

(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 7 月 23 日 (23.07.2020)



(10) 国际公布号
WO 2020/147426 A1

(51) 国际专利分类号:
G06Q 20/38 (2012.01)

(21) 国际申请号: PCT/CN2019/120519

(22) 国际申请日: 2019 年 11 月 25 日 (25.11.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910048692.X 2019 年 1 月 18 日 (18.01.2019) 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 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。

(72) 发明人: 张小利 (ZHANG, Xiaoli); 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 (入驻深圳市前海商务秘书有限公司), Guangdong 518000 (CN)。

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路 80 号汇华商贸大厦 1508 室, Guangdong 510070 (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 INFORMATION AUTHORIZATION METHOD AND DEVICE, MEDIUM AND ELECTRONIC APPARATUS

(54) 发明名称: 基于区块链的信息授权方法、装置、介质及电子设备

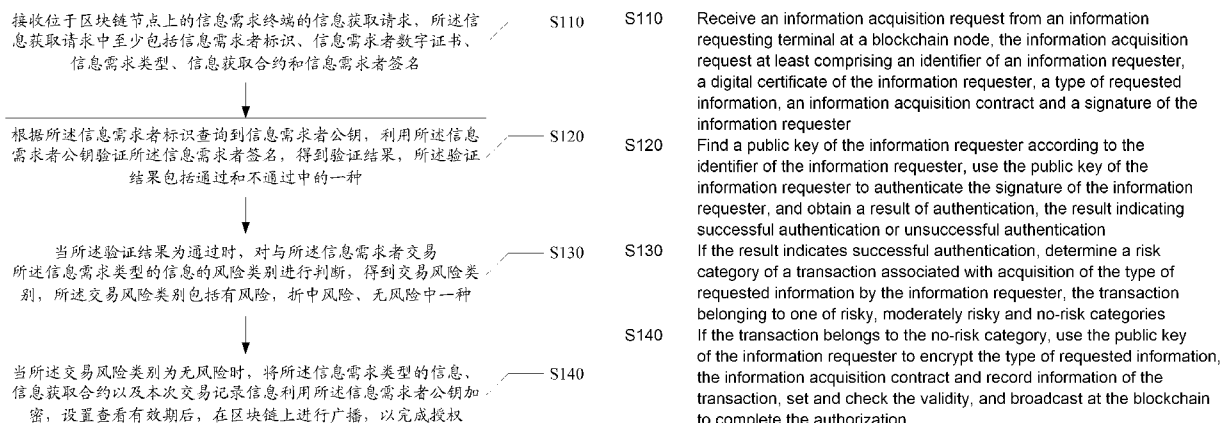


图 1

(57) **Abstract:** The present invention relates to the technical field of blockchain applications. Disclosed are a blockchain-based information authorization method and device, a medium and an electronic apparatus. The method comprises: receiving an information acquisition request from an information requesting terminal at a blockchain node; using a public key of an information requester found according to an identifier of the information requester indicated in the information acquisition request to authenticate a signature of the information requester, and obtaining a result of authentication; if the result indicates that the authentication is successful, determining a risk category of a type of information to be obtained by the information requester; if a transaction belongs to a no-risk category, an information providing terminal using the public key of the information requester to encrypt the type of requested information, an information acquisition contract and record information of the transaction, setting and checking the validity, and broadcasting to the information requesting terminal to complete the authorization. The invention uses blockchain to realize secure authorization of information at the security level, and on this basis, by evaluating transaction risks in advance, effectively ensures blockchain authorization-based secure authorization of information at the legal level.

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: 本公开是关于一种基于区块链的信息授权方法、装置、介质及电子设备, 属于区块链应用技术领域, 该方法包括: 接收位于区块链节点上的信息需求终端的信息获取请求; 根据信息获取请求中的信息需求者标识查询到的信息需求者公钥验证信息需求者签名, 得到验证结果; 当验证结果为通过, 对信息需求者获取该类型的信息的风险类别进行判断; 当交易风险类别为无风险, 信息提供终端将信息需求类型的信息、信息获取合约以及该次交易记录信息利用信息需求者公钥加密, 设置查看有效期后, 向信息需求终端进行广播, 完成授权。本公开在利用区块链实现信息安全层面的安全授权基础上, 通过交易风险的提前评估, 有效保证了基于区块链授权信息的合法层面的安全授权。

基于区块链的信息授权方法、装置、介质及电子设备

本申请要求于 2019 年 01 月 18 日提交中国专利局、申请号为 201910048692.X、申请名称为“基于区块链的信息授权方法、装置、介质及电子设备”的中国专利申请的优先权，其全部内容通过引用结合在本申请中。

技术领域

本公开涉及区块链应用技术领域，具体而言，涉及一种基于区块链的信息授权方法、装置、介质及电子设备。

背景技术

信息授权就是信息拥有者按照一定的相互协议将拥有的各种信息授权给需要相关信息的其他用户使用。

基于区块链进行信息授权时就是在区块链上的节点上的各设备之间将信息通过加密的形式进行授权分享，只有被授权的一方才可以通过自己独有的私钥解密，以区块链技术来提供相关信息的授权，被授权信息都是密文上链，信息授权时可以有效保证信息授权的安全性，即信息在信息安全层面的安全授权。但是，各种具有隐私性和机密性的信息在授权时，不仅要保证信息的安全，同时要保证信息授权时的在法律法规层面的安全性、可靠性，利用区块链进行授权时信息需求者不透明等原因会导致进行信息交易时具有潜在的风险，目前，没有一种在区块链信息授权时进行合法层面安全性评估授权的方法，带来潜在授权风险。

需要说明的是，在上述背景技术部分公开的信息仅用于加强对本公开的背景的理解，因此可以包括不构成对本领域普通技术人员已知的现有技术的信息。

发明内容

本公开的目的在于提供一种基于区块链的信息授权方案，进而至少在一定程度上在保证信息授权的合法合规的情况下，实现信息的安全、可靠授权。

根据本公开的一个方面，提供一种基于区块链的信息授权方法，其包括：

接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；

根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；

当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；

当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

根据本公开的一个方面，提供一种基于区块链的信息授权装置，包括：

获取模块，用于接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；

验证模块，用于根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；

判断模块，用于当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；

授权模块，用于当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

根据本公开的一个方面，提供一种计算机可读存储介质，其上存储有基于区块链的信息授权程序，所述基于区块链的信息授权程序被处理器执行时实现上述任一项所述的方法。可选的，该计算机可读存储介质可以为计算机非易失性可读存储介质。

根据本公开的一个方面，提供一种电子设备，包括：

处理器；以及

存储器，用于存储所述处理器的基于区块链的信息授权程序；其中，所述处理器配置为经由执行所述基于区块链的信息授权程序来执行上述任一项所述的方法。

本公开一种基于区块链的信息授权方法及装置，首先，接收位于区块链节点上的信息需求终端的信息获取请求；区块链一个节点上的信息提供终端获取到信息需求终端广播的信息获取请求，以查看自己是否拥有所需求的类型的信息，当有该信息的时候进行后续的步骤，可以有效减少信息授权之前询问的步骤浪费的时间，提高工作效率。根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果；信息需求者签名是利用信息需求者的私钥添加，同时只有利用信息需求者公钥才可以验证，通过验证说明本次操作为信息需求者的真实操作，有效保证安全性。当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种。在确保本次操作为需求者的真实操作后，与信息需求者交易该类型的信息是否合法具有很大的潜在风险，通过交易风险评估可以有效保证该次交易的合法性保障。当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权；当本次交易评估后为无风险时，将信息用信息需求者公钥加密实现私密传输，只有信息需求者私钥可以解密；最后在一定程度上在保证信息授权的合法合规的情况下，实现信息的安全、可靠授权。

