

(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 2 月 20 日 (20.02.2020)



(10) 国际公布号
WO 2020/034527 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2018/122636
- (22) 国际申请日: 2018 年 12 月 21 日 (21.12.2018)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201810941440.5 2018 年 8 月 17 日 (17.08.2018) 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: 潘灶烽(PAN, Zhaofeng); 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: 深圳市世纪恒程知识产权代理事务所 (CENFO INTELLECTUAL PROPERTY

AGENCY); 中国广东省深圳市南山区粤海街道高新技术产业园北区松坪山路 3 号奥特讯电力大厦 201, Guangdong 518057 (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, 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,

(54) **Title:** USER PERSONAL INFORMATION ENCRYPTION AND AUTHORISATION METHOD, APPARATUS, AND DEVICE, AND READABLE STORAGE MEDIUM

(54) 发明名称: 用户个人信息加密授权方法、装置、设备及可读存储介质

接收用户上传的用户个人信息, 并确定所述用户个人信息中是否存在待认证信息 S101

↓

若所述用户个人信息中存在待认证信息, 则对所述待认证信息进行认证, 并在认证通过后, 对所述用户个人信息进行加密, 且将加密后的用户个人信息存储至区块链中 S102

↓

当接收到用户终端发送的机构授权请求时, 依据所述机构授权请求, 对所述区块链中的对应用户个人信息进行解密与筛选, 并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端 S103

S101 Receive user personal information uploaded by a user terminal, and determine whether there is information to be authenticated in the user personal information

S102 If there is information to be authenticated in the user personal information, implement authentication of the information to be authenticated and, after authentication passes, encrypt the user personal information and store the encrypted user personal information in a blockchain

S103 When receiving an institution authorisation request sent by the user terminal, on the basis of the institution authorisation request, decrypt and filter the corresponding user personal information in the blockchain, and transmit the filtered user personal information after encryption to the institution terminal corresponding to the institution authorisation request

图 2

(57) **Abstract:** Provided in the present application are a user personal information encryption and authorisation method, apparatus, and device, and a readable storage medium, the method comprising: receiving user personal information uploaded by a user terminal, and determining whether there is information to be authenticated in the user personal information; if there is information to be authenticated in the user personal information, implementing authentication of the information to be authenticated and, after authentication passes, encrypting the user personal information and storing the encrypted user personal information in a blockchain; when receiving an institution authorisation request sent by the user terminal, on the basis of the institution authorisation request, decrypting and filtering the corresponding user personal information in the blockchain, and transmitting the filtered user personal information after encryption to the institution terminal corresponding to the institution authorisation request. The present application can effectively increase the security of user personal information.

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：本申请提供一种用户个人信息加密授权方法、装置、设备及可读存储介质，该方法包括：接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。本申请能够有效的提高用户个人信息的安全性。

用户个人信息加密授权方法、装置、设备及可读存储介质

- [1] 本申请要求于2018年8月17日提交中国专利局、申请号为201810941440.5、发明名称为“用户个人信息加密授权方法、装置、设备及可读存储介质”的中国专利申请优先权，其全部内容通过引用结合在申请中。
- [2] 技术领域
- [3] 本申请涉及互联网的技术领域，尤其涉及一种用户个人信息加密授权方法、装置、设备及可读存储介质。
- [4] 背景技术
- [5] 随着互联网的快速发展，各行各业都采用互联网技术推广、销售和维护产品，即开发APP（Application Program，应用程序），供用户使用，用户使用APP时，需要注册相应的账号，并向服务器上传用户的个人信息，如身份证、手机号码和常驻地址等，金融贷款类APP，还需要需要上传如银行卡号、学历、公司名称、公司职位、所属行业、年龄和婚姻状况等较为重要的用户个人信息。
- [6] 然而，上传的用户个人信息存储在服务器中，用户本身并未对个人信息加密，使得开发APP的公司能够在服务器中查询到用户个人信息，如果开发APP的公司滥用用户个人信息，容易导致用户个人信息的泄露，无法保证用户个人信息的安全性。
- [7] 因此，如何提高用户个人信息的安全性是目前亟待解决的问题。
- [8] 发明内容
- [9] 本申请的主要目的在于提供一种用户个人信息加密授权方法、装置、设备及可读存储介质，旨在提高用户个人信息的安全性。
- [10] 为实现上述目的，本申请提供一种用户个人信息加密授权方法，所述用户个人信息加密授权方法包括以下步骤：
- [11] 接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；

- [12] 若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；
- [13] 当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。
- [14] 此外，为实现上述目的，本申请还提供一种用户个人信息加密授权装置，所述用户个人信息加密授权装置包括：
- [15] 接收确定模块，用于接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；
- [16] 认证加密模块，用于若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；
- [17] 信息授权模块，用于当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。
- [18] 此外，为实现上述目的，本申请还提供一种用户个人信息加密授权设备，所述用户个人信息加密授权设备包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的用户个人信息加密授权可读指令，其中所述用户个人信息加密授权可读指令被所述处理器执行时，实现如上述的用户个人信息加密授权方法的步骤。
- [19] 此外，为实现上述目的，本申请还提供一种可读存储介质，所述可读存储介质上存储有用户个人信息加密授权可读指令，其中所述用户个人信息加密授权可读指令被处理器执行时，实现如上述的用户个人信息加密授权方法的步骤。
- [20] 本申请提供一种用户个人信息加密授权方法、装置、设备及可读存储介质，本申请通过对用户个人信息进行认证，并将通过认证的用户个人信息加密后存储至区块链中，当接收到机构授权请求时，对存储在区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与对应的机构

终端，由于用户个人信息经过认证，有效保证用户个人信息的准确性，且用户个人信息经过加密后存储在区块链中，可以防止他人篡改用户个人信息，且机构需要查询用户个人信息时，需要用户个人信息的拥有者授权给机构，机构才能够查询，有效的提高了用户个人信息的安全性。

