



(12)发明专利申请

(10)申请公布号 CN 110598394 A

(43)申请公布日 2019.12.20

(21)申请号 201910934833.8

(22)申请日 2019.03.28

(62)分案原申请数据

201910245109.4 2019.03.28

(71)申请人 腾讯科技(深圳)有限公司

地址 518057 广东省深圳市南山区高新区
科技中一路腾讯大厦35层

(72)发明人 刘攀

(74)专利代理机构 深圳翼盛智成知识产权事务
所(普通合伙) 44300

代理人 汪阮磊

(51)Int.Cl.

G06F 21/46(2013.01)

G06F 21/62(2013.01)

G06F 21/64(2013.01)

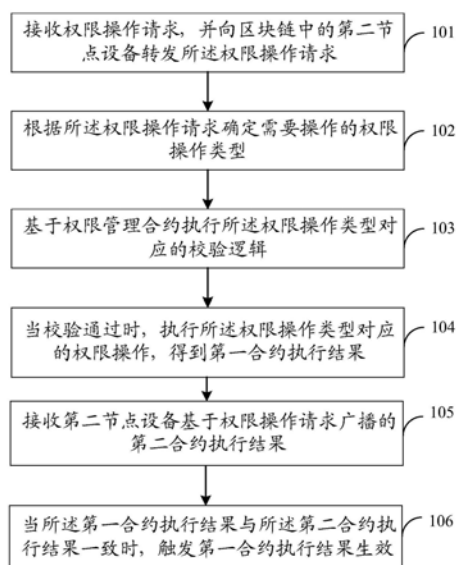
权利要求书2页 说明书21页 附图10页

(54)发明名称

一种权限验证方法、装置和存储介质

(57)摘要

本发明实施例公开了一种权限验证方法、装置和存储介质;本发明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;根据权限操作请求确定需要操作的权限操作类型,权限操作类型为用户权限验证;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,确定用户权限验证通过。该方案可以提升数据的安全性。



1. 一种权限验证方法,其特征在于,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;
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;
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。
2. 如权利要求1所述的权限验证方法,其特征在于,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。
3. 如权利要求2所述的权限验证方法,其特征在于,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,包括:
基于所述权限管理合约对调用参数、请求发起用户的功能权限以及签名中的至少一种进行验证;
当验证通过时,确定请求发起用户的操作合法。
4. 如权利要求2所述的权限验证方法,其特征在于,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,包括:
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。
5. 如权利要求3所述的权限验证方法,其特征在于,基于所述权限管理合约对请求发起用户的功能权限进行验证,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所有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请求发起用户所需执行的功能时,确定功能权限验证通过。
6. 如权利要求5所述的权限验证方法,其特征在于,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:
遍历角色令牌集合;
查询所述角色令牌集合内当前角色对应的功能权限;
确定当前角色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,则确定角色令牌集合是否遍历完;若角色令牌集合未遍历完,则返回执行查询角色令牌集合内当前角色对应的功能权限的步骤。

7.如权利要求6所述的权限验证方法,其特征在于,当所述角色令牌集合中所有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,包括:

当角色令牌集合遍历完时,确定所述角色令牌集合中所有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;

从区块链合约账本中获取请求发起用户的代理角色令牌集合。

8.如权利要求7所述的权限验证方法,其特征在于,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:

遍历所述代理角色令牌集合;

检查所述代理角色集合内当前代理角色的代理是否过期;

若没有过期,则查询所述代理角色集合内当前代理角色对应的功能权限;

确定当前代理角色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。

9.一种权限验证装置,其特征在于,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确定需要操作的权限操作类型;

校验单元,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,所述权限操作类型为用户权限验证;

操作单元,用于当校验通过时,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;

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。

10.一种存储介质,其特征在于,所述存储介质存储有多条指令,所述指令适于处理器进行加载,以执行权利要求1至8任一项所述的权限验证方法中的步骤。

一种权限验证方法、装置和存储介质

[0001] 本申请要求申请日为2019年3月28日、申请号为201910245109.4、发明名称为“一种权限管理方法、装置和存储介质”的专利申请的分案申请，该母案申请的全部内容通过引用结合在本申请中。

技术领域

[0002] 本发明涉及计算机技术领域，具体涉及一种权限管理、验证方法、装置和存储介质。

背景技术

[0003] 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。由于管理权限过于中心化，在系统中是非常不安全的，不可信任的，很有可能管理者会篡改权限去谋取不当的利益以及对整个系统进行破坏性攻击等，导致数据的安全性较差。

发明内容

[0004] 本发明实施例提供一种权限管理、验证方法、装置和存储介质，可以提升数据的安全性。

[0005] 本发明实施例还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：

[0006] 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；

[0007] 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；

[0008] 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；

[0009] 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；

[0010] 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；

[0011] 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。

[0012] 相应地，本发明实施例还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：

[0013] 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；

[0014] 确定单元，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；

[0015] 校验单元，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，所述权限操作类型为用户权限验证；

[0016] 操作单元，用于当校验通过时，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；

[0017] 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；

[0018] 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。

[0019] 在一实施例中,所述校验单元,包括:

[0020] 第一验证子单元,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;

[0021] 第二验证子单元,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。

[0022] 在一实施例中,第一验证子单元,用于:基于所述权限管理合约对调用参数、请求发起用户的功能权限以及签名中的至少一种进行验证;当验证通过时,确定请求发起用户的操作合法。

[0023] 在一实施例中,第一验证子单元,用于:

[0024] 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;

[0025] 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;

[0026] 当所述角色令牌集合中所有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;

[0027] 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。

[0028] 在一实施例中,第一验证子单元,用于:

[0029] 遍历角色令牌集合;

[0030] 查询所述角色令牌集合内当前角色对应的功能权限;

[0031] 确定当前角色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;

[0032] 若包含,则确定功能权限验证通过;

[0033] 若不包含,则确定角色令牌集合是否遍历完;若角色令牌集合未遍历完,则返回执行查询角色令牌集合内当前角色对应的功能权限的步骤。

[0034] 在一实施例中,第一验证子单元,用于:

[0035] 当角色令牌集合遍历完时,确定所述角色令牌集合中所有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;

[0036] 从区块链合约账本中获取请求发起用户的代理角色令牌集合。

[0037] 在一实施例中,第一验证子单元,用于:

[0038] 遍历所述代理角色令牌集合;

[0039] 检查所述代理角色集合内当前代理角色的代理是否过期;

[0040] 若没有过期,则查询所述代理角色集合内当前代理角色对应的功能权限;

[0041] 确定当前代理角色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;

