基于区块链的⾼校学⽣信息管理系统链改⽅案

学号：2019000101159

所属专业：区块链运用与技术（信息安全方向）

项目人：李俊

# 一，总体：高校学生信息管理系统业务描述

**0** 概要

该系统以以太坊为基础，对⽬前⾼校学⽣信息管理系统进⾏链改优化，能够为学⽣发展提供 更加⾼效、畅通、透明的校园信息化基础设施，期望可供国内外各⼤⾼校管理⼈员使⽤。

本链改⽅案针对原有系统中的三⼤功能模块进⾏链改，链改中遵循「是否上链由数据主⼈选择」与「避免主观数据上链」两个原则——

1）**「学⽣信息管理模块」**—— 通过与数字身份系统的连接，解决「信息单薄、身份封闭」 的问题，可以使多个学院间进行资源互通，进⽽达到互惠共赢**1+1>>2** 的效果。

2）**「业务信息管理模块」**—— 基于数字身份系统与⾏为轨迹记录，对传统模块进⾏链改，解决「⽆法保证公平公正的「⼈治」、⽆法保证学⽣提交信息的真实性、⽆法做到彻底的群众监督」的问题，实现「根据提供的筛选算法⾃动得出结果、数字身份 **+** ⾏为轨迹记录作弊难、全过程透明可监督」的成效。

3）**「信息反馈模块」**—— 信息反馈模块也即我们常说的投诉系统，基于数字身份系统，从「封闭式信息反馈模块」转变为「全透明的链上反馈模块」，解决「过程⿊箱、被限制的查看权、记录可篡改、负责⼈找不到」的问题，达到「全程可追踪、全⽹公开的读权限、全过程不可篡改、每⼀个环节都能找到负责人的效果。

表**1** 链改模块总结



（续）表**1** 链改模块总结

|  |  |
| --- | --- |
| 链改模块 | 链改效果 |
| 学⽣信息管理模块 | 信息丰富、身份开放：多个分院线下资源 互通，互惠共赢，**1+1>>2** |
| 业务信息管理模块 | 根据提供的筛选算法⾃动得出结果、数字身份 **+**⾏为轨迹记录作弊难、全  过程透明可监督 |
| 信息反馈模块（投  诉系统） | 全程可追踪、全⽹公开的读权限、全过程不可篡改、每⼀个环节都能找到  负责⼈ |

**「链上数据不可篡改、数据库读权限完全开放、时间戳不可篡改」**等特性，是使⽤区块链技术进⾏系统改造的重要依据。

此外，在 后面对基于「数字身份」与「链上⾏为轨迹记录」的新型凭证系统（链上⾏为轨迹

记录：如记录课程表现）进⾏了分析，包括：

**1）新型凭证系统相对于传统凭证系统的优势（传统凭证：如毕业证、成绩单）**

能颁发可信凭证的机构数量少 → **凭证/凭证颁发机构多级化**

凭证中包含的信息少 → **凭证附带⼤量可信客观数据**

造假成本低 → **造假成本⾼**

·伪造链上⻓期的记录成本⾼

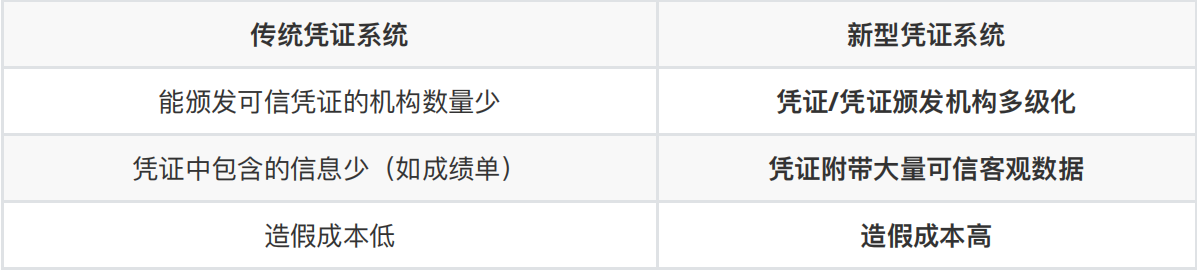
·与物理实体⼀⼀对应的数字身份系统让作恶⻛险巨⼤

**2）⾏为轨迹的「可延续性」**

⾏为轨迹存在可延续性，这个特性让同⼀个个体的不同身份不再相互孤⽴。

例如，⼩明毕业后，「学⽣身份」成为了旧的身份，但他的「⾏为轨迹」继续被记录，只不过新的记录依附在他的「职业身份」下。

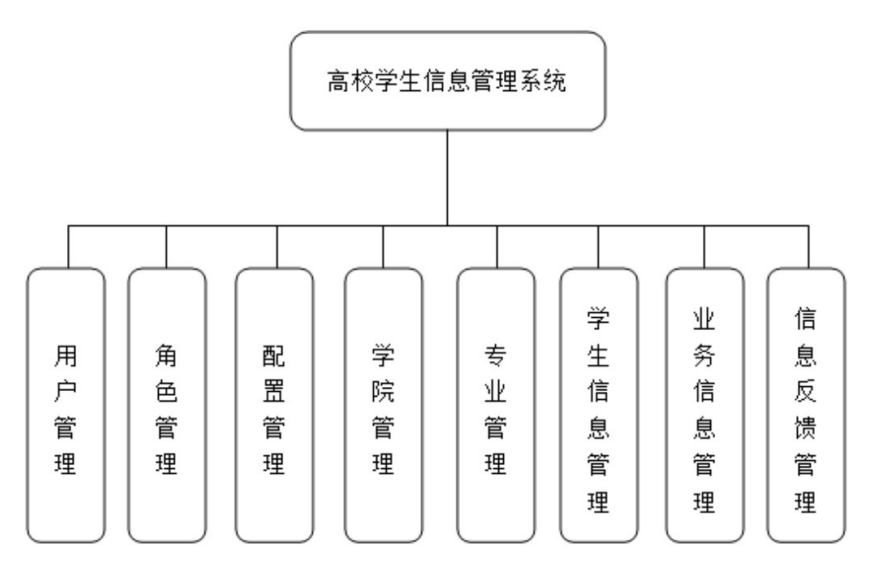
表**2** 新型凭证系统相对于传统凭证系统的优势



**1** ⾼校学⽣信息管理系统业务描述

**1.1** 系统中的三⼤模块简述

对于⽬前的各⼤⾼校⽽⾔，学⽣信息管理系统基本相同，可划分为如下模块：



**图1 系统总体功能结构图**

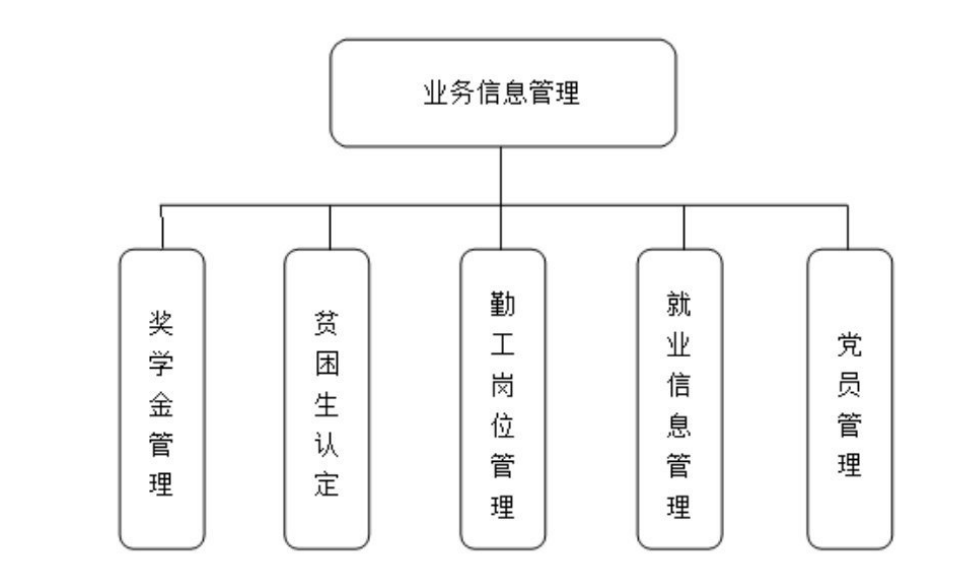
我们在本⽂中要讨论的主要是**业务信息管理、学⽣信息管理与信息反馈三个模块。**