[21] 附图说明

[22] 图1为本申请各实施例涉及的用户个人信息加密授权设备的硬件结构示意图；

[23] 图2为本申请用户个人信息加密授权方法第一实施例的流程示意图；

[24] 图3为本申请用户个人信息加密授权方法第二实施例的流程示意图；

[25] 图4为本申请用户个人信息加密授权装置第一实施例的功能模块示意图。

[26] 本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

[27] 具体实施方式

[28] 应当理解，此处所描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

[29] 本申请实施例涉及的用户个人信息加密授权方法主要应用于用户个人信息加密授权设备，该用户个人信息加密授权设备可以是PC（个人计算机personal computer）、便携计算机、移动终端等具有显示和处理功能的设备。

[30] 参照图1，图1为本申请实施例方案中涉及的用户个人信息加密授权设备的硬件结构示意图。本申请实施例中，用户个人信息加密授权设备可以包括处理器1001（例如中央处理器Central Processing Unit、CPU），通信总线1002，用户接口1003，网络接口1004，存储器1005。其中，通信总线1002用于实现这些组件之间的连接通信；用户接口1003可以包括显示屏（Display）、输入单元比如键盘（Keyboard）；网络接口1004可选的可以包括标准的有线接口、无线接口（如WI-FI接口）；存储器1005可以是高速RAM存储器，也可以是稳定的存储器（non-volatile memory），例如磁盘存储器，存储器1005可选的还可以是独立于前述处理器1001的存储装置。本领域技术人员可以理解，图1中示出的硬件结构并不构成对本申请的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[31] 继续参照图1，图1中作为一种可读存储介质的存储器1005可以包括操作系统、

网络通信模块以及用户个人信息加密授权可读指令。在图1中，网络通信模块主要用于连接服务器，与服务器进行数据通信；而处理器1001可以调用存储器1005中存储的用户个人信息加密授权可读指令，并执行本申请实施例提供的用户个人信息加密授权方法。

[32] 本申请实施例提供了一种用户个人信息加密授权方法。

[33] 参照图2，图2为本申请用户个人信息加密授权方法第一实施例的流程示意图。

[34] 本实施例中，该用户个人信息加密授权方法由用户个人信息加密授权设备实现，该用户个人信息加密授权设备可以是PC、掌上电脑和平板电脑等终端设备，可选为图1所示的设备，该用户个人信息加密授权方法包括以下步骤：

[35] 步骤S101，接收用户终端上传的用户个人信息，并确定用户个人信息中是否存在待认证信息；

[36] 步骤S102，若用户个人信息中存在待认证信息，则对待认证信息进行认证，并在认证通过后，对用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；

[37] 步骤S103，当接收到用户终端发送的机构授权请求时，依据机构授权请求，对区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与机构授权请求对应的机构终端。

[38] 用户个人信息存储在服务器中，用户本身并未对个人信息加密，使得开发APP的公司能够在服务器中查询到用户个人信息，如果开发APP的公司滥用用户个人信息，容易导致用户个人信息的泄露，无法保证用户个人信息的安全性。考虑到上述问题，本实施例中提出一种用户个人信息加密授权方法，以下详细介绍用户个人信息加密授权方法的具体步骤：

[39] 步骤S101，接收用户终端上传的用户个人信息，并确定用户个人信息中是否存在待认证信息；

[40] 本实施例中，该用户终端包括但不限于PC、笔记本电脑、智能手机和平板电脑，该用户个人信息包括但不限于身份证、手机号码、联系地址、银行卡号、驾照、学历、公司名称、公司职位、所属行业、年龄和婚姻状况。具体实施中，用户通过用户终端的信息输入界面输入用户个人信息，在用户个人信息输入完

成之后，用户终端将输入的用户个人信息上传至用户个人信息加密授权设备，该设备接收用户终端上传的用户个人信息，并确定用户个人信息中是否存在待认证信息，即确定是否需要对该用户个人信息进行认证，如果该用户个人信息中存在待认证信息，则需要对该用户个人信息进行认证，反之，如果该用户个人信息中不存在待认证信息，则不需要对该用户个人信息进行认证。

[41] 具体地，当接收到用户终端上传的用户个人信息时，设备确定该用户个人信息中是否存在至少一信息字段位于预设字段组，如果该用户个人信息中存在至少一信息字段位于预设字段组，则可以确定用户个人信息中存在待认证信息，即需要认证，且待认证信息为该至少一信息字段对应的具体信息，如果该用户个人信息中的信息字段均不位于预设字段组，则可以确定用户个人信息中不存在待认证信息，即不需要认证。其中，信息字段包括但不限于年龄、身份证、学历、银行卡号、驾照、房产证、手机号码和公司名称。需要说明的是，上述预设字段组可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。

[42] 步骤S102，若用户个人信息中存在待认证信息，则对待认证信息进行认证，并在认证通过后，对用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；

[43] 本实施例中，如果用户个人信息中存在待认证信息，则对待认证信息进行认证，即验证用户个人信息的真实性，其中，待认证信息为身份证号码与姓名、手机号码、银行卡号和学历等中的一种或几种。具体地，确定待认证信息所属的认证接口，即从待认证信息中提取信息字段，查询信息字段与认证接口之间的映射关系表，将与待认证信息中信息字段对应的认证接口确定为待认证信息所属的认证接口，并通过所属的认证接口对该待认证信息进行认证。其中，认证接口包括但不限于公安部接口、运营商接口、银行接口和学信网接口，通过公安部接口认证姓名和身份证号码、通过运营商接口认证手机号码、通过各银行接口认证银行卡号以及通过学信网接口认证学历。

[44] 具体实施中，为了保证输入的用户个人信息为本人的信息，可先认证身份证号码与姓名，即用户首先输入身份证信息，包括姓名和身份证号码，并上传到设

备，由设备通过公安部接口认证身份证信息，并在身份证信息通过认证后，提示用户人脸识别，确定输入的身份证信息是否为本人的信息，在确定输入的身份证信息为本人的信息之后，提醒用户输入其他用户个人信息，结合身份证信息对其他用户个人信息进行认证。

