이더리움 기반 학습 인증 서비스 개발

2021후기 착수보고

PLMS

부산대학교

이승윤, 심재영, 김유미

지도교수 김호원



# 과제 배경과 필요성

## 배경

### 선정 이유

학습은 일상이다. 우리는 태어나서 죽을 때까지 평생을 배우며 살아가야한다. 매일 사용하는 휴대 전화 사용 방법부터 발표, 수학, 그림, 노래, 지켜야할 예절까지. 새로운 것을 탐구하여 배우고 반복해서 익혀 능숙하게 할 수 있게 된다. 공자의 논어 학이편 1장에는 학이시습지 불역열호(배우고 때때로 익힌다면 또한 기쁘지 아니한가)가 가장 먼저 등장한다. 예부터 강조되어 온 학습의 중요성은 빠르게 변화하고 발전하는 기술과 유행에 대응해야 하는 개발자에게 있어서도 매우 중요하게 여겨진다.

### 기존 학습 과정의 문제점

학습 분야에서 중요한 것은 학습 데이터이며 특히 데이터의 안전성과 투명성이 중요하다. 특정 서버에 저장된 데이터는 서버의 안정성과 보안성 수준에 따라 데이터 관리 수준이 직결된다.[1] 중앙 집중형 서버에서는 데이터 유실, 악의적 조작에 대한 위험을 간과할 수 없다. 특히 증명 관련 데이터와 학습 활동 데이터를 업체 또는 개인이 해킹하거나 이익을 위해 조작할 수 있는 가능성이 있다.[2]

인증서를 매번 발급하고 위변조를 확인해야 하는 문제를 해결할 수 없을까? 우리는 때때로 학습한 내용을 증명해야 할 필요가 있을 때가 있다. 이런 경우 수료증, 성적표, 졸업장 같이 다양한 종류의 인증서를 매번 새로 발급해서 회사 또는 기관에 제출해야 한다. 인증서를 제출 받은 곳에서는 인증서의 위변조 여부를 발급 기관을 통해 별도로 확인하여 인증서를 다시 검증해야 한다. 또 발급 기관에서는 위변조 방지를 위해 통상적으로 일정 기간 이후에 만료되도록 설정하므로 미리 발급받은 인증서를 사용할 수 없는 경우도 있다.

결과만 나와있는 인증서, 학습 진행 과정은 알 수 없을까? 인증서를 발급받으면 수료한 과정(또는 과목)의 결과만 나와있어 학습 진행 과정을 파악하기 어렵다. 진행 과정을 파악할 수 있다면 학습자가 학습을 완료한 후 내려진 평가가 공정하였는지 투명하게 확인하고 비교할 수 있어 기존 평가 시스템의 공정성 문제를 해결할 수 있다. 학습 진행 중에도 각종 평가와 진행 사항을 손쉽게 나타낼 수 있으며 다른 사람과 공유할 수 있게 되는 장점도 있다.

온라인 학습 사이트에서 발행된 인증서 믿을 수 있을까? 우리는 인터넷을 통해 누구나 원하는 강의를 수강할 수 있다. 디지털 전환 속도가 빨라지고 비대면 교육의 필요성이 증가하면서 전문 온라인 교육 기관을 찾는 사람 역시 많아지고 있다. [3] 영세한 사이트의 경우 홍보 또는 금전적인 목적으로 결과를 조작하여 인증서를 발급하는 문제가 발생할 수 있다. 심지어 사이트가 없어지는 경우 발급과 증명이 불가능한 상황이 발생한다. 특정 기업 또는 제작자가 대부분의 이익을 가져가고 참여를 원하는 소수가 공평하게 참여할 수 없는 형평성의 문제 [1]도 간과할 수 없는 이슈이다.

