한국사물인터넷학회논문지 Vol. 4, No. 2, pp. 13-20, 2018 https://doi.org/10.20465/KIOTS.2018.4.2.013

# 블록체인을 활용한 Single Sign-On 기반 인증 시스템

임지혁, 이명하, 이형우*
한신대학교 컴퓨터공학부

# Single Sign-On based Authentication System combined with Blockchain

**Im Jihyeok, Lee Myeongha, Hyung-Woo Lee***
**Division of Computer Engineering, Hanshin University**

**요 약** 본 논문은 최근 대두된 신기술인 '블록체인' 기술을 기반으로 'Single-Sign-On'과 'Token 기반 인증 방식'을 접목한 인증 시스템을 제안하였다. Single-Sign-On 기반 인증 방식에 블록체인 기술을 접목하여 '접근제어' 기능과 '무결성'을 제공하였으며, Token 기반 인증 방식을 사용하여 Stateless한 Self-Contained 인증 기능을 제공하였다. 암호화 기반 Token 발급 및 인증 과정을 수행하여 보안성을 높일 수 있었으며, Web Server에 대한 인증 편리성을 제공하였다. 또한 SSO과 Token 기반 인증을 통해 번거로운 인증 과정을 보다 편리하게 개선할 수 있는 방법을 제시하였다.

**주제어 :** 블록체인, SSO, 인증, 보안시스템, 정보보호.

**Abstract** In this paper, we propose an authentication system that combines 'Single-Sign-On' and 'Token-based authentication' based on 'Block Chain' technology. We provide 'access control' function and 'integrity' by combining block-chain technology with single-sign-on authentication method and provided stateless self-contained authentication function using Token based authentication method. It was able to enhance the security by performing the encryption based Token issuance and authentication process and provided convenience of authentication to Web Server. As a result, we can provide token-based SSO authentication service efficiently by providing a convenient way to improve the cumbersome authentication process.

**Key Words :** Blockchain, Single Sign On, Authentication, Security System, Information Security.

## 1. 서론

블록체인[1, 2]은 2017년 말에 암호화폐의 상승장부터 크게 대두되고 있으며, 4차 산업 혁명의 정보통신 기술에 있어서 신뢰성과 효율성을 제공할 새로운 기술로 관심받고 있다.

기존 사회 인프라는 대부분 중앙집권적인 특징을 갖고 있어 관리 비용이 많이 들고 해킹에 취약하다. 블록체인은 탈중앙화가 된 네트워크에 기반한 분산 원장으로 보안성과 투명성을 특징으로 하며, 분산 시스템이 갖추어야 할 요건인 신뢰성, 가용성, 분리 내구성을 모두 만족하는 기술이다[3, 4].

Single-Sign-On(이하 SSO)[5, 6]은 한 번의 인증 과정으로 여러 컴퓨터의 자원을 이용 가능하게 하는 인증 기능이다. SSO은 여러 응용 프로그램의 로그인 처리가 간소화되어 편리성을 도모할 수 있는 반면, 통합인증의

*교신저자 : 이형우(hyungwoo8299@gmail.com)
접수일 2018년 07월 15일 수정일 2018년 08월 25일 심사완료일 2018년 09월 10일

시작점이 되는, 즉 최초의 로그인 대상이 되는 응용 프로그램 혹은, 운영체제에 대한 접근 보안이 중요하게 된다. 보안위험이 적은 환경에서는 편리성만을 추구하면 되지만, 보안이 요구되는 환경에서는 1회용 비밀번호를 이용하는 등, 이중 인증 등으로 보안을 강화할 필요가 있다.

본 논문에서는 이와 같은 블록체인의 특장점들을 이용해서 SSO의 부족한 보안성을 보완하는 한편, Token 기반 인증 방식을 접목시켜서 보다 간단한 탈중앙화 된 새로운 인증 시스템을 제시한다. 이와 같은 연구의 '목적'은 새로운 기술을 접목한 시스템을 개발하고, 서로의 단점을 보완해줄 기술들을 통합하여 보다 완전한 시스템을 개발함에 있으며, 기업들이 자체적으로 사용하는 기존의 상용 인증 시스템과의 차별적으로 신기술들을 기반으로 개념·이론만으로 연구하여 하나의 온전한 시스템을 개발함에 있다.

