

选题背景

网络能够提供的服务越来越多，如聊天，支付，论坛，视频浏览……这些都是要用账号来进行用户信息存储的，每一个服务就要注册一个账号，不同服务之间信息的互通，记录，保存十分麻烦。虽然有一些提供 OAuth 身份认证服务的公司，如 QQ，但数据本质上还是被腾讯公司控制了。如果这些账号是基于区块链认证的，这样账号可以自己保护，也不用担心被篡改

选题构思

基于区块链的身份认证

1. 要登录的网站请求用户在链上的账户地址，用于确定账户身份，同时查询获得账户公钥
2. 网站对用户发起挑战(一个或多个)
3. 用户基于私钥加密挑战，将结果发送给网站
4. 网站用公钥进行验证，确认用户身份

进一步扩展的话：

1. 某些网站的会员可通过区块链的形式发放，然后用类似的方法验证会员权益；
2. 用户想让不同网站的数据同步，也用类似的方式验证两个用户的身份