(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 2020/186823 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01)

(21) 国际申请号: PCT/CN2019/122575

(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:
201910218386.6 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, SYSTEM AND APPARATUS, AND STORAGE MEDIUM

(54) **发明名称**: 区块链的数据查询方法、装置、系统、设备及存储介质

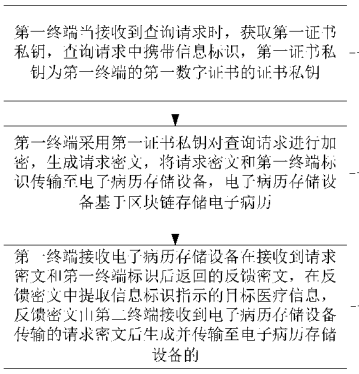

图 1A

101 Upon receiving a query request, a first terminal acquires a first certificate private key, wherein the query request carries an information identifier, and the first certificate private key is a certificate private key of a first digital certificate of the first terminal

102 The first terminal uses the first certificate private key to encrypt the query request and generate a request ciphertext, and transmits the request ciphertext and an identifier of the first terminal to an electronic medical record storage apparatus, wherein the electronic medical record storage apparatus stores electronic medical records on the basis of a blockchain

103 The first terminal receives a feedback ciphertext returned by the electronic medical record storage apparatus after receiving the request ciphertext and the identifier of the first terminal, and extracts, from the feedback ciphertext, target medical information indicated by the information identifier, wherein the feedback ciphertext is generated by a second terminal after receiving the request ciphertext transmitted by the electronic medical record storage apparatus, and then the feedback ciphertext is transmitted to the electronic medical record storage apparatus

(57) **Abstract:** The present invention relates to the technical field of data transmission. Disclosed are a blockchain-based data querying method, device, system and apparatus, and a storage medium capable of preventing a first terminal from freely accessing electronic medical records of users, thereby reducing risks of malicious information spreading, preventing dissemination of information, and enhancing information security. The method comprises: upon receiving a query request, acquiring a first certificate private key, wherein the query request carries an information identifier; using the first certificate private key to encrypt the query request, generating a request ciphertext, and transmitting the request ciphertext and an identifier of a first terminal to an electronic medical record storage apparatus; and receiving a feedback ciphertext returned by the electronic medical record storage apparatus after receiving the request ciphertext and the identifier of the first terminal, and extracting, from the feedback ciphertext, target medical information indicated by the information identifier.

WO 2020/186823 A1

[见续页]

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：本申请公开了一种区块链的数据查询方法、装置、系统、设备及存储介质，涉及数据传输技术领域，可以使第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。所述方法包括：当接收到查询请求时，获取第一证书私钥，查询请求中携带信息标识；采用第一证书私钥对查询请求进行加密，生成请求密文，将请求密文和第一终端标识传输至电子病历存储设备；接收电子病历存储设备在接收到请求密文和第一终端标识后返回的反馈密文，在反馈密文中提取信息标识指示的目标医疗信息。

区块链的数据查询方法、装置、系统、设备及存储介质

[0001] 本申请申明享有2019年03月21日递交的申请号为201910218386.6、名称为“区块链的数据查询方法、装置、系统、设备及存储介质”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] 本申请涉及数据传输技术领域，特别是涉及一种区块链的数据查询方法、装置、系统、设备及存储介质。

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存储及电子病历中数据的传输。

[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，也即将用户的医疗信息与用户的身份信息、联系方式信息等个人信息绑定存储，当医生需要查询某位病人的医疗信息时，直接根据用户的姓名在向信息系统请求数据，信息系统便会将数据传输给医生。

[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] 医生可以随意查看信息系统中存储的个人的医疗信息，很有可能导致信息系统中的医疗信息被恶意传播，造成信息的扩散，信息的安全性较低。

发明概述

技术问题

[0007] 有鉴于此，本申请提供了一种区块链的数据查询方法、装置、系统、设备及存储介质，主要目的在于解决目前医生可以随意查看信息系统中存储的个人的医疗信息，很有可能导致信息系统中的医疗信息被恶意传播，造成信息的扩散，

信息的安全性较低的问题。

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] 当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

[0010] 采用所述第一证书私钥对所述查询请求进行加密，生成请求密文，将所述请求密文和第一终端标识传输至电子病历存储设备，所述电子病历存储设备基于区块链存储电子病历；

[0011] 接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，所述反馈密文由第二终端接收到所述电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的。

发明的有益效果

有益效果

[0012] 在本申请实施例中，与目前医生可以随意查看信息系统中存储的个人的医疗信息的方式相比，本申请第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

对附图的简要说明

附图说明

[0013] 图1A示出了本申请实施例提供的一种区块链的数据查询方法流程示意图；

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

[0015] 图1C示出了本申请实施例提供的一种区块链的数据查询方法流程示意图；

[0016] 图2示出了本申请实施例提供的一种区块链的数据查询方法流程示意图；

[0017] 图3A示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0018] 图3B示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0019] 图4A示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0020] 图4B示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0021] 图5A示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0022] 图5B示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0023] 图5C示出了本申请实施例提供的一种区块链的数据查询装置的结构示意图；

[0024] 图6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区块链的数据查询方法，可以采用第一证书私钥生成请求密文，由电子病历存储设备将请求密文传输给第二终端，使得第二终端基于该请求密文来确定是否将信息展示给第一终端，保证第一终端请求查看信息需要经过第二终端的允许，达到降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高的目的，如图1A所示，该方法包括：

[0026] 101、第一终端当接收到查询请求时，获取第一证书私钥，查询请求中携带信息标识，第一证书私钥为第一终端的第一数字证书的证书私钥。

[0027] 在本申请实施例中，当接收到查询请求时，为了对查询请求进行加密，从而保证查询请求在传输过程中的安全性，第一终端获取第一证书私钥，以便在后续基于该第一证书私钥对查询请求进行加密。

[0028] 102、第一终端采用第一证书私钥对查询请求进行加密，生成请求密文，将请求密文和第一终端标识传输至电子病历存储设备，电子病历存储设备基于区块链存储电子病历。

[0029] 在本申请实施例中，当第一终端获取到第一证书私钥后，便可以采用第一证书私钥对查询请求进行加密，生成加密后的查询请求，也即请求密文，并将该请求密文传输至电子病历存储设备，以便保证请求密文在传输的过程中不会被篡改。

[0030] 103、第一终端接收电子病历存储设备在接收到请求密文和第一终端标识后返

回的反馈密文，在反馈密文中提取信息标识指示的目标医疗信息，反馈密文由第二终端接收到电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的。

[0031] 在本申请实施例中，当第一终端接收到电子病历存储设备在接收到请求密文后返回的反馈密文后，由于反馈密文是第二终端根据第一终端传输的请求密文生成的，因此，可以在反馈密文中提取到信息标识指示的目标医疗信息。

[0032] 本申请实施例提供的方法，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0033] 本申请实施例提供了一种区块链的数据查询方法，可以采用第一证书私钥生成请求密文，由电子病历存储设备将请求密文传输给第二终端，使得第二终端基于该请求密文来确定是否将信息展示给第一终端，保证第一终端请求查看信息需要经过第二终端的允许，达到降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高的目的，如图1B所示，该方法包括：

[0034] 104、电子病历存储设备当接收到第一终端传输的请求密文和第一终端标识时，将请求密文和第一终端标识传输至第二终端，请求密文由第一终端采用第一证书私钥对查询请求进行加密生成，查询请求中携带信息标识，第一证书私钥为第一终端的第一数字证书的证书私钥。

[0035] 在本申请实施例中，当电子病历存储设备当接收到第一终端传输的请求密文时，为了使第二终端可以确定是否可以为第一终端提供其希望查询的信息，电子病历存储设备将请求密文传输至第二终端。

[0036] 105、电子病历存储设备当接收到第二终端返回的信息标识时，查询存储信息标识指示的目标医疗信息的信息密文，将信息密文传输至第二终端。

[0037] 在本申请实施例中，当电子病历存储设备接收到第二终端返回的信息标识时，由于电子病历存储设备中存储有全部用户的电子病历，因此，电子病历存储设备可以根据信息标识查询到信息标识指示的信息密文，并将该信息密文传输至第二终端，以便第二终端决定是否可以将信息标识指示的信息密文传输给第一

