중고거래 시스템을 위한 퍼블릭 블록체인 플랫폼 설계 및 구현

신현수*
*경북대학교 컴퓨터학부
e-mail : hyunsoo7708@gmail.com

Design and implementation public blockchain platform for second-hand shop

Hyun-Soo Shin*
*Dept of Computer Science, Kyungpook Naktional University

요 약
중고거래를 위한 퍼블릭 블록체인 플랫폼을 설계 및 구현한다.

1. 서론

인터넷상에서의 중고거래는 중개자가 없기에 신뢰를 할 수 없다. 중앙화된 중개자 프로그램을 통해 거래를 할 경우 많은 수수료를 부담하게 된다. 중앙화된 시스템(프로토콜)은 회사의 이익을 위해 언제든지 악의적인 행동을 할 가능성이 없지 않다. 이처럼 중개시스템을 통한 모든거래의 신뢰는 중개시스템을 100% 의존한다. 블록체인을 기반으로 한다면 중앙화된 시스템은 사용하지 않아도 되며 값싼 수수료 및 위변조가 불가능하고 신뢰할 수 있는 정보를 얻을 수 있다. 본 연구는 판매자의 판매기록정보를 퍼블릭 블록체인에서 분산된 원장으로 관리될 수 있게 설계 및 구현하였다. 구매자는 물품을 구매하기 전 판매자의 판매기록을 조회할 수 있고, 거래가 성사되거나 실패한다면 알고리즘에 따라 판매자의 기록정보가 퍼블릭 블록체인에 기록된다. 본 연구의 코드는 오픈소스[1]를 기반으로 작성되었다.

2. 거래처리 흐름

중고거래 웹서버와 블록체인 메인넷은 서로 완전히 독립적이다. 웹서버는 웹에서의 중고거래 커뮤니티를 위한 ID,비밀번호 및 개인정보를 저장한다. 회원가입을 하고나면 공개키와 비공개키가 자동으로 생성되어 이메일로 보내지고 공개키는 웹서버 데이터베이스에도 저장된다. 판매자는 물품을 판매할 때 추후에 거래성공여부에 따라 블록체인 데이터베이스가 업데이트 되어야 하므로 서명을 위해 웹서버로 비공개키를 제공해야 한다. 구매자는 판매글을 클릭하는 순간 판매자 판매기록정보를 웹서버로 요청하고 웹서버는 판매자의 공개키로 블록체인 메인넷에 조회요청을 한다. 블록체인 메인넷은 요청을받고 판매자의 거래기록은 UTXO[2]모델로 저장되며 판매자의 UTXO를 조회 한 뒤, 판매기록정보를 응답한다. 구매자는 판매자의 판매기록을 보고 신뢰도를 확인할 수 있다.

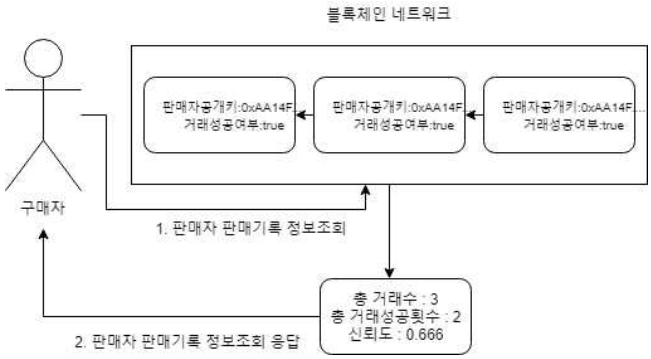

그림 1 판매자의 거래기록 정보조회.

판매자의 거래기록조회를 하기위해 블록체인 메인넷에서 판매자의 공개키에 해당하는 UTXO집합을 모아 거래성공여부가 적혀있는 트랜잭션의 개수를 거래성공여부 속성이 true인 트랜잭션의 갯수로 나누고 100을 곱한다.

$$A := UTXO\ set$$
$$B := success\ transaction$$
$$confidence = \frac{n(B)}{n(A)} \times 100$$

그림 2 신뢰도 측정

판매자의 판매기록 업데이트 트랜잭션은 다음과 같이 구성된다.

