(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 107332847 A
(43)申请公布日 2017.11.07

(21)申请号 201710540062.5

(22)申请日 2017.07.05

(71)申请人 武汉凤链科技有限公司
地址 430000 湖北省武汉市硚口区园博园南路9号汉江湾四号楼

(72)发明人 金海 代炜琦 邹德清 王晨龙 刘钟泽 柴芳百

(74)专利代理机构 武汉臻诚专利代理事务所（普通合伙）42233
代理人 宋业斌

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

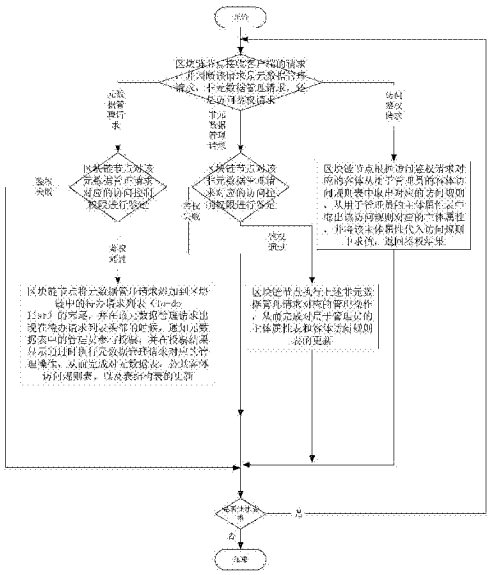
权利要求书2页 说明书5页 附图1页

(54)发明名称

一种基于区块链的访问控制方法和系统

(57)摘要

本发明公开了一种基于区块链的访问控制方法，包括：在区块链上抽象出一个关系型数据库，为访问控制策略的实现提供技术基础，使访问控制信息在区块链上的存储更加高效、便捷；提出了一种基于ABAC并且适合在区块链上用智能合约实现的访问控制模型；提出了一种基于投票的访问控制元数据管理机制，保障了访问控制绝对严格；提供了方便被其他智能合约调用的接口，使得其他合约简单实现自己的访问控制模型；具体包括联盟、机构管理员、访问主体、访问客体、初始化模块、投票模块、主客体管理模块、规则求值模块、表结构元数据管理模块、表数据管理模块。本发明为解决智能合约的访问控制问题提供了安全可靠的框架，在提高安全性的同时降低了开发成本。



CN 107332847 A

1.一种基于区块链的访问控制方法,其特征在于,包括以下步骤:

(1)区块链节点接收来自于客户端的请求,并判断该请求是元数据管理请求,非元数据管理请求,还是访问鉴权请求,如果是元数据管理请求,则转入步骤(2),如果是非元数据管理请求,则转入步骤(4),如果是访问鉴权请求,则转入步骤(6);

(2)区块链节点对该元数据管理请求对应的访问控制权限进行鉴定,如果鉴定通过,则转入步骤(3),否则过程结束;

(3)区块链节点将元数据管理请求添加到区块链中的待办请求列表的末尾,并在该元数据管理请求出现在待办请求列表头部的时候,通知元数据表中的管理员参与投票,并在投票结果显示通过时执行元数据管理请求对应的管理操作,从而完成对元数据表、公共客体访问规则表、以及表结构表的更新;

(4)区块链节点对该非元数据管理请求对应的访问控制权限进行鉴定,如果鉴定通过,则转入步骤(5),否则过程结束;

(5)区块链节点执行上述非元数据管理请求对应的管理操作,从而完成对用于管理员的主体属性表和客体访问规则表的更新;

(6)区块链节点根据访问鉴权请求对应的客体从用于管理员的客体访问规则表中取出对应的访问规则,从用于管理员的主体属性表中取出该访问规则对应的主体属性,并将该主体属性代入访问规则中求值,返回鉴权结果。

