

(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 1 日 (01.10.2020)



(10) 国际公布号
WO 2020/192743 A1

(51) 国际专利分类号:
G06F 21/46 (2013.01)

(21) 国际申请号: PCT/CN2020/081526

(22) 国际申请日: 2020 年 3 月 27 日 (27.03.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910245109.4 2019年3月28日 (28.03.2019) CN

(71) 申请人: 腾讯科技(深圳)有限公司 (TENCENT TECHNOLOGY (SHENZHEN) COMPANY LIMITED) [CN/CN]; 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。

(72) 发明人: 刘攀 (LIU, Pan); 中国广东省深圳市南山区高新区科技中一路腾讯大厦 35 层, Guangdong 518057 (CN)。

(74) 代理人: 深圳市深佳知识产权代理事务所(普通合伙) (SHENPAT INTELLECTUAL PROPERTY AGENCY); 中国广东省深圳市罗湖区南湖街道春风路庐山大厦 B 座 18C2、18D、18E、18E2, Guangdong 518001 (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, 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,

(54) Title: PERMISSION MANAGEMENT METHOD, PERMISSION VALIDATION METHOD AND RELATED APPARATUSES

(54) 发明名称: 权限管理方法、权限验证方法和相关装置

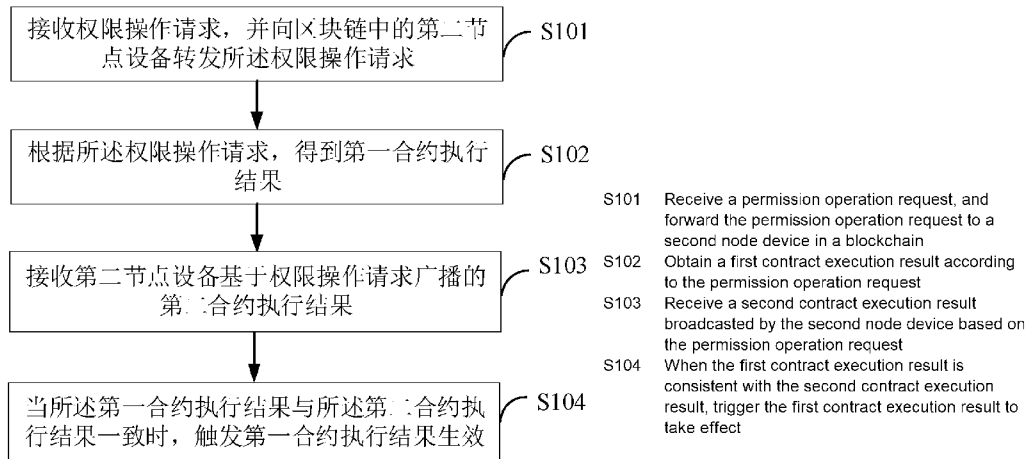


图 2

(57) Abstract: Disclosed in embodiments of the present application are a permission management method, a permission validation method and related apparatuses. According to the embodiments of the present application, the method comprises: receiving a permission operation request, and forwarding the permission operation request to a second node device in a blockchain, wherein the second node device is a node device in the blockchain other than the first node device; obtaining a first contract execution result according to the permission operation request; receiving a second contract execution result broadcasted by the second node device based on the permission operation request; and when the first contract execution result is consistent with the second contract execution result, triggering the first contract execution result to take effect. The solution implements decentralized permission management based on a blockchain permission management contract system, compares the own first contract execution result with the received second contract execution result, and triggers the first contract execution result to take effect only when the own contract execution result is consistent with the contract execution results of other node devices to reach a consensus, thereby improving data security.

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))。

(57) 摘要: 本申请实施例公开了一种权限管理方法、权限验证方法和相关装置; 本申请实施例可以接收权限操作请求, 并向区块链中的第二节点设备转发权限操作请求; 其中, 第二节点设备为区块链中除第一节点设备以外的节点设备; 根据权限操作请求, 得到第一合约执行结果; 接收第二节点设备基于权限操作请求广播的第二合约执行结果; 当第一合约执行结果与第二合约执行结果一致时, 触发第一合约执行结果生效。该方案基于区块链权限管理合约体系实现去中心化的权限管理, 将自身的第一合约执行结果与接收到的第二合约执行结果进行对比, 当自身合约执行结果与其他节点设备的合约执行结果一致实现达成共识, 才触发第一合约执行结果生效, 由此可以提升数据的安全性。

权限管理方法、权限验证方法和相关装置

本申请要求于 2019 年 03 月 28 日提交中国专利局、申请号为 201910245109.4、申请名称为“一种权限管理方法、装置和存储介质”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。

5

技术领域

本申请涉及计算机技术领域，具体涉及权限管理技术和权限验证技术。

背景技术

10 目前传统的用户权限管理方法都是中心化管理，针对不同的角色赋予不同的权限，管理权限过于集中。

发明内容

15 本申请实施例提供一种权限管理方法、权限验证方法和相关装置，可以提升数据的安全性。

一方面，本申请实施例提供一种权限管理方法，由区块链中的第一节点设备执行，包括：

接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；

20 根据所述权限操作请求，得到第一合约执行结果；

接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；

当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。

25 一方面，本申请实施例还提供一种权限管理装置，适用于区块链中的第一节点设备，包括：

第一接收单元，用于接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；

确定单元，用于根据所述权限操作请求，得到第一合约执行结果；

-2-

第二接收单元,用于接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果;

触发单元,用于当所述第一合约执行结果与所述第二合约执行结果一致时,触发第一合约执行结果生效。

5 一方面,本申请实施例提供了一种权限验证方法,由区块链中的第一节点设备执行,包括:

接收权限操作请求,并向所述区块链中的第二节点设备转发所述权限操作请求;其中,所述第二节点设备为所述区块链中除所述第一节点设备以外的节点设备;

10 根据所述权限操作请求,得到第一合约执行结果;

接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果;

当所述第一合约执行结果与所述第二合约执行结果一致时,确定用户权限验证通过。

15 一方面,本申请实施例提供了一种权限验证装置,集成在区块链中的第一节点设备中,包括:

第一接收单元,用于接收权限操作请求,并向所述区块链中的第二节点设备转发所述权限操作请求;其中,所述第二节点设备为所述区块链中除所述第一节点设备以外的节点设备;

确定单元,用于根据所述权限操作请求,得到第一合约执行结果;

20 第二接收单元,用于接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果;

触发单元,用于当所述第一合约执行结果与所述第二合约执行结果一致时,确定用户权限验证通过。

25 一方面,本申请实施例提供了一种计算机设备,所述计算机设备包括:处理器、通信接口、存储器和通信总线;

其中,所述处理器、所述通信接口和所述存储器通过所述通信总线完成相互间的通信;所述通信接口为通信模块的接口;

所述存储器,用于存储程序代码,并将所述程序代码传输给所述处理器;

所述处理器,用于调用存储器中程序代码的指令执行权限管理方法或者权

限验证方法。

一方面，本申请实施例提供了一种存储介质，所述存储介质用于存储计算机程序，所述计算机程序用于执行上述权限管理方法或者权限验证方法。

5 一方面，本申请实施例提供了一种包括指令的计算机程序产品，当其在计算机上运行时，使得所述计算机执行上述权限管理方法或者权限验证方法。

本申请实施例提供了由区块链中第一节点设备执行的权限管理方法、权限验证方法和相关装置，具体地，接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；根据所述权限操作请求，得到第一合约执行结果；接收
10 所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。该方案可以基于区块链权限管理合约体系实现去中心化的权限管理，将自身的
15 第一合约执行结果与接收到的第二合约执行结果进行对比，当自身合约执行结果与其他节点设备的合约执行结果一致实现达成共识，才触发第一合约执行结果生效，由此提升了权限和数据的安全性。

附图说明

为了更清楚地说明本申请实施例或现有技术中的技术方案，下面将对实施例或现有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
20 中的附图仅仅是本申请的实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图获得其他的附图。

图1是本申请实施例提供的权限管理方法的场景示意图；

图2是本申请实施例提供的权限管理方法的流程图；

图3a是本申请实施例提供的得到第一合约执行结果的方法流程图；

25 图3b是本申请实施例提供的映射关系示意图；

图3c是本申请实施例提供的权限分配的流程示意图；

图3d是本申请实施例提供的角色分配的流程示意图；

图4是本申请实施例提供的权限移交的流程示意图；

图5是本申请实施例提供的委托代理角色的流程示意图；

图6是本申请实施例提供的撤回委托角色的流程示意图;

图7是本申请实施例提供的用户功能权限验证的流程示意图;

图8是本申请实施例提供的智能合约系统的架构示意图;

图9a是本申请实施例提供的权限管理装置的结构示意图;

5 图9b是本申请实施例提供的权限管理装置的一结构示意图;

图9c是本申请实施例提供的权限管理装置的一结构示意图;

图10是本申请实施例提供的数据处理设备的结构示意图。

具体实施方式

10 下面将结合本申请实施例中的附图,对本申请实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本申请一部分实施例,而不是全部的实施例。基于本申请中的实施例,本领域技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本申请保护的范围。

15 在对本申请实施例进行详细地解释说明之前,先对本申请实施例涉及到的一些名词进行解释说明。

权限管理:区块链系统中与权限相关的管理操作,比如,包括区块链系统中的用户权限操作、用户角色操作等等。譬如,权限验证、权限转移、权限委托、角色分配、权限分配等等操作。

20 区块链:区块链技术脱胎于比特币技术,是比特币的底层技术,其是去中心化的分布式账本数据库。区块链本身是一串使用密码学算法相关联产生的数据块(即区块),每一个数据块中包含了多次区块链网络交易有效确认的信息。正是基于此,所以无法通过篡改区块上的数据来进行作弊,能够确保任何区块上的数据均是公开透明的,确保了数据的安全性。

25 区块链可以分为公有链、私有链、联盟链。其中,联盟链则介于公有链和私有链之间,由若干组织一起合作维护一条区块链,该区块链的使用必须是有权限的管理,相关信息会得到保护,典型如金融组织。

总结来说,区块链是由节点参与的分布式数据库系统,或者,也可称之为一个基于点对点(Peer-to-Peer, P2P)网络的分布式公共账本,其特点是不可更改、不可伪造,还可以将其理解为账簿系统。

区块链的节点设备：参与构建区块链的节点设备，可以为权限管理的执行主体、节点设备之间交互可以实现交易等业务等。该节点设备存储有相关区块数据，比如，权限管理合约、区块链合约账本等等。

接下将介绍本申请实施例提供的一种权限管理方法、装置和存储介质。其中，该权限管理装置可以集成在区块链的节点设备中，该节点设备可以为服务器等网络设备。

参考图1，本申请实施例提供了基于区块链的权限管理系统，该系统可以实现权限管理和其他业务，比如电子票据管理等业务。该系统可以包括多个节点设备10，其中，多个节点设备之间通过网络连接。

每个节点设备10可以用于管理系统中的用户权限，也可以作为区块链的记账节点，用于存储交易过程中的交易信息，并定时进行更新，使得实施环境中的其他节点可以共享交易信息，从而使得各个节点可以为交易信息提供一致性证明，提高了交易信息的安全性，如，当一次权限操作过程完成时，该记账节点可以根据各个节点的节点标识(如网络地址)将交易信息共享至各个节点的区块链上。

在权限管理场景中，节点设备可以接收请求设备如用户设备如手机11或者电脑12、其他节点设备10发送的权限操作请求，并向区块链中的第二节点设备10转发权限操作请求；其中，第二节点设备为区块链中除第一节点设备10以外的节点设备10；根据权限操作请求确定需要操作的权限操作类型；基于权限管理合约执行权限操作类型对应的校验逻辑；当校验通过时，执行权限操作类型对应的权限操作，得到第一合约执行结果；接收第二节点设备10基于权限操作请求广播的第二合约执行结果；当第一合约执行结果与第二合约执行结果一致时，触发第一合约执行结果生效。

以下分别进行详细说明。需说明的是，以下实施例的描述顺序不作为对实施例优选顺序的限定。

本实施例将从权限管理装置的角度进行描述，该权限管理装置可以集成在区块链的节点设备中，该节点设备可以为数据处理设备等网络设备，该数据处理设备可以是终端设备。其中，终端设备例如可以是智能手机、计算机、个人数字助理(Personal Digital Assistant，简称PDA)、平板电脑、销售终端(Point

of Sales, 简称 POS)、车载电脑等设备。该数据处理设备可以是服务器, 服务器可以是独立的服务器, 也可以是集群中的服务器。

本申请实施例提供的一种权限管理方法, 该方法可以由区块链中的第一节点设备的处理器执行, 如图2所示, 该权限管理方法的具体流程可以如下:

5 S101、接收权限操作请求, 并向区块链中的第二节点设备转发权限操作请求。

其中, 权限操作请求可以携带请求用户标识、权限操作信息等信息, 比如, 权限操作信息可以包括权限操作类型。

10 该权限操作请求可以由区块链系统中的请求设备发送, 该请求设备可以包括系统内的终端或者其他节点设备如服务器等。

其中, 第二节点设备为区块链中除第一节点设备以外的节点设备。本申请实施例中, 区块链的某个节点设备接收到权限操作请求时, 还需要将请求转发如广播给区块链的其他节点设备, 以便其他设备进行相应的权限操作执行及其校验。

15 例如, 当需要进行权限操作时, 请求用户可以通过终端向第一节点设备发送权限操作请求, 此时, 第一节点设备可以对该请求进行接收, 并向第二节点设备转发该权限操作请求。

20 在一实施例中, 该权限操作请求可以由节点设备自己触发, 比如, 当接收到合约交易请求时, 可以根据交易请求触发权限操作请求, 此时, 节点设备可以对该权限操作请求接收。在一实施例中, 权限操作请求还可以包括交易请求等。

S102、根据权限操作请求, 得到第一合约执行结果。

25 需要说明, 本申请实施例不限定根据权限操作要求得到第一合约执行结果的方式。可以根据实际情形或不同需求, 选择适合的方式得到第一合约执行结果。在一种可能的实现方式中, 参见图3a, 该图示出了本申请实施例提供的得到第一合约执行结果的方法流程图, 该S102的方法可以包括:

S1011、根据权限操作请求, 确定需要操作的权限操作类型。

其中, 权限操作类型可以根据实际需求划分, 比如, 权限操作类型可以包括: 权限分配(如给用户或者用户角色分配权限等)、权限转移、权限代理、

权限验证等等；在一实施例中，权限操作类型还可以包括用户角色操作，比如，角色分配、角色代理（如委托其他用户代理角色）、撤回代理角色（如撤回委托给其他用户代理的角色等等）。

可以理解的是：权限操作类型的划分不限于上述介绍的权限类型划分，还可以为他权限类型划分，比如，划分为管理员权限操作、普通用户权限操作等等。又比如，还可以基于权限等级来划分，可以划分为低等权限操作、中等权限操作、高等权限操作。又比如，还可以基于权限操作的安全性来划分，可以划分为正常权限操作、高危权限操作等等。

本申请实施例中确定权限类型的方式可以有多种，比如，在一实施例中，权限操作请求可以携带权限操作信息（如权限操作类型标识），此时，可以根据权限操作信息确定权限类型。又比如，还可以权限操作请求携带权限操作内容时，可以对权限操作内容进行识别，以确定权限类型。

S1012、基于权限管理合约执行权限操作类型对应的校验逻辑。

其中，权限管理合约是一套以数字形式定义、传播、验证或执行的权限管理约定，包括合约参与方可以在上面执行这些约定的协议。智能合约允许在没有第三方的情况下进行可信交易，这些交易可追踪且不可逆转。

本申请实施例中，区块链中每个节点设备均部署有或存储有权限管理合约，以实现权限管理合约的非法篡改。其中，权限管理合约存储方式有多种，比如，在一实施例中，可以采用区块链方式存储以取代传统的关系数据库来存储，这样提高了权限防篡改的能力。此时，权限管理合约对应的数据可以保存区块链合约账本中。该区块链合约账本为一个分布式账本，可以包括记录权限管理合约的相关数据，并可以保证数据不被篡改或丢失。

在一实施例中，权限管理合约数据可以包括用户、角色和权限之间的映射关系，比如，参考图3b所示，为用户身份证标识号(Identity document, ID)、角色、权限映射图。用户ID可以一对多个角色，而一个角色可以对应多个权限。不同的角色可以有相同的权限。

实际应用中，权限管理合约可以由区块链满足条件的合约交易等业务触发，并由区块链虚拟机执行，该区块链虚拟机由节点设备来实现。

本申请实施例中，权限管理合约还可以包括权限操作类型对应的校验逻辑。

辑,该校验逻辑可以根据实际需求配置。其中,每一种权限操作类型可以对应于一种校验逻辑。比如,当前如果权限操作类型为a,那么可以执行权限类型a对应的校验逻辑a'。

具体地,为了提升数据的安全性,权限操作类型对应的校验逻辑可以包括:

5 对请求用户的操作合法性验证、以及权限操作类型对应的操作对象的验证。比如,针对S1012、基于权限管理合约执行权限操作类型对应的校验逻辑,可以包括:

(1)、基于权限管理合约对请求发起用户的操作合法性进行验证。

10 其中,请求发起用户的操作合法的验证可以根据实际需求设定,比如,在一实施例中,可以包括验证请求发起用户的身份是否合法、是否具有相应的功能权限等等。

15 比如,“基于权限管理合约对请求发起用户的操作合法性进行验证”,可以包括:基于所述权限管理合约对操作参数进行验证;当验证通过时,确定请求发起用户的操作合法,否则操作不合法。其中,操作参数包括调用参数、请求发起用户的功能权限和签名中的一种或多种组合。譬如,可以包括如下方式:

(1.1)、基于权限管理合约对请求发起用户的功能权限和签名进行验证;当请求发起用户的功能权限和签名验证通过时,确定请求发起用户的操作合法;否则确定请求用户的操作不合法。

20 例如,可以先对请求发起用户的功能权限进行验证,当功能权限验证通过时,对请求发起用户的签名进行验证,当签名验证通过时,确定请求发起用户的操作合法。

25 其中,功能权限的验证包括验证请求发起用户是否具有执行权限操作类型对应的操作的功能权限;比如,当权限操作类型为权限分配时,那么需要验证请求发起用户是否具有分配权限的功能权限;当权限操作类别为角色分配,那么需要验证请求发起用户是否具有角色分配的功能权限;又比如,当权限操作类型为超级权限转移时,那么需要验证请求发起用户是否具有管理员权限等。

在一实施例中,基于权限管理合约对请求发起用户的功能权限进行验证的过程可以如下:

基于权限管理合约从区块链合约账本中获取请求发起用户的角色令牌集

合;

当角色令牌集合中角色令牌对应的功能权限包含权限操作类型所需的目标功能权限时, 确定功能权限验证通过;

5 当角色令牌集合中所有角色令牌对应的功能权限未包含权限操作类型所需的目标功能权限时, 从区块链合约账本中获取请求发起用户所代理的代理角色令牌集合;

当代理角色令牌集合中代理角色令牌对应的功能权限包含权限操作类型所需的目标功能权限时, 确定功能权限验证通过; 否则功能权限验证不通过。

10 (1.2)、基于权限管理合约对请求发起用户的签名进行验证; 当请求发起用户的签名验证通过时, 确定请求发起用户的操作合法; 否则确定请求用户的操作不合法。

其中, 请求发起用户的签名为区块链中的数字签名, 保证数据在整个系统中不可篡改, 并保证交易双方的身份真实可靠。数字签名使用了非对称加密技术和数字摘要技术, 保证了数据在传输过程中的完整性、发送者身份真实不可假冒。非对称加密技术会产生一个公钥 (Publickey) 和一个私钥 (Privatekey), 15 公钥和私钥是一对, 私钥保存在所有者手中, 需要对外人保密不可让外人知道, 公钥可以向其他信息接收方公开。如果用私钥对数据加密只有公钥才能解密, 相反公钥加密过的数据, 只有对应的私钥才能解密。

20 数字摘要是利用哈希函数把任意长度的信息变成固定长度的信息, 哈希函数是单向生成体制, 通过生成的哈希值不可逆向生成输入值。另外哈希函数是一种压缩映射, 输出是固定长度的信息。

(1.3)、基于权限管理合约对调用参数和请求发起用户的签名进行验证; 基于权限管理合约对调用参数和请求发起用户的签名进行验证; 当调用参数和签名验证通过时, 确定请求发起用户的操作合法; 否则确定请求用户的操作不 25 合法。

其中, 调用参数可以包括执行权限管理合约时所需调用的参数, 比如, 调用的接口参数等。具体校验哪种参数可以根据实际需求设定。

(2)、当请求发起用户的操作合法时, 对权限操作类型对应的操作对象的权限信息进行验证。

其中，操作对象为权限操作类型对应的权限操作所针对的目标，该目标可以包括用户、角色等。比如，当权限操作类型为权限分配时，操作对象就为待分配权限的用户，又比如，当权限操作类型为角色分配时，操作对象可以为待分配角色用户等等。

- 5 其中，操作对象的权限信息验证可以与权限操作类型相对应，由权限操作类型来决定操作对象的权限信息验证的具体逻辑。下面将介绍各权限类型对应的权限信息验证：

(2.1)、权限操作类型包括权限分配：

比如，管理员给用户的角色分配权限等。

- 10 其中，操作对象可以包括待分配权限的角色，即待分配角色。

操作对象的权限信息验证包括：当请求发起用户的操作合法时，从区块链合约账本中获取待分配角色对应的已分配功能权限集合，区块链合约账本包括用户、角色和已分配功能权限之间的映射关系；

当已分配功能权限集合不包含待分配权限时，确定权限信息验证通过。

- 15 也就是说，当需要分配权限时，需验证待分配用户是否已经具有待分配功能权限，如果没有确定待分配用户的权限信息验证通过，允许给该用户分配权限，否则不通过，拒绝给该用户分配权限。

(2.2)、权限操作类型包括：角色分配；

比如，管理员给用户分配角色。

- 20 其中，操作对象可以包括待分配角色的用户，即待分配用户。

操作对象的权限信息校验可以包括：当请求发起用户的操作合法时，基于权限管理合约给待分配用户分配一个角色令牌；

从区块链合约账本中获取待分配用户对应的角色令牌集合；

当角色令牌集合不包含待分配的角色令牌时，确定权限信息验证通过。

- 25 也就是说，在给用户分配角色时，需要校验待分配用户的是否已经具有该角色，如果没有确定待分配用户的权限信息验证通过，允许给该用户分配角色，否则不通过，拒绝给该用户分配角色。

(2.3)、权限操作类型包括：权限转移；

比如，管理员（Admin）将超级权限移交给新的管理员。

其中，操作对象可以包括将权限转移到的用户即待转移用户。

当请求发起用户的操作合法时，对待转移用户的身份合法性进行检查；

当待转移用户的身份合法时，确定权限信息验证通过。

也就是说，在转移权限时，需要校验待转移用户的身份是否合法，若合法

5 确定待转移用户的权限信息验证通过，允许转移权限给该用户，否则不通过，拒绝转移权限。

(2.4)、权限操作类型包括：角色委托代理；

比如，用户委托其他用户临时或者在一定期限代理角色。

其中，操作对象可以包括需要被委托代理角色的用户，即待委托用户。

10 权限信息校验可以包括：当请求发起用户的操作合法时，对待委托用户的身份合法性进行检查；当待委托用户的身份合法时，基于待委托角色对请求发起用户和待委托用户的角色进行检查；当检查到请求发起用户具有待委托角色、待委托用户不具有待委托角色时，从区块链合约账本中获取待委托用户的已代理角色；当已代理角色不包含待委托角色时，确定权限信息验证通过。

15 具体地，可以检查请求发起用户是否具有待委托角色；若请求发起用户有待委托角色，检查待委托用户是否具有待委托角色；若待委托用户不具有待委托角色，从区块链合约账本中查询待委托用户的已经代理角色状态；基于已经代理角色状态确定待委托用户是否已代理待委托角色；若未已代理待委托角色，则确定权限信息验证通过。

20 也就是说，在委托其他用户代理角色时，需要校验委托用户是否具有该角色、待委托用户是否不具有该角色，若委托用户有，待委托用户没有，则确定权限信息验证通过，允许角色委托，否则拒绝角色委托。

(2.5)、权限操作类型包括：角色委托撤回；

比如，用户撤回委托给其他用户代理的角色。

25 其中，操作对象可以包括需要被撤回委托代理角色的用户，即代理用户。

权限信息验证可以包括：当请求发起用户的操作合法时，检查请求发起用户是否有待撤回角色令牌；若有待撤回的角色令牌，从区块链合约账本中获取代理用户的代理角色令牌集合；当代理角色令牌集合包含待撤回角色令牌时，确定权限信息验证通过。

-12-

也就是说,当请求发起用户具有待撤回角色、代理用户存在该待撤回角色时,确定验证通过,允许撤回角色,否则拒绝撤回角色。

(2.6)、权限操作类型包括:权限验证;

比如,系统对某个用户的功能权限验证,如请求发起用户的功能权限验证。

5 其中,操作对象可以包括待验证功能权限的用户,即待验证用户,比如请求发起用户。

权限信息验证可以包括:基于权限管理合约从区块链合约账本中获取待验证用户的角色令牌集合;

10 当角色令牌集合中角色令牌对应的功能权限包含权限操作类型所需的目标功能权限时,确定功能权限验证通过;

当角色令牌集合中角色令牌对应的功能权限未包含权限操作类型所需的目标功能权限时,从区块链合约账本中获取待验证用户所代理的代理角色令牌集合;

15 当代理角色令牌集合中代理角色令牌对应的功能权限包含权限操作类型所需的目标功能权限时,确定功能权限验证通过;否则功能权限验证不通过。

以上介绍了几种权限类型的校验逻辑,实际应用中不仅限于上述的校验逻辑。

20 本申请实施例中,第一节点设备在通过上述过程得到第一校验结果后,可以向区块链中第二节点设备广播该第一校验结果。比如,可以对校验结果签名后,即添加签名后广播。其中,第一校验结果可以包括校验通过、或者不通过等内容。

S1013、当校验通过时,执行权限操作类型对应的权限操作,得到第一合约执行结果。

25 其中,第一合约执行结果可以包括权限操作结果,比如,权限操作成功、权限操作失败等结果等,在一实施例中,第一合约执行结果还可以包括权限操作带来的变化结果数据等,比如,在权限分配时,可以包括已添加功能权限的权限集合,在角色分配时可以包括已添加角色的角色令牌集合等等。

对于节点设备来说其执行校验逻辑、权限操作等相关权限操作均是在权限管理合约下执行的,因此,在执行权限操作时,可以认为合约结束执行,此时

所产生的结果可以成为合约执行结果。

本申请实施例可以当校验通过时，先执行权限操作类型对应的权限操作，如权限分配、验证、角色分配等等。此时，合约执行结果并未生效，比如，可以将第一合约执行结果写入到缓存如合约缓存中。

5 比如，权限类型为权限分配的情况下，当校验通过时，可以将待分配权限添加到待分配角色对应的已分配功能权限集合中。

又比如，权限类型为角色分配的情况下，当校验通过时，可以将待分配的角色令牌添加到待分配用户对应的角色令牌集合中。

10 又比如，权限类型为权限转移的情况下，当校验通过时，将待转移权限的用户更新为待转移用户。

又比如，权限类型为角色委托代理的情况下，当校验通过时，将待委托角色添加为待委托角色的已代理角色。

在一实施例中，当已代理角色不包含待委托角色时，可以更新待委托角色的代理信息，如登记、有效期等。

15 又比如，权限类型为角色委托撤回的情况下，当校验通过时，从代理用户的代理角色令牌集合中撤回待撤回的角色令牌。

在一实施例中，当校验不通过时，可以返回权限操作失败的合约执行结果，或者返回拒绝服务的合约执行结果等等，具体可以根据实际需求设定。

S103、接收第二节点设备基于权限操作请求广播的第二合约执行结果。

20 其中，区块链中其他节点设备即第二节点设备在接收到广播的权限操作请求之后，可以在相同的权限管理合约下执行与第一节点设备相同或类似的校验和权限操作过程，比如，确定权限操作类型、执行权限操作类型对应的校验逻辑，在校验通过时，得到相应的合约执行结果（如权限操作成功、失败、允许权限操作、拒绝权限操作等等），第二节点设备得到的合约执行结果称为第二
25 合约执行结果，在得到第二合约执行结果后可以向区块链中除自身以外的节点设备广播该合约执行结果。

