

이더리움 기반 학습 인증 서비스 개발

2021 후기 착수보고

PLMS



부산대학교

이승윤, 심재영, 김유미

지도교수 김호원

목차

| | | |
|-----|--------------------|----|
| 1 | 과제 배경과 필요성 | 2 |
| 1.1 | 배경..... | 2 |
| 1.2 | 필요성 | 5 |
| 2 | 과제 목표와 내용 | 6 |
| 2.1 | 목표..... | 6 |
| 2.2 | 주요 기능 | 7 |
| 2.3 | 활용 방안과 기대 효과..... | 8 |
| 3 | 요구사항과 제약사항 분석..... | 9 |
| 3.1 | 요구사항 분석..... | 9 |
| 3.2 | 제약사항 분석..... | 11 |
| 4 | 설계..... | 11 |
| 4.1 | 개발 환경 | 12 |
| 4.2 | 사용 기술 | 12 |
| 4.3 | 시스템 흐름도..... | 15 |
| 5 | 개발 일정과 역할 분담..... | 16 |
| 5.1 | 개발 일정 | 16 |
| 5.2 | 역할 분담 | 16 |
| 6 | 인용 자료..... | 17 |

1 과제 배경과 필요성

1.1 배경

1.1.1 선정 이유

인간의 삶은 학습의 연속이다. 매일 사용하는 휴대 전화 사용 방법부터 언어, 수학, 그림, 노래, 지켜야 할 예절까지. 새로운 것을 탐구하여 배우고 반복해서 익혀 능숙하게 할 수 있게 된다. 고로 우리는 태어나서 죽을 때까지 평생을 배우며 살아가야 한다.

공자의 논어 학이편 1 장에는 “학이시습지 불역열호(배우고 때때로 익힌다면 또한 기쁘지 아니한가)”가 가장 먼저 등장한다. 예부터 강조되어 온 학습의 중요성은 앞으로도 지속될 뿐만 아니라 더욱 강조되고 있다. 현대 사회의 인간은 넘쳐나는 정보통 속에 살고 있다. 그렇기에 방대한 정보 속에서 어떤 교육을 듣고 학습하며 어떤 능력을 갖추었는지를 분별하는 것 또한 매우 중요해지고 있다. 이로써 세상은 인간에게 더 많은 정보를 더 빠르게 학습하는 능력을 원하고 있다.

종래 변화의 속도는 점차 빨라져 이제는 1-2 년 내에 모든 것이 바뀌는 시대다. 빠르게 변화하고 발전하는 기술과 유행에 대응해야 하는 개발자에게 있어서 학습 능력이 매우 중요하게 다가온다. 따라서 우리는 다양한 사람들이 질 좋은 교육 콘텐츠와 마주하고 학습을 통해 갖춘 자신의 능력을 체계화된 방법으로 증명할 수 있는 학습 서비스를 만들고자 한다.



그림 1 공자 [18]

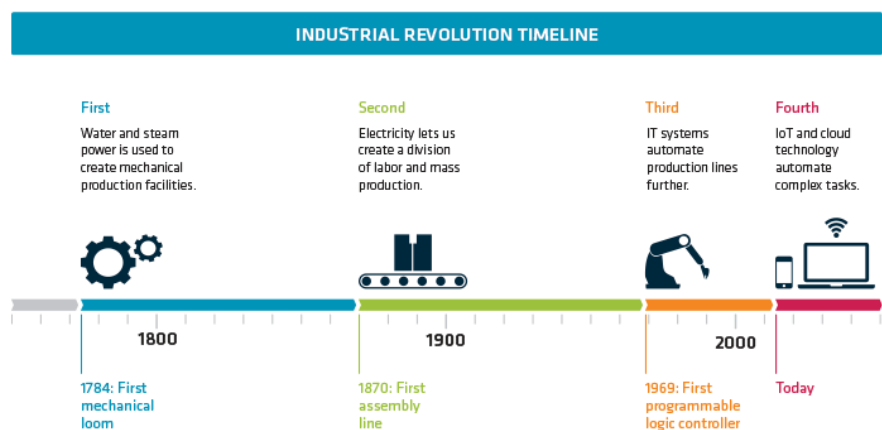


그림 2 산업 혁명 연대표 [19]

1.1.2 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 매년 발급하고 위변조를 확인해야 하는 문제를 해결할 수 없을까? 우리는 때때로 학습한 내용을 증명해야 할 필요가 있을 때가 있다. 이런 경우 수료증, 성적표, 졸업장같이 다양한 종류의 인증서를 매년 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.

1.1.3 개발 방향

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.

1.2 필요성

기존 학습 과정에서 발견한 문제 해결 방법은 없을까? 인증서를 매년 새로 발급하고 위변조 여부를 확인해야 하는 과정을 보다 안전하게 간단히 처리하고, 학습 과정을 확인하고 증명할 수 있도록 하여 평가의 공정성 문제를 해결하며, 누구나 강의를 만들 수 있고 인증서 발급과 학습 증명이 가능하도록 하는 기술. 우리는 블록체인에서 그 답을 찾을 수 있을 것이라 확신한다.