트랜잭션 인덱스: nil
트랜잭션 아웃풋 아이디: nil
서명: 판매자의 공개키로 타원곡선 암호화
공개키: 0xF22B...

그림 3 판매기록 업데이트 트랜잭션 인풋

토큰량: 0
구매자 공개키: nil
거래성공여부: true or false
판매자 공개키: 0xF22B
판매상품해쉬: nil
운송장번호: nil

그림 4 판매기록 업데이트 트랜잭션 아웃풋

본 연구에서 구현한 블록체인은 판매자의 배송전달 과정에서 중앙화된 시스템의 도움을 받는다, 따라서 완전한 탈중앙화는 아니고 탈중앙화+중앙화 모델이 결합되었다.

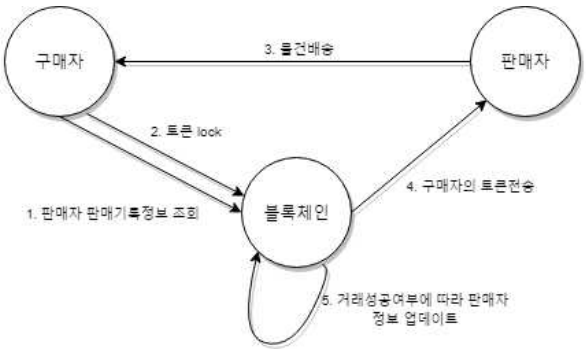

그림 5 전체적인 거래 처리 흐름

트랜잭션의 종류는 세가지이다. 토큰을 전송하는 트랜잭션과 구매자의 토큰을 잠그는(lock)트랜잭션과 판매자기록정보를 업데이트하는 트랜잭션과 구매자가 판매자에게 토큰을 전송하는 트랜잭션으로 총 3가지로 구성된다. 트랜잭션은 트랜잭션풀에 저장되며 총 2가지의 transaction pool과 locked transaction pool로 구성된다. 구매자가 물품을 구매하기 위해서는 현금을 토큰화한뒤, 구매트랜잭션을 만들어 전송한다. 구매트랜잭션은 다음과 같이 구성된다.

트랜잭션 아이디: 0xA5542...(트랜잭션아웃풋 아이디)
트랜잭션 아웃풋 인덱스: 3
서명: 판매자의 공개키로 타원곡선 암호화
공개키: 0x7ABF...

그림 6 구매 트랜잭션 인풋

트랜잭션 아이디는 UTXO 집합에서 트랜잭션 해쉬값이고 트랜잭션아웃풋 인덱스는 그 해당 트랜잭션에서의 인덱스를 말한다. 따라서 트랜잭션 인풋은 서명 및 토큰사용을 했음을 의미한다.

토큰량: 17
구매자 공개키: 0x7ABF...
거래성공여부: nil
판매자 공개키: 0xEE1A...
판매상품해쉬: 0x133BAA...
운송장번호: nil

그림 7 구매 트랜잭션 아웃풋

구매자의 공개키는 트랜잭션이 폐기될 경우 토큰을 반환받기 위해 필요하다. 구매자의 구매트랜잭션이 locked transaction pool에 저장된다. 판매자가 물품을 택배로 전송한 후 운송장번호를 포함하여 배송트랜잭션을 만든다. 배송트랜잭션은 다음과 같이 구성된다.

트랜잭션 인덱스: nil
트랜잭션 아웃풋 아이디: nil
서명: 판매자의 공개키로 타원곡선 암호화
공개키: 0xEE1A...

그림 8 판매자의 배송트랜잭션 인풋

토큰량: 0
구매자 공개키: nil
거래성공여부: nil
판매자 공개키 : 0xEE1A...
판매상품해쉬: 0x133BAA
운송장번호: 155432123...

