

이더리움 기반 학습 인증 서비스 개발

2021 후기 중간보고

08 번-PLMS 팀-D 분과



부산대학교

201645825 이승윤, 201645819 심재영, 201824444 김유미

지도교수 김호원

목차

1	요구조건 및 제약사항 분석에 대한 수정사항.....	2
1.1	과제 목표.....	2
1.2	요구사항 분석과 수정.....	3
1.3	제약사항 분석과 수정.....	3
2	설계 상세화 및 변경 내역.....	4
2.1	웹.....	4
2.2	서버.....	4
2.3	블록체인.....	5
3	갱신된 과제 추진 계획.....	6
3.1	개발 일정.....	6
4	구성원별 진척도.....	7
4.1	구성원별 진행사항.....	7
5	보고 시점까지의 과제 수행 내용 및 중간 결과.....	8
5.1	요약.....	8
5.2	웹.....	8
5.3	서버.....	12
5.4	블록체인.....	15
6	인용 자료.....	16

1 요구조건 및 제약사항 분석에 대한 수정사항

1.1 과제 목표

매번 발급하고 위변조를 확인해야 하는 인증서, 결과만 나와있는 인증서, 다양한 기관에서 발행된 인증서, 과연 믿을 수 있을까? 우리 PLMS 팀은 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 콘텐츠를 공급하고 [1] 소비할 수 있으며 학습한 내용을 손쉽게 인증할 수 있다.

요구조건

강의 수강

- 웹을 통해 강의를 수강할 수 있는 시스템

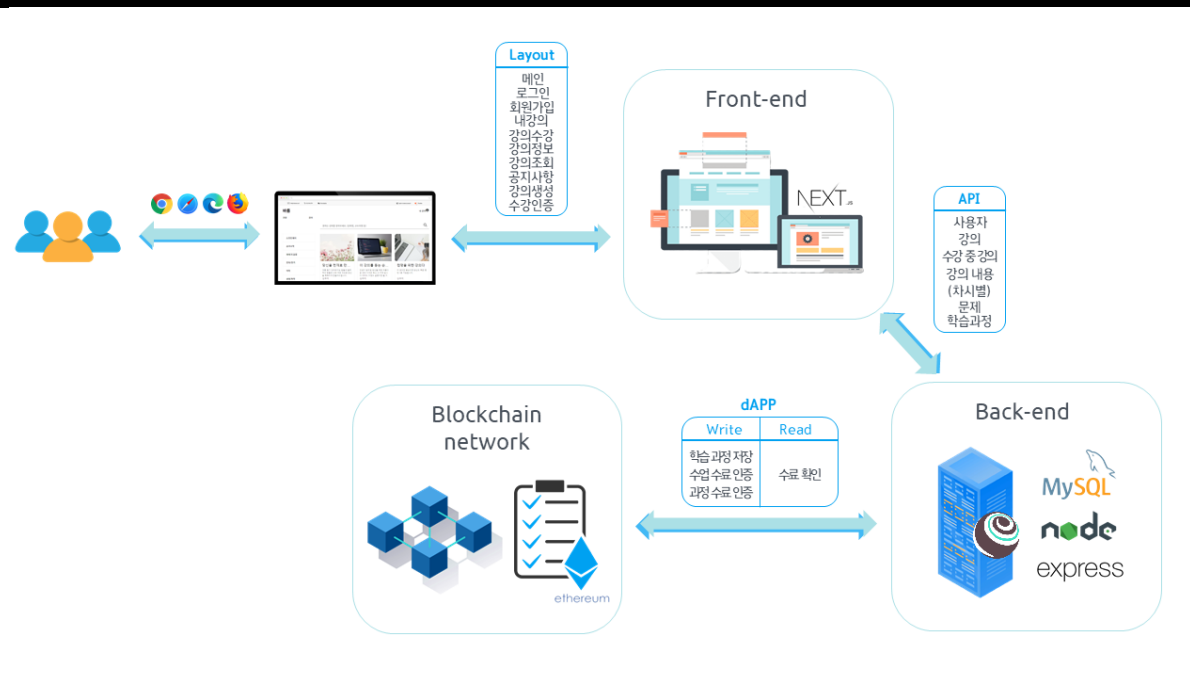
강의 수강 인증

- 학습 데이터를 이더리움 블록체인 상에 저장, 읽기
- 스마트 컨트랙트로 강의 수수료 처리

강의 생성

- 웹을 통해 강의를 생성할 수 있는 시스템

시스템 구성도



1.2 요구사항 분석과 수정

요구사항	수정 내용
계정	기존에는 사용자 ID 와 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 URL 을 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

1.3 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.	오프라인 및 타사 학습 데이터를 등록할 수 있도록 지원한다. 학습 과정 데이터가 단계별로 남아있는 경우 블록체인에 진행 과정과 결과를 반영하고 수료 확인 서비스를 제공한다. 학습 결과만 있는 경우라도 수료 확인 서비스를 제공한다. 단 학습 진행 과정은 조회할 수 없다.