·**业务管理信息模块**

业务信息管理包括奖学⾦管理、贫困⽣认定管理、勤⼯岗位申请管理、就业信息管理、党员

管理等板块，学⽣可以通过系统申请奖贷助学⾦、勤⼯岗位等[1]。

业务信息管理功能结构图如下图所示：



图**2** 业务信息管理模块

·**学⽣信息管理模块**

在传统的学⽣管理系统中，学⽣的信息管理是指管理⼈员维护学⽣的个⼈基本信息，⽐如学

⽣在校期间的活动管理、学籍管理等。对于学⽣⽽⾔，可以查看⾃⼰的有关信息，⽽管理员

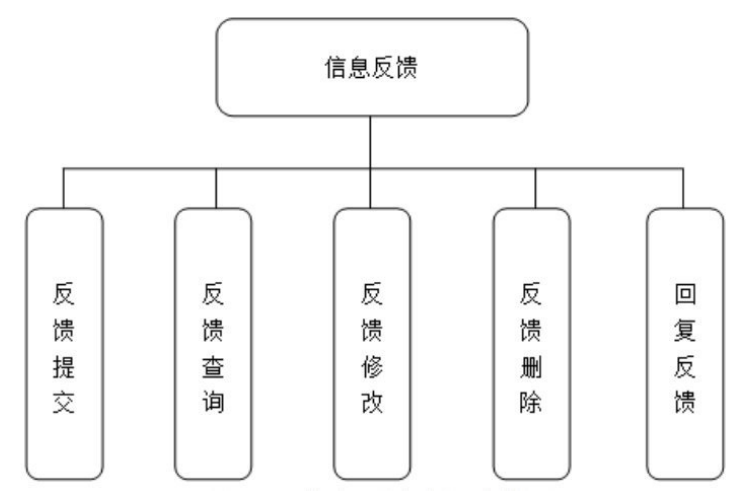
则可以查看对应权限范围的学⽣的信息。管理员应该具备有修改学⽣基本信息的权限。

·**信息反馈模块**

信息反馈的主要功能就是建⽴线上的沟通途径。学⽣可以通过提交反馈和查 看⾃⼰提交的反

馈。有关的管理⼈员则可以查看所有⼈的反馈以及对这些反馈意 ⻅进⾏修改、删除以及回

复。



图**3** 信息反馈模块

**1.2 三⼤模块的传统运作流程及弊病**

**1.2.1 学⽣信息管理模块**

（**1**）**运⾏流程简述**

学⽣信息由管理员进⾏「增减查改」的操作，学⽣仅有查询信息的权利。

（**2**）**传统⽅案的弊病**

·**信息单薄**

传统⽅案中，学⽣信息仅包括基本资料，⽽不能涵盖更多的数据，如学⽣参加社团与⽐赛的数据。

·**身份封闭**

学⽣卡的适⽤范围仅是本校，难以实现**多个分院间的信息共享，身份共⽤**。

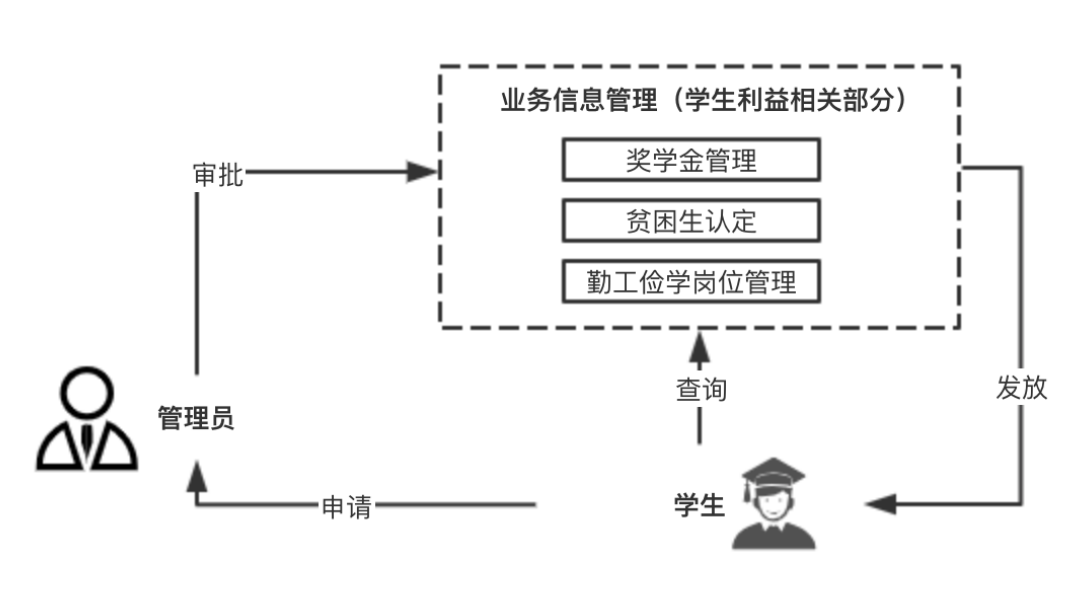
**1.2.2 业务信息管理模块**

传统的业务信息管理模块中包含两个部分，⼀部分和学⽣利益挂钩，如奖学⾦管理、贫困⽣认定、勤⼯俭学岗位管理等；另⼀部分是和学⽣利益⽆关，例如毕业后的就业信息管理。

**1.2.2.1 和学⽣利益挂钩的部分**

（**1**）**运⾏流程简述**

对于和学⽣利益挂钩的部分⽽⾔，简要运⾏流程如下图所示。学⽣仅具有两种权限：查询信息与提交申请，具体的审批由管理员（例如辅导员）全权负责。



图**4** 与学⽣利益挂钩部分的运⾏流程

（**2**）**传统⽅案弊病**

传统⽅案存在如下问题：

·**⽆法保证「⼈治」是公平公正的**

管理员完全掌握审批权限，导致存在「权⼒滥⽤」的可能性。

·**⽆法保证学⽣提交信息的「真实性」**

除考试成绩等客观数据外，其它提交的资料存在「造假」的可能性。

·**⽆法做到彻底的群众监督**

最后虽然会公布结果，但是由于信息缺失（⼤多数情况下我们只是知道个⼈名罢了），⽆法做到彻底的群众监督。

因为如上的⼀些问题，这样的事件颇为常⻅ —— 「⾮贫困⽣」因为各种各样的原因拿到了贫困助学⾦，⽽真正的贫困⽣却⽆法拿到。

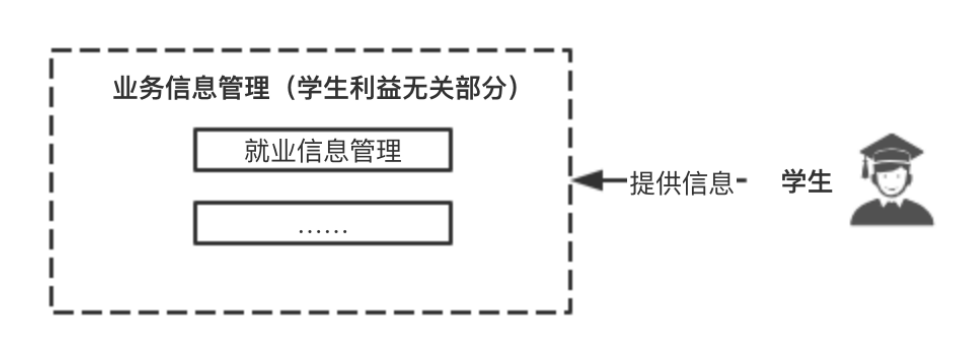
**（3）现有的解决⽅案**

近年来，部分学校也针对如上的问题提出了解决⽅案，例如通过分析学⽣的饭卡消费情况，来判断学⽣是否真的是贫困学⽣，但这些解决⽅案的适⽤范围⽐较狭窄。

**1.2.2.2** 和学⽣利益⽆关的部分

**（1）运⾏流程简述**

简要运⾏流程如下图所示，学校要求学⽣向学校⼀次性地提供就业信息：



图**5** 和学⽣利益⽆关部分的运⾏流程

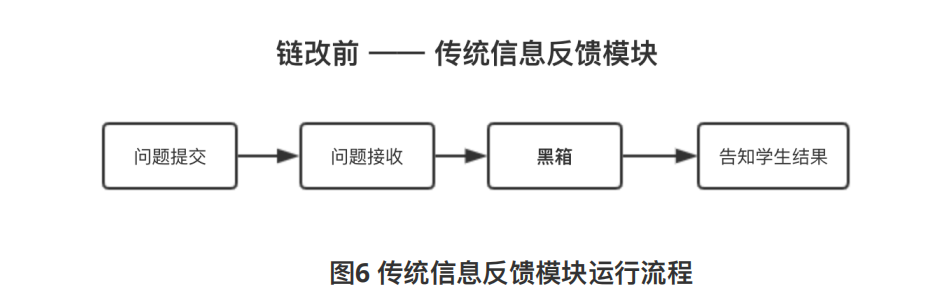
**（2）传统⽅案弊病**

传统⽅案近乎⼀种形式主义 —— 在提交⼀次⽆法确认真假的就业信息之后，学⽣基本上相当于和学校信息系统「失联」，「学⽣进⼊社会后的就业轨迹」这类重要的信息⽆法被学校掌握。

**1.2.3** 信息反馈模块

**（1）运⾏流程简述**

学⽣提交反馈信息，管理⼈员处理后通知。



**（2）传统⽅案的弊病**

·**⿊箱的过程**

传统投诉系统中的处理流程是⼀个「⿊箱」的过程，在投诉后只能等待最终处理结果。在这个过程

中，往往不知道已经进⾏到了哪⼀步，以及负责⼈是谁。

·**被限制的查看权**

有的传统投诉系统中，投诉⼈只能看到⾃⼰的投诉信息，⽆法形成「全⽹监督」。

·**被篡改的记录**

传统投诉系统中，记录可以被「增删查改」，以往的处理历史可以被轻易抹除。

·**找不到的负责⼈**

传统投诉系统中，我们难以知道我们的问题现在正在什么⼈⼿上被处理。

**2 ⾼校学⽣信息管理系统链改⽅案**

系统的链改并⾮「⼀蹴⽽就」的过程，⽽是要根据现有的系统、链改的成本、链改的成效等要素进⾏综 合核算后，设计逐步链改⽅案。对于本链改⽅案来说，数字身份系统是重要基础设施，是其它所有链改模块的「原点」。

