

블록체인 기술을 이용한 안전 거래 시스템 구축(사례:중고자동차)

안병태
안양대학교 교양대학 교수

Construction for Safe Transaction System using Blockchain Technology(Case:Used Car)

Byeongtae Ahn
Professor, Liberal & Arts College, Anyang University

요 약 온라인 상에서의 전자 상거래 관리 시스템은 점차 증가하고 있으며 다양한 항목에서 거래가 이루어지고 있다. 그러나 온라인 상에서의 중고 거래시 자동차와 같은 고액 거래에서는 판매자와 구매자 간의 신뢰성이 매우 중요하다. 그럼에도 불구하고, 기존의 중고 거래 시스템에서는 사기를 방지하거나 판매자를 신뢰할 수 있는 장치가 미흡하다. 본 논문은 중고 거래시 발생하는 신뢰성 향상을 위해 블록체인 기반의 중고 거래 관리 시스템을 개발하였다. 여러 분야의 중고 거래가 있지만 가장 금액이 큰 중고 자동차에 대한 거래 관리 시스템을 개발함으로써 안전 거래 시스템을 향상시켰다. 본 시스템은 이더리움 기반의 스마트 컨트랙트를 이용하여 제 3자의 개입 없이도 신뢰성을 보장하는 방식이다. 스마트 컨트랙트를 활용해서 중고자동차 거래에 필요한 계약을 설계하여 기존의 중고차 거래 시 거래 참가자의 노력과 시간을 감소시키고 동시에 안전한 거래가 가능하도록 하였다. 그리고 본 시스템은 구매자와 판매자 간 정보의 비대칭성을 완화시키고 제 3자가 개입하지 않는 유통과정의 중개수수료를 절감 및 예방하였다.

주제어 : 블록체인, 이더리움, 중고자동차, 온라인 거래

Abstract Online e-commerce management systems are gradually increasing, and transactions are made in various items. However, the reliability between sellers and buyers is very important in high-priced transactions such as automobiles when used transactions online. Nevertheless, in the existing used trading system, a device that prevents fraud or trusts the seller is insufficient. This paper developed a blockchain-based used transaction management system to improve the reliability that occurs during used transactions. We have improved the safety trading system by developing a trading management system for used cars with the highest amount of used cars in various fields. This system uses Ethereum-based smart contract to guarantee reliability without third party intervention. By designing the contracts required for used car trading by utilizing smart contracts, it was possible to reduce the effort and time of trading participants in the existing used car transactions, while enabling safe transactions. In addition, this system mitigated information asymmetry between buyers and sellers, and reduced and prevented brokerage fees in the distribution process without third parties.

Key Words : Blockchain, Ethereum, Used Car, On-line Transaction

*Corresponding Author : Byeongtae Ahn(ahnbt@anyang.ac.kr)

Received March 3, 2020
Accepted April 20, 2020

Revised April 3, 2020
Published April 28, 2020

1. 서론

우리나라 중고차 시장의 거래규모는 매년 거래 건수가 증가하고 있지만 중고차 거래 피해 또한 지속적으로 증가하고 있다. 한국 소비자원 발표에 따르면 중고차 피해 구제 신청은 줄고 있으나 중고차 성능 및 상태 점검에 관한 피해 비중이 늘고 있고 중고차 거래 피해의 80%가 정보의 허위성으로 인해 발생하고 있다. 이처럼 중고차 거래 피해가 정보의 비대칭성 즉, 판매자나 딜러가 구매자보다 훨씬 많은 정보를 가지고 있어서 구매자는 판매자나 딜러를 믿을 수밖에 없는 프로세스 때문에 중고차 거래 피해가 발생하고 있다[1]. 이와 같은 프로세스 허점을 이용해서 일부 양심 없는 판매자와 딜러가 부당이익을 취하고 있고 계속해서 중고차 거래 피해자가 나오고 있는 실정이다. 국가는 이와 같은 문제를 해결하기 위해서 중고차 구매 가이드라인을 제시하고, 구매자가 차량의 사고 이력을 조회할 수 있도록 지원하는 등 여러가지 해결 방안을 찾고 있지만 소비자의 중고차 거래 피해는 여전하다[2]. 해외에서는 블록체인을 기반으로 차량 출시부터 차량을 등록하여 데이터를 관리하는 서비스를 진행하고 있다. 그러나 여전히 계약 자체에 대한 문제가 발생한다. 정보의 비대칭성에 의한 중고 자동차 사기 및 차량 품질 문제가 악화되고 있다. 그리고 자동차 시장 참가자들에게 신뢰성 있는 차량 데이터를 통합하여 제공할 필요성이 대두되고 있다. 따라서, 본 논문에서는 이러한 문제를 해결하기 위해서 블록체인 기반으로 신뢰성 있는 차량의 정보 제공하여 거래 참가자들의 정보의 비대칭성을 줄이고, 스마트 컨트랙트를 통한 믿을 수 있는 거래 환경을 제공하는 중고차 거래 관리 시스템을 제안한다. 본 시스템은 블록체인 기술 중 스마트 컨트랙트가 지원되는 이더리움 기반의 중고 자동차 직거래 시스템을 연구하였다. 현재 블록체인 기술 중에서 이더리움 기반으로 개발된 것은 없다. 따라서, 이더리움 기반의 스마트 컨트랙트를 이용하여 웹 상에서 거래가 이루어지도록 한 것이다. 본 논문의 구성은 다음과 같다. 2장에서는 퍼블릭 블록체인 기반의 이더리움을 이용한 중고 자동차 거래 시스템 설계를 위한 연구 동향에 대해서 알아보고 3장에서는 이더리움을 활용한 중고 자동차 거래 시스템 설계를 위한 기법을 제안한다. 4장에서는 퍼블릭 블록체인 기반의 이더리움을 이용한 중고 자동차 거래 시스템을 설계하고 5장에서는 결론 및 향후과제를 제안한다.

