(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110474865 A
(43)申请公布日 2019.11.19

(21)申请号 201810445990.8

(22)申请日 2018.05.11

(71)申请人 北京轻信科技有限公司
地址 100020 北京市朝阳区广顺南大街16号院2号楼12层1202

(72)发明人 周柳 吴玉会 陈磊

(74)专利代理机构 北京中济纬天专利代理有限公司 11429
代理人 覃婧婵

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

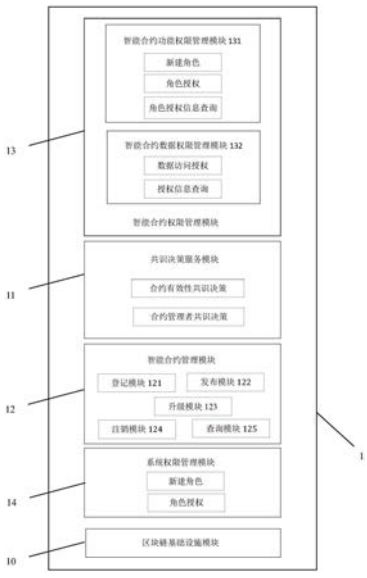
权利要求书2页 说明书6页 附图2页

(54)发明名称

区块链用户权限系统及实现方法

(57)摘要

为了解决现有技术存在的基于区块链技术的企业级应用中，如何搭建满足企业级应用需求的行业规则和标准数据的区块链用户访问权限管理的问题，本发明提出了一种基于不同区块链平台的区块链用户权限系统以及该系统中的权限实现方法，所述权限系统由区块链基础设施模块、共识决策服务模块、智能合约管理模块、智能合约权限管理模块和系统权限管理模块组成，通过上述模块搭建的系统利用共识机制确定智能合约的有效性，并选出新智能合约管理者，通过同时判定合约有效性和合约管理者任命有效性从而对智能合约的访问权限管理，最终达到区块链用户访问权限管理去中心化、高安全的目的。



CN 110474865 A

1.一种区块链用户权限系统,其特征在于:该系统由区块链基础设施模块、共识决策服务模块、智能合约管理模块、智能合约权限管理模块和系统权限管理模块组成,其中,

所述智能合约管理模块,用于管理智能合约的登记、发布、升级、注销和/或查询;

所述共识决策服务模块,用于对智能合约有效性,和智能合约管理者任命进行共识决策;

所述智能合约权限管理模块,用于管理授权区块链中的智能合约的访问权限;

所述系统权限管理模块,用于管理授权区块链用户对区块链用户权限系统的操作权限;

所述区块链基础设施模块,包含区块链基础设施。

2.如权利要求1所述的系统,其特征在于:优选的,所述智能合约管理模块进一步包括,

智能合约登记模块:用于登记所述智能合约的各种信息;

智能合约发布模块:用于申请发布所述智能合约;

智能合约升级模块:用于对所述智能合约进行升级操作;

智能合约注销模块:用于对所述智能合约进行注销操作;

智能合约查询模块:用于对所述智能合约进行查询操作。

3.如权利要求1所述的系统,其特征在于:所述智能合约权限管理模块需要查询智能合约是否为有效状态,以及智能合约管理权限授予的智能合约管理者是否有效,只有在两者全部都有效时,智能合约的访问权限才能被所述智能合约管理者授予客体。

4.如权利要求3所述的系统,其特征在于:所述智能合约权限管理模块进一步包括智能合约功能权限管理模块,和智能合约数据权限管理模块;其中智能合约功能权限管理模块对智能合约的函数信息进行控制和管理,而智能合约数据权限管理模块对智能合约的查询操作进行数据过滤操作。

5.如权利要求3所述的系统,在客体访问智能合约时,所述智能合约权限管理模块进一步校验所述客体是否对所述智能合约拥有新增和修改操作的权限或者当所述客体访问的是智能合约中加密的数据,所述智能合约权限管理模块在校验该客体拥有数据访问权限后,进一步对所述客体访问的加密数据进行解密操作。

