



(12)发明专利申请

(10)申请公布号 CN 109714348 A

(43)申请公布日 2019. 05. 03

(21)申请号 201811644077.7

(22)申请日 2018.12.29

(71)申请人 百度在线网络技术(北京)有限公司

地址 100085 北京市海淀区上地十街10号

百度大厦三层

(72)发明人 段兵 肖伟 谭待

(74)专利代理机构 北京品源专利代理有限公司

11332

代理人 孟金喆

(51)Int.Cl.

H04L 29/06(2006.01)

G06F 21/31(2013.01)

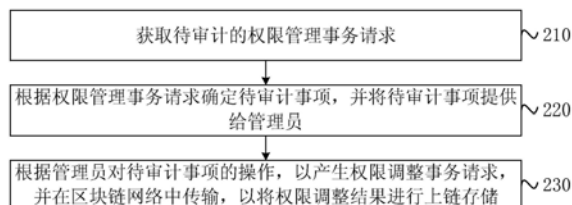
权利要求书2页 说明书13页 附图5页

(54)发明名称

基于区块链实现的权限处理方法、装置、设备和介质

(57)摘要

本发明实施例公开了一种基于区块链实现的权限处理方法、装置、设备和介质。该方法包括：获取待审计的权限管理事务请求；根据所述权限管理事务请求确定待审计事项，并将所述待审计事项提供给管理员；根据所述管理员对待审计事项的操作，以产生权限调整事务请求，并在区块链网络中传输，以将权限调整结果进行上链存储。本发明实施例通过区块链对权限数据的统一管控，为管理员提供了权限审计依据；同时区块链网络中的任一节点均可以为管理员提供权限审计操作的入口，将权限审计工作分散并行处理，优化了权限处理方式，提高权限处理过程中的审计效率和公信力。



1. 一种基于区块链实现的权限处理方法,其特征在于,应用于区块链节点,所述方法包括:

获取待审计的权限管理事务请求;

根据所述权限管理事务请求确定待审计事项,并将所述待审计事项提供给管理员;

根据所述管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

2. 根据权利要求1所述的方法,其特征在于,所述获取待审计的权限管理事务请求,包括:

根据用户或管理员对权限智能合约的操作,产生权限管理事务请求;或

接收其他区块链节点发送的权限管理事务请求,所述权限管理事务请求基于权限智能合约产生。

3. 根据权利要求1所述的方法,其特征在于,所述将所述待审计事项提供给管理员,包括:

将所述待审计事项以可视化界面的方式提供给管理员。

4. 根据权利要求1所述的方法,其特征在于,所述根据所述管理员对待审计事项的操作,以产生权限调整事务请求,包括:

获取所述管理员对待审计事项操作而输入的审计结果参数;

根据权限智能合约和所述审计结果参数,产生权限调整事务请求。

5. 根据权利要求1-4中任一项所述的方法,其特征在于,在所述根据所述管理员对待审计事项的操作,以产生权限调整事务请求的同时或之后,还包括:

获取所述管理员的身份标识和签名密钥,对所述权限调整事务请求进行身份签名。

6. 根据权利要求1-4中任一项所述的方法,其特征在于,还包括:

如果接收到其他区块链节点发送的权限调整事务请求,从所述权限调整事务请求中获取管理员的身份标识;

在本地区块链中获取预先声明为管理员的身份标识和签名密钥;

根据本地获取的签名密钥对所述权限调整事务请求进行验证;

在验证通过后,接受所述权限调整事务请求。

7. 根据权利要求6所述的方法,其特征在于,还包括:

获取管理员权限声明事务请求,根据所述管理员权限声明事务请求将至少一个管理员的身份标识和签名密钥在区块链中进行存储。

8. 根据权利要求1-4中任一项所述的方法,其特征在于,在所述将权限调整结果进行上链存储之后,还包括:

根据权限调整结果更新区块链本地存储的权限管理表,其中,所述权限管理表中包括用户的身份角色和身份角色对应的权限。

9. 根据权利要求8所述的方法,其特征在于,还包括:

获取应用功能事务请求;

如果所述应用功能事务请求存在用户身份权限的鉴权需求,则在本地存储的权限管理表中进行鉴权,或发起鉴权事务请求,以请求其他区块链节点进行鉴权;

获取鉴权结果,根据鉴权结果处理所述应用功能事务请求。

10. 根据权利要求9所述的方法,其特征在于,在所述获取鉴权结果之后,还包括:

将基于鉴权结果处理的所述应用功能事务请求的信息,作为鉴权记录,对应于用户记录到所述权限管理表中。

11. 根据权利要求1所述的方法,其特征在于,还包括:

接收用户发起的权限管理信息查询请求,在本地的权限管理表中查询并反馈,或请求其他区块链节点进行查询并反馈。

12. 一种基于区块链实现的权限处理装置,其特征在于,配置于区块链节点,所述装置包括:

权限管理事务请求获取模块,用于获取待审计的权限管理事务请求;

待审计事项确定模块,用于根据所述权限管理事务请求确定待审计事项,并将所述待审计事项提供给管理员;

权限调整模块,用于根据所述管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

13. 一种设备,其特征在于,包括:

一个或多个处理器;

存储器,用于存储一个或多个程序;

当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现如权利要求1-11中任一项所述的基于区块链实现的权限处理方法。

14. 一种计算机可读存储介质,其上存储有计算机程序,其特征在于,该程序被处理器执行时实现如权利要求1-11中任一项所述的基于区块链实现的权限处理方法。

基于区块链实现的权限处理方法、装置、设备和介质

技术领域

[0001] 本发明实施例涉及区块链的数据处理技术领域,尤其涉及一种基于区块链实现的权限处理方法、装置、设备和介质。

背景技术

[0002] 随着区块链技术的普及,去中心化的分散式应用程序(Decentralized Application,DApp)的落地场景也越来越多,例如基于区块链的版权登记系统,基于区块链的资产交换系统等。在各种DApp的运行过程中,大多会遇到需要控制用户身份权限的需求,且每种不同的身份具有不同的操作权限。其中,操作权限可以是指操作不同智能合约的权限、或操作不同数据的权限等。

[0003] 但是,目前市场上的DApp普遍面临一个问题,即权限审计中心化。DApp中各个用户需要向中心化的服务器进行身份注册、申请更改身份或更改权限等,管理权限的管理员需要通过中心化服务器对各种身份或权限的调整请求进行审计,从而确定是否可进行授权等权限调整操作。

[0004] 然而,现有技术的中心化权限处理模式中,管理员需要基于海量数据来进行审计判断,同时需要审计大量的权限调整请求,所以审计效率较低,无法满足快速审计的应用场景。

发明内容

[0005] 本发明实施例提供了一种基于区块链实现的权限处理方法、装置、设备和介质,以优化权限处理方式,提高权限处理过程中的审计效率。

[0006] 第一方面,本发明实施例提供了一种基于区块链实现的权限处理方法,应用于区块链节点,所述方法包括:

[0007] 获取待审计的权限管理事务请求;

[0008] 根据所述权限管理事务请求确定待审计事项,并将所述待审计事项提供给管理员;

[0009] 根据所述管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

[0010] 第二方面,本发明实施例提供了一种基于区块链实现的权限处理装置,配置于区块链节点,所述装置包括:

[0011] 权限管理事务请求获取模块,用于获取待审计的权限管理事务请求;

[0012] 待审计事项确定模块,用于根据所述权限管理事务请求确定待审计事项,并将所述待审计事项提供给管理员;

[0013] 权限调整模块,用于根据所述管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

[0014] 第三方面,本发明实施例提供了一种设备,包括:

