(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110321732 A
(43)申请公布日 2019.10.11

(21)申请号 201910434980.9

(22)申请日 2019.05.23

(71)申请人 深圳壹账通智能科技有限公司
地址 518000 广东省深圳市前海深港合作区前湾一路1号A栋201室

(72)发明人 赵达悦 王梦寒 陆一帆

(74)专利代理机构 深圳市隆天联鼎知识产权代理有限公司 44232
代理人 刘抗美

(51)Int.Cl.
G06F 21/62(2013.01)
G06F 21/60(2013.01)

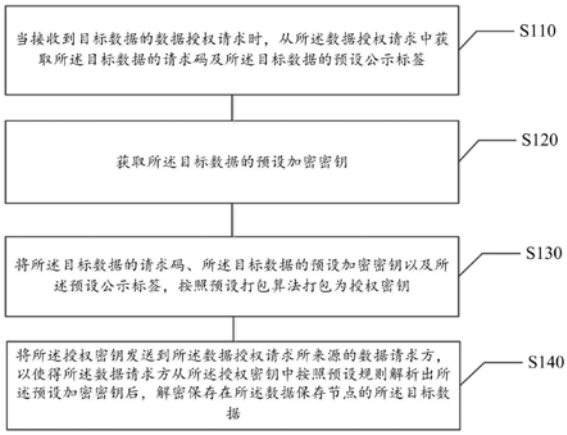
权利要求书2页 说明书11页 附图3页

(54)发明名称

区块链系统的数据授权方法、装置、存储介质及电子设备

(57)摘要

本公开是关于一种区块链系统的数据授权方法、装置、存储介质及电子设备，属于区块链应用技术领域，该方法包括：当接收到目标数据的数据授权请求时，从数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；获取所述目标数据的预设加密密钥；将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方解析出预设加密密钥后，解密保存在所述数据保存节点的目标数据。本公开通过预先将加密数据上链，通过密钥授权，在保证数据授权的安全性情况下，有效提高区块链系统上数据授权的便捷性及高效性。



CN 110321732 A

1.一种区块链系统的数据授权方法，其特征在于，所述区块链系统包括数据保存节点子网络以及与所述数据保存节点子网络中数据保存节点相连的数据授权节点，所述数据授权方法由所述数据授权节点执行，所述数据授权方法包括：

当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；

获取所述目标数据的预设加密密钥；

将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；

将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

2.根据权利要求1所述的方法，其特征在于，所述获取所述目标数据的预设加密密钥，包括：

从源数据库中，查询所述目标数据的预设公示标签；

当查询到所述目标数据的预设公示标签，获取与所述目标数据的预设公示标签关联存储的预设加密密钥。

3.根据权利要求1所述的方法，其特征在于，所述将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥，包括：

获取所述数据授权请求所来源的数据请求方的第一区块节点码；

获取所述数据授权节点的第二区块节点码；

将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥。

4.根据权利要求3所述的方法，其特征在于，所述将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥，包括：

将所述第一区块节点码和所述第二区块节点码设置为函数系数；

将所述目标数据的请求码和所述预设公示标签设置为函数解；

将所述目标数据的预设加密密钥设置为函数值；

进行算法拟合得到授权密钥。

5.根据权利要求1所述的方法，其特征在于，在所述当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签之前，所述方法还包括：

当检测到目标数据上传到所述数据保存节点，为所述目标数据添加预设公示标签；

获取为所述目标数据事先设置的预设加密密钥；

将所述预设公示标签和所述预设加密密钥关联存储。

6.根据权利要求1所述的方法，其特征在于，在所述当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签之前，所述方法还包括：

数据请求节点将所述目标数据的请求码及所述目标数据的预设公示标签利用信息授

权节点的公钥加密，得到目标数据的数据授权请求；

将所述目标数据的数据授权请求发送到数据授权节点。

7.根据权利要求1所述的方法，其特征在于，所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥，包括：

触发对所述授权密钥的解析操作，得到解析指令输入界面；

将所述所述目标数据的请求码以及所述预设公示标签输入所述解析指令输入界面并进行确认，得到所述预设加密密钥。

8.一种区块链系统的数据授权装置，其特征在于，包括：

接收模块，用于当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；

获取模块，用于获取所述目标数据的预设加密密钥；

打包模块，用于将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；

发送模块，用于将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

9.一种计算机可读存储介质，其上存储有区块链系统的数据授权程序，其特征在于，所述区块链系统的数据授权程序被处理器执行时实现权利要求1-7任一项所述的方法。

10.一种电子设备，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区块链系统的数据授权程序；其中，所述处理器配置为经由执行所述区块链系统的数据授权程序来执行权利要求1-7任一项所述的方法。