终端进行查看。

[0038] 106、电子病历存储设备接收第二终端返回的反馈密文，将反馈密文传输至第一终端，反馈密文由第二终端在接收到信息密文后生成并发送的。

[0039] 在本申请实施例中，电子病历存储设备如果接收到第二终端返回的反馈密文，则表示第二终端允许第一终端是可以查看信息的，因此，电子病历存储设备将第二终端传输的反馈密文传输给第一终端，以便第一终端对该反馈密文进行查看。

[0040] 本申请实施例提供的方法，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0041] 本申请实施例提供了一种区块链的数据查询方法，可以采用第一证书私钥生成请求密文，由电子病历存储设备将请求密文传输给第二终端，使得第二终端基于该请求密文来确定是否将信息展示给第一终端，保证第一终端请求查看信息需要经过第二终端的允许，达到降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高的目的，如图1C所示，该方法包括：

[0042] 107、第二终端当接收到电子病历存储设备传输的请求密文和第一终端标识时，采用第一终端标识指示的第一证书公钥对请求密文解密，请求密文由第一终端生成并传输至电子病历存储设备，第一证书公钥为第一终端的第一数字证书的证书公钥，电子病历存储设备基于区块链存储电子病历。

[0043] 在本申请实施例中，当第二终端接收到电子病历存储设备传输的请求密文时，由于请求密文是采用第一终端的第一证书私钥加密生成的，且证书私钥和证书公钥是可以相互加密解密的，因此，第二终端采用第一证书公钥对请求密文进行解密。

[0044] 108、第二终端如果采用第一证书公钥对请求密文解密成功，则在请求密文中提取信息标识，将信息标识传输至电子病历存储设备。

[0045] 在本申请实施例中，如果第二终端采用第一证书公钥对请求密文解密成功，则表示该请求密文在传输的过程中并没有被篡改，因此，可以在解密后的请求密

文中提取到信息标识。由于用户的电子病历都存储在电子病历存储设备中，因此，为了获取到信息标识指示的信息，第二终端需要将信息标识传输给电子病历存储设备，以便电子病历存储设备按照信息标识给第二终端返回其需要获取的信息。

[0046] 109、第二终端接收电子病历存储设备返回的信息密文，在信息密文中提取信息标识指示的目标医疗信息。

[0047] 在本申请实施例中，当第二终端接收到电子病历存储设备返回的信息标识指示的信息密文后，由于信息密文通常采用第二终端的第二证书公钥加密得到，因此，第二终端可以采用自身的第二证书私钥对信息密文进行解密，从而在信息密文中提取到目标医疗信息。

[0048] 110、第二终端基于第一证书公钥对目标医疗信息进行加密，生成反馈密文，将反馈密文传输至电子病历存储设备。

[0049] 在本申请实施例中，当第二终端获取到目标医疗信息后，为了保证目标医疗信息在传输过程中的安全性，且该目标医疗信息仅能由第一终端查看，因此，第二终端基于第一证书公钥对目标医疗信息加密，生成反馈密文，并将该反馈密文传输至电子病历存储设备，由电子病历存储设备将反馈密文传输至第一终端，使得第一终端采用自身的第一证书私钥便可以对反馈密文进行解密，从而读取到反馈密文中的目标医疗信息。

[0050] 本申请实施例提供的方法，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0051] 本申请实施例提供了一种基于区块链的数据传输方法，可以采用第一证书私钥生成请求密文，由电子病历存储设备将请求密文传输给第二终端，使得第二终端基于该请求密文来确定是否将信息展示给第一终端，保证第一终端请求查看信息需要经过第二终端的允许，达到降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高的目的，如图2所示，该方法应用于第一终端、电子病历存储设备以及第二终端，涉及到第一终端、电子病历存储设备以及第二终

端之间的交互，该方法包括：

[0052] 201、当第一终端接收到查询请求时，获取第一证书私钥，采用第一证书私钥对查询请求进行加密，生成请求密文，将请求密文和第一终端标识传输至电子病历存储设备。

[0053] 在本申请实施例中，申请人认识到，电子病历存储设备中接入有大量的终端，其中不乏医院的终端以及用户所持的终端。而通常来说，用户的电子病历都是存储在电子病历存储设备中的，为了保证电子病历存储设备中存储的电子病历的安全性以及公正性，电子病历存储设备通常采用区块链技术存储用户的电子病历。区块链技术具有去中心化的特性，这个特性使得存储在电子病历存储系统中的信息都是公开且透明的，为了避免医院随意在电子病历存储系统中获取用户电子病历中的信息而导致电子病历存储系统中的信息泄露，本申请实施例在进行信息的访问时，需要医院向用户请求查看信息，并由用户通过电子病历存储系统，将医院想要查看的信息进行分享。在本申请实施例中，以医院的终端为第一终端，用户的终端为第二终端为例进行说明，而在实际应用的过程中，电子病历存储系统中还可以接入大量其他的终端，本申请实施例对电子病历存储系统中接入的终端数量不进行具体限定。

[0054] 其中，为了满足医院与用户之间的信息传输需求，电子病历存储系统可以为第一终端与第二终端提供客户端，并基于该客户端为第一终端与第二终端提供信息传输的服务。客户端可提供信息传输入口，当检测到第一终端中有用户触发该信息传输入口时，确定接收到第一终端的查询请求时，为了使第二终端在接收到查询请求时可以确定第一终端请求查看哪种信息，查询请求中需要携带信息标识，具体地，信息标识可为用户的用户姓名、用户账号、用户身份证号码等。

[0055] 考虑到查询请求在传输的过程中可能会被不法分子篡改，第一终端在接收到查询请求后，需要对查询请求进行加密，并将加密后的查询请求进行传输。其中，由于接入电子病历存储设备中的每一个终端均配置有唯一且固定的数字证书，数字证书中包括证书公钥和证书私钥，证书公钥是公开给所有人的，证书私钥是终端自己持有的，且证书公钥和证书私钥具有相互加密和解密的特性，因

此，第一终端在对查询请求进行加密时，由于自身的证书公钥（也即第一证书公钥）是对外公开的，因此，可以采用自身的证书私钥（也即第一证书私钥）对查询请求进行加密，生成请求密文，并将请求密文传输给电子病历存储系统，以便基于该请求密文来实现向第二终端请求进行信息查询的操作。其中，为了对多个终端的多个数字证书进行区分，可以将每个终端的数字证书与该终端的终端标识对应存储，以便在查询数字证书时，可以基于终端标识进行查询。

[0056] 在实际应用的过程中，为了使第二终端在接收到电子病历存储设备传输的请求密文时，可以获知是哪一种终端请求查询信息，第一终端在向电子病历存储设备传输请求密文时，可以提取该自身的终端名称或者终端编号，将终端名称或者终端编号作为第一终端标识，并将第一终端标识也随着请求密文传输给第二终端，以使第二终端还可以根据第一终端的身份来确定是否可以向第一终端传输信息。

[0057] 202、当电子病历存储设备接收到第一终端传输的请求密文和第一终端标识时，将请求密文和第一终端标识传输至第二终端。

[0058] 在本申请实施例中，当电子病历存储设备接收到第一终端传输的请求密文和第一终端标识时，由于只有用户才可以授权医生是否可以查询自己的电子病历，因此，电子病历存储设备将接收到的第一终端传输的请求密文和第一终端标识传输至第二终端，以便第二终端确定是否向第一终端传输其想要查询的信息。

[0059] 203、当第二终端接收到电子病历存储设备传输的请求密文和第一终端标识时，采用第一终端标识指示的第一证书公钥对请求密文进行解密，如果采用第一证书公钥对请求密文解密失败，则执行下述步骤204至步骤206；如果采用第一证书公钥对请求密文解密成功，则执行下述步骤207至步骤211。

[0060] 在本申请实施例中，当第二终端接收到电子病历存储设备传输的请求密文时，由于请求密文是由第一终端基于自身的第一数字证书的第一证书私钥签名生成的，因此，只要第二终端采用第一证书公钥可以对请求密文进行解密，则表示该请求密文在传输的过程中并没有被篡改，第二终端是可以对该请求密文进行信任的，这样，如果第二终端采用第一证书公钥对请求密文解密失败，则表示该请求密文在传输的过程中很可能被篡改，或者该请求密文不是由第一终端发

