

(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
2022 年 10 月 27 日 (27.10.2022)



(10) 国际公布号
WO 2022/222722 A1

(51) 国际专利分类号:
H04L 9/08 (2006.01) **H04L 9/32** (2006.01)

(21) 国际申请号: PCT/CN2022/084185

(22) 国际申请日: 2022 年 3 月 30 日 (30.03.2022)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202110419392.5 2021 年 4 月 19 日 (19.04.2021) CN
202111203497.3 2021 年 10 月 15 日 (15.10.2021) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION CO., LTD RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。中国移动通信集团有限公司 (CHINA MOBILE COMMUNICATIONS GROUP CO., LTD.) [CN/CN]; 中国北京市西城区金融大街 29 号, Beijing 100032 (CN)。

(72) 发明人: 刘福文 (LIU, Fuwen); 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。阎军智 (YAN, Junzhi); 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。杨波 (YANG, Bo); 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。栗栗 (SU, Li); 中国北京

市西城区宣武门西大街 32 号, Beijing 100053 (CN)。何申 (HE, Shen); 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。

(74) 代理人: 北京派特恩知识产权代理有限公司 (CHINA PAT INTELLECTUAL PROPERTY OFFICE); 中国北京市海淀区海淀南路 21 号中关村知识产权大厦 B 座 2 层, Beijing 100080 (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, IT, JM, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT,

(54) Title: ID-PKC INFORMATION PROCESSING METHOD AND APPARATUS, AND NODE AND STORAGE MEDIUM

(54) 发明名称: ID-PKC 信息处理方法、装置、节点及存储介质

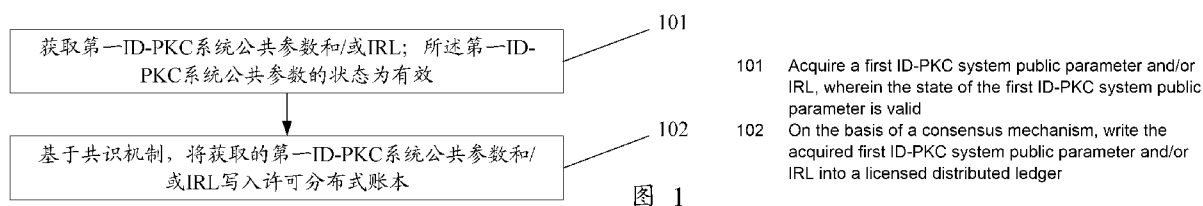


图 1

(57) Abstract: Disclosed in the present application are an identity-based public key cryptograph (ID-PKC) information processing method and apparatus, and a node and a storage medium. The method comprises: a first node acquiring a first ID-PKC system public parameter and/or identity revocation list (IRL), wherein the state of the first ID-PKC system public parameter is valid, and the first node is an accounting node; and on the basis of a consensus mechanism, writing the acquired first ID-PKC system public parameter and/or IRL into a licensed distributed ledger.

(57) 摘要: 本申请公开了一种基于标识的公共密码 (ID-PKC) 信息处理方法、装置、节点及存储介质。其中, 方法包括: 第一节点获取第一 ID-PKC 系统公共参数和/或标识吊销列表 (IRL); 所述第一 ID-PKC 系统公共参数的状态为有效; 所述第一节点为记账节点; 基于共识机制, 将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

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))。

ID-PKC 信息处理方法、装置、节点及存储介质

相关申请的交叉引用

本申请基于申请号为 202110419392.5、申请日为 2021 年 04 月 19 日的中国专利，以及申请号为 202111203497.3、申请日为 2021 年 10 月 15 日的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本申请作为参考。

技术领域

本申请涉及网络安全技术领域，尤其涉及一种基于标识的公共密码（ID-PKC，IDentity-based Public Key Cryptograph）信息处理方法、装置、节点及存储介质。

背景技术

ID-PKC 系统中，不需要使用证书传递公钥，因此不再依赖证书和证书管理系统。在 ID-PKC 系统中，ID-PKC 系统的公共参数和/或标识吊销列表（IRL，Identity Revocation List）不需要加密传输，但是传递时不能有任何改动，因此，相关技术中，通过使用传输层安全（TLS）协议来实现 ID-PKC 系统公共参数和 IRL 传递的安全性。

然而，使用 TLS 协议时 TLS 安全通道的建立需要使用证书，也就是说，ID-PKC 系统的引导过程实际上依赖于基于公钥基础设施（PKI）的公共密码（PKI-PKC，PKI based Public Key Cryptography）系统，这样会使得 PKI-PKC 系统的缺陷引入到 ID-PKC 系统。

发明内容

为解决相关技术问题，本申请实施例提供一种 ID-PKC 信息处理方法、装置、节点及存储介质。

本申请实施例的技术方案是这样实现的：

本申请实施例提供一种 ID-PKC 信息处理方法，应用于第一节点，包括：获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；

基于共识机制，将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

上述方案中，所述第一 ID-PKC 系统公共参数由密钥生成中心（KGC，

Key Generate Center) 的公共参数服务器 (PPS, Public Key Server) 生成;
所述第一 ID-PKC 系统公共参数至少包括以下至少之一:

域名称;

区块链名称;

系统公共参数状态;

用于隐藏用户标识的哈希算法。

上述方案中, 所述域名称为按照统一资源标识符 (URI) 或统一资源定位器 (URL) 定义的名称, 或为自定义的名称。

上述方案中, 所述第一 ID-PKC 系统公共参数还包括:

PPS 名称;

标识管理服务器 (IMS, Identity Management Server) 名称。

上述方案中, 所述 PPS 名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

上述方案中, 所述为按照 URI 或 URL 定义的名称, 或为自定义的名称。

上述方案中, 所述 IRL 由 KGC 的 IMS 生成;

所述 IRL 至少包括以下至少之一:

域名称;

区块链名称;

吊销标识集合。

上述方案中, 所述域名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

上述方案中, 所述 IRL 还包括:

IMS 名称。

上述方案中, 所述 IMS 名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

上述方案中, 所述吊销标识集合包含以下至少之一:

吊销标识是否匿名;

吊销标识;

吊销原因。

上述方案中, 所述方法还包括:

获取第二 ID-PKC 系统公共参数; 所述第二 ID-PKC 系统公共参数的状态为无效; 所述第二 ID-PKC 系统公共参数与第一 ID-PKC 系统公共参数除生产时间和状态外的其他参数相同;

基于共识机制, 将获取的第二 ID-PKC 系统公共参数写入所述许可分布式账本;

获取新生成的第三 ID-PKC 系统公共参数; 所述第三 ID-PKC 系统公共参数是所述第一 ID-PKC 系统公共参数更新的; 所述第三 ID-PKC 系统公共参数的状态为有效;

基于共识机制,将获取的第三 ID-PKC 系统公共参数写入所述许可分布式账本。

本申请实施例还提供一种 ID-PKC 信息处理方法,应用于第二节点,包括:

- 5 获取第一请求; 所述第一请求用于请求获取 ID-PKC 系统公共参数;
从许可分布式账本查询对应的 ID-PKC 系统公共参数;
根据查询结果返回响应。

上述方案中,所述从许可分布式账本查询对应的 ID-PKC 系统公共参数时,所述方法包括:

- 10 从所述许可分布式账本最新的区块开始查询。

上述方案中,所述第一请求携带域名称以及区块链名称;

利用所述第一请求携带的域名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

上述方案中,所述第一请求还携带 PPS 名称;

- 15 利用所述第一请求携带的域名称和/或 PPS 名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

上述方案中,所述根据查询结果返回响应,包括:

当未查询到对应的 ID-PKC 系统公共参数时,返回错误信息;

或者,

- 20 当查询到对应的 ID-PKC 系统公共参数,且查询到的 ID-PKC 系统公共参数的状态为无效时,返回错误信息;

或者,

当查询到对应的 ID-PKC 系统公共参数,且查询到的 ID-PKC 系统公共参数的状态为有效时,返回查询到的 ID-PKC 系统公共参数。

- 25 本申请实施例还提供一种 ID-PKC 信息处理方法,应用于第三节点,包括:

获取第二请求; 所述第二请求用于请求查询第一标识是否已被吊销;

从许可分布式账本查询第一标识是否已被吊销; 所述许可分布式账本记录有 IRL;

- 30 根据查询结果返回响应。

上述方案中,所述第二请求携带所述第一标识及区块链名称; 利用所述第一标识在所述区块链名称对应的许可分布式账本进行查询。

上述方案中,所述第二请求携带对所述第一标识利用 ID-PKC 系统公共参数指示的哈希函数进行运算后的运算结果及区块链名称;

- 35 利用所述运算结果在所述区块链名称对应的许可分布式账本进行查询。

上述方案中,所述根据查询结果返回响应,包括:

当查询到所述第一标识已被吊销时,返回第一信息; 所述第一信息指示所述第一标识已被吊销;

或者，

当未查找到所述第一标识时，返回第二信息；所述第二信息指示所述第一标识有效。

本申请实施例还提供一种 ID-PKC 信息处理装置，设置在第一节点上，
5 包括：

第一获取单元，配置为获取第一 ID-PKC 系统公共参数和/或 IRL；所述
第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；

第一处理单元，配置为基于共识机制，将获取的第一 ID-PKC 系统公共
参数和/或 IRL 写入许可分布式账本。

10 本申请实施例还提供一种 ID-PKC 信息处理装置，包括：

第二获取单元，配置为获取第一请求；所述第一请求用于请求获取
ID-PKC 系统公共参数；

第二处理单元，配置为从许可分布式账本查询对应的 ID-PKC 系统公共
参数；根据查询结果返回响应。

15 本申请实施例还提供一种 ID-PKC 信息处理装置，包括：

第三获取单元，配置为获取第二请求；所述第二请求用于请求查询第
一标识是否已被吊销；

第三处理单元，配置为从许可分布式账本查询第一标识是否已被吊销；
所述许可分布式账本记录有 IRL；根据查询结果返回响应。

20 本申请实施例还提供一种第一节点，包括：第一通信接口及第一处理
器；其中，

所述第一通信接口，配置为获取第一 ID-PKC 系统公共参数和/或 IRL；
所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；