2.根据权利要求1所述的访问控制方法,其特征在于,进一步包括在步骤(1)之前初始化的操作,即建立表结构表、元数据表、公共客体访问规则表、用于管理员的主体属性表和客体访问规则表,其中表结构表中反映了表类型、表名称、属性名称、属性类型、属性默认值、是否主键之间的映射关系,元数据表中反映了管理员标识符、管理员公钥、表名称以及表类型之间的映射关系,公共客体访问规则表中反映了客体名称和访问规则之间的映射关系,用于管理员的主体属性表反映了主体名称与主体安全属性之间的映射关系,用于管理员的客体访问规则表中反映了客体名称与客体访问规则之间的映射关系。

3.根据权利要求2所述的访问控制方法,其特征在于,表结构表的建立过程是将表类型、表名称作为键值对中的键,将属性名称、属性类型、属性默认值、是否主键作为键值对中的值存入区块链的键值对数据库中,存入之前检查该键对应的数据是否存在,如果不存在则存入该数据,如果存在则结束该条数据的存入过程。其对应的映射关系如下:

[表类型][表名]→[属性名称][属性类型][属性默认值][主键]。

4.根据权利要求2所述的访问控制方法,其特征在于,元数据表的建立过程是将表类型、表名称、管理员标识符作为键值对中的键,将表中所有数据作为键值对中的值存入到区块链的键值对数据库中,在插入每条数据之前检查数据中每个项与表结构表中元数据表中对应的属性类型是否匹配,检查插入数据是否已在表中存在,如果匹配且不存在,则允许插入,否则拒绝该数据的插入,格式如下所示:

[表类型][表名称][管理员标识符]→[管理员标识符][管理员公钥][表类型][表名称]。

5.根据权利要求2所述的访问控制方法,其特征在于,公共客体访问规则表、用于管理员的主体属性表和客体访问规则表的建立过程是插入数据之前检查数据中每个项与表结构表中元数据表中对应的属性类型是否匹配,检查插入数据是否已在表中存在,如果匹配

且不存在，则允许插入，否则拒绝该数据的插入，格式如下所示：

[表类型][表名][主键属性值]→[所有属性值]。

6.根据权利要求1所述的访问控制方法，其特征在于，步骤(2)具体包括以下子步骤：

(2-1)区块链节点根据元数据管理请求中的管理员标识符、请求操作表类型、请求操作表名称在元数据表中是否存，如果存在，转入步骤(2-2)，否则表示管理员鉴权失败，过程结束；

(2-2)区块链节点根据元数据表中管理员的公钥并使用非对称加密算法验证元数据管理请求中的签名信息的是否合法，如果合法，表示管理员鉴权通过，否则表示管理员鉴权失败，过程结束。

7.根据权利要求1所述的访问控制方法，其特征在于，步骤(4)具体包括以下子步骤：

(4-1)区块链节点根据非元数据管理请求中的管理员标识符、请求操作表类型、请求操作表名称在元数据表中是否存在，如果存在，转入步骤(4-2)，否则表示管理员鉴权失败，过程结束；

(4-2)区块链节点根据元数据表中管理员的公钥并使用非对称加密算法验证非元数据管理请求中的签名信息的是否合法，如果合法，表示管理员鉴权通过，否则表示管理员鉴权失败，过程结束。

8.一种基于区块链的访问控制系统，其设置于区块链节点中，其特征在于，包括：

第一模块，用于接收来自于客户端的请求，并判断该请求是元数据管理请求，非元数据管理请求，还是访问鉴权请求，如果是元数据管理请求，则转入第二模块，如果是非元数据管理请求，则转入第四模块，如果是访问鉴权请求，则转入第六模块；

第二模块，用于对该元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入第三模块，否则过程结束；

第三模块，用于将元数据管理请求添加到区块链中的待办请求列表的末尾，并在该元数据管理请求出现在待办请求列表头部的时候，通知元数据表中的管理员参与投票，并在投票结果显示通过时执行元数据管理请求对应的管理操作，从而完成对元数据表、公共客体访问规则表、以及表结构表的更新；