应当理解的是，以上的一般描述和后文的细节描述仅是示例性和解释性的，并不能限制本公开。

附图说明

此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本公开的实施例，并与说明书一起用于解释本公开的原理。显而易见地，下面描述中的附图仅仅是本公开的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

图 1 示意性示出一种基于区块链的信息授权方法的流程图。

图 2 示意性示出一种基于区块链的信息授权方法的应用场景示例图。

图 3 示意性示出一种信息需求者获取该类型的信息的信息风险类别进行判断方法流程图。

图 4 示意性示出一种基于区块链的信息授权装置的方框图。

图 5 示意性示出一种用于实现上述基于区块链的信息授权方法的电子设备示例框图。

图 6 示意性示出一种用于实现上述基于区块链的信息授权方法的计算机可读存储介质。

具体实施方式

现在将参考附图更全面地描述示例实施方式。然而，示例实施方式能够以多种形式实施，且不应被理解为限于在此阐述的范例。

此外，附图仅为本公开的示意性图解，并非一定是按比例绘制。图中相同的附图标记表示相同或类似的部分，因而将省略对它们的重复描述。附图中所示的一些方框图是功能实体，不一定必须与物理或逻辑上独立的实体相对应。可以采用软件形式来实现这些功能实体，或在一个或多个硬件模块或集成电路中实现这些功能实体，或在不同网络和/或处理器装置和/或微控制器装置中实现这些功能实体。

本示例实施方式中首先提供了基于区块链的信息授权方法，该基于区块链的信息授权方法可以运行于服务器，也可以运行于服务器集群或云服务器等，当然，本领域技术人员也可以根据需求在其他平台运行本申请（本公开）的方法，本示例性实施例中对此不做特殊限定。参考图 1 所示，该基于区块链的信息授权方法可以包括以下步骤：

步骤 S110. 接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名。

步骤 S120. 根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种。

步骤 S130. 当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险、折中风险、无风险中一种。

步骤 S140. 当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

上述基于区块链的信息授权方法中，首先，接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信

息需求类型、信息获取合约和信息需求者签名；区块链一个节点上的信息提供终端获取到信息需求终端广播的信息获取请求，以查看自己是否拥有所需求的类型的信息，当有该信息的时候进行后续的步骤，可以有效减少信息授权之前问询的步骤浪费的时间，提高工作效率。根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；信息需求者签名是利用信息需求者的私钥添加，同时只有利用信息需求者公钥才可以验证，通过验证说明本次操作为信息需求者的真实操作，有效保证安全性。

当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种。在确保本次操作为需求者的真实操作后，与信息需求者交易该类型的信息是否合法具有很大的潜在风险，通过交易风险评估可以有效保证该次交易的合法性保障。当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权；当本次交易评估后为无风险时，将信息用信息需求者公钥加密实现私密传输，只有信息需求者私钥可以解密；最后在一定程度上在保证信息授权的合法合规的情况下，实现信息的安全、可靠授权。

下面，将结合附图对本示例实施方式中上述基于区块链的信息授权方法中的各步骤进行详细的解释以及说明。

在步骤 S110 中，接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名。

在本示例实施方式中，参考图 2 所示，首先，位于区块链的一个节点上的信息需求终端 202，在需要一种信息时，向区块链中其它的节点的具有所述信息的信息提供终端 201 广播获取该信息的信息获取请求；其中，信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；信息需求者标识用于查询信息需求者公钥，信息需求者数字证书用于获取信息需求者信息，信息需求类型用于准确定位所需要的信息的类型，信息获取合约就是指本次信息获取的双方合约，信息需求者签名是用信息需求者私钥添加，可以用公钥验证签名，表明信息需求者真实操作。

在步骤 S120 中，根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种。

在本示例的实施方式中，信息需求者标识与信息需求者公钥相关联，公钥保存在区块链的节点上；可以根据所述信息需求者标识查询到信息需求者公钥信息需求者签名是用信息需求者私钥添加，只能够用信息需求者的公钥进行验证的签名，信息需求者只有用私钥添加签名，才能表明本次操作是信息需求者的真实意愿；通过信息需求者的公钥进行验证的签名，验证结果未通过说明本次交易是信息需求者的真实操作，进而可以进行接下来的交易。

在步骤 S130 中，当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类

型的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种。

在本示例的实施方式中，区块链中进行交易时，使用区块链技术来提供相关信息的授权，被授权信息都是密文上链，授权过程安全可靠；但是信息授权具有很大的风险，例如不合法、不合规章等；利用区块链进行授权时与信息需求者不透明，进行交易时，具有潜在的风险；所以需要交易的交易的风险进行判断，判断信息需求终端来源的信息需求者获取该类型的信息的风险，只有保证无风险时才可以进行交易。本示例中在验证结果为通过，对信息需求终端来源的信息需求者获取该类型的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种，可以有效保证信息授权的合法合规性，在交易风险类别无风险时进行本次交易。

在本示例的一种实施方式中，参考图 3 所示，所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种，包括步骤 S310、步骤 S320 及步骤 S330：

步骤 S310. 利用所述信息需求者数字证书获取所述信息需求者数字证书指向的需求者行业类别；

步骤 S320. 依据所述信息需求类型在区块链交易记录中获取该类型信息交易频率；

步骤 S330. 将所述需求者行业类别、信息交易频率以及信息需求类型的作为输入数据输入预先训练好的机器学习模型，得到与该行业类别的信息需求者交易该类型信息的风险类别预测结果，所述预测结果包括有风险，折中风险、无风险中一种，

其中，所述机器学习模型的训练方法是：

收集需求者行业类别、信息交易频率以及信息需求类型样本组集，其中，每个样本组事先标定了与样本组中行业类别的信息需求者交易所述信息需求类型的信息的风险类别；

将每个样本组的数据分别输入机器学习模型，得到对样本组事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型的信息的风险类别，所述风险类别包括有风险，折中风险、无风险中一种；

如果机器学习模型的输出与事先对样本组事先标定的不一致，则调整机器学习模型的系数，使得机器学习模型针对所有样本组的输出，与事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型信息的风险类别一致，训练结束。

通过训练机器学习模型可以自动的通过打标签的形式进行交易风险的预测，得到信息需求终端来源的信息需求者获取该类型的信息的风险类别的预测结果。其中训练机器学习模型的样本选用事先标定了与一种行业类别的信息需求者交易一种类型信息的风险类别的需求者行业类别、信息交易频率、信息需求类型样本组，不同行业类别信息需求者对一种类型的信息的需求情况不同，同时这种类型的信息的交易频率可以反映该类型的信息的大众需求程度，这几个要素可以较为准确的指引与一种行业类别的信息需求者交易一种类型信息的风险，例如一家外资企业获取国防类型的信息时，这就具有极大的交易风险。

