

# 차량 네트워크에 적용한 블록체인 기반 평판 시스템에 관한 분석

이수진\*, 김에영\*\*, 서승현\*

\*한양대학교 전자공학과

\*\*한양대학교 공학기술연구소

e-mail:tssn195@hanyang.ac.kr

## Analysis of Blockchain-based Reputation Systems in Vehicular Network

Soojin Lee\*, Aeyoung Kim\*\*, Seung-Hyun Seo\*

\*Dept of Electronic Engineering, Hanyang University

\*\*Research Institute of Engineering & Technology, Hanyang University

요 약

차량 포그 컴퓨팅 및 자율주행 자동차 개발 기술이 발전하면서 자동차 내부에 탑재된 IoT 센서들은 교통 정보 관련 다양한 정보를 수집할 수 있게 되었고, 더불어 자동차와 자동차간, 차량과 교통 인프라 간의 통신을 통해 수집된 교통 정보의 공유가 가능해졌다. 그러나 이 과정에서 알지 못하는 차량으로부터 받은 메시지를 어떻게 신뢰할 수 있는지에 대한 문제가 존재한다. 이를 보완하기 위해 평판 시스템을 적용한 연구들이 있으나 여전히 불안정한 데이터 저장방식과 통신 트래픽 문제가 존재한다. 이를 해결하기 위해 블록체인 기술을 사용된다. 본고에서는 블록체인 기반의 차량 네트워크의 평판 시스템 연구 사례를 분석한다.

### 1. 서론

통신 네트워크와 자율 주행 자동차 기술이 발전하면서 도로위의 차량들은 단순한 이동수단을 넘어서 연산과 센싱 능력을 지닌 하나의 컴퓨터로서의 역할을 하게 되었다. 자율 주행 자동차는 그 안에 탑재된 IoT 센서들을 통해 도로에서 발생하는 교통 정보, 주변 환경 정보 수집할 수 있는 기능을 가지고 있다. 또한 지능형 교통체제(Intelligent Transport System: ITS)[1]를 기반으로 차량 엣지 컴퓨팅(Vehicular Edge Computing)[2] 기술을 이용하여 차량과 차량 혹은 차량과 Roadside Units(RSU)간의 통신 환경이 마련되면서 차량과 RSU는 교통상황 및 사고 정보들을 수시로 공유할 수 있게 되었다. 차량들은 주변 차량으로부터 전달받은 교통 혼잡정도, 사고발생, 날씨, 그리고 도로 상태 등의 정보를 바탕으로 안전하고 효율적인 도로 주행이 가능하다[3].

그러나 차량 간의 통신 과정에서 악의적인 차량이 존재할 경우, 자신의 특정 목적을 위해 고의적으로 잘못된 정보를 전달할 가능성이 있다. 악의적인 차량은 실제 사고가 발생했을 때, 도로가 안전하다는 거짓 메시지를 보내거나,

반대로 거짓 사고발생 메시지를 생성하여 교통의 혼란을 일으킨다. 악의적인 차량의 공격을 방지하기 위해서는 송신 차량의 메시지의 신뢰성을 판단하는 근거로써 차량 평판 시스템이 필요하다. 차량의 평판 점수에 따라 악의적인 차량과 정직한 차량을 구분가능하다. 이에 따라 최근까지 차량 네트워크에서 차량 평판 시스템을 적용한 연구들이 등장하고 있다[4]-[9].

대부분의 기존 연구들은 중앙 기관에 데이터베이스를 두어 일괄적으로 차량 평판을 관리하거나 차량의 이동성을 고려하여 RSU를 통해 차량 평판 정보를 분산하여 저장하였다. 그러나 중앙 기관을 이용하는 경우, 통신 트래픽의 과부하가 발생해 실시간 서비스 제공이 어렵다. 분산된 차량 평판 테이블을 적용한 연구 사례의 경우, 분산되어 위치한 모든 제 3자 노드들이 실시간으로 업데이트되는 평판 정보에 대해 위조되지 않고 동일한 정보를 갖는 것은 한계가 있다. 다행히도 분산된 원장의 무결성과 일관성을 만족하는 블록체인[10]의 특성을 이용하면 본 문제점들을 해결할 수 있다.

본 논문에서는 차량 네트워크에서 블록체인 기술을 기반으로 차량 평판시스템을 제안한 연구 사례들을 비교 분석한다. 블록체인을 적용함으로써 갖는 장점과 여전히 발견되는 한계점에 대해 설명한다. 또한 이를 분석하여 앞으로 나아가야 할 연구 방향에 대해 논의한다.

본 논문의 구성은 다음과 같다. 2장에서는 차량 네트워크에서 블록체인을 기반으로 구축한 평판 시스템 연구 사

이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No.2018R1A2B6006903). 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2018-0-01417).

례에 대해 설명한다. 3장은 연구 사례들을 비교하여 분석하고 4장에서 결론을 다룬다.

## 2. 차량 네트워크에 적용한 블록체인 기반 평판 시스템 연구 사례

이 장에서는 블록체인 기반 차량 평판 시스템 연구 사례들을 소개한다. 블록체인 기반 차량 평판 시스템은 블록을 채굴하는 노드 종류에 따라 크게 차량이 채굴자인 경우, RSU가 채굴자인 경우, 그리고 차량과 RSU가 채굴자인 경우로 나눌 수 있다. 본 장에서는 각 경우의 연구 사례를 소개하고 한계점을 분석한다.

### 2.1 차량이 채굴자인 경우

Zhe Yang[11]이 제안하는 평판 시스템은 차량들은 다른 차량으로부터 메시지를 받으면 주변 환경에 대한 지식을 토대로 해당 메시지의 신뢰 여부를 투표한다. 각 메시지에 대한 차량들의 투표 결과는 블록에 저장된다. 이 때 차량의 센싱 능력이 높을수록 올바른 판단을 할 확률이 높기 때문에 작업증명을 선택하여 블록을 생성할 차량을 결정한다. 차량들은 블록에 저장된 내용을 토대로 다른 차량의 평판을 계산한다. 블록체인을 통해 평판 정보의 무결성과 일관성을 만족하지만 일부 계산능력이 높은 차량들이 집중적으로 블록을 채굴하기 때문에 완전한 분산화를 이루지 못한다. 또한 계산 능력이 높은 악의적인 차량이 채굴자로 선택된다면, 거짓된 투표 정보가 블록에 올라가거나 특정 차량의 표를 거부할 가능성이 있다.

Zhaojun Lu[12]는 블록체인 기반의 익명 평판 시스템(blockchain-based anonymous reputation system: BARS)을 제안하였다. 공개키를 가명으로 사용해 차량의 프라이버시를 보호한다. 목적에 따라 세 가지의 블록체인을 운영하는데 그 중 하나인 MesBC (Blockchain for Messages)는 차량이 전달한 모든 메시지를 기록하여 평판 평가에 사용한다. 그 외에 CerBC (Blockchain for Certificates)와 RevBC (Blockchain for Revoked Public Keys)는 각각 공인 인증서와 공개키를 기록한다. 차량의 평판 점수는 발생한 메시지의 중요도, 연속적으로 해당 메시지를 보낸 차량의 수, 메시지를 받은 차량의 수를 고려하여 평가한다. 공인인증서 내용에는 차량의 평판 점수를 포함하며 차량의 평판 점수는 새로운 인증서가 발급될 때마다 업데이트된다. 이 시스템은 인증서와 공개키를 발급하는 과정과 트랜잭션을 검증하는 과정에서 신뢰할 수 있는 기관들과 RSU에 의존한다. 또한 차량이 작업증명을 적용하여 채굴을 하므로 Zhe Yang[11]와 마찬가지로 완전한 분산화를 이루는데 한계가 있다.

### 2.2 RSU가 채굴자인 경우

Zhe Yang[13]는 RSU가 차량의 평판 값을 업데이트하고 차량들에게 제공하는 분산화된 신뢰 측정 방법을 제안했

다. 차량들은 주변에 위치한 이웃 차량들에게 받은 메시지들을 차량 들 간의 거리와 차량들의 평판에 따라 신뢰도를 계산하고 메시지의 신뢰여부를 투표한다. 그 투표 내용은 RSU에 업로드되고 RSU는 이를 토대로 차량의 평판을 계산하고 블록에 올린다. RSU는 고정적인 위치에서 블록을 채굴하므로 차량이 채굴자인 경우보다 블록의 전달과 원장의 동기화가 효율적이다. 그러나 차량이 다른 차량의 평판 점수를 알기 위해서는 RSU에 요청해야 하므로 완전한 분산화를 이룬 시스템으로 보기 어렵다. 또한 악의적인 RSU가 의도적으로 원하는 메시지만 선택하여 블록에 올릴 수 있다.

Jiawen Kang[14]는 안전하게 채굴자를 선정하기 위한 이-단계 소프트웨어 보안 개선 기법(two-stage soft security enhancement scheme)을 제안했다. Zhe Yang[13]은 차량에 대한 평판을 계산하였으나 이 논문은 RSU에 대한 평판을 차량들이 평가한다. 차량들은 RSU와의 과거 교류 내용과 다른 차량의 의견을 근거로 RSU의 신뢰도를 평가하고 채굴자로 투표한다. 가장 많은 득표를 한 RSU가 다음 블록을 채굴한다. 블록에는 차량의 데이터 공유 내용과 차량들이 제공한 RSU에 대한 평판 정보가 저장한다. 이에 따라 악의적인 RSU가 블록을 생성할 가능성이 줄어들었다. 그러나 차량이 직접적으로 블록에 접근할 수 없어 필요한 정보를 요청할 때 RSU에 의존해야 한다. 그리고 차량들이 데이터를 공유할 때, 어떻게 잘못된 정보를 구분할 수 있는지에 대한 방법은 언급하지 않았다.

### 2.3 차량과 RSU가 채굴자인 경우

Farah Kandah[15]에서는 멀티-계층 블록체인 구조의 Global Trustworthy System을 제안했다. 전체 시스템 구조는 크게 특정 영역에 위치한 차량들이 노드로 참여하는 platoon 블록체인과 RSU가 참여하는 global 블록체인으로 나눌 수 있다. platoon 블록체인은 특정 그룹의 차량의 신뢰값을 저장한다. 차량의 높은 이동성을 고려하고 악의적인 차량의 채굴을 막기 위해 trust-bidding 시스템을 채굴자 선정에 적용했다. 차량들은 자신들의 신뢰값을 제시하고, 가장 높은 값을 제시한 차량이 채굴자가 된다. global 블록체인에서는 작업증명을 통해 블록을 생성할 RSU를 선정한다. 채굴을 맡는 RSU는 여러 platoon 블록체인을 받아서 블록에 저장한다. platoon 블록체인이 블록에 올라가면 platoon 블록체인의 채굴자는 이전 블록의 해쉬값을 모르므로 첫 번째 블록부터 다시 채굴을 한다.

차량 평판을 알기 위해 RSU와 통신하면서 생기는 오버헤드 문제를 해결하고 차량들은 모든 신뢰 내용을 저장하지 않아도 된다. 그러나 Global Trustworthy System[15]는 특정 구역에서 만나는 차량들의 평판을 계산하는 구체적인 방안을 제시하지 않았다. 또한 platoon 블록체인의 경우, 좁은 범위에서 블록체인 네트워크를 이루므로 해당 그룹에서 악의적인 차량들이 전체 노드의 과반수가 될 확률이 높다. 또한 이전의 차량 행동을 알기 위해서는 RSU

<표 1> 연구 사례 비교

	[11]	[12]	[13]	[14]	[15]
채굴자	차량		RSU		차량, RSU
제안 시스템	Decentralized Reputation System	Blockchain-based anonymous reputation system(BARS)	Decentralized Trust Management Scheme	Two-stage Soft Security Enhancement Solution	Global Trustworthy System
운영 블록체인	Rating Blockchain	MesBC, CerBC, RevBC	Trust Blockchain	Vehicular Blockchain	Platoon Blockchain, Global Blockchain
차량의 평판 정보 접근성	직접적 접근 가능		간접적 접근 가능		특정 시간 내에 일부 블록에 대해 직접적 접근 가능, 이 외는 간접적 접근 가능
합의 알고리즘	PoW		Joint PoW and PoS	reputation-based voting scheme	trust-bidding system(Platoon Blockchain), PoW(Global Blockchain)
블록체인에 저장하는 정보	메시지에 대한 투표내역	공인인증서, 공개키, 차량 평판 점수, 공유된 메시지 내역	차량의 평판 정보 list	RSU에 대한 평판 의견, 데이터 공유기록	차량의 신뢰 요소(trust factor)

에 정보를 요청해야한다. RSU가 악의적인 목적을 가지고 위조된 정보를 주더라도 차량들은 알 수 없다.

**3. 연구 사례 비교분석**

<표 1>은 2장에서 언급한 연구들을 각 주요 특징별로 비교한다. 차량의 평판 정보 접근성 항목을 보면 다른 분류와 다르게 블록체인의 채굴자가 차량인 경우, 차량이 평판 정보를 직접적으로 접근한다. 따라서 차량이 접근한 평판 정보는 신뢰가능하고 다른 객체의 도움 없이 메시지의 신뢰여부를 결정한다. 단, Zhaojun Lu[12]는 차량의 프라이버시 보호를 하기 때문에 다른 차량의 신원과 평판 정보를 매핑할 수 없다. 반면 RSU가 채굴자인 경우, 차량이 RSU가 전달한 블록의 내용을 검증할 수 없어 위조된 평판 정보를 받을 가능성이 있으며 한 지역에 차량이 많을 경우, RSU와의 통신 오버헤드로 인해 실시간 정보 제공이 어렵다. Farah Kandah[15]는 이 둘을 결합한 이-계층(two-layer) 블록체인을 통해 해당 단점을 보완했다.

[11],[12]는 계산능력이 높은 차량의 정보가 신뢰도가 높다는 가정 아래, 합의 알고리즘으로 작업증명을 이용했다. Zhe Yang[13]의 경우, RSU를 항상 신뢰할 수 있는 노드로 고려하며 신뢰도와 상관없이 블록의 정보량과 RSU의 계산능력에 따라 채굴자를 선택한다. 따라서 채굴자 선출에서도 평판을 적용한 합의 알고리즘을 제안한 [14],[15]은 [11]-[13]보다 악의적인 채굴자의 공격에 안전하다.

대다수 사례들은 블록체인의 차량 평판 관련 정보를 저장하지만 Jiawen Kang[14]은 RSU의 평판 의견을 블록에

저장하는 차이가 있다. Zhaojun Lu[12]의 경우, 공개키 정보 관리도 고려하여 블록 내용을 구성했다.

**4. 결론**

블록체인을 적용한 차량 평판 시스템 연구들은 블록체인을 통해 차량 평판 정보 혹은 평판 투표 내용을 안전하게 보관한다. 또한 [14],[15]처럼 합의 알고리즘에 후보 채굴자의 신뢰점수를 고려하여 보다 안전한 채굴자 선정 방법을 제안하기도 하였다. 그러나 차량이 채굴을 하는 경우, 계산능력이 높은 악의적인 차량에 의해 잘못된 정보가 올라갈 가능성이 있다. 또한 RSU와 같은 다른 객체가 참여하는 경우, 완전한 분산화를 만족하지 않으며, 해당 객체의 신뢰 문제가 발생한다. 이를 해결하기 위해서는 차량이 다른 노드의 도움 없이 직접 블록체인에 접근할 수 있어야 하며, 동시에 효율적으로 블록정보를 저장하는 방안이 연구되어야 한다. 또한 추가적으로 차량 네트워크 특성상 장소의 이동이 잦으므로 이를 고려한 유동적인 블록체인을 구상하는 연구가 필요하다.

**참고문헌**

[1] J. Zhang, F. Wang, K. Wang, W. Lin, X. Xu, C Chen, "Data-Driven Intelligent Transportation Systems: A Survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, 2011  
 [2] X. Hou, Y. Li, M. Chen, D. Wu, D. Jin, S. Chen,

- “Vehicular Fog Computing: A Viewpoint of Vehicles as the Infrastructures,” *IEEE Transactions on Vehicular Technology*, vol. 65, 2016
- [3] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, Y. Zhang, “Blockchain for secure and efficient data sharing in vehicular Edge computing and networks,” *IEEE Internet Things J.* 2019.
- [4] G. Serne, “A Reputation Agent Model for Reliable Vehicle-to-Vehicle Information,” *19th Workshop “From Objects to Agents”*, vol. 2215, 2018, Pages 33-38.
- [5] G. Costantino, F. Martinelli, I. Matteucci, A. Bertolino, A. Calabro, and E. Marchetti, “CARS: Context Aware Reputation Systems to Evaluate Vehicles’ Behaviour,” *2018 26th Euromicro International Conference on Parallel, Distributed and Network-based Processing(PDP)*, Mar. 2018, pp. 446 - 453.
- [6] M. A. Azad, S. Bag, S. Parkinson, F. Hao, “TrustVote: Privacy-preserving Node Ranking in Vehicular Networks,” *IEEE internet of Things Journal*, 2018
- [7] M. A. Javed, S. Zeadally, Z. Hamid, “Trust-based security adaptation mechanism for Vehicular Sensor Networks,” *Computer Networks*, vol. 137, 2018
- [8] M. Javed, S. Zeadally, “RepGuide: Reputation-Based Route Guidance Using Internet of Vehicles,” *IEEE Communications Standards Magazine*, vol. 2, 2018
- [9] Z. Tian, X. Gao, S. Su, J. Qiu, X. Du, M. Guizani, “Evaluating Reputation Management Schemes of Internet of Vehicles based on Evolutionary Game Theory,” 2019
- [10] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
- [11] Z. Yang, K. Zheng, K. Yang, and V. C. M. Leung, “A blockchain-based reputation system for data credibility assessment in vehicular networks,” *IEEE 2017 Annual International Symposium on Personal, Indoor, and Mobile Radio Communication (PIMRC)*, Montreal, Canada, Oct. 2017, pp. 1-5.
- [12] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, “A privacy-preserving trust model based on blockchain for VANETs,” *IEEE Access*, vol. 6, pp. 45655 - 45664, 2018.
- [13] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. Leung, “Blockchain-based decentralized trust management in vehicular networks,” *IEEE Internet of Things Journal*, 2018.
- [14] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao. “Towards secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory.” 2018.
- [15] F. Kandah, B. Huber, A. Skjellum and A. Altarawneh, “A Blockchain-based Trust Management Approach for Connected Autonomous Vehicles in Smart Cities,” *2019 IEEE 9<sup>th</sup> Annual Computing and Communication Workshop and Conference(CCWC)*