[0015] 一个或多个处理器；

[0016] 存储器,用于存储一个或多个程序；

[0017] 当所述一个或多个程序被所述一个或多个处理器执行,使得所述一个或多个处理器实现本发明任意实施例所述的基于区块链实现的权限处理方法。

[0018] 第四方面,本发明实施例提供了一种计算机可读存储介质,其上存储有计算机程序,该程序被处理器执行时实现本发明任意实施例所述的基于区块链实现的权限处理方法。

[0019] 本发明实施例通过获取权限管理事务请求,并传输至区块链网络中,区块链节点根据权限管理事务请求确定待审计事项,并将待审计事项提供给管理员,以使区块链网络中的至少一个具有管理员身份的节点依据管理员的操作结果,生成权限调整事务请求,并传输至区块链网络中,以对权限进行调整并将权限调整结果写入区块链中。本发明实施例通过区块链对权限数据的统一管控,为管理员提供了权限审计依据;同时区块链网络中的任一节点均可管理员提供权限审计操作的入口,优化了权限处理方式,提高权限处理过程中的审计效率和公信力。

附图说明

[0020] 图1为本发明实施例提供的DApp的结构框图；

[0021] 图2为本发明实施例一提供的一种基于区块链实现的权限处理方法的流程图；

[0022] 图3为本发明实施例二提供的一种基于区块链实现的权限处理方法的流程图；

[0023] 图4为本发明实施例三提供的验证权限调整事务请求的流程图；

[0024] 图5为本发明实施例四提供的鉴权用户身份权限的流程图；

[0025] 图6为本发明实施例五提供的一种基于区块链实现的权限处理装置的结构示意图；

[0026] 图7为本发明实施例六提供的一种设备的结构示意图。

具体实施方式

[0027] 为清楚介绍实施例的技术方案,首先介绍区块链网络中轻量级节点的实现方式。

[0028] 轻量级节点是未存储或存储部分区块数据和事务数据的区块链网络节点。图1中配置于终端设备110的轻量级节点提供了上层交互接口,用于通过上层交互接口与应用程序客户端进行数据交互。轻量级节点可以通过软件实现功能,集成于操作系统中。上层交互接口可以是轻量级节点直接与客户端交互的接口,也可以是通过操作系统配置的接口。

[0029] 其中,上层交互接口可以从应用程序客户端获取客户端交互数据。示例性地,客户端交互数据可以是用户触发应用程序客户端的功能选项所产生的相应的功能需求数据;还可以是应用程序客户端接收到终端设备110中的其他应用程序或者接收到其他终端设备所传输的功能需求数据。其中,功能需求数据可以理解为涉及区块链网络的各控制指令以及涉及实体数据的事务请求。

[0030] 配置于终端设备110的轻量级节点还提供了网络交互接口,用于通过网络交互接口与区块链网络中其他区块链网络节点130进行数据交互。

[0031] 其中,客户端交互数据与区块链网络节点交互数据相关联。示例性地,区块链网络

节点交互数据可以是客户端交互数据;还可以是将客户端交互数据转化为区块链网络可传输形式的客户端交互数据关联数据;还可以是基于客户端交互数据或客户端交互数据关联数据所接收的区块链网络所反馈的数据。

[0032] 需要说明的是,轻量级节点可以加载在终端设备110的操作系统中,以通过终端设备110的驱动程序直接驱动诸如CPU、存储设备、网络通信设备等硬件来实现相应的功能;轻量级节点还可以作为一个独立的第三方应用程序安装到终端设备110中,通过该第三方应用程序的运行实现相应的功能。

[0033] 由于轻量级节点部署有区块链的部署数据,因此可以参与区块链的事务请求交互过程,但并不存储所有区块数据,当轻量级节点需要查询区块内事务数据时,可以实时向其他节点获取,并采取设定方式进行验证。

[0034] 本发明实施例中,将基于角色的权限访问控制模型(Role-Based Access Control, RBAC)应用于DApp中,通过智能合约对RBAC模型进行去中心化处理,作为其他DApp的访问控制模块,为管理员提供权限审计依据,提高用户权限的审计效率。具体的, RBAC模型以用户、角色以及权限为管理基础,其中,权限与角色相关联,角色是为了完成各种工作而创造,角色可以视为一系列权限的集合,是权限分配的单位与载体。进而用户通过申请成为适当的角色成员,从而获得该角色所关联的权限。用户则依据自身的责任和资格来被指派相应的角色,用户可以很容易地从一个角色被指派到另一个角色。角色可依新的需求和系统的合并而赋予新的权限,而权限也可根据需要而从某角色中回收。

[0035] 本发明实施例中,通过智能合约对用户、角色以及权限进行处理,并将处理流程和处理结果保存在区块链中。

[0036] 下面结合附图和实施例对本发明实施例作进一步的详细说明。可以理解的是,此处所描述的具体实施例仅仅用于解释本发明实施例,而非对本发明的限定。另外还需要说明的是,为了便于描述,附图中仅示出了与本发明实施例相关的部分而非全部结构。

[0037] 实施例一

[0038] 图2为本发明实施例一提供的一种基于区块链实现的权限处理方法的流程图,本实施例可适用于调整权限的情况,特别适合在某个业务功能的DApp的运行过程中,进行用户权限的调整控制。该方法可由一种基于区块链实现的权限处理装置来执行,该装置可以采用软件和/或硬件的方式实现,优选是配置于区块链节点中,可以是常规区块链节点,也可以是轻量级区块链节点。该方法具体包括如下步骤:

[0039] S210、获取待审计的权限管理事务请求。

[0040] 在本发明具体实施例中,依据DApp的应用场景不同,角色以及角色所关联的权限可能存在不同。其中,角色可以依据其分工或责任而创建或命名,并赋予对应的权限,权限可以包括基本的读权限、写权限以及应用相关的各种权限等。

[0041] 本实施例中,权限管理事务请求可以由用户发起的、或管理员发起的、或由于业务能够运行的需求而发起的,用于触发区块链节点,告知管理员进行权限审计。权限管理事务请求可以包括角色的注册、撤销或更改,以及角色中各种权限的新增、删除或更改等。

[0042] 在区块链网络中,部分或全部区块链节点均可提供管理员操作界面和用户操作界面。管理员即用户权限审计的特定工作人员,用于基于区块链网络以及本地存储的权限处理数据,对用户权限进行审核,确定用户需求是否通过,从而对用户权限进行调整或对用户

享有的应用功能进行限制。其中,权限处理数据可以全部或部分的同步于区块链中,也可以部分的同步于各区块链节点的本地存储空间中。权限处理数据可以包括用户ID、所处理的权限内容、处理时间、处理用户、权限调整发起者以及处理结果等。

[0043] 示例性的,假设用户想要申请注册某一角色,则该用户可以通过DApp,基于用户交互界面,对DApp中预先部署的权限智能合约进行操作,产生权限管理事务请求,从而区块链节点接收到该权限管理事务请求,等待进行审计。

[0044] S220、根据权限管理事务请求确定待审计事项,并将待审计事项提供给管理员。

[0045] 在本发明具体实施例中,区块链节点可以对权限管理事务请求进行信息提取,以确定待审计事项,即管理员所要审核的权限处理相关信息。其中,根据权限管理事务请求的发起者不同,待审计事项也可能不同。待审计事项可以包括角色的注册、撤销或更改,或者可以包括角色中各种权限的新增、删除或更改,相应的,待审计事项还可以包括发起者用户ID或所要调整权限的用户ID。

[0046] 本实施例中,区块链网络中各个区块链节点均可以提供管理员交互界面,但是未必每个区块链节点都有管理员在操作。可以通过配置管理员的登录账号,来处理管理员交互界面,避免非管理员的随意操作。

