



(12) 发明专利申请

(10) 申请公布号 CN 113541965 A

(43) 申请公布日 2021.10.22

(21) 申请号 202110826770.1

G06F 16/27 (2019.01)

(22) 申请日 2021.01.27

(62) 分案原申请数据

202110111606.2 2021.01.27

(71) 申请人 支付宝(杭州)信息技术有限公司

地址 310000 浙江省杭州市西湖区西溪路  
556号8层B段801-11

申请人 蚂蚁区块链科技(上海)有限公司

(72) 发明人 张翼翔 代平 沈陈侃

(74) 专利代理机构 北京博思佳知识产权代理有  
限公司 11415

代理人 李威

(51) Int. Cl.

H04L 9/32 (2006.01)

G06F 21/64 (2013.01)

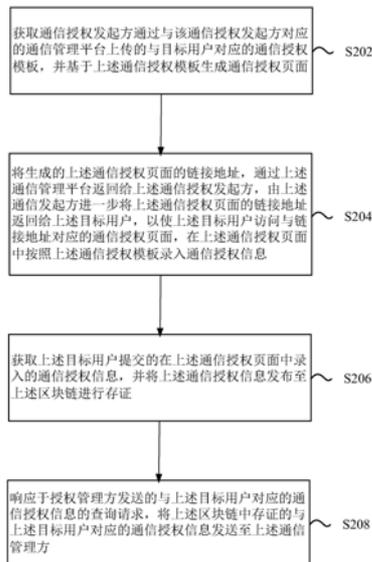
权利要求书2页 说明书13页 附图8页

(54) 发明名称

一种基于区块链的通信授权方法、装置、设备和存储介质

(57) 摘要

本申请提出一种基于区块链的通信授权方法、装置、设备和存储介质。其中,该方法应用于基于上述区块链构建的授权平台。该方法可以包括,获取通信授权发起方上传的与目标用户对应的通信授权模板,并基于上述通信授权模板生成通信授权页面。将生成的上述通信授权页面的链接地址返回给上述通信授权发起方,由上述通信发起方进一步将上述通信授权页面的链接地址返回给上述目标用户,以使上述目标用户访问与链接地址对应的通信授权页面,在上述通信授权页面中按照上述通信授权模板录入通信授权信息。获取上述目标用户提交的在上述通信授权页面中录入的通信授权信息,并将上述通信授权信息发布至上述区块链进行存证。响应于授权管理方发送的与上述目标用户对应的通信授权信息的查询请求,将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方



1. 一种基于区块链的通信授权方法,应用于基于所述区块链构建的授权平台;所述授权平台对接多个通信管理平台;所述方法包括:

获取通信授权发起方通过与该通信授权发起方对应的通信管理平台上传的与目标用户对应的通信授权模板,并基于所述通信授权模板生成通信授权页面;

将生成的所述通信授权页面,通过所述通信管理平台返回给所述通信授权发起方,由所述通信授权发起方进一步将所述通信授权页面返回给所述目标用户,以使所述目标用户在所述通信授权页面中按照所述通信授权模板录入通信授权信息;

获取所述目标用户提交的在所述通信授权页面中录入的通信授权信息,并将所述通信授权信息发布至所述区块链进行存证;

接收所述多个通信管理平台中的任N个通信管理平台发起的授权记录查询请求;

将存证的授权记录发送至所述任N个通信管理平台完成授权记录的共享。

2. 根据权利要求1所述的方法,还包括:

响应于授权管理方发送的与所述目标用户对应的通信授权信息的查询请求,将所述区块链中存证的与所述目标用户对应的通信授权信息发送至所述授权管理方;其中,所述授权管理方包括对通信授权进行管理的第三方监管方。

3. 根据权利要求1所述的方法,所述授权平台包括区块链即服务BaaS平台;以及,与区块链即服务BaaS平台连接的若干台区块链节点设备。

4. 根据权利要求1所述的方法,所述区块链部署了用于对通信授权信息进行管理的智能合约;

所述将所述通信授权信息发布至所述区块链进行存证,包括:

调用合约的校验逻辑对所述通信授权信息进行数据校验;如果校验通过,调用合约的存证逻辑在区块链存证所述通信授权信息,并将存证的所述通信授权信息存证标记为已授权状态。

5. 根据权利要求4所述的方法,还包括:

响应于所述目标用户发起的针对所述通信授权信息的通信授权撤销请求,调用所述智能合约中的撤销逻辑,将存证的所述通信授权信息由已授权状态更新为撤销状态。

6. 根据权利要求1所述的方法,所述将所述通信授权信息发布至所述区块链进行存证,包括:

对所述通信授权信息进行数据校验;

如果校验通过,生成包含授权状态的授权记录,将所述授权记录存证至所述区块链。

7. 根据权利要求6所述的方法,还包括:

响应于所述目标用户发起的针对所述授权记录的通信授权撤销请求,从所述区块链中获取所述授权记录;

将所述授权记录对应的状态标识置为撤销状态,并将包含撤销状态的授权记录存证至所述区块链。

8. 根据权利要求1所述的方法,所述将所述通信授权信息发布至所述区块链进行存证,包括:

对所述通信授权信息进行数据校验;

如果校验通过,将所述通信授权信息发布至所述区块链进行存证,并获取与所述通信

授权信息对应的存证标识；

在搭载的中心化数据库中存储所述存证标识，并将所述存证标识标记为已授权状态。

9. 根据权利要求8所述的方法，还包括：

响应于所述目标用户发起的通信授权撤销请求，将所述中心化数据库中存储的与所述通信授权信息对应的存证标识的由已授权状态更新为撤销状态。

10. 根据权利要求1所述的方法，所述将所述区块链中存证的与所述目标用户对应的通信授权信息发送至所述授权管理方，包括：

将所述区块链中存证的与所述目标用户对应的通信授权信息，以及，与通信授权信息对应的状态发送至所述授权管理方。

11. 根据权利要求1所述的方法，所述通信管理平台包括云呼叫平台；所述通信授权包括云呼叫授权。

12. 一种基于区块链的通信授权装置，应用于基于所述区块链构建的授权平台；所述授权平台对接多个通信管理平台；所述装置包括：

生成模块，获取通信授权发起方通过与该通信授权发起方对应的通信管理平台上传的与目标用户对应的通信授权模板，并基于所述通信授权模板生成通信授权页面；

返回模块，将生成的所述通信授权页面，通过所述通信管理平台返回给所述通信授权发起方，由所述通信授权发起方进一步将所述通信授权页面返回给所述目标用户，以使所述目标用户在所述通信授权页面中按照所述通信授权模板录入通信授权信息；

发布模块，获取所述目标用户提交的在所述通信授权页面中录入的通信授权信息，并将所述通信授权信息发布至所述区块链进行存证；

接收模块，接收所述多个通信管理平台中的任N个通信管理平台发起的授权记录查询请求；

存证模块，将存证的授权记录发送至所述任N个通信管理平台完成授权记录的共享。

13. 一种电子设备，包括：

处理器；

存储器；

其中，所述处理器被配置为调用所述存储器中存储的可执行指令，实现如所述权利要求1-11任一所述的通信授权方法。

14. 一种计算机可读存储介质，所述存储介质存储有计算机程序，所述计算机程序用于使处理器执行如所述权利要求1-11任一所述的通信授权方法。

## 一种基于区块链的通信授权方法、装置、设备和存储介质

### 技术领域

[0001] 本申请涉及计算机技术,具体涉及一种基于区块链的通信授权方法、装置、设备和存储介质。

### 背景技术

[0002] 通信授权,是指用户授权企业通过通信管理平台以诸如短息或邮件等通信方式向用户推送消息。上述通信管理平台通常是为企业提供通信管理服务的平台。例如,上述通信管理平台可以是呼叫平台或云呼叫平台。

[0003] 在通信授权领域中,目前是用户对企业的授权过程是二者自行完成,用户对企业的授权记录也是存储在通信管理平台中。

[0004] 可见,一方面,用户的授权过程是没有被监控的,并且授权记录也是存在数据可被篡改的中心化数据库中,从而导致用户授权过程和授权记录不可信;

[0005] 另一方面,授权管理方(例如,第三方监管机构)也无法获取真实可靠的授权记录。

### 发明内容

[0006] 有鉴于此,本申请公开一种基于区块链的通信授权方法,应用于基于上述区块链构建的授权平台;上述方法包括:

[0007] 获取通信授权发起方通过与该通信授权发起方对应的通信管理平台上传的与目标用户对应的通信授权模板,并基于上述通信授权模板生成通信授权页面;

[0008] 将生成的上述通信授权页面的链接地址,通过上述通信管理平台返回给上述通信授权发起方,由上述通信发起方进一步将上述通信授权页面的链接地址返回给上述目标用户,以使上述目标用户访问与链接地址对应的通信授权页面,在上述通信授权页面中按照上述通信授权模板录入通信授权信息;

[0009] 获取上述目标用户提交的在上述通信授权页面中录入的通信授权信息,并将上述通信授权信息发布至上述区块链进行存证;

[0010] 响应于授权管理方发送的与上述目标用户对应的通信授权信息的查询请求,将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方。

[0011] 本申请还公开一种基于区块链的通信授权装置,应用于基于上述区块链构建的授权平台;上述装置包括:

[0012] 生成模块,获取通信授权发起方通过与该通信授权发起方对应的通信管理平台上传的与目标用户对应的通信授权模板,并基于上述通信授权模板生成通信授权页面;

[0013] 返回模块,将生成的上述通信授权页面的链接地址,通过上述通信管理平台返回给上述通信授权发起方,由上述通信发起方进一步将上述通信授权页面的链接地址返回给上述目标用户,以使上述目标用户访问与链接地址对应的通信授权页面,在上述通信授权页面中按照上述通信授权模板录入通信授权信息;

[0014] 发布模块,获取上述目标用户提交的在上述通信授权页面中录入的通信授权信

息,并将上述通信授权信息发布至上述区块链进行存证;

[0015] 发送模块,响应于授权管理方发送的与上述目标用户对应的通信授权信息的查询请求,将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方。

[0016] 本申请还公开一种电子设备,包括:

[0017] 处理器;

[0018] 用于存储上述处理器可执行指令的存储器;

[0019] 其中,上述处理器被配置为调用上述存储器中存储的可执行指令,实现如前述任一实施例示出的基于区块链的通信授权方法。

[0020] 本申请还公开一种计算机可读存储介质,上述存储介质存储有计算机程序,上述计算机程序用于执行如前述任一实施例示出的基于区块链的通信授权方法。

[0021] 在上述方案中,第一方面,由于上述授权平台可以获取并存储通信授权发起方上传的通信授权模板,并生成链接地址供目标用户进行访问授权,以及将上述目标用户上传的通信授权信息进行存证,因此实现了通过授权平台监管通信授权发起方与用户之间的授权过程,并将通信授权发起方与用户之间的授权信息存证在区块链中,由此一方面,可以对用户与授权发起方之间的授权过程进行记录与监管,进而保证可以得到用户真实的授权信息;另一方面,可以利用区块链透明度高,不可篡改等特性,保证存证的授权信息的可信性。

[0022] 第二方面,上述授权平台在接收到授权管理方针对通信授权信息发起的查询请求后,可以向该授权管理方返回存证的通信授权信息,进而保证授权管理方获取可信的授权信息。

[0023] 应当理解的是,以上述的一般描述和后文的细节描述仅是示例性和解释性的,并不能限制本申请。

## 附图说明

[0024] 为了更清楚地说明本申请一个或多个实施例或相关技术中的技术方案,下面将对实施例或相关技术描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本申请一个或多个实施例中记载的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动性的前提下,还可以根据这些附图获得其他的附图。

[0025] 图1为本申请示出的一种创建智能合约的示意图;

[0026] 图2为本申请示出的一种基于区块链的通信授权方法的方法流程图;

[0027] 图3为本申请示出的一种呼叫授权场景示意图;

[0028] 图4为本申请示出的一种呼叫授权的流程图;

[0029] 图5为本申请示出的一种撤销授权记录的方法流程图;

[0030] 图6为本申请示出的一种获取授权记录的方法流程图;

[0031] 图7为本申请示出的一种基于区块链的通信授权装置的结构示意图;

[0032] 图8为本申请示出的一种电子设备的硬件结构示意图。

## 具体实施方式

[0033] 下面将详细地对示例性实施例进行说明,其示例表示在附图中。下面的描述涉及

附图时,除非另有表示,不同附图中的相同数字表示相同或相似的要素。以下示例性实施例中所描述的实施方式并不代表与本发明相一致的所有实施方式。相反,它们仅是与如所附权利要求书中所详述的、本发明的一些方面相一致的设备和方法的例子。

[0034] 在本申请使用的术语是仅仅出于描述特定实施例的目的,而非旨在限制本申请。在本申请和所附权利要求书中所使用的单数形式的“一种”、“上述”和“该”也旨在可以包括多数形式,除非上述下文清楚地表示其他含义。还应当理解,本文中使用的术语“和/或”是指并包含一个或多个相关联的列出项目的任何或所有可能组合。还应当理解,本文中使用的词语“如果”,取决于语境,可以被解释成为“在……时”或“当……时”或“响应于确定”。

[0035] 区块链技术,也被称之为分布式账本技术,是一种由若干台计算设备共同参与“记账”,共同维护一份完整的分布式数据库的新兴技术。由于区块链技术具有去中心化、公开透明、每台计算设备可以参与数据库记录、并且各计算设备之间可以快速的进行数据同步的特性,使得区块链技术已在众多的领域中广泛的进行应用。

[0036] 区块链一般被划分为三种类型:公有链(Public Blockchain),私有链(PrivateBlockchain)和联盟链(Consortium Blockchain)。此外,还有多种类型的结合,比如私有链+联盟链、联盟链+公有链等不同组合形式。其中去中心化程度最高的是公有链。公有链以比特币、以太坊为代表,加入公有链的参与者可以读取链上的数据记录、参与交易以及竞争新区块的记账权等。

[0037] 而且,各参与者(即节点)可自由加入以及退出网络,并进行相关操作。私有链则相反,该网络的写入权限由某个组织或者机构控制,数据读取权限受组织规定。简单来说,私有链可以为一个弱中心化系统,参与节点具有严格限制且少。这种类型的区块链更适合于特定机构内部使用。

[0038] 联盟链则是介于公有链以及私有链之间的区块链,可实现“部分去中心化”。联盟链中各个节点通常有与之相对应的实体机构或者组织;参与者通过授权加入网络并组成利益相关联盟,共同维护区块链运行。

[0039] 不论是公有链、私有链还是联盟链,都可能提供智能合约的功能。区块链上的智能合约是在区块链系统上可以被交易触发执行的合约。智能合约可以通过代码的形式定义。

[0040] 以以太坊为例,支持用户在以太坊网络中创建并调用一些复杂的逻辑,这是以太坊区别于比特币区块链技术的最大挑战。以太坊作为一个可编程区块链的核心是以太坊虚拟机(EVM),每个以太坊节点都可以运行EVM。EVM是一个图灵完备的虚拟机,这意味着可以通过它实现各种复杂的逻辑。用户在以太坊中发布和调用智能合约就是在EVM上运行的。实际上,虚拟机直接运行的是虚拟机代码(虚拟机字节码,下简称“字节码”)。部署在区块链上的智能合约可以是字节码的形式。

[0041] 例如图1所示,Bob将一个包含创建智能合约信息的交易(Transaction)发送到以太坊网络后,节点1的EVM可以执行这个交易并生成对应的合约实例。图1中的“0x68e12cf284…”代表了该合约的地址,交易的数据字段保存的可以是字节码,交易的to字段为一个空的账户。节点间通过共识机制达成一致后,这个合约成功创建,后续用户可以调用这个合约。

[0042] 合约创建后,区块链上出现一个与该智能合约对应的合约账户,并拥有一个特定的地址,合约代码和账户存储将保存在该合约账户中。智能合约的行为由合约代码控制,而

智能合约的账户存储 (Storage) 则保存了合约的状态。换句话说, 智能合约使得区块链上产生包含合约代码和账户存储的虚拟账户。

[0043] 前述提到, 包含创建智能合约的交易的data字段保存的可以是该智能合约的字节码。字节码由一连串的字节组成, 每一字节可以标识一个操作。基于开发效率、可读性等多方面考虑, 开发者可以不直接书写字节码, 而是选择一门高级语言编写智能合约代码。例如, 采用诸如Solidity、Serpent、LLL语言等高级语言。对于采用高级语言编写的智能合约代码, 可以经过编译器编译, 生成可以部署到区块链上的字节码。

[0044] 以Solidity语言为例, 用其编写的合约与面向对象编程语言中的类(Class)很相似, 在一个合约中可以声明多种成员, 包括状态变量、函数、函数修改器、事件等。状态变量是永久存储在智能合约的账户存储中的值, 用于保存合约的状态。

[0045] 本申请旨在提出一种基于区块链的通信授权方法。该方法通过授权平台监管通信授权发起方与用户之间的授权过程, 并将通信授权发起方与用户之间的授权信息存证在区块链中, 由此一方面, 可以对用户与授权发起方之间的授权过程进行记录与监管, 进而保证可以得到用户真实的授权信息; 另一方面, 可以利用区块链透明度高, 不可篡改等特性, 保证存证的授权信息的可信性。

[0046] 该方法还可在接收到授权管理方针对通信授权信息发起的查询请求后, 向该授权管理方返回存证的通信授权信息, 进而保证授权管理方获取可信的授权信息。

[0047] 上述方法可以应用与基于区块链构建的授权平台。在一些例子中, 上述授权平台可以包括区块链以及可以与该区块链交互的服务平台中。在一些例子中, 上述服务平台可以包括区块链即服务BaaS平台。一方面, 该平台可以与区块链系统进行交互, 在上述区块链中存证或获取数据。另一方面, 该平台可以与区块链外的用户、以及通信管理平台进行数据交互。

[0048] 上述区块链可以包括若干节点设备。上述节点设备可以是部署于区块链中的任意电子设备。需要说明的是, 本申请不对节点设备的设备类型进行特别限定。

[0049] 上述区块链可以是公有链、私有链或联盟链。在一些例子中, 上述区块链可以是联盟链。当上述区块链为联盟链时, 上述节点设备可以通过验证后才加入上述区块链的节点设备, 从而确保加入的节点设备时可信的, 进而可以将区块链中存证的数据共享至联盟链中的任意可信设备。