25 第一处理器，配置为基于共识机制，将获取的第一 ID-PKC 系统公共参
数和/或 IRL 写入许可分布式账本。

本申请实施例还提供一种第二节点，包括：第二通信接口及第二处理
器；其中，

所述第二通信接口，配置为获取第一请求；所述第一请求用于请求获
取 ID-PKC 系统公共参数；

30 所述第二处理器，配置为从许可分布式账本查询对应的 ID-PKC 系统公
共参数；根据查询结果通过所述第二通信接口返回响应。

本申请实施例还提供一种第三节点，包括：第三通信接口及第三处理
器；其中，

35 所述第三通信接口，配置为获取第二请求；所述第二请求用于请求查
询第一标识是否已被吊销；

所述第三处理器，配置为从许可分布式账本查询第一标识是否已被吊
销；所述许可分布式账本记录有 IRL；根据查询结果通过所述第三通信接口
返回响应。

本申请实施例还提供一种第一节点，包括：第一处理器和配置为存储能够在处理器上运行的计算机程序的第一存储器，

其中，所述第一处理器配置为运行所述计算机程序时，执行所述第一节点侧任一方法的步骤。

5 本申请实施例还提供一种第二节点，包括：第二处理器和配置为存储能够在处理器上运行的计算机程序的第二存储器，

其中，所述第二处理器配置为运行所述计算机程序时，执行上述第二节点侧任一方法的步骤。

10 本申请实施例还提供一种第三节点，包括：第三处理器和配置为存储能够在处理器上运行的计算机程序的第三存储器，

其中，所述第三处理器配置为运行所述计算机程序时，执行上述第三节点侧任一方法的步骤。

15 本申请实施例还提供一种存储介质，其上存储有计算机程序，所述计算机程序被处理器执行时实现上述第一节点侧任一方法的步骤，或者实现上述第二节点侧任一方法的步骤，或者实现上述第三节点侧任一方法的步骤。

20 本申请实施例提供的 ID-PKC 信息处理方法、装置、节点及存储介质，第一节点获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；基于共识机制，将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本；第二节点获取第一请求；所述第一请求用于请求获取 ID-PKC 系统公共参数；从许可分布式账本查询对应的 ID-PKC 系统公共参数；并根据查询结果返回响应；第三节点获取第二请求；所述第二请求用于请求查询第一标识是否已被吊销；从许可分布式账本查询第一标识是否已被吊销；所述许可分布式账本记录有 IRL；并根据查询结果返回响应。本申请实施例提供的方案，基于许可分布式账本进行 ID-PKC 系统公共参数的发布和标识撤销的管理，通过使用许可分布式账本，ID-PKC 系统参数和 IRL 可以跨域传递，并使得标识吊销能够跨域查询，从而实现了不依赖于 PKI-PKC 系统，使用 ID-PKC 系统就能实现跨域安全通信。

30 附图说明

图 1 为本申请实施例一种 ID-PKC 信息处理的方法流程示意图；
图 2 为本申请实施例第二种 ID-PKC 信息处理的方法流程示意图；
图 3 为本申请实施例第二种 ID-PKC 信息处理的方法流程示意图；
图 4 为本申请实施例第一种 ID-PKC 信息处理装置结构示意图；
35 图 5 为本申请实施例第二种 ID-PKC 信息处理装置结构示意图；
图 6 为本申请实施例第三种 ID-PKC 信息处理装置结构示意图；

图 7 为本申请实施例第一节点结构示意图;
图 8 为本申请实施例第二节点结构示意图;
图 9 为本申请实施例第三节点结构示意图。

具体实施方式

下面结合实施例对本申请再作进一步详细的描述。

在描述本申请实施例之前,先了解一下相关技术。

传统的基于证书的密钥系统中,通过在证书中公钥和标识的绑定,并由可信的第三方认证中心(CA, Certification Authority)签名实现用户标识和公钥的可验证性传播。虽然基于证书密钥系统已得到广泛的应用,但存在

(1) 在安全应用中需要交换证书;

(2) 证书使用时需要验证有效性;

(3) 证书的颁发和管理非常复杂。

为了解决依赖证书和证书管理系统的基于证书密钥系统比如 PKI-PKC 系统的上述这些问题,以色列密码学家 Shamir 于 1984 年提出 ID-PKC 体系,也可以称为(基于标识的密码(IBC, Identity-Based Cryptograph)体系)。在 ID-PKC 体系中,最主要的观点是不需要使用证书传递公钥,而是使用用户标识如姓名、网际互联协议(IP)地址、电子邮箱地址、或手机号码等代表用户的标识信息作为公钥,私钥则由 KGC 根据系统主密钥和用户标识计算得出,因此,这类系统就不再依赖证书和证书管理系统(比如 PKI-PKC 系统),从而极大地简化了管理密码系统的复杂性。在提出 ID-PKC 概念的同时,Shamir 提出了一个采用 RSA 算法的基于标识的签名算法(IFS)。然而基于标识的加密算法(IBE, Identity Based Encryption)长时期未能找到有效解决方法。直到 2001 年,D. Boneh 和 M. Franklin 提出的基于椭圆曲线上的对(pairing)才实现了安全的 IBE 系统。目前比较高效的基于标识的签名算法是采用椭圆曲线的基于椭圆曲线无证书签名用于基于标识的加密(ECCSI, The Elliptic Curve-based Certificateless Signatures for Identity-based Encryption)方案。

ID-PKC 系统公共参数不需要加密传输,但是要求传递时不能有任何改动(即需要保证完整性),这是因为公共参数的完整性对于正确使用 ID-PKC 系统至关重要。在域内初始化 ID-PKC 系统要比跨域相对容易,域内的用户可以安全地(例如通过离线方法)获取用户私钥和 ID-PKC 系统的公共参数。可以通过使用传输层安全(TLS)协议来实现 ID-PKC 系统的用户私钥和公共参数传递的安全性,即在用户和 KGC 之间建立 TLS 安全通道,通过 TLS 安全通道传递 ID-PKC 系统公共参数。

另一方面, ID-PKC 系统中需要标识吊销,以防止继续使用不再有效或

存在安全漏洞的身份或凭证，例如服务中止或私钥泄露。撤销标识的，应当将标识设置为撤销状态。吊销的标识构成 IRL，向用户传递 IRL 也需要一个可靠的渠道。可以通过在用户和 KGC 之间建立的 TLS 安全通道传递 IRL。

然而，TLS 安全通道的建立需要使用证书，这就意味着 ID-PKC 系统的引导过程实际上依赖于 PKI，这与 ID-PKC 系统的最初设计意图背道而驰。此外，基于证书的密钥系统中的多 CA 信任问题被传导到 ID-PKC 系统。

基于此，在本申请的各种实施例，基于许可分布式账本进行 ID-PKC 系统公共参数的发布和标识撤销的管理。

本申请实施例中，将 ID-PKC 系统的公共参数和/或 IRL 通过许可分布式账本的共识机制写入许可分布式账本，通过使用许可分布式账本，ID-PKC 系统参数和 IRL 可以跨域传递，并使得标识吊销能够跨域查询，从而实现了不依赖于 PKI 系统，使用 ID-PKC 系统就能实现跨域安全通信。

本申请实施例提供一种 ID-PKC 信息处理方法，应用于第一节点，如图 1 所示，该方法包括：

步骤 101：获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；

步骤 102：基于共识机制，将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

这里，实际应用时，所述 ID-PKC 系统公共参数也可以称为 ID-PKC 系统参数，或者 ID-PKC 参数，需要说明的是，所述 ID-PKC 系统公共参数也可以被命名为其他名称，只要是与 ID-PKC 系统公共参数的功能或作用相同即可，本申请实施例对此不作限定。相应地，IRL 也可以采用其他名称，只要是与 IRL 的功能或作用相同即可，本申请实施例对此不作限定。

所述许可分布式账本（也可以称为联盟链或者许可链，许可分布式账本，联盟链，许可链这三者是同义词，具有相同的意义）是区块链，是指由若干个机构共同参与管理的区块链。许可分布式账本内部指定多个预选的节点为记账节点，每个块的生成由所有的预选节点使用共识机制共同决定，其他接入节点可以读取链上信息，但不过问记账过程。许可分布式账本使用分布式账本和分布式共识技术从而构成数据不可篡改的分布式数据库。只要在链上发布的信息就是真实可信的。

在本申请实施例中，所述机构可以包括一个域的 KGC。一个域的 KGC 可以对应一个或多个记账节点。

实际应用时，所述第一 ID-PKC 系统公共参数可由 KGC 生成。这里，需要说明的是：本申请实施例对生成的 ID-PKC 系统公共参数的机构的名称不作限定。

其中，KGC 通常包含以下三部分：

私钥生成器（PKG，Private Key Generator），配置为根据 ID-PKC 系统

安全存储的主密码和用户身份生成用户私钥。私钥通过安全通道分发给用户，提供机密性和完整性保护。因此，只有具有关联身份的用户才知道私钥。

PPS，配置为向用户提供 ID-PKC 系统公共参数和描述 PKG 操作的策略信息。由于公共参数和策略信息的完整性对 ID-PKC 系统的正常运行至关重要，因此用户与 PPS 之间的通信通道应是可信的。这里，实际应用时，用户和 PPS 之间的通信通道不一定是保密的，因为公共参数和策略信息是任何人都可以获取的公共信息。因此，所述第一 ID-PKC 系统公共参数可由 KGC 的 PPS 生成。

IMS，配置为管理用户的标识，包括确保用户标识在管理域内的唯一性，维护标识的状态（包括有效和吊销），发布 IRL。用户与 IMS 之间的通信通道应是可信的。这里，实际应用时，用户和 IMS 之间的通信通道不一定是保密的，因为标识吊销列表是任何人都可以获取的公共信息。

ID-PKC 系统公共参数可以包含很多参数，在本申请实施例中，由于 ID-PKC 系统公共参数存储在许可分布式账本，因此，ID-PKC 系统公共参数除了通用参数外，还需要包含与许可分布式账本相关联的参数。

基于此，在一实施例中，所述第一 ID-PKC 系统公共参数至少包括以下至少之一：

域名称（即 KGC 所在域的名称）；

区块链名称；

系统公共参数状态；

用于隐藏用户标识的哈希算法。

其中，域名称指示生成第一 ID-PKC 系统公共参数的 KGC 所在域的名称；区块链名称也可以称为许可分布式账本名称，指示第一 ID-PKC 系统公共参数对应的许可分布式账本的名称；系统公共参数状态指示第一 ID-PKC 系统公共参数的状态，具体为有效；所述用于隐藏用户标识的哈希算法，用于在 IRL 中对标识进行匿名。