6.如权利要求1所述的系统,其特征在于:

所述区块链基础设施模块包括一个跨区块链平台的网关,该网关集成当前主流的以太网Ethereum或者IBM超级账本HyperLedger或者区块链框架CITA区块链平台,并提供统一的RPC访问接口来访问不同区块链平台的方法。

7.一种区块链用户权限的实现方法,其特征在于:该方法包括以下步骤:

步骤1:选择区块链平台,部署区块链用户权限系统;

步骤2:发布人部署智能合约,并登记智能合约信息;

步骤3:发布人申请发布智能合约;

步骤4:对智能合约有效性和智能合约管理者的任命进行共识决策,并由共识决策设定的参与决策者决定共识决策是否通过;

步骤5:共识决策通过任命的智能合约管理者对用户授予访问权限。

8.如权利要求7所述的实现方法,其特征在于:

所述方法进一步包括步骤6:被授权用户获得权限,对智能合约进行访问、登记、发布、

升级、注销操作。

9.如权利要求8所述的实现方法，其特征在于：

所述对智能合约进行访问操作具体为，被授权用户根据授予的权限，对智能合约进行函数信息的访问，新增和/或修改操作，操作前智能合约中的函数先校验所述智能合约是否有效，然后再校验访问用户是否被智能合约管理者授权，只有校验都通过，才允许访问，新增和/或修改操作。

10.如权利要求9所述的实现方法，其特征在于：

所述对智能合约的访问操作进一步包括：当被授权用户访问智能合约的加密数据，在取出加密数据后，进一步校验被授权用户是否被智能合约管理者授权访问加密数据，如果校验通过，对访问数据进行解密，并明文显示。

11.如权利要求8所述的实现方法，其特征在于：

所述登记操作进一步包括：

步骤6.1：发布人在所述区块链用户权限系统中新建一智能合约；

步骤6.2：发布人提交智能合约信息，将智能合约信息保存到区块链，并将智能合约信息状态变为已登记状态。

12.如权利要求8所述的实现方法，其特征在于：

所述发布操作进一步包括：

步骤6.1：发布人在所述区块链用户权限系统中查询智能合约的状态，若此时智能合约状态是已登记，则申请发布智能合约、并选择推荐智能合约管理者；

步骤6.2：申请发布智能合约后，由参与决策者共识决策，在共识决策通过后，将智能合约状态修改为有效状态，并将智能合约的管理者信息更新为步骤1中推荐智能合约的管理者。

13.如权利要求8所述的实现方法，其特征在于：

所述升级操作进一步包括；

步骤6.1：智能合约管理者在所述区块链用户权限系统中查询原始智能合约，申请升级智能合约；

步骤6.2：若查询到的智能合约状态是有效状态，智能合约管理者需要经过参与决策者的共识决策，只有在共识决策通过后，才能升级智能合约。

14.如权利要求8所述的实现方法，其特征在于：

所述注销操作进一步包括；

步骤6.1：智能合约管理者在所述区块链用户权限系统中查询自己管理的智能合约，申请注销智能合约；

步骤6.2：若此时智能合约状态是有效状态，智能合约管理者需要经由参与决策者共识决策，在共识决策通过后，才能注销智能合约。

区块链用户权限系统及实现方法

技术领域

[0001] 本发明涉及计算机网络、计算机安全，计算机认证的技术领域，尤其涉及一种区块链用户权限系统及实现方法。

背景技术

[0002] 区块链原本是一项开发“比特币交易平台”的技术，用于记录虚拟资产的转移，后来被发展到其它技术领域作为底层技术支撑。

[0003] 随着区块链技术在各个行业的发展，为了不同行业的需求，也涌现出了多种区块链的平台，比如金融圈的R3，IBM为代表的超级账本HyperLedger，开源平台以太坊Ethereum以及比特币的Blockchain等。基于这些平台，目前国内外正加速区块链技术在行业应用中的落地。