[0050] 请参见图2, 图2为本申请示出的一种基于区块链的通信授权方法的方法流程图。

[0051] 如图2所示, 上述方法可以包括:

[0052] S202, 获取通信授权发起方通过与该通信授权发起方对应的通信管理平台上传的与目标用户对应的通信授权模板, 并基于上述通信授权模板生成通信授权页面。

[0053] 上述通信授权发起方(以下简称发起方), 具体是指有授权需求的一方。例如, 上述通信授权发起方可以是电商商家, 企业等。

[0054] 上述通信管理平台通常是为通信授权发起方提供通信管理服务的平台。例如, 上述通管理平台可以是呼叫平台或云呼叫平台。上述通信管理平台可以与上述授权平台进行通信。在一些例子中, 上述授权平台可以诸如API接口的方式与通信管理平台进行交互。

[0055] 在一些例子中, 上述通信管理平台可以对接多个通信管理平台。此时授权平台可以接收上述多个通信管理平台中的任N个通信管理平台发起的授权记录查询请求, 将存证

的授权记录发送至上述任N个通信运营商完成授权记录的共享。

[0056] 由此可以将区块链存证的通信授权信息共享至上述多个通信管理平台,从而保证上述多个通信管理平台可以获取到可信的通信授权信息,并避免用户针对不同的通信管理平台进行重复授权。

[0057] 上述通信授权模板,可以是由通信授权发起方上传的包括与授权相关的内容的模板。在一些例子中,上述通信授权模板可以是授权协议。该授权协议中可以载明上述通信授权发起方的企业名称,联系方式等信息,以及用户授权给企业的授权范围等。

[0058] 上述通信授权页面,具体是指根据上述通信授权模板包含的内容生成的可呈现给用户操作的页面。

[0059] 在一些例子中在执行S202时,通信授权发起方可以在对应的客户端中填写针对目标用户的授权模板。然后,该发起方可以将该模板打包至授权请求中发送至通信管理平台。上述通信管理平台接收到上述授权请求后,可以获取该授权请求中包括的该模板。然后将该模板发送至上述授权平台。

[0060] 上述授权平台可以对上述通信授权模板包括的各组件进行渲染,生成与上述通信授权页面对应的页面组件,并存储在上述授权平台对应的数据库中。

[0061] 之后,上述授权平台可以执行S204,将生成的上述通信授权页面的链接地址,通过上述通信管理平台返回给上述通信授权发起方,由上述通信发起方进一步将上述通信授权页面的链接地址返回给上述目标用户,以使上述目标用户访问与链接地址对应的通信授权页面,在上述通信授权页面中按照上述通信授权模板录入通信授权信息。

[0062] 上述连接地址,具体可以是与上述通信授权页面对应的查询地址。例如,上述通信授权页面可以存储至上述授权平台对应的数据库中。该数据库可以基于是是通信授权页面的存储地址等信息生成诸如URL的连接地址。通过该连接地址可以访问存储在上述授权平台中的通信授权页面。

[0063] 上述通信授权信息,具体可以是上述目标用户在同意的授权时,在上述通信授权页面中填写的信息。在一些例子中,上述是通信授权信息包括但不限于上述目标用户的名称,联系方式,数字签名等。

[0064] 在一些例子中,在执行S204时,上述授权平台可以在获取该链接地址后,将该链接地址返回至上述通信管理平台。上述通信管理平台可以再将该链接地址返回至上述通信授权发起方。上述通信授权发起方可以通过诸如发短信的方式将上述链接地址返回给上述目标用户。

[0065] 在一些例子中,上述短息中处理包括上述链接地址信息外,还可以包括上述发起方邀请上述目标用户进行通信授权的相关邀请信息。

[0066] 上述目标用户在接收到该链接地址后,可以通过访问链接地址的方式,从上述授权平台获取上述通信授权页面。上述目标用户如果同意授权,则可以在上述通信授权页面中按照指示内容录入通信授权信息,并将完成录入的是通信授权信息提交至上述授权平台。

[0067] 之后,上述授权平台可以执行S206,获取上述目标用户提交的在上述通信授权页面中录入的通信授权信息,并将上述通信授权信息发布至上述区块链进行存证。

[0068] 在一些例子中,上述授权平台在接收到上述通信授权信息后,可以基于上述通信

授权信息打包一笔存证交易,并将该交易发布至上述区块链中。当上述区块链中的各节点设备完成共识后,可以玩下上述通信授权信息的存证。

[0069] 在上述方案中,由于上述授权平台可以获取并存储通信授权发起方上传的通信授权模板,并生成链接地址供目标用户进行访问授权,以及将上述目标用户上传的通信授权信息进行存证,因此实现了通过授权平台监管通信授权发起方与用户之间的授权过程,并将通信授权发起方与用户之间的授权信息存证在区块链中,由此一方面,可以对用户与授权发起方之间的授权过程进行记录与监管,进而保证可以得到用户真实的授权信息;另一方面,可以利用区块链透明度高,不可篡改等特性,保证存证的授权信息的可信性。

[0070] 在一些例子中,上述区块链完成授权信息存证后,可以将上述目标用户与上述发起方之间的授权结果通知至上述通信管理平台,上述发起方以及上述目标用户。

[0071] 上述授权平台还可以执行S208,响应于授权管理方发送的与上述目标用户对应的通信授权信息的查询请求,将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方。

[0072] 上述授权管理方,可以是对通信授权进行管理的第三方监管方。当用户接收到某企业的信息骚扰时,可以向上述授权管理方发起针对该企业的投诉。上述授权管理方可以向上述授权平台发送针对该目标用户的通信授权信息的查询请求。在一些例子中,上述查询请求可以包括通信授权信息对应的唯一ID。其中,上述ID可以是上述区块链在存证通信授权信息后返回的存证地址。

[0073] 上述授权平台可以通过上述查询请求中携带的ID,从上述区块链中获取与上述ID对应的通信授权信息,并将该通信息返回至上述通信管理方。

[0074] 在上述方案中,上述授权平台在接收到授权管理方针对通信授权信息发起的查询请求后,可以向该授权管理方返回存证的通信授权信息,进而保证授权管理方获取可信的授权信息。

[0075] 在一些例子中,上述区块链中可以部署用于对通信授权信息进行管理的智能合约。其中,上述智能合约可以由项目运营方(例如,通信业务运营方)根据业务需求预先开发,并发布在上述区块链中的。

[0076] 上述智能合约可以包括校验逻辑。通过上述校验逻辑可以对用户上传的通信授权信息进行交易,并在校验通过时,完成通信授权信息的存证,进而保证通信授权信息的真实性,提升通信授权的可信性。

[0077] 在一些例子中,在执行S206存证通信授权信息时,上授权平台可以执行S2062,调用合约的校验逻辑对上述通信授权信息进行数据校验;如果校验通过,调用合约的存证逻辑在区块链存证上述通信授权信息,并将存证的上述通信授权信息存证标记为已授权状态。

[0078] 上述数据校验,可以是针对通信授权信息的身份校验。例如,可以验证该通信授权信息是否包括上述目标用户与上述发起方对应的数字签名,如果包括则认为通过上述数据校验。

[0079] 上述智能合约可以维护上述通信授权信息的状态。例如,可以维护指示上述通信授权信息状态的标识位。上述标识位可以包括第一数值和第二数值。其中,第一数值表征通信授权信息为已授权状态。第二数值表征通信授权信息已撤销。

[0080] 在一些例子中,上述发起方与上述目标用户预先在上述授权平台中完成注册。上述授权平台为上述发起方与上述目标用户分别分配了公私钥对,并分别发送至上述发起方与上述目标用户。上述发起方在填写完成授权模板后可以通过自身持有的私钥对授权模板进行签名。上述目标用户在针对授权模板填写完授权信息后,可以在生成的通信授权信息中进行数字签名。

[0081] 在执行S2062时,上述授权平台可以构建一笔智能合约调用交易,从上述区块链中获取上述智能合约,并在本地EVM中进行执行。上述智能合约可以通过校验逻辑,获取上述发起方与上述目标用户对应的公钥,并通过获取的公钥对用户上传的通信授权信息包括的数字签名信息进行身份验证。如果验证通过,则确定校验通过,则将上述通信授权信息对应的标识为设置为上述第一数值,并将处于已授权状态的通信授权信息存证在上述区块链中。

[0082] 在一些例子中,上述目标用户可以撤销已经授权的上述通信授权信息。上述目标用户可以通过客户端针对上述通信授权信息构建通信授权撤销请求。

[0083] 上述授权平台可以响应于上述目标用户发起的针对上述通信授权信息的通信授权撤销请求,调用上述智能合约中的撤销逻辑,将存证的上述通信授权信息由已授权状态更新为撤销状态。

[0084] 在一些例子中,上述通信授权撤销请求可以包括与上述通信授权信息对应的唯一存证ID。

[0085] 上述智能合约可以将该存证ID对应的通信授权信息的标识位设置为上述第二数值,表征上述通信授权信息为撤销状态。

[0086] 由此可以实现用户对通信授权信息的灵活管控,保护用户的利益。

[0087] 在一些例子中,在将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方时,上述授权平台可以将上述区块链中存证的与上述目标用户对应的通信授权信息,以及,与通信授权信息对应的状态发送至上述授权管理方。