区块链系统的数据授权方法、装置、存储介质及电子设备

技术领域

[0001] 本公开涉及区块链应用技术领域，具体而言，涉及一种区块链系统的数据授权方法、装置、存储介质及电子设备。

背景技术

[0002] 区块链系统是由多个子网络构成，每个子网络又包括多个节点，上传到区块链的数据会在区块链上的各个节点上进行共享，也就是每个节点上存在数据备份。

[0003] 现有技术中利用区块链系统进行数据共享时，通常按照密钥对机制，也就是公钥私钥机制，实时将数据进行公钥加密后上传的区块链节点，然后进行广播到数据需求节点以进行授权。现有技术中，需要每次将数据进行上传以进行数据的授权操作，授权操作不方便。

[0004] 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

[0005] 本公开的目的在于提供一种区块链系统的数据授权方案，进而至少在一定程度上保证数据授权的安全性情况下，有效提高区块链系统上数据授权的便捷性及高效性。

[0006] 根据本公开的一个方面，提供一种区块链系统的数据授权方法，所述区块链系统包括数据保存节点子网络以及与所述数据保存节点子网络中数据保存节点相连的数据授权节点，所述数据授权方法由所述数据授权节点执行，所述数据授权方法包括：

[0007] 当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；

[0008] 获取所述目标数据的预设加密密钥；

[0009] 将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；

[0010] 将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

[0011] 在本公开的一种示例性实施例中，所述当接收到目标数据的数据授权请求时，所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签，包括：

[0012] 利用信息授权节点的私钥解密所述目标数据的数据授权请求，得到所述目标数据的请求码及所述目标数据的预设公示标签。

[0013] 在本公开的一种示例性实施例中，所述获取所述目标数据的预设加密密钥，包括：

[0014] 从源数据库中，查询所述目标数据的预设公示标签；

[0015] 当查询到所述目标数据的预设公示标签，获取与所述目标数据的预设公示标签关联存储的预设加密密钥。

[0016] 在本公开的一种示例性实施例中，所述将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥，包括：

[0017] 获取所述数据授权请求所来源的数据请求方的第一区块节点码；

[0018] 获取所述数据授权节点的第二区块节点码；

[0019] 将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥。

[0020] 在本公开的一种示例性实施例中，所述将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥，包括：

[0021] 将所述第一区块节点码和所述第二区块节点码设置为函数系数；

[0022] 将所述目标数据的请求码和所述预设公示标签设置为函数解；

[0023] 将所述目标数据的预设加密密钥设置为函数值；

[0024] 进行算法拟合得到授权密钥。

[0025] 在本公开的一种示例性实施例中，在所述当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签之前，所述方法还包括：

[0026] 当检测到目标数据上传到所述数据保存节点，为所述目标数据添加预设公示标签；

[0027] 获取为所述目标数据事先设置的预设加密密钥；

[0028] 将所述预设公示标签和所述预设加密密钥关联存储。

[0029] 在本公开的一种示例性实施例中，在所述当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签之前，所述方法还包括：

[0030] 数据请求节点将所述目标数据的请求码及所述目标数据的预设公示标签利用信息授权节点的公钥加密，得到目标数据的数据授权请求；

[0031] 将所述目标数据的数据授权请求发送到数据授权节点。

[0032] 在本公开的一种示例性实施例中，将所述授权密钥发送到所述数据授权请求所来源的数据请求方，包括：

[0033] 将所述授权密钥利用所述所述数据授权请求所来源的数据请求方的公钥加密后，发送到所述数据授权请求所来源的数据请求方。

[0034] 在本公开的一种示例性实施例中，在将所述授权密钥利用所述所述数据授权请求所来源的数据请求方的公钥加密后，发送到所述数据授权请求所来源的数据请求方之后，还包括：

[0035] 利用数据请求方私钥解密所述公钥加密的授权密钥，得到授权密钥；

[0036] 从所述授权密钥中按照预设规则解析出所述预设加密密钥。

[0037] 在本公开的一种示例性实施例中，所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥，包括：

[0038] 触发对所述授权密钥的解析操作，得到解析指令输入界面；

[0039] 将所述所述目标数据的请求码以及所述预设公示标签输入所述解析指令输入界

面并进行确认，得到所述预设加密密钥。

[0040] 根据本公开的一个方面，提供一种区块链系统的数据授权装置，其特征在于，包括：

[0041] 接收模块，用于当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；

[0042] 获取模块，用于获取所述目标数据的预设加密密钥；

[0043] 打包模块，用于将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；

[0044] 发送模块，用于将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

[0045] 根据本公开的一个方面，提供一种计算机可读存储介质，其上存储有区块链系统的数据授权程序，其特征在于，所述区块链系统的数据授权程序被处理器执行时实现上述任一项所述的方法。