블록체인의 중요한 특징으로는 기록이 담긴 원장을 제 3자에게 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 획기적으로 해결할 수 있다.

먼저 수료증, 졸업장, 성적표 등 다양한 인증서를 필요할 때마다 매년 새로 발급받지 않아도 된다. 네트워크에 이미 연결된 어느 한 블록을 수정하거나 삭제하려면 모든 참여자의 컴퓨터에 있는 해당 블록의 모든 내용을 한꺼번에 바꾸어야 하기 때문에 내용 위변조가 거의 불가능하다. 학습 내용이 추가되어 내역이 변경되는 경우에도 블록체인 네트워크의 원장에 반영되어 최신 상태를 확인 가능하다. 따라서 인증서를 새로 발급하고 위변조 여부를 감정하는 과정을 없앨 수 있다.

두번째로 수료한 과정(또는 과목)의 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 확인할 수 있다. 이를 통해 학습자는 강의자의 평가(성적 부여)가 타당한지 확인할 수 있다. 예비학습자와 검증자는 평가 시스템을 믿을 수 있는지 판단할 수 있다.

마지막으로 누구나 강의를 만들고 믿을 수 있는 학습 증명이 가능하다. 특정 업체와 제작자가 독점하여 큰 이익을 가져가는 것이 아니라 참여를 원하는 강의자가 공평하게 참여하여 강의를 제작하는 생태계를 구축할 수 있다. 악의적인 온라인 업체가 돈만 받고 인증서를 발급해주거나 수강자의 성적을 우수하게 조작하여 교육 효과가 큰 것처럼 실적을 조작하는 것이 불가능해진다. 또 중앙 집중형 서버에서 인증서를 발급하고 증명해주는 것이 아니라 참여자 간에 직접 기록을 확인할 수 있어 온라인 강의 사이트가 사라져서 인증을 받을 수 없는 상황을 원천적으로 차단할 수 있다.

2 과제 목표와 내용

2.1 목표

개발할 서비스는 쉬운 학습 과정 인증, 투명한 평가 시스템, 신뢰받는 열린 학습 시스템으로 블록체인 기술을 활용하여 기존 학습 시스템을 획기적으로 개선한다. 학습 플랫폼 이름은 바름으로 정하였다. 표준국어대사전을 보면 “바르다”에는 3 가지 의미가 있다. 먼저 사실과 어긋남이 없다, 겉으로 보기에 비뚤어지거나 굽은 데가 없다는 의미를 가진다. [5] 블록체인을 통한 학습 진행 과정 저장, 과정(수업) 수료 인증으로 투명하고 정확한 학습 절차 인증 과정을 구현한다. 다음으로 껍질을 벗기어 속에 들어 있는 알맹이를 집어내다는 뜻이 있다. [5] 학습 결과만 나오는 껍데기 인증서 대신 알맹이인 학습 진행 과정을 살펴볼 수 있어 학습자와 검증자 모두가 믿을 수 있는 평가 시스템을 구현한다. 마지막으로 다른 물건(물체)의 표면에 고르게 붙인다는 의미도 있다. [5] 특정 업체의 독점 없이 강의를 원하는 사람이라면 고르게 누구나 참여할 수 있는 학습 플랫폼을 구현한다.

다양한 블록체인 플랫폼 중 이더리움을 기반으로 과제를 수행할 것이다. 이더리움은 퍼블릭 블록체인이고 스마트 컨트랙트가 동작하는 탈중앙화 어플리케이션을 개발할 수 있어 학습 데이터의 안전성과 투명성을 보장하여 문제를 해결하는데 가장 적합하다고 판단하였다. 과제를 수행하면서 이더리움으로 학습 데이터를 블록에 추가하고 스마트 컨트랙트를 통해 수업과 과정 수료 인증 기능을 구현하는 것이 첫번째 목표이며 NFT, POS, 이더리움 2.0(합의 계층) [6] 등의 개념을 추가적으로 연구하는 것이 이번 과제의 목표이다.

2.2 주요 기능

2.2.1 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.

2.2.2 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.

2.2.3 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.

2.2.4 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 QR 코드에 별도의 만료 기간을 부여할 필요없이 발급한 QR 코드를 재발급 없이 계속해서 사용할 수 있다.

2.3 활용 방안과 기대 효과

4차 산업혁명의 핵심기술로 주목받고 있는 블록체인 기술은 탈중앙화, 투명성, 공유성의 특성이 있다. 신뢰 기반으로 상호작용이 가능하며 조작할 수 없는 디지털 프로세스를 제공하여 블록체인이 교육 분야를 변화시킬 것으로 예측된다. [7] 블록체인 기술을 활용한 플랫폼에서는 중개인의 개입없이 개인간 직접 상호작용할 수 있다.

