利要求 6] 根据权利要求4所述的方法，其特征在于，所述方法还包括：

当接收到电子病历查询请求时，在所述电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名；

对所述待查询用户标识、待查询数字证书和所述待查询证书签名进行验证；

如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功，则在所述至少一个用户信息区块中查询所述待查询数字证书指示的待查询病历密文，将所述待查询病历密文返回；

如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败，则生成失败响应，并返回所述失败响应。

[权利要求 7] 根据权利要求6所述的方法，其特征在于，所述对所述待查询用户标识、待查询数字证书和所述待查询证书签名进行验证，包括：

在所述待查询数字证书中提取待查询证书公钥，采用所述待查询证书公钥对所述待查询证书签名解密，判断所述待查询证书公钥是否成功对所述待查询证书签名解密；

在所述病历区块链中查询所述待查询用户标识对应的数字证书与所述待查询数字证书是否一致；

相应地，当采用所述待查询证书公钥对所述待查询证书签名解密成功，且确定所述待查询用户标识对应的数字证书与所述待查询数字证书一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功；

当采用所述待查询证书公钥对所述待查询证书签名解密失败，或确定所述待查询用户标识对应的数字证书与所述待查询数字证书不一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败。

[权利要求 8] 一种用户认证装置，其特征在于，包括：

提取模块，用于当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息，所述认证请求中携带所述个人信息；

生成模块，用于根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

签名模块，用于基于所述证书私钥，对所述个人信息和所述证书公钥进行签名，生成数字证书；

传输模块，用于将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[权利要求 9] 一种用户认证装置，其特征在于，包括：

接收模块，用于接收所述认证中心传输的绑定认证的数字证书和用户标识，所述数字证书由所述认证中心对所述用户标识指示的用户进行

认证后，并根据所述用户标识指示的用户的个人信息生成；

统计模块，用于检测病历区块链中至少一个用户信息区块的可用数据量，统计所述绑定认证的数字证书和用户标识的目标数据量，根据所述目标数据量，在所述至少一个用户信息区块中确定目标用户信息区块，所述目标用户信息区块的可用数据量大于等于所述目标数据量；

存储模块，用于将所述绑定认证的数字证书和用户标识添加至所述目标用户信息区块中进行存储。

[权利要求 10] 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息，所述认证请求中携带所述个人信息；

根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

基于所述证书私钥，对所述个人信息和所述证书公钥进行签名，生成数字证书；

将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[权利要求 11] 根据权利要求10所述的计算机设备，其特征在于，所述当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息之后，还包括：

对所述个人信息进行验证，判断所述个人信息是否为真实的个人信息；

如果确定所述个人信息是真实的个人信息，则继续执行上述获取证书公钥并生成数字证书的过程；

如果确定所述个人信息不是真实的个人信息，则生成失败响应，将所述失败响应返回至所述用户。

[权利要求 12] 根据权利要求10所述的计算机设备，其特征在于，所述根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥，包括：

获取公开信息模板，按照所述公开信息模板，在所述个人信息中提取符合所述公开信息模板的公开信息，将所述公开信息作为所述证书公钥；

确定所述加密算法，采用所述加密算法，对所述证书公钥进行计算，生成证书私钥，所述加密算法至少为高级加密标准AES算法。

[权利要求 13] 一种计算机设备，包括存储器和处理器，所述存储器存储有计算机可读指令，其特征在于，所述处理器执行所述计算机可读指令时实现如下步骤：

接收所述认证中心传输的绑定认证的数字证书和用户标识，所述数字证书由所述认证中心对所述用户标识指示的用户进行认证后，并根据所述用户标识指示的用户的个人信息生成；

检测病历区块链中至少一个用户信息区块的可用数据量，统计所述绑定认证的数字证书和用户标识的目标数据量，根据所述目标数据量，在所述至少一个用户信息区块中确定目标用户信息区块，所述目标用户信息区块的可用数据量大于等于所述目标数据量；

将所述绑定认证的数字证书和用户标识添加至所述目标用户信息区块中进行存储。

[权利要求 14] 根据权利要求13所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

当接收到电子病历存储请求时，确定所述电子病历存储请求中携带的用户标识指示的目标数字证书；

对所述目标数字证书进行数据读取，提取所述目标数字证书包括的证书公钥，基于所述证书公钥，对待存储电子病历进行加密，生成病历密文；

基于所述病历密文，生成病历区块，将所述病历区块添加至所述病历

区块链中存储。

[权利要求 15] 根据权利要求13所述的计算机设备，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

当接收到电子病历查询请求时，在所述电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名；

对所述待查询用户标识、待查询数字证书和所述待查询证书签名进行验证；

如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功，则在所述至少一个用户信息区块中查询所述待查询数字证书指示的待查询病历密文，将所述待查询病历密文返回；

