블록체인 가상화폐 발행 및 거래 시스템 개발

최영창, 정재엽, 안규보, 황경호

국립한밭대학교 컴퓨터공학과
choiyoungchang@edu.hanbat.ac.kr, jungjaeyeop@edu.hanbat.ac.kr,
ahngyubo@edu.hanbat.ac.kr, gabriel@hanbat.ac.kr

Development of blockchain cryptocurrency issuance and transaction system

Young-Chang Choi, Jae-Yeop Jung, Gyu-Bo Ahn, Gyung-Ho Hwang

Hanbat National University, Dept. Computer Engineering

요 약

본 논문은 프라이빗 블록체인인 하이퍼레저 패브릭(Hyperledger Fabric) 네트워크를 사용하여 가상화폐를 생성하고, 관리하는 시스템을 구현하였다. 관리자는 웹 프론트를 통해 가상화폐와 가맹점을 관리할 수 있으며, 사용자는 안드로이드 어플리케이션을 통해 자신의 자산을 확인하고, 가상화폐를 전송할 수 있다. 가상화폐와 관련된 요청은 블록체인 네트워크에서 이루어지며, 트랜잭션으로 기록된다. 이를 통해 보안성, 투명성이 보장되는 네트워크를 구축할 수 있다. 관리자와 사용자는 전용 웹, 어플리케이션을 통해 거래 결과를 확인 할 수 있다. 시스템을 구성하기 위해 스프링 프레임워크를 활용하여 백엔드 서버를 구축하고, 관리자와 사용자의 요청을 하이퍼레저 패브릭 네트워크로 전송한다. 모든 트랜잭션 기록은 관리자 웹 프론트에서 확인 할 수 있다.

Ⅰ. 서 론

블록체인 기술이 발전하면서 이를 활용한 가상화폐도 많은 관심을 받고 있다. 하지만 가장 잘 알려진 비트코인의 경우 시세의 변동성이 높아 안정된 가치를 보장하기 힘들다. 이는 거래 시스템을 개발하는데 큰 문제점이 된다. 본 논문에서는 프라이빗 블록체인인 하이퍼레저 패브릭 네트워크를 활용하여 기존 코인의 문제점인 변동성을 해결하고, 투명한 거래시스템을 구현하고자 하였다. 또한 용도에 따라 가상화폐를 생성, 사용할 수 있고, 종이 화폐를 대체하여 사용할 수 있는 시스템을 구현하고자 한다. 본 논문에서 구현한 전체적인 시스템 구성도는 <그림 1>과 같다. 관리자는 웹 페이지를 통해 가상화폐를 생성할 수 있다. 웹 페이지를 통해서 생성한 가상화폐의 목록과 총 발행량을 확인할 수 있으며, 회원 전부에게 배포를 하거나, 개인에게 전송할 수 있다. 사용자는 안드로이드 어플리케이션을 통해서 회원가입, 로그인이 가능하며, 자신이 보유하고 있는 가상화폐의 목록과 양을 확인할 수 있으며, 보유하고 있는 가상화폐를 다른 사용자에게 전송할 수 있다. 생성한 가상화폐의 목록과 양은 하이퍼레저 패브릭 네트워크에 저장되며, 관리자는 거래가 일어날 때마다 하이퍼레저 패브릭에 생성되는 트랜잭션을 확인하여 거래 기록 등을 확인할 수 있다. 이를 통해 투명성을 확보 할 수 있다.