2. 관련 연구

이 장에서는 서론에서 언급 한 블록 체인 기반 중고 거래 관리 시스템을 개발하기 위한 관련 연구를 기술하였다.

2.1 블록 체인

블록체인은 기존 은행에 적용된 중앙은행 시스템을 없애고 탈중앙화로 중앙 장부에 저장된 데이터들을 체인에 연결된 사용자들의 컴퓨터에 데이터를 저장한다. 그리고, 실제 거래를 할 때 제 3자를 거치지 않고 1:1 방식의 P2P(Peer to Peer) 시스템을 구축하였다[3,4].

블록체인은 작업증명(PoW) 방식을 사용한다. PoW는 비트코인(bitcoin)을 획득하는데 사용된 알고리즘으로 컴퓨터가 난해한 수학 문제를 내면 체인에 관여 된 모든 노드가 해당 문제를 풀어서 임의 숫자(nonce)를 발견한다. 임의 숫자를 발견한 노드는 전송에 성공한다. Fig. 1은 이전 블록과 해시 값에 의해 연결된 구조를 갖게 된다[5,6]. Fig. 1과 같이 블록과 블록의 연결은 다음 블록이 이전 해시 값을 가짐으로써 체인 형식으로 연결이 된다.

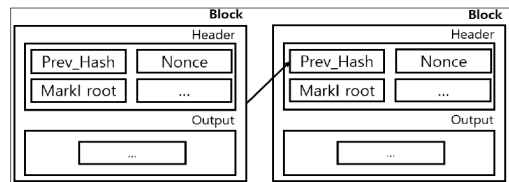


Fig. 1. Structure of Blockchain

블록체인을 이용한 최초의 상품인 암호 화폐 기술은 4가지로 분류된다.[7]. 첫째, 암호 화폐(Crypto-Currency), 둘째, 자산 발행 기술(Asset Registry), 셋째, 응용 플랫폼(Application Stack), 마지막으로 자산 중심 기술(Asset Centric)이다[8]. Fig. 2는 비트코인에서 사용하는 블록체인의 내부 모습을 나타낸 것이다. 블록에 내부에 이전 해시 값이 저장되어 체인으로 연결한 것처럼 나타난다. 실제 비트코인 블록 구조를 나타낸 것이다.

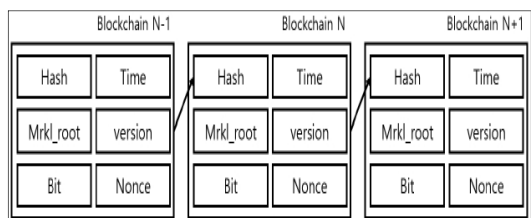


Fig. 2. Blockchain connected by a hash function

2.2 스마트 계약

스마트 계약은 Nick Szabo가 처음으로 제안한 개념이다. 기존 계약서는 서면으로 되어 있어서 계약 조건을 이행하려면 사람이 직접 수행해야 한다. 그러나, 디지털 계약(digital contract)은 조건에 따라 자동으로 체결된다. 블록체인은 여러 노드가 데이터를 검증하고, 검증된 것들을 기반으로 노드들이 공유하는 방식이다[9].