[0004] 区块链技术在行业应用中的落地，本质是为了解决企业与企业之间的信任问题，让应用去中心化。当前市场上出现的基于区块链的行业应用，大部分都只是挖掘了区块链的数据存储价值，这在行业应用中想解决信任问题是远远不够的。行业应用领域的信任构建核心是行业规则和标准数据，而借助区块链技术能够让行业应用的参与者集体维护一个可靠的行业规则和标准数据，从而解决信任问题。

[0005] 区块链用户权限管理是区块链技术在行业领域实用化的核心内容。传统的权限管理技术可以分为功能访问控制和数据访问控制，这些访问控制技术都能很好地解决行业应用问题，但是存在一个核心问题“中心化”，即：中心化生产规则和数据、中心化授权规则和数据应用、中心化访问控制规则和数据。

[0006] 当前的区块链平台应用特性都是共识规则恒定、数据公开，访问公开。在基于区块链技术的联盟链企业级应用中，没有好的办法对规则和标准数据进行去中心化访问限制。

[0007] 现有技术中，发明CN105488431A区块链系统权限管理方法和装置公开的方法，主要根据用户注册信息生成以用户为根节点的权限树，通过权限树对用户的权限进行合法性判断。但该方法具有以下2个问题：

[0008] 1、该发明不是针对基于多个企业级应用的区块链智能合约权限管理应用。智能合约在区块链中是可以被公开访问的，该发明没有涉及针对不同企业级应用的不同智能合约的权限管理。

[0009] 2、该发明不涉及多个企业级应用的区块链智能合约发布、升级管理应用。

[0010] 发明CN107332847A一种基于区块链的访问控制方法和系统，主要提供一种基于投票的访问控制元数据管理机制，从而控制访问权限。但该方法具有以下问题：

[0011] 1、该发明是基于对传统关系型数据库在区块链上的映射应用，没涉及针对区块链新智能合约的共识发布、升级管理。

[0012] 2、该发明的管理员是一种中心化设计，没有涉及针对管理员的权限去中心化授予方法。

[0013] 3、该发明对智能合约的访问控制没有校验智能合约的有效性，如果是无效的智能

合约被访问影响后续的逻辑处理并将影响整个区块链应用的安全性。

[0014] 4、该发明对智能合约的数据访问权限没有做控制，智能合约数据在区块链上是公开的，任何客体在没有被授权的情况下都能够访问，如果数据不做加密处理将会泄露用户数据隐私。

发明内容

[0015] 为了解决上述现有技术中存在的如何在基于区块链技术的企业级应用中，搭建满足企业级应用需求的行业规则和标准数据的区块链用户访问权限管理的问题，本发明能够基于不同的区块链平台，创建一个区块链用户权限系统，用共识机制确定新智能合约的有效性，选出新智能合约管理者，并对新智能合约进行访问权限管理，最终达到区块链用户访问权限管理去中心化、高安全性的目的。

[0016] 本发明公开了一个区块链用户权限系统，具体地，该系统由区块链基础设施模块、共识决策服务模块、智能合约管理模块、智能合约权限管理模块和系统权限管理模块组成，其中，