[0046] 根据本公开的一个方面，提供一种电子设备，其特征在于，包括：

[0047] 处理器；以及

[0048] 存储器，用于存储所述处理器的区块链系统的数据授权程序；其中，所述处理器配置为经由执行所述区块链系统的数据授权程序来执行上述任一项所述的方法。

[0049] 本公开一种区块链系统的数据授权方法及装置。首先，当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；通过获取数据请求方的数据授权请求中的预先发布的数据的预设公示标签，可以准确的查找到目标数据；以及获取数据请求方设置唯一作为验证码的目标数据的请求码，可以在后续步骤中进行数据加密。然后，获取所述目标数据的预设加密密钥；通过获取数据授权方对目标数据进行加密设置的预设加密密钥，可以实现预先将加密数据储存在区块链中，只向数据请求方传输预设加密密钥的便捷数据授权。然后，将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；这样可以有效保证向数据请求方传输预设加密密钥的安全性，进而有效保证数据授权的安全性。最后，将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据；这样可以实企业预先将加密数据保存在区块链上，根据用户需求便捷地、安全地传输数据密钥实现数据授权，有效提高数据授权的效率。

[0050] 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

[0051] 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。

[0052] 图1示意性示出一种区块链系统的数据授权方法的流程图。

[0053] 图2示意性示出一种区块链系统的数据授权方法的应用场景示例图。

[0054] 图3示意性示出一种授权密钥的打包方法流程图。

[0055] 图4示意性示出一种区块链系统的数据授权装置的方框图。

[0056] 图5示意性示出一种用于实现上述区块链系统的数据授权方法的电子设备示例框图。

[0057] 图6示意性示出一种用于实现上述区块链系统的数据授权方法的计算机可读存储介质。

具体实施方式

[0058] 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；相反，提供这些实施方式使得本公开将更加全面和完整，并将示例实施方式的构思全面地传达给本领域的技术人员。所描述的特征、结构或特性可以以任何合适的方式结合在一个或更多实施方式中。在下面的描述中，提供许多具体细节从而给出对本公开的实施方式的充分理解。然而，本领域技术人员将意识到，可以实践本公开的技术方案而省略所述特定细节中的一个或更多，或者可以采用其它的方法、组元、装置、步骤等。在其它情况下，不详细示出或描述公知技术方案以避免喧宾夺主而使得本公开的各方面变得模糊。

[0059] 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。

[0060] 本示例实施方式中首先提供了区块链系统的数据授权方法，其中，区块链系统包括数据保存节点子网络以及与该数据保存节点子网络中数据保存节点相连的数据授权节点，数据授权方法由数据授权节点执行。该区块链系统的数据授权方法可以运行于的服务器，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发明的方法，本示例性实施例中对此不做特殊限定。参考图1所示，该区块链系统的数据授权方法可以包括以下步骤：

[0061] 步骤S110，当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；

[0062] 步骤S120，获取所述目标数据的预设加密密钥；

[0063] 步骤S130，将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥；

[0064] 步骤S140，将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

[0065] 上述区块链系统的数据授权方法中。首先，首先，当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标

签;通过获取数据请求方的数据授权请求中的预先发布的数据的预设公示标签,可以准确的查找到目标数据;以及获取数据请求方设置唯一作为验证码的目标数据的请求码,可以在后续步骤中进行数据加密。然后,获取所述目标数据的预设加密密钥;通过获取数据授权方对目标数据进行加密设置的预设加密密钥,可以实现预先将加密数据储存在区块链中,只向数据请求方传输预设加密密钥的便捷数据授权。然后,将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签,按照预设打包算法打包为授权密钥;这样可以有效保证向数据请求方传输预设加密密钥的安全性,进而有效保证数据授权的安全性。最后,将所述授权密钥发送到所述数据授权请求所来源的数据请求方,以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后,解密保存在所述数据保存节点的所述目标数据;这样可以实企业预先将加密数据保存在区块链上,根据用户需求便捷地、安全地传输数据密钥实现数据授权,有效提高数据授权的效率。

[0066] 下面,将结合附图对本示例实施方式中上述区块链系统的数据授权方法中的各步骤进行详细的解释以及说明。

[0067] 在步骤S110中,当接收到目标数据的数据授权请求时,从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签。

[0068] 在本示例的实施方式中,参考图2所示,区块链授权节点上的服务器201接收到区块链网络中的数据请求节点上的服务器202发送的目标数据的数据授权请求时,从数据授权请求中获取目标数据的请求码及目标数据的预设公示标签,然后就可以在后续步骤中,由服务器201获取保存在数据保存节点服务器203中的目标数据的预设加密密钥。其中,服务器201、服务器202及服务器203可以是任何具有执行程序指令的、数据存储功能终端,例如手机、电脑、等,在此不做特殊限定。