如果对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败，则生成失败响应，并返回所述失败响应。

[权利要求 16] 根据权利要求15所述的计算机设备，其特征在于，所述对所述待查询用户标识、待查询数字证书和所述待查询证书签名进行验证，包括：

在所述待查询数字证书中提取待查询证书公钥，采用所述待查询证书公钥对所述待查询证书签名解密，判断所述待查询证书公钥是否成功对所述待查询证书签名解密；

在所述病历区块链中查询所述待查询用户标识对应的数字证书与所述待查询数字证书是否一致；

相应地，当采用所述待查询证书公钥对所述待查询证书签名解密成功，且确定所述待查询用户标识对应的数字证书与所述待查询数字证书一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证成功；

当采用所述待查询证书公钥对所述待查询证书签名解密失败，或确定所述待查询用户标识对应的数字证书与所述待查询数字证书不一致时，确定对所述待查询用户标识、所述待查询数字证书和所述待查询证书签名验证失败。

[权利要求 17] 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处理器执行时实现如下步骤：

当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息，所述认证请求中携带所述个人信息；

根据所述个人信息中的公开信息，生成证书公钥，采用加密算法，对所述证书公钥进行计算，生成证书私钥；

基于所述证书私钥，对所述个人信息和所述证书公钥进行签名，生成数字证书；

将所述数字证书和所述个人信息绑定认证，提取所述公开信息作为用户标识，将绑定认证后的所述数字证书和所述用户标识传输至病历区块链，所述病历区块链用于存储用户的电子病历。