在本示例的一种实施方式中，在区块链的一个节点上设置了信息授权风险判断终端，所述信息授权风险判断终端来源于历史信息授权监控机构，

所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种，包括：

向信息授权风险判断终端广播风险判断需求；

当接收到所述信息授权风险判断终端对所述风险判断需求的响应时，将所述信息需求者数字证书、所述信息需求类型和信息交易记录签名，利用信息授权风险判断终端公钥加密后，广播至信息授权风险判断终端；

获取所述信息授权风险判断终端判断的所述交易风险类别。

通过在区块链的节点上设置信息授权风险判断终端，用于对信息需求终端来源的信息需求者获取该类型的信息的信息的风险类别进行判断，在信息提供终端需要判断信息需求终端来源的信息需求者获取该类型的信息的信息的风险类别时，只需要将相关信息广播至信息授权风险判断终端，就可以使得交易风险判断由专门的第三方终端信息授权风险判断终端进行，有效降低信息提供终端的处理负荷，进一步的对信息需求终端的评价更加客观。

在本示例的一种实施方式中，在所述获取所述信息授权风险判断终端判断的所述交易风险类别中，

所述信息授权风险判断终端判断所述交易风险类别的方法是：

利用所述信息授权风险判断终端的私钥解密所述广播对应的内容，得到所述信息需求者数字证书、所述信息需求类型和信息交易记录签名，利用与所述广播对应的内容相关联的信息提供者公钥验证所述信息交易记录签名；

当利用所述信息提供者公钥验证所述信息交易记录签名，验证通过后，判断所述信息交易记录真实性，得到判断结果，所述判断结果包括真实和不真实中的一种；

当所述判断结果为真实时，利用所述信息需求者数字证书、所述信息需求类型判断与所述信息需求者交易所述信息需求类型的信息的交易风险类别。

信息授权风险判断终端在获取到信息需求者数字证书、所述信息需求类型和信息交易记录签名后，通过利用与所述广播对应的内容相关联的信息提供者公钥验证信息交易记录签名，就可知道本次操作是不是信息需求者的真实操作；然后判断本次交易记录的真实性，可以保证在具有真实交易的情况下在进行风险判断，保证每个用户的隐私；在判断为真实存在交易后，对信息需求者交易所述信息需求类型的信息的交易风险类别进行判断，可以保证信息需求者的隐私安全。

在本示例的一种实施方式中，当利用所述信息提供者公钥验证所述信息交易记录签名，验证通过后，判断所述信息交易记录真实性，得到判断结果，所述判断结果包括真实和不真实中的一种，包括：

向所述区块链节点上的信息需求终端广播交易记录真实性验证请求；

当接收到所述信息需求终端对所述验证请求的响应时，将所述交易记录签名且所述利用信息需求者公钥加密后，广播至信息需求终端；

获取所述信息需求终端对所述交易记录的真实性的判断结果，所述判断结果包括真实和不真实中的一种。

只有在交易记录是真实的情况下才进行所述信息需求终端来源的信息需求者获取该类

型的信息的风险类别，可以保证对信息需求者的公平性，防止其他其它节点的恶意获取评价，保证信息不被滥用，同时避免区块链的节点上产生多余的信息；通过向信息需求者验证交易记录的真实性，可以在信息需求者的同意的情况下进行风险判断，进一步的保证信息需求者的公平性；同时，当信息需求者不进行所述交易记录的真实性验证时可以说明本次交易具有风险。

在本示例的一种实施方式中，所述历史信息授权监控机构按照每个信息需求者数字证书指向的信息需求者标签对应保存了根据所述信息需求者的历史交易评价的信誉类别，其中所述信誉类别包括良好、折中和差中的一种，

当所述判断结果为真实时，利用所述信息需求者数字证书、所述信息需求类型判断与所述信息需求者交易所所述信息需求类型的信息的交易风险类别，包括：

根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的所述信息需求者交易信誉类别；

根据所述交易信誉类别，判断所述交易风险类别。

历史信息授权监控机构保存有区块链上所有用户的信息交易记录以及信息需求者交易信誉类别，通过每个用户唯一的标签，也就是信息需求者标签，可以准确的爬取到信息需求者的交易信息记录，进而根据信息交易记录中的交易信誉类别，判断所述风险类别。这样可以根据用户的历史记录准确的判断出本次交易的风险。

在本示例的一种实施方式中，所述根据所述交易信誉类别，判断所述风险类别，包括：

根据所述交易信誉类别为良好，判断所述交易风险类别为无风险；

根据所述交易信誉类别为折中，判断所述交易风险类别为折中风险；

根据所述交易信誉类别为差，判断所述交易风险类别为有风险。

通过根据所述信息需求者的历史交易评价的信誉类别，例如违法违纪等信誉类别，就可以直接判断出与该信息需求者的交易的交易风险类别，例如，所述信息需求者的交易信誉类别为良好时，说明与该信息需求者进行交易时，可以有效保证交易之后的信息安全，而所述信息需求者的交易信誉类别为良好时，则相反。

在本示例的一种实施方式中，所述当所述验证结果为真实时，利用所述信息需求者数字证书、所述信息需求类型，判断与所述信息需求终端来源的信息需求者交易所所述信息需求类型的信息的风险类别，包括：

信息授权风险判断终端根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的该信息需求者交易所所述信息需求类型的信息的记录和该信息需求类型的信息在区块链中的交易记录；

根据所述信息需求者交易所所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录，判断与所述信息需求终端来源的信息需求者交易所所述信息需求类型的信息的风险类别。

根据所述信息需求者交易所所述信息需求类型的信息的记录可以判断出该用户对该类型的信息的实际需求度，根据信息需求类型的信息在区块链中的交易记录可以判断出该类型

的信息的所有用户的需求度，结合两个需求度就可以准确的判断出与所述信息需求终端来源的信息需求者交易该类型的信息的风险类别，例如当用户对该类型的信息在交易记录中非常的少，整个区块链中的交易记录中也非常的少，这就说明本次交易具有较高的风险，需要进行一定的实际考量决定时候进行交易，有效保证区块链中交易信息的低风险性。

本示例的一种实施方式中，所述根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录判断与所述信息需求终端来源的信息需求者交易所述信息需求类型的信息的风险类别，包括：

获取所述信息需求者交易所述信息需求类型的信息的记录中该信息需求类型的信息的第一交易频率；

获取所述信息需求类型的信息在区块链中的交易记录中该信息需求类型的信息的在包括当前时刻点之前的预定时间段的第二交易频率；

利用所述第一交易频率和第二频率判断与所述信息需求终端来源的信息需求者获取该类型的信息的风险类别。

当不能够直接根据例如交易信誉等判断出一个信息需求者的交易风险时，通过获取该信息交易者历史上交易该信息的记录，通过交易记录计算得到当前时刻点的类型的信息的第一交易频率，可以判断出该信息需求者的主要交易信息类型是否是该类型的信息；通过整个区块链中所述类型的信息的交易记录，计算包括当前时刻点之前的预定时间段的该类型信息的第二交易频率，可以知道该类型的信息是否在最近的时间段为大部分企业所需要的；通过获取所述信息需求者交易所述信息需求类型的信息的记录中该信息需求类型的信息的第一交易频率，例如第一交易频率为 0，说明该信息需求者对该类型的信息需求度极低；通过获取所述信息需求类型的信息在区块链中的交易记录中该信息需求类型的信息的在包括当前时刻点之前的预定时间段的第二交易频率，例如为 0.01%，说明所有用户对该信息的需求度也很低，反应出该类型的信息是比如国防、敏感言论等信息；然后，利用所述第一交易频率和第二频率判断与所述信息需求终端来源的信息需求者获取该类型的信息的风险类别；就可以根据两个交易频率准确的判断出本次交易的风险，进而在进一步的实地考量后决定是否授权该信息。

