



블록체인을 활용한 자전거 관리 시스템 구축

Building bicycle management system using Blockchain

저자 (Authors)	안규황, 서화정 Kyu-hwang An, Hwajeong Seo
출처 (Source)	한국정보통신학회논문지 22(8) , 2018.8, 1139–1145 (7 pages) Journal of the Korea Institute of Information and Communication Engineering 22(8) , 2018.8, 1139–1145 (7 pages)
발행처 (Publisher)	한국정보통신학회 The Korea Institute of Information and Communication Engineering
URL	http://www.dbpia.co.kr/Article/NODE07523522
APA Style	안규황, 서화정 (2018). 블록체인을 활용한 자전거 관리 시스템 구축. 한국정보통신학회논문지, 22(8), 1139–1145.
이용정보 (Accessed)	한성대학교 61.38.12.*** 2018/10/31 15:25 (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.

블록체인을 활용한 자전거 관리 시스템 구축

안규황¹ · 서화정^{1*}

Building bicycle management system using Blockchain

Kyu-hwang An¹ · Hwajeong Seo^{1*}

¹*Department of IT Engineering, Hansung University, Seoul 02876, Korea

요 약

검찰청의 2014년 통계에 의하면 자전거 이용자의 53%가 도난 경험이 있다고 응답하였다. 우리나라의 자전거 도난율이 높은 이유는 자전거 관리 시스템이 없기 때문이다. 이는 자동차처럼 차대번호를 활용하여 자전거를 관리하지 않기 때문이다. 대부분의 사람들은 자전거에 차대번호가 있는지 모르기 때문이다. 구매자가 자전거 관리 블록체인 시스템에 자전거를 등록하게 된다면 누구나 체인에 등록 된 정보를 조회할 수 있어, 차대 번호만 기입하면 누구의 자전거인지 확인할 수 있다. 또한 사고가 발생하면 블록체인(Blockchain)은 자전거와 관련된 모든 정보를 관리하기 위해 자동차와 같이 어떤 장비가 교체되고 있는지를 기록한다. 이렇게 되면 중고 거래를 할 때 소비자는 사고 이력이 있던 제품인지 조회 할 수 있어 현명한 소비가 가능하다. 본 논문에서는 자전거 차대 번호를 활용하여 자전거 관리 시스템을 구축하는 방법을 제안한다.

ABSTRACT

According to the prosecutors' office's statistics for 2014, 53% of a bicycle users have experienced theft. The reason for the high rate of bicycle stolen in Korea is that there is no bicycle management system. This is because they do not use bicycle numbers to manage bikes like cars do. Most people do not know if they have a VIN(Vehicle Identification Number) on their bike. If the buyer registers the bicycle in the bicycle management blockchain system, anyone can view the information registered in the chain, so that if the bicycle number is filled in, the bicycle can be identified. In addition, when an accident occurs, blockchain will record what kind of equipment it is replacing, like an automobile, to manage all the information about the bicycle. In this way, consumers can inquire whether they have a history of accident when they make a second-hand transaction. In this paper, we propose a method to construct bicycle management system using bicycle VIN.

키워드 : 블록체인, 자전거, 차대 번호, 중고거래, 관리 시스템

Key word : Blockchain, Bicycle, VIN, Used article deal, management system

Received 18 May 2018, Revised 25 May 2018, Accepted 17 June 2018

* Corresponding Author Hwa-jeong Seo(E-mail:hwajeong@hansung.ac.kr, Tel:+82-2-760-8033)

Department of IT Engineering, Hansung University, Seoul 02876, Korea

Open Access <http://doi.org/10.6109/jkiice.2018.22.8.1139>

print ISSN: 2234-4772 online ISSN: 2288-4165

© This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License(<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.
Copyright © The Korea Institute of Information and Communication Engineering.

