一种区块链系统的聚合签名方法、装置及存储介质

## 摘要

本发明涉及一种基于区块链保护用户隐私的匿名注册方法和系统。该方法涉及实体身份激活流程和匿名账号注册流程：用户的实体身份证件在经过一个实体身份认证机构的验证之后，可将身份证件信息的承诺发布至区块链上；用户在完成实体身份激活后，在某个网站上进行匿名注册时，可利用零知识证明技术证明自己的实体身份的合法性以及属性的合规性。本发明可以避免在注册过程中将用户身份证件的非必要的隐私信息泄露给注册服务器，能够使得注册服务器在确信用户身份属性符合要求的同时，无法获知冗余的身份隐私信息

## 应用

匿名的身份撤销：当实体身份需要撤销时，权威中心会通过一个身份撤销事务隐蔽的通知相关的注册服务器，使得相关的注册服务器获知在其注册的相应的匿名账号AId对应的实体身份已被撤销，同时保证注册服务器无法获知任何实体身份信息。

匿名账号追溯：当匿名账号由于恶意行为需要被追溯时，注册服务器可以在权威中心的协助下对匿名账号的实体身份进行追溯。