스마트 컨트랙트 기반 원자재 유통 가격 추적 어플리케이션 연구

최지호, 노융두, 강홍철, 유민재, 원유재*
충남대학교 컴퓨터공학과
cheekorkind@naver.com, yoongdoo0819@naver.com, khc7362@gmail.com,
vicerascal@cnu.ac.kr, yjwon@cnu.ac.kr
*Corresponding author : Yoojae Won

Development of smart contract-based raw material distribution price tracking application

Jiho Choi, Yoongdoo Noh, Hongcheol Kang, Minjae Yoo, Yoojae Won
Dept of Computer Engineering, Chungnam National University

요 약

2016년 말, 조류인플루엔자 확산에 의해 달걀 생산량이 감소하였고, 가격은 폭등하였다. 그러나 한 가지 납득할 수 없는 것은, 비록 달걀 생산량이 감소하였을지라도 전체적인 생산 비율에서 따져본다면 가격이 폭등할 만큼은 아니라는 것이다. 소비자는 유통 과정에서 벌어지는 일들에 대한 의문점이 있을 수 있으며 알 권리가 있다. 본 논문에서는 이러한 문제점을 해결하기 위해 거래의 투명성을 보장하는 블록체인 플랫폼에서 이더리움 가상화폐 및 스마트 컨트랙트를 사용하여 거래할 것을 제안하고자 한다. 블록체인을 활용하면 거래 내역이 모두에게 공개되기 때문에, 소비자는 이 시스템으로 하여금 상품의 가격이 각각의 유통 단계를 거치면서 얼마나 비싸지는지를 확인할 수 있다. 이로 인해 도·소매업자들이 폭리를 취하는 것 역시 줄일 수 있다.

1. 서론

2016년 말, 조류인플루엔자 확산으로 달걀 생산량이 하루 평균 4,200만개에서 약 2개월 만에 3,200만개로 1,000만개 정도 줄어들었다. 하지만 국내 달걀 소비량은 하루 평균 3,600만개이며, 즉 실제 부족량은 400만개 정도이다. 실제 수요에 비해 생산량이 400만개 정도 줄어들었다고 수급대란과 가격폭등으로 이어지는 것은 이해하기 힘들며, 이에 대해 정부 측은 일부 중간도매상들의 사재기 때문으로 보고 있다.

이처럼 유통과정에서 중간상인들의 폭리가 존재한다면 생산자와 소비자들은 손해를 입을 수밖에 없다. 또한 농산물 유통과정에서의 유통 단계는 공산품에 비해 복잡하고 길다는 특성이 있으며, 이러한 특성은 중간상인들의 폭리 가능성을 높여준다.

생산자로부터 소비자에 이르기까지의 유통과정은 모두가 신뢰할 수 있어야 한다. 그 방법으로, 전 유통과정의 거래 내역(송금일, 송금액, 품목명, 수량 등)을 블록체인(Blockchain)의 Transaction에 기록한다면 생산자, 도·소매업자, 소비자가 모두 확인할 수 있기 때문에 중간상인의 폭리를 감소시키는 데 일조할 수 있을 것이다.

따라서 본 논문에서는 생산자와 도·소매업자들이 블록체인을 기반으로 한 이더리움(Ethereum)과 스마트 컨트랙트(Smart Contract)를 이용하여 거래를 성사시킴으로써 소비자들이 어떻게 신뢰성을 바탕으로 한 유통 가격을 추적할 수 있는 지에 대한 연구를 소개한다.

2. 관련 연구

생산자와 도·소매업자가 거래하는 농산물들이 소비자에게 이르기까지의 유통 단계는 기본적으로 3~5단계 이상이다. 그러나 유통 단계에서 이루어지는 거래들은 각각 독립적이기 때문에 본인이 한 거래 외에는 다른 도·소매업자들의 거래 정보를 알 수 없다. 즉, 제3자는 유통 과정 중간에서 무슨 일이 벌어지고 있는지 알 수 있는 방법이 없다. 이러한 거래의 투명성과 관련된 문제점의 해결방안으로 블록체인을 적용할 수 있다.