[权利要求 18] 根据权利要求17所述的计算机可读存储介质，其特征在于，所述当接收到用户的认证请求时，在所述认证请求中提取所述用户的个人信息之后，还包括：

对所述个人信息进行验证，判断所述个人信息是否为真实的个人信息；

如果确定所述个人信息是真实的个人信息，则继续执行上述获取证书公钥并生成数字证书的过程；

如果确定所述个人信息不是真实的个人信息，则生成失败响应，将所述失败响应返回至所述用户。

[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处理器执行时实现如下步骤：

接收所述认证中心传输的绑定认证的数字证书和用户标识，所述数字证书由所述认证中心对所述用户标识指示的用户进行认证后，并根据所述用户标识指示的用户的个人信息生成；

检测病历区块链中至少一个用户信息区块的可用数据量，统计所述绑定认证的数字证书和用户标识的目标数据量，根据所述目标数据量，

在所述至少一个用户信息区块中确定目标用户信息区块，所述目标用户信息区块的可用数据量大于等于所述目标数据量；

将所述绑定认证的数字证书和用户标识添加至所述目标用户信息区块中进行存储。

[权利要求 20] 根据权利要求19所述的计算机可读存储介质，其特征在于，所述处理器执行所述计算机可读指令时还实现如下步骤：

当接收到电子病历存储请求时，确定所述电子病历存储请求中携带的用户标识指示的目标数字证书；

对所述目标数字证书进行数据读取，提取所述目标数字证书包括的证书公钥，基于所述证书公钥，对待存储电子病历进行加密，生成病历密文；

基于所述病历密文，生成病历区块，将所述病历区块添加至所述病历区块链中存储。

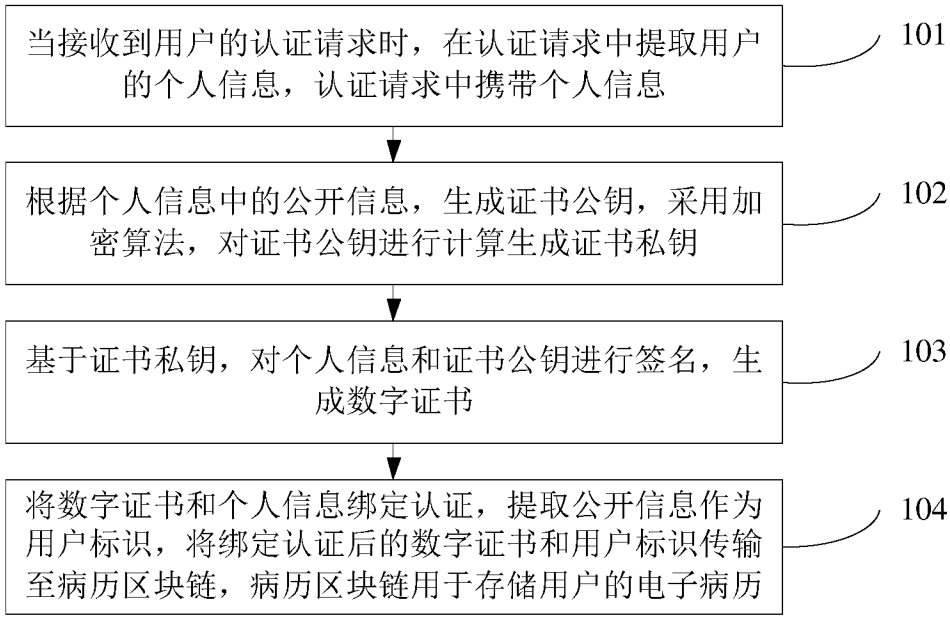
当接收到用户的认证请求时，在认证请求中提取用户的个人信息，认证请求中携带个人信息
101
根据个人信息中的公开信息，生成证书公钥，采用加密算法，对证书公钥进行计算生成证书私钥
102
基于证书私钥，对个人信息和证书公钥进行签名，生成数字证书
103
将数字证书和个人信息绑定认证，提取公开信息作为用户标识，将绑定认证后的数字证书和用户标识传输至病历区块链，病历区块链用于存储用户的电子病历
104

图 1A

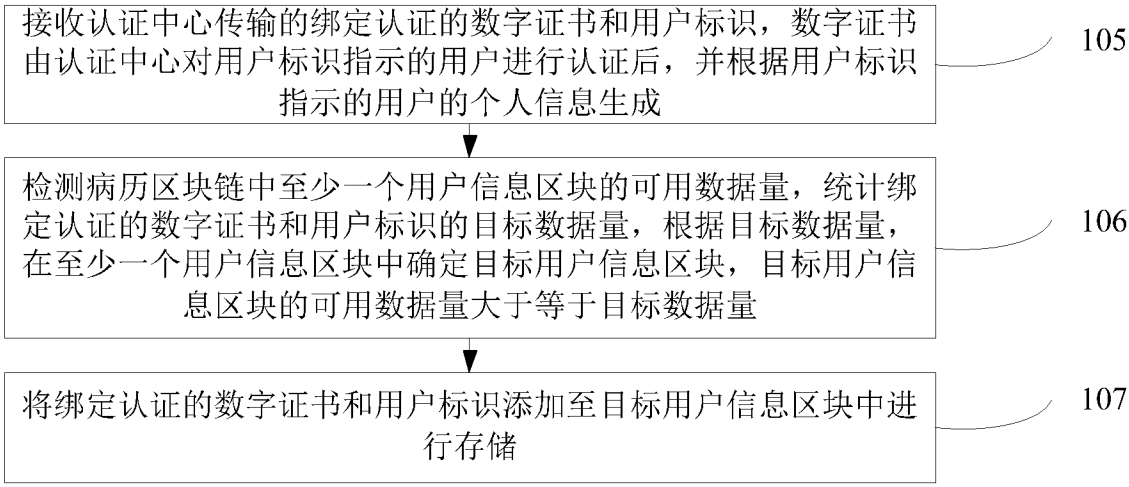
接收认证中心传输的绑定认证的数字证书和用户标识，数字证书由认证中心对用户标识指示的用户进行认证后，并根据用户标识指示的用户的个人信息生成
105
检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，目标用户信息区块的可用数据量大于等于目标数据量
106
将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储
107

