

http://dx.doi.org/10.17703/JCCT.2019.5.1.451

JCCT 2019-2-58

블록체인을 활용한 개인 맞춤형교육 통합모델 제안

A Proposal on the personalized integrated Education Model Using the Blockchain

유경성*, 권미란**

Kyoung-sung Yu*, Mee-Rhan Kwon**

요약 우리나라 학생들의 학업성과 삶의 만족도가 반비례 한다는 보고가 나와 충격을 받고 있다. 경제협력개발기구(OECD)가 발표한 국제학업성취도평가(PISA) '2015 학생 삶의 질 만족도 보고서'에 의하면 한국 학생들의 학력수준은 OECD 국가 가운데 최상위층이지만 '삶의 만족도'는 비 OECD국가를 포함한 OECD국가 48개국 중 47위로 최하위권으로 나타났다.[1] 이것은 집단적인 성적위주 평가방식의 일방적인 교육이 그 요인이라고 보고 블록체인 기술을 활용한 개인맞춤형 통합 모델을 연구하고자 한다.

보안성, 투명성, 분산성이 특징인 블록체인 기술을 활용하여 공급자 일방의 교육 및 일방적인 개인성적 공개위주 시스템에서 선택교육 및 개인승인을 통한 개인맞춤형 교육 및 평가시스템 모델을 연구하였다. 이 연구를 통하여 교육의 본질을 고려하면서 개인별 맞춤교육 및 평가관리시스템이 학생 삶의 질 개선에 기여한 의의를 가지고자 한다.

주요어 : 블록체인, 개인 맞춤형교육, 평가방법, 삶의질, 교육의 본질

Abstract Our students are shocked by the results that there is an inverse proportion between academic achievement and life satisfaction. Recently, the Organization for Economic Cooperation and Development (OECD) published the PISA 2015 Student Well-Being Report. According to the report, Korean students' education is the highest among OECD countries, but their life satisfaction is the 47th ranked among the 48 OECD and non-OECD countries.[1] This is the cause of the unilateral education using collective achievement in evaluation methods. Therefore, I propose a personalized integrated model utilizing block chain technology.

I suggest a personalized education and evaluation system model using selective education and personal approval rather than from teachers' unilateral education. This will no longer open the student's achievement grade system to the public. This change will be accomplished utilizing block chain technology. This technology is characterized by security, transparency and dispersion. The result of this work can be used to improve students' quality of living through a management system of personalized education and evaluation, based on the nature of education.

Key words : Block chain, Personalized Education, Evaluation Methods, Quality of Living, The nature of Education

*정회원, 한세대학교 IT융합학과 (교신저자)

**정회원, 나사렛대학교 아동학과 (참여저자)

접수일: 2018년 12월 9일, 수정완료일: 2019년 1월 3일

게재확정일: 2019년 1월 10일

Received: December 12, 2019 / Revised: January 3, 2019

Accepted: January 10, 2019

*Corresponding Author: olley@naver.com

Dept. of ICT, Hansei Univ, Korea

I. 서론

한국교육신문 2017년 4월23일자 기사에서 우리나라 학생의 82%가 학급에 최고, 75%가 이른바 성적 스트레스에 시달리고 있는 것으로 나타났다. 이에 OECD(경제협력개발기구) 국가들은 각각 59%, 66%였다. 우리나라 학부모는 54%정도만이 자녀와 매일 대화하는 것으로 조사되었다. 운동도 가장 안하는 것으로 조사되었다.

다음은 OECD가 전 세계 15세 학생 54만 명을 대상으로 전반적인 삶의 만족도와 부모와의 관계, 성취동기, 신체활동 등과 쓰기, 읽기 등 학업성취도 평가와 함께 2015년에 조사한 내용과 비교해 발표한 것이다.