本申请实施例中，第二合约执行结果的数量与第二节点设备相同，比如，当存在多个第二节点设备时，可以接收到多个第二合约执行结果。

S104、当第一合约执行结果与第二合约执行结果一致时，触发第一合约执

行结果生效。

区块链中节点设备在接收到其他节点设备广播的第二合约执行结果后，可以将自身的第一合约执行结果与接收到的第二合约执行结果进行对比，当自己的合约执行结果与其他节点设备的合约执行结果一致即达成共识，且都为权限操作成功时，可以触发第一合约执行结果生效。

其中，触发第一合约执行结果生效指的是：使得执行权限操作类型对应的权限操作有效，比如，可以基于第一合约执行结果更新区块链合约账本，譬如，第一合约执行结果包含权限操作结果数据或者权限操作带来的变化数据时，可以将权限操作结果数据或者变化数据写入区块链合约账本中，使得第一合约执行结果生效。

在一实施例中，可以执行权限操作类型对应的权限操作，并将第一合约执行结果数据写入缓存如合约缓存中；当第一合约执行结果与第二合约执行一致时，基于缓存中的数据更新区块链合约账本，比如，将合约缓存数据写入区块链合约账本，从而使得第一合约执行结果生效。

比如，权限类型为权限分配的情况下，当本端节点设备（如第一节节点设备）校验通过时，将待分配权限添加到待分配角色对应的已分配功能权限集合，得到权限分配结果数据，并将可以权限分配结果数据写入合约缓存；当本端节点设备和其他节点设备（如第二节节点设备）的合约执行结果达成共识，且时，将合约缓存数据写入区块链合约账本，以更新账本、从而触发权限分配操作生效。

又比如，权限类型为角色分配的情况下，本端节点设备（如第一节节点设备）校验通过时，将待分配的角色令牌添加到待分配用户对应的角色令牌集合中，得到角色分配结果数据，并将可以角色分配结果数据写入合约缓存；当本端节点设备和其他节点设备（如第二节节点设备）的合约执行结果达成共识，且时，将合约缓存数据写入区块链合约账本，以更新账本、从而触发角色分配操作生效。

又比如，权限类型为权限转移的情况下，本端节点设备（如第一节节点设备）校验通过时，将待转移权限的用户更新为待转移用户，得到权限转移结果数据，并可以将权限转移结果数据写入合约缓存；当本端节点设备和其他节点设备（如第二节节点设备）的合约执行结果达成共识，且时，将合约缓存数据写入区

块链合约账本,以更新账本、从而触发权限转移操作生效。

又比如,权限类型为角色委托代理的情况下,本端节点设备(如第一节点设备)校验通过时,将待委托角色添加为待委托角色的已代理角色,得到角色委托代理结果数据,并将可以角色委托代理结果数据,写入合约缓存;当本端节点设备和其他节点设备(如第二节点设备)的合约执行结果达成共识,且时,将合约缓存数据写入区块链合约账本,以更新账本、从而触发角色委托代理操作生效。

在一实施例中,当已代理角色不包含待委托角色时,可以更新待委托角色的代理信息,如登记、有效期等。

又比如,权限类型为角色委托撤回的情况下,本端节点设备(如第一节点设备)校验通过时,从代理用户的代理角色令牌集合中撤回待撤回的角色令牌,得到角色委托撤回结果数据,并将可以角色委托撤回结果数据,写入合约缓存;当本端节点设备和其他节点设备(如第二节点设备)的合约执行结果达成共识,且时,将合约缓存数据写入区块链合约账本,以更新账本、从而触发角色委托撤回操作生效。

本申请实施例提供的权限管理方法可以适应于各种场景,比如,如区块链电子发票、区块链供应链金融、互联网存证等。

由上可知,本申请实施例提供的权限管理方案可以基于区块链权限管理合约体系实现去中心化的权限管理,因此,可以提升权限和数据的安全性,如提升区块链(如联盟链)中数据和权限的安全性。

在上述实施例描述的基础上,下面将介绍几种常见的权限管理场景:

在一实施例提供的一种权限分配方法,该方法可以由区块链中第一节点设备执行,参考图3c,具体流程如下:

S201、第一节点设备接收交易发起方发起的合约交易请求,并将合约交易请求广播给第二节点设备。

其中,用户如管理员可以通过交易触发给用户的角色分配权限,比如,通过终端向区块链的第一节点设备发送合约交易请求。

S202、第一节点设备根据合约交易请求确定权限操作类型为权限分配。

比如,合约交易请求可以携带权限操作类型,此时,可以直接基于请求确

定权限操作类型。

S203、第一节点设备根据权限管理合约检查交易发起者是否具有角色分配权限，若是，则执行S204，若否，则执行S208。

比如，区块链记账节点收到交易后，触发虚拟机调用权限管理合约。

5 如果具有角色分配权限，则合约执行结束，返回操作成功的合约执行结果。

S204、第一节点设备验证校验发起者的签名是否合法，若合法，则执行S205，若否，则执行S208。

具体地，当签名不合法则返回拒绝服务的合约执行结果。

10 S205、第一节点设备查询区块链合约账本获取待分配角色对应的已分配功能权限集合。

S206、第一节点设备检查已分配功能权限集合是否存在待分配权限，若存在执行，若不存在，执行S207。

具体地，当不存在时，合约执行结束，返回拒绝服务的合约执行结果。

15 S207、第一节点设备将待分配权限添加到待分配角色的已分配功能权限集合中，并将权限操作结果数据写入合约缓存。

在一实施例中，执行完权限操作后可以返回操作成功的结合约执行结果。

S208、第一节点设备将结果签名后在区块链中广播给第二节点设备，接收到第二节点设备广播的结果。

20 其中，结果可以包括合约执行结果（如权限操作成功、失败等）、或者权限分配的校验结果（如校验通过等）。比如，可以将本端的合约执行结果签名后广播给区块链中其他的节点设备。

S209、当第一节点设备的结果与第二节点设备的结果一致时，第一节点设备将合约缓存数据写入区块链合约账本。

25 比如，区块链记账节点对结果签名后广播，达成共识后，将合约缓存数据写入合约账本。

在一实施例提供的一种角色分配方法，该方法可以由区块链中第一节点设备执行，参考图3d，具体流程如下：

S301、第一节点设备接收交易发起方发起的合约交易请求，并将合约交易请求广播给第二节点设备。

其中，用户如管理员可以通过交易触发给用户分配角色，比如，通过终端向区块链的第一节点设备发送合约交易请求。

S302、第一节点设备根据合约交易请求确定权限操作类型为角色分配。

比如，合约交易请求可以携带权限操作类型，此时，可以直接基于请求确定权限操作类型。

S303、第一节点设备根据权限管理合约检查交易发起者是否具有管理员权限，若是，则执行S304，若否，则执行S309。

比如，区块链记账节点收到交易后，触发虚拟机调用权限管理合约。一般情况下管理员权限最大，包含角色分配等权限。

10 如果不具有管理员权限，则合约执行结束，返回拒绝服务的结果，即校验失败。

S304、第一节点设备验证校验发起者的签名是否合法，若合法，则执行S205，若否，则执行S309。

具体地，当签名不合法则返回拒绝服务的合约执行结果。

15 S305、第一节点设备基于权限管理合约给待分配用户分配一个角色令牌。

S306、第一节点设备查询区块链合约账本中获取待分配用户对应的角色令牌集合。

S307、第一节点设备检查角色令牌集合是否包含待分配的角色令牌，若不包含执行S308，若包含执行S309。

20 S308、第一节点设备将待分配的角色令牌添加到待分配用户对应的角色令牌集合中，并将角色分配结果数据写入合约缓存。

在一实施例中，执行完权限操作后可以返回操作成功的合约执行结果。

S309、第一节点设备将结果签名后在区块链中广播给第二节点设备，接收到第二节点设备广播的结果。

25 其中，结果可以包括合约执行结果（如权限操作成功、失败等）、或者权限分配的校验结果（如校验通过等）。比如，可以将本端的合约执行结果签名后广播给区块链中其他的节点设备。

S310、当第一节点设备的结果与第二节点设备的结果一致时，第一节点设备将合约缓存数据写入区块链合约账本。

比如，区块链记账节点对结果签名后广播，达成共识后，将合约缓存写入合约账本。

在一实施例提供的一种权限转移方法，该方法可以由区块链中第一节点设备执行，参考图4，具体流程如下：

5 S401、第一节点设备接收交易发起方发起的合约交易请求，并将合约交易请求广播给第二节点设备。

其中，用户如管理员可以通过交易触发给将管理员的权限转移给新管理员，比如，通过终端向区块链的第一节点设备发送合约交易请求。

S402、第一节点设备根据合约交易请求确定权限操作类型为权限转移。

10 比如，合约交易请求可以携带权限操作类型，此时，可以直接基于请求确定权限操作类型。

S403、第一节点设备根据权限管理合约检查交易发起者是否具有管理员权限，若是，则执行S404，若否，则执行S407。

15 比如，区块链记账节点收到交易后，触发虚拟机调用权限管理合约。一般情况下管理员权限最大，包含权限转移或移交等权限。

如果不具有管理员权限，则合约执行结束，返回拒绝服务的合约执行结果。

S404、第一节点设备验证校验发起者的签名是否合法，若合法，则执行S405，若否，则执行S407。

具体地，当签名不合法则返回拒绝服务的合约执行结果，执行S407。

20 S405、第一节点设备检查传入的待转移用户ID是否合法，若是，执行S406，若否则执行S407。

在一实施例中，当不合法时，返回拒绝服务的合约执行结果。

S406、第一节点设备将待转移权限的当前用户ID更新为待转移用户ID，并将权限转移结果数据写入合约缓存。

25 在一实施例中，执行完权限操作后可以返回操作成功的合约执行结果。

S407、第一节点设备将结果签名后在区块链中广播给第二节点设备，接收到第二节点设备广播的结果。

其中，结果可以包括合约执行结果（如权限操作成功、失败等）、或者权限分配的校验结果（如校验通过等）。比如，可以将本端的合约执行结果签名

后广播给区块链中其他的节点设备。

S408、当第一节点设备的结果与第二节点设备的结果一致时，第一节点设备将合约缓存数据写入区块链合约账本。

在一实施例提供的一种角色委托代理方法，该方法可以由区块链中第一节点设备执行，参考图5，具体流程如下：

S501、第一节点设备接收交易发起方发起的合约交易请求，并将合约交易请求广播给第二节点设备。

其中，用户如管理员可以通过交易触发委托其他用户代理角色，比如，通过终端向区块链的第一节点设备发送合约交易请求。

10 S502、第一节点设备根据合约交易请求确定权限操作类型为角色委托代理。

比如，合约交易请求可以携带权限操作类型，此时，可以直接基于请求确定权限操作类型。

15 S503、第一节点设备根据权限管理合约校验调用的参数是否合法，若是，则执行S504，若否，则执行S512。

如果不合法，则合约执行结束，返回拒绝服务的合约执行结果。

S504、第一节点设备验证校验发起者的签名是否合法，若合法，则执行S505，若否，则执行S512。

具体地，当签名不合法则合约执行结束，返回拒绝服务的合约执行结果。

20 S505、第一节点设备检查出入的委托ID是否合法，若是，执行S506，若否则执行S512。

在一实施例中，当不合法时，返回拒绝服务的合约执行结果，执行S512。

S506、第一节点设备查询区块链合约账本检查交易发送者是否具有待委托角色，若是，则执行S507，若否，执行S512。

25 当检查交易发送者不具有待委托角色时，合约结束执行，返回拒绝服务的合约执行结果执行S512。

S507、第一节点设备查询区块链合约账本检查待委托用户是否具有待委托角色，若否，则执行S507，若是，执行S512。

当检查到待委托用户具有待委托角色时，合约执行结束、返回拒绝服务的

合约执行结果，并执行S512。

S508、第一节点设备检查交易发送者的待委托角色的等级以及有效期。

如果等级过低或者有效期过期，合约结束执行，返回拒绝服务的合约执行结果，并执行S512。

5 S509、当等级大于预设等级、以及有效期未过期时，查询区块链合约账本获取待委托用户的已代理角色状态。

S510、第一节点设备检查待委托角色是否已经被待委托用户代理，若否，则执行S511，若是，则执行S512。

10 若已经被代理，则更新代理的等级，有效期，返回操作成功或失败的合约执行结果，并执行S512。

S511、第一节点设备将待委托角色添加为待委托角色的已代理角色，并将角色委托结果数据写入合约缓存。

S512、第一节点设备将结果签名后在区块链中广播给第二节点设备，接收到第二节点设备广播的结果。

15 其中，结果可以包括合约执行结果（如权限操作成功、失败等）、或者权限分配的校验结果（如校验通过等）。比如，可以将本端的合约执行结果签名后广播给区块链中其他的节点设备。