图 1B

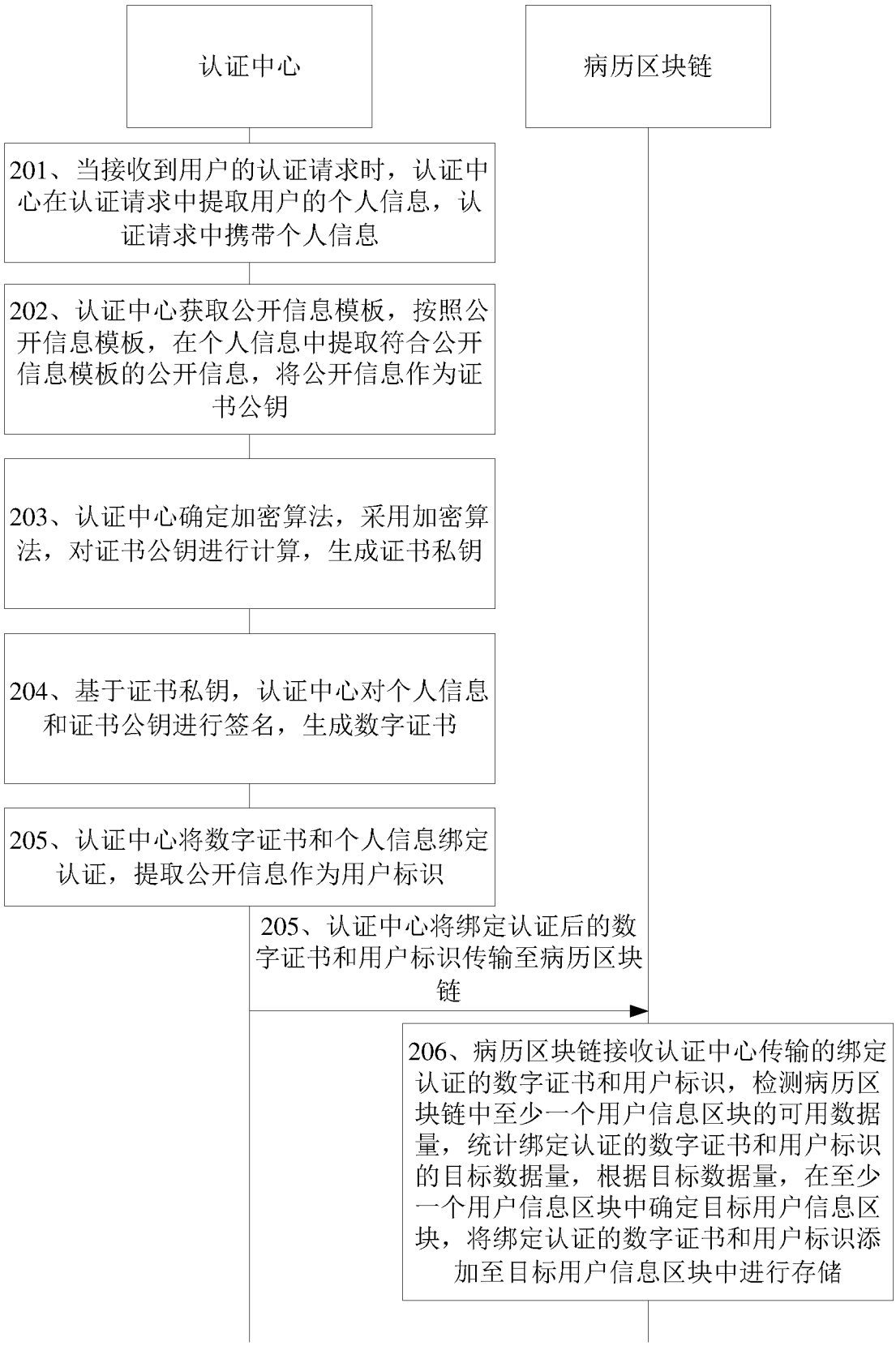
认证中心
病历区块链
201、当接收到用户的认证请求时，认证中心在认证请求中提取用户的个人信息，认证请求中携带个人信息
202、认证中心获取公开信息模板，按照公开信息模板，在个人信息中提取符合公开信息模板的公开信息，将公开信息作为证书公钥
203、认证中心确定加密算法，采用加密算法，对证书公钥进行计算，生成证书私钥
204、基于证书私钥，认证中心对个人信息和证书公钥进行签名，生成数字证书
205、认证中心将数字证书和个人信息绑定认证，提取公开信息作为用户标识
205、认证中心将绑定认证后的数字证书和用户标识传输至病历区块链
206、病历区块链接收认证中心传输的绑定认证的数字证书和用户标识，检测病历区块链中至少一个用户信息区块的可用数据量，统计绑定认证的数字证书和用户标识的目标数据量，根据目标数据量，在至少一个用户信息区块中确定目标用户信息区块，将绑定认证的数字证书和用户标识添加至目标用户信息区块中进行存储

