# 通用资源访问控制设计方案

[1. 概述 1](#_Toc26456646)

[2. 设计思路 1](#_Toc26456647)

[3. 整体架构 2](#_Toc26456648)

[4. 模块设计 3](#_Toc26456649)

[4.1 资源访问后端模块 3](#_Toc26456650)

[4.2 资源访问合约模块 4](#_Toc26456651)

[5. 功能设计 7](#_Toc26456652)

[5.1 资源访问后端功能设计 7](#_Toc26456653)

[5.1.1 资源上链和确权 7](#_Toc26456654)

[5.1.2 资源授权 8](#_Toc26456655)

[5.1.3 资源回收权限 9](#_Toc26456656)

[5.1.4 目录删除联动清除权限数据 10](#_Toc26456657)

[5.1.5 权限查询 11](#_Toc26456658)

[5.1.6 Token生成 12](#_Toc26456659)

[5.2 资源访问控制合约功能设计 13](#_Toc26456660)

[5.2.1 资源归属确权与查询 14](#_Toc26456661)

[5.2.2 资源授权、更新、回收 15](#_Toc26456662)

[5.2.3 资源权限删除 16](#_Toc26456663)

[5.2.4 权限查询 17](#_Toc26456664)

## 概述

本方案主要目的是实现通用的资源访问控制设计功能。为了保证资源的所有权、控制资源的隐私及资源交换授权，因此设计了资源的权属控制、访问控制和使用控制。资源权属控制保证资源不被篡改，资源访问控制保证资源对不同机构具有不同的可见性，资源访问控制保证资源可以授权给别人使用。

## 设计思路

本系统设计目标是通用化、去中心化、低耦合、高内聚。通用化指权限控制针对任意的资源，而不是针对某个特定系统资源。去中心化指系统架构具有去中心化的特性，没有统一的管理中心。低耦合高内聚指避免和现有其它系统功能交叉，只关注和解决资源的权限方面问题。

目前，去中心化特性通过区块链实现。现有区块链网络已经具有了节点准入机制，节点通过证书授权才能加入网络。节点间通信使用TLS通道保证传输安全性，交易提案带有证书及签名保证发送者的真实性。结合以上特性来实现资源的访问控制，具体如下：

1. 资源权属控制，将证书里机构ID和资源ID进行绑定，更新时检查请求者是否为资源所有者。
2. 资源所有者设置其他机构的资源访问权限，合约向有访问权限的机构推送资源详情。
3. 机构向资源所有者申请访问权限，所有者授权通过，合约通知申请机构拉取资源详情。
4. 机构对资源发起合约申请，资源所有者审核合约通过，机构对资源具有使用权限。合约执行过程中交换节点检查合约执行者是否具有资源交换权限。

本系统通过合约来实现具体功能，合约存储所有资源的权限信息，提供对外操作接口，主要包括权限设置接口、权限查询接口。

## 整体架构



资源访问控制由合约和后端两部分组成，资源访问合约提供接口供资源访问后端和目录链合约调用，资源访问后端提供接口供上层应用调用。底层服务之间尽量不产生耦合，模块各司其职，保持简单独立，通过暴露接口提供给上层应用使用，具体如何使用和组合接口由上层应用自己决定。

访问控制设置目录资源上链，通过目录链合约调用访问控制合约写入资源ID和机构ID的绑定关系，完成资源的确权关系；

目录链的后端调用资源访问控制后端对其机构的资源进行授权、更新、回收权限操作；

以及目录链删除目录操作级联删除目录授权绑定关系；以及目录链调用访问控制接口对机构归属的资源、被授予的资源查询、以及机构授权机构查询；

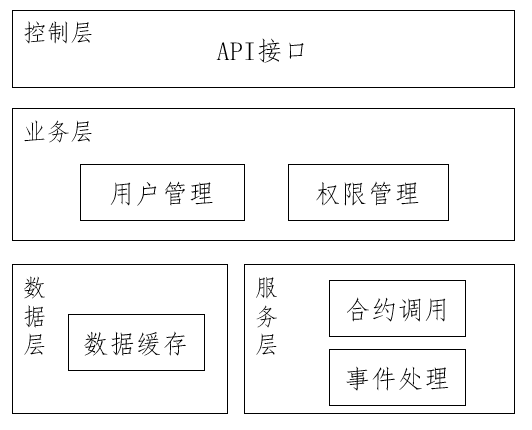
## 模块设计

## 资源访问后端模块

资源访问后端是资源访问控制的服务层，基本作用是封装资源访问合约接口，提供API给上层应用使用。另外，该层也可以实现更多功能，比如：权限数据缓存、token分发以及验证、本地缓存权限查询。

同目录链后端一样，资源访问后端在架构上也具有去中心化的特性，在一个数据交换网络中，每个机构内部都会部署一个资源访问服务节点，节点数据同步通过合约事件实现。节点数据同步的实现可参考《目录链设计方案》。

后端模块设计如下图：



## 资源访问合约模块

权限合约通用型模块设计主要实现了资源上链归属权、访问权、使用权的控制，防止未经授权的同组织用户或者具有背书策略的其他组织机构用户对资源无限制的修改、访问；其中我们规定，归属权是原始上链数据的归属者赋予的权利，某个上链数据的归属者可以更新、删除、查询数据的权利；访问权是原始数据的归属者赋予的查询数据的权利；使用权是原始数据的所有者赋予的使用数据的权利；

权限合约大致可分三个小模块：

* 资源归属权设置与查询；

初始上链数据和归属者绑定，解决资源原始拥有者可以修改、删除、访问资源数据，其他未授权用户不得删除、更新操作；

* 如下图1所示，数据上链的用户在权限合约设置资产的绑定关系，资源的拥有者可以赋权其他人访问、使用资源；资源所有者拥有归属权，即可删除、修改、查询资源；

图1

* 资源拥有者授权及权限更新
* 主要是资源拥有者授权其他组织机构或者人员可访问、使用资源的权限，可设置新的权限或者对已有的权限更新；
* 如图2所示：
* 资源拥有者将资源ID和其他机构ID绑定、授予一定的访问权或使用权，以达到其他组织机构访问、使用资源的权利；

图2

* 资源使用、访问权限查询；

主要是解决其他机构访问资源时，可获取权限合约中设置的资源权属关系，以判断自己是否有权限访问资源；

如图3所示



图3

## 功能设计

## 资源访问后端功能设计

资源访问后端与资源访问控制合约交互，原始归属权数据是由目录链提交的，后续资源授权、更新、回收权限由资源访问后端提供操作接口，可以批量一次进行多个不同类型、多个资源ID的授权、更新、回收操作；同时提供机构名下的归属的资源、以及被授予的资源，授予其他机构权限的查询操作；

### 资源上链和确权

目录链前端触发目录上链操作，目录链后端提交资源到目录链合约，目录链合约将资源id、资源类型传递给资源访问控制，资源访问控制获取发送此交易者x509证书中的机构ID，完成资源类型、资源id、机构id、归属权限的四项数据绑定；待目录上链交易打包区块，则此事务完成，目录链根据链上监听事件，确认目录资源数据、权限数据分布式系统数据一致性；

资源的确权如下图4流程：



图4

### 资源授权

资源授权是在已有的资源权属关系下，资源的归属者将资源的使用权授权给其他机构；

前端调用目录链接口进行授权，目录链调用资源访问控制接口，传递资源id和类型、被授权机构id、权限数值，资源访问控制使用本地公私钥发起授权上链交易，资源访问控制合约获取发起交易者x509证书中的机构id，判断资源id是否是自己的，是自己归属的资源则进行资源类型、资源id、被授权机构id、权限的绑定关系，完成资源授权操作、待授权交易打包区块，资源访问控制后端监听到打包的区块，完成确认交易数据分布式一致性、并将授权绑定关系存储数据库，待查询使用；

