

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2020 年 10 月 15 日 (15.10.2020)



(10) 国际公布号
WO 2020/207233 A1

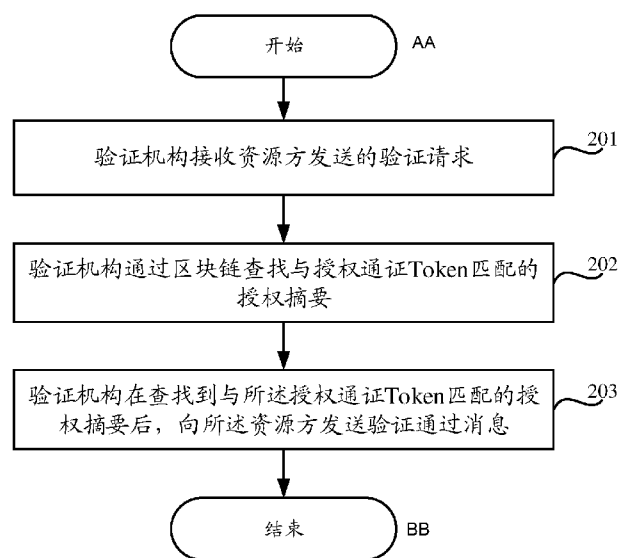
- (51) 国际专利分类号:
G06F 21/30 (2013.01) **H04L 29/08** (2006.01)
- (21) 国际申请号: PCT/CN2020/080519
- (22) 国际申请日: 2020 年 3 月 20 日 (20.03.2020)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201910287244.5 2019年4月11日 (11.04.2019) CN
- (71) 申请人: 深圳前海微众银行股份有限公司
(**WEBANK CO., LTD.**) [CN/CN]; 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。
- (72) 发明人: 胡朝新 (**HU, Chaixin**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201

室, Guangdong 518027 (CN)。张俊麒 (**ZHANG, Junqi**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。陈浩 (**CHEN, Hao**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。苏小康 (**SU, Xiaokang**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。张开翔 (**ZHANG, Kaixiang**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。范瑞彬 (**FAN, Ruibin**); 中国广东省深圳市前海深港合作区前湾一路1号A栋201室, Guangdong 518027 (CN)。

(74) 代理人: 北京同达信恒知识产权代理有限公司
(**TDIP & PARTNERS**); 中国北京市西城区裕民路18号北环中心A座2002, Beijing 100029 (CN)。

(54) **Title:** PERMISSION CONTROL METHOD AND APPARATUS FOR BLOCKCHAIN

(54) 发明名称: 一种区块链的权限控制方法及装置



- 201 A verification authority receives a verification request sent by a resource party
- 202 The verification authority searches for an authorization digest matching an authorization token by means of a blockchain
- 203 After the authorization digest matching the authorization token is found, the verification authority sends a verification successful message to the resource party
- AA Start
- BB End

图 2

(57) **Abstract:** Disclosed are a permission control method and apparatus for a blockchain, which relate to the technical field of fintech, and are used for solving the problem in the prior art of a rule storm occurring when the number of users and the volume of business grow rapidly. The method comprises: a verification authority receiving a verification request sent by a resource party, and if an authorization digest matching an authorization token in the verification request is found by means of a blockchain, sending a verification successful message to the resource party. An authorization token authorized by an authorization party is verified by means of a verification authority, so that the problem of a rule storm caused by overabundant permission rules configured on a blockchain can be prevented, and the privacy of the authorization token can be ensured. Moreover, since the authorization token stores a corresponding authorization

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, 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, 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))。

digest by means of a blockchain, the problem of relatively low security of authorization caused by the possibility of an illegal behavior of an authorization party can also be prevented, and the security of the authorization token is ensured.

(57) 摘要: 一种区块链的权限控制方法及装置, 涉及金融科技(Fintech)技术领域, 用以解决现有技术在使用户数、业务量快速增长的情况下所出现的规则风暴的问题。方法包括: 验证机构接收资源方发送的验证请求, 若通过区块链查找到与验证请求中的授权Token匹配的授权摘要, 则向资源方发送验证通过的消息。通过验证机构验证授权方授权的授权Token, 能够避免区块链上设置权限规则过多所导致的规则风暴问题, 并能保证授权Token的隐私性。且, 由于授权Token通过区块链存储对应的授权摘要, 因此还能避免由于授权方存在作恶的可能性所导致的授权的安全性较低的问题, 保证授权Token的安全性。

一种区块链的权限控制方法及装置

相关申请的交叉引用

本申请要求在2019年04月11日提交中国专利局、申请号为201910287244.5、
申请名称为“一种区块链的权限控制方法及装置”的中国专利申请的优先权，
其全部内容通过引用结合在本申请中。

技术领域

本发明实施例涉及金融科技（Fintech）技术领域，尤其涉及一种区块链
的权限控制方法及装置。

背景技术

随着计算机技术的发展，越来越多的技术应用在金融领域，传统金融业
正在逐步向金融科技（Fintech）转变，单点登录技术也不例外，但由于金融
行业的安全性、实时性要求，也对技术提出的更高的要求。

单点登录，（Single Sign-On, SSO）是一个用户认证的过程，允许用户在
经过一次认证后，就可访问系统中的不同应用；而无需在访问每个应用时，
都重新输入用户账号和密码。

SSO 将一个企业内部所有域中的用户登录和用户帐号管理集中到一起，
可以减少用户在不同系统中登录所耗费的时间，减少用户登录出错的可能性，
实现安全的同时避免处理和保存多套系统用户的认证信息，减少系统管理员
增加、删除和修改用户权限的时间，增加了安全性。且，系统管理员有了更
好的方法来管理用户，比如直接禁止用户或删除用户，以取消该用户对所有
系统资源的访问权限。

目前，在对 SSO 进行权限控制时，在用户数、业务量快速增长的情况下，
容易出现规则风暴的问题；另外，现有技术中经由授权方为用户提供权限管
理，而授权方存在作恶的可能性，无法保证授权的安全性。

发明内容

由于目前基于角色的权限控制方法中账户权限受限于角色的预设权限，在用户数、业务量快速增长的情况下，会出现规则风暴的问题，本发明提供了一种区块链的权限控制方法及装置。

5 第一方面，本发明提供一种区块链的权限控制方法，包括：

验证机构接收资源方发送的验证请求，所述验证请求包括授权通证 Token；所述验证机构通过区块链查找与所述授权 Token 匹配的授权摘要，并在查找
10 到与所述授权 Token 匹配的授权摘要后，向所述资源方发送验证通过消息；所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

10 本发明中，通过验证机构验证授权方授权的授权 Token，而不是像现有技术中验证权限规则，能够避免区块链上设置权限规则过多所导致的规则风暴问题，并能保证授权 Token 的隐私性。另外，由于该授权 Token 通过区块链存储对应的授权摘要，因此还能避免在为用户进行权限管理的过程中，由于
15 授权方存在作恶的可能性所导致的授权的安全性较低的问题，保证授权 Token 的安全性。

一种可能的实现方式，所述方法还包括：所述验证机构接收授权方发送的上传请求，所述上传请求中包括授权 Token；所述验证机构验证所述授权
Token 中的授权方合法且所述授权 Token 中的授权内容包括授权的资源，则将
所述授权 Token 的授权摘要上传至所述区块链。

20 在上述实现方式中，该授权 Token 通过区块链存储对应的授权摘要，并在链上验证授权 Token 的合法性，使得授权 Token 的安全性能得到保证，避免由授权方为用户进行权限管理的方式所存在的授权方作恶的可能性。

一种可能的实现方式，所述区块链中还存储有账户信息，所述账户信息包括账户与属性的对应关系、属性与资源权限的对应关系；所述验证机构验
25 证所述授权 Token 中的授权方合法，包括：根据所述账户与属性的对应关系，确定所述授权方的属性，根据所述属性与资源权限的对应关系，确定所述授权方的属性中是否具有所述授权 Token 中的授权内容的访问权限，若有，则