图 2A

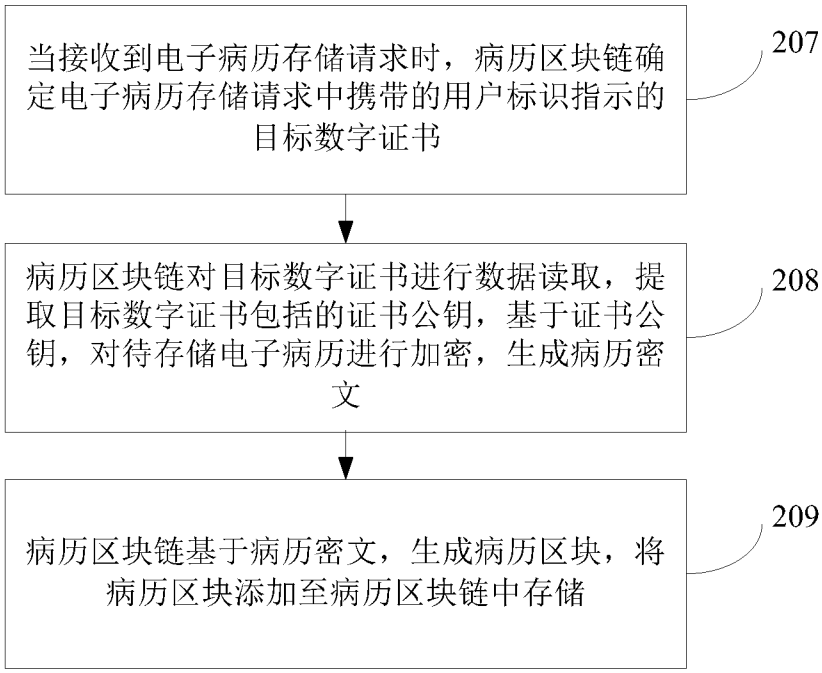
当接收到电子病历存储请求时，病历区块链确定电子病历存储请求中携带的用户标识指示的目标数字证书
207
病历区块链对目标数字证书进行数据读取，提取目标数字证书包括的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文
208
病历区块链基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储
209

图 2B

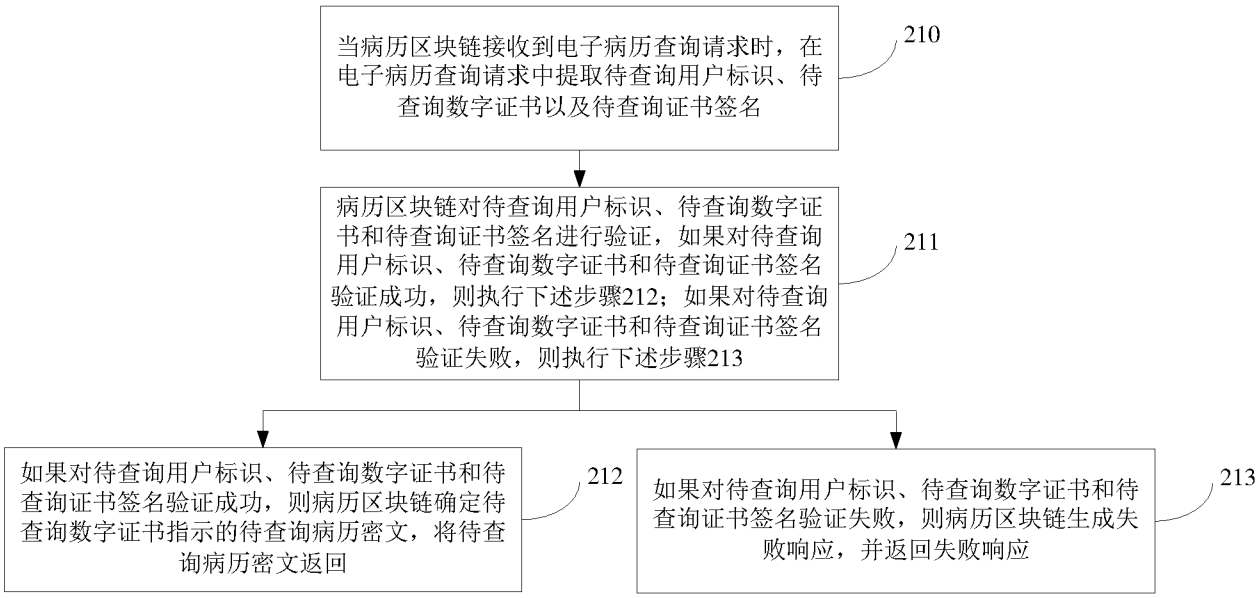
当病历区块链接收到电子病历查询请求时，在电子病历查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名
210
病历区块链对待查询用户标识、待查询数字证书和待查询证书签名进行验证，如果对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则执行下述步骤212；如果对待查询用户标识、待查询数字证书和待查询证书签名验证失败，则执行下述步骤213
211
如果对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则病历区块链确定待查询数字证书指示的待查询病历密文，将待查询病历密文返回
212
如果对待查询用户标识、待查询数字证书和待查询证书签名验证失败，则病历区块链生成失败响应，并返回失败响应
213