### 개발 결심

우리 팀에서는 학습 데이터의 안전성과 투명성을 높인 새로운 학습 플랫폼을 제안한다. 블록체인 기술을 이용하여 원장에 학습자의 학습 과정과 내용을 기록하여 별도의 발급 절차 없이 학습자가 학습 정도를 확인하고 공유할 수 있도록 한다. 배운 내용을 단계적으로 확인할 수 있으므로 학습자는 강의자의 평가가 공정했는지 투명하게 확인할 수 있으며 검증자(제출요구자)는 학습자가 성실하게 열심히 수업에 참여하였는지 어떤 부분에서 큰 두각을 나타내었는지를 판별할 수 있다. 기존의 대형 온라인 학습 플랫폼뿐만 아니라 수업을 제공하고자 하는 누구나 수업을 개설하고 학습 과정 이수 여부를 증명해 줄 수 있다. 블록체인 네트워크에 모든 원장의 내용이 공유되므로 일정 노드 이상이 확보된 경우 학습 데이터의 조작 및 삭제를 막을 수 있다.

## 필요성

문제 해결 필요성을 서술한다. 기존 시스템 또는 관련 기술로부터의 개선점을 포함한다.

- 인증서(수료증/졸업장/성적표) 매번 발급하고 위변조 확인하는 문제 해결

- 배운 내용을 단계적으로 확인, 증명할 수 있음 + 평가의 공정성 문제 투명하게 함

- 온라인 기반 학습에서 사이트 자체 발급으로 인한 조작 문제 해결, 사이트 없어지는 경우 발급 증명

블록체인의 중요한 특징으로는 기록이 담긴 원장을 제3자에게 맡기지 않고, 참여자들이 직접 검증과 승인 등의 활동을 하며 만들고 관리할 수 있는 탈중앙성, 블록의 거래 기록을 참여자들 누구나 볼 수 있는 투명성, 연결된 블록은 수정하거나 삭제하기 어려운 불변성이 있다 [4]. 이런 특징을 이용한다면 현재 학습 시스템이 가진 문제점을 해결할 수 있다.

먼저 수료증, 졸업장, 성적표 등 다양한 인증서를 필요할 때마다 매번 새로 발급해야하는 문제를 해결할 수 있다. 연결된 어느 한 블록을 수정하거나 삭제하려면 모든 참여자의 컴퓨터에 있는 모든 블록 내용을 한꺼번에 바꾸어야 하기 때문에 내용을 위변조할 수 없다. 따라서 인증서를 새로 발급하고 별도로 확인해야하는 과정을 없앨 수 있다.

두번째로 현재의 결과만 나와있는 인증서와 달리 학습을 진행하면서 받은 평가와 진행 사항을 블록에 기록하여 학습 진행 과정을 명확하게 파악할 수 있다. 학습자가 어떤 순서로 과정을 수강했는지, 활동을 했다면 어떤 역할을 맡았는지, 또 어떤 평가를 받았는지를 투명하게 확인하여 평가 시스템을 믿을 수 있는지 판단할 수 있다.

마지막으로 []. 또 중앙 집중형 서버에서 인증서를 발급하고 증명해주는 것이 아니라 참여자 간에 직접 기록을 확인할 수 있어 현재의 사이트가 사라졌을 때 인증을 받을 수 없는 문제를 해결할 수 있다.

# 과제 목표와 내용

## 목표

개발할 기능을 서술한다.

개발 서비스에 대한 간단한 요약(비전) 제시, 이더리움 관련 학습 방향 제시

## 주요 기능

### 강의 수강

학습자는 강의자가 등록한 수업 중 원하는 강의를 수강할 수 있다. 강의를 검색하여 강의 정보를 조회하고 수강 중인 강의의 진도 확인, 수강(영상), 과제, 시험 기능을 제공할 것이다. 강의 진도와 영상 재생은 기존 학습 시스템인 Naver의 edwith와 패스트캠퍼스 수강 시스템을 참고하여 만들 예정이며 과제, 시험 등의 기능은 우리 학교 PLATO 플랫폼을 참고하여 계획하고 있다.

### 블록체인을 통한 학습 진행 과정 저장

매 강의 영상, 과제, 시험을 완료할 경우 블록체인 원장에 기록되어 학습 상태가 저장된다. 학습자는 강의 정보 화면에서 학습 진도와 상태를 확인할 수 있다. 학습자와 검증자 모두 학습 진행 과정을 단계별로 확인할 수 있다. 이를 통해 학습자는 강의자가 평가한 내용을 투명하게 확인하고 비교할 수 있어 평가의 공정성 문제를 해소할 수 있다. 검증자는 학습자가 학습을 어떻게 진행하였으며 잘하는 부분은 어디인지 상세하게 살펴볼 수 있어 학습자의 실력을 파악하기 수월하다.

