이더리움 기반 학습 인증 서비스 개발

2021후기 중간보고

08번-D분과-PLMS팀

부산대학교

201645825이승윤, 201645819심재영, 201824444김유미

지도교수 김호원



**목차**

[1 요구사항 및 제약사항 분석에 대한 수정사항 2](#_Toc99307070)

[1.1 과제 목표 2](#_Toc99307071)

[1.2 요구사항 분석과 수정 3](#_Toc99307072)

[1.3 제약사항 분석과 수정 5](#_Toc99307073)

[2 설계 상세화 및 변경 내역 6](#_Toc99307074)

[2.1 블록체인 6](#_Toc99307075)

[2.2 서버 6](#_Toc99307076)

[2.3 웹 6](#_Toc99307077)

[3 갱신된 과제 추진 계획 7](#_Toc99307078)

[3.1 개발 일정 7](#_Toc99307079)

[4 구성원별 진척도 8](#_Toc99307080)

[4.1 구성원별 진행사항 8](#_Toc99307081)

[5 보고 시점까지의 과제 수행 내용 및 중간 결과 8](#_Toc99307082)

[5.1 과제 수행 내용 8](#_Toc99307083)

[5.2 중간 결과 8](#_Toc99307084)

[6 인용 자료 8](#_Toc99307085)

# 요구조건 및 제약사항 분석에 대한 수정사항

## 과제 목표

매번 발급하고 위변조를 확인해야 하는 인증서, 결과만 나와있는 인증서, 다양한 기관에서 발행된 인증서, 과연 믿을 수 있을까? 우리 PLMS팀은 블록체인을 이용하여 자신의 능력을 체계화된 방법으로 증명하고 다양한 사람들이 질 좋은 교육 콘텐츠와 만날 수 있는 “바름” 플랫폼을 개발하고 있다. 블록체인을 이용하여 학습 데이터의 안정성과 투명성을 보장하여 위변조를 방지할 수 있다. [1] [2] 학습 진행 과정을 파악하여 평가 시스템의 공정성을 확보하고 학습 과정에 대한 신뢰성을 높인다. 누구나 학습 컨텐츠를 공급하고 [1] 소비할 수 있으며 학습한 내용을 손쉽게 인증할 수 있다.



그림 1 시스템 구조도

## 요구사항 분석과 수정

|  |  |
| --- | --- |
| 요구사항 | 수정 내용 |
| 계정 | 기존에는 사용자 ID와 이메일을 따로 수집하였지만 아이디를 이메일로 하여 중복 항목을 수집하지 않도록 개선하였다. |
| 강의 검색 | 강의 제목으로 검색하는 기능 외에 강의 요약, 강의자에 키워드가 포함된 경우를 검색 가능하도록 수정하였다. |
| 강의 수강 | 사용자가 수강하지 않는 강의를 URL을 통해 접속할 경우 강의 정보 화면으로 이동하여 강의 정보를 살펴보고 수강 신청할 수 있도록 하였다. |
| 학습 진행 과정 저장 | 비용 문제를 고려하여 모든 단계에 대해 기록하는 것이 아니라 각 수업 차시 별로 출석 또는 채점 완료가 된 이후에 이더리움 블록체인에 기록하도록 정하였다. |
| 과정, 수업 수료 인증  수료 확인 | 별도 수정사항 없음 |

표 1 요구사항 수정사항

## 제약사항 분석과 수정

|  |  |
| --- | --- |
| 제약사항 | 대책 |
| 대부분의 학습 과정에 있어 인터넷 연결이 필요하다. | 강의 영상 오프라인 다운로드를 고려하였으나 첫째, 강의 영상 수강 완료 여부를 바르게 확인할 수 없다. 둘째, 오프라인 다운로드에 의한 네트워크 부담이 예상된다. 셋째, 웹 기반 서비스로 별도의 재생 관리 어플리케이션이 없는 상태이다. 따라서 해당 기능 지원이 어렵다고 판단하였다. 향후 모바일용 어플리케이션을 제작할 경우 오프라인 재생 기능 탑재 고려할 수 있다.  현재는 인터넷 연결이 가능한 경우에만 서비스 가능하다. |
| 기존 학습 데이터의 연동이 필요하다. | 해당 사이트에 학습 진행 과정 기록이 남아있는 경우 블록체인에 진행 과정과 결과를 반영하고 수료 확인 서비스도 즉시 제공 가능하다. 학습 결과만 있는 경우 수료 확인 정보만 제공 가능하다. 수강한 사이트가 없어지거나 간편한 인증을 위해 우리 서비스를 사용하도록 유도할 수 있다. |

표 2 제약사항 수정사항

# 설계 상세화 및 변경 내역

## 웹

## 서버

데이터베이스를 설계하면서 기존 기능 요구사항의 중복된 항목에 대한 통합을 수행하였다. 강의와 관련된 테이블을 정리하여 강의, 수강 중인 강의, 강의 내용(차시별), 문제, 학습 과정으로 테이블을 구성하였다. 또한 테이블 내부에서 칼럼이 중복되지 않도록 예를 들어 강의 사용자 id와 이메일을 통합하였다. 이 과정에서 기능 요구사항이 일부 변경되었다.

