Journal of Korea Multimedia Society Vol. 24, No. 2, February 2021(pp. 255-266)
https://doi.org/10.9717/kmms.2020.24.2.255

퍼블릭 블록체인기반 대학 포인트 분산 시스템 개발

정세훈[†], 김정훈[††], 심춘보[†††]

Implementation of University Point Distributed System based on Public Blockchain

Se-Hoon, Jung[†], Jeong Hoon Kim[††], Chun-Bo, Sim[†††]

ABSTRACT

Most common web or application system architectures have central network. As a result, central network can be supervised and controlled in all situation. And It has the advantage of easy to manage and fast to work. However, central network have a disadvantage of weak to security and unclear. In particular, many institutions used by web system be has many problems by central network. In this paper, we proposed blokchain technology based on ethereum to resolve of problem and trading structure that arise in cental network. We propose a decentralized application based on points including cryptocurrency functions and smart contract to the advantages of blockchain with a decentralized structure. The results of the performance experiment are as follows; It has shown the advantages of reliable use and security in a variety of environments(Windows, Ubuntu, Mac).

Key words: Block Chain, DApp, Ethereum, Point, Smart Contract

1. 서 론

4차 산업기술 중 하나인 블록체인 기술은 중앙에서만 관리하지 않고 여러 시스템이 주가 되는 분산시스템 기술로 전통적인 정보 처리 방식으로 금융, 사회, 산업 전반을 변화시킬 새로운 기술로 떠오르는 중이다. 블록체인은 비트코인이 새로운 금융 상품으로 인식되면서 암호화폐를 중심으로 언급되고 있다. 블록체인 기술은 암호화폐를 위해 만들어진 새로운 암호화폐와 단순히 데이터를 안전하게 보관하는 것이 아닌 각 사용자의 조건이 반영된 계약 내용을 디지털 정보로 기록하고 사용자 계약의 성립 및 이행이 자동으로 실행하고 이행되는 스마트 계약(Smart Contract)으로 개념이 발전되었다. 블록체인 기술의 진화로 사회 전반을 아우르는 영역에 적용되어 각 분야에 알맞는 프로그램의 형태로 변형되고 있는 실정이다. 블록체인의 네트워크는 분산 원장 기술(Distributed Ledger Technology)을 사용하며 기능으로는 해당 블록체인 네트워크 내에 참가한 모든 사람이 모든 거래 내역을 기록한 원장을 소유하는 기술이다. 이 기술은 거래의 투명성이 높아 위변조가 불가하는 특징이 있으며 거래기록을 관리하는 거대

※ Corresponding Author : Chun Bo Sim, Address: (57922) 255, Jungang-ro, Suncheon-si, Jeollanam-do, Republic of Korea, TEL : +82-61-750-3830, FAX : +82-61-750-3834, E-mail : cbsim@scnu.ac.kr
Receipt date : Jan. 20, 2021, Revision date : Jan. 22, 2021
Approval date : Jan.22, 2021
[†] School of Creative Convergence, Andong National University
(E-mail : jungsh@anu.ac.kr)
[††] School of Information Commucation·Multimedia Eng., Sunchun National University
(E-mail : wjdngs111@naver.com)
[†††] School of Information Commucation·Multimedia Eng., Sunchun National University
※ This research was supported by Grand Information Technology Research Center support program(IITP-2020-0-01489) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation).

한 중앙시스템이 필요 없다는 점이 큰 특징이다. 새로운 블록을 추가 시 네트워크에 참가한 모든 참여자에게 거래기록의 타당성을 검증받아야 하므로 부정거래 혹은 위변조 등을 방지할 수 있다. 블록체인 기술은 앞서 언급한 바와 같이 여러 특징, 강점을 가진 기술로 산업 전반에 적용할 수 있다. 특히 블록체인 기술은 보안에 취약하고 불투명한 정보와 중앙집중화로 인해 피해를 보는 분야에 적용이 되면 기술 도입이 빨라지고 널리 활성화되고 있는 실정이다[1-4].

현재 대학교의 포인트는 저학년 때부터 체계적인 취업 준비를 지원하기 위해 다양한 취업 준비활동에 일정 점수 포인트를 부여하고 취득한 포인트를 합산하여 학생들의 관심이 많은 장학생, 해외 연수생, 생활관생 선발 시 반영함으로써 학생들의 취업 준비 활동에 동기를 부여해 주는 시스템이다.

본 논문에서는 불록체인 기술을 적용하여 대학교 포인트를 관리하는 시스템을 제안한다. 대학교에서 관리되는 시스템은 중앙집중형 시스템으로 대학교 관리 시스템의 기능인 포인트 신청과 승인과 포인트 상승, 포인트 조회 부분에 블록체인 기술을 접목하여 중앙집중형 시스템을 분산 원장 시스템으로 변경하여 신뢰성과 안전성, 보안성이 해당되는 플랫폼을 제안한다.

구성은 2장에서 본 논문의 활용되는 기술인 블록체인의 기본 이론, 이더리움, 스마트 계약, 메타마스크에 대하여 정의한 다음, 3장에서 시스템 설계를 제시하며, 어플리케이션의 구성, 흐름도, 클래스 다이어그램을 서술한다. 그리고 4장에서는 블록체인 기술을 적용한 대학 포인트 분산 애플리케이션의 구현 및 실험과 관련 연구와 비교를 서술하고 5장에서 결론을 맺는다.

2. 관련 연구

2.1 블록체인

블록체인은 기술적으로 거래, 계약 등의 정보가 분산 원장 상에 암호화 및 연결 저장된 데이터 사슬이다. 확대해서 정의하면 중앙서버 없이 프로그램의 자기 실행(Self-Execution)이 가능한 분산원장 네트워크 및 그에 수반되는 기술이다[4]. 블록체인은 2008년 사토시 나카모토에 의해 비트코인(Bitcoin)이 등장하면서 더욱 활발히 연구되기 시작하였다. 비트코인은 은행이 필요 없는 새로운 전자화폐를 제안하였다. 2009년 1월부터 일반 화폐와 다르게 중앙은행과 같은 중개 기관 없이 P2P 기반으로 사용자 간 자유롭게 온라인 가상화폐로서 거래할 수 있게 되었다[5]. 이처럼 블록체인은 암호화폐의 기술로 알려지고 사용되면서 시작되었다. 블록체인은 블록체이닝(Block Chaining)과 합의 알고리즘이라는 두 핵심기술로 구성되어 있다. 블록체이닝 기술은 일정 기간 내에 생성된 새로운 정보들을 블록 단위로 묶어서 가장 최근에 만들어진 블록에 연결하는 방식이다. 가장 최근에 생성된 블록의 정보를 암호화된 해시값으로 변환하여 현재 생성한 블록에 함께 저장한다.