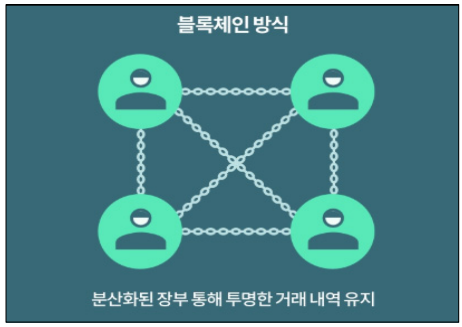
본 논문에 사용된 프로그램은 간단한 인증 시스템 구현을 위해 사용되어 등록, 토큰 발급, 로그인을 통해서 Token 기반 인증 시스템을 적용한 SSO 시스템의 특징들을 보여준다.

본 논문의 구성은 2장에서부터 관련 기술 서술, 3장에서 시스템 설계에 대한 설명과 4장에서 개발 환경에 대한 설명과 5장에서 프로그램 구현 및 인터페이스와 작동 순서에 대해 설명하고, 6장에서 마지막으로 본 논문의 결론을 제시한다.

## 2. 관련 기술

### 2.1 블록체인

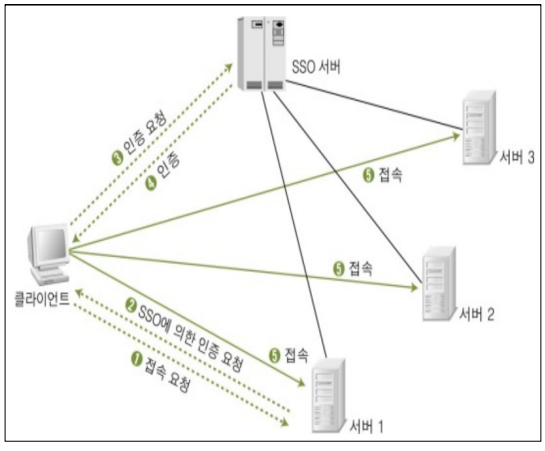
블록체인은 데이터 분산 처리 기술이다. 즉, 네트워크에 참여하는 모든 사용자가 모든 거래 내역 등의 데이터를 분산, 저장하는 기술을 지칭하는 말이다. 블록들은 형성된 후 시간의 흐름에 따라 순차적으로 연결된 체인 구조를 가지게 된다. 모든 사용자가 거래 내역을 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인해야한다. 이 때문에 블록체인은 공공 거래장부 또는 분산 거래장부로 불리기도 한다[7].




[Fig. 2.2.1] Block Chain Trading Method

### 2.2 Single-Sign-On

Single-Sign-On(이하 SSO)은 가장 기본적인 인증 시스템으로, 시스템이 몇 대가 되어도 하나의 시스템에서 인증에 성공하면 다른 시스템에 대한 접근 권한도 모두 얻는 것이다. 기본 원리는 처음에 클라이언트가 서버에 연결을 요청하면, 서버는 클라이언트로 하여금 SSO 서버로부터 인증을 받은 후 접속을 요청한다. 클라이언트가 SSO 서버로부터 인증을 받으면 SSO 서버와 연결된 나머지 서버들에도 별도의 인증이 필요 없이 인증 된 사용자의 권한을 가지고 접근할 수 있다[8].



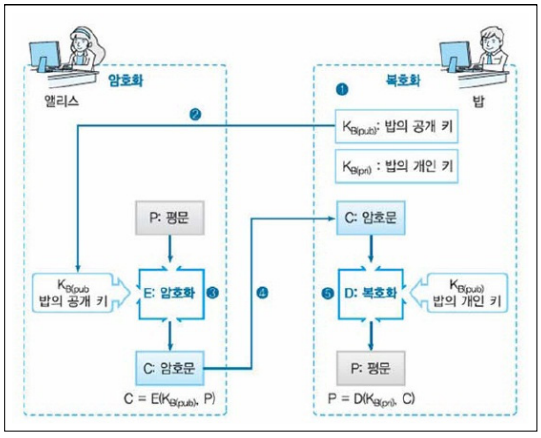

[Fig. 2.2.2] Single-Sign-On based Authentication

### 2.3 RSA Algorithm

공개키 알고리즘은 암호화하는 키(공개키)와 복호화하는 키(개인키)가 동일하지 않도록 고안된 방식이다. 공개키 알고리즘을 이용하면, 공개키가 외부에 공개되어도 개인키를 모르면 암호문을 해독할 수 없다.