确定所述授权 Token 的授权方合法。

在上述实现方式中，通过设置账户与属性的对应关系、属性与资源权限的对应关系，使得验证机构根据授权方的属性即可验证授权方的访问权限，减少验证过程的复杂度；且，由于减少了需要存储的账户对应的权限规则，还能进一步避免规则风暴的问题。

一种可能的实现方式，所述授权 Token 是授权机构生成的。

在上述实现方式中，通过授权机构生成授权 Token，能够避免授权方私下生成授权 Token，从而可以提高授权 Token 的安全性。

第二方面，本发明提供一种区块链的权限控制方法，包括：

资源方获取资源请求方发送的针对第一资源的访问请求，所述访问请求包括授权 Token，所述授权 Token 包括授权方及授权内容；所述资源方确定所述访问请求满足访问所述第一资源的第一访问条件时，向所述资源请求方发送所述资第一资源；所述第一访问条件为通过区块链查找到与所述授权 Token 匹配的授权摘要、所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括所述第一资源；所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

本发明中，资源请求方通过在访问请求中携带授权 Token，使得资源方能够对授权 Token 进行多方验证，比如验证授权 Token 的合法性、授权 Token 的授权内容、授权方的权限等，如此，资源方通过验证授权方授权的授权 Token 确定权限，而不是像现有技术中验证权限规则，不仅可以避免区块链上设置权限规则过多所导致的规则风暴的问题，保证授权 Token 的隐私性，还能够保证验证结果的有效性。并且，由于该授权 Token 通过区块链存储对应的授权摘要，并在链上验证授权 Token 的合法性，使得授权 Token 的安全性能得到保证，避免使用授权方为用户进行权限管理所存在的授权方作恶的可能性。

一种可能的实现方式，所述访问请求还包括授权方签名，所述授权方签名是所述授权方对生成的授权 Token 进行签名得到的；所述资源方确定所述

访问请求满足访问所述第一资源的访问条件前，还通过所述授权方签名确定所述授权 Token 为所述授权方发布的。

在上述实现方式中，通过对授权 Token 进行数字签名，能进一步提高授权 Token 的安全性。

5 一种可能的实现方式，所述资源方确定所述访问请求满足访问所述第一访问条件之前，还确定所述访问请求不满足访问所述第二访问条件；所述第二访问条件为所述资源请求方的账户是所述账户信息中记录的针对所述第一资源具有访问权限的账户。

10 在上述实现方式中，通过预先验证资源请求方对应的账户的权限，能够确保验证的全面性，提高验证的有效性。

一种可能的实现方式，所述授权内容包括授权的属性；确定所述授权 Token 中的授权内容包括所述第一资源，为根据以下方式确定的：根据所述授权的属性，在所述属性与资源权限的对应关系中，查找所述授权的属性对应的资源是否包括所述第一资源；若确定包括所述第一资源，则确定所述授权
15 Token 中的授权内容包括所述第一资源。

在上述实现方式中，通过设置授权的属性，使得授权 Token 的授权和验证更加灵活，并且通过压缩授权 Token 的字段，还能缩短验证的传输时间，通过验证授权的属性或授权的属性对应的资源来验证授权 Token，使得提供的可选的验证方式更多，验证效率更高。

20 一种可能的实现方式，所述授权内容包括授权的资源；确定所述授权 Token 中的授权内容包括所述第一资源，为根据以下方式确定的：若确定所述授权内容中的授权的资源包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

25 在上述实现方式中，通过在授权内容中设置授权的资源，能够通过查找授权内容中的授权的资源直接确定是否存在第一资源，缩短验证时间，提高验证效率。

第三方面，本发明实施例提供一种区块链的权限控制装置，包括：

收发单元，用于接收资源方发送的验证请求，所述验证请求包括授权 Token;

处理单元，用于通过区块链查找与所述授权 Token 匹配的授权摘要；所述区块链中存储有各授权方生成的授权 Token 的授权摘要；

5 所述收发单元，用于在查找到与所述授权 Token 匹配的授权摘要后，向所述资源方发送验证通过消息。

一种可能的实现方式，所述收发单元还用于：接收授权方发送的上传请求，所述上传请求中包括授权 Token；所述处理单元，还用于验证所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括授权的资源，则将
10 所述授权 Token 的授权摘要上传至所述区块链。

一种可能的实现方式，所述区块链中还存储有账户信息，所述账户信息包括账户与属性的对应关系、属性与资源权限的对应关系；所述处理单元，具体用于根据所述账户与属性的对应关系，确定所述授权方的属性；根据所述属性与资源权限的对应关系，确定所述授权方的属性中是否具有所述授权
15 Token 中的授权内容的访问权限；若有，则确定所述授权 Token 的授权方合法。

一种可能的实现方式，所述授权 Token 是授权机构生成的。

第四方面，本发明实施例提供一种区块链的权限控制装置，包括：

收发单元，用于获取资源请求方发送的针对第一资源的访问请求；所述访问请求包括授权凭证 Token；所述授权 Token 包括授权方及授权内容；

20 处理单元，用于确定所述访问请求满足访问所述第一资源的第一访问条件时，向所述资源请求方发送所述第一资源；所述第一访问条件为通过区块链查找到与所述授权 Token 匹配的授权摘要、所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括所述第一资源；所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

25 一种可能的实现方式，所述访问请求还包括授权方签名，所述授权方签名是所述授权方对生成的授权 Token 进行签名得到的；所述处理单元确定所述访问请求满足访问所述第一资源的访问条件前，还通过所述授权方签名确

定所述授权 Token 为所述授权方发布的。

一种可能的实现方式，所述处理单元确定所述访问请求满足访问所述资源的第一访问条件之前，还确定所述访问请求不满足访问所述资源的第二访问条件；所述第二访问条件为所述资源请求方的账户是所述账户信息中记录的针对所述第一资源具有访问权限的账户。

一种可能的实现方式，所述授权内容包括授权的属性；所述处理单元，具体用于根据所述授权的属性，在所述属性与资源权限的对应关系中，查找所述授权的属性对应的资源是否包括所述第一资源；若确定包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

一种可能的实现方式，所述授权内容包括授权的资源；所述处理单元，具体用于若确定所述授权内容中的授权的资源包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

第五方面，本发明实施例提供了一种计算机设备，包括至少一个处理单元、以及至少一个存储单元，其中，所述存储单元存储有计算机程序，当所述程序被所述处理单元执行时，使得所述处理单元执行区块链的权限控制方法的步骤。

第六方面，本发明实施例提供了一种计算机可读介质，其存储有可由终端设备执行的计算机程序，当所述程序在终端设备上运行时，使得所述终端设备执行区块链的权限控制方法的步骤。

附图说明

为了更清楚地说明本发明实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简要介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域的普通技术人员来讲，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。

图 1 为本发明实施例提供的一种区块链网络的系统架构示意图；

图 2 为本发明实施例提供的一种区块链的权限控制方法的流程示意图；

图 3 为本发明实施例提供的一种区块链的权限控制方法的流程示意图；

图 4 为本发明实施例提供的一种区块链的权限控制方法的流程示意图；

图 5 为本发明实施例提供的一种区块链的权限控制装置的结构示意图；

图 6 为本发明实施例提供的又一种区块链的权限控制装置的结构示意图；

5 图 7 为本发明实施例提供的一种计算设备的结构示意图。

具体实施方式

为了使本发明的目的、技术方案及有益效果更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体
10 实施例仅仅用以解释本发明，并不用于限定本发明。

为了方便理解，下面对本发明实施例中涉及的名词进行解释。

区块链：区块链是利用块链式数据结构来验证与存储数据、利用分布式
节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的
安全、利用自动化脚本代码组成的智能合约来编程和操作数据等一项或多项
15 的一种全新的分布式基础架构与计算方式。

本发明实施例提供一种区块链的权限控制方法，可以应用于区块链网络
场景中，以提高单点登录的安全性，避免授权方作恶的可能。

示例性地，图 1 为本发明实施例提供的一种区块链网络的系统架构示意
图，如图 1 所示，区块链网络中包括多个网络节点，比如网络节点 101、网络
20 节点 102 和网络节点 103，任一网络节点中包括区块链的权限控制装置。其中，
每个网络节点可以是一台服务器，也可以是若干台服务器组成的服务器集群，
各个网络节点之间通过无线网络连接。

在维护区块链的机构中，每个机构可以对应一个或多个网络节点，区块
链中各网络节点中的表实时同步。针对每个网络节点，机构在其它网络节点
25 中通过交易账户发起交易请求，该网络节点在接收到交易请求后，根据交易
信息确定待操作的内容。其中，交易请求可以为访问资源的访问请求，也可
以为验证请求等。对应的，待操作的内容可以为访问资源，也可以为验证权

限等。进一步地，该网络节点从预设的权限表中确定待操作的内容对应的交易账户，在确定交易账户与待操作的内容对应的权限账户匹配时，返回给用户需要访问的资源。之后，该网络节点生成待操作的内容的操作记录，并将所述操作记录发送至区块链网络中的其他网络节点，操作记录包括待操作的内容标识、待操作的内容的权限内容和交易账户。

其中，本发明中提到的资源可以为资源 URI。例如，数据网页统一资源定位符（Uniform Resource Location，URL）、可执行的状态转移应用程序接口（Resource Representational State Transfer Application Programming Interface，RESTful API），例如 GET/POST/DELETE 等，不作限定。

区块链上的用户拥有不同的角色，同时对不同的资源有不同的访问权限，用户存在着权限授权的需求。传统安全领域里存在一种现有的权限管理方法，在该方法中，授权一般通过 SSO Token 来表示，但 SSO Token 直接移植到区块链系统上会出现规则风暴的问题。比如，若每个权限都不加区分地上链，则会导致授权类型单一的问题，且还需要设置大量的权限规则，每个权限在使用时都需要链上检查等。如此，在用户数、业务量快速增长的情况下（即业务量较大），过多的规则会使得传统数据库难以接纳，从而出现规则风暴的问题。

基于上述问题，本发明实施例提供了一种区块链的权限控制方法的流程，用以解决现有技术为用户数、业务量快速增长的情况下出现的规则风暴的技术问题。

图 2 为本发明实施例提供的区块链的权限控制方法的流程示意图，该方法可以由区块链的权限控制装置执行，如图 2 所示，包括以下步骤：

步骤 201：验证机构接收资源方发送的验证请求，所述验证请求包括授权 Token。

其中，资源方具体是指资源的持有者。授权 Token 为用于描述授权信息的单元，可以表示为一个 json 字符串。授权 Token 的字段可以包括：授权 Token 的通用唯一识别码（Universally Unique Identifier，UUID），UUID 用于表示授

权 Token 的唯一标识; 授权原用户区块链地址; 授权目的用户区块链地址 (可以通配); 授权内容; 授权发生时间; 授权终止时间; 授权用户数字签名等。

步骤 202: 验证机构通过区块链查找与所述授权 Token 匹配的授权摘要; 所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

5 步骤 203: 验证机构在查找到与所述授权 Token 匹配的授权摘要后, 向所述资源方发送验证通过消息。

10 本发明实施例中, 由授权方生成授权 Token, 使得授权 Token 的授权内容不需要完全保存在权限表中, 因此当资源请求方的账户发起访问请求时, 可以直接验证授权方及授权 Token, 以灵活实现对访问资源的权限控制。且, 由于授权方在生成授权 Token 时, 无需写入权限表, 因此授权方还可以根据自身的权限自由设置账户的具体权限, 并基于实际需要对授权 Token 的授权内容进行增删, 以实现对授权的权限的自由增删, 避免将所有规则都上链所导致的规则风暴的问题, 提高授权 Token 的隐私保护。

15 在步骤 201 中, 授权方可以为资源请求方创建对应的授权 Token。其中, 资源请求方可以为单点登录系统中的任一用户, 也可以为区块链上注册的任一账户。

其中, 具体的生成过程可以包括:

20 授权方根据授权目标账户 (结合上述场景, 可以为资源请求方)、授权方账户、授权内容、授权起止时间, 生成指定格式的授权 Token。授权方可以在链外为资源请求方创建对应的授权 Token, 例如, 授权方为授权机构, 授权机构可以为链外的设备, 授权机构经过验证后, 就可以将授权 Token 发送给资源请求方。

25 示例性地, 可以从区块链网络中推选出管理节点, 然后将管理节点对应的账户设置为管理员账户, 只有管理员账户可以成为授权方, 非管理员账户不能成为授权方, 即非管理账户无授权功能。

本发明实施例中, 授权 Token 的授权内容可以包括属性、资源这两种类型的授权内容。其中, 属性授权是指授权方可以将自己的某个属性授权给资

源方使用。需要说明的是，属性可以为账户的任一特征，例如账户的角色，账户的地理位置，访问时间等特征，在此不做限定。资源授权是指授权方可以将自己对某个资源的访问权限授权给资源请求方使用。

具体地，权限信息可以存储于权限表中，用于确定权限控制使用规则。

5 在设置一个账户对某个表的权限时，在权限表中添加该账户对应的权限记录。示例性地，权限表位于区块链的区块中，在更新权限表时，更新后的权限表在当前区块的下一个区块生效。比如，在权限表中添加新权限记录 A 时，在当前区块之后生成新区块，将新权限记录 A 保存在新区块的区块主体中。或者，在权限表中修改权限记录 B 时，在当前区块之后生成新区块，将修改后
10 的权限记录 B 保存在新区块的区块主体中。

具体实施中，可以采用预设的权限合约接口对权限表进行操作。权限合约接口可以包括写入接口、移除接口、查询接口等。写入接口通过表名称和账户地址设置权限记录，并返回设置的记录数，设置的记录将保存在权限表中，若权限记录为已存在的权限记录，则拒绝重复设置相同的权限记录，即
15 直接返回 0。移除接口通过表名称和账户地址移除设置的权限记录，并返回移除的记录数。查询接口通过表名称查询设置的权限记录，并返回查询得到的权限记录，记录可以以 json 字符串的形式返回。

一种可能的实现方式中，权限表可以包括属性账户表及属性权限表。其中，属性账户表用于存储注册的账户中的属性，以及每个属性对应的账户。
20 属性账户表中的记录可以由注册方写入，也可以由授权方写入。相应地，属性权限表用于存储注册的账户中的每个属性对应的资源的访问权限。

一种可能的实现方式中，授权内容包括授权的属性；授权方根据授权目标账户所需授权的资源，及授权目标账户的属性，确定授权 Token 的授权内容。其中，授权目标账户的属性可以是授权方为授权目标账户设置的，也可以
25 是授权目标账户在注册时，注册方为授权目标账户设置的，在此不做限定。

在上述实现方式中，通过设置账户与属性的对应关系、属性与资源权限的对应关系，使得能够根据授权方的属性直接验证授权方的访问权限，减少

验证过程的复杂度；且，通过减少需要存储的账户对应的权限规则，能够进一步避免规则风暴的问题。

本发明实施例中，若授权目标账户的属性是授权目标账户在注册时注册方为授权目标账户设置的，则注册方还可以在授权目标账户注册时，将授权目标账户的属性写入区块链。例如，将授权目标账户的属性与授权目标账户的账户写入账户属性表中。如此，授权方可以通过查询账户属性表，直接确定授权目标账户的账户对应的属性。

示例性地，由于区块链上的账户属性表是公开的，因此，为提高授权 Token 的安全性，并减少规则的设置，避免规则风暴，在授权方为授权目标账户设置授权 Token 时，还可以重新设置授权目标账户的属性，即授权 Token 中的授权属性不写入授权目标账户的账户中。

示例性地，授权 Token 中的授权内容包括第一资源，判断是否包括第一资源的方式可以为：验证机构根据授权的属性，在该属性与资源权限的对应关系中，查找授权的属性对应的资源是否包括第一资源；若确定包括第一资源，则确定授权 Token 中的授权内容包括第一资源。通过设置授权的属性，使得授权 Token 的授权和验证更加灵活，并且压缩了授权 Token 的字段，缩短了验证的传输时间，如此，验证机构可以通过验证授权的属性来验证授权 Token，也可以通过验证授权的属性对应的资源来验证授权 Token，从而提供了更多可选的验证方式，提高验证效率。

一种可能的实现方式中，为提高授权 Token 的安全性，并减少规则的设置，避免规则风暴，授权方在为授权目标账户设置授权 Token 时，还可以采用重新设置授权目标账户的资源权限的方式，即授权 Token 中的授权资源不写入权限表中。

具体的，授权内容可以包括授权的资源；授权方根据授权目标账户所需授权的资源，确定授权 Token 的授权内容，如此，授权 Token 中的授权内容为授权资源。

示例性地，授权 Token 中的授权内容包括第一资源，判断是否包括第一

资源的方式可以为：若确定授权内容中的授权的资源包括第一资源，则确定授权 Token 中的授权内容包括第一资源。通过在授权内容中设置授权的资源，能够缩短验证时间，提高验证效率。

示例性地，为提高授权 Token 的安全性，还可以使用授权方的私钥对授权 Token 进行签名。其中，授权方的私钥为授权方在区块链上注册时生成并存储每个账户的公钥数据。具体地，为用户创建账户时，先生成账户的公私钥对，再将公钥存入公钥数据合约；当然，也可以先为用户上传符合算法格式要求的公钥，再验证并存储。

一种可能的实现方式中，授权 Token 由授权机构生成。如此，通过授权机构生成授权 Token，能够避免授权方私下生成授权 Token，从而提高授权 Token 的安全性。

本发明实施例中，授权机构可以为区块链外的机构，也可以为区块链上的机构；验证机构可以为区块链上的机构，也可以为区块链外的机构，不作限定。

一种可能的实现方式中，授权 Token 全部上链。此时，上链逻辑由具体的用户转向成为智能合约，如此，规则和执行均全网可见，而不须额外的道德风险。其次，授权记录可以减少一个字段，以降低存储开销和未来的索引时间开销。

一种可能的实现方式中，授权 Token 全部不上链。此时，授权 Token 的安全性可以通过授权用户的数字签名来保证，如此，通过链外执行可以使得验签算法时间开销大大降低。

一种可能的实现方式中，授权 Token 的上链方式可以通过链外机构上链，链外机构可以为确定出的至少一个权威维护方，权威维护方用于维护授权数据记录表。如此，每个授权方需要授权 Token 上链时，可以向至少一个权威维护者发送上传请求。

其中，权威维护者上链的链外工具可以按照本发明实施例中的方案的流程实现，且接受审计监督。链外工具可以为 SDK/RESTful Client。

示例性地，授权数据记录表中的授权记录中还增加一个上链者签名的字段，上链者签名可以根据权威维护者的私钥生成。

一种可能的实现方式中，为减少区块链的存储内容，并提高授权 Token 的安全性，授权方还可以对自己创建的授权 Token 上链。具体实施中，验证机构可以接收授权方发送的上传请求，上传请求中包括授权 Token；进一步地，验证机构若验证授权 Token 中的授权方合法且授权 Token 中的授权内容包括授权的资源，则将授权 Token 的授权摘要上传至区块链。

其中，上传请求可以由链上的节点进行处理。具体包括：

步骤一，验证机构检查该授权 Token 内容是否合法。

具体实施中，验证机构可以检查授权 token 的数字签名，判断能否正确地解出授权方的公钥值。如果可以，则执行步骤二；否则，执行步骤四。

步骤二、验证机构调用属性管理模块检查该授权是否有效。

此处，授权的验证逻辑可以在链外，也可以在链上。但是，验证机构接收的任何包括授权 Token 的请求均需验证授权 Token 的有效性和签名。

具体的，验证机构可以检测授权方是否有对应的授权资源的访问权限。若无，则执行步骤四；否则，执行步骤三；

步骤三、验证机构生成授权 Token 的哈希值（即 Hash 值），并存入链上。

此处，可以存入区块链上的授权数据表，并返回授权方的链上表项索引。

一种可能的实现方式中，授权 Token 的授权摘要可以为授权 Token 的哈希值。其中，存于链上授权数据记录表的授权记录可以包括以下字段：UUID；Hash 值。授权 Token 的哈希值可以为基于摘要生成算法生成的摘要值，如 sha3（授权 Token）。

在上述实现方式中，由于通过区块链存储授权 Token 对应的授权摘要，因此，在链上验证授权 Token 的合法性，使得授权 Token 的安全性能得到保证，避免使用授权方管理用户权限所存在的授权方作恶的可能性。

示例性地，为提高验证 Token 的安全性，授权数据记录表只允许验证机构单向访问。也就是说，一旦新增某条记录，则该条记录后续不可修改。

图 3 为本发明实施例提供的一种区块链的权限控制方法的流程示意图，如图 3 所示，验证机构的验证逻辑与授权数据表中的数据分离，对应的验证合约只用于验证机构进行验证授权 Token，验证机构支持升级与数据迁移。授权数据表中，每条记录均存在有效期，授权记录主要包括如下两类：

5 i. 属性授权记录：每条属性授权记录的数据表示存在属性类型的授权 Token 的摘要，即，已有相同属性的账户可以授权他人复用同样属性。

ii. 资源授权记录：每条资源授权记录的数据表示存在资源类型的授权 Token 的摘要，即，已有相同操作权限的账户可以授权他人访问某资源。

10 以上两个表的内容可以被区块链上的所有节点公开查询，每条授权记录的授权方可以对授权记录进行修改。

步骤四、验证机构向授权方返回上传请求失败的消息。

为了更好的解释本发明实施例，下面结合具体的实施场景描述本发明实施例提供的区块链的权限控制方法，该方法可以由网络节点在链上执行，也可以链外执行，该方法包括以下步骤：

15 步骤一、授权方向授权机构发送授权 Token 的生成请求。

其中，授权 Token 的生成请求中包括授权 Token 的参数，即授权目标账户（结合上述场景，可以为资源请求方）、授权方账户、授权内容、授权起止时间、数字签名等。

20 步骤二、授权机构对授权 Token 的参数进行合法性检查，如果检查通过，则执行步骤三；否则，执行步骤五。

步骤三、授权机构生成授权 Token，并使用授权方传入的私钥对授权 Token 进行签名。

步骤四、授权机构将生成的授权 Token 发送至授权方。

步骤五、授权机构向授权方返回生成失败的消息。

25 为了更好的解释本发明实施例，下面结合具体的实施场景描述本发明实施例提供的区块链的权限控制方法，该方法可以由网络节点在链上执行，也可以链外执行，该方法包括以下步骤：

步骤一、授权方向验证机构发送已签名的授权 Token。

步骤二、验证机构检查授权 Token 的参数合法性，参数包括授权 Token 的有效期、签名等。如果检查通过，则执行步骤三；否则，执行步骤五。

5 步骤三、验证机构访问权限表，检查授权 Token 的授权内容是否真实有效。例如，检查授权方中是否有所声明的资源权限可以用于授权。如果检查通过，则执行步骤四；否则，执行步骤五。

步骤四、验证机构生成授权 Token 的 Hash 值，存入至链上授权数据表，并给授权方返回上传成功的信息，和/或授权数据表的记录。

10 为了更好的解释本发明实施例，下面结合具体的实施场景描述本发明实施例提供的一种区块链的权限控制方法，该方法可以由网络节点在链上执行，也可以链外执行，该方法包括以下步骤：

步骤一、资源方上传需要验证的授权 Token。

15 一种可能的实现方式中，资源方也可以选择性上传资源请求方链上的授权 Token 所对应的链上记录信息，例如授权 Token 的授权摘要的索引，以便验证机构快速验证所述授权 Token。

步骤二、验证机构对授权 Token 进行参数合法性检查；若合法，则执行步骤三；否则，执行步骤五。

20 具体的，验证机构可以访问属性管理模块，以检查授权 Token 的授权内容是否真实有效，即授权 Token 的授权方中是否有所声明的资源可以被用来授权。

步骤三、如果传入的链上记录信息不为空，则验证机构访问链上的授权记录表，确定出需要验证的授权 Token 的 Hash 值，并对比该 Hash 值与授权记录表中的 Hash 值是否一致。若是，则执行步骤四；否则，执行步骤五。

步骤四、确定资源方上传的需要验证的授权 Token 验证成功。

25 步骤五、确定资源方上传的需要验证的授权 Token 验证失败。

需要说明的是，步骤三与步骤四可以交换验证顺序，在此不做限定。

图 4 为本发明实施例提供一种区块链的权限控制方法，如图 4 所示，该方法包括：

步骤 401：资源方获取资源请求方发送的针对第一资源的访问请求。

其中，访问请求包括授权凭证 Token，授权 Token 包括授权方及授权内容。

5 步骤 402：资源方确定所述访问请求满足访问所述第一资源的第一访问条件时，向所述资源请求方发送所述第一资源。

此处，区块链中存储有各授权方生成的授权 Token 的授权摘要。

相应地，所述第一访问条件为：在区块链中查找到与所述授权 Token 匹配的授权摘要，且所述授权 Token 中的授权方合法，且所述授权 Token 中的
10 授权内容包括所述第一资源。

本发明实施例中，通过资源请求方携带授权 Token，并对授权 Token 进行多方验证，比如验证授权 Token 的合法性、验证授权 Token 的授权内容、验证授权方的权限等，能够保证验证结果的有效性。且，通过授权方在生成授权 Token，可以无需将授权 Token 写入权限表中，如此，授权方可以根据自身的
15 权限自由设置账户的具体权限，并能基于实际需要授权 Token 的授权内容进行增删，以实现对授权的权限的自由增删，相比于现有技术验证权限规则的方式来说，能够避免对所有规则都上链所导致的规则风暴的问题，提高授权 Token 的隐私保护。此外，该授权 Token 还能通过区块链存储对应的授权摘要，如此，通过在链上验证授权 Token 的合法性，使得授权 Token 的安全性能够
20 得到保证，避免授权方管理用户权限时所存在的授权方作恶的可能性。

一种可能的实现方式中，所述访问请求还包括授权方签名；所述资源方确定所述访问请求满足访问所述第一资源的访问条件前，还通过所述授权方签名确定所述授权 Token 为所述授权方发布的；所述授权方签名是所述授权
25 方对生成的授权 Token 进行签名得到的。如此，通过基于数字签名来验证授权 Token，还能进一步提高授权 Token 的安全性。

一种可能的实现方式中，所述资源方确定所述访问请求满足访问所述资

源的第一访问条件之前，还确定所述访问请求不满足访问所述资源的第二访问条件；所述第二访问条件为所述资源请求方的账户是所述账户信息中记录的针对所述第一资源具有访问权限的账户。如此，通过预先验证资源请求方对应的账户的权限，能够确保验证的全面性，提高验证的有效性。

5 本发明提出的方案旨在灵活性和可扩展性上取得平衡，并保证授权内容的多维、多粒度、授权 Token 的不可篡改性。且，授权方可以对授权类型进行划分，还可以在属性、资源两个授权类型上，将自己的能力授权给授权目标账户，同时允许撤销授权。且，授权 Token 的授权摘要可以存储在区块链上，由于只存储授权 Token 的授权摘要，因此能够保证其最小披露且不可篡改。
10 改。基于此，故而本发明能大大降低了规则风暴的影响，具有良好的可扩展性。

为了更好的解释本发明实施例，下面结合具体的实施场景描述本发明实施例提供的区块链的权限控制方法，该方法由网络节点执行，该方法包括以下步骤：

15 步骤一、资源请求方向资源方发送资源请求，所述资源请求包括授权 Token，及链上授权记录地址。

步骤二、资源方检查资源请求方在不使用授权 Token 的情况下能否直接满足访问资源的第二访问资源条件；若是，则执行步骤五，否则，执行步骤三。

20 步骤三、资源方通过验证机构，验证授权 Token。若验证成功，则执行步骤五；否则，执行步骤六。

具体流程见上述实施例中的验证授权 Token 的方法，在此不再赘述。

步骤四、资源方根据授权 Token 中的授权内容，检查授权 Token 是否满足第一访问资源条件；若是，则执行步骤五。

25 步骤五、资源方向资源请求方返回所请求资源的内容。

步骤六、资源方向资源请求方返回请求失败的消息。

示例性地，本发明实施例中，授权机构为区块链外的机构，验证机构为

区块链上的机构；或，授权机构与验证机构均为区块链外的机构。

基于相同的技术构思，本发明实施例提供了一种区块链的权限设置装置。

图 5 为本发明实施例提供的一种区块链的权限设置装置的结构示意图，如图 5 所示，包括：

5 收发单元 501，用于接收资源方发送的验证请求，所述验证请求包括授权 Token；

处理单元 502，用于通过区块链查找与所述授权 Token 匹配的授权摘要；所述区块链中存储有各授权方生成的授权 Token 的授权摘要；

10 所述收发单元 501，还用于在查找到与所述授权 Token 匹配的授权摘要后，向所述资源方发送验证通过消息。

一种可能的实现方式中，所述收发单元 501 还用于接收授权方发送的上传请求，所述上传请求中包括授权 Token；

15 所述处理单元 502，还用于在验证所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括授权的资源后，将所述授权 Token 的授权摘要上传至所述区块链。

一种可能的实现方式中，所述区块链中还存储有账户信息，所述账户信息包括账户与属性的对应关系、属性与资源权限的对应关系；

20 所述处理单元 502，具体用于根据所述账户与属性的对应关系，确定所述授权方的属性；根据所述属性与资源权限的对应关系，确定所述授权方的属性中是否具有所述授权 Token 中的授权内容的访问权限；若有，则确定所述授权 Token 的授权方合法。

一种可能的实现方式，所述授权 Token 是授权机构生成的。

图 6 为本发明实施例提供的又一种区块链的权限设置装置的结构示意图，如图 6 所示，包括：

25 收发单元 601，用于获取资源请求方发送的针对第一资源的访问请求；所述访问请求包括授权凭证 Token；所述授权 Token 包括授权方及授权内容；

处理单元 602，用于确定所述访问请求满足访问所述第一资源的第一访问

条件时，向所述资源请求方发送所述第一资源；所述第一访问条件为通过区块链查找到与所述授权 Token 匹配的授权摘要、所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括所述第一资源；所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

5 一种可能的实现方式中，所述访问请求还包括授权方签名，所述授权方签名是所述授权方对生成的授权 Token 进行签名得到的；

所述处理单元 602 确定所述访问请求满足访问所述第一资源的访问条件前，还用于：

通过所述授权方签名确定所述授权 Token 为所述授权方发布的。

10 一种可能的实现方式，所述处理单元 602 确定所述访问请求满足访问所述资源的第一访问条件之前，还用于：

确定所述访问请求不满足访问所述资源的第二访问条件；所述第二访问条件为所述资源请求方的账户是所述账户信息中记录的针对所述第一资源具有访问权限的账户。

15 一种可能的实现方式，所述授权内容包括授权的属性；

所述处理单元 602，具体用于根据所述授权的属性，在所述属性与资源权限的对应关系中，查找所述授权的属性对应的资源是否包括所述第一资源；若确定包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

20 一种可能的实现方式，所述授权内容包括授权的资源；

所述处理单元 602，具体用于若确定所述授权内容中的授权的资源包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

25 基于相同的技术构思，本发明实施例提供了一种计算设备，如图 7 所示，包括至少一个处理器 701，以及与至少一个处理器连接的存储器 702，本发明实施例中不限定处理器 701 与存储器 702 之间的具体连接介质，图 7 中处理器 701 和存储器 702 之间通过总线连接为例。总线可以分为地址总线、数据总线、控制总线等。

在本发明实施例中，存储器 702 存储有可被至少一个处理器 701 执行的指令，至少一个处理器 701 通过执行存储器 702 存储的指令，可以执行前述的区块链的权限控制方法中所包括的步骤。