这里，所述 ID-PKC 系统公共参数所述第一 ID-PKC 系统公共参数还可以包括以下至少之一：

PPS 名称；

IMS 名称。

其中，所述 PPS 名称指示 PPS 的名称。所述 IMS 名称指示 IMS 的名称。

实际应用时，根据编码方法，比如 ASN.1 方法，ID-PKC 系统公共参数可以描述如下：

```
ID-PKCSysParams ::= SEQUENCE {
    version                INTEGER {V1(1)},
    domainName             OCTET STRING,
    ppsName                OCTET STRING OPTIONAL,
```

```

imsName          OCTET STRING OPTIONAL,
domainSerial      INTEGER,
validity          ValidityPeriod,
id-pkcPublicParameters ID-PKCPublicParameters,
5 id-pkcIdentityType OBJECT IDENTIFIER,
distributedLedgerName OCTET STRING,
  hashAlgorithm    AlgorithmIdentifier
  id-pkcParamStatus ID-PKCParamStatus,
id-pkcParamExtensions [0] IMPLICIT ID-PKCParamExtensions OPTIONAL,
10 }

```

其中，各字段的含义如下：

version: 是 ID-PKC 系统公共参数的版本号；

domainName: 是 KGC 所在域的名称，用于 KGC 寻址，它可以是按照 URI 或 URL 定义的名称，也可以是用户用自己方式定义的名称，即自定义的名称；

ppsName: 是 PPS 的名称，用于 PPS 寻址，它可以是按照 URI 或 URL 定义的名称，也可以是用户用自己方式定义的名称，即自定义的名称。

imsName: 是 IMS 的名称，用于 IMS 寻址，它可以是按照 URI 或 URL 定义的名称，也可以是用户用自己方式定义的名称，即自定义的名称。

domainSerial: 该字段是一个整数，代表唯一的可在 domainName 上使用的 ID-PKC 系统公共参数的集合，即代表可以在 domainName 指示的 KGC 所在域上使用的 ID-PKC 系统公共参数的集合；

Validity: 有效性字段，该字段定义 ID-PKC 系统公共参数的生存期，并定义为以下内容：

```

25 ValidityPeriod ::= SEQUENCE {
    notBefore    GeneralizedTime,
    notAfter     GeneralizedTime
}

```

id-pkcPublicParameters: 是一种结构，其中包含 ID-PKC 系统支持的 ID-PKC 算法相对应的公共参数。该结构定义如下：

```

ID-PKCPublicParameters ::= SEQUENCE (1..MAX) OF
ID-PKCPublicParameter
ID-PKCPublicParameter ::= SEQUENCE {
    id-pkcAlgorithm    OBJECT IDENTIFIER,
35 publicParameterData OCTET STRING
}

```

这里，id-pkcAlgorithm: 一个 ID-PKC 系统支持的至少一个 ID-PKC 算法；

publicParameterData: 是可辨别编码规则（DER）编码的结构，包含实际的密码参数。该字段的具体结构取决于算法。

id-PKCIdentityType: 用于定义在一个域内使用身份的类型，此字段的使用方式取决于应用程序；

distributedLedgerName: ID-PKC 系统公共参数发布在区块链（即许可分布式账本）上，此字段用于指示分布式账本的名称；

hashAlgorithm: 此字段指示用于隐藏用户标识的哈希算法，用于在 IRL 中对用户标识进行匿名，该字段的定义如下：

5 hashAlgorithm ::= AlgorithmIdentifier,
AlgorithmIdentifier ::= CHOICE {
SHA-256,
SHA-3,
}

10 id-pkcParamStatus: 用于指示 ID-PKC 系统公共参数的状态，具体可以有两个状态，分别是：有效和无效（也可以称为吊销），该字段的定义如下：

ID-PKCParamStatus ::= ENUMERATED {
valid (0),
invalid (1)
}

15 id-pkcParamExtensions: 它是一组扩展，可用于定义特定的实现可能需要的其他参数。该字段的结构定义如下：

ID-PKCParamExtensions ::= SEQUENCE OF ID-PKCParamExtension
ID-PKCParamExtension ::= SEQUENCE {
20 id-pkcParamExtensionOID OBJECT IDENTIFIER,
id-pkcParamExtensionValue OCTET STRING
}

需要说明的是：本申请实施例对上述各字段的名称不作限定。

25 实际应用时，在步骤 102 中，所述第一节点可以基于共识机制，将获取的第一 ID-PKC 系统公共参数形成区块，然后将形成的区块发布到许可分布式账本中。在许可分布式账本中，区块按照时间顺序（比如生成 ID-PKC 系统公共参数的时间顺序）链接成许可分布式账本。

示例性地，ID-PKC 系统公共参数写入许可分布式账本的具体步骤包括：

30 步骤 1: 一个域的 KGC 的 PPS 生成 ID-PKC 系统公共参数，并把其状态标为有效，即 id-pkcParamStatus 字段设置为有效。

步骤 2: 该 KGC 的 PPS 在许可分布式账本上的一个或几个记账节点与其它域的 KGC 的 PPS 在许可分布式账本的记账节点一起，即许可分布式账本上的所有记账节点，使用共识机制，将该 KGC 的 PPS 生成的 ID-PKC 系统公共参数写入许可分布式账本。

35 其中，实际应用时，KGC 与记账节点可能会合设在一起，KGC 与记账节点也可能会分开设置，在分开设置的情况下，KGC 与记账节点之间通过安全通道进行交互。

这里，经过步骤 1 和 2，就完成了 ID-PKC 系统公共参数的上链。

实际应用时，ID-PKC 系统公共参数的信息有可能需要更新，如密码算

法改变了等。由于许可分布式账本上的消息无法删除，因此就需要生成一个与原来 ID-PKC 系统公共参数一样的 ID-PKC 系统公共参数，把它的状态标为无效，并把生成的 ID-PKC 系统公共参数写入许可分布式账本；然后再生成一个内容已更新的 ID-PKC 系统公共参数，把它的状态标为有效并将它写入许可分布式账本，从而完成 ID-PKC 系统公共参数的更新。

基于此，在一实施例中，该方法还可以包括：

获取第二 ID-PKC 系统公共参数；所述第二 ID-PKC 系统公共参数的状态为无效；所述第二 ID-PKC 系统公共参数与第一 ID-PKC 系统公共参数除生产时间和状态外的其他参数相同；

基于共识机制，将获取的第二 ID-PKC 系统公共参数写入所述许可分布式账本；

获取新生成的第三 ID-PKC 系统公共参数；所述第三 ID-PKC 系统公共参数是所述第一 ID-PKC 系统公共参数更新的；

所述第三 ID-PKC 系统公共参数的状态为有效；

基于共识机制，将获取的第三 ID-PKC 系统公共参数写入所述许可分布式账本。

示例性地，ID-PKC 系统公共参数更新的具体步骤包括：

步骤 1：PPS 生成一个与已上链 ID-PKC 系统公共参数内容一样的 ID-PKC 系统公共参数（除了状态项和生成时间不同以外其它项都相同），即生成第二 ID-PKC 系统公共参数，并把其状态标为无效；

步骤 2：该 PPS 在许可分布式账本上的一个或几个记账节点与其它域的记账节点一起，使用共识机制，把步骤 1 中生成的 ID-PKC 系统公共参数写入许可分布式账本；

步骤 3：该 PPS 再生成一个信息内容已更新的 ID-PKC 系统公共参数，即生成第三 ID-PKC 系统公共参数，并把其状态标为有效；

步骤 4：该 PPS 在许可分布式账本上的一个或几个记账节点与其它域的记账节点一起，使用共识机制，把信息内容已更新的 ID-PKC 系统参数写入许可分布式账本。

实际应用时，所述 IRL 可由 KGC 生成。具体地，所述 IRL 可由 KGC 的 IMS 生成。

IRL 可以包含很多参数，在本申请实施例中，由于 IRL 存储在许可分布式账本，因此，IRL 除了通用参数外，还需要包含与许可分布式账本相关联的参数。

基于此，在一实施例中，所述 IRL 至少包括以下至少之一：

域名称；

区块链名称；

吊销标识集合。

其中，域名称指示生成 IRL 的 KGC 所在域的名称；区块链名称也可以

称为许可分布式账本名称，指示 IRL 对应的许可分布式账本的名称。

在一实施例中，所述 IRL 还可以包括：

IMS 名称。

其中，IMS 名称指示 MIS 的名称。

5 在一实施例中，所述吊销标识集合包含以下至少之一：

吊销标识是否匿名；

吊销标识；

吊销原因。

实际应用时，根据编码方法，比如 ASN.1 方法，IRL 可以描述如下：

```

10 IdentityRevocationList ::= SEQUENCE {
    version          INTEGER { v1(1) },
    issuer           Name,
    irlNumber        INTEGER OPTIONAL,
    deltaList        BOOLEAN OPTIONAL,
15  domainName       OCTET STRING,
    domainSerial     INTEGER,
    imsName          OCTET STRING OPTIONAL,
    thisUpdate       Time,
    nextUpdate       Time OPTIONAL,
20  distributedLedgerName OCTET STRING
    revokedIdentities SEQUENCE OF SEQUENCE {
        anonymity      Anonymimity,
        identity       ID-PKCIDentityInfo,
        revokeReason   RevokeReason
25  revocationDate    Time,
    irlEntryExtensions Extensions OPTIONAL
    }
    }

```

30 其中，各字段的含义如下：

Version: 是 IRL 的版本号；

Issuer: 用于区别 IRL 的发行者；

35 irlNumbe: 是当前 IRL 的发行者编号；它从 0 开始，对于每个完整的 IRL 发布（即在某个时间点 KGC 发布的 IRL 包含所有的吊销标识），数字都增加 1，它是可选的；

deltaList: 指示当前 IRL 是否为增量 IRL（即在某个时间点比前一个时间点所增加的吊销标识），该列表仅包含自 irlNumber 索引的完整 IRL 发布以来被撤销的身份信息；