图 2C

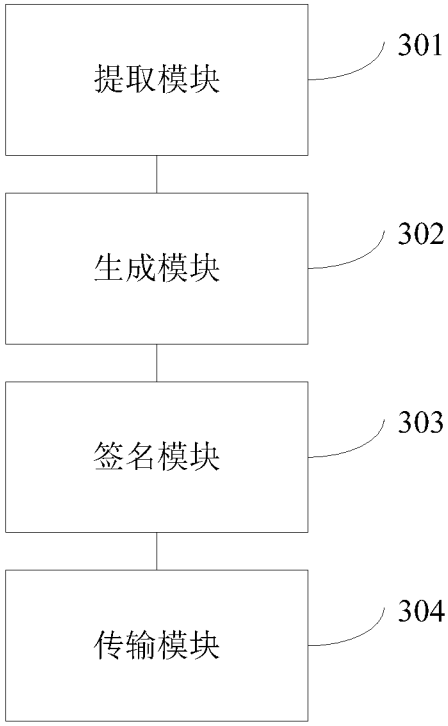
提取模块
301
生成模块
302
签名模块
303
传输模块
304

图 3A

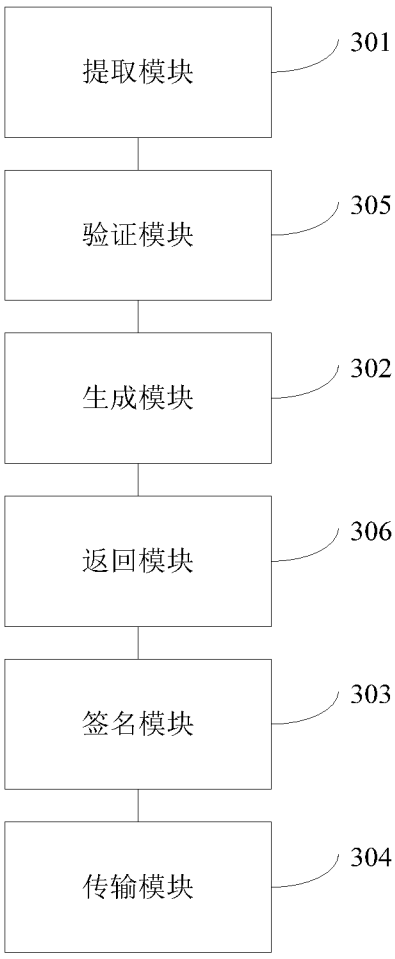
提取模块
301
验证模块
305
生成模块
302
返回模块
306
签名模块
303
传输模块
304