합의 알고리즘 기술은 네트워크에 참여하는 참여자들 간에 정보 도달에 시차가 있는 P2P 네트워크와 같은 분산 시스템에서, 참여자들이 하나의 결과에 대한 합의를 얻기 위한 알고리즘이다. 블록체인은 분산 시스템으로 여러 참여자가 네트워크에 참여하기 때문에, 각 노드에서 만든 블록의 정당성을 검토하고 네트워크 전체에 공유하는 블록체인에 반영하기 위해 합의 알고리즘을 사용한다[6,7]. 비트코인 등장 이후 블록체인 기술을 기반으로 한 암호화폐가 등장하였다. 비트코인 캐시, 리플, 라이트코인, 대시, 이더리움 클래식, 모네로, Zcash 등이 비트코인 프로토콜을 수정하여 개발되었다. 이러한 암호화폐들은 기존에 중앙기관이 한 곳에서 관리와 감독하는 방식을 벗어나 탈중앙화된 거래방식 시스템으로 서비스를 제공하고 있다[8,9].

2.2 이더리움

이더리움은 이더리움 재단에서 관리하는 블록체인 플랫폼이다. 2015년 7월 비탈릭 부테린(Vitalik Buterin)에 의해 개발되었다. 이더리움은 비트코인과 마찬가지로 이더(Ether)라는 암호화폐를 사용한다. 이더리움은 금융거래에 한정, 특화된 블록체인 프로토콜을 기타 모든 분야로 확장할 수 있다는 것을 기술적으로 제시하였다. 비트코인을 비롯한 다수 블록체인에 없는 스마트 계약 기술을 적용하였다. 이더리움을 이용하면 법, 계약, 게임, 투표 등 모든 분야에 블록체인 기술을 접목할 수 있다. 이러한 기술 적용 분야는 화폐로써 활용된 1세대 블록체인과 다른 용도로 DApp(Distribution Application, 이하 분산 애플리케이션)으로 오픈 플랫폼을 발전하였다. 이러한

블록체인 기술의 발전으로 2세대 블록체인 즉, 블록체인 2.0 시대로 진입하였다[10,11]. 이러리움 플랫폼은 Solidity라는 별도 언어를 활용하여 스마트 컨트랙트라는 프로그램을 개발할 수 있다. 또한 스마트 컨트랙트를 통해 웹 또는 앱에서 활용할 수 있도록 web3라는 인터페이스를 통해 응용 프로그램과 상호작용을 한다. 그러나 이더리움은 퍼블릭 블록체인으로써 저장된 컨트랙트의 접근 권한이 모든 사용자가 될 수 있으므로 데이터 보안이 필요한 경우 별도의 시스템이 필요할 수 있다.

2.3 스마트 컨트랙트

Fig. 1은 스마트 컨트랙트의 구성도이다[12]. 스마트 계약은 현실의 권리 증명이나 이동 등을 포함한 계약을 자동으로 실행하는 소스 코드를 말한다. 블록체인 안에서 설정한 기준을 만족하면 계약을 자동으로 이행되는 자동 계약 프로그램을 뜻한다. 이 개념은 비트코인 전부터 존재하던 개념이며 1994년 암호학자인 닉 스자보(Nick Szabo)에 의해 발표되었다. 스마트 계약은 많은 장점이 있는 프로그램이다. 첫 번째 장점은 상대를 신뢰하지 않아도 거래에 문제가 발생하지 않는다. 조건에 부합한 상황이 발생하면 자동으로 실행되기 때문에 상대를 신뢰이지 않더라도 거래가 자동으로 실행된다. 두 번째 장점은 중개자가 필요하지 않다. 기존 중앙집중형 거래에서 신뢰할 수 있는 중개자나 신용 기관을 스마트 계약이 대체할 수 있다. 세 번째 장점은 비용을 절감할 수 있다. 스마트 계약을 이용하면 자동으로 거래처리가 가능하여 사람의 개입과 신뢰 기관의 개입 필요성이 없어 비용이 절감된다. 네 번째는 정확성이 높아진다. 사람의 손으로 작업하던 계약과 내용 전달 부분에서 자동화된 시스템으로 관리되기 때문에 조작, 불이행, 오류를 대부분 제거한다.

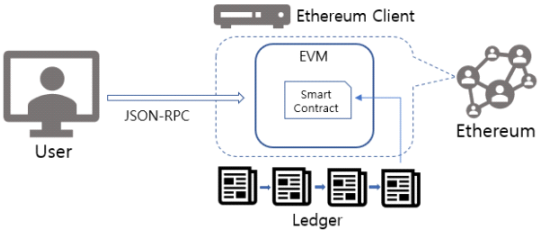


Fig. 1. Configuration Diagram of Ethereum Smart Contract.

이러한 장점들이 있는 스마트 계약은 각각의 거래에 대해 중복된 작업이 빈번한 경우 편리하게 적용될 수 있다. 특히 스마트 계약을 적용하기 좋은 분야는 계약의 범위가 좁고, 객관적이고, 기계적이고, 조건과 산출물이 명확하게 정의될 수 있는 분야이다[13].

2.4 메타마스크

블록체인 지갑(wallet)은 블록체인 계정의 잔고를 관리하는 것만이 아닌 사용자의 개인키를 저장하고, 사용자를 대신해 트랜잭션을 생성해 Broadcast할 수 있다. 이런 의미에서 지갑은 일반 사용자의 블록체인 네트워크로의 가장 쉬운 접근방식이라 할 수 있다[14]. 메타마스크는 이더리움 지원 분산 응용 프로그램 또는 일반 크롬 브라우저의 분산 애플리케이션에 액세스하기 위한 크롬 확장 프로그램이다. Fig. 2와 같이 확장 프로그램은 이더리움 웹 어플리케이션에서 JSON-RPC와 Web3 API를 모든 웹 사이트의 자바 스크립트 컨텍스트에 적용하여 분산 애플리케이션이 블록체인에서 읽을 수 있도록 한다. 메타마스크는 또한 사용자가 자신의 ID를 생성하고 관리할 수 있게 해주므로 분산 애플리케이션이 트랜잭션을 수행하고 블록체인에 쓰려고 할 때 트랜잭션을 승인하거나 거부하기 전에 트랜잭션을 검토할 수 있는 안전한 인터페이스를 활용하게 된다.

3. 시스템 설계

3.1 대학교 포인트 활용 시스템 구성

본 논문에서의 대학교 포인트를 볼록체인 기술인 이더리움과 스마트 컨트랙트를 활용하여 분산 애플리케이션을 설계를 제안한다. 제안하는 분산 애플리케이션은 프론트엔드, 백엔드, 스마트 컨트랙트와 같이 세가자제가지 부분으로 구분되며 Fig. 3과 같다.