공개키(Public Key)는 송신자가 원문서를 암호화하는

데 사용하므로 원칙적으로 누구에게나 공개된다. 수신자는 암호문을 해독하기 위해 개인키(Private Key)를 사용한다. 개인키는 타인에게 노출되면 안 되지만, 공개키는 도청자가 봐도 괜찮다. 보내지는 암호문은 도청자가 봐도 괜찮다. 이유는 도청자는 송신자의 공개키는 해킹할 수 있지만, 송신자의 공개키로 복호화할 수 없기 때문이다.




[Fig. 2.3.1] RSA Algorithm

## 3. 시스템 설계

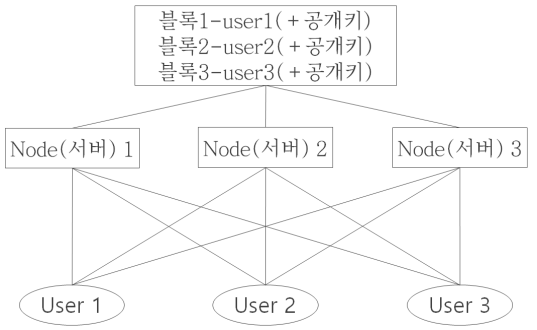
### 3.1 시스템 구조도

그림 [3.1.1]은 본 논문의 시스템 구조도이다. 해당 시스템은 다음과 같이 동작한다.

각 서버(노드)들은 분산 네트워크(블록체인)에 참여한다. 체인으로 연결된 블록(원장)은 참여된 노드들에 분산 저장되며, 각 노드들은 합의 알고리즘을 통해서 이를 유지/관리한다.

노드들의 서비스를 이용하려는 유저는 블록체인에 참여된 어느 한 노드에서 자신의 정보를 바탕으로 등록을 해도 이는 블록체인의 합의 알고리즘에 의해서 참여된 모든 노드들은 동일한 원장을 가지게 된다.

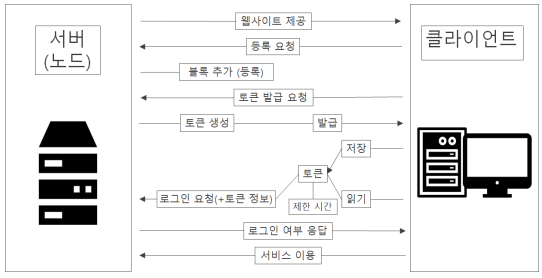
유저는 서비스를 이용할 노드에서 인증을 통해서 토큰을 발급받는다. 후에 발급된 토큰을 저장한 유저는 이를 통해서 분산 네트워크에 참여된 어떠한 노드에서든지 일정 시간(제한 시간)동안 별도의 인증 없이 서비스를 이용 가능하다.




[Fig. 3.1.1] System structure diagram

### 3.2 시스템 작동 순서

본 논문의 시스템의 작동 순서는 다음과 같이 작동한다. 가장 먼저 서버는 기본적으로 클라이언트에게 웹 사이트를 제공한다. 서버에 등록을 원하는 클라이언트가 서버에 자신의 개인정보의 등록을 요청하면 서버는 클라이언트에게 받은 정보를 바탕으로 새 블록을 추가한다. 이후 서비스에 접근을 원하는 클라이언트가 서버에 토큰의 발급을 요청하면 서버는 토큰을 생성하여 클라이언트에게 발급한다. 클라이언트는 발급받은 토큰 정보를 기반으로 제한 시간 내에 서버에 로그인을 요청하면 서버는 토큰을 검증하여 로그인을 허용하고 클라이언트는 서비스를 이용한다. 순서에 따른 세부적인 요소들은 다음 챕터인 4챕터에서 하도록 한다.




[Fig. 3.1.2] System operation sequence

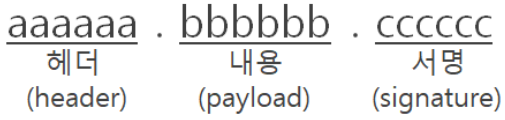
## 4. 개발환경

활용한 Blockchain Open-source[9]가 Python 기반이라 Python을 Base로 개발했다. Python은 Interpreter 언어로 다양한 라이브러리 사용과 간결한 코드 작성이 가능하다[10]. Flask는 Python의 웹 개발 프레임워크 중 하

나로, 타 프레임워크에 비해 가볍고 간단하게 사용이 가능하다. Node들의 Server 구현에 사용됐다. 해당 프로젝트의 Client는 이로 제작된 Web- Server와 상호작용한다[11, 12]. Flask로 제작된 Web-Server의 HTTP 통신을 위한 HTML Template 제작에 사용됐다[13]. 또한,—Pycryptodome를 이용하여, 암/복호화를 위해 사용한 라이브러리, 해당 프로젝트에는 RSA 공개키/개인키 알고리즘이 사용됐다[14]. Key:Value 쌍으로 데이터를 표현하며 Blockchain의 Ledger를 JSON을 사용하여 표현했다.


[Fig. 4.5.1] Ledger implemented with JSON

토큰 기반 인증 방식을 사용하기 위해 JWT를 채택했고 Json Web Token의 약자로 다음과 같은 구조를 가지고 있다[15, 16].



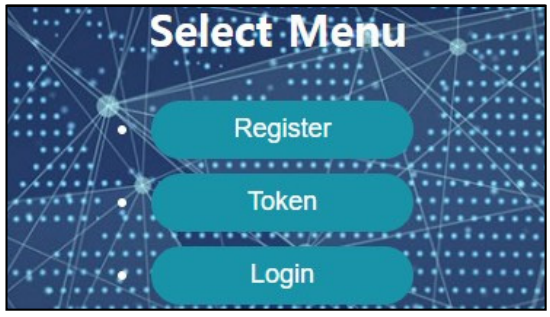

[Fig. 4.6.1] JWT structure

해당 프로젝트에서 Web의 GET/ POST Request를 위해 Postman 프로그램을 사용하였다. 운영체제는 windows10을 사용했다. 그 외에 필요한 라이브러리로는 time, datetime, uuid, wrap, urlparse, random, request, hashlib 등이 있다.

## 5. 시스템 작동 시나리오 및 인터페이스

### 5.1 메인 메뉴

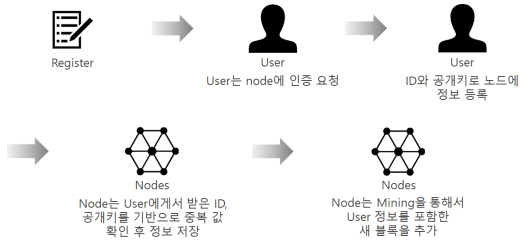
메인 메뉴인 Select Menu에서 Register, Token, Login을 선택하여 다음의 과정들을 진행한다.




[Fig. 5.1.1] Main Menu

### 5.2 Register

Register는 [그림 5.2.2]와 같이 메인메뉴에서 'Register' 버튼을 클릭해서 시작되며, User가 [그림 5.2.3]과 같이 ID와 공개키로 Node에 정보를 등록을 요청한다. 이에 따라서 Node는 User에게 받은 ID와 공개키를 기반으로 중복 값을 블록체인에서 확인한 후에, (해당 정보가 블록체인에 없으면) 정보를 저장하고 Mining을 통해서 User의 정보를 포함한 새 블록을 블록체인에 추가하고 완료 메시지를 [그림 5.2.4]와 같이 User에게 보여준다.