40 domainName: 是生成 IRL 的 KGC 所在域的名称，用于 KGC 寻址，它可以是按照 URI 或 URL 定义的名称，也可以是用户用自己方式定义的名称，即自定义的名称；

domainSerial: 此字段是一个整数，代表唯一的可在 domainName 上使用的 IRL 的集合，即代表可以在 domainName 指示的 KGC 所在域上使用的 IRL 的集合；

imsName: 是 IMS 的名称, 用于 IMS 寻址, 它可以是按照 URI 或 URL 定义的名称, 也可以是用户用自己方式定义的名称, 即自定义的名称。

thisUpdate: 指示此 IRL 表生成时间;

nextUpdate: 指示下一个 IRL 生成时间, 是可选的;

distributedLedgerName: IRL 发布在区块链 (即许可分布式账本) 上, 此字段用于指示分布式账本的名称;

revokedIdentities: 用于指示吊销标识集合, 包含以下字段: anonymity, identity, revokeReason, revocationDate, irlEntryExtensions。这些字段说明如下:

(1) anonymity: 用于说明吊销标识是否需要匿名, 即吊销标识是否匿名, 该字段具体描述如下:

anonymimity::= Anonymimity

Anonymimity::=CHOICE{

YES,

NO,

}

(2) identity: 用于说明吊销标识, 该字段具体描述如下:

identity::= ID-PKCIDentityInfo

ID-PKCIDentityInfo::=CHOICE{

Hash (RovokedIdendity),

RovokedIdentity,

}

其中, 如果 anonymity 是 YES, 则 ID-PKCIDentityInfo 字段对应的是吊销标识的哈希值, 否则, ID-PKCIDentityInfo 字段对应的是吊销标识本身;

(3) revokeReason: 用于说明标识吊销的原因, 该字段描述如下:

revokeReason ::=RevokeReason

RevokeReason ::= ENUMERATED {

unspecified (0),

keyCompromise (1),

kgcCompromise (2),

affiliationChanged (3),

superseded (4),

cessationOfOperation (5),

}

irlEntryExtensions: 该字段定义可能的吊销标识扩展。

需要说明的是: 本申请实施例对上述各字段的名称不作限定。

实际应用时, 在步骤 102 中, 所述第一节点可以基于共识机制, 将获取的 IRL 形成区块, 然后将形成的区块发布到许可分布式账本中。在许可分布式账本中, 区块按照时间顺序 (比如生成 IRL 的时间顺序) 链接成许可分布式账本。

示例性地, IRL 数写入许可分布式账本 (即将 IRL 发布 (也可以理解

为颁发)在联盟上)的具体步骤包括:

步骤 1: 一个域的 KGC 的 IMS 生成 IRL;

步骤 2: 该 IMS 在许可分布式账本上的一个或几个记账节点与其它域的 KGC 的 IMS 在许可分布式账本的记账节点一起,即许可分布式账本上的所有记账节点,使用共识机制,把 IRL 写入许可分布式账本。

当 ID-PKC 系统公共参数和 IRL 写入许可分布式账本后,用户就可以查询 ID-PKC 系统公共参数和 IRL。

基于此,本申请实施例还提供了一种 ID-PKC 信息处理方法,应用于第二节点,如图 2 所示,该方法包括:

步骤 201: 获取第一请求;所述第一请求用于请求获取 ID-PKC 系统公共参数;

步骤 202: 从许可分布式账本查询对应的 ID-PKC 系统公共参数;

步骤 203: 根据查询结果返回响应。

其中,实际应用时,所述第二节点可以是记账节点,也可以是普通的接入节点。

实际应用时,ID-PKC 系统公共参数写入许可分布式账本时,可以以域名称为关键词(key);另外,网络中存在多条许可分布式账本,在查询时,需要找到待查询的 ID-PKC 系统公共参数所在的许可分布式账本。

基于此,在一实施例中,所述第一请求携带域名称及区块链名称;相应地,所述第二节点利用所述第一请求携带的域名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

其中,实际应用时,当 ID-PKC 系统公共参数包含 PPS 名称时,且 ID-PKC 系统公共参数写入许可分布式账本时,可以以域名称和/或 PPS 名称为 key。

基于此,在一实施例中,所述第一请求还携带 PPS 名称;

利用所述第一请求携带的域名称和/或 PPS 名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

在许可分布式账本上,区块按照时间顺序链接,因此,查询时可以从许可分布式账本上最新的区块开始查询。

当所述第一请求携带的域名称在对应的许可分布式账本未检索到时,说明未查询到对应的 ID-PKC 系统公共参数时,所述第二节点返回错误信息,此时错误信息可以指示待查询的 ID-PKC 系统公共参数不存在。

当查询到对应的 ID-PKC 系统公共参数,且查询到的 ID-PKC 系统公共参数的状态为无效时,返回错误信息,此时错误信息可以指示待查询的 ID-PKC 系统公共参数的状态是失效。

当查询到对应的 ID-PKC 系统公共参数,且查询到的 ID-PKC 系统公共参数的状态为有效时,返回查询到的 ID-PKC 系统公共参数。

示例性地,ID-PKC 系统公共参数的查询步骤可以包括:

步骤 1: 用户需要获得 ID-PKC 系统公共参数, 首先用 domainName 字段和/或 ppsName 字段向联盟区块链发起查询, 即发起第一请求; 这里, 用户通过应用程序编程接口 (API) 发起第一请求;

5 步骤 2: 检索从区块链上最新的区块 (即整个链接的最后, 从后往前检索) 开始, 如果要查询的 domainName 字段和/或 ppsName 字段在该区块链上没有检索到, 则终止查询并向用户返回被叫错误信息 (即 ID-PKC 系统参数不存在), 如果在该区块链上检索到, 则对获得的最新 (即对应 domainSerial 是最大的) 的 ID-PKC 系统公共参数进行检查, 如果其状态为无效状态, 则返回给被叫错误信息 (即存在 ID-PKC 系统参数但状态失效);
10 如果最新的 ID-PKC 系统公共参数的状态为有效状态, 则返回给用户想要获取的 ID-PKC 系统公共参数。

本申请实施例还提供了一种 ID-PKC 信息处理方法, 应用于第三节点, 如图 3 所示, 该方法包括:

15 步骤 301: 获取第二请求; 所述第二请求用于请求查询第一标识是否已被吊销;

步骤 302: 从许可分布式账本查询第一标识是否已被吊销; 所述许可分布式账本记录有 IRL;

步骤 303: 根据查询结果返回响应。

20 其中, 实际应用时, 所述第三节点可以是记账节点, 也可以是普通的接入节点。

在步骤 302 中, 所述第三节点在 IRL 中查询所述第一标识是否已被吊销。

实际应用时, IRL 写入许可分布式账本时, 以域名称和/或 IMS 名称 (当 IRL 包括 IMS 名称时) 为 key; 另外, 网络中存在多条许可分布式账本, 在
25 查询时, 需要找到待查询的 IRL 所在的许可分布式账本。

基于此, 在一实施例中, 所述第二请求携带所述第一标识及区块链名称; 所述第三节点利用所述第一标识在所述区块链名称对应的许可分布式账本进行查询。

30 实际应用时, 第一标识可能是匿名标识, 即所述第一标识是隐藏用户标识, 为了实现对匿名标识的查询, 可以用对第一标识进行哈希算法的运算结果来进行查询。

基于此, 在一实施例中, 所述第二请求携带对所述第一标识利用 ID-PKC 系统公共参数指示的哈希函数进行运算后的运算结果及区块链名称;

35 利用所述运算结果在所述区块链名称对应的许可分布式账本进行查询。

当查询到所述第一标识已被吊销时, 返回第一信息; 所述第一信息指示所述第一标识已被吊销;

当未查找到所述第一标识时, 返回第二信息; 所述第二信息指示所述

第一标识有效。

示例性地，标识查询的具体过程可以包括：

步骤 1：用户使用标识向许可分布式账本进行查询，如果找到，则说明此标识已废除（即已被吊销），向用户返回用户消息（即该用户标识已被废除），如果没有找到，则进行步骤 2；这里，用户通过 API 发起查询请求；

步骤 2：用户使用 ID-PKC 系统公共参数中指示的哈希函数对要查询的标识进行运算，得到运算结果，使用运算结果向许可分布式账本进行查询，如果存在与运算结果相同的值，则说明此用户标识已废除，向用户返回用户消息（即该用户标识已被废除）；如果没有找到相同的值，则说明该用户标识有效，向用户返回用户消息（即该用户标识有效），通过上述方式，匿名的标识是否有效也能在许可分布式账本上查询到。

实际应用时，步骤 302 中，当第三节点是普通节点时，第三节点可以根据 ID-PKC 系统公共参数中的 IMS 名称寻址到对应的 IMS（可以是与第三节点属于同一个域的 IMS，也可以是与第三节点属于不同域的 IMS），然后向对应的 IMS 发起查询请求，以查询第一标识是否已被吊销。

当第三节点是所述区块链名称对应许可分布式账本的记账节点时，可以直接查询第一标识是否已被吊销。

从上面的描述可以看出，本申请实施例中，包含 PKG、PPS 和 IMS 的 KGC 与用户终端组成许可分布式账本。一个 PPS 经过共识流程后在许可分布式账本上写入对应的 ID-PKC 系统公共参数。一个 IMS 经过共识流程后在许可分布式账本上写入对应域内的 IRL。用户终端不能在许可分布式账本上写入数据，只能从许可分布式账本上读取数据。

本申请实施例提供的 ID-PKC 信息处理方法，第一节点获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；基于共识机制，将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本；第二节点获取第一请求；所述第一请求用于请求获取 ID-PKC 系统公共参数；从许可分布式账本查询对应的 ID-PKC 系统公共参数；并根据查询结果返回响应；第三节点获取第二请求；所述第二请求用于请求查询第一标识是否已被吊销；从许可分布式账本查询第一标识是否已被吊销；所述许可分布式账本记录有 IRL；并根据查询结果返回响应。本申请实施例提供的方案，基于许可分布式账本进行 ID-PKC 系统公共参数的发布和标识撤销的管理，通过使用许可分布式账本，ID-PKC 系统参数和 IRL 可以跨域传递，并使得标识吊销能够跨域查询，从而实现了不依赖于 PKI 系统，使用 ID-PKC 系统就能实现跨域安全通信。

为了实现本申请实施例的方法，本申请实施例还提供了一种 ID-PKC 信息处理装置，设置在第一节点上，如图 4 所示，该装置包括：

第一获取单元 401，配置为获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；

第一处理单元 402, 配置为基于共识机制, 将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

其中, 在一实施例中, 所述第一获取单元 401, 还配置为获取第二 ID-PKC 系统公共参数; 所述第二 ID-PKC 系统公共参数的状态为无效; 所述
5 第二 ID-PKC 系统公共参数与第一 ID-PKC 系统公共参数除生产时间和状态外的其他参数相同;