2.1 블록체인

블록체인은 이루어지는 모든 거래에 대하여 모든 사람이 확인할 수 있도록 거래 내역을 공개하는 분산형 디지털 장부를 말한다[1]. 사용자가 거래하면 특정 시간 동안 발생한

모든 거래 정보가 기록된 블록을 생성하여 블록체인 네트워크상의 모든 참여자에게 전송한다. 각 참여자가 전송된 블록의 유효성을 확인하여 승인하게 되면 기존 블록체인에 거래 내역이 추가되면서 거래가 완료된다.[2] 블록체인에는 탈중앙화, 보안성, 신속성, 확장성, 투명성을 가지고 있는데 [3] 여기서 보안성과 투명성을 핵심 기능으로써 보여주고자 한다. 그 예로 블록체인에 기록되어 있는 거래내역을 변조하여 해킹을 시도하려고 할 때, 이를 위해 동일한 블록체인 네트워크 참가자들의 과반수를 해킹하여 그 이후 모든 블록의 위·변조된 거래 내역을 승인받아야 되기 때문에 변조 및 해킹하는 것은 사실상 불가능에 가깝다.[4] 즉, 블록체인을 활용하면 농산물 유통 과정의 모든 거래내역을 고객들에게 보여줄 때 보안성과 투명성을 토대로 신뢰를 줄 수 있다.

이러한 특성을 가진 블록체인 상에서 실질적으로 금액을 송·수신하기 위해서는 가상화폐가 필요하다. 대표적인 블록체인 기반의 가상화폐로는 비트코인, 이더리움 등이 있으며, 본 논문에서는 이더리움을 토대로 한 연구 내용을 다룬다.

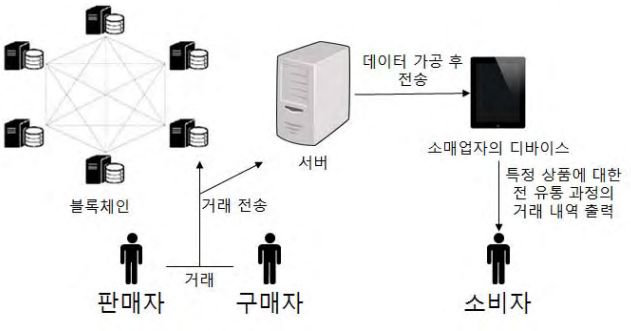
2.2 이더리움

이더리움은 비트코인의 서비스 개발 한계에 착안, 추가 기능을 효율적으로 구현하기 위해 만들어졌다. 이더리움은 타 가상화폐와 달리 이더리움 버추얼 머신(EVM: Ethereum Virtual Machine)이라는 프로그램 코드를 실행시킬 수 있는 환경을 가지고 있으며, 이 EVM에는 일반적인 컴퓨터 구조와 비슷하게 스택, 메모리, 프로그램 카운터 등이 존재한다[5]. 즉, 이더리움은 조건 분기문을 가지고 있고 메모리의 임의 위치 값을 변경할 수 있는 튜링 완전 언어(C/C++, Pascal 등)를 제공하는 플랫폼[6]이라고 할 수 있다. 이 화폐가 타 가상화폐와 달리 또 다른 특이점은, EVM 내에서 구동시킬 프로그램 코드는 바이트코드로 변환되며 이 코드들을 실행시키기 위해 'gas'라는 수수료가 사용된다는 점이다. 이 개념 덕분에 프로그램 코드상에서 무한 루프에 빠지는 일을 피할 수 있으며[7], 결국 이런 컴퓨팅 기능을 토대로 이더리움 가상화폐는 스마트 컨트랙트라는 디지털 계약서를 사용할 수 있게 된다. 스마트 컨트랙트의 필요성은 제3자의 역할을 대체한다는 것이다. 일반 거래 방식에서는 구매자와 판매자가 직접 마주하지 않는 이상 거래를 보증해줄 수 있는 중간 매개체가 필요하다(판매자가 물건을 보냈는데 구매자가 돈을 안 보낼 경우, 혹은 그 반대일 경우를 대비하기 위하여). 허나 디지털 계약서를 이용하면 구매자가 돈을 전송하고, 판매자가 물건을 정확히 보냈을 경우에만 거래가 이루어지도록 프로그래밍할 수 있기 때문에 유동적으로 상황에 대처할 수 있다.