资源授权如下图5



图5

### 资源回收权限

资源权限回收由目录链前端发起，传递被回收的资源类型、资源id、被授权机构id，目录链传递参数到资源访问控制，资源访问控制使用本地公私钥发起回收权限上链交易，资源访问控制合约获取发起交易者x509证书中的机构id，判断资源id是否是这个机构id的资源，是自己归属资源则删除资源类型对应资源id被授权机构id的记录，完成对资源的授权回收、待回收授权交易打包区块，资源访问控制后端监听到打包的区块，完成确认交易数据分布式一致性、并将删除被授权机构对应的类型的资源id权限数据，完成本地缓存数据的清除；

注：资源权限的更新也是类似操作，不在明细说明；

资源权限回收如图6



图6

### 目录删除联动清除权限数据

目录链前端发起删除目录资源操作，目录链后端直径发起合约交易，清除目录链合约中的数据目录资源数据，待目录清除交易打包成块，目录链后端监听交易，对其本地缓存目录资源进行标记清除状态，同时目录链后端对资源访问控制发起清除对应目录资源id的级联权限清除操作，资源访问后端接收到要清除的资源类型、资源id、资源访问控制使用本地公私钥发起交易，清除对应资源id的所有权限绑定记录，资源访问控制合约获取发起交易者x509证书中的机构id，判断资源id是否是这个机构id的资源，是自己归属资源则可清除自己对应的资源id以及清除被授权其他机构此资源的绑定记录；

目录资源删除操作，关联权限数据清除，如图7



图7

### 权限查询

目录链发起对目录资源的访问操作，目录链后端读取对应机构id在资源访问控制后端是否有对应机构id和资源id的权限绑定关系，如果有则判断权限是否是访问权，否则拒绝操作；

权限数据查询操作，包括对应资源id和机构是否有权验证查询操作，还包括对机构id下的所有归属资源、被授权资源、以及授权其他机构列表的查询操作，与下图类似的查询路径，具体不在明细说明；

权限查询如图8



图8

### Token生成

机构用户使用用户名、密码、机构id请求目录链生成token，目录链使用用户名、密码、机构id等参数发送给资源访问控制，访问控制和用户中心交互，验证此机构id下是否有对应用户名和密码的合法用户，如果验证通过则生成含过期时间、机构id、用户名的加密token字符串(可配置采用对等加密或者非对等加密token字符串)，否则返回验证失败提示，资源访问控制对生成的token返回给目录链，目录链在返回给前端机构；

采用token之后，机构用户调用目录链机构接口，在http-head带上token，目录链采用公钥验证token是否合法，如果合法则可调用目录链接口，否则禁止调用；同时目录链调用访问控制机构也可以起到token验证是否合法，防止非法调用资源访问控制接口(可配置，默认可关闭)

在目录链调用上链接口时，从已经验证过的token中获取机构id，在根据机构id检索出对应的公私钥，采用此机构的公私钥做上链交易；（本地的公私钥由目录链前期在ca从注册申请）

如果采用对等密钥验证token，则资源访问控制采用对等密钥加密的token，因目录链需验证token，所以也会内置对等密码，防止对等密钥的泄露，可配置的采用非对等加密，访问控制采用私钥加密token，目录链内置公钥验证，即使公钥泄露，第三者也无法生成合法的token(以为没有私钥)；

可配置调用接口token认证流程如下图9



图9

## 资源访问控制合约功能设计

资源访问控制合约，起到分布式权限数据一致性关键流程运行，对权限数据的安全性起到关键作用，考虑到分布式部署，不同组织机构参与其中，防止权限数据非法篡改，必须考虑调用合约函数操作权限数据的权限控制、绑定的权限记录的不可篡改，对查询、验证权限接口稳定、高效要求，对权限运作起到关键作用；

合约可保存数据库为kv键值对，同时为更快的检索数据，我们将资源的归属者单独建立key(orgID~type~resID)即，机构ID~资源类型~资源id，这样在判断资源归属可直接检索判断；