所述第一处理单元 402, 还配置为基于共识机制, 将获取的第二 ID-PKC 系统公共参数写入所述许可分布式账本;

所述第一获取单元 401, 还配置为获取新生成的第三 ID-PKC 系统公共
10 参数; 所述第三 ID-PKC 系统公共参数是所述第一 ID-PKC 系统公共参数更新的; 所述第三 ID-PKC 系统公共参数的状态为有效;

所述第一处理单元 402, 还配置为基于共识机制, 将获取的第三 ID-PKC 系统公共参数写入所述许可分布式账本。

实际应用时, 所述第一获取单元 401 可由 ID-PKC 信息处理装置中的通
15 信接口实现; 所述第一处理单元 402 可由 ID-PKC 信息处理装置中的通信接口结合处理器实现。

为了实现本申请实施例第二节点侧的方法, 本申请实施例还提供了一种 ID-PKC 信息处理装置, 设置在第二节点上, 如图 5 所示, 该装置包括:

第二获取单元 501, 配置为获取第一请求; 所述第一请求用于请求获取
20 ID-PKC 系统公共参数;

第二处理单元 502, 配置为从许可分布式账本查询对应的 ID-PKC 系统公共参数; 根据查询结果返回响应。

其中, 在一实施例中, 所述第二处理单元 502 从许可分布式账本查询对应的 ID-PKC 系统公共参数时, 从所述许可分布式账本最新的区块开始查
25 询。

在一实施例中, 所述第一请求携带域名称以及区块链名称;

所述第二处理单元 502, 配置为利用所述第一请求携带的域名称从所述
区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

在一实施例中, 所述第一请求还携带 PPS 名称;

30 利用所述第一请求携带的域名称和/或 PPS 名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

在一实施例中, 所述第二处理单元 502, 配置为:

当未查询到对应的 ID-PKC 系统公共参数时, 返回错误信息;

或者,

35 当查询到对应的 ID-PKC 系统公共参数, 且查询到的 ID-PKC 系统公共参数的状态为无效时, 返回错误信息;

或者,

当查询到对应的 ID-PKC 系统公共参数, 且查询到的 ID-PKC 系统公共参

数的状态为有效时，返回查询到的 ID-PKC 系统共参数。

实际应用时，所述第二获取单元 501 可由 ID-PKC 信息处理装置中的通信接口实现；所述第二处理单元 502 可由 ID-PKC 信息处理装置中的通信接口结合处理器实现。

为了实现本申请实施例第三节点侧的方法，本申请实施例还提供了一种 ID-PKC 信息处理装置，设置在第三节点上，如图 6 所示，该装置包括：

第三获取单元 601，配置为获取第二请求；所述第二请求用于请求查询第一标识是否已被吊销；

第三处理单元 602，配置为从许可分布式账本查询第一标识是否已被吊销；所述许可分布式账本记录有 IRL；根据查询结果返回响应。

其中，在一实施例中，所述第二请求携带所述第一标识及区块链名称；所述第三处理单元 602 利用所述第一标识在所述区块链名称对应的许可分布式账本进行查询。

在一实施例中，所述第二请求携带对所述第一标识利用 ID-PKC 系统公共参数指示的哈希函数进行运算后的运算结果及区块链名称；

所述第三处理单元 602 利用所述运算结果在所述区块链名称对应的许可分布式账本进行查询。

在一实施例中，所述第三处理单元 602，配置为：

当查询到所述第一标识已被吊销时，返回第一信息；所述第一信息指示所述第一标识已被吊销；

或者，

当未查找到所述第一标识时，返回第二信息；所述第二信息指示所述第一标识有效。

实际应用时，所述第三获取单元 601 可由 ID-PKC 信息处理装置中的通信接口实现；所述第三处理单元 602 可由 ID-PKC 信息处理装置中的通信接口结合处理器实现。

需要说明的是：上述实施例提供的 ID-PKC 信息处理装置在进行 ID-PKC 信息处理时，仅以上述各程序模块的划分进行举例说明，实际应用中，可以根据需要而将上述处理分配由不同的程序模块完成，即将装置的内部结构划分成不同的程序模块，以完成以上描述的全部或者部分处理。另外，上述实施例提供的 ID-PKC 信息处理装置与 ID-PKC 信息处理方法实施例属于同一构思，其具体实现过程详见方法实施例，这里不再赘述。

基于上述程序模块的硬件实现，且为了实现本申请实施例第一节点侧的方法，本申请实施例还提供了一种第一节点，如图 7 所示，该第一节点 700 包括：

第一通信接口 701，能够与其他节点（比如其他记账节点）进行信息交互；

第一处理器 702，与所述第一通信接口 701 连接，以实现与其他节点进

行信息交互，配置为运行计算机程序时，执行上第一节点侧一个或多个技术方案提供的方法；

第一存储器 703，所述计算机程序存储在所述第一存储器 703 上。

具体地，所述第一通信接口 701，配置为获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点 700 为记账节点；

所述第一处理器 702，配置为基于共识机制，将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

其中，在一实施例中，所述第一通信接口 701，还配置为获取第二 ID-PKC 系统公共参数；所述第二 ID-PKC 系统公共参数的状态为无效；所述第二 ID-PKC 系统公共参数与第一 ID-PKC 系统公共参数除生产时间和状态外的其他参数相同；

所述第一处理器 702，还配置为基于共识机制，将获取的第二 ID-PKC 系统公共参数写入所述许可分布式账本；

所述第一通信接口 701，还配置为获取新生成的第三 ID-PKC 系统公共参数；所述第三 ID-PKC 系统公共参数是所述第一 ID-PKC 系统公共参数更新的；所述第三 ID-PKC 系统公共参数的状态为有效；

所述第一处理器 702，还配置为基于共识机制，将获取的第三 ID-PKC 系统公共参数写入所述许可分布式账本。

需要说明的是：第一处理器 702 的具体处理过程可参照上述方法理解。

当然，实际应用时，第一节点 700 中的各个组件通过总线系统 704 耦合在一起。可理解，总线系统 704 配置为实现这些组件之间的连接通信。总线系统 704 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 7 中将各种总线都标为总线系统 704。

本申请实施例中的第一存储器 703 配置为存储各种类型的数据以支持第一节点 700 的操作。这些数据的示例包括：用于在第一节点 700 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第一处理器 702 中，或者由所述第一处理器 702 实现。所述第一处理器 702 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过所述第一处理器 702 中的硬件的集成逻辑电路或者软件形式的指令完成。

上述的所述第一处理器 702 可以是通用处理器、数字信号处理器（DSP，Digital Signal Processor），或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第一处理器 702 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于第一

存储器 703, 所述第一处理器 702 读取第一存储器 703 中的信息, 结合其硬件完成前述方法的步骤。

在示例性实施例中, 第一节点 700 可以被一个或多个应用专用集成电路 (ASIC, Application Specific Integrated Circuit)、DSP、可编程逻辑器件 (PLD, Programmable Logic Device)、复杂可编程逻辑器件 (CPLD, Complex Programmable Logic Device)、现场可编程门阵列 (FPGA, Field-Programmable Gate Array)、通用处理器、控制器、微控制器 (MCU, Micro Controller Unit)、微处理器 (Microprocessor)、或者其他电子元件实现, 配置为执行前述方法。

基于上述程序模块的硬件实现, 且为了实现本申请实施例第二节点侧的方法, 本申请实施例还提供了一种第二节点, 如图 8 所示, 该第二节点 800 包括:

第二通信接口 801, 能够与其他节点和用户等进行信息交互;

第二处理器 802, 与所述第二通信接口 801 连接, 以实现与其他节点和用户等进行信息交互, 配置为运行计算机程序时, 执行上述第二节点侧一个或多个技术方案提供的方法;

第二存储器 803, 所述计算机程序存储在所述第二存储器 803 上。

具体地, 所述第二通信接口 801, 配置为获取第一请求; 所述第一请求用于请求获取 ID-PKC 系统公共参数;

所述第二处理器 802, 配置为从许可分布式账本查询对应的 ID-PKC 系统公共参数; 根据查询结果通过所述第二通信接口返回响应。

其中, 在一实施例中, 所述第二处理器 802 从许可分布式账本查询对应的 ID-PKC 系统公共参数时, 从所述许可分布式账本最新的区块开始查询。

在一实施例中, 所述第一请求携带域名称以及区块链名称;

所述第二处理器 802, 配置为利用所述第一请求携带的域名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

在一实施例中, 所述第一请求还携带 PPS 名称;

所述第二处理器 802, 配置为利用所述第一请求携带的域名称和/或 PPS 名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

在一实施例中, 所述第二处理器 802, 配置为:

当未查询到对应的 ID-PKC 系统公共参数时, 返回错误信息;

或者,

当查询到对应的 ID-PKC 系统公共参数, 且查询到的 ID-PKC 系统公共参数的状态为无效时, 返回错误信息;

或者,

当查询到对应的 ID-PKC 系统公共参数, 且查询到的 ID-PKC 系统公共参数的状态为有效时, 返回查询到的 ID-PKC 系统公共参数。

需要说明的是: 第二处理器 802 的具体处理过程可参照上述方法理解。

当然，实际应用时，第二节点 800 中的各个组件通过总线系统 804 耦合在一起。可理解，总线系统 804 配置为实现这些组件之间的连接通信。总线系统 804 除包括数据总线之外，还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见，在图 8 中将各种总线都标为总线系统 804。

5 本申请实施例中的第二存储器 803 配置为存储各种类型的数据以支持第二节点 800 操作。这些数据的示例包括：用于在第二节点 800 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第二处理器 802 中，或者由所述第二处理器 802 实现。所述第二处理器 802 可能是一种集成电路芯片，具有信号的处理能力。在实现过程中，上述方法的各步骤可以通过
10 所述第二处理器 802 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第二处理器 802 可以是通用处理器、DSP，或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第二处理器 802 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤，可以直接体现为硬件译码处理器执行完成，或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中，该存储介质位于第二存储器 803，所述第二处理器 802 读取第二存储器 803 中的信息，结合其硬件完成前述方法的步骤。

20 在示例性实施例中，第二节点 800 可以被一个或多个 ASIC、DSP、PLD、CPLD、FPGA、通用处理器、控制器、MCU、Microprocessor、或其他电子元件实现，配置为执行前述方法。

基于上述程序模块的硬件实现，且为了实现本申请实施例第三节点侧的方法，本申请实施例还提供了一种第三节点，如图 9 所示，该第三节点
25 900 包括：

第三通信接口 901，能够与其他节点和用户等进行信息交互；

第三处理器 902，与所述第三通信接口 901 连接，以实现与其他节点和用户等进行信息交互，配置为运行计算机程序时，执行上述第三节点侧一个或多个技术方案提供的方法；

30 第三存储器 903，所述计算机程序存储在所述第三存储器 903 上。

具体地，所述第三通信接口 901，配置为获取第二请求；所述第二请求用于请求查询第一标识是否已被吊销；

所述第三处理器 902，配置为从许可分布式账本查询第一标识是否已被吊销；所述许可分布式账本记录有 IRL；根据查询结果通过所述第三通信接口
35 返回响应。

其中，在一实施例中，所述第二请求携带所述第一标识及区块链名称。所述第三处理器 902 利用所述第一标识在所述区块链名称对应的许可分布式账本进行查询。

在一实施例中,所述第二请求携带对所述第一标识利用 ID-PKC 系统公共参数指示的哈希函数进行运算后的运算结果及区块链名称;

所述第三处理器 902 利用所述运算结果在所述区块链名称对应的许可分布式账本进行查询。

5 在一实施例中,所述第三处理器 902,配置为:

当查询到所述第一标识已被吊销时,返回第一信息;所述第一信息指示所述第一标识已被吊销;

或者,

10 当未查找到所述第一标识时,返回第二信息;所述第二信息指示所述第一标识有效。

需要说明的是:第三处理器 902 的具体处理过程可参照上述方法理解。

当然,实际应用时,第三节点 900 中的各个组件通过总线系统 904 耦合在一起。可理解,总线系统 904 配置为实现这些组件之间的连接通信。总线系统 904 除包括数据总线之外,还包括电源总线、控制总线和状态信号总线。但是为了清楚说明起见,在图 9 中将各种总线都标为总线系统 904。

本申请实施例中的第三存储器 903 配置为存储各种类型的数据以支持第三节点 900 操作。这些数据的示例包括:用于在第三节点 900 上操作的任何计算机程序。

上述本申请实施例揭示的方法可以应用于所述第三处理器 902 中,或者由所述第三处理器 902 实现。所述第三处理器 902 可能是一种集成电路芯片,具有信号的处理能力。在实现过程中,上述方法的各步骤可以通过所述第三处理器 902 中的硬件的集成逻辑电路或者软件形式的指令完成。上述的所述第三处理器 902 可以是通用处理器、DSP,或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。所述第三处理器 902 25 可以实现或者执行本申请实施例中的公开的各方法、步骤及逻辑框图。通用处理器可以是微处理器或者任何常规的处理器等。结合本申请实施例所公开的方法的步骤,可以直接体现为硬件译码处理器执行完成,或者用译码处理器中的硬件及软件模块组合执行完成。软件模块可以位于存储介质中,该存储介质位于第三存储器 903,所述第三处理器 902 读取第三存储器 903 中的信息,结合其硬件完成前述方法的步骤。

在示例性实施例中,第三节点 900 可以被一个或多个 ASIC、DSP、PLD、CPLD、FPGA、通用处理器、控制器、MCU、Microprocessor、或其他电子元件实现,配置为执行前述方法。

可以理解,本申请实施例的存储器(第一存储器 703、第二存储器 803、35 第三存储器 903)可以是易失性存储器或者非易失性存储器,也可包括易失性和非易失性存储器两者。其中,非易失性存储器可以是只读存储器(ROM, Read Only Memory)、可编程只读存储器(PROM, Programmable Read-Only Memory)、可擦除可编程只读存储器(EPROM, Erasable Programmable

Read-Only Memory)、电可擦除可编程只读存储器 (EEPROM, Electrically Erasable Programmable Read-Only Memory)、磁性随机存取存储器 (FRAM, ferromagnetic random access memory)、快闪存储器 (Flash Memory)、磁表面存储器、光盘、或只读光盘 (CD-ROM, Compact Disc Read-Only Memory);
5 磁表面存储器可以是磁盘存储器或磁带存储器。易失性存储器可以是随机存取存储器 (RAM, Random Access Memory), 其用作外部高速缓存。通过示例性但不是限制性说明, 许多形式的 RAM 可用, 例如静态随机存取存储器 (SRAM, Static Random Access Memory)、同步静态随机存取存储器 (SSRAM, Synchronous Static Random Access Memory)、动态随机存取存
10 储器 (DRAM, Dynamic Random Access Memory)、同步动态随机存取存储器 (SDRAM, Synchronous Dynamic Random Access Memory)、双倍数据速率同步动态随机存取存储器 (DDRSDRAM, Double Data Rate Synchronous Dynamic Random Access Memory)、增强型同步动态随机存取存储器 (ESDRAM, Enhanced Synchronous Dynamic Random Access Memory)、同
15 步连接动态随机存取存储器 (SLDRAM, SyncLink Dynamic Random Access Memory)、直接内存总线随机存取存储器 (DRRAM, Direct Rambus Random Access Memory)。本申请实施例描述的存储器旨在包括但不限于这些和任意其它适合类型的存储器。

在示例性实施例中, 本申请实施例还提供了一种存储介质, 即计算机
20 存储介质, 具体为计算机可读存储介质, 例如包括存储计算机程序的第一存储器 703, 上述计算机程序可由第一节点 700 的第一处理器 702 执行, 以完成前述第一节点侧方法所述步骤, 再比如包括存储计算机程序的第二存储器 803, 上述计算机程序可由第二节点 800 的第二处理器 802 执行, 以完成前述第二节点侧方法所述步骤; 再比如包括存储计算机程序的第三存
25 储器 903, 上述计算机程序可由第三节点 900 的第三处理器 902 执行, 以完成前述第三节点侧方法所述步骤。计算机可读存储介质可以是 FRAM、ROM、PROM、EPROM、EEPROM、Flash Memory、磁表面存储器、光盘、或 CD-ROM 等存储器。

需要说明的是: “第一”、“第二”等是用于区别类似的对象, 而不必用于描述特定的顺序或先后次序。

另外, 本申请实施例所记载的技术方案之间, 在不冲突的情况下, 可以任意组合。

以上所述, 仅为本申请的较佳实施例而已, 并非用于限定本申请的保护范围。

权利要求书

1、一种基于标识的公共密码 ID-PKC 信息处理方法,应用于第一节点,包括:

获取第一 ID-PKC 系统公共参数和/或标识吊销列表 IRL; 所述第一 ID-PKC 系统公共参数的状态为有效; 所述第一节点为记账节点;

基于共识机制, 将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

2、根据权利要求 1 所述的方法, 其中, 所述第一 ID-PKC 系统公共参数由密钥生成中心 KGC 的公共参数服务器生成;

所述第一 ID-PKC 系统公共参数至少包括以下至少之一:

域名称;

区块链名称;

系统公共参数状态;

用于隐藏用户标识的哈希算法。

3、根据权利要求 2 所述的方法, 其中, 所述域名称为按照统一资源标识符 URI 或统一资源定位器 URL 定义的名称, 或为自定义的名称。

4、根据权利要求 2 所述的方法, 其中, 所述第一 ID-PKC 系统公共参数还包括以下至少之一:

公共参数服务器名称;

标识管理服务器名称。

5、根据权利要求 4 所述的方法, 其中, 所述公共参数服务器名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

6、根据权利要求 4 所述的方法, 其中, 所述标识管理服务器名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

7、根据权利要求 1 所述的方法, 其中, 所述 IRL 由 KGC 的标识管理服务器生成;

所述 IRL 至少包括以下至少之一:

域名称;

区块链名称;

吊销标识集合。

8、根据权利要求 7 所述的方法, 其中, 所述域名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

9、根据权利要求 7 所述的方法, 其中, 所述 IRL 还包括:

标识管理服务器名称。

10、根据权利要求 9 所述的方法, 其中, 所述标识管理服务器名称为按照 URI 或 URL 定义的名称, 或为自定义的名称。

11、根据权利要求 7 所述的方法，其中，所述吊销标识集合包含以下至少之一：

吊销标识是否匿名；
吊销标识；
5 吊销原因。

12、根据权利要求 1 至 11 任一项所述的方法，其中，所述方法还包括：

获取第二 ID-PKC 系统公共参数；所述第二 ID-PKC 系统公共参数的状态为无效；所述第二 ID-PKC 系统公共参数与第一 ID-PKC 系统公共参数除生产时间和状态外的其他参数相同；

10 基于共识机制，将获取的第二 ID-PKC 系统公共参数写入所述许可分布式账本；

获取新生成的第三 ID-PKC 系统公共参数；所述第三 ID-PKC 系统公共参数是所述第一 ID-PKC 系统公共参数更新的；所述第三 ID-PKC 系统公共参数的状态为有效；