블록체인 네트워크에 기록된 내용을 바탕으로 기존 교육 기관, 업체와 무관하게 학습 증명이 가능하다. 모든 학습 과정이 블록에 기록되어 있으므로 위변조의 위험 없이 회사 또는 기관 제출용으로 사용 가능하다. 현재에는 인증서의 진위 여부를 판단하기 위해 해당 교육 기관 및 업체에 직접 확인해야 하며 변경사항 반영, 위변조 위험 때문에 매년 재발급해야 하는 문제가 있다. 이런 방식에서 벗어나 인증서를 요청하는 기관에 블록체인 기반의 인정서를 제출하면 신청 받은 기관은 즉시 사실 여부를 검증할 수 있어 종이 인증서 발급으로 인한 시간적, 경제적 비용을 크게 감소시킬 수 있다. [8] 타 플랫폼과 연동하여 다른 플랫폼에서 수강하는 학습 내역을 네트워크에 저장한다면 통합된 인증서 플랫폼으로 확장이 가능하다.

학습 진행 과정을 알 수 있어 투명하고 신뢰할 수 있는 평가 시스템을 제공한다. 온라인 기업 교육이 크게 증가하는 상황 [3]에서 학습자의 학습 과정과 평가 내용을 확인하여 채용, 승진의 참고 자료로 활용할 수 있다. 학습자는 진행 과정을 보며 강의자의 평가가 적절한지 확인하여 교육자와 학습자 간에 상호소통을 원활하게 한다. 투명하고 신뢰할 수 있는 평가 시스템은 학습자에게 동기를 부여하고 다른 수강자의 학습 내역을 확인하여 학습 기간과 강의의 질을 예측할 수 있어 더욱 체계적인 학습을 할 수 있을 것으로 기대된다.

탈중앙화된 학습 증명과 투명하고 신뢰할 수 있는 평가 시스템을 통해 누구나 질 좋은 강의를 만들고 수강할 수 있다. 부실한 업체가 짧은 기간 돈만 받고 자격증, 인증서를 발급하는 경우, 매우 초보적인 내용으로만 강의를 구성하여 성적을 우수하게 보여 교육 효과가 큰 것처럼 광고하는 경우를 쉽지 않게 찾아볼 수 있다. [9] 학습자는 수강 전 다른 학습자의 과정과 평가를 미리 찾아볼 수 있어 낮은 수준의 강의 선택을 회피할 수 있다. 회사와 기관에서는 명칭만 전문가, 심화 과정인지 실제 강의를 어떤 수준이고 학습자의 실력은 어느 정도인지 면밀히 파악할 수 있는 효과가 있다. 단순히 수료 인증서만 발급할 때보다 질 높은 강의의 힘이 커지고 더 좋은 강의를 나올 수 있는 원동력으로 작용한다.

3 요구사항과 제약사항 분석

3.1 요구사항 분석

3.1.1 계정

학습 시스템 접근과 사용자 구분을 위해 계정 기능이 필요하다. 세부적으로 로그인, 로그아웃, 회원가입 기능이 요구된다.

학습을 하거나 강의를 등록하기 원하는 사용자는 회원가입을 통해 기능 접근 권한을 부여 받아야한다. 회원가입을 위해 이름, 아이디, 비밀번호, 휴대전화 번호, 이메일을 입력 받는다. 사용자 아이디는 다른 사용자와 중복해서 사용될 수 없으며 8자리 이상을 사용해야 한다. 회원가입을 완료한 사용자는 로그인 화면으로 이동한다.

회원가입한 사용자는 로그인하여 학습 또는 강의를 등록할 수 있다. 회원가입시 입력한 아이디와 비밀번호를 통해 로그인 가능하다. 로그인에 성공할 경우 메인 화면으로 이동한다. 실패한 경우 다시 로그인해야 한다.

로그인한 사용자는 로그아웃하여 컴퓨터를 사용하는 다른 사용자가 강의를 수강하거나 등록하지 못하게 할 수 있다. 로그아웃에 성공할 경우 메인 화면으로 이동한다.

3.1.2 강의 찾기

강의 수강을 위해 강의 조회(검색)로 강의를 찾아 강의 정보(상세)를 확인할 수 있는 기능을 제공한다.

사용자는 강의 조회(검색) 기능을 이용하여 과정과 강의를 검색할 수 있다. 검색 상자에 원하는 검색어를 입력하면 강의 제목, 강의 요약, 강의자에 해당 검색어가 포함되어 있는 경우 목록으로 표시된다. 검색 결과 목록의 각 항목은 강의 제목, 강의 요약, 강의자 정보로 구성된다. 사용자가 원하는 강의를 선택하면 강의 정보(상세)가 표시된다.