其中，处理器 701 是计算设备的控制中心，可以利用各种接口和线路连接计算设备的各个部分，通过运行或执行存储在存储器 702 内的指令以及调用存储在存储器 702 内的数据，从而控制权限。可选的，处理器 701 可包括一个或多个处理单元，处理器 701 可集成应用处理器和调制解调处理器，其中，应用处理器主要处理操作系统、用户界面和应用程序等，调制解调处理器主要处理无线通信。可以理解的是，上述调制解调处理器也可以不集成到处理器 701 中。在一些实施例中，处理器 701 和存储器 702 可以在同一芯片上实现，在一些实施例中，它们也可以在独立的芯片上分别实现。

处理器 701 可以是通用处理器，例如中央处理器（CPU）、数字信号处理器、专用集成电路（Application Specific Integrated Circuit, ASIC）、现场可编程门阵列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，可以实现或者执行本发明实施例中公开的各方法、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。结合本发明实施例所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

存储器 702 作为一种非易失性计算机可读存储介质，可用于存储非易失性软件程序、非易失性计算机可执行程序以及模块。存储器 702 可以包括至少一种类型的存储介质，例如可以包括闪存、硬盘、多媒体卡、卡型存储器、随机访问存储器（Random Access Memory, RAM）、静态随机访问存储器（Static Random Access Memory, SRAM）、可编程只读存储器（Programmable Read Only Memory, PROM）、只读存储器（Read Only Memory, ROM）、带电可擦除可编程只读存储器（Electrically Erasable Programmable Read-Only Memory, EEPROM）、磁性存储器、磁盘、光盘等等。存储器 702 是能够用于携带或存储具有指令或数据结构形式的期望的程序代码并能够由计算机存取的任何其

他介质，但不限于此。本发明实施例中的存储器 702 还可以是电路或者其它任意能够实现存储功能的装置，用于存储程序指令和/或数据。

基于同一发明构思，本发明实施例提供了一种计算机可读介质，其存储有可由终端设备执行的计算机程序，当所述程序在终端设备上运行时，使得
5 所述终端设备执行区块链的权限控制方法的步骤。

本领域内的技术人员应明白，本发明的实施例可提供为方法、或计算机程序产品。因此，本发明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，本发明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（包括但不限于磁盘存储器、
10 CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、
15 嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图
25 一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了

基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

显然，本领域的技术人员可以对本发明进行各种改动和变型而不脱离本发明的精神和范围。这样，倘若本发明的这些修改和变型属于本发明权利要求及其等同技术的范围之内，则本发明也意图包含这些改动和变型在内。

5

权 利 要 求

1、一种区块链的权限控制方法，其特征在于，所述方法包括：

验证机构接收资源方发送的验证请求，所述验证请求包括授权通证 Token；

所述验证机构通过区块链查找与所述授权 Token 匹配的授权摘要；所述
5 区块链中存储有各授权方生成的授权 Token 的授权摘要；

所述验证机构在查找到与所述授权 Token 匹配的授权摘要后，向所述资源方发送验证通过消息。

2、如权利要求 1 所述的方法，其特征在于，所述方法还包括：

所述验证机构接收授权方发送的上传请求，所述上传请求中包括授权
10 Token；

所述验证机构验证所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括授权的资源，则将所述授权 Token 的授权摘要上传至所述区块链。

3、如权利要求 2 所述的方法，其特征在于，所述区块链中还存储有账户
15 信息，所述账户信息包括账户与属性的对应关系、属性与资源权限的对应关系；

所述验证机构验证所述授权 Token 中的授权方合法，包括：

根据所述账户与属性的对应关系，确定所述授权方的属性；

根据所述属性与资源权限的对应关系，确定所述授权方的属性中是否具有
20 所述授权 Token 中的授权内容的访问权限；

若有，则确定所述授权 Token 的授权方合法。

4、如权利要求 1 所述的方法，其特征在于，所述授权 Token 是授权机构生成的。

5、一种区块链的权限控制方法，其特征在于，所述方法包括：

资源方获取资源请求方发送的针对第一资源的访问请求；所述访问请求
25 包括授权凭证 Token；所述授权 Token 包括授权方及授权内容；

所述资源方确定所述访问请求满足访问所述第一资源的第一访问条件时，向所述资源请求方发送所述第一资源；所述第一访问条件为通过区块链查找到与所述授权 Token 匹配的授权摘要、所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括所述第一资源；所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

6、如权利要求 5 所述的方法，其特征在于，所述访问请求还包括授权方签名；

所述资源方确定所述访问请求满足访问所述第一资源的访问条件前，还包括：

所述资源方通过所述授权方签名确定所述授权 Token 为所述授权方发布的；所述授权方签名是所述授权方对生成的授权 Token 进行签名得到的。

7、如权利要求 6 所述的方法，其特征在于，所述资源方确定所述访问请求满足访问所述第一资源的第一访问条件之前，还包括：

所述资源方确定所述访问请求不满足访问所述第二访问条件；所述第二访问条件为所述资源请求方的账户是所述账户信息中记录的针对所述第一资源具有访问权限的账户。

8、如权利要求 5 所述的方法，其特征在于，所述授权内容包括授权的属性；所述授权 Token 中的授权内容包括所述第一资源为根据以下方式确定的：

根据所述授权的属性，在所述属性与资源权限的对应关系中，查找所述授权的属性对应的资源是否包括所述第一资源；

若确定包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

9、如权利要求 5 所述的方法，其特征在于，所述授权内容包括授权的资源；所述授权 Token 中的授权内容包括所述第一资源为根据以下方式确定的：

若确定所述授权内容中的授权的资源包括所述第一资源，则确定所述授权 Token 中的授权内容包括所述第一资源。

10、一种区块链的权限控制装置，其特征在于，所述装置包括：

收发单元，用于接收资源方发送的验证请求，所述验证请求包括授权 Token;

处理单元，用于通过区块链查找与所述授权 Token 匹配的授权摘要；所述区块链中存储有各授权方生成的授权 Token 的授权摘要；

5 所述收发单元，还用于在查找到与所述授权 Token 匹配的授权摘要后，向所述资源方发送验证通过消息。

11、一种区块链的权限控制装置，其特征在于，所述装置包括：

收发单元，用于获取资源请求方发送的针对第一资源的访问请求；所述访问请求包括授权凭证 Token；所述授权 Token 包括授权方及授权内容；

10 处理单元，用于确定所述访问请求满足访问所述第一资源的第一访问条件时，向所述资源请求方发送所述第一资源；所述第一访问条件为通过区块链查找到与所述授权 Token 匹配的授权摘要、所述授权 Token 中的授权方合法且所述授权 Token 中的授权内容包括所述第一资源；所述区块链中存储有各授权方生成的授权 Token 的授权摘要。

15 12、一种计算机设备，其特征在于，包括至少一个处理单元、以及至少一个存储单元，其中，所述存储单元存储有计算机程序，当所述程序被所述处理单元执行时，使得所述处理单元执行权利要求 1~4 或权利要求 5~9 任一权利要求所述方法的步骤。

20 13、一种计算机可读介质，其特征在于，其存储有可由终端设备执行的计算机程序，当所述程序在终端设备上运行时，使得所述终端设备执行权利要求 1~4 或权利要求 5~9 任一所述方法的步骤。