먼저, 프론트엔드는 HTML, CSS, JavaScript로 User가 분산 애플리케이션에 접근하기 위한 웹페이

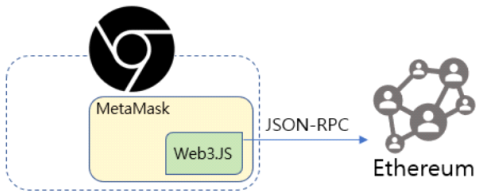


Fig. 2. Configuration Diagram of JSON-RPC and web2.

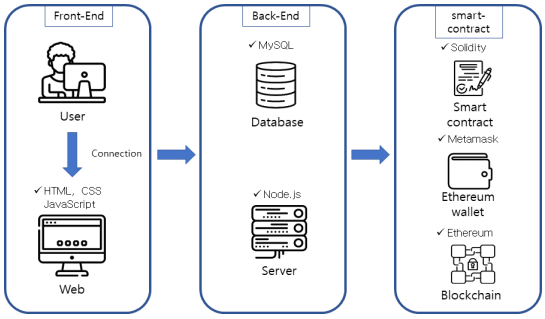


Fig. 3. Configuration Diagram of Proposed System.

지를 적용다. 백엔드는 서버인 Node.js로 구성되었으며, 사용자 정보를 받을 Database인 MySQL를 사용하였으며 마지막 스마트 컨트랙트는 Solidity이며 포인트 토큰과 이더리움을 보관, 관리하는 이더리움 지갑인 메타마스크를 적용한다. 해당 연구에는 메타마스크 로그인이 되어야 시스템을 활용할 수 있다.

3.2 대학 포인트 시스템 구성자 설계

분산 애플리케이션 구성자는 먼저 메타마스크가 등록되어야 한다. 메타마스크는 크롬의 확장 프로그램에 해당하는 이더리움 지갑이다. User는 3가지인 관리자, 사용자, 담당자로 나뉘며 관리자는 스마트 컨트랙트를 배포한 이더리움 지갑 주소가 관리자가 된다. 사용자는 웹 사이트의 sign up을 통해 정의된다. 사용자와 관리자의 처리 프로세스 설계는 다음과 같다.

3.2.1 사용자 처리 프로세스

Fig. 4와 Fig. 5는 대학 포인트 분산 시스템의 사용자 처리 프로세스 설계도이며, Usecase Diagram과 Sequence Diagram이다. User는 포인트 분산 애플리케이션을 참여하기 위해서는 sign up을 통해 회원을 가입해야 한다. 정보 입력 후 가입 시 Solidity로 만들어진 코드 즉, 스마트 컨트랙트가 활성화되며 메타마스크의 트랜잭션 확인 창이 나타난다.

User는 승인 시 회원가입이라는 기능(memberindexing 스마트 컨트랙트 함수)을 실행되며 메타마스크 지갑에 있는 이더리움이 소모되며 블록체인 내에 사용자의 정보가 가입이 된다. 웹사이트로 인한 가입은 회원ID로 구분하여 memberindexing의 함수에 맞게 사용자, 행사 담당자로 나뉜다. upload를 통해 User는 포인트 획득을 위한 정보들을 입력하는 부분이다. 획득할 해당 종목, 내용, 첨부파일을 작성하고

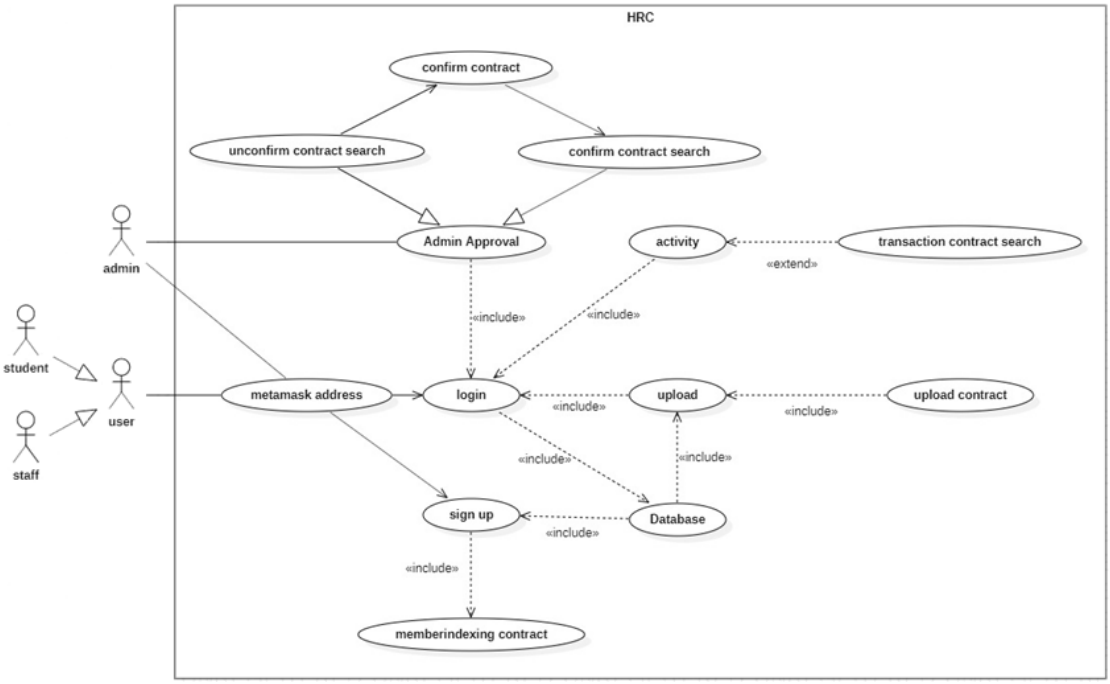


Fig. 4. User Usecase Diagram.