[Fig. 5.2.1] Register scenario

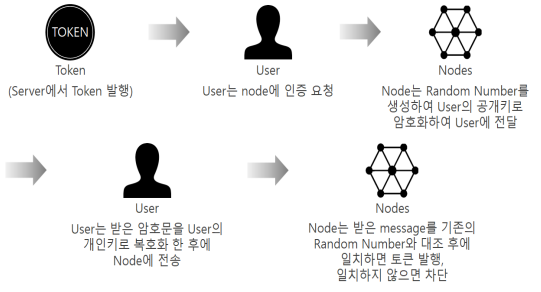

[Fig. 5.2.2] Select Register from Select Menu


[Fig. 5.2.3] Request information after request

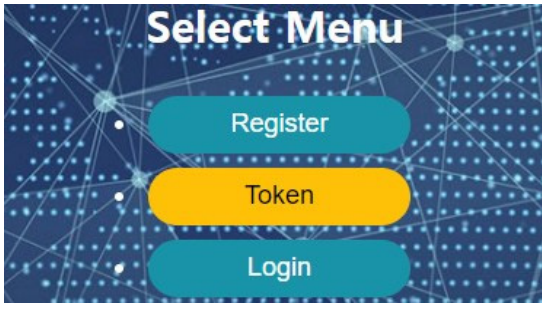

[Fig. 5.2.4] Output message when successful completion

## 5.3 Issuing Token

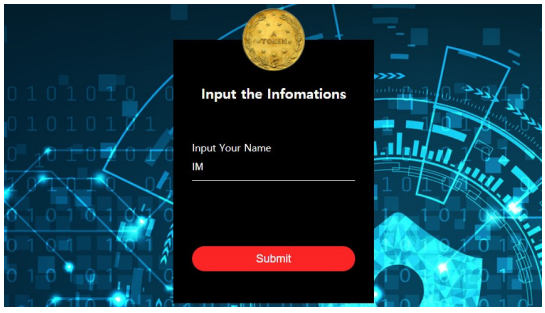
Token 발급은 [그림 5.3.2]와 같이 메인메뉴에서 'Token' 버튼을 클릭해서 시작되며, [그림 5.3.3]과 같이 User가 자신의 ID로 Node에 Token 발급을 요청하면, Node는 Random Number를 생성하여 User의 공개키로 암호화하여 [그림 5.3.4]처럼 User에 전달한다. User는 받은 암호문을 User의 개인키로 복호화 한 후에 Node에 전송하고 Node는 받은 message를 기존의 Random Number와 대조 후에 일치하면 [그림 5.3.5]처럼 Token을 발행하고, 일치하지 않으면 Fail Message를 보낸다.



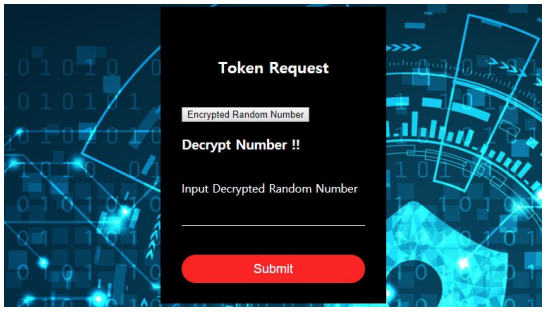

[Fig. 5.3.1] Token creation scenario



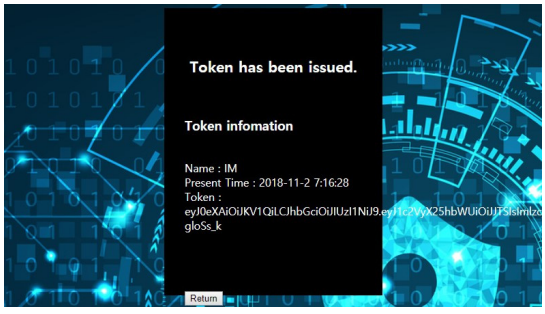

[Fig. 5.3.2] Select Token from Select Menu




[Fig. 5.3.3] Request by User's ID



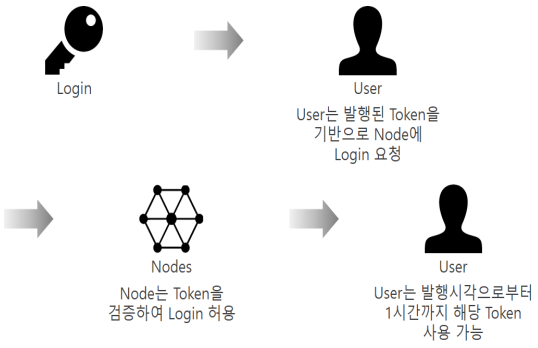

[Fig. 5.3.4] Node generates and encrypts a random number and requests decryption from User