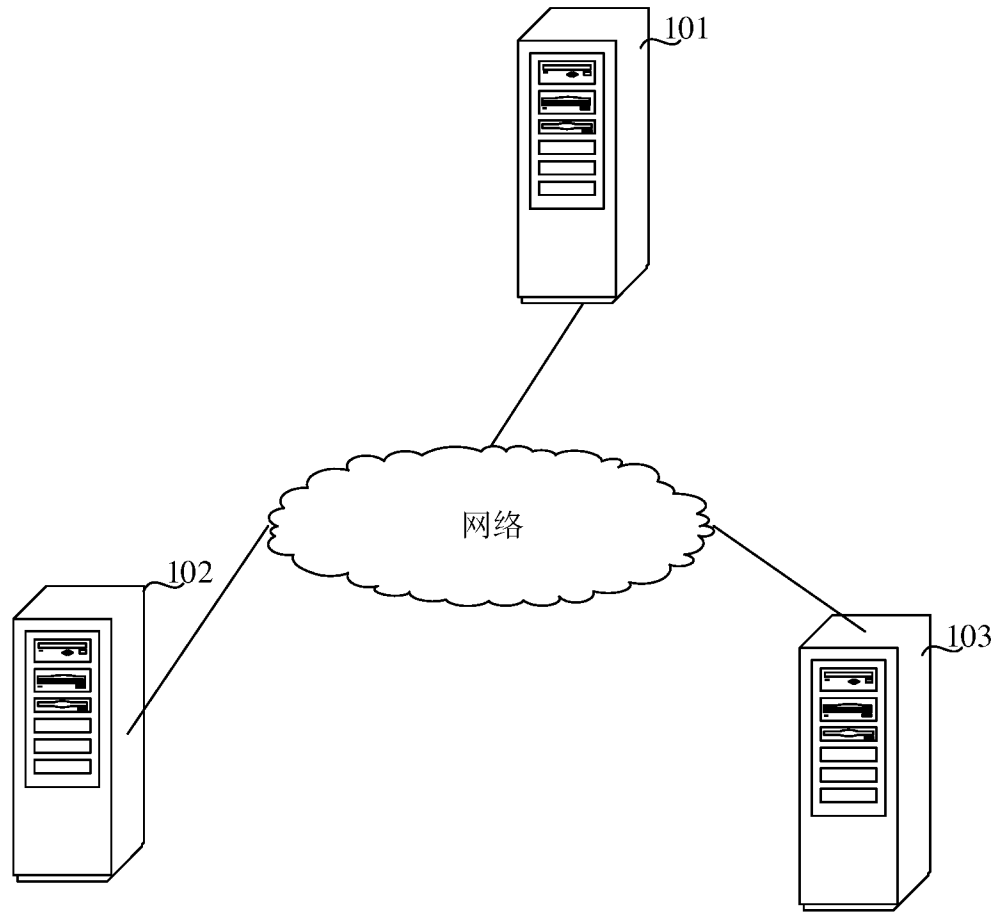


图 1

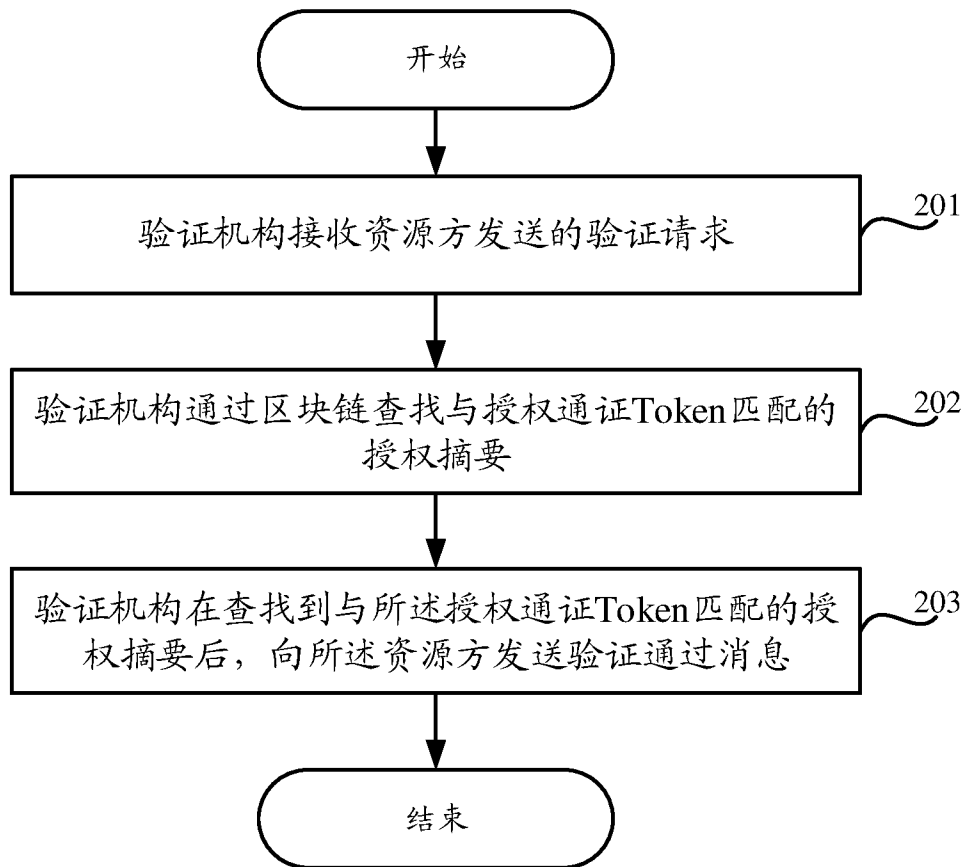


图 2

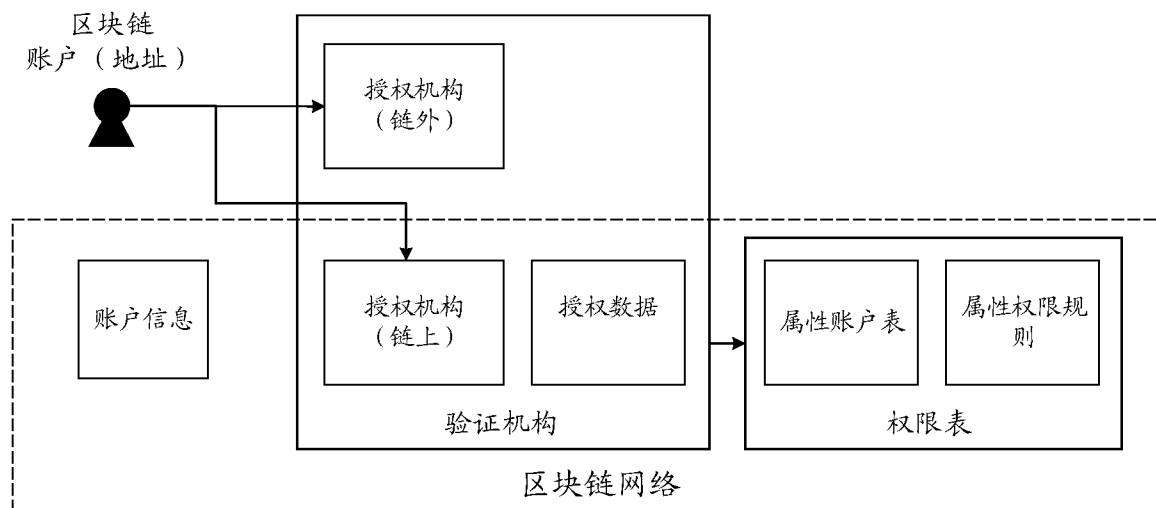


图 3

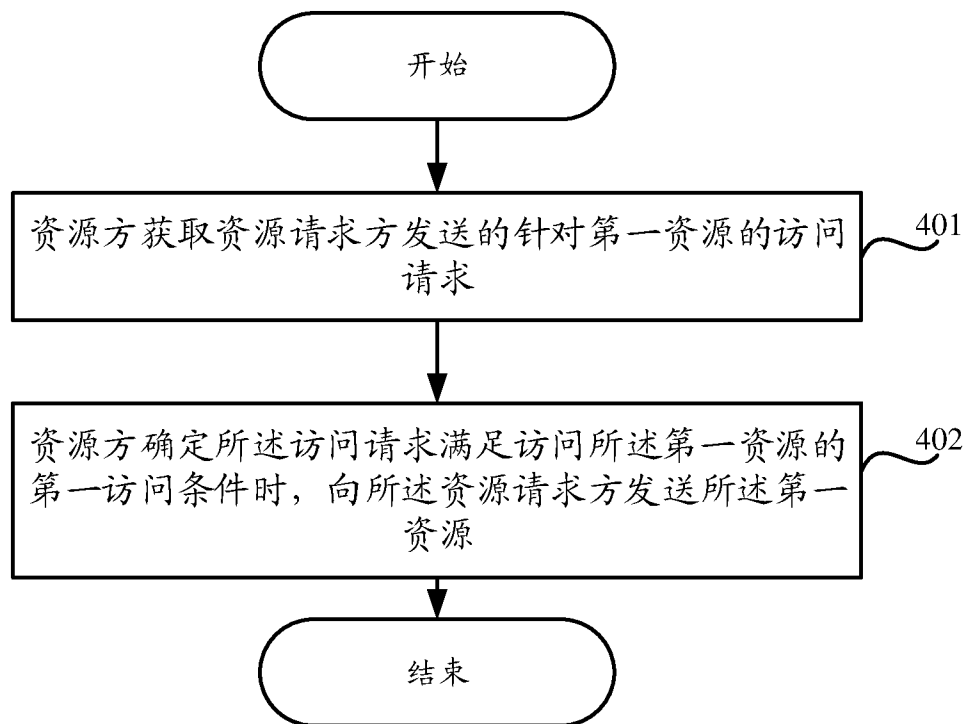


图 4

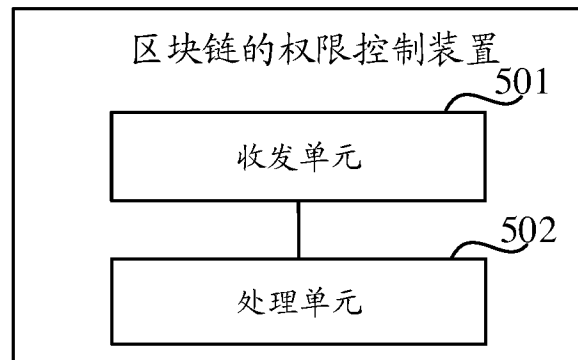


图 5

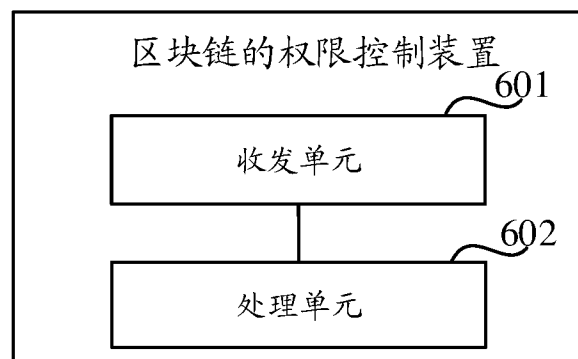


图 6

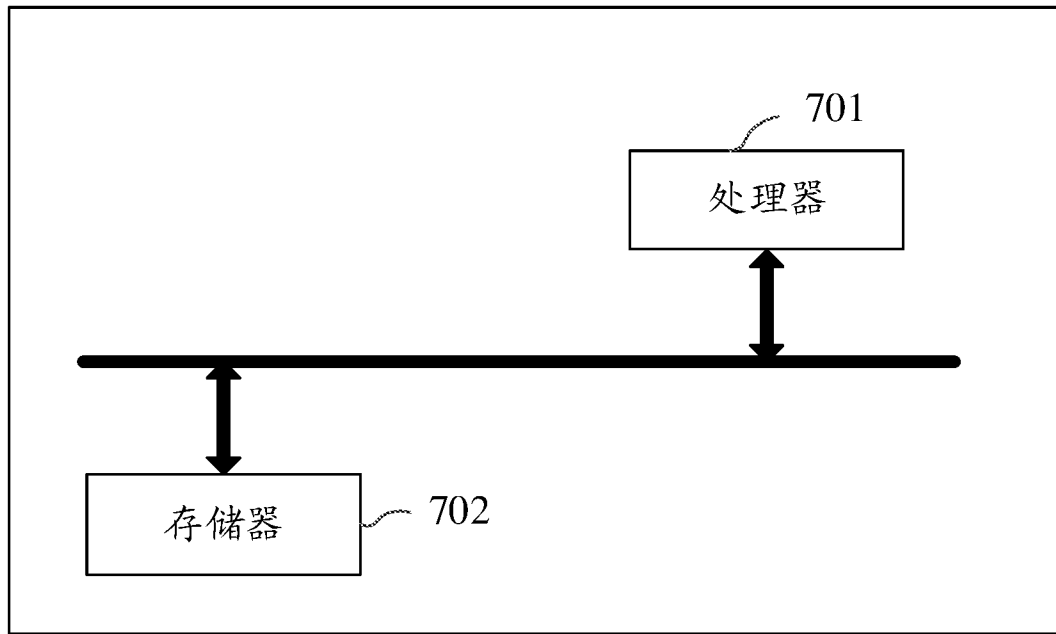


图 7

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/080519

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/30(2013.01)i; H04L 29/08(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)

G06F 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)

CNABS; CNTXT; CNKI; SIPOABS; DWPI; USTXT; WOTXT; EPTXT: 区块链, 记账本, 认证, 权限, 授权, 请求, 令牌, 单点登录, 摘要, 哈希, 相同, 查找, 访问, 匹配, 对比, 验证, 账户, block chain, authentication, popedom, authorization, token, sso, single sign on, hmac, hash, same, search, access, match, compare, validate, account

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110069908 A (SHENZHEN QIANHAI WEBANK CO., LTD.) 30 July 2019 (2019-07-30) claims 1-13, description, paragraphs [0065]-[0195]	1-13
Y	CN 108599936 A (XIDIAN UNIVERSITY) 28 September 2018 (2018-09-28) description, paragraphs [0044]-[0117]	1-13
Y	CN 108833363 A (WEN, Dan) 16 November 2018 (2018-11-16) description, paragraphs [0023]-[0034]	1-13
Y	CN 109242636 A (YINGYING HANGZHOU NETWORK TECHNOLOGY CO., LTD.) 18 January 2019 (2019-01-18) description, paragraphs [0078]-[0121]	1-13
A	CN 106209749 A (ALIBABA GROUP HOLDING LIMITED) 07 December 2016 (2016-12-07) entire document	1-13

☐ 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

23 April 2020

Date of mailing of the international search report

10 June 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Authorized officer