**2.1 通过DID数字身份⽅案，针对学⽣信息管理模块的链改**

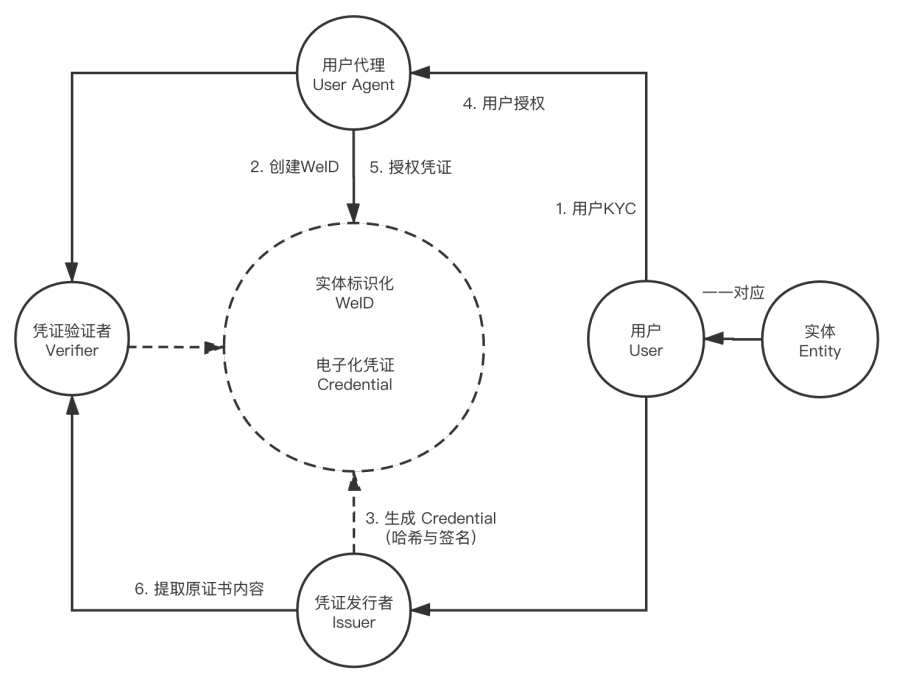
**2.1.1 链改⽅案**

**2.1.1.1 数字身份系统架构简介**

**DID**： Decentralized Identity，去中⼼化数字身份。

将⽤户的身份所有权和使⽤权回归⽤户是区块链业界中的⼀个重要命题，去中⼼化数字身份也将是区块 链⽣态中的重要基础设施。⽬前 W3C 等组织已经建⽴起了完整的 DID 协议。同时，腾讯等企业针对 DID 提出了完整的解决⽅案：https://www.odaily.com/post/5132523

因此，我们⾸先可以做的，是通过 DID 对传统的学⽣信息管理模块进⾏链改，在诸如⼤学城的环境中实 现学⽣卡的「跨校使⽤」。 以腾讯 WeIdentity 为例，我们来简要阐明数字身份的基本架构。



图**7** 数字身份的基本架构

**特性：**

·**实体标识化**（**WeID**）

为每个实体（⼈或物）在区块链上⽣成符合国际规范（DID）的全球唯⼀ID。

·**电⼦化凭证**（**Credential**）

将物理世界中的纸质证明⽂件电⼦化，并利⽤区块链不可篡改的特性，将原始数据的 Hash 上链，

并附上权威机构 (Issuer) 的签名，确保数据不可伪造，可验证权威性。

以学⽣管理系统为例，那么学⽣身份凭证便是此处的「电⼦化凭证」。

·**⽤户授权即交易**（**Authorization**）

原始数据的跨机构传输需要得到⽤户的授权，授权记录由 User Agent 上链，符合 GDPR（⼀般资料保护规范）。

**⻆⾊定义：**

·**实体**（**Entity**）

实体对象（⼈或者物），为⽤户（User）在现实中的唯⼀映射。

·**⽤户**（**User**）

与实体⼀⼀对应，拥有链上身份 ID，可申请凭证并授权相关机构使⽤⾃身相关数据。

·**⽤户代理**（**User Agent**）

为⽤户⽣成链上ID 及提供 KYC 服务，⼀般为权威可信机构，实体通过该机构与链上身份或数据进⾏交互。

·**凭证发⾏者**（**Issuer**）

对身份/证书/数据进⾏发⾏和认证的机构或个体。权威机构发⾏的数据具备权威性，个体发⾏的数

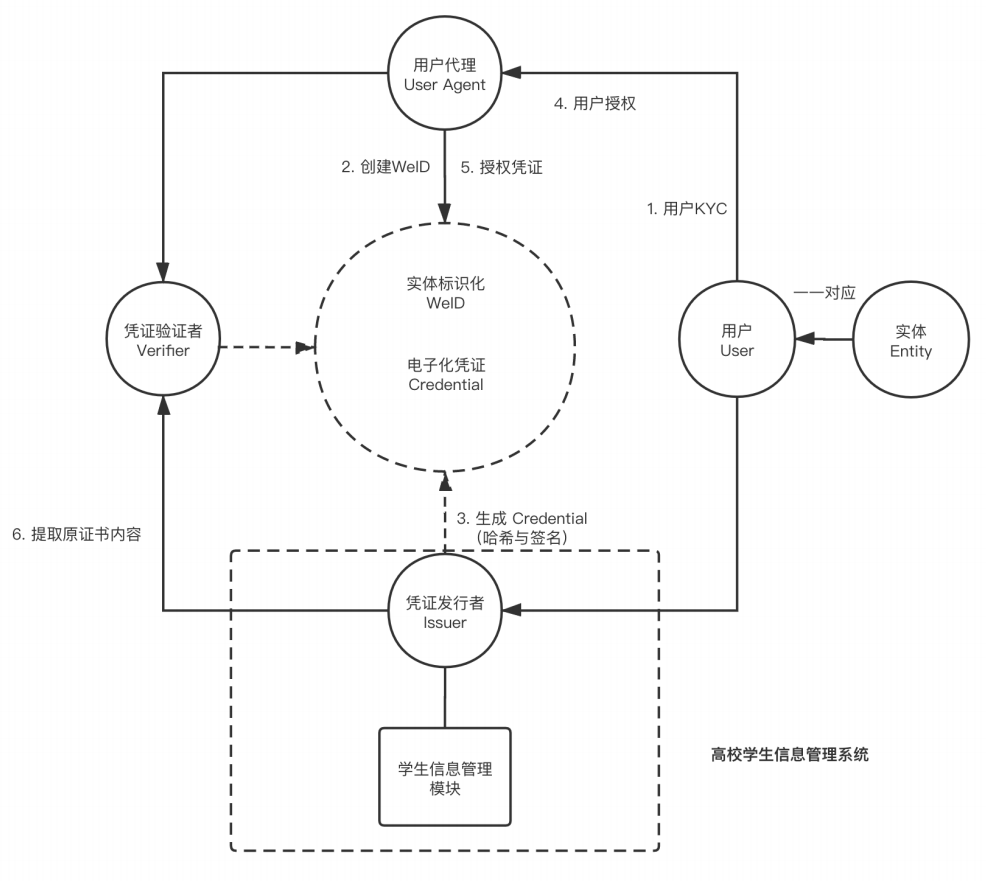
据不具备权威性，权威机构的认定取决于具体业务场景及参与⻆⾊。

·**凭证验证者**（**Verififier**）

使⽤身份/证书/数据的机构，如⽤⼈企业，可验证数据是否被篡改、是否经过凭证发⾏⽅认证。

**2.1.1.2 学⽣信息管理系统与数字身份系统的对接**

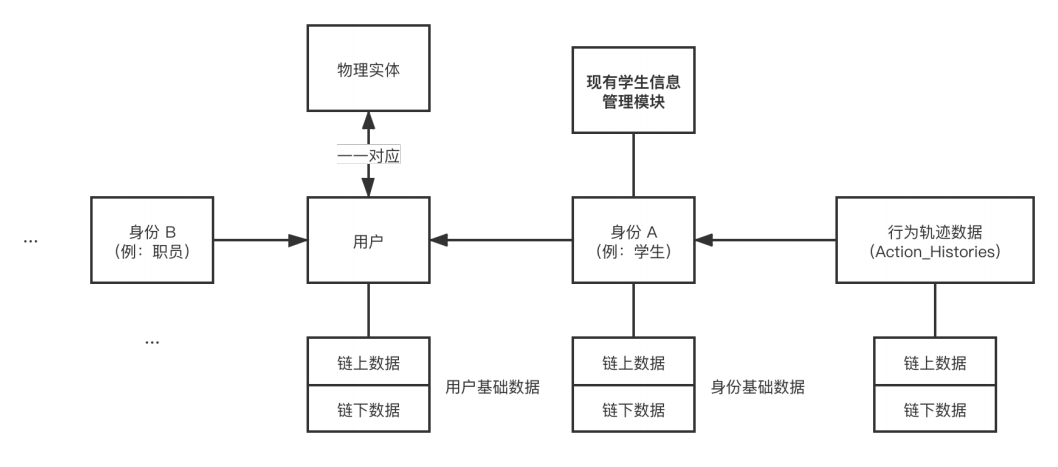
**「⾼校学⽣信息管理系统」中的「学⽣信息管理模块」，通过由学校建⽴的凭证发⾏者（Issuer）连接到「数字身份系统」。**