第四模块，用于对该非元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入第五模块，否则过程结束；

第五模块，用于执行上述非元数据管理请求对应的管理操作，从而完成对用于管理员的主体属性表和客体访问规则表的更新；

第六模块，用于根据访问鉴权请求对应的客体从用于管理员的客体访问规则表中取出对应的访问规则，从用于管理员的主体属性表中取出该访问规则对应的主体属性，并将该主体属性代入访问规则中求值，返回鉴权结果。

一种基于区块链的访问控制方法和系统

技术领域

[0001] 本发明属于计算机应用软件领域，更具体地，涉及一种基于区块链的访问控制方法和系统。

背景技术

[0002] 近来兴起的区块链(Blockchain)和在其上运行的智能合约(Smartcontract)技术在金融、大数据、物联网、教育、公益等众多领域掀起了一轮颠覆性的革命。

[0003] 其中智能合约的本质是运行在区块链上的一段可执行代码，它的执行是由链上的所有节点共同见证的，因此一旦合约开始执行，它就会按照预定的流程进行，没有人能够试图抵赖或者恶意地影响合约的执行结果。其优点是公正公开，不可篡改，可审计，可追溯，不可抵赖，计算结果安全可信。然而，目前的智能合约存在如下不足：

[0004] (1)目前区块链平台基本没有智能合约的访问控制模块，智能合约被公开而不可更改地存储在区块链上，没有访问控制权限的主体可以随意调用其中的任何方法；

[0005] (2)每编写一个新的智能合约需要从头到尾实现访问控制，开发成本高且不能在不同合约之间复用；

[0006] (3)区块链平台的文件系统或相应的键值对状态数据库不适合对访问控制规则等数据的存储和管理；

[0007] (4)区块链中没有集中化的访问控制元数据管理方法(对管理员权限等的管理)，多管理员对元数据的修改较难达成一致。

发明内容

[0008] 针对现有技术的以上缺陷或改进需求，本发明提供了一种基于区块链的访问控制方法和系统，其目的在于，解决现有区块链中存在的没有访问控制权限的主体随意调用智能合约中的方法、智能合约之间不能复用访问控制方法、区块链的存储模式不方便对访问控制规则数据的管理以及多管理员对访问控制元数据的修改难达成一致的问题。

[0009] 为实现上述目的，按照本发明的一个方面，提供了一种基于区块链的访问控制方法，包括以下步骤：

[0010] (1)区块链节点接收来自于客户端的请求，并判断该请求是元数据管理请求，非元数据管理请求，还是访问鉴权请求，如果是元数据管理请求，则转入步骤(2)，如果是非元数据管理请求，则转入步骤(4)，如果是访问鉴权请求，则转入步骤(6)；

[0011] (2)区块链节点对该元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入步骤(3)，否则过程结束；

[0012] (3)区块链节点将元数据管理请求添加到区块链中的待办请求列表的末尾，并在该元数据管理请求出现在待办请求列表头部的时候，通知元数据表中的管理员参与投票，并在投票结果显示通过时执行元数据管理请求对应的管理操作，从而完成对元数据表、公共客体访问规则表、以及表结构表的更新；

[0013] (4)区块链节点对该非元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入步骤(5)，否则过程结束；

[0014] (5)区块链节点执行上述非元数据管理请求对应的管理操作，从而完成对用于管理员的主体属性表和客体访问规则表的更新；

[0015] (6)区块链节点根据访问鉴权请求对应的客体从用于管理员的客体访问规则表中取出对应的访问规则，从用于管理员的主体属性表中取出该访问规则对应的主体属性，并将该主体属性代入访问规则中求值，返回鉴权结果。