[Fig. 5.3.5] Pass Token information to User when random number is matched

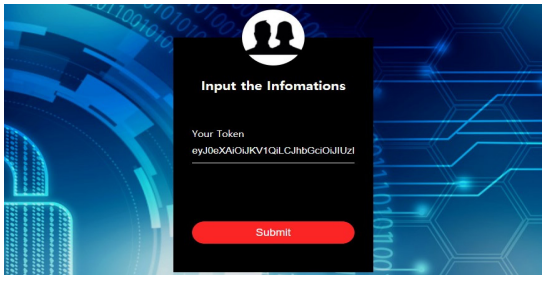
### 5.4 로그인

Login은 [그림 5.4.2]와 같이 메인메뉴에서 'Login' 버튼을 클릭해서 시작되며, [그림 5.4.3]과 같이 User가 (앞서 [5.3]에서 발행된) Token을 기반으로 Node에 Login을 요청하면 [그림 5.4.4]처럼 Node는 Token을 검증하여 Login을 허용한다. 이후 User는 'Public Home'과 'Private Home'을 선택할 수 있으며, 전자는 [그림 5.4.5]와 같이 별도의 User 권한이 필요 없이 누구나 접근 가능한 Page고, 후자는 [그림 5.4.6]과 같이 Token을 통한 Login된 User의 권한으로만 접근 가능한 Page이다. User는 Token 발행 시각으로부터 1시간 후까지 해당 Token을 Login에 사용할 수 있다.



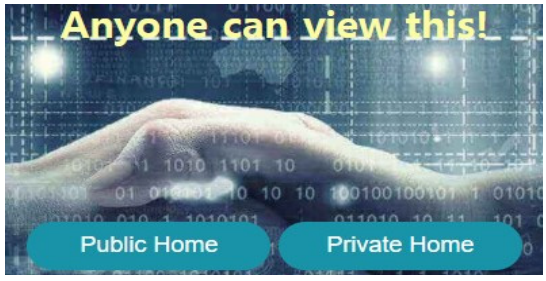

[Fig. 5.4.1] Login scenario


[Fig. 5.4.2] Select Login from Select Menu




[Fig. 5.4.3] Login request with Token information


[Fig. 5.4.4] Pass validation success message




[Fig. 5.4.5] Public site access without permission when clicking Public Home


[Fig. 5.4.6] Accessing sites that require User privileges when clicking Private Home

## 6. 결론

IT 기술은 날이 갈수록 새로운 기술들이 나타난다. 블록체인은 크게 이슈 되고부터 많은 기업들이 이를 활용하여 다양한 방식의 시스템을 개발했다. 인증 시스템에 관련해서는 당해 초기에부터 대기업, 금융권 위주로 자체적으로 인증 시스템을 도입해나갔다. 다음은 그에 따른 블록체인 시장을 주도하고 있는 대표적인 상용 시스템과 본 논문의 연구의 비교·분석이다.

이와 같은 상용 서비스들은 상용화 된지 얼마 되지 않았고, 시스템이 외적으로 보이는 게 없고 내부적인 것은

비공개라 비교함에 있어 장애가 있다. 그러나 대체적으로 각 기업의 공식 사이트를 통한 솔루션에 대한 설명으로 미루어봤을 때, 해당 시스템들은 기존 SSO 솔루션을 개발한 기업에서 새롭게 블록체인 기술을 접목시킨 것으로, 이미 그 효용성에 대해서는 인증 된 시스템이다. 따라서 본 논문에서 연구한 시스템은 일반적인 SSO Server를 통한 상용 인증 방식과는 달리, Token 기반 인증 시스템을 접목시켜 Stateless한 Self- Contained적인 인증 시스템을 연구·개발하였다. 이는 위와 같은 상용 시스템과는 질적으로는 차이가 있겠으나 해당 기술들에 대한 개념·이론만을 기반으로 추가적인 기술을 접목시켜 온전한 시스템을 연구·개발한 것에 있어서 의의가 있다.