### 블록체인을 통한 과정, 수업 수료 인증

이미 학습 과정에서 블록체인 네트워크에 학습 진행 과정이 저장되었으므로 학습자가 별도의 발급 절차를 거치지 않더라도 수업과 과정에 대한 수료 인증 서비스를 제공할 수 있다. 여러 수업을 하나의 과정(트랙)으로 지정하여 수업을 체계적으로 이수할 경우 과정을 수료한 것으로 인증할 수 있도록 한다. 이러한 방법으로 스마트 컨트랙트를 설계하여 기존 정규 과정에서 특정 과목을 몇 학점(시간) 이상 이수하면 졸업장(또는 수료증)을 발급하는 과정을 자동으로 수행할 수 있다. 모든 학습 과정이 원장에 기록되어 있기 때문에 학습 데이터의 삭제, 조작이 불가능하여 위변조를 방지할 수 있다. 설령 강의가 없어지더라도 학습 데이터가 그대로 보존되기 때문에 지속적인 학습 인증이 가능하다.

### QR 코드로 수료 확인

QR 코드를 통해 과정, 수업 진행 경과를 공유하여 쉽게 학습 내역을 증명할 수 있도록 한다. 블록체인 네트워크에 기록된 내용을 이용하기 때문에 위변조가 불가능하고 학습 데이터의 안전성과 투명성이 보장된다. 따라서 인증서 및 QR코드에 별도의 만료 기간을 부여할 필요없이 발급한 QR코드를 재발급 없이 계속해서 사용할 수 있다.

## 활용 방안과 기대 효과

해당 기능을 활용하는 방안과 그에 따른 효과를 기입한다. (효과 인용 필요)

# 요구사항과 제약사항 분석

## 요구사항 분석

요구사항 분석 내용을 작성한다.

기존 요구사항 분석 내용 삽입 + 과정 관련 내용 + QR 코드 관련 내용 추가 포함

## 제약사항 분석

특정 요구사항에 제한사항이 있는지 확인하고 그 대책을 서술한다.

Ex) 블록체인 네트워크 연결시 인터넷 연결 필요

# 설계

## 개발 환경

개발 언어, 개발 도구, 실행 환경, 데이터베이스 등 서술한다.

+ 사용환경(SW, HW)도 서술

|  |  |
| --- | --- |
| 개발 언어 | JavaScript, Solidity |
| 개발 도구 |  |
| 실행 환경 |  |
| 데이터베이스 |  |
|  |  |

## 사용 기술

사용하려는 기술을 작성한다.

이더리움(스마트 컨트랙트), Node.js, express, React

## 시스템 흐름도

전체 시스템의 동작 흐름을 이미지로 제시한다.

# 개발 일정과 역할 분담

## 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 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 스마트 컨트랙트 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 서버 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 웹 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 학습 컨텐츠 제작 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 중간보고서 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 스마트 컨트랙트 개발 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 서버 개발 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 웹 개발 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 추가 연구 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 최종보고서 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 최종 발표 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| SW 등록 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

표 1 개발 일정 계획안

## 역할 분담

|  |  |
| --- | --- |
| 이름 | 역할 |
| 이승윤 | 블록체인 네트워크 구축, 스마트 컨트랙트 개발, 이더리움 추가 연구  서버 API 설계, 개발 책임  학습 컨텐츠 제작  발표, 문서 정리 |
| 심재영 | 블록체인 네트워크 구축, 이더리움 추가 연구  웹 APP 개발  학습 컨텐츠 제작, 영상 제작/수정 책임 |
| 김유미 | 블록체인 네트워크 구축, 이더리움 추가 연구  웹 APP 개발 책임  UI 디자인  서버 API 연동 |

표 2 구성원별 역할

# 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] | 김명희, “패스트캠퍼스, 2021년 기업교육 매출 130억 달성,” 전자신문, 24 1 2022. [온라인]. Available: https://m.etnews.com/20220124000028. [액세스: 19 2 2022]. |