3. 원자재 유통 가격 추적 어플리케이션

3.1 시나리오에 포함된 노드들

거래가 어떻게 이루어지고, 이루어진 거래를 어떻게 확인할 수 있는지에 대한 시나리오를 언급하기에 앞서 시나리오에 포함된 각각의 노드들에 대하여 설명한다.

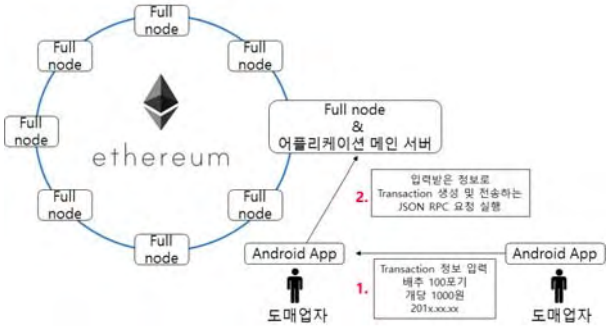


(그림 1) 원자재 유통 가격 추적 시나리오

(그림 1)에서의 시나리오는 간소화된 형태로 유통 단계를 1단계로 가정하였다. 판매자와 구매자는 생산자 및 도매인, 중소형 마트, 대형마트 등 도·소매업자들이 서로 역할이 바뀌어 행해질 수 있다. 이런 이유로 이를 대표하는 노드들이기 때문에 간단하게 1단계적으로 나타내었다. 본 시나리오의 목적은 모든 유통 과정을 거치면서 중간 유통 과정에서 폭리 등 부당한 일이 발생하지 않았다는 것을 소비자에게 알려줄 수 있어야 한다. 즉, 특정 품목에 대한 거래가 이루어졌을 때, 해당 거래를 블록체인 네트워크에 전파하여 거래 내역이 변조되지 못하도록 투명성을 얻어야 하며, 판매자와 구매자들의 유통 과정에서 기록해온 거래 내역들을 가공한 후 소비자에게 보여줄 수 있는 어플리케이션 서버의 역할이 필요하다. 끝으로, 유통 과정의 마지막인 소매업자는 서버로부터 받은 가공된 거래 내역들을 소비자에게 보여준다.

3.2 거래 시나리오

이더리움 가상화폐를 이용한 거래는 계정(account)과 비밀번호(Passphrase)를 필요로 한다. 본 논문에서 제안하는 '거래' 시나리오는 아래의 (그림 2)와 같이 진행된다. 판매자와 구매자 모두 자신의 이더리움 계정을 가지고 있다고 전제한다. 판매자는 송금일, 송금액, 품목명, 수량, 판매자 가상화폐 주소를 입력한다. 거래가 이루어지기 전에 판매자와 구매자가 거래 정보를 마지막으로 확인하고, 확인 후에 구매자가 자신의 account와 비밀번호를 입력함으로써 거래가 성사된다. 판매자와 구매자에 의해 만들어진 거래는 블록체인 네트워크로 전송되고, 결국 승인받은 거래는 블록체인에 연결된다. 또한 해당 거래내역은 어플리케이션 서버로 전송된다.