S513、当第一节点设备的结果与第二节点设备的结果一致时，第一节点设备将合约缓存数据写入区块链合约账本。

20 比如，区块链记账节点对结果签名后广播，达成共识后，将合约缓存写入合约账本。

在一实施例提供的一种撤回委托角色方法，该方法可以由区块链中第一节点设备执行，参考图6，具体流程如下：

25 S601、第一节点设备接收交易发起方发起的合约交易请求，并将合约交易请求广播给第二节点设备。

其中，用户如管理员可以通过交易触发撤回委托给其他用户代理的角色，比如，通过终端向区块链的第一节点设备发送合约交易请求。

S602、第一节点设备根据合约交易请求确定权限操作类型为角色委托撤回。

比如，合约交易请求可以携带权限操作类型，此时，可以直接基于请求确定权限操作类型。

S603、第一节点设备验证校验发起者的签名是否合法，若合法，则执行S604，若否，则执行S608。

5 具体地，当签名不合法则合约执行结束，返回拒绝服务的合约执行结果，执行S608。

S604、第一节点设备查询区块链合约账本检查交易发送者是否委托的角色令牌，若是，执行S605，若否则执行S608。

10 在一实施例中，当没有该角色令牌时，合约执行结束返回拒绝服务的合约执行结果，执行S608。

S605、第一节点设备查询区块链合约账本查询代理用户所代理的角色。

S606、第一节点设备比对代理的角色是否包含交易发送者委托的角色，若有执行S607，若没有执行S608。

15 当代理的角色不包含交易发送者委托的角色时，合约结束执行，返回拒绝服务的合约执行结果，执行S608。

S607、第一节点设备撤回委托的角色，并将撤回委托角色数据写入合约缓存。

S608、第一节点设备将结果签名后在区块链中广播给第二节点设备，接收到第二节点设备广播的结果。

20 S609、当第一节点设备的结果与第二节点设备的结果一致时，第一节点设备将合约缓存数据写入区块链合约账本。

比如，区块链记账节点对结果签名后广播，达成共识后，将合约缓存写入合约账本。

25 在一实施例提供的一种用户权限验证方法，该方法可以由区块链中第一节点设备执行，参考图7，具体流程如下：

S701、第一节点设备接收交易发起方发起的合约交易请求，并将合约交易请求广播给第二节点设备。

其中，用户如管理员可以通过交易触发验证用户权限，比如，通过终端向区块链的第一节点设备发送合约交易请求。

S702、第一节点设备根据合约交易请求确定权限操作类型为用户权限验证。

比如，合约交易请求可以携带权限操作类型，此时，可以直接基于请求确定权限操作类型。

5 S703、第一节点设备验证校验发起者的签名是否合法，若合法，则执行S704，若否，则执行S715。

具体地，当签名不合法则合约执行结束，返回拒绝服务的合约执行结果，执行S715。

10 S704、第一节点设备查询区块链合约账本获取交易发送者的角色令牌集合。

S705、第一节点设备通过遍历角色令牌集合，查询合约账本获取集合内当前角色令牌对应的功能权限。

S707、第一节点设备确定功能权限是否包含交易发送者想要执行的功能，若否，执行S708，若是确定功能权限验证通过，执行S715。

15 S708、第一节点设备确定角色令牌集合是否遍历完，若否，则获取集合内下一个角色令牌，返回执行S707，若是，则执行S709。

也即：第一节点设备对角色令牌集合中每一个角色令牌，查询合约账本获取对应的功能权限；比对功能权限是否包含交易发送者想要执行的功能，如果有，合约结束执行，返回允许操作的结果。如果没有继续S708。

20 S709、第一节点设备查询合约账本获取交易发送者所代理的代理角色令牌集合。

S710、当等级大于预设等级、以及有效期末过期时，查询区块链合约账本获取待委托用户的已代理角色状态。

25 S711、第一节点设备通过遍历代理角色令牌集合，检查代理角色令牌集合内代理角色令牌的代理是否过期，若否，则执行S712，若是执行S714。

S712、第一节点设备查询合约账本获取代理角色令牌集合内代理角色令牌对应的功能权限。

S713、第一节点设备确定功能权限是否包含交易发送者想要执行的功能，若否，执行S714，若是，则确定功能权限验证通过，执行S715。

S714、第一节点设备确定代理角色令牌集合是否遍历完，若否，则获取集合内下一个代理角色令牌，返回执行S712，若是，则确定功能权限验证通过，执行S715。

5 S715、第一节点设备将结果签名后在区块链中广播给第二节点设备，接收到第二节点设备广播的结果。

其中，结果可以包括合约执行结果，比如，具体可以包括功能权限验证结果，如成功、失败，或者权限验证通过、不通过等。

S716、当第一节点设备的结果与第二节点设备的结果一致时，允许交易发送者进行相应操作。

10 比如，区块链记账节点对结果签名后广播，达成共识后，允许交易发送者进行相应操作。

该方案可以基于区块链权限管理合约体系实现去中心化的权限验证，因此，可以提升权限和数据的安全性。

15 本申请实施例提的方案可以适用大部分需要权限管理的应用场景，比如区块链电子发票、区块链供应链金融、互联网存证等。本实施例以区块链电子发票为产品表现为例来说明。

参考下表1，该表1展示了为角色配置的相关权限：

表1 角色与权限的配置关系表

角色	权限
个人用户	可以接收发票资产、查看和转让自己名下的发票资产详情
企业用户	可以申领空白票资产，开具发票，受票，查看自己名下的发票资产详情
服务商用户	可以代企业用户进行发票申领、开具、受票、查看详情
地方局用户	可以注册企业用户、服务商用户、设置税控指令、查询税控指令、查看自己注册的所有企业的发票详细信息
总局用户	可以注册总局用户、地方局用户、

	拥有全量数据的查看权限和资产转让权限
--	--------------------

以注册权限为例，参考表2，不同类型的用户可以有不同的注册权限，理论上总局用户可以拥有最高权限，但是实际情况中总局不参与实际业务，所以为了职责的单一性我们在设计的时候只为总局用户保留税局用户的注册权限，另外个人用户与企业用户相比管理难度更高也更离散，所以暂时不开放个人用户的自行注册流程，所有的个人用户都应该是有服务商代位注册的。

详细注册权限如下所示。

表2 用户与注册权限的关系表

	是否 可注册总 局用户	是否 可注册地 方局用户	是否 可注册企 业用户	是否 可注册服 务商用户	是否 可注册个 人用户
总局用 户	是	是	否	否	否
地方局 用户	否	否	是	是	否
企业用 户	否	否	否	否	否
服务商 用户	否	否	否	否	是
个人用 户	否	否	否	否	否

参考图8，将用户注册权限部署到智能合约体系后，基于区块链的节点设备A,B,C,D含有相同的合约内容，这时候不同类型的用户可以向智能合约体系提交注册申请。

个人用户申请注册流程描述：

第一步：节点设备D收到个人请求后，智能合约会执行权限检查，个人用户没有权限注册拒绝注册；同时将请求消息广播给节点设备A,B,C，节点设备A,B,C收到请求后也执行智能合约权限检查。

—25—

第二步：节点设备A,B,C,D广播检查结果。

第三步：节点设备A,B,C,D收到检查结果后通过共识模块校验结果是否一致，并将拒绝注册申请的结果返回给个人用户。

由于其他类型用户注册流程和个人用户流程类似，不再重复。

5 本申请实施例采用去中心化的智能合约自动管理权限，可以消除联盟链中恶意节点作恶的情况，增强了联盟链的安全度；另外采用智能合约去管理权限，更容易扩展到不通的业务，不需要像中心化集中管理那样定制。

为了更好地实施以上方法，相应的，本申请实施例还提供一种权限管理装置，该权限管理装置具体可以集成在区块链的节点设备中，该节点设备可以为
10 服务器等设备。

例如，如图9a所示，该权限管理装置可以包括第一接收单元801、确定单元802、第二接收单元805以及触发单元806，如下：

第一接收单元801，用于接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；
15 确定单元802，用于根据所述权限操作请求，得到第一合约执行结果；

第二接收单元805，用于接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；

触发单元806，用于当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。
20

在一实施例中，参考图9b，该图示出了本申请实施例提供的权限管理装置的一结构示意图，所述确定单元802，具体用于：

根据所述权限操作请求确定需要操作的权限操作类型；

所述装置还包括：

25 校验单元803，用于基于权限管理合约执行所述权限操作类型对应的校验逻辑；

接收单元804，当校验通过时，执行所述权限操作类型对应的权限操作，得到第一合约执行结果。

在一实施例中，参考图9c，校验单元803，可以包括：

第一验证子单元8031,用于基于所述权限管理合约对请求发起用户的操作合法性进行验证;

第二验证子单元8032,用于当请求发起用户的操作合法时,对权限操作类型对应的操作对象的权限信息进行验证;当权限信息验证通过时,确定校验通过。

在一实施例中,第一验证子单元8031,可以具体用于:

基于所述权限管理合约对请求发起用户的功能权限和签名进行验证;

当请求发起用户的功能权限和签名验证通过时,确定请求发起用户的操作合法。

10 在一实施例中,所述权限操作类型包括权限分配;第二验证子单元8032,可以具体用于:

当请求发起用户的操作合法时,从区块链合约账本中获取待分配角色对应的已分配功能权限集合,所述区块链合约账本包括用户、角色和已分配功能权限之间的映射关系;

15 当所述已分配功能权限集合不包含所述待分配权限时,确定权限信息验证通过;

操作单元804,用于当校验通过时,将所述待分配权限添加到所述已分配功能权限集合中。

20 在一实施例中,所述权限操作类型包括:角色分配;第二验证子单元8032,可以具体用于:

当请求发起用户的操作合法时,基于所述权限管理合约给待分配用户分配角色令牌;

从区块链合约账本中获取待分配用户对应的角色令牌集合;

当所述角色令牌集合不包含所述角色令牌时,确定权限信息验证通过;

25 操作单元804,用于当校验通过时,将所述角色令牌添加到所述角色令牌集合中。

在一实施例中,所述权限操作类型包括权限转移;第二验证子单元8032,可以具体用于:

当请求发起用户的操作合法时,对待转移用户的身份合法性进行检查;

当待转移用户的身份合法时，确定权限信息验证通过；

操作单元804，用于当校验通过时，将待转移权限的用户更新为待转移用户。

在一实施例中，第一验证子单元8031，可以具体用于：

5 基于所述权限管理合约对调用参数和请求发起用户的签名进行验证；

当调用参数和签名验证通过时，确定请求发起用户的操作合法性验证通过。

在一实施例中，所述权限操作类型包括：角色委托代理；第二验证子单元8032，可以具体用于：

10 当请求发起用户的操作合法时，对待委托用户的身份合法性进行检查；

当待委托用户的身份合法时，基于待委托角色对所述请求发起用户和所述待委托用户的角色进行检查；

当检查到所述请求发起用户具有所述待委托角色且所述待委托用户不具有所述待委托角色时，从区块链合约账本中获取待委托用户的已代理角色；

15 当所述已代理角色不包含所述待委托角色时，确定权限信息验证通过；

操作单元804，用于当校验通过时，将所述待委托角色添加为所述待委托角色的已代理角色。

在一实施例中，所述权限操作类型包括：角色委托撤回；第二验证子单元8032，可以具体用于：

20 当请求发起用户的操作合法时，检查请求发起用户是否有待撤回角色令牌；

若有待撤回的角色令牌，从区块链合约账本中获取代理用户的代理角色令牌集合；

25 当所述代理角色令牌集合包含所述待撤回角色令牌时，确定权限信息验证通过；从所述代理角色令牌集合中撤回所述待撤回角色令牌。

在一实施例中，第一验证子单元8031，可以具体用于：

当所述角色令牌集合中角色令牌对应的功能权限包含所述权限操作类型所需的目标功能权限时，确定功能权限验证通过；

当所述角色令牌集合中角色令牌对应的功能权限未包含所述权限操作类

型所需的目标功能权限时,从区块链合约账本中获取请求发起用户所代理的代理角色令牌集合;

当所述代理角色令牌集合中代理角色令牌对应的功能权限包含所述权限操作类型所需的目标功能权限时,确定功能权限验证通过;

5 基于权限管理合约对请求发起用户的签名进行验证。

具体实施时,以上各个单元可以作为独立的实体来实现,也可以进行任意组合,作为同一或若干个实体来实现,以上各个单元的具体实施可参见前面的方法实施例,在此不再赘述。

由上可知,本实施例的权限管理装置可以通过第一接收单元801接收权限操作请求,并向区块链中的第二节点设备转发所述权限操作请求;其中,所述第二节点设备为区块链中除第一节点设备以外的节点设备;由确定单元802根据所述权限操作请求确定需要操作的权限操作类型;由校验单元803基于权限管理合约执行所述权限操作类型对应的校验逻辑;由操作单元804当校验通过时,执行所述权限操作类型对应的权限操作,得到第一合约执行结果;由第二接收单元805接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果;由触发单元806当所述第一合约执行结果与所述第二合约执行结果一致时,触发第一合约执行结果生效。该方案可以基于区块链权限管理合约体系实现去中心化的权限管理,将自身的第一合约执行结果与接收到的第二合约执行结果进行对比,当自身合约执行结果与其他节点设备的合约执行结果一致实现达成共识,才触发第一合约执行结果生效,由此可以提升权限和数据的安全性。

此外,本申请实施例还提供一种数据处理设备,如图10所示,其示出了本申请实施例所涉及的数据处理设备如网络设备的结构示意图,具体来讲:

25 该网络设备可以包括一个或者一个以上处理核心的处理器 111、一个或一个以上计算机可读存储介质的存储器 112、电源 113 和输入单元 114 等部件。本领域技术人员可以理解,图 11 中示出的网络设备结构并不构成对网络设备的限定,可以包括比图示更多或更少的部件,或者组合某些部件,或者不同的部件布置。其中:

处理器 111 是该网络设备的控制中心,利用各种接口和线路连接整个网络

设备的各个部分，通过运行或执行存储在存储器 112 内的软件程序和/或模块，以及调用存储在存储器 112 内的数据，执行网络设备的各种功能和处理数据，从而对网络设备进行整体监控。可选的，处理器 111 可包括一个或多个处理核心；优选的，处理器 111 可集成应用处理器和调制解调处理器，其中，应用处
5 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 111 中。

存储器 112 可用于存储软件程序以及模块，处理器 111 通过运行存储在存储器 112 的软件程序以及模块，从而执行各种功能应用以及数据处理。存储器 112 可主要包括存储程序区和存储数据区，其中，存储程序区可存储操作系统、
10 至少一个功能所需的应用程序（比如声音播放功能、图像播放功能等）等；存储数据区可存储根据网络设备的使用所创建的数据等。此外，存储器 112 可以包括高速随机存取存储器，还可以包括非易失性存储器，例如至少一个磁盘存储器件、闪存器件、或其他易失性固态存储器件。相应地，存储器 112 还可以包括存储器控制器，以提供处理器 111 对存储器 112 的访问。

