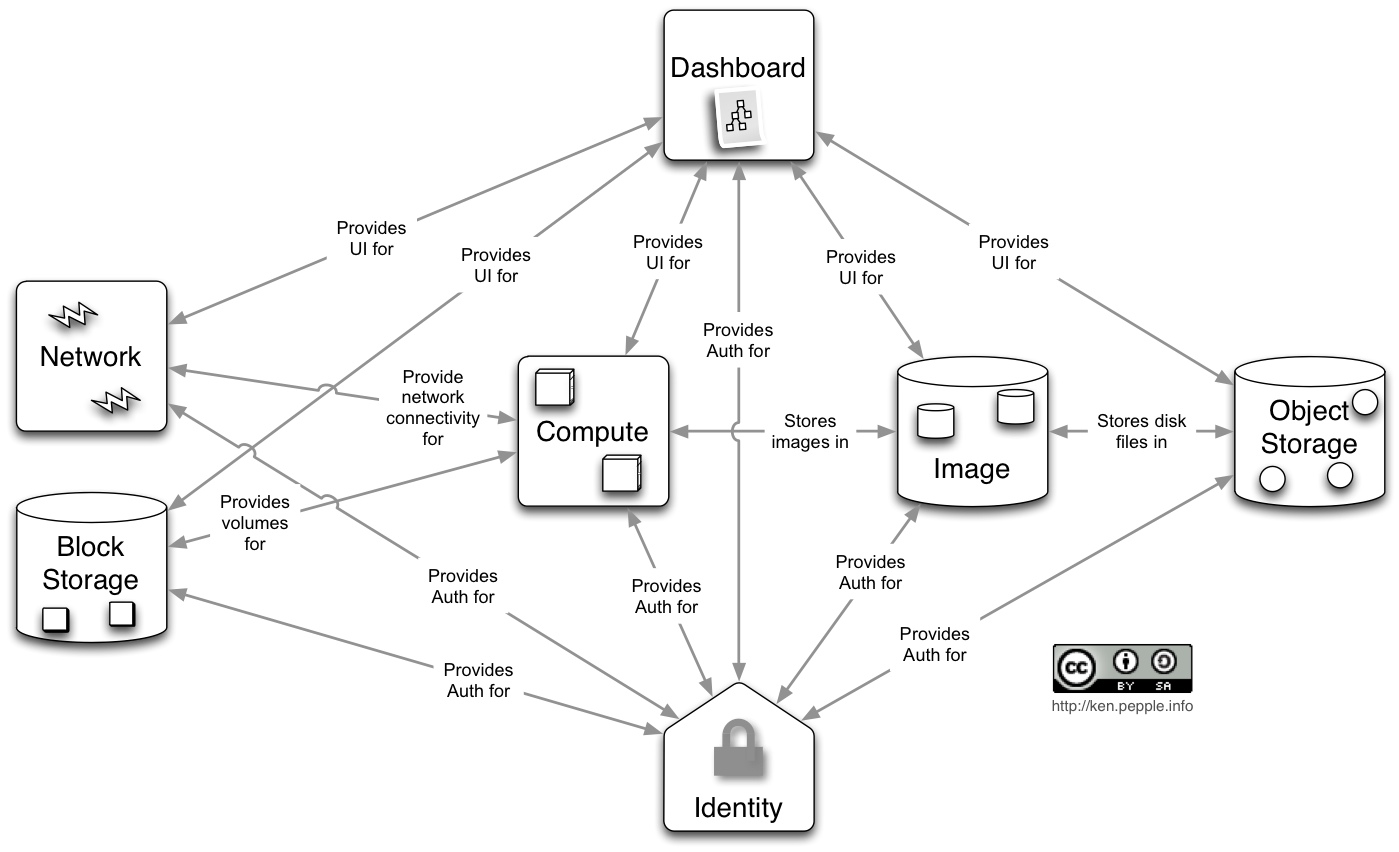
1. keystone的基本功能

keystone作为openstack的Identity Service，提供了用户信息管理和完成各个模块认证服务。

* 用户信息管理：user/tenant基本信息，tenant管理
* 认证服务：登录认证，各个组件API的权限控制

keystone为各个模块提供认证服务，所以各个模块与keystone都有所交互。

其中登录认证体现在用户访问各个组件的API时，调用了WSGI框架的authtoken filter，该filter最调用keystoneclient ，最终通过keystone验证token，完成对用户的登录认证。如果认证失败，用户将不能访问该API。





以创建一个虚拟机（server）为例，结合下图简述下keystone在openstack的访问流程。

         1）用户Alice通过自己的户名和密码向keystone申请token，keystone认证用户名和密码后，返回token1

         2）Alice通过token1发送keystone查询他所拥有的租户，keystone验证token1成功后，返回Alice的所有Tenant

         3)  Alice选择一个租户，通过用户名和密码申请token，keystone认证用户名、密码、tenant后，返回token2。（其实1、2步仅仅是为了查询tenant，如果已经知道tenant，可以忽略1、2步）

         4）Alice通过token2发送创建server的请求，keystone验证token2(包括该token是否有效，是否有权限创建虚拟机等)成功后，然后再把请求下发到nova，最终创建虚拟机