블록체인 기능과의 통합이 필요하다. 앞서 산학협력 프로젝트 멘토님께서 조언해주신 대로 기능/통합 테스트를 추가하여 먼저 웹과 서버의 통합 테스트를 거친 후 블록체인 기능을 서버에 도입하여 서버 내에서 기능 테스트를 거쳐 배포하고 웹과 통합하여 다시 통합 테스트를 수행할 예정이다.

## 블록체인

웹과 서버 연동 테스트 이후 본격적인 이더리움 탈중앙화 분산 어플리케이션 제작과 서버와의 연동 과정을 수행 예정이다. 우선적으로 Geth, 가나슈, 트러플, 메타마스크를 이용하여 개발환경 설정을 완료하였다.

모든 정보를 블록체인에 저장한다면 많은 수수료 비용이 발생하고 트랜잭션 처리에 따른 문제가 발생할 수 있다. 가장 중요한 학습 데이터 중 완전히 학습을 완료하여 더 이상 데이터 변경이 발생하지 않는 데이터만 블록체인에 기록하도록 설계를 변경하였다.

과정 수료 인증 기능에서 과정에 새로운 수업이 포함된다면 dApp을 다시 배포해야 하므로 강의자가 임의로 과정을 생성하거나 추가할 수 없도록 웹 레이아웃을 변경할 예정이다.

# 갱신된 과제 추진 계획

## 개발 일정

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 업무 | 2월 | | | | 3월 | | | | 4월 | | | | | 5월 | | | | 6월 | | | | |
| 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 | 1 | 2 | 3 | 4 | 1 | 2 | 3 | 4 | 5 |
| 지도교수 상담 및 멘토 매칭 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 착수보고서 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 이더리움 학습 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 웹 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 서버 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 데이터베이스 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 학습 컨텐츠 제작 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 중간보고서 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 웹 개발 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 서버 개발 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 스마트 컨트랙트 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 기능/통합 테스트 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 스마트 컨트랙트 개발 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 추가 연구 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 최종보고서 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 최종 발표 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SW 등록 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

완료된 일정은 검정, 진행 예정인 일정은 밝은 회색으로 표시하였다.

# 구성원별 진척도

## 구성원별 진행사항

|  |  |
| --- | --- |
| 이름 | 역할 |
| 이승윤 | 서버, 데이터베이스, API 설계 (완료)  Local 서버(windows) 및 remote 서버(ubuntu) 구축 (완료)  데이터베이스 구축 (완료)  API 제작 및 연동 (진행 중)  탈중앙화 분산 어플리케이션(dApp) 개발 (진행 중) |
| 심재영 | 각자 맡은 역할 서술 (상태 – 완료, 진행 중) |
| 김유미 | 각자 맡은 역할 서술 (상태 – 완료, 진행 중) |
| 공통 | 블록체인, 이더리움 개념 학습  웹 페이지 레이아웃 설계  개발 환경 설정 |

표 5 구성원별 역할

# 보고 시점까지의 과제 수행 내용 및 중간 결과

## 웹

## 서버

### 데이터베이스 설계

* 사용자

|  |
| --- |
| user 사용자 |
| id VARCHAR(64) PRIMARY KEY, |
| pw VARCHAR(32) NOT NULL, |
| detail VARCHAR(256) NOT NULL, |
| phone VARCHAR(16) NOT NULL |

* 강의

|  |
| --- |
| class 강의 |
| id INT PRIMARY KEY AUTO\_INCREMENT, |
| name VARCHAR(128) NOT NULL, |
| detail VARCHAR(1024), |
| userId VARCHAR(64), |
| FOREIGN KEY (userId) REFERENCES user (id) |

* 수강 중인 강의

|  |
| --- |
| takingClass 수강 중인 강의 |
| userId VARCHAR(64), |
| classId INT, |
| PRIMARY KEY (userId, classId), |
| FOREIGN KEY (userId) REFERENCES user (id), |
| FOREIGN KEY (classId) REFERENCES class (id) |