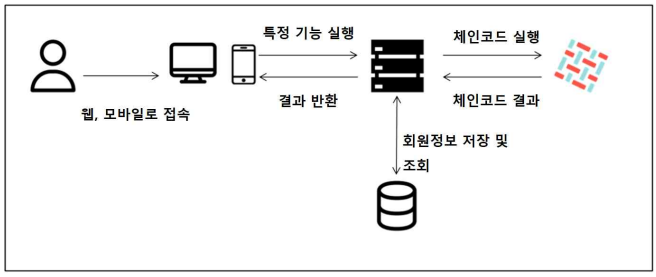

그림 1. 블록체인 가상화폐 발행 및 거래 시스템 구성도

Ⅱ. 본 론

2.1 스프링 서버와 하이퍼레저 패브릭 네트워크

본 논문에서는 블록체인 네트워크로 오픈소스인 하이퍼레저 패브릭 네트워크를 사용하였다. 하이퍼레저 패브릭 네트워크는 프라이빗 블록체인으로 허가된 사용자만이 접속할 수 있으며 기존 비트코인과 같은 가상화폐가 누구나 접속할 수 있는 퍼블릭 블록체인인 것과 대비된다. 관리자만이 가상화폐를 생성하고 배포할 수 있으며, 이를 통해 변동성을 해결하고자 하였다. 하이퍼레저 패브릭 네트워크는 체인코드를 사용하여 트랜잭션을 생성하는데, 이 체인코드에 자산의 유형과, 가상화폐를 생성하고 전송하는 로직을 정의하였다. 관리자 웹 프론트와, 사용자 안드로이드 어플리케이션의 요청을 받고, 결과를 전송하기 위한 서버로는 Spring 프레임워크를 사용하였고, 하이퍼레저 패브릭 네트워크를 연결하여 사용자의 요청을 하이퍼레저 패브릭으로 전송하고, 결과를 받아 사용자에게 전송하는 서버를 구축하였다. 웹 서버는 REST API를 제공한다. 사용자 목록, 거래기록 등은 별도로 DB에 저장하여 사용하며, 가상화폐의 목록과 각 사용자가 보유한 가상화폐의 양은 하이퍼레저 패브릭 네트워크에 별도로 저장된다.

Spring 서버는 하이퍼레저 패브릭 Java용 SDK를 사용하여 연결하였다. 최초 접속 시 인증 정보를 Wallet 폴더에 저장한다. 이때 저장된 인증 정보는 추후 서버가 하이퍼레저 패브릭 네트워크에 다시 접속할 때 사용된다.

2.2 관리자 웹 프론트

본 논문에서 개발한 시스템은 관리자와 사용자로 역할을 구분해 놓았고, 관리자는 웹을, 사용자는 안드로이드 어플리케이션을 통해 시스템에 접속한다. 웹 구현은 React를 사용하였다. 웹 페이지의 진입화면은 <그림 2>와 같다. 로그인은 ID, PW 입력 후 버튼을 누르면 정보를 서버에 전송하여 로그인 요청을 보내고, 반환받은 JWT 토큰을 로컬에 저장하여 이후 이루어지는 요청에 같이 전송한다.

메인 페이지에서는 각 기능들의 간략한 정보들을 보여주는 대시보드

화면이 <그림 3>과 같이 구성되어 있다. 대시보드에서는 최근 거래 기록 등을 확인할 수 있으며, 현재까지 발행된 가상화폐들의 비율과 가상화폐들의 거래량을 그래프로 확인할 수 있다. 가상화폐 관리에서는 가상화폐 발행, 배포, 전송, 제거가 가능하다. 가상화폐 발행에서 생성할 가상화폐의 이름을 입력하고 발행 버튼을 누르면 정보가 서버로 전송된다. 서버에서는 요청받은 기능의 파라미터 값을 하이퍼레저 패브릭 네트워크로 전송하고, 하이퍼레저 패브릭 네트워크에서는 가상화폐를 생성한 결과를 서버로 반환한다. 서버는 받은 결과를 웹 페이지로 전송한다. 본 논문에서 사용자는 역할별로 구분을 하며, 가상화폐 배포의 경우 해당하는 역할과 배포할 가상화폐, 그리고 수량을 입력하는 창이 생성되며, 값을 입력하고 배포 버튼를 누르면 해당하는 역할의 사용자에게 일괄 배포된다. 전송 기능은 사용자 개인에게 가상화폐를 전송하는 기능이다.

트랜잭션 페이지는 <그림 4>와 같다. 하이퍼레저 패브릭 네트워크 내에서 일어난 모든 거래기록은 트랜잭션으로 저장되며, 웹 페이지에서 모든 트랜잭션을 확인할 수 있다. 목록을 클릭하면 하단에 트랜잭션ID, 송신자, 수신자, 가상화폐 이름, 수량, 거래시간 등이 표시되며 관리자는 이를 확인할 수 있다.