15 基于共识机制，将获取的第三 ID-PKC 系统公共参数写入所述许可分布式账本。

13、一种 ID-PKC 信息处理方法，应用于第二节点，包括：

获取第一请求；所述第一请求用于请求获取 ID-PKC 系统公共参数；
从许可分布式账本查询对应的 ID-PKC 系统公共参数；

20 根据查询结果返回响应。

14、根据权利要求 13 所述的方法，其中，所述从许可分布式账本查询对应的 ID-PKC 系统公共参数时，所述方法包括：

从所述许可分布式账本最新的区块开始查询。

25 15、根据权利要求 13 所述的方法，其中，所述第一请求携带域名称以及区块链名称；

利用所述第一请求携带的域名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

16、根据权利要求 15 所述的方法，其中，所述第一请求还携带公共参数服务器名称；

30 利用所述第一请求携带的域名称和/或公共参数服务器名称从所述区块链名称对应的许可分布式账本查询对应的 ID-PKC 系统公共参数。

17、根据权利要求 13 至 16 任一项所述的方法，其中，所述根据查询结果返回响应，包括：

当未查询到对应的 ID-PKC 系统公共参数时，返回错误信息；

35 或者，

当查询到对应的 ID-PKC 系统公共参数，且查询到的 ID-PKC 系统公共参数的状态为无效时，返回错误信息；

或者，

当查询到对应的 ID-PKC 系统公共参数，且查询到的 ID-PKC 系统共参数的状态为有效时，返回查询到的 ID-PKC 系统共参数。

18、一种 ID-PKC 信息处理方法，应用于第三节点，包括：

获取第二请求；所述第二请求用于请求查询第一标识是否已被吊销；

5 从许可分布式账本查询第一标识是否已被吊销；所述许可分布式账本记录有 IRL；

根据查询结果返回响应。

19、根据权利要求 18 所述的方法，其中，所述第二请求携带所述第一标识及区块链名称；利用所述第一标识在所述区块链名称对应的许可分布
10 式账本进行查询。

20、根据权利要求 18 所述的方法，其中，所述第二请求携带对所述第一标识利用 ID-PKC 系统公共参数指示的哈希函数进行运算后的运算结果及区块链名称；

利用所述运算结果在所述区块链名称对应的许可分布式账本进行查询。

15 21、根据权利要求 18 至 20 任一项所述的方法，其中，所述根据查询结果返回响应，包括：

当查询到所述第一标识已被吊销时，返回第一信息；所述第一信息指示所述第一标识已被吊销；

或者，

20 当未查找到所述第一标识时，返回第二信息；所述第二信息指示所述第一标识有效。

22、一种 ID-PKC 信息处理装置，设置在第一节点上，包括：

第一获取单元，配置为获取第一 ID-PKC 系统公共参数和/或 IRL；所述第一 ID-PKC 系统公共参数的状态为有效；所述第一节点为记账节点；

25 第一处理单元，配置为基于共识机制，将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

23、一种 ID-PKC 信息处理装置，包括：

第二获取单元，配置为获取第一请求；所述第一请求用于请求获取 ID-PKC 系统公共参数；

30 第二处理单元，配置为从许可分布式账本查询对应的 ID-PKC 系统公共参数；根据查询结果返回响应。

24、一种 ID-PKC 信息处理装置，包括：

第三获取单元，配置为获取第二请求；所述第二请求用于请求查询第一标识是否已被吊销；

35 第三处理单元，配置为从许可分布式账本查询第一标识是否已被吊销；所述许可分布式账本记录有 IRL；根据查询结果返回响应。

25、一种第一节点，包括：第一通信接口及第一处理器；其中，

所述第一通信接口，配置为获取第一 ID-PKC 系统公共参数和/或 IRL；

所述第一 ID-PKC 系统公共参数的状态为有效; 所述第一节点为记账节点;
第一处理器, 配置为基于共识机制, 将获取的第一 ID-PKC 系统公共参数和/或 IRL 写入许可分布式账本。

26、一种第二节点, 包括: 第二通信接口及第二处理器; 其中,

所述第二通信接口, 配置为获取第一请求; 所述第一请求用于请求获取 ID-PKC 系统公共参数;

所述第二处理器, 配置为从许可分布式账本查询对应的 ID-PKC 系统公共参数; 根据查询结果通过所述第二通信接口返回响应。

27、一种第三节点, 包括: 第三通信接口及第三处理器; 其中,

所述第三通信接口, 配置为获取第二请求; 所述第二请求用于请求查询第一标识是否已被吊销;

所述第三处理器, 配置为从许可分布式账本查询第一标识是否已被吊销; 所述许可分布式账本记录有 IRL; 根据查询结果通过所述第三通信接口返回响应。

28、一种第一节点, 包括: 第一处理器和配置为存储能够在处理器上运行的计算机程序的第一存储器,

其中, 所述第一处理器配置为运行所述计算机程序时, 执行权利要求 1 至 12 任一项所述方法的步骤。

29、一种第二节点, 包括: 第二处理器和配置为存储能够在处理器上运行的计算机程序的第二存储器,

其中, 所述第二处理器配置为运行所述计算机程序时, 执行权利要求 13 至 17 任一项所述方法的步骤。

30、一种第三节点, 包括: 第三处理器和配置为存储能够在处理器上运行的计算机程序的第三存储器,

其中, 所述第三处理器配置为运行所述计算机程序时, 执行权利要求 18 至 21 任一项所述方法的步骤。

31、一种存储介质, 其上存储有计算机程序, 其中, 所述计算机程序被处理器执行时实现权利要求 1 至 12 任一项所述方法的步骤, 或者实现权利要求 13 至 17 任一项所述方法的步骤, 或者实现权利要求 18 至 21 任一项所述方法的步骤。