스마트 계약 실행을 적용한 블록체인 동작은 다음과 같다. 물품을 구매하는 구매자와 판매자가 있을 때, 판매자는 블록체인에 물품을 등록시킨다. 이때 스마트 계약은 트랜잭션에 따라 해당 블록체인에 새로운 노드를 등록하여 실시간으로 최신화 한다. 구매자는 검색을 이용해 해당 블록체인을 조회하며 물품을 구매한다면 스마트 계약이 해당 노드의 정보를 최신화 한다[10].

행된다. 스마트 계약 실행을 위해서는 이더리움 가상 머신(EVM)이 구동된다.

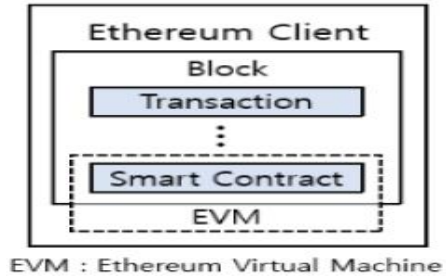


Fig. 3. Smart Contract Runtime Environment in Ethereum

2.3 블록 체인 합의 알고리즘

블록체인 알고리즘은 2가지 종류가 있다. 퍼블릭 블록체인과 프라이빗 블록체인이다[11]. 프라이빗 블록체인의 경우 체인을 구성하려는 최초의 노드가 선정한 신뢰할 수 있는 노드만이 블록체인에 들어올 수 있다. 반면에 퍼블릭 블록체인은 데이터의 신뢰성 검증시 규제 없이 참여할 수 있으며 노드들은 채굴을 통해 암호 화폐를 획득한다[12]. 본 논문에서 제안하고자 하는 것은 블록체인 기반 기술의 스마트 계약을 활용한 중고 자동차 거래를 위한 시스템 연구이다. 본 연구에서 블록체인은 퍼블릭 블록체인 알고리즘을 적용하였다. 프라이빗 블록체인의 경우 체인으로 구성된 노드들만 블록안의 데이터를 검색하기 때문에 퍼블릭 블록체인을 적용한다[13].

3. 블록체인 기반 중고차 거래 시스템 설계

중고차를 구매하기 전에 소비자들은 인터넷 상에 떠돌아다니는 체크해야 할 목록들에 대해 검색해보곤 한다. 그러나 일반인들은 그러한 방법으로 폭우로 침수 됐던 차인지 아닌지 다른 사고가 나진 않았는지 확인을 하기 어렵다. 이때 중고차를 판매하는 딜러가 이 사실을 속이고 소비자에게 판매한다면 그 피해는 고스란히 소비자에게 돌아오게 된다. 그 까닭은 바로 정보의 비대칭성 때문이다.

기존에는 중앙 서버에 모든 데이터를 저장하여 특정 데이터에 접근 권한이 있는 사람만이 해당 데이터 열람이 가능하였으나 블록체인은 탈중앙화 시스템으로 모든 데이터를 체인에 참여한 노드들이 관리하고 체인에 참여한 사람이라면 누구나 데이터 열람이 가능하다.

2.4 이더 리움

이더리움은 분산형 네트워크 플랫폼으로 클라이언트 프로그램으로 사용 가능하다[14]. 이더리움의 화폐 단위는 이더로서 거래를 위한 수수료로 사용된다. 이더리움에서는 금융 거래 프로그래밍이 필요 없지만 스마트 계약을 위해 프로그래밍을 지원한다. 수신자와 발신자 사이에 트랜잭션이나 계약 형태로 전달되며, 전달 시 시스템을 보호하는 차원에서 수수료인 이더를 함께 전달한다. 화폐의 종류는 거래를 위한 이더, 결제를 위한 finney, 수수료 지급을 위한 szabo, wei가 있다[15].

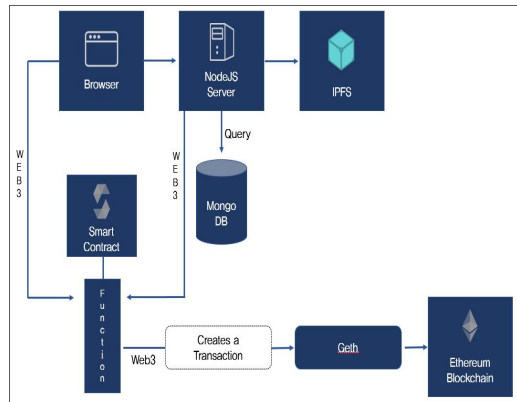


Fig. 4. Structure of System

Fig. 3은 이더리움 기반에서 스마트 계약이 구동되는 흐름을 나타낸 것이다. 개발되는 계약서는 블록에 포함시켜 블록체인의 다른 블록에 전달되고 검증 시

Fig. 4는 본 시스템의 구성도를 나타낸 것이다.