I. 서 론

일본의 경우 자동차, 오토바이뿐만 아니라 자전거 또한 등록을 하고 사용을 해야 한다. 그러나 우리나라의 경우 자동차, 오토바이만 강제적으로 등록의 의무가 있지 자전거는 해당 의무에서 제외된다.

검찰청의 2014년 통계에 따르면 지난 2013년 집계된 자전거 도난 범죄는 1만5774건에 달한다. 2008년 4915건 대비 3배 이상 증가한 수치다. 자전거 이용자의 53%가 도난을 경험했다는 통계도 있다. 이렇게 절도한 자전거는 본인이 타기보단 중고 매매 사이트에 팔아 현금을 획득할 목적으로 훔친다. 이는 자동차, 오토바이보다 도난의 위험에 많이 노출 된 면도 있지만 자전거를 개인 소유물로 등록해 놓지 않기 때문이다. 이렇게 도난당한 자전거는 개인의 소유물로 등록해 놓지 않았기 때문에 주인은 찾을 방법이 없고 심지어 거래 사이트에서 매매 되기도 한다.

자동차는 고유 차대번호를 번호판을 이용하여 탈부착 형식으로 구성되어 있지만 자전거는 그림 1¹⁾과 같이 자전거 고유의 차대 번호가 각인되어 있다. 이 번호를 활용하여 본인 정보와 함께 자전거 차대번호를 등록하는 블록체인 시스템을 만들고자 한다. 자전거를 처음 구입할 때 주인은 해당 차대번호를 블록체인 시스템상에 등록하게 된다. 블록체인의 탈중앙화 시스템특성 때문에 모든 사람이 차대번호를 조회하면 주인이 있음을 확인할 수 있다. 따라서 중고거래를 할 때 차대번호를 조회하여 해당 주인이 맞는지 확인하여 안전한 매물임을 확인할 수 있으며, 중고 거래를 할 경우 자전거의 소유권을 자전거 주인이 구매자에게 전달하여 자전거의 주인이 바뀌었음을 나타낸다. 만약 자전거를 잃어버렸는데 해당 차대 번호가 게재 된 자전거 판매 글이 올라온다면 본래 주인에게 해당 글의 알림이 가도록 한다. 본 기법을 활용한다면 두 명에 한 명 이상 꼴로 발생하던 절도율을 낮춰 안전한 사회를 만드는데 이바지할 것이라고 본다.

본 논문의 구성은 다음과 같다. 2장에서는 블록체인을 활용한 자전거 관리 시스템 구축을 위한 관련 연구 동향에 대해 살펴보고, 3장 본문에서는 블록체인을 활용한 자전거 관리 시스템 구축을 위한 제안 기법에 대해

여 설명하고, 4장에서는 본 논문에서 제안하는 기법에 대한 성능평가가 이루어질 것이며 마지막 5장에서 결론을 맺도록 하겠다.

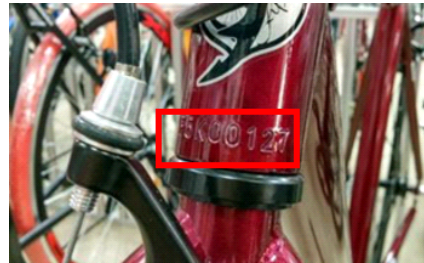


Fig. 1 Bicycle VIN number

II. 관련 연구 동향

본장에서는 본 논문에서 제안할 기법의 기초인 블록체인 기술이 무엇인지 알아본 후에 블록체인 기술을 적용한 중고 거래 플랫폼, 블록체인 기반의 애완동물 돌봄 거래, 블록체인 기반의 중고차 거래에 대하여 알아보도록 하겠다.

2.1. Blockchain Technology

최초의 블록체인 기술은 사토시 나카모토(Satoshi Nakamoto)[1]에 의해 제안되었다. 블록체인은 기존 은행에 적용되어있는 중앙은행 시스템을 없애고 탈중앙화 기법으로 중앙 장부에 저장했던 데이터들을 체인에 구성 된 사용자들의 컴퓨터에 데이터를 저장하게 하여 거래를 할 때 제 3자를 거치지 않고 1:1로 거래할 수 있는 P2P(Peer to Peer) 시스템을 구축하였다.