[0042] 若包含,则确定功能权限验证通过。

[0043] 此外,本发明实施例还提供一种存储介质,所述存储介质存储有多条指令,所述指

令适于处理器进行加载,以执行本发明实施例提供的任一种权限管理方法、权限验证方法中的步骤。

[0044] 本发明实施例提供了由区块链中第一节点设备执行的权限验证方法,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确定需要操作的权限操作类型,所述权限操作类为权限验证;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;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。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。

附图说明

[0045] 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单地介绍,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,对于本领域技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0046] 图1a是本发明实施例提供的权限管理方法的场景示意图;

[0047] 图1b是本发明实施例提供的权限管理方法的流程图;

[0048] 图1c是本发明实施例提供的映射关系示意图;

[0049] 图2是本发明实施例提供的权限分配的流程示意图

[0050] 图3是本发明实施例提供的角色分配的流程示意图;

[0051] 图4是本发明实施例提供的权限移交的流程示意图;

[0052] 图5是本发明实施例提供的委托代理角色的流程示意图;

[0053] 图6是本发明实施例提供的撤回委托角色的流程示意图;

[0054] 图7是本发明实施例提供的用户功能权限验证的流程示意图;

[0055] 图8是本发明实施例提供的用户注册权限示意图;

[0056] 图9是本发明实施例提供的智能合约系统的架构示意图;

[0057] 图10a是本发明实施例提供的权限管理装置的结构示意图;

[0058] 图10b是本发明实施例提供的权限管理装置的另一结构示意图;

[0059] 图11是本发明实施例提供的网络设备的结构示意图。

具体实施方式

[0060] 下面将结合本发明实施例中的附图,对本发明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发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,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,都属于本发明保护的范围。

[0061] 在对本发明实施例进行详细地解释说明之前,先对本发明实施例涉及到的一些名词进行解释说明。

[0062] 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。

[0063] 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。

[0064] 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。

[0065] 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P2P(点对点)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。

[0066] 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。

[0067] 接下将介绍本发明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。

[0068] 参考图1a,本发明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。

[0069] 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。

[0070] 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。

[0071] 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。

[0072] 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,该节点设备可以为服务器等网络设备。

[0073] 本发明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1b所示,该权限管理方法的具体流程可以如下:

[0074] 101、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。

[0075] 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。

[0076] 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。

[0077] 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。本发明实施例中,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。

[0078] 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。

[0079] 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。

[0080] 102、根据权限操作请求确定需要操作的权限操作类型。

[0081] 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)。

[0082] 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。

[0083] 本发明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,以确定权利类型。

[0084] 103、基于权限管理合约执行权限操作类型对应的校验逻辑。

[0085] 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。

[0086] 本发明实施例中,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。

[0087] 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1c所示,为用户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。

[0088] 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。

[0089] 本发明实施例中, 权限管理合约还可以包括权限操作类型对应的校验逻辑, 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'。

[0090] 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: 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, 步骤“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:

[0091] (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。

[0092] 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。

[0093] 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调用参数、请求发起用户的功能权限以及签名中的至少一种进行验证; 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。譬如, 可以包括如下方式:

[0094] (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。

[0095] 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。

[0096] 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。

[0097] 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:

[0098] 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;

[0099] 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;

[0100] 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;

[0101] 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。

[0102] (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。

[0103] 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),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。

[0104] 数字摘要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。

[0105] (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合法。

[0106] 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。

[0107] (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。

[0108] 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。

[0109] 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:

[0110] (2.1)、权限操作类型包括权限分配:

[0111] 比如,管理员给用户的角色分配权限等。

[0112] 其中,操作对象可以包括待分配权限的角色,即待分配角色。

[0113] 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;

[0114] 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。

[0115] 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。

[0116] (2.2)、权限操作类型包括:角色分配;

[0117] 比如,管理员给用户分配角色。

[0118] 其中,操作对象可以包括待分配角色的用户,即待分配用户。

[0119] 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;

[0120] 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;

[0121] 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。

[0122] 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。

- [0123] (2.3)、权限操作类型包括:权限转移;
- [0124] 比如,管理员(Admin)将超级权限移交给新的管理员。
- [0125] 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。
- [0126] 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;
- [0127] 当待转移用户的身份合法时,确定权限信息验证通过。
- [0128] 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。
- [0129] (2.4)、权限操作类型包括:角色委托代理;
- [0130] 比如,用户委托其他用户临时或者在一定期限代理角色。
- [0131] 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。
- [0132] 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。
- [0133] 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。
- [0134] 也就说,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。
- [0135] (2.5)、权限操作类型包括:角色委托撤回;
- [0136] 比如,用户撤回委托给其他用户代理的角色。
- [0137] 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。
- [0138] 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。
- [0139] 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。
- [0140] (2.6)、权限操作类型包括:权限验证;
- [0141] 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。
- [0142] 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。
- [0143] 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;
- [0144] 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;
- [0145] 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待验证用户所代理的代理角色令牌集合;

[0146] 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。

[0147] 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。

[0148] 本实施例中,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。

[0149] 104、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。

[0150] 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。

[0151] 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。

[0152] 本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

[0153] 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。

[0154] 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。

[0155] 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。

[0156] 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。

[0157] 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。

[0158] 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

[0159] 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。

[0160] 105、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。

[0161] 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。

[0162] 本发明实施例中,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。

[0163] 106、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。

[0164] 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。

[0165] 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。

[0166] 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。

[0167] 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。

[0168] 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。

[0169] 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,并将可以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。

[0170] 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。

[0171] 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。

[0172] 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。

[0173] 本发明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。

[0174] 由上可知,本发明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。

[0175] 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:

[0176] 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2,具体流程如下:

[0177] 201、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。

[0178] 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。

[0179] 202、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。

[0180] 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。

[0181] 203、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,则执行步骤204,若否,则执行步骤208。

[0182] 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。

[0183] 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。

[0184] 204、第一节点设备验证校验发起者的签名是否合法,若合法,则执行步骤205,若否,则执行步骤208。

[0185] 具体地,当签名不合法则返回拒绝服务的合约执行结果。

[0186] 205、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。

[0187] 206、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,执行步骤207。

[0188] 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。

[0189] 207、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。

[0190] 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。

[0191] 208、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。

[0192] 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。

[0193] 209、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。

[0194] 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。

[0195] 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3,具体流程如下:

[0196] 301、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。

[0197] 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。

[0198] 302、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。

[0199] 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。

[0200] 303、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,则执行步骤304,若否,则执行步骤309。

[0201] 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。

[0202] 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。

[0203] 304、第一节点设备验证校验发起者的签名是否合法,若合法,则执行步骤205,若否,则执行步骤309。

[0204] 具体地,当签名不合法则返回拒绝服务的合约执行结果。

[0205] 305、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。

[0206] 306、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。

[0207] 307、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,若不包含执行步骤308,若包含执行步骤309。