[0069] 接收到区块链系统上的某个数据请求节点发送的目标数据的数据授权请求,该数据授权请求中至少包含目标数据的请求码及目标数据的预设公示标签。其中,目标数据请求码是数据需求方设置的唯一的请求码,只有数据请求方知道,可以在后续步骤中用于加密操作,目标数据请求码就可以作为唯一的密码,保证数据请求方请求到数据只有数据请求方可以获取,有效保证数据请求的安全性和数据请求方的权益。目标数据的预设公示标签是对区块链上存储的加密数据添加的用于表征每个数据的主旨、用途等作用的标签,可以让区块链上相关数据需求方进行目标数据的查询,有效保证数据查询的便捷性和准确性。在一种示例中,目标数据直接从应用系统通过接口写入区块链网络,确保写入区块链网络上的数据与自身应用系统的数据保持一致。

[0070] 在本示例的一种实施方式中,所述当接收到目标数据的数据授权请求时,从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签,包括:

[0071] 利用信息授权节点的私钥解密所述目标数据的数据授权请求,得到所述目标数据的请求码及所述目标数据的预设公示标签。

[0072] 通过数据请求节点将目标数据的请求码及目标数据的预设公示标签利用信息授权节点的公钥加密,得到目标数据的数据授权请求,然后发送到数据授权节点。信息授权节点的公钥是区块链上公知的,与信息授权节点的私钥对应。信息授权节点的公钥只有信息授权节点的私钥可以解密。这样可以保证目标数据的请求私密性与安全性。

[0073] 在步骤S120中,获取所述目标数据的预设加密密钥。

[0074] 在本示例的实施方式中，预设加密密钥是将应用数据进行加密后预先设置的密码，可以用该预设加密密钥解密加密的应用数据。将各种应用数据事先加密后，从应用系统通过接口写入区块链网络，确保写入区块链网络上的数据与自身应用系统的数据保持一致。进而在进行数据授权时只需要获取目标数据的预设加密密钥进行密码传送，就可以完成数据的授权，有效保证信息授权的便捷性。

[0075] 在本示例的一种实施方式中，所述获取所述目标数据的预设加密密钥，包括：

[0076] 从源数据库中，查询所述目标数据的预设公示标签；

[0077] 当查询到所述目标数据的预设公示标签，获取与所述目标数据的预设公示标签关联存储的预设加密密钥。

[0078] 通过查询所述目标数据的预设公示标签，就可以知道数据需求方需要的数据是否存储于数据存储节点，记录在数据授权节点。然后当查询到所述目标数据的预设公示标签，获取与所述目标数据的预设公示标签关联存储的预设加密密钥，可以准确地获取数据需求方需要的目标数据的预设密码，保证获取准确性。

[0079] 在步骤S130中，将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥。

[0080] 在本示例的实施方式中，将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥，也就是利用所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签形成只有数据需求方可以解密的授权密钥，通过解密授权密钥获取目标数据的预设加密密钥。目标数据的请求码是数据请求方唯一知道的请求码，目标数据的预设加密密钥是用来进行目标数据解密的密码，预设公示标签可以准确指示数据请求方需要获取的目标数据。进而可以按照预设打包算法，例如以只有数据请求方知道的请求码为解的算法包，也就是授权密钥。然后，在后续步骤中，将该授权密钥发送给数据请求方，这样通过数据加密机解密授权的方式完成数据的定向传递，保证企业的数据隐私，同时有效保证密码传输的安全性，进而有效提高数据授权的安全性和便捷性。

[0081] 在本示例的一种实施方式中，参考图3所示，所述将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥，包括：

[0082] 步骤S310，获取所述数据授权请求所来源的数据请求方的第一区块节点码；

[0083] 步骤S320，获取所述数据授权节点的第二区块节点码；

[0084] 步骤S330，将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥。

[0085] 区块节点码，就是区块链系统上为每个节点分配的节点码，例如阿拉伯数字或者应为代号等。通过获取数据授权请求所来源的数据请求方的第一区块节点码；获取数据授权节点的第二区块节点码，可以直接地将两个节点进行联系，因为节点码是唯一的；这样当数据请求方的应用系统需要的数据范围非常狭窄时，可以保证目标数据的直接传递，进而保证数据请求方的应用系统的安全性稳定性。然后将第一区块节点码、第二区块节点码、目标数据的请求码、目标数据的预设加密密钥以及预设公示标签进行算法拟合，可以得到点到点的授权密钥，只有数据请求方可以解密。

[0086] 在本示例的一种实施方式中，所述将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥，包括：

[0087] 将所述第一区块节点码和所述第二区块节点码设置为函数系数；

[0088] 将所述目标数据的请求码和所述预设公示标签设置为函数解；

[0089] 将所述目标数据的预设加密密钥设置为函数值；

[0090] 进行算法拟合得到授权密钥。

[0091] 这样就可以利用例如M＝10X+100Y的规则进行算法拟合，其中，M为将所述目标数据的预设加密密钥设置为函数值；X为目标数据的请求码设置为函数第一解；Y为预设公示标签设置为函数第二解；函数系数10为第一区块节点码；函数系数100为第二区块节点码。这样只有输入数据请求方设置的请求码以及需要的函数的标签才可以准确的得到需要的目标数据的预设加密密钥。这样可以实现预设密钥的点对点传输，有效保证密钥传输的安全性、准确性。

[0092] 在步骤S140中，将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

[0093] 在本示例的实施方式中，将授权密钥发送到数据授权请求所来源的数据请求方，数据请求方在接收到授权密钥，就可以利用区块链上预设规则解析出目标数据的加密密钥，然后数据请求方应用系统就可以从区块链的数据储存节点利用相关接口调用获取区块链网络上的数据，按照预设规则解密目标数据，实现数据的安全、便捷授权，使得数据的输出方与输入方都可以减少大量的人工操作，并且保证了数据在传递过程中的一致性。其中，将授权密钥发送到数据授权请求所来源的数据请求方是通过数据授权节点直接发送到数据请求方对应的数据请求节点上；预设规则是和上述预设打包算法相适应的解析规则，是该区块链系统上的公知规则，例如规定在解析密码是输入何种信息等。进一步的，在一种示例中，将授权密钥发送到数据授权请求所来源的数据请求方，也可以是通过数据授权节点在区块链上进行广播，以实现将授权密钥发送到数据授权请求所来源的数据请求方。

[0094] 在本示例的一种实施方式中，将所述授权密钥发送到所述数据授权请求所来源的数据请求方，包括：

[0095] 将所述授权密钥利用所述所述数据授权请求所来源的数据请求方的公钥加密后，发送到所述数据授权请求所来源的数据请求方。

[0096] 数据请求方的公钥是区块链上公知的，与数据请求方的私钥对应，数据请求方的公钥只有数据请求方的私钥可以解密；这样将所述授权密钥利用所述所述数据授权请求所来源的数据请求方的公钥加密后，发送到所述数据授权请求所来源的数据请求方，可以保证授权密钥传输的安全性。

[0097] 在本示例的一种实施方式中，在将所述授权密钥利用所述所述数据授权请求所来源的数据请求方的公钥加密后，发送到所述数据授权请求所来源的数据请求方之后，还包括：

[0098] 利用数据请求方私钥解密所述公钥加密的授权密钥，得到授权密钥；

[0099] 从所述授权密钥中按照预设规则解析出所述预设加密密钥。

[0100] 数据请求方的公钥是区块链上公知的，与数据请求方的私钥对应，数据请求方的公钥只有数据请求方的私钥可以解密，这样可以保证授权密钥只有数据请求方利用私钥解密加密公钥后进行获取，然后，就可以从所述授权密钥中按照预设规则解析出预设加密密钥。

[0101] 在本示例的一种实施方式中，所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥，包括：

[0102] 触发对所述授权密钥的解析操作，得到解析指令输入界面；

[0103] 将所述所述目标数据的请求码以及所述预设公示标签输入所述解析指令输入界面并进行确认，得到所述预设加密密钥。

[0104] 通过对接收到授权密钥的点击等操作的触发，对授权密钥进行解析，自动弹出用于解析指令输入的界面，然后输入目标数据的请求码以及所述预设公示标签就可以直接解析出预设加密密钥。

[0105] 在本示例的一种实施方式中，在所述当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签之前，所述方法还包括：

[0106] 当检测到目标数据上传到所述数据保存节点，为所述目标数据添加预设公示标签；

[0107] 获取为所述目标数据事先设置的预设加密密钥；

[0108] 将所述预设公示标签和所述预设加密密钥关联存储。

[0109] 将所述预设公示标签和所述预设加密密钥关联存储，可以准确的根据数据请求方的目标数数据的标签进行目标数据是否存在的验证，同时准确地获取目标数据的预设加密密钥。

[0110] 在本示例的一种实施方式中，在所述当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签之前，所述方法还包括：

[0111] 数据请求节点将所述目标数据的请求码及所述目标数据的预设公示标签利用信息授权节点的公钥加密，得到目标数据的数据授权请求；

[0112] 将所述目标数据的数据授权请求发送到数据授权节点。

[0113] 信息授权节点的公钥是区块链上公知的，与信息授权节点的私钥对应，信息授权节点的公钥只有信息授权节点的私钥可以解密。将目标数据的请求码及目标数据的预设公示标签利用信息授权节点的公钥加密，就可以将公钥加密后得到的数据授权请求，发送给数据授权节点，优数据授权节点的私钥解密，这样可以保证目标数据的请求私密性和安全性。

[0114] 本公开还提供了一种区块链系统的数据授权装置。参考图4所示，该区块链系统的数据授权装置可以包括接收模块410、获取模块420、打包模块430以及发送模块440。其中：

