Web 3.0 서버 환경에서 이더리움 거래 시스템 구현

임정수[1], 최민[2] [1)]
1충북대학교 정보통신공학과 석사과정
2충북대학교 정보통신공학과 교수
jeongsuim187@google.com, mchol@chungbuk.ac.kr

Implementation of Ethereum Transaction Systems in Web 3.0 Server Environment

jeong-su im[1], Min chol[2]
[1]Dept. of information and communication enginerring, chung-buk University
[2]Dept. of Computer Engineering, chung-buk University

요 약

본 연구는 web3.0(웹3.0) 서버 환경에서 이더리움 시스템을 구현하려는 것에 목적이 있다. 이더리움 거래 시스템을 만들기 위해 서버 시스템은 web3.0(웹3.0)과 node.js를 사용하였으며, 알케미를 사용하여 기존의 서버 기능을 구현하였다. 또한, 이더리움 실제 거래를 구현하기 위해 메타마스크를 사용하였으며, 이더리움 거래한 데이터를 보기 위해 이더스캔을 사용하였다. 이더리움 거래는 가스를 이용하여 거래의 승인을 하며, 매수자와 매도자는 ERC-20으로 만들어진 토큰을 거래하여 서로의 거래가 성사된다. 그리고 매수자와 매도자의 데이터를 삽입하여 그 정보를 토대로 거래할 수 있게 하였고,. 본 연구에서는 부동산 거래정보를 반응형 웹에 넣어서 그 정보에 의하여 서로 거래가 이루어 질 수 있도록 하였다.

1. 서론

블록체인, 인공지능 등 첨단 기술을 중심으로 한 4차 산업혁명 시대가 본격화됨에 따라 관련 기술의 생태계 확장을 위한 관심이 높아지고 있다. 따라서 기존 기술에서는 구현이 불가했던 거래 시스템을 구현할 수 있다. Web 3.0(웹3.0)은 인공지능과 블록체인을 기반으로 맞춤형 정보를 제공하고 데이터 소유를 개인화하는 3세대 인터넷이며, 블록체인을 기반으로 보안을 강화할 수 있는 기술이다. web3.0(웹3.0)을 이용하여 블록체인 거래 시스템을 만들 수 있으며 이는 부동산, 은행 등 많은 분야에서 핵심 기술로 거론된다.

본 연구에서 web3.0(웹3.0)의 구현은 node.js를 활용한 npm 실행으로 구현하였다. 아울러 데이터 보안 및 암호화가 중요해 짐에 따라 거래 데이터의 실질적인 운영을 위한 연구가 활발히 진행되었다. 기존의 이더리움 거래는 토큰을 이용하지 않고 이더리움 화폐에서 가스만 서로 교환하는 것으로 진행되었는데, 본 연구에서는 이더리움 화폐거래를 승인하는데 사용하고, 토큰을 활용하여 서로 거래를 하는 것으로 하였다. 그리고 네트워크는 테스트넷을 사용하여 미리 보안 관련성 및 데이터를 테스트 할 수 있게 하였다.

1) This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Strategic Research Program(NRF-2017R1E1A1A01075128) supervised by the National Research Foundation of Korea (NRF) and under the Grand Information Technology Research Center support program((IITP-2023-2020-0-01462) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation)

2. 관련 연구

(1) 블록체인

블록체인은 분산원장 형태의 거래 시스템으로서, 중개자 없이도 매수자와 매도자가 서로 투명하게 신뢰하여 거래를 할 수 있는 시스템을 말한다[1]. 블록체인의 특성은 크게 4가지로 구성되어 있다. 블록체인의 특성은 투명성, 안정성, 효율성, 보안성이다. 이 중에 이더리움 거래를 이용하면 거래의 투명성과 안정성의 특성을 실현할 수 있다. 투명성은 모든 참여자가 볼 수 있는 블록체인의 정보로서 내용이 변화되지 않고 특정인이 수정할 수 없다는 특성을 가지고있다. 안정성은 블록체인의 서버 특성이 P2P(Peer-to-Peer)로 서로 분산되어 있어, 한 서버

를 공격해도 다른 서버들로 인하여 거래 기록이 안정적으로 돌아갈 수 있다. 블록체인의 거래에서의 특성은 한 사람의 거래 기록을 볼 수 있지만, 거래 기록이 수정되지 않고 누가 거래를 했는지 추적이 어렵다는 점이다.

(2) web 3.0(웹 3.0)

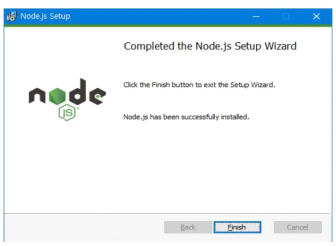
[2] web3.0(웹3.0)에서는 web2.0(웹2.0) 기술의 단점이었던 특정 플랫폼에 정보가 집중되는 단점을 해결하여 분산원장을 통하여 개인이 플랫폼을 소유할 수 있도록 하는 특성이 있다. 중앙집중형 단점을 극복한 web3.0(웹3.0)은 웹 생태계에서 사용자와 소비자의 역할을 강화하고, 개인이 시스템에 접속하여 플랫폼의 통제 없이도 자산을 직접 거래할 수 있게 한다. 그래서 web3.0(웹3.0)은 블록체인 거래의 핵심이 되며, 스마트 컨트랙트 기술을 시연할 수 있는 가장 중요한 도구가 된다.

(3) ERC-20 토큰

ERC-20 토큰의 거래는 이더리움 네트워크에서 ERC-20 토큰을 활용하여 거래할 수 있다. 이더리움의 ERC-20 토큰은 누구나 이더리움에서 정한 지침을 준수하는 스마트 계약 준수 암호화폐를 만들 수 있도록 하는 열쇠로서, NFT(Non Fungible Token)와는 다르게 고유한 토큰은 아니며, 서로 다른 개인 간의 상황을 서로 연결할 수 있도록 한다[3]. ERC-20 토큰은 지정된 거래소가 아닌 거래소에서도 서로 거래가 가능하며, 거래소의 보안 및 신뢰성으로 믿을 만한 장소를 선택하는 것이 중요하다.

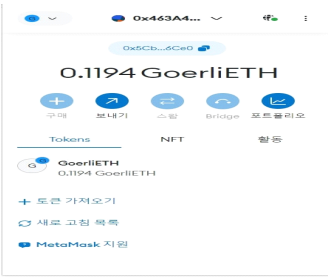
3. 이더리움 거래 시스템 구현

이더리움 거래 시스템은 web3.0(웹3.0)을 실행 시킬 수 있는 도구인 node.js의 설치로부터 시작된다. 그림 1과 같이 node.js의 설치가 완료가 되어야만 npm 엔진을 쓸 수 있고, npm install & npm start를 이용하여 반응형 웹이 실행 가능하다.

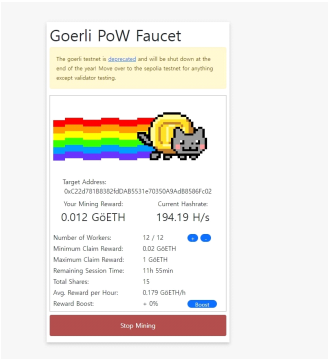


(그림 1) node.js 설치

반응형 웹을 실행한 후, 다음과 같은 화면이 나오면 그림 2와 같이 connect를 눌러, 메타마스크를 연결해야 한다. 메타마스크를 연결한 후 이더리움 승인 거래의 의미로 승인을 누른다. 이때, 이더리움 거래는 메타마스크의 설정인 goeril 테스트넷을 이용하며, 만약 가스가 부족할 경우 그림 3과 같이 faucet을 통하여 이더리움을 충전한다. 1PC당 1개의 주소만 이더리움 충전이 가능하다.

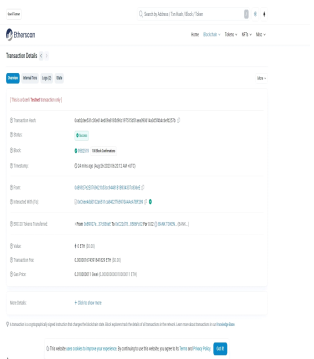


(그림 2) 메타마스크 연결



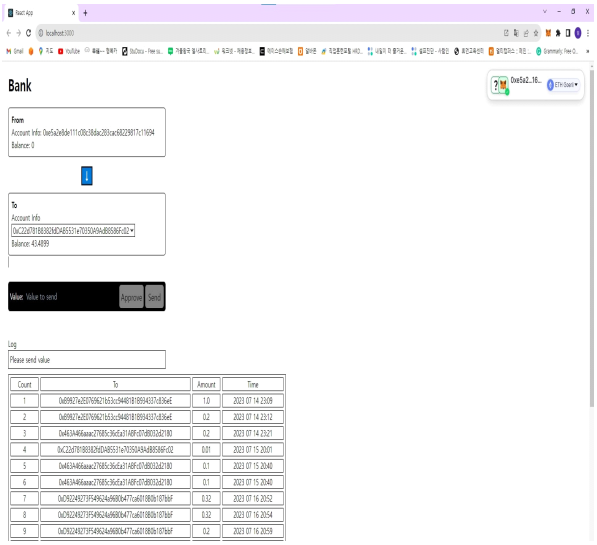
(그림 3) faucet으로 이더리움 받기

메타마스크에서 거래 승인을 누르면, 가스의 양을 비교하여 서로 이더리움 거래가 되고, 거래가 되면 테스트넷용 이더스캔을 통해서 그림4와 같이 정보를 볼 수 있으며, 이더스캔으로 볼 수 있는 정보는 거래 시간, 가스의 양, 보낸 주소, 받은 주소 등이 있다.



(그림 4) 이더스캔 거래 정보

거래가 승인이 된 상태에서, ERC-20 토큰을 보내려면 보내려는 양을 입력하고, send를 누르면 된다. 그러면, Balance에 표시된 토큰의 상태가 보낸 양만큼 바뀔 것이다. 거래가 된 후, 그림 5의 밑을 보면 로그가 쌓이는데, count는 거래한 순서를 나타내며, To는 보내는 사람의 계좌 아이디를 나타내며, amount는 ERC-20 토큰을 거래한 양을 나타낸다. 그리고, Time을 거래한 시간을 나타내는데, 거래의 관련한 간단한 정보가 표시된다고 할 수 있다.



(그림 5) 토큰 거래

4. 결론 및 향후 연구 방향

본 연구는 블록체인의 안정성, 투명성을 기반으로 하여 서로 다른 웹 이용자가 한 플랫폼 안에서 중앙의 통제 없이 서로 거래를 하는 것을 목적으로 하였다. 이를 위해서 [4] 사용자가 메타마스크로 서로 접속하여 자기 지갑을 가지고 거래를 할 수 있으며, web3.0(웹3.0)을 이용하여 개인의 정보 데이터를 직접 입력하는 가운데, 서버의 데이터가 보호될 수 있도록 하였다. 또한, 테스트넷을 통하여 토큰을 주고받는 시스템을 구현함으로써, 개인이 거래 시스템을 미리 테스트해 볼 수 있고, 그리하여 실수나 취약점으로 인한 문제를 미리 점검할 수 있다. 또한, 기업에서는 데이터 입력 후 거래 시에 거래 로그를 활용하여 보고서를 만들어 미리 거래 데이터를 측정할 수 있을 것이다. 테스트 거래가 아닌 실제 거래를 할 때 개인 정보와 암호화된 키에 대한 보호 문제가 있는데 이는 블록체인 연구의 중요한 과제 중 하나이다. 테스트넷 거래에서 더 나아가서, 실제 데이터를 암호화하여 실제 거래를 할 수 있는 방안을 앞으로 연구해 보겠다.

참고문헌

[1] hudson Lee, Crypto for Beginners: A Simple Non-Technical Guide on the Blockchain Revolution and Crypto Investing for Creating Multi-Generational Wealth, Montreal, Quebec, Canada, Hudson Lee Publishers, 2022. 10. 16

[2] 김성태,김여진,김진희 "웹(Web)기술 발전단계별 이용자의 정치참여 행태 연구." 언론과학연구 11.4 (2011): 103-137.

[3] 우청원. "블록체인 기반 연구데이터 플랫폼 구축 방안." 과학기술정책연구원-- (2020)

[4] 양성훈,진회용,김상균, "거래 비용 절감을 위한 블록체인 기반 재능거래 플랫폼." 방송공학회논문지 25.6 (2020): 922-934

Acknowledgement

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the Strategic Research Program(NRF-2017R1E1A1A01075128) supervised by the National Research Foundation of Korea (NRF) and under the Grand Information Technology Research Center support program((IITP-2023-2020-0-01462) supervised by the IITP(Institute for Information & communications Technology Planning & Evaluation)