图**8** 数字身份架构与⾼校学⽣信息管理系统的对接

**2.1.1.3 数字身份系统的数据结构**

在 2.1.1.1节 的系统架构的基础上，数据结构如下所示：



图**9** 数字身份系统的数据结构

通过这个数据结构，可以达成下⾯⼏项⽬标：

·在与现有学⽣信息管理模块对接中，只需要现有的模块开放 API 接⼝，⽆需进⾏过多的代码改动。

·通过链接数字身份系统，能做到在不修改原有系统数据库的情况下，扩充学⽣身份中的信息的丰富

程度。

·通过⾏为轨迹、身份、⽤户均可追溯到唯⼀的物理实体，实现**⽆⻢甲**，进⽽实现**「极⾼作恶成本」**。

·⾏为轨迹数据保持连续，消除以往身份切换时的「数据断崖」（详细说明⻅ 2.2 节 与 第 4 章）。

**2.1.2** **链改效果**

**信息单薄** **→ 信息丰富**

通过链接数字身份系统，能做到在不修改原有系统数据库的情况下，扩充学⽣身份中的信息的丰富

程度。

**身份封闭** **→ 身份开放**

传统的学⽣信息（学⽣卡）只能在本校内本识别与验证，导致学⽣只能使⽤本院的图书馆、运动场、⻝堂、讲座、线上线下课程等资源。

通过与数字身份系统，可以让互信实现「权限控制」下的资源共享，共享⾃然也要遵循逐步推进的原则。

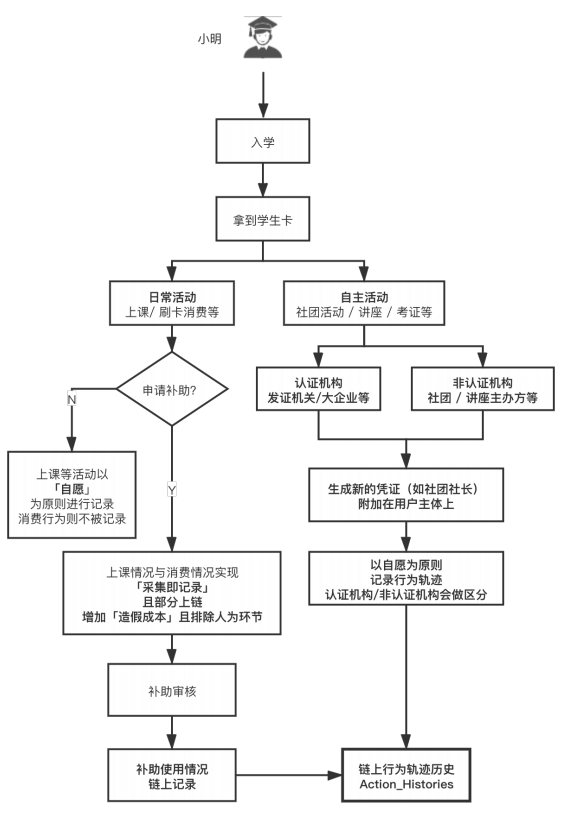
激进⽅案导致的结果：

曾许诺“不建围墙”的⼴州⼤学城，还是向现实低了头

**2.2 基于⾏为轨迹记录，针对业务信息管理模块的链改**

**2.2.1 链改⽅案**

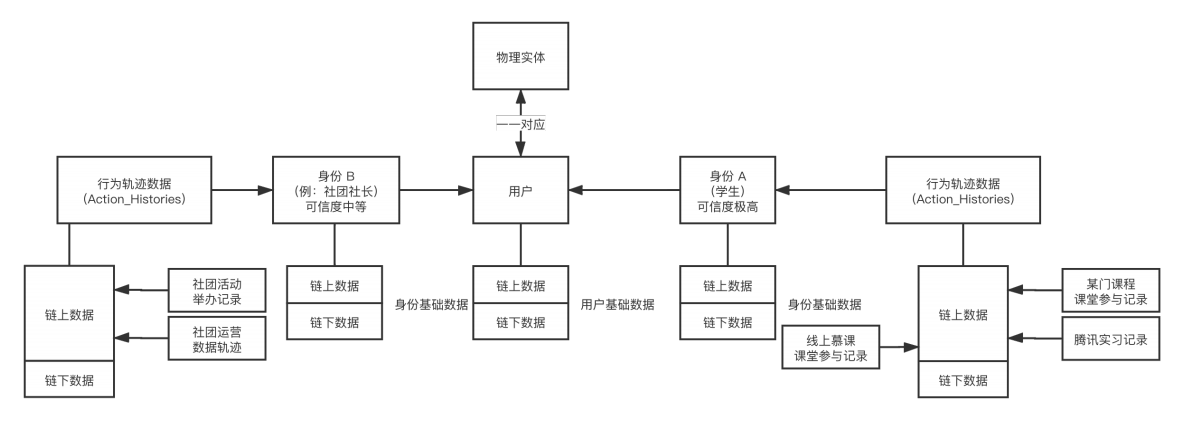
相较于信息管理模块，业务信息管理模块的链改更进⼀步，在经过学⽣同意的情况下，将学⽣的⾏为轨迹记录在链上。 我们以学⽣⼩明的⼤学⽣涯为例说明⾏为轨迹是如何记录的：



图**11** ⼩明的⾏为轨迹记录流程

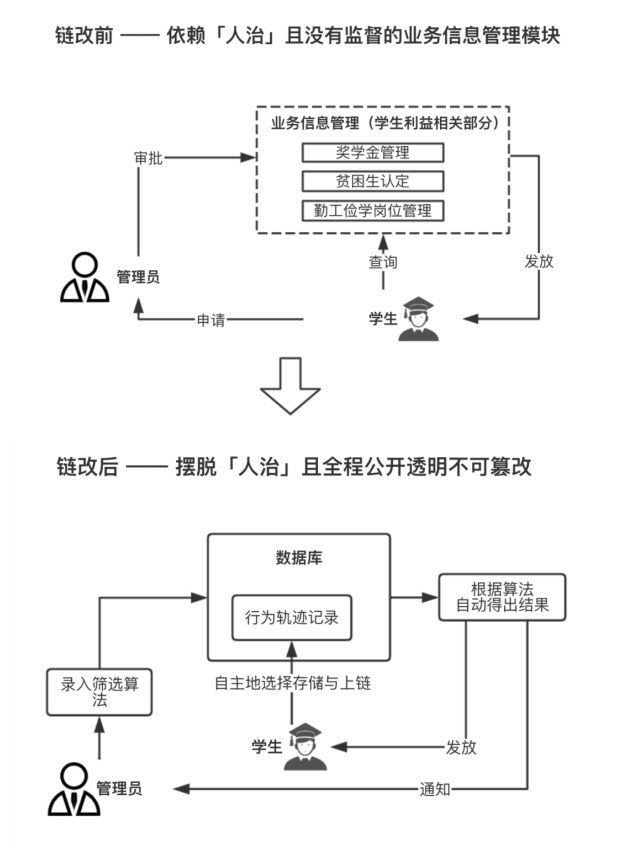
⼩明在学校的⾏为轨迹通过区块链记录下来，并附着在数字身份凭证上，例如作为社⻓所举办的活动记

录附着在社⻓身份凭证上。在纳⼊⾏为轨迹记录的功能模块后，我们可以展示出 2.1.1.3节 中所描述的数字身份系统的数据结构的全貌了：



图**12** 完整的数字身份系统的数据结构 **—** 以某学⽣为例

在纳⼊⾏为轨迹记录的功能模块后，图 4 所描述的传统运⾏流程将转变为如下图所示的新流程：



图**13** 链改改变运⾏流程

**2.2.2 链改效果**

我们可以看到，链改解决了传统流程中的三⼤问题：

·**⽆法保证公平公正的「⼈治」→ 根据提供的筛选算法⾃动得出结果**

传统系统中，管理员完全掌握审批权限，导致存在「权⼒滥⽤」的可能性。链改之后，管理员仅能提供筛选算法，结果由算法在数据库中筛查后⾃动给出，消除了过程中的⼈治。

·**⽆法保证学⽣提交信息的真实性 → 数字身份 + ⾏为轨迹记录作弊难**

传统系统中，除考试成绩等客观数据外，其它提交的资料存在「造假」的可能性。链改之后：**1**）伪造链上⻓期的记录成本⾼；**2**）与物理实体⼀⼀对应的数字身份系统让作恶⻛险巨⼤。

·**⽆法做到彻底的群众监督 → 全过程透明可监督**

传统系统中，最后虽然会公布结果，但是由于信息缺失（⼤多数情况下我们只是知道个⼈名罢了），⽆法做到彻底的群众监督。链改后，基于区块链数据透明化的特性，可保证全过程透明可监督。

⽐⽅说，任何⼀个⼈看到⼩明获得了「⼀等奖学⾦」，都可以去链上查询他⾃愿公开出来的客观信息。

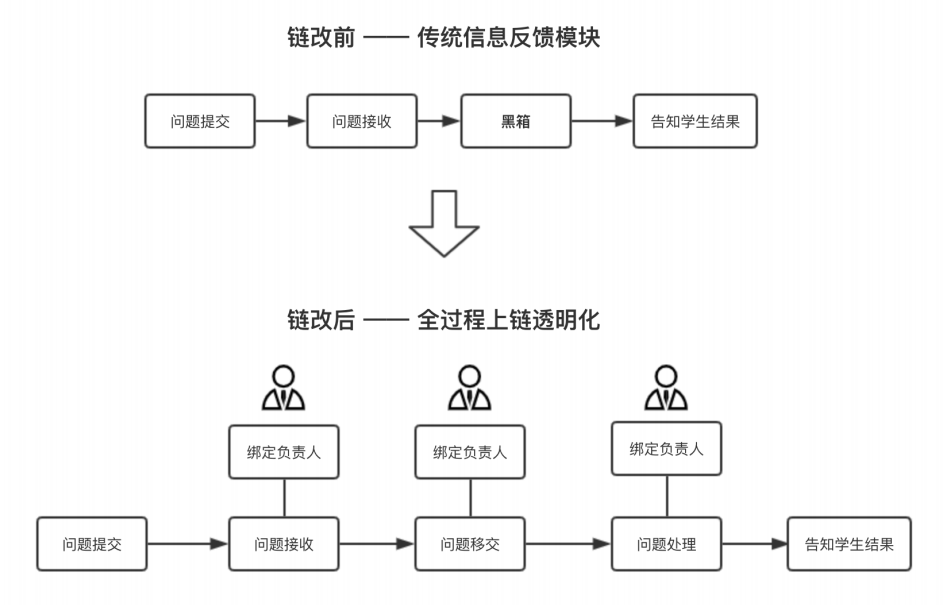
**2.3 基于数字身份，对信息反馈模块的链改**

数字身份并不局限学⽣，信息管理系统中的管理员（如辅导员），同样应该具备数字身份。

通过数字身份与区块链技术的综合运⽤，反馈信息的链路才能保证「全程可追踪、全⽹公开的读权限、全过程不可篡改、每⼀个环节都能找到负责⼈」这四⼤特性。

虽然，⽬前是以学⽣信息管理系统中的信息反馈模块的链改为例⼦来说明信息的追踪，但本思路同样适⽤于其它的投诉系统（例如企业与政府的投诉系统）。

**2.3.1 链改⽅案**



图**14** 信息反馈模块的链改

信息反馈模块链改⽅案的特性如下：

·连接数字身份系统，使每⼀个环节都和具体负责⼈绑定；

·利⽤区块链「公开透明」的数据特性使全过程可追查；

·利⽤区块链「不可篡改」的特性使全过程不可篡改；

·每⼀条记录均会加上时间戳。例：「某年某⽉某⽇，某问题转交给某个负责⼈」。

**2.3.2 链改效果**

对于各类投诉系统⽽⾔，通过「公开透明且不可篡改」的区块链技术可以解决传统系统中的如下问题：

·**⿊箱的过程 → 全程可追踪**

传统投诉系统中的处理流程是⼀个「⿊箱」的过程，在投诉后只能等待最终处理结果。在这个过程中，往往不知道已经进⾏到了哪⼀步，以及负责⼈是谁。基于区块链数据透明化的特性，我们可以**实现问题处理全程可追踪。**

·**被限制的查看权 → 全⽹公开的读权限**

有的传统投诉系统中，投诉⼈只能看到⾃⼰的投诉信息，⽆法形成「全⽹监督」。链改之后，基于区块链数据透明化的特性，**我们可以实现所有记录均可被全⽹查看。**

·**被篡改的记录→ 全过程不可篡改**

传统投诉系统中，记录可以被「增删查改」，以往的处理历史可以被轻易抹除。链改之后，**所有的历史记录都会被保存下来被所有⼈监督。**

·**找不到的负责⼈→每⼀个环节都能找到负责⼈**

传统投诉系统中，我们难以知道我们的问题现在正在什么⼈⼿上被处理。链改之后，基于数字身份的投诉系统让每⼀个环节都和具体的负责⼈绑定，我们可以**清楚地知道「该问谁」。**

**2.4 链改⽅案的注意事项**

**2.4.1 是否上链由数据主⼈选择**

信息上传区块链意味着所有⼈对这份数据都具有了「读权限」。那么，⾸先我们要厘清「开放读权限」的优点与缺点。

**优点**：权限的开放增强了信息的「可达性」，任何⼈都能⽆⻔槛的读取数据。

**缺点**：⼀旦不适合上链的数据上链，就会⾯临「数据滥⽤」的可能性。

所以，就⽬前⽽⾔，⼀个好的解决⽅案是让「上链权归数据主⼈」，数据主⼈（如学⽣）⾃主选择哪些数据应该上链。

**2.4.2 避免主观数据上链**

对于⼀个区块链应⽤⽽⾔，数据上链的⽬标是增强数据的「可信度」。

例如，我们使⽤基于区块链的唯⼀性的数字身份系统，就会增加「将不可信数据上链」的作恶成本，从⽽增强了链上数据的**可信度。**

那么我们思考⼀个问题：**主观数据的上链对于增强数据的可信度有帮助吗？**

我认为答案是否。客观数据是容易证伪的，⼤家可以验证「某⼈某年某⽉某⽇在某地做某事」是否真实。但是主观数据——例如某⼈对另⼀个⼈的评价并不具有⼀种可证伪性。

因此，我们在系统设计的时候应该避免主观数据的上链。

**3 链改⽅案总结**

这⼀链改⽅案的基础是**「数字身份系统」。**

构建了和物理实体唯⼀挂钩的数字身份系统，避免「换⻢甲」和「记录可篡改」，「守信奖励」和「失信惩罚」才有了意义。

在数字身份系统的基础上，基于区块链的「链上数据不可篡改、数据库读权限完全开放、时间戳不可篡改」等特性，我们有如下几条发展路径：

·**建⽴学⽣⾏为轨迹记录**

传统的业务信息存在「⽆法保证公平公正的「⼈治」、⽆法保证学⽣提交信息的真实性、⽆法做到彻底的群众监督」三⼤问题，通过数字身份系统 + ⾏为轨迹记录，我们能实现「根据提供的筛选算法⾃动得出结果、数字身份 **+** ⾏为轨迹记录作弊难、全过程透明可监督」的成效。

·**建⽴链上信息反馈系统**

传统的信息反馈系统具有过程⿊箱、查看权被限制、记录可篡改、负责⼈找不到等缺点，利⽤区块链公开透明的特性，结合数字身份系统，可以实现「全程可追踪、全⽹公开的读权限、全过程不可篡改、每⼀个环节都能找到负责⼈」的链上信息反馈系统。在整个链改过程中，我们需要遵循「是否上链由数据主⼈选择」与「避免主观数据上链」两个原则。

在以上这些发展路径中，就成本⽽⾔，线上互通与链上信息反馈系统的研发成本较低，线下资源互通与⾏为轨迹记录的研发成本较⾼。

需要说明的是，链改⽅案并未给出降本增效的详细测算，原因如下：

⾼校学⽣信息管理系统的运营主体是⾼校⽽⾮企业，产品逻辑和企业的商业逻辑有所区别，就链改效果⽽⾔，更偏向于定性⽽⾮定量。

**4 基于「数字身份」与「⾏为轨迹记录」的新型凭证系统**

在本章中，将对 2.1节 与 2.2节 中所提到基于「数字身份」与「链上⾏为轨迹记录」的新型凭证系统

（链上⾏为轨迹记录：如记录课堂表现）的特性进⾏详细阐述。

**4.1 从「传统凭证系统」到「新型凭证系统」**

传统凭证系统中的凭证（如毕业证、成绩单）如存在以下缺点：

·**能颁发可信凭证的机构数量少**

只有少量的凭证可以被签发与验证，例如学位证、毕业证、等级证书等。可信证书的发⾏是⼀件⾮常中⼼化的事情。

·**凭证中包含的信息少**

「⼤学成绩单」是「⼤学毕业证」的⼀项「附属表」，仅凭「⼤学成绩单」我们所能掌握的信息并不多。传统的⽅案下，信息在浓缩、归纳时损失了⼤量的客观信息。

·**造假成本低**

凭证造假是⼀种⾮常常⻅的⾏为。⼀⽅⾯，这种⾏为增加了企业成本；另⼀⽅⾯，造假造成的「失信成本」由包括守信者在内的所有⼈共同承担。

基于「链上⾏为轨迹记录」的系统克服了上述缺点，具有如下特点：

**·能颁发可信凭证的机构数量少 → 凭证/凭证颁发机构多级化**

发⾏凭证的单位有多个级别，⽽不是过去可信单位/不可信单位的⼆分法。例如，⾼校中⼀个运营了⼗年以上的有良好信誉的社团，可以有更⾼的信⽤等级。

这样，发⾏凭证实现了「弱中⼼化」，提⾼了凭证的多样性。

**·凭证中包含的信息少 → 凭证附带⼤量可信客观数据**

通过记录「⾏为轨迹」，凭证中附带了⼤量的可信客观数据。在传统的⽅案中，在凭证中存储的其实是客观数据的抽象，相当于「客观数据-哈希函数-> 凭证附

带的描述」，我们⽆法从附带数据中还原客观数据。即使从客观到描述的函数在后来进⾏了优化，我们也⽆法重新⽣成描述。

此外，对于第三⽅（例如企业）来说，并不总能相信这些函数，例如，为了学⽣好就业，学校可以「美化」他的成绩单。

因此，⼀个更合理的数据模型是对客观数据进⾏持久的、不可篡改的保存。这样，我们随时都能根据客观数据与不同的函数⽣成客观描述。我们甚⾄可以设想这样⼀个全新的毕业⽣求职场景——学⽣仅提供客观数据，分析由企业进⾏，避免了函数（算法）层⾯的不可信。