[0047] 有管理员控制的区块链节点,可以通过区块链节点获知权限审计需求。可选的,可以将待审计事项以可视化界面的方式进行呈现,以及时告知节点的管理员进行权限审计。从而管理员可以在区块链网络中的任意一个节点上进行审计操作,或者多个管理员在不同的节点上一起对海量的权限管理事务请求进行操作,避免权限审计中心化服务的瓶颈,其中,还可以将权限审计工作分散到多个节点上处理,提高了权限审计效率。

[0048] 示例性的,在上述示例中,区块链节点对权限管理事务请求进行信息提取,将用户ID及其所要注册的角色确定为待审计事项,并以弹窗的形式对管理员进行审计事项通知,由管理员对弹窗进行回应,可以通过输入管理员身份和密码进入审计界面,获取待审计事项的具体内容,并结合区块链中存储的该用户ID的相关历史数据以及本地存储中该用户ID的历史数据,对待审计事项进行审核处理。

[0049] S230、根据管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

[0050] 在本发明具体实施例中,管理员对待审计事项的操作可以是指,管理员通过交互界面将待审计事项的审计结果进行上传或添加操作等,其中审计结果可以包括审核是否通过或权限调整具体事宜等。从而区块链节点根据审计结果,生成权限调整事务请求,并传输至区块链网络中,由区块链网络中的节点依据权限调整事务请求进行权限调整,并将权限调整结果进行上链存储。

[0051] 具体的,权限调整结果可以包括用户ID、所调整权限、调整时间、权限调整的发起者以及权限调整的具体结果等信息。其中,可以将用户ID、所调整权限、调整时间以及权限调整的发起者等能够标识权限调整事务的信息作为一条记录进行链上存储,而对于权限调整的具体结果等详细信息进行链下存储,保存并同步到节点的本地存储空间中。进而通过链上信息的存储,保证了权限调整相关信息的公信力,同时通过链下信息的存储,保证了节点本地存储中同步有依据链上信息而产生的详细信息,从而节省了链上存储空间占用,以及数据在区块链网络中传输时网络资源的占用,提升了数据的传输效率和数据处理效率。

[0052] 可选的,在根据管理员对待审计事项的操作,以产生权限调整事务请求的同时或之后,还包括:获取管理员的身份标识和签名密钥,对权限调整事务请求进行身份签名。

[0053] 本实施例中,为了防止非管理员身份的用户对待审计事项的恶意审计,防止用户权限的任意调整,区块链节点在产生权限调整事务请求的同时或之后,可以对权限调整事务请求进行数字签名,以标明权限调整事务请求的发起者为管理员。具体的,在区块链网络中,管理员具有全局唯一的身份标识和签名密钥,其中,签名密钥包括私钥和公钥,私钥只有管理员本身拥有,而管理员的身份标识和公钥可以是预先在区块链中进行声明。管理员的身份标识和公钥可以保存在区块链中,也可以保存在节点的本地存储中。从而区块链节点在根据管理员对待审计事项的操作产生权限调整事务请求的同时或之后,可以通过获取管理员的身份标识和私钥,对权限调整事务请求进行身份签名,而后再在区块链网络中传输。其中,可以通过管理员登录时的ID来获取管理员的身份标识和签名密钥,也可以在管理员对待审计事项进行操作的同时上传信息,来获取管理员的身份标识和签名密钥。

[0054] 相应的,在权限调整事务请求传输至区块链中时,区块链中的节点可以通过从区块链或本地存储中获取管理员的身份标识和公钥,对权限调整事务请求进行身份验证,从而接收权限调整事务请求。

[0055] 本实施例的技术方案,通过获取权限管理事务请求,并传输至区块链网络中,区块链节点根据权限管理事务请求确定待审计事项,并将待审计事项提供给管理员,以使区块链网络中的至少一个具有管理员身份的节点依据管理员的操作结果,生成权限调整事务请求,并传输至区块链网络中,以对权限进行调整并将权限调整结果写入区块链中。本发明实施例通过区块链对权限数据的统一管控,为管理员提供了权限审计依据;同时区块链网络中的任一节点均具有供管理员进行权限审计操作的入口,优化了权限处理方式,提高权限处理过程中的审计效率和公信力。

[0056] 实施例二

[0057] 本实施例在上述实施例一的基础上,提供了基于区块链实现的权限处理方法的一个优选实施方式,能够依据管理员的权限审计结果进行权限调整。图3为本发明实施例二提供的一种基于区块链实现的权限处理方法的流程图,如图3所示,该方法包括以下具体步骤:

[0058] S310、获取待审计的权限管理事务请求。

[0059] 在本发明具体实施例中,权限管理事务请求可以是意图申请权限的用户发起的,也可以是意图调整权限的管理员发起的。权限管理事务请求可以由区块链节点本身产生,也可以由其他区块链节点产生,并接收其他区块链节点产生的权限管理事务请求。

[0060] 可选的,根据用户或管理员对权限智能合约的操作,产生权限管理事务请求。

[0061] 本实施例中,权限智能合约预先部署于区块链中,用于限制用户权限的处理规则。在各个区块链节点中,可以调用权限智能合约的交互界面,为用户或管理员提供需求的输入。从而区块链节点可以根据用户或管理员对权限智能合约的操作,产生权限管理事务请求。其中,权限管理事务请求中可以不包括权限智能合约的全部代码,以减少数据传输对于网络资源的占用。相应的,接收到权限管理事务请求的区块链节点可以从本地调用权限智能合约的代码,依据权限管理事务请求包括的参数,来执行权限智能合约,实现权限的调整。

[0062] 可选的,接收其他区块链节点发送的权限管理事务请求,所述权限管理事务请求基于权限智能合约产生。

[0063] 本实施例中,区块链节点也可以接收其他区块链节点发送的权限管理事务请求。该权限管理事务请求同样基于区块链中预先部署的权限智能合约而生成的。而其他区块链节点的权限管理事务请求不受限制,同样可以是用户发起的,也可以是管理员发起的。

[0064] S320、根据权限管理事务请求确定待审计事项,并将待审计事项提供给管理员。

[0065] S330、获取管理员对待审计事项操作而输入的审计结果参数。

[0066] 在本发明具体实施例中,管理员作为权限审计的工作人员,在接收到待审计事项之后,可以通过待审计事项中包括的用户信息,从区块链中获取该用户的历史权限记录,也可以从区块链节点本地存储中获取该用户的历史权限审计流程和审计结果,从而在区块链提供的审计证据的基础上,对本次待审计事项进行审核,得到审计结果参数。

[0067] 具体的,管理员可以根据历史权限记录、历史权限审计流程和审计结果,对待审计事项的合理性、一致性以及安全性等各方面进行审核。例如是否存在恶意申请历史、是否存在重复注册历史,以及历史记录中是否存在欺骗、盗用等违规行为等。从而生成审计结果构成审计结果参数,审计结果参数可以包括审核是否通过,还可以包括权限调整方案等。最终管理员可以通过交互界面将待审计事项的审计结果进行上传或添加操作,由区块链节点获得该审计结果参数。

[0068] 其中,对于待审计事项的审核可以由区块链网络中任意一个管理员执行的。也可以由区块链网络中的多个管理员同时执行的,基于不同管理员的审核结果得到最终一致的审计结果参数,从而避免了中心化的服务。还可以是将待审计事项分散给多个管理员同时并行执行的,从而大大提高了待审计事项的审核效率。当多个管理员并行审计时,可以结合采用区块链的共识机制来确定审计结果,例如,相同审计结果的比例或绝对值达到设定条件就接受该审计结果。