送的，可能是其他的恶意节点伪造的，也即执行下述步骤204至步骤206。如果第二终端采用第一证书公钥对请求密文解密成功，则表示该请求密文在传输的过程中并没有被篡改，该请求密文包括的内容是真实的，且该请求密文确定由第一终端生成并发送的，也即执行下述步骤207至步骤211。

[0061] 其中，由于电子病历存储设备在传输请求密文时，携带了第一终端标识，因此，第二终端可以通过第一终端标识查询到第一终端的第一数字证书，并在第一数字证书中获取到第一证书公钥，基于第一证书公钥实现对请求密文的解密。具体地，第二终端根据第一终端标识获取第一证书公钥的过程与上述步骤201中第一终端获取第二证书公钥的过程一致，此处不再进行赘述。

[0062] 需要说明的是，如果电子病历存储设备在传输请求密文时还携带了第一终端的第一终端标识，则第二终端在接收到第一终端的第一终端标识后，还可以将该第一终端标识展示给第二终端的用户，若第二终端的用户不允许将信息传输给第一终端，也即第二终端的用户不希望授权第一终端查看信息，则第二终端可以直接执行下述步骤204至步骤206，而无需再对请求密文进行解密。

[0063] 204、如果采用第一证书公钥对请求密文解密失败，则第二终端生成失败响应，并将失败响应传输至电子病历存储设备。

[0064] 在本申请实施例中，如果第二终端采用第一证书公钥对请求密文解密失败，则表示请求密文在传输的过程中可能被篡改，或者该请求密文不是由第一终端发送的，可能是其他的恶意节点伪造的，因此，生成失败响应，并将该失败响应传输给电子病历存储设备，以便电子病历存储将该失败响应输给第一终端，使第一终端在获取到该失败响应后，可以重新发送请求密文。

[0065] 205、电子病历存储设备接收第二终端传输的失败响应，将失败响应传输至第一终端。

[0066] 在本申请实施例中，当电子病历存储设备接收到第二终端传输的失败响应时，为了使第一终端可以基于该失败响应确定传输的请求密文没有被第二终端认可，以便第一终端可以重新发送请求密文，电子病历存储设备将接收到的失败响应传输给第一终端。

[0067] 206、第一终端接收电子病历存储设备传输的失败响应，重新执行上述生成请

求密文，并将请求密文传输至电子病历存储设备的过程。

[0068] 在本申请实施例中，当第一终端接收到电子病历存储设备传输的失败响应后，便可以确定之前发送的请求密文并没有被第二终端所认可，这样，第一终端便需要重新执行上述步骤201，重新生成新的请求密文，并将生成的新的请求密文再次传输给电子病历存储设备进行传输。其中，生成请求密文并进行传输的过程与上述步骤201中所示的过程一致，此处不再进行赘述。

[0069] 207、如果第二终端采用第一证书公钥对请求密文解密成功，则在请求密文中提取信息标识，将信息标识传输至电子病历存储设备。

[0070] 在本申请实施例中，如果第二终端采用第一证书公钥对请求密文解密成功，则表示请求密文是真实的，并没有在传输的过程中进行篡改，因此，可以基于该请求密文为第一终端传输信息。其中，由于第二终端已经对该请求密文进行解密成功，因此，第二终端可以在解密成功的请求密文中提取到信息标识，并根据信息标识来确定第一终端请求查询的信息。

[0071] 在实际应用的过程中，由于个人的医疗信息均存储在电子病历存储设备中，因此，为了获取到第一终端请求查询的信息，第二终端将获取到的信息标识传输给电子病历存储设备，以便电子病历存储设备根据信息标识确定目标医疗信息，并将目标医疗信息返回给第二终端，由第二终端决定是否将目标医疗信息传输给第一终端。

[0072] 208、电子病历存储设备接收第二终端返回的信息标识，提取信息标识指示的信息密文，将信息密文传输至第二终端。

[0073] 在本申请实施例中，当电子病历存储设备接收到第二终端返回的信息标识后，便可以按照信息标识，提取到第二终端请求的信息，并将获取到的信息传输给第二终端。其中，由于电子病历存储设备在存储每个用户的电子病历时都会采用用户的证书公钥对电子病历进行加密，并将加密后的电子病历进行存储，也即存储包括电子病历的信息密文，因此，电子病历存储设备仅能根据信息标识获取到信息密文，这样，电子病历存储设备仅需将获取到的信息密文传输给第二终端即可。

[0074] 在实际应用的过程中，由于电子病历存储设备是采用区块链技术进行信息存储

的，因此，在获取信息密文时，电子病历存储设备可以首先根据信息标识确定信息密文所在的目标区块，并获取到该目标区块；随后，在该目标区块中提取信息标识指示的信息密文，将该信息密文传输给第二终端。

[0075] 209、第二终端接收电子病历存储设备返回的信息密文，在信息密文中提取信息标识指示的目标医疗信息，基于第一证书公钥对目标医疗信息进行加密，生成反馈密文，将反馈密文传输至电子病历存储设备。

[0076] 在本申请实施例中，当第二终端接收到电子病历存储设备返回的信息密文后，由于该信息密文是加密的，且通常是采用第二终端的第二数字证书的第二证书公钥加密得到的，因此，只有第二终端才可以对该信息密文进行解密，从而获取到该信息密文中信息标识指示的目标医疗信息。具体地，首先，第二终端接收电子病历存储设备返回的信息标识指示的信息密文，并获取自身所存储的第二证书私钥；随后，采用第二证书私钥对信息密文进行解密，在信息密文中提取目标医疗信息。这样，第二终端在接收到信息密文后，采用第二证书私钥对该信息密文进行解密，从而在信息密文中提取到目标医疗信息。

[0077] 进一步地，为了保证目标医疗信息在传输至第一终端的过程中不会被不法分子篡改或者窃取，第二终端基于第一证书公钥对目标医疗信息进行加密，生成包括目标医疗信息的反馈密文，并将该反馈密文传输给电子病历存储设备，以便电子病历存储设备将该反馈密文传输给第一终端，实现第一终端请求的信息查询。

[0078] 210、电子病历存储设备接收第二终端返回的反馈密文，将反馈密文传输至第一终端。

[0079] 在本申请实施例中，当电子病历存储设备接收到第二终端返回的反馈密文后，便可以将该反馈密文传输给第一终端，以便第一终端在反馈密文中获取到目标医疗信息。

[0080] 211、第一终端接收电子病历存储设备在接收到请求密文后返回的反馈密文，获取第一证书私钥，采用第一证书私钥，对反馈密文进行解密，在反馈密文中提取到信息标识指示的目标医疗信息。

[0081] 在本申请实施例中，当第一终端接收到电子病历存储设备返回的反馈密文后，

由于反馈密文是采用第一终端的第一证书公钥加密得到的，因此，第一终端可以获取第一证书私钥，并采用该第一证书私钥对反馈密文进行解密，在解密后的反馈密文中提取到信息标识指示的目标医疗信息。

[0082] 本申请实施例提供的方法，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0083] 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区块链的数据查询装置，如图3A所示，所述装置包括：获取模块301，加密模块302和提取模块303。

[0084] 该获取模块301，用于当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

[0085] 该加密模块302，用于采用第一证书私钥对查询请求进行加密，生成请求密文，将请求密文和第一终端标识传输至电子病历存储设备，电子病历存储设备基于区块链存储电子病历；

[0086] 该提取模块303，用于接收电子病历存储设备在接收到请求密文和第一终端标识后返回的反馈密文，在反馈密文中提取信息标识指示的目标医疗信息，反馈密文由第二终端接收到电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的。

[0087] 在具体的应用场景中，如图3B所示，该提取模块303，包括接收单元3031和解密单元3032。

[0088] 该接收单元3031，用于接收电子病历存储设备在接收到请求密文后返回的反馈密文，获取第一证书私钥；

[0089] 该解密单元3032，用于采用第一证书私钥，对反馈密文进行解密，在反馈密文中提取到信息标识指示的目标医疗信息。

[0090] 在具体的应用场景中，该获取模块301，还用于如果接收到电子病历存储设备返回的失败响应，则重新执行上述生成请求密文，并将请求密文传输至电子病

历存储设备的过程。

[0091] 本申请实施例提供的装置，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0092] 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区块链的数据查询装置，如图4A所示，所述装置包括：第一传输模块401，提取模块402和第二传输模块403。