전문가들이 블록체인이 위·변조가 불가능한 아주 안전한 기술이라고 칭하는 이유는, 바로 해시 값(hash value)에 있다. 전송이 일어나기 전, 해당 블록에는 고유의 해시 값이 생성되게 되는데 블록 헤드(head)에서 이전 해시 값과 현재 해시 값을 갖고 있어 만약 누군가 악의적인 목적으로 특정 블록의 데이터값을 위·변조 하려고 시도한다면 해당 블록의 해시 값이 변경되게 되고, 앞·뒤에 연결 되어있는 블록의 이전 해시 값, 현재 해시 값 또한 변경이 이루어져야하기 때문에 일반적으로 수십 만개 이상으로 구성되어 있는 블록체인의 모든 블록

1) Fig. 1. Where is the bicycle VIN? [Internet]. Available: <https://goo.gl/v5XJSs>.

의 해시 값을 변경할 수는 없다고 판단하여 이를 매우 안전한 기술이라고 칭한다.

블록체인은 작업증명(Proof of Work; PoW) 알고리즘을 사용한다. PoW는 비트코인(bitcoin)을 획득하는데 사용되는 알고리즘으로, 컴퓨터가 어려운 수학 문제를 내면 체인에 참여 한 모든 노드가 해당 문제를 풀어 임의의 숫자(nonce)를 발견하는 행위를 한다. 임의의 숫자를 발견한 노드는 전송에 성공하게 되며 그림 2와 같이 이전 블록과 해시 값에 의해 연결되는 구조를 갖게 된다. 또한 해당 노드에게는 일정 비트코인을 제공하며 이를 채굴(mining)이라 칭한다. 이 뿐만 아니라 전송은 2가지 방법에 의해 시행되는데 첫 번째가 위에서 언급한 채굴이며, 두 번째로 다른 사용자에게 비트코인을 송금할 때 전송이 일어난다. 이때에는 출력부(output section)에 어떤 사용자에게 얼마를 송금하는지에 대한 내용을 담아서 보내게 된다.

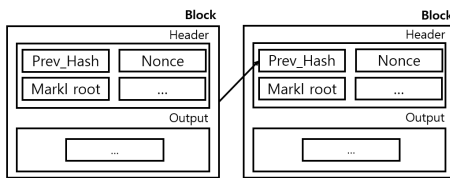


Fig. 2 Structure of blockchain

2.2. Developed P2P pet-sitting trading platform based on blockchain

P2P Pet-sitting trading platform[2]을 개발한 개발자는 현 사회의 공유 경제 모델은 소비자, 중개인, 생산자로 구성되어 있으며, 대부분의 수익이 소비자와 생산자가 아닌 중개인에게 돌아가는 것을 보고 중개인을 제외하여 생산자가 그 온전한 대가를 갖게 하고 소비자는 합리적인 가격으로 물건을 구매할 수 있게 하는데 목적을 두었다. 이에, 블록체인 기술이야말로 중개인을 제외하고 1:1로 거래할 수 있게 만들어주는 완벽한 기술이라고 판단하여 해당 플랫폼에 블록체인 기술을 도입하였다.

본 플랫폼은 소비자와 생산자 간의 신뢰를 바탕으로 돌아가는 시스템으로 블록체인은 체인 내에서 일어나는 모든 거래 내역을 블록 단위로 연결하여 모든 내역을 저장하기 때문에 시간이 흐를수록 신뢰성 있는 거래가 일어날 수 있다. 블록체인의 데이터베이스(database)안에는 등록된 회원들의 기본 정보와 애완동물의 기본정보를 관리한다. 만약 애완동물 돌봄이(pet sitter)로 활동

하고 싶을 경우 실시간으로 알아야하는 가격, 활동 기간, 활동 가능한 시간 같은 것들을 추가적으로 관리한다. 만약 소비자가 특정 애완동물 돌봄이가 마음에 들어 거래가 일어날 경우 이때 전송이 그림 3과 같이 발생하며 기존에 있던 거래 내역들과 연결이 되며 하나의 블록 덩어리로 관리되게 된다. 소비자들은 쿼리(query)를 사용하여 기존에 거래된 블록 덩어리들을 검색할 수 있다.

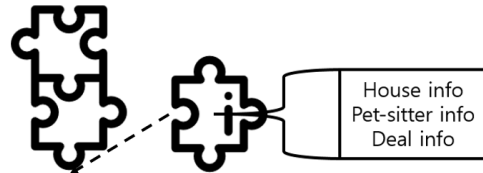


Fig. 3 Transaction flow of Blockchain

2.3. Blockchain deal with used car

중고차를 구매하기 전에 소비자들은 인터넷 상에 떠돌아다니는 체크해야 할 목록들에 대해 검색해보곤 한다. 그러나 일반인들은 그러한 방법으로 폭우로 침수됐던 차인지 아닌지 다른 사고가 나진 않았는지 계재되어 있는 내용과 다른 이상은 없는지 등의 확인을 하기 어렵다고 한다. 이때 중고차를 판매하는 딜러가 이 사실을 속이고 소비자에게 판매한다면 그 피해는 고스란히 소비자에게 돌아오게 된다. 그 까닭은 바로 정보의 비대칭성 때문이다. 그 차를 구매하고자 할 때 누구나 두려워할 정보를 한쪽에게만 치우치게 제공되어 다른 한쪽은 피해를 보게 되는 것이다. 정보의 비대칭성을 없애기 위하여 TTimes[3]에서는 블록체인 기술을 도입하는 것을 제안한다.

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. 이러한 특징을 자동차 정보에 적용하여 어떤 자동차가 언제, 어디서, 무엇을 왜 수리하였는지 분산 저장한다면 누구나 해당 정보를 열람할 수 있어 선의의 피해자가 발생하지 않을 수 있다. 이 뿐만 아니라 판매자는 축적된 데이터에 의해 기존의 거래들을 검색하여 나의 자동차가 얼마 정도에 거래 되었는지 알 수 있어 납득할 만한 가격에 처분이 가능하고 구매자 또한 이 모두 검색할 수 있기 때문에 좋은 가격에 구매가 가능하다.

III. 제안 기법

우리나라에서 중고차를 사고 팔 때 자동차의 정보를 얻기 위해 자동차 번호를 조회하고 싶을 경우 자동차민원대국민포털 사이트[4]를 이용하면 차주가 이력 조회를 동의한 경우 대부분의 정보를 열람할 수 있으며 이력 조회를 동의하지 않은 경우 제한된 정보(ex, 대포차)를 열람할 수 있다. 그러나 자전거의 경우 자전거가 최초로 출고되어 나올 때 자전거 번호가 각인되어 나오면서도 불구하고 해당 번호를 활용되어지고 있지 않다. 그래서 자전거를 중고 거래 할 때도 사람들은 이 자전거가 훔친 자전거인지 확인할 방법이 없어 선의의 피해자가 발생하기도 한다. 따라서 본 논문에서는 자동차와 마찬가지로 자전거를 구입하면 그 즉시 의무적으로 등록을 해야 사용할 수 있는 블록체인 기반의 자전거 차대 번호를 활용한 자전거 관리 시스템을 제안하고자 한다.

본 시스템은 그림 4와 같이 웹을 기반으로 돌아가며 후미단(back-end section)에서 블록체인을 활용한 SW가 사용된다. 자전거가 처음 출고되어 나오면 해당 자전거를 구입한 소비자는 웹 사이트에 차대 번호를 등록하여 본인이 주인임을 인증해야하며 허위 등록을 방지하기 위해 자전거를 생산한 업체에서 위 차대 번호가 제대로 출고된 것이 맞는지 확인을 거친 후 소유주가 등록하게 된다. 이때 블록체인 안에서는 기존에 다른 노드들이 본인의 소유임을 증명한 전송된 블록들이 존재하고 허위 등록이 아님을 인증 받은 자전거가 다음 블록으로 전송되어 등록되게 된다. 블록 안 헤더에는 기존의 블록들과 연결되기 위한 이전 해시 값, 전송 시간 그리고 차대 번호인 3개의 값이 들어가며 출력에는 자전거 차대번호 검색에 필요한 소유주, 구매일, 사고이력 이 3가지 정보가 기입되어 하나의 블록을 형성한다. 이렇게

등록된 블록들은 본 웹 사이트를 이용하여 누구나 조회를 할 수 있다. 자전거 주인이 동의를 하지 않은 경우 구입일, 사고이력은 모두 보여 지지만 개인 정보 보호를 위해 이름의 경우 성만 보여 지며 이름은 blind 처리 된다.

사고가 발생 할 경우나 기본 부품에서 무언가 더 특별한 부품으로 바꾸고자 할 때 자전거 수리 점을 찾게 될 것이다. 자전거 수리 점에서는 모든 사람의 알 권리를 위해 수리를 하로 온 자전거의 이상 정보를 모두 기입하고 그에 따라 무엇을 어떻게 수리하였는지 사고 이력(accident history)에 작성한 후 전송한다. 그러나 이때 자전거 차대번호가 과거의 구입 하자마자 등록한 거래 내역에 의해 중복으로 등록하게 된다. 만약 최초의 전송을 한 이름과 2차, 3차 그 이상으로 전송하는 사람의 이름이 같을 경우에는 별 다른 문제없이 전송에 성공하게 된다. 그러나 최초의 이름과 그 후의 이름이 다를 경우에는 이상이 있음을 감지하여 마지막으로 등록한 사람에게 팝업 메시지(pop-up message)가 전달되며 누군가 블록을 최신화하려는 시도를 한다는 것을 알리며 해당 사람의 동의를 얻어야만 전송이 가능하다. 이는 나 이외의 사람이 악의적인 목적으로 자전거 주인 명의를 바꾼 다든지 사고가 발생하지 않았음에도 발생했다고 하는 사고 이력을 조작하는 것을 방지함에 있으며, 누군가 훔친 자전거를 팔 때 정상적인 매물이 아님을 구매자는 확인할 수 있다. 또한 자전거 수리하면서 수리하는 자전거가 블록상에 기입된 주인과 맞는지 확인하여 자전거 절도를 예방할 수 있다. 구체적인 작동 절차는 그림 5와 같다.

중고 거래가 이루어질 경우에는 자전거 소유자는 판매를 희망한다는 글을 올리고 소비자는 해당 글에 있는 bicycle VIN를 활용하여 자전거 과거 이력을 조회할 수 있다. 위 제품이 마음에 들어 구매를 희망 할 경우 소비자는 본 시스템에서 \$1 = 1코인에 상응하는 암호 화폐(crypto-currency)를 환전하고 판매자에게 해당 코인(coin)을 송금을 한다. 판매자는 코인이 들어옴을 확인하고 자전거를 소비자에게 보내준다. 이때 판매자에게 전송된 암호 화폐는 바로 인출이 불가하다. 소비자에게 물건을 발송하지 않을 수 있기 때문에 소비자가 물건을 받았다는 승락 버튼을 눌러주어야만 암호 화폐를 받을 수 있다. 이때도 마찬가지로 소비자가 승락 버튼을 안 누를 수 있기 때문에 거래 성사 후 30일이 이후에는 거래가 성사된 걸로 간주하여 판매자에게 암호 화폐를 제공한다. 판매자가 판매한 금액으로 받은 암호 화폐를 실