[0016] 优选地，该方法进一步包括在步骤(1)之前初始化的操作，即建立表结构表、元数据表、公共客体访问规则表、用于管理员的主体属性表和客体访问规则表，其中表结构表中反映了表类型、表名称、属性名称、属性类型、属性默认值、是否主键之间的映射关系，元数据表中反映了管理员标识符、管理员公钥、表名称以及表类型之间的映射关系，公共客体访问规则表中反映了客体名称和访问规则之间的映射关系，用于管理员的主体属性表反映了主体名称与主体安全属性之间的映射关系，用于管理员的客体访问规则表中反映了客体名称与客体访问规则之间的映射关系。

[0017] 优选地，表结构表的建立过程是将表类型、表名称作为键值对中的键，将属性名称、属性类型、属性默认值、是否主键作为键值对中的值存入区块链的键值对数据库中，存入之前检查该键对应的数据是否存在，如果不存在则存入该数据，如果存在则结束该条数据的存入过程。其对应的映射关系如下：

[0018] [表类型][表名]→[属性名称][属性类型][属性默认值][主键]。

[0019] 优选地，元数据表的建立过程是将表类型、表名称、管理员标识符作为键值对中的键，将表中所有数据作为键值对中的值存入到区块链的键值对数据库中，在插入每条数据之前检查数据中每个项与表结构表中元数据表中对应的属性类型是否匹配，检查插入数据是否已在表中存在，如果匹配且不存在，则允许插入，否则拒绝该数据的插入，格式如下所示：

[0020] [表类型][表名称][管理员标识符]→[管理员标识符][管理员公钥][表类型][表名称]。

[0021] 优选地，公共客体访问规则表、用于管理员的主体属性表和客体访问规则表的建立过程是插入数据之前检查数据中每个项与表结构表中元数据表中对应的属性类型是否匹配，检查插入数据是否已在表中存在，如果匹配且不存在，则允许插入，否则拒绝该数据的插入，格式如下所示：

[0022] [表类型][表名][主键属性值]→[所有属性值]。

[0023] 优选地，步骤(2)具体包括以下子步骤：

[0024] (2-1)区块链节点根据元数据管理请求中的管理员标识符、请求操作表类型、请求操作表名称在元数据表中是否存，如果存在，转入步骤(2-2)，否则表示管理员鉴权失败，过程结束；

[0025] (2-2)区块链节点根据元数据表中管理员的公钥并使用非对称加密算法验证元数据管理请求中的签名信息的是否合法，如果合法，表示管理员鉴权通过，否则表示管理员鉴权失败，过程结束。

[0026] 优选地，步骤(4)具体包括以下子步骤：

[0027] (4-1)区块链节点根据非元数据管理请求中的管理员标识符、请求操作表类型、请求操作表名称在元数据表中是否存在，如果存在，转入步骤(4-2)，否则表示管理员鉴权失败，过程结束；

[0028] (4-2)区块链节点根据元数据表中管理员的公钥并使用非对称加密算法验证非元数据管理请求中的签名信息的是否合法，如果合法，表示管理员鉴权通过，否则表示管理员鉴权失败，过程结束。

[0029] 按照本发明的另一个方面，提供了一种基于区块链的访问控制系统，其设置于区块链节点中，其特征在于，包括：

[0030] 第一模块，用于接收来自于客户端的请求，并判断该请求是元数据管理请求，非元数据管理请求，还是访问鉴权请求，如果是元数据管理请求，则转入第二模块，如果是非元数据管理请求，则转入第四模块，如果是访问鉴权请求，则转入第六模块；

[0031] 第二模块，用于对该元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入第三模块，否则过程结束；

[0032] 第三模块，用于将元数据管理请求添加到区块链中的待办请求列表的末尾，并在该元数据管理请求出现在待办请求列表头部的时候，通知元数据表中的管理员参与投票，并在投票结果显示通过时执行元数据管理请求对应的管理操作，从而完成对元数据表、公共客体访问规则表、以及表结构表的更新；

[0033] 第四模块，用于对该非元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入第五模块，否则过程结束；