* 강의 (차시별) 내용 종류

|  |
| --- |
| contentType 강의 내용 종류 |
| name VARCHAR(16) PRIMARY KEY |

* 강의 (차시별) 내용

|  |
| --- |
| content 강의 내용 |
| classId INT, |
| contentId INT, |
| type VARCHAR(16) NOT NULL, |
| title VARCHAR(128) NOT NULL, |
| url VARCHAR(128), |
| PRIMARY KEY (classId, contentId), |
| FOREIGN KEY (classId) REFERENCES class (id), |
| FOREIGN KEY (type) REFERENCES contentType (name) |

* 강의 (차시별) 내용 시험

|  |
| --- |
| question 문제 |
| classId INT, |
| contentId INT, |
| questionId Int, |
| title VARCHAR(128) NOT NULL, |
| answer VARCHAR(1024) NOT NULL, |
| PRIMARY KEY (classId, contentId, questionId), |
| FOREIGN KEY (classId, contentId) REFERENCES content (classId, contentId) |

* 학습 과정 상태

|  |
| --- |
| processState 학습 과정 상태 |
| name VARCHAR(32) PRIMARY KEY |

* 학습 과정

|  |
| --- |
| Process 학습 과정 |
| classId INT, |
| contentId INT, |
| date DATETIME NOT NULL DEFAULT CURRENT\_TIMESTAMP ON UPDATE CURRENT\_TIMESTAMP |
| state VARCHAR(32) NOT NULL, |
| score INT NOT NULL, |
| feedback VARCHAR(1024), |
| isSaved BOOLEAN NOT NULL DEFAULT FALSE, |
| PRIMARY KEY (classId, contentId), |
| FOREIGN KEY (state) REFERENCES processState (name) |

* 강의 공지사항

|  |
| --- |
| Notice 강의 공지 |
| id INT PRIMARY KEY AUTO\_INCREMENT, |
| classId INT, |
| title VARCHAR(128) NOT NULL, |
| contents VARCHAR(1024) NOT NULL, |
| userId VARCHAR(64), |
| date DATETIME NOT NULL DEFAULT CURRENT\_TIMESTAMP, |
| modificationDate DATETIME NOT NULL DEFAULT CURRENT\_TIMESTAMP ON UPDATE CURRENT\_TIMESTAMP |
| FOREIGN KEY (classId) REFERENCES class (id), |
| FOREIGN KEY (userId) REFERENCES user (id) |

### API 설계

|  |  |  |  |
| --- | --- | --- | --- |
| 기능 | 주소(address) | 파라미터(parameter) | 반환(return) |
| 로그인 | user/signin | id, pw | user, result |
| 로그아웃 | user/signout |  | result |
| 회원가입 | user/signup | id, pw, detail, phone | result |
| 강의 조회 | class/search/:query |  | class[] |
| 학습 목록 | class/my/:userId |  | class[] |
| 강의 정보 | class/:classId |  | class[] |
| 강의 진도 | class/process/:userId/:classId |  | process[] |
| 강의 공지 | class/notice/:classId |  | notice[] |
| 강의 수강 | class/:classId/:contentId |  | content |

## 블록체인

### 개발 환경 설정 및 dApp 개발

* Geth

이더리움 클라이언트 기능 사용 위해 Go Ethereum 클라이언트를 설치하였다.

Geth는 CLI 기반 메인 이더리움 클라이언트로 메인 테스트, 사설 이더리움 네트워크에 접근할 수 있도록 하는 프로그램, 이더리움의 모든 상태를 저장하는 풀 아카이브 노드와 실시간으로 검색 데이터를 검색할 수 있는 라이트 노드 기능이 있다. [3]

Geth를 사용하여 제네시스 블록을 생성하고 사설 이더리움 네트워크를 실행하였다.

텍스트이(가) 표시된 사진

자동 생성된 설명

* Truffle과 Ganache

텍스트이(가) 표시된 사진

자동 생성된 설명

* Remix

텍스트, 스크린샷, 모니터, 전자기기이(가) 표시된 사진

자동 생성된 설명

# 인용 자료

|  |  |
| --- | --- |
| [1] | 김용성, “블록체인, 교육을 바꾸다,” 소프트웨어정책연구소, 22 3 2019. [온라인]. Available: https://spri.kr/posts/view/22599. [액세스: 19 2 2022]. |
| [2] | Byline Network, “에듀테크에서 블록체인 사용 매뉴얼,” Byline Network, 5 11 2018. [온라인]. Available: https://byline.network/2018/11/5-30/. [액세스: 19 2 2022]. |
| [3] | 조수현, 이정빈, 박재용, 이대건 그리고 인호, 이더리움 베이직, 북스타, 2017. |