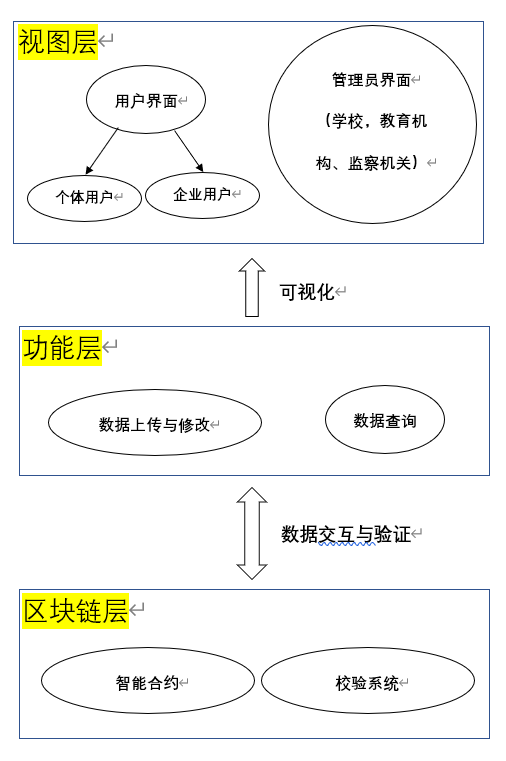
系统架构与可行性分析System Architecture and Feasibility Analysis

1. 系统架构System Architecture

 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。

The system architecture of the blockchain-based academic certification is shown in Figure 1. The system can be divided into 3 modules, view layer, functional layer and blockchain layer.

1.1视图层View layer

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。The view layer is mainly used for non-core business logic processing and interface display. Sensitive information cannot be stored, and all core data needs to be extracted from the blockchain. Therefore, in order to improve efficiency, it is optimized in two aspects. On the one hand, data persistence is improved to improve the time for the view layer to cache data. On the other hand, when the authorized node set is screened, trusted nodes with higher performance are preferred to achieve the purpose of quickly providing data to the view layer.

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。The view level is mainly divided into 3 types of operation interfaces, individual users, enterprise users and administrators (educational institutions, schools, etc.), to meet the operational needs of mobile end and web end, will use HTML5 standards to develop front-end web pages and WeChat Mini Program to develop mobile end pages.

1.2 功能层Functional layer

功能层主要进行数据的查询，上传以及修改。The functional layer mainly performs data query, upload and modification.

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。The write function will complete the academic information provided to individual users, such as: personal information, school grades, and proof materials, such as: scanned copies of award certificates, and enter them into the system. The process is as follows: 1) The system pops up the resume input window after receiving the instruction to request input information. 2) The user fills in the academic information and uploads the proof materials in the form of a file. 3) The system transmits the received information to the blockchain layer for verification, and it will be put on the chain after the verification is successful. Enterprise users and administrators cannot use the write function.

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。The modification function meets the needs of individual users to modify the wrong resume information and the administrator to deprive them of their degrees. After the user sends a modification application, he needs to fill in the resume information again and submit it to the system. The system will verify the authenticity of the received information again, and store the information on the chain if it is correct. Otherwise, the user will be prompted again to verify the correctness of the information. The administrator cannot directly modify the user's academic information. In the process of implementing the "modification" function, the essence is to add an invalidation statement to the user's corresponding academic information.

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。The data query function is for ordinary users and administrators. The system reads the requested data from the blockchain and provides it to the user. Users are divided into individual users and enterprise users. The difference is that individual users can only view their resume information, while enterprise users can view the academic authentication information of all candidates. After the user sends a viewing request to the system, the system will first determine the user type. Yes, individual users will find the corresponding academic authentication information according to the user's identity authentication information, and then show it to the user; if it is an enterprise user, submit an application to the individual user according to the condition information provided by it, and return the corresponding information after obtaining authorization.

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。Data storage is the core function of the system. The data storage module provides data access services to other modules in the system. Due to the large amount of data to be stored and the few change operations, the erasure code redundancy algorithm can be used for data handling and storage at this stage.

The module generally uses the RS code in the erasure code as the main coding and decoding method. The core idea is to sharding the received database first to obtain k sharding data. Then add m check data through RS coding to form n coding data, and store the coded data on the chain. When performing reduction, the system reads coding data from more than or equal to k alliance chains, and can be multiplied by generating the inverse matrix of the corresponding data matrix and the coding data column vector to obtain the original data source.

1

1.3 区块链层Blockchain layer

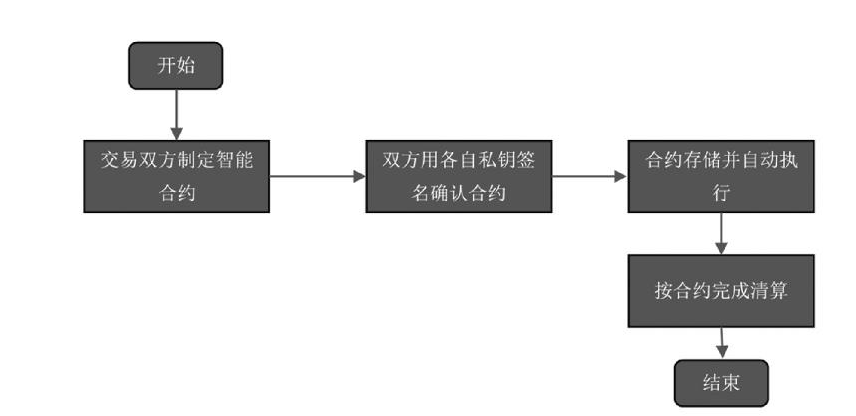
1.3.1智能合约Smart contract

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]。A smart contract is a set of digitally defined conventions, including agreements on which contract participants can enforce those conventions. The basic idea of a smart contract is that various contract terms can be embeddings into the hardware and software people use, making it costly for attackers to attack [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 In short, smart contracts are contracts that are automatically executed by programs that replace legal language with computer language to record terms.

This concept was proposed by cryptographer Nick Saab in the 1990s. Due to the lack of a trusted execution environment at that time, smart contracts were not applied and developed. It was not until the emergence of Ethereum that smart contracts were "resurrected". Its operation process in the blockchain is shown in Figure 2

****

与传统的合约相比，智能合约有三大特点：Compared with traditional contracts, smart contracts have three characteristics:

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。

1. The content of the contract is open and transparent

Smart contracts are deployed on the blockchain, and their contract content can be queried by all nodes.

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。

2. The content of the contract cannot be tampered with

Like the transaction information in the block, if the attacker wants to modify the contract, he needs to continuously calculate the hash value of the parent block until the genesis block. The whole process requires at least 51% of the computing power of the entire block chain system, so the content of the contract can hardly be tampered with.

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。

3. Permanent operation

The smart contract running on the blockchain is also jointly maintained by the network nodes on the blockchain. As long as the blockchain is there, the smart contract can continue to be maintained and run.

因而与传统的合约相比，智能合约主要有如下优势：Therefore, compared with traditional contracts, smart contracts mainly have the following advantages:

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

1. To trust.

Because the content of the smart contract is open, transparent and cannot be tampered with. It greatly enhances the trust between both parties to the transaction, thus promoting the safe conduct of the transaction.

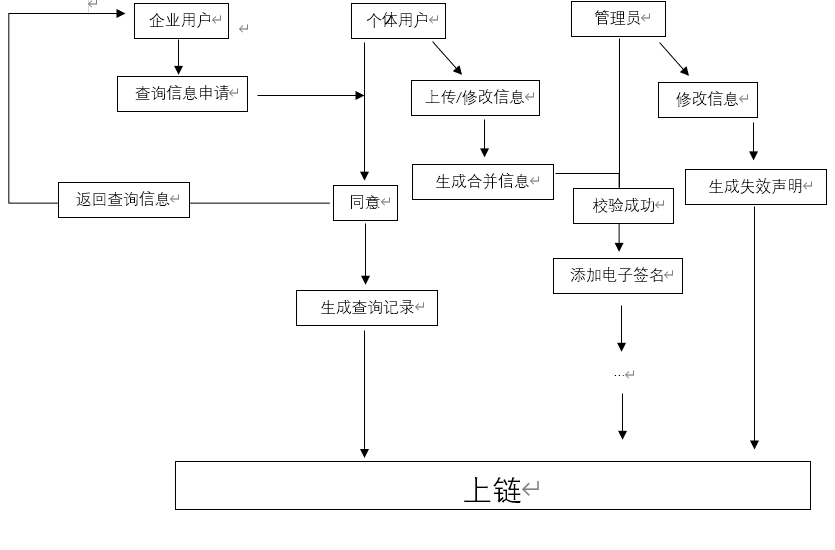
2. Economical and efficient

Compared with traditional contracts, disputes often arise due to differences in understanding of contract terms; smart contracts can avoid differences through computational language, thereby reducing the cost of reaching consensus.

3. No need for third-party arbitration

Smart contracts execute automatically based on the final result, thus avoiding third-party arbitration.

In this system, the operation process of the smart contract is as follows



所用接口如表1The interface used is shown in Table 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 |

|  |  |  |
| --- | --- | --- |
| Data name | Data Type | Data meaning |
| Address | String | Issuing department |
| Name | String | Name |
| Id | Uint | Unique id identifier |
| Num | Uint | Certificate number |
| Time | Uint | Issue time |

1.3.2校验系统Verification system

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。

The verification system uses an electronic signature algorithm to encrypt and verify the stored content.

1. 可行性分析2. Feasibility analysis

2.1 技术可行性Technical feasibility

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。With the help of blockchain technology, the efficiency and reliability degree of data storage in the system and the security of information sharing can be guaranteed. Combined with erasure code technology, the reliable preservation of the original data source can be realized and the demand for storage resources can be reduced. The decentralization and immutability of the blockchain are mainly used when depositing certificates. In each data node to maintain a backup, even if a single node is tampered with by the attack information, the correctness of the original data source can still be guaranteed by the remaining nodes; in addition, the update authentication will leave an immutable record in multiple nodes to ensure data authenticity.

2.2 市场可行性Market feasibility

**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。

**R & D Capability/Cycle**

**The government and enterprises conducted research and found that there are still large-scale vacancies in the market for competing products, the demand for products is still strong, and the products will be competitive in the market after the research and development is completed.**

**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。

Funding Requirements/Allocation

The initial reserve funds will support the initial research and development of the product, the first round of financing will be carried out after the initial formation of the product, and the project will be properly supported by special project subsidies from the Ministry of Education and the Ministry of Finance.

**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。

Market demand

At present, due to the cumbersome steps in the process of student academic certification and verification, the phenomenon of academic fraud still exists and there is a lack of simple and efficient solutions. Job seekers use fraud to obtain interview opportunities or even be hired, which seriously damages the interests of enterprises and ordinary applicants. Under this circumstance, the academic certification system based on blockchain has great market potential. Due to the traceability, transparency and immutability of the blockchain system, the security and authority of the system are guaranteed, which can well meet the market demand.

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.