同时存储Key(orgID~type~id)即资源归属者或授权机构id、资源类型、资源id；方便检索用户用户名下资源或者被授权用户是否有此资源访问权限；

Key(type~id~orgID)即资源类型、资源id、资源归属者id或者被授权机构id，方便检索对应资源用户的权限，以快速的验证用户是否有对应资源的权限；



图11

### 资源归属确权与查询

资源的归属权，如图12所示，目录链调用目录链合约写目录资源数据，同时目录链合约调用访问控制合约，传递目录资源id、资源类型，资源访问控制合约获取做交易的用户x509证书的机构id，完成机构id、资源类型、资源id的key(orgID~type~resID)建立，完成资源的确权操作；

从交易者x509证书获取机构id（如果不这样获取，那么只有传递输入参数机构id），是为了解决防止没有此证书的用户对此资源的直接传递误导性参数，直接操作此资源；

对已经写入的key(orgID~type~resID)可以直接查询机构orgID检索其所有不同类型的资源，或检索其某个固定的类型和资源id的资源是否存在，方便对其进行授权其他机构时，可以快速的检索数据；

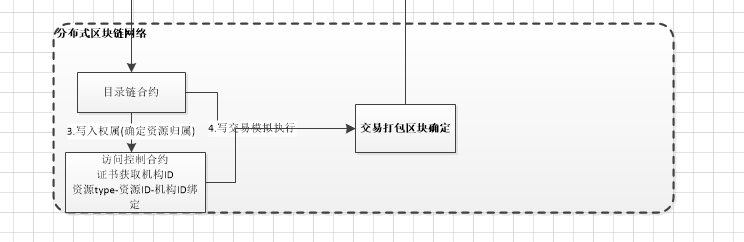


图12

### 资源授权、更新、回收

对合约中权限数据的授权、更新、回收发起是目录链的前端，最终数据上链操作由资源访问控制后端发起，授权、更新、回收操作必须是此机构下的资源归属者操作，否则其他机构无权操作此机构下的资源授权给第三方或者回收第三方已经授权的权限或者更新权限；

授权操作以被授权机构id、资源类型、资源id为key值，被授权机构id+资源的归属者id+资源类型+资源id+权限值作为整个value值；

更新操作首先判断此资源id是否是资源的归属的资源（具体判断参照5.2.1）然后根据被授权机构、资源类型、资源id检索授权绑定对是否存在，存在的情况下，对其auth权限进行更新操作；

回收操作也是首先判断此资源id是否是资源的归属的资源（具体判断参照5.2.1）然后根据被授权机构、资源类型、资源id检索授权绑定对是否存在，存在的情况下，直接构造此Key(orgID~type~id)对其直接删除；

数据流程图参照如下图13



图13

### 资源权限删除

资源权限删除操作，首先判断其归属是否有此资源（具体判断参照5.2.1），在有此资源的情况下，删除key(orgID~type~resID)即机构id、资源类型、资源id构造的复合key值，检索合约进行删除操作，完成对自己的资源的权限的授权清除工作；

同时对之前已经授权此类型id的资源的其他机构进行遍历检索，采用Key(type~id)构造资源到机构的复合键，检索出所有授权的机构，然后构造完整的Key(type~id~orgID)复合键，对其资源的授权数据的完全删除；

### 权限查询

对资源的确权、授权、更新、回收、删除数据对都是发起链上交易，所以所有访问控制在监听分布式的区块链网络事件，都能监听到链上发起的数据变动交易，根据监听到不同类型事件，如是授权事件在本地数据库记录其授权数据对、更新权限事件则更新数据库中对应机构的资源权限数值，如是回收、删除事件，则删除数据库中记录的权限数据绑定对；所以查询首先查询本地数据库中的权限对，如权限不存在的情况下，查询合约中的数据；

合约提供对机构名下所有资源的查询，主要是检索key(orgID~type~resID)数据对，根据机构orgID检索出所有的资源类型type和资源resid，完成对机构名下的所有归属的资源的查询；

合约查询自己被授权列表，只要检索Key(orgID~type~id)数据对，根据机构orgID检索出所有的资源类型type和资源resid，完成对机构名下的所有被授权资源的查询；

合约查询机构的授权列表，需要检索key(orgID~type~resID)或者此机构下的所有资源类型type和resID，然后根据Key(type~id~orgID)检索出所有的orgID，此orgID就是被授权机构的ID值；