Node.js 서버 기반의 Mongo 데이터베이스를 이용하여 데이터를 저장하고 스마트 컨트랙트에 저장된 해쉬 함수를 반환하기 위해 IPFS를 사용하였다. 서버는 스마트 컨트랙트의 함수와 상호작용하기 위해 Web3.JS를 사용하였으며 스마트 컨트랙트 호출을 위해 Tx를 이용하였다. 그리고 블록체인 트랜잭션들은 geth을 통해 이더리움 블록체인에 보내도록 하였다. 즉, 웹 브라우저 환경에 접속하여 서버 기반에서 거래가 이루어진다. 계약서는 IPFS에 저장되고 거래 내역은 스마트 컨트랙트에서 관리되며 EVM을 통해 바이트 코드로 생성되어 거래가 이루어진다.

본 논문에서 구현한 중고차 거래 플랫폼은 블록체인에 기록된 차량 정보를 누구나 열람할 수 있기 때문에 구매자와 판매자 간 정보의 비대칭성을 해결한다. 트랜잭션의 위조와 변조가 불가능해 차량 정보에 대해 신뢰성을 보장할 수 있다. 또한 스마트 컨트랙트의 사용으로 중개인인 딜러가 차량 구매 과정에서 생략되어 적은 비용으로 신뢰성 있는 계약을 실행할 수 있게 된다.

따라서 구매자는 차량에 대한 신뢰성 있고 통합적인 정보를 제공 받을 수 있고 매매 과정에서의 딜러 개입의 생략으로 합리적인 가격으로 차량 구매가 가능하다. 또한 판매자는 수수료 절감뿐만 아니라 차량 데이터의 통합으로 차량 등록 처리 과정을 간소화 할 수 있다.

4. 블록체인 기반 중고차 거래 관리 시스템 구현

본 시스템은 Windows 10 기반 시스템으로 코드 인테리센스 기능 및 Typescript를 지원하는 Visual Studio Code 1.26 버전을 사용하였다. Visual Studio는 IDE중 확장 기능이 가장 뛰어나다. 서버로는 풀스택이 가능하고 비동기 프로그래밍을 지원하는 Node.js 8.11을 사용하였다. 스마트 컨트랙트 작성을 위한 언어로는 Solidity 0.4.21 버전을 사용하였다. 웹 및 앱 지원을 위한 프로그래밍 언어로는 HTML5, CSS3, Javascript 언어를 사용하였다. 서버 내 데이터베이스로는 메모리 DB인 MongoDB 3.4.1를 사용함으로써 트랜잭션 처리를 향상시켰으며 Contract 컴파일을 위해 가장 실시간 효율성이 좋은 Remix를 사용하였다.

4.1 중고차 거래 시스템 판매자 인터페이스

판매자가 중고 자동차를 등록하기 위해서는 해당 사이트에 접속하여 판매 하고자 하는 차량을 등록하여야 한다. 중고 자동차 매물 등록은 해당 사이트에 접속하여 판매자의 기본 정보를 입력한 후, 차량 등록에 관련 정보를 입력해야 한다.

Fig. 5. Interfade of Vehicle Sale Registration

Fig. 5는 차량에 대한 매물 등록을 위한 초기 화면을 나타낸 것이다. 가장 기본적으로 차량명과 차량에 대한 상세 정보를 입력하도록 되어 있다. 그외에도 기어 변속 방식, 연료 종류, 출고 연도, 주행거리, 원화가격을 입력하도록 되어 있다. 그리고 원화 가격이 아닌 이더리움으로 거래가 가능할 수 있도록 이더리움 가격도 등록되도록 되어 있다. 이러한 상세 정보를 입력하고 제출 버튼을 누르면 차량 등록 리스트에 등록이 된다.

4.2 중고차 거래 시스템 구매자 인터페이스

구매자가 차량을 구입하기 위해서는 중고 거래 시스템 사이트에 접속하여 판매자와 동일하게 기본 정보를 입력하고 매물 등록 리스트를 누르면 현재 등록된 모든 차량 정보를 제공한다.



Fig. 6. Platform for Used Car Transaction

Fig. 6은 차량 등록 리스트에서 실제 거래가 성립된 정보와 아직 판매되지 않은 차량 정보를 보여주고 있다. 구매자가 아래 차량들 중 원하는 차량을 선택하면 해당 차량에 대한 세부정보가 블록체인 기반에서 스마트 컨트랙트로 제공된다. 구매자가 해당 차량이 마음에 들어 구매를 하게되면 실시간 거래에 대한 현황 정보를 제공한다.