그림 9 판매자의 배송트랜잭션 아웃풋

판매자는 여러 상품을 판매할 수 있으므로 트랜잭션이 어떤 상품에대한 트랜잭션인지 판별할 수 있게하기 위해 판매상품해쉬라는 임의의해쉬값을 만들어낸다. 배송트랜잭션은 transaction pool에 저장되므로 채굴자가 블록을 채굴하면 배송트랜잭션안에 있는 운송장번호로 검증을하고 검증이 올바르다면 locked trasaction pool에 있는 구매자의 트랜잭션을 transaction pool로 이동시킨다. transaction pool로 옮겨지면 서명검증을 통해 검증을 한번 더 한다. 서명검증까지 통과하면 거래는 완료된다. 만약 운송장번호가 허위번호라면 트랜잭션을 폐기시키고 구매자에게 토큰을 반환한다.

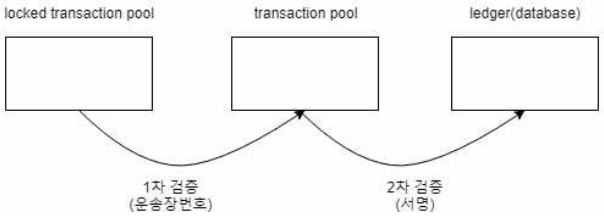

그림 10 거래 검증 과정

운송장번호로 검증하는 과정이 중앙화된 시스템을 이용하는 것이다. 이외에는 중앙화된 시스템을 이용하지 않는다.

3. 블록체인 동작과정

본 연구에서 구현한 블록체인에서 네트워크에 참여하는 노드는 검증,채굴,데이터베이스 총 3가지의 역할을 함께 수행한다. 블록체인에 새롭게 참여하는 노드는 하드코딩되어있는 DNS Seeder[3]에게 블록을 얻기위한 요청을 보낸다. 자신의 데이터베이스에 정보가 있다면 바로 응답해주며 없다면 DNS Seeder가 가지고있는 peer list내의 peer들에게 정보를 요청하고 요청을 받은 peer들은 자신의 데이터베이스 내에 정보가 있다면 블록정보를 응답한다. 구매자와 판매자간의 거래가 완료되면 판매자의 판매기록업데이트 트랜잭션이 블록체인 네트워크로 전송되며 transaction pool에 저장된다. 채굴자는 블록을 채굴한 뒤 판매자 기록업데이트 트랜잭션을 판매자가 만들었는지 검증하고 블록에 토큰전송트랜잭션, 판매자기록 업데이트 트랜잭션 총 2가지의 트랜잭션이 저장되며 자신이 가지고있는 peer list를 참고하여 peer들에게 블록을 전송한다. 네트워크를 유지시키기 위해 네트워크 참여자들에게 네트워크에 기여하는것이 이득이 될 수 있는 동기를 부여하기위해 보상시스템이 필요하다. 블록을 채굴하면 일정량의 토큰을 지급함으로써 네트워크 활성화를 촉진시킨다.

4. 오라클

본 연구에서 개발한 시뮬레이터는 판매자들의 판매기록정보가 블록체인에 저장된다. 즉, 신뢰할 수 있는 데이터이고 Dapp에서 소프트웨어 오라클[4]을 통해 데이터를 쉽게 받을 수 있다. 판매자의 판매기록정보를 통해 신뢰도를 평가하고자 하는 다른 플랫폼에서 gRPC[5]기반의 API 호출 통해 정보를 조회 할 수 있다.

gRPC를 채택한 이유는 통신을 위한 stub code[6]를 자동으로 생성해주며 많은 언어를 지원하기 때문이다. 본 연구에서 개발한 블록체인은 HTTP[7]기반의 API 호출도 지원한다.