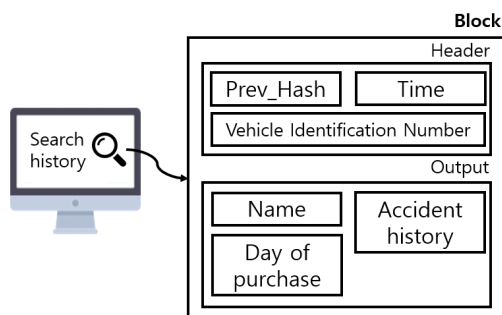


Fig. 4 Search mechanism for VIN number of bicycle

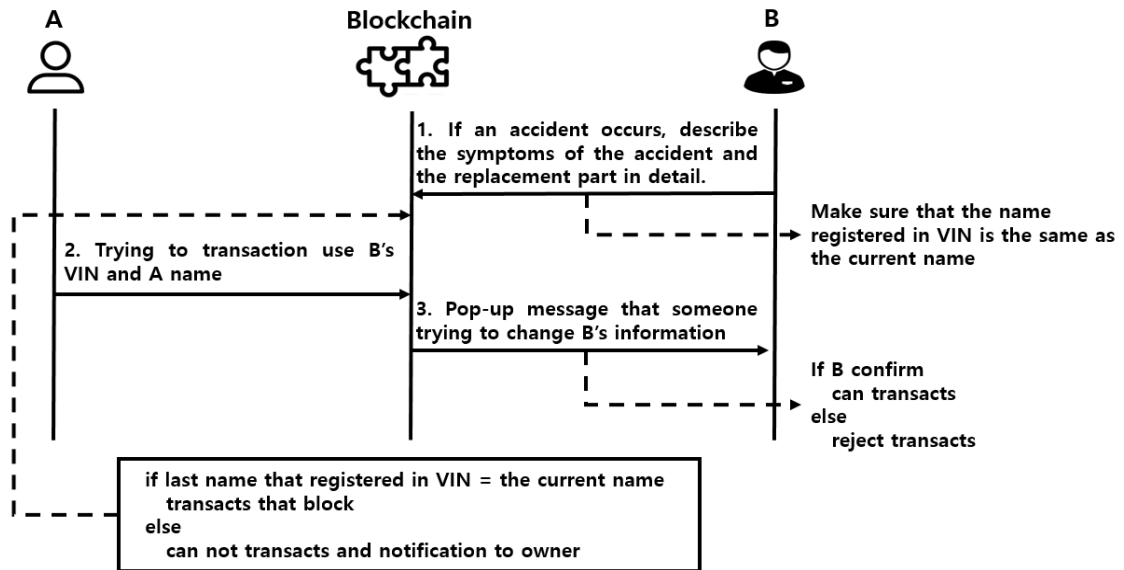


Fig. 5 Scenario for identical VIN when accident occur. VIN can verified who is the origin owner of the bicycle

제 통화로 환전할 때 전체 금액의 0.05%의 금액을 수수료로 받아 본 시스템 유지비로 사용한다. 마지막으로 자전거의 주인이 바뀌었음을 블록에 나타내기 위해 소비자는 승낙 버튼을 누르는 동시에 스마트 계약(smart contract)[5]를 기반으로 자전거 주인 정보가 자동으로 바뀌는 전송이 이루어진다.

IV. 성능 평가

현 시장에서 관리되고, 거래되고 있는 자전거 중고 매매 절차[6]와 본 논문에서 제안하는 기법의 웹 사이트에 대한 성능을 표 1과 같이 평가하여 진행하고자 한다.

