

(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)



(10) 国际公布号
WO 2020/186822 A1

(51) 国际专利分类号:
G16H 10/60 (2018.01)

(21) 国际申请号: PCT/CN2019/122574

(22) 国际申请日: 2019 年 12 月 3 日 (03.12.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910219136.4 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, 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,

(54) Title: BLOCKCHAIN-BASED DATA QUERYING METHOD, DEVICE AND APPARATUS, AND READABLE STORAGE MEDIUM

(54) 发明名称: 基于区块链的数据查询方法、装置、设备及可读存储介质

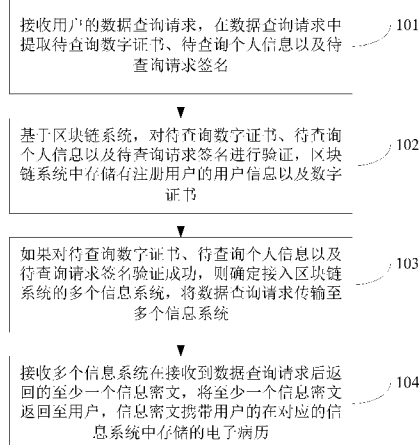


图 1A

- 101 Receive a data query request from a user, and extract, from the data query request, a digital certificate, personal information and a request signature for use in a query
- 102 Perform, on the basis of a blockchain system, authentication on the digital certificate, personal information and request signature, the blockchain system storing user information of a registered user and a digital certificate
- 103 If authentication of the digital certificate, personal information and request signature is successful, access multiple information systems of the blockchain system, and transmit the data query request to the multiple information systems
- 104 Receive at least one information ciphertext returned by the multiple information systems after receiving the data query request, and return the at least one information ciphertext to the user, the information ciphertext carrying electronic medical records of the user stored in the corresponding information system

(57) Abstract: The present invention relates to the field of blockchain-based data querying methods, devices and apparatuses, and readable storage mediums. Disclosed are a blockchain-based data querying method, device and apparatus, and a readable storage medium. In the invention, a data query request is transmitted to multiple information systems, and then information ciphertexts returned by the multiple information systems are received, thereby obtaining query data from the multiple information systems without having to send multiple data query requests, reducing the workload of a user querying data, and conserving a large amount of resources. The method comprises: receiving a data query request from a user, and extracting a digital certificate, personal information and a request signature for use in a query; performing authentication on the digital certificate, personal information and request signature; if the authentication is successful, transmitting the data query request to multiple information systems; and receiving at least one information ciphertext returned by the multiple information systems after receiving the data query request, and returning the at least one information ciphertext to the user.

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))。

(57) 摘要: 本申请公开了一种基于区块链的数据查询方法、装置、设备及可读存储介质, 涉及基于区块链的数据查询方法、装置、设备及可读存储介质领域, 将数据查询请求传输给多个信息系统, 并接收多个信息系统返回的信息密文, 使得可查询到多个信息系统的数据, 无需多次请求数据查询, 减少了用户查询数据的工作量, 节省了大量资源。所述方法包括: 接收用户的数据查询请求, 提取待查询数字证书、待查询个人信息以及待查询请求签名; 对待查询数字证书、待查询个人信息以及待查询请求签名进行验证; 如果验证成功, 则将数据查询请求传输至多个信息系统; 接收多个信息系统在接收到数据查询请求后返回的至少一个信息密文, 将至少一个信息密文返回至用户。

基于区块链的数据查询方法、装置、设备及可读存储介质

[0001] 本申请申明享有2019年03月21日递交的申请号为201910219136.4、名称为“基于区块链的数据查询方法、装置、设备及可读存储介质”中国专利申请的优先权，该中国专利申请的整体内容以参考的方式结合在本申请中。

技术领域

[0002] 本申请涉及互联网技术领域，特别是涉及一种基于区块链的数据查询方法、装置、设备及可读存储介质。

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数据存储及数据查询。

[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，也即将用户的电子病历与用户的身份信息、联系方式信息等个人信息绑定存储，在进行电子病历的数据查询时，用户将个人信息提供给信息系统，信息系统确定用户提供的个人信息对应的电子病历，将对应的电子病历直接返回给用户。

[0005] 在实现本申请的过程中，申请人发现相关技术至少存在以下问题：

[0006] 信息系统获取到的数据仅为其所服务的医院中用户的电子病历，如果用户想要查询其他医院的电子病历数据，需要再次向其他医院申请查询，导致用户查询电子病历的工作量较大，浪费了大量资源。

发明概述

技术问题

[0007] 有鉴于此，本申请提供了一种基于区块链的数据查询方法、装置、设备及可读

存储介质，主要目的在于解决目前用户查询电子病历的工作量较大，浪费了大量资源的问题。

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基于区块链的数据查询方法，该方法包括：

[0009] 接收用户的数据查询请求，在所述数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名；

[0010] 基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，所述区块链系统中存储有注册用户的用户信息以及数字证书；

[0011] 如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功，则确定接入所述区块链系统的多个信息系统，将所述数据查询请求传输至所述多个信息系统；

[0012] 接收所述多个信息系统在接收到所述数据查询请求后返回的至少一个信息密文，将所述至少一个信息密文返回至所述用户，所述信息密文携带所述用户的在对应的信息系统中存储的电子病历。

发明的有益效果

有益效果

[0013] 在本申请实施例中，与目前信息系统获取到的数据仅为其所服务的医院中用户的电子病历的方式相比，本申请通过验证的数据查询请求传输给接入区块链系统的多个信息系统，多个信息系统均可以返回符合数据查询请求的信息密文，使得在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，减少了用户查询电子病历的工作量，节省了大量资源。

对附图的简要说明

附图说明

[0014] 图1A示出了本申请实施例提供的一种基于区块链的数据查询方法流程示意图；

- [0015] 图1B示出了本申请实施例提供的一种基于区块链的数据查询方法流程示意图；
- [0016] 图2A示出了本申请实施例提供的一种基于区块链的数据查询方法流程示意图；
- [0017] 图2B示出了本申请实施例提供的一种基于区块链的数据查询方法流程示意图；
- [0018] 图3A示出了本申请实施例提供的一种基于区块链的数据查询装置的结构示意图；
- [0019] 图3B示出了本申请实施例提供的一种基于区块链的数据查询装置的结构示意图；
- [0020] 图3C示出了本申请实施例提供的一种基于区块链的数据查询装置的结构示意图；
- [0021] 图4A示出了本申请实施例提供的一种基于区块链的数据查询装置的结构示意图；
- [0022] 图4B示出了本申请实施例提供的一种基于区块链的数据查询装置的结构示意图；
- [0023] 图4C示出了本申请实施例提供的一种基于区块链的数据查询装置的结构示意图；
- [0024] 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

- [0025] 本申请实施例提供了一种基于区块链的数据查询方法，可以将通过验证的数据查询请求传输给接入区块链系统的多个信息系统，多个信息系统均可以返回符合数据查询请求的信息密文，使得在进行数据查询时，可以查询到多个信息系统的数据库，无需多次向多个信息系统请求数据查询，达到减少了用户查询电子病历的工作量，节省了大量资源的目的，如图1A所示，该方法包括：
- [0026] 101、接收用户的数据查询请求，在数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名。
- [0027] 在本申请实施例中，为了使区块链系统在接收到数据查询请求时，可以获知需要请求查询哪一种数据，因此，数据查询请求中会携带待查询数字证书、待查询个人信息以及待查询请求签名，这样，区块链系统便可以在数据查询请求中

提取到待查询数字证书、待查询个人信息以及待查询请求签名。

[0028] 102、基于区块链系统，对待查询数字证书、待查询个人信息以及待查询请求签名进行验证，区块链系统中存储有注册用户的用户信息以及数字证书。

[0029] 在本申请实施例中，为了确定该数据查询请求在传输的过程中是否被篡改，以及用户提供的待查询数字证书是否真实，区块链系统在提取到待查询数字证书、待查询个人信息以及待查询请求签名后，对待查询数字证书、待查询个人信息以及待查询请求签名进行验证。

[0030] 103、如果对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，则确定接入区块链系统的多个信息系统，将数据查询请求传输至多个信息系统。

[0031] 在本申请实施例中，如果对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，则表示该待查询数字证书是真实的，该数据查询请求在传输的过程中并没有被篡改，是可以进行数据查询的。由于区块链系统中接入有多个信息系统，每个信息系统中均可能存储有符合数据查询请求的数据，因此，为了使返回给用户的数据是完整的，区块链系统会将通过验证的数据查询请求下发给接入到区块链系统中的每一个信息系统，以便信息系统对数据进行查询。