강의 정보(상세) 기능으로 강의 정보를 살펴볼 수 있다. 강의 제목, 강의 요약, 강의자, 학습 목록을 표시한다. 강의 진도는 블록을 이용하여 학습한 순서대로 표시한다. 출석, 과제, 시험 종류에 따라 다른 색상의 블록으로 표시하고 완료 날짜를 함께 제공한다. 강의 공지사항은 최신 게시글을 기준으로 5개까지 목록으로 표시한다. 공지사항 게시글은 강의별로 구분되며 제목, 내용, 작성자, 작성일자로 구성된다.

3.1.3 강의 수강

강의 수강 기능으로 강의를 학습할 수 있다. 좌측면에는 강의에서 학습할 내용이 순서대로 목록으로 표시된다. 영상, 과제, 시험 종류 별로 다른 화면을 사용한다. 수강(영상)은 수강 필요, 수강 완료 상태가 존재한다. 과제는 제출 필요, 제출 완료, 채점 완료 상태가 존재한다. 따라서 과제에는 제출 여부와 채점 상황이 표시된다. 시험은 응시 필요, 응시 완료, 채점 완료 상태가 존재한다. 과제와 시험은 채점 완료 상태인 경우 점수를 표시한다. 수강, 과제, 시험 항목마다 최종 상태 변화 시간을 표시한다. 수강(영상)은 수강 완료, 과제는 채점 완료, 시험은 채점 완료 상태가 되면 네트워크 상의 블록에 기록된다.

3.1.4 블록체인을 통한 학습 진행 과정 저장

강의 수강 과정에서 수행한 학습 활동은 블록체인에 저장된다. 수강 완료, 과제 채점 완료, 시험 채점 완료 상태가 되었을 때 원장에 기록한다. 이 때 공통적으로 강의 번호, 강의명, 학습자, 시간이 저장된다. 수강 완료 상태의 경우 해당 학습 영상의 번호와 제목이 함께 저장된다. 과제 채점 완료 상태에서는 과제 내용, 채점 내용, 점수가 저장된다. 시험 채점 완료 상태에서는 시험 내용, 채점 내용, 점수가 저장된다. 학습자는 강의 정보 화면에서 블록 형태로 정리된 학습 진행 사항을 확인할 수 있으며 QR 코드를 이용하여 학습 진행 과정을 공유할 수 있다.

3.1.5 블록체인을 통한 과정, 수업 수료 인증

블록체인에 저장된 학습 진행 과정 내용을 바탕으로 스마트 컨트랙트를 통해 조건이 갖춰지면 자동으로 과정, 수업을 수료한 것으로 기록한다. 모든 영상을 시청 완료하고 각 과제와 시험 점수가 60 점이상인 경우 수업(강의)을 수료한 것으로 인정한다. 과정은 강의자가 과정에 지정한 수업을 80% 이상 수료할 경우 해당 과정을 수료한 것으로 인정한다. 학습자는 수료한 과정과 수업에 대해 인증서를 발급할 수 있다. 인증서에는 학습자 이름, 강의명, 강의 요약과 QR 코드가 표시된다.

3.1.6 QR 코드로 수료 확인

검증자 또는 학습자로부터 공유 받은 자는 QR 코드를 통해 학습 진행 과정과 수료 여부를 확인할 수 있다. QR 코드에 플랫폼 링크를 삽입하여 학습 진행 과정 및 수료 여부 확인 화면으로 연결된다. 해당 화면에서는 블록 형태로 학습 진행 과정이 완료 날짜, 점수와 함께 표시되며 수강, 과제, 시험 종류에 따라 다른 색상으로 표시된다. 과제와 시험은 추가 정보를 확인할 수 있다. 과제의 경우 과제 내용과 채점 내용을, 시험의 경우 시험 내용과 채점 내용을 확인할 수 있다.

3.2 제약사항 분석

3.2.1 인터넷 연결 필요

강의 수강과 학습 진행 과정 저장, 수료 인증같이 전 기능 요구사항에 걸쳐 인터넷 연결이 필요하다. 계정, 강의 찾기, 블록체인을 이용한 학습 진행 과정 저장, 과정/수업 수료 인증, 수료 확인 기능에 대해서는 인터넷 연결이 필수적으로 필요하다. 계정 기능의 경우 사용자 확인, 가입 기능 수행이 필요하며 강의 찾기 기능은 강의 검색과 정보 조회를 위해 인터넷 연결이 필요하다. 강의 수강 기능의 경우 학습자가 사전 다운로드한 강의(영상)에 대해 오프라인 시청 기능 지원을 고려할 수 있다. 블록체인을 이용한 학습 진행 과정 저장과 과정/수업 수료 인증 기능의 경우 블록체인 네트워크상의 원장에 학습 진행 과정을 기록하고 스마트 컨트랙트가 실행되어 수료 인증이 완료되기 때문에 인터넷 연결이 필요하다. 수료 확인 기능에 대해서는 기존처럼 인증서를 발급하고 확인시에만 인증서의 QR 코드를 이용하여 인터넷에 접속하는 방법으로 대응할 수 있다.