15 网络设备还包括给各个部件供电的电源 113，优选的，电源 113 可以通过电源管理系统与处理器 111 逻辑相连，从而通过电源管理系统实现管理充电、放电、以及功耗管理等功能。电源 113 还可以包括一个或一个以上的直流或交流电源、再充电系统、电源故障检测电路、电源转换器或者逆变器、电源状态指示器等任意组件。

20 该网络设备还可包括输入单元 114，该输入单元 114 可用于接收输入的数字或字符信息，以及产生与用户设置以及功能控制有关的键盘、鼠标、操作杆、光学或者轨迹球信号输入。

尽管未示出，网络设备还可以包括显示单元等，在此不再赘述。具体在本
25 实施例中，网络设备中的处理器 111 会按照如下的指令，将一个或一个以上的应用程序的进程对应的可执行文件加载到存储器 112 中，并由处理器 111 来运行存储在存储器 112 中的应用程序，从而实现各种功能，如下：

接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；根据所述权限操作请求，得到第一合约执行结果；接收所述第二节点设备基于所

述权限操作请求广播的第二合约执行结果；当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。

以上各个操作的具体实施可参见前面的实施例，在此不再赘述。

由上可知，本实施例的网络设备可以作为区块链中的节点设备如第一节点设备，该设备可以接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；根据所述权限操作请求，得到第一合约执行结果；接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。该方案基于区块链权限管理合约体系实现去中心化的权限管理，将自身的第一合约执行结果与接收到的第二合约执行结果进行对比，当自身合约执行结果与其他节点设备的合约执行结果一致实现达成共识，才触发第一合约执行结果生效，由此可以提升权限和数据的安全性。

本领域普通技术人员可以理解，上述实施例的各种方法中的全部或部分步骤可以通过指令来完成，或通过指令控制相关的硬件来完成，该指令可以存储于一计算机可读存储介质中，并由处理器进行加载和执行。

在一个实施方式中，提供了一种计算机设备，该计算机设备可以是服务器或终端。该计算机设备，包括处理器、通信接口、存储器和通信总线，其中，所述处理器、所述通信接口和所述存储器通过所述通信总线完成相互间的通信；所述通信接口为通信模块的接口；

所述存储器，用于存储程序代码，并将所述程序代码传输给所述处理器；

所述处理器，用于调用存储器中程序代码的指令执行上述各个实施例中的方法。

本申请实施例还提供一种存储介质，所述存储介质用于存储计算机程序，所述计算机程序用于执行上述各个实施例中的方法。其中存储有多条指令，该指令能够被处理器进行加载，以执行上述各个实施例中的方法。例如，该指令可以执行如下步骤：

接收权限操作请求，并向区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为区块链中除第一节点设备以外的节点设备；根

据所述权限操作请求，得到第一合约执行结果；接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。

以上各个操作的具体实施可参见前面的实施例，在此不再赘述。

- 5 其中，该存储介质可以包括：只读存储器（ROM，Read Only Memory）、随机存取记忆体（RAM，Random Access Memory）、磁盘或光盘等。

由于该存储介质中所存储的指令，可以执行本申请实施例所提供的任一种方法中的步骤，因此，可以实现本申请实施例所提供的任一种方法所能实现的有益效果，详见前面的实施例，在此不再赘述。

- 10 在一示例性实施例中，本申请实施例还提供了一种包括指令的计算机程序产品，当其在服务器上运行时，使得服务器执行上述各个实施例中的方法。

- 15 以上对本申请实施例所提供的一种权限管理方法、权限验证方法和相关装置进行了详细介绍，本文中应用了具体个例对本申请的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本申请的方法及其核心思想；同时，对于本领域的技术人员，依据本申请的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本申请的限制。

权 利 要 求

1、一种权限管理方法，由区块链中的第一节点设备执行，包括：

接收权限操作请求，并向所述区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为所述区块链中除所述第一节点设备以外的节点设备；

根据所述权限操作请求，得到第一合约执行结果；

接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；

当所述第一合约执行结果与所述第二合约执行结果一致时，触发第一合约执行结果生效。

2、根据权利要求1所述的权限管理方法，所述根据所述权限操作请求，得到第一合约执行结果，包括：

根据所述权限操作请求确定需要操作的权限操作类型；

基于权限管理合约执行所述权限操作类型对应的校验逻辑；

当校验通过时，执行所述权限操作类型对应的权限操作，得到第一合约执行结果。

3、根据权利要求2所述的权限管理方法，所述基于所述权限管理合约执行所述权限操作类型对应的校验逻辑，包括：

基于所述权限管理合约对请求发起用户的操作合法性进行验证；

当所述请求发起用户的操作合法时，对所述权限操作类型对应的操作对象的权限信息进行验证；

当所述权限信息验证通过时，确定校验通过。

4、根据权利要求3所述的权限管理方法，所述基于所述权限管理合约对请求发起用户的操作合法性进行验证，包括：

基于所述权限管理合约对操作参数进行验证，所述操作参数包括调用参数、请求发起用户的功能权限和签名中的一种或多种组合；

当验证通过时，确定所述请求发起用户的操作合法。

5、根据权利要求3所述的权限管理方法，所述权限操作类型包括权限分配；

所述当所述请求发起用户的操作合法时，对所述权限操作类型对应的操作对象的权限信息进行校验，包括：

当所述请求发起用户的操作合法时,从区块链合约账本中获取待分配角色对应的已分配功能权限集合,所述区块链合约账本包括用户、角色和已分配功能权限之间的映射关系;

当所述已分配功能权限集合不包含所述待分配权限时,确定权限信息验证通过;

所述执行所述权限操作类型对应的权限操作,包括:

将所述待分配权限添加到所述已分配功能权限集合中。

6、根据权利要求3所述的权限管理方法,所述权限操作类型包括:角色分配;

10 所述当所述请求发起用户的操作合法时,对所述权限操作类型对应的操作对象的权限信息进行校验,包括:

当所述请求发起用户的操作合法时,基于所述权限管理合约给待分配用户分配角色令牌;

从区块链合约账本中获取待分配用户对应的角色令牌集合;

15 当所述角色令牌集合不包含所述角色令牌时,确定权限信息验证通过;

所述执行所述权限操作类型对应的权限操作,包括:

将所述角色令牌添加到所述角色令牌集合中。

7、根据权利要求3所述的权限管理方法,所述权限操作类型包括权限转移;

所述当所述请求发起用户的操作合法时,对所述权限操作类型对应的操作

20 对象的权限信息进行校验,包括:

当所述请求发起用户的操作合法时,对待转移用户的身份合法性进行检查;

当所述待转移用户的身份合法时,确定权限信息验证通过;

所述执行所述权限操作类型对应的权限操作,包括:

25 将待转移权限的用户更新为所述待转移用户。

8、根据权利要求3所述的权限管理方法,所述基于所述权限管理合约对请求发起用户的操作合法性进行验证,包括:

基于所述权限管理合约对调用参数和所述请求发起用户的签名进行验证;

当所述调用参数和所述签名验证通过时,确定所述请求发起用户的操作合

法性验证通过。

9、根据权利要求8所述的权限管理方法，所述权限操作类型包括：角色委托代理；

5 所述当所述请求发起用户的操作合法时，对所述权限操作类型对应的操作对象的权限信息进行校验，包括：

当所述请求发起用户的操作合法时，对待委托用户的身份合法性进行检查；

当所述待委托用户的身份合法时，基于待委托角色对所述请求发起用户和所述待委托用户的角色进行检查；

10 当检查到所述请求发起用户具有所述待委托角色且所述待委托用户不具有所述待委托角色时，从区块链合约账本中获取所述待委托用户的已代理角色；

当所述已代理角色不包含所述待委托角色时，确定权限信息验证通过；

所述执行所述权限操作类型对应的权限操作，包括：

15 将所述待委托角色添加为所述待委托角色的已代理角色。

10、根据权利要求3所述的权限管理方法，所述权限操作类型包括：角色委托撤回；

所述当所述请求发起用户的操作合法时，对所述权限操作类型对应的操作对象的权限信息进行校验，包括：

20 当所述请求发起用户的操作合法时，检查所述请求发起用户是否有待撤回角色令牌；

若有所述待撤回角色令牌，从区块链合约账本中获取代理用户的代理角色令牌集合；

25 当所述代理角色令牌集合包含所述待撤回角色令牌时，确定权限信息验证通过；

所述执行所述权限操作类型对应的权限操作，包括：

从所述代理角色令牌集合中撤回所述待撤回角色令牌。

11、根据权利要求4所述的权限管理方法，所述基于所述权限管理合约对操作参数进行验证，包括：

基于权限管理合约从区块链合约账本中获取所述请求发起用户的角色令牌集合;

当所述角色令牌集合中角色令牌对应的功能权限包含所述权限操作类型所需的目标功能权限时, 确定功能权限验证通过;

- 5 当所述角色令牌集合中角色令牌对应的功能权限未包含所述权限操作类型所需的目标功能权限时, 从所述区块链合约账本中获取所述请求发起用户所代理的代理角色令牌集合;

当所述代理角色令牌集合中代理角色令牌对应的功能权限包含所述权限操作类型所需的目标功能权限时, 确定功能权限验证通过;

- 10 基于权限管理合约对所述请求发起用户的签名进行验证。

12、一种权限管理装置, 集成在区块链中的第一节点设备中, 包括:

第一接收单元, 用于接收权限操作请求, 并向所述区块链中的第二节点设备转发所述权限操作请求; 其中, 所述第二节点设备为所述区块链中除所述第一节点设备以外的节点设备;

- 15 确定单元, 用于根据所述权限操作请求, 得到第一合约执行结果;

第二接收单元, 用于接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果;

触发单元, 用于当所述第一合约执行结果与所述第二合约执行结果一致时, 触发第一合约执行结果生效。

- 20 13、一种权限验证方法, 由区块链中的第一节点设备执行, 包括:

接收权限操作请求, 并向所述区块链中的第二节点设备转发所述权限操作请求; 其中, 所述第二节点设备为所述区块链中除所述第一节点设备以外的节点设备;

根据所述权限操作请求, 得到第一合约执行结果;

- 25 接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果;

当所述第一合约执行结果与所述第二合约执行结果一致时, 确定用户权限验证通过。

14、根据权利要求13所述的权限验证方法, 所述根据所述权限操作请求, 得到第一合约执行结果, 包括:

根据所述权限操作请求确定需要操作的权限操作类型,所述权限操作类型为用户权限验证;

基于权限管理合约执行所述权限操作类型对应的校验逻辑;

当校验通过时,执行所述权限操作类型对应的权限操作,得到第一合约执行结果。

15、根据权利要求14所述的权限验证方法,所述基于所述权限管理合约执行所述权限操作类型对应的校验逻辑,包括:

基于所述权限管理合约对请求发起用户的操作合法性进行验证;

当所述请求发起用户的操作合法时,对所述权限操作类型对应的操作对象的权限信息进行验证;

当所述权限信息验证通过时,确定校验通过。

16、根据权利要求15所述的权限验证方法,所述基于所述权限管理合约对请求发起用户的操作合法性进行验证,包括:

基于所述权限管理合约对操作参数进行验证,所述操作参数包括调用参数、请求发起用户的功能权限和签名中的一种或多种组合;

当验证通过时,确定所述请求发起用户的操作合法。

17、根据权利要求15所述的权限验证方法,所述基于所述权限管理合约对请求发起用户的操作合法性进行验证,包括:

基于所述权限管理合约对调用参数和所述请求发起用户的签名进行验证;

当所述调用参数和所述签名验证通过时,确定所述请求发起用户的操作合法性验证通过。

18、根据权利要求16所述的权限验证方法,所述基于所述权限管理合约对操作参数进行验证,包括:

基于权限管理合约从区块链合约账本中获取所述请求发起用户的角色令牌集合;

当所述角色令牌集合中角色令牌对应的功能权限包含所述请求发起用户所需执行的功能时,确定功能权限验证通过;

当所述角色令牌集合中角色令牌对应的功能权限未包含所述请求发起用户所需执行的功能时,从所述区块链合约账本中获取所述请求发起用户所代理

的代理角色令牌集合;

当所述代理角色令牌集合中代理角色令牌对应的功能权限包含所述请求发起用户所需执行的功能时, 确定功能权限验证通过。

19、根据权利要求18所述的权限验证方法, 所述当所述角色令牌集合中角色令牌对应的功能权限包含所述请求发起用户所需执行的功能时, 确定功能权限验证通过, 包括:

通过遍历角色令牌集合, 查询所述角色令牌集合内角色令牌对应的功能权限;

确定所述角色令牌对应的功能权限是否包含所述请求发起用户所需执行的功能;

若包含, 则确定功能权限验证通过;

若不包含, 则确定所述角色令牌集合是否遍历完; 若所述角色令牌集合未遍历完, 则执行所述通过遍历角色令牌集合, 查询所述角色令牌集合内角色令牌对应的功能权限的步骤。

20、根据权利要求19所述的权限验证方法, 所述当所述角色令牌集合中角色令牌对应的功能权限未包含所述请求发起用户所需执行的功能时, 从所述区块链合约账本中获取所述请求发起用户所代理的代理角色令牌集合, 包括:

当所述角色令牌集合遍历完时, 确定所述角色令牌集合中角色令牌对应的功能权限未包含所述请求发起用户所需执行的功能;

从所述区块链合约账本中获取所述请求发起用户的代理角色令牌集合。

21、根据权利要求20所述的权限验证方法, 所述当所述代理角色令牌集合中代理角色令牌对应的功能权限包含所述请求发起用户所需执行的功能时, 确定功能权限验证通过, 包括:

通过遍历所述代理角色令牌集合, 检查所述代理角色令牌集合内代理角色令牌的代理是否过期;

若没有过期, 则查询所述代理角色令牌集合内所述代理角色令牌对应的功能权限;

确定所述代理角色令牌对应的功能权限是否包含所述请求发起用户所需执行的功能;