[0088] 在一些例子中,上述查询请求包括与上述通信授权信息对应的唯一存证ID。上述授权平台可以调用上述智能合约包括的返回逻辑,获取与上述存证ID对应的通信授权信息,并获取上述通信授权信息对应的授权状态。然后上述智能合约可以通过上述授权平台将上述通信授权信息以及与通信授权信息对应的状态通过上述授权平台发送至上述授权管理方。

[0089] 由此一方面可以将授权管理方获取通信授权信息的记录存证至上述区块链,继而保证获取流程的透明化;另一方面,可以保证授权管理方获取真实可信的通信授权信息以及通信授权信息对应的状态,进而是授权管理方针对用户投诉做出正确的判别。

[0090] 在一些例子中,在执行S206存证通信授权信息时,上述授权平台可以对上述通信授权信息进行数据校验。如果校验通过,生成包含授权状态的授权记录,将上述授权记录存证至上述区块链。

[0091] 上述授权记录,具体是指可以表征上述发起方与上述目标用户之间的授权过程的记录信息。上述授权记录可以包括状态标识。上述状态标识可以表征授权记录是否为授权状态。在一些例子中,上述授权平台可以将上述状态标识置为第一数值,表征上述授权记录为已授权状态。

[0092] 上述数据交易与前述实施例相同,在此不作详述。

[0093] 在本例中,上述授权平台可以对通信授权信息进行校验,进而保证通信授权信息的真实性。

[0094] 在一些例子中,当接收到用户撤销请求时,上述授权平台可以响应于上述目标用户发起的针对上述通信授权信息的通信授权撤销请求,从上述区块链中获取上述通信授权信息。然后生成包含撤销状态的撤销记录,将上述撤销记录存证至上述区块链。

[0095] 上述撤销记录,用于表征上述通信授权信息的状态为撤销状态。

[0096] 由此,可以针对上述通信授权信息生成撤销状态的撤销记录,并覆盖之前的授权记录完成撤销上述用户与发起方之间的通信授权。

[0097] 在一些例子中,通信管理方发起的查询请求中包括与授权记录对应的存证ID。其中上述存证ID包括上述区块链在存证上述授权记录后返回的存证ID。

[0098] 在将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方时,上述授权平台可以根据上述查询请求包括的存证ID,从上述区块链中获取与上述存证ID对应的授权记录以及上述授权记录对应的授权状态。然后将上述通信授权信息以及与通信授权信息对应的状态通过上述授权平台发送至上述授权管理方。

[0099] 由此可以保证授权管理方获取真实可信的通信授权信息以及通信授权信息对应的状态,进而是授权管理方针对用户投诉做出正确的判别。

[0100] 在一些例子中,在执行S206存证通信授权信息时,上述授权平台可以对上述通信授权信息进行数据校验。如果校验通过,将上述通信授权信息发布至上述区块链进行存证,并获取与上述通信授权信息对应的存证标识。然后,在搭载的 centralized 数据库中存储上述存证标识,并将上述存证标识标记为已授权状态。

[0101] 在一些例子中,当接收到用户撤销请求时,上述授权平台可以响应于上述目标用户发起的通信授权撤销请求,将上述 centralized 数据库中存储的与上述通信授权信息对应的存证标识的由已授权状态更新为撤销状态。

[0102] 在一些例子中,通信管理方发起的查询请求中包括与授权记录对应的唯一身份ID。

[0103] 在将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方时,上述授权平台可以根据上述查询请求包括的身份ID,从上述 centralized 数据库中获取与上述身份ID对应的授权记录以及上述授权记录对应的授权状态。然后将上述通信授权信息以及与通信授权信息对应的状态通过上述授权平台发送至上述授权管理方。

[0104] 由此可以保证授权管理方获取真实可信的通信授权信息以及通信授权信息对应的状态,进而是授权管理方针对用户投诉做出正确的判别。

[0105] 以下结合呼叫授权场景进行实施例说明。

[0106] 请参见图3,图3为本申请示出的一种呼叫授权场景示意图。

[0107] 如图3所示,上述呼叫授权场景中包括有授权需求的企业B;上述企业B使用的呼叫平台C(以下简称平台C),以及通过呼叫平台C呼叫的用户A;以及授权平台D(以下简称平台D)。

[0108] 上述平台D包括基于区块链构建的业务平台。上述平台D可以包括区块链以及授权服务端E(以下简称授权宝E)。

[0109] 用户A与企业B可以预先在上述平台D中进行注册。完成注册后,平台D会向用户A与企业B分别返回公私钥对。其中,私钥可以用用户数字签名,公钥可以广播。

[0110] 企业B在向用户A发起呼叫之前,需要获取用户A的授权。

[0111] 请参见图4,图4为本申请示出的一种呼叫授权的流程图。

[0112] 此时,企业B可以执行S401,通过客户端填写针对用户A的授权模板,并构建授权请求发送至平台C。其中,上述授权模板可以包括企业B对应的数字签名。

[0113] 平台C可以执行S402,获取该授权请求中的授权模板,并将上述授权模板发送至授权宝E。

[0114] 授权宝E可以执行S403,基于上述通信授权模板生成通信授权页面,并存储上述通信授权页面,以及获取与上述通信授权页面对应的链接地址。

[0115] 之后,上述授权宝E可以执行S404,将上述链接地址返回平台C。

[0116] 上述平台C可以执行S405,将上述链接地址返回企业B。

[0117] 上述企业B可以执行S406,可以构建授权邀请信息,并通过短信方式将授权邀请信息以及链接地址发送至用户A。

[0118] 上述用户A可以执行S407,通过上述连接地址获取通信授权页面,并按照上述通信授权模板录入通信授权信息。其中,上述通信授权信息可以包括企业B对应的数字签名,以及用户A对应的数字签名。

[0119] 上述用户A可以执行S408,将上述通信授权信息发送至授权宝E。

[0120] 上述授权宝E可以执行S409,基于用户A与企业B的公钥对通信授权信息包括的数字签名进行身份验证。如果验证通过,则基于上述通信授权信息生成针对用户A与企业B的授权记录,并将该授权记录标识为已授权状态。

[0121] 然后,上述授权宝E可以执行S410,将已授权状态的授权记录存证至上述区块链。

[0122] 上述区块链返回与上述授权记录对应的存证ID。

[0123] 上述授权宝E一方面,执行S411,将上述存证ID返回至用户A完成通信授权;另一方面,执行S412,将上述授权记录发送至平台C,将授权结果通知给平台C,以使平台C存储上述授权结果。

[0124] 在这里,当授权宝E与多个平台C对接时,可以响应于任一平台的授权记录获取请求,向该平台返回授权记录,从而实现授权记录的共享,避免用户与企业针对每个平台重复进行授权流程。

[0125] 在上述方案中,平台D可以管控用户A与企业B之间的通信授权流程,并通过区块链存证用户A与企业B之间的授权记录,从一方面,可以对用户A与企业B之间的授权过程进行记录与监管,进而保证可以得到用户A真实的授权信息;另一方面,可以利用区块链透明度高,不可篡改等特性,保证存证的授权记录的可信性。

[0126] 以下介绍用户A撤销授权记录的实施例。

[0127] 请参见图5,图5为本申请示出的一种撤销授权记录的方法流程图。

[0128] 如图5所示,当有撤销授权记录需求时,用户A可以执行S501,构建撤销请求,并将上述撤销请求发送至上述授权宝E。其中上述撤销请求可以包括与上述授权记录对应的存证ID。

[0129] 上述授权宝E可以执行S502,响应于上述撤销请求,从上述区块链中获取与上述存

证ID对应的授权记录。然后,可以执行S503,将上述授权记录对应的状态标识置为撤销状态,并将包含撤销状态的授权记录存证至上述区块链以完成针对授权记录的撤销。

[0130] 之后,上述授权宝可以执行S504,向平台C通知该次撤销结果。

[0131] 由此,可以实现用户A对授权记录的灵活管控,保护用户A的权益。

[0132] 以下介绍监管方获取链上存证的授权记录的实施例。

[0133] 请参见图6,图6为本申请示出的一种获取授权记录的方法流程图。

[0134] 如图6所示,当用户A接收到企业B的短息或电话骚扰时,可以执行S601,向监管方发起投诉请求。其中,上述投诉请求可以包括与上述授权记录对应的存证ID。

[0135] 上述监管方可以执行S602,向上述授权宝E发送针对上述授权记录的查询请求。其中,上述查询请求包括上述存证ID。

[0136] 上述授权宝E可以执行S603,基于上述存证ID,从上述区块链中获取存证的授权记录,以及上述授权记录对应的状态标识。

[0137] 然后,上述授权宝E可以执行S604,将上述授权记录以及上述授权记录对应的状态标识返回至上述监管方。

[0138] 上述监管方可以根据上述授权记录以及上述状态标识对用户A发起的投诉进行处理。

[0139] 由此监管方可以获取真实可信的授权记录信息,进而可以做出公正可信的处理。

[0140] 与上述任一实施例相对应的,本申请还提出一种基于区块链的通信授权装置70。该装置70可以应用于基于上述区块链构建的授权平台。

[0141] 请参见图7,图7为本申请示出的一种基于区块链的通信授权装置的结构示意图。

[0142] 如图7所示,上述装置70可以包括:

[0143] 生成模块71,获取通信授权发起方通过与该通信授权发起方对应的通信管理平台上传的与目标用户对应的通信授权模板,并基于上述通信授权模板生成通信授权页面;

[0144] 返回模块72,将生成的上述通信授权页面的链接地址,通过上述通信管理平台返回给上述通信授权发起方,由上述通信发起方进一步将上述通信授权页面的链接地址返回给上述目标用户,以使上述目标用户访问与链接地址对应的通信授权页面,在上述通信授权页面中按照上述通信授权模板录入通信授权信息;

[0145] 发布模块73,获取上述目标用户提交的在上述通信授权页面中录入的通信授权信息,并将上述通信授权信息发布至上述区块链进行存证;

[0146] 发送模块74,响应于授权管理方发送的与上述目标用户对应的通信授权信息的查询请求,将上述区块链中存证的与上述目标用户对应的通信授权信息发送至上述通信管理方。

[0147] 在示出的一些实施例中,上述授权平台对接多个通信管理平台;上述装置70还包括:

[0148] 接收模块,接收上述多个通信管理平台中的任N个通信管理平台发起的授权记录查询请求;

[0149] 存证模块,将存证的授权记录发送至上述任N个通信运营商完成授权记录的共享。

[0150] 在示出的一些实施例中,上述授权平台包括区块链即服务BaaS平台;以及,与区块链即服务BaaS平台连接的若干台区块链节点设备。

[0151] 在示出的一些实施例中,上述区块链部署了用于对通信授权信息进行管理的智能合约;上述发布模块73具体用于:

[0152] 调用合约的校验逻辑对上述通信授权信息进行数据校验;如果校验通过,调用合约的存证逻辑在区块链存证上述通信授权信息,并将存证的上述通信授权信息存证标记为已授权状态。

[0153] 在示出的一些实施例中,上述装置70还包括:

[0154] 第一更新模块,响应于上述目标用户发起的针对上述通信授权信息的通信授权撤销请求,调用上述智能合约中的撤销逻辑,将存证的上述通信授权信息由已授权状态更新为撤销状态。

[0155] 在示出的一些实施例中,上述发布模块73具体用于:

[0156] 对上述通信授权信息进行数据校验;

[0157] 如果校验通过,生成包含授权状态的授权记录,将上述授权记录存证至上述区块链。

[0158] 在示出的一些实施例中,上述装置70还包括:

[0159] 第二更新模块,响应于上述目标用户发起的针对上述授权记录的通信授权撤销请求,从上述区块链中获取上述授权记录;

[0160] 将上述授权记录对应的状态标识置为撤销状态,并将包含撤销状态的授权记录存证至上述区块链。

[0161] 在示出的一些实施例中,上述发布模块73具体用于:

[0162] 对上述通信授权信息进行数据校验;

[0163] 如果校验通过,将上述通信授权信息发布至上述区块链进行存证,并获取与上述通信授权信息对应的存证标识;

[0164] 在搭载的 centralized 数据库中存储上述存证标识,并将上述存证标识标记为已授权状态。

[0165] 在示出的一些实施例中,上述装置70还包括:

[0166] 第三更新模块,响应于上述目标用户发起的通信授权撤销请求,将上述 centralized 数据库中存储的与上述通信授权信息对应的存证标识的由已授权状态更新为撤销状态。

[0167] 在示出的一些实施例中,上述发送模块74具体用于:

[0168] 将上述区块链中存证的与上述目标用户对应的通信授权信息,以及,与通信授权信息对应的状态发送至上述授权管理方。

[0169] 在示出的一些实施例中,上述通信管理平台包括云呼叫平台;上述通信授权包括云呼叫授权。

[0170] 本申请示出的基于区块链的通信授权装置的实施例可以应用于电子设备上。相应地,本申请公开了一种电子设备。该设备可以包括:处理器。

[0171] 用于存储处理器可执行指令的存储器。

[0172] 其中,上述处理器被配置为调用上述存储器中存储的可执行指令,实现如上述任一实施例示出的通信授权方法。

[0173] 请参见图8,图8为本申请示出的一种电子设备的硬件结构示意图。

[0174] 如图8所示,该电子设备可以包括用于执行指令的处理器,用于进行网络连接的网

络接口,用于为处理器存储运行数据的内存,以及用于存储通信授权装置对应指令的非易失性存储器。

[0175] 其中,通信授权装置的实施例可以通过软件实现,也可以通过硬件或者软硬件结合的方式实现。以软件实现为例,作为一个逻辑意义上的装置,是通过其所在电子设备的处理器将非易失性存储器中对应的计算机程序指令读取到内存中运行形成的。从硬件层面而言,除了图8所示的处理器、内存、网络接口、以及非易失性存储器之外,实施例中装置所在的电子设备通常根据该电子设备的实际功能,还可以包括其他硬件,对此不再赘述。

[0176] 可以理解的是,为了提升处理速度,通信授权装置对应指令也可以直接存储于内存中,在此不作限定。

[0177] 本申请提出一种计算机可读存储介质。上述存储介质存储有计算机程序,上述计算机程序用于执行上述任一实施例示出的通信授权方法。

[0178] 本领域技术人员应明白,本申请一个或多个实施例可提供为方法、系统或计算机程序产品。因此,本申请一个或多个实施例可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且,本申请一个或多个实施例可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(可以包括但不限于磁盘存储器、CD-ROM、光学存储器等)上述实施的计算机程序产品的形式。

[0179] 本申请中的“和/或”表示至少具有两者中的其中一个,例如,“A和/或B”可以包括三种方案:A、B、以及“A和B”。

[0180] 本申请中的各个实施例均采用递进的方式描述,各个实施例之间相同相似的部分互相参见即可,每个实施例重点说明的都是与其他实施例的不同之处。尤其,对于数据处理设备实施例而言,由于其基本相似于方法实施例,所以描述的比较简单,相关之处参见方法实施例的部分说明即可。

[0181] 上述对本申请特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下,在权利要求书中记载的行为或步骤可以按照不同于实施例中的顺序来执行并且仍然可以实现期望的结果。另外,在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中,多任务处理和并行处理也是可以的或者可能是有利的。

[0182] 本申请中描述的主题及功能操作的实施例可以在以下中实现:数字电子电路、有形体现的计算机软件或固件、可以包括本申请中公开的结构及其结构性等同物的计算机硬件、或者它们中的一个或多个的组合。本申请中描述的主题的实施例可以实现为一个或多个计算机程序,即编码在有形非暂时性程序载体上上述以被数据处理装置执行或控制参数处理装置的操作的计算机程序指令中的一个或多个模块。可替代地或附加地,程序指令可以被编码在人工生成的传播信号上,例如机器生成的电、光或电磁信号,该信号被生成以将信息编码并传输到合适的接收机装置以由数据处理装置执行。计算机存储介质可以是机器可读存储设备、机器可读存储基板、随机或串行存取存储器设备、或它们中的一个或多个的组合。

[0183] 本申请中描述的处理及逻辑流程可以由执行一个或多个计算机程序的一个或多个可编程计算机执行,以通过根据输入数据进行操作并生成输出来执行相应的功能。上述处理及逻辑流程还可以由专用逻辑电路—例如FPGA(现场可编程门阵列)或ASIC(专用集成

电路)来执行,并且装置也可以实现为专用逻辑电路。

[0184] 适合用于执行计算机程序的计算机可以包括,例如通用和/或专用微处理器,或任何其他类型的中央处理单元。通常,中央处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的基本组件可以包括用于实施或执行指令的中央处理单元以及用于存储指令和数据的一个或多个存储器设备。通常,计算机还将可以包括用于存储数据的一个或多个大容量存储设备,例如磁盘、磁光盘或光盘等,或者计算机将可操作地与此大容量存储设备耦接以从其接收数据或向其传送数据,抑或两种情况兼而有之。然而,计算机不是必须具有这样的设备。此外,计算机可以嵌入在另一设备中,例如移动电话、个人数字助理(PDA)、移动音频或视频播放器、游戏操纵台、全球定位系统(GPS)接收机、或例如通用串行总线(USB)闪存驱动器的便携式存储设备,仅举几例。

[0185] 适合于存储计算机程序指令和数据的计算机可读介质可以包括所有形式的非易失性存储器、媒介和存储器设备,例如可以包括半导体存储器设备(例如EPROM、EEPROM和闪存设备)、磁盘(例如内部硬盘或可移动盘)、磁光盘以及CD ROM和DVD-ROM盘。处理器和存储器可由专用逻辑电路补充或并入专用逻辑电路中。

[0186] 虽然本申请包含许多具体实施细节,但是这些不应被解释为限制任何公开的范围或所要求保护的公开的范围,而是主要用于描述特定公开的具体实施例的特征。本申请内在多个实施例中描述的某些特征也可以在单个实施例中被组合实施。另一方面,在单个实施例中描述的各种特征也可以在多个实施例中分开实施或以任何合适的子组合来实施。此外,虽然特征可以如上述在某些组合中起作用并且甚至最初如此要求保护,但是来自所要求保护的组合中的一个或多个特征在一些情况下可以从该组合中去除,并且所要求保护的组合可以指向子组合或子组合的变型。

[0187] 类似地,虽然在附图中以特定顺序描绘了操作,但是这不应被理解为要求这些操作以所示的特定顺序执行或顺次执行、或者要求所有例示的操作被执行,以实现期望的结果。在某些情况下,多任务和并行处理可能是有利的。此外,上述实施例中的各种系统模块和组件的分离不应被理解为在所有实施例中均需要这样的分离,并且应当理解,所描述的程序组件和系统通常可以一起集成在单个软件产品中,或者封装成多个软件产品。

[0188] 由此,主题的特定实施例已被描述。其他实施例在所附权利要求书的范围以内。在某些情况下,权利要求书中记载的动作可以以不同的顺序执行并且仍实现期望的结果。此外,附图中描绘的处理并非必需所示的特定顺序或顺次顺序,以实现期望的结果。在某些实现中,多任务和并行处理可能是有利的。

[0189] 以上仅为本申请一个或多个实施例的较佳实施例而已,并不用以限制本申请一个或多个实施例,凡在本申请一个或多个实施例的精神和原则之内,所做的任何修改、等同替换、改进等,均应包含在本申请一个或多个实施例保护的范围内。

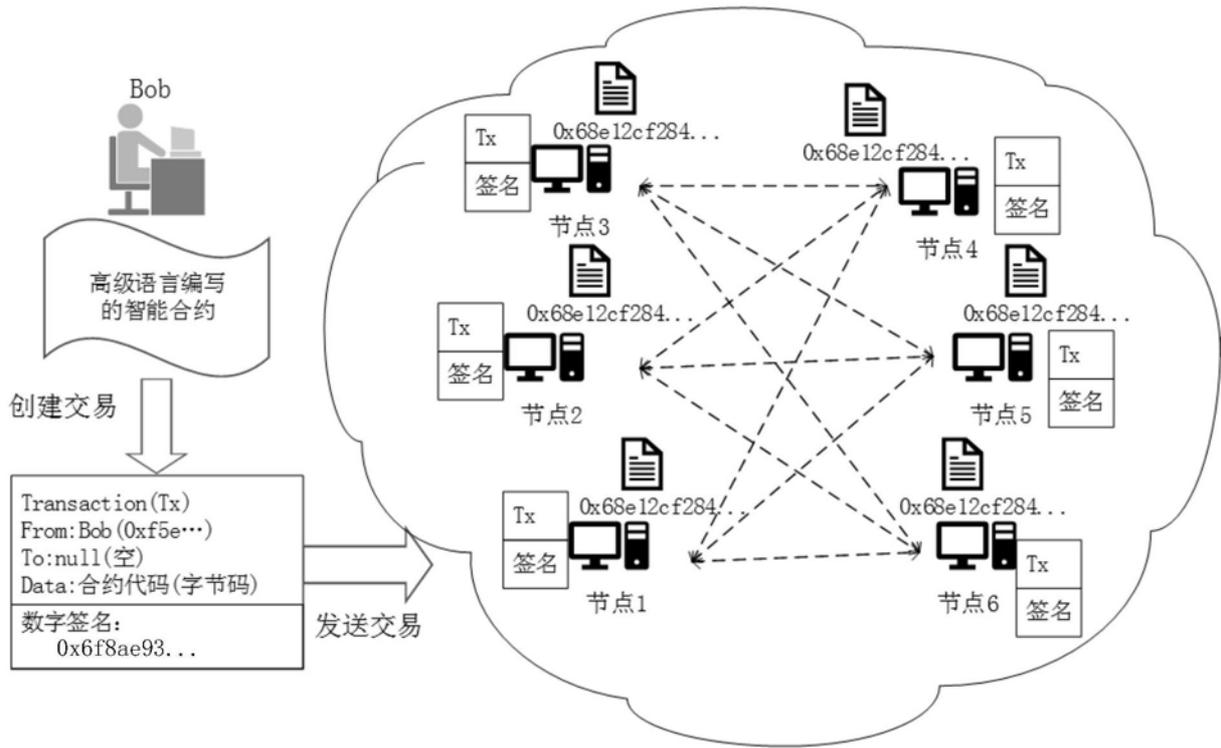


图1

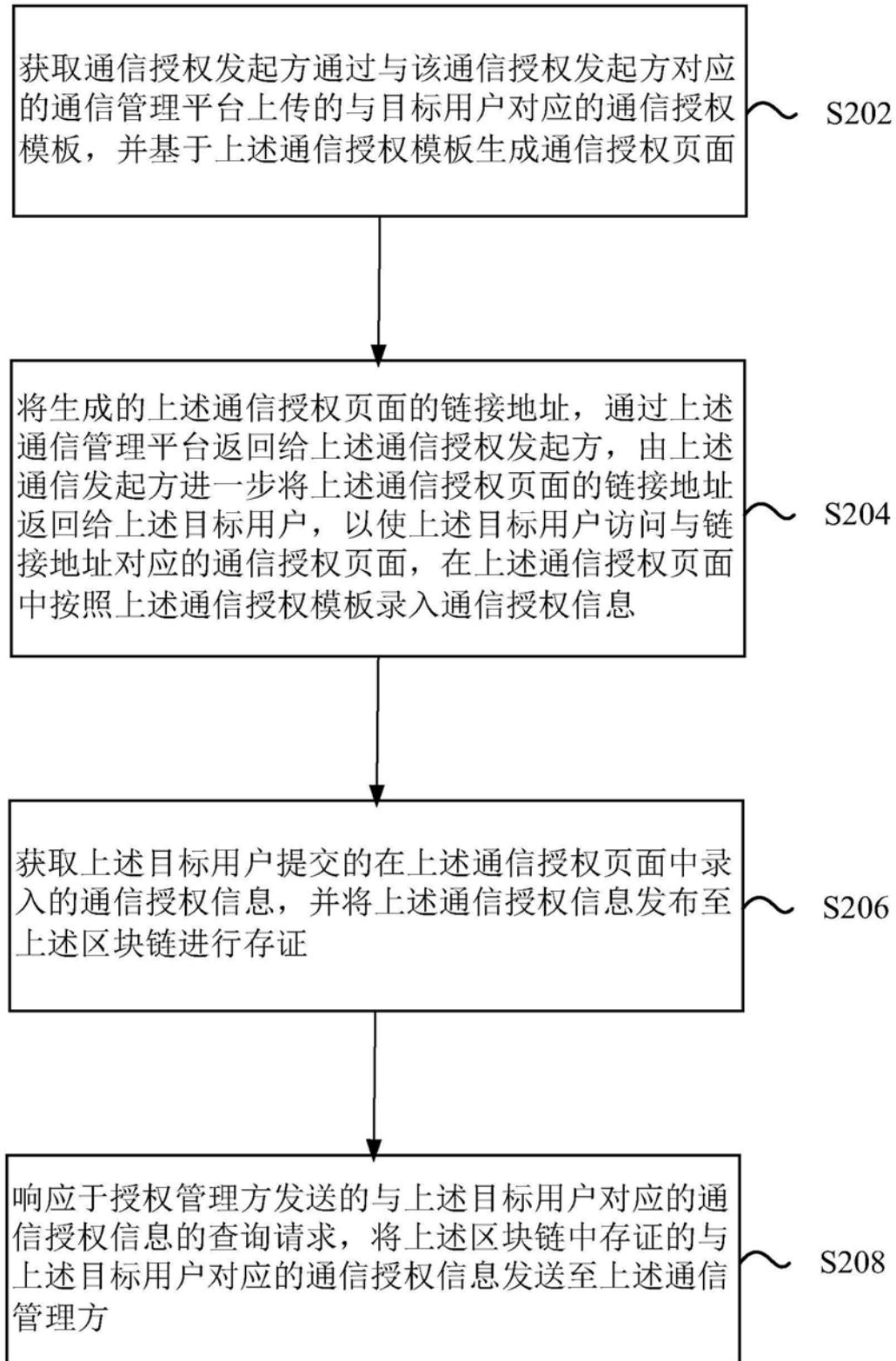


图2

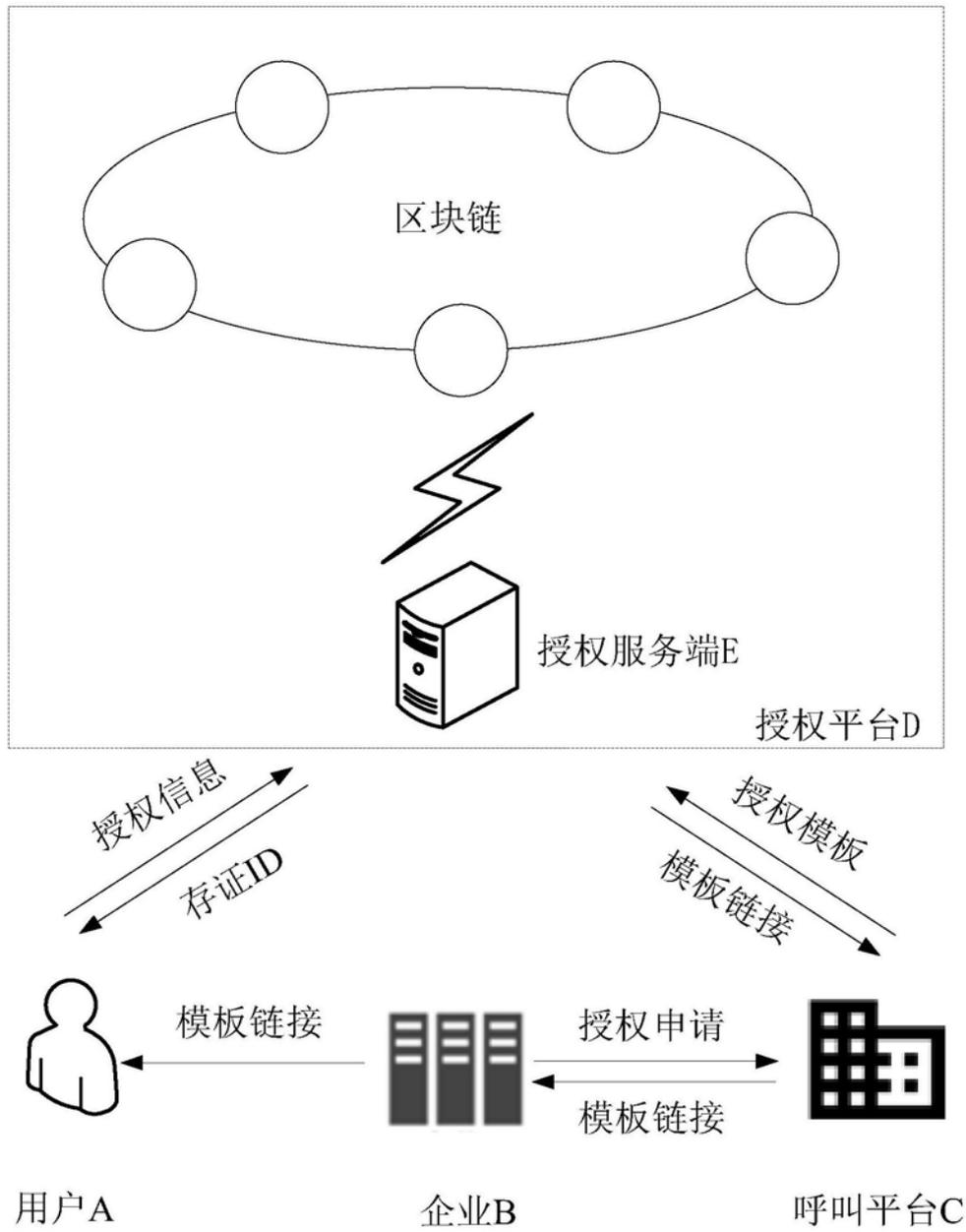


图3

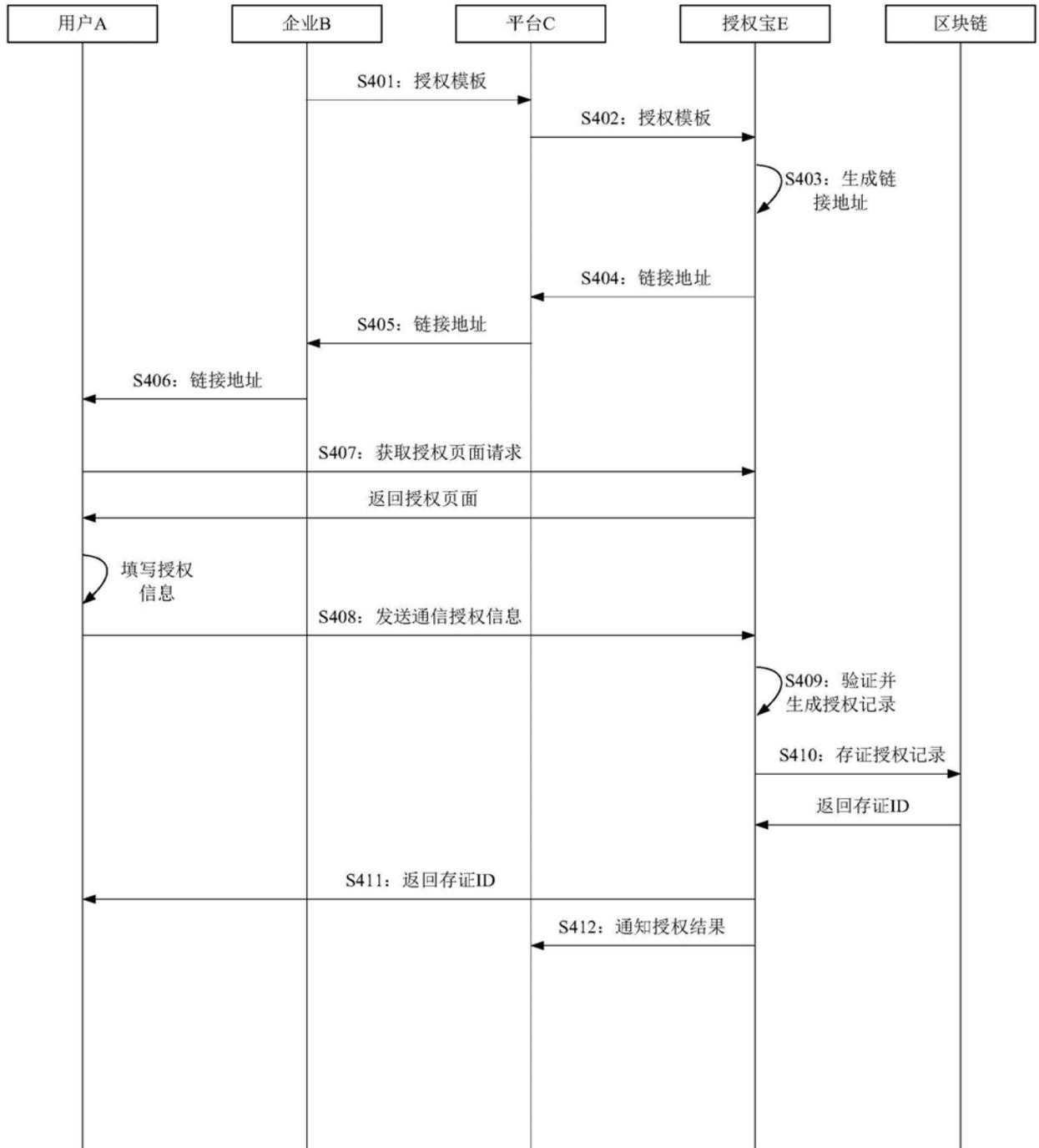


图4

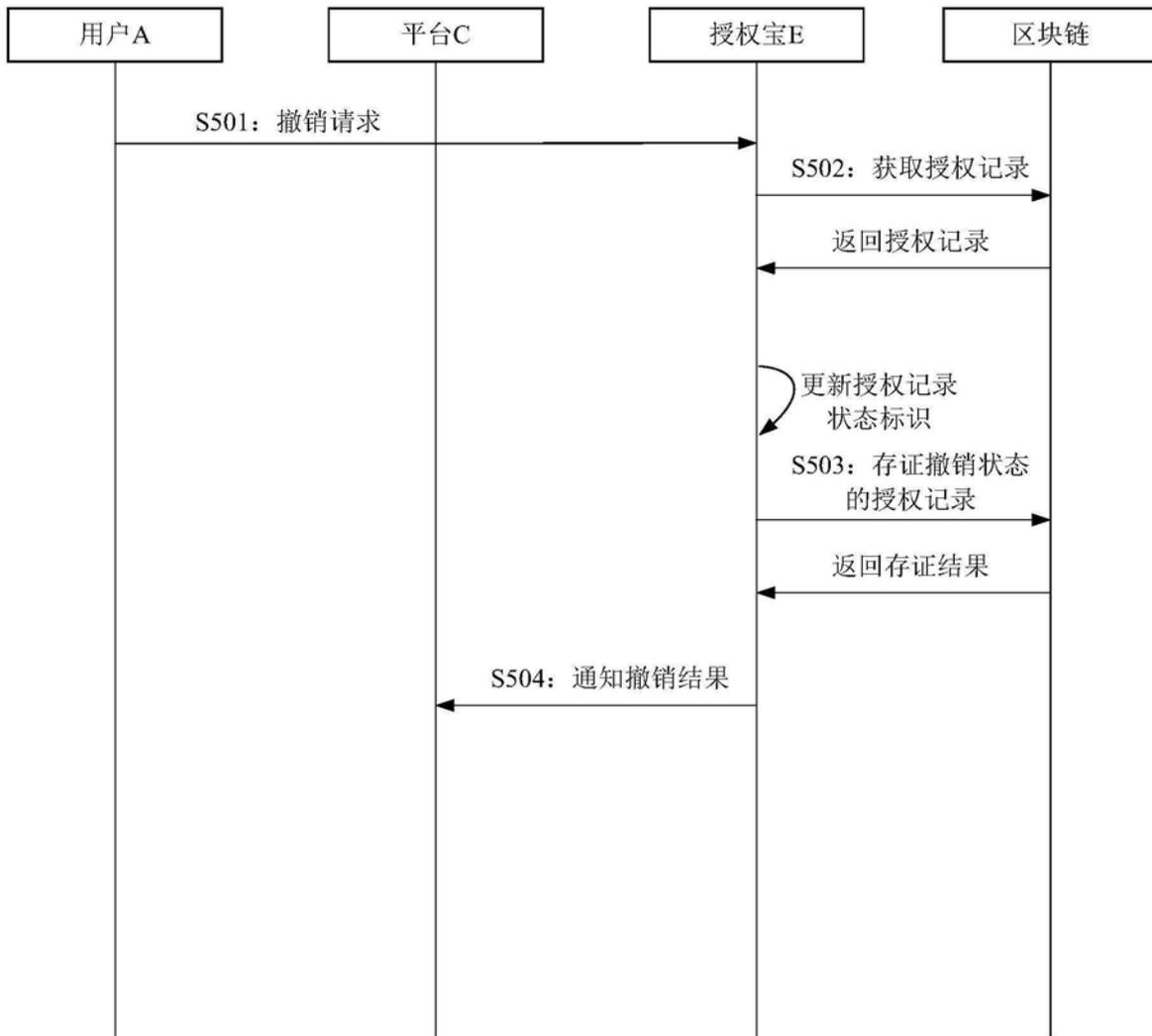


图5

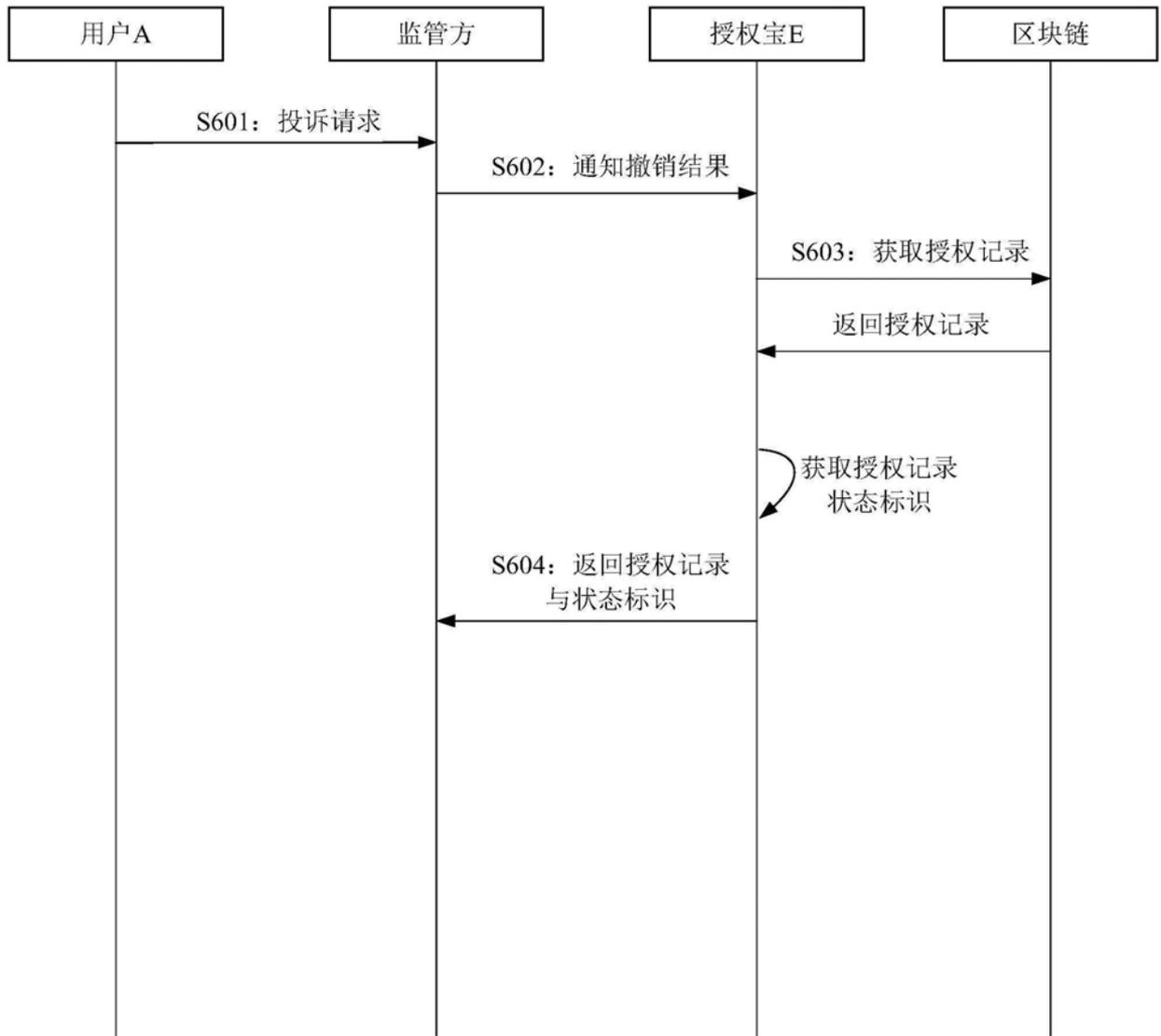


图6

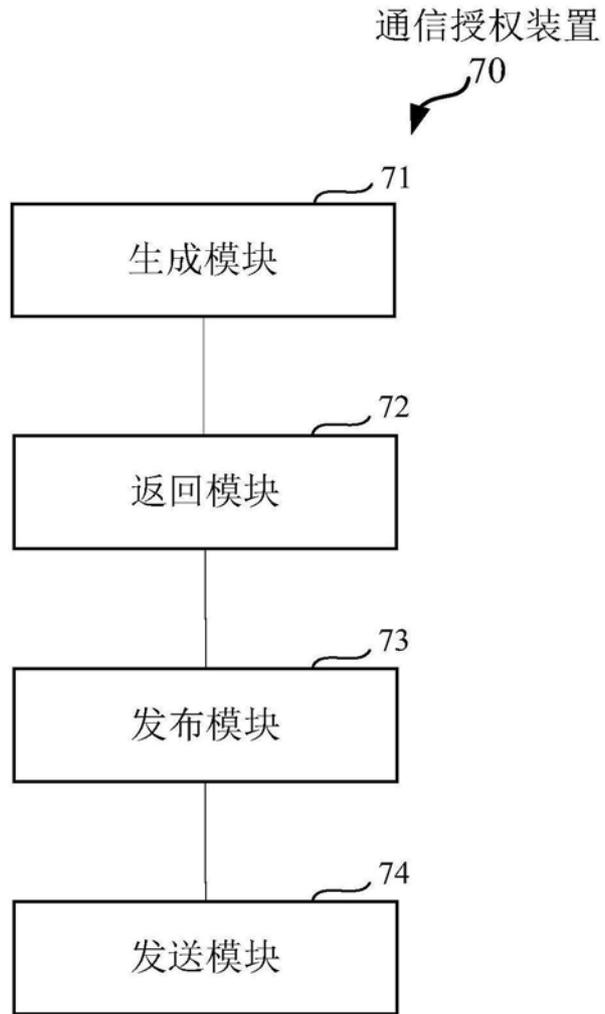


图7

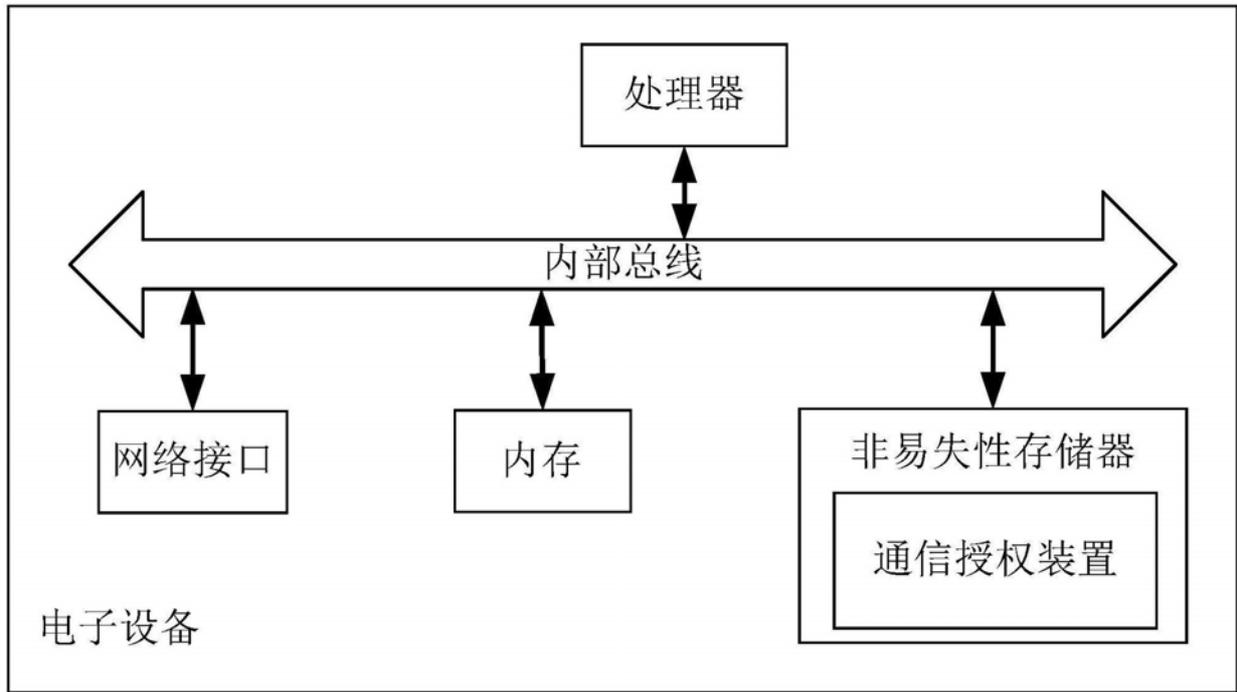


图8