OECD가 개인 삶의 만족도를 0점(최저)~10점(최고) 기준으로 학생들을 조사한 결과, 우리나라 학생들의 평균점수는 6.36점으로 OECD 28개 나라 중에서 터키(6.12점) 다음으로 낮았다. 비(非)OECD 국가를 합친 48개국 중에서도 터키 다음으로 최하위였다. 그리고 청소년들은 공부를 잘 하고, 열심히 할수록 교사나 부모에게 관심과 칭찬을 받기 때문에, 성적 성취도가 삶의 만족도에 많은 부분을 차지하는 것으로 분석됐다.[2]

이러한 문제의 원인은 공급자 편의위주의 교육시스템에서 발생되고 있음을 알 수 있다. 학생개인의 희망이나 적성과 별개로 중앙에서 계획된 집단교육 및 평가 시스템에서 문제를 발견할 수 있다. 교육의 본질적 목표보다는 생산성과 효율성을 중심에 두고 있다는 점이다. 기존의 교육시스템을 일거에 개선하는 데는 많은 제한요소가 있을 수 있다. 이에 현재의 교육시스템에 블록체인을 활용하여 이상적인 교육시스템 개선이 가능하도록 모델 연구를 하였다.

II. 관련 연구

1. 블록체인의 개요

블록체인은 2007년 나카모토 사토시가 글로벌 금융 위기사태를 목도한 후에 중앙집권화 된 금융시스템의 문제점을 해결할 수 있는 방안으로 개인거래가 가능한 블록체인 기술을 고안하면서 시작되었다.

블록체인의 완전한 영어 이름은 Blockchain Security Technology이며 블록과 체인의 합성어이다. [그림 1]과 같이 블록은 데이터를 담아 체인 형태로 연

결하여 네트워크 컴퓨터에 동시에 기록해서 저장하는 분산형 데이터 관리 기술이다. 공공 거래 원장이라고도 부른다. 중앙 서버에 거래 기록을 보관하지 않고 거래에 참여하는 모든 네트워크 사용자에게 원장을 보내 주며, 거래 때마다 네트워크 참여자들이 데이터를 공유하고 이를 대조해 데이터 위·변조를 할 수 없도록 되어 있다.[3]

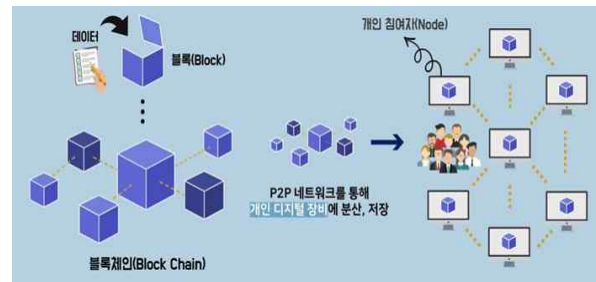


그림 1. 블록체인의 개념
Figure 1 Blockchain's Concept

2. 블록체인의 개요

블록체인의 주요특징은 분산성과 보안성이라고 할 수 있다. 분산된 데이터를 합의알고리즘에 의해 증명하여 데이터의 위변조가 불가능하도록 설계가 되어 있다. 다음 표는 블록체인의 주요특징이다.[3]

구 분	내 용
분산성	분산형 네트워크(P2P)환경 하에서 처리
투명성	거래 양성화 및 비용 절감
보안성	거래 장부를 네트워크 참여자 모두에게 공동 소유함으로써 데이터 위변조 방지
무결성	분산형 네트워크상 데이터 삭제나 파괴제한
익명성	데이터 소유자 임의로 확인 어려움

표 1. 블록체인의 특징
Table 1. Blockchain's Characteristics

3. 블록체인 구조

[그림 2]와 같이 블록은 데이터를 저장 단위로 헤더와 바디로 구분되고 헤더에는 머클해시(머클루트), nonce(Nonce)등의 암호코드가 담겨있다. 처음 시작되는 블록을 제네시스 블록이라고 하며 약 10분 주기로 생성된다. 블록검색 시 database index 방식으로 데이터 값을 찾는다.[4]

