现状分析

近年来，区块链技术加快演进，不断与金融、物流、能源、制造、生命科学、医疗保健、销售等领域融合，区块链技术也引起了高等教育工作者的关注。 很多国家制定了推动区块链高等教育应用的战略规划。 例如：爱沙尼亚推出 Disciplina项目， 旨在利用区块链帮助学生监控自己的教育记录，帮助教师建立个人档案等；荷兰成立了区块链联盟，帮助高等教育机构应对区块链应用挑战；德国联邦政府资助一项基于区块链技术的高等教育证书验证项目。

信息技术的快速发展促使高等教育机构为学生提供多形式学习机会，如何记录、验证、共享所有形式的学习，实现学生、高等教育机构和潜在雇主等之间的数据互通，避免教育记录造假，以及保护开放教育资源版权等成为高等教育机构面临的挑战。 在教育领域中，区块链应用具有可靠、可信、安全和高效率等优势，具备存储、传输、验证考试报告、学习成绩、学术成就、职业兴趣、毕业证等能力。通过分布式数据存储、点对点传输、共识机制、加密算法等技术，区块链允许学生控制自己的数据、简化教育机构的活动、提高数据访问的安全性并验证学生的学历，这为高等教育机构应对信息化挑战提供了支持。 当前，不同的教育机构开始尝试利用区块链技术应对挑战。 例如：霍尔伯顿学校利用区块链技术帮助学生记录学习行为和课堂活动表现等；立陶宛 BitDegree 平台为在职人员提供学习机会，记录并验证考试成绩、作业、问题解决能力等信息， 支持利用比特币支付课程费用及申请奖学金等。

研究调查结果显示，区块链高等教育应用主要领域包括数字证书管理、 费用与奖励/资助和学生就业， 如图 1 所示。 所选样本中，25 所高等教育机构（66%）利用区块链技术发放、存储、共享、认证数字证书；10 所高等教育机构（26%）允许 学生利用代币支付学费，以及发放奖学金助学金、获得捐赠等；9 所高等教育机构（24%）利用区块链技术将学生、教育机构和潜在雇主链接，帮助学生就业。 区块链在招生、数字身份、学习档案、评价与指导、学习环境、学分转移、资料审查、学术活动、知识保护等方面的应用较少。 所选样本中，利用区块链技术记录学习档案、对学生与教师等进行评价与指导、管理学习环境的高等教育机构各有 3 所，利用区块链技术进行招生、学分转移和知识保护的高等教育机构各有 2 所，利用区块链技术管理数字身份、审核资料的高等教育机构各有 1 所，没有高等教育机构利用区块链技术管理学术活动。

区块链技术可以实现多方输入、分布式存储数据、应对多方输入造成的信任缺失、 实现非中介化交易关联、按照特定规则自动交易、利用交易日志进行验证、实现价值存储等。 在信息技术快速发展的背景下，区块链技术对高等教育改革有积极作用。 它不仅可以进行教育全方位精准画像，赋予学生对其学习记录的自主权和控制权，提高高等教育机构的工作效率，还可以推进高等教育机构、学生、潜在雇主新型关系的重构。 当前， 高等教育机构以各种创新的方式将区块链技术应用于不同的教育情境其中数字证书管理、费用与奖励/资助、学生就业是最主要的应用。 同时，高等教育机构已开始探究区块链技术在学习档案、评价与指导、学习环境、学分转移、知识保护、数字身份和资料审查等方面的应用。

然而， 大多数高等教育机构仅提出了相关规划或正处于试点测试阶段， 区块链技术在高等教育领域中的应用仍处于初级阶段， 其广泛应用仍面临很多问题和挑战。 从技术角度看，区块链技术在高等教育中的应用面临可扩展性、集成性、数据隐私、数据安全、延迟和标准化等挑战；从推广角度看，区块链技术教育应用仍存在推广度低、数字鸿沟大、实施成本高等问题。高等教育机构应充分意识到区块链技术的优势与不足，消除应用区块链技术的障碍，抓住区块链重塑未来高等教育的机遇。

高等教育机构应当加强对区块链技术的研究，提高区块链技术的成熟度。 虽然，区块链技术通过去中心化可以实现数据安全，但是仍面临被攻击的风险。 高等教育机构应避免数据篡改、泄露等问题，保护学生、教师、机构的数据隐私和安全；加强学生化名与真实身份的映射关系，避免匿名化泛滥带来的数据监控问题。 同时，还应提高区块链技术的可扩展性，打破区块链交易速度低的瓶颈，以应对高等教育机构学生人数众多、教育数据庞大的挑战。 此外，高等教育机构应当设计或选用操作界面简单易操作的平台或程序，为所有师生提供技术支持，从而提高区块链的可用性和师生接受度；还要增加区块链应用的成本投入，鼓励科研人员加强区块链技术平台或程序的设计与开发，购置数据存储设备和应用设备，保证数据的存储、管理。