[0017] 所述智能合约管理模块，用于管理智能合约的登记、发布、升级、注销和查询；

[0018] 所述共识决策服务模块，用于对智能合约有效性，和智能合约管理者进行共识决策；

[0019] 所述智能合约权限管理模块，用于管理授权区块链中的有效智能合约的访问权限；

[0020] 所述系统权限管理模块，用于管理区块链用户对区块链用户权限系统的功能操作权限；

[0021] 区块链基础设施模块10，包含区块链基础设施。

[0022] 此外，本发明还公开了一种区块链用户权限的实现方法，具体为：

[0023] 步骤1：选择区块链平台，部署区块链用户权限系统；

[0024] 步骤2：发布人部署智能合约，并登记智能合约信息；

[0025] 步骤3：发布人申请发布智能合约；

[0026] 步骤4：对智能合约的有效性和管理者的任命有效性进行共识决策并由共识决策设定的参与决策者决定共识决策是否通过；

[0027] 步骤5：步骤4中共识决策通过后任命的智能合约管理者对用户授予访问权限。

[0028] 与现有技术相比，本发明能够在多个不同的区块链平台、不同的企业级应用中去中心化发布智能合约、去中心化的管理智能合约、去中心化的授权用户访问智能合约。

附图说明

[0029] 图1为本发明中区块链用户权限系统的结构框架图；

[0030] 图2为本发明中区块链用户权限实现方法的方法流程图。

具体实施方式

[0031] 基于现有技术中存在的缺陷，本发明提出了一种新的区块链用户权限系统1，该系统由区块链基础设施模块10、共识决策服务模块11、智能合约管理模块12、智能合约权限管

理模块13、系统权限管理模块14组成。

[0032] 具体地，下面将结合附图1对本发明的区块链用户权限系统进行详细的描述。

[0033] 如图1所示，区块链用户权限系统1，由区块链基础设施模块10、共识决策服务模块11、智能合约管理模块12、智能合约权限管理模块13、和系统权限管理模块14组成。

[0034] 其中，所述智能合约管理模块12用于管理在企业级应用中智能合约的登记、发布、升级、注销和查询。具体地，智能合约管理模块12进一步包括，

[0035] 智能合约登记模块121：发布人可以利用该模块，登记智能合约的地址信息、函数信息和操作白皮书信息。

[0036] 智能合约发布模块122：若智能合约状态是已登记状态，发布人可利用该模块申请发布该智能合约，并由参与决策者共识决策，通过后，智能合约状态为有效状态，并更新该智能合约管理者的信息。

[0037] 智能合约升级模块123：智能合约管理者可以利用该模块对原始智能合约进行升级操作，更新成新的智能合约的地址信息、函数信息和操作白皮书信息。只有此时智能合约的状态是有效状态，智能合约管理者才可以升级该智能合约，并由参与决策者共识决策，通过后，原始智能合约状态为已失效状态，而升级的新智能合约状态为有效状态。

[0038] 智能合约注销模块124：智能合约管理者可以利用该模块对智能合约进行注销操作，注销智能合约时，需登记智能合约的注销原因和具体说明书。只有此时智能合约状态是有效状态时，智能合约管理者才可注销该智能合约，并由参与决策者共识决策，通过后，智能合约状态为注销状态。若智能合约状态已经是注销状态，则管理者无法进行注销操作。

[0039] 智能合约查询模块125：被授权的用户可以利用该模块对智能合约进行查询操作，具体地可以查询智能合约当前的状态信息、合约地址信息、合约函数信息、合约管理者信息、合约发布人信息、操作白皮书信息等。

[0040] 所述共识决策服务模块11用于对智能合约是否有效，以及智能合约管理者是谁进行共识决策，采用的方式可以为常用的方式，例如：投票方式。如果共识决策通过，则智能合约为有效状态，此时所述智能合约可以被应用到企业级应用中，并由共识决策通过指定的合约管理者进行管理访问授权。如果决策不通过，则所述智能合约不能被应用到企业级应用中。该共识决策服务模块11通过对智能合约有效性和合约管理者任命有效性同时进行决策的方式，极大提高了认证安全性以及实现了去中心化，并解决了现有技术中没有对智能合约进行有效性共识和管理者任命有效性共识的问题。