[0208] 308、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。

[0209] 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。

[0210] 309、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。

[0211] 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。

[0212] 310、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。

[0213] 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。

[0214] 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:

[0215] 401、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。

[0216] 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。

[0217] 402、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。

[0218] 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。

[0219] 403、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,则执行步骤404,若否,则执行步骤407。

[0220] 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。

[0221] 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。

[0222] 404、第一节点设备验证校验发起者的签名是否合法,若合法,则执行步骤405,若否,则执行步骤407。

[0223] 具体地,当签名不合法则返回拒绝服务的合约执行结果,执行步骤407。

[0224] 405、第一节点设备检查传入的待转移用户ID是否合法,若是,执行步骤406,若否则执行步骤407。

[0225] 在一实施例中,当不合法时,返回拒绝服务的合约执行结果。

[0226] 406、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。

[0227] 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。

[0228] 407、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。

[0229] 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。

[0230] 408、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。

[0231] 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:

[0232] 501、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。

[0233] 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。

[0234] 502、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。

[0235] 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。

[0236] 503、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,则执行步骤504,若否,则执行步骤512。

- [0237] 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。
- [0238] 504、第一节点设备验证校验发起者的签名是否合法,若合法,则执行步骤505,若否,则执行步骤512。
- [0239] 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。
- [0240] 505、第一节点设备检查出入的委托ID是否合法,若是,执行步骤506,若否则执行步骤512。
- [0241] 在一实施例中,当不合法时,返回拒绝服务的合约执行结果,执行步骤512。
- [0242] 506、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,则执行步骤507,若否,执行步骤512。
- [0243] 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步骤512。
- [0244] 507、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,则执行步骤507,若是,执行步骤512。
- [0245] 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,并执行步骤512。
- [0246] 508、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。
- [0247] 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,并执行步骤512。
- [0248] 509、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。
- [0249] 510、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,则执行步骤511,若是,则执行步骤512。
- [0250] 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,并执行步骤512。
- [0251] 511、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。
- [0252] 512、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。
- [0253] 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。
- [0254] 513、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。
- [0255] 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。
- [0256] 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:
- [0257] 601、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。

[0258] 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。

[0259] 602、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。

[0260] 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。

[0261] 603、第一节点设备验证校验发起者的签名是否合法,若合法,则执行步骤604,若否,则执行步骤608。

[0262] 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,执行步骤608。

[0263] 604、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,执行步骤605,若否则执行步骤608。

[0264] 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,执行步骤608。

[0265] 605、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。

[0266] 606、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,若有执行步骤607,若没有执行步骤608。

[0267] 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,执行步骤608。

[0268] 607、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。

[0269] 608、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。

[0270] 609、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。

[0271] 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。

[0272] 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:

[0273] 701、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。

[0274] 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。

[0275] 702、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。

[0276] 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。

[0277] 703、第一节点设备验证校验发起者的签名是否合法,若合法,则执行步骤704,若否,则执行步骤715。

[0278] 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,执行步骤715。

[0279] 704、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。

- [0280] 705、第一节点设备遍历角色令牌集合。
- [0281] 706、第一节点设备查询合约账本获取集合内当前角色对应的功能权限。
- [0282] 707、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,执行步骤708,若是确定功能权限验证通过,执行步骤715。
- [0283] 708、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,返回执行步骤707,若是,则执行步骤709。
- [0284] 也即:第一节点设备对角色令牌集合中每一个角色,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。如果没有继续步骤708。
- [0285] 709、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。
- [0286] 710、第一节点设备遍历代理角色令牌集合。
- [0287] 711、第一节点设备检查代理角色集合内当前代理角色的代理是否过期,若否,则执行步骤712,若是执行步骤714。
- [0288] 712、第一节点设备查询合约账本获取代理角色集合内当前代理角色对应的功能权限。
- [0289] 713、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,执行步骤714,若是,则确定功能权限验证通过,执行步骤715。
- [0290] 714、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,返回执行步骤712,若是,则确定功能权限验证通过,执行步骤715。
- [0291] 715、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。
- [0292] 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。
- [0293] 716、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。
- [0294] 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。
- [0295] 本本发明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。
- [0296] 参考下表,为给角色的权限配置:

	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
[0297]	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
[0298]		和资产转让权限

[0299] 以注册权限为例，参考图8，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服务商代位注册的。详细注册权限如下如所示。

[0300] 参考图9，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。

[0301] 个人用户申请注册流程描述：

[0302] 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

[0303] 第二步：节点设备A,B,C,D广播检查结果

[0304] 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

[0305] 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。

[0306] 本发明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。

[0307] 为了更好地实施以上方法,相应的,本发明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,该节点设备可以为服务器等设备。

[0308] 例如,如图10a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、校验单元803、操作单元804、第二接收单元805以及触发单元806,如下:

[0309] 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;

[0310] 确定单元802,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;

[0311] 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;

[0312] 操作单元804,用于当校验通过时,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;

[0313] 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;

[0314] 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。

[0315] 在一实施例中,参考图10b,校验单元803,可以包括:

[0316] 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;

[0317] 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。

[0318] 在一实施例中,第一验证子单元8031,可以具体用于:

[0319] 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;

[0320] 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。

[0321] 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:

[0322] 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;

[0323] 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;

[0324] 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待分配角色对应的已分配功能权限集合中。

[0325] 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:

[0326] 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一个角色令牌;

[0327] 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;

[0328] 当所述角色令牌集合不包含所述待分配的角色令牌时,确定权限信息验证通过;

[0329] 操作单元804,用于当校验通过时,将待分配的角色令牌添加到所述待分配用户对应的角色令牌集合中。

[0330] 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：

- [0331] 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;
- [0332] 当待转移用户的身份合法时,确定权限信息验证通过;
- [0333] 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。
- [0334] 在一实施例中,第一验证子单元8031,可以具体用于:
- [0335] 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;
- [0336] 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。
- [0337] 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:
- [0338] 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;
- [0339] 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;
- [0340] 当检查到所述请求发起用户具有所述待委托角色、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;
- [0341] 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;
- [0342] 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。
- [0343] 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:
- [0344] 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;
- [0345] 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;
- [0346] 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的角色令牌。
- [0347] 在一实施例中,第一验证子单元8031,可以具体用于:
- [0348] 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;
- [0349] 当所述角色令牌集合中所有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;
- [0350] 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;
- [0351] 基于权限管理合约对请求发起用户的签名进行验证。
- [0352] 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。
- [0353] 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，因此，可以提升权限和数据的安全性。

[0354] 此外，本发明实施例还提供一种网络设备，如图11所示，其示出了本发明实施例所涉及的网络设备的结构示意图，具体来讲：

[0355] 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：

[0356] 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。

[0357] 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、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。

[0358] 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。

[0359] 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。

[0360] 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：

[0361] 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；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。