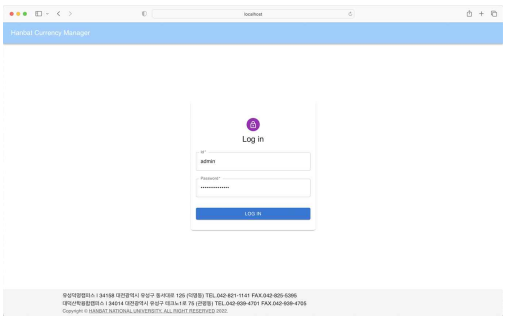

그림 2. 관리자 웹 페이지 로그인 화면

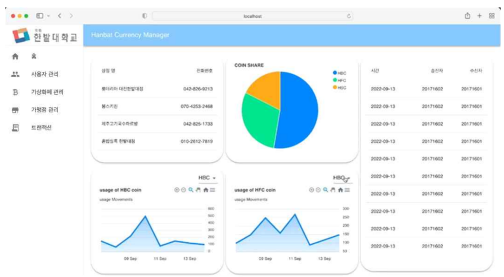

그림 3. 웹 페이지 대시보드

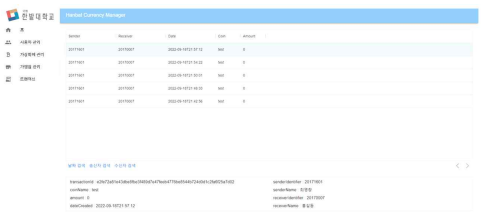

그림 4. 웹 페이지 트랜잭션 UI

2.3 사용자 안드로이드 어플리케이션

사용자는 안드로이드 어플리케이션을 통해서 자신의 자산을 확인하고, 다른 사용자에게 가상화폐를 전송할 수 있다. 안드로이드 어플리케이션은 오픈 소스인 Retrofit을 사용하여 서버에 HTTP 요청을 보낸다.

본 논문에서 구현한 안드로이드 어플리케이션의 진입화면은 <그림 5>와 같다. 회원가입을 누르면 회원가입을 위한 Activity로 전환된다. 로그인 버튼을 누르면 ID와 PW를 JSON으로 서버에 전송하고, 서버에서 JWT 토큰을 받아 메모리에 저장하며 어플리케이션은 로그인 이후에 이루어지는 모든 요청에 JWT 토큰을 헤더에 담아서 서버에 전송한다.

어플리케이션의 메인화면에서는 바텀 네비게이션을 통해서 프래그먼트를 전환하고, 각 프래그먼트마다 자산 확인, 전송, QR 코드 생성, 사용자 정보 확인 등의 기능을 제공한다. 메인 프래그먼트는 <그림 6>와 같다. 사용자가 보유한 가상화폐 목록과 최근 거래기록을 확인할 수 있으며. 전체 거래기록은 거래 칸의 이름을 클릭하면 Activity가 전환되어 볼 수 있다.

전송 화면은 <그림 7>와 같다. 사용자가 보유한 가상화폐의 목록을 스피너로 선택할 수 있으며 선택한 화폐의 잔액이 표시된다. 수신자와 전송한 양을 입력 후 전송 버튼을 누르면 웹 서버로 요청된다. QR아이콘을 클릭하면 카메라로 전환되어 QR코드를 스캔할 수 있으며 QR코드를 스캔할 시 필드가 자동으로 채워진다.

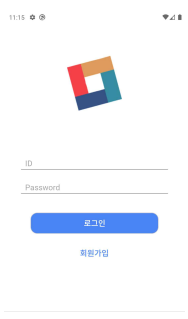

그림 5. 앱 로그인 UI

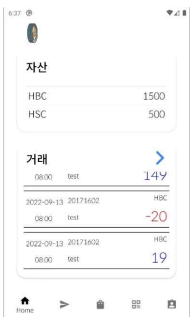

그림 6. 메인 화면 UI

그림 7. 전송 화면 UI

Ⅲ. 결론

본 논문에서는 하이퍼레저 패브릭 네트워크와 Spring 프레임워크로 구현한 웹 서버와 React로 구현한 웹 페이지, 안드로이드 어플리케이션을 사용하여 관리자가 용도별 가상화폐를 생성, 배포하고, 사용자들을 관리하고, 트랜잭션 기록을 확인할 수 있으며, 사용자는 가상화폐를 확인, 전송할 수 있는 시스템을 구현하였다. 용도별로 가상화폐를 생성하여 투표나 소규모 행사에서 통용되는 화폐 시스템으로 사용할 경우 투명성을 보장할 수 있을 것으로 기대된다.

Acknowledgements

본 연구는 2022년 과학기술정보통신부 및 정보통신기획평가원의 SW중심대학사업의 연구결과로 수행되었음. (2022-0-01068)

참 고 문 헌

[1] Won-Yong Hwang, Hyo-Kwan Kim. “A Study on Implementation of BlockChain Voting System using Hyperledger Fabric”. *Journal of Korea Institute of Information, Electronics, and Communication Technology*, v.13, no.4, pp.298-305, 2020.

[2] Sangjin Son, Soonhong Kwon, Sein Myung, Jong-Hyouk Lee. “Analysis of transaction flow and smart contract procedures of Ethereum and Hyperledger Fabric”, *Proceedings of Symposium of the Korean Institute of communications and Information Sciences*, pp.205-206, 2020.