(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 2020/168772 A1

(51) 国际专利分类号:
G16H 10/60 (2018.01)

(21) 国际申请号: PCT/CN2019/121815

(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:
201910119326.9 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: 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 2020/168772 A1

(54) **Title:** ELECTRONIC MEDICAL RECORD STORING METHOD, SYSTEM, APPARATUS, AND DEVICE, AND MEDIUM

(54) **发明名称**: 一种电子病历存储方法、系统、装置、设备及介质

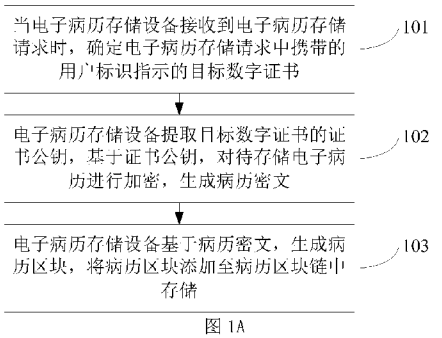

图 1A

101 When receiving an electronic medical record storing request, an electronic medical record storing device determines a target digital certificate indicated by a user identifier carried in the electronic medical record storing request

102 The electronic medical record storing device extracts a certificate public key of the target digital certificate, and encrypts an electronic medical record to be stored on the basis of the certificate public key to generate medical record ciphertext

103 The electronic medical record storing device generates a medical record block on the basis of the medical record ciphertext, and adds the medical record block into a medical record blockchain for storage

(57) **Abstract:** An electronic medical record storing method, system, apparatus, and device, and a medium, relating to the technical field of Internet. A medical record block can be added to a medical record blockchain for storage; by making use of the decentralized characteristic of the blockchain, the security of an electronic medical record is ensured, and the electronic medical record can be shared, thereby avoiding repeated personal medical item examination and saving medical resources. The method comprises: upon receipt of an electronic medical record storing request, determines a target digital certificate indicated by a user identifier carried in the electronic medical record storing request (101); an electronic medical record storing device extracts a certificate public key of the target digital certificate, and encrypts an electronic medical record to be stored on the basis of the certificate public key to generate medical record ciphertext (102); and the electronic medical record storing device generates a medical record block on the basis of the medical record ciphertext, and adds the medical record block into a medical record blockchain for storage (103).

(57) **摘要**: 一种电子病历存储方法、系统、装置、设备及介质，涉及互联网技术领域，可以将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的共享，避免个人医疗项目重复检测，节省了医疗资源。该方法包括：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（101）；电子病历存储设备提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文（102）；电子病历存储设备基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储（103）。

[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))。

说明书

发明名称：一种电子病历存储方法、系统、装置、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201910119326.9、发明名称为“电子病历存储方法、系统、装置、设备及可读存储介质”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] 本申请属于互联网技术领域，尤其涉及一种电子病历存储方法、系统、装置、设备及介质。

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数据并实时更新数据，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，也即用户将自身的电子病历与用户的身份证信息、联系方式信息等个人信息绑定存储，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中至少存在以下技术问题：

[0006] 个人具有流动性，通常会在多家医院进行就诊，医疗资源分布的不均恒性会进一步导致病人跨地域进行就医，而异地的医院可能并没有存储病人的电子病历，需要病人重新去做各种检查，使得个人医疗项目重复检测，造成医疗资源的浪费。

发明概述

技术问题

[0007] 有鉴于此，本申请提供了一种电子病历存储方法、系统、装置、设备及介质，主要目的在于解决目前个人医疗项目重复检测，造成医疗资源的浪费的问题。

问题的解决方案

技术解决方案

[0008] 本申请实施例的第一方面提供了一种电子病历存储方法，包括：

[0009] 当接收到电子病历存储请求时，在病历区块链中查询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；

[0010] 提取所述目标数字证书的证书公钥，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；

[0011] 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。

[0012] 本申请实施例的第二方面提供了一种电子病历存储方法，包括：

[0013] 当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

[0014] 获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

[0015] 将所述电子病历存储请求传输至电子病历存储设备。

[0016] 本申请实施例的第三方面提供了一种电子病历存储系统，包括：用户设备和电子病历存储设备，其中，

[0017] 所述用户设备当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

[0018] 所述用户设备获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

[0019] 所述用户设备将所述电子病历存储请求传输至电子病历存储设备；

[0020] 所述电子病历存储设备当接收到电子病历存储请求时，在病历区块链中查询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；

[0021] 所述电子病历存储设备提取所述目标数字证书的证书公钥，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；

[0022] 所述电子病历存储设备基于所述病历密文，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。

[0023] 本申请实施例的第四方面提供了一种电子病历存储装置，包括：

[0024] 确定模块，用于当接收到电子病历存储请求时，在病历区块链中查询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；

[0025] 加密模块，用于提取所述目标数字证书的证书公钥，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；

[0026] 第一存储模块，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。

[0027] 本申请实施例的第五方面提供了一种电子病历存储装置，包括：

[0028] 第一接收模块，用于当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

[0029] 第一生成模块，用于获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

[0030] 第一传输模块，用于将所述电子病历存储请求传输至电子病历存储设备。

[0031] 本申请实施例的第六方面提供了一种终端设备，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上述任意一个所述电子病历存储方法的步骤。

[0032] 本申请实施例的第四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述任意一个所述电子病历存储方法的步骤。

发明的有益效果

有益效果

[0033] 与目前采用中心化的信息系统存储电子病历的方式相比，本申请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，并提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的共享，避免个人医疗项目重复检测，节省了医疗资源。

对附图的简要说明

附图说明

[0034] 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。

[0035] 图1A示出了本申请实施例提供的一种电子病历存储方法流程示意图；

[0036] 图1B示出了本申请实施例提供的一种电子病历存储方法流程示意图；

[0037] 图2A示出了本申请实施例提供的一种电子病历存储方法流程示意图；

[0038] 图2B示出了本申请实施例提供的一种电子病历存储方法流程示意图；

[0039] 图2C示出了本申请实施例提供的一种电子病历存储方法流程示意图；

[0040] 图3A示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0041] 图3B示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0042] 图3C示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0043] 图4A示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0044] 图4B示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0045] 图4C示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0046] 图4D示出了本申请实施例提供的一种电子病历存储装置的结构示意图；

[0047] 图5示出了本申请实施例提供的一种设备的装置结构示意图。

发明实施例

本发明的实施方式

[0048] 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。

[0049] 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。

[0050] 本申请实施例提供了一种电子病历存储方法，可以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，并提取目

标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还达到了电子病历共享的目的，避免个人医疗项目重复检测，节省了医疗资源，如图1A所示，该方法包括：

[0051] 101、当电子病历存储设备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。

[0052] 在本申请实施例中，由于电子病历存储系统中存储有已经注册的用户的用户标识以及对应的数字证书，因此，当接收到用户端传输的电子病历存储请求时，为了对保证用户想要存储的待存储电子病历中数据的安全性，首先，在电子病历存储请求中提取携带的用户标识；随后，确定该用户标识指示的目标数字证书，以便后续基于该目标数字证书实现对待存储电子病历的加密。

[0053] 102、电子病历存储设备提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文。

[0054] 在本申请实施例中，当获取到目标数字证书后，由于存储在电子病历存储系统中的数字证书中均包括证书公钥，因此，可以在目标数字证书中提取到证书公钥，并基于该证书公钥，对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，实现对待存储电子病历的加密。

[0055] 103、电子病历存储设备基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储。

[0056] 在本申请实施例中，在生成了病历密文后，由于病历区块链中是采用病历区块的形式存储数据的，因此，基于该病历密文，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，从而实现待存储电子病历在病历区块链中的存储。

[0057] 本申请实施例提供的方法，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，并提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中

心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的共享，避免个人医疗项目重复检测，节省了医疗资源。

[0058] 本申请实施例提供了一种电子病历存储方法，可以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，并提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还达到了电子病历共享的目的，避免个人医疗项目重复检测，节省了医疗资源，如图1B所示，该方法包括：

[0059] 104、当用户设备检测到用户请求存储电子病历时，接收用户的待存储电子病历。

[0060] 在本申请实施例中，当检测到用户请求存储电子病历时，需要接收用户上传的待存储电子病历，以便后续将待存储电子病历存储到电子病历存储系统中。

[0061] 105、用户设备获取用户的用户标识，基于待存储电子病历以及用户标识，生成电子病历存储请求。

[0062] 在本申请实施例中，为了使电子病历存储系统在接收到待存储电子病历后，可以明确是哪一个用户的电子病历，进而将存储的全部电子病历进行区分，需要获取用户的用户标识，并基于待存储电子病历以及用户标识，生成电子病历存储请求，以便后续电子病历存储系统可以将用户标识与待存储电子病历对应存储。

[0063] 106、用户设备将电子病历存储请求传输至电子病历存储设备。

[0064] 在本申请实施例中，当生成了电子病历存储请求后，便可以将该电子病历存储请求传输至电子病历存储系统，以便电子病历存储系统对待存储电子病历进行存储。

[0065] 本申请实施例提供的方法，当检测到用户请求存储电子病历时，接收用户的待存储电子病历，获取用户的用户标识，基于待存储电子病历以及用户标识，生成电子病历存储请求，将电子病历存储请求传输至电子病历存储系统，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的

共享，避免个人医疗项目重复检测，节省了医疗资源。

[0066] 本申请实施例提供了一种电子病历存储方法，可以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，并提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还达到了电子病历共享的目的，避免个人医疗项目重复检测，节省了医疗资源，如图2A所示，该方法用于用户端和电子简历存储系统，包括：

[0067] 201、当用户设备检测到用户请求存储电子病历时，接收用户的待存储电子病历，获取用户的用户标识，基于待存储电子病历以及用户标识，生成电子病历存储请求，并将电子病历存储请求传输至电子病历存储设备。

[0068] 发明人认识到，在存储电子病历时，通常采用诸如MySQL（Structured Query Language，关系型数据库管理系统）等的传统数据库，这种传统数据库通常是独立存在的，也即不同的数据库之间是不互通的，这样，就导致如果用户仅在医院A看过病，没有在医院B看过病，则用户A的电子病历仅能存储在医院A的电子病历，而医院B是无法查询到用户在医院A的历史电子病例的，如果医院B存在治疗需要的话，用户还需要在医院B中重新做以前在医院A做过的检查，浪费了大量的医疗资源。因此，本申请采用区块链系统存储用户的电子病历，也即建立了基于区块链技术实现的电子病历存储设备，并基于该电子病历存储设备存储用户的电子病历，以及后续为用户提供电子病历的查询服务等。

[0069] 其中，电子病历存储设备中接入了大量的用户设备，使得用户可以通过用户设备将自己的电子病历上传到电子病历存储设备中存储，用户设备具体可为医院所持的智能手机、平板电脑等智能终端。用户设备中可以为用户提供存储入口，当检测到用户触发该存储入口时，确定检测到用户请求存储电子病历，显示电子病历上传页面，并在检测到用户对该电子病历上传页面确认时，确定接收到用户的待存储电子病历。由于电子病历存储设备中存储有大量的电子病历，为了使电子病历存储设备在接收到电子病历时，将不同用户的电子病历进行区分，因此，在接收到用户的电子病历后，获取用户的用户标识，并基于该待存

储电子病历以及用户标识，生成电子病历存储请求，将该电子病历存储请求传输至电子病历存储设备中。需要说明的是，用户标识可为用户姓名、用户身份证号码等可以用于指示用户身份的唯一标识，本申请实施例对用户标识的具体内容不进行限定。

[0070] 202、当电子病历存储设备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。

[0071] 在本申请实施例中，为了保证电子病历存储设备中存储的电子病历的安全性，避免所有人都可以对电子病历进行读取，造成电子病历中涉及的医疗信息的泄露，电子病历存储设备中存储有每一个在电子病历存储设备中注册过的用户的数字证书，并在接收到电子病历存储请求时，基于该电子病历存储请求指示的数字证书来对待存储电子病历进行加密存储，从而保证待存储电子病历的真实性。

[0072] 数字证书为用户自行向证书下发机构申请的一种身份凭证，每个用户的数字证书均是唯一且不同的。数字证书包括证书公钥以及证书私钥，证书公钥随数字证书保存在电子病历存储设备中，是公开的；证书私钥由用户个人保管，只有用户个人知晓，证书公钥和证书私钥属于非对称密钥，也即，采用证书公钥加密的文件可以采用证书私钥进行解密，采用证书私钥加密的文件也可以采用证书公钥进行解密。

[0073] 其中，由于电子病历存储请求中携带有用户标识，且电子病历存储设备中存储有每一个注册过的用户的数字证书，因此，当接收到电子病历存储请求时，电子病历存储设备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，并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。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，也即电子病历存储设备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，需要用户在区块链中进行注册后才可以将电子病历存储在区块链中，这样，便不能继续执行下述操作。

[0074] 203、电子病历存储设备提取目标数字证书的证书公钥，基于证书公钥，对待

存储电子病历进行加密，生成病历密文。

[0075] 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。

[0076] 204、电子病历存储设备基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储。

[0077] 在本申请实施例中，由于电子病历存储设备基于病历区块链存储生成的病历密文，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。

[0078] 需要说明的是，接入到电子病历存储设备中的每一个用户设备中都存储有与电子病历存储设备的病历区块链一致的区块链。为了保证每个接入电子病历存储设备中的每一个用户设备中的病历区块链的数据是一致的，从而使得在哪一个用户设备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接入电子病历存储设备的每一个用户设备，以便每一个用户设备均将该病历区块添加至自身存储的区块链中，从而保证数据的一致性。

[0079] 在实际应用的过程中，为了防止有不法分子随意向电子病历存储设备上传病历，造成电子病历存储设备由于数据过载而瘫痪，因此，需要将电子病历上传至电子病历存储设备中保存的用户要事先在电子病历存储设备中进行注册，参见图2B，该方法包括：

[0080] 205、当用户设备检测到用户请求注册时，接收用户的用户信息以及待验证数字证书，在待验证数字证书中提取待验证证书私钥，采用待验证证书私钥对待验证数字证书进行签名，生成待验证证书签名。

[0081] 在本申请实施例中，用户设备可以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。其中，由于用户的身

份是基于数字证书体现的，为了验证用户身份的真实性以及安全性，在用户进行注册时，需要用户提供数字证书，以便基于该数字证书对用户的身份进行验证。在检测到用户对该注册页面确认后，确定接收到用户的用户信息以及待验证数字证书，由于数字证书的证书私钥是由用户自己保管的，用户设备为用户所使用的终端，因此，用户设备可以提取到该待验证数字证书的待验证证书私钥，或者用户可以向该用户设备提供待验证证书私钥。为了进一步保证待验证数字证书在传输过程中的安全性，可以采用待验证证书私钥，对待验证数字证书进行签名，签名的过程实质为加密的过程，将加密后的待验证数字证书作为待验证证书签名，以便在后续可以通过验证该待验证证书签名实现对待验证数字证书的验证。

[0082] 206、用户设备基于用户信息、待验证证书签名以及待验证数字证书，生成注册请求，将注册请求传输至电子病历存储设备。

[0083] 在本申请实施例中，当生成了待验证证书签名后，便可以基于用户信息、待验证证书签名以及待验证数字证书，生成注册请求，并将注册请求传输至电子病历存储设备，以便电子病历存储设备对注册请求进行验证，并在验证成功时完成用户在电子病历存储设备中的注册。

[0084] 207、电子病历存储设备接收用户的注册请求，在注册请求中提取用户信息、待验证证书签名以及待验证数字证书，采用待验证数字证书对待验证证书签名进行验证，如果采用待验证证书公钥对待验证证书签名验证成功，则执行下述步骤208；如果采用待验证证书公钥对待验证证书签名验证失败，则执行下述步骤209。

[0085] 在本申请实施例中，电子病历存储设备接收用户设备传输的注册请求，并在注册请求中提取用户信息、待验证证书签名以及待验证数字证书。由于该待验证数字证书的待验证证书公钥是随待验证证书携带的，且是公开的，因此，可以在该待验证数字证书中提取到待验证证书公钥。另外，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，并根据是否解密成功来确定待验证证书签名的真实性。具体地，在

采用待验证证书公钥对待验证证书签名进行验证时，首先，在待验证数字证书中提取待验证证书公钥；随后，采用待验证证书公钥对待验证证书签名解密，并判断待验证证书公钥是否成功对待验证证书签名解密。如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密成功，则表示注册请求在传输的过程中并没有被篡改，可以保证注册请求的真实性，因此，该用户可以在电子病历存储设备中进行注册，也即执行下述步骤208；如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密失败，则表示注册请求在传输的过程中很有可能被篡改了，该待验证证书签名已经不是最初的签名了，因此，该用户不可以在电子病历存储设备中注册，需要用户重新发送注册请求，也即执行下述步骤209。

[0086] 208、如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密成功，则提取用户的待存储用户标识，将待存储用户标识、用户信息和待验证数字证书存储至病历区块链中。

[0087] 在本申请实施例中，如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密成功，则表示当前用户可以在电子病历存储设备中注册，因此，电子病历存储设备为该用户提取待存储用户标识，并将该待存储用户标识、用户信息以及待验证数字证书存储在病历区块链中，完成该用户在电子病历存储设备中的注册。其中，待存储用户标识可以在用户的用户信息中提取出来，例如，将用户的用户姓名、身份证号等提取出来作为待存储用户标识；或者还可以为用户分配一个注册账号，将该注册账号作为该用户的待存储用户标识，并将该注册账号返回给用户，使用户以后基于该注册账号便可以实现在电子病历存储设备中存储电子病历以及查询电子病历。

[0088] 209、如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密失败，则生成失败响应，将失败响应返回至用户。

[0089] 在本申请实施例中，如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密失败，则表示该注册请求很可能在传输的过程中被篡改，真实性无法验证，此时，便不能实现用户在电子病历系统中的注册，需要用户重新提供相关信息进行注册，因此，生成失败响应，并将该失败响应返回给用户，以便用

户接收到失败响应可以重新发送注册请求。

[0090] 在实际应用的过程中，用户在医院中看病时，需要医院在电子病历存储设备中获取用户之前的电子病历，因此，电子病历存储设备还为用户提供电子病历查询服务，参见图2C，该方法包括：

[0091] 210、当用户设备检测到用户请求查询时，接收用户的待查询用户标识以及待查询数字证书，在待查询数字证书中提取待查询证书私钥，采用待查询证书私钥对待查询数字证书进行签名，生成待查询证书签名。

[0092] 在本申请实施例中，用户设备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。由于电子病历存储设备中存储电子病历时是按照用户标识进行存储的，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向电子病历存储设备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，还可以采用待查询证书私钥对待查询数字证书进行签名，从而生成待查询证书签名，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。其中，生成待查询证书签名与上述步骤205中所述的生成待验证证书签名的方法一致，此处不再进行赘述。

[0093] 211、用户设备基于待查询用户标识、待查询数字证书以及待查询证书签名，生成查询请求，将查询请求传输至电子病历存储设备。

[0094] 在本申请实施例中，当用户设备接收到该待查询用户标识、待查询数字证书以及待查询证书签名后，便可以基于该待查询用户标识、待查询数字证书以及待查询证书签名，生成查询请求，并将该查询请求传输至电子病历存储设备，实现电子病历的查询。

[0095] 212、当电子病历存储设备接收到查询请求时，在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213至步骤214；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215至步骤216。

[0096] 在本申请实施例中，当电子病历存储设备接收到查询请求时，便需要在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，以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。采用待查询证书公钥对待查询证书签名解密验证的方式与上述步骤207中所示的采用待验证数字证书对待验证证书签名进行验证的方式一致，此处不再进行赘述。随后，为了验证该用户是否在电子病历存储设备中注册过，避免未能在电子病历存储设备中注册的不法分子将恶意信息混入电子病历存储设备中，因此，需要根据待查询用户标识验证用户是否在电子病历存储设备中注册过，具体地，在病历区块链中查询是否存储有与待查询用户标识对应的待查询用户信息。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213至步骤214；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，或者用户未在电子病历存储设备中注册，此时，便需要用户重新发送查询请求，也即执行下述步骤215至步骤216。

[0097] 213、如果电子病历存储设备对待查询用户标识、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。

[0098] 在本申请实施例中，如果电子病历存储设备对待查询用户标识、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电子病历存储设备中注册过，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。

[0099] 需要说明的是，由于电子病历存储设备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，电子病历存储设备根据待查询用户标识获取到的也是病历密文，这样，电子病历存储设备便将获取到的待查询病历密文返回至用户设备，以便用户设备通过对该病历密文进行解密实现对电子病历的查看。

[0100] 214、用户设备接收电子病历存储设备返回的病历密文，采用待查询证书私钥对病历密文进行解密，获取待查询电子病历。

[0101] 在本申请实施例中，当用户设备接收到电子病历存储设备返回的病历密文时，由于该病历密文是采用该用户的数字证书的证书公钥加密生成的，只有用户的证书私钥可以解密，且证书私钥是由用户自行保管的，因此，该用户采用自身的数字证书的证书私钥即可对该病历密文进行解密，这样，用户设备便可以采用获取待查询数字证书的待查询证书私钥，采用该待查询证书私钥对该病历密文进行解密，从而在该病例密文中获取到该待查询电子病历。

[0102] 215、如果电子病历存储设备对待查询用户标识、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。

[0103] 在本申请实施例中，如果电子病历存储设备对待查询用户标识、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，或者用户没有在电子病历存储设备中注册，因此，生成失败响应，并返回失败响应。

[0104] 216、用户设备重新执行上述生成并传输查询请求的过程。

[0105] 在本申请实施例中，当用户设备接收到电子病历存储设备传输的失败响应时，便表示本次用户请求进行电子病历查询失败了，此时，用户设备便需要重新执行上述生成并传输查询请求的过程。

[0106] 本申请实施例提供的方法，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，并提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历

密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的共享，避免个人医疗项目重复检测，节省了医疗资源。

[0107] 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电子病历存储装置，如图3A所示，所述装置包括：确定模块301，加密模块302和第一存储模块303。

[0108] 该确定模块301，用于当接收到电子病历存储请求时，在病历区块链中查询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；

[0109] 该加密模块302，用于提取所述目标数字证书的证书公钥，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；

[0110] 该第一存储模块303，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。

[0111] 在具体的应用场景中，如图3B所示，该装置还包括第一接收模块304，第一验证模块305，第二存储模块306和第一返回模块307。

[0112] 该第一接收模块304，用于接收用户的注册请求，在所述注册请求中提取用户信息、待验证证书签名以及待验证数字证书；

[0113] 该第一验证模块305，用于采用所述待验证数字证书对所述待验证证书签名进行验证；

[0114] 该第二存储模块306，用于如果采用所述待验证证书对所述待验证证书签名验证成功，则在所述用户信息中提取待存储用户标识，将所述待存储用户标识、所述用户信息和所述待验证数字证书对应存储至所述病历区块链中；

[0115] 该第一返回模块307，用于如果采用所述待验证证书对所述待验证证书签名验证失败，则生成失败响应，将所述失败响应返回至所述用户。

[0116] 在具体的应用场景中，该第一验证模块305，用于在所述待验证数字证书中提取待验证证书公钥；采用所述待验证证书公钥对所述待验证证书签名解密，判断所述待验证证书公钥是否成功对所述待验证证书签名解密。

[0117] 在具体的应用场景中，如图3C所示，该装置还包括第二接收模块308，第二验证模块309，第二返回模块310和第三返回模块311。

[0118] 该第二接收模块308，用于当接收到查询请求时，在所述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；

[0119] 该第二验证模块309，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；

[0120] 该第二返回模块310，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，则在所述病例区块链中获取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；

[0121] 该第三返回模块311，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。

[0122] 在具体的应用场景中，该第二验证模块309，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是否存储有与所述待查询用户标识对应的待查询用户信息；

[0123] 相应地，该第二返回模块310，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，且确定所述病历区块链中存储有与所述待查询用户标识对应的待查询用户信息时，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；

[0124] 该第三返回模块311，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，或确定所述病历区块链中未存储有与所述待查询用户标识对应的待查询用户信息时，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。

[0125] 本申请实施例提供的装置，可以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，并提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文，随后基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的共享，避免个人医疗项目重复检测，节省了医疗资源。

[0126] 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电子病历

存储装置，如图4A所示，所述装置包括：第一接收模块401，第一生成模块402和第一传输模块403。

[0127] 该第一接收模块401，用于当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

[0128] 该第一生成模块402，用于获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

[0129] 该第一传输模块403，用于将所述电子病历存储请求传输至电子病历存储设备。

[0130] 在具体的应用场景中，如图4B所示，该装置还包括：第二接收模块404，第一签名模块405，第二生成模块406和第二传输模块407。

[0131] 该第二接收模块404，用于当检测到用户请求注册时，接收所述用户的用户信息以及待验证数字证书；

[0132] 该第一签名模块405，用于在所述待验证数字证书中提取待验证证书私钥，采用所述待验证证书私钥对所述待验证数字证书进行签名，生成待验证证书签名；

[0133] 该第二生成模块406，用于基于所述用户信息、所述待验证证书签名以及所述待验证数字证书，生成注册请求；

[0134] 该第二传输模块407，用于将所述注册请求传输至所述电子病历存储设备。

[0135] 在具体的应用场景中，如图4C所示，该装置还包括：第三接收模块408，第二签名模块409，第三生成模块410和第三传输模块411。

[0136] 该第三接收模块408，用于当检测到用户请求查询时，接收所述用户的待查询用户标识以及待查询数字证书；

[0137] 该第二签名模块409，用于在所述待查询数字证书中提取待查询证书私钥，采用所述待查询证书私钥对所述待查询数字证书进行签名，生成待查询证书签名；

[0138] 该第三生成模块410，用于基于所述待查询用户标识、所述待查询数字证书以及所述待查询证书签名，生成查询请求；

[0139] 该第三传输模块411，用于将所述查询请求传输至所述电子病历存储设备。

[0140] 在具体的应用场景中，如图4D所示，该装置还包括：解密模块412。

[0141] 该解密模块412，用于如果接收到病历密文，则采用所述待查询证书私钥对所述病历密文进行解密，获取待查询电子病历，所述病历密文由所述电子病历存储设备接收到所述查询请求后获取并返回的；

[0142] 该第二签名模块409，还用于如果接收到失败响应，则重新执行上述生成并传输查询请求的过程。

[0143] 本申请实施例提供的装置，可以当检测到用户请求存储电子病历时，接收用户的待存储电子病历，获取用户的用户标识，基于待存储电子病历以及用户标识，生成电子病历存储请求，将电子病历存储请求传输至电子病历存储系统，利用区块链去中心化的特性，不仅保证了电子病历的安全性，还实现了对电子病历的共享，避免个人医疗项目重复检测，节省了医疗资源。

[0144] 需要说明的是，本申请实施例提供的一种电子病历存储装置所涉及各功能单元的其他相应描述，可以参考图1A和图1B中的对应描述，在此不再赘述。

[0145] 在示例性实施例中，参见图5，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，执行上述实施例中的电子病历存储方法。其中，该设备可为用户设备以及电子病历存储设备。

[0146] 一种可读存储介质，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的电子病历存储方法的步骤。其中，该可读存储介质分别在用户设备以及电子病历存储设备中部署。

[0147] 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。

[0148] 本领域技术人员可以理解附图只是一个优选实施场景的示意图，附图中的模块或流程并不一定是实施本申请所必须的。

[0149] 本领域技术人员可以理解实施场景中的装置中的模块可以按照实施场景描述进行分布于实施场景的装置中，也可以进行相应变化位于不同于本实施场景的一个或多个装置中。上述实施场景的模块可以合并为一个模块，也可以进一步拆分成多个子模块。

[0150] 上述本申请序号仅仅为了描述，不代表实施场景的优劣。

[0151] 以上公开的仅为本申请的几个具体实施场景，但是，本申请并非局限于此，任何本领域的技术人员能思之的变化都应落入本申请的保护范围。

权利要求书

[权利要求 1] 一种电子病历存储方法，其特征在于，包括：

当接收到电子病历存储请求时，在病历区块链中查询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；

提取所述目标数字证书的证书公钥，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 2] 如权利要求1所述的方法，其特征在于，所述当接收到电子病历存储请求时，在病历区块链中查询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之前，包括：

接收用户的注册请求，在所述注册请求中提取用户信息、待验证证书签名以及待验证数字证书；

采用所述待验证数字证书对所述待验证证书签名进行验证；

如果采用所述待验证证书对所述待验证证书签名验证成功，则在所述用户信息中提取待存储用户标识，将所述待存储用户标识、所述用户信息和所述待验证数字证书对应存储至所述病历区块链中；

如果采用所述待验证证书对所述待验证证书签名验证失败，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] 如权利要求2所述的方法，其特征在于，所述采用所述待验证数字证书对所述待验证证书签名进行验证，包括：

在所述待验证数字证书中提取待验证证书公钥；

采用所述待验证证书公钥对所述待验证证书签名解密，判断所述待验证证书公钥是否成功对所述待验证证书签名解密。

[权利要求 4] 如权利要求1所述的方法，其特征在于，所述方法还包括：

当接收到查询请求时，在所述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，则在所述病例区块链中获取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 5] 如权利要求4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是否存储有与所述待查询用户标识对应的待查询用户信息；

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，且确定所述病历区块链中存储有与所述待查询用户标识对应的待查询用户信息时，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，或确定所述病历区块链中未存储有与所述待查询用户标识对应的待查询用户信息时，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 6] 一种电子病历存储方法，其特征在于，包括：

当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

将所述电子病历存储请求传输至电子病历存储设备。

[权利要求 7] 如权利要求6所述的方法，其特征在于，所述当检测到用户请求存储

电子病历时，接收所述用户的待存储电子病历之前，包括：

当检测到用户请求注册时，接收所述用户的用户信息以及待验证数字证书；

在所述待验证数字证书中提取待验证证书私钥，采用所述待验证证书私钥对所述待验证数字证书进行签名，生成待验证证书签名；

基于所述用户信息、所述待验证证书签名以及所述待验证数字证书，生成注册请求；

将所述注册请求传输至所述电子病历存储设备。

[权利要求 8] 如权利要求6所述的方法，其特征在于，所述方法还包括：

当检测到用户请求查询时，接收所述用户的待查询用户标识以及待查询数字证书；

在所述待查询数字证书中提取待查询证书私钥，采用所述待查询证书私钥对所述待查询数字证书进行签名，生成待查询证书签名；

基于所述待查询用户标识、所述待查询数字证书以及所述待查询证书签名，生成查询请求；

将所述查询请求传输至所述电子病历存储设备。

[权利要求 9] 如权利要求8所述的方法，其特征在于，所述将所述查询请求传输至所述电子病历存储设备之后，所述方法还包括：

如果接收到病历密文，则采用所述待查询证书私钥对所述病历密文进行解密，获取待查询电子病历，所述病历密文由所述电子病历存储设备接收到所述查询请求后获取并返回的；

如果接收到失败响应，则重新执行上述生成并传输查询请求的过程。

[权利要求 10] 一种电子病历存储系统，其特征在于，包括用户设备和电子病历存储设备，其中，

所述用户设备当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

所述用户设备获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

所述用户设备将所述电子病历存储请求传输至电子病历存储设备；

所述电子病历存储设备当接收到电子病历存储请求时，在病历区块链中查询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；

所述电子病历存储设备提取所述目标数字证书的证书公钥，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；

所述电子病历存储设备基于所述病历密文，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 11] 一种电子病历存储装置，其特征在于，包括：

确定模块，用于当接收到电子病历存储请求时，在病历区块链中查询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；

加密模块，用于提取所述目标数字证书的证书公钥，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；

第一存储模块，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。

[权利要求 12] 如权利要求11所述的装置，其特征在于，还包括：

第一接收模块，用于接收用户的注册请求，在所述注册请求中提取用户信息、待验证证书签名以及待验证数字证书；

第一验证模块，用于采用所述待验证数字证书对所述待验证证书签名进行验证；

第二存储模块，用于如果采用所述待验证证书对所述待验证证书签名验证成功，则在所述用户信息中提取待存储用户标识，将所述待存储用户标识、所述用户信息和所述待验证数字证书对应存储至所述病历区块链中；

第一返回模块，用于如果采用所述待验证证书对所述待验证证书签名验证失败，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 13] 如权利要求12所述的装置，其特征在于，第一验证模块，用于：

在所述待验证数字证书中提取待验证证书公钥；

采用所述待验证证书公钥对所述待验证证书签名解密，判断所述待验证证书公钥是否成功对所述待验证证书签名解密。

[权利要求 14] 如权利要求13所述的装置，其特征在于，还包括：

第二接收模块，用于当接收到查询请求时，在所述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；

第二验证模块，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；

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成功，则在所述病例区块链中获取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；

第三返回模块，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。

[权利要求 15] 如权利要求14所述的装置，其特征在于，第二验证模块，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是否存储有与所述待查询用户标识对应的待查询用户信息；

相应地，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成功，且确定所述病历区块链中存储有与所述待查询用户标识对应的待查询用户信息时，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；

第三返回模块，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，或确定所述病历区块链中未存储有与所述待查询用户标识对应的待查询用户

信息时，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 16] 一种电子病历存储装置，其特征在于，包括：

第一接收模块，用于当检测到用户请求存储电子病历时，接收所述用户的待存储电子病历；

第一生成模块，用于获取所述用户的用户标识，基于所述待存储电子病历以及所述用户标识，生成电子病历存储请求；

第一传输模块，用于将所述电子病历存储请求传输至电子病历存储设备。

[权利要求 17] 如权利要求16所述的装置，其特征在于，还包括：

第二接收模块，用于当检测到用户请求注册时，接收所述用户的用户信息以及待验证数字证书；

第一签名模块，用于在所述待验证数字证书中提取待验证证书私钥，采用所述待验证证书私钥对所述待验证数字证书进行签名，生成待验证证书签名；

第二生成模块，用于基于所述用户信息、所述待验证证书签名以及所述待验证数字证书，生成注册请求；

第二传输模块，用于将所述注册请求传输至所述电子病历存储设备。

[权利要求 18] 如权利要求16所述的装置，其特征在于，还包括：

第三接收模块，用于当检测到用户请求查询时，接收所述用户的待查询用户标识以及待查询数字证书；

第二签名模块，用于在所述待查询数字证书中提取待查询证书私钥，采用所述待查询证书私钥对所述待查询数字证书进行签名，生成待查询证书签名；

第三生成模块，用于基于所述待查询用户标识、所述待查询数字证书以及所述待查询证书签名，生成查询请求；

第三传输模块，用于将所述查询请求传输至所述电子病历存储设备。

[权利要求 19] 一种终端设备，其特征在于，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权利要求1至5任一项所述方法的步骤，或者实现如权利要求6至9任一项所述方法的步骤。

[权利要求 20] 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权利要求1至7任一项所述方法的步骤，或者实现如权利要求6至9任一项所述方法的步骤。

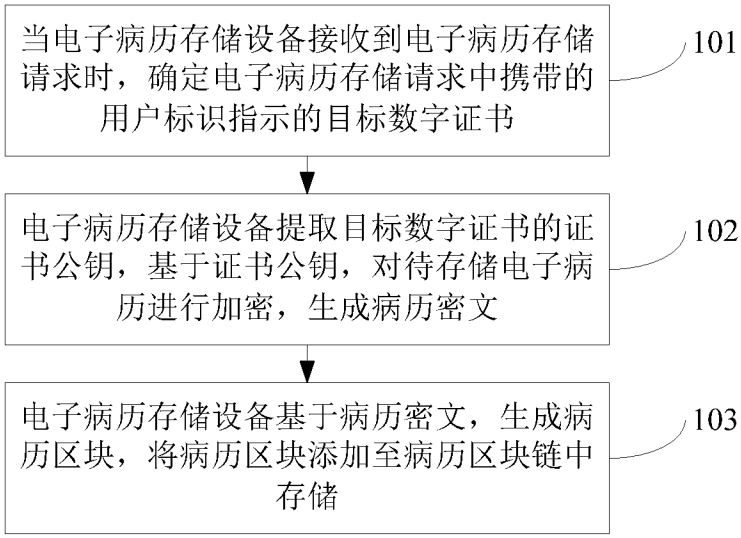
当电子病历存储设备接收到电子病历存储请求时，确定电子病历存储请求中携带的用户标识指示的目标数字证书
101
电子病历存储设备提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文
102
电子病历存储设备基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储
103

图 1A

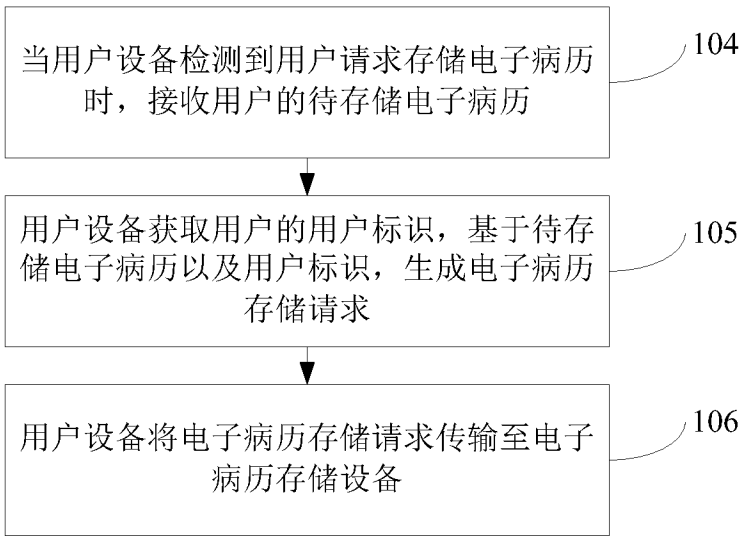
当用户设备检测到用户请求存储电子病历时，接收用户的待存储电子病历
104
用户设备获取用户的用户标识，基于待存储电子病历以及用户标识，生成电子病历存储请求
105
用户设备将电子病历存储请求传输至电子病历存储设备
106

图 1B

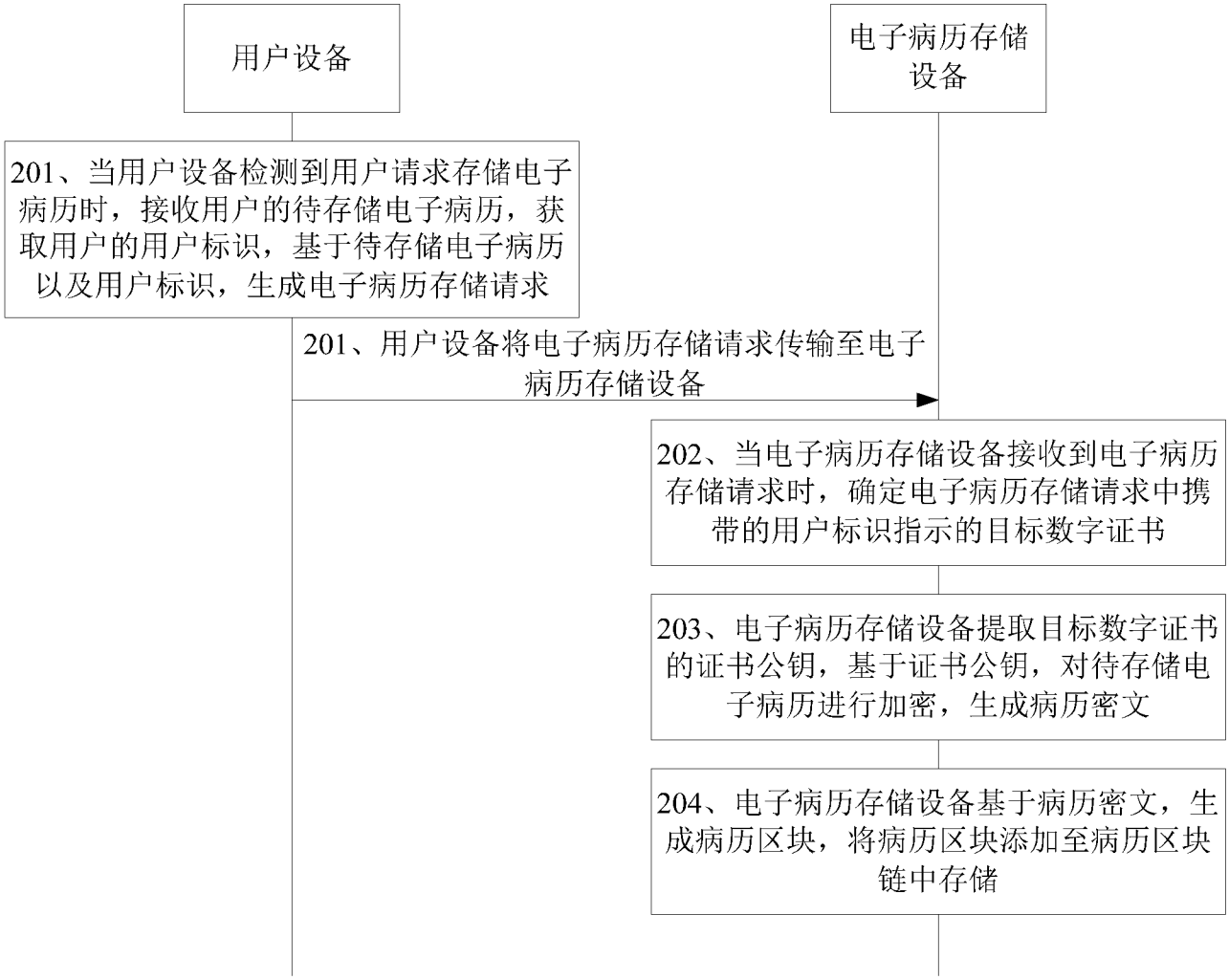
用户设备
电子病历存储设备
201、当用户设备检测到用户请求存储电子病历时，接收用户的待存储电子病历，获取用户的用户标识，基于待存储电子病历以及用户标识，生成电子病历存储请求
201、用户设备将电子病历存储请求传输至电子病历存储设备
202、当电子病历存储设备接收到电子病历存储请求时，确定电子病历存储请求中携带的用户标识指示的目标数字证书
203、电子病历存储设备提取目标数字证书的证书公钥，基于证书公钥，对待存储电子病历进行加密，生成病历密文
204、电子病历存储设备基于病历密文，生成病历区块，将病历区块添加至病历区块链中存储

图 2A

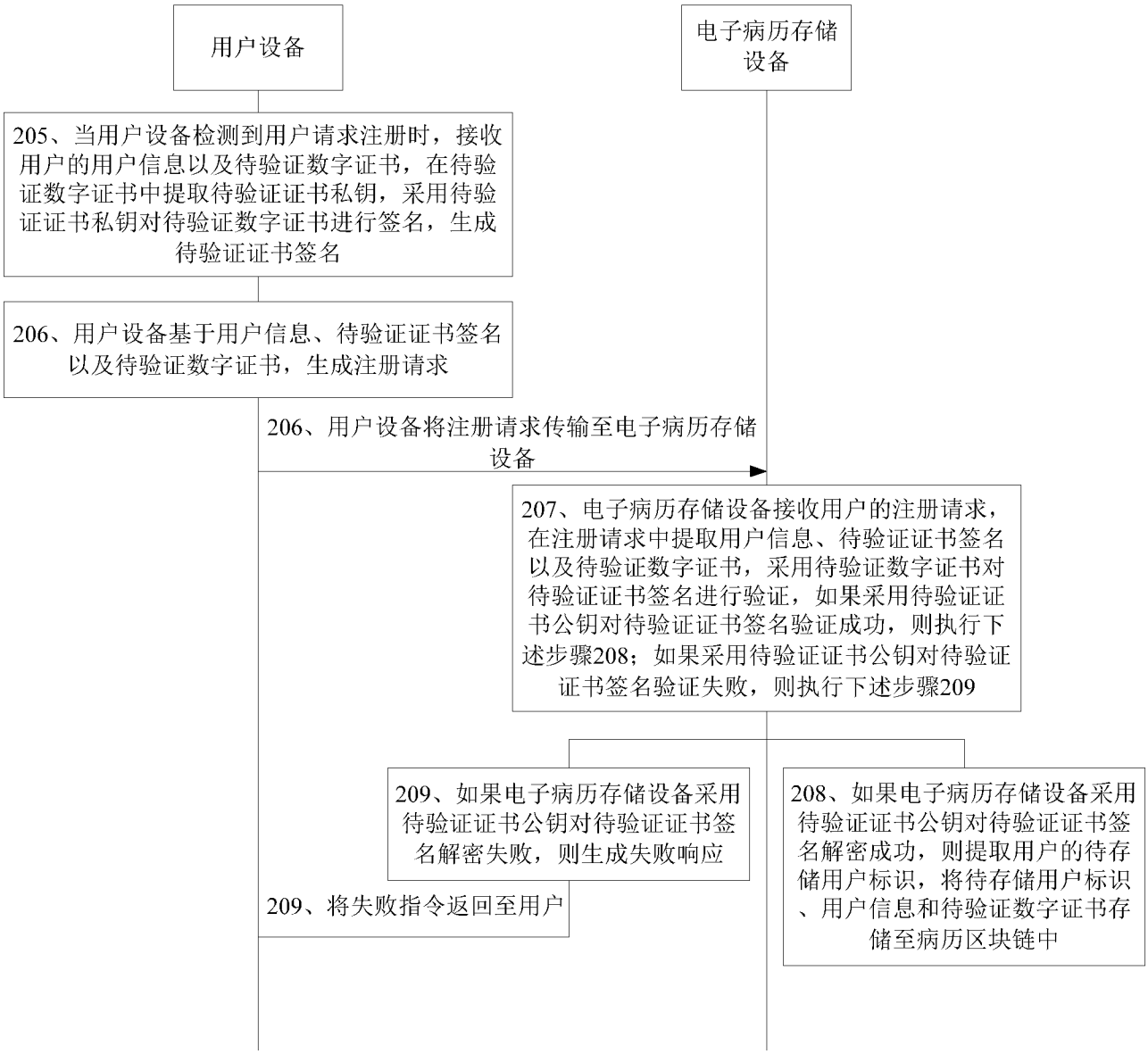
用户设备
电子病历存储设备
205、当用户设备检测到用户请求注册时，接收用户的用户信息以及待验证数字证书，在待验证数字证书中提取待验证证书私钥，采用待验证证书私钥对待验证数字证书进行签名，生成待验证证书签名
206、用户设备基于用户信息、待验证证书签名以及待验证数字证书，生成注册请求
206、用户设备将注册请求传输至电子病历存储设备
207、电子病历存储设备接收用户的注册请求，在注册请求中提取用户信息、待验证证书签名以及待验证数字证书，采用待验证数字证书对待验证证书签名进行验证，如果采用待验证证书公钥对待验证证书签名验证成功，则执行下述步骤208；如果采用待验证证书公钥对待验证证书签名验证失败，则执行下述步骤209
209、如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密失败，则生成失败响应
209、将失败指令返回至用户
208、如果电子病历存储设备采用待验证证书公钥对待验证证书签名解密成功，则提取用户的待存储用户标识，将待存储用户标识、用户信息和待验证数字证书存储至病历区块链中

图 2B

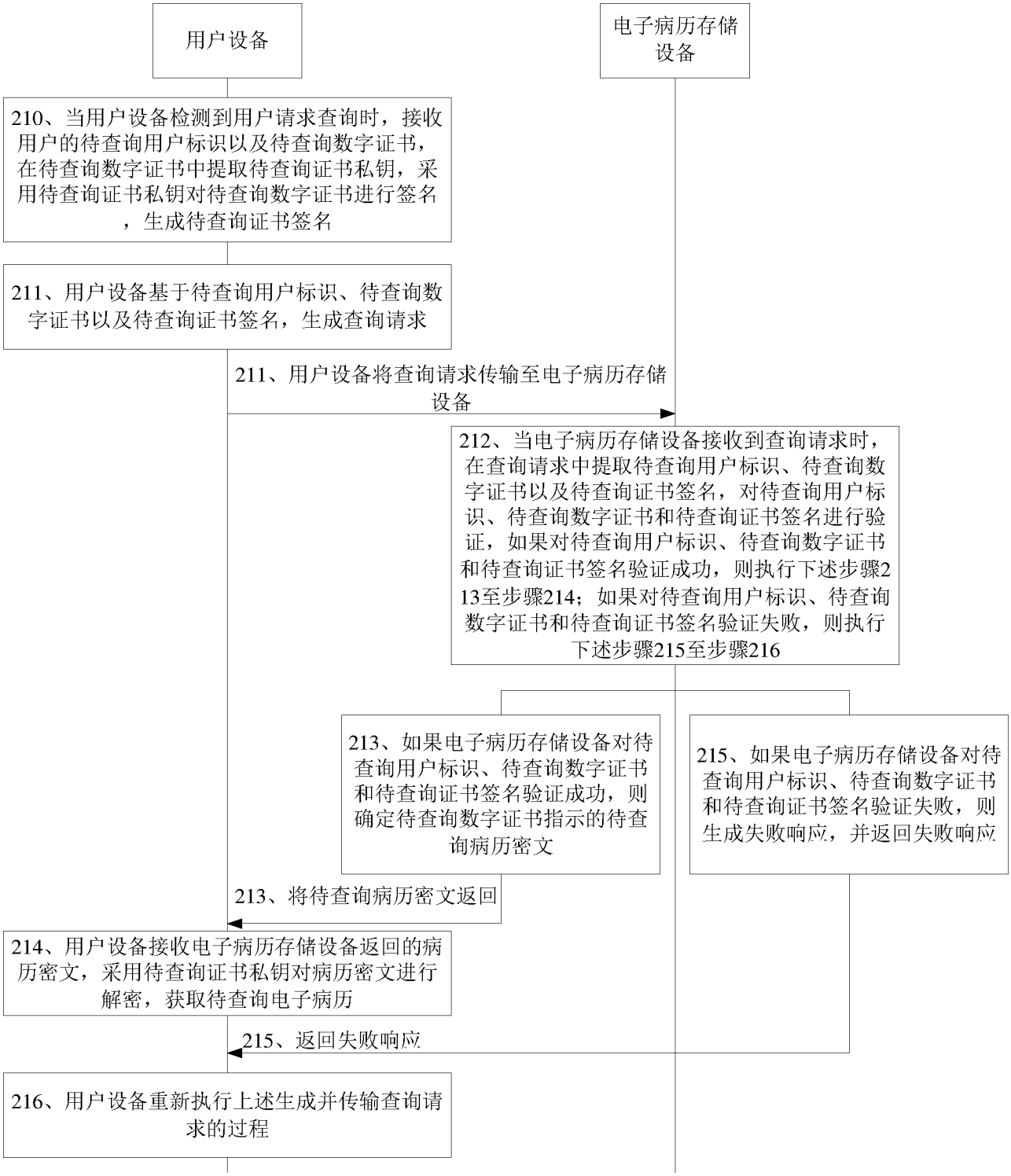
用户设备
电子病历存储设备
210、当用户设备检测到用户请求查询时，接收用户的待查询用户标识以及待查询数字证书，在待查询数字证书中提取待查询证书私钥，采用待查询证书私钥对待查询数字证书进行签名，生成待查询证书签名
211、用户设备基于待查询用户标识、待查询数字证书以及待查询证书签名，生成查询请求
211、用户设备将查询请求传输至电子病历存储设备
212、当电子病历存储设备接收到查询请求时，在查询请求中提取待查询用户标识、待查询数字证书以及待查询证书签名，对待查询用户标识、待查询数字证书和待查询证书签名进行验证，如果对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则执行下述步骤213至步骤214；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215至步骤216
213、如果电子病历存储设备对待查询用户标识、待查询数字证书和待查询证书签名验证成功，则确定待查询数字证书指示的待查询病历密文
215、如果电子病历存储设备对待查询用户标识、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
213、将待查询病历密文返回
214、用户设备接收电子病历存储设备返回的病历密文，采用待查询证书私钥对病历密文进行解密，获取待查询电子病历
215、返回失败响应
216、用户设备重新执行上述生成并传输查询请求的过程

图 2C

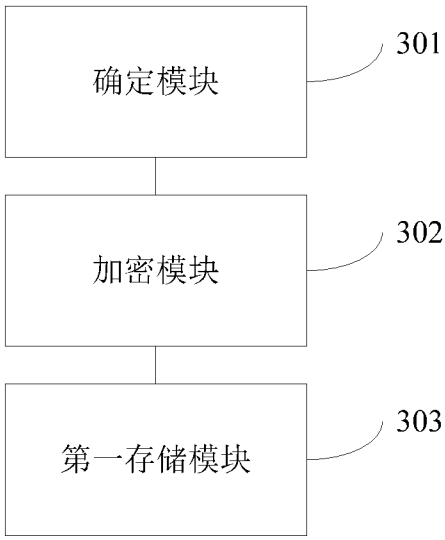
确定模块
301
加密模块
302
第一存储模块
303

图 3A

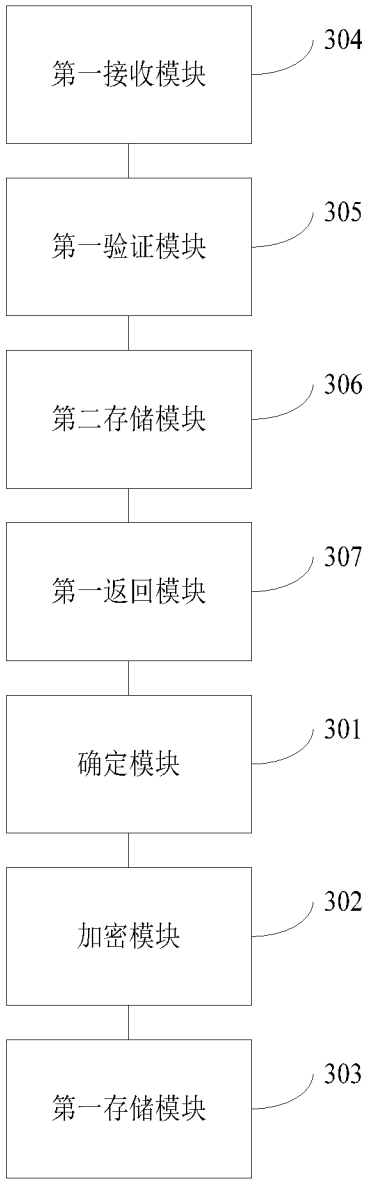
第一接收模块
304
第一验证模块
305
第二存储模块
306
第一返回模块
307
确定模块
301
加密模块
302
第一存储模块
303

图 3B

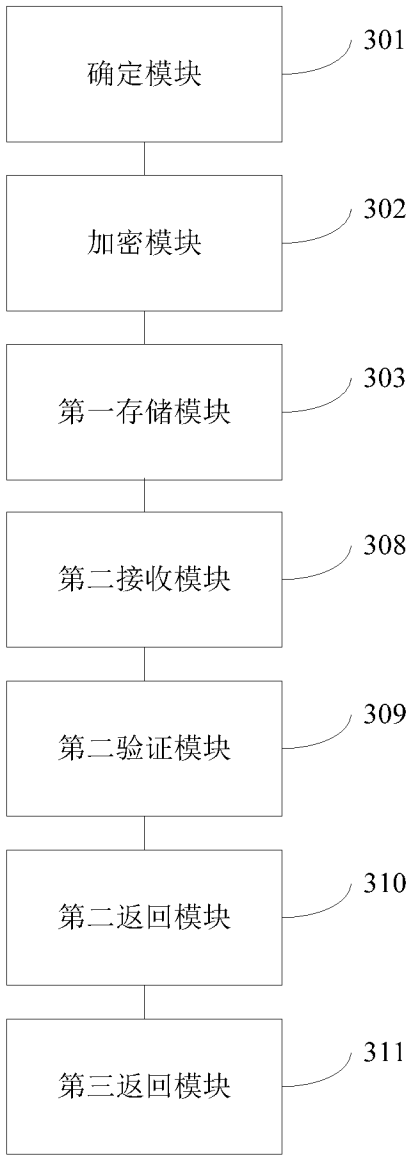
确定模块
301
加密模块
302
第一存储模块
303
第二接收模块
308
第二验证模块
309
第二返回模块
310
第三返回模块
311

图 3C

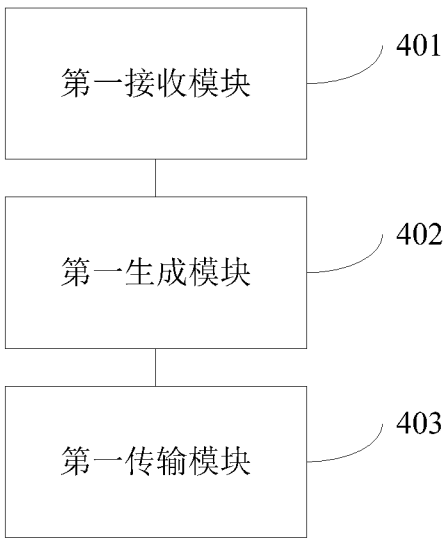
第一接收模块
401
第一生成模块
402
第一传输模块
403

图 4A

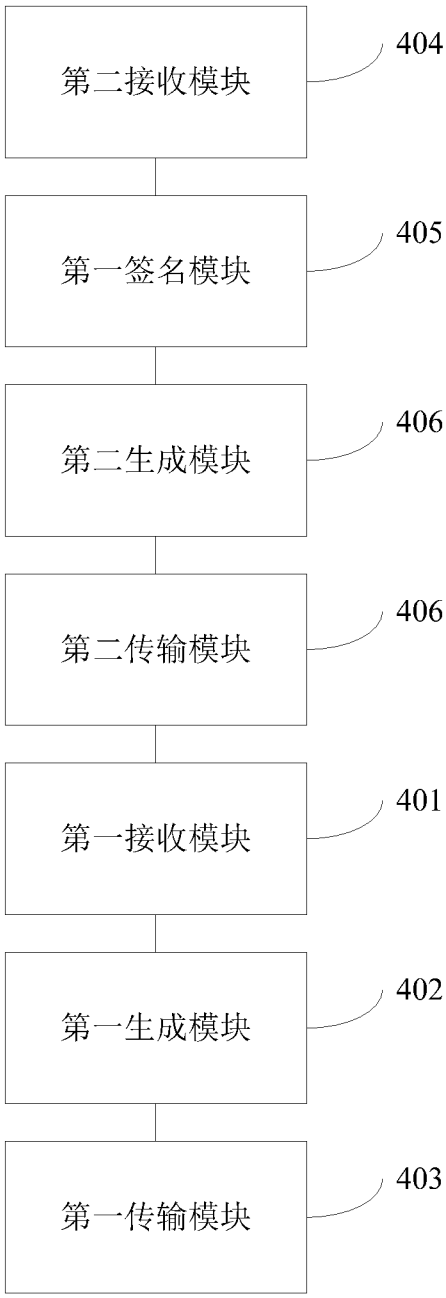
第二接收模块
404
第一签名模块
405
第二生成模块
406
第二传输模块
406
第一接收模块
401
第一生成模块
402
第一传输模块
403

图 4B

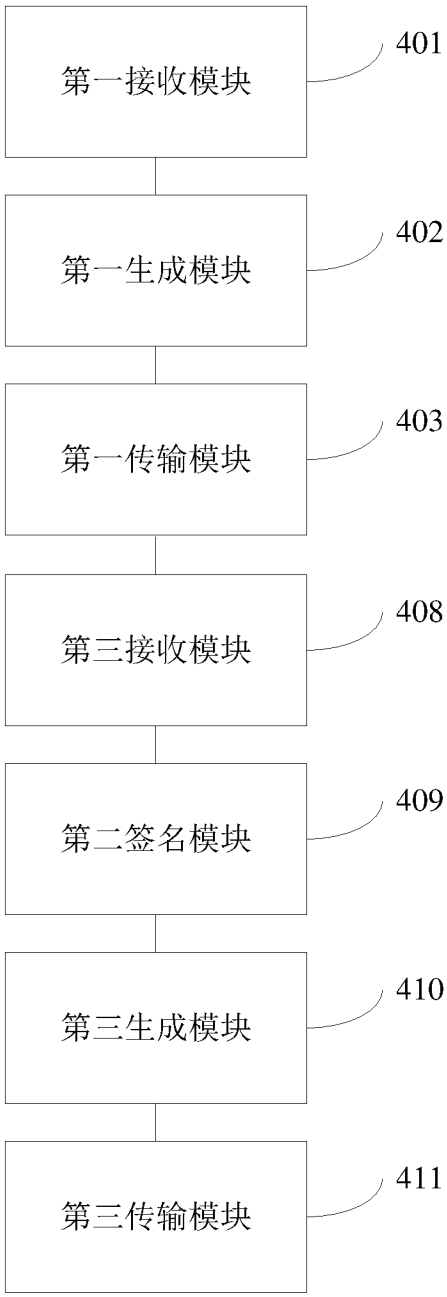
第一接收模块
401
第一生成模块
402
第一传输模块
403
第三接收模块
408
第二签名模块
409
第三生成模块
410
第三传输模块
411

图 4C

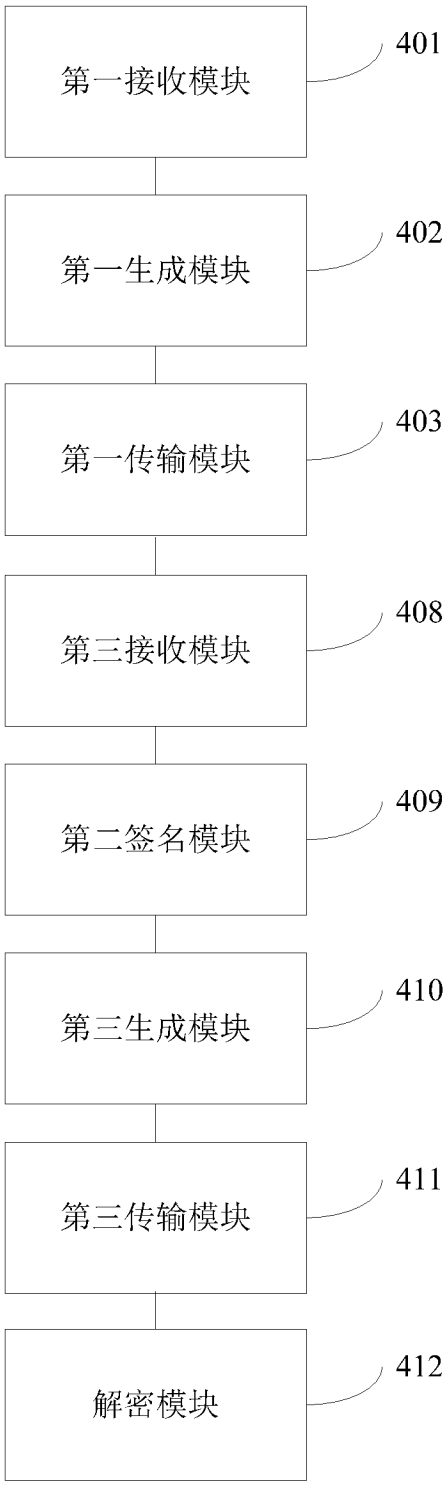
第一接收模块
401
第一生成模块
402
第一传输模块
403
第三接收模块
408
第二签名模块
409
第三生成模块
410
第三传输模块
411
解密模块
412

图 4D

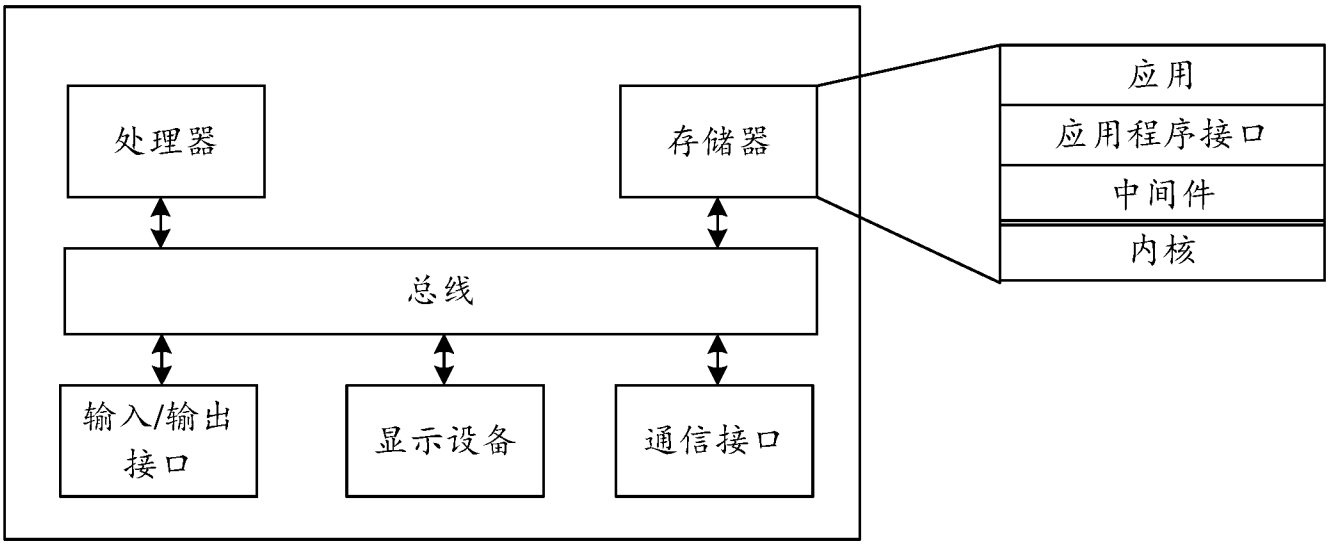

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/121815

A. CLASSIFICATION OF SUBJECT MATTER

G16H 10/60(2018.01)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)

G16H

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)

CNKI, DWPI, CNTXT, CNABS, IEEE: 病历, 证书, 区块链, 公钥, 用户, medical history, certificate, block chain, public key, user

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110010213 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 12 July 2019 (2019-07-12) claims 1-10 and description, paragraph 91	1-20
X	CN 107579979 A (CHENGDU UNIVERSITY OF TECHNOLOGY) 12 January 2018 (2018-01-12) description, paragraphs 4-16	1-20
A	CN 107563112 A (SHANGHAI RUOLING SOFTWARE TECHNOLOGY CO., LTD.) 09 January 2018 (2018-01-09) entire document	1-20
A	US 6952771 B1 (ENTRUST LIMITED) 04 October 2005 (2005-10-04) entire document	1-20
A	US 8788836 B1 (SYMANTEC CORPORATION) 22 July 2014 (2014-07-22) 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
27 February 2020	**06 March 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/CN2019/121815

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110010213 A	12 July 2019	None	
CN 107579979 A	12 January 2018	None	
CN 107563112 A	09 January 2018	None	
US 6952771 B1	04 October 2005	US 2006095769 A1	04 May 2006
		US 7685421 B2	23 March 2010
		US 6988198 B1	17 January 2006
US 8788836 B1	22 July 2014	None	

国际检索报告

国际申请号
PCT/CN2019/121815

A. 主题的分类

G16H 10/60(2018.01)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)

G16H

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））

CNKI, DWPI, CNTXT, CNABS, IEEE: 病历, 证书, 区块链, 公钥, 用户, medical history, certificate, block chain, public key, user

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 110010213 A (深圳壹账通智能科技有限公司) 2019年 7月 12日 (2019-07-12) 权利要求1-10，说明书第91段	1-20
X	CN 107579979 A (成都理工大学) 2018年 1月 12日 (2018-01-12) 说明书第4-16段	1-20
A	CN 107563112 A (上海若灵软件技术有限公司) 2018年 1月 9日 (2018-01-09) 全文	1-20
A	US 6952771 B1 (ENTRUST LIMITED) 2005年 10月 4日 (2005-10-04) 全文	1-20
A	US 8788836 B1 (SYMANTEC CORPORATION) 2014年 7月 22日 (2014-07-22) 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 27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 边臻 电话号码 86-(10)-53961419

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/121815

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	110010213	A	2019年 7月 12日	无			
CN	107579979	A	2018年 1月 12日	无			
CN	107563112	A	2018年 1月 9日	无			
US	6952771	B1	2005年 10月 4日	US	2006095769	A1	2006年 5月 4日
				US	7685421	B2	2010年 3月 23日
				US	6988198	B1	2006年 1月 17日
US	8788836	B1	2014年 7月 22日	无			