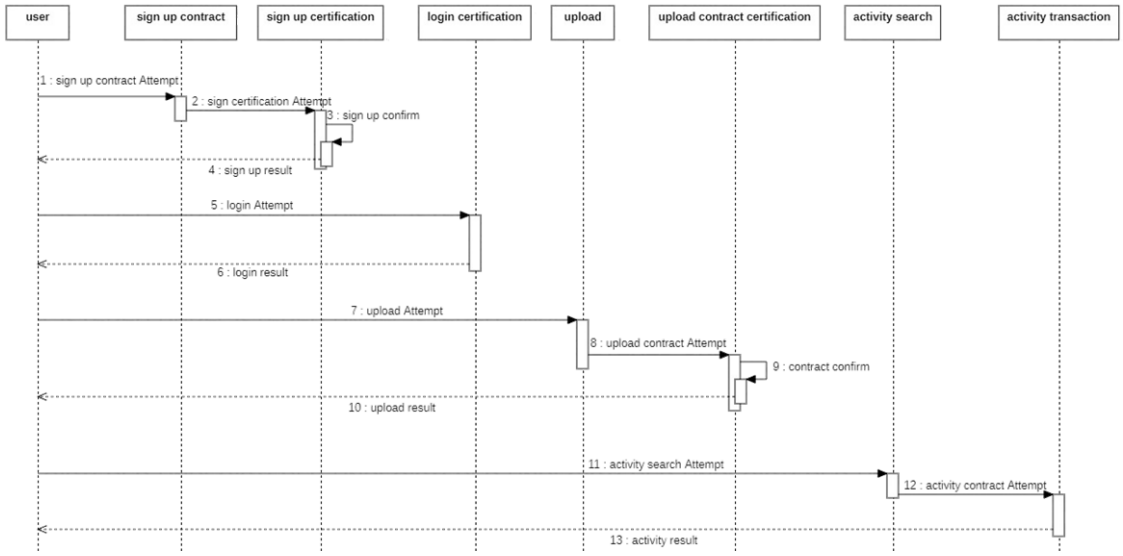


Fig. 5. User Sequence Diagram.

자동입력된 작성자, 학번, 지갑주소, 작성일시를 업로드와 승인을 하면 스마트 컨트랙트 학생 또는 행사 담당자의 upload 함수가 실행되고 트랜잭션이 발생하고 해당 블록체인 내에 사용자의 upload내역이 업로드된다. 마지막 activity는 사용자가 업로드한 내역을 볼 수 있으며 각각의 information과 포인트와 총 적립 포인트를 알 수 있는 웹페이지이며 블록체인 내에 업로드된 내역을 web3.js를 통해 검색해 출력한다.

3.2.2 관리자 처리 프로세스

Fig. 6은 관리자 Seqence Diagram으로 학생과 행사 담당자가 포인트 정보를 업로드한 내역들을 승인을 하기 위한 처리 프로세스이다. 관리자는 Admin 페이지에 접속하여 업로드된 포인트 정보들을 확인할 수 있다. 관리자가 직접 정보를 확인 후 승인을

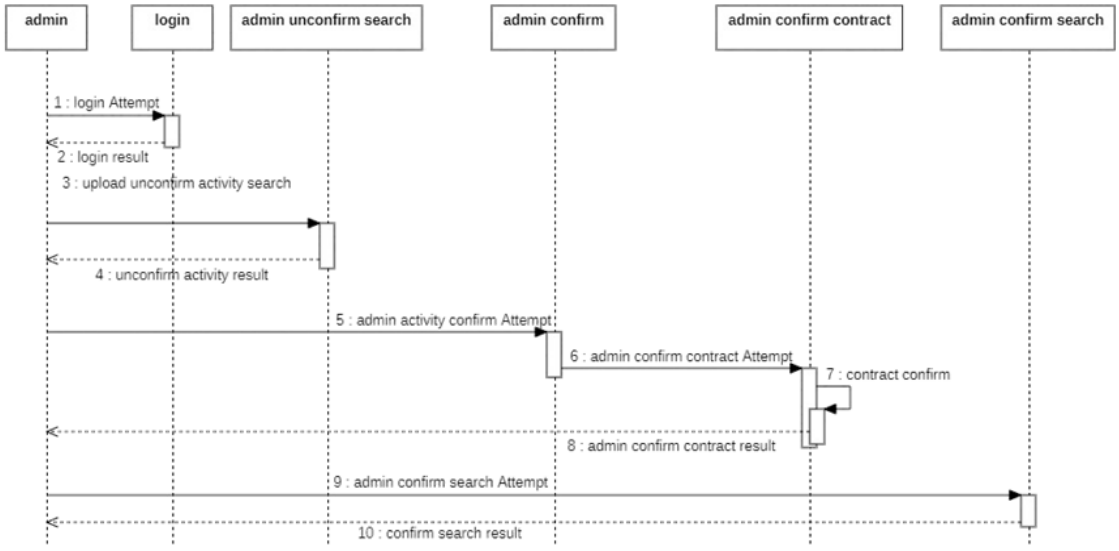


Fig. 6. Admin Sequence Diagram.

할 시 스마트 컨트랙트의 confirm함수가 실행된다. confirm함수의 내의 조건과 맞을 시 해당 포인트 내역은 블록체인 정보 내에서 승인 정보 내역으로 이동하여 저장하게 된다.

3.2.3 시스템 클래스 다이어그램

Fig. 7은 전체 시스템인 퍼블릭 블록체인기반 포인트 분산 애플리케이션 구현의 Class Diagram이다. 관리자와 일반 사용자(학생, 담당자)로 나눠진다. 먼저, 관리자 기준으로 관리자는 login, admin과 home만 이용한다. 관리자는 따로 스마트 컨트랙트가 배포 시 배포한 이더리움 지갑주소가 관리자가 되므로 sign up과 포인트 업로드인 upload와 적립된 포인트를 볼 수 있는 activity는 제외가 된다.

관리자는 자신의 id, password, address(메타마스크 지갑 주소정보)를 입력을 하여 login을 할 수 있다. login시 관리자는 home과 admin을 사용할 수 있으며 home에서는 Database에서 저장되어 있는 name를 출력하게 되고 *web3.eth.getAccounts()*로 지갑계정을 찾아 school_id와 address를 *web3.eth.getBalance()*로 ethurum을 *contract.balanceOf()*로 포인트를 알 수 있다. admin은 일반사용자가 포인트 승인할 내역인 Request이벤트 함수를 통해 address, school_id, file_hash, point을 보고 승인 스마트 컨트랙트인 contract.confirmData과 포인트를 획득할 *contract.transfer()*함수를 실행한다. 만약 포인트 내역이 올바르지 않으면 관리자는 승인을 하지 않으면 된다. 사용자는 admin을 제외한 모든 기능을 사용한다. 먼저 블록체인 내에 사용자의 정보를 등록하기 위해 school_id, password를 기입하여 스마트 컨트랙트 *contract.memberindexing()*을 통해 가입을 하고 MySQL에는 name까지 추가하여 저장한다. login에서는 관리자와 같이 id, password, 이더리움 지갑주소를 기입하여 로그인을 한다. 해당 정보는 MySQL에 저장된 사용자 정보를 찾아 비교하여 로그인이 된다. 다음 upload는 포인트 획득할 정보인 종목인 category, name, school_id, address, createDate, filehash, contents를 기입하여 업로드한다. 업로드는 *contract.uploadDate()*스마트 컨트랙트 함수로 실행되며 업로드하는 사람이 로그인 정보와 같으면 등록이 된다. home부분은 관리자와 같다. activity는 *web3.eth.getAccounts()*를 사용해 현재 사용중인 지갑 사용자 정보를 불러 *contract.balanceOf()*로 포인트를 불러오고 *contract.RequestStudent()*로 포인트 내역인 info와 point를 불러와 출력하게 된다.

