



블록체인 기반 신뢰성 있는 온라인 중고 물품 거래 플랫폼

Blockchain-based online platform for used-goods transaction

저자 (Authors)	문용성, 김락현, 김태형 Yong-Seong Moon, Lak-Hyeon Kim, Tae-Hyong Kim
출처 (Source)	한국정보과학회 학술발표논문집 , 2018.12, 1970-1972(3 pages)
발행처 (Publisher)	한국정보과학회 KOREA INFORMATION SCIENCE SOCIETY
URL	http://www.dbpia.co.kr/journal/articleDetail?nodeId=NODE07614156
APA Style	문용성, 김락현, 김태형 (2018). 블록체인 기반 신뢰성 있는 온라인 중고 물품 거래 플랫폼. 한국정보과학회 학술발표논문집, 1970-1972
이용정보 (Accessed)	금오공과대학교 202.31.128.*** 2019/12/17 01:00 (KST)

저작권 안내

DBpia에서 제공되는 모든 저작물의 저작권은 원저작자에게 있으며, 누리미디어는 각 저작물의 내용을 보증하거나 책임을 지지 않습니다. 그리고 DBpia에서 제공되는 저작물은 DBpia와 구독계약을 체결한 기관소속 이용자 혹은 해당 저작물의 개별 구매자가 비영리적으로만 이용할 수 있습니다. 그러므로 이에 위반하여 DBpia에서 제공되는 저작물을 복제, 전송 등의 방법으로 무단 이용하는 경우 관련 법령에 따라 민, 형사상의 책임을 질 수 있습니다.

Copyright Information

Copyright of all literary works provided by DBpia belongs to the copyright holder(s) and Nurimedia does not guarantee contents of the literary work or assume responsibility for the same. In addition, the literary works provided by DBpia may only be used by the users affiliated to the institutions which executed a subscription agreement with DBpia or the individual purchasers of the literary work(s) for non-commercial purposes. Therefore, any person who illegally uses the literary works provided by DBpia by means of reproduction or transmission shall assume civil and criminal responsibility according to applicable laws and regulations.

블록체인 기반 신뢰성 있는 온라인 중고 물품 거래 플랫폼

문용성[○] 김락현 김태형

금오공과대학교 컴퓨터공학과

{forever9882, rlafrkus963}@gmail.com, taehyong@kumoh.ac.kr

Blockchain-based online platform for used-goods transaction

Yong-Seong Moon[○] Lak-Hyeon Kim Tae-Hyong Kim

Dept. of Computer Eng, Kumoh National Institute of Technology (KIT)

요 약

온라인 상의 중고 거래에는 판매자와 구매자 간의 신뢰가 중요하다. 그러나 기존의 중고 거래 플랫폼은 사기를 방지하거나 판매자를 믿을 수 있는 장치가 미흡하다. 본 논문은 블록체인을 사용하여 거래 이력을 기반으로 판매자의 신뢰도를 평가하고, 물건의 신뢰성 보장을 위한 보증 정보를 기록하는 중고 거래 플랫폼을 구현하였다. 특정 블록체인 플랫폼 대신 기초적 오픈소스로 프라이빗 블록체인을 구현하였고, 휴대폰 앱 기반으로 참여할 수 있도록 서버에 블록체인 가상 네트워크를 구성하고, 휴대폰은 자원 사용을 최소화한 라이트 노드로 동작하도록 설계하였다. 또한, 서버에 대한 공격 상황에서도 블록체인의 안정성을 보장하기 위해 서버와 휴대폰 간 블록 분산 저장 기술을 적용하였다.