[0041] 智能合约权限管理模块13，用于管理授权区块链中的有效智能合约的访问权限。与现有技术相比，本发明中的智能合约的访问权限能否被授予客体，需要在智能合约管理模块12的智能合约查询模块125中查询智能合约是否为有效状态，以及智能合约管理权限授予的智能合约管理者是否有效，只有在两者全部都有效时，智能合约的访问权限才可以被智能合约管理者授予客体。

[0042] 进一步，智能合约的访问权限包括功能访问权限和数据访问权限。因此，智能合约权限管理模块13进一步包括智能合约功能权限管理模块131，和智能合约数据权限管理模块132。其中智能合约功能权限管理模块131，可以对智能合约的函数信息进行控制和管理，而智能合约数据权限管理模块132，可以对智能合约的查询操作进行数据过滤操作进而对数据访问进行控制和管理。

[0043] 进一步，在客体访问智能合约时，该模块13还会校验所述客体是否对所述智能合约拥有新增和修改操作的权限。若所述客体访问的是智能合约中加密的数据，该模块13还会在校验该客体拥有数据访问权限后，对所述客体访问的加密数据进行解密操作。

[0044] 系统权限管理模块14，主要用于授权区块链用户对区块链用户权限系统1的功能操作权限管理。具体而言，系统权限管理模块14，可以新建角色，对新建角色授权，对数据访问授权等。

[0045] 通过系统权限管理模块14，用户权限系统1给区块链地址新建发布人角色并给与授权，经授权的发布人通过用户权限系统1中智能合约管理模块12中的智能合约登记模块121登记智能合约并通过智能合约发布模块122申请发布智能合约。此外，用户权限系统1还可以通过系统权限管理模块14给区块链地址授予参与决策者角色，参与决策者通过共识决策服务模块11进行共识决策判断，最终由共识决策通过指定的智能合约管理者通过用户权限系统1的智能合约管理模块12参与智能合约的升级、注销等操作。

[0046] 区块链基础设施模块10，包含了区块链基础设施，具体地，可以是一个跨区块链平台的网关，该网关能够集成当前主流的Ethereum(以太坊)，或者新涌现的HyperLedger(美国IBM公司的超级账本)、CITA(杭州秘猿科技有限公司开发的区块链框架)等区块链平台，并提供统一的RPC访问接口来访问不同区块链平台的方法。

[0047] 本发明的区块链用户权限系统1，通过共识决策机制确定智能合约有效性，并选出智能合约的管理者，从而结合了智能合约有效性和智能合约管理者有效性的双重有效性判定，管理智能合约的访问权限，实现了区块链用户访问权限管理去中心化、高安全的目的。

[0048] 此外，本发明还公开了一种区块链用户权限的实现方法，下面将结合附图2对本方法进行详细的描述。

[0049] 一种区块链用户权限的实现方法，具体地，该方法包括以下步骤：

[0050] 步骤1：选择区块链平台，如以太坊的Ethereum、IBM的HyperLedger等，借助区块链网关系统，部署区块链用户权限系统；

[0051] 步骤2：发布人部署智能合约，并登记智能合约信息，具体地，登记的信息包括但不限于区块链地址信息、智能合约函数方法信息、以及智能合约操作白皮书等信息；

[0052] 步骤3：发布人申请发布智能合约。具体地，通过设定共识规则，例如选择投票的方式，选择区块链上某一个应用，设定共识范围的参与决策者，完成后提交申请发布。

[0053] 步骤4：对步骤3中的智能合约的有效性和管理者的任命进行共识决策，由共识决策设定的参与决策者决定共识决策是否通过。具体地，参与决策者是区块链的节点验证人，由系统权限管理模块进行角色授权，并由共识决策智能合约统一管理。参与决策者在区块链平台以投票或者其他方式，决策智能合约的有效性并任命智能合约管理者。如果通过，智能合约将被应用到企业级应用中，并由指定的智能合约管理者进行访问权限管理。通过后，智能合约的状态将变成有效状态，并且智能合约的管理者信息被更新。如果不通过，智能合约将不能被应用到企业级应用中。