**·造假成本低 → 造假成本⾼**

⚪**伪造链上⻓期的记录成本⾼**

「给记录加上不可篡改的时间戳」是区块链系统的重要特性。

对于单次⾏为来说，造假的成本有限，例如「⽣成⼀张成绩单」、「参加⼀次活动」这样的单次数据容易造假，但是作为⼀种⻓期的记录，对「⾏为轨迹」持续造假的成本⾮常⾼昂。

⚪**与物理实体⼀⼀对应的数字身份系统让作恶⻛险巨⼤**

「**⾏为轨迹」是「凭证」的附属，「凭证」⼜是「数字身份」的附属，「数字身份」和「物理实体」是⼀对⼀的关系。**

在过去，造假⾏为的存在，仰仗于⼀个物理实体可以注册多个账户，如果某个账户作恶，那么⼀是可以将历史记录通过某种⽅式进⾏修改，例如在⽹站上进⾏评论控制；⼜或者直接换个⻢甲，例如「求职者提交虚假简历」的场景。

在新型的数字身份模型⾥，通过区块链技术我们可以做到三点：

**1）历史数据不可篡改。**

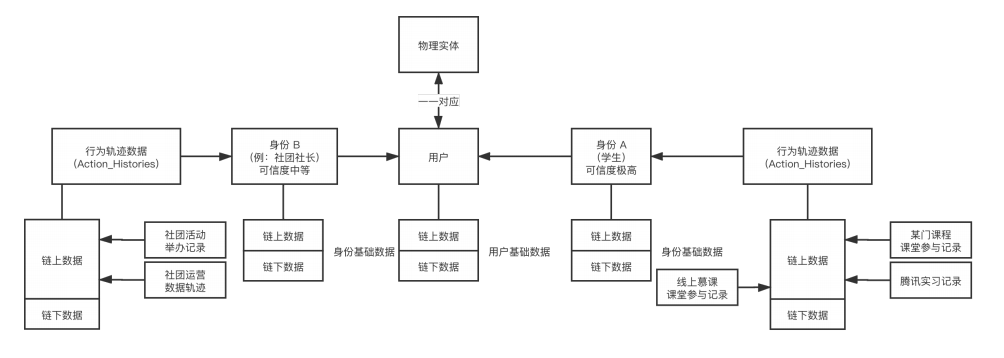
**2）历史数据和物理实体对应。**

**3）区块链数据库永久对所有⼈开放读权限。**

这两点保证了如果有使⽤者作恶，那么⼀⽅⾯他⽆法删除作恶证据，另⼀⽅⾯他⽆法更换⻢甲，另⼀⽅⾯任何区块链的访问者都有识破它的可能，这样就导致⼀个结果——使⽤者「⼀次作恶，终身承担作恶成本」，且随着时间的增加，作恶被⼈发现的可能不断增加。

从⽽，我们通过合理的机制（模型），⽽⾮道德遏制了作恶的可能性。

我们再来回顾⼀下 2.2.1节 中所提到的完整的数字身份系统的数据结构：



图**12** 完整的数字身份系统的数据结构 **—** 以某学⽣为例

**4.2 ⾏为轨迹的可延续性**

传统系统中，「不同的身份」之间是割裂的，相互之间联系薄弱。例如，⼩明毕业后去做了软件⼯程 师，他的「⼯程师」的身份和过去的「学⽣」身份间并没有什么联系。

正如前面所述，在这种情况下，学⽣**「毕业即失联」**，学校⽆法追踪学⽣毕业后的动向，除⾮学⽣主动提供信息。即使有主动的信息提供，这些信息往往也是模糊的，例如「在某段时间在某某公司就职」。

在新的基于「⾏为轨迹」的数字身份系统中，⾏为轨迹始终具有⼀致性。例如，⼩明毕业后，「学⽣身份」成为了旧的身份，但他的「⾏为轨迹」继续被记录，只不过新的记录依附在他的「职业身份」下。

在新的模式下，**校⽅便不再是被动接收学⽣提供的信息，⽽是可以主动从链上查询学⽣毕业后的动向，且查询到的是详细客观数据**。

事实上，学校课程体系与社会需求的⽭盾在互联⽹时代变得更加尖锐。如果学校能对学⽣在校数据与学⽣就业后的数据进⾏主动分析，并依据分析结果对学校现有的教学体系进⾏改善，这种现有的「断层」可能会缩短，离「学⽣ — 职场」⽆缝衔接的理想⽬标便会⼜进⼀步，但这⼜是另⼀个命题了。

# 个例：（学习小组项目- 现状与不足）

### 外国语协会“学习小组”项目申请

**一，简表**

目的：我们都知道水滴石穿的道理，但由于人类懒惰的天性，是很难坚持去做某一件事。正因如此，我想为社员申请创立一个学习小组项目。在记录每位社员的日常学习情况的同时，也可以记录他们的成长状态。每位社员都可以在小组里讨论学习，由组长负责对组员的激励，形成点对点的有效沟通，在日常的激励过程中开展相应的自发学习交流活动。在老师与核心成员的带领下，形成一个持续、有效、多方面的学习环境。

1. **立项依据**

**2.1背景**

长期以来，课堂教学以单一的个体学习为主，重个人能力的培养，忽视集体观念的教育；重学生独立思考，忽视群体之间的合作；重师生的纵向交流忽视学生之间的横向沟通。中国有一句俗语：一个中国人是条龙，三个中国人是条虫。虽然这句话有失偏颇，但确实反映了一些问题：我们培养的学生缺少合作精神与团队意识，不善于听取别人的意见，语言沟通能力较差。在全球化已成为21世纪重要特征的今天，人与人之间，民族与民族之间，国家与国家之间，以及人与自然之间互相依存的程度越来越高。学会共同生活（学会共处）成了一个重要的教育命题。与此一致，新课程也体现了诸如国家意识、民族精神、社会责任感、团队精神、民主与法制、人与自然和谐相处等新的培养目标，同时在课程实施改革中提出培养学生的“交流与合作能力”。该学习小组的成立符合时代发展的趋势，有利于外国语协会的持续发展。

**2.2费曼学习法**

费曼学习法的灵感源于[诺贝尔](https://baike.baidu.com/item/%E8%AF%BA%E8%B4%9D%E5%B0%94" \t "https://baike.baidu.com/item/%E8%B4%B9%E6%9B%BC%E5%AD%A6%E4%B9%A0%E6%B3%95/_blank)物理奖获得者理查德·费曼（Richard Feynman），运用费曼学习法，每个人只需花上20分钟就能深入理解知识点,而且记忆深刻,难以[遗忘](https://baike.baidu.com/item/%E9%81%97%E5%BF%98" \t "https://baike.baidu.com/item/%E8%B4%B9%E6%9B%BC%E5%AD%A6%E4%B9%A0%E6%B3%95/_blank)。知识分为两类，而我们绝大多数人关注的都是错误的那类。第一类知识注重了解某个事物的名称。第二类知识注重了解某件事物。两类看似无差别，但本质的确不同。著名的诺贝尔物理学家理查德·费曼（Richard Feynman）能够理解这二者间的差别，这也是他成功最重要的原因之一。事实上，他创造了一种新的学习方法，这使得他比别人对同一件事物了解的更透彻。

费曼学习法可以简化为四个单词：Concept （概念）、Teach （教给别人）、Review （回顾）、Simplify （简化）。

在学习小组的学习过程中，该项目为核心组长的学习成长提供了一个良好的学习机会。它需要核心组长具有较强的自我学习能力，能够利用费曼学习法将所学内容快速转化为内在知识，再向小组成员讲解概念的过程中进行二次学习，强化对该知识点的理解，并最终掌握并加以运用。

**2.3学习环境的定义**

### 国内已有定义

朱晓鸽（1996）在其论文中指出，学习环境指的是一种面对面的发生在学生与学习资源之间交流的学习过程。

杨开诚（2000）认为，学习环境是一种支持学习者进行建构性学习的各种学习资源（不仅仅是信息资源）的组合。其中学习资源不仅包括信息资源、认知工具、人类教师等物理资源，还包括任务情境等软资源。

武法提（2000）认为，学习环境是一个动态概念，它与动态的学习进程是紧紧联系在一起的，是学习活动展开的过程中赖以持续的情况和条件。武法提博士认为学习环境的要素就不仅仅是支撑学习过程的物质条件（学习资源），而且还包括教学模式、教学策略、学习氛围、人际关系等非物质条件。

何克抗、李文光（2002）两位学者认为，学习环境是学习资源和人际关系的组合。学习资源包括学习材料（即信息）、帮助学习者学习的认知工具（获取、加工、保存信息的工具）、学习空间（比如教室或虚拟网上学校）等等。人际关系包括学生之间的人际交往和师生人际交往。

### 国外已有定义

Wilson(1995)认为：学习环境是这样一个场所，学习者在这里相互合作，相互支持，并且用多种工具和信息资源相互支持，参与解决问题的活动，以达到学习目标。

荷兰学者Kirschner（1997）认为：学习环境是学习者能找到充分的信息资料和教育辅助手段的地方，借助学习环境，学习者能够有机会去根据自身的情况及其与他人的关系去构建定向基础，决定他们将介入的目标与活动。

乔纳森（Jonassen，1999）认为：学习环境是学习者共同体一起学习或相互支持的空间，学习者控制学习活动，并且运用信息资源和知识建构工具来解决问题。乔纳森认为，学习环境是以技术为支持的，在学习过程中技术是学习者探索、建构和反思学习的工具，提出了认知工具和学习策略的重要性并且还考虑了社会背景的支持因素问题。