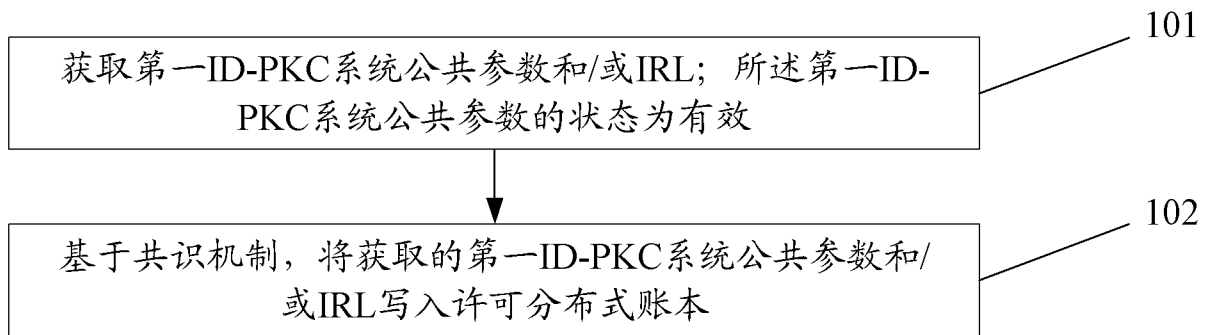


图 1

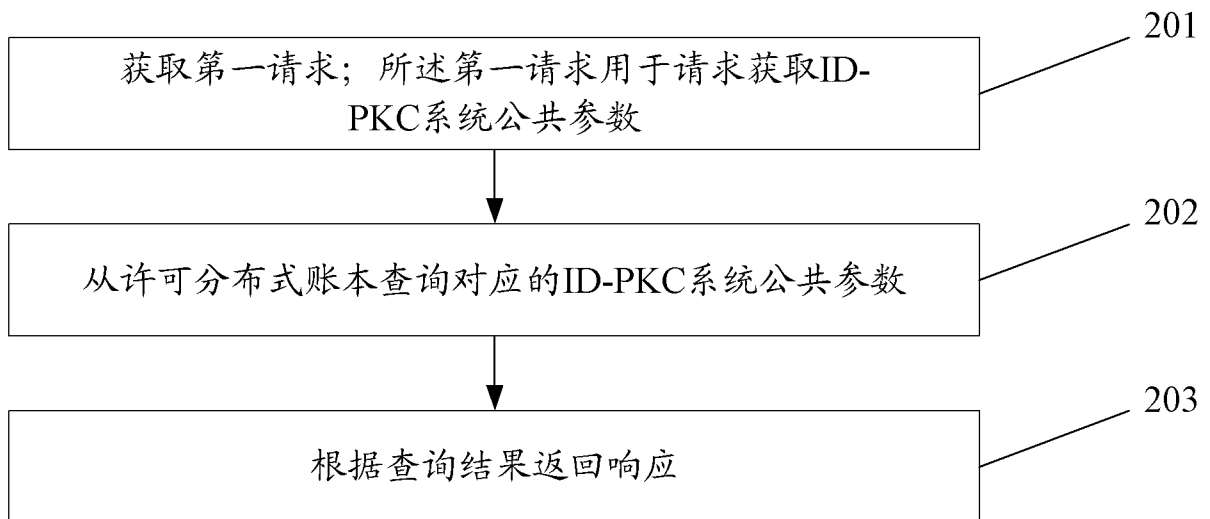


图 2

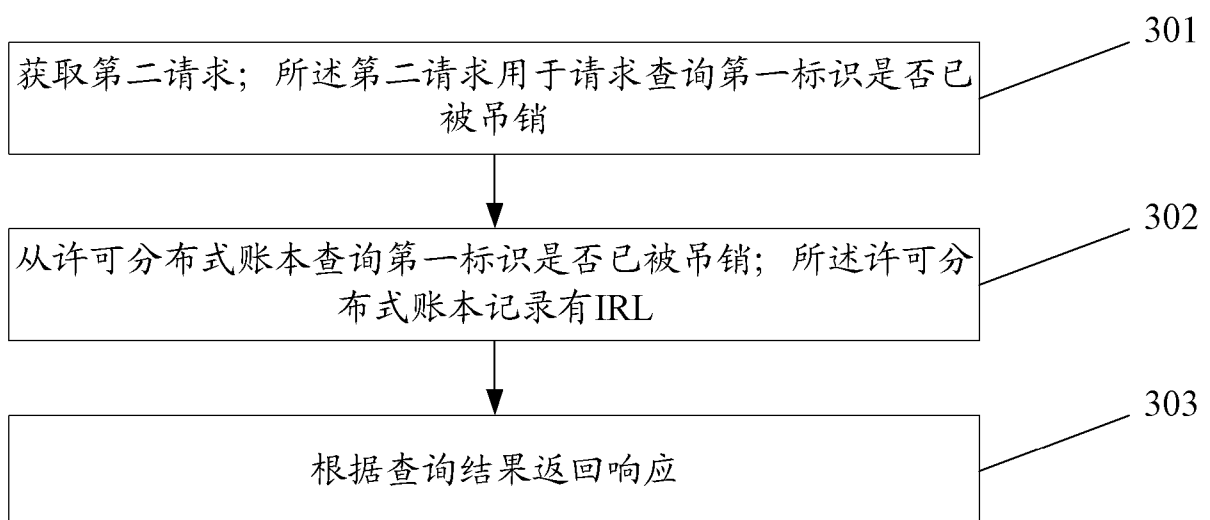


图 3

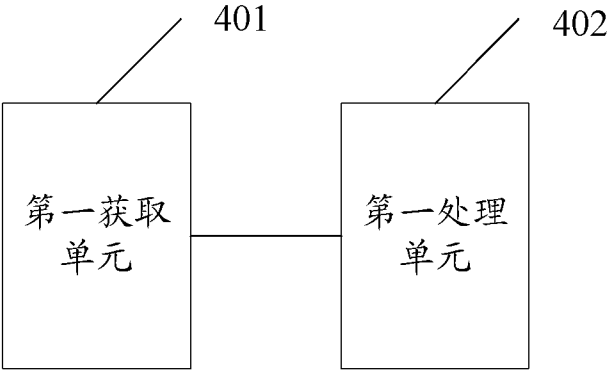


图 4

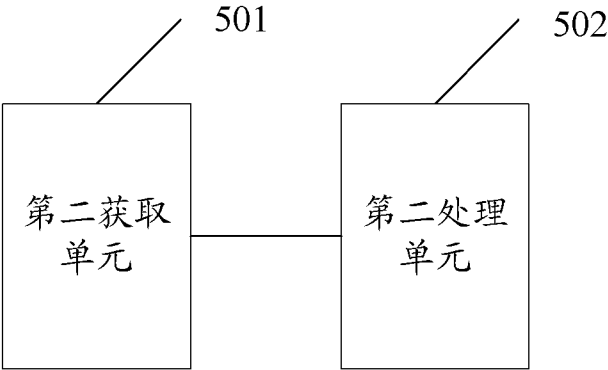


图 5

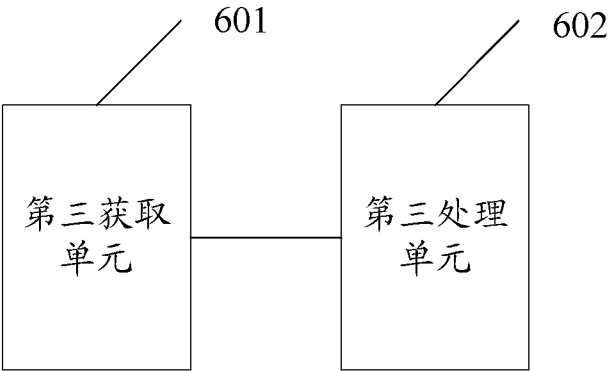


图 6

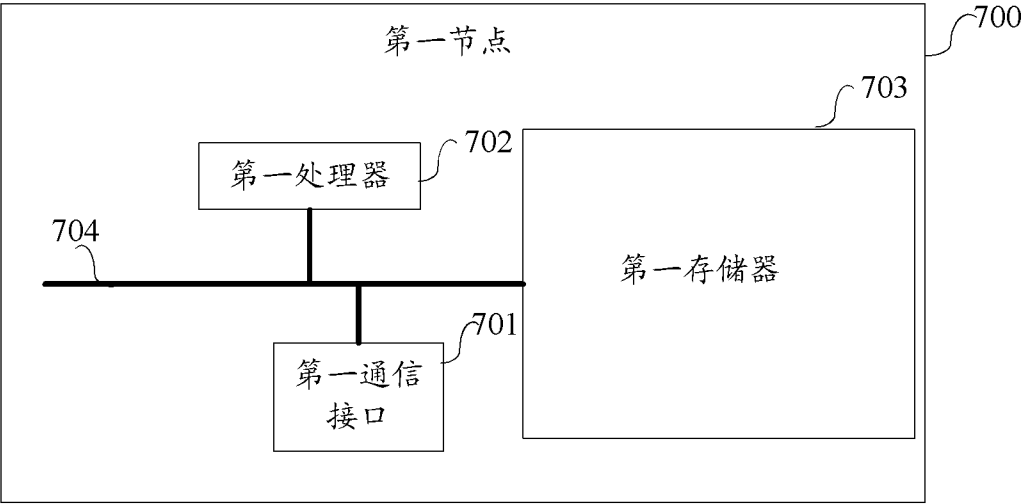


图 7

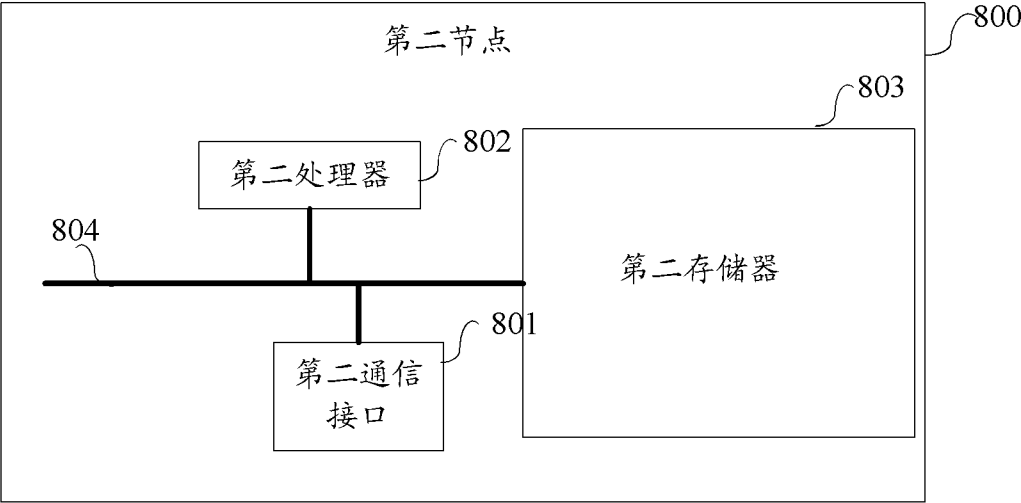


图 8

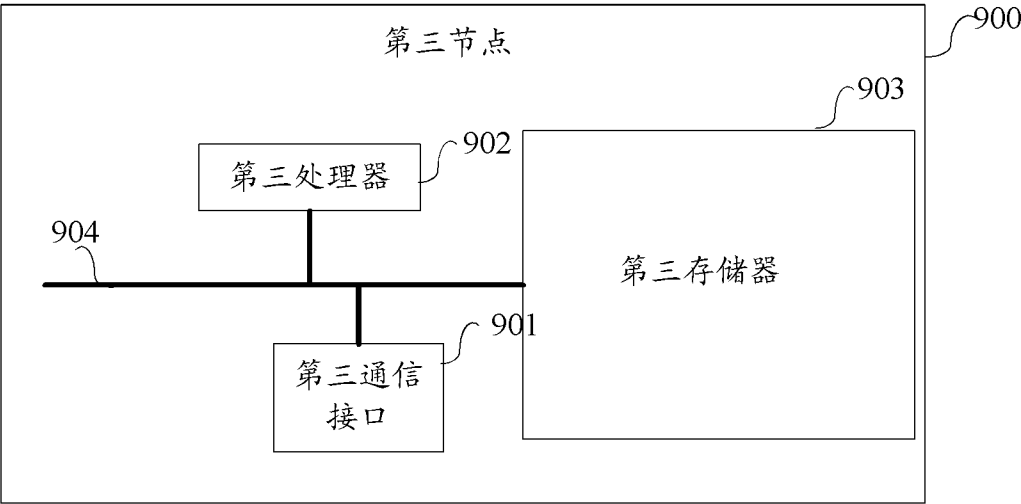


图 9

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2022/084185

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/08(2006.01)i; H04L 9/32(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPABSC; CNTXT; ENTXTC; CNKI; IEEE: 区块链, 联盟链, 许可链, 分布式账本, 公共密码, 公共密钥, 公共参数, 域名, 标识吊销列表, 标识撤销列表, 共识机制, ID-PKC, IBC, IRL

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 110138560 A (BEIJING INSTITUTE OF TECHNOLOGY) 16 August 2019 (2019-08-16) description, paragraphs 5-111	1-31
Y	CN 107360001 A (ALIBABA GROUP HOLDING LTD.) 17 November 2017 (2017-11-17) description, paragraphs 94-251	1-31
A	CN 112581051 A (NANJING UNIVERSITY OF POSTS AND TELECOMMUNICATIONS) 30 March 2021 (2021-03-30) entire document	1-31
A	US 2013212377 A1 (MALEK, B.) 15 August 2013 (2013-08-15) entire document	1-31



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

06 June 2022

Date of mailing of the international search report

16 June 2022

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/CN2022/084185

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110138560	A	16 August 2019	None			
CN	107360001	A	17 November 2017	US	2021281430	A1	09 September 2021
				US	2019036712	A1	31 January 2019
				EP	3607697	A1	12 February 2020
				JP	2020512714	A	23 April 2020
				WO	2019023452	A1	31 January 2019
				KR	20190118561	A	18 October 2019
				US	2020127855	A1	23 April 2020
				TW	201911172	A	16 March 2019
				SG	11201906755V	A	27 August 2019
				US	2021336802	A1	28 October 2021
				PH	12019501709	A1	24 February 2020
CN	112581051	A	30 March 2021	None			
US	2013212377	A1	15 August 2013	EP	2847928	A1	18 March 2015
				WO	2013116928	A1	15 August 2013
				CN	104641592	A	20 May 2015

国际检索报告

国际申请号

PCT/CN2022/084185

A. 主题的分类

H04L 9/08(2006.01)i; H04L 9/32(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

WPABSC;CNTXT;ENTXTC;CNKI;IEEE:区块链, 联盟链, 许可链, 分布式账本, 公共密码, 公共密钥, 公共参数, 域名, 标识吊销列表, 标识撤销列表, 共识机制, ID-PKC, IBC, IRL

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
Y	CN 110138560 A (北京理工大学) 2019年8月16日 (2019 - 08 - 16) 说明书第5-111段	1-31
Y	CN 107360001 A (阿里巴巴集团控股有限公司) 2017年11月17日 (2017 - 11 - 17) 说明书第94-251段	1-31
A	CN 112581051 A (南京邮电大学) 2021年3月30日 (2021 - 03 - 30) 全文	1-31
A	US 2013212377 A1 (MALEK BEHZAD) 2013年8月15日 (2013 - 08 - 15) 全文	1-31

☐ 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

2022年6月6日

国际检索报告邮寄日期

2022年6月16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

代悦宁

电话号码 010-62411527

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2022/084185

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	110138560	A	2019年8月16日	无			
CN	107360001	A	2017年11月17日	US	2021281430	A1	2021年9月9日
				US	2019036712	A1	2019年1月31日
				EP	3607697	A1	2020年2月12日
				JP	2020512714	A	2020年4月23日
				WO	2019023452	A1	2019年1月31日
				KR	20190118561	A	2019年10月18日
				US	2020127855	A1	2020年4月23日
				TW	201911172	A	2019年3月16日
				SG	11201906755V	A	2019年8月27日
				US	2021336802	A1	2021年10月28日
				PH	12019501709	A1	2020年2月24日
CN	112581051	A	2021年3月30日	无			
US	2013212377	A1	2013年8月15日	EP	2847928	A1	2015年3月18日
				WO	2013116928	A1	2013年8月15日
				CN	104641592	A	2015年5月20日