[0115] 接收模块410可以用于当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签；

[0116] 获取模块420可以用于获取所述目标数据的预设加密密钥；

[0117] 打包模块430可以用于将所述目标数据的请求码、所述目标数据的预设加密密钥

以及所述预设公示标签，按照预设打包算法打包为授权密钥；

[0118] 发送模块440可以用于将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据。

[0119] 上述区块链系统的数据授权装置中各模块的具体细节已经在对应的区块链系统的数据授权方法中进行了详细的描述，因此此处不再赘述。

[0120] 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。

[0121] 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。

[0122] 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。

[0123] 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。

[0124] 所属技术领域的技术人员能够理解，本发明的各个方面可以实现为系统、方法或程序产品。因此，本发明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”。

[0125] 下面参照图5来描述根据本发明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，不应对本发明实施例的功能和使用范围带来任何限制。

[0126] 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。

[0127] 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发明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：当接收到区块链网络中的目标节点发送的目标数据获取请求时，从所述目标数据获取请求中获取目标数据信息；S120：根据所述目标数据信息进行企业资源计划系统中源数据适配，得到预写入数据；步骤S130：判断所述预写入数据中是否存在预定权限数据；步骤S140：当所述预写入数据中不存在预定权限数据时，将所述预写入数据写入所述区块链网络中的所述目标节点。

[0128] 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。

[0129] 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。

[0130] 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。

[0131] 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。

[0132] 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。

[0133] 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,本发明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发明各种示例性实施方式的步骤。

[0134] 参考图6所示,描述了根据本发明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,本发明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。

[0135] 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。

[0136] 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。

[0137] 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。

[0138] 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发明操作的程序代码，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”语言或类似的程序设计语言。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)。

[0139] 此外，上述附图仅是根据本发明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。

[0140] 本领域技术人员在考虑说明书及实践这里公开的发明后，将容易想到本公开的其他实施例。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。说明书和实施例仅被视为示例性的，本公开的真正范围和精神由权利要求指出。