本示例的一种实施方式中，利用所述第一交易频率和第二频率判断与所述信息需求终端来源的信息需求者获取该类型的信息的风险类别，包括：

当所述第一频率超过第一预定阈值，同时第二频率超过第二预定阈值，判断所述风险类别为无风险；当所述第一频率没有超过第一预定阈值，同时第二频率没有超过第二预定阈值，判断所述风险类别为有风险；当所述第一频率超过第一预定阈值，同时第二频率没有超过第二预定阈值，或者，第一频率没有超过第一预定阈值，同时第二频率超过第二预定阈值，判断所述风险类别为折中风险。

当第一频率超过第一预定阈值，例如 10%，同时第二频率超过第二预定阈值，例如 5%，说明企业获取该类型的信息是非常合理的，也就是无风险；当第一频率没有超过第一预定阈值 10%，同时第二频率没有超过第二预定阈值 5%，判断所述风险类别为有风险，说明该信息需求者获取该类型的信息存在异常情况，为了保证信息授权的低风险即合法合规等，需要进一步调查研究或者直接拒绝授权；当所述第一频率超过第一预定阈值 10%，同时第

二频率没有超过第二预定阈值 5%，或者，第一频率没有超过第一预定阈值 10%，同时第二频率超过第二预定阈值 5%，说明该信息需求者获取所述信息的情况在有风险和无风险之间，判断所述风险类别为折中风险，需要进一步的沟通协调后决定是否授权。

在步骤 S140 中，响应于所述交易风险类别为无风险，信息提供终端将所述信息需求类型的信息、信息获取合约以及该次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，向信息需求终端进行广播，以完成授权。

在本示例的实施方式中，当判断到交易风险类别为无风险说明可以安全交易，信息提供终端将需要的信息需求类型的信息、信息获取合约以及该次交易记录信息利用所述信息需求者的公钥加密，并且设置查看有效期后，向信息需求终端进行广播，以完成授权，只有信息需求者的私钥才可以进行解密查看，同时设置查看有效期可以进一步保证所述信息的安全传输。

本公开还提供了一种基于区块链的信息授权装置。参考图 4 所示，该基于区块链的信息授权装置可以包括获取模块 410、验证模块 420、判断模块 430 以及授权模块 440。其中：

获取模块 410 可以用于接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；

验证模块 420 可以用于根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；

判断模块 430 可以用于当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；

授权模块 440 可以用于当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

上述基于区块链的信息授权装置中各模块的具体细节已经在对应的基于区块链的信息授权方法中进行了详细的描述，因此此处不再赘述。

应当注意，尽管在上文详细描述中提及了用于动作执行的设备的若干模块或者单元，但是这种划分并非强制性的。实际上，根据本公开的实施方式，上文描述的两个或更多模块或者单元的特征和功能可以在一个模块或者单元中具体化。反之，上文描述的一个模块或者单元的特征和功能可以进一步划分为由多个模块或者单元来具体化。

此外，尽管在附图中以特定顺序描述了本公开中方法的各个步骤，但是，这并非要求或者暗示必须按照该特定顺序来执行这些步骤，或是必须执行全部所示的步骤才能实现期望的结果。附加的或备选的，可以省略某些步骤，将多个步骤合并为一个步骤执行，以及/或者将一个步骤分解为多个步骤执行等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式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）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、移动终端、或者网络设备等）执行根据本公开实施方式的方法。

在本公开的示例性实施例中，还提供了一种能够实现上述方法的电子设备。

所属技术领域的技术人员能够理解，本申请的各个方面可以实现为系统、方法或程序产品。因此，本申请的各个方面可以具体实现为以下形式，即：完全的硬件实施方式、完全的软件实施方式（包括固件、微代码等），或硬件和软件方面结合的实施方式，这里可以统称为“电路”、“模块”或“系统”。

下面参照图 5 来描述根据本申请的这种实施方式的电子设备 500。图 5 显示的电子设备 500 仅仅是一个示例，不对本申请实施例的功能和使用范围带来任何限制。

如图 5 所示，电子设备 500 以通用计算设备的形式表现。电子设备 500 的组件可以包括但不限于：上述至少一个处理单元 510、上述至少一个存储单元 520、连接不同系统组件（包括存储单元 520 和处理单元 510）的总线 530。

其中，所述存储单元存储有程序代码，所述程序代码可以被所述处理单元 510 执行，使得所述处理单元 510 执行本说明书上述“示例性方法”部分中描述的根据本申请各种示例性实施方式的步骤。例如，所述处理单元 510 可以执行如图 1 中所示的步骤 S110：接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；S120：根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；步骤 S130：当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；步骤 S140：当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

存储单元 520 可以包括易失性存储单元形式的可读介质，例如随机存取存储单元（RAM）5201 和/或高速缓存存储单元 5202，还可以进一步包括只读存储单元（ROM）5203。

存储单元 520 还可以包括具有一组（至少一个）程序模块 5205 的程序/实用工具 5204，这样的程序模块 5205 包括但不限于：操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。

总线 530 可以为表示几类总线结构中的一种或多种，包括存储单元总线或者存储单元控制器、外围总线、图形加速端口、处理单元或者使用多种总线结构中的任意总线结构的局域总线。

电子设备 500 也可以与一个或多个外部设备 700（例如键盘、指向设备、蓝牙设备等）通信，还可与一个或者多个使得客户能与该电子设备 500 交互的设备通信，和/或与使得该电子设备 500 能与一个或多个其它计算设备进行通信的任何设备（例如路由器、调制解调器等等）通信。这种通信可以通过输入/输出（I/O）接口 550 进行。并且，电子设备 500 还可以通过网络适配器 560 与一个或者多个网络（例如局域网（LAN），广域网（WAN）

和/或公共网络，例如因特网）通信。如图所示，网络适配器 560 通过总线 530 与电子设备 500 的其它模块通信。应当明白，尽管图中未示出，可以结合电子设备 500 使用其它硬件和/或软件模块，包括但不限于：微代码、设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID 系统、磁带驱动器以及数据备份存储系统等。

通过以上的实施方式的描述，本领域的技术人员易于理解，这里描述的示例实施方式可以通过软件实现，也可以通过软件结合必要的硬件的方式来实现。因此，根据本公开实施方式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）中或网络上，包括若干指令以使得一台计算设备（可以是个人计算机、服务器、终端装置、或者网络设备等）执行根据本公开实施方式的方法。