〈Table 6.1〉 Commercial Systems Analysis

| Corporation | Solution name | Characteristics |
|---|---|---|
| Company C | Integrated authentication platform using blockchain | Applying the patent technology for blockchain-based personal certificate |
| Company I | KT Integrated Authentication Solution | Combine blockchain technology from partner (K) and their certification solutions |
| Company I | Blockchain Integrated Authentication Service | Increase efficiency with our integrated development support platform |
| this paper study | SSO Certification System Utilizing Block Chain | Static self-contained authentication is possible by introducing Token-based authentication method into blockchain SSO |

## REFERENCES


[1] Blockchain Web site: https://www.blockchain.com

[2] Blockchain, WIKIPEDIA, Accessed on Nov. 23, 2018. [Online] Available: https://en.wikipedia.org/wiki/Blockchain

[3] HYPERLEDGER FABRIC, Accessed on Nov. 23, 2018. [Online] Available: https://hyperledger-fabric.readthedocs.io/en/release-1.3/

[4] A look at blockchain technology, https://www.columnfivemedia.com/best-100-technology-infographics/technology-infographics-3

[5] Wikipedia, “Single Sign On”, https://en.wikipedia.org/wiki/Single_sign-on, [May. 13, 2018]

[6] Wikipedia, “Single Sign On”, https://ko.wikipedia.org/wiki/%ED%86%B5%ED%95%A9_%EC%9D%B8%EC%A6%9D, [May. 13, 2018]

[7] Wikipedia, https://en.wikipedia.org/wiki/Blockchain [Apr. 10, 2018]

[8] Wikipedia, https://en.wikipedia.org/wiki/Single_sign-on, [May. 13, 2018]

[9] Hackernoon, “Blockchain”, https://hackernoon.com/learn-blockchains-by-building-one-117428612f46, [Jun. 09, 2018]

[10] Eungyong Park, “Do it! Jump to Python,” Easy’s Publishing, 2016.

[11] frhyme.code, “Flask”, https://frhyme.github.io, [Jun. 28, 2018]

[12] Youtube, “Flask Send File”, https://www.youtube.com/user/sentdex, [Sep. 13, 2018]

[13] K.H.Ko, “Do it! HTML5+CSS3 Web standards”, esaypublishing, 2017.

[14] Hirosi Yuki, “Introduction to Information Security,” Infinity Books, 2012.

[15] Velopert.Log, “JWT”, https://velopert.com, [Oct. 02, 2018]

[16] Youtube, “Flask JWT”, https://www.youtube.com/channel/UC-QDfvrRIDB6F0bIO4I4HkQ, [Oct. 02, 2018]

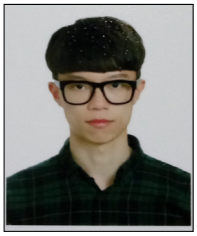


임 지 혁(Jihyeok Im) [학생회원]

▪ 1993년 7월 14일
▪ 2012년 서원고등학교 졸업
▪ 2019년 한신대학교 컴퓨터공학부 졸업 예정

<관심분야>
사물인터넷, 정보통신

이 명 하(Myeongha Lee) [학생회원]



- 1994년 6월 22일
- 2013년 성보고등학교 졸업
- 2019년 한신대학교
  컴퓨터공학부 졸업 예정

<관심분야>
사물인터넷, 정보통신

이 형 우(Hyung-Woo Lee) [종신회원]

- 1994년 2월 : 고려대학교 컴퓨터 학과 (학사)
- 1996년 2월 : 고려대학교 컴퓨터 학과 (석사)
- 1999년 2월 : 고려대학교 컴퓨터 학과 (박사)
- 2003년 3월 ~ 현재 : 한신대학교 컴퓨터공학부 교수

<관심분야>
사물인터넷, 정보보호, 모바일 보안 및 디지털 포렌식