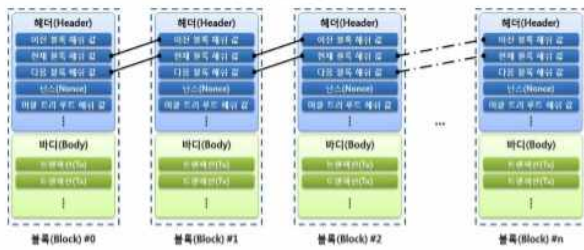


그림 2. 블록체인의 연결구조
 Figure 2. Blockchain's structure

4. 블록체인 구조

1) 디지털 서명과 해시함수

디지털 서명은 개인키(Private key)와 공개키(Public key)가 한 단위로 구성된다. 개인키는 공개키에 대한 패스워드 같은 것으로 개인키로부터 공개키를 알아낼 수 있지만 공개키로부터 개인키를 알아낼 수는 없다. 네트워크상에서 송신자는 ‘자신의 개인키로 암호화한 디지털 서명’과 ‘거래 내역’ 두 가지를 함께 수신자에게 보낸다. 수신자는 디지털 서명이 된 데이터를 송신자의 공개키로 복호화하고 함께 받은 처리내역과 비교하여 일치하는지를 확인함으로써 전송 과정에 데이터 위변조가 없는지를 검증한다.

거래 내역을 암호화하기 위하여 해시함수(Hash function)가 쓰인다. 해시함수는 암호화뿐 아니라 데이터보안 분야에서 널리 쓰이고 있으며 데이터를 정해진 길이의 무작위 문자열로 교환하는 함수다. 해시함수는 ‘SHA-256’으로 입력하는 자료의 내용과 관계없이 언제나 64자리의 16진법 문자열을 나타낸다. 동일한 문자열이 나오게 하는 입력 정보를 찾으려면 2,256개의 데이터를 하나하나 확인해야 한다. 2,256을 10진법으로 표시하면 1077 정도로 많은 숫자다. 해시 값으로 입력 정보를 찾는 것은 거의 불가능하다.[5]

2) 분산원장 기술

블록체인은 피어 간(Peer to Peer)에 완전한 공유 네트워크를 기반으로 한다. 피어(Peer)라는 의미는 네트워크에 참여하는 개인이 상호간에 동료이자 동등한 지위를 가지고 있어 모든 노드(node)가 네트워크 서비스를 공유하는 것을 의미한다. 인터넷상에서 통상적으로 이용되고 있는 서버-클라이언트 방식의 경우 메인 서버에 모든 원본 자료를 저장하는 반면, 블록체인의 분산원장 방식은 네트워크 참여자들이 모두 원장을 공유하고 보관한다. 블록체인으로 생성된 데이터는 디지털 서명과 해시함수

를 통해 보관되며 단독 중앙 서버가 아닌 네트워크 참여자의 각 서버에 분산되어 복제, 저장되므로 사실상 위변조가 불가능하다.[6]

5. 블록체인 활용한 교육시스템 사례

블록체인을 활용한 본격적인 교육시스템은 아직 뚜렷하게 개발되어 있지 않지만 단순한 학위나 성적인증에서 벗어나고자 하는 시도는 활발하게 나타나고 있다. 대표적인 예로 MIT가 민간업체와 공동개발한 ‘Blockcerts’를 들 수 있다. 또한 여러 교육기관에서는 단순학위 인증에서 확장된 교육시스템을 생각하고 있다. 그 예로 ‘Open University UK’ (이하 ‘OU’)가 있다. John Domingue 교수는 블록체인을 기존 교육 시스템을 대체하는 것을 넘어서 새로운 의미의 교육 체계가 만들어질 것이라고 예견하고 있다.

III. 블록체인을 활용한 기본 시스템

본 시스템의 구성은 [그림 3]과 같이 A. Solidity 코드, B. Ethereum 클라이언트, C. 블록체인 네트워크로 구성되어 있으며 시스템 관리자는 E. 콘솔을 사용하여 명령을 조작하며 학교 등 공급자와 학생 등 수요자는 D. 웹 브라우저를 통해 과제기능을 사용하게 된다. [7]

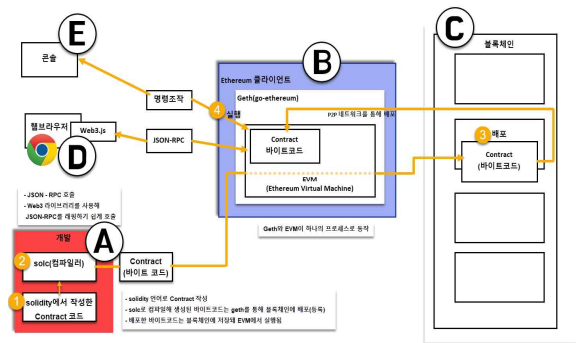


그림 3. 교육관계자 시스템 구성도
 Figure 3. Educational personnel's system schematic diagram

1. 개발 부분

개발은 Solidity언어로 진행했으며 이때 최종적으로 생성되는 것은 교육스마트 컨트랙트이므로 수강, 확인 등의 교육에 필요한 기능을 코드로 작성한 뒤에 solc 컴파일러로 컴파일하여 바이트 코드로 변환한 뒤에 Ethereum 블록체인 네트워크에 배포해야 사용이 가능하다. 때문에 본 시스템에서도 코드를 작성한 후에는

컴파일과정이 이루어져 바이트 코드를 직접 Ethereum 블록체인 네트워크에 배포한다.

2. Ethereum 클라이언트

시스템에서 사용된 Ethereum 클라이언트로 개발한 스마트 컨트랙트를 배포해주고 사용할 수 있게 한다. 우리는 이 클라이언트를 사용해 블록체인 네트워크를 구축하고 스마트 컨트랙트를 사용할 수 있게 유저 인터페이스를 웹 페이지 형식으로 제작하였다.

3. 블록체인 네트워크

시스템에서 가장 핵심이 되는 부분으로 기존 교육시스템에서는 보장해주지 못했던 보안성과 무결성 문제를 해결한다. 우리는 공개와 사설 네트워크 중 사설 블록체인 네트워크를 구축하여 이후 신뢰 가능한 기업 또는 공기업 등의 참여가 가능하도록 하였다.

4. 유저 인터페이스

유저 인터페이스는 웹페이지 형식으로 만들어서 사용하도록 했다. 이때 JSON-RPC 와 Web3.js를 사용하여 관리 및 확인 등의 기능들이 올바르게 작동되도록 코드를 작성하였다.

5. 콘솔

콘솔에서도 마찬가지로 기능을 수행할 수 있지만 주로 계정을 추가하거나 트랜잭션의 상태를 확인하는 용도로 사용하였다. 계정 추가의 경우에 일일이 한 계정 한 계정 입력을 하며 생성을 해줘야 하는 비효율적인 문제가 있어 자동으로 계정을 만들도록 하는 코드를 작성하여 추가했다.

IV. 교육 통합모델 구성 제안

1. 교육 통합모델

지금까지의 교육시스템은 공급자 위주의 교육이었다고 하면 통합시스템에서는 [그림 4]와 같이 학생 중심의 시스템이라고 할 수 있다. 성적이나 학업성취는 본인의 선택이나 승인에 의해서 교환, 확인할 수 있으며 데이터는 블록체인에 의해 관리되어진다.

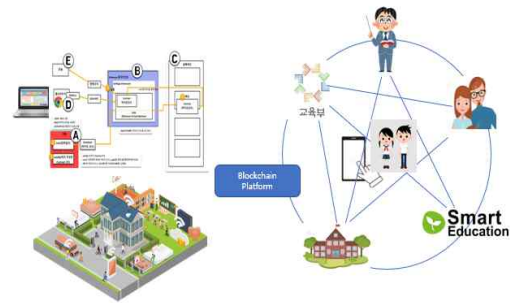


그림 4. 교육 통합모델

Figure 4. Integrated System Concept Model

시스템은 학교, 학생, 교수, 학부모, 외부기관 등이 기존에는 학교의 중앙서버에 의해 기록 및 관리된 것을 각 계정을 부여하여 분산네트워크에 저장하도록 변경하였다. 이더리움기반의 스마트컨트랙트를 활용하여 학생은 각종 평가, 봉사활동, 실습, 발표, 작품제출 등을 디지털 신원에 의해 확인되어 평가받고 평가자는 학생의 신원을 직접확인할 수 없도록 하였다.