2 설계 상세화 및 변경 내역

2.1 웹

기능 요구사항 분석을 통하여 메인, 로그인, 회원가입, 내 강의, 강의 수강, 강의 정보, 강의 조회, 강의 공지, 강의 생성, 수강 인증 레이아웃을 설계하였다. 우선적으로 메인, 로그인, 회원가입, 내 강의, 강의 수강, 강의 정보, 강의 조회 화면 구현을 완료하였다. 이 과정에서 기존에는 가로 전체를 차지하던 검색 상자 크기를 좌측 레이아웃에 맞게 변경하였다. 현재 강의 콘텐츠와 서버 API 연동 작업이 진행 중이며 통합 테스트를 진행하여 서버와 통신하는 코드를 수정하고 컴포넌트 형식을 서버 응답에 맞게 수정하고 있다. 서버의 중복 항목 통합 및 추가로 회원가입, 수강 인증 페이지 레이아웃을 변경하고 있다. 이외 레이아웃은 기존 설계와 동일하게 유지되었다. 강의 생성, 공지사항, 서비스 소개 페이지를 구현한 후 다음 통합 테스트가 예정되어 있으므로 이 페이지들에 대한 레이아웃 변경이 예상된다.

2.2 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. 기능 요구사항에 따라 일부 누락된 칼럼을 추가하였다. api와 직관적으로 연동되도록 설계를 변경하였다. 예를 들어 강의 내용 테이블은 클래스 ID와 콘텐츠 ID를 키로 하여 api 호출시 클래스 ID와 콘텐츠 ID를 이용한 별도 탐색이나 계산없이 바로 해당 레코드에 접근 가능하다.

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.

2.3 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 dApp 을 다시 배포해야 하므로 강의자가 임의로 과정을 생성하거나 추가할 수 없도록 웹 레이아웃을 변경할 예정이다.

3 갱신된 과제 추진 계획

3.1 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																						
웹 설계																						
서버 설계																						
데이터베이스 설계																						
학습 콘텐츠 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 회색**으로 표시하였다.

4 구성원별 진척도

4.1 구성원별 진행사항

이름	역할
이승윤	서버, 데이터베이스, API 설계 (완료) 로컬 및 원격 서버 구축 (완료) 데이터베이스 구축 (완료) API 제작 및 연동 (진행 중) 이더리움 탈중앙화 분산 어플리케이션(dApp) 개발 (진행 중)
심재영	UI 디자인 (완료) 웹 레이아웃 구현 (진행 중)
김유미	UI 디자인 (완료) 웹 레이아웃 구현 (완료) 서버와 API 연동 (진행 중)
공통	블록체인, 이더리움 개념 학습 웹 페이지 레이아웃 설계 개발 환경 설정