[0362] 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。

[0363] 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；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。

[0364] 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。

[0365] 为此，本发明实施例还提供一种存储介质，其中存储有多条指令，该指令能够被处理器进行加载，以执行本发明实施例所提供的任一种权限管理方法中的步骤。例如，该指令可以执行如下步骤：

[0366] 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；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。

[0367] 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。

[0368] 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。

[0369] 由于该存储介质中所存储的指令，可以执行本发明实施例所提供的任一种权限管理方法中的步骤，因此，可以实现本发明实施例所提供的任一种权限管理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。

[0370] 以上对本发明实施例所提供的一种权限管理方法、装置和存储介质进行了详细介绍，本文中应用了具体个例对本发明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发明的方法及其核心思想；同时，对于本领域的技术人员，依据本发明的思想，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本发明的限制。

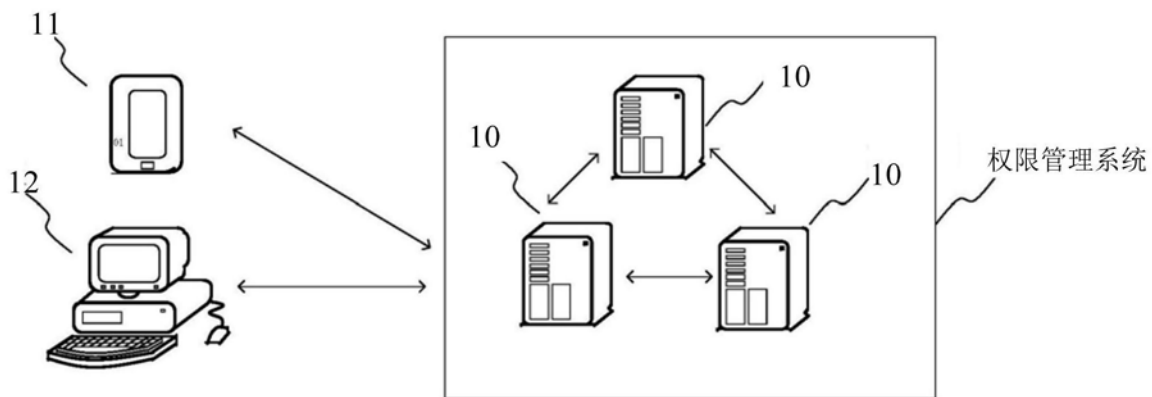