1. 서 론

인터넷이 발전하면서 소비자가 제품을 구매하는 방법이 점점 다변화 되고 있고, 더욱 저렴하게 제품을 구매하기 위해서 온라인 중고 거래 사이트를 이용하는 구매자들이 꾸준히 증가하고 있다. 그런데 온라인 거래는 구매자가 직접 물건을 확인할 수 없으므로 거래의 신뢰성을 보장하기 어려운 문제가 있다[1]. 대부분의 온라인 중고 거래 플랫폼은 사기를 방지하기 위해 안전거래 사이트 혹은 판매자의 사기 거래 이력을 조회할 수 있는 사기 피해 조회 사이트를 이용할 것을 권장하고 있다. 이러한 예방책에도 불구하고 번거로움으로 인해 예방 사이트의 이용률은 높지 않은 편이다. 더욱이, 안전거래 사이트 자체가 피싱(phishing)에 이용될 수도 있으므로 완전히 안전한 방식이라고 하기도 어렵다.

구매자가 삼자의 개입 없이 거래를 신뢰할 수 있기 위해서는 판매자 및 판매 물품에 대한 인증이 필요하다. 판매자의 판매 이력이나 신뢰도가 안전하게 제공될 경우 거래의 신뢰성을 보다 높일 수 있다. 블록체인(blockchain) 기술은 정보를 중앙 서버 대신 P2P 네트워크 노드들에 분산시켜 정보의 신뢰성을 보장하는 기술이다[2]. 본 논문에서는 블록체인 기술을 이용해 판매자와 판매 물품에 대한 정보 및 판매 이력에 대한 정보를 관리하여 거래의 신뢰성을 보장할 수 있는 온라인 중고 거래 플랫폼을 제시한다. 제안된 플랫폼은 블록체인에 중고 거래 시에 발생하는 트랜잭션들을 상황별로 나누어 기록할 뿐 아니라 판매자와 판매 물품의 인증을 위한 정보를 수집하고 검증할 수 있는 기능을 도입하여 거래의 신뢰성 및 이용의 편의성을 높일 수 있다. 또한 온라인 거래를 주로 휴대폰에서 이용하는 점에 착안하여 휴대폰 사용자가 블록체인 네트워크에 효과적으로 참여하면서도 보안 문제를 최소화할 수 있는 방안을 마련코자 한다.

2. 블록체인 기반 중고 거래 플랫폼

2.1 블록체인 서버 설계

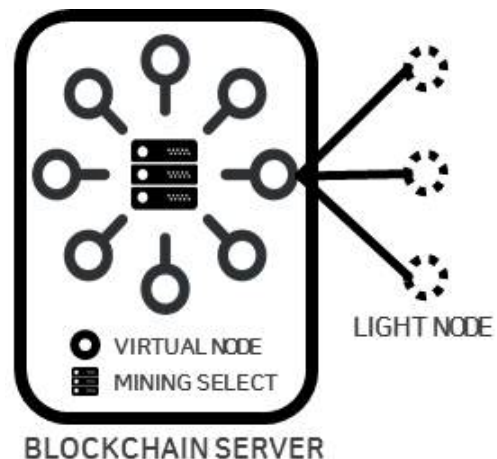


그림 1 블록체인 서버 구성도

블록체인 기술이 활용도를 넓혀감에 따라 다양한 특성의 개발 플랫폼이 등장하였다. 이더리움(Ethereum)이나 하이퍼레저(Hyperledger) 등의 본격적인 오픈 플랫폼은 신뢰성이 우수한 반면 크기가 방대해서 다소 무거우며, 관리 부담이 크고, API 의존도가 높다는 점에서 신속하고 유연한 개발이 쉽지 않은 문제점이 있다. 따라서 본 논문에서는 오픈 플랫폼을 사용하지 않고 자바 언어로 된 블록체인 오픈소스[3]를 사용하여 API 사용의 부담감을 줄이면서도 안정성과 빠른 트랜잭션 처리를 확보할 수 있도록 하였다. 본 개발 시스템은 프로세싱 및 메모리 자원이 제한되어 있는 스마트폰이 풀 노드(full node)로 네트워크에 참여하기 어려운 문제점을 극복하기 위해 그림 1과 같이 블록 생성 및 관리 기

능을 서버 내의 가상의 노드에서 담당하는 구조를 채택하였다. 순수한 P2P 네트워크에 기반하지 않음으로써 발생할 수 있는 보안 문제는 그림 2와 같이 서버와 노드 간 데이터를 분산 저장하여 해결하고자 한다.