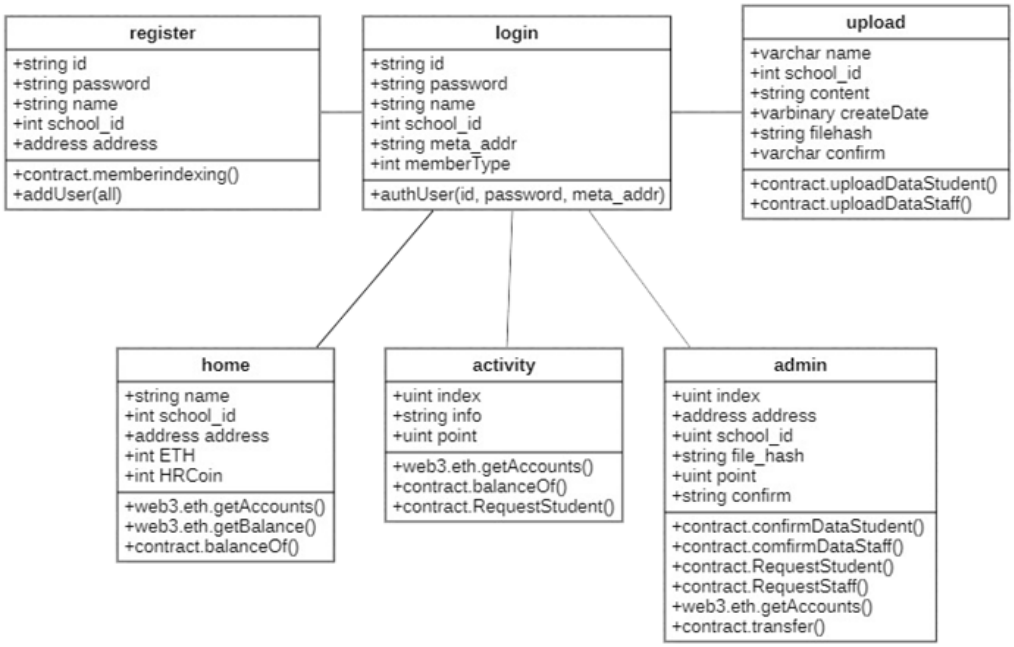


Fig. 7. Smart Contract Class Diagram.

```
contract ERC20 is MembershipSetting, Upload
{
    using SafeMath for uint256;

    string public name;
    string public symbol;
    uint8 public decimals;

    mapping (address => uint256) private _balances;
    mapping (address => mapping (address => uint256)) private _allowed;

    uint256 private _totalSupply;

    event Transfer(address indexed _from, address indexed _to, uint256 _value);
    event Approval(address indexed _owner, address indexed _spender, uint256 _value);

    constructor() public{
    name = "HACoin";
    symbol = "HAC";
    decimals = 18;
    _mint(msg.sender, 100000 * (10 ** 18));
    }
}
```

Fig. 8. Creative Code of Token and Coin.

3.3 사용자 코인 및 토큰 생성 설계

Fig. 8은 사용자의 인증정보를 기반으로 생성된 지갑에 작성된 포인트 데이터에 대한 토큰 생성과 코인 생성에 대한 함수를 나타낸다. 사용자의 지갑 주소와 생성한 값을 전달받아 해당 값을 원장에서 조회하고 조회한 결과에 따른 토큰 생성과 원장에 저장하는 코드이다. 이를 위해 ERC-20을 기반으로 토큰과 코인을 생성한다.

4. 대학 포인트 분산 애플리케이션 구현

4.1 개발 환경 및 구현

제안하는 대학 포인트 분산 시스템인 분산 애플리케이션은 Table 1의 환경에서 구현과 테스트가 진행되었다. 분산 애플리케이션은 메인 서버 1대와 서브 서버 2대(사용자, 담당자)로 이루어졌으며, 메인 서버는 Web 서버와 Database의 서버를 오픈하는 용도로 사용되었으며, 나머지 서브 서버는 각각 사용자와 담당자로 구분하여 구성된다.

Table 1. Implementation and Test Environment.

Item	Content
OS	Window 10
Smart Contract	Solidity
Distributed Computing Platform	Ethereum
Database	MySQL
Server	Node.js
Web	HTML, CSS, Javascript

4.2 분산 애플리케이션 인터페이스 구현

Fig. 9는 프론트엔드 웹 인터페이스 부분이다. 메인 서버는 Node.js로 해당된 프로젝트 index.js에서 서버를 구동한다. 각각의 인터페이스는 아래 그림과 같다.