[0054] 步骤5：步骤4中共识决策任命的智能合约管理者对用户授予访问权限。具体地，所述智能合约管理者可以为区块链某一应用的区块链用户授权智能合约的功能访问权限，也可以为其他区块链的用户授予在此智能合约存储的隐私数据的数据访问权限。

[0055] 进一步的，被授权用户获得权限，访问智能合约。具体地，被授权用户根据授予的

权限，可以对智能合约进行函数信息的新增、修改操作，若进行上述操作，智能合约中的函数首先会校验该智能合约是否有效，然后再校验访问用户是否被智能合约管理者授权，如果校验都通过，则访问成功。被授权用户访问智能合约的加密数据，在取出加密数据后，进一步校验被授权用户是否被智能合约管理者授权访问加密数据，如果校验通过，对访问数据进行解密，并明文显示。

[0056] 进一步地，被授权用户被智能合约管理者授予权限，则被授权用户可以对智能合约进行登记、发布、升级、注销等操作。

[0057] 具体地，在一实施例中，智能合约的登记方法，具体为：

[0058] 步骤1：发布人在所述区块链用户权限系统中新建一智能合约。具体地，在新建智能合约时，填写智能合约的详细信息，包括但不限于区块链地址信息、智能合约函数方法信息、智能合约操作白皮书等信息。

[0059] 步骤2：发布人提交智能合约信息，将智能合约信息保存到区块链，并将智能合约信息状态变为已登记状态；

[0060] 若步骤2的已登记状态修改成功，发布人在所述系统中可查询到上述已登记的智能合约信息。

[0061] 在另一实施例中，智能合约的发布方法，具体为：

[0062] 步骤1：发布人在所述区块链用户权限系统中查询智能合约的状态，若此时智能合约状态是已登记，则申请发布智能合约、并选择推荐智能合约管理者，一般情况下，可以是推荐发布人作为智能合约管理者，若智能合约状态不是已登记状态，则无法进行智能合约发布操作，系统会提醒发布人该合约为未登记状态；

[0063] 步骤2：申请发布智能合约后，由参与决策者共识决策，在共识决策通过后，将智能合约状态修改为有效状态，并将智能合约的管理者信息更新为步骤1中推荐智能合约的管理者。

[0064] 在另一实施例中，智能合约的升级方法，具体为：

[0065] 步骤1：智能合约管理者在所述区块链用户权限系统中查询原始智能合约，申请升级智能合约。

[0066] 步骤2：若查询到的智能合约状态是有效状态，智能合约管理者需要经过参与决策者的共识决策，只有在共识决策通过后，才能升级智能合约，升级成功后，原智能合约状态为失效，升级的新智能合约为有效。升级成功后，智能合约的地址信息、函数信息和操作白皮书信息将被更新为新的升级后的智能合约的信息。

[0067] 在另一实施例中，智能合约的注销方法，具体为：

[0068] 步骤1：智能合约管理者在所述区块链用户权限系统中查询自己管理的智能合约，申请注销智能合约，申请时，需登记智能合约注销原因和具体说明书。

[0069] 步骤2：若此时智能合约状态是有效状态，智能合约管理者需要经由参与决策者共识决策，在共识决策通过后，才能注销智能合约，注销成功后，智能合约状态为注销状态，管理者将无法操作已注销的智能合约。

[0070] 本发明提出的区块链用户权限系统及实现方法，通过共识机制确定智能合约的有效性，选出智能合约管理者，并对新智能合约进行访问权限管理，从而达到区块链用户访问权限管理去中心化、高安全的目的。在不脱离本发明的精神和范围内的修改和完善，均应包