在本公开的示例性实施例中，还提供了一种计算机可读存储介质，其上存储有能够实现本说明书上述方法的程序产品。在一些可能的实施方式中，本申请的各个方面还可以实现为一种程序产品的形式，其包括程序代码，当所述程序产品在终端设备上运行时，所述程序代码用于使所述终端设备执行本说明书上述“示例性方法”部分中描述的根据本申请各种示例性实施方式的步骤。

参考图 6 所示，描述了根据本申请的实施方式的用于实现上述方法的程序产品 600，其可以采用便携式紧凑盘只读存储器(CD-ROM)并包括程序代码，并可以在终端设备，例如个人电脑上运行。然而，本申请的程序产品不限于此，在本文件中，可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。所述程序产品可以采用一个或多个可读介质的任意组合。可读介质可以是可读信号介质或者可读存储介质。可读存储介质例如可以为但不限于电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。可读存储介质的更具体的例子（非穷举的列表）包括：具有一个或多个导线的电连接、便携式盘、硬盘、随机存取存储器（RAM）、只读存储器（ROM）、可擦式可编程只读存储器（EPROM 或闪存）、光纤、便携式紧凑盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。

计算机可读信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了可读程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。可读信号介质还可以是可读存储介质以外的任何可读介质，该可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于无线、有线、光缆、RF 等等，或者上述的任意合适的组合。

可以以一种或多种程序设计语言的任意组合来编写用于执行本申请操作的程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如 Java、C++等，还包括常规的过程式程序设计语言—诸如“C”语言或类似的设计语言。程序代码可以完全地在客户计算设备上执行、部分地在客户设备上执行、作为一个独立的软件包执行、部分在客户计算设备上部分在远程计算设备上执行、或者完全在远程计算设备或服务器上执行。在涉及远程计算设备的情形中，远程计算设备可以通过任意种类的网络，包括局域网（LAN）或广域

网（WAN），连接到客户计算设备，或者，可以连接到外部计算设备（例如利用因特网服务提供商来通过因特网连接）。

此外，上述附图仅是根据本申请示例性实施例的方法所包括的处理的示意性说明，而不是限制目的。易于理解，上述附图所示的处理并不表明或限制这些处理的时间顺序。另外，也易于理解，这些处理可以是例如在多个模块中同步或异步执行的。

本申请旨在涵盖本公开的任何变型、用途或者适应性变化，这些变型、用途或者适应性变化遵循本公开的一般性原理并包括本公开未公开的本技术领域中的公知常识或惯用技术手段。

权利要求

1. 一种基于区块链的信息授权方法，其特征在于，包括：

接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；

根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；

当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；

当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

2. 根据权利要求1所述的方法，其特征在于，所述所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种，包括：

利用所述信息需求者数字证书获取所述信息需求者数字证书指向的需求者行业类别；

依据所述信息需求类型在区块链交易记录中获取该类型信息交易频率；

将所述需求者行业类别、信息交易频率以及信息需求类型的作为输入数据输入预先训练好的机器学习模型，得到与该行业类别的信息需求者交易该类型信息的信息的风险类别预测结果，所述预测结果包括有风险，折中风险、无风险中一种，

其中，所述机器学习模型的训练方法是：

收集需求者行业类别、信息交易频率以及信息需求类型样本组集，其中，每个样本组事先标定了与样本组中行业类别的信息需求者交易所述信息需求类型的信息的信息的风险类别；

将每个样本组的数据分别输入机器学习模型，得到对样本组事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型的信息的信息的风险类别，所述风险类别包括有风险，折中风险、无风险中一种；

如果机器学习模型的输出与事先对样本组事先标定的不一致，则调整机器学习模型的系数，使得机器学习模型针对所有样本组的输出，与事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型信息的信息的风险类别一致，训练结束。

3. 根据权利要求1所述的方法，在区块链的一个节点上设置了信息授权风险判断终端，所述信息授权风险判断终端来源于历史信息授权监控机构，其特征在于，

所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种，包括：

向信息授权风险判断终端广播风险判断需求；

当接收到所述信息授权风险判断终端对所述风险判断需求的响应时，将所述信息需求者数字证书、所述信息需求类型和信息交易记录签名，利用信息授权风险判断终端公钥加

密后，广播至信息授权风险判断终端；

获取所述信息授权风险判断终端判断的所述交易风险类别。

4. 根据权利要求3所述的方法，其特征在于，在所述获取所述信息授权风险判断终端判断的所述交易风险类别中，

所述信息授权风险判断终端判断所述交易风险类别的方法是：

利用所述信息授权风险判断终端的私钥解密所述广播对应的内容，得到所述信息需求者数字证书、所述信息需求类型和信息交易记录签名，利用与所述广播对应的内容相关联的信息提供者公钥验证所述信息交易记录签名；

当利用所述信息提供者公钥验证所述信息交易记录签名，验证通过后，判断所述信息交易记录真实性，得到判断结果，所述判断结果包括真实和不真实中的一种；

当所述判断结果为真实时，利用所述信息需求者数字证书、所述信息需求类型判断与所述信息需求者交易所述信息需求类型的信息的交易风险类别。

5. 根据权利要求4所述的方法，其特征在于，当利用所述信息提供者公钥验证所述信息交易记录签名，验证通过后，判断所述信息交易记录真实性，得到判断结果，所述判断结果包括真实和不真实中的一种，包括：

向所述区块链节点上的信息需求终端广播交易记录真实性验证请求；

当接收到所述信息需求终端对所述验证请求的响应时，将所述交易记录签名且所述利用信息需求者公钥加密后，广播至信息需求终端；

获取所述信息需求终端对所述交易记录的真实性的判断结果，所述判断结果包括真实和不真实中的一种。

6. 根据权利要求4所述的方法，所述历史信息授权监控机构按照每个信息需求者数字证书指向的信息需求者标签对应保存了根据所述信息需求者的历史交易评价的信誉类别，其中所述信誉类别包括良好、折中和差中的一种，其特征在于，

当所述判断结果为真实时，利用所述信息需求者数字证书、所述信息需求类型判断与所述信息需求者交易所述信息需求类型的信息的交易风险类别，包括：

根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的所述信息需求者交易信誉类别；

根据所述交易信誉类别，判断所述交易风险类别。

7. 根据权利要求1所述的方法，其特征在于，所述对与所述信息需求者交易所述信息需求类型的信息的风险类别进行判断，包括：

根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的该信息需求者交易所述信息需求类型的信息的记录和该信息需求类型的信息在区块链中的交易记录；

根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录，判断与所述信息需求者交易所述信息需求类型的信息的风险类别。

8. 根据权利要求7所述的方法，其特征在于，所述根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录，判断与所述信

息需求者交易所述信息需求类型的信息的风险类别，包括：

获取所述信息需求者交易所述信息需求类型的信息的记录中该信息需求类型的信息的第一交易频率；

获取所述信息需求类型的信息在区块链中的交易记录中该信息需求类型的信息的在包括当前时刻点之前的预定时间段的第二交易频率；

利用所述第一交易频率和第二频率判断与所述信息需求者获取该类型的信息的风险类别。

9. 一种基于区块链的信息授权装置，其特征在于，包括：

获取模块，用于接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；

验证模块，用于根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；

判断模块，用于当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；

授权模块，用于当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

10. 根据权利要求9所述的装置，其特征在于，所述判断模块具体用于：

利用所述信息需求者数字证书获取所述信息需求者数字证书指向的需求者行业类别；

依据所述信息需求类型在区块链交易记录中获取该类型信息交易频率；

将所述需求者行业类别、信息交易频率以及信息需求类型的作为输入数据输入预先训练好的机器学习模型，得到与该行业类别的信息需求者交易该类型信息的信息风险类别预测结果，所述预测结果包括有风险，折中风险、无风险中一种，