[0069] S340、根据权限智能合约和审计结果参数,产生权限调整事务请求。

[0070] 在本发明具体实施例中,区块链节点可以依据审计结果参数执行智能合约,从而生成权限调整事务请求,用于指示区块链中进行用户权限的调整。其中,该权限智能合约与上述生成权限管理事务请求的权限智能合约可以相同,也可以不同。该权限智能合约同样预先部署于区块链中,用于限制用户权限的处理规则。

[0071] 具体的,权限智能合约中可以包括生成至少一个权限相关事务请求的执行代码。其中,若权限智能合约中可以仅包括生成一个权限相关事务请求的执行代码,则生成权限调整事务请求的权限智能合约中可以仅包括生成权限调整事务请求的一段执行代码,而上述生成权限管理事务请求的权限智能合约中可以仅包括生成权限管理事务请求的另一段执行代码。因此上述两个权限智能合约为不同的合约内容。此外,若权限智能合约中可以包括生成所有权限相关事务请求的执行代码,即权限智能合约中同时包括了生成上述两种请求的两段执行代码,则上述两个权限智能合约为相同的合约内容。

[0072] S350、获取管理员的身份标识和签名密钥,对权限调整事务请求进行身份签名。

[0073] 本发明具体实施例中,为了防止非管理员身份的用户对权限调整事务请求的模仿,防止用户权限的任意调整,因此对权限调整事务请求进行身份签名,为权限调整事务请求的验证提供依据。相应的,权限调整事务请求中可以包括管理员的身份标识以及数字签

名信息。

[0074] 本实施例的技术方案,通过获取用户或管理员等进行权限调整而发起的权限管理事务请求,并传输至区块链网络中,区块链节点根据权限管理事务请求确定待审计事项,并将待审计事项提供给管理员,以使区块链网络中的至少一个具有管理员身份的节点依据管理员的操作结果,生成权限调整事务请求,并传输至区块链网络中,以对权限进行调整并将权限调整结果写入区块链中。本发明实施例通过区块链对权限数据的统一管控,为管理员提供了权限审计依据;同时区块链网络中的任一节点均能提供管理员进行权限审计操作的入口,将权限审计工作分散并行处理,优化了权限处理方式,提高权限处理过程中的审计效率和公信力。

[0075] 实施例三

[0076] 本实施例在上述实施例二的基础上,提供了基于区块链实现的权限处理方法的一个优选实施方式,能够对区块链网络中传输的权限调整事务请求进行验证。图4为本发明实施例三提供的验证权限调整事务请求的流程图,如图4所示,该方法包括以下具体步骤:

[0077] S410、如果接收到其他区块链节点发送的权限调整事务请求,从权限调整事务请求中获取管理员的身份标识。

[0078] 在本发明具体实施例中,在区块链节点接收到其他区块链节点发送的权限调整事务请求后,为了确保该事务请求是由管理员发起的,且确保该权限调整是真实所需的,因此区块链节点可以对权限调整事务请求进行数字签名的验证。具体的,首先对权限调整事务请求进行信息提取,从权限调整事务请求中获取管理员的身份标识。

[0079] S420、在本地区块链中获取预先声明为管理员的身份标识和签名密钥。

[0080] 在本发明具体实施例中,管理员的身份标识和签名密钥是预先在区块链中声明并进行存储的数据信息。

[0081] 可选的,获取管理员权限声明事务请求,根据管理员权限声明事务请求将至少一个管理员的身份标识和签名密钥在区块链中进行存储。

[0082] 本实施例中,由于管理员身份的特殊性,可以采用中心服务器对管理员身份进行统一管理,为每个管理员赋予全局唯一的身份标识以及签名密钥,从而由中心服务器向区块链网络发起管理员权限声明事务请求,管理员权限声明事务请求中包括至少一个需要声明的管理员的身份标识和签名密钥。区块链节点在接收到管理员权限声明事务请求后,对管理员权限声明事务请求进行信息提取,将管理员的身份标识和签名密钥在区块链中进行存储。其中,可以进行链上存储和链下存储。优选的,由于区块链中的管理员可以不止一个,因此为了减少区块链资源的占用,可以预先将区块链中声明的管理员的身份标识和签名密钥保存在区块链节点的本地存储中。

[0083] 相应的,区块链节点可以依据获取的管理员的身份标识,从本地存储中查询该身份标识关联的签名密钥即公钥。

[0084] S430、根据本地获取的签名密钥对权限调整事务请求进行验证。

[0085] 在本发明具体实施例中,利用获取的公钥对权限调整事务请求进行验证。其中,若公钥与签名权限调整事务请求的私钥均属于同一管理员的签名密钥,则区块链节点利用获取的公钥对权限调整事务请求验证通过。由于管理员身份标识的公开性,若公钥与签名权限调整事务请求的私钥不属于同一管理员的签名密钥,则区块链节点利用获取的公钥对权

限调整事务请求验证不通过,此时可以表明区块链中存在恶意用户对管理员的身份进行盗用。

[0086] S440、在验证通过后,接受权限调整事务请求。

[0087] 在本发明具体实施例中,若权限调整事务请求验证通过,则可以确定发起权限调整事务请求的管理员身份的真实性,以及可以确定权限调整事务的真实性,从而区块链节点可以接受该验证通过的权限调整事务请求。而对于验证不通过的权限调整事务请求进行拒绝,还可以追溯权限调整事务请求验证不通过的原因,例如管理员身份虚假等。

[0088] 本实施例的技术方案,通过获取权限调整事务请求中获取管理员的身份标识,以及区块链中预先声明的管理员的签名密钥,并根据本地获取的签名密钥对权限调整事务请求进行验证,从而只接受验证通过的权限调整事务请求。本发明实施例通过区块链对权限数据的统一管控,能够对权限审计后的权限调整事务请求进行验证,以确保发起权限调整事务请求的管理员身份的真实性,以及权限调整事务的真实性,为后续权限的调整提供有力的支持依据,优化了权限处理方式,提高权限处理的公信力。

[0089] 实施例四

[0090] 本实施例在上述实施例二的基础上,提供了基于区块链实现的权限处理方法的一个优选实施方式,能够在将权限调整结果进行上链存储之后,还包括,根据权限调整结果更新区块链本地存储的权限管理表。

[0091] 在本发明具体实施例中,区块链节点接受验证通过的权限调整事务请求,对权限调整事务请求进行响应得到权限调整结果,例如角色的注册、撤销或更改,或者角色中各种权限的新增、删除或更改等。从而可以将能够标识权限调整事务的信息作为一条记录进行链上存储,例如用户ID、所调整权限、调整时间以及权限调整的发起者等。此外,对于权限调整的具体结果等详细信息进行链下存储,保存到节点本地存储的权限管理表中,以更新权限管理表,为后续的权限审计提供审计依据。其中,权限管理表中包括用户的身份角色和身份角色对应的权限。

[0092] 可选的,接收用户发起的权限管理信息查询请求,在本地的权限管理表中进行查询并反馈,或请求其他区块链节点进行查询并反馈。

[0093] 本实施例中,用户还可以发起权限管理信息查询请求,以对区块链中的权限管理信息进行查询。具体的,区块链节点可以依据权限管理信息查询请求,对发起者用户权限进行审计,从而在确定发起者具有对应内容的查询权限时,在本地的权限管理表中进行查询并反馈。若本地存储中尚未同步对应的信息,则请求其他区块链节点进行查询并反馈。

[0094] 此外,在上述更新区块链本地存储的权限管理表的基础上,本实施例还能够对应用功能事务请求关联的用户身份权限进行鉴权。图5为本发明实施例四提供的鉴权用户身份权限的流程图,如图5所示,执行如下具体方案:

[0095] S510、获取应用功能事务请求。

[0096] 在本发明具体实施例中,在区块链的具体应用场景中,用户可以进行相应应用场景下的具体应用功能操作,即发起应用功能事务请求。因此,区块链节点可以获取应用功能事务请求,其中应用功能事务请求可以包括用户ID以及应用功能请求等。

[0097] 示例性的,假设在基于区块链的版权登记系统中,应用功能事务请求可以是版权登记事务请求、侵权取证事务请求、或版权交易事务请求等。

[0098] S520、如果应用功能事务请求存在用户身份权限的鉴权需求,则在本地存储的权限管理表中进行鉴权,或发起鉴权事务请求,以请求其他区块链节点进行鉴权。

[0099] 在本发明具体实施例中,为了验证用户发起的应用功能事务请求的安全可靠性以及信息一致性等,并验证用户是否可以进行相应的应用操作,若应用功能事务请求存在用户身份权限的鉴权需求,则区块链节点可以对用户身份权限进行鉴权。区块链节点可以根据本地存储的权限管理表进行用户身份鉴权,若本地存储中尚未同步对应的信息,则请求其他区块链节点进行用户身份鉴权。

[0100] S530、获取鉴权结果,根据鉴权结果处理应用功能事务请求。

[0101] 在本发明具体实施例中,区块链节点通过本地的鉴权或其他区块链节点的鉴权,获取鉴权结果,并根据鉴权结果处理应用功能事务请求。具体的,若鉴权通过,则区块链节点可以响应该应用功能事务请求,接受用户的应用操作。若鉴权不通过,则区块链节点可以拒绝该应用功能事务请求,即不允许用户的应用操作。

[0102] 可选的,在获取鉴权结果之后,将基于鉴权结果处理的应用功能事务请求的信息,作为鉴权记录,对应于用户记录到权限管理表中。

[0103] 本实施例中,可以对应用功能事务添加标识,从而将事务关联的信息和鉴权结果作为鉴权记录,存储于用户ID所属的权限管理表中。其中,鉴权结果可以包括鉴权是否通过,事务关联的信息至少可以包括事务ID,还可以进一步包括事务发起者、事务发起时间以及涉及权限类别等。

[0104] 同时,鉴权记录的保存同样为管理员的权限审计提供依据,便于管理员识别恶意用户,确定用户的恶意行为或违规行为,对用户是否能够拥有权限的审核提供参考依据。

[0105] 本实施例的技术方案,通过将对于用户的权限调整结果或鉴权结果记录于区块链节点本地存储的权限管理表中,为管理员在后续权限审计和鉴权提供了依据,同时在接收到用户的应用功能事务请求之后,能够依据权限管理表对用户权限进行鉴权,从而根据鉴权结果处理应用功能事务请求。本发明实施例通过区块链对权限数据以及处理结果的统一管控,为管理员在后续权限审计和鉴权提供了依据,以确保发起应用功能事务请求的用户身份的真实性,以及应用操作的真实性,优化了权限处理方式,提高权限处理的公信力。

[0106] 实施例五

[0107] 图6为本发明实施例五提供的一种基于区块链实现的权限处理装置的结构示意图,本实施例可适用于调整权限的情况,该装置可实现本发明任意实施例所述的基于区块链实现的权限处理方法。该装置可配置于区块链节点中,并具体包括:

[0108] 权限管理事务请求获取模块601,用于获取待审计的权限管理事务请求;

[0109] 待审计事项确定模块602,用于根据所述权限管理事务请求确定待审计事项,并将所述待审计事项提供给管理员;

[0110] 权限调整模块603,用于根据所述管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

[0111] 可选的,所述权限管理事务请求获取模块601具体用于:

[0112] 根据用户或管理员对权限智能合约的操作,产生权限管理事务请求;或

[0113] 接收其他区块链节点发送的权限管理事务请求,所述权限管理事务请求基于权限智能合约产生。

- [0114] 可选的,所述待审计事项确定模块602具体用于:
- [0115] 将所述待审计事项以可视化界面的方式提供给管理员。
- [0116] 可选的,权限调整模块603具体用于:
- [0117] 获取所述管理员对待审计事项操作而输入的审计结果参数;
- [0118] 根据权限智能合约和所述审计结果参数,产生权限调整事务请求。
- [0119] 进一步的,所述装置还包括事务请求签名模块604;所述事务请求签名模块604具体用于:
- [0120] 在所述根据所述管理员对待审计事项的操作,以产生权限调整事务请求的同时或之后,获取所述管理员的身份标识和签名密钥,对所述权限调整事务请求进行身份签名。
- [0121] 进一步的,所述装置还包括事务请求验证模块605;所述事务请求验证模块605具体用于:
- [0122] 如果接收到其他区块链节点发送的权限调整事务请求,从所述权限调整事务请求中获取管理员的身份标识;
- [0123] 在本地区块链中获取预先声明为管理员的身份标识和签名密钥;
- [0124] 根据本地获取的签名密钥对所述权限调整事务请求进行验证;
- [0125] 在验证通过后,接受所述权限调整事务请求。
- [0126] 进一步的,所述装置还包括管理员权限声明模块606;所述管理员权限声明模块606具体用于:
- [0127] 获取管理员权限声明事务请求,根据所述管理员权限声明事务请求将至少一个管理员的身份标识和签名密钥在区块链中进行存储。
- [0128] 进一步的,所述装置还包括权限管理表更新模块607;所述权限管理表更新模块607具体用于:
- [0129] 在所述将权限调整结果进行上链存储之后,根据权限调整结果更新区块链本地存储的权限管理表,其中,所述权限管理表中包括用户的身份角色和身份角色对应的权限。
- [0130] 进一步的,所述装置还包括鉴权模块608;所述鉴权模块608具体用于:
- [0131] 获取应用功能事务请求;
- [0132] 如果所述应用功能事务请求存在用户身份权限的鉴权需求,则在本地存储的权限管理表中进行鉴权,或发起鉴权事务请求,以请求其他区块链节点进行鉴权;
- [0133] 获取鉴权结果,根据鉴权结果处理所述应用功能事务请求。
- [0134] 进一步的,所述装置还包括鉴权信息记录模块609;所述鉴权信息记录模块609具体用于:
- [0135] 在所述获取鉴权结果之后,将基于鉴权结果处理的所述应用功能事务请求的信息,作为鉴权记录,对应于用户记录到所述权限管理表中。
- [0136] 进一步的,所述装置还包括权限管理信息查询模块610;所述权限管理信息查询模块610具体用于:
- [0137] 接收用户发起的权限管理信息查询请求,在本地的权限管理表中进行查询并反馈,或请求其他区块链节点进行查询并反馈。
- [0138] 本实施例的技术方案,通过各个功能模块之间的相互配合,实现了权限管理事务请求的接收、待审计事项的确定、待审计事项的通知、权限智能合约的操作、审计结果的获

取、权限调整事务请求的生成、权限调整结果的写入、事务请求的签名、事务请求的验证、权限管理表的更新、用户身份权限的鉴权、鉴权信息的记录以及权限管理信息的查询等功能。本发明实施例通过区块链对权限数据的统一管控,为管理员提供了权限审计依据;同时区块链网络中的任一节点均可为管理员提供进行权限审计操作的入口,将权限审计工作分散并行处理,优化了权限处理方式,提高权限处理过程中的审计效率和公信力。

[0139] 实施例六

[0140] 图7为本发明实施例六提供的一种设备的结构示意图,图7示出了适于用来实现本发明实施例实施方式的示例性设备的框图。图7显示的设备仅仅是一个示例,不应对本发明实施例的功能和使用范围带来任何限制。

[0141] 图7显示的设备12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。该设备12优选为承载区块链节点的电子设备。