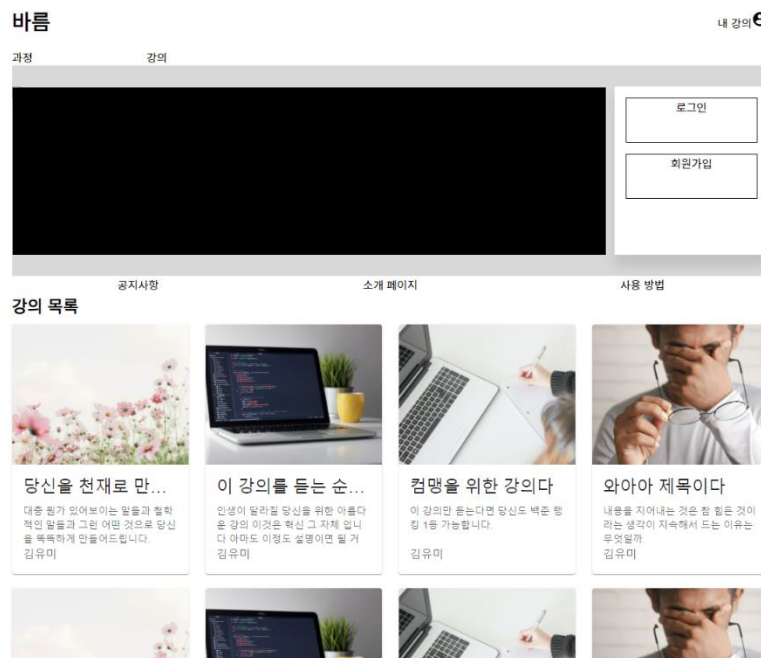
5 보고 시점까지의 과제 수행 내용 및 중간 결과

5.1 요약

현재 웹, 서버, 데이터베이스 설계가 완료된 상태이다. 웹은 Next.js 를 이용 전체 레이아웃 10 개 중 7 개 제작이 완료되었다. MySQL 로 데이터베이스 구축을 완료했으며 Node.js 기반으로 Express 프레임워크를 이용하여 서버 API 제작이 완료된 상태이다. 현재 완성된 레이아웃에 대해서는 사용자 기능(로그인, 로그아웃, 회원가입)에 대한 서버내 기능 테스트와 웹과의 통합 테스트가 완료되어 연동을 수행하였다. 현재 강의 수강 및 생성 기능에 대해 서버-웹간 연동 작업을 수행하고 있다. Truffle 과 Ganache 로 dApp 개발 환경을 구축 완료하였으며 강의 수강 관련 API 테스트 및 연동 작업 완료 이후 스마트 컨트랙트를 개발한다.

5.2 웹

- 메인 페이지



- 로그인 페이지

바름

과정

강의

내 강의 

로그인

testuser

로그인

- 회원가입 페이지

바름

과정

강의

내 강의 

회원가입

성명
ID
Password
회원가입

- 내 강의 페이지

바름

내 강의 9

과정

강의

수강 중

수강 완료

생성 강의

강의명 당신을 천재로 만들어주는 강의
강의자 김유미
강의기간 11:42:31
진도율 100%

수료중



강의명 이 강의를 듣는 순간 인생이 달라진다
강의자 김유미
강의기간 04:59:12
진도율 78%



강의명 컴맹을 위한 강의다
강의자 김유미
강의기간 00:42:31
진도율 3%



- 강의 수강 페이지

나는 강의명이다!!!

김유미

강의 목록

1번 강의다!!

2번 강의다!!!

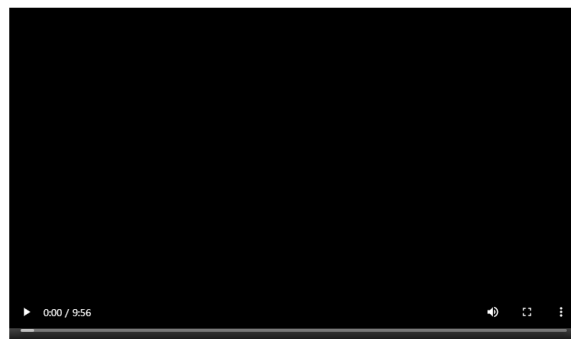
3번 강의다!!!

4번 강의다!!!!

5번 강의다!!!!

6번 강의다!!!!

1번 강의다!!



● 강의 정보 페이지

나는 강의명이다!!!

김유미

강의 목록

1번 강의다!!

2번 강의다!!!

3번 강의다!!!

4번 강의다!!!

5번 강의다!!!

6번 강의다!!!

나는 강의명이다!!!

김유미

강의 요약

이것은 강의요약이다. 왜냐면 강의 요약이기 때문이다. 대충 몇줄 정도를 적어야 강의 요약이라고 할 수 있을까?? 그것은 정해지지 않았다. 왜냐면 요약은 내 맘이기 때문이다. 이정도면 되겠지??

블록이 들어갈 공간을 만들어보자!!

강의 목록

1번 강의다!!
2번 강의다!!!
3번 강의다!!!
4번 강의다!!!

● 강의 조회 페이지

바름

과정

강의

내 강의

원하는 강의를 찾아보세요. (강제명, 교수자명 등)



소프트웨어
공과수학
재테크/금융
진자/전기
역학
생명/화학
졸업과제

당신을 천재로 만...

대충 뭔가 있어보이는 말들과 철학적인 말들과 그런 어떤 것으로 당신을 독특하게 만들어드립니다.

김유미

이 강의를 듣는 순...

인생이 달라질 당신을 위한 아름다운 강의 이것은 혁신 그 자체입니다. 아마도 이정도 설명이면 될 거

김유미

캠명을 위한 강의다

이 강의만 듣는다면 당신도 백종원 형 1등 가능합니다.

김유미

와아아 제목이다

내용을 지어내는 것은 참 힘든 것이라는 생각이 지속해서 드는 이유는 무엇일까.

김유미

당신을 천재로 만...

대충 뭔가 있어보이는 말들과 철학적인 말들과 그런 어떤 것으로 당신을 독특하게 만들어드립니다.

김유미

이 강의를 듣는 순...

인생이 달라질 당신을 위한 아름다운 강의 이것은 혁신 그 자체입니다. 아마도 이정도 설명이면 될 거

김유미

5.3 서버

5.3.1 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)	

5.3.2 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 목록	class/main		class[]
강의 목록	class/all		class[]
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

5.4 블록체인

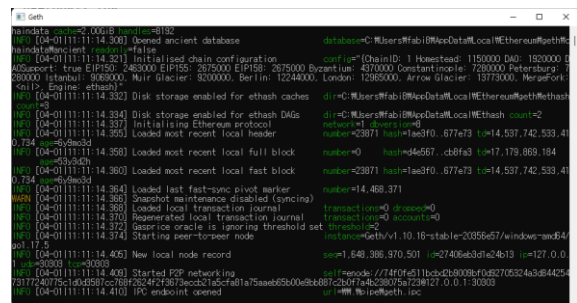
5.4.1 dApp 개발 환경

- Geth

이더리움 클라이언트 기능 사용 위해 Go Ethereum 클라이언트를 설치하였다.

Geth 는 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]

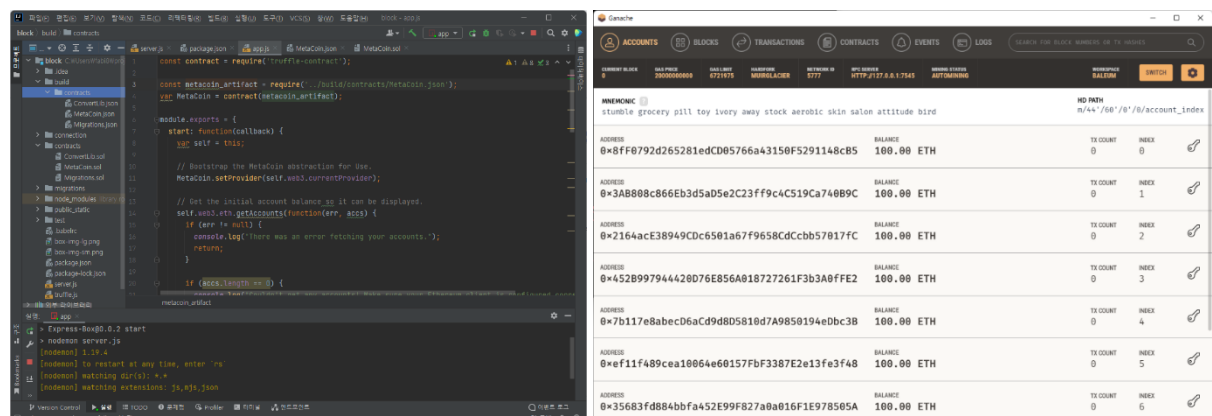
Geth 를 사용하여 제네시스 블록을 생성하고 사설 이더리움 네트워크를 실행해 보았다.



- Truffle 과 Ganache

트러플은 이더리움 가상 머신을 사용하는 블록체인을 위한 개발 환경, 테스트 프레임워크, 에셋 파이프라인을 제공한다. [4] Truffle boxes 는 dApp 을 빠르게 만들 수 있도록 하는 여러 템플릿으로 구성된다. 이 중 Express-Box 를 사용하여 기존 서버의 코드와 통합 작업을 수행하고 스마트 컨트랙트 코드를 작성할 수 있다.

가나슈는 이더리움 개발에 사용할 수 있는 개인용 블록체인으로 스마트 계약을 배포, 테스트해볼 수 있는 간이 블록체인을 제공한다. 네트워크 연결 필요 없이 로컬에서 작동시킬 수 있다. [5] Truffle 은 Ganache 를 통한 테스트를 기본적으로 지원하므로 로컬 환경에서 자유롭게 작성한 스마트 컨트랙트를 배포하여 테스트할 수 있다.



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] 조수현, 이정빈, 박재용, 이대건 그리고 인호, 이더리움 베이직, 북스타, 2017.
- [4] Truffle Suite, "Truffle | Overview," 31 3 2022. [온라인]. Available: <https://trufflesuite.com/docs/truffle/>. [엑세스: 31 3 2022].
- [5] 해시넷, "가나슈 - 해시넷," 1 9 2019. [온라인]. Available: <http://wiki.hash.kr/index.php/%EA%B0%80%EB%82%98%EC%8A%88>. [엑세스: 29 3 2022].