其中，所述机器学习模型的训练方法是：

收集需求者行业类别、信息交易频率以及信息需求类型样本组集，其中，每个样本组事先标定了与样本组中行业类别的信息需求者交易所述信息需求类型的信息的信息风险类别；

将每个样本组的数据分别输入机器学习模型，得到对样本组事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型的信息的信息风险类别，所述风险类别包括有风险，折中风险、无风险中一种；

如果机器学习模型的输出与事先对样本组事先标定的不一致，则调整机器学习模型的系数，使得机器学习模型针对所有样本组的输出，与事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型信息的信息风险类别一致，训练结束。

11. 根据权利要求9所述的装置，在区块链的一个节点上设置了信息授权风险判断终端，所述信息授权风险判断终端来源于历史信息授权监控机构，其特征在于，所述判断模块具体用于：

向信息授权风险判断终端广播风险判断需求；

当接收到所述信息授权风险判断终端对所述风险判断需求的响应时，将所述信息需求者数字证书、所述信息需求类型和信息交易记录签名，利用信息授权风险判断终端公钥加密后，广播至信息授权风险判断终端；

获取所述信息授权风险判断终端判断的所述交易风险类别。

12. 根据权利要求 9 所述的装置，其特征在于，所述判断模块具体用于：

根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的所述信息需求者交易信誉类别；所述历史信息授权监控机构按照每个信息需求者数字证书指向的信息需求者标签对应保存了根据所述信息需求者的历史交易评价的信誉类别，其中所述信誉类别包括良好、折中和差中的一种；

根据所述交易信誉类别，判断所述交易风险类别。

13. 根据权利要求 9 所述的装置，其特征在于，所述对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，包括：

根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的该信息需求者交易所述信息需求类型的信息的记录和该信息需求类型的信息在区块链中的交易记录；

根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录，判断与所述信息需求者交易所述信息需求类型的信息的信息的风险类别。

14. 根据权利要求 13 所述的装置，其特征在于，所述判断模块在根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录，判断与所述信息需求者交易所述信息需求类型的信息的信息的风险类别时，具体用于：

获取所述信息需求者交易所述信息需求类型的信息的记录中该信息需求类型的信息的第一交易频率；

获取所述信息需求类型的信息在区块链中的交易记录中该信息需求类型的信息的在包括当前时刻点之前的预定时间段的第二交易频率；

利用所述第一交易频率和第二频率判断与所述信息需求者获取该类型的信息的信息的风险类别。

15. 一种计算机可读存储介质，其上存储有基于区块链的信息授权程序，其特征在于，所述基于区块链的信息授权程序被处理器执行时实现权利要求 1-8 任一项所述的方法。

16. 一种电子设备，其特征在于，包括：

处理器；以及

存储器，用于存储所述处理器的基于区块链的信息授权程序；其中，所述处理器配置为经由执行所述基于区块链的信息授权程序来执行以下步骤：

接收位于区块链节点上的信息需求终端的信息获取请求，所述信息获取请求中至少包括信息需求者标识、信息需求者数字证书、信息需求类型、信息获取合约和信息需求者签名；

根据所述信息需求者标识查询到信息需求者公钥，利用所述信息需求者公钥验证所述

信息需求者签名，得到验证结果，所述验证结果包括通过和不通过中的一种；

当所述验证结果为通过时，对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别，所述交易风险类别包括有风险，折中风险、无风险中一种；

当所述交易风险类别为无风险时，将所述信息需求类型的信息、信息获取合约以及本次交易记录信息利用所述信息需求者公钥加密，设置查看有效期后，在区块链上进行广播，以完成授权。

17. 根据权利要求 16 所述的电子设备，其特征在于，所述处理器在执行所述对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别时，具体执行以下步骤：

利用所述信息需求者数字证书获取所述信息需求者数字证书指向的需求者行业类别；

依据所述信息需求类型在区块链交易记录中获取该类型信息交易频率；

将所述需求者行业类别、信息交易频率以及信息需求类型的作为输入数据输入预先训练好的机器学习模型，得到与该行业类别的信息需求者交易该类型信息的信息的风险类别预测结果，所述预测结果包括有风险，折中风险、无风险中一种，

其中，所述机器学习模型的训练方法是：

收集需求者行业类别、信息交易频率以及信息需求类型样本组集，其中，每个样本组事先标定了与样本组中行业类别的信息需求者交易所述信息需求类型的信息的信息的风险类别；

将每个样本组的数据分别输入机器学习模型，得到对样本组事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型的信息的信息的风险类别，所述风险类别包括有风险，折中风险、无风险中一种；

如果机器学习模型的输出与事先对样本组事先标定的不一致，则调整机器学习模型的系数，使得机器学习模型针对所有样本组的输出，与事先标定的与样本组中行业类别的信息需求者交易所述信息需求类型信息的信息的风险类别一致，训练结束。

18. 根据权利要求 16 所述的电子设备，在区块链的一个节点上设置了信息授权风险判断终端，所述信息授权风险判断终端来源于历史信息授权监控机构，其特征在于，

所述处理器在执行所述对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断，得到交易风险类别时，具体执行以下步骤：

向信息授权风险判断终端广播风险判断需求；

当接收到所述信息授权风险判断终端对所述风险判断需求的响应时，将所述信息需求者数字证书、所述信息需求类型和信息交易记录签名，利用信息授权风险判断终端公钥加密后，广播至信息授权风险判断终端；

获取所述信息授权风险判断终端判断的所述交易风险类别。

19. 根据权利要求 16 所述的电子设备，其特征在于，所述处理器在执行所述对与所述信息需求者交易所述信息需求类型的信息的信息的风险类别进行判断时，具体执行以下步骤：

根据所述信息需求者数字证书获取所述信息需求者数字证书指向的信息需求者标签；

根据所述信息需求者标签爬取记录在历史信息授权监控机构的该信息需求者交易所述信息需求类型的信息的记录和该信息需求类型的信息在区块链中的交易记录；

根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录,判断与所述信息需求者交易所述信息需求类型的信息的风险类别。

20. 根据权利要求 19 所述的电子设备,其特征在于,所述处理器在执行所述所述根据所述信息需求者交易所述信息需求类型的信息的记录和所述信息需求类型的信息在区块链中的交易记录,判断与所述信息需求者交易所述信息需求类型的信息的风险类别时,具体执行以下步骤:

获取所述信息需求者交易所述信息需求类型的信息的记录中该信息需求类型的信息的第一交易频率;

获取所述信息需求类型的信息在区块链中的交易记录中该信息需求类型的信息的在包括当前时刻点之前的预定时间段的第二交易频率;