图 3B

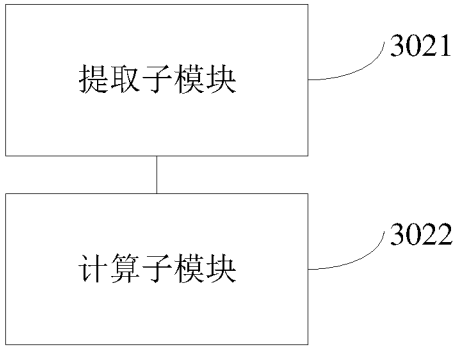

图 3C

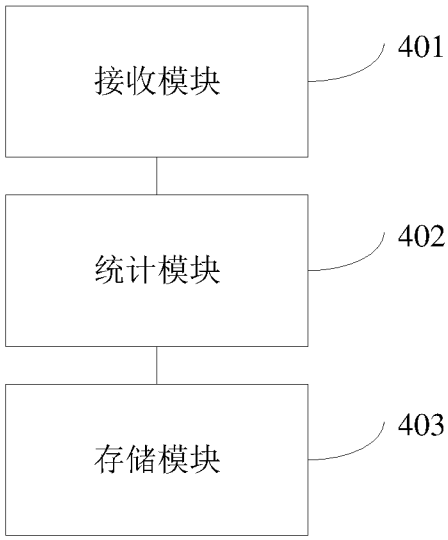

图 4A

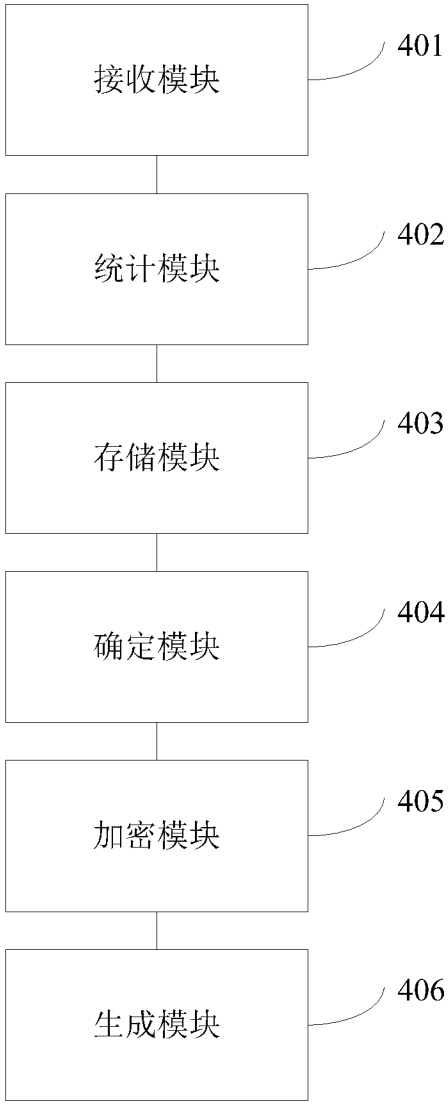

图 4B

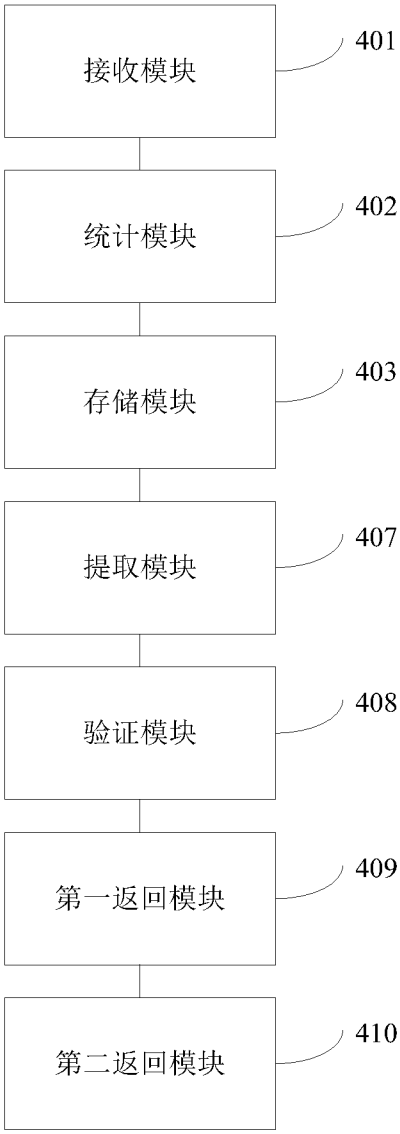
接收模块
401
统计模块
402
存储模块
403
提取模块
407
验证模块
408
第一返回模块
409
第二返回模块
410

图 4C

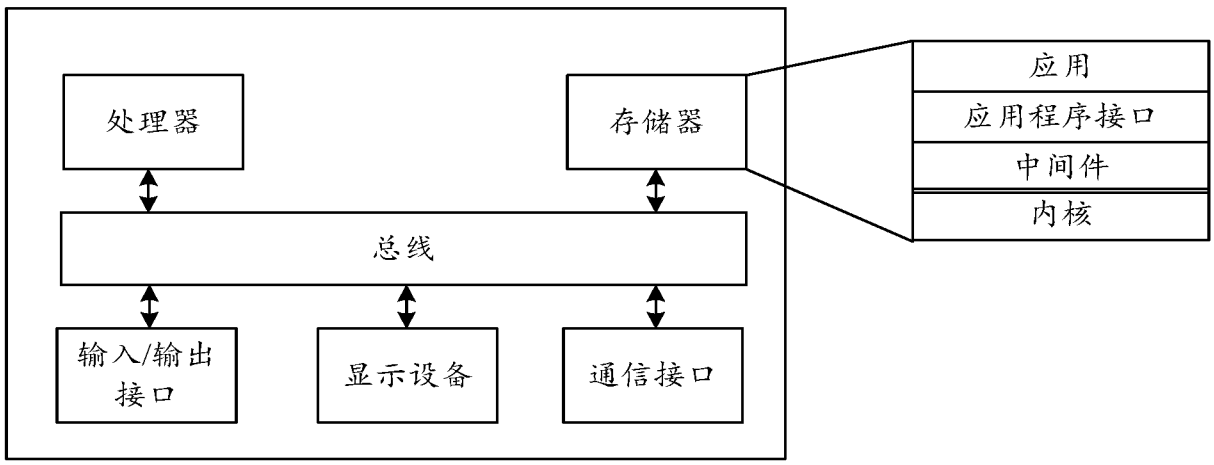
处理器
存储器
应用
应用程序接口
中间件
内核
总线
输入/输出接口
显示设备
通信接口