### 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.

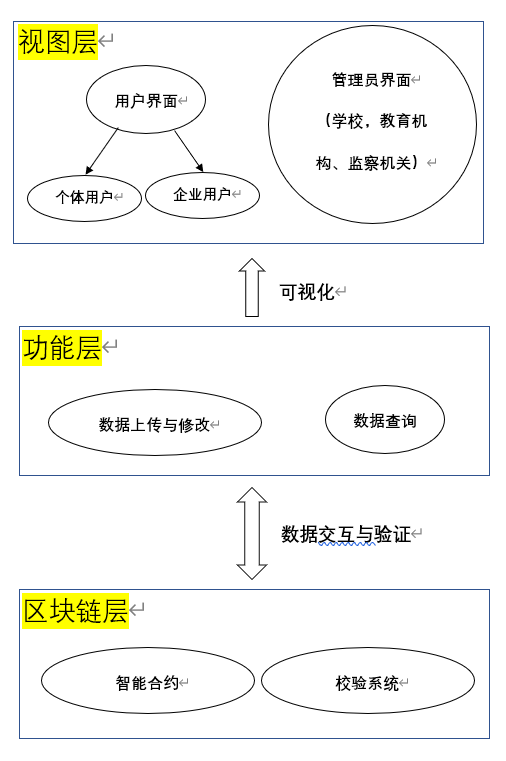
（3）恶意用户追溯: 针对教育资源共享时, 用户量大.确保当系统中出现恶意用户时, 可以及时将恶意用户记录在本域和跨域区块链上, 并且不再为该用户服务. 这样可以防止恶意用户在其他机构节点进行再次注册.

（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。

# 系统架构与可行性分析

1. 系统架构

 基于区块链的学历认证的系统架构如图1 所示，该系统可分为３个模块，视图层、功能层及区块链层。

1.1视图层

视图层主要用于非核心业务逻辑处理以及界面展示，无法储存敏感信息，所有核心数据需要从区块链中提取。因此为了提高效率，在两方面进行了优化，一方面是数据持久化，提高视图层缓存数据的时间，另一方面是在授权节点集筛选时，优先选择性能较高的可信节点，以达到快速向视图层提供数据的目的。

视图层面主要分为3种操作界面，个体用户、企业用户与管理员（教育机构、学校等），满足移动端与网页端的操作需求，将采用 HTML5 标准开发前端网页和微信小程序开发移动端页面。

1.2 功能层

功能层主要进行数据的查询，上传以及修改。

写入功能将完成对个体用户提供的学业信息，如：个人信息、在校成绩，以及证明材料，如：获奖证书扫描件，录入系统的操作。流程如下：1）系统在收到请求录入信息的指令后弹出履历输入窗口。2）用户填写学业信息并以文件形式上传证明材料。3）系统将收到的传输至区块链层进行校验，校验成功后上链。企业用户与管理员无法使用写入功能。

修改功能满足个人用户对错误履历信息的修改和管理员进行学位剥夺的需求。用户在发出修改申请后，需重新填写履历信息并提交系统。系统将对收到的信息再次进行真实性验证，无误则把信息链上存证，否则将再次提示用户检验信息正确性。管理员无法直接修改用户的学历信息，在实施“修改”功能的过程中，实质为向用户相对应学历信息后追加失效声明。

数据查询功能面向普通用户与管理员，系统从区块链上读取请求的数据并提供给用户。用户分为个人用户与企业用户，区别在于个人用户仅可查看本人的履历信息，而企业用户可查看所有应聘者的学业认证信息。用户向系统发出查看请求后，系统将首先判断用户类型。是个人用户将根据用户身份认证信息查找对应的学业认证信息，然后向用户展示；若是企业用户，则依据其提供的条件信息向个人用户提交申请，获得授权后返回对应信息。

数据储存是本系统最核心的功能。数据储存模块向系统中其他模块提供数据存取服务。由于需储存的数据量大且更改操作较少，现阶段可用纠删码冗余算法进行数据处理与储存。

该模块一般采用纠删码中的RS码作为主要的编解码手段。其核心思路是先将接受到的数据分片，得到k个分片数据。然后通过RS编码增加m 个校验数据后形成n个编码数据，并将编码后的数据储存于链上。在进行还原时系统从大于等于k个联盟链中读取编码数据,及可通过生成对应数据矩阵的逆矩阵与编码数据列向量进行乘积,获得原始数据。