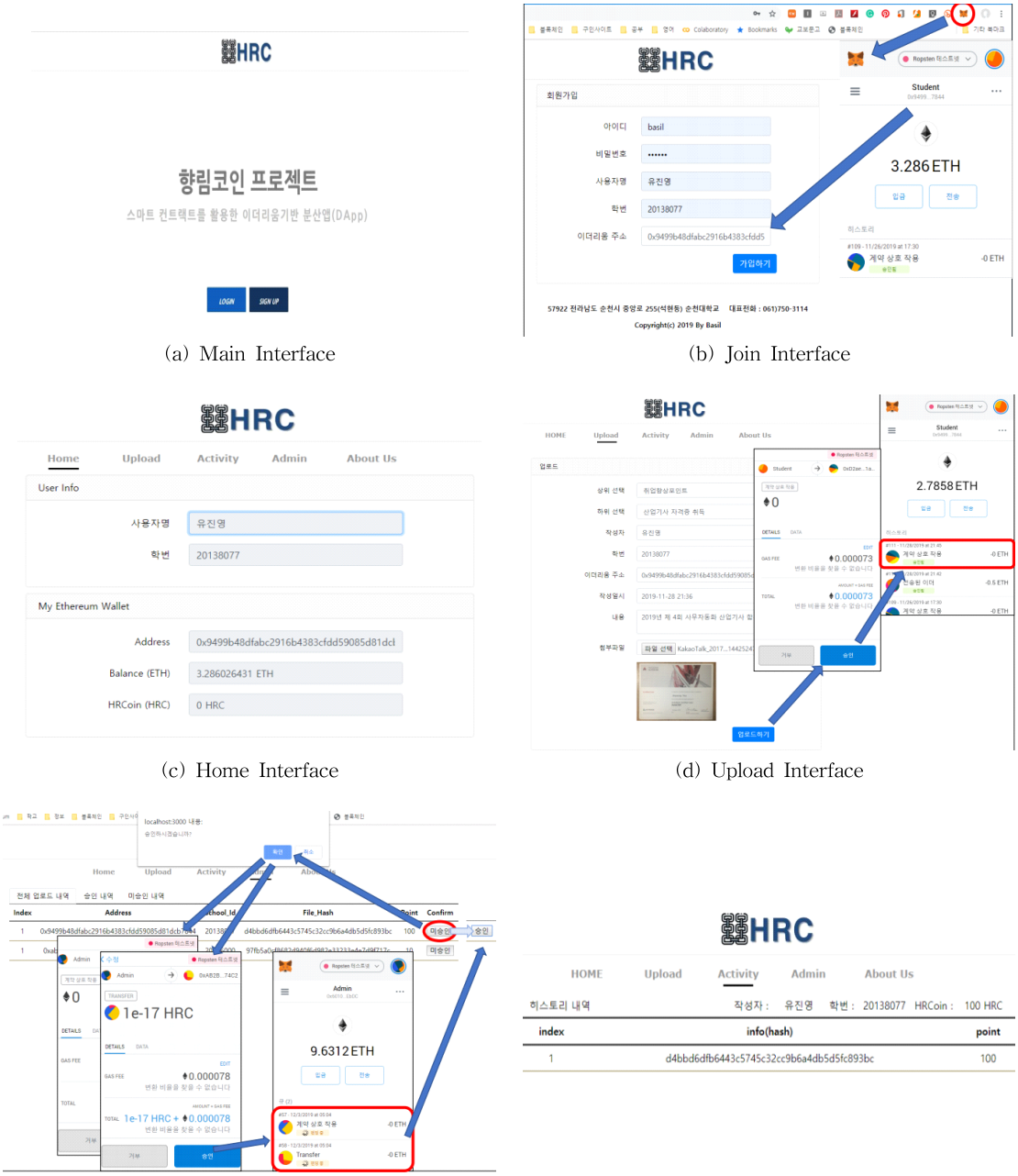
총 6개의 인터페이스로 구분되어 있으며, Main Interface, Join Interface, Home Interface, Upload Interface, Admin Interface. Activity Interface로 분류한다. Main Interface는 프론트엔드 인터페이스의 기본 페이지로써 로그인의 유무를 확인하는 페이지이다. Join Interface는 회원가입 페이지로써 새로운 회원가입 및 이러디움의 주소값을 확인할 수있다. Home Interface는 로그인 후 지갑 주소와 포인트 정보를 확인할 수 있는 개인 정보 페이지이다. Upload Interface는 새로운 포인트를 작성하는 페이지이다. Admin Interface는 새롭게 작성된 포인트를 승인하는 페이지로써 관리자 인터페이스에 해당된다. Activity Interface는 승인된 포인트를 확인할 수 있는 페이지이다. 사용자와 관리자에 따라 인터페이스가 구분되어 있으며, 각각의 인터페이스는 사용자 인터페이스와 관리자 인터페이스로 구분하여 설명한다.

4.3 사용자 인터페이스

Fig. 10은 User(사용자와 담당자)에 대한 인터페이스이다. User는 해당 분산 애플리케이션의 데이터베이스에 회원 정보가 없기 때문에 sign up을 하여 가입하기를 누르면 메타마스크 트랜잭션 창이 나와 승인을 하게 되면서 해당 트랜잭션이 성공을 하면 성공화면이 출력되면서 회원가입이 된다. 로그인 페이지에는 로그인을 하면 home 페이지에 개인신상과 이더리움, 코인이 출력된다. upload 페이지에서는 항목 선택, 내용, 첨부파일을 삽입하여 업로드하기를 하면 되면 메타마스크 트랜잭션 창이 나오면서 승인을 하면서 해당 트랜잭션이 성공을 하면 성공화면이 출력되면서 업로드된다. 마지막 activity 페이지에서는 자신이 업로드한 내역과 누적 코인을 볼 수 있는 페이지 항목이다.

4.4 관리자 인터페이스

Fig. 11은 Admin(관리자) 인터페이스로써 별도의 회원가입 없이 바로 로그인 페이지에서 로그인을 진



(a) Main Interface (b) Join Interface

(c) Home Interface (d) Upload Interface

(e) Admin Interface (f) Activity Interface

Fig. 9. Implementation Interface.

행한다. Admin 페이지로 접속하여 사용자, 담당자가 업로드된 미승인된 내역중 하나를 승인하고자 할 경우, 승인 버튼을 누르고 확인을 하면 메타마스크 트랜잭션 창이 출력되고 승인 처리를 함에 따라 미승인을 승인으로 변경해준다.

4.5 실험 및 성능평가

본 논문에서 제안하는 관련 연구는 블록체인 2세대인 이더리움을 사용하여 보안성과 투명성을 높인 것으로 말할 수 있다. Table 2는 분산 애플리케이션을 블록체인 기술을 사용하지 않은 일반 어플리케이

Table 2. Comparison of Feature Between Existing and Proposed Applications.

Item	Proposed DApp	Exisiting Applications
Security	High	Normal
Transparency	High	Low
Speed	Low	High
Forgery	Impossible	Normal
Network	Distribution Network	Central Network

션과 정성적인 비교 평가표이다. 제안한 포인트 시스템은 보안성과 투명성이 주요 목적이기 때문에 일반 애플리케이션보다 높다고 할 수 있으며 속도는 메타마스크와 블록체인 기술이 활용되어 승인 클릭과 승인되는 시간 때문에 일반 애플리케이션보다 비용이 많이 발생한다는 단점이 존재한다. 위변조 부분은 분산 애플리케이션은 스마트 컨트랙트로 구성된 블록체인의 정보는 변경이 불가하는 특성 때문에 가능성이 없었으며 일반 애플리케이션은 사용자에 따라 다르므로 가능성이 있다.

