**1、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**，使用户在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。

在现有的匿名凭证系统中，凭证与区块链是分离的，初凭证本身外，其传输过程、验证流程**没有统一标准**。现有匿名凭证系统是**以用户为中心的**，当凭证发给其他持有者时，凭证的持有人就**失去了对凭证的控制**。引入**UTXO交易模型**，可以将凭证资产化，**以凭证为中心**进行凭证管理，实现**双离线验证**和**凭证撤销**的功能。离线验证是UTXO相对于Account交易模型的优势，双离线验证可以保证在用户和发证方都不在线的情况下对凭证进行验证。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。

**2、研究现状**

现阶段，所有的平台都在研究选择性披露，包括基于Hash的选择性披露，基于Merkle Tree的选择性披露，基于零知识证明的选择性披露等。基于Hash的选择性披露和基于Merkle Tree的选择性披露本质是一样的，相同的输入才有相同的输出。虽然在理论上依据hash值反推原文比较困难，但是仍存在通过hash碰撞的方式来推测原文，而解决哈希碰撞的方式又会造成**验证过程的复杂、增加交互流程**等问题。基于零知识证明的选择性披露，可以不提供原文即能证明凭证的正确性。零知识证明虽然保护了隐私，但是需要平衡其可审计性和**灵活性**。现有的基于零知识证明的选择性披露的方案中十分缺乏灵活性，需要发证方在生成凭证前就选择生成普通类型还是选择性披露类型的，同时**导致对于第三方机构的依赖（中心化）以及凭证不自主可控。**

W3C中DID标准和可验证凭证标准都未对凭证的传输（交易）进行规定，现有的项目中，大多采用DAPP、数字钱包和离线存储等方式。凭证只是在链上生成、存证、验证，并未在链上流通；因此造成凭证与区块链是分离的，同时没有统一的标准，不利于推进大规模应用。

现阶段，凭证撤销，大致包括基于动态累加器的撤销机制，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。存在着**依赖可信第三方，中心化，开销大**（需要进行复杂的密码学计算，在区块链上维护凭证撤销列表）等问题，并不适合去中心化的匿名凭证场景下的凭证撤销。

**3、研究内容**

研究BBS+数字签名，实现**基于属性的多消息数字签名**，进而实现选择型披露匿名凭证；达到用户**自主控制**生成选择型披露凭证的目标。

研究UTXO模型，**在Account中引入UTXO交易模型**，将匿名凭证资产化；凭证的生成以用户为中心，凭证的传输、验证、撤销等过程**以凭证为中心**。同时可以实现**双离线验证，凭证撤销**的功能。

**4、工作安排**

（1）研究BBS+数字签名，实现基于属性的多消息数字签名；

（2）结合零知识证明实现选择性披露；

（3）研究比特币UTXO模型和源码，构建以凭证为中心的匿名凭证验证模型；

（4）更改UTXO实现撤销凭证功能；

（5）更改UTXO实现匿名凭证验证模型。

**5、模型对比**

比特币UTXO交易模型：

（1）对比特币进行交易；

（2）以比特币为中心；

（3）上一笔交易的输出作为下一笔交易的输入；

（4）可以有多个输入和多个输出；

（5）原比特币交易之后被销毁，无法再次使用；

（6）SPV快速验证检验交易；

（7）离线验证；

改进的凭证UTXO对比：

（1）对凭证进行交易；

（2）以凭证为中心；

（3）控制凭证只能交易一次，或者多次（若想再次使用凭证，只能将输出作为输入）；

（4）可以有多个凭证输入，限定只有一个凭证输出；

（5）设定凭证撤销机制（销毁机制）；

（6）快速验证凭证；

（7）双离线验证；