[0142] 如图7所示,设备12以通用计算设备的形式表现。设备12的组件可以包括但不限于:一个或者多个处理器16,系统存储器28,连接不同系统组件(包括系统存储器28和处理器16)的总线18。

[0143] 总线18表示几类总线结构中的一种或多种,包括存储器总线或者存储器控制器,外围总线,图形加速端口,处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说,这些体系结构包括但不限于工业标准体系结构(ISA)总线,微通道体系结构(MAC)总线,增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0144] 设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被设备12访问的可用介质,包括易失性和非易失性介质,可移动的和不可移动的介质。

[0145] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质,例如随机存取存储器(RAM)30和/或高速缓存存储器32。设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例,存储系统34可以用于读写不可移动的、非易失性磁介质(图7未显示,通常称为“硬盘驱动器”)。尽管图7中未示出,可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器,以及对可移动非易失性光盘(例如CD-ROM,DVD-ROM或其它光介质)读写的光盘驱动器。在这些情况下,每个驱动器可以通过一个或者多个数据介质接口与总线18相连。系统存储器28可以包括至少一个程序产品,该程序产品具有一组(例如至少一个)程序模块,这些程序模块被配置以执行本发明实施例各实施例的功能。

[0146] 具有一组(至少一个)程序模块42的程序/实用工具40,可以存储在例如系统存储器28中,这样的程序模块42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。程序模块42通常执行本发明实施例所描述的实施例中的功能和/或方法。

[0147] 设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信,还可与一个或者多个使得用户能与该设备12交互的设备通信,和/或与使得该设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡,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22进行。并且,设备12还可以通过网络适配器20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20通过总线18与设备12的其它模块通信。应当明白,尽管图中未示出,可以结合

设备12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、冗余处理器、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。

[0148] 处理器16通过运行存储在系统存储器28中的程序,从而执行各种功能应用以及数据处理,例如实现本发明实施例所提供的基于区块链实现的权限处理方法。

[0149] 实施例七

[0150] 本发明实施例七还提供一种计算机可读存储介质,其上存储有计算机程序(或称为计算机可执行指令),该程序被处理器执行时用于执行一种基于区块链实现的权限处理方法,该方法包括:

[0151] 获取待审计的权限管理事务请求;

[0152] 根据所述权限管理事务请求确定待审计事项,并将所述待审计事项提供给管理员;

[0153] 根据所述管理员对待审计事项的操作,以产生权限调整事务请求,并在区块链网络中传输,以将权限调整结果进行上链存储。

[0154] 本发明实施例的计算机存储介质,可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是一——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。计算机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、便携式计算机磁盘、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、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中,计算机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。

[0155] 计算机可读的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,其中承载了计算机可读的程序代码。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。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质,该计算机可读介质可以发送、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。

[0156] 计算机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、电线、光缆、RF等等,或者上述的任意合适的组合。

[0157] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明实施例操作的计算机程序代码,所述程序设计语言包括面向对象的程序设计语言——诸如Java、Smalltalk、C++,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用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或设备上执行。在涉及远程计算机的情形中,远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)——连接到用户计算机,或者,可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0158] 注意,上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解,本发明不限于这里所述的特定实施例,对本领域技术人员来说能够进行各种明显的变化、

重新调整和替代而不会脱离本发明的保护范围。因此,虽然通过以上实施例对本发明实施例进行了较为详细的说明,但是本发明实施例不仅仅限于以上实施例,在不脱离本发明构思的情况下,还可以包括更多其他等效实施例,而本发明的范围由所附的权利要求范围决定。