图1a

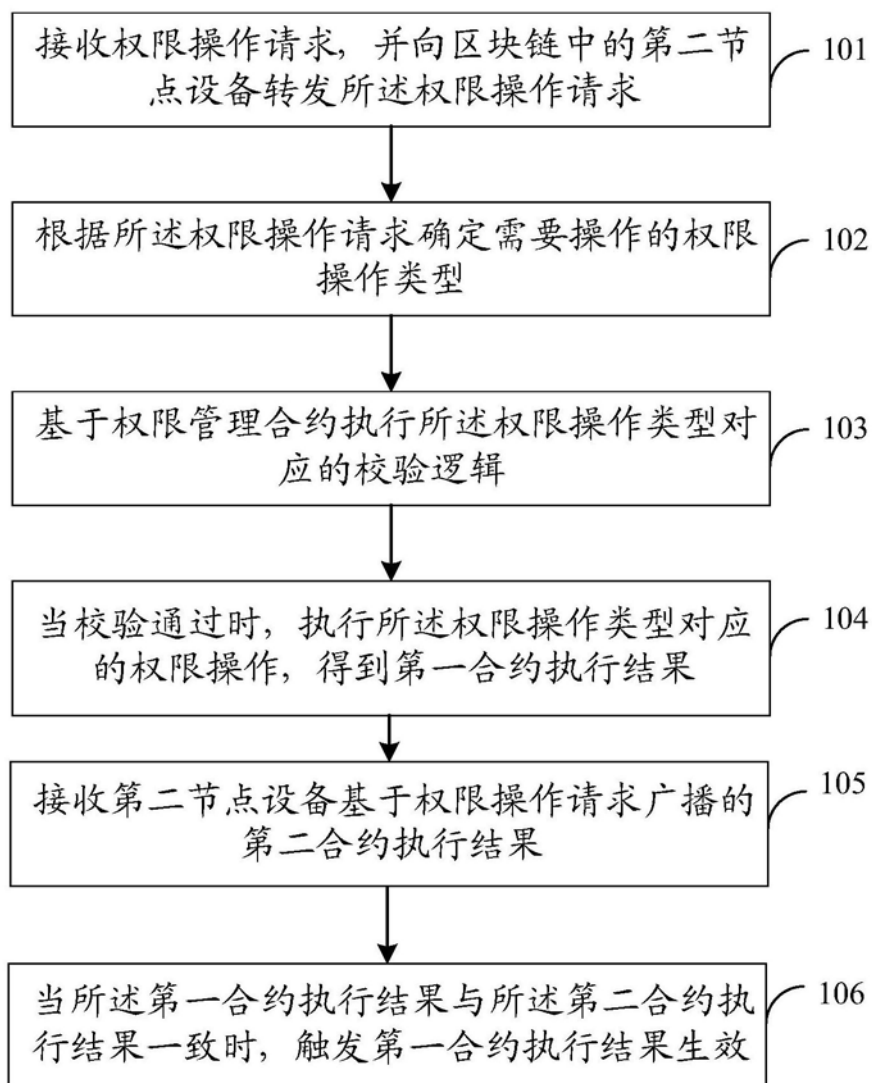


图1b

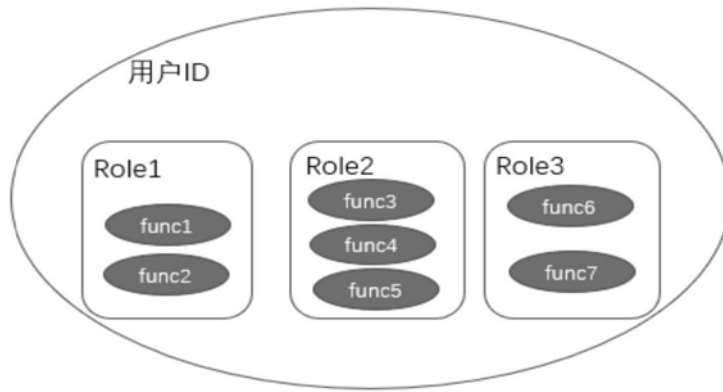


图1c

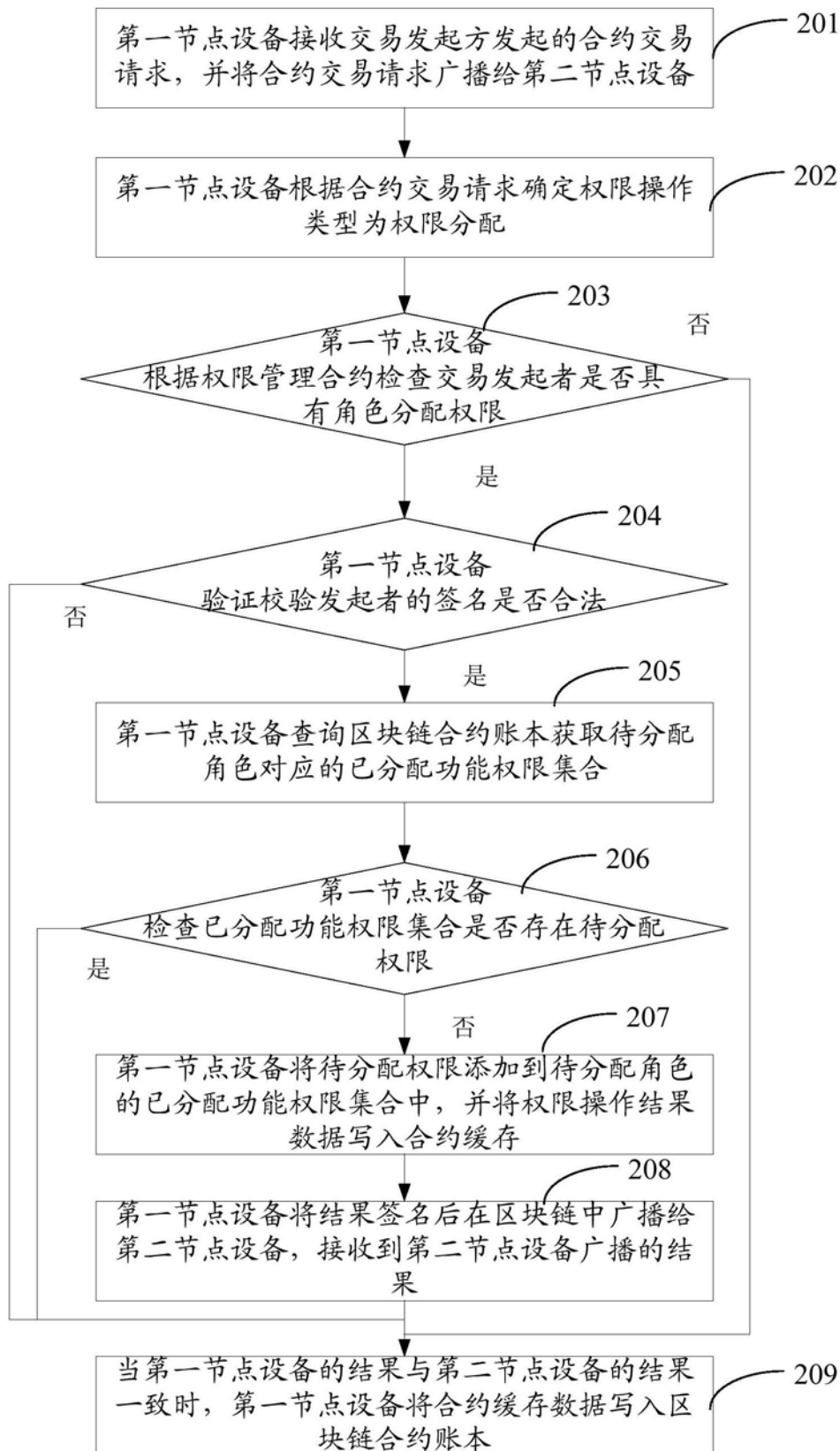


图2

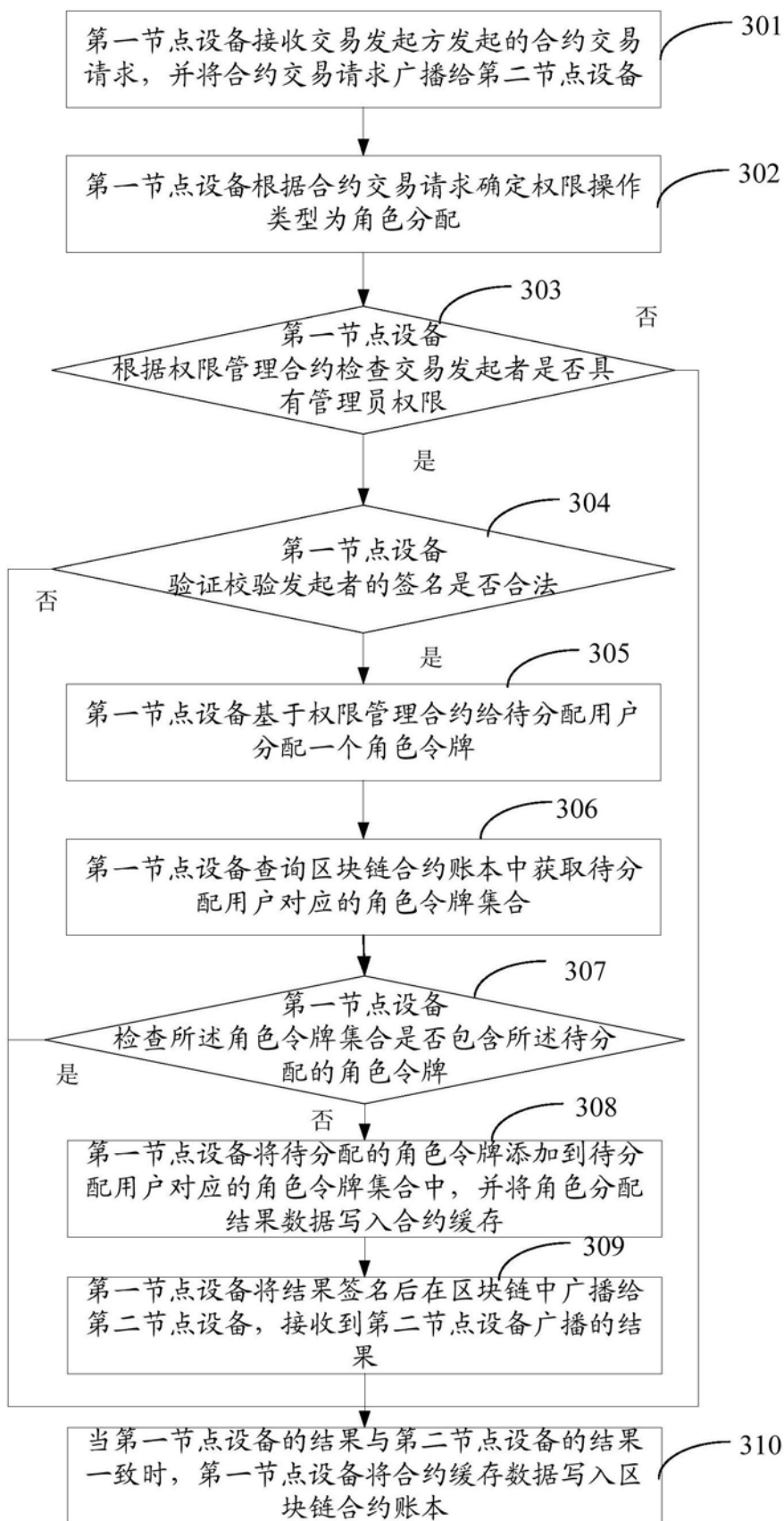


图3

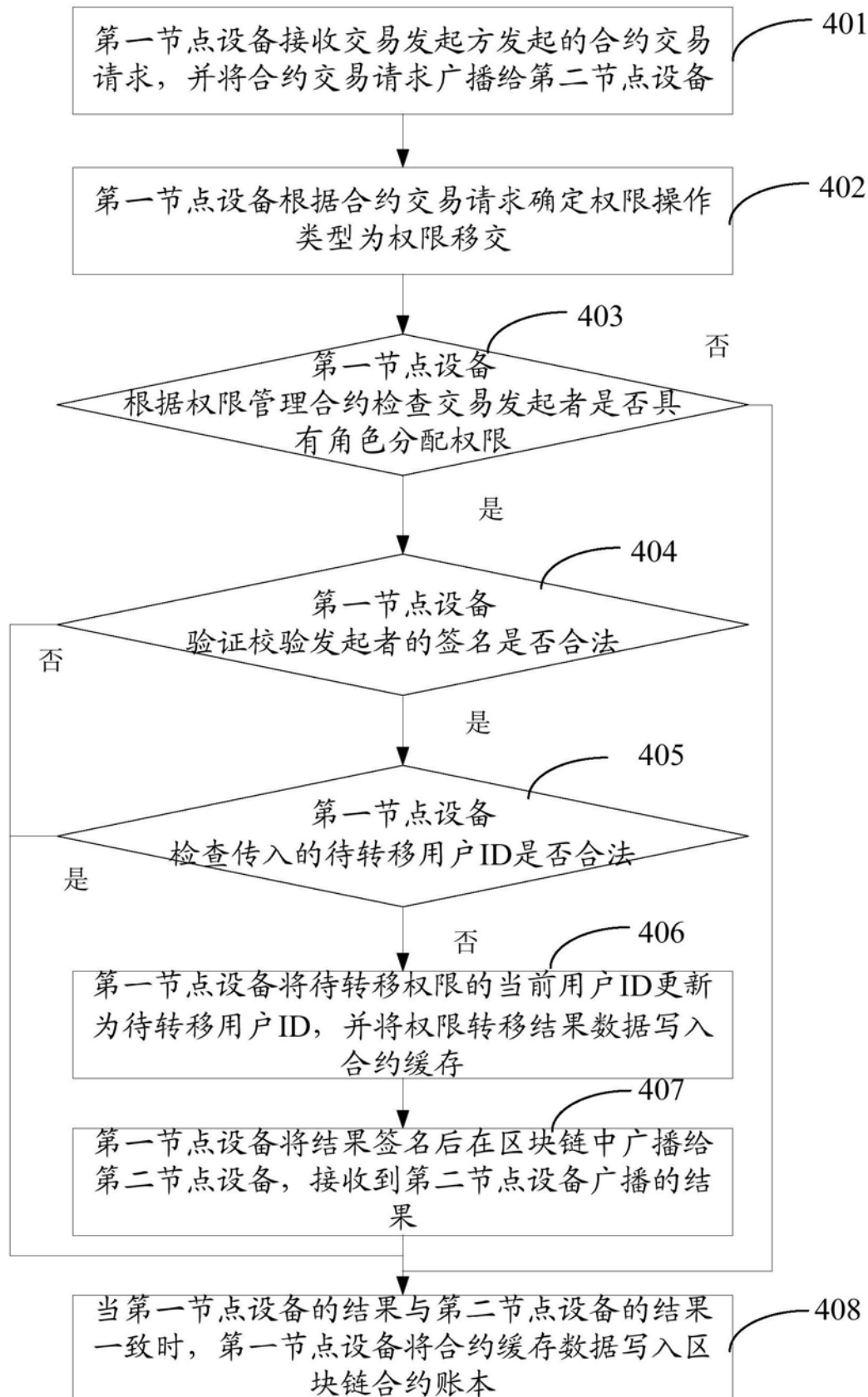


图4

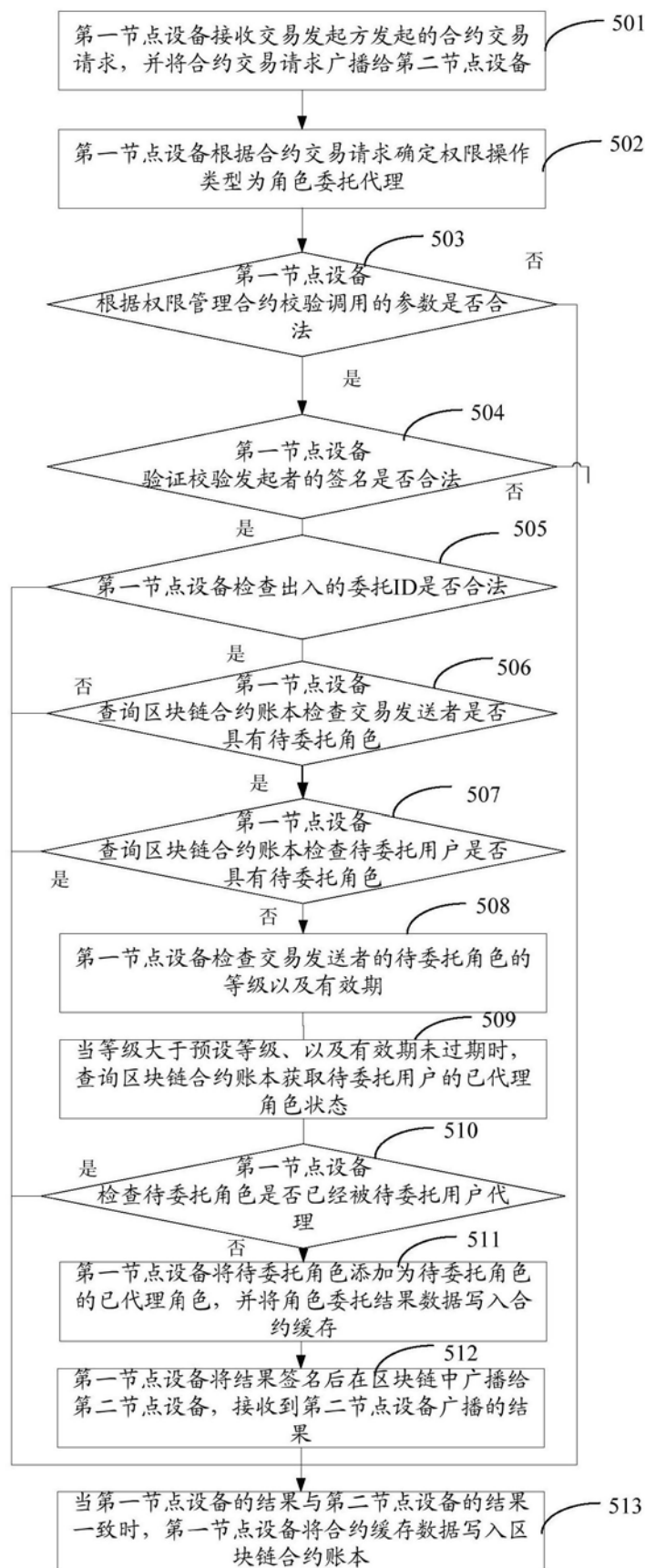


图5

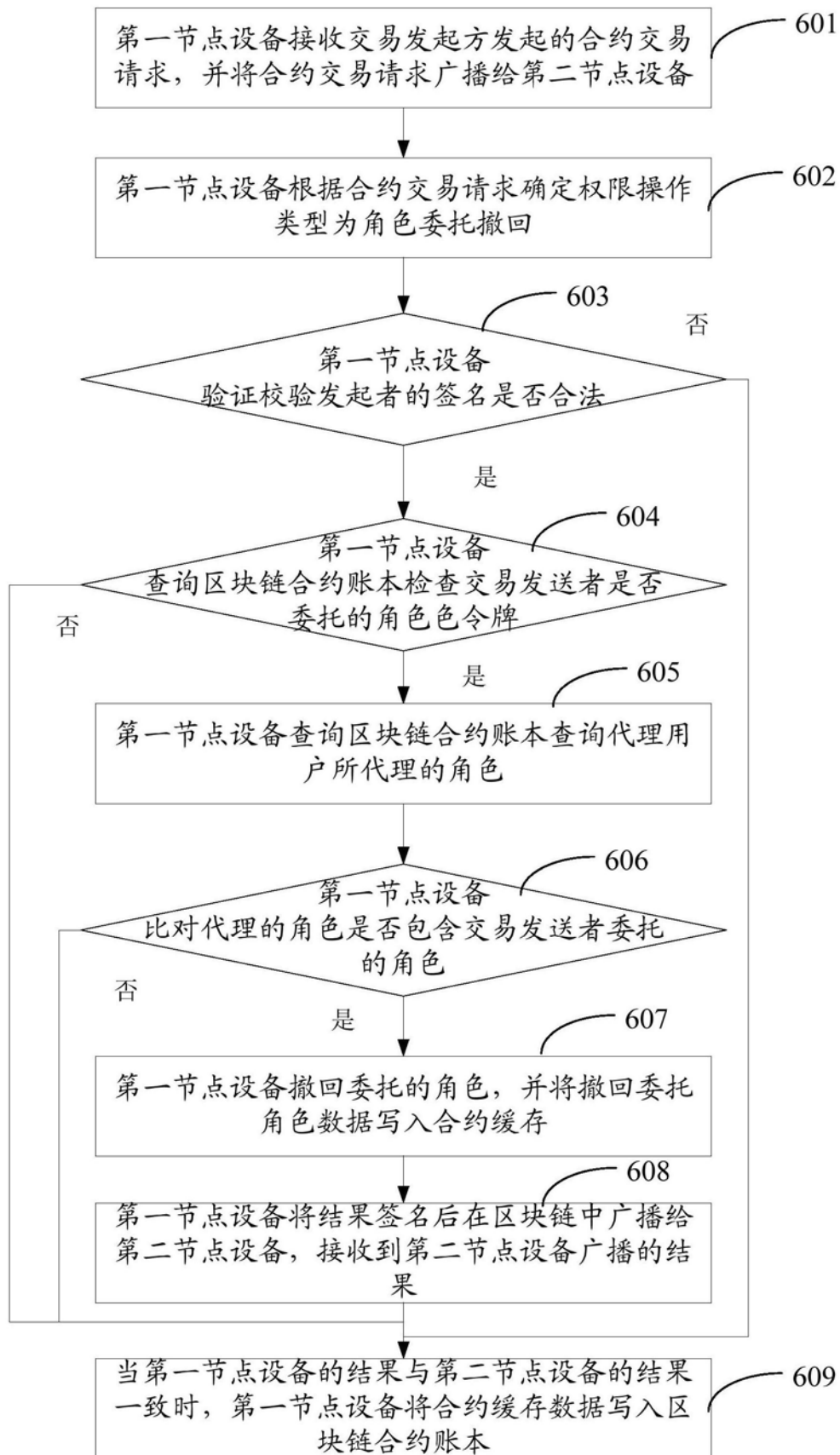