[0093] 该第一传输模块401，用于当接收到第一终端传输的请求密文和第一终端标识时，将请求密文和第一终端标识传输至第二终端，请求密文由第一终端采用第一证书私钥对查询请求进行加密生成，查询请求中携带信息标识，第一证书私钥为第一终端的第一数字证书的证书私钥；

[0094] 该提取模块402，用于当接收到第二终端返回的信息标识时，查询存储信息标识指示的目标医疗信息的信息密文，将信息密文传输至第二终端；

[0095] 该第二传输模块403，用于接收第二终端返回的反馈密文，将反馈密文传输至第一终端，反馈密文由第二终端在接收到信息密文后生成并发送的。

[0096] 在具体的应用场景中，如图4B所示，该装置还包括第三传输模块404。

[0097] 该第三传输模块404，用于如果接收到第二终端返回的失败响应，则将失败响应传输至第一终端。

[0098] 本申请实施例提供的装置，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0099] 进一步地，作为图1C所述方法的具体实现，本申请实施例提供了一种区块链的数据查询装置，如图5A所示，所述装置包括：解密模块501，提取模块502，接收模块503和加密模块504。

[0100] 该解密模块501，用于当接收到电子病历存储设备传输的请求密文和第一终端标识时，采用第一终端标识指示的第一证书公钥对请求密文解密，请求密文由

第一终端生成并传输至电子病历存储设备，第一证书公钥为第一终端的第一数字证书的证书公钥，电子病历存储设备基于区块链存储电子病历；

[0101] 该提取模块502，用于如果采用第一证书公钥对请求密文解密成功，则在请求密文中提取信息标识，将信息标识传输至电子病历存储设备；

[0102] 该接收模块503，用于接收电子病历存储设备返回的信息密文，在信息密文中提取信息标识指示的目标医疗信息；

[0103] 该加密模块504，用于基于第一证书公钥对目标医疗信息进行加密，生成反馈密文，将反馈密文传输至电子病历存储设备。

[0104] 在具体的应用场景中，如图5B所示，该接收模块503，包括获取单元5031和解密单元5032。

[0105] 该获取单元5031，用于接收电子病历存储设备返回的信息标识指示的信息密文，获取第二证书私钥，第二证书私钥为第二终端的第二数字证书的证书私钥；

[0106] 该解密单元5032，用于采用第二证书私钥对信息密文进行解密，在信息密文中提取信息标识指示的目标医疗信息。

[0107] 在具体的应用场景中，如图5C所示，该装置还包括生成模块505。

[0108] 该生成模块505，用于如果采用第一证书公钥对请求密文解密失败，则生成失败响应，并将失败响应传输至电子病历存储设备。

[0109] 本申请实施例提供的装置，第一终端在请求查询信息时，需要生成请求密文，借助电子病历存储设备向第二终端传输请求密文，并在第二终端的允许下才能获取到想要查询的目标医疗信息，使得第一终端不能随意获取用户的电子病历，降低了信息被恶意传播的风险，避免信息的扩散，信息的安全性较高。

[0110] 需要说明的是，本申请实施例提供的一种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1C和图2中的对应描述，在此不再赘述。

[0111] 在示例性实施例中，参见图6，还提供了一种设备，该设备600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区块

链的数据传输方法。

[0112] 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区块链的数据传输方法的步骤。

[0113] 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，或者网络设备等）执行本申请各个实施场景所述的方法。

[0114] 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。

[0115] 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。

[0116] 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。

[0117] 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] 一种区块链的数据查询方法，其特征在于，包括：

当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

采用所述第一证书私钥对所述查询请求进行加密，生成请求密文，将所述请求密文和第一终端标识传输至电子病历存储设备，所述电子病历存储设备基于区块链存储电子病历；

接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，所述反馈密文由第二终端接收到所述电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的。

[权利要求 2] 根据权利要求1所述的方法，其特征在于，所述接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，包括：

接收所述电子病历存储设备在接收到所述请求密文后返回的所述反馈密文，获取所述第一证书私钥；

采用所述第一证书私钥，对所述反馈密文进行解密，在所述反馈密文中提取到所述信息标识指示的目标医疗信息。

[权利要求 3] 根据权利要求1所述的方法，其特征在于，所述方法还包括：

如果接收到所述电子病历存储设备返回的失败响应，则重新执行上述生成请求密文，并将所述请求密文传输至所述电子病历存储设备的过程。

[权利要求 4] 一种区块链的数据查询方法，其特征在于，包括：

当接收到第一终端传输的请求密文和第一终端标识时，将所述请求密文和所述第一终端标识传输至第二终端，所述请求密文由所述第一终端采用第一证书私钥对查询请求进行加密生成，所述查询请求中携带信息标识，所述第一证书私钥为所述第一终端的第一数字证书的证书私钥；

当接收到所述第二终端返回的所述信息标识时，查询存储所述信息标识指示的目标医疗信息的信息密文，将所述信息密文传输至所述第二终端；

接收所述第二终端返回的反馈密文，将所述反馈密文传输至所述第一终端，所述反馈密文由所述第二终端在接收到所述信息密文后生成并发送的。

[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：

如果接收到所述第二终端返回的失败响应，则将所述失败响应传输至所述第一终端。

[权利要求 6] 一种区块链的数据查询方法，其特征在于，包括：

当接收到电子病历存储设备传输的请求密文和第一终端标识时，采用所述第一终端标识指示的第一证书公钥对所述请求密文解密，所述请求密文由第一终端生成并传输至所述电子病历存储设备，所述第一证书公钥为所述第一终端的第一数字证书的证书公钥，所述电子病历存储设备基于区块链存储电子病历；

如果采用所述第一证书公钥对所述请求密文解密成功，则在所述请求密文中提取信息标识，将所述信息标识传输至所述电子病历存储设备；

接收所述电子病历存储设备返回的信息密文，在所述信息密文中提取所述信息标识指示的目标医疗信息；

基于所述第一证书公钥对所述目标医疗信息进行加密，生成反馈密文，将所述反馈密文传输至所述电子病历存储设备。

[权利要求 7] 根据权利要求6所述的方法，其特征在于，所述接收所述电子病历存储设备返回的信息密文，在所述信息密文中提取所述信息标识指示的目标医疗信息，包括：

接收所述电子病历存储设备返回的所述信息密文，获取第二证书私钥，所述第二证书私钥为第二终端的第二数字证书的证书私钥；

采用所述第二证书私钥对所述信息密文进行解密，在所述信息密文中

提取所述信息标识指示的目标医疗信息。

[权利要求 8] 根据权利要求6所述的方法，其特征在于，所述方法还包括：

如果采用所述第一证书公钥对所述请求密文解密失败，则生成失败响应，并将所述失败响应传输至所述电子病历存储设备。

[权利要求 9] 一种区块链的数据查询系统，其特征在于，包括第一终端、电子病历存储设备以及第二终端，其中，所述电子病历存储设备基于区块链存储电子病历，

所述第一终端当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

所述第一终端采用所述第一证书私钥对所述查询请求进行加密，生成请求密文，将所述请求密文和第一终端标识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所述第一终端传输的所述请求密文和第一终端标识时，将所述请求密文和第一终端标识传输至所述第二终端；

所述第二终端当接收到所述电子病历存储设备传输的所述请求密文和第一终端标识时，采用所述第一终端标识指示的第一证书公钥对所述请求密文解密，所述第一证书公钥为所述第一终端的第一数字证书的证书公钥；