[0032] 104、接收多个信息系统在接收到数据查询请求后返回的至少一个信息密文，将至少一个信息密文返回至用户，信息密文携带用户的在对应的信息系统中存储的电子病历。

[0033] 在本申请实施例中，由于信息系统在接收到数据查询请求后均会进行数据查询，且查询到数据的信息系统会将查询到的数据返回给区块链系统，因此，区块链系统可以接收到信息系统返回的至少一个信息密文，并将接收到的全部信息密文返回给用户。

[0034] 在实际应用的过程中，可能用户之前并没有在任何的医院就医，使得每一个信息系统均不能查询到符合数据查询请求的数据，因此，区块链系统还可能不会接收到任何信息密文，这时，区块链系统对用户进行提示即可。本申请实施例对区块链系统接收到信息密文的个数不进行具体限定。

[0035] 本申请实施例提供的方法，将通过验证的数据查询请求传输给接入区块链系统

的多个信息系统，多个信息系统均可以返回符合数据查询请求的信息密文，使得在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，减少了用户查询电子病历的工作量，节省了大量资源。

[0036] 本申请实施例提供了一种基于区块链的数据查询方法，可以当信息系统接收到区块链系统发送的数据查询请求时，会将自身包括的与数据查询请求相关的数据返回给区块链系统，使得区块链在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，达到减少了用户查询电子病历的工作量，节省了大量资源的目的，如图1B所示，该方法包括：

[0037] 105、当接收到区块链系统的数据查询请求时，确定数据查询请求指示的目标电子病历。

[0038] 在本申请实施例中，当信息系统接收到区块链系统传输的数据查询请求时，由于数据查询请求中包括了待查询个人信息，因此，信息系统可以确定数据查询请求指示的电子病历作为目标电子病历。

[0039] 需要说明的是，考虑到用户可能并没有在信息系统所服务的医院中就医，使得信息系统中可能并不会获取到与数据查询请求匹配的目标电子病历，因此，如果信息系统获取目标电子病历失败了，则信息系统可以直接向区块链系统返回无数据指令，并终止执行下述步骤106和步骤107，继续接收其他的数据查询请求。

[0040] 106、在数据查询请求中提取待查询数字证书，基于待查询数字证书和目标电子病历，生成信息密文。

[0041] 在本申请实施例中，由于数据查询请求中还会携带待查询数字证书，为了保证目标电子病历在传输过程中的安全性，信息系统可以在数据查询请求中提取待查询数字证书，并基于该待查询数字证书和目标电子病历，生成信息密文，并在后续将该信息密文传输。

[0042] 107、将信息密文传输至区块链系统。

[0043] 在本申请实施例中，当信息系统生成了信息密文后，便可以将信息密文传输给区块链系统，以便区块链系统将接收到的信息密文返回给用户。

[0044] 本申请实施例提供的方法，当信息系统接收到区块链系统发送的数据查询请求

时，会将自身包括的与数据查询请求相关的数据返回给区块链系统，使得区块链在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，减少了用户查询电子病历的工作量，节省了大量资源。

[0045] 本申请实施例提供了一种基于区块链的数据查询方法，可以将通过验证的数据查询请求传输给接入区块链系统的多个信息系统，多个信息系统均可以返回符合数据查询请求的信息密文，使得在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，达到减少了用户查询电子病历的工作量，节省了大量资源的目的，如图2A所示，该方法包括：

[0046] 201、区块链系统接收用户的数据查询请求，在数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名。

[0047] 在本申请实施例中，区块链系统中接入有多个医院的信息系统，每个信息系统中都存储有大量的用户信息，为了确定具体用户请求查询哪种信息，以便根据用户的需求为用户提供信息查询的服务，数据查询请求中需要携带待查询数字证书、待查询个人信息以及待查询请求签名。

[0048] 在实际应用的过程中，区块链系统可以提供专门为用户提供各项服务的客户端，用户通过在私人终端中下载该客户端来享受区块链系统提供的服务。其中，该客户端中可以提供数据查询入口，当检测到用户触发该数据查询入口时，显示数据查询页面，在该数据查询页面中提供数字证书上传框、个人信息输入框以及请求签名输入框等。在检测到用户对数据查询页面的确认时，确定接收到用户的数据查询请求，在数据查询请求中进行提取，获取到数据查询请求携带的待查询数字证书、待查询个人信息以及待查询请求签名。其中，由于只有在区块链系统中注册过的用户才会将电子病历上传到区块链系统中，而在区块链中注册过的用户都会拥有数字证书，因此，在进行数据查询时，用户需要在数据查询请求中携带待查询数字证书，以便区块链系统根据该待查询数字证书来确定用户是否在区块链系统中注册过。

[0049] 另外，为了避免数据查询请求在传输的过程中被篡改，数据查询请求中还可以包括待查询请求签名，待查询请求签名是采用待查询数字证书的待查询证书公钥对待查询个人信息解密后生成的，可由用户所持的终端在接收到用户上传的

待查询个人信息以及待查询数字证书后自行生成，这样，当区块链系统接收到数据查询请求时，便可以基于该待查询请求签名对数据查询请求进行验证，从而确定该数据查询请求是否在传输的过程中被篡改。

[0050] 202、区块链系统对待查询数字证书、待查询个人信息以及待查询请求签名进行验证，如果对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，则执行下述步骤203至步骤206；如果对待查询数字证书、待查询个人信息以及待查询请求签名验证失败，则执行下述步骤207。

[0051] 在本申请实施例中，当获取到待查询数字证书、待查询个人信息以及待查询请求签名后，为了避免将不法分子的恶意请求下发给各个医院的信息系统，导致各个医院的信息系统存在安全隐患，需要先对获取到的待查询数字证书、待查询个人信息以及待查询请求签名进行验证，并在通过验证后才可以进一步的将数据查询请求下发给各个信息系统。

[0052] 由于区块链在数据查询请求中可以获取到待查询数字证书、待查询个人信息以及待查询请求签名，因此，在对待查询数字证书、待查询个人信息以及待查询请求签名进行验证时，考虑到在区块链系统中注册过的用户会有个人信息存储在区块链系统，这样，首先，在区块链系统中查询是否存在与待查询个人信息一致的个人信息，通过查询区块链系统中是否包括待查询个人信息来确定该用户是否在区块链系统中注册过；随后，考虑到待查询请求签名是基于待查询数字证书的待查询证书公钥生成的，因此，获取待查询数字证书的待查询证书公钥，采用待查询证书公钥对待查询请求签名解密，通过解密的方式对待查询请求签名进行验证，从而判断该待查询请求签名的真实性。需要说明的是，由于在区块链系统中成功注册的用户数字证书也会存储在区块链系统中，因此，在进行验证时，如果区块链系统中存储有与待查询个人信息一致的个人信息，则还可以获取该个人信息对应的数字证书，将该数字证书与待查询数字证书进行比对，如果确定该数字证书与该待查询数字证书一致，则确定该待查询数字证书是真实的，该待查询数字证书通过验证，继续对其他对象进行验证。需要说明的是，在对待查询数字证书、待查询个人信息以及待查询请求签名进行验证时，验证的顺序并不是固定的，先对哪一项进行验证都可以，本申请实施例

对验证的顺序不进行具体限定。

[0053] 通过上述对待查询数字证书、待查询个人信息以及待查询请求签名的验证，当区块链系统中存在与待查询个人信息一致的个人信息，且采用待查询证书公钥对待查询请求签名解密成功时，表明数据查询请求中携带的待查询数字证书、待查询个人信息以及待查询请求签名均通过了验证，这时，便可以确定对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，继续执行下述步骤203至步骤206；当区块链系统中不存在与待查询个人信息一致的个人信息，或采用待查询证书公钥对待查询请求签名解密失败时，表明数据查询请求中携带的待查询数字证书、待查询个人信息以及待查询请求签名没有通过验证，这时，便可以确定对待查询数字证书、待查询个人信息以及待查询请求签名验证失败，继续执行下述步骤207。需要说明的是，只要待查询数字证书、待查询个人信息以及待查询请求签名中有任一项没有通过验证，则即可确定整个数据查询请求都没有通过验证，只能执行下述步骤207。

[0054] 203、如果对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，则确定接入区块链系统的多个信息系统，区块链系统将数据查询请求传输至多个信息系统。