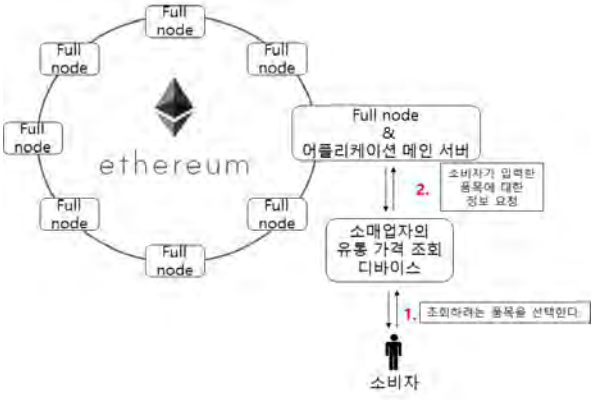


(그림 2) 거래 시나리오

3.3 거래 내역 확인 시나리오

아래의 (그림 3)처럼 소비자는 대형 마트와 같은 소매업자가 제공하는 기기를 통하여 가격을 추적할 수 있는 품목을 선택한다. 판매자와 구매자가 거래할 때 판매자는 이전 거래내역을 선택해야만 한다. 이전 거래내역을 선택함으로써 특정 품목에 대한 유통 과정이 하나로 연결될 수 있으며, 즉 소비자는 전 유통 과정을 확인할 수 있게 된다. 소비자가 요청한 특정 품목에 대한 데이터를 어플리케이션 서버가 가공한 후 해당 정보를 소매업자의 기기로 전송하고, 소비자는 기기에서 출력되는 정보를 통하여 유통 과정에서 거래할 때마다 얼마나 이윤이 붙었는지, 의심되는 거래는 없었는지 등을 확인할 수 있다.

블록체인에 저장된 거래 내역들은 앞서 데이터 변조나 해킹이 불가능에 가깝다고 하였다. 그러나 소매업자의 기기로 전송되는 데이터들은 결국 서버로부터 받기 때문에 서버가 해킹당하면 무용지물이 될 수 있다. 하지만 어플리케이션 서버는 단순히 소비자에게 편의를 제공하기 위한 데이터 가공을 목적으로 제공한다. 그러므로 서버가 해킹당하여도 주기적으로 블록체인으로부터 데이터를 받아 오기 때문에 데이터 위변조에 대한 위험요소를 배제할 수 있다.



(그림 3) 거래 내역 확인 시나리오

4. 결론

본 논문에서는 원자재의 유통 과정에서 가격 변동에 따른 문제점이 존재하는 것을 인지하였다. 이에 따른 대체 방안으로 거래의 투명성을 가질 수 있도록 블록체인 플랫폼에서 이더리움 가상화폐 및 스마트 컨트랙트를 이용하여 거래와 거래 내역 확인에 따른 각각의 시나리오를 제안하였다. 앞의 시나리오에 의해 소비자들은 유통과정 상의 가격 변동을 파악할 수 있어 신뢰를 가질 수 있고, 도매업자들은 소비자들의 신뢰에 따른 매출 상승을 기대할 수 있다.

향후, 본 논문에서 제시한 시스템의 시나리오에 따라 이더리움 블록체인 환경에 적용하여 구체적으로 설계한다. 그리고 이 방법에 따라 어떤 방식을 사용하고 적용할 지에 대해서 추가적인 연구를 진행할 것이고, 사용자들에게 편의성을 제공할 수 있는 안드로이드 어플리케이션에 대한 프로토타입을 구축하여 제안한 내용을 적용한 실제 환경에 대해 테스트를 진행할 예정이다.

감사의글

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음 (2015-0-00930)

참고문헌

[1] 성신여자대학교, “블록체인기술 금융분야 도입 방안을 위한 연구”, 2016. 6.
[2] 임명환(한국전자통신연구원), “블록체인 기술의 영향과 문제점 및 시사점”, 정보통신기술진흥센터 주간기술동향, 2016. 12.
[3] 박수민 외 3명, “블록체인 기반의 안전한 핀테크 서비스 정책 제언.”, 한국인터넷정보학회 학술발표대회 논문집, 2016. 4.
[4] 정보통신기술진흥센터, “미래를 바꿀 기술, 블록체인”, 2017. 1.
[5] 한국전자통신연구원, “이더리움”, 2017.
[6] 금융보안원, “이더리움(Ethereum) 소개 및 특징 분석”, 2016. 3.
[7] 신다혜 · 이종협(가천대학교), “핀테크를 위한 스마트 컨트랙트 보안”, 2015.