본 블록체인 네트워크는 가상 노드(virtual node), 라이트 노드(light node), 마이닝 셀렉트(mining select)의 세 가지 유형의 노드로 구성된다. 가상 노드란 일반적인 블록체인 네트워크에서 블록체인 원장 작성에 참여하는 풀 노드와 기능적으로 동일하다. 가상 노드는 그림 1과 같이 하나의 쓰레드로서 동작하면서 여러 개의 라이트 노드를 관리한다. 라이트 노드는 자원이 제한적인 스마트 폰에서 동작하며 블록체인의 일부 데이터를 가지고 있고 트랜잭션 발생과 데이터 검증만을 하는 노드를 말한다. 마지막으로 마이닝 셀렉트는 서버 내부의 가상 노드들 중 어느 노드에서 블록을 생성할 것 인지를 결정한다. 이는 작업 증명(PoW: Proof of Work) 합의 알고리즘에 기초하며 블록 생성에 따른 마이너에 대한 보상 없이 블록을 생성한다. 또한 마이닝 셀렉트를 이용하여 체인의 분기 없이 지분증명(PoS: Proof of Stake) 합의 알고리즘처럼 블록 생성 시점에서 한 개의 블록만 생성이 가능하다. 그림 1과 같이 서버를 구성함으로써 데이터베이스의 사용 없이 데이터 무결성을 보장받을 수 있고, 라이트 노드 개념을 사용함으로써 스마트 폰에서도 데이터 검증에 대한 참여가 가능하다.

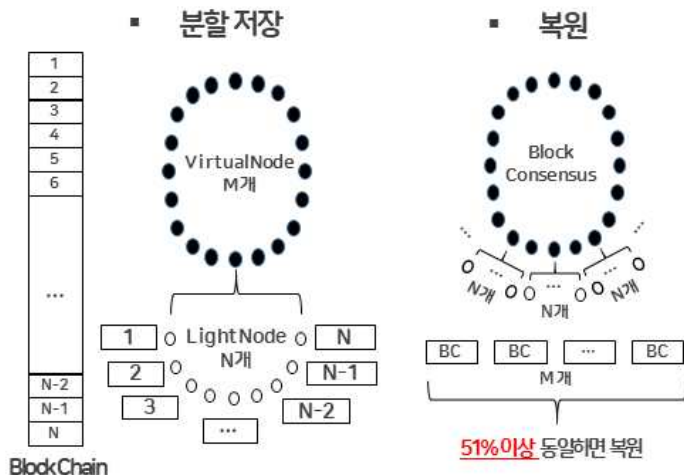


그림 2 블록체인의 분할 저장과 복원

그림 2는 데이터 분산 저장을 활용한 서버 보안 개념을 보여준다. 본 논문은 기존의 블록체인 시스템과는 달리 중앙 집중적인 하나의 서버로 블록체인의 기능을 구현했기 때문에 서버에 저장되어 있는 블록체인 데이터에 대한 안정성을 보장하기 어렵다. 따라서 데이터의 안정성을 확보하기 위해 하나의 서버에서 관리하는 블록체인을 각 가상 노드에서 관리하고 있는 라이트 노드들에게 분산하여 저장한다. 각각의 가상 노드에 연결된 라이트 노드의 수로 블록체인을 나눈 후 블록 단위로 파일화시켜 분산 저장한다. 중앙 서버의 블록체인 데이터의 무결성에 문제가 생길 경우 각 가상 노드는 라이트 노드가 가지고 있는 블록체인 조각을 이용해 체인을 구성하고 M개의 블록체인에 대하여 합의의 알

고리즘을 통해 1개의 유효한 체인을 결정하여 유지한다.