所述第二终端如果采用所述第一证书公钥对所述请求密文解密成功，则在所述请求密文中提取信息标识，将所述信息标识传输至所述电子病历存储设备；

所述电子病历存储设备当接收到所述第二终端返回的所述信息标识时，提取所述信息标识指示的信息密文，将所述信息密文传输至所述第二终端；

所述第二终端接收所述电子病历存储设备返回的所述信息标识指示的所述信息密文，在所述信息密文中提取目标医疗信息；

所述第二终端基于所述第一证书公钥对所述目标医疗信息进行加密，生成反馈密文，将所述反馈密文传输至所述电子病历存储设备；

所述电子病历存储设备接收所述第二终端返回的所述反馈密文，将所述反馈密文传输至所述第一终端；

所述第一终端接收所述电子病历存储设备在接收到所述请求密文后返回的所述反馈密文，在所述反馈密文中提取所述信息标识指示的所述目标医疗信息。

[权利要求 10] 一种区块链的数据查询装置，其特征在于，包括：

获取模块，用于当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

加密模块，用于采用所述第一证书私钥对所述查询请求进行加密，生成请求密文，将所述请求密文和第一终端标识传输至电子病历存储设备，所述电子病历存储设备基于区块链存储电子病历；

提取模块，用于接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，所述反馈密文由第二终端接收到所述电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的。

[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：

当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

采用所述第一证书私钥对所述查询请求进行加密，生成请求密文，将所述请求密文和第一终端标识传输至电子病历存储设备，所述电子病历存储设备基于区块链存储电子病历；

接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标

识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，所述反馈密文由第二终端接收到所述电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的。

[权利要求 12] 根据权利要求11所述的终端设备，其特征在于，所述接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，包括：

接收所述电子病历存储设备在接收到所述请求密文后返回的所述反馈密文，获取所述第一证书私钥；

采用所述第一证书私钥，对所述反馈密文进行解密，在所述反馈密文中提取到所述信息标识指示的目标医疗信息。

[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，所述处理器执行所述计算机可读指令时还执行以下步骤：

如果接收到所述电子病历存储设备返回的失败响应，则重新执行上述生成请求密文，并将所述请求密文传输至所述电子病历存储设备的过程。

[权利要求 14] 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：

当接收到第一终端传输的请求密文和第一终端标识时，将所述请求密文和所述第一终端标识传输至第二终端，所述请求密文由所述第一终端采用第一证书私钥对查询请求进行加密生成，所述查询请求中携带信息标识，所述第一证书私钥为所述第一终端的第一数字证书的证书私钥；

当接收到所述第二终端返回的所述信息标识时，查询存储所述信息标识指示的目标医疗信息的信息密文，将所述信息密文传输至所述第二终端；

接收所述第二终端返回的反馈密文，将所述反馈密文传输至所述第一

终端，所述反馈密文由所述第二终端在接收到所述信息密文后生成并发送的。

[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：

当接收到电子病历存储设备传输的请求密文和第一终端标识时，采用所述第一终端标识指示的第一证书公钥对所述请求密文解密，所述请求密文由第一终端生成并传输至所述电子病历存储设备，所述第一证书公钥为所述第一终端的第一数字证书的证书公钥，所述电子病历存储设备基于区块链存储电子病历；

如果采用所述第一证书公钥对所述请求密文解密成功，则在所述请求密文中提取信息标识，将所述信息标识传输至所述电子病历存储设备；

接收所述电子病历存储设备返回的信息密文，在所述信息密文中提取所述信息标识指示的目标医疗信息；

基于所述第一证书公钥对所述目标医疗信息进行加密，生成反馈密文，将所述反馈密文传输至所述电子病历存储设备。

[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：

当接收到查询请求时，获取第一证书私钥，所述查询请求中携带信息标识，所述第一证书私钥为第一终端的第一数字证书的证书私钥；

采用所述第一证书私钥对所述查询请求进行加密，生成请求密文，将所述请求密文和第一终端标识传输至电子病历存储设备，所述电子病历存储设备基于区块链存储电子病历；

接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，所述反馈密文由第二终端接收到所述电子病历存储设备

传输的请求密文后生成并传输至电子病历存储设备的。

[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，所述接收所述电子病历存储设备在接收到所述请求密文和所述第一终端标识后返回的反馈密文，在所述反馈密文中提取所述信息标识指示的目标医疗信息，包括：

接收所述电子病历存储设备在接收到所述请求密文后返回的所述反馈密文，获取所述第一证书私钥；

采用所述第一证书私钥，对所述反馈密文进行解密，在所述反馈密文中提取到所述信息标识指示的目标医疗信息。

[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，所述计算机可读指令被处理器执行时还实现如下步骤：

如果接收到所述电子病历存储设备返回的失败响应，则重新执行上述生成请求密文，并将所述请求密文传输至所述电子病历存储设备的过程。

[权利要求 19] 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：

当接收到第一终端传输的请求密文和第一终端标识时，将所述请求密文和所述第一终端标识传输至第二终端，所述请求密文由所述第一终端采用第一证书私钥对查询请求进行加密生成，所述查询请求中携带信息标识，所述第一证书私钥为所述第一终端的第一数字证书的证书私钥；

当接收到所述第二终端返回的所述信息标识时，查询存储所述信息标识指示的目标医疗信息的信息密文，将所述信息密文传输至所述第二终端；

接收所述第二终端返回的反馈密文，将所述反馈密文传输至所述第一终端，所述反馈密文由所述第二终端在接收到所述信息密文后生成并发送的。

[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：

当接收到电子病历存储设备传输的请求密文和第一终端标识时，采用所述第一终端标识指示的第一证书公钥对所述请求密文解密，所述请求密文由第一终端生成并传输至所述电子病历存储设备，所述第一证书公钥为所述第一终端的第一数字证书的证书公钥，所述电子病历存储设备基于区块链存储电子病历；

如果采用所述第一证书公钥对所述请求密文解密成功，则在所述请求密文中提取信息标识，将所述信息标识传输至所述电子病历存储设备；

接收所述电子病历存储设备返回的信息密文，在所述信息密文中提取所述信息标识指示的目标医疗信息；

基于所述第一证书公钥对所述目标医疗信息进行加密，生成反馈密文，将所述反馈密文传输至所述电子病历存储设备。

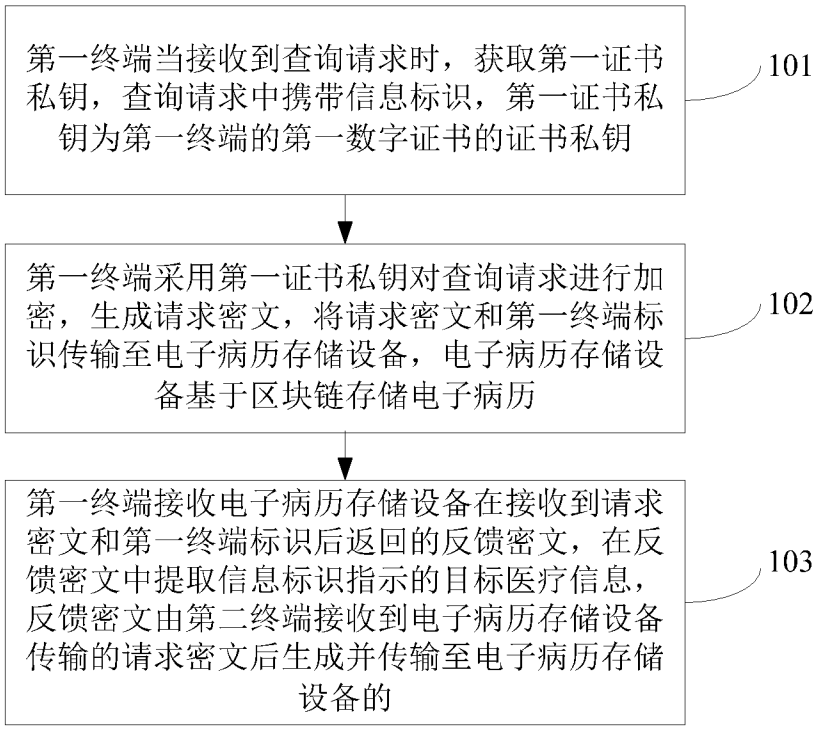
第一终端当接收到查询请求时，获取第一证书私钥，查询请求中携带信息标识，第一证书私钥为第一终端的第一数字证书的证书私钥
101
第一终端采用第一证书私钥对查询请求进行加密，生成请求密文，将请求密文和第一终端标识传输至电子病历存储设备，电子病历存储设备基于区块链存储电子病历
102
第一终端接收电子病历存储设备在接收到请求密文和第一终端标识后返回的反馈密文，在反馈密文中提取信息标识指示的目标医疗信息，反馈密文由第二终端接收到电子病历存储设备传输的请求密文后生成并传输至电子病历存储设备的
103