利用所述第一交易频率和第二频率判断与所述信息需求者获取该类型的信息的风险类别。

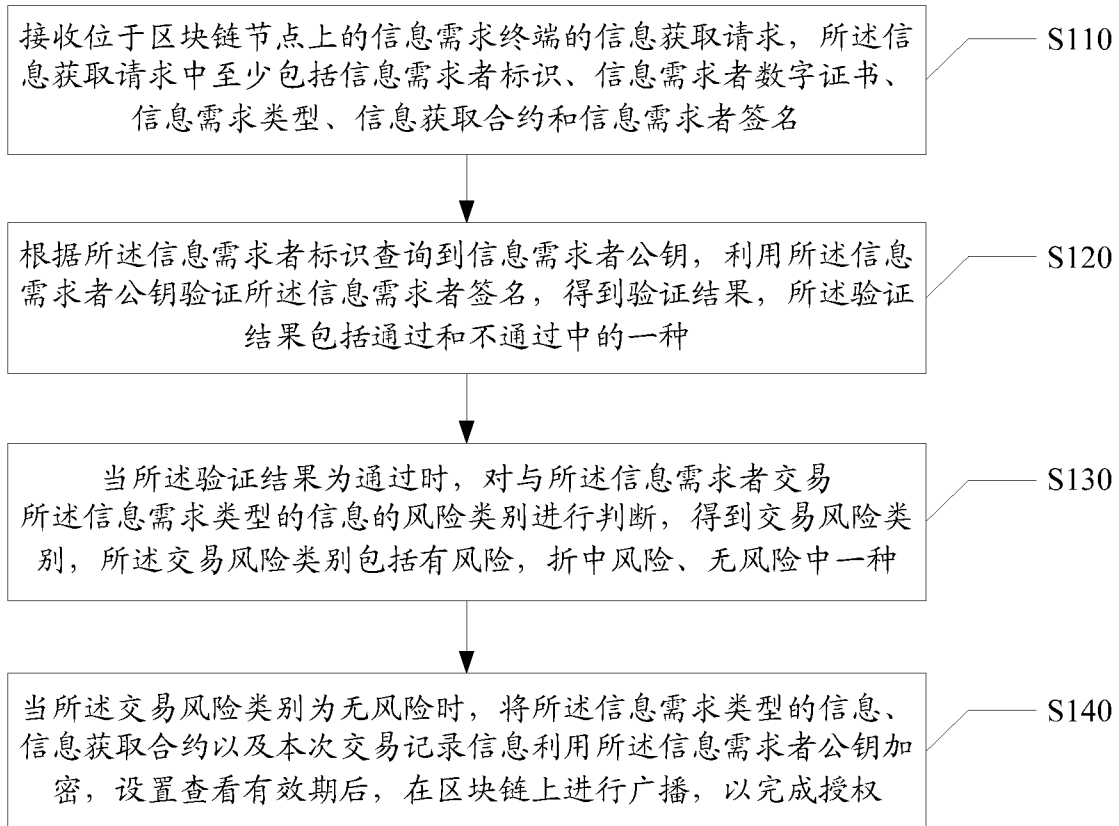


图 1

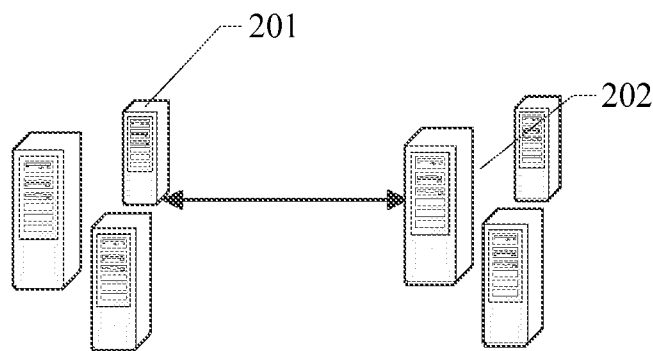


图 2

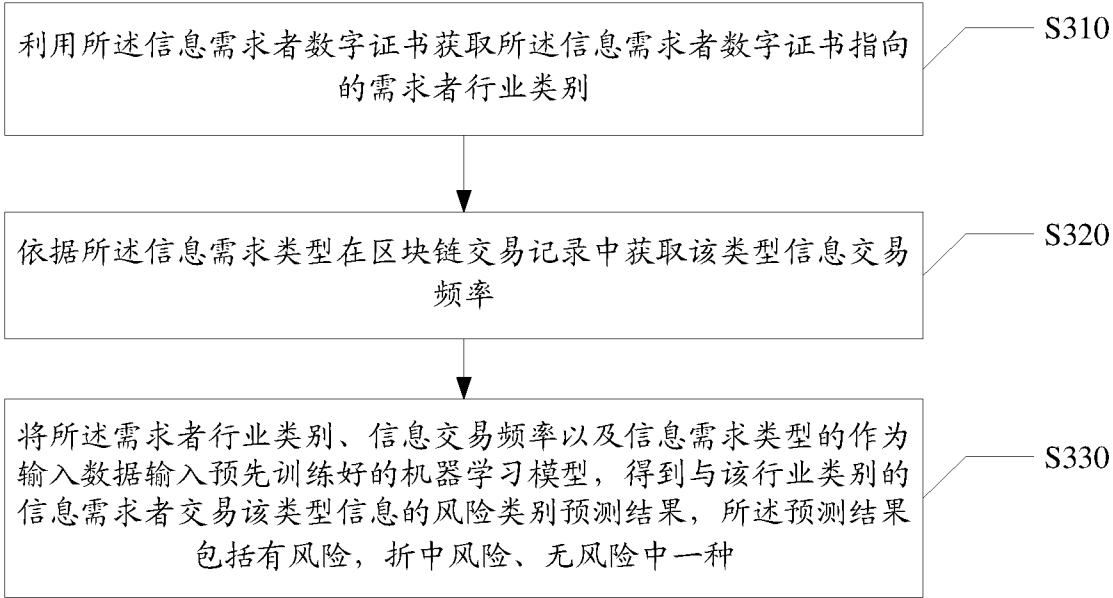


图 3

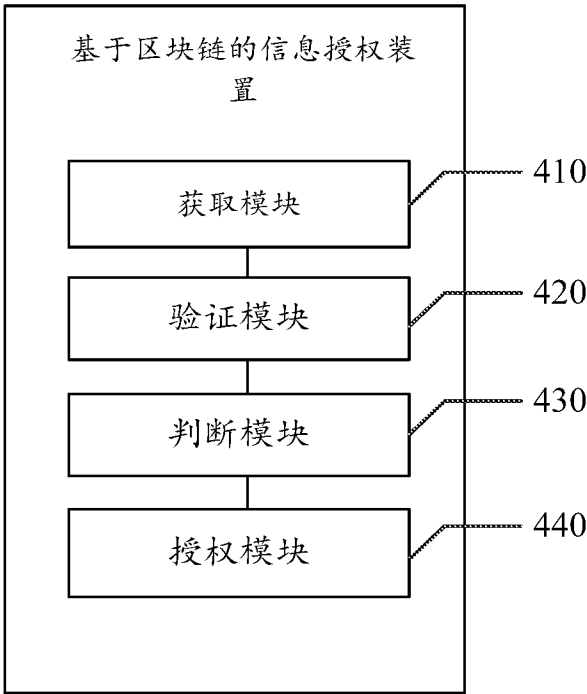


图 4

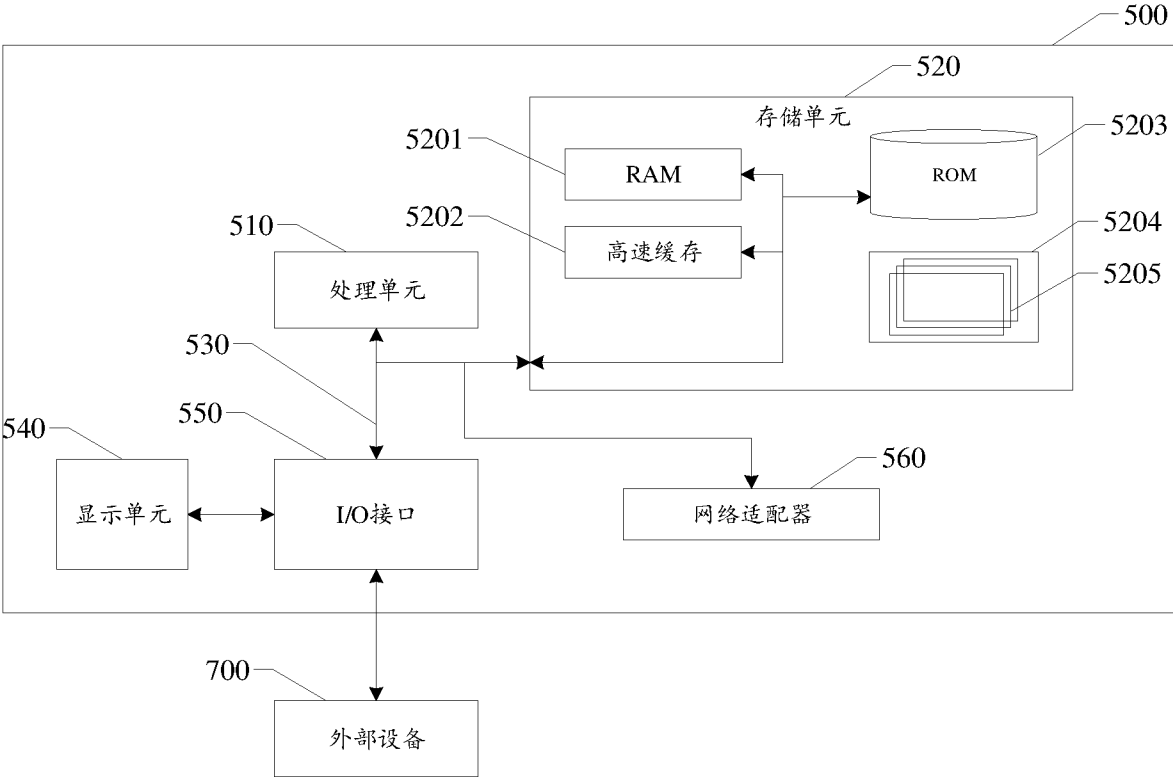


图 5

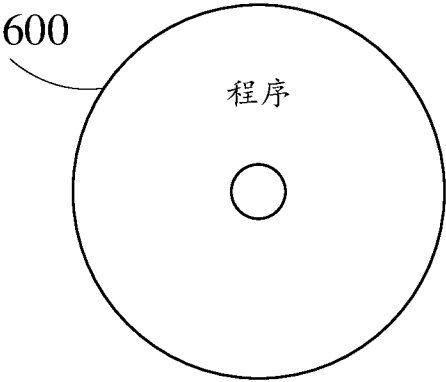


图 6

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2019/120519

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)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)

G06Q 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)

WPI, EPODOC, CNPAT, CNKI: 请求, 加密, 风险, 标识, 签名, 无风险, 授权, 类别, 广播, 区块链, ID, 公钥, request, encrypt, risk, id, identifier, signature, risk free, authorize, sort, broadcast, blockchain, public key

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 109903042 A (SHENZHEN ONECONNECT TECHNOLOGY CO., LTD.) 18 June 2019 (2019-06-18) description, paragraphs [0006]-[0063]	1-20
Y	CN 107257340 A (ALIBABA GROUP HOLDING LIMITED) 17 October 2017 (2017-10-17) description, paragraphs [0055]-[0082], [0089]-[0114], and [0208]	1-20
Y	CN 108717443 A (BEIJING JD FINANCE TECHNOLOGY CO., LTD.) 30 October 2018 (2018-10-30) description, paragraphs [0091]-[0097]	1-20
A	US 2017221022 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 03 August 2017 (2017-08-03) 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

19 January 2020

Date of mailing of the international search report

11 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
Information on patent family members

International application No.

PCT/CN2019/120519

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	109903042	A	18 June 2019	None			
CN	107257340	A	17 October 2017	WO	2018233536	A1	27 December 2018
				US	2019386975	A1	19 December 2019
				TW	201906389	A	01 February 2019
				KR	20190127676	A	13 November 2019