2. 계정부여 설계 및 코드

```

<wallet.html>
<!Doctype html>
<html>
<head>
<meta charset="UTF-8">
<script type="text/javascript"
src="/lib/bignumber.min.js"></script>
<script type="text/javascript"
src="/lib/web3-light.js"></script>
<script type="text/javascript">
    var Web3 = require('web3');
    var web3 = new Web3();
    //개설한 네트워크 ip와 포트번호를 입력
    web3.setProvider(new
web3.providers.HttpProvider("http://10.30.91.125:8
545"));
    // 잔고를 출력한다.
    function refreshBalance() {
        // tablePlace를 초기화하고 계정수 만큼
테이블의 행을 생성한다.
document.getElementById("tablePlace").innerText
= " ";
        var idiv = document.createElement('div');
document.getElementById("tablePlace").appendChi
    
```

```

ld(idiv);
    var list = web3.eth.accounts;
    var total = 0;
    var input = "<table>";
    for(var i = 0; i<list.length; i++){
        var tempB=
parseFloat(web3.fromWei(
web3.eth.getBalance(list[i],"ether"));
        input += "<tr><td>" + list[i] +
"</td><td>"
        + tempB + " ETHER</td></tr>";
        total+=tempB;
    }
    input += "<tr><td><strong> TOTAL
</strong></td><td><strong>" +
total+"ETHER</strong></td></tr></table>";
    idiv.innerHTML = input;
web3.eth.filter('latest').watch(function() {
refreshBalance();});
    }
    
```

현재 생성되어있는 사용자 계정 상태를 테이블 형식으로 보여주어 현재 상태를 확인하며 학생 등의 계정을 추가할 수 있게 한다.

```

<wallet.html>
//사용자 계정을 생성한다. 여기서 비밀 키
는 "123"으로 지정했다.
function makeWallet(n){
    for(var i=0;i<n;++i){
web3.personal.newAccount("123");
    }
}
    
```

이후에 입력받은 수만큼 계정 생성을 진행한다. 이때 기본적으로 "123"을 비밀 키로 지정하여 빠르게 천개 이상의 계정을 생성했다.

사용자 계정 생성 시 콘솔명령을 사용할 수 있지만, 테스트 시뮬레이션을 위해서 천개이상의 계좌를 생성하기에는 무리가 있다. 때문에 html을 작성하고 json-rpc를 사용하여 동시에 n개 단위로 계정을 생성하는 코드를 작성하여 사용했다.

3. 온라인시험 스마트컨트랙트 설계

```

<Test.sol>
pragma solidity ^0.4.11;
contract On-line {
    
```

```

        mapping (address=>bool) isTested; //1번의 시험
        선택 가능하게 매핑한다.
        mapping (string=>uint) studentObtained; // 점
        수를 매핑한다.
        mapping (uint8 => string) Lectures;//강의 리스트
        매핑한다.
        string private testName; // 해당 학과학년의 이름
        (ex IT융합과, 경영학과 등)
        address private contractAdmin; //해당 컨트랙트의
        관리자
        uint8 private numberOftests; //시험 수
        uint private endTime; //마감시간
        ////////////////////////////////// method
        //생성자
        constructor (string eleName_,uint endDday_)
        public {
            contractAdmin = msg.sender; //생성한 사람이 컨트
            랙트의 소유자가 된다.
            electionName = testName_; // 시험명. (ex
            2018년1학기 IT학과 중간고사 등)
            numberOfTests = 0; //시험의 수는 처음에
            0으로 초기화
            endTime = now + (endDday_ * 1 days); //
            시험 마감 기간 결정
        }
    
```

생성자 부분인 constructor 부분에서는 해당 컨트랙트를 생성을 호출하는 시험 관리위원회가 컨트랙트의 소유자로 지정하고 이후 시험 관리위원회는 시험추가, 시험마감 등 관리자만이 수행할 수 있는 기능을 사용하게 된다.

```

<Test.sol>
////////////////////////////////////// modifier
modifier onlyAdmin() { // 시험관리위원회만 접근
가능한 조건을 줄 때 사용
    require(msg.sender==contractAdmin);
    ;
}
modifier notTimeOver() { // 마감기간 이전의
조건을 줄 때 사용
    require(now < endTime);
    ;
}
    
```

Solidity에서 제공하는 modifier 기능을 사용하여 onlyAdmin() 이라는 modifier를 정의하여 보안상 오직 관리자만 실행해야할 메서드의 경우에는 해당 modifier

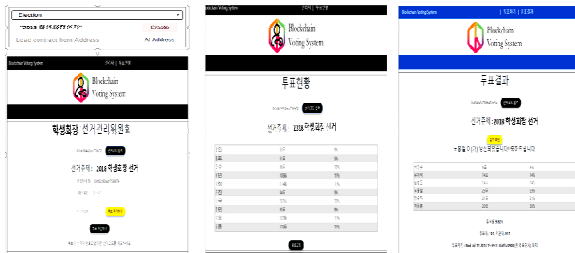
를 함께 사용했다. 추가적으로 notTimeOver()라는 modifier는 마감기한 이전의 조건일 때만 매서드가 수행되도록 해야 하는 함수에 적용하여 사용했다.[8]~[11]

4. 교육 통합모델 결과

교육 통합모델의 일부인 학생회장 선거관리를 위한 시스템을 이용한 화면은 [그림 5]와 같다.