图 1A

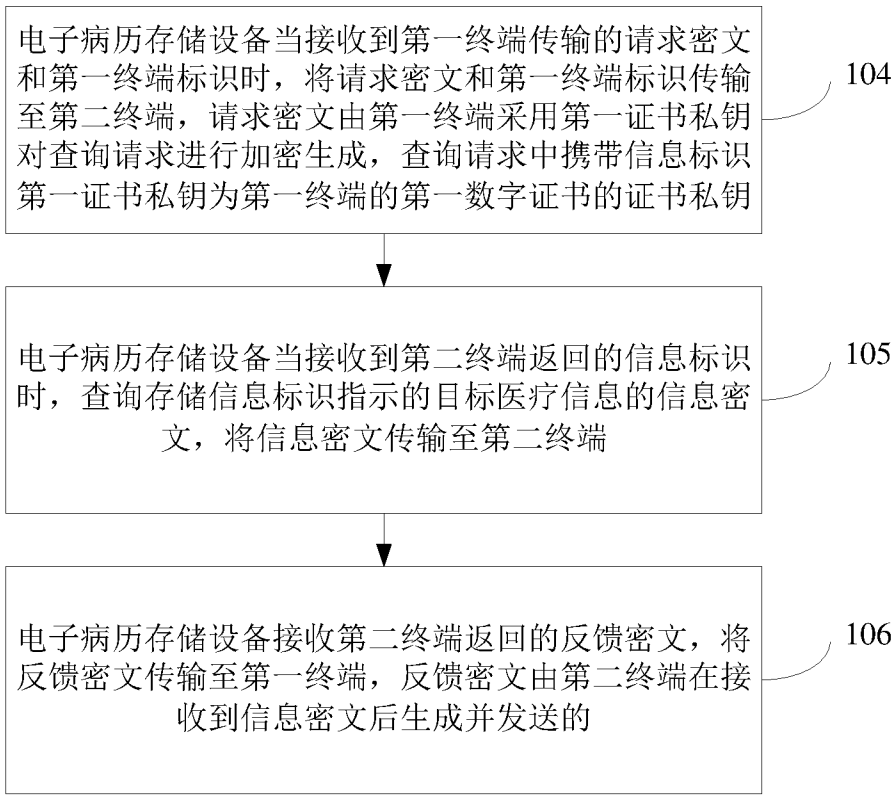
电子病历存储设备当接收到第一终端传输的请求密文和第一终端标识时，将请求密文和第一终端标识传输至第二终端，请求密文由第一终端采用第一证书私钥对查询请求进行加密生成，查询请求中携带信息标识第一证书私钥为第一终端的第一数字证书的证书私钥
104
电子病历存储设备当接收到第二终端返回的信息标识时，查询存储信息标识指示的目标医疗信息的信息密文，将信息密文传输至第二终端
105
电子病历存储设备接收第二终端返回的反馈密文，将反馈密文传输至第一终端，反馈密文由第二终端在接收到信息密文后生成并发送的
106

图 1B

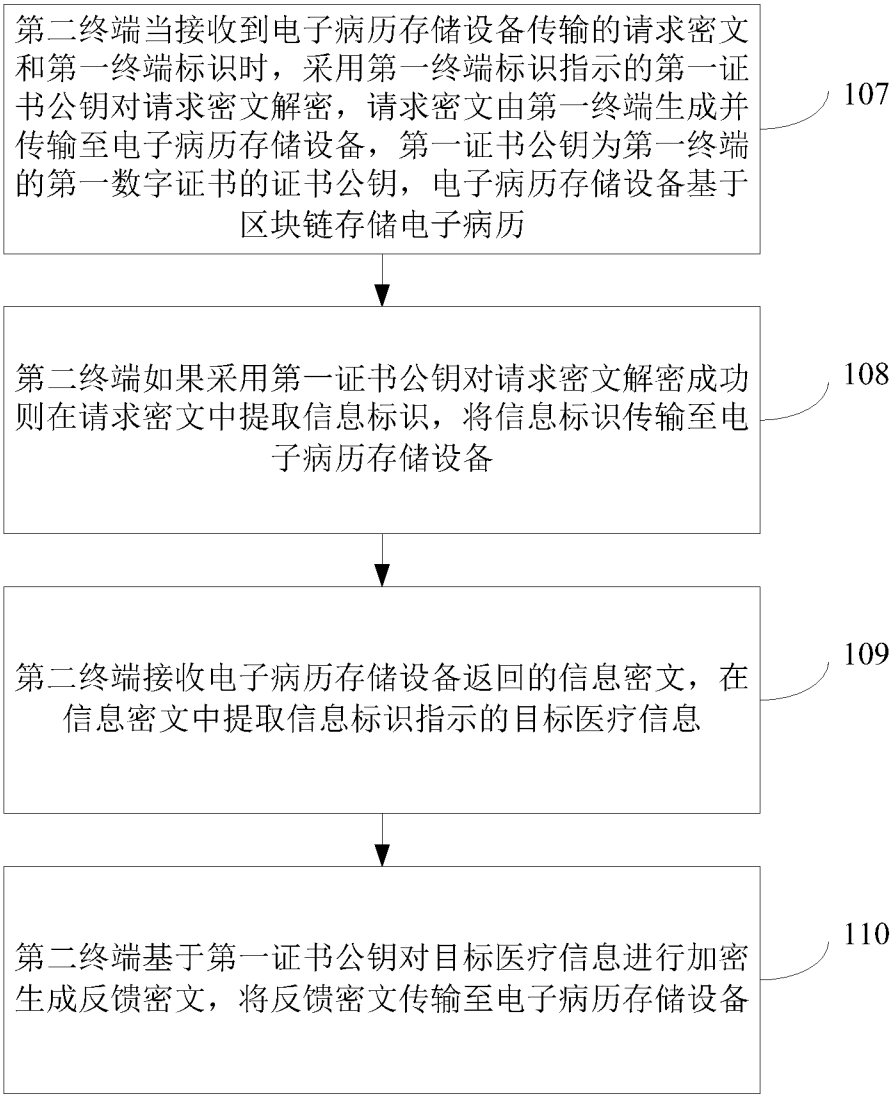
第二终端当接收到电子病历存储设备传输的请求密文和第一终端标识时，采用第一终端标识指示的第一证书公钥对请求密文解密，请求密文由第一终端生成并传输至电子病历存储设备，第一证书公钥为第一终端的第一数字证书的证书公钥，电子病历存储设备基于区块链存储电子病历
107
第二终端如果采用第一证书公钥对请求密文解密成功则在请求密文中提取信息标识，将信息标识传输至电子病历存储设备
108
第二终端接收电子病历存储设备返回的信息密文，在信息密文中提取信息标识指示的目标医疗信息
109
第二终端基于第一证书公钥对目标医疗信息进行加密生成反馈密文，将反馈密文传输至电子病历存储设备
110