1

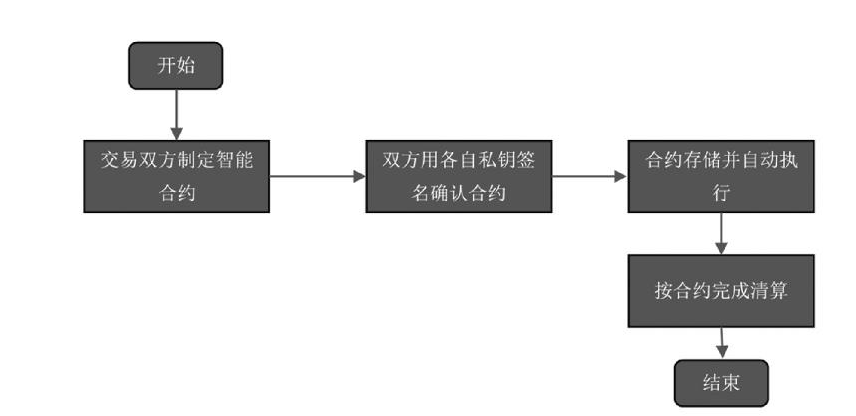
1.3 区块链层

1.3.1智能合约

智能合约是一套以数字形式定义的约定，包括合约参与方可以在上面执行这些约定的协议.智能合约的基本思想是，各种各样的合约条款可以嵌入到人们使用的硬件和软件中，从而使得攻击者攻击时需要付出很大的代价[1]。

简而言之，智能合约是用计算机语言取代了法律语言记录条款、由程序自动执行的合约。

这个概念是上世纪90年代由密码学家尼克·萨博提出，由于当时缺乏可信的执行环境，智能合约没有被应用和发展，直到以太坊的出现，才让智能合约得以“复活”。其在区块链中的运作流程如图2

****

与传统的合约相比，智能合约有三大特点：

1、合约内容公开透明

智能合约部署在区块链上，其合约内容可被所有节点查询。

2、合约内容不可篡改

同区块中的交易信息一样，若攻击者希望对合约进行修改，则需要不断计算父区块的哈希值直至创世区块，整个过程至少达到需要整个区块链系统算力的51%，因此合约内容几乎不可篡改。

3、永久运行

运行在区块链上的智能合约，同样被区块链上网络节点共同维护，只要区块链在，智能合约就能不断得到维护而运行下去。

因而与传统的合约相比，智能合约主要有如下优势：

1、去信任。

由于智能合约内容公开透明且不可篡改。极大增强了交易双方的信任感，因而促进交易安全进行。

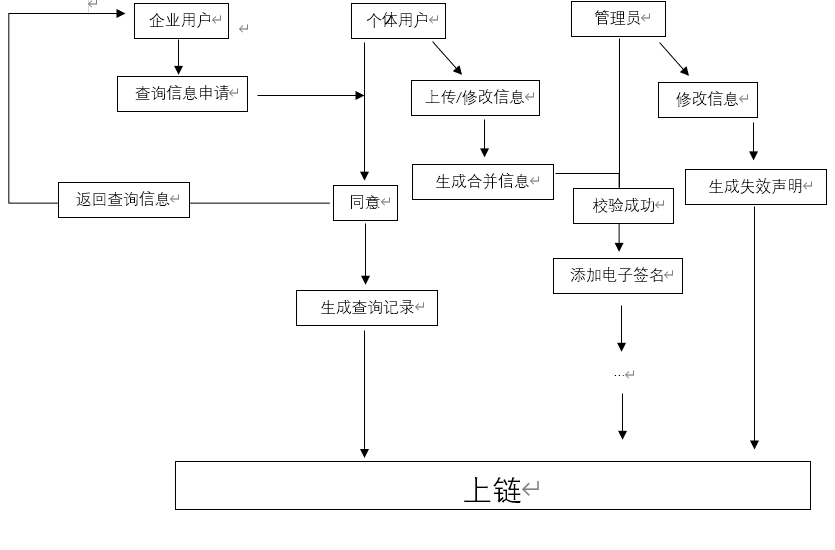
2、经济、高效

相比传统合约经常会因为对合约条款理解的分歧，造成纠纷；智能合约通过计算语言能够很好避免了分歧，从而降低达成共识的成本。

3、无需第三方仲裁

智能合约根据最终的结果自动执行，因而能够避免进行第三方仲裁。

在本系统中，智能合约运行流程如下



所用接口如表1

|  |  |  |
| --- | --- | --- |
| 数据名称 | 数据类型 | 数据含义 |
| Address | String | 颁发单位 |
| Name | String | 姓名 |
| Id | Uint | 唯一id标识 |
| Num | Uint | 证书编号 |
| Time | Uint | 签发时间 |

