### 系统功能分析

为应对传统学历证书造假、由教育机构单方面保存不当，同时探索推动区块链技术在学历认证、求职就业等领域的应用，提高数字认证可信性。提出利用区块链处理证书认证的相关问题

基于区块链的可信认证系统，主要依赖于区块链的共识机制，共识机制能够有效地增加认证的可信度，其学历学位认证机制主要具有以下特点特性，使其设计的基于区块链的认证系统拥有不可篡改、不可抵赖和去中心化的特点。依赖于区块链中的智能合约机制，使得认证过程严格按照合约要求执行，无须人工参与，可信机制具备中立性和安全性。

通常情况下来讲：对于一个证书管理过程，涉及到三方角色：颁发机构、证书持有者、证书验证者。

对于传统的证书管理平台，数字证书将现有的纸质证书转换成电子数据，由颁发机构上传给第三方证书注册平台，借助数字签名进行有效性的验证。

在区块链系统中，认证机构负责从原有数据系统导入数据和检查证书结果。导入数据后，认证机构对证书进行签名并将其存储到链上，并确认证书的真实性和有效性。每个证书都会获得独一无二的数字标识，作为在链上流转的“身份证”。

对于证书验证者而言，不需要手工验证或向发证机构查询证书的真伪，可直接发起证书验证请求，通过区块链证书管理平台进行验证。

在证书管理平台上的任何操作，例如添加证书，都要求调用方被经过注册的认证机构进行授权。

因此，对证书持有者而言，除了学历证书，还可向认证机构提交其他技能水平证书，由认证人员审核后加入区块链账本，一同进行证书记录。

以学位证书为例：

1. 教育局统一上传学历学位认证信息和教育部直属 的技能认证考核证书。由教育部统一录入保证了数据来源是 真实性和可靠性，也可以提高录入的效率，防止各个机构录 入的信息不同步，给用户造成一定的不便。
2. 学校录入在校学生每个学期的情况，其中包括一 个学期学生的绩点、获得奖项、处分以及总体表现等能够体 现出学生的学习情况。同时，也可以查询在校学生学习情况， 可以更方便地进行学生管理。
3. 培训机构上传每个课程的考核标准，在系统进行备案以便被审查。在每个课程结束以后，上传该学员的在该 课程整个的表现，并且对通过考核的学员上传该课程的技能 认证证书。
4. 工商局审核培训机构加入区块链，并且在一定时 期进行根据培训机构上传的考核标准进行考察，防止培训机 构恶意颁发证书的现象。
5. 个体用户可以查询自己所有的技能证书和学历学 位认证信息，并且根据学历学位的毕业院校查到在该学校所有学期的学习情况。
6. 用人单位查询应聘者的学历和技能证书的真伪性， 而且还可以查询该应聘者的获取学历期间的表现与学习情况，可以更好地进行择取。

然而仅仅实现上述功能显然是不足以发挥区块链的优势。对于本文阐述的相关链中，需要实现如下几个技术难题：

（1）用户身份安全认证：证书认证涉及个人信息流动。 教育资源共享平台往往掌握大量

用户数据, 为了保证用户的隐私安全, 采用匿名的用户身份, 并且让用户私钥掌握在自己手中.

（2）双认证环节：在证书认证过程中，不仅仅限于 机构对用户进行认证, 用户同样也对机构进行认证.双向认证可以提高用户的信任, 增加用户的使用率. 并且可以及时发现用户或者机构的恶意行为.

（3）恶意用户追溯: 针对教育资源共享时, 用户量大.确保当系统中出现恶意用户时, 可以及时将恶意用户记录在本域和跨域区块链上, 并且不再为该用户服务. 这样可以防止恶意用户在其他机构节点进行再次注册.

（4）可信度量机制

采取可信的度量机制对链中的静态以及动态行为进行可信度度量，及时将可信度反馈给网络其他节点，保证授权节点集的实时可信。