[0034] 第五模块，用于执行上述非元数据管理请求对应的管理操作，从而完成对用于管理员的主体属性表和客体访问规则表的更新；

[0035] 第六模块，用于根据访问鉴权请求对应的客体从用于管理员的客体访问规则表中取出对应的访问规则，从用于管理员的主体属性表中取出该访问规则对应的主体属性，并将该主体属性代入访问规则中求值，返回鉴权结果。

[0036] 总体而言，通过本发明所构思的以上技术方案与现有技术相比，能够取得下列有益效果：

[0037] (1)本发明由于采用了步骤(1)至步骤(6)，因此能够解决现有智能合约由于缺乏访问控制权限，导致其他主体可以随意调用其中方法的技术问题。

[0038] (2)本发明由于采用了步骤(6)，因此能够解决其他智能合约需要从头到尾实现访问控制且不能在合约之间复用的问题。

[0039] (3)本发明由于采用了所有步骤之前的初始化操作，因此能够解决区块链键值对数据库存储访问规则的问题。

[0040] (4)本发明由于采用了步骤(2)至步骤(3)，因此能够解决多管理员对访问控制元数据修改难以达成一致的问题。

附图说明

[0041] 图1是本发明基于区块链的访问控制方法的流程图。

具体实施方式

[0042] 为了使本发明的目的、技术方案及优点更加清楚明白，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，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。此外，下面所描述的本发明各个实施方式中所涉及到的技术特征只要彼此之间未构成冲突就可以相互组合。

[0043] 本发明的整体思路在于，利用区块链的安全特性保证访问控制框架的防止单节点数据库篡改、计算结果伪造、管理员身份冒用等攻击；利用投票机制保证访问控制策略元数据的可信；下面给出本发明的访问控制方法和系统的具体实施方案。

[0044] 如图1所示，本发明基于区块链的访问控制方法包括以下步骤：

[0045] (1)区块链节点接收来自于客户端的请求，并判断该请求是元数据管理请求，非元数据管理请求，还是访问鉴权请求，如果是元数据管理请求，则转入步骤(2)，如果是非元数据管理请求，则转入步骤(4)，如果是访问鉴权请求，则转入步骤(6)；

[0046] 需要注意的是，本发明的方法还包括在本步骤之前初始化的操作，即建立表结构表、元数据表、公共客体访问规则表、用于管理员的主体属性表和客体访问规则表，其中表结构表中反映了表类型、表名称、属性名称、属性类型(整型、浮点型和字符串类型)、属性默认值、是否主键之间的映射关系，元数据表中反映了管理员标识符、管理员公钥、表名称以及表类型(主体即用户、客体)之间的映射关系，公共客体访问规则表中反映了客体名称和访问规则之间的映射关系，用于管理员的主体属性表反映了主体(即用户)名称与主体安全属性之间的映射关系，用于管理员的客体访问规则表中反映了客体名称与客体访问规则之间的映射关系。

[0047] 其中表结构表的建立过程是将表类型、表名称作为键值对中的键，将属性名称、属性类型(整型、浮点型和字符串类型)、属性默认值、是否主键作为键值对中的值存入区块链的键值对数据库中，存入之前检查该键对应的数据是否存在，如果不存在则存入该数据，如果存在则结束该条数据的存入过程。其对应的映射关系如下所示：

[0048] [表类型][表名]→[属性名称][属性类型][属性默认值][主键]

[0049] 元数据表的建立过程是将表类型、表名称、管理员标识符作为键值对中的键，将表中所有数据作为键值对中的值存入到区块链的键值对数据库中，在插入每条数据之前检查数据中每个项与表结构表中元数据表中对应的属性类型是否匹配，检查插入数据是否已在表中存在，如果匹配且不存在，则允许插入，否则拒绝该数据的插入，格式如下所示：

[0050] [表类型][表名称][管理员标识符]→[管理员标识符][管理员公钥][表类型][表名称]

[0051] 其他表的建立过程是插入数据之前检查数据中每个项与表结构表中元数据表中对应的属性类型是否匹配，检查插入数据是否已在表中存在，如果匹配且不存在，则允许插入，否则拒绝该数据的插入，格式如下所示：

[0052] [表类型][表名][主键属性值]→[所有属性值]

[0053] (2)区块链节点对该元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入步骤(3)，否则过程结束；

[0054] 本步骤具体包括以下子步骤：

[0055] (2-1)区块链节点根据元数据管理请求中的管理员标识符、请求操作表类型、请求操作表名称在元数据表中是否存，如果存在，转入步骤(2-2)，否则表示管理员鉴权失败，过

程结束；

[0056] (2-2)区块链节点根据元数据表中管理员的公钥并使用非对称加密算法验证元数据管理请求中的签名信息的是否合法，如果合法，表示管理员鉴权通过，否则表示管理员鉴权失败，过程结束。

[0057] (3)区块链节点将元数据管理请求添加到区块链中的待办请求列表(To-do list)的末尾，并在该元数据管理请求出现在待办请求列表头部的时候，通知元数据表中的管理员参与投票，并在投票结果显示通过时执行元数据管理请求对应的管理操作，从而完成对元数据表、公共客体访问规则表、以及表结构表的更新；

[0058] 具体而言，投票结果满足预定规则时，表示投票结果通过，例如，50％的投票者同意，或者50个投票者同意。

[0059] (4)区块链节点对该非元数据管理请求对应的访问控制权限进行鉴定，如果鉴定通过，则转入步骤(5)，否则过程结束；

[0060] 本步骤具体包括以下子步骤：

[0061] (4-1)区块链节点根据非元数据管理请求中的管理员标识符、请求操作表类型、请求操作表名称在元数据表中是否存在，如果存在，转入步骤(4-2)，否则表示管理员鉴权失败，过程结束；

[0062] (4-2)区块链节点根据元数据表中管理员的公钥并使用非对称加密算法验证非元数据管理请求中的签名信息的是否合法，如果合法，表示管理员鉴权通过，否则表示管理员鉴权失败，过程结束。

[0063] (5)区块链节点执行上述非元数据管理请求对应的管理操作，从而完成对用于管理员的主体属性表和客体访问规则表的更新。

[0064] (6)区块链节点根据访问鉴权请求对应的客体从用于管理员的客体访问规则表中取出对应的访问规则，从用于管理员的主体属性表中取出该访问规则对应的主体属性，并将该主体属性代入访问规则中求值，返回鉴权结果。

[0065] 本领域的技术人员容易理解，以上所述仅为本发明的较佳实施例而已，并不用以限制本发明，凡在本发明的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明的保护范围之内。