含在上述的权利要求范围内。

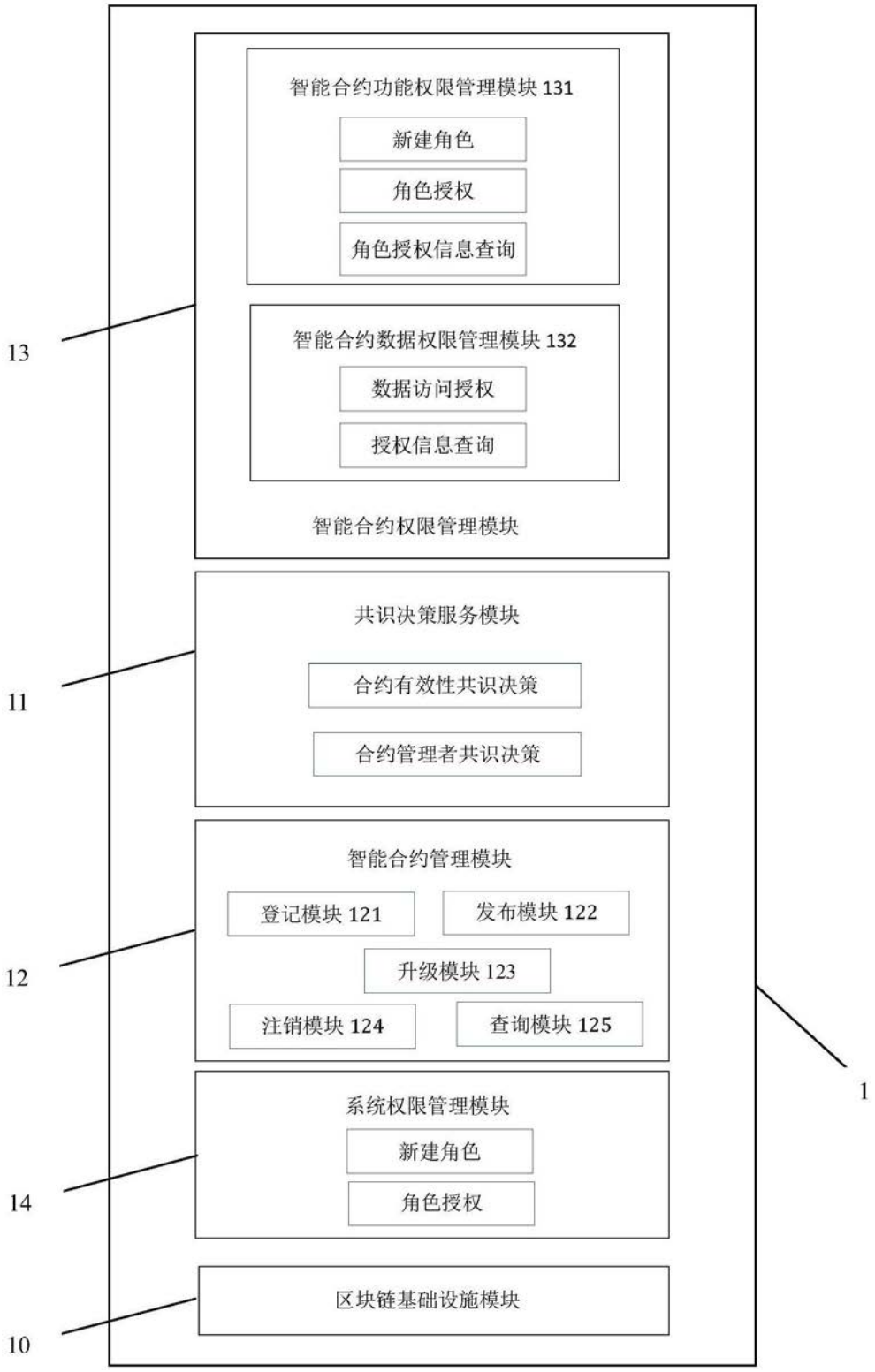

智能合约功能权限管理模块 131
新建角色
角色授权
角色授权信息查询
智能合约数据权限管理模块 132
数据访问授权
授权信息查询
智能合约权限管理模块
13
共识决策服务模块
合约有效性共识决策
合约管理者共识决策
11
智能合约管理模块
登记模块 121
发布模块 122
升级模块 123
注销模块 124
查询模块 125
12
系统权限管理模块
新建角色
角色授权
14
区块链基础设施模块
10
1