[0055] 在本申请实施例中，如果对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，则表示该数据查询请求通过验证，此时，便可以将数据查询请求下发给接入到区块链系统中的多个信息系统，以便信息系统按照数据查询请求查询并返回数据。

[0056] 其中，多个信息系统是以节点的形式接入到区块链系统中的，因此，区块链系统可以通过与信息系统之间的数据连接，将数据查询请求传输给接入到区块链系统中的每一个信息系统。

[0057] 204、当信息系统接收到区块链系统的数据查询请求时，在数据查询请求中提取待查询个人信息，基于待查询个人信息，提取待查询个人信息对应的目标电子病历。

[0058] 在本申请实施例中，对于多个信息系统中的任一信息系统，当信息系统接收到区块链系统传输的数据查询请求时，由于数据查询请求中携带了待查询个人信

息，因此，信息系统可以在数据查询请求中提取待查询个人信息，根据待查询个人信息在信息系统中查询该待查询个人信息对应的电子病历作为目标电子病历，并将该目标电子病历提取出来，以便后续将该目标电子病历返回给区块链系统。

[0059] 在实际应用的过程中，可能用户没有当前的信息系统所服务的医院中进行过治疗，使得该信息系统中无法确定目标电子病历，这样，信息系统便可以不再执行下述的其他内容。另外，为了使区块链系统可以知晓当前的信息系统中不存在目标电子病历，如果信息系统没有获取到目标电子病历，则可以生成无数据指令，并将该无数据指令返回给区块链系统，以便区块链系统可以获知当前信息系统中没有存储该用户的电子病历，而非信息系统发生故障。

[0060] 205、在数据查询请求中提取待查询数字证书，获取待查询数字证书的待查询证书公钥，采用待查询证书公钥，对目标电子病历进行加密，生成信息密文，将信息密文传输至区块链系统。

[0061] 在本申请实施例中，由于用户在申请数字证书时，需要先生成证书公私钥对，证书私钥自己保存，将证书公钥和用户信息提交给认证机构，由认证机构将证书公钥与用户的个人信息绑定并进行签名，从而签发数字证书，使得数字证书中包含有证书公钥。这样，在获取到目标电子病历后，考虑到采用证书公钥加密后的密文可以采用证书私钥进行解密，因此，为了保证目标电子病历在传输过程中的安全，信息系统在将目标电子病历传输给区块链系统之前，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目标电子病历进行加密，生成信息密文，并将该信息密文传输给区块链系统，以便保证目标电子病历在传输过程中的安全性，避免目标电子病历中的数据被人窃取。

[0062] 206、区块链系统接收多个信息系统在接收到数据查询请求后返回的至少一个信息密文，将至少一个信息密文返回至用户。

[0063] 在本申请实施例中，由于区块链系统在将数据查询请求下发给多个信息系统后，每个信息系统均会查询并获取到对应的用户电子病历，且还会对电子病历进行加密生成信息密文，因此，在区块链系统将查询请求传输给多个信息系统后，会接收到多个信息系统返回的信息密文，而考虑到有些信息系统可能没有查

询到需要查询的信息，因此，可能接收到至少一个信息密文，这时，区块链系统便可以将至少一个信息密文整合起来返回给用户。需要说明的是，考虑到用户可能没有在某些医院检查过，使得该医院不会给区块链系统返回信息密文，可能仅会给区块链系统返回一个无数据指令，因此，区块链系统仅需将获取到的信息密文返回给用户即可，无需一定要全部的医院均给予信息密文的回馈。另外，还可能存在用户未在任何医院就医的情况，这时，可能不会获取到任何的信息密文，这时，区块链系统便可以生成无数据指令，并将该无数据指令返回给用户，本申请对得到的信息密文的个数或者是否能够获取到信息密文不进行具体限定。

[0064] 207、如果对待查询数字证书、待查询个人信息以及待查询请求签名验证失败，则生成查询失败响应，将查询失败响应传输至用户。

[0065] 在本申请实施例中，如果对待查询数字证书、待查询个人信息以及待查询请求签名验证失败，则表示该数据查询请求没有通过区块链系统的验证，此时，区块链系统是不能将该数据查询请求传输给信息系统的，需要用户重新提供数字证书、个人信息以及请求签名，因此，生成查询失败响应，将该查询失败响应传输给用户，以使用户重新发送数据查询请求。

[0066] 需要说明的是，区块链系统在生成查询失败响应时，可以在查询请求指令中携带错误指示，也即提醒用户待查询数字证书、待查询个人信息以及待查询请求签名中的哪一项信息发生了错误，以使用户更加注意该项信息的输入，避免再次发生错误。本申请实施例对查询失败响应包括的内容不进行具体限定。

[0067] 在实际应用的过程中，为了防止不法分子随意向区块链系统下发各种指令，导致区块链系统的瘫痪以及数据的丢失，用户在使用区块链系统提供的各项服务之前，需要在区块链系统中进行注册，并在注册成功后，方可向区块链系统下发指令，参见图2B，该方法包括：

[0068] 208、当接收到用户注册请求时，在用户注册请求中提取待注册用户信息、待注册数字签名以及待注册数字证书。

[0069] 在本申请实施例中，区块链系统的客户端中可以为用户提供注册入口，当用户所持的终端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，需要用户提供自身所持的数字证书作为待注册数字证书，以便基于该待注册数字证书对用户的身份进行验证。在实际应用的过程中，用户所持的终端为了进一步保证待注册数字证书以及待注册用户信息在传输过程中的安全性，通常会采用待注册数字证书中的待注册证书私钥对待注册数字证书进行签名得到的待注册数字签名，签名的过程实质为加密的过程，也即用户所持的终端将加密后的待注册数字证书作为待注册数字签名，并将该待注册数字签名也携带在用户注册请求中，使得区块链系统可以接收到携带待注册用户信息、待注册数字签名以及待注册数字证书的用户注册请求，以便在后续可以通过验证该待注册数字签名实现对待注册数字证书的验证。

[0070] 这样，当区块链系统接收到用户基于所持终端中下载的客户端发送的用户注册请求后，便可以在该用户注册请求中提取到待注册用户信息、待注册数字签名以及待注册数字证书。

[0071] 209、在待注册数字证书中提取证书签名，将证书签名与预设签名进行比对，在待注册数字证书中提取待注册证书公钥，采用待注册证书公钥对待注册数字签名解密，如果证书签名与预设签名一致，且采用待注册证书公钥对待注册数字签名解密成功，则执行下述步骤210；如果证书签名与预设签名不一致，或采用待注册证书公钥对待注册数字签名解密失败，则执行下述步骤211。

[0072] 在本申请实施例中，预设签名为证书机构提供的用于验证证书签名是否有效的签名。由于认证机构在下发数字证书时，都会在数字证书中携带证书签名，将该证书签名作为防伪标志，从而证明数字证书是由认证机构下发的，因此，可以在待注册数字证书中提取证书签名，将该证书签名与认证机构提供的预设签名进行比对，通过判断该证书签名与预设签名是否一致来确定该待注册数字正式是否是认证机构下发的，而不是不法分子伪造的。另外，由于用户注册请求中还携带待注册数字签名，待注册数字签名是基于待注册数字证书的待注册证书私钥对待注册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，可以采用待注册证书公钥对待注册证书签名解密，并根据是否签名

成功来确定待注册数字签名的真实性。

[0073] 综上所述，在对待注册数字签名以及待注册数字证书进行验证时，首先，在待注册数字证书中提取证书签名，将证书签名与预设签名进行比对；随后，在待注册数字证书中提取待注册证书公钥，采用待注册证书公钥对待注册数字签名解密，从而实现对待注册数字签名以及待注册数字证书的验证。本申请实施例对验证待注册数字签名以及待注册数字证书的先后顺序不进行具体限定。

[0074] 其中，如果证书签名与预设签名一致，且采用待注册证书公钥对待注册数字签名解密成功，则表示待注册数字签名以及待注册数字证书通过验证，该用户是可以在区块链系统中注册的，因此，为用户进行注册，也即执行下述步骤210；如果证书签名与预设签名不一致，或采用待注册证书公钥对待注册数字签名解密失败，则表示待注册数字签名以及待注册数字证书没有通过验证，待注册数字签名以及待注册数字证书不真实或者是错误的，该用户是不可以在区块链系统中注册的，需要用户提供真实的或者正确的待注册数字签名以及待注册数字证书，也即执行下述步骤211。