2.2 물품 인증 및 검증

구매자는 중고물품을 구입하기 전 물품 상태와 구입 시기 등을 확인할 필요가 있지만 가장 중요한 것은 실제로 판매자가 해당 물품을 가지고 있고 본인이 직접 구입한 것 인지를 확인하는 것이다. 본 시스템은 판매 물품의 신뢰성을 높이기 위하여 그림 3과 같은 물품 인증 개념을 도입하였다.



그림 3 물품 인증 과정

본 논문에서 제시하는 중고거래 플랫폼 사용자들은 새로운 물품을 구입하였을 때 구매 영수증과 상품과 같이 나오는 이미지를 플랫폼에 등록할 수 있다. 이를 통해 추후 해당 물품을 중고 거래 플랫폼에 내놓을 때 본인이 직접 구입하였음을 인증할 수 있다. 등록된 이미지 원본은 블록체인이 아닌 서버에 저장하게 되고 사용자 정보, 구매 제품 정보, 이미지 해시 값을 블록체인에 저장한다. 판매 물품 비교는 물품 인증 시의 이미지와 판매 당시의 물품 이미지를 비교하는 것으로 그림 4와 같이 사용자가 중고품 판매 글을 작성할 때 이루어진다. 과거 사용자가 물품 인증한 사진 해시를 블록체인에서 가져온 후 서버에서 해시를 키값으로 검색하여 인증된 물품 원본 이미지를 가지고 온 다음, 현재 판매할 동일 물품을 촬영한 사진과 같은 카테고리(모니터, 헤드셋 등)의 물품인지 확인한다. 최근 물품 사진에 대한 판단은 이미지의 EXIF(EXchangeable Image File format) 정보를 활용한다.

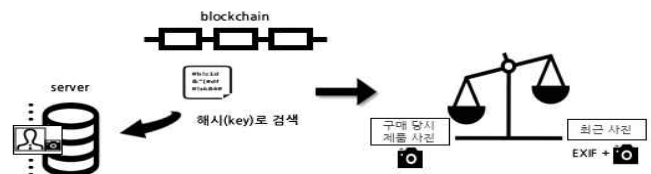


그림 4 물품 검증 과정

2.3 트랜잭션 설계와 흐름도

그림 5는 판매자와 구매자 간의 거래 흐름을 나타낸다. 이는 판매자 게시물 작성, 구매자 구매 요청, 구매자 입금, 판매자 물건 발송, 구매자 수취 확인 5단계로 구성되어 있으며 각 단계의 기록을 하나의 트랜잭션으로 보고 블록체인에 저장한다. 각 단계별 트랜잭션에는 기본적인 판매자와 구매자의 정보와 단계별로 들어가야 할 필수 정보를 포함한다. 예를 들면 판매자가 물건을 발송할 때에는 실제 물건을 발송했는지 확인하기 위해 송장번호나 택배 발송 사진을 플랫폼에 등록하도록 한다.

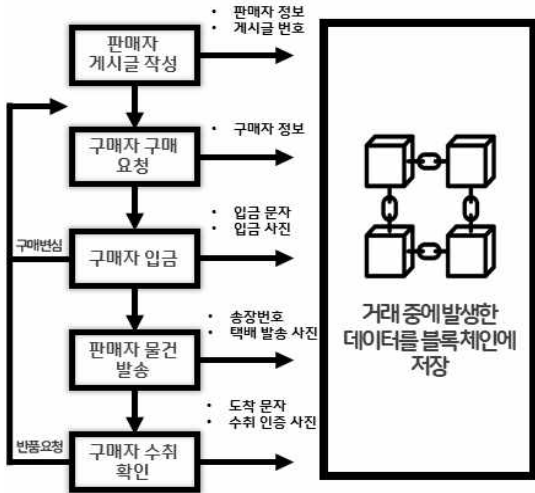


그림 5 단계별 중고 거래 흐름도

3. 어플리케이션 및 서버 구현

회원 가입을 통해 인증된 판매자는 판매 물품에 대한 인증 단계를 거쳐야 한다. 인증 단계를 통해서 검증된 물품만 판매 글 등록이 가능하다. 그림 6은 판매 물품을 인증하기 위한 화면이다.