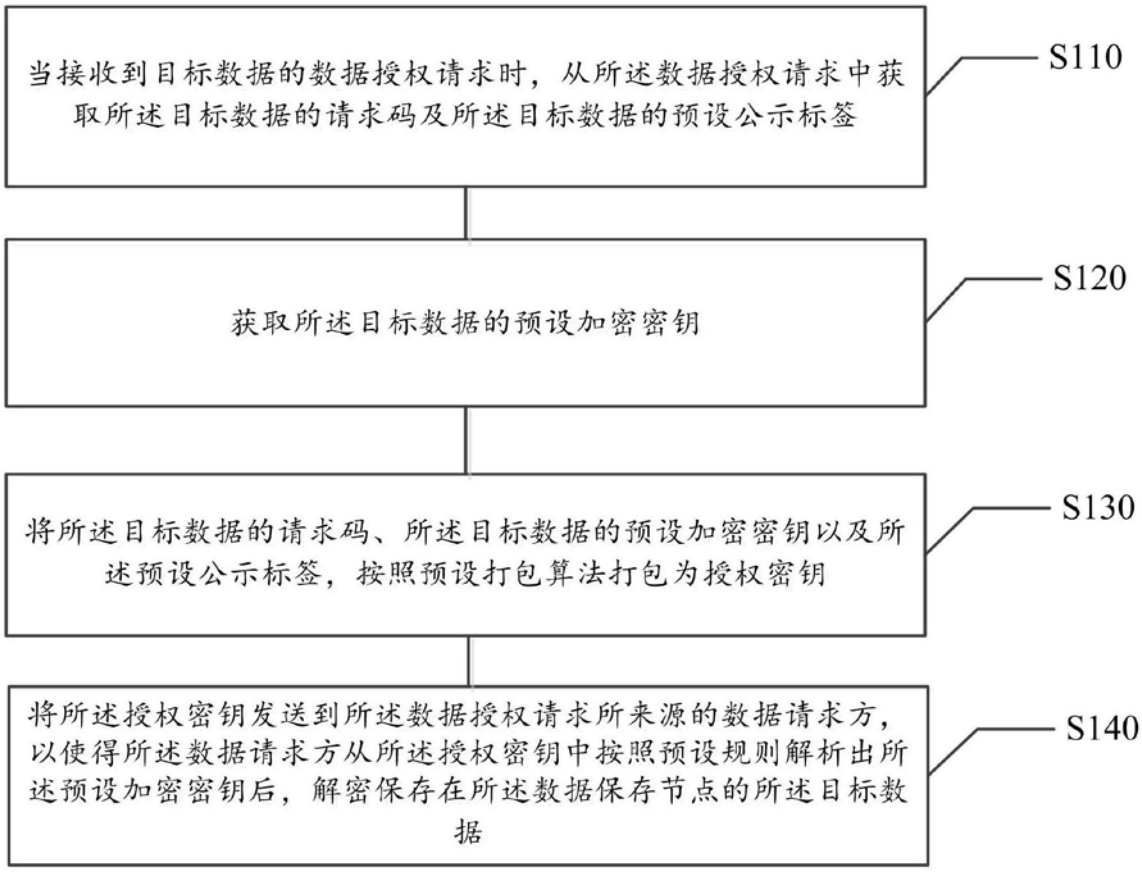

当接收到目标数据的数据授权请求时，从所述数据授权请求中获取所述目标数据的请求码及所述目标数据的预设公示标签
S110
获取所述目标数据的预设加密密钥
S120
将所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签，按照预设打包算法打包为授权密钥
S130
将所述授权密钥发送到所述数据授权请求所来源的数据请求方，以使得所述数据请求方从所述授权密钥中按照预设规则解析出所述预设加密密钥后，解密保存在所述数据保存节点的所述目标数据
S140

图1

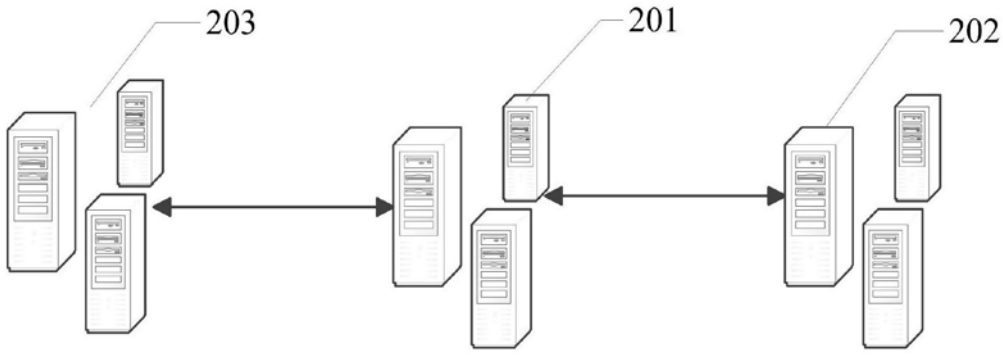

203
201
202

图2

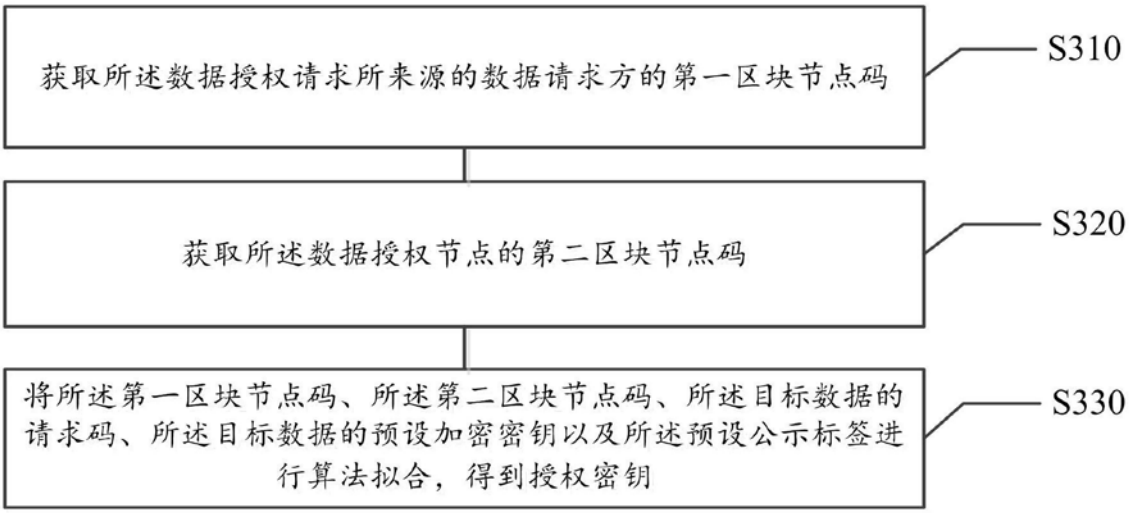

获取所述数据授权请求所来源的数据请求方的第一区块节点码
S310
获取所述数据授权节点的第二区块节点码
S320
将所述第一区块节点码、所述第二区块节点码、所述目标数据的请求码、所述目标数据的预设加密密钥以及所述预设公示标签进行算法拟合，得到授权密钥
S330