그림 5. 학생회장선거 화면

Figure 5. the student body president election screen



블록체인을 이용한 이력관리(출결, 성적, 수업참여도, 봉사활동 등)는 접근성이 좋고, 비용이 절감되며, 학생이 데이터를 소유하게 되어 학생중심의 교육시스템이 가능하다. 또한 논란이 되는 각종 증명서 등은 비용 없이 발급, 인정 등이 가능하여 비용적인 측면에서도 효과를 볼 수 있다.

V. 결론

본 논문에서는 블록체인을 활용한 교육시스템 통합 모델을 제안하였다. 이러한 시스템은 '선택의 문제가 아니라 어떻게 활용할 것인가'에 대한 방법의 문제이다. 즉 패러다임의 변화를 예고하고 있다. 논문에서는 광범위한 통합시스템 모델을 제안하고 있지만 기술발전과 더불어 개선된 블록체인 캠퍼스 프로젝트가 여러 곳에서 시도되고 있다. 블록체인 교육 통합시스템을 통하여 교수는 학생에게 필요한 교육과정을 개설하고, 학생은 선택해서 배우고 상호 평가하고 검증받아 신뢰된 데이터를 바탕으로 맞춤형 교육을 진행할 수 있게 될 것이다. 그렇게 된다면 현재의 집단성적위주의 평가에서 벗어나 학생위주의 교육본연의 가치를 제고할 것으로 기대한다.

References

- [1] "the present state of Korean students whose grades and satisfaction with life are inversely proportional." Korea Education Newspaper. last modified n.d., accessed Nov 10, 2018, <http://www.hangyo.com/news/article.html?no=80825>.
- [2] Dae-Koo Kang, Byung-Hwan Lee. "A Study of School Maladjustment Action Factors in Secondary School Students." Journal of Education & Culture, 20(3), 125-148. 2014.
- [3] "NAVER, Knowledge Encyclopedia ." NAVER. last modified n.d., accessed NOV 11, 2018. <https://terms.naver.com/entry.nhn?docId=2838482&cid=43667&categoryId=43667>.
- [4] Security Technology Team, BlockChain and Bitcoin Security Technology. n.p.: Financial security, 2015.
- [5] Yeol-Mae Kim, BlockChain and Digital Economy. n.p.: Eugene Investment & Securities, 2017.
- [6] Investment analysis team, Block Chain Technology and Bitcoin Outlook. n.p.: Hanwha Investment & Securities, 2017.
- [7] Kyoung-Sung Yu, "On-line Auction System Using Blockchain"(2018). Hnasei Uiv, n.p..
- [8] Seung-Jung Shin, "Development of Life Management System for Elderly and People with Disabilities." 14, no. 1 (2014): 275 - 79. doi:10.7236/JIIBC.2014.14.1.275.
- [9] Seung-Jung Shin, Kyoung-Seung Jang, and Jin-kwan Jung, "A Study on Recognition for Quality Importance of Cloud Services ." The journal of the Institute of Internet Broadcasting and Communication 15, no. 2 (2015): 39 - 44. doi:10.7236/JIIBC.2015.15.2.39.
- [10] IJin-mo Im, Weol-Youg Kim, Byoun, Woo-Jin Byoun, Seung-Jung Shin, "Fruit price prediction study using artificial intelligence.", Journal of the convergence on culture technology v.4 no.2(, 2018)197-204. <https://doi.org/10.17703/JCCT.2018.4.2.197>.
- [11] Weol-Youg Kim, Seung-Jung Shin, "Large orchard apple classification system", Journal of the convergence on culture technology vol. 4. No4.(2018);393-399. <http://dx.doi.org/10.17703/JCC T.2018.4.4.393>.