				SG	11201906764 Q	A	27 August 2019
CN	108717443	A	30 October 2018	None			
US	2017221022	A1	03 August 2017	CN	108475457	A	31 August 2018
				WO	2017132336	A1	03 August 2017
				EP	3200167	A1	02 August 2017
				AU	2017212504	A1	14 June 2018
				CA	3011600	A1	03 August 2017

国际检索报告

国际申请号

PCT/CN2019/120519

A. 主题的分类

G06Q 20/38 (2012.01) 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)

G06Q 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))

WPI, EPDOC, CNPAT, CNKI: 请求, 加密, 风险, 标识, 签名, 无风险, 授权, 类别, 广播, 区块链, ID, 公钥, request, encrypt, risk, id, identifier, signature, risk free, authorize, sort, broadcast, blockchain, public key

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 109903042 A (深圳壹账通智能科技有限公司) 2019年 6月 18日 (2019 - 06 - 18) 说明书第[0006]-[0063]段	1-20
Y	CN 107257340 A (阿里巴巴集团控股有限公司) 2017年 10月 17日 (2017 - 10 - 17) 说明书第[0055]-[0082]、[0089]-[0114]、[0208]段	1-20
Y	CN 108717443 A (北京京东金融科技控股有限公司) 2018年 10月 30日 (2018 - 10 - 30) 说明书第[0091]-[0097]段	1-20
A	US 2017221022 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 2017年 8月 3日 (2017 - 08 - 03) 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 1月 19日

国际检索报告邮寄日期

2020年 2月 11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

王欣

电话号码 86-(10)-53961617

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2019/120519

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	109903042	A	2019年 6月 18日	无			
CN	107257340	A	2017年 10月 17日	WO	2018233536	A1	2018年 12月 27日
				US	2019386975	A1	2019年 12月 19日
				TW	201906389	A	2019年 2月 1日
				KR	20190127676	A	2019年 11月 13日
				SG	11201906764Q	A	2019年 8月 27日
CN	108717443	A	2018年 10月 30日	无			
US	2017221022	A1	2017年 8月 3日	CN	108475457	A	2018年 8月 31日
				WO	2017132336	A1	2017年 8月 3日
				EP	3200167	A1	2017年 8月 2日
				AU	2017212504	A1	2018年 6月 14日
				CA	3011600	A1	2017年 8月 3日