图3

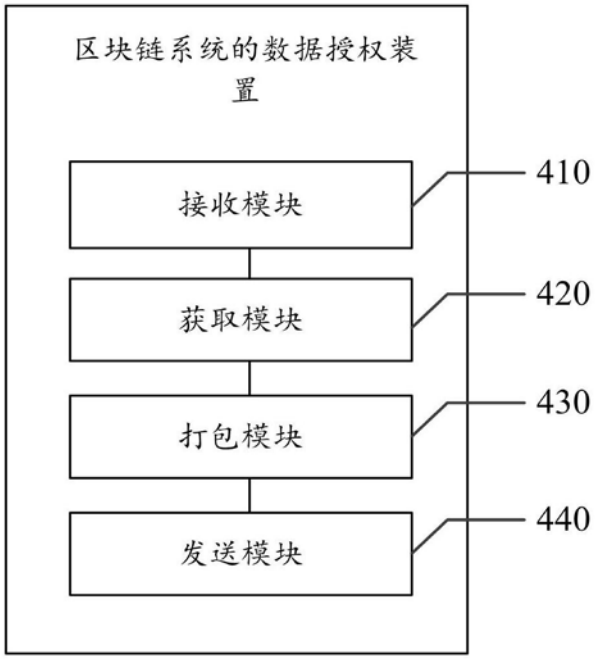

区块链系统的数据授权装置
接收模块
410
获取模块
420
打包模块
430
发送模块
440

图4

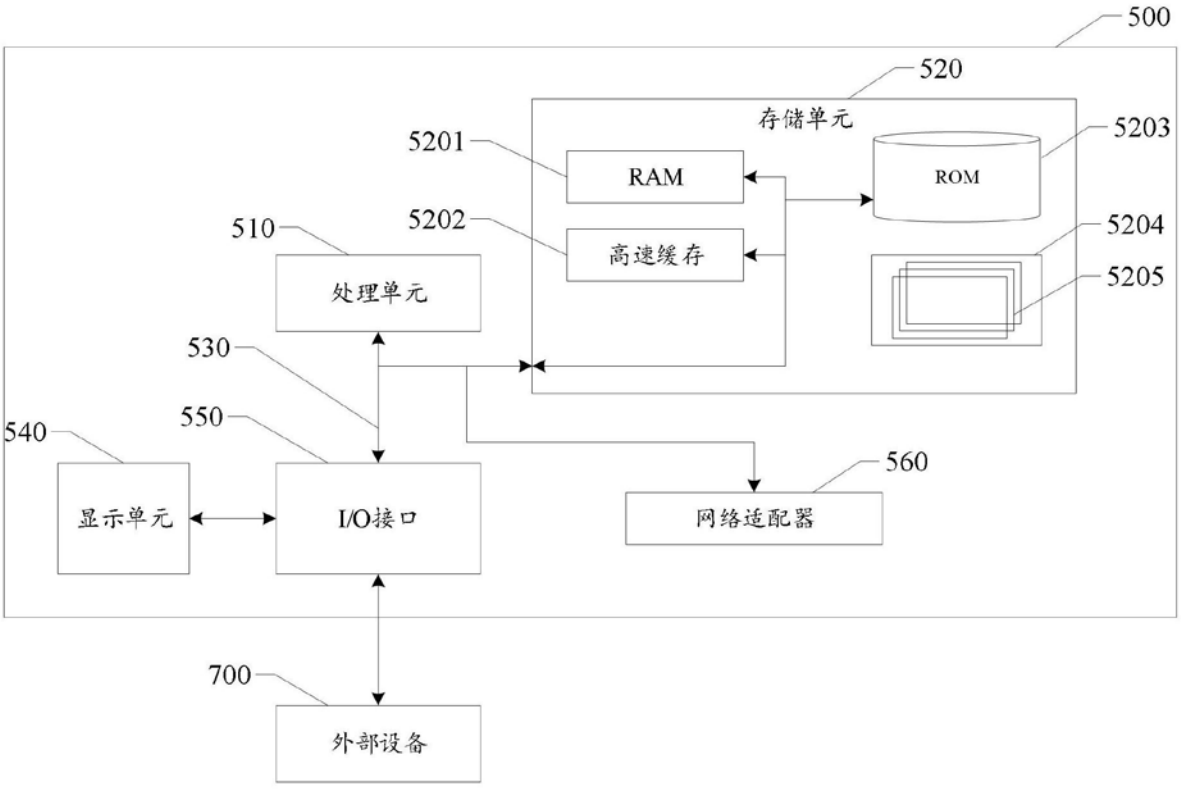

500
520
存储单元
5201
RAM
5203
ROM
5202
高速缓存
5204
5205
510
处理单元
530
550
540
560
显示单元
I/O接口
网络适配器
700
外部设备

图5

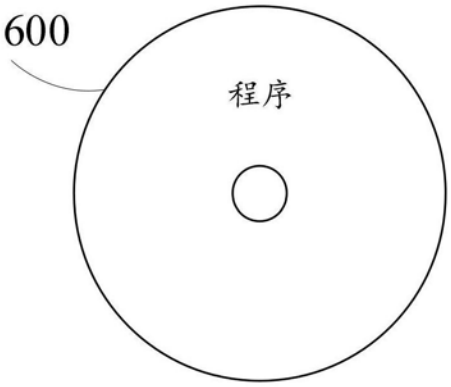

600
程序

图6