—38—

若包含，则确定功能权限验证通过。

22、一种权限验证装置，集成在区块链中的第一节点设备中，包括：

第一接收单元，用于接收权限操作请求，并向所述区块链中的第二节点设备转发所述权限操作请求；其中，所述第二节点设备为所述区块链中除所述第一节点设备以外的节点设备；

确定单元，用于根据所述权限操作请求，得到第一合约执行结果；

第二接收单元，用于接收所述第二节点设备基于所述权限操作请求广播的第二合约执行结果；

10 触发单元，用于当所述第一合约执行结果与所述第二合约执行结果一致时，确定用户权限验证通过。

23、一种计算机设备，所述计算机设备包括：

处理器、通信接口、存储器和通信总线；

其中，所述处理器、所述通信接口和所述存储器通过所述通信总线完成相互间的通信；所述通信接口为通信模块的接口；

15 所述存储器，用于存储程序代码，并将所述程序代码传输给所述处理器；

所述处理器，用于调用存储器中程序代码的指令执行权利要求 1-11 任意一项所述的方法，或者，执行权利要求 13-21 任意一项所述的方法。

24、一种存储介质，所述存储介质用于存储计算机程序，所述计算机程序用于执行权利要求 1-11 任意一项所述的方法，或者，执行权利要求 13-21 任意一项所述的方法。

20 25、一种包括指令的计算机程序产品，当其在计算机上运行时，使得所述计算机执行权利要求1-11任意一项所述的方法，或者，执行权利要求13-21任意一项所述的方法。