[45] 在认证通过后，设备对用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中，即设备利用非对称加密算法生成一对用户的公开密钥（publickey）和私有密钥（privatekey），并根据该公有密钥对认证后的用户个人信息加密，并将加密后的用户个人信息存储至区块链中。其中，非对称加密算法包括但不限于RSA加密算法、Elgamal算法、背包算法、素数测试算法、D-H（Diffie-Hellman）算法和椭圆曲线加密算法，需要说明的是，上述非对称加密算法可由本领域技术人员基于实际情况进行设置，本专利提案对此不作具体限定。可以理解的是，由私有密钥可以算出公有私钥，而由公有私钥反向算出私有密钥是不可行的，因此只有用户自己的私有密钥，才能解密和阅读自己的用户个人信息，有效保护了个人隐私，保证用户个人信息的安全性。

[46] 步骤S103，当接收到用户终端发送的机构授权请求时，依据机构授权请求，对区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与机构授权请求对应的机构终端。

[47] 本实施例中，机构需要查询对应用户的用户个人信息时，通过机构终端确定需要查询的用户个人信息的信息类型，即待查询信息类型，并获取需要查询对应用户的公有私钥，然后基于该公有私钥对该待查询信息类型进行加密，并生成一包含加密的待查询信息类型的查询授权请求，且将该查询授权请求发送至用户终端。其中，机构终端包括但不限于PC、笔记本电脑、智能手机和平板电脑，信息类型包括身份证、手机号码、联系地址、银行卡号、学历、公司名称、公司职位、所属行业、年龄和婚姻状况等信息类型。

[48] 用户终端接收机构终端发送的查询授权请求，并依据本机的私有密钥对该查询授权请求中的待查询信息类型进行解密，然后显示包含有待查询信息类型、同意授权控件和拒绝授权控件的授权界面，如果用户点击拒绝授权控件，则查询授权流程结束，并向机构终端返回对应的信息；如果用户点击同意授权控件，

则生成一包含有授权信息类型、机构密钥信息（机构的公有密钥）、用户身份识别码、用户密钥信息（用户的私有密钥）和机构终端识别码的机构授权请求，并向设备发送该机构授权请求。

[49] 设备接收到用户终端发送的机构授权请求时，依据该机构授权请求，对区块链中的对应用户个人信息进行解密与筛选，具体地，设备从机构授权请求中读取授权信息类型、用户身份识别码和用户密钥信息，并从区块链中读取与该用户身份识别码对应的用户个人信息，然后依据该用户密钥信息，即用户的私钥密钥对该用户个人信息进行解密，并依据该授权信息类型，从解密后的用户个人信息中，筛选出授权用户个人信息，最后将筛选后的用户个人信息，即授权用户个人信息，经加密后传输至与机构授权请求对应的机构终端，即从该机构授权请求中读取机构终端识别码和机构密钥信息，并依据机构密钥信息，即机构的公有密钥对筛选后的用户个人信息，即授权用户个人信息进行加密，并将加密后授权用户个人信息传输至与机构终端识别码对应的机构终端。机构终端接收设备发送的授权用户个人信息，并依据机构的私有密钥对授权用户个人信息解密。具体实施中，授权用户个人信息具备有效时长，当授权用户个人信息的存储时间超过有效时长之后，自动删除授权用户个人信息。

[50] 本实施例中，本申请通过对用户个人信息进行认证，并将通过认证的用户个人信息加密后存储至区块链中，当接收到机构授权请求时，对存储在区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与对应的机构终端，由于用户个人信息经过认证，有效保证用户个人信息的准确性，且用户个人信息经过加密后存储在区块链中，可以防止他人篡改用户个人信息，且机构需要查询用户个人信息时，需要用户个人信息的拥有者授权给机构，机构才能够查询，有效的提高了用户个人信息的安全性。

[51] 进一步地，参照图3，基于上述第一实施例，提出了本申请用户个人信息加密授权方法的第二实施例，与前述实施例的区别在于，步骤S103之后，还包括：

[52] 步骤S104，统计用户个人信息的授权机构数量，并依据授权机构数量确定用户个人信息的信用增加值；

[53] 本实施例中，当设备接收到用户终端发送的机构授权请求时，记录机构授权请

求中的机构终端识别码，每一授权机构具有唯一的机构终端识别码，每接收到携带有不同机构终端识别码的机构授权请求，则被授权的用户个人信息的授权机构数量加1。设备定时统计用户个人信息的授权机构数量，并依据该授权机构数量确定用户个人信息的信用增加值，即查询预存的授权机构数量与信用增加值之间的映射关系表，获取该授权机构数量对应的信用增加值，或者确定该授权机构数量所属的数量区间，并查询预存的数量区间与信用增加值的映射关系表，获取该授权机构数量所处的数量区间对应的信用增加值。需要说明的是，上述授权机构数量与信用增加值之间的映射关系表以及数量区间与信用增加值的映射关系表可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。

[54] 步骤S105，依据用户个人信息的基础信用值和信用增加值确定用户个人信息的可信度等级。

[55] 本实施例中，设备在确定用户个人信息的信用增加值之后，依据用户个人信息的基础信用值和信用增加值确定用户个人信息的可信度等级，即获取该用户个人信息的基础信息值，并用该基础信息值加上该信用增加值，以获取该用户个人信息的总信用值，然后确定该总信用值所处的信用值区间，查询预存的信用区间与可信度等级之间的映射关系表，获取该信用区间对应的可信度等级。其中，可信度等级越高，则表示用户个人信息的可信程度越高，而可信度等级越低，则表示用户个人信息的可信程度越低。需要说明的是，上述信用区间与可信度等级之间的映射关系表可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。