图1

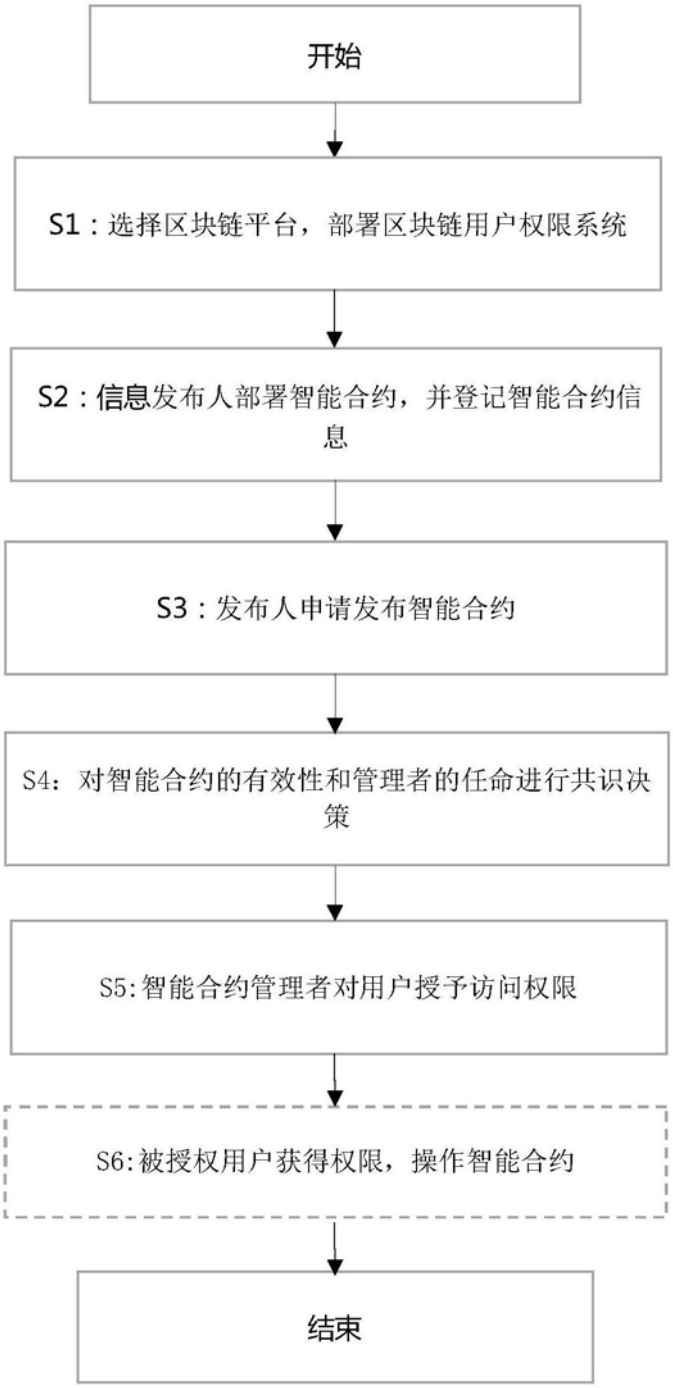

开始
S1：选择区块链平台，部署区块链用户权限系统
S2：信息发布人部署智能合约，并登记智能合约信息
S3：发布人申请发布智能合约
S4：对智能合约的有效性和管理者的任命进行共识决策
S5:智能合约管理者对用户授予访问权限
S6:被授权用户获得权限，操作智能合约
结束

图2