— 1/11 —

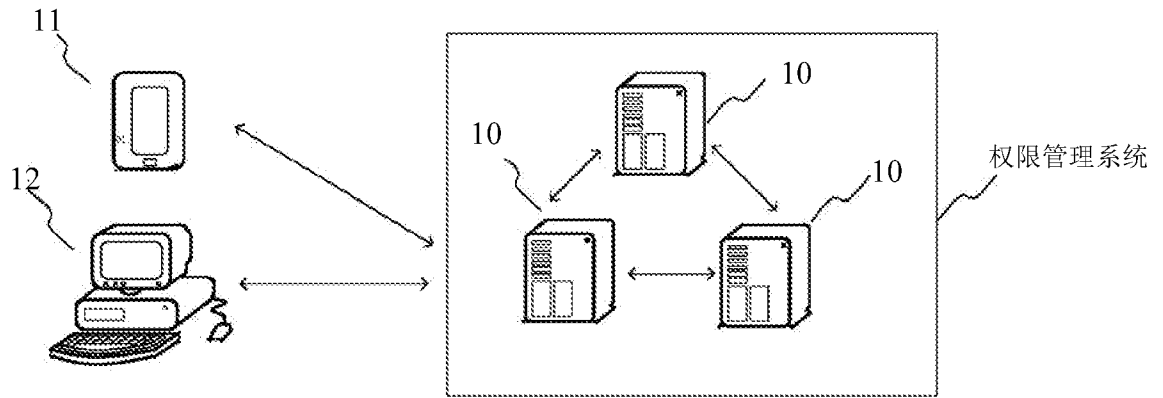


图 1

—2/11—

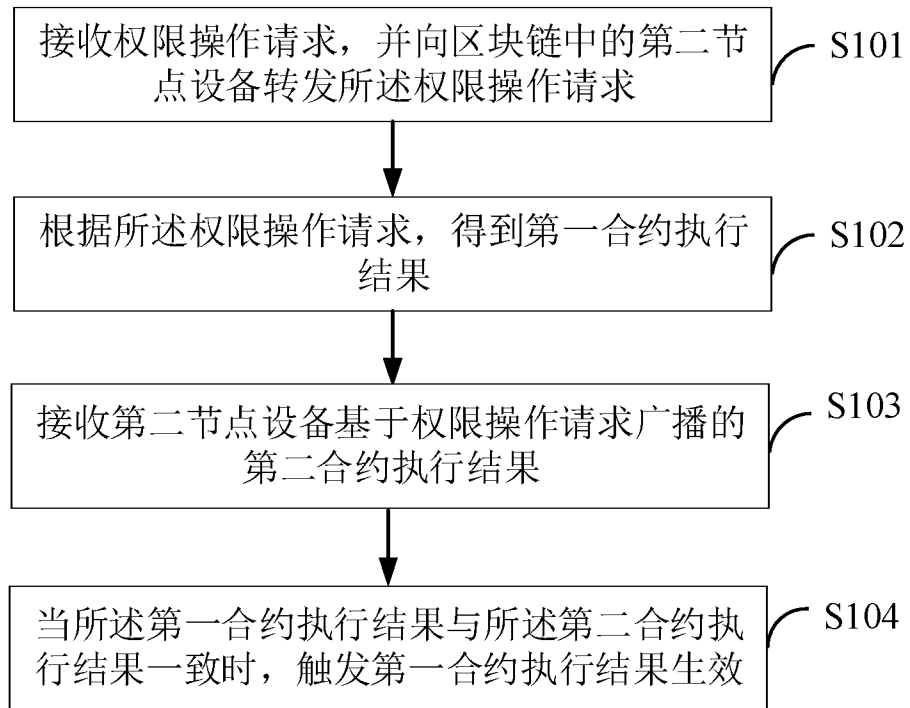


图 2

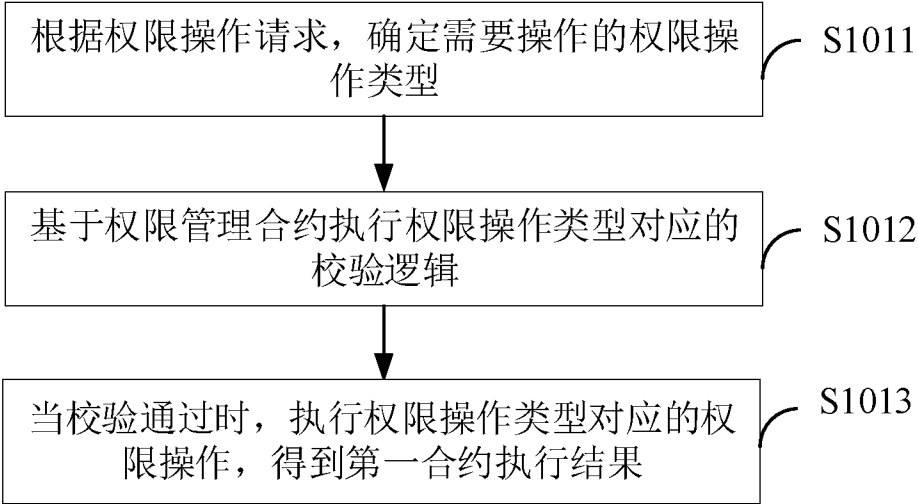


图 3a

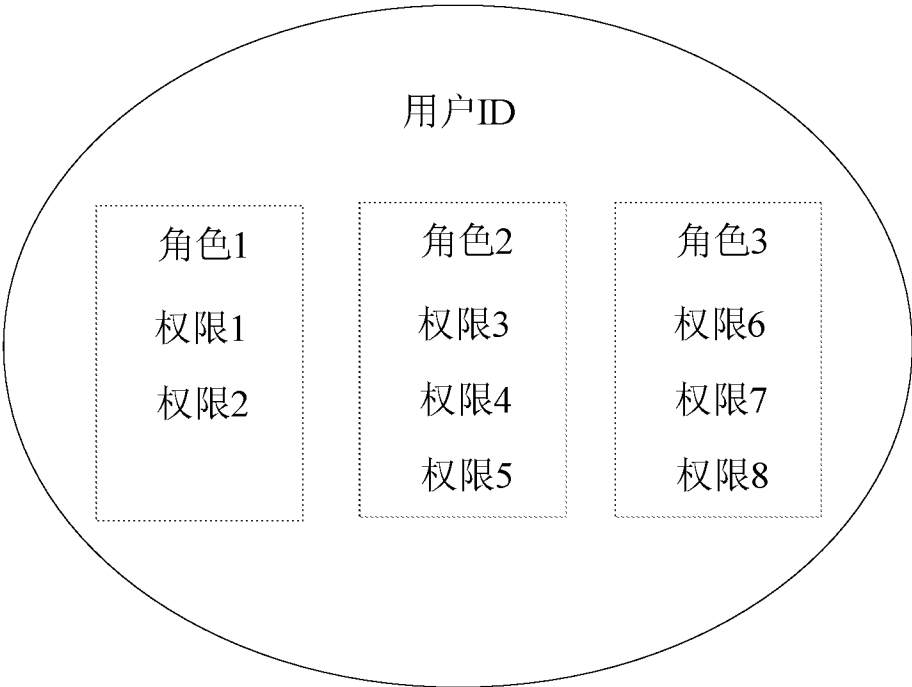


图 3b

— 4/11 —

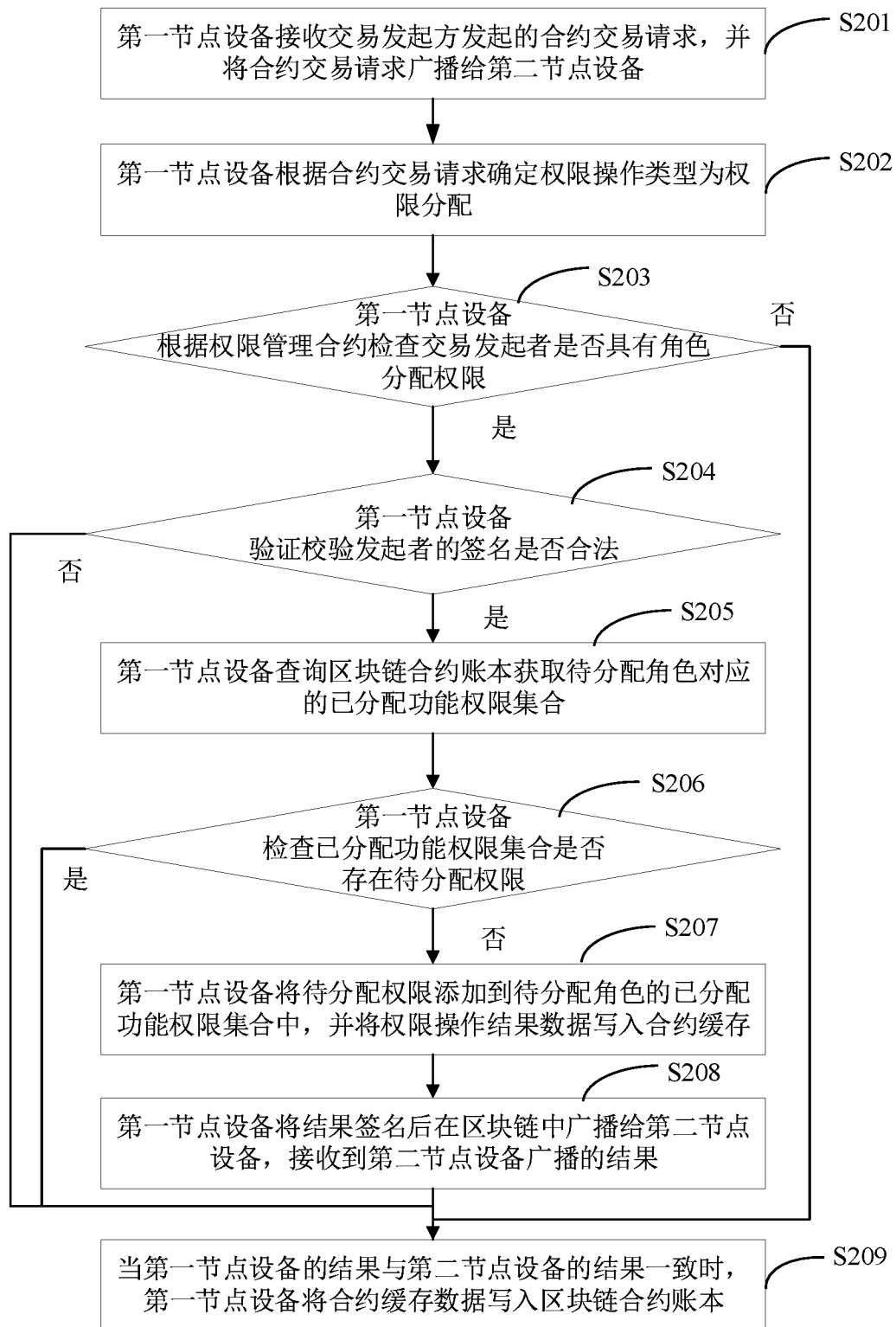


图 3c

— 5/11 —

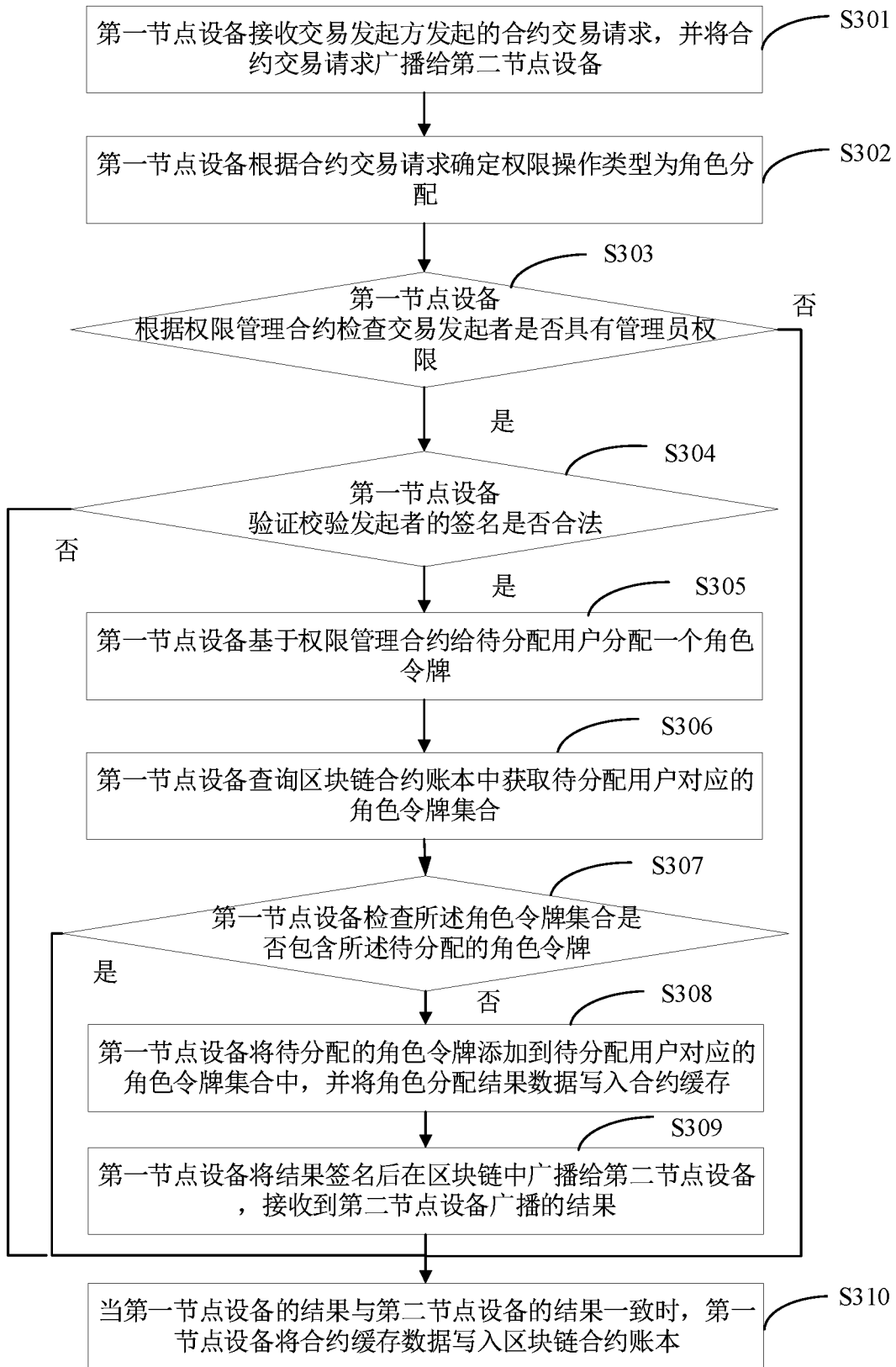


图 3d

—6/11—

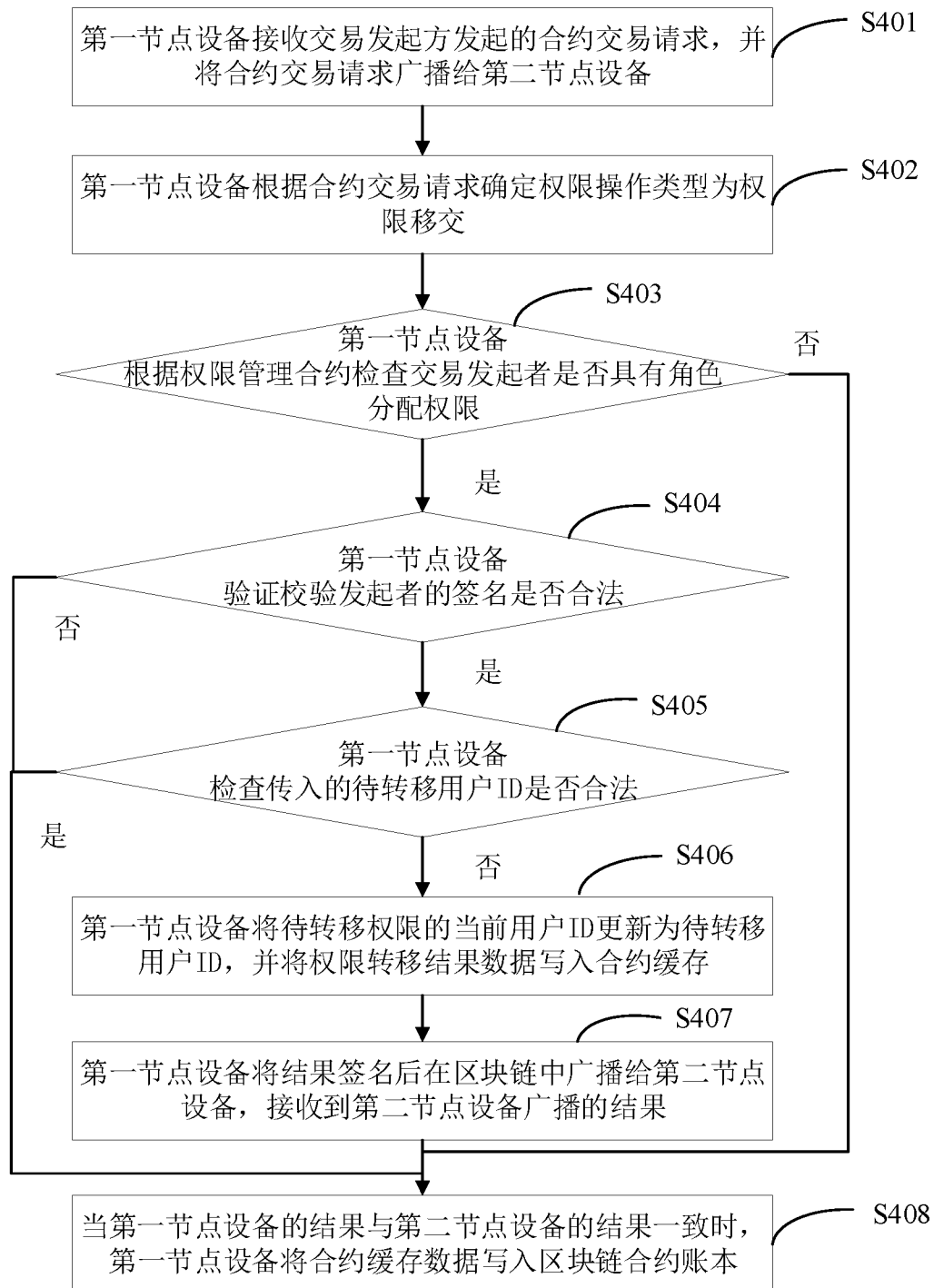


图 4

— 7/11 —

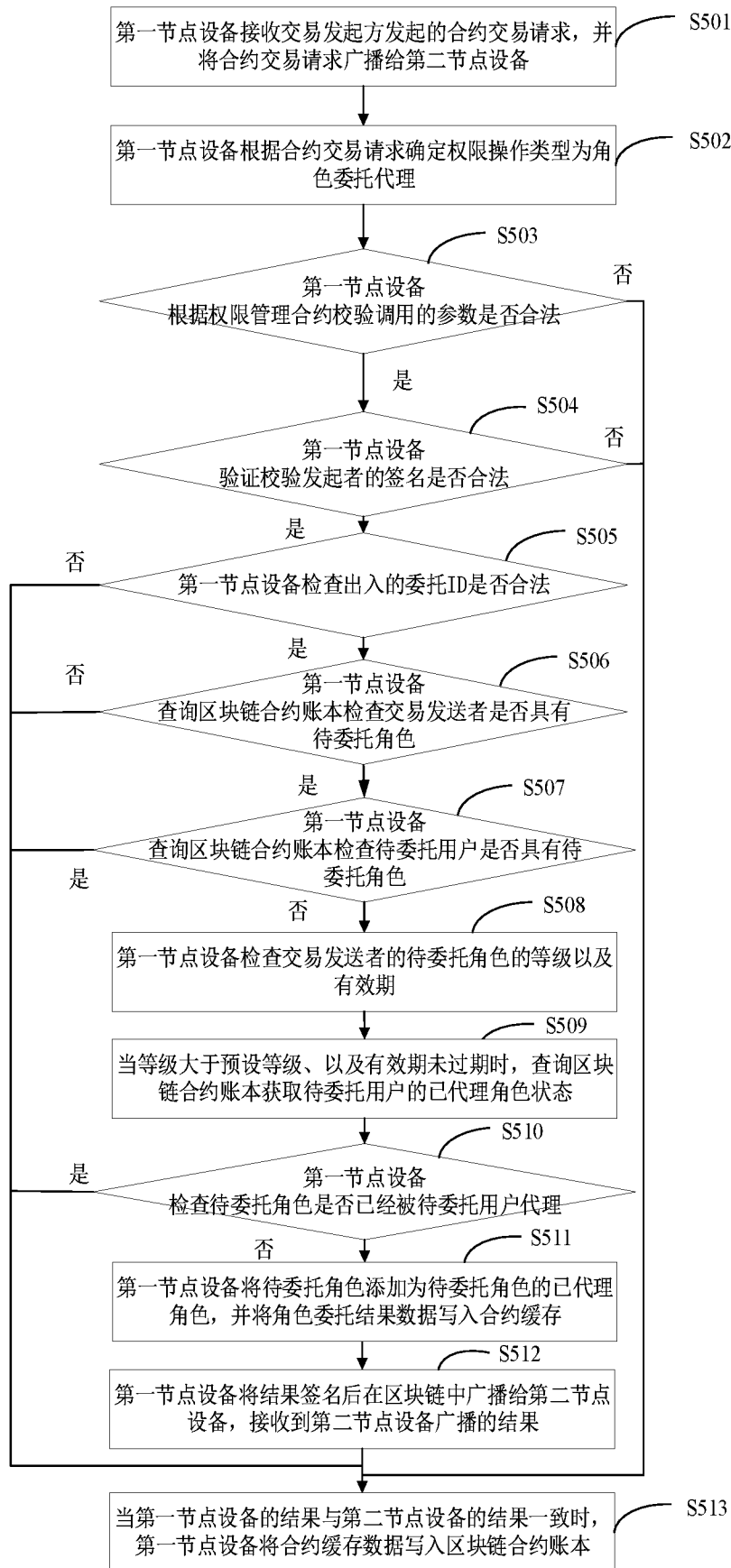


图 5

-8/11-

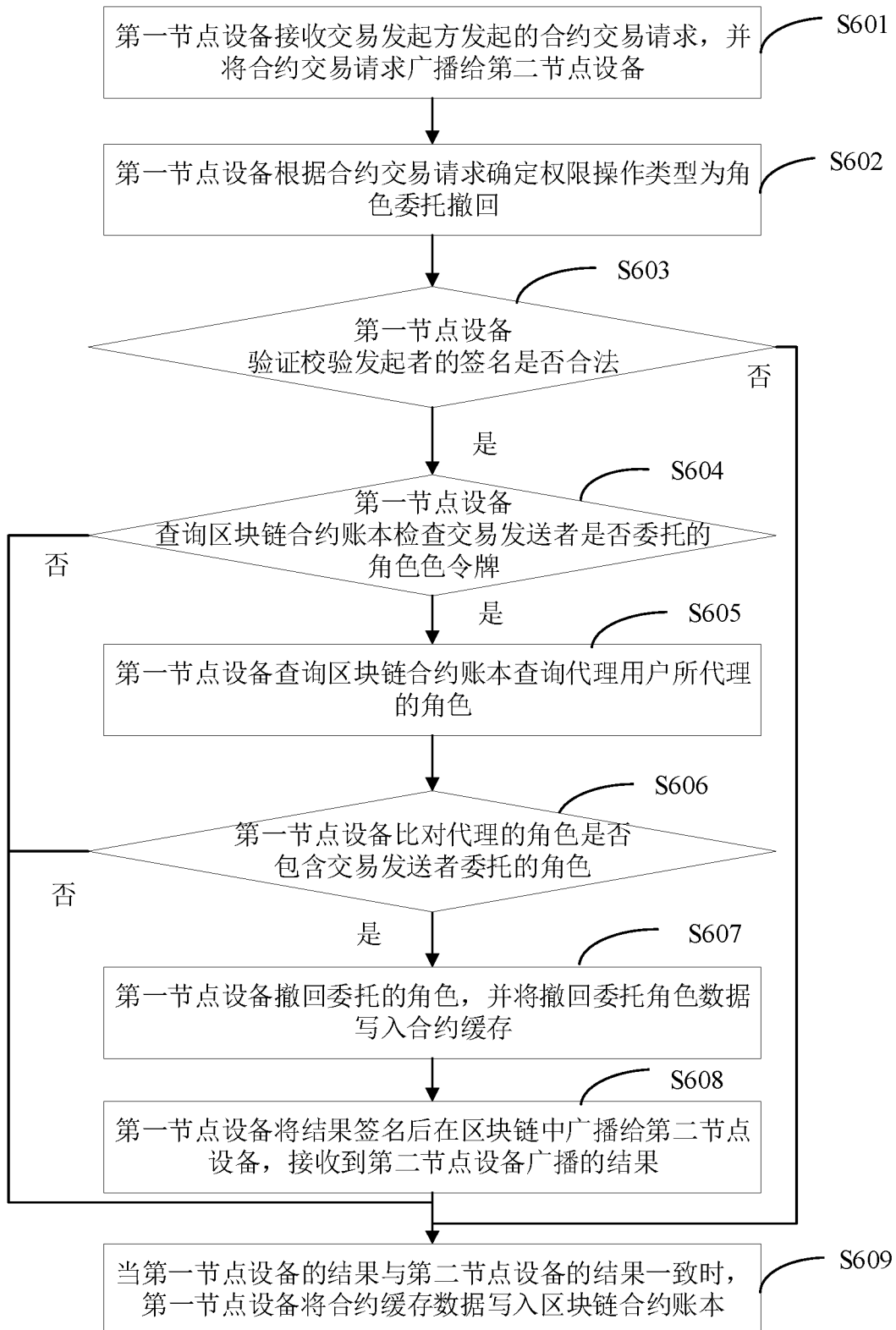


图 6

—9/11—

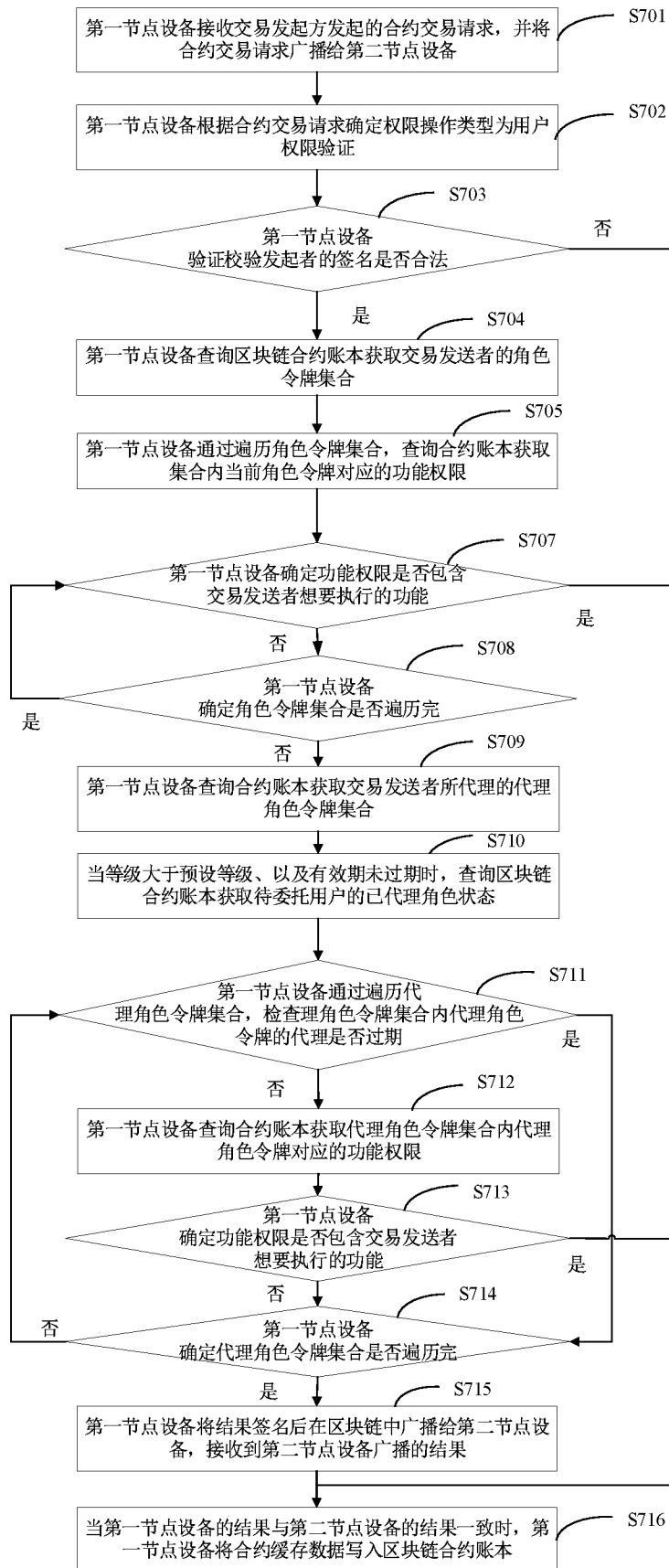


图 7

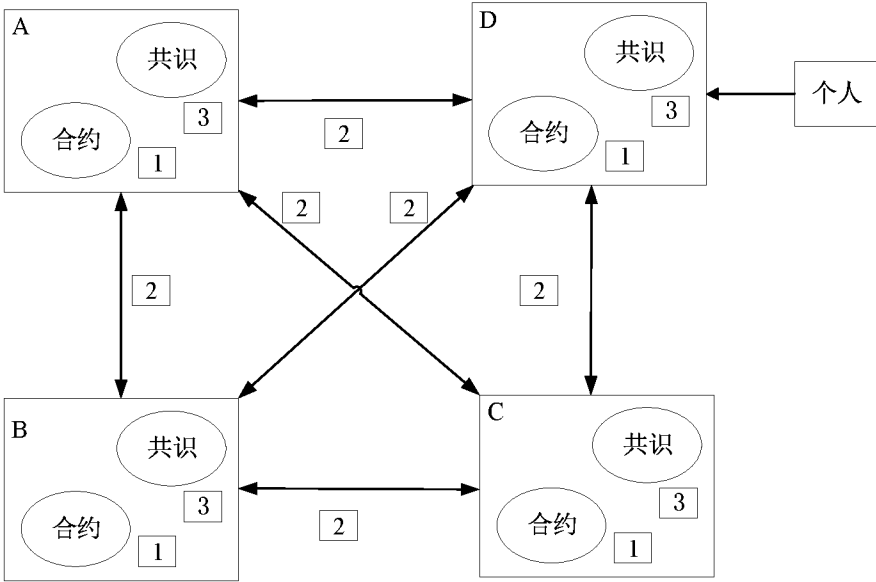


图 8

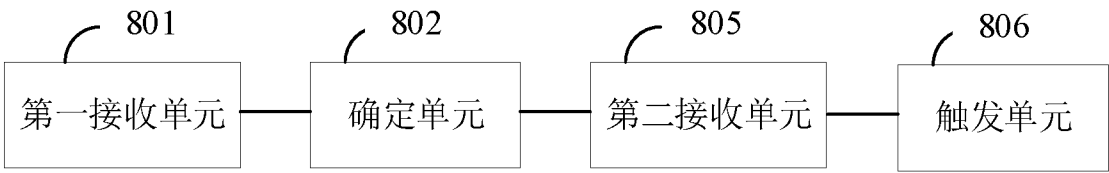


图 9a

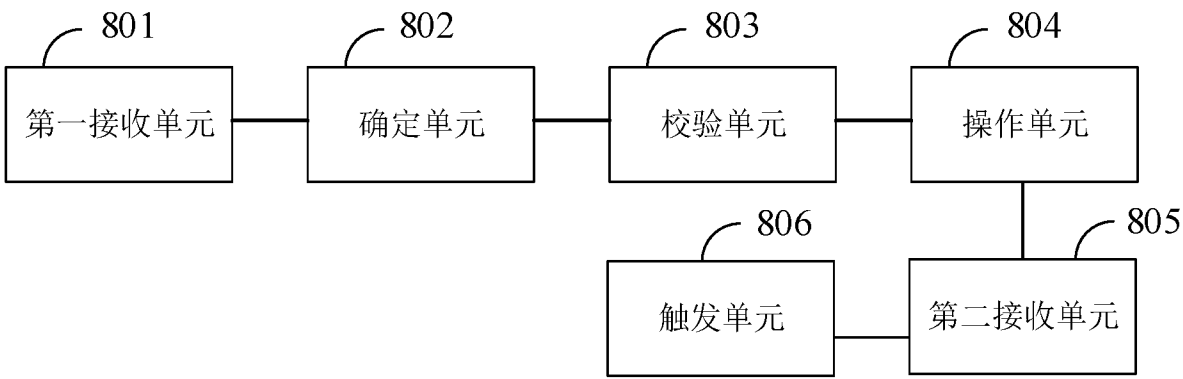


图 9b

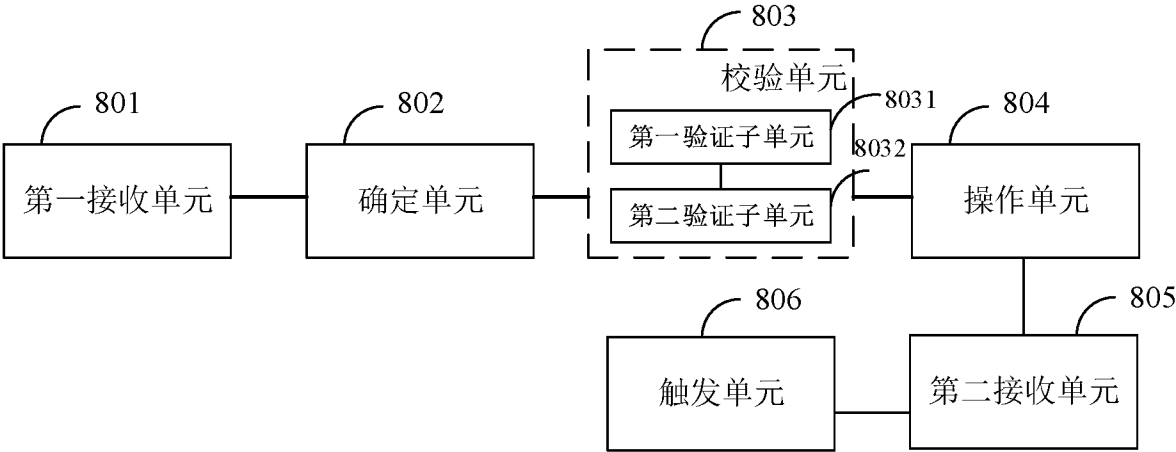


图 9c

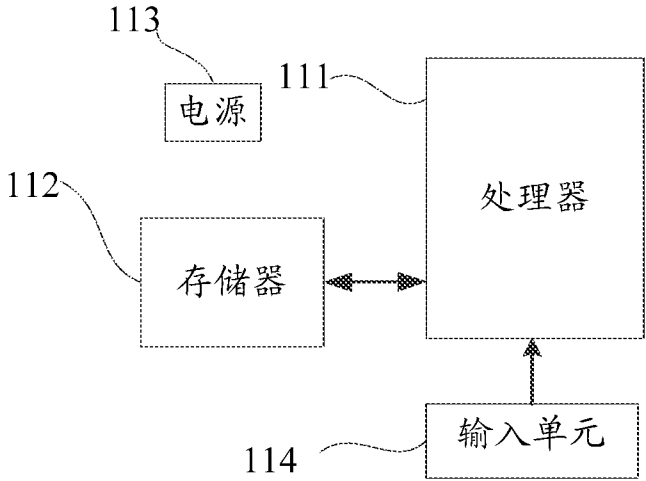


图 10

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/081526

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/46(2013.01)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, G06Q, 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)

DWPI; SIPOABS; CNABS; CNTXT; CNKI: 区块链, 分布式账本, 共享账本, 智能合约, 权限, 设置, 管理, 验证, 校验, blockchain, block chain, block-chain, distributed ledger, shared ledger, intelligent contract, smart contract, authori+, permission, set, manag+, validat+, authenticat+, verify+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 107911373 A (HANGZHOU BLOCKCHAIN TECHNOLOGY RESEARCH INSTITUTE, ZHONGCHAO CREDIT CARD INDUSTRY DEVELOPMENT CO., LTD.) 13 April 2018 (2018-04-13) description, paragraphs 56-110 and 139	1-25
PX	CN 110032865 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 19 July 2019 (2019-07-19) description, paragraphs 42-148	1-25
PX	CN 110598394 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD.) 20 December 2019 (2019-12-20) description, paragraphs 67-173	1-25
A	CN 106603698 A (BEIJING GOOPAL TECHNOLOGY CO., LTD.) 26 April 2017 (2017-04-26) entire document	1-25
A	CN 108632268 A (TENCENT TECHNOLOGY SHENZHEN CO., LTD. et al.) 09 October 2018 (2018-10-09) entire document	1-25



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

09 June 2020

Date of mailing of the international search report

19 June 2020

Name and mailing address of the ISA/CN

China National Intellectual Property Administration
 No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
 100088
 China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/081526**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	TW 646487 B (MODERNITY FINANCIAL HOLDINGS LTD.) 01 January 2019 (2019-01-01) entire document	1-25