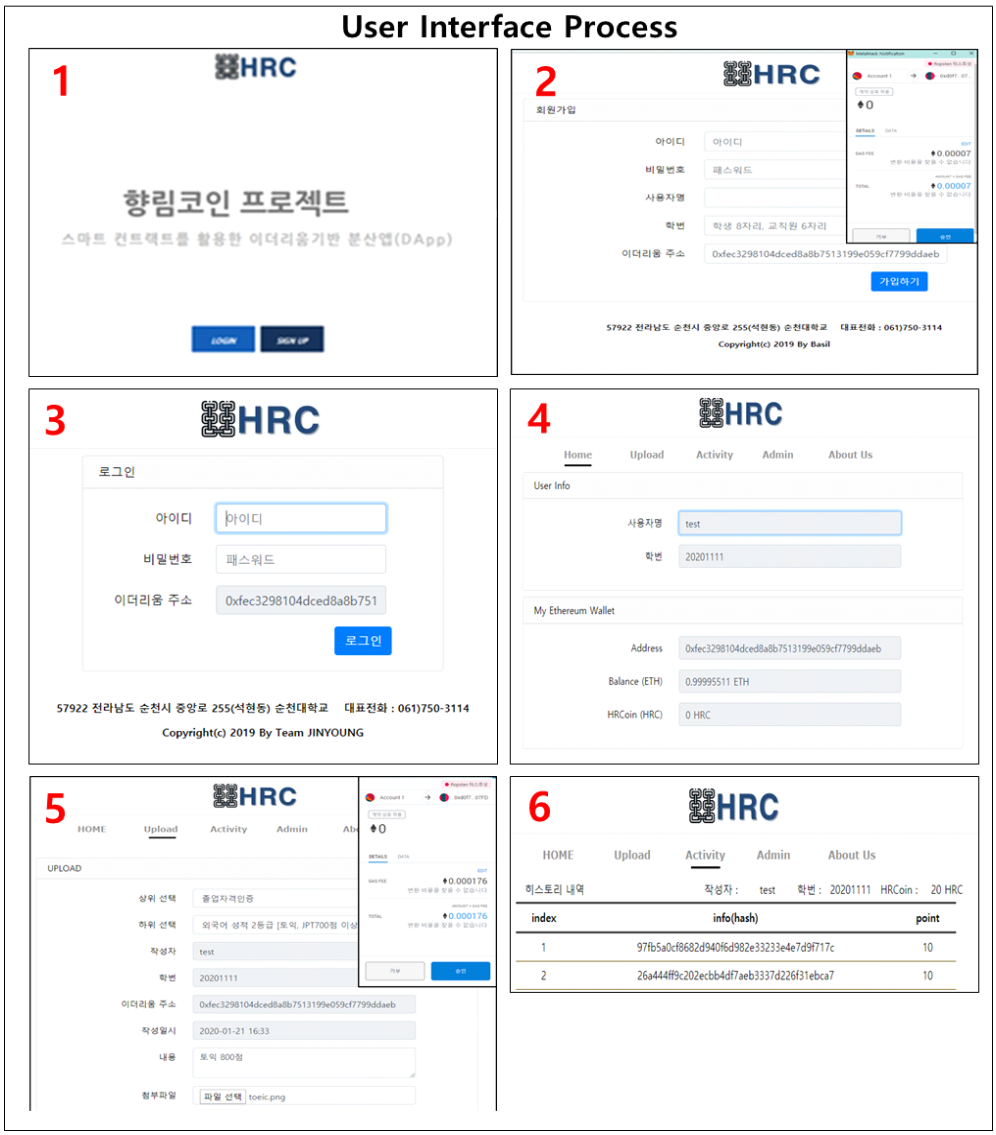


Fig. 10. User Interface Process.

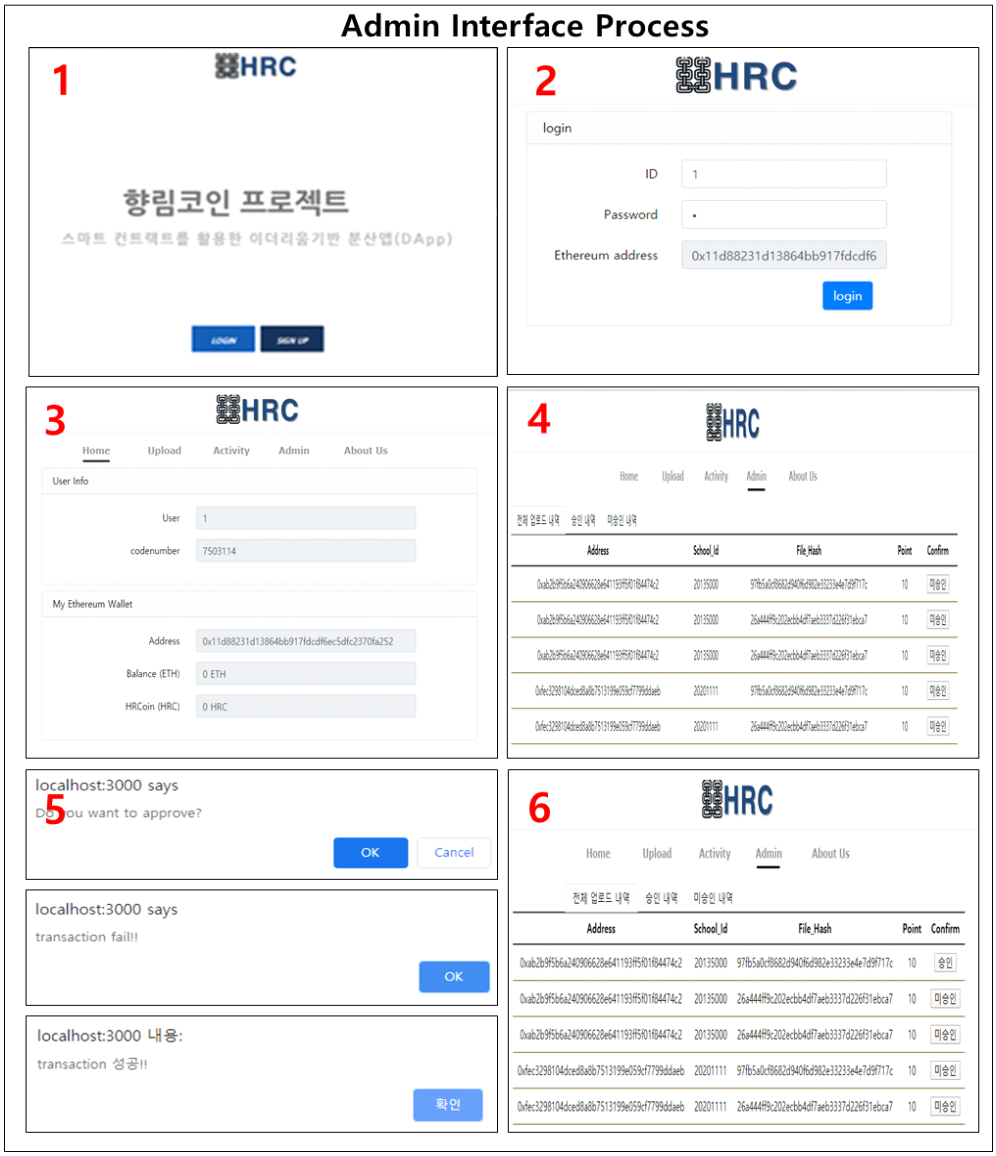


Fig. 11. Admin Interface Process.