[0075] 210、如果证书签名与预设签名一致，且采用待注册证书公钥对待注册数字签名解密成功，则将待注册用户信息和待注册数字证书对应存储至区块链系统。

[0076] 在本申请实施例中，如果证书签名与预设签名一致，且采用待注册证书公钥对待注册数字签名解密成功，则表示该用户是可以在区块链系统中注册的，因此，区块链系统将该待注册用户信息以及待注册数字证书对应存储在区块链系统中，完成该用户在区块链系统中的注册。

[0077] 211、如果证书签名与预设签名不一致，或采用待注册证书公钥对待注册数字签名解密失败，则生成并返回注册失败响应。

[0078] 在本申请实施例中，如果证书签名与预设签名不一致，或采用待注册证书公钥对待注册数字签名解密失败，则表示该用户注册请求很可能在传输的过程中被篡改，真实性无法验证，或者用户提供的待注册数字证书和待注册数字签名可能是虚假的或者不正确的，此时，便不能实现用户在区块链系统中的注册，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，以使用户接收到失败响应可以重新发送用户注册请求。

- [0079] 本申请实施例提供的方法，通过验证的数据查询请求传输给接入区块链系统的多个信息系统，多个信息系统均可以返回符合数据查询请求的信息密文，使得在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，减少了用户查询电子病历的工作量，节省了大量资源。
- [0080] 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基于区块链的数据查询装置，如图3A所示，所述装置包括：接收模块301，验证模块302，第一传输模块303和第一返回模块304。
- [0081] 该接收模块301，用于接收用户的数据查询请求，在所述数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名；
- [0082] 该验证模块302，用于基于区块链系统，对待查询数字证书、待查询个人信息以及待查询请求签名进行验证，区块链系统中存储有注册用户的用户信息以及数字证书；
- [0083] 该第一传输模块303，用于如果对待查询数字证书、待查询个人信息以及待查询请求签名验证成功，则确定接入区块链系统的多个信息系统，将数据查询请求传输至多个信息系统；
- [0084] 该第一返回模块304，用于接收多个信息系统在接收到数据查询请求后返回的至少一个信息密文，将至少一个信息密文返回至用户，信息密文携带用户的在对应的信息系统中存储的电子病历。
- [0085] 在具体的应用场景中，如图3B所示，该装置还包括：提取模块305，比对模块306，签名模块307，存储模块308和第二返回模块309。
- [0086] 该提取模块305，用于当接收到用户注册请求时，在所述用户注册请求中提取待注册用户信息、待注册数字签名以及待注册数字证书；
- [0087] 该比对模块306，用于在所述待注册数字证书中提取证书签名，将所述证书签名与预设签名进行比对，所述预设签名为证书机构提供的用于验证所述证书签名是否有效的签名；
- [0088] 该签名模块307，用于在所述待注册数字证书中提取待注册证书公钥，采用所述待注册证书公钥对所述待注册数字签名解密；
- [0089] 该存储模块308，用于如果所述证书签名与所述预设签名一致，且采用所述待

注册证书公钥对所述待注册数字签名解密成功，则将所述待注册用户信息和所述待注册数字证书对应存储至所述区块链系统；

[0090] 该第二返回模块309，用于如果所述证书签名与所述预设签名不一致，或采用所述待注册证书公钥对所述待注册数字签名解密失败，则生成并返回注册失败响应。

[0091] 在具体的应用场景中，该验证模块302，用于在所述区块链系统中查询是否存在与所述待查询个人信息一致的个人信息；获取所述待查询数字证书的待查询证书公钥，采用所述待查询证书公钥对所述待查询请求签名解密；

[0092] 相应地，该存储模块308，用于当所述区块链系统中存在与所述待查询个人信息一致的个人信息，且采用所述待查询证书公钥对所述待查询请求签名解密成功时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功；

[0093] 该第一返回模块304，用于当所述区块链系统中不存在与所述待查询个人信息一致的个人信息，或采用所述待查询证书公钥对所述待查询请求签名解密失败时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败。

[0094] 在具体的应用场景中，如图3C所示，该装置还包括：第二传输模块310。

[0095] 该第二传输模块310，用于如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败，则生成查询失败响应，将所述查询失败响应传输至所述用户。

[0096] 本申请实施例提供的装置，将通过验证的数据查询请求传输给接入区块链系统的多个信息系统，多个信息系统均可以返回符合数据查询请求的信息密文，使得在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，减少了用户查询电子病历的工作量，节省了大量资源。

[0097] 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基于区块链的数据查询装置，如图4A所示，所述装置包括：确定模块401，生成模块402和传输模块403。

[0098] 该确定模块401，用于当接收到区块链系统的数据查询请求时，确定所述数据

查询请求指示的目标电子病历；

[0099] 该生成模块402，用于在所述数据查询请求中提取待查询数字证书，基于所述待查询数字证书和所述目标电子病历，生成信息密文；

[0100] 该传输模块403，用于将所述信息密文传输至所述区块链系统。

[0101] 在具体的应用场景中，如图4B所示，该确定模块401，包括提取子模块4011和查询子模块4012。

[0102] 该提取子模块4011，用于当接收到所述区块链系统的数据查询请求时，在所述数据查询请求中提取待查询个人信息；

[0103] 该查询子模块4012，用于基于所述待查询个人信息，在所述区块链系统中提取所述待查询个人信息对应的目标电子病历。

[0104] 在具体的应用场景中，如图4C所示，该生成模块402，包括获取子模块4021和生成子模块4022。

[0105] 该获取子模块4021，用于在所述数据查询请求中提取待查询数字证书，获取所述待查询数字证书的待查询证书公钥；

[0106] 该生成子模块4022，用于采用所述待查询证书公钥，对所述目标电子病历进行加密，生成所述信息密文。

[0107] 本申请实施例提供的装置，当信息系统接收到区块链系统发送的数据查询请求时，会将自身包括的与数据查询请求相关的数据返回给区块链系统，使得区块链在进行数据查询时，可以查询到多个信息系统的数据，无需多次向多个信息系统请求数据查询，减少了用户查询电子病历的工作量，节省了大量资源。

[0108] 需要说明的是，本申请实施例提供的一种基于区块链的数据查询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2B中的对应描述，在此不再赘述。

[0109] 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基于区块链的数据查询方法。

- [0110] 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的基于区块链的数据查询方法的步骤。
- [0111] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到本申请可以通过硬件实现，也可以借助软件加必要的通用硬件平台的方式来实现。基于这样的理解，本申请的技术方案可以以软件产品的形式体现出来，该软件产品可以存储在一个非易失性存储介质（可以是CD-ROM，U盘，移动硬盘等）中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备）执行本申请各个实施场景所述的方法。
- [0112] 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。
- [0113] 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。
- [0114] 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计算机非易失性可读取存储介质中，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。
- [0115] 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] 一种基于区块链的数据查询方法，其特征在于，包括：
- 接收用户的数据查询请求，在所述数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名；
- 基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，所述区块链系统中存储有注册用户的用户信息以及数字证书；
- 如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功，则确定接入所述区块链系统的多个信息系统，将所述数据查询请求传输至所述多个信息系统；
- 接收所述多个信息系统在接收到所述数据查询请求后返回的至少一个信息密文，将所述至少一个信息密文返回至所述用户，所述信息密文携带所述用户的在对应的信息系统中存储的电子病历。
- [权利要求 2] 根据权利要求1所述的方法，其特征在于，所述接收用户的数据查询请求，在所述数据查询请求中提取待查询数据标识、待查询数字证书、待查询个人信息以及待查询请求签名之前，包括：
- 当接收到用户注册请求时，在所述用户注册请求中提取待注册用户信息、待注册数字签名以及待注册数字证书；
- 在所述待注册数字证书中提取证书签名，将所述证书签名与预设签名进行比对，所述预设签名为证书机构提供的用于验证所述证书签名是否有效的签名；
- 在所述待注册数字证书中提取待注册证书公钥，采用所述待注册证书公钥对所述待注册数字签名解密；
- 如果所述证书签名与所述预设签名一致，且采用所述待注册证书公钥对所述待注册数字签名解密成功，则将所述待注册用户信息和所述待注册数字证书对应存储至所述区块链系统；
- 如果所述证书签名与所述预设签名不一致，或采用所述待注册证书公钥对所述待注册数字签名解密失败，则生成并返回注册失败响应。