5. 결론 및 향후 과제

본 논문에서는 중고차 거래 시장의 문제를 해결하기 위해 이더 리움 기반의 스마트 계약을 사용하는 중고차 거래 시스템을 구현하였다. 이 시스템은 신뢰할 수 있는 데이터가 입력되었다고 가정합니다. 즉, 데이터 입력 후 무결성이 보장되지만 입력 전에 유효성 검증이 수반되어야 합니다. 이러한 한계에도 불구하고, 본 연구는 최근 문제인 블록 체인 기술을 사용하여 기존 중고차 시장의 문제를 해결함으로써 신뢰성이 보장되는 중고 자동차를 거래할 수 있었다. 향후 연구과제로는 중고자동차 거래 뿐만 아니라 전체 자동차 데이터를 투명하게 거래 관리할 수 있도록 시스템을 확장해야 한다. 그리고 이러한 시스템은 테스트 베드로 구현되기 때문에 실제 상용화가 될 수 있도록 추가 개발을 해야 한다.

REFERENCES

- [1] C. H. Cheng, C. H. Chen, You-Shyang Chen, Ho-Long Guo and Chien-Ku Lin. (2019). Exploring Taiwanese's smartphone user intention: an integrated model of technology acceptance model and information system successful model. *International Journal of Social and Humanistic Computing*, 3(2), 97-107.
- [2] Yuting Pana Xia osong Zhanga YiW. (2019). Application of Blockchain in Carbon Trading. *Energy Procedia*, 158(2), 4286-4291. DOI: 10.1109/TIFS.2017.2725820
- [3] C. Zhang, Q. Wang & D. Shi. (2016). Scenario-based potential effects of carbon trading in China: An integrated approach. *Applied Energy*, 182, 177-190.
- [4] S. Noor, W. Yang & M. Guo. (2018), Energy Demand Side Management within micro-grid networks enhanced by blockchain. *Applied Energy*, 228, 1385-1398.
- [5] Y. Zhou, J. Wu & C. Long. (2018). Evaluation of peer-to-peer energy sharing mechanisms based on a multiagent simulation framework. *Applied Energy*, 222, 993-1022.
- [6] Sikorski JJ, Haughton J and Kraft M. (2017). Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Applied Energy*, 195, 234-246.
- [7] X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso, P. Rimba. (2017). A taxonomy of blockchain-based systems for architecture design. *IEEE International Conference on Software Architecture (ICSA)*, 243-252.
- [8] Zibin Zheng, Shaoan Xie, Hong-Ning Dai and Weili Chen. (2020). An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105, 475-491.
- [9] Ahmet Bugday, Adnan Ozsoy, Serdar Murat Öztaner and Hayri Sever. (2019). Creating consensus group using online learning based reputation in blockchain networks. *Pervasive and Mobile Computing*, 59, 111-125.
- [10] Matevž Pustišek and Andrej Kos. (2018). Approaches to Front-End IoT Application Development for the Ethereum Blockchain. *Procedia Computer Science*, 129, 410-419.
- [11] D. C. Guo, J. Q. Dong & Kai Wang. (2019). Graph structure and statistical properties of Ethereum transaction relationships. *Information Sciences*, 492, 58-71.
- [12] R. Cong & A. Y. Lo. (2017) Emission trading and carbon market performance in Shenzhen. *Applied Energy*, 193, 414-425.
- [13] J. Jiang, D. Xie & B. Ye. (2016). Research on China's cap-and-trade carbon emission trading scheme.

Applied Energy, 178, 902–917.

- [14] K. N .Khaqqi, J. J. Sikorski & K. Hadinoto. (2018). Incorporating seller/buyer reputation-based system in blockchain-enabled emission trading application. Applied Energy, 209, 8–19.
- [15] N. Nizamuddin, K. Salah, M. Ajmal Azad & J. Arshad. (2019). Decentralized document version control using ethereum blockchain and IPFS. Computers & Electrical Engineering, 76, 183–197.

안 병 태(Byeongtae Ahn)

[정회원]



- 1999년 2월 : 국민대학교 컴퓨터과학부(이학사)
- 2006년 8월 : 경상대학교 컴퓨터과학부(공학박사)
- 2012년 3월 ~ 현재 : 안양대학교 교양대학 컴퓨터전공 교수
- 관심분야 : 블록체인, 전자상거래, 암호

화폐, 스마트 컨트랙트

· E-Mail : ahnbt@anyang.ac.kr