현재 사용되는 자전거 관리 및 중고 매매 사이트는 중고 거래를 함에 있어 자전거 소유주와 구매를 희망하는 소비자 간의 1:1 거래가 아닌 제 3자를 거쳐서 구매를 해야 하기 때문에 중개 수수료가 발생하게 되고 이에 따라 소유주는 본 가격보다 낮은 가격을 갖게 되고, 소비자는 수수료가 붙기 때문에 본래 가격보다 비싼 가격에 구매를 하게 된다. 그러나 제안 기법에서는 자전거 소유주와 소비자가 1:1로 거래가 가능하여 별다른 수수료가 들어가지 않기 때문에 소유주는 기존 가격에 그리고 소비자 또한 기존 가격에 구매가 가능하다. 또한 중앙 서버를

관리 시스템 같은 경우 관리자가 꼭 관리를 이루어 주어야지만 시스템이 돌아가는 반면 블록체인을 활용한 중개 사이트 같은 경우 지정 된 관리자가 굳이 있지 않더라도 체인에 참여한 모든 노드가 관리자가 되기 때문에 운영, 관리 하는 면에서 훨씬 우수하다.

현재 매매되는 중고 사이트 같은 경우 제 3자인 사이트 중개인을 거쳐서 팔기 때문에 문제가 있는 제품을 싼 값에 구매하여 문제 있는 부품만 새 제품으로 바꾸어 관리가 잘 된 제품인 것처럼 판단면 소비자로서는 기존에 문제가 있었는지 알 수 있는 방법이 없으며, 실제로 약의 적인 의도를 갖고 있는 중개상 중에는 과거에 큰 사고가 났던 이를 태면 침수차량과 같은 과거 이력을 숨기고 소비자에게 파는 행위도 이루어진다. 그러나 제안 기법에서는 모든 관리 이력이 블록체인에 전송되어 남기 때문에 소비자는 과거 이력을 조회하여 사고가 났던 이력이 있다면 무엇이 문제가 있었고 어떻게 조치를 취했는지 검색할 수 있다. 이는 바로 블록체인의 보안 특성 덕분이다. 중앙 관리 시스템의 경우 과거에 작성한 글을 자유롭게 삭제 및 수정이 가능하지만 블록체인 같은 경우 과거에 전송했던 블록 내역에 대해 삭제 및 수정이 불가능하다. 따라서 만약 과거에 큰 사고가 발생하였고 그에 따라 특정 부품을 교체하였다면, 누구나 해당 사고 이력을 조회하여 볼 수 있어 구매하는데 참고할 수 있다.

이에, 기존의 중고 매매 사이트 보다 높은 신뢰성을 갖는다.

본 논문의 제안 기법의 가장 큰 차이는 관리 시스템이 있는가 없는가의 차이이다. 기존의 중고 거래 사이트에서는 자전거 차대번호를 활용하지 않고 자전거를 사고, 파는데 목적을 두어서 자전거의 출처는 신경도 쓰지 않는다. 이렇게 해서 자전거 절도범들은 아무런 규제 없이 자전거를 팔 수 있던 것이다. 그러나 본 시스템은 자전거 차대 번호로 자전거를 관리할 수 있는 시스템을 구축했기 때문에 누구나 자전거를 사고 팔 수 없게 되어 1차 규제조건이 생기게 된다.

Table. 1 Compared with typical resale web site and suggesting technology in this paper

	Current method [6]	Proposed method
Agent	O	X
Price	HIGH	LOW
Trust	X	O
Management system	X	O

V. 결 론

일본의 경우 자전거 방법 등록[7]을 통해 자전거를 등록하는데, 자전거 가게(shop)에 500엔과 구매 영수증을 제출하면 스티커를 쥐 자전거 위에 붙인 후 사용하게 한다. 대한민국의 경우 자전거 번호를 각인하여 생산함에도 불구하고 이를 활용하여 관리하는 시스템은 전무하였다. 본 기법은 대한민국에 아직 정의되지 않은 자전거 관리 시스템을 블록체인 기술을 사용하여 관리하는 방법을 최초로 제안한다.