- [权利要求 3] 根据权利要求1所述的方法，其特征在于，所述基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，包括：
- 在所述区块链系统中查询是否存在与所述待查询个人信息一致的个人信息；
- 获取所述待查询数字证书的待查询证书公钥，采用所述待查询证书公钥对所述待查询请求签名解密；
- 相应地，当所述区块链系统中存在与所述待查询个人信息一致的个人信息，且采用所述待查询证书公钥对所述待查询请求签名解密成功时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功；
- 当所述区块链系统中不存在与所述待查询个人信息一致的个人信息，或采用所述待查询证书公钥对所述待查询请求签名解密失败时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败。
- [权利要求 4] 根据权利要求1所述的方法，其特征在于，所述基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证之后，所述方法还包括：
- 如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败，则生成查询失败响应，将所述查询失败响应传输至所述用户。
- [权利要求 5] 一种基于区块链的数据查询方法，其特征在于，包括：
- 当接收到区块链系统的数据查询请求时，确定所述数据查询请求指示的目标电子病历；
- 在所述数据查询请求中提取待查询数字证书，基于所述待查询数字证书和所述目标电子病历，生成信息密文；
- 将所述信息密文传输至所述区块链系统。
- [权利要求 6] 根据权利要求5所述的方法，其特征在于，所述当接收到区块链系统

的数据查询请求时，确定所述数据查询请求指示的目标电子病历，包括：

当接收到所述区块链系统的数据查询请求时，在所述数据查询请求中提取待查询个人信息；

基于所述待查询个人信息，在所述区块链系统中提取所述待查询个人信息对应的目标电子病历。

[权利要求 7]

根据权利要求5所述的方法，其特征在于，所述在所述数据查询请求中提取待查询数字证书，基于所述待查询数字证书和所述目标电子病历，生成信息密文，包括：

在所述数据查询请求中提取待查询数字证书，获取所述待查询数字证书的待查询证书公钥；

采用所述待查询证书公钥，对所述目标电子病历进行加密，生成所述信息密文。

[权利要求 8]

一种基于区块链的数据查询装置，其特征在于，包括：

接收模块，用于接收用户的数据查询请求，在所述数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名；

验证模块，用于基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，所述区块链系统中存储有注册用户的用户信息以及数字证书；

第一传输模块，用于如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功，则确定接入区块链系统的多个信息系统，将所述数据查询请求传输至所述多个信息系统；

第一返回模块，用于接收所述多个信息系统在接收到所述数据查询请求后返回的至少一个信息密文，将所述至少一个信息密文返回至所述用户，所述信息密文携带所述用户的在对应的信息系统中存储的电子病历。

[权利要求 9]

如权利要求8所述的数据查询装置，其特征在于，还包括：

提取模块，用于当接收到用户注册请求时，在所述用户注册请求中提

取得注册用户信息、待注册数字签名以及待注册数字证书；

比对模块，用于在所述待注册数字证书中提取证书签名，将所述证书签名与预设签名进行比对，所述预设签名为证书机构提供的用于验证所述证书签名是否有效的签名；

比对模块，用于在所述待注册数字证书中提取待注册证书公钥，采用所述待注册证书公钥对所述待注册数字签名解密；

存储模块，用于如果所述证书签名与所述预设签名一致，且采用所述待注册证书公钥对所述待注册数字签名解密成功，则将所述待注册用户信息和所述待注册数字证书对应存储至所述区块链系统；

第二返回模块，用于如果所述证书签名与所述预设签名不一致，或采用所述待注册证书公钥对所述待注册数字签名解密失败，则生成并返回注册失败响应。

[权利要求 10]

一种基于区块链的数据查询装置，其特征在于，包括：

确定模块，用于当接收到区块链系统的数据查询请求时，确定所述数据查询请求指示的目标电子病历；

生成模块，用于在所述数据查询请求中提取待查询数字证书，基于所述待查询数字证书和所述目标电子病历，生成信息密文；

传输模块，用于将所述信息密文传输至所述区块链系统。

[权利要求 11]

一种终端设备，其特征在于，所述终端设备包括存储器、处理器以及存储在所述存储器中并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执行以下步骤：

接收用户的数据查询请求，在所述数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名；

基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，所述区块链系统中存储有注册用户的用户信息以及数字证书；

如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功，则确定接入所述区块链系统的多个信息系统，将所

述数据查询请求传输至所述多个信息系统；

接收所述多个信息系统在接收到所述数据查询请求后返回的至少一个信息密文，将所述至少一个信息密文返回至所述用户，所述信息密文携带所述用户的在对应的信息系统中存储的电子病历。

[权利要求 12]

根据权利要求11所述的终端设备，其特征在于，所述接收用户的数据查询请求，在所述数据查询请求中提取待查询数据标识、待查询数字证书、待查询个人信息以及待查询请求签名之前，所述处理器执行所述计算机可读指令时还执行以下步骤：

当接收到用户注册请求时，在所述用户注册请求中提取待注册用户信息、待注册数字签名以及待注册数字证书；

在所述待注册数字证书中提取证书签名，将所述证书签名与预设签名进行比对，所述预设签名为证书机构提供的用于验证所述证书签名是否有效的签名；

在所述待注册数字证书中提取待注册证书公钥，采用所述待注册证书公钥对所述待注册数字签名解密；

如果所述证书签名与所述预设签名一致，且采用所述待注册证书公钥对所述待注册数字签名解密成功，则将所述待注册用户信息和所述待注册数字证书对应存储至所述区块链系统；

如果所述证书签名与所述预设签名不一致，或采用所述待注册证书公钥对所述待注册数字签名解密失败，则生成并返回注册失败响应。

[权利要求 13]

根据权利要求11所述的中的终端设备，其特征在于，所述基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，包括：

在所述区块链系统中查询是否存在与所述待查询个人信息一致的个人

信息；
获取所述待查询数字证书的待查询证书公钥，采用所述待查询证书公钥对所述待查询请求签名解密；

相应地，当所述区块链系统中存在与所述待查询个人信息一致的个人

信息，且采用所述待查询证书公钥对所述待查询请求签名解密成功时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功；

当所述区块链系统中不存在与所述待查询个人信息一致的个人信息，或采用所述待查询证书公钥对所述待查询请求签名解密失败时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败。

[权利要求 14] 根据权利要求11所述的终端设备，其特征在于，所述基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证之后，所述处理器执行所述计算机可读指令时还执行以下步骤：

如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败，则生成查询失败响应，将所述查询失败响应传输至所述用户。

[权利要求 15] 一种终端设备，其特征在于，所述终端设备包括存储器、处理器以及存储在所述存储器中并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执行以下步骤：

当接收到区块链系统的数据查询请求时，确定所述数据查询请求指示的目标电子病历；

在所述数据查询请求中提取待查询数字证书，基于所述待查询数字证书和所述目标电子病历，生成信息密文；

将所述信息密文传输至所述区块链系统。

[权利要求 16] 一种计算机非易失性可读存储介质，所述计算机非易失性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：

接收用户的数据查询请求，在所述数据查询请求中提取待查询数字证书、待查询个人信息以及待查询请求签名；

基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及

所述待查询请求签名进行验证，所述区块链系统中存储有注册用户的用户信息以及数字证书；

如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功，则确定接入所述区块链系统的多个信息系统，将所述数据查询请求传输至所述多个信息系统；

接收所述多个信息系统在接收到所述数据查询请求后返回的至少一个信息密文，将所述至少一个信息密文返回至所述用户，所述信息密文携带所述用户的在对应的信息系统中存储的电子病历。

[权利要求 17]

根据权利要求16所述的计算机非易失性可读存储介质，其特征在于，所述接收用户的数据查询请求，在所述数据查询请求中提取待查询数据标识、待查询数字证书、待查询个人信息以及待查询请求签名之前，所述计算机可读指令被处理器执行时还实现如下步骤：

当接收到用户注册请求时，在所述用户注册请求中提取待注册用户信息、待注册数字签名以及待注册数字证书；

在所述待注册数字证书中提取证书签名，将所述证书签名与预设签名进行比对，所述预设签名为证书机构提供的用于验证所述证书签名是否有效的签名；

在所述待注册数字证书中提取待注册证书公钥，采用所述待注册证书公钥对所述待注册数字签名解密；

如果所述证书签名与所述预设签名一致，且采用所述待注册证书公钥对所述待注册数字签名解密成功，则将所述待注册用户信息和所述待注册数字证书对应存储至所述区块链系统；

如果所述证书签名与所述预设签名不一致，或采用所述待注册证书公钥对所述待注册数字签名解密失败，则生成并返回注册失败响应。

[权利要求 18]

根据权利要求16所述的计算机非易失性可读存储介质，其特征在于，所述基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证，包括：

在所述区块链系统中查询是否存在与所述待查询个人信息一致的个人

信息；

获取所述待查询数字证书的待查询证书公钥，采用所述待查询证书公钥对所述待查询请求签名解密；

相应地，当所述区块链系统中存在与所述待查询个人信息一致的个人信息，且采用所述待查询证书公钥对所述待查询请求签名解密成功时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证成功；

当所述区块链系统中不存在与所述待查询个人信息一致的个人信息，或采用所述待查询证书公钥对所述待查询请求签名解密失败时，确定对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败。

[权利要求 19] 根据权利要求16所述的计算机非易失性可读存储介质，其特征在于，所述基于区块链系统，对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名进行验证之后，所述计算机可读指令被处理器执行时还实现如下步骤：

如果对所述待查询数字证书、所述待查询个人信息以及所述待查询请求签名验证失败，则生成查询失败响应，将所述查询失败响应传输至所述用户。

[权利要求 20] 一种计算机非易失性可读存储介质，所述计算机非易失性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：

当接收到区块链系统的数据查询请求时，确定所述数据查询请求指示的目标电子病历；

在所述数据查询请求中提取待查询数字证书，基于所述待查询数字证书和所述目标电子病历，生成信息密文；

将所述信息密文传输至所述区块链系统。

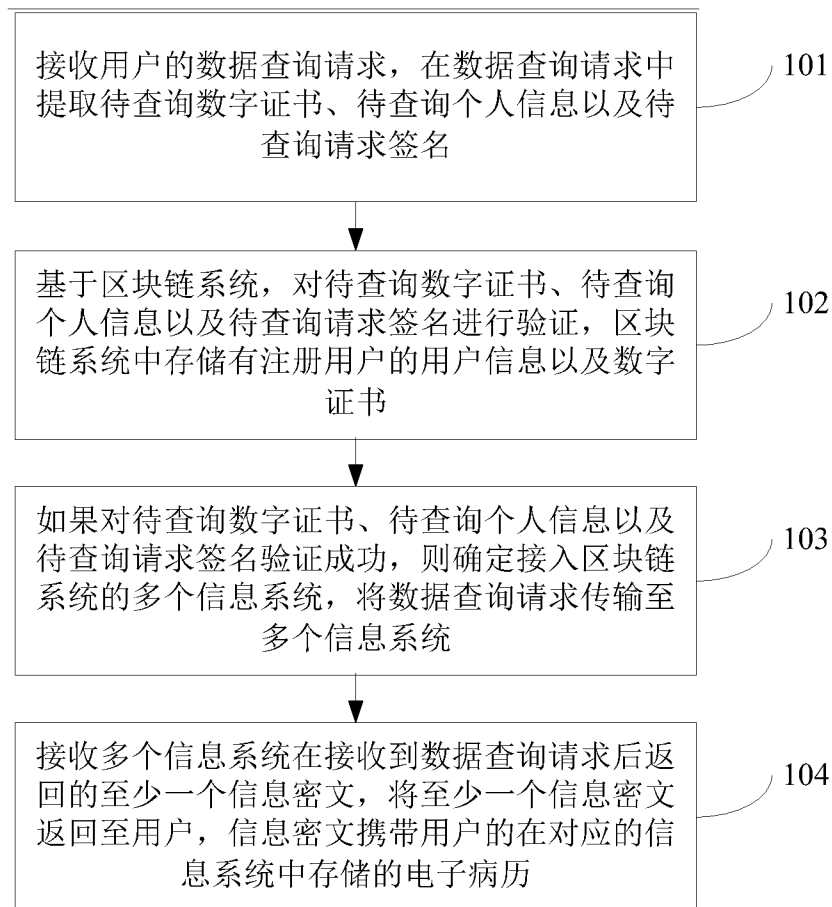


图 1A

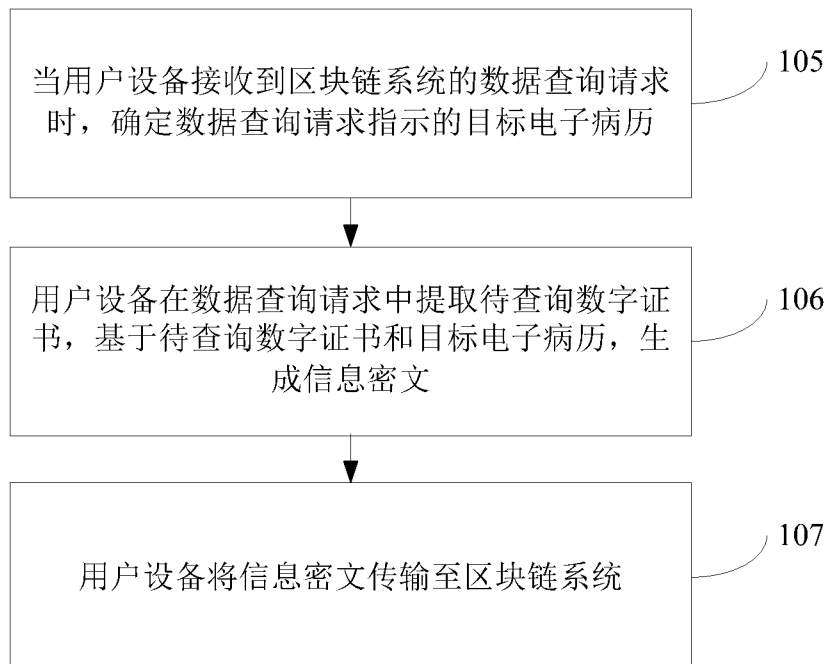


图 1B

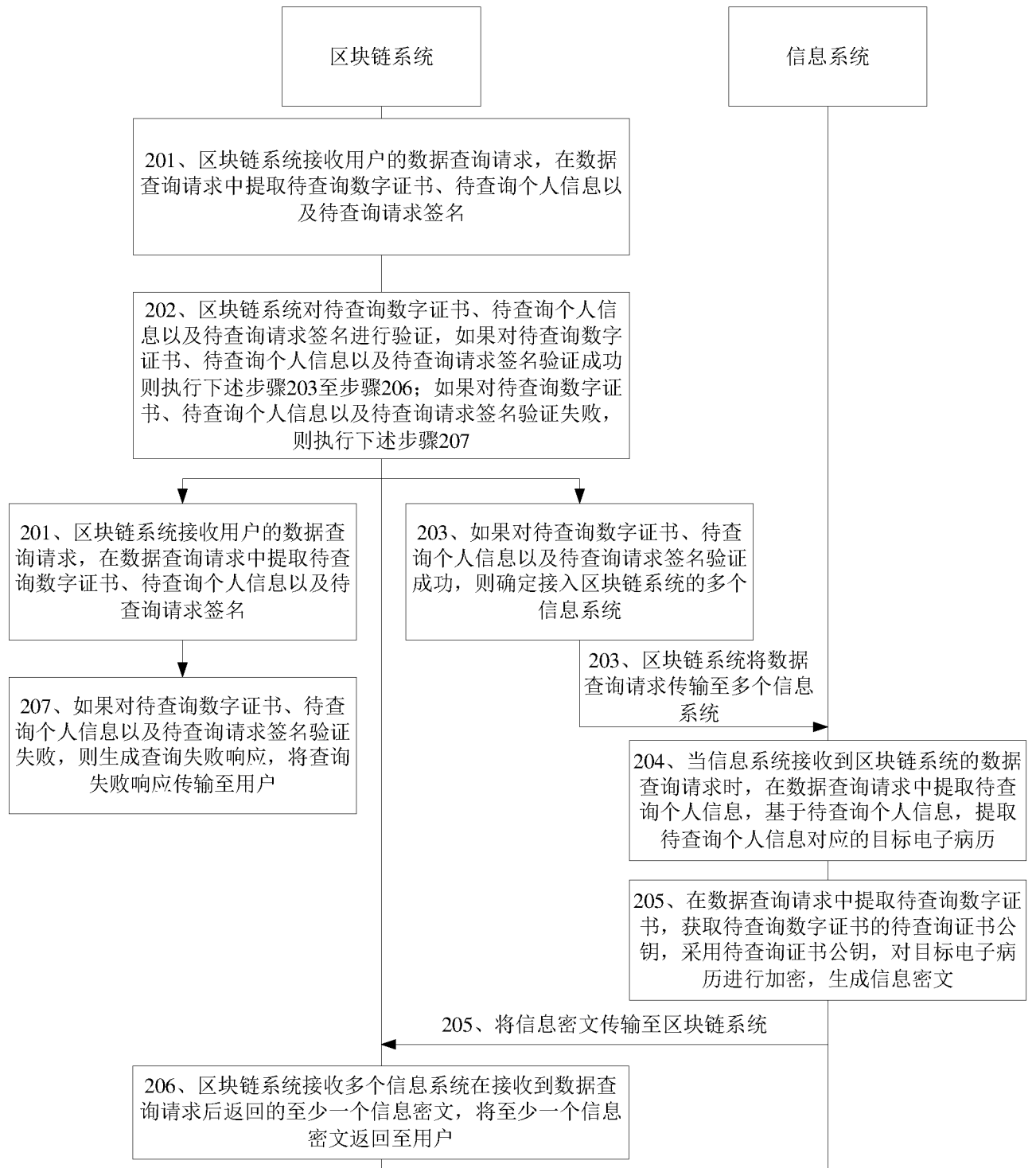


图 2A

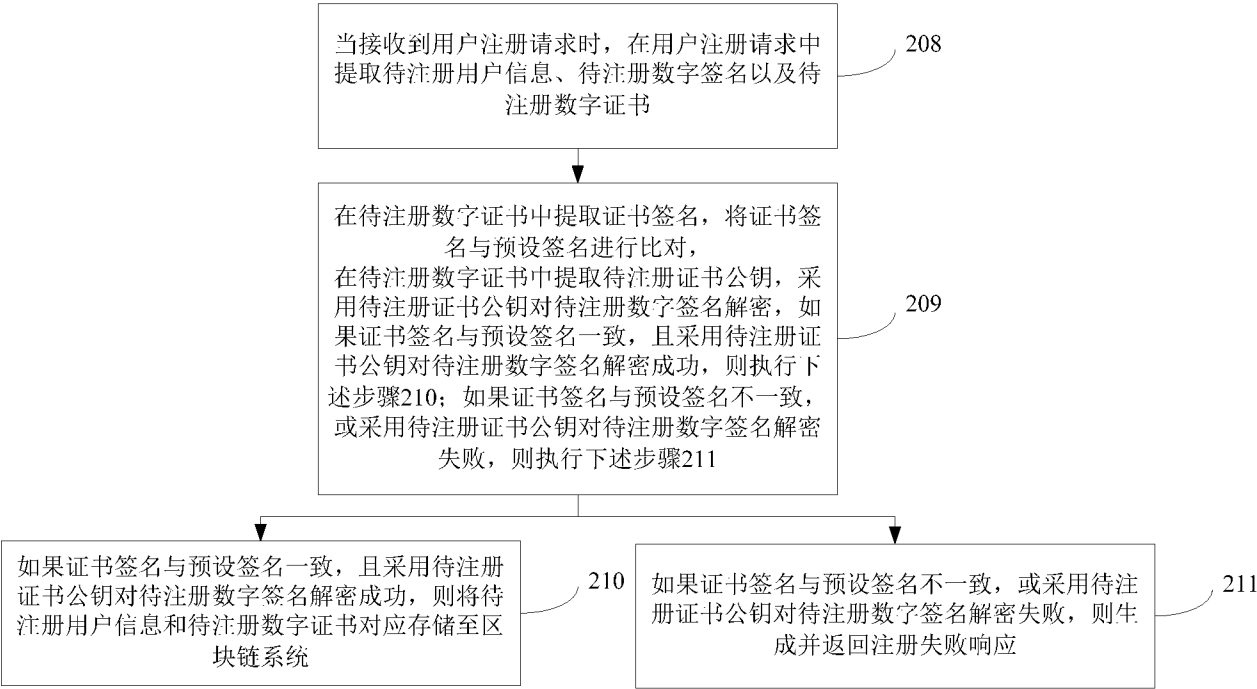


图 2B

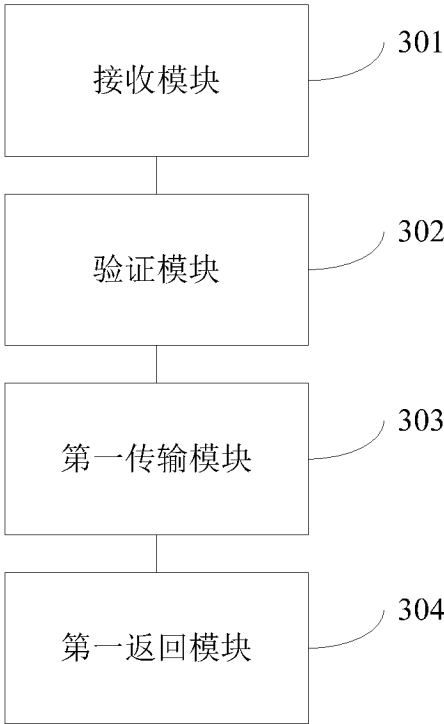


图 3A

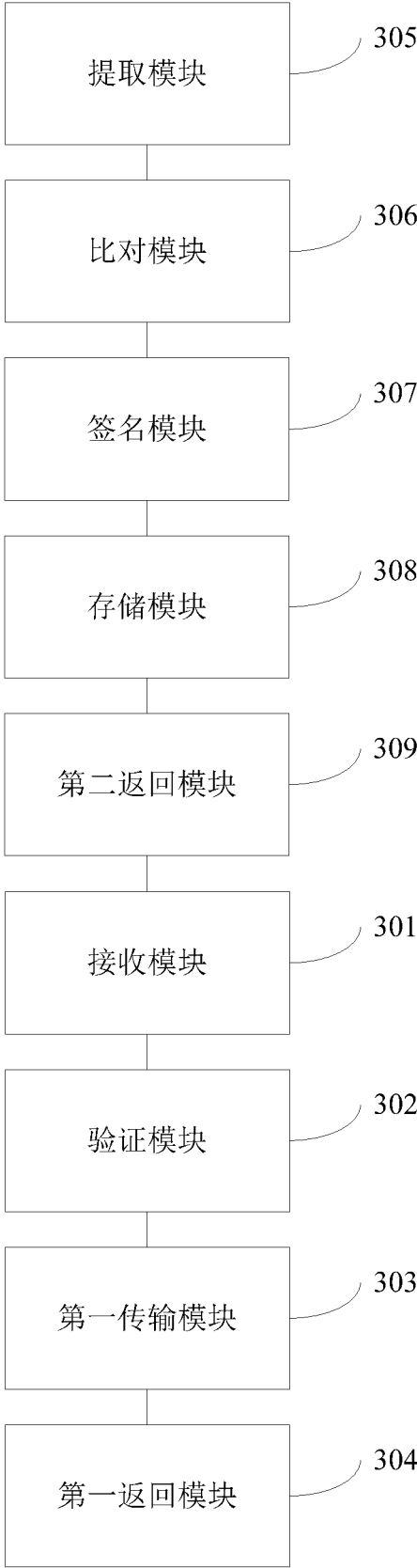


图 3B

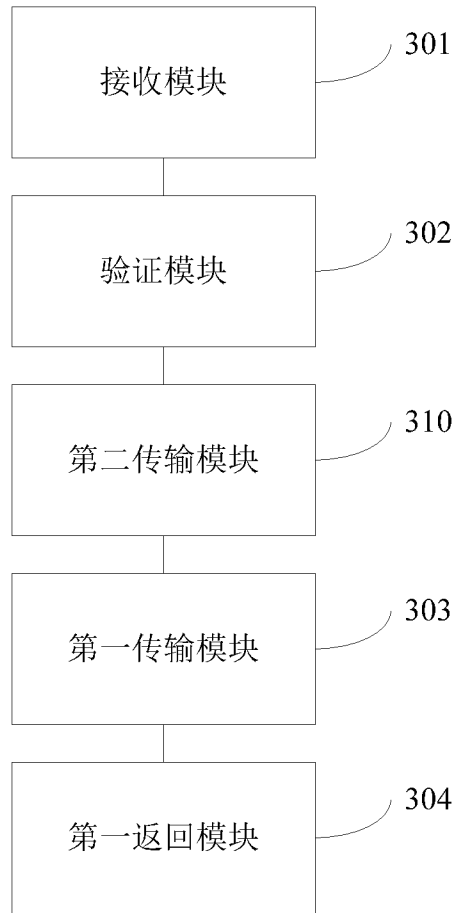


图 3C

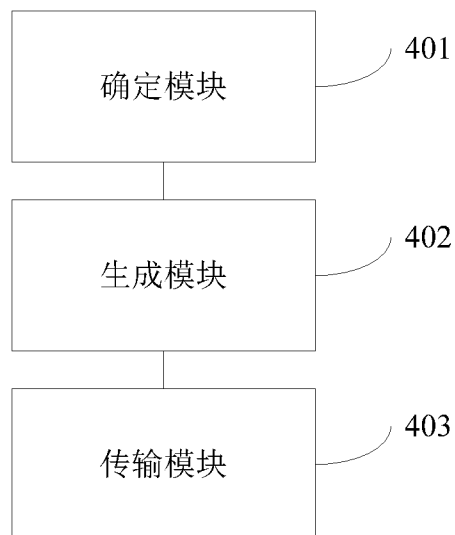


图 4A

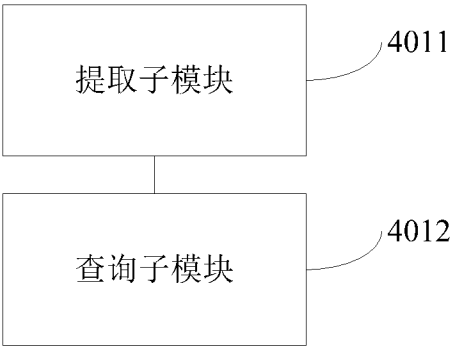


图 4B

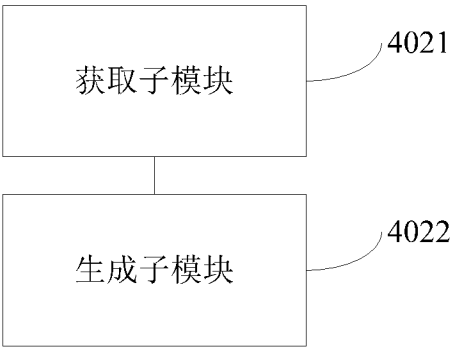


图 4C

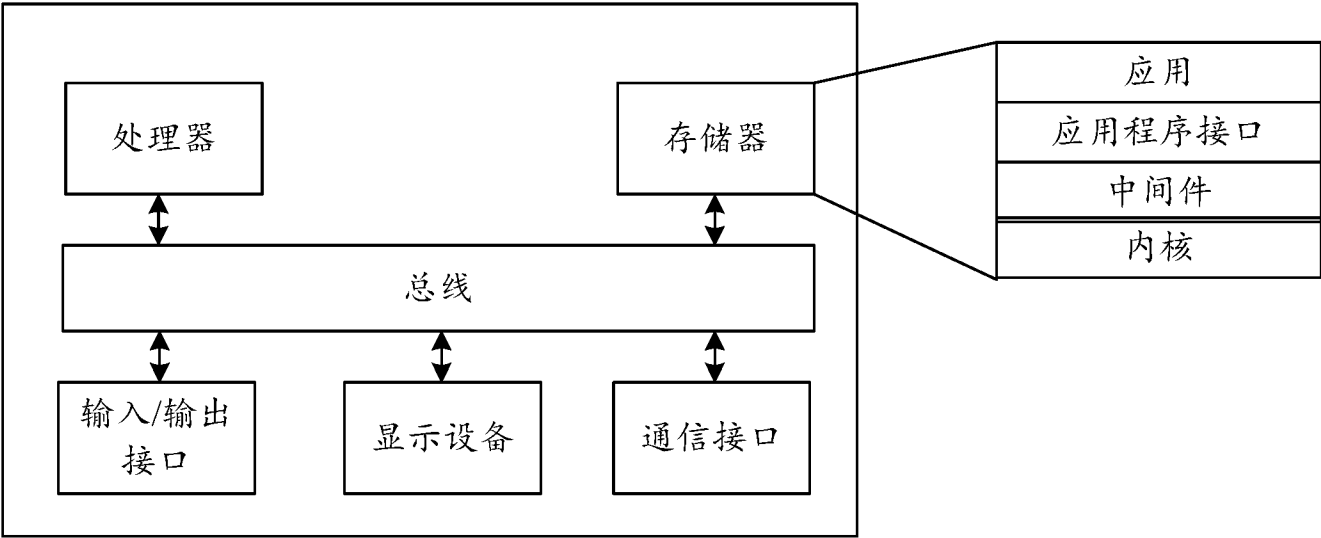


图 5

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/122574

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; G06F; G06Q; H04L

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: 区块链, 医疗, 数据, 病历, 共享, 查询, 验证, 认证, 签名, 证书, 公钥, 加密, 密文, block chain, medical, data, record, share, query, inquiry, verification, certification, certificate, signature, public key, encrypt

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110070926 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 30 July 2019 (2019-07-30) claims 1-10	1-20
Y	CN 107391944 A (TAI CLOUD CORPORATION) 24 November 2017 (2017-11-24) description, paragraphs 0030-0045	1-4, 8, 9, 11-14, 16-19
Y	CN 106682530 A (HANGZHOU DIANZI UNIVERSITY) 17 May 2017 (2017-05-17) description, paragraphs 0019-0026, and claim 1	1-4, 8, 9, 11-14, 16-19
X	CN 106682530 A (HANGZHOU DIANZI UNIVERSITY) 17 May 2017 (2017-05-17) description, paragraphs 0019-0026, and claim 1	5-7, 10, 15, 20
A	CN 107766574 A (TIANJIN HAPPY LIFE TECHNOLOGY CO., LTD.) 06 March 2018 (2018-03-06) entire document	1-20
A	CN 107579979 A (CHENGDU UNIVERSITY OF TECHNOLOGY) 12 January 2018 (2018-01-12) 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

18 February 2020

Date of mailing of the international search report

26 February 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/122574

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2018227119 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 09 August 2018 (2018-08-09) entire document	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2019/122574

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110070926	A	30 July 2019	None	
CN	107391944	A	24 November 2017	None	
CN	106682530	A	17 May 2017	None	
CN	107766574	A	06 March 2018	None	
CN	107579979	A	12 January 2018	None	
US	2018227119	A1	09 August 2018	US 2018227118 A1	09 August 2018

国际检索报告

国际申请号

PCT/CN2019/122574

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; G06F; G06Q; H04L 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, EPDOC: 区块链, 医疗, 数据, 病历, 共享, 查询, 验证, 认证, 签名, 证书, 公钥, 加密, 密文, block chain, medical, data, record, share, query, inquiry, verification, certification, certificate, signature, public key, encrypt		
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 110070926 A (深圳壹账通智能科技有限公司) 2019年 7月 30日 (2019 - 07 - 30) 权利要求1-10	1-20
Y	CN 107391944 A (北京太一云科技有限公司) 2017年 11月 24日 (2017 - 11 - 24) 说明书第0030-0045段	1-4, 8-9, 11-14, 16-19
Y	CN 106682530 A (杭州电子科技大学) 2017年 5月 17日 (2017 - 05 - 17) 说明书第0019-0026段, 权利要求1	1-4, 8-9, 11-14, 16-19
X	CN 106682530 A (杭州电子科技大学) 2017年 5月 17日 (2017 - 05 - 17) 说明书第0019-0026段, 权利要求1	5-7, 10, 15, 20
A	CN 107766574 A (天津开心生活科技有限公司) 2018年 3月 6日 (2018 - 03 - 06) 全文	1-20
A	CN 107579979 A (成都理工大学) 2018年 1月 12日 (2018 - 01 - 12) 全文	1-20
A	US 2018227119 A1 (INTERNATIONAL BUSINESS MACHINES CORPORATION) 2018年 8月 9日 (2018 - 08 - 09) 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 2020年 2月 18日		国际检索报告邮寄日期 2020年 2月 26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 靳晶 电话号码 86-(10)-53961790

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/122574

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	110070926	A	2019年 7月 30日	无	
CN	107391944	A	2017年 11月 24日	无	
CN	106682530	A	2017年 5月 17日	无	
CN	107766574	A	2018年 3月 6日	无	
CN	107579979	A	2018年 1月 12日	无	
US	2018227119	A1	2018年 8月 9日	US 2018227118 A1	2018年 8月 9日