Table 3은 100개의 시드를 적용하여 메타마스크 지원 브라우저에서 암호 서명 데이터의 공개 키와 연결된 지갑주소간의 데이터를 안정적으로 복구하는 ecRecover 복구 실험을 각 운영체제에서 100회 실시한 결과이다. 실험은 사용자의 지갑 주소 복구 횟수와 실험 횟수를 반영한 백분율을 평가하였다. 성능평가 결과를 통해 메타마스크의 서명 알고리즘이 실험에 반영한 브라우저에서 동일하게 동작하여 같은 암호 서명 데이터를 출력하는 것을 확인할 수 있다. 그리고 실험에 적용한 3가지 운영체제인 Windows, macOS, Linux 환경에서 정상적으로 사용자의 지갑 주소를 복구하는 것을 확인하였다.

Table 3. Performance Evaluation of ecRecover Rate (Recover Success Rate).

Item	Chrome	Firefox	Opera
Windows	100%	100%	100%
Ubuntu	100%	100%	100%
macOS	100%	100%	100%

5. 결 론

지난 몇 년간 블록체인이라는 기술은 비트코인이 새로운 금융 상품으로 인식되면서 암호화폐를 중심으로 다양한 분야에서 중요성이 언급되고 있다. 블록체인 기술은 암호화폐를 위해 만들어진 새로운 암호화폐와 단순히 데이터를 안전하게 보관하는 것이 아니라 각 사용자의 조건이 반영된 계약 내용을 디지털 정보로 기록하고 사용자 계약의 성립 및 이행이 자동으로 실행하고 이행되는 스마트 계약으로 개념이 발전되고 있다. 본 논문에서는 블록체인 이더리움을 이용하여 대학교 포인트 분산 애플리케이션 개발 및 구현을 진행하였다. 해당 분산 애플리케이션에서는 블록체인 기술인 이더리움, 분산 원장 기술과 스마트 컨트랙트를 사용하여 대학교 코인에 대해 신뢰성과 보안성을 늘린 분산 애플리케이션이라고 할 수 있다. 제안하는 시스템을 적용하여 실험 및 평가를 진행한 결과 기존의 시스템과는 달리 포인트에 대한 위변조가 불가능한 블록체인으로 인해 보안성이 향상되었으며, 사용자의 편의성과 안정성, 신뢰성을 제공하였다. 또한 브라우저에서 암호 서명 데이터의 공개 키와 연결된 지갑주소를 리턴을 증명하는 복구하는 ecRecover 실험을 통해 다양한 환경의 브라우저에서 데이터 손실율이 없는 100%의 성능을 확인하였다.

본 논문에서는 블록체인을 이용하여 대학의 포인트 얻기 위해 사용자들의 업로드와 관리자의 승인/미승인 부분에 한정하여 연구를 진행하였지만 향후에는 위변조되기 어려운 점을 이용한 신뢰성과 보안성을 기준으로 기숙사, 행사 참여, 도서이용 기간 확장, 장학금 등에 활용되면 좋을 것이며 교외 기준으로는 취업연계와 연결하여 코인을 획득시 가산점으로 활용하는 대학교 통합 분산 애플리케이션에 대한 연구를 진행할 것이다.

REFERENCE

[1] Z. Zheng, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proceeding of 6th IEEE International Congress on Big Data*, pp. 558-560, 2017.

[2] S. Y. Hong, S. R. Cho, and S. H. Kim, “Blockchain Beyond Bitcoin,” *Electronics and Telecommunications Research Institute*, Vol. 32, No. 1, pp. 72-81, 2017.

[3] S. Panicker, V. Patil, and D. Kulkarni, “An Overview of Blockchain Architecture and it’s Applications,” *International Journal of Innovative Research in Science, Engineering and Technology*, Vol. 5, Issue 11, pp. 1111-1125, 2016.

[4] K. N. Lee and G. H. Jeon, “A Study on Improvement of Used-goods Market Platform Using Blockchain,” *Journal of Digital Convergence*, Vol. 16, No. 9, pp. 133-145, 2018.

[5] D. H. Kim and K. R. Seo, “Measuring Email User Reliability in a Blockchain Environment,” *Journal of Korea Multimedia Society*, Vol. 23, No. 8, pp. 1030-1039, 2020.

[6] D. H. Kim and K. R. Seo, “PGP Certification System in Blockchain Environments,” *Journal of Korea Multimedia Society*, Vol. 23, No. 5, pp. 658-666, 2020.

[7] S. Y. Hong, S. R. Cho, and S. H. Kim, “Blockchain Beyond Bitcoin,” *Electronics and Telecommunications Research Institute*, Vol. 32, No. 1, pp. 72-81, 2017.

[8] C. H. Lee, *Design and Implementation of IoT System using Blockchain Technology*, Master Thesis of Sejong University, 2019.

[9] K. H. An and H. J. Seo, “Donate system development using Blockchain technology,” *Journal of the Korea Institute of Information and Communication Engineering*, Vol. 22, No. 5, pp. 812-817, 2018.

[10] D. K. Lee and T. K. Kwon, “Automated Classification of Unknown Smart Contracts of Ethereum Using Machine Learning,” *Journal of the Korea Institute of Information Security & Cryptology*, Vol. 28, No. 6, pp. 1319-1328, 2018.

[11] S. G. Kim, “A Study on the Blockchain 2.0 Ethereum Platform Analysis for DApp Development,” *Journal of Korea Institute of Information, Electronics, and Communication Technology*, Vol. 11, No. 6, pp. 718-723, 2018.

[12] N. H. Choi, and H. Y. Kim, "A Blockchain-based User Authentication Model Using Metamask," *Journal of Internet Computing and Services*, Vol. 20, No. 6, pp. 119-127, 2019.
[13] S. Jani, "An Overview of Ethereum & Its Comparison with Bitcoin," *International Journal of Scientific & Engineering Research*, Vol. 10, Issue. 8, pp. 1-7, 2018.

정 세 훈

2010년 2월 순천대학교 멀티미디어공학과 공학사
2012년 2월 순천대학교 멀티미디어공학과 공학석사
2017년 2월 순천대학교 멀티미디어공학과 공학박사
2018년 9월~2020년 2월 영산대학교 빅데이터융합전공 조교수
2020년 3월~현재 안동대학교 창의융합학부 조교수
관심분야 : 최적화 알고리즘, 강화학습, 블록체인

김 정 훈

2020년 2월 순천대학교 멀티미디어공학과 졸업(공학사)
2020년 3월~현재 순천대학교 대학원 멀티미디어공학과 석사과정
관심분야 : 딥러닝, 블록체인, 자연어처리

심 춘 보

1996년 2월 전북대학교 컴퓨터공학과 공학사
1998년 2월 전북대학교 컴퓨터공학과 공학석사
2003년 2월 전북대학교 컴퓨터공학과 공학박사
2005년 3월~현재 순천대학교 정보통신·멀티미디어공학부 교수
관심분야 : 빅데이터 시스템, 머신러닝, IoT/IoE 플랫폼, 멀티미디어