본 기법을 제안하기 전까지 자전거는 마치 가방을 사거나 옷을 사는 것과 같이 따로 내 소유물임을 증명하지 않았다. 그러나 개인 여가생활을 존중하는 삶이 사회적 분위기를 형성함에 따라 사람들은 취미생활을 찾기 시작하였고, 많은 사람들이 자전거에 관심을 쏟기 시작했다. 입문용으로 쓰는 자전거는 최소 몇 십 만원 단위이며 보다 고수준(high level)으로 올라갈수록 몇 백 만원에서 심지어는 1,000만원을 호가하는 자전거도 있다.

자전거와 사람이 사고가 나면 차대 사람으로 취급하

여 자전거를 자동차와 동일 선상에서 바라보지만 자전거는 자동차와 달리 등록해야하는 의무가 없기 때문에 제대로 관리가 이루어지지 않고 있다. 이 때문에 많은 절도 사건이 발생하여도 다시 주인을 찾기는 어려운 실정이다. 그러나 본 기법의 자전거 차대 번호를 사용하여 자전거를 등록하고 사용한다면 내 자전거 정비 이력을 보다 쉽게 관리할 수 있으며 자전거가 고장이나 정비를 맡길 때 차대 번호를 조회하여 정비 이력을 최신 화하는 과정에서 실 주인이 맞는지 확인도 가능해 절도 율을 현재보다 낮출 수 있을 것을 기대한다.

본 논문에서 제안하는 기법은 사용자 인증에 매우 탁월한 기술이며 최근에 제안된 블록체인 기반 기부 시스템과의 연동 시 새로운 응용 도출이 가능하다 [8, 9].

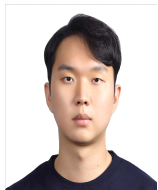
ACKNOWLEDGEMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5075742). This research of Hwajeong Seo was financially supported by Hansung University.

References

- [1] Bitcoin. Bitcoin: A Peer-to-Peer Electronic Cash System [Internet]. Available: <https://bitcoin.org/bitcoin.pdf>.
- [2] IBM. Developed P2P pet-sitting trading platform based on blockchain [Internet]. Available: <https://developer.ibm.com/kr/cloud/blockchain/2017/06/12/>.
- [3] TTimes. How does the block chain capture the problem of the used car market? [Internet]. Available: <https://goo.gl/UL4MoJ>.
- [4] ECAR. Used car history inquiry [Internet]. Available: <http://asm.ecar.go.kr/>.
- [5] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, pp. 839-858, 2016.
- [6] United States Patent, Method of exchanging goods over the internet [Internet]. Available: <https://patents.google.com/patent/US6847938B1/en>.
- [7] dinwy's tistory. How to register bicycle identification

- number in Japan [Internet]. Available: <https://goo.gl/rpkqXe>
- [8] Y. Chang, K. Bhavam "A Computational Dynamic Trust Model for User Authorization," *Asia-pacific Journal of Convergent Research Interchange*, vol. 1, no. 4, pp.1-6, Dec. 2015.
- [9] K. An, H. Seo, "Donate system development using Blockchain technology," *Journal of Korea Institute of Information and Communication Engineering*, vol. 22, no. 5, pp. 812-817, May 2018.



안규황(Kyu-hwang An)

2018년 2월: 한성대학교 IT응용시스템공학과 공학 학사
 2018년 3월~현재: 한성대학교 정보시스템공학과 석사과정
 ※관심분야: 블록체인, 블록암호, IoT 보안



서화정(Hwa-jeong Seo)

2010년 2월: 부산대학교 컴퓨터공학과 학사 졸업
 2012년 2월: 부산대학교 컴퓨터공학과 석사 졸업
 2012년 3월~ 2016년 1월: 부산대학교 컴퓨터공학과 박사 졸업
 2016년 1월~2017년 3월: 싱가포르 과학기술청
 2017년 4월~현재: 한성대학교 IT 융합공학부 조교수
 ※관심분야: 정보보호, 암호화 구현, IoT