1. 凭证撤销机制
2. 研究目的

凭证撤销机制的作用不仅是在凭证到期之后进行撤销，其另外一个重要作用是保护用户信息不被泄露、凭证被信任等。

例如，当用户A向机构B发送凭证，中途被恶意用户C截获，恶意用户C得到用户A的凭证后，可以冒充用户A的身份使用A的凭证；凭证撤销机制的研究就是为了解决类似问题。

1. 研究现状

四种主流撤销机制：

基于动态累加器的撤销机制；

基于TTP的撤销机制；

基于凭证撤销列表（CRL）的撤销机制；

基于公开匿名身份的撤销机制。

以上四种主流凭证撤销机制是中心化的，将原有凭证撤销机制移植到区块链平台可以实现去中心化，近两年也出现了相关研究但是比较少。

1. 研究方向

进一步研究“区块链 + 凭证撤销”的可能性，探索适合分布式身份认证的凭证撤销机制，更好的保护凭证和用户的信息不被泄露。

1. 选择性披露
2. 研究目的

现有的普通凭证无法保护用户隐私，用户在提供所需信息的同时往往会造成非必要信息的泄露。实现凭证属性选择性披露，使用户再提供凭证的时候有选择性的选择披露具体哪一个属性，有效的保护用户隐私。

1. 研究现状

基于merkle树的选择性披露；

基于hash的选择性披露；

基于零知识证明的选择性披露。

1. 研究方向

零知识证明 + 数字签名（BBS+/CL） + 自主控制 + 离线验证；

实现数字凭证的多属性数字签名；实现凭证的自主控制，可以自主选择（不经过发证机构）披露的属性，颁发选择性披露凭证；颁发的选择性披露凭证在机构离线的情况下也可以进行验证。

1. 跨链、跨平台身份认证（协议）
2. 研究目的

现有“区块链 + 数字身份”产品无法真正的实现跨行业、跨机构、跨地域间的身份认证，原因是每个产品有各自支持的底层链，有各自的平台，不能实现数据共享，不能互容互通。因此实现跨链、跨平台的身份认证协议，才能真正的促进“区块链 + 数字身份”的发展。

1. 研究现状

身份认证跨链的本质应当是和常规跨链技术是一样的——数据跨链。

资产跨链和身份认证跨链有很大的区别；资产跨链是将一个链上的资产锁定，在另一条链上发行等值资产；身份认证跨链是B链上的机构可以为在A链上注册的用户颁发凭证，这个凭证被C链上的机构进行验证。

1. 研究方向

合约跨链——实现身份跨链认证。