| 요구사항 | 대책 |
|---|------------------------|
| 계정, 강의 찾기 학습 진행 과정 저장 과정/수업 수료 인증 | 인터넷 연결 필요 |
| 강의 수강 | 강의 영상 오프라인 다운로드 |
| 수료 확인 | 별도 인증서 발급 (검증에는 연결 필요) |

표 1 인터넷 연결 대책

3.2.2 기존 학습 데이터 연동

기존의 학습 데이터를 연동한다면 개인별로 모든 학습 내역을 인증할 수 있는 통합 플랫폼 서비스를 제공할 수 있다. 먼저 교육 기관, 업체에서 학습 진행 과정(수강, 과제, 시험 기록)을 이관 받을 수 있다면 블록체인 네트워크 상의 블록에 바로 학습 진행 과정을 반영하고 과정/수업 수료 인증 서비스를 제공할 수 있다. 만약 학습 진행 과정 데이터가 없다면 학습 결과만 이관 받아 반영할 수 있다. 단 진행 과정이 표시되는 여타 강의와 구별을 위해 학습 진행 과정이 없다는 내용을 인증 페이지에 표시하여 구분한다.

| 데이터 | 대책 |
|--------------|--|
| 학습 진행 과정 포함 | 블록체인에 진행 과정, 결과 반영 수료 확인 서비스 즉시 제공 가능 |
| 학습 결과만 있는 경우 | 블록체인에 결과 반영 수료 확인 서비스에 별도 메시지 표시 |

표 2 학습 데이터 연동 대책

4 설계

4.1 개발 환경

| | |
|--------|--|
| 개발 언어 | JavaScript, Solidity |
| 개발 도구 | Visual Studio Code, IntelliJ idea, Git Node.js, Express, React, Web3.js |
| 실행 환경 | Windows 10/11, Ubuntu 20.04.2, Chrome |
| 데이터베이스 | MySQL |

표 3 개발 환경

4.2 사용 기술

4.2.1 블록체인

블록체인은 여러 거래내역을 묶어 블록을 구성하고 해시를 이용하여 여러 블록을 체인처럼 연결하여 다수의 사람들이 복사하여 분산 저장하는 알고리즘이다. [10] 비즈니스 네트워크에서 거래내역을 기록하고 자산을 추적하는 프로세스를 효율화하는 변하지 않는 공유 원장이다. [11] 블록체인 기술은 신뢰성, 안전성, 탈중앙화의 특성을 가진다. 데이터의 위변조가 불가능하여 중개기관 없이 신뢰 가능한 안전한 거래, 데이터 처리가 가능하다. [10]

교육 분야에서는 데이터의 안정성과 투명성, 형평성 문제를 [2] 해결하기 위해 블록체인 도입이 필요하다. 먼저 매번 새로 인증서를 발급받지 않아도 되고 위변조 감별 절차가 간소화된다. 블록체인 네트워크에 학습 데이터가 지속적으로 반영되므로 항상 최신 상태의 학습 내역을 확인할 수 있다. 데이터 조작이 불가능하므로 기록된 학습 데이터를 신뢰할 수 있다. 다음으로 학습 진행 과정을 볼 수 있어 평가 시스템의 신뢰성을 높이고 강의의 질을 높인다. 학습자는 강의자의 평가가 적절한지 확인할 수 있으며 다른 학습자를 통해 학습 기간과 강의 품질을 확인할 수 있다. 검증자는 학습자가 강의에 적극적으로 참가했는지 강의와 학습자의 수준은 어느 정도되는지 자세하게 파악할 수 있다. 학습 과정이 공개되므로 질 낮은 강의와 자격증으로 교육 효과가 큰 것처럼 광고하거나 [9] 돈만 받고 인증서를 발급해주는 악의적인 사례를 예방할 수 있다. 마지막으로 누구나 강의를 만들고 참여할 수 있다. [1] 참여를 원하는 강의자가 공평하게 참여하여 강의를 제작하고 인증해 줄 수 있다. 강의가 사라지더라도 학습 데이터는 그대로 보존되므로 영구적인 학습 인증이 가능하다.

4.2.2 이더리움

이더리움은 암호 화폐 이더와 분산형 어플리케이션을 구동하는 커뮤니티 운영 기술(플랫폼)이다. [12] 이전의 블록체인 기술은 화폐에 특화된 기능으로 구현되어 암호 화폐 이외 영역에서 사용되기에는 어려움이 있었다. 그러나 이더리움은 프로그래밍이 가능하여 스마트 컨트랙트가 적용된 탈중앙화 어플리케이션(이하 디앱)을 개발할 수 있다. 디앱은 이더리움에 배포되면 항상 프로그래밍된 대로 동작하므로 완전히 신뢰가능하다. [12] 이더리움에서 스마트 컨트랙트를 도입함으로써 블록체인을 이용하여 위변조 방지가 필요한 계약서 작성 기능을 구현할 수 있게 되었다.

이더리움의 스마트 컨트랙트는 자동 실행, 예측 가능한 결과, 공공 기록, 개인 정보 보호, 공개된 조건의 특징을 가진다. [13] 스마트 컨트랙트는 계약 조건이 만족되면 결과가 자동으로 실행된다. 예를 들어 강의자가 등록한 영상을 모두 시청하면 해당 수업을 수료한 것으로 처리할 수 있다. 스마트 컨트랙트는 예측 가능한 결과를 생성한다. 말 또는 글로 표현된 계약은 사람마다 서로 다르게 해석할 가능성이 존재한다. 그러나 스마트 컨트랙트는 코드로 작성된 조건에 따라 정확하게 실행되며 동일한 상황에서 동일한 결과를 생성한다. 스마트 컨트랙트는 공적인 기록에도 적합하다. 학습 데이터는 공개된 블록체인에 있기 때문에 검증자가 학습자의 학습 정보를 정확하게 추적, 검증할 수 있다. 이더리움은 가명 네트워크로 거래에는 거래자의 신원이 아닌 고유한 암호화 주소가 사용된다. 따라서 관찰자로부터 개인 정보를 보호할 수 있다. 스마트 컨트랙트의 계약 조건을 미리 확인할 수 있다. 계약 조건이 모두에게 투명하게 공개되어 있기 때문에 신용할 수 있다. 예를 들어 모든 영상을 수료하고 평균 점수가 60 점 이상일 때 수료를 하는 스마트 컨트랙트가 있다면 해당 스마트 컨트랙트의 적용을 받는 수업의 수료 인증을 신뢰할 수 있다.

4.2.3 QR 코드

QR 코드는 흑백 격자무늬 패턴 코드로 정보를 나타내는 매트릭스 형식의 이차원 코드이다. 기존에 사용되던 바코드는 1 차원으로 숫자, 문자 정보가 가능하였다. QR 코드는 2 차원 형태를 가져 바코드보다 더 많은 정보를 담을 수 있으며 더 작은 공간을 차지한다. 오염과 손상에 강하며 어느 방향에서도 인식 가능하다는 특징이 있다. 최대 16 분할하여 데이터를 표현하여 좁고 긴 표면에도 큰 데이터를 인쇄할 수 있다. [14]

인증서 검증을 위해 QR 코드를 스캔할 경우 사이트로 이동하여 학습 과정을 볼 수 있도록 구현할 수 있다. 또는 암호화된 사용자 주소를 삽입, 이를 이용하여 학습 정보를 추적, 검증할 수 있도록 할 수 있다.

4.2.4 Node.js

Node.js 는 Chrome V8 JavaScript 엔진으로 빌드된 JavaScript 엔진이다. 비동기 이벤트 기반 자바스크립트 런타임으로 확장성 있는 네트워크 어플리케이션 설계에 유용하다. 다수의 연결을 동시에 처리할 수 있으며 실행할 작업이 없는 경우 대기한다. [15] 특히 I/O 처리에서 우수한 성능을 보여 학습 플랫폼에 적합하다고 판단되어 도입하였다. 아래에서 설명할 Express 와 React 모두 노드 기반으로 동작하는 프레임워크이다.

4.2.5 Express

Express 는 Node.js 를 위한 빠르고 개방적인 간결한 웹 프레임워크이다. 유틸리티 메소드와 라우팅 기능, 다양한 미들웨어를 사용하여 쉽고 빠르게 강력하게 API 를 작성할 수 있다. [16] 계정, 강의 찾기, 강의 수강, 학습 진행 과정 저장, 과정/수업 수료 인증 같은 기능 수행시 데이터베이스 추가/수정/제거/저장, 이더리움 블록체인 네트워크에 기록 및 조회하는 API 서버 역할을 수행한다.

4.2.6 React

사용자 인터페이스를 만들기 위한 자바스크립트 라이브러리이다. 노드 서버에서 렌더링한다. 리엑트는 데이터가 변경되면 변경이 필요한 컴포넌트만 갱신하여 렌더링하기 때문에 효율적이고 상호작용이 많은 UI 를 만들 때 생기는 어려움을 줄여준다. 컴포넌트는 스스로 상태를 관리하는 캡슐화된 자바스크립트 코드이다. 컴포넌트를 조합하여 더 복잡한 UI 를 설계할 수 있다. DOM 과는 따로 상태를 관리할 수 있고 다양한 형식의 데이터를 앱 내부에서 쉽게 전달 가능하다. [17] 사용자 인터페이스는 리엑트를 통해 표시되며 익스프레스로 제작된 API 서버와 연동하여 데이터를 표시한다.

4.3 시스템 흐름도

사용자는 웹 서버를 통해 강의를 찾고 수강할 수 있다. 강의 정보와 영상 같이 큰 데이터는 클라우드 서버에 저장하고 데이터의 불변성, 투명성이 중요한 학습 데이터는 이더리움 네트워크의 블록에 저장한다. 학습 진행 과정이 저장됨에 따라 설정한 조건이 만족되면 스마트 컨트랙트가 실행되어 과정과 수업을 수료한 것으로 처리된다. 학습 인증은 이더리움 원장에 기록된 학습 과정 데이터를 통해 조회할 수 있다.

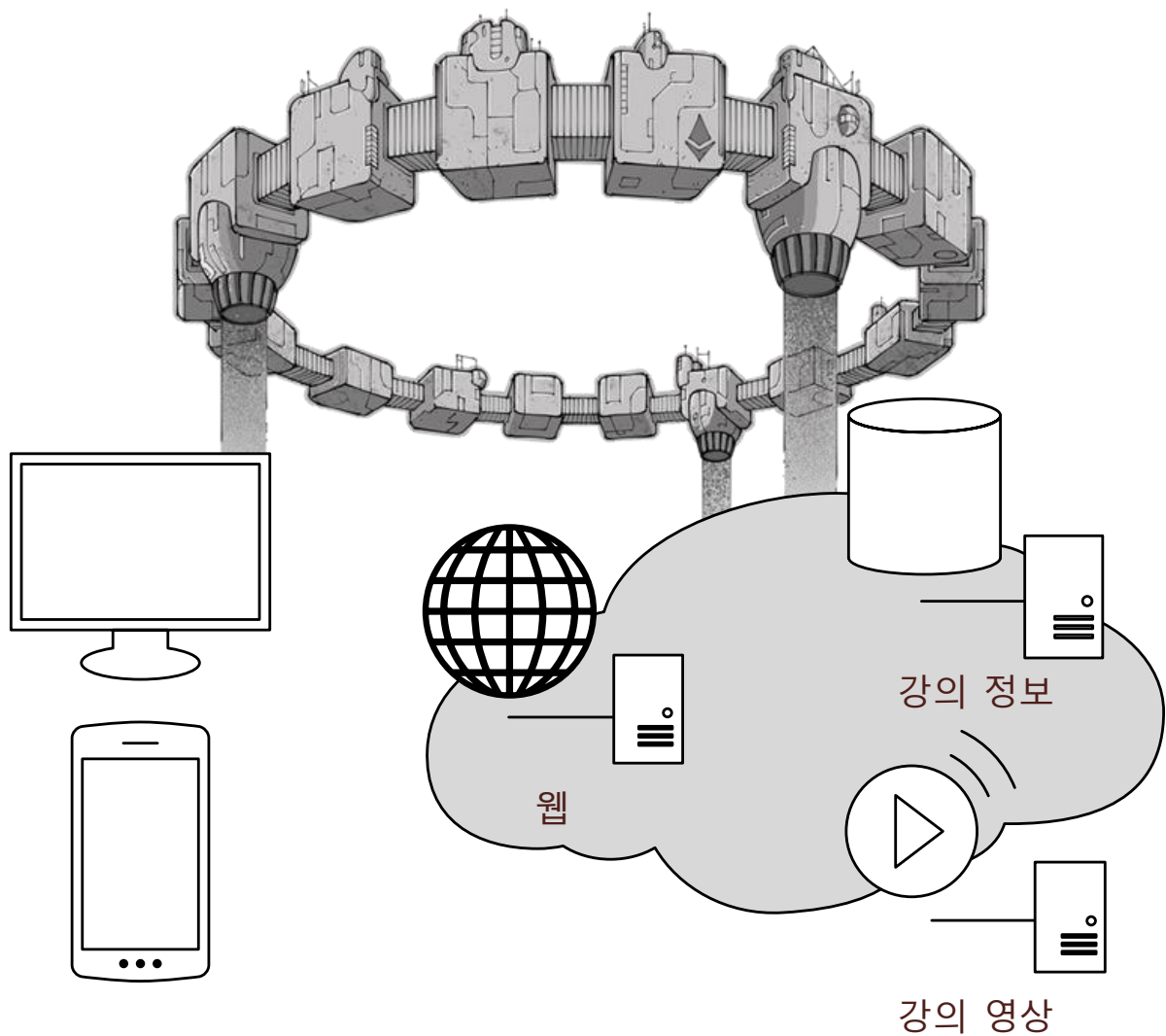


그림 3 시스템 흐름도 [6]

5 개발 일정과 역할 분담

5.1 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 콘텐츠 제작 | | | | | | | | | | | | | | | | | | | | | | |
| 중간보고서 | | | | | | | | | | | | | | | | | | | | | | |
| 스마트 컨트랙트 개발 | | | | | | | | | | | | | | | | | | | | | | |
| 서버 개발 | | | | | | | | | | | | | | | | | | | | | | |
| 웹 개발 | | | | | | | | | | | | | | | | | | | | | | |
| 추가 연구 | | | | | | | | | | | | | | | | | | | | | | |
| 최종보고서 | | | | | | | | | | | | | | | | | | | | | | |
| 최종 발표 | | | | | | | | | | | | | | | | | | | | | | |
| SW 등록 | | | | | | | | | | | | | | | | | | | | | | |

표 4 개발 일정 계획안

5.2 역할 분담

| 이름 | 역할 |
|-----|---|
| 이승윤 | Web3, 스마트 컨트랙트 개발, 이더리움 추가 연구 서버 API 설계, 개발 책임 학습 콘텐츠 제작 발표, 문서 정리 |
| 심재영 | 이더리움 추가 연구 웹 APP 개발 학습 콘텐츠 제작, 영상 제작/수정 책임 |
| 김유미 | 이더리움 추가 연구 웹 APP 개발 책임 UI 디자인 서버 API 연동 |

표 5 구성원별 역할

6 인용 자료

- [1] 김용성, "블록체인, 교육을 바꾸다," 소프트웨어정책연구소, 22 3 2019. [온라인]. Available: <https://spri.kr/posts/view/22599>. [엑세스: 19 2 2022].
- [2] Byline Network, "에듀테크에서 블록체인 사용 매뉴얼," Byline Network, 5 11 2018. [온라인]. Available: <https://byline.network/2018/11/5-30/>. [엑세스: 19 2 2022].
- [3] 김명희, "패스트캠퍼스, 2021 년 기업교육 매출 130 억 달성," 전자신문, 24 1 2022. [온라인]. Available: <https://m.etnews.com/20220124000028>. [엑세스: 19 2 2022].
- [4] 김준수, "[미래 성장동력, 블록체인] 탈중앙성·투명성·불변성 기술적 특징으로 비즈니스 패러다임 변혁할 기술로 부상," *부산발전포럼*, pp. 8-15, 10 2019.
- [5] 국립국어원, "국립국어원 표준국어대사전," [온라인]. Available: <https://stdict.korean.go.kr/search/searchResult.do?pageSize=10&searchKeyword=%EB%B0%94%EB%A5%B4%EB%8B%A4>. [엑세스: 20 2 2022].
- [6] ethereum.org, "Ethereum upgrades (formerly "Eth2")," ethereum.org, 19 2 2022. [온라인]. Available: <https://ethereum.org/ko/upgrades/>. [엑세스: 22 2 2022].
- [7] 김승진 그리고 장환영, "기업교육에서의 블록체인 활용방안 연구," *기업교육과인재연구*, 제 21, 번호: 4, pp. 43-64, 2019.
- [8] 이재우, "블록체인 기반 교육 분야 인증서 발급시스템에 관한 연구," %1 *동국대학교 석사학위논문*, 2022.
- [9] 이소현, "2 주 수업받고 메타버스 전문가?...부실 자격증 '우후죽순'," 한국경제, 20 2 2022. [온라인]. Available: <https://www.hankyung.com/it/article/202202194675i>. [엑세스: 21 2 2022].
- [10] 해시넷, "블록체인 - 해시넷," 10 8 2021. [온라인]. Available: <http://wiki.hash.kr/index.php/%EB%B8%94%EB%A1%9D%EC%B2%B4%EC%9D%B8>. [엑세스: 21 2 2022].

- [11] IBM, "블록체인 기술이란? - IBM 블록체인," IBM, [온라인]. Available: <https://www.ibm.com/kr-ko/topics/what-is-blockchain>. [엑세스: 21 2 2022].
- [12] ethereum.org, "이더리움이란 무엇인가요?," ethereum.org, 19 2 2022. [온라인]. Available: <https://ethereum.org/ko/what-is-ethereum/>. [엑세스: 21 2 2022].
- [13] ethereum.org, "Introduction to smart contracts," ethereum.org, 19 2 2022. [온라인]. Available: <https://ethereum.org/en/smart-contracts/>. [엑세스: 22 2 2022].
- [14] DENSO WAVE INCORPORATED, "QR 코드란?," DENSO WAVE INCORPORATED, [온라인]. Available: <https://www.qrcode.com/ko/about/>. [엑세스: 22 2 2022].
- [15] OpenJS Foundation, "About | Node.js," OpenJS Foundation, [온라인]. Available: <https://nodejs.org/ko/about/>. [엑세스: 21 2 2022].
- [16] StrongLoop, Inc, "Express - Node.js 웹 애플리케이션 프레임워크," StrongLoop, Inc, [온라인]. Available: <https://expressjs.com/ko/>. [엑세스: 22 2 2022].
- [17] Meta Platforms, Inc, "React - A JavaScript library for building user interfaces," Meta Platforms, Inc, 2022. [온라인]. Available: <https://reactjs.org/>. [엑세스: 22 2 2022].
- [18] 나무위키, "공자 - 나무위키," 19 2 2022. [온라인]. Available: <https://namu.wiki/w/%EA%B3%B5%EC%9E%90>. [엑세스: 21 2 2022].
- [19] B. G. Jeppesen, "REALIZING THE FOURTH INDUSTRIAL REVOLUTION," Mjolner, 14 1 2015. [온라인]. Available: <https://mjolner.dk/2015/01/14/realizing-the-fourth-industrial-revolution/>. [엑세스: 19 2 2022].