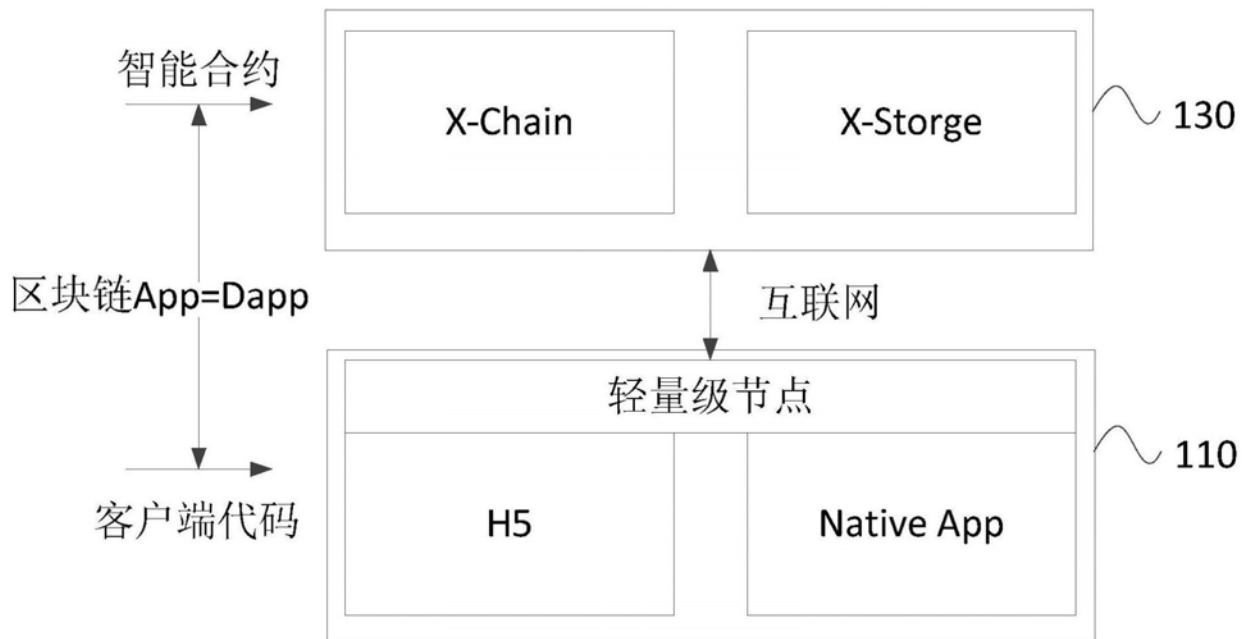


图1

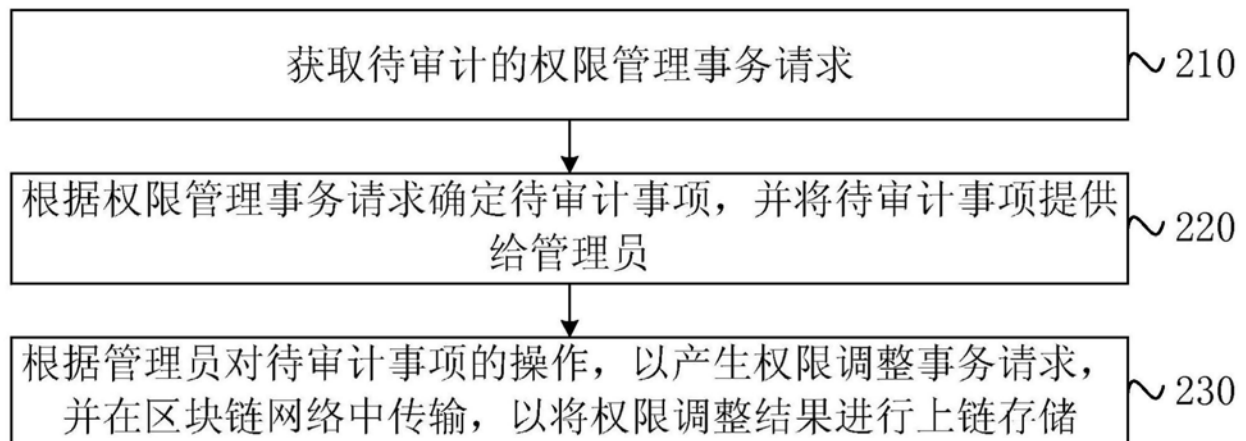


图2

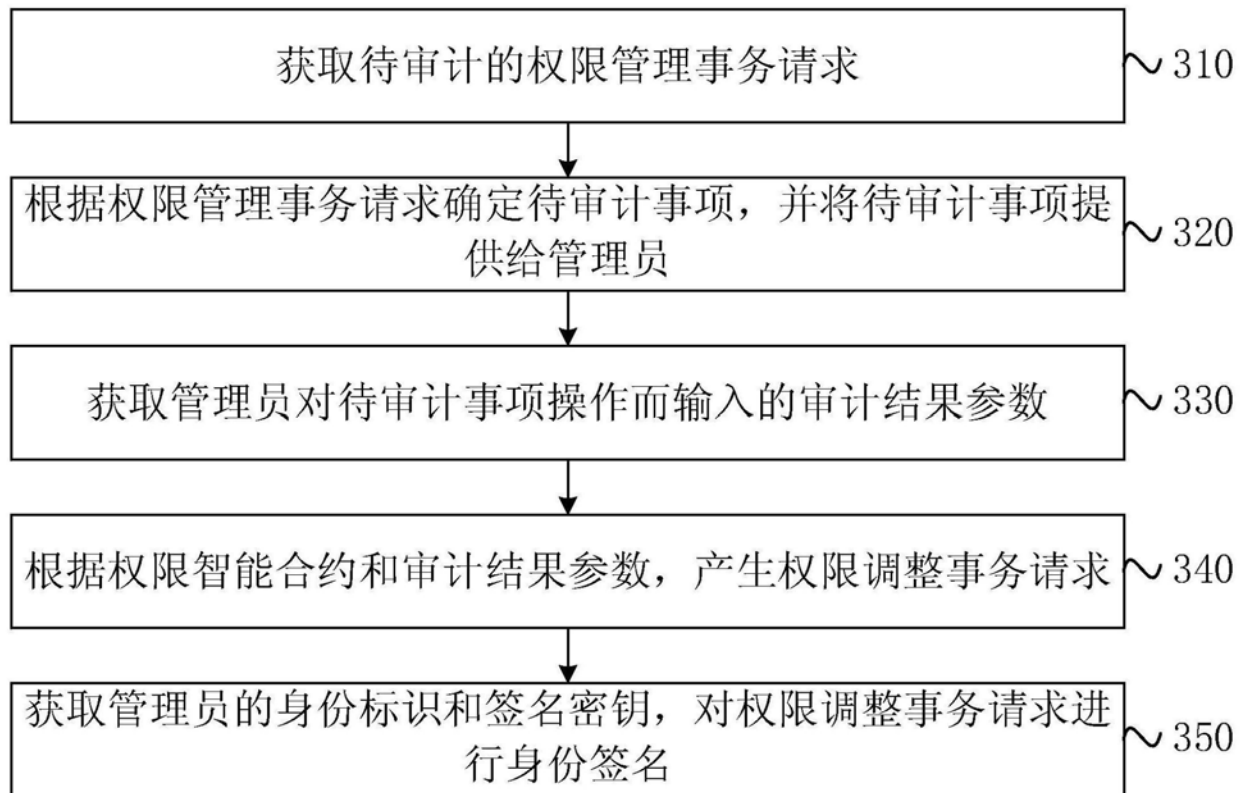


图3

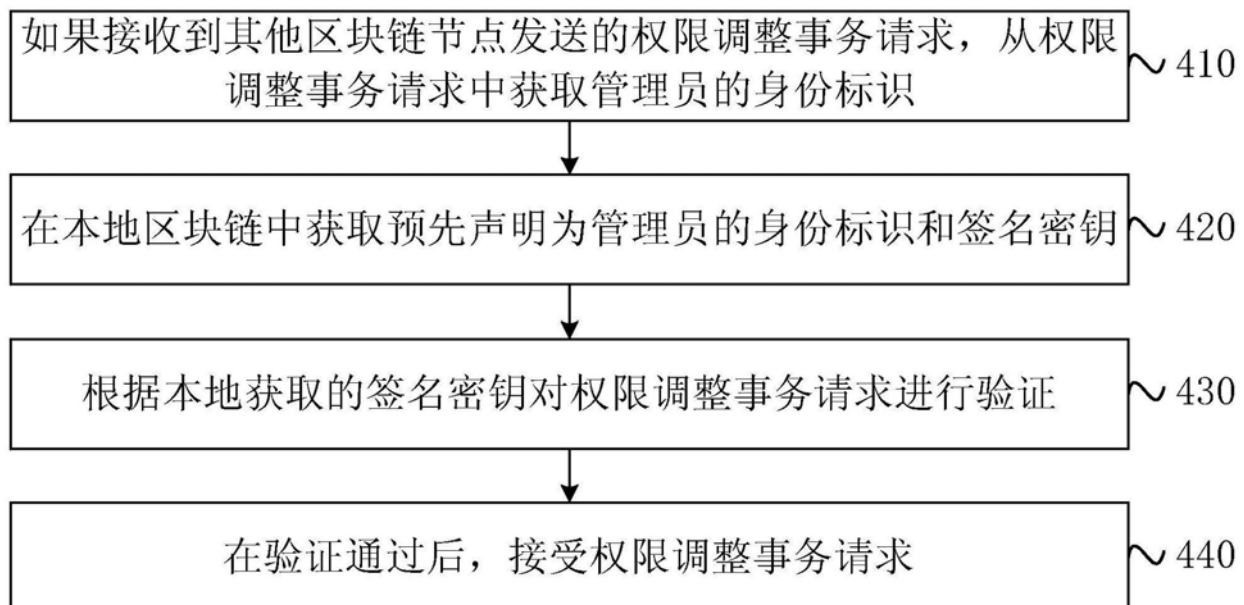