图 1C

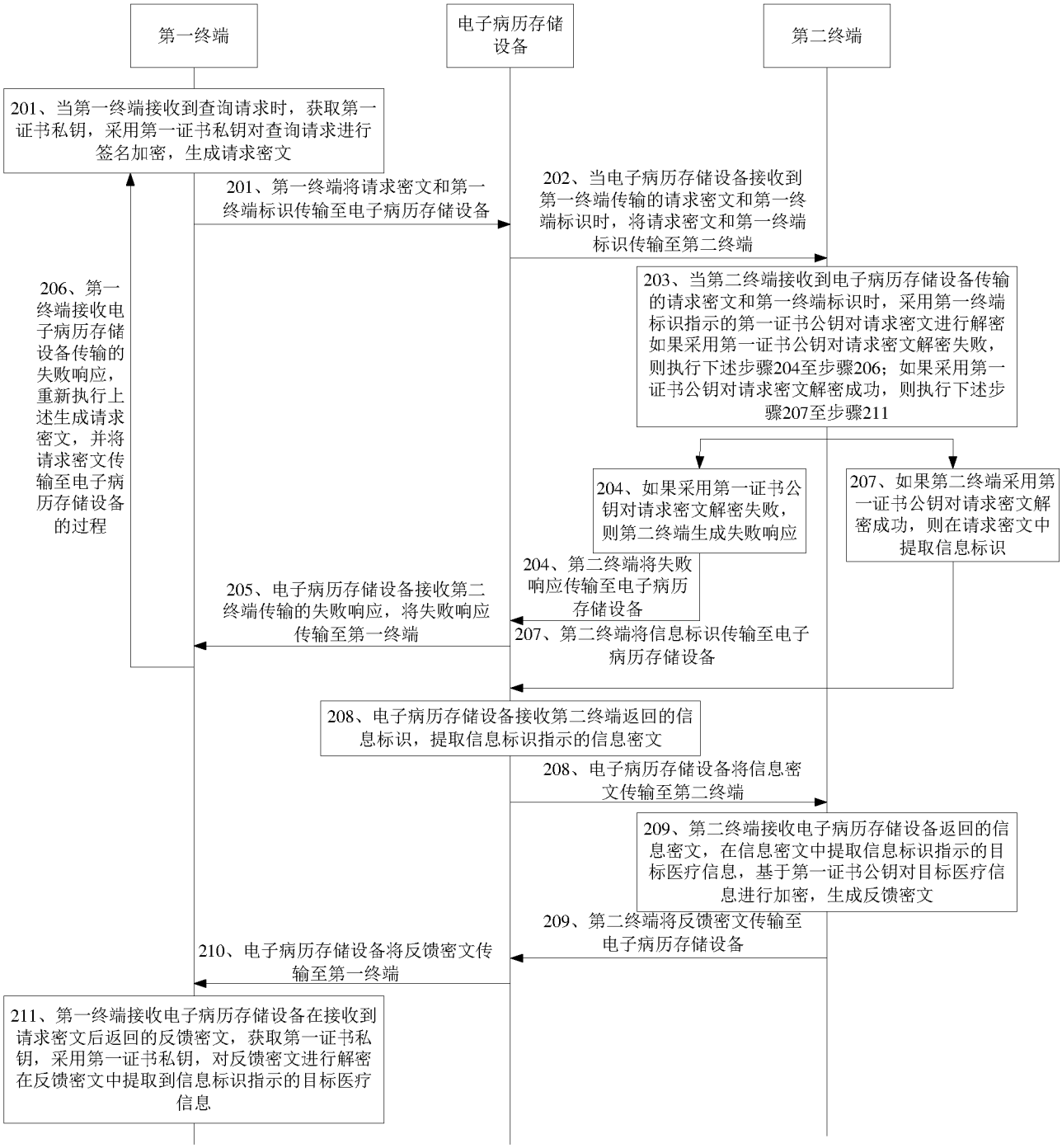
第一终端
电子病历存储设备
第二终端
201、当第一终端接收到查询请求时，获取第一证书私钥，采用第一证书私钥对查询请求进行签名加密，生成请求密文
201、第一终端将请求密文和第一终端标识传输至电子病历存储设备
202、当电子病历存储设备接收到第一终端传输的请求密文和第一终端标识时，将请求密文和第一终端标识传输至第二终端
203、当第二终端接收到电子病历存储设备传输的请求密文和第一终端标识时，采用第一终端标识指示的第一证书公钥对请求密文进行解密如果采用第一证书公钥对请求密文解密失败，则执行下述步骤204至步骤206；如果采用第一证书公钥对请求密文解密成功，则执行下述步骤207至步骤211
206、第一终端接收电子病历存储设备传输的失败响应，重新执行上述生成请求密文，并将请求密文传输至电子病历存储设备的过程
204、如果采用第一证书公钥对请求密文解密失败，则第二终端生成失败响应
207、如果第二终端采用第一证书公钥对请求密文解密成功，则在请求密文中提取信息标识
204、第二终端将失败响应传输至电子病历存储设备
205、电子病历存储设备接收第二终端传输的失败响应，将失败响应传输至第一终端
207、第二终端将信息标识传输至电子病历存储设备
208、电子病历存储设备接收第二终端返回的信息标识，提取信息标识指示的信息密文
208、电子病历存储设备将信息密文传输至第二终端
209、第二终端接收电子病历存储设备返回的信息密文，在信息密文中提取信息标识指示的目标医疗信息，基于第一证书公钥对目标医疗信息进行加密，生成反馈密文
209、第二终端将反馈密文传输至电子病历存储设备
210、电子病历存储设备将反馈密文传输至第一终端
211、第一终端接收电子病历存储设备在接收到请求密文后返回的反馈密文，获取第一证书私钥，采用第一证书私钥，对反馈密文进行解密在反馈密文中提取到信息标识指示的目标医疗信息

图 2

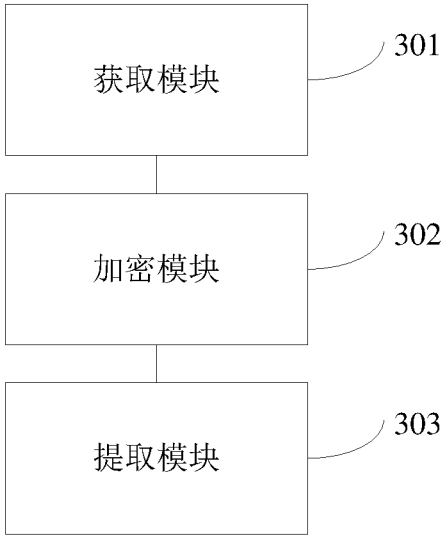
获取模块
301
加密模块
302
提取模块
303

图 3A

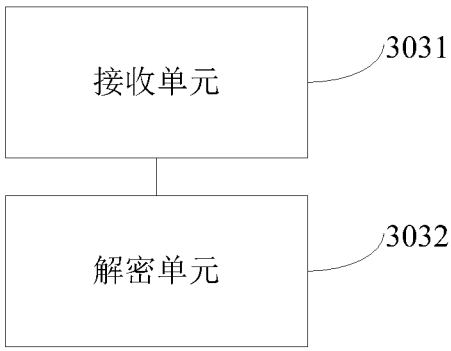
接收单元
3031
解密单元
3032

图 3B

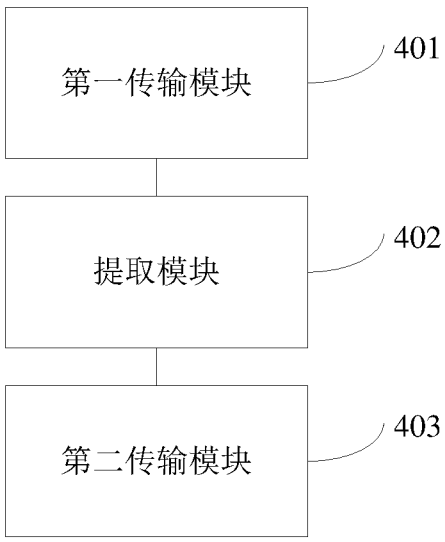
第一传输模块
401
提取模块
402
第二传输模块
403

图 4A

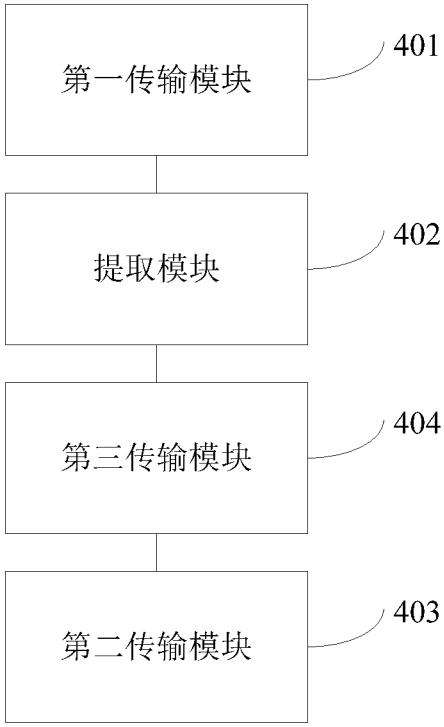
第一传输模块
401
提取模块
402
第三传输模块
404
第二传输模块
403

图 4B

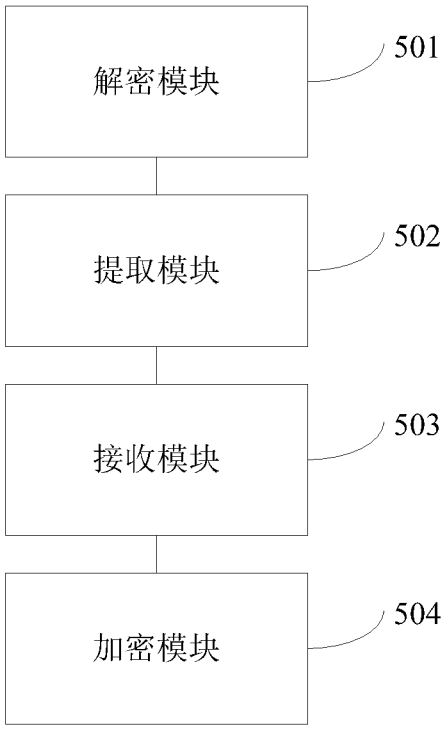
解密模块
501
提取模块
502
接收模块
503
加密模块
504

图 5A

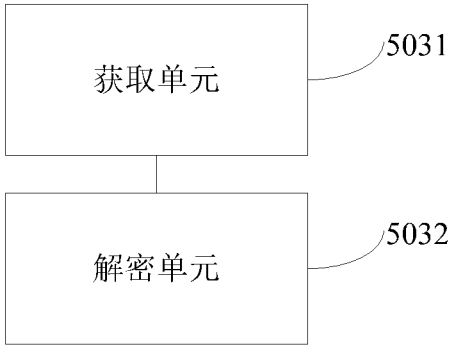
获取单元
5031
解密单元
5032

图 5B

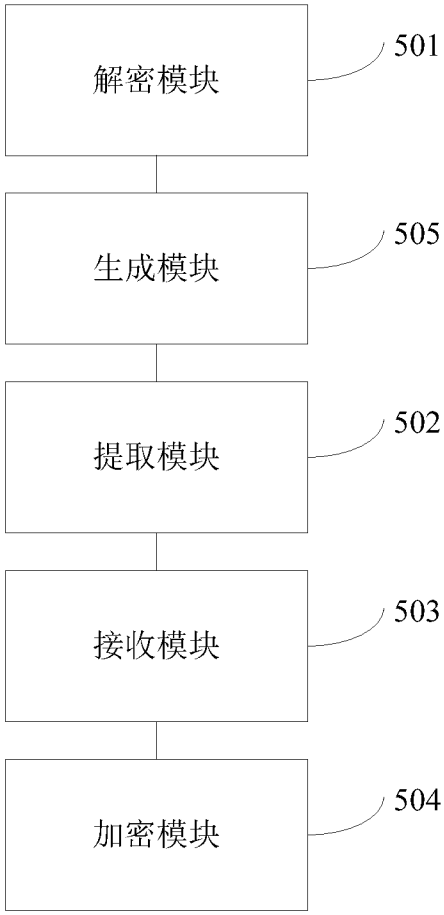
解密模块
501
生成模块
505
提取模块
502
接收模块
503
加密模块
504

图 5C

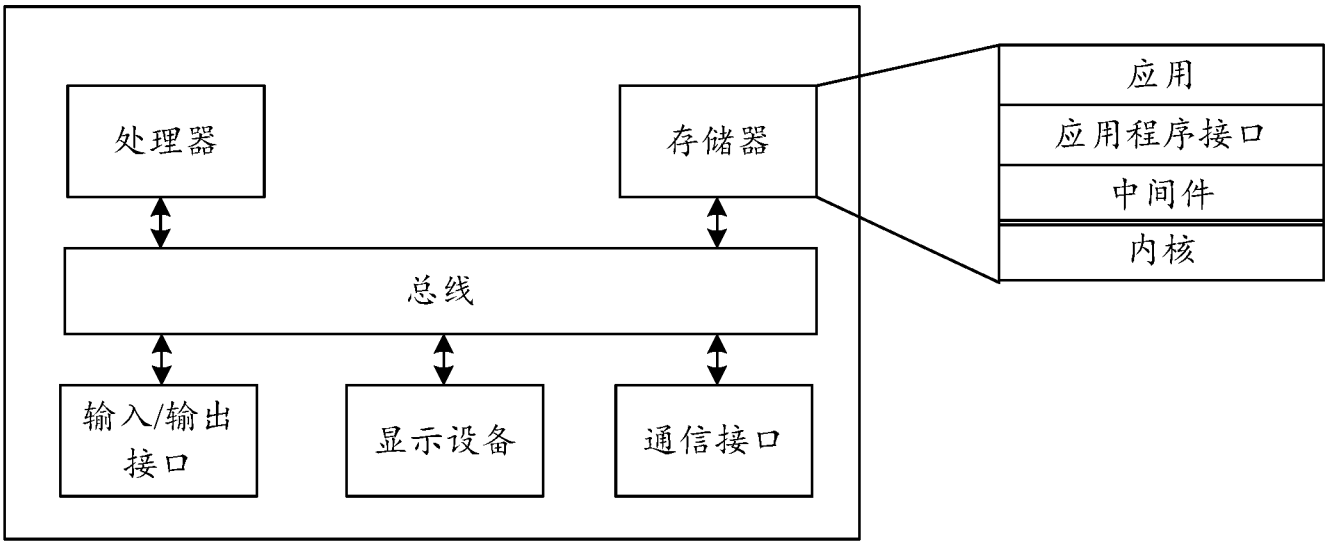

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2019/122575

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(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)

CNABS; VEN; CNTXT; WOTXT; USTXT; EPTXT; CNKI: 电子病历, 区块链, 私钥, 查询, 反馈, 密文, 医疗信息, 标识, medical, record, blockchain, private key, query, ID, feedback, ciphertext, medical information

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110049016 A (ONE CONNECT SMART TECHNOLOGY CO., LTD. (SHENZHEN)) 23 July 2019 (2019-07-23) description, paragraphs [0084]-[0177]	1-20
X	CN 109326337 A (XIDIAN UNIVERSITY) 12 February 2019 (2019-02-12) description, paragraphs [0010]-[0052], and figure 1	1-20
X	CN 108449359 A (JINAN INSPUR HIGH-TECH INVESTMENT DEVELOPMENT CO., LTD.) 24 August 2018 (2018-08-24) description, paragraphs [0006]-[0053]	1-20
A	CN 107579979 A (CHENGDU UNIVERSITY OF TECHNOLOGY) 12 January 2018 (2018-01-12) entire document	1-20
A	US 2018089374 A1 (GIBSON TILLATA CORLETTE) 29 March 2018 (2018-03-29) 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
28 February 2020	**10 March 2020**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration **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/CN2019/122575

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 110049016 A	23 July 2019	None	
CN 109326337 A	12 February 2019	None	
CN 108449359 A	24 August 2018	None	
CN 107579979 A	12 January 2018	None	
US 2018089374 A1	29 March 2018	None	

国际检索报告

国际申请号
PCT/CN2019/122575

A. 主题的分类

H04L 29/06(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））

CNABS;VEN;CNTXT;WOTXT;USTXT;EPTXT;CNKI:电子病历,区块链,私钥,查询,反馈,密文,医疗信息,标识,medical, record,blockchain,private key,query,ID,feedback, ciphertext,medical information

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 110049016 A (深圳壹账通智能科技有限公司) 2019年 7月 23日 (2019-07-23) 说明书第[0084]-[0177]段	1-20
X	CN 109326337 A (西安电子科技大学) 2019年 2月 12日 (2019-02-12) 说明书第[0010]-[0052]段，图1	1-20
X	CN 108449359 A (济南浪潮高新科技投资发展有限公司) 2018年 8月 24日 (2018-08-24) 说明书第[0006]-[0053]段	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 2018089374 A1 (GIBSON TILLATA CORLETTE) 2018年 3月 29日 (2018-03-29) 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 28日	2020年 3月 10日

ISA/CN的名称和邮寄地址	受权官员
中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	徐刚
传真号 (86-10)62019451	电话号码 86-(010)-62411238

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2019/122575

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 110049016 A	2019年 7月 23日	无	
CN 109326337 A	2019年 2月 12日	无	
CN 108449359 A	2018年 8月 24日	无	
CN 107579979 A	2018年 1月 12日	无	
US 2018089374 A1	2018年 3月 29日	无	