A	US 2019014116 A1 (VCHAIN TECHNOLOGY LIMITED) 10 January 2019 (2019-01-10) entire document	1-25

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/081526

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	107911373	A	13 April 2018	CN	107911373	B	06 September 2019
CN	110032865	A	19 July 2019	CN	110598394	A	20 December 2019
CN	110598394	A	20 December 2019	CN	110032865	A	19 July 2019
CN	106603698	A	26 April 2017	None			
CN	108632268	A	09 October 2018	WO	2019205849	A1	31 October 2019
				CN	110602050	A	20 December 2019
TW	646487	B	01 January 2019	TW	I646487	B	01 January 2019
				TW	201905813	A	01 February 2019
US	2019014116	A1	10 January 2019	WO	2019012329	A1	17 January 2019

国际检索报告

国际申请号

PCT/CN2020/081526

A. 主题的分类

G06F 21/46 (2013.01) 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, G06Q, 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))

DWPI; SIPOABS; CNABS; CNTXT; CNKI: 区块链, 分布式账本, 共享账本, 智能合约, 权限, 设置, 管理, 验证, 校验, blockchain, block chain, block-chain, distributed ledger, shared ledger, intelligent contract, smart contract, authori+, permission, set, manag+, validat+, authenticat+, verify+

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
X	CN 107911373 A (中钞信用卡产业发展有限公司杭州区块链技术研究院) 2018年 4月 13日 (2018 - 04 - 13) 说明书第56-110、139段	1-25
PX	CN 110032865 A (腾讯科技深圳有限公司) 2019年 7月 19日 (2019 - 07 - 19) 说明书第42-148段	1-25
PX	CN 110598394 A (腾讯科技深圳有限公司) 2019年 12月 20日 (2019 - 12 - 20) 说明书第67-173段	1-25
A	CN 106603698 A (北京果仁宝科技有限公司) 2017年 4月 26日 (2017 - 04 - 26) 全文	1-25
A	CN 108632268 A (腾讯科技深圳有限公司等) 2018年 10月 9日 (2018 - 10 - 09) 全文	1-25
A	TW 646487 B (MODERNITY FINANCIAL HOLDINGS LTD) 2019年 1月 1日 (2019 - 01 - 01) 全文	1-25
A	US 2019014116 A1 (VCHAIN TECH LIMITED) 2019年 1月 10日 (2019 - 01 - 10) 全文	1-25

☐ 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 6月 9日

国际检索报告邮寄日期

2020年 6月 19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

吴广平

电话号码 (86-10) 62411829

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/081526

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	107911373	A	2018年 4月 13日	CN	107911373	B	2019年 9月 6日		
CN	110032865	A	2019年 7月 19日	CN	110598394	A	2019年 12月 20日		
CN	110598394	A	2019年 12月 20日	CN	110032865	A	2019年 7月 19日		
CN	106603698	A	2017年 4月 26日	无					
CN	108632268	A	2018年 10月 9日	WO	2019205849	A1	2019年 10月 31日		
				CN	110602050	A	2019年 12月 20日		
TW	646487	B	2019年 1月 1日	TW	I646487	B	2019年 1月 1日		
				TW	201905813	A	2019年 2月 1日		
US	2019014116	A1	2019年 1月 10日	WO	2019012329	A1	2019年 1月 17日		