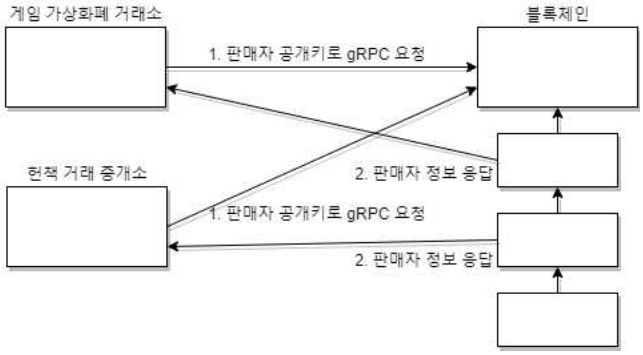

그림 10 gRPC를 이용해 다른플랫폼에서 판매자 정보쿼리

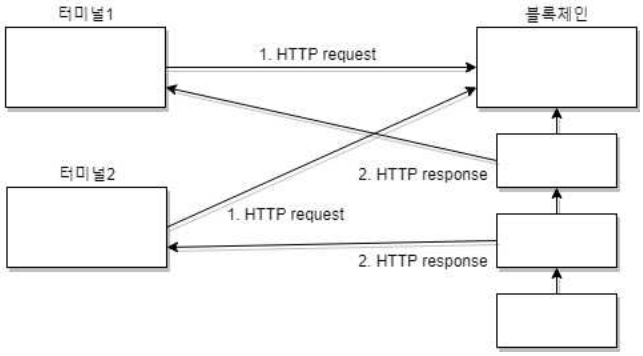

그림 11 RESTful API를 이용해 다른 플랫폼에서 판매자 정보쿼리

5. 실행화면

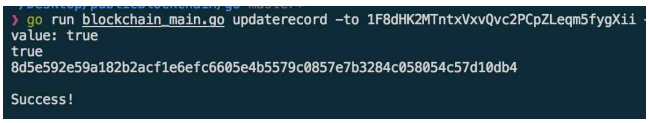

그림 12 판매자 거래기록 업데이트 시뮬레이트

그림 13 판매자 거래기록 조회

그림 14 gRPC를 이용해 javascript기반 node.js플랫폼에서 판매자 거래기록 조회

그림 15 HTTP기반 JSON-RPC 호출을 이용한 판매자 거래기록 조회

5. 개선되어야 할 점

본 연구에서는 판매자가 물품을 배송했는지에 대한 검증으로 운송장번호조회를 채택했다. 운송장번호조회는 거대한 중앙화된 시스템에서 제공하는 정보이다. 이 부분을 개선하여 탈 중앙화 할 수 있다면 비로소 완전한 중고거래를 위한 탈중앙화 플랫폼으로써 거듭날 수 있다.

6. 결론

블록체인이 가지고있는 핵심은 탈중앙화이며 탈중앙화가 필요한 서비스에 블록체인 기술이 많이 투입되고있고 연구되고있다. 본 연구에서는 기존의 중앙화된 중고거래시스템에 대해서 탈중앙화된 모델을 제시하였으며 중개자가 필요하고 모든 정보가 공개적으로 오픈되어야 하는 서비스에서는 이러한 블록체인의 연구가 더 활발하고 발전될 것이다.

참고문헌

[1] Blockchain open source : https://github.com/Jeiwan/blockchain_go
[2] UTXO set : https://en.bitcoin.it/wiki/Bitcoin_Core_0.11_(ch_2):_Data_Storage#The_UTXO_set_.28chainstate_leveldb.29
[3] DNS Seeder : https://en.bitcoin.it/wiki/Satoshi_Client_Node_Discovery#DNS_Addresses
[4] Oracle : https://en.bitcoin.it/wiki/Oracle
[5] gRPC :https://en.wikipedia.org/wiki/GRPC
[6] Stub code : https://en.wikipedia.org/wiki/Stub_(distributed_computing)
[7] HTTP : https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol