

중고자동차 데이터의 신뢰성을 보장하는 DID기반 거래 모델

김호윤¹, 한군희², 신승수^{3*}

¹동명대학교 컴퓨터미디어공학과 학생, ²백석대학교 컴퓨터공학부 교수, ³동명대학교 정보보호학과 교수

A DID-Based Transaction Model that Guarantees the Reliability of Used Car Data

Ho-Yoon Kim¹, Kun-Hee Han², Seung-Soo Shin^{3*}

¹Student, Dept. of Computers & Media Engineering, Tongmyong University

²Professor, Division of Computer Engineering, Baekseok University

³Professor, Dept. of Information Security, Tongmyong University

요약 ICT의 발달과 거래 플랫폼의 증가로 다양한 분야에서는 온라인 거래가 더욱 친숙하다. 특히 중고거래 플랫폼과 이용자의 증가로 거래액이 증가하고 있으며 중고거래는 특성상 신뢰성이 매우 중요하다. 그중 자동차는 장기간에 걸쳐 운용하기 때문에 중고자동차 시장은 거래가 매우 활발하다. 그러나 중고자동차 거래는 정보의 비대칭성이 적용되는 대표적인 시장이다. 본 논문에서는 중고자동차 거래에서 허위광고, 허위매물에 대한 문제점을 해결하기 위해 신뢰성이 보장되는 DID 기반의 거래 모델을 제시한다. 중고자동차 거래 모델에서 판매자는 최초 매물 등록 시 허위매물을 방지하기 위해 발행기관으로부터 발급받은 데이터만 등록한다. 발급과정에서는 DID Auth로 인증하기 때문에 스니핑, 중간자 공격 등의 공격으로부터 안전하다. 제시한 거래 모델에서는 VP의 Proof 항목으로 무결성을 검증하여 신뢰성을 높이고 정보의 비대칭성을 해결한다. 또한 구매자와 판매자 간의 직접 거래로 제3자의 개입이 없어 수수료를 절감하는 효과가 있다.

주제어 : 탈중앙화 신원증명, 중고자동차, 신뢰성, 인증, 온라인 거래

Abstract Online transactions are more familiar in various fields due to the development of the ICT and the increase in trading platforms. In particular, the amount of transactions is increasing due to the increase in used transaction platforms and users, and reliability is very important due to the nature of used transactions. Among them, the used car market is very active because automobiles are operated over a long period of time. However, used car transactions are a representative market to which information asymmetry is applied. In this paper presents a DID-based transaction model that guarantees reliability to solve problems with false advertisements and false sales in used car transactions. In the used car transaction model, sellers only register data issued by the issuing agency to prevent false sales at the time of initial sales registration. It is authenticated with DID Auth in the issuance process, it is safe from attacks such as sniping and middleman attacks. In the presented transaction model, integrity is verified with VP's Proof item to increase reliability and solve information asymmetry. Also, through direct transactions between buyers and sellers, there is no third-party intervention, which has the effect of reducing fees.

Key Words : Decentralized Identifier, Used Car, Reliability, Authentication, On-line Transaction

*This research was supported by the BB21plus funded by Busan Metropolitan City and Busan Institute for Talent & Lifelong Education(BIT).

*This article is extended and excerpted from the conference paper presented at The Korean Institute of Information Technology.

*Corresponding Author : Seung-Soo Shin(shinss@tu.ac.kr)

1. 서론

ICT의 발달과 온라인 기술의 발전으로 현대에는 오프라인보다 온라인에서 쇼핑, 거래 등의 일이 더 친숙하다. 코로나-19의 확산으로 ‘언택트’ 시대로 접어들면서 중고거래 플랫폼(당근마켓, 번개장터 등)이 늘어나고 그 거래액이 증가하고 있다[1,2]. 특히 자동차 산업은 국가 경제의 한 축이며 다수의 협력업체와 연계되어 파급효과가 크고 향후 자율주행 자동차와 같이 발전 여지가 매우 많은 분야이다. 자동차는 특성상 장기간에 걸쳐 운용하며 다른 분야에 비해 중고시장에서 거래가 매우 활성화되어 있다[3]. 신차 구매는 구매 계약을 한 뒤 수개월간 기다린 후 수령하는 반면 중고자동차는 기다릴 필요 없이 구매 후 바로 수령이 가능하다는 장점이 있다. 특히 코로나-19로 인한 자동차용 반도체 대란으로 신차 출고 기간이 더욱 늘어나며, 인기 차종의 경우 1년 이상 기다려야 하므로 중고자동차를 구매하여 바로 운용하는 현상이 늘고 있다[4,5]. 중고자동차는 온라인에서 구매 시 실제 매매단지에 비해 더 많은 매물 정보를 얻을 수 있고, 딜러가 거래에 관여하는 정도가 적어 소신 있는 선택이 가능하다. 하지만 허위매물 등 문제 발생 시 사후 대처가 어렵고 매물을 직접 보지 않고 구매해야 하는 만큼 환불제도 등의 확인을 꼼꼼히 해야 한다.

중고자동차 시장의 거래액은 꾸준히 증가하는 만큼 피해액도 증가하고 있으며 정보의 비대칭성이 적용되는 대표적인 시장이다[6]. 정보의 비대칭성으로 인해 소비자는 딜러를 믿고 거래할 수밖에 없는 구조로 이루어져 있다. 일부 양심 없는 딜러는 이를 악용하여 이익을 취하는 등으로 소비자들은 꾸준히 피해를 받고 있다. 해결방안으로 블록체인의 기반 중고거래 플랫폼이 많은 관심을 받고 있다. 블록체인을 기반으로 차량 데이터에 대한 무결성을 보장하고 정보에 대한 비대칭성을 줄이고자 한다.

본 논문에서는 중고자동차 거래 시 DID를 기반으로 하여 차량 판매를 위한 매물 등록 과정에서 발행기관으로부터 검증을 받은 차량에 대해서만 등록한다. DID 기반은 블록체인의 특성으로 차량 등록 후 데이터 수정이 불가능한 것과 최초 차량 매물 등록 시점부터 검증받은 데이터를 등록하여 허위거래와 허위매물을 방지하여 신뢰성을 더욱 향상할 수 있다. 이후 판매자와 구매자 간의 차량 거래는 Chain Code를 이용하여 계약을 진행한다.

2. 관련 연구

본 장에서는 중고자동차 시장의 현황과 문제점을 분석하고 기존 블록체인 기반 중고자동차 거래 시스템에 대해 분석한다.

2.1 중고자동차 시장 현황

2020년 기준 자동차 등록 대수는 2,437만대이다[7]. 중고자동차 시장의 거래 규모는 30조 원에 이르며 신차 시장에 비해 거래 규모가 매우 빠르게 증가하고 있다[8]. 1998년도에 중고자동차 거래 규모는 신차 시장을 앞서기 시작하고[9], 2019년도에는 369만대(신차 178만대)로 약 2배를 넘어서고 있다. 연도별 차량 판매 규모는 Table 1과 같다[10].

Table 1. The size of the used car market (Unit: 10,000 units)

Year	2016	2017	2018	2019
Business Transaction	234.0	228.0	234.7	232.7
Personal transaction	144.0	145.4	142.3	136.8
Sum	378.0	373.4	377.0	369.5
Selling new cars	182.5	179.3	181.3	178.1
Multiplication compared to new car sales	2.07	2.08	2.08	2.07

온라인 시장이 커짐에 따라 정보를 쉽게 얻을 수 있어 중고자동차 시장 또한 확대되고 있다. 온라인 중고자동차 시장은 자동차 보험, 대출, 세금 납부 등의 다양한 서비스를 하나의 웹사이트에서 해결함으로써 고객에 대한 차량 거래 편의를 제공한다. 온라인 거래는 실물 자동차를 확인하는 절차가 생략되거나 간소화되기 때문에 신뢰라는 요소가 매우 중요하다. 인터넷을 통한 중고자동차 거래 시 사이트의 신뢰도가 형성되어야 구매 의도가 높아지며, 인터넷을 이용한 중고자동차 거래의 활성화를 위해서 신뢰 향상이 필요하다[11]. 미국, 유럽연합(EU) 등 선진국은 이미 신차 대비 중고차 거래 비율이 3배에 달하는 만큼 여전히 중고차 시장 성장 여력이 크다. 국내 중고차 시장 규모가 2020년 39조 원에서 2025년 50조 원 수준으로 급성장할 것이라는 전망도 나오고 있다[12].

2.2 중고자동차 거래 문제점

본 절에서는 중고자동차 거래에서 신뢰성과 허위매물

에 대한 문제점을 분석한다.

2.2.1 신뢰성

중고자동차 시장에서 매매업자를 통한 거래보다 개인 등 당사자 간 거래의 비중이 더 높은 것으로 나타나 매매업자에 대한 소비자 불신이 심각한 수준이라는 분석이 나왔다[13]. 개인 간 거래 등 중고차 매매상의 개입 없이 이뤄진 당사자 간 거래는 137.6만대로 54.7%를 차지했고, 매매업자를 통한 거래는 113.9만대로 45.3%였다[14].

중고자동차 시장에 대한 소비자의 신뢰 회복과 다수의 건전한 매매업체를 위해서는 시장구조의 개선이 필요하다. 매매업체는 거래 과정에서 '정보의 비대칭'을 활용한다. 품질이 평균 이하인 중고자동차를 보유한 매매업체가 품질이 상대적으로 좋은 중고자동차를 보유한 매매업체보다 많은 이윤을 취하는 문제가 있다. 중고자동차 매입가격은 품질에 비례하여 차이가 있으나, 매도 가격은 유사하게 설정된다. 거래가 지속되면 오히려 품질이 좋은 중고자동차를 매입하는 업체가 시장에서 먼저 도태될 가능성이 크다[15].

2.2.2 허위매물

경기도에서 허위매물 판매가 의심되는 중고자동차 사이트 31곳의 조사 결과 95%가 허위매물이었다. 자동차 관리법에 따라 중고자동차 판매자는 상사명의로 소유권을 이전한 후 상품용 중고자동차를 정식 등록하고, 상품이 판매된 후에는 해당 상품을 삭제해야 한다. 조사대상 사이트의 차량 3,096대 중 중고자동차를 상사명의로 소유권 이전 후 매매상품용으로 정식 등록된 차량은 150대(4.8%)에 불과했다. 나머지 2,946대(95.2%)는 허위매물이다[16]. 허위매물의 문제점으로 온라인에 올라온 매물을 보고 실제 매매단지에 찾아가면 정작 구매하려는 매물은 없고 딜러는 다른 자동차를 추천하며 소개한다. 온라인에 올라온 매물 중 대다수는 허위매물일 가능성이 높고, 소비자를 끌어들이기 위한 미끼 수단일 수 있다.

2.3 블록체인 기반 중고자동차 거래 시스템

안병태[17]는 블록체인을 이용한 중고자동차 안전 거래 시스템을 설계하였고, 김의현[18] 등은 블록체인과 스마트 계약을 이용한 중고자동차 매매 플랫폼을 구축하였다. 본 논문에서는 안병태[17]의 논문을 중심으로 분석한다. 안병태[17]의 거래 시스템은 이더리움을

기반하여 스마트 계약을 이용한 계약 시스템이다. Node.js 서버 기반으로 Mongo Database를 이용한다. 데이터를 저장하고 스마트 계약에 저장된 해시 함수를 반환하기 위해서는 IPFS(InterPlanetary File System)를 사용한다. Web.JS를 사용하고 스마트 계약 호출을 위해 Tx를 사용한다. 블록체인상에 저장된 차량 데이터는 누구나 열람 가능하여 구매자와 판매자 간 정보의 비대칭성을 해결한다. 또한 트랜잭션의 위조와 변조가 불가능하여 차량 데이터에 대한 무결성을 보장한다. 블록체인 시스템은 정보의 비대칭성을 해결하지만, 신뢰도의 문제점이 있다. 차량 데이터를 블록체인상에 등록 후에는 위조, 변경, 수정 삭제 등이 불가하지만, 최초 등록 시 데이터를 입력할 때 판매자에 대한 인증과 차량 데이터에 대한 유효성 검증이 수반되지 않는다. 인증 과정을 거치지 않기 때문에 누구나 판매자가 되어 매물 등록이 가능하며, 차량에 대한 허위 데이터를 등록하여 구매자를 속일 수 있다. 이는 중고자동차 거래의 문제점인 허위매물을 방지하지 못한다.

3. DID 기반의 중고자동차 거래 모델

중고자동차 거래의 대다수 문제점은 판매자와 구매자 간 정보의 비대칭성에서 온다. 정보의 비대칭성을 해결하고 신뢰 있는 거래를 위해 본 논문에서는 DID에 기반한 중고자동차 거래 모델을 제안한다[19].

3.1 중고자동차 거래 모델 구성

중고자동차 거래 모델은 발행기관(Issuer), 판매자(Seller), 구매자(Buyer), 웹(Web), 그리고 분산저장소(Verifiable Data Registry)로 구성된다. 구성요소 간의 상호작용 관계도는 Fig. 1과 같다.

3.1.1 발행기관

발행기관은 검증기관으로써 자동차관리법 시행규칙 제120조 제1항에 따른다. 발행기관은 판매자가 요청한 중고자동차에 대해 차량 데이터를 발급한다. 발행기관은 판매자의 DID를 이용하여 분산저장소에 저장된 DID document를 획득한 후 판매자의 공개키로 Challenge-Response를 생성하여 DID Auth를 요청한다. DID Auth 인증이 완료되면 발행기관은 판매자에게 성능 상태 점검을 토대로 차량 검증 후 데이터에 대한 VC(Verifiable Credential)를 발행한다. VC 항목의 요소는 Fig. 2와 같다.

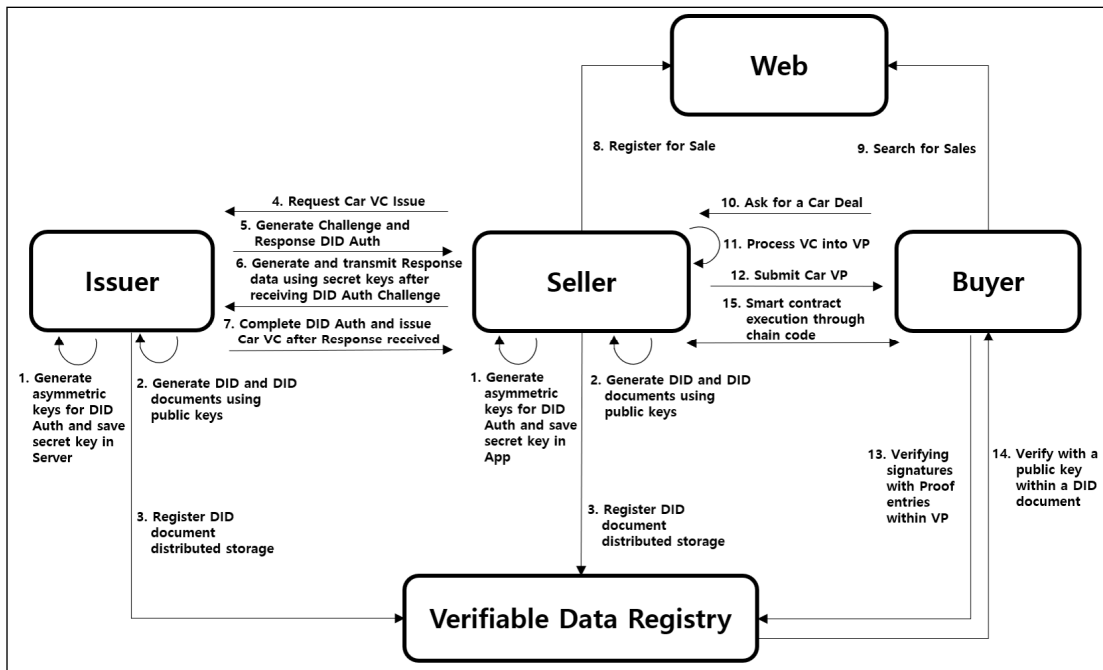


Fig. 1. Proposed Model Scenario

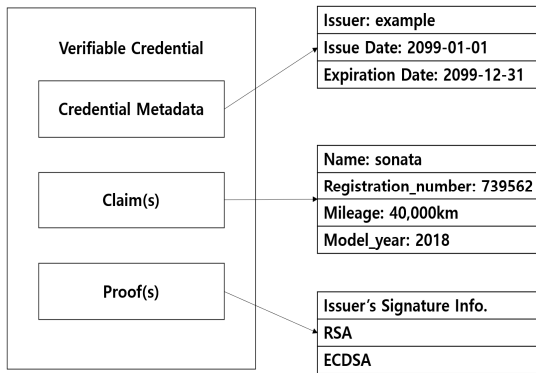


Fig. 2. The components of VC

3.1.2 판매자

판매자는 중고자동차를 판매하기 위해 발행기관으로부터 발급받은 차량 데이터를 웹상에 등록한다. 판매자는 구매자로부터 요청받은 차량 데이터를 검증하기 위해 VC를 판매자의 서명이 포함된 VP(Verifiable Presentation) 형태로 재가공하여 구매자에게 전달한다. 구매자는 분산저장소를 통해 DID document를 이용하여 VP의 진위를 검증한 후 판매자에게 거래를 요청하면 Chain Code를 통해 스마트 계약을 한다. VP

항목의 요소는 Fig. 3과 같다.

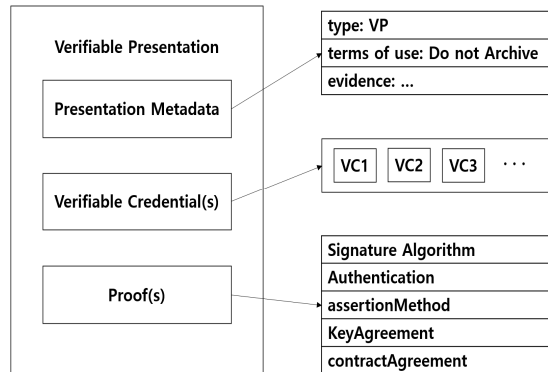


Fig. 3. The components of VP

3.1.3 구매자

구매자는 웹에 등록되어있는 중고차량 중 원하는 매물을 찾은 뒤 판매자에게 매물의 진위확인을 요청한다. 구매자는 판매자로부터 받은 VP의 진위를 확인하기 위해 분산저장소에 등록된 판매자의 DID document로부터 공개키를 가져와 VP 항목 중 Proof 항목을 검증하여 진위를 확인한다. VP의 Proof 항목에는 발행기관

의 서명과 판매자의 서명을 포함한다. 검증이 완료되면 구매를 위해 판매자에게 스마트 계약을 요청한다.

3.1.4 웹

판매자는 발행기관으로부터 발급받은 차량 VC를 웹에 등록하여 구매자에게 차량 데이터를 제공한다. 구매자는 웹에 등록된 매물 중 원하는 매물을 검색하여 판매자와 거래한다.

3.1.5 분산저장소

분산저장소는 기본적으로 구성원들의 DID document를 저장한다. DID로부터 분산저장소에 저장된 DID document의 위치를 가져오며 DID document는 소유 인증에 사용되는 공개키를 포함하고 있다. 공개키는 신원 인증과 데이터 검증에 이용된다.

3.2 중고자동차 거래

구매자는 웹에 등록되어있는 중고차량 중 원하는 매물을 찾은 뒤 판매자에게 매물의 진위확인을 요청한다. 구매자는 판매자로부터 받은 VP의 진위를 확인하기 VC 발행을 요청받은 발행기관은 신분을 인증하기 위해 판매자의 DID를 이용하여 분산저장소에 저장된 DID document를 가져온다. DID document에 저장된 판매자의 공개키를 이용하여 DID Auth인 Challenge-Response를 진행하고 상호 신분을 인증한다. 구매자는 웹에 등록되어있는 중고차량 중 원하는 매물을 찾은 뒤 판매자에게 매물의 진위확인을 요청한다. 구매자는 판매자로부터 받은 VP의 진위를 확인하기 판매자는 발급받은 VC 데이터를 웹에 등록함으로써 차량 데이터를 구매자에게 제공한다.

구매자는 웹에 등록된 차량을 검색하고, 원하는 차량 데이터에 대해 판매자에게 검증을 요청한다. 판매자는 발급받은 VC를 제출에 필요한 항목인 VP로 재가공한 후 구매자에게 제출한다. 구매자는 분산저장소로부터 판매자와 발행기관의 DID document를 가져와 공개키를 이용하여 차량 데이터를 검증한다. VP에 포함된 VC의 Proof 항목에서 발행기관이 발행한 VC가 위변조되지 않고 올바른지, VP를 제출하는 판매자가 본인 이 맞는지 VP 내에 있는 proof 항목으로 검증한다.

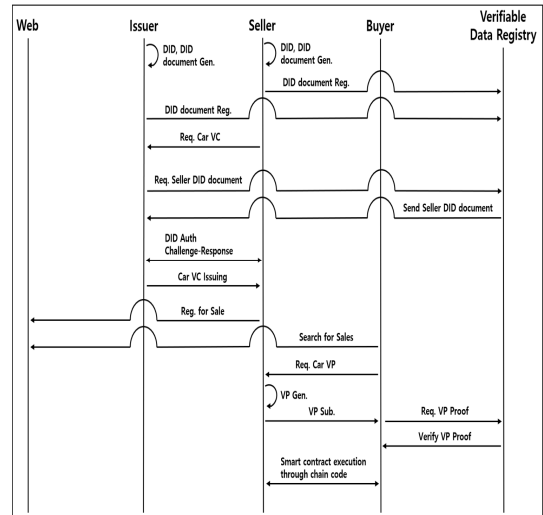


Fig. 4. Proposed model flow chart

성능 상태 점검 차량 데이터의 VC 예제는 Fig. 5와 같으며 Type은 VC를 정의하고 Issuer 항목에 발행기관과 날짜가 들어간다. Claim 속성으로 CredentialSubject 항목에는 판매자의 ID 속성과 차량에 대한 정보가 기재된다. Proof 항목에는 검증에 필요한 서명 값이 들어간다. 구매자는 진위 검증을 완료한 후 판매자에게 거래 요청하고, 거래 요청받은 판매자는 Chain Code를 이용한 스마트 계약을 진행한다.

```

1 {
2   "@context": [
3     "https://www.w3.org/2018/credentials/v1",
4     "https://www.korgov.example.org/context"
5   ],
6   "id": "http:korgov.example.org/credential/1234",
7   "type": ["VerifiableCredential", "KoreaGovContext"],
8   "issuer": "did:test:Vehicle Verification Agency",
9   "issuanceDate": "2021-01-01T20:00:00Z",
10  "expirationDate": "2021-01-01T20:00:00Z",
11  "credentialSubject": {
12    "id": "did:test:1234",
13    "Car_Info": {
14      "name": "sonata",
15      "registration_number": "739562",
16      "mileage": "40,000km",
17      "model_year": "2018"
18    }
19  },
20  "proof": {
21    "type": "RsaSignature2018",
22    "ProofPurpose": "assertionMethod",
23    "created": "2021-01-01T20:00:00Z",
24    "creator": "Vehicle Verification Agency",
25    "verificationMethod": "did:test:AAAA#Key-1",
26    "jws": "eyJhbGciOiAiM2VudCIsImNyaGUiOiAiZm9udCIsImVudCI6IHR5cGU6ICJ2ZXIiLCJ1aWkiOiAidmVudC1234IiwiaWF0IjoiMjAyMS0xMS0wMSJ9"
27  }
28 }
    
```

Fig. 5. Example of VC

대부분의 중고자동차 거래는 딜러의 개입이 있고 제 3 자로 인해 수수료가 발생한다. 그러나 본 논문에서 제안하는 Fig. 4와 같은 시나리오를 이용하면 누구나 등록된 매물을 열람하여 판매자에게 데이터 검증 요청을 할 수 있어 구매자는 차량 데이터에 대한 정보의 비대칭성을 해결할 수 있다. 또한 거래 과정에서 딜러의 개입이 없어 합리적인 가격으로 거래가 가능하다.

4. 분석

중고자동차 거래에서는 거래 당사자 간 신뢰가 가장 중요하다. 중고자동차 거래의 가장 큰 문제점인 정보의 비대칭성을 해결하기 위해 웹과 분산저장소를 통해 중고자동차 데이터는 누구나 열람할 수 있고 검증이 가능하다. 본 장에서는 DID 표준화를 제정하고 있는 W3C의 보안 요구 사항을 토대로 분석한다.

4.1 안전성 분석

DID 표준 보안 요구에 대한 제안 모델의 안전성을 분석한다.

첫 번째, 무결성 및 인증에 관한 안전성 분석은 다음과 같다. 구매자는 VP 차량 데이터의 진위를 VP에 포함된 VC의 proof, VC의 credentialSubject와 DID에 대한 DID Auth, VP의 포함된 proof 항목을 검증한다. 발행기관이 발행한 VC의 proof 항목은 VC를 발행한 기관이 올바른 기관인지 해당 VC가 위·변조되지 않았는지 검증한다. 또한 VC의 credentialSubject와 DID Auth는 VC가 가리키는 객체가 판매자가 맞는지 확인함으로써 인증한다. VP의 포함된 proof 항목은 해당 VP를 제출하는 판매자의 본인 여부와 제출된 VP가 위·변조되었는지 여부를 인증하고 데이터의 무결성을 검증한다.

제안한 모델에서 DID 시스템은 PKI를 기반한 암호화 시스템이다. 발행기관, 판매자 그리고 구매자는 DID Auth를 인증할 때 매번 다른 값의 Challenge-Response를 수행한다. 개인키는 소유자만이 가지고 있어 공격자는 알 수 없으므로 매번 다른 임의의 난수 값을 생성한 후 약속된 암호화 알고리즘으로 인증을 수행하는 DID Auth의 Response 값을 만들어 내지 못한다. 이는 중간자 공격, 재전송 공격으로부터 안전하다. 또한 차량의 데이터는 차량의 소유자인 판매자만이 관리하며 가지

고 있다. 이는 중앙집중식형식에서 오는 서버 관리자의 악의적인 데이터 변경, 삽입 그리고 삭제 등이 불가하여 내부자 공격으로부터 안전하다.

두 번째, 가용성에 대한 안전성 분석은 다음과 같다. 중고자동차 거래에 있어서 정보의 비대칭성을 해결하기 위해 구매자는 차량 데이터에 대한 검증을 언제든지 할 수 있어야 한다. 제안 모델에서는 판매자가 차량에 대한 데이터를 직접 관리하며, 개인키를 가지고 있는 판매자만이 접근하여 구매자에게 제출할 수 있다. DID는 분산원장 기술을 기반으로 분산저장소는 같은 정보가 담긴 데이터가 각각의 네트워크 참여자들에 의해 분산 저장 및 관리된다. 중앙집중식이 아닌 분산원장 기술로 DDoS, DRDoS 등의 공격으로 인해 어느 한 곳에 장애가 발생하여도 가용성에 문제가 없다.

4.2 효율성 분석

안병태[17]는 중고자동차 거래의 문제점인 정보의 비대칭성을 해결하기 위해 블록체인을 이용한다. 차량에 대한 데이터를 입력 후에 블록체인 네트워크에 등록하여 저장함으로써 위·변조가 불가능하여 차량 데이터에 대한 무결성을 제공한다. 하지만 차량 데이터를 최초 입력할 때 유효성 검증이 수반되지 않아 정보의 비대칭성을 해결하지만, 신뢰도의 문제점이 있다. 이는 판매자와 구매자 간 중고자동차 거래의 문제점인 허위매물은 방지하지 못한다.

본 논문에서 제안하는 모델은 차량에 대한 데이터를 발행기관으로부터 검증받은 후 등록한다. 구매자가 구매하고자 하는 차량이 판매자가 등록한 매물이 맞는지 차량 데이터의 변경이 없는지 proof 항목으로 검증한다. 판매자는 인증 과정을 거친 후 차량 데이터를 등록하는 시점과 등록한 후 모두 무결성과 신뢰성을 보장하여 중고자동차의 허위매물을 방지한다. 안병태[17]와 제안 모델의 비교는 Table 2와 같다.

Table 2에서 안병태[17]는 데이터가 분산화되어 있으며 무결성과 가용성을 제공한다. 그리고 차량 판매자와 구매자 간 정보의 비대칭성을 해결하고 차량 거래 시 이더리움 기반 스마트 컨트랙트를 이용하여 수수료 절감 효과가 있다. 그러나 차량 매물을 등록하기 전에 차량 데이터에 대한 유효성 검증과 판매자의 인증이 없다. 이는 검증되지 않은 데이터를 누구나 판매자가 되어 매물 등록이 가능하며, 결과적으로 허위매물을 막을

수 없다.

제안하는 모델은 차량 매물을 등록할 때 차량 데이터에 대한 유효성 검증과 판매자의 인증 과정을 거친 후 등록한다. 제안 모델은 DID를 위해 분산저장소를 이용하고, 차량 데이터에 대한 무결성과 가용성을 제공한다. 이는 차량 판매자와 구매자 간 정보의 비대칭성을 해결하고 허위매물을 방지한다. 차량 거래 시에는 딜러와 같은 제3 자의 개입이 없고, Chain Code를 이용한 스마트 컨트랙트 거래로 수수료 절감 효과가 있다.

Table 2. A comparison between the existing system and the proposed model

Classification	Blockchain	DID
Validation before data input	X	O
Decentralized	O	O
Integrity	O	O
Availability	O	O
Authentication	X	O
Smart contract	O	O
To resolve information asymmetry	O	O
Possibility of false car data	O	X
Transaction fee	Lowness	Lowness

5. 결론

중고자동차 거래에 있어 신뢰도는 무엇보다 중요하다. 온라인 시장의 발전과 이용자의 증가로 인해 정보를 쉽게 얻을 수 있는 만큼 허위광고와 허위매물의 문제점이 있다. 중고자동차 거래의 신뢰성을 높이고 정보의 비대칭성을 해결하기 위해 블록체인을 이용한 중고자동차 안전 거래 시스템이 있다. 블록체인 기반의 중고자동차 거래 시스템은 차량 데이터를 블록체인 네트워크에 등록한 뒤에는 무결성을 보장해 주지만 차량 데이터를 최초 등록 시 허위로 등록할 수 있다는 치명적인 문제점이 있었다. 본 논문에서는 정보의 비대칭성과 허위매물 등의 문제점을 해결하기 위해 DID를 적용하였다. 차량 데이터를 최초 등록 시에도 발행기관으로부터 발급받은 신뢰 있는 데이터를 등록함으로써 허위매물을 방지하고 DID Auth와 Proof 항목으로 인증과

무결성을 보장하였다. 제안 모델은 차량 데이터에 대해 누구나 열람이 가능하고 검증할 수 있어 정보의 비대칭성을 해결하였다. 판매자는 차량 데이터를 직접 소유함으로써 데이터에 대한 자기 주권을 실현하며, 분산원장 기술로 네트워크 어느 한 곳에 장애가 일어나도 가용성 문제를 해결할 수 있다. 향후 연구로는 실제 스마트 계약을 위한 시스템과 전반적인 중고자동차 거래를 위한 플랫폼 구축이 필요하다.

REFERENCES

- [1] G. Y. Park & S. I. Kim. (2021). A Study on User Experience of the Security in Online Trading of used goods -Focused on Danggeun Market and Bungae Jangter-. *Journal of Digital Convergence*, 19(7), 313-318.
DOI : 10.14400/JDC.2021.19.7.313
- [2] S. P. Kim. (2021). A Study on the User Structure Analysis of Second Hand Market Apps -Focusing on Joongonara, Bungaejangter, Danggeunmarket-. *Journal of the Korea Academia-Industrial cooperation Society*, 22(7), 449-458.
- [3] H. S. Byeon. (2017). A Convergent Perspective on Preference Attributes by Purchase Channel Choosing Used Cars. *Journal of the Korea Convergence Society*, 8(3), 215-223.
DOI : 10.15207/JKCS.2017.8.3.215
- [4] Y. M. Kim. (2021). *The endless "semiconductor chaos"... "Self-production"*. KBS(Online).
<https://news.kbs.co.kr/news/view.do?ncd=5309056>
- [5] J. W. Lee. (2021). Semiconductor chaos for vehicles 3 causes. TechDaily(Online).
<http://www.techdaily.co.kr/news/articleView.html?idxno=10358>
- [6] G. A. Akerlof. (1970). The Market for 'Lemon': Qualitative Uncertainty and the Market Mechanism. *Quarterly Journal of Economics*, 84(3), 488-500.
- [7] Statistics KOREA Government. (2021). *Car registration status*(Online).
https://www.index.go.kr/potal/main/EachDtlPageDetail.do?idx_cd=1257
- [8] J. W. Oh & J. K. Choi. (2014). Used Car Market - W10 Trillion Potential. *KTB Investment & Securities Report*.
- [9] S. S. Han & J. K. Jun. (2017). Determinants of Price Premium and Inventory Period of Imported Used Cars on the Online-Offline Linked Sales

Platform. *Global e-Business Association*, 18(4), 37-50.

DOI : 10.20462/TeBS.2017.08.18.4.37

- [10] J. W. Yang. (2020). Current status and challenges of the used car market. *KATECH*, Vol. 49.
- [11] S. C. Lee. (2009). Trust Building of Buyers Who Perceive Quality Risk High in Online Used Car Transactions: A Dyadic Trust Relationship. *Journal of Distribution Science*, 7(3), 49-69.
- [12] K. M. Kim. (2021). *Used car market...Popularity due to online activation due to delayed release of new cars*. MKeconomy(Online). https://n.news.naver.com/article/024/0000071969?cde=news_edit
- [13] H. W. Kwon. (2021). *I can't trust the seller. 55% of used car transactions in Korea are sold between the parties*. YNA(Online). <https://www.yna.co.kr/view/AKR2021102507940003>
- [14] KAMA. (2021). *Of the 2.51 million used car transactions in 2020, 54.7% were between the parties*(Online). http://www.kama.or.kr/BoardController?cmd=V&boardmaster_id=Bodo&board_id=554&menunum=0002&searchGubun=&searchValue=&pagenum=4
- [15] S. G. Hwang. (2021). Structural improvement is needed to advance the used car market. *The Korea Transport Institute*, Vol. 275.
- [16] B. K. Lee. (2020). *According to a survey of 31 used car sites, 95% of them were for sale*. Hankookilbo(Online). <https://www.hankookilbo.com/News/Read/A2020072709040004091>
- [17] B. T. Ahn. (2020). Construction for Safe Transaction System using Blockchain Technology(Case:Used Car). *Journal of Digital Convergence*, 18(4), 237-242.
DOI : 10.14400/JDC.2020.18.4.237
- [18] U. H. Kim, M. J. Kim, T. Y. Kim & J. G. Hong. (2018). Used Car Trading Platform Using Block Chain and Smart Contract. *Korean Institute of Information Technology*, 76-79.
- [19] H. Y. Kim, C. Y. Gwak, D. B. Yoon & S. S. Shin. (2021). A Used Car Trading Model Based on DID. *The Korean Institute of Information Technology*.

김 호 윤(Ho-Yoon Kim) [정회원]



- 2021년 2월 : 동명대학교 정보보호학과 (공학사)
- 2021년 3월 ~ 현재 : 동명대학교 컴퓨터미디어공학과 석사과정
- 관심분야 : Blockchain, DID, 암호 프로토콜, IoT
- E-Mail : miask376@gmail.com

한 군 희(Kun-Hee Han) [종신회원]



- 2001년 3월 ~ 현재 : 백석대학교 컴퓨터공학부 교수
- 관심분야 : 멀티미디어, 유비쿼터스, DB보안, 암호 프로토콜/알고리즘
- E-Mail: hankh@bu.ac.kr

신 승 수(Seung-Soo Shin) [정회원]



- 2001년 2월 : 충북대학교 수학과 (이학박사)
- 2004년 8월 : 충북대학교 컴퓨터공학과(공학박사)
- 2005년 3월 ~ 현재 : 동명대학교 소프트웨어융합보안학과 교수

- 관심분야 : 암호프로토콜, 네트워크 보안, U-헬스케어, IoT, 데이터분석
- E-Mail : shinss@tu.ac.kr