图4

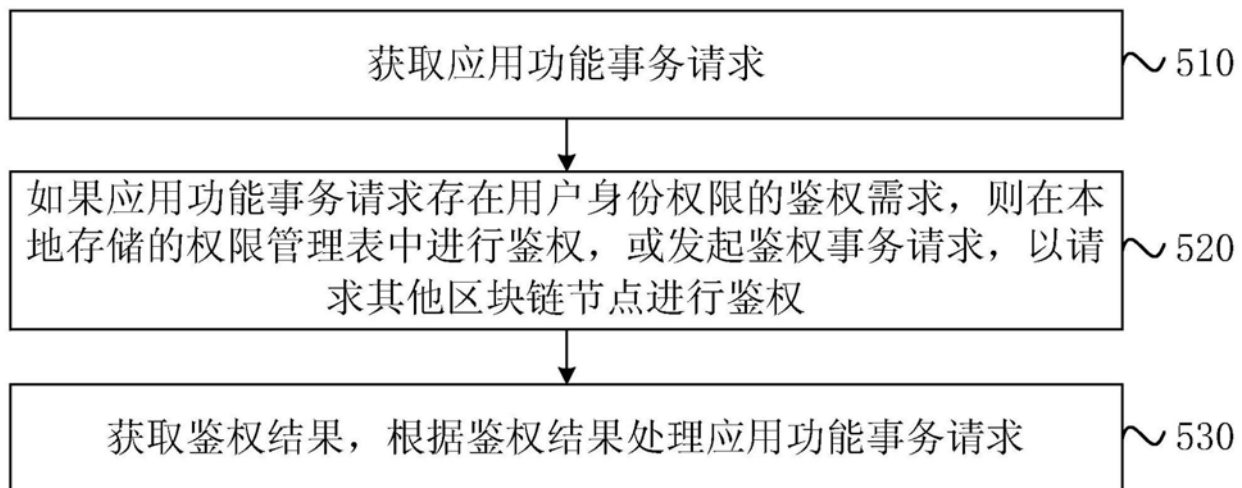


图5

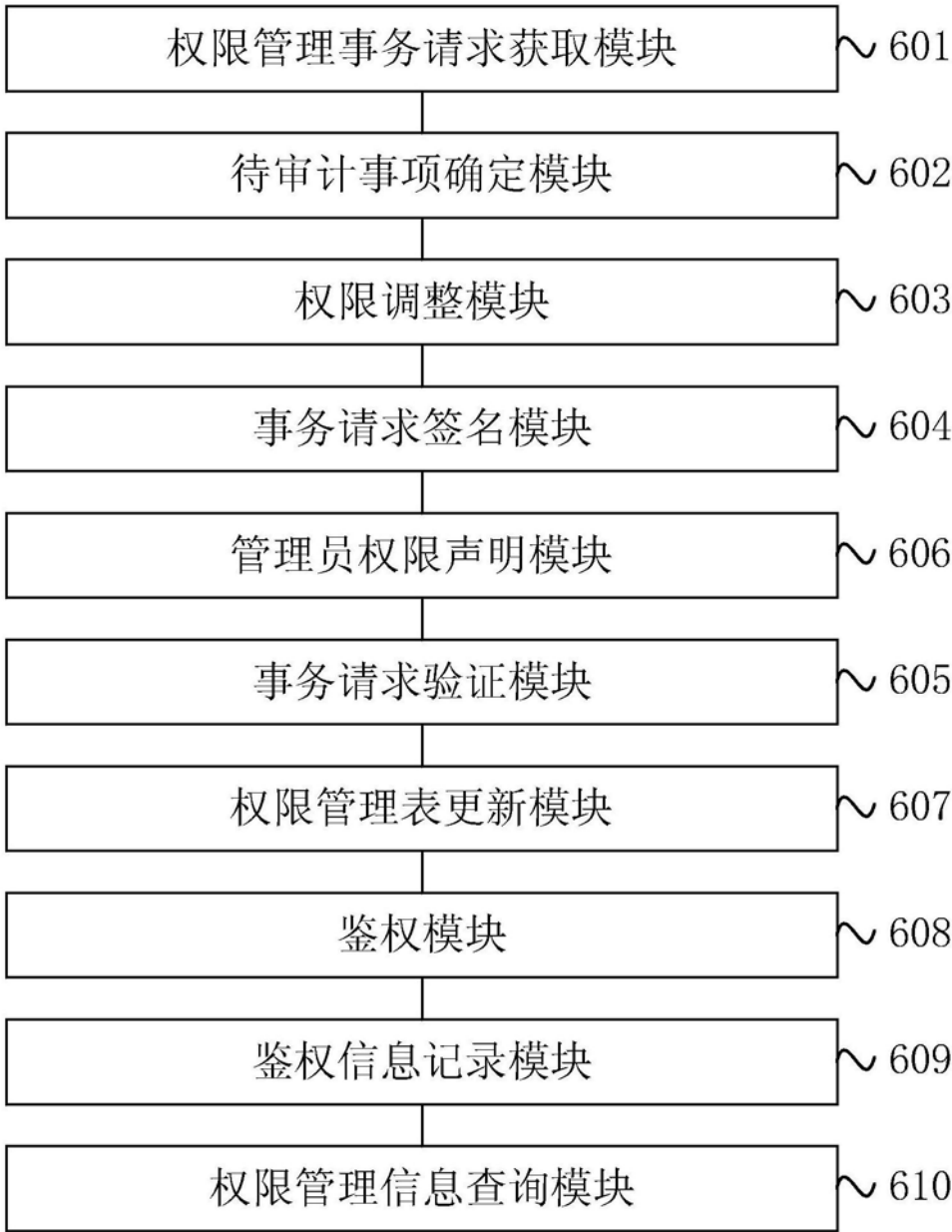


图6

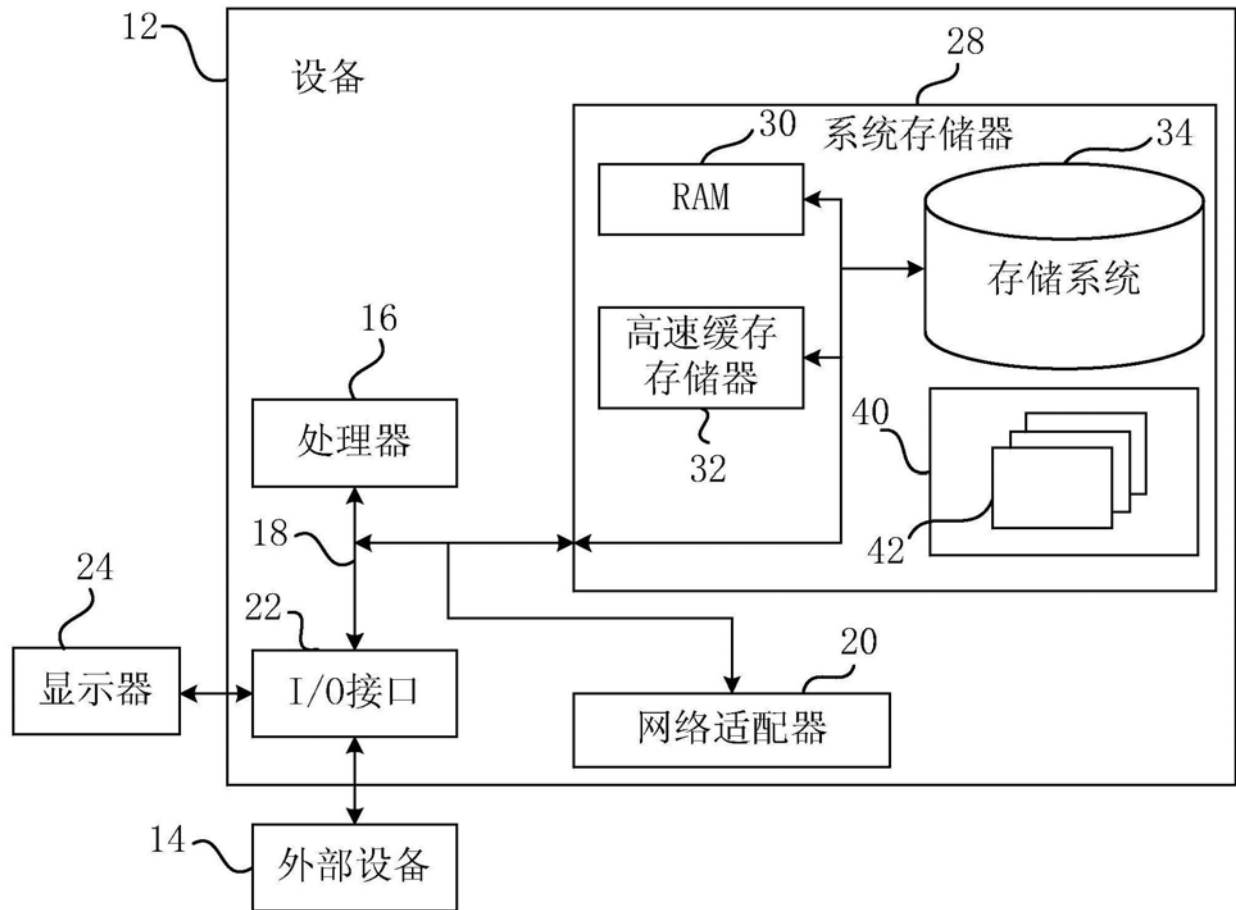


图7