1.3.2校验系统

校验系统为利用电子签名算法对所储存内容进行加密校验。

1. 可行性分析

2.1 技术可行性

借助区块链技术，可以保证系统中数据存证的高效性与可靠性以及信息共享时的安全性。结合纠删码技术，可实现对原始数据的可靠保存并减少对储存资源的需求。存证时主要利用区块链的去中心性和不可篡改性。在每一个数据节点都保有备份，即使单一节点遭受攻击信息被篡改，依旧可通过其余节点保证原始数据的正确性；此外在更新认证将在多个节点留下不可篡改的记录，保障数据真实性。

2.2 市场可行性

**研发能力/周期**

对政府与企业进行调研，发现竞品在市场仍存在大范围空缺，产品需求仍然旺盛，产品在研发完成后投入市场竞争将具有市场竞争力。

**资金需求/配置**

初始储备资金将支持产品完成初步研发，第一轮融资将于产品初步成型后进行，并且项目将正确来自教育部和财政部的专项补贴支持。

**市场需求**

目前由于学生学业认证、核实过程步骤繁琐，学历造假现象依旧存在且缺少简单高效的解决手段。求职者通过造假以获得面试机会甚至被录用，严重损害了企业与普通应聘者的利益。在这一情况下，基于区块链的学业认证系统有着极大的市场潜力。由于区块链系统的可追溯性、透明性、不可篡改性，系统的安全性与权威性得到保障，能够很好地满足市场需求。

[1]徐宁 & 樊郁徽.(2020).基于区块链技术的商品交易智能合约设计. 怀化学院学报(05),99-104. doi:10.16074/j.cnki.cn43-1394/z.2020.05.020.

# 不足与展望

结合上文不难发现，区块链在教育终端的应用范围十分广泛且有效，有望进一步提升信息化时代教育模式和教育形式，提高各方在教育信息等方面的信息公开化、透明化，极大地解决了目前学位造假、论文造假等问题，是区块链在应用领域下的一大分支。

然而，区块链在教育等方面的解决方案与应用也从来不是十全十美的，其自身仍存在一些不足与弊端亟待解决。首先，存储机制耗费资源。这是区块链本身运行机制导致的弊端，区块链系统每一个节点都实时同步完整账本数据，来实现其数据防篡改、抗摧毁。不过这种模式产生了大量冗余数据，并将随着区块链的数据存储量增长、数据操作量的增加，大量消耗存储资源；同时，各个节点也将耗费大量的计算资源和电量用于处理数据同步。据报道，2017年某数字货币单个节点的区块链体积已经超过180GB，新的用户将花费大量的时间来同步这些数据。由此可见，随着时间的推移，每个节点的存储压力将越发增大，新节点的接入难度也相应增加，这很不利于系统的部署与拓展。其次，运行机制影响效率。区块链中每一次数据修改，都会牵动系统内所有节点的账本数据同步更新，也就意味着每次操作过程都需耗费大量时间，而且这种运行机制也将给系统所在网络带来极大考验。由于每次操作都是全网的行为，短时间内如果操作次数较多，则会造成网络的堵塞。据外媒报道，某数字货币曾由于交易量增大，每次交易所需时长由10分钟增加到最长24小时以上，区块链网络崩溃的新闻也比比皆是。所以，若将区块链技术用于关键领域，其运行机制仍需进行结构性优化。

此外，抛开技术层面，区块链结合教育的发展本身建设思路也存在一定逻辑问题值得我们去深思。首先，一个不容否认的事实是，信息时代的学习方式、学习过程、学习形态已经发生变化，但学习成果的认证仍然保持传统的方式。学分银行的出现在某种程度上是为了解决了这一问题。但在学分银行建设实践中，仍然试图采用传统的思维方式来解决一个全新的问题，寄希望构建一个强大且巨大的“中心体”来存储和认定所有学习者的所有正式、非正规、非正式学习成果。这个“中心体”希望拥有所辖范围内所有学习者的个人信息和学习成果记录，对所有学习成果的层次和质量进行权威性认定，指导规范所有学习成果之间的相互转换。也就是说，我们虽然采用了区块链这样一种“去中心化”的技术去避免学术造假，但这样一个技术应用的背景确实需要政府或者相关具有相当公信力的机构去进行背书的，这本质上还是没能跳脱出“中心化”这样一个理念的鸿沟。未来区块链在教育方面的应用还需要长久的改革与探索，不仅仅是在技术上的完善，更需要一类逻辑上对于教育认证方式的转变。