图6

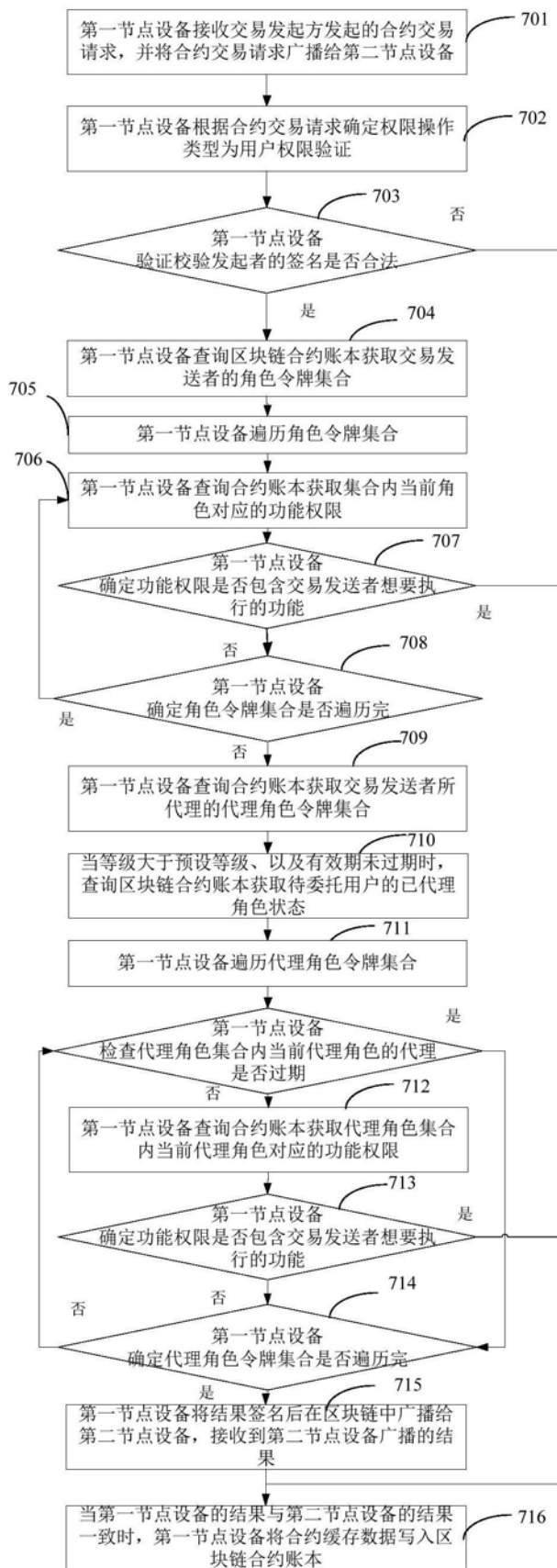


图7

	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

图8

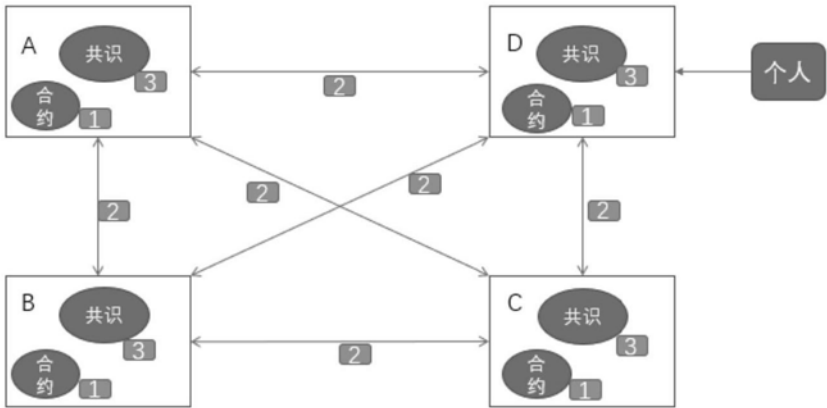


图9

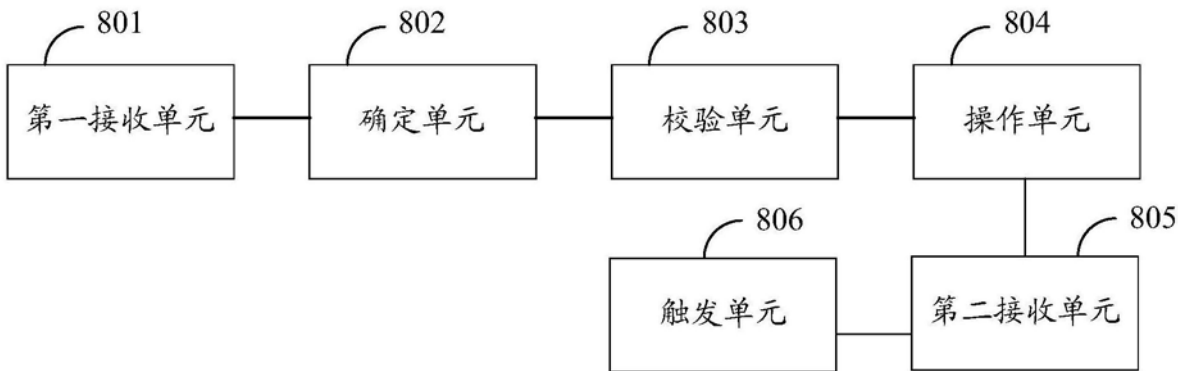


图10a

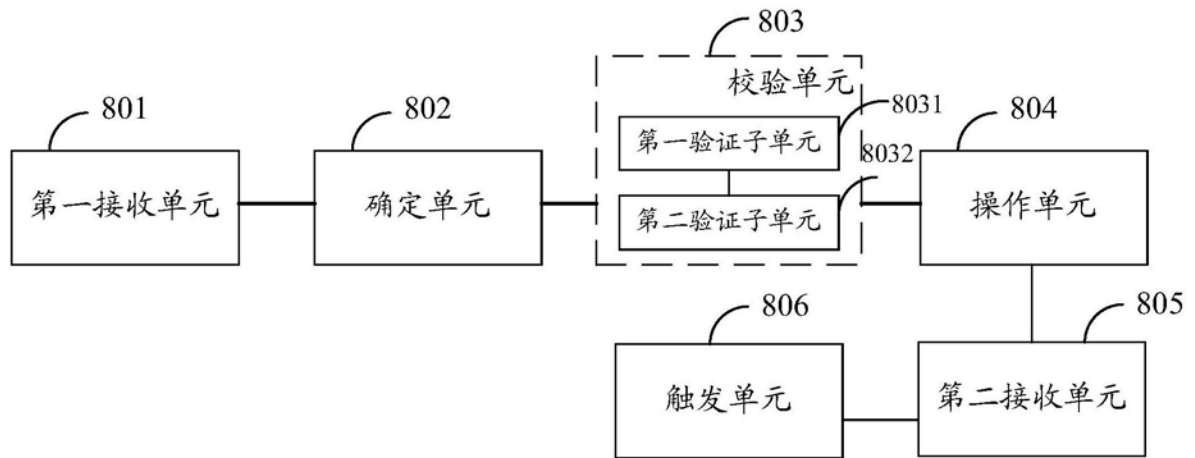


图10b

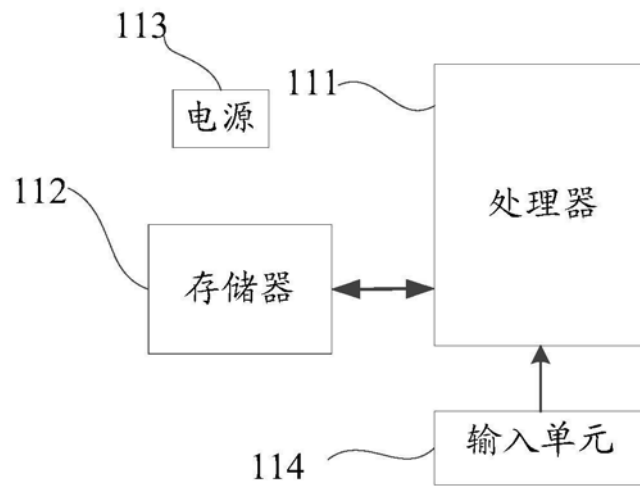


图11