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/122879

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)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)

H04L G06F

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)

CNPAT; CNKI; WPI; EPODOC; IEEE: 认证, 验证, 公钥, 私钥, 数字证书, 用户, 签名, 病历, 区块链, 隐私, 泄露, 加密, 解密, 存储, verify, authentication, public, private, key, digital certificate, user, signature, blockchain, privacy, leakout, encrypt, decrypt, store

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110086608 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 02 August 2019 (2019-08-02) descrption, paragraphs 0006-0136, and claims 1-10	1-20
X	CN 107579817 A (GRG BANKING EQUIPMENT CO., LTD.) 12 January 2018 (2018-01-12) description, paragraphs 0003-0032 and 0171-0177	4-5, 9, 13-14, 19-20
A	CN 108712431 A (GUANGDONG UNIVERSITY OF TECHNOLOGY) 26 October 2018 (2018-10-26) entire document	1-20
A	US 2008104615 A1 (MICROSOFT CORPORATION) 01 May 2008 (2008-05-01) 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
26 February 2020	**06 March 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2019/122879

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110086608 A	02 August 2019	None	
CN 107579817 A	12 January 2018	WO 2019052286 A1	21 March 2019
CN 108712431 A	26 October 2018	None	
US 2008104615 A1	01 May 2008	KR 20090083331 A	03 August 2009
		WO 2008057973 A2	15 May 2008
		JP 2010508610 A	18 March 2010
		CA 2661928 A1	15 May 2008
		EP 2087462 A2	12 August 2009
		CN 101536021 A	16 September 2009
		IN 200902870 P4	21 August 2009
		US 2008104615 A1	01 May 2008
		IL 197425 A	31 October 2012

国际检索报告

国际申请号
PCT/CN2019/122879

A. 主题的分类

H04L 9/08(2006.01)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)

H04L G06F

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））

CNPAT; CNKI; WPI; EPODOC; IEEE: 认证，验证，公钥，私钥，数字证书，用户，签名，病历，区块链，隐私，泄露，加密，解密，存储， verify, authentication, public, private, key, digital certificate, user, signature, blockchain, privacy, leakout, encrypt, decrypt, store

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 110086608 A (深圳壹账通智能科技有限公司) 2019年 8月 2日 (2019-08-02) 说明书第0006-0136段，权利要求1-10项	1-20
X	CN 107579817 A (广州广电运通金融电子股份有限公司) 2018年 1月 12日 (2018-01-12) 说明书第0003-0032、0171-0177段	4-5、9、13-14、19-20
A	CN 108712431 A (广东工业大学) 2018年 10月 26日 (2018-10-26) 全文	1-20
A	US 2008104615 A1 (MICROSOFT CORPORATION) 2008年 5月 1日 (2008-05-01) 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 26日	2020年 3月 6日
ISA/CN的名称和邮寄地址 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 传真号 (86-10)62019451	受权官员 刘静微 电话号码 86-10-53961592

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/122879

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	110086608	A	2019年 8月 2日		无		
CN	107579817	A	2018年 1月 12日	WO	2019052286	A1	2019年 3月 21日
CN	108712431	A	2018年 10月 26日		无		
US	2008104615	A1	2008年 5月 1日	KR	20090083331	A	2009年 8月 3日
				WO	2008057973	A2	2008年 5月 15日
				JP	2010508610	A	2010年 3月 18日
				CA	2661928	A1	2008年 5月 15日
				EP	2087462	A2	2009年 8月 12日
				CN	101536021	A	2009年 9月 16日
				IN	200902870	P4	2009年 8月 21日
				US	2008104615	A1	2008年 5月 1日
				IL	197425	A	2012年 10月 31日