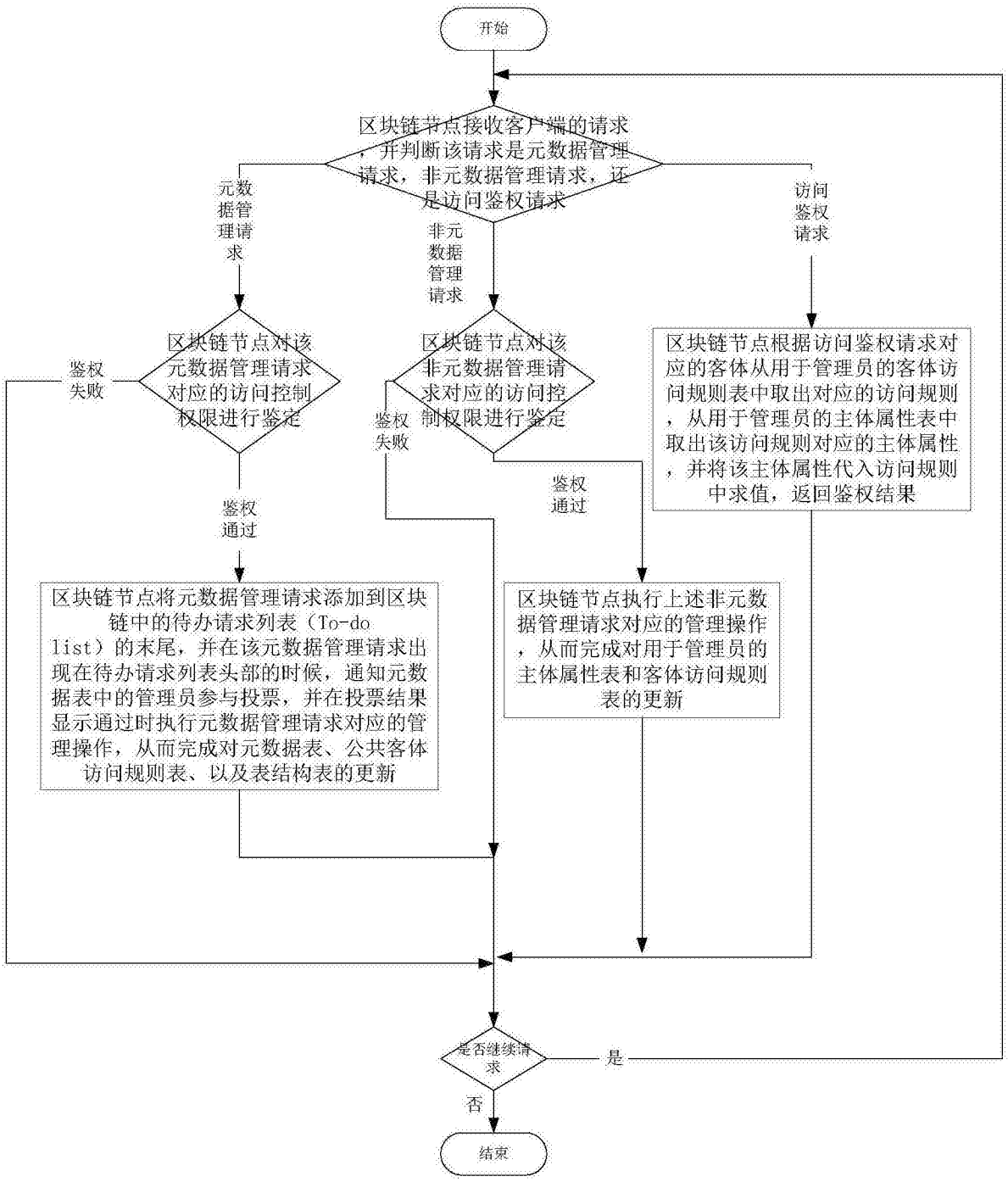

开始
区块链节点接收客户端的请求，并判断该请求是元数据管理请求，非元数据管理请求，还是访问鉴权请求
元数据管理请求
非元数据管理请求
访问鉴权请求
区块链节点对该元数据管理请求对应的访问控制权限进行鉴定
区块链节点对该非元数据管理请求对应的访问控制权限进行鉴定
区块链节点根据访问鉴权请求对应的客体从用于管理员的客体访问规则表中取出对应的访问规则，从用于管理员的主体属性表中取出该访问规则对应的主体属性，并将该主体属性代入访问规则中求值，返回鉴权结果
鉴权失败
鉴权通过
鉴权失败
鉴权通过
区块链节点将元数据管理请求添加到区块链中的待办请求列表（To-do list）的末尾，并在该元数据管理请求出现在待办请求列表头部的时候，通知元数据表中的管理员参与投票，并在投票结果显示通过时执行元数据管理请求对应的管理操作，从而完成对元数据表、公共客体访问规则表、以及表结构表的更新
区块链节点执行上述非元数据管理请求对应的管理操作，从而完成对用于管理员的主体属性表和客体访问规则表的更新
是否继续请求
是
否
结束

图1