Facsimile No. (86-10)62019451

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/080519

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	110069908	A	30 July 2019	None	
CN	108599936	A	28 September 2018	None	
CN	108833363	A	16 November 2018	None	
CN	109242636	A	18 January 2019	None	
CN	106209749	A	07 December 2016	None	

国际检索报告

国际申请号

PCT/CN2020/080519

A. 主题的分类

G06F 21/30(2013.01)i; H04L 29/08(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)

G06F 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))

CNABS;CNTXT;CNKI;SIPOABS;DWPI;USTXT;WOTXT;EPTXT: 区块链, 记账本, 认证, 权限, 授权, 请求, 令牌, 单点登录, 摘要, 哈希, 相同, 查找, 访问, 匹配, 对比, 验证, 账户, block chain, authentication, popedom, authorization, token, sso, single sign on, hmac, hash, same, search, access, match, compare, validate, account

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
PX	CN 110069908 A (深圳前海微众银行股份有限公司) 2019年 7月 30日 (2019 - 07 - 30) 权利要求第1-13项, 说明书第[0065]-[0195]段	1-13
Y	CN 108599936 A (西安电子科技大学) 2018年 9月 28日 (2018 - 09 - 28) 说明书第[0044]-[0117]段	1-13
Y	CN 108833363 A (文丹) 2018年 11月 16日 (2018 - 11 - 16) 说明书第[0023]-[0034]段	1-13
Y	CN 109242636 A (盈盈杭州网络技术有限公司) 2019年 1月 18日 (2019 - 01 - 18) 说明书第[0078]-[0121]段	1-13
A	CN 106209749 A (阿里巴巴集团控股有限公司) 2016年 12月 7日 (2016 - 12 - 07) 全文	1-13

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2020年 4月 23日

国际检索报告邮寄日期

2020年 6月 10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

授权官员

刘凤娇

电话号码 (86-512) 88995746

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/080519

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	110069908	A	2019年 7月 30日	无	
CN	108599936	A	2018年 9月 28日	无	
CN	108833363	A	2018年 11月 16日	无	
CN	109242636	A	2019年 1月 18日	无	
CN	106209749	A	2016年 12月 7日	无	