### 对学习环境的理解

综合以上国内外学者对学习环境的定义，我们发现，学习环境与学习场所、空间、支持、技术工具、信息资源、共同体、建构性学习、情况与条件、社会环境有着密切的关系，我们可以从以下几个方面理解：

1.学习环境最基本的理念是以学习者为中心；

2.学习环境是一种支持性的条件；

3.学习环境是为了促进学习者更好的开展学习活动而创设的；

4.学习环境是一种学习空间，包括物质空间、活动空间、心理空间；

5.学习环境和学习过程密不可分，是一种动态概念，而非静态的。它包括物质和非物质两个方面，其中既有丰富的学习资源，又有人际互动的因素；

6.学习者在学习环境中处于主动地位，由学习者自己控制学习；

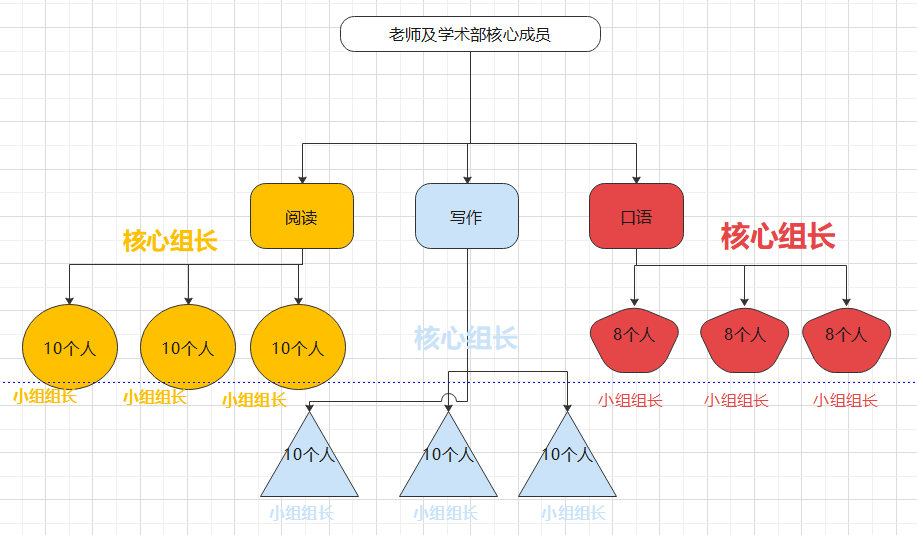
7.学习环境需要各种信息资源、认知工具、教师、学生等因素的支持；

8.学习环境可以支持自主、探究、协作或问题解决等类型的学习。

学习环境：是影响学习者学习的外部环境，是激发学习者主动学习和促进能力生成的外部条件。

学习小组是以学生为中心的自治组织形式，其发展状况的好与坏，一定程度上体现在其营造的学习环境。学习小组的初心就是为了吸引那些对英语感兴趣，想学好并熟练掌握的在校学生，大家一起交流，鼓舞与激励，形成我基础好我愿意教他人，我基础差我有动力与方向去学习的一种互帮互助的成长型学习环境。在知识上有老师与核心组长的答疑解惑，在行动上有小组成员间的相互激励，在社交上有一个可交流可共享的平台。总而言之，学习小组在今后的发展方向将不仅仅为英语学习提供有关良好的环境，还可以对其他语言与学科进行扩展，形成一个积极的，有效的，多方面的，友好的学习生态环境。

**三，学习小组结构图及成员选取：**



（1）.  确定小组规模。目前我们协会有180人左右，但由于我们学生整体基础较差，各方面都优秀的学生较少，缺乏可以胜任组长的人选，我们经过仔细考虑之后决定将我们协会分成阅读，写作与口语三大部分，每部分小组分别以10，10，8人为一小组进行划分。

（2）.  进行小组划分。小组建立的主要目的就在于帮助每个学生更好地进行学习，因此小组的划分应以学生的学习成绩作为重要依据。一般情况下，应使每个小组都同时拥有高、中、低三个层次的学生，在此基础上，再根据学生的性别、性格及单科成绩等特点进行个别调整，实现人力资源的最佳组合，我们将其称之为“组间同质，组内异质，优势互补”原则。“组内异质”能为小组成员之间互相帮助提供较大的可能（因为“差异”本身就是一种资源），而“组间同质”又可以为各小组间的公平竞争奠定良好的基础。

（3）.确定核心组长。根据协会目前的实际情况，我们核心组长的选取都来自于外国语协会学术部的成员。核心组长负责为小组成员制定相应的学习计划与任务，并能够第一时间回答小组成员有关的学习问题，在学习的过程中能够提供有效的学习渠道与资源，并对小组组长负责，与小组组长一起营造良好的学习氛围与环境。核心组长是灵活变动的，在学习小组成熟后，将会进行季度筛选，核心组长可以由协会或协会外任何一位具有扎实基础与较强组织能力的同学担任，经负责老师与协会成员的考核后上任，保证核心组长的流动性和成长性。从而确保小组组员学习知识来源的可靠性与学习的有效性。

（4）.确定小组组长。小组组长由核心组长任命，并对小组成员负责。需要其平时较认真负责，能起好领头和组织小组合作学习的作用。小组组长还需要了解小组组员的学习进程，记录小组学习的过程和结果，检查小组成员的学习情况，确认每位成员是否完成每日的学习任务等。小组组长可以采取轮流制，尽可能让每位组员都参与进来，发表自己的看法和见解，从而锻炼学生的语言组织能力，同时也避免出现有学生“搭车”的现象。小组组长应能与小组成员进行互动，善于营造学习氛围（比如，在小组成立的初期，让每位组员先自我介绍，说说学习的目标与目的，增加大家的公开项，相互熟悉，为之后小组成员间的交流与提问奠定了良好的基础.....）。

（5）.确定小组成员。小组组员必须是以自发性为前提的，对自己负责。我们欢迎并鼓励协会的每位成员积极地参与到我们学习小组中。对于自身的学习状态与情况，我们坚持客观，公平公正地态度去评价。各成员能够清晰明白自身学习的能力与学习的阶段，不好高骛远，脚踏实地，在小组中按时完成小组布置的任务并积极提。自身基础较好，不骄傲自满；自身基础较差，能够积极进取。秉承‘三人行必有我师焉’的学习态度，正确的与其他组员进行学习上的交流与沟通。

**四，预期进展**

（一），初步小组规模90人（11月1号到12月底）

各小组初步成立初期，先营造学习氛围，了解各小组成员的学习目标与学习情况后，确定学习材料与任务。

1. ，中期小组规模150人 （次年1月至一月底）

核心组长的第二轮筛选。小组组长的优化。小组成员以“组间同质，组内异质，优势互补”进行重新优化分组。学习材料与任务将向更加系统性的方向发展。

1. ，后期小组规模，全协会成员 （2020年第二学期开始）

将会开展小组间的“学习竞争”互补，激励学习的环境与平台。学习语言与环境多方面发展的方向及小组性质的重新整合。

整体阶段：学习小组在今后的发展一定不单单只有阅读小组，写作小组与口语小组，可能还会演化出戏剧小组，日语小组，歌唱小组，品茶小组，冥想小组以及学习国内外文化的相关小组等。外国语协会能做到的就是提供一个平台，任由有能力与想法的协会成员去将各小组发展壮大，并为之提供等价的服务，让协会的成员在每个小组中找到最适合自己的部分，并不断地挖掘放大，从中找寻自我价值与意义，激发学习的探索欲并享受其中。使其能够在学习小组的良好环境中学会自我成长，懂得如何与他人建立友好的关系。建立一个即使是组员在离校后，也能相互学习与交流的一个小组。在将来的学习与工作中为自我，为他人，为协会，为学校，为社会，为国家，为全世界，乃至全宇宙创造价值并提供不懈动力。

1. **学习小组发展需思考的问题**

1.学习小组的初心（如何在面临经济与权限的冲突时，保持协会的初心与学习小组初心始终如一？）

2.核心组长与小组组长的选取 （作为学习小组的中坚力量，如何做到有效又合理的选取？）

3.推送内容的来源与任务布置（如何保证一个优质的学习内容与任务的有效传输？）

4.如何有效的提高小组成员的学习积极性 （如何调动学习基础差又毫无学习动力的成员？）

5.是否有相关奖励机制 （如何合理利用会费去奖励相关负责人与相关活动与工作有关的人员？）

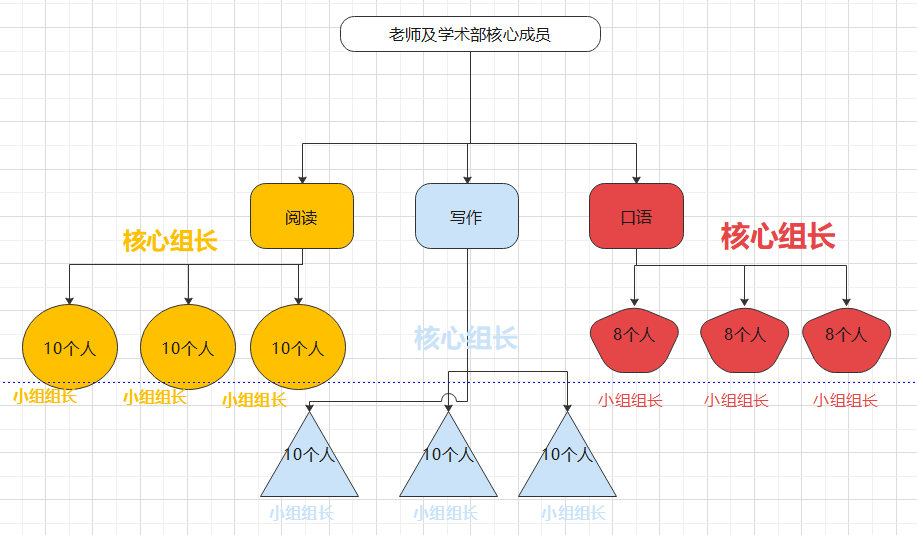
6.如何有效的进行小组管理 （怎样去创造有关成长型的协会与学习小组？）

7.对小组未来发展方向的思考 （是以短期协会利益的被动性的线性影响，还是以长期集体利益的自发性的幂次影响为主？ 这是我们各组组长乃至协会全体干事都必须去思考的重要事情。）

**第一阶段（2020年10月16日-10月30）**

1. 目的：我们都知道水滴石穿的道理，但由于人类懒惰的天性，是很难坚持去做某一件事。正因如此，我想为社员申请创立一个学习小组项目。在记录每位社员的日常学习情况的同时，也可以记录他们的成长状态。每位社员都可以在小组里讨论学习，由组长负责对组员的激励，形成点对点的有效沟通，在日常的激励过程中开展相应的自发学习交流活动。在老师与核心成员的带领下，形成一个持续、有效、多方面的学习环境。

2.成员结构



1. 闪光点

口语小组敢于开口说英语的小伙伴多

口语小组大部分同学坚持每日学习打卡，为自己一天的学习状态开了头

阅读与写作小组的有为每日知识点做了详细笔记与扩展的同学

1. 存在的问题

①出题组成员主要由学术部的成员担任，成员较少，压力大，出题内容水平不一。

②没有专门的指导老师，缺少指导依托。

③缺少可交流话题，成员与成员间交流少。

④缺少专门的学习场地，可供大家一起晨读，自习或者学习交流。

⑤单一主体，缺少自主运营性，负责人压力大。(部长每天晚上要催出题，要审查题目，要反馈出题，要优化出题界面和内容。为此操碎了心。[叹气])

⑥口语，阅读与写作小组的学习氛围不平衡。

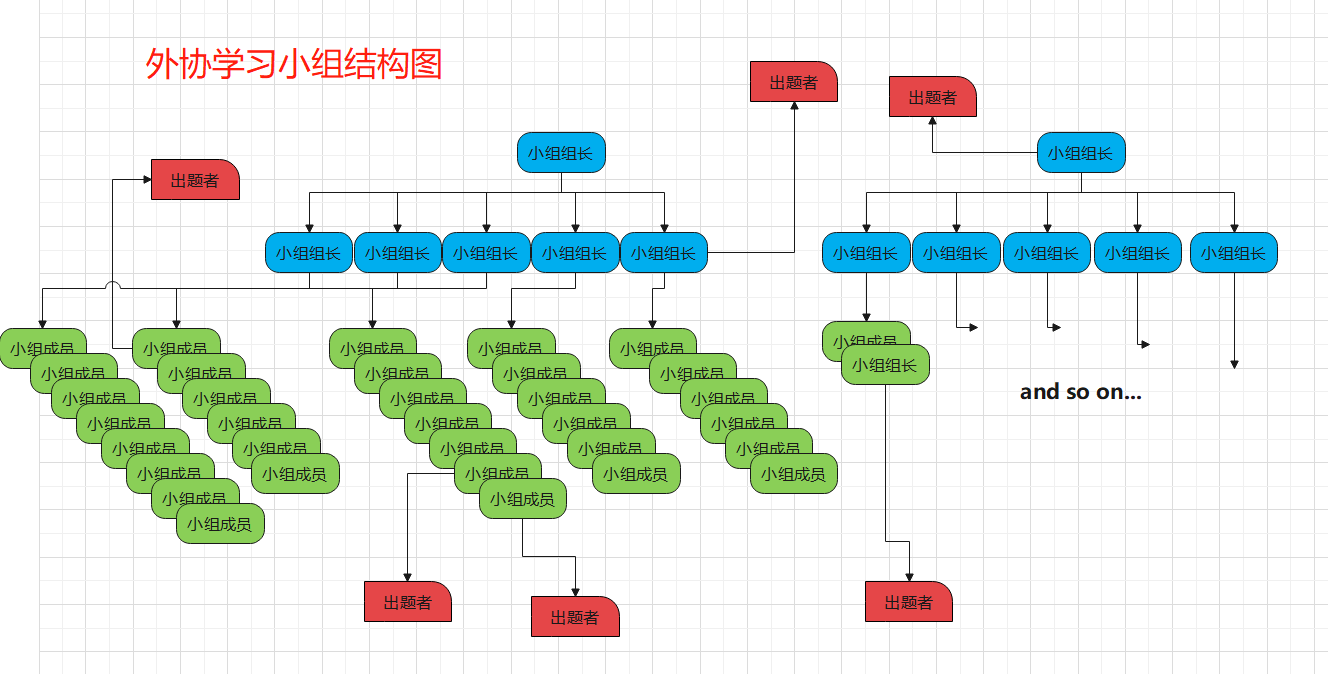
⑦缺少奖励机制与大目标

**第二阶段（2020年11月30日起）**

1. 目的

还是保持初心不变。小组组长对组员日常学习情况记录负责，为大家提供一个可交流，可互助，可成长的自主型平台。每日的学习任务可助于养成坚持做某事的习惯，5-10分钟的小任务开启自己一天的学习状态。

1. 成员结构



1. 运作模式

①出题成员由学术部成员转向学习小组成员，可以是小组组长或者小组成员自愿申请出题。（每周日前确定下一周每日的出题人。星期六进行这一周的出题的评比，获票最多者可获得一定金额的“奖励金”。若此周出题人未满4名，“奖励金”积累至下周。）

②学习小组的每位成员都会有自己的小组组长，小组组长对自己的小组成员日常学习情况负责（现在主要是记录自己小组成员的任务完成情况）。

③小组组长自愿担任，可向群里说明意愿申请加入小组组长。小组组长根据自己的精力与意愿设置成员人数，建议管理的小组成员为（8-10）人。

④每日学习任务的记录以出题人的任务为主。如果该天没有出题人，则以自己的英语学习任务为主，在有关英语的学习材料上截图发给自己的小组组长。

⑤小组成员的学习情况会在学期结束后进行结算，进行排名奖励。

1. 出题者要求

①内容以英语为主

②题目内容精简，完成时间5-10分钟左右

③有详细的解析或者自己的见解

④题目尽量原创，可结合自己的专业知识与学习技巧，给人启示

⑤题目界面整洁，字体适中（PPT或者word）

⑥能清楚地解析小组成员对题目的疑惑

1. 闪光点

①无主体运行，自主式学习

②出题者与小组成员的互动，有利于提高小组成员的出题水平与学习交流氛围

③任务自主性强，不单单是依托出题者，而是更在于自己的每日英语学习

④有一定的奖励机制

⑤集思广益，出题者为成员提供了一个学习方法与思想

⑥可在无专门老师指导的情况下，营造我有意愿与能力我当“老师”的学习氛围

**第三阶段（展望）**

1目标：

学习小组在今后的发展一定不单单只有阅读小组，写作小组与口语小组（现今三组合并为统一的学习小组），可能还会演化出戏剧小组，日语小组，歌唱小组，品茶小组，冥想小组以及学习国内外文化的相关小组等。外国语协会能做到的就是提供一个平台，任由有能力与想法的协会成员去将各小组发展壮大，并为之提供等价的服务，让协会的成员在每个小组中找到最适合自己的部分，并不断地挖掘放大，从中找寻自我价值与意义，激发学习的探索欲并享受其中。使其能够在学习小组的良好环境中学会自我成长，懂得如何与他人建立友好的关系。建立一个即使是组员在离校后，也能相互学习与交流的一个小组。在将来的学习与工作中为自我，为他人，为协会，为学校，为社会，为国家，为全世界，乃至全宇宙创造价值并提供不懈动力。

1. 发展观

没有如何事情是一蹴而就的，不管是学习也好，还是学习小组的发展也好。我们都要相信万事万物都是一个螺旋式上升的一个过程。既然大家当初选择了加入我们的外国语协会，一定保证想学好它的期望。我也希望大家能积极地参与与协会有关的一切活动，因为我们才刚刚开始，可能会有许多地方都做的不太好。我希望我们能一起去改善之，并从中得到一份成长。我希望大家能通过这个平台在日常的学习交流中，摆脱本能的固定型的思维，行成一种成长型的思维模式。

至此，因为专业的原因，我可能先与各位告一段落。感谢前两个星期各位成员的参与，感谢那些为了出一份满意的题目而修改多次的出题成员，感谢我们的小组组长的协助，也感谢外协这个平台让我们在此相遇。也希望在学习小组的第二个阶段，我们会有所知，有所好，有所乐。愿我们在各自的领域展翅翱翔....

# 结合个例对其他可扩展的方向的结合

从具体实践中我们可以发现，基于区块链的数字身份认证的对学生身份的必要性。数字身份认证能够记录学生的活动状态。有效的促进有意义的社团活动的活跃度，在一定的程度上减少了活动成员的“划水现象”。

# 技术的实现

1. 需要工具： remix
2. 利用“供应链”模式，解决数字身份系统的运用。