그림 6 구매 물품 인증 단계 어플리케이션 화면

인증 단계에서는 판매할 물품의 초기 사진과 구매 내역을 함께 촬영하고, 제품의 고유 번호와 카테고리, 물품에 대한 설명을 작성하여 등록한다. 등록 후에는 해당 물품에 대한 판매 글을 작성할 수 있다.

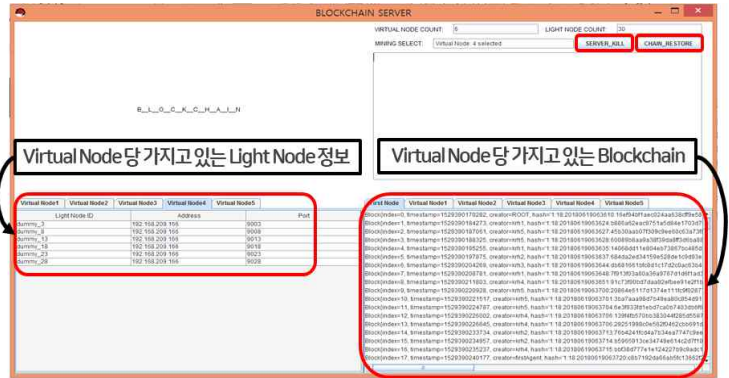


그림 7 서버 모니터링 프로그램

그림 7은 시스템에서 블록체인 서버의 상황을 모니터링하는 화면이다. 왼쪽 박스는 현재 가상 노드가 연결되어 있는 라이트 노드 정보를 보여주고 있고, 오른쪽 박스는 가상 노드 당 가지고 있는 블록체인 내용을 보여준다. 우측 상단 Server_kill 버튼을 통해 서버가 다운되었을 때의 상황을 시뮬레이션 할 수 있는데 이때 가상 노드들은 가지고 있는 블록 정보들을 모두 잃어버리게 된다. Chain_Restore 버튼은 잃어버린 블록의 정보를 라이트 노드에 분산 저장된 블록 조각들을 가져와 복원하는 기능을 실행시킨다.

4. 결론 및 향후 연구

본 논문은 블록체인을 사용하여 거래 이력을 기반으로 판매자의 신뢰도를 평가하고, 물건의 신뢰성 보장을 위한 보증 정보를 기록하는 중고 거래 플랫폼을 구현하였다. 각 사용자는 휴대폰을 통해 라이트 노드로 참여하고 블록의 생성은 서버의 가상 노드에서 이루어 기존의 블록 생성에 따른 보상 개념은 제외되어 있다. 향후 일종의 코인 시스템을 도입하여 거래 성공 시에 판매자와 구매자로부터 약간의 수수료를 코인으로 징수하고 거래의 평가에 따라 평판이 높은 사용자에게 코인을 부여하는 방식을 활용한다면 중고거래 플랫폼의 지속적 관리 및 사용자 확보에 기여하여 플랫폼의 가치를 높일 수 있을 것으로 판단된다.

5. 참고 문헌

- [1] 연합뉴스, 끊이지 않는 중고 거래 사기...이렇게 막는다, 박성은 기자, 2018. 9. 10
- [2] Nakamoto, Satoshi. "Bitcoin: A peer-to-peer electronic cash system." (2008).
- [3] <https://github.com/Will1229/Blockchain>
- [4] 이제영, "블록체인(Blockchain) 기술동향과 시사점", 동향과 이슈, (34), 1-21p