[56] 本实施例中，本申请依据用户个人信息的授权机构数量，确定用户个人信息的可信度等级，便于用户和机构直观的知晓用户个人信息的可信程度。

[57] 进一步地，基于上述第二实施例，提出了本申请用户个人信息加密授权方法的第三实施例，与前述实施例的区别在于，该步骤S104之后，该用户个人信息加密授权方法还包括：

[58] 步骤a，统计用户个人信息的总授权次数，并依据总授权次数确定是否需要调整所述信用增加值；

- [59] 本实施例中，设备每接收到携带有不同机构终端识别码的机构授权请求，则被授权的用户个人信息的总授权次数加1，设备在用户个人信息的信用增加值之后，统计用户个人信息的总授权次数，并确定该总授权次数是否超过预设授权次数，即确定是否需要调整信用增加值，如果该总授权次数超过预设授权次数，则需要调整信用增加值，反之，如果该总授权次数未超过预设授权次数，则需要调整信用增加值。需要说明的是，上述预设授权次数可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。
- [60] 步骤b，若总授权次数超过预设授权次数，则依据总授权次数和授权机构数量重新确定用户个人信息的信用增加值。
- [61] 本实施例中，如果总授权次数超过预设授权次数，则依据该总授权次数和该授权机构数量重新确定用户个人信息的信用增加值，即查询预存的总授权次数与信用增加值之间的映射关系表，将与该总授权次数对应的信用增加值确定为用户个人信息的第二信用增加值，以及查询预存的授权机构数量与信用增加值之间的映射关系表，将与该授权机构数量对应的信用增加值确定为用户个人信息的第二信用增加值，然后获取第一预设权重系数和第二预设权重系数，并用第一预设权重系数乘以该第一信用增加值，以获取第一权重信用增加值，以及用第二预设权重系数乘以该第二信用增加值，以获取第二权重信用增加值，最后将第一权重信用增加值与第二权重信用增加值之和确定为用户个人信息的信用增加值。需要说明的是，总授权次数与信用增加值之间的映射关系表、上述授权机构数量与信用增加值之间的映射关系表、第一预设权重系数和第二预设权重系数可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。
- [62] 本实施例中，本申请结合授权机构数量和总授权次数，确定用户个人信息的信用增加值，有效的提高信用增加值的准确性，从而提高可信度等级的准确性。
- [63] 进一步地，基于上述第一或第二实施例，提出了本申请用户个人信息加密授权方法的第四实施例，与前述实施例的区别在于，该用户个人信息加密授权方法还包括：
- [64] 步骤c，统计用户个人信息的各授权机构的授权次数，并依据各授权机构的授

权次数确定用户个人信息的信用增加值；

[65] 本实施例中，当设备接收到用户终端发送的机构授权请求时，记录机构授权请求中的机构终端识别码，每一授权机构具有唯一的机构终端识别码，每接收到机构授权请求，则被授权的用户个人信息的对应授权机构的授权次数加1。设备统计用户个人信息的各授权机构的授权次数，并依据各授权机构的授权次数确定该用户个人信息的信用增加值。

[66] 具体地，设备查询预存的授权次数与信用增加值之间的映射关系表，确定各授权机构的信用增加值，然后读取各授权机构的机构类型标签，并查询预存的机构类型标签与权重系数之间的映射关系表，确定该用户个人信息的各授权机构的信用增加值，然后读取各授权机构的机构类型标签，并查询预存的机构类型标签与权重系数之间的映射关系表，确定各信用增加值的权重系数，最后用各信用增加值，乘以各信用增加值的对应权重系数之后，累加各乘积，并将累加值确定为该用户个人信息的信用增加值，以重新确定用户个人信息的信用增加值。其中，机构类型标签包括但不限于银行标签和贷款公司。需要说明的是，上述机构类型标签与权重系数之间的映射关系表以及机构类型标签与权重系数之间的映射关系表可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。

[67] 步骤d，依据用户个人信息的基础信用值和信用增加值确定用户个人信息的可信度等级。

[68] 本实施例中，设备在确定用户个人信息的信用增加值之后，依据用户个人信息的基础信用值和信用增加值确定用户个人信息的可信度等级，即获取该用户个人信息的基础信息值，并用该基础信息值加上该信用增加值，以获取该用户个人信息的总信用值，然后确定该总信用值所处的信用值区间，查询预存的信用区间与可信度等级之间的映射关系表，获取该信用区间对应的可信度等级。需要说明的是，上述信用区间与可信度等级之间的映射关系表可由本领域技术人员基于实际情况进行设置，本实施例对此不作具体限定。

[69] 本实施例中，本申请依据用户个人信息的各授权机构的授权次数，能够更加准确的确定用户个人信息的可信度等级，便于用户和机构直观的知晓用户个人信

息的可信程度。

[70] 此外，本申请实施例还提供一种用户个人信息加密授权装置。

[71] 参照图4，图4为本申请用户个人信息加密授权装置第一实施例的功能模块示意图。

[72] 本申请用户个人信息加密授权装置为虚拟装置，存储于图1所示用户个人信息加密授权设备的存储器1005中，用于实现用户个人信息加密授权可读指令的所有功能；接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。

[73] 具体的，本实施例中，所述用户个人信息加密授权装置包括：

[74] 接收确定模块101，用于接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；

[75] 认证加密模块102，用于若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；

[76] 信息授权模块103，用于当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。

[77] 进一步地，所述接收确定模块101还用于：

[78] 确定所述用户个人信息中是否存在至少一信息字段位于预设字段组；

[79] 若所述用户个人信息中存在至少一信息字段位于预设字段组，则确定所述用户个人信息中存在待认证信息。

[80] 进一步地，所述信息授权模块103还用于：

[81] 从所述机构授权请求中读取授权信息类型、用户身份识别码和用户密钥信息；

- [82] 从所述区块链中读取与所述用户身份识别码对应的用户个人信息，并依据所述用户密钥信息对所述用户个人信息进行解密；
- [83] 依据所述授权信息类型，从解密后的用户个人信息中，筛选出授权用户个人信息。
- [84] 进一步地，所述用户个人信息加密授权装置还包括：
- [85] 统计确定模块，用于统计所述用户个人信息的授权机构数量，并依据所述授权机构数量确定所述用户个人信息的信用增加值；
- [86] 可信度确定模块，用于依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。
- [87] 进一步地，所述统计确定模块还用于：
- [88] 统计所述用户个人信息的总授权次数，并确定所述总授权次数是否超过预设授权次数；
- [89] 若所述总授权次数超过预设授权次数，则依据所述总授权次数和所述授权机构数量重新确定所述用户个人信息的信用增加值。
- [90] 进一步地，所述统计确定模块还用于统计所述用户个人信息的各授权机构的授权次数，并依据各授权机构的授权次数确定所述用户个人信息的信用增加值；
- [91] 所述可信度确定模块，还用于依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。
- [92] 进一步地，所述统计确定模块还用于：
- [93] 查询预存的授权次数与信用增加值之间的映射关系表，确定所述用户个人信息的各授权机构的信用增加值；
- [94] 读取各授权机构的机构类型标签，并查询预存的机构类型标签与权重系数之间的映射关系表，确定各信用增加值的权重系数；
- [95] 用各信用增加值，乘以各信用增加值的对应权重系数之后，累加各乘积，并将累加值确定为所述用户个人信息的信用增加值。
- [96] 其中，上述用户个人信息加密授权装置中各个模块的功能实现与上述用户个人信息加密授权方法实施例中各步骤相对应，其功能和实现过程在此处不再一一赘述。

[97] 此外，本申请实施例还提供一种可读存储介质。

[98] 本申请可读存储介质上存储有用户个人信息加密授权可读指令，其中所述用户个人信息加密授权可读指令被处理器执行时，实现如上述的用户个人信息加密授权方法的步骤。

[99] 其中，该可读存储介质可以为非易失性计算机可读存储介质，该用户个人信息加密授权可读指令被执行时所实现的方法可参照本申请用户个人信息加密授权方法的各个实施例，此处不再赘述。

[100] 需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者系统不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[101] 上述本申请实施例序号仅仅为了描述，不代表实施例的优劣。

[102] 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上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本申请的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本申请各个实施例所述的方法。

[103] 以上仅为本申请的优选实施例，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权利要求书

- [权利要求 1] 一种用户个人信息加密授权方法，其特征在于，所述用户个人信息加密授权方法包括以下步骤：
- 接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；
- 若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，并将加密后的用户个人信息存储至区块链中；
- 当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。
- [权利要求 2] 如权利要求1所述的用户个人信息加密授权方法，其特征在于，确定所述用户个人信息中是否存在待认证信息的步骤包括：
- 确定所述用户个人信息中是否存在至少一信息字段位于预设字段组；
- 若所述用户个人信息中存在至少一信息字段位于预设字段组，则确定所述用户个人信息中存在待认证信息。
- [权利要求 3] 如权利要求1所述的用户个人信息加密授权方法，其特征在于，对所述区块链中的对应用户个人信息进行解密与筛选的步骤包括：
- 从所述机构授权请求中读取授权信息类型、用户身份识别码和用户密钥信息；
- 从所述区块链中读取与所述用户身份识别码对应的用户个人信息，并依据所述用户密钥信息对所述用户个人信息进行解密；
- 依据所述授权信息类型，从解密后的用户个人信息中，筛选出授权用户个人信息。
- [权利要求 4] 如权利要求1所述的用户个人信息加密授权方法，其特征在于，所述将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端的步骤之后，还包括：
- 统计所述用户个人信息的授权机构数量，并依据所述授权机构数量确

定所述用户个人信息的信用增加值；

依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。

[权利要求 5]

如权利要求4所述的个人信息加密授权方法，其特征在于，依据所述授权机构数量确定所述用户个人信息的信用增加值的步骤之后，还包括：

统计所述用户个人信息的总授权次数，并确定所述总授权次数是否超过预设授权次数；

若所述总授权次数超过预设授权次数，则依据所述总授权次数和所述授权机构数量重新确定所述用户个人信息的信用增加值。

[权利要求 6]

如权利要求4所述的个人信息加密授权方法，其特征在于，所述将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端的步骤之后，还包括：

统计所述用户个人信息的各授权机构的授权次数，并依据各授权机构的授权次数确定所述用户个人信息的信用增加值；

依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。

[权利要求 7]

如权利要求6所述的个人信息加密授权方法，其特征在于，所述依据各授权机构的授权次数确定所述用户个人信息的信用增加值的步骤包括：

查询预存的授权次数与信用增加值之间的映射关系表，确定所述用户个人信息的各授权机构的信用增加值；

读取各授权机构的机构类型标签，并查询预存的机构类型标签与权重系数之间的映射关系表，确定各信用增加值的权重系数；

用各信用增加值，乘以各信用增加值的对应权重系数之后，累加各乘积，并将累加值确定为所述用户个人信息的信用增加值。

[权利要求 8]

一种用户个人信息加密授权装置，其特征在于，所述用户个人信息加密授权装置包括：

接收确定模块，用于接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；

认证加密模块，用于若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；

信息授权模块，用于当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。

[权利要求 9]

一种用户个人信息加密授权设备，其特征在于，所述用户个人信息加密授权设备包括处理器、存储器、以及存储在所述存储器上并可被所述处理器执行的用户个人信息加密授权可读指令，其中所述用户个人信息加密授权可读指令被所述处理器执行时，实现以下步骤：

接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；

若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；

当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。

[权利要求 10]

如权利要求9所述的用户个人信息加密授权设备，其特征在于，确定所述用户个人信息中是否存在待认证信息的步骤包括：

确定所述用户个人信息中是否存在至少一信息字段位于预设字段组；

若所述用户个人信息中存在至少一信息字段位于预设字段组，则确定所述用户个人信息中存在待认证信息。

[权利要求 11]

如权利要求9所述的用户个人信息加密授权设备，其特征在于，对所述区块链中的对应用户个人信息进行解密与筛选的步骤包括：

从所述机构授权请求中读取授权信息类型、用户身份识别码和用户密钥信息；

从所述区块链中读取与所述用户身份识别码对应的用户个人信息，并依据所述用户密钥信息对所述用户个人信息进行解密；

依据所述授权信息类型，从解密后的用户个人信息中，筛选出授权用户个人信息。

[权利要求 12] 如权利要求9所述的用户个人信息加密授权设备，其特征在于，所述将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端的步骤之后，还包括：

统计所述用户个人信息的授权机构数量，并依据所述授权机构数量确定所述用户个人信息的信用增加值；

依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。

[权利要求 13] 如权利要求12所述的用户个人信息加密授权设备，其特征在于，依据所述授权机构数量确定所述用户个人信息的信用增加值的步骤之后，还包括：

统计所述用户个人信息的总授权次数，并确定所述总授权次数是否超过预设授权次数；

若所述总授权次数超过预设授权次数，则依据所述总授权次数和所述授权机构数量重新确定所述用户个人信息的信用增加值。

[权利要求 14] 如权利要求12所述的用户个人信息加密授权设备，其特征在于，所述将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端的步骤之后，还包括：

统计所述用户个人信息的各授权机构的授权次数，并依据各授权机构的授权次数确定所述用户个人信息的信用增加值；

依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。

[权利要求 15] 如权利要求14所述的用户个人信息加密授权设备，其特征在于，所述

依据各授权机构的授权次数确定所述用户个人信息的信用增加值的步骤包括：

查询预存的授权次数与信用增加值之间的映射关系表，确定所述用户个人信息的各授权机构的信用增加值；

读取各授权机构的机构类型标签，并查询预存的机构类型标签与权重系数之间的映射关系表，确定各信用增加值的权重系数；

用各信用增加值，乘以各信用增加值的对应权重系数之后，累加各乘积，并将累加值确定为所述用户个人信息的信用增加值。

[权利要求 16] 一种可读存储介质，其特征在于，所述可读存储介质上存储有用户个人信息加密授权可读指令，其中所述用户个人信息加密授权可读指令被处理器执行时，实现以下步骤：

接收用户终端上传的用户个人信息，并确定所述用户个人信息中是否存在待认证信息；

若所述用户个人信息中存在待认证信息，则对所述待认证信息进行认证，并在认证通过后，对所述用户个人信息进行加密，且将加密后的用户个人信息存储至区块链中；

当接收到用户终端发送的机构授权请求时，依据所述机构授权请求，对所述区块链中的对应用户个人信息进行解密与筛选，并将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端。

[权利要求 17] 如权利要求16所述的可读存储介质，其特征在于，确定所述用户个人信息中是否存在待认证信息的步骤包括：

确定所述用户个人信息中是否存在至少一信息字段位于预设字段组；

若所述用户个人信息中存在至少一信息字段位于预设字段组，则确定所述用户个人信息中存在待认证信息。

[权利要求 18] 如权利要求16所述的可读存储介质，其特征在于，对所述区块链中的对应用户个人信息进行解密与筛选的步骤包括：

从所述机构授权请求中读取授权信息类型、用户身份识别码和用户密钥信息；

从所述区块链中读取与所述用户身份识别码对应的用户个人信息，并依据所述用户密钥信息对所述用户个人信息进行解密；
依据所述授权信息类型，从解密后的用户个人信息中，筛选出授权用户个人信息。

[权利要求 19] 如权利要求16所述的可读存储介质，其特征在于，所述将筛选后的用户个人信息经加密后传输至与所述机构授权请求对应的机构终端的步骤之后，还包括：

统计所述用户个人信息的授权机构数量，并依据所述授权机构数量确定所述用户个人信息的信用增加值；

依据所述用户个人信息的基础信用值和所述信用增加值确定所述用户个人信息的可信度等级。

[权利要求 20] 如权利要求19所述的可读存储介质，其特征在于，依据所述授权机构数量确定所述用户个人信息的信用增加值的步骤之后，还包括：

统计所述用户个人信息的总授权次数，并确定所述总授权次数是否超过预设授权次数；

若所述总授权次数超过预设授权次数，则依据所述总授权次数和所述授权机构数量重新确定所述用户个人信息的信用增加值。

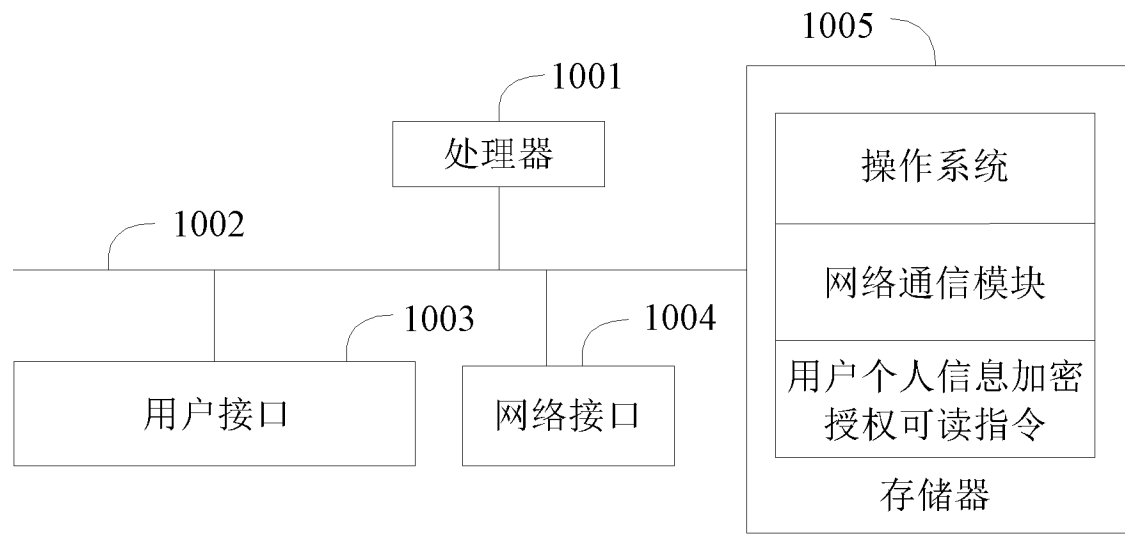


图 1

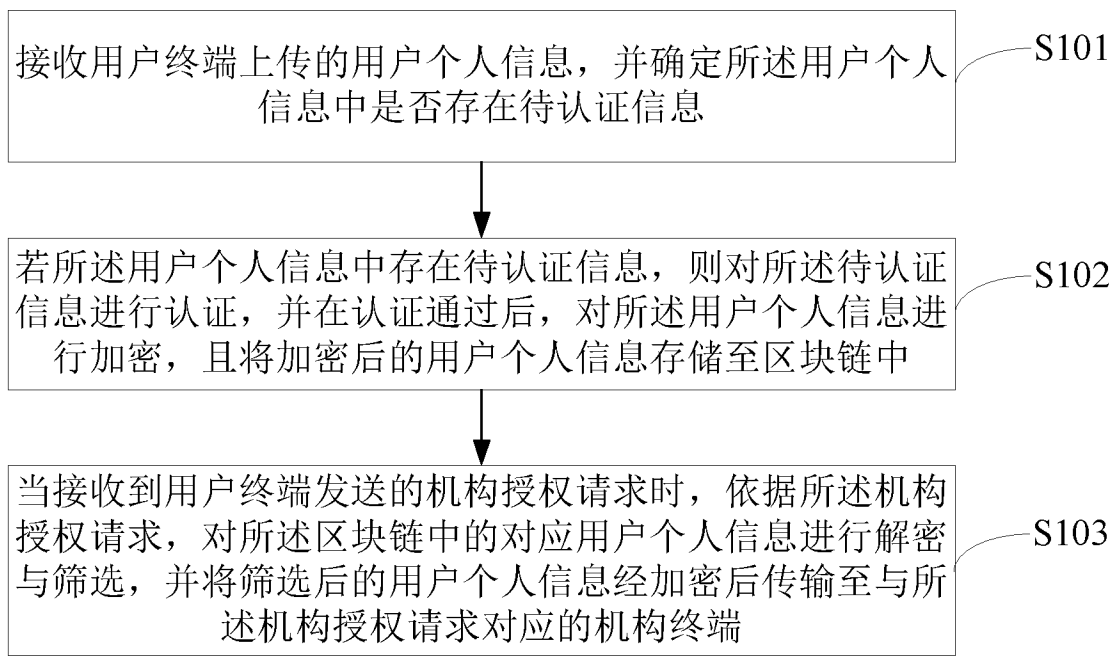


图 2

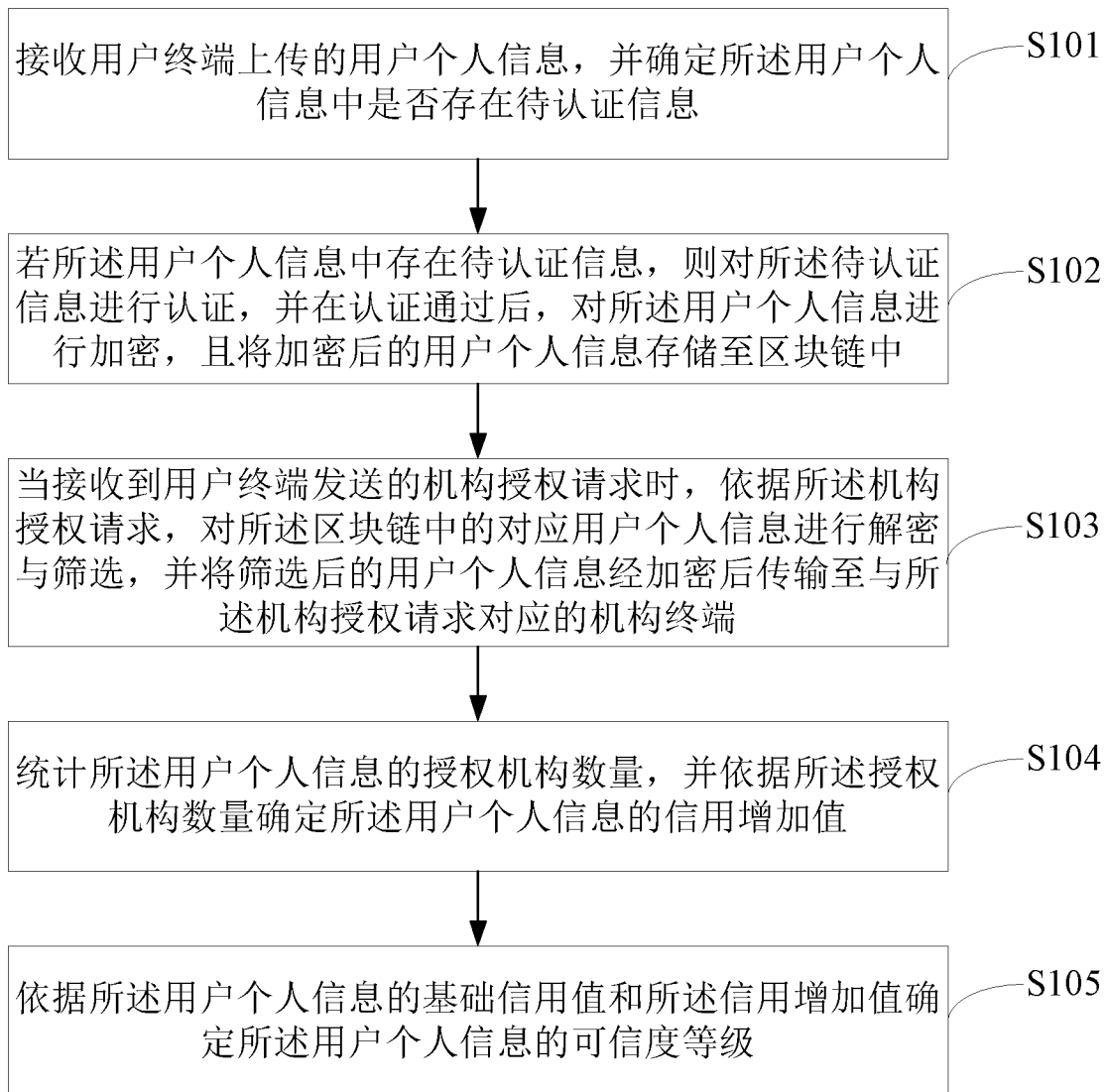


图 3

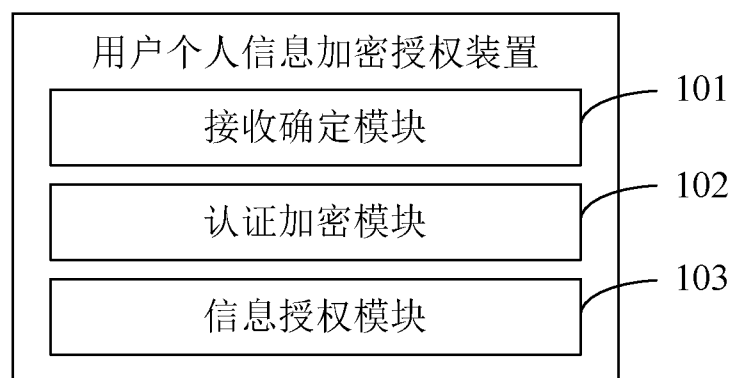


图 4

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/122636

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

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; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT: 应用, 注册信息, 用户信息, 个人信息, 隐私, 泄露, 泄密, 滥用, 保护, 实名, 认证, 验证, 加密, 存储, 区块链, app, information, registration, privacy, leakage, misus+, disclosure, protect, certificate, encode, encrypted, storage, block chain

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 104618401 A (SICHUAN NINGCHAO TECHNOLOGY CO., LTD.) 13 May 2015 (2015-05-13) description, paragraphs [0003]-[0011]	1-20
Y	CN 105072108 A (XIAOMI TECHNOLOGY CO., LTD.) 18 November 2015 (2015-11-18) description, paragraphs [0006]-[0054]	1-20
A	CN 102647430 A (SI, WEN) 22 August 2012 (2012-08-22) entire document	1-20
A	US 2015039889 A1 (ZEVA INC.) 05 February 2015 (2015-02-05) 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

03 April 2019

Date of mailing of the international search report

09 May 2019

Name and mailing address of the ISA/CN

State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/122636

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	104618401	A	13 May 2015	None			
CN	105072108	A	18 November 2015	CN	105072108	B	19 October 2018
CN	102647430	A	22 August 2012	None			
US	2015039889	A1	05 February 2015	WO	2015053819	A1	16 April 2015
				US	9438568	B2	06 September 2016

国际检索报告

国际申请号

PCT/CN2018/122636

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 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; CNTXT; CNKI; VEN; USTXT; EPTXT; WOTXT; 应用, 注册信息, 用户信息, 个人信息, 隐私, 泄露, 泄密, 滥用, 保护, 实名, 认证, 验证, 加密, 存储, 区块链, app, information, registration, privacy, leakage, misus+, disclosure, protect, certificate, encode, encrypted, storage, block chain																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>CN 104618401 A (四川省宁潮科技有限公司) 2015年 5月 13日 (2015 - 05 - 13) 说明书第[0003]-[0011]段</td> <td>1-20</td> </tr> <tr> <td>Y</td> <td>CN 105072108 A (小米科技有限责任公司) 2015年 11月 18日 (2015 - 11 - 18) 说明书第[0006]-[0054]段</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>CN 102647430 A (司文) 2012年 8月 22日 (2012 - 08 - 22) 全文</td> <td>1-20</td> </tr> <tr> <td>A</td> <td>US 2015039889 A1 (ZEVA INC) 2015年 2月 5日 (2015 - 02 - 05) 全文</td> <td>1-20</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	Y	CN 104618401 A (四川省宁潮科技有限公司) 2015年 5月 13日 (2015 - 05 - 13) 说明书第[0003]-[0011]段	1-20	Y	CN 105072108 A (小米科技有限责任公司) 2015年 11月 18日 (2015 - 11 - 18) 说明书第[0006]-[0054]段	1-20	A	CN 102647430 A (司文) 2012年 8月 22日 (2012 - 08 - 22) 全文	1-20	A	US 2015039889 A1 (ZEVA INC) 2015年 2月 5日 (2015 - 02 - 05) 全文	1-20
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
Y	CN 104618401 A (四川省宁潮科技有限公司) 2015年 5月 13日 (2015 - 05 - 13) 说明书第[0003]-[0011]段	1-20															
Y	CN 105072108 A (小米科技有限责任公司) 2015年 11月 18日 (2015 - 11 - 18) 说明书第[0006]-[0054]段	1-20															
A	CN 102647430 A (司文) 2012年 8月 22日 (2012 - 08 - 22) 全文	1-20															
A	US 2015039889 A1 (ZEVA INC) 2015年 2月 5日 (2015 - 02 - 05) 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 2019年 4月 3日		国际检索报告邮寄日期 2019年 5月 9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		授权官员 马小瑜 电话号码 86-(512)-88996083															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/122636

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	104618401	A	2015年 5月 13日	无	
CN	105072108	A	2015年 11月 18日	CN	105072108 B 2018年 10月 19日
CN	102647430	A	2012年 8月 22日	无	
US	2015039889	A1	2015年 2月 5日	WO	2015053819 A1 2015年 4月 16日
				US	9438568 B2 2016年 9月 6日