Blockchain-based Decentralized Incentive Mechanism for Trusted Data Management on Internet of Vehicle

Muhammad Firdaus* and Kyung-Hyune Rhee**

*Department of Artificial Intelligence Convergence
Pukyong National University
**Department of IT Convergence and Application Engineering
Pukyong National University
e-mail: mfirdaus@pukyong.ac.kr, khrhee@pknu.ac.kr

Abstract

The Internet of Vehicles (IoV), which combines smart vehicles and the internet, has emerged to enhance traffic safety and efficiency. Moreover, it also is promoted to advance the future of intelligent transportation system (ITS) applications. However, The existing IoV is still facing challenges in providing a trusted management system and information security protection. Hence the participant's vehicle may be unwilling to share their data since the transaction system still relies on a centralized server approach with the potential risk of data leakage and privacy security. Also, vehicles have difficulty evaluating the credibility of the messages they received because of untrusted environments. To address these challenges, we propose consortium blockchain and smart contracts to accomplish a decentralized trusted data sharing management system in IoV. This system allows vehicles to validate the credibility of messages from their neighboring by generating a reputation rating. Moreover, the incentive mechanism is utilized to trigger the vehicles to store and share their data honestly; thus, they will obtain certain rewards from the system.

1. Introduction

The IoV allows vehicles to share road-related information messages with their neighbors, e.g., road conditions, traffic congestions, accident information, and safety warnings. Consequently, vehicles can be more aware of traffic situations, as well as contribute to improving the system transportation safety and efficiency [1]. However, the conventional architecture of IoV with a centralized approach has crucial challenges related to user's data security and privacy. In this sense, the potential exposure of user information with Single Point of Failure (SPoF) challenges still will reasonably occur since the IoV framework's data is centralized on a central server. Hence, the IoV network participants might be hesitant in the data sharing process that contains private information such as customer identities, vehicle numbers, and driving preference. Moreover, the risk of selfish behaviors might diminish participants' enthusiasm to cooperate with each other in the system. This problem becomes more serious when there exists a malicious vehicle in the network. The various adversarial actions may threaten the privacy security to gather the user's private information for personal benefit as well as endanger traffic safety and efficiency by giving the incorrect report to the system.

In order to address these issues, in this paper, we utilize a consortium blockchain and leverage the smart contracts to develop a decentralized trusted data sharing management system in IoV. Moreover, we propose an appropriate incentive mechanism based on the vehicle's contribution by leveraging smart contracts' self-execution nature. This scheme aims to motivate vehicles to participate positively in maintaining trusted data sharing activities and ensuring the system's security and sustainability.

The rest of this paper is organized as follows: Section 2 describes problem definition based on traditional vehicular ad-hoc networks and centralized incentive mechanism. Then, we present the design architecture of the IoV-blockchain, including its detailed procedures in Section 3. We demonstrate the proposed design by analyzing security and evaluating performance in Section 4. Finally, Section 5 concludes this paper.

2. Background

2.1 Data Management in Vehicular Networks

In the vehicular networks (VNs) environment, the primary entities in the data sharing process are vehicles and roadside units (RSUs), which form two types of communication, namely vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I). Vehicles interact with other neighboring vehicles by using onboard units (OBUs) equipped with several sensing devices with simple computation and communication capabilities. OBUs are also used to automatically recognize traffic-related information and facilitate the vehicles to send notification messages to others using V2V communication standards to improve traffic safety and efficiency. On the other hand, V2I facilitates a single or multi-hop communication between vehicle and RSU, supported by dedicated short-range communication (DSRC) standards [2]. RSUs, as the roadside infrastructure, provide wireless communications along the road to vehicles. Thus, RSUs are prepared to aggregate the traffic data in a particular coverage area in the VN system.

2.2 Blockchain-based Incentive Mechanism

Previous work considers that vehicle may share their data voluntarily [3]. Unfortunately, it might cause the low participation of vehicles in the data sharing process and then affects the system's reliability in the future. Moreover, due to self-interest characteristics, vehicles may also be unenthusiastic to share the data because they do not obtain particular benefits or compensation from the system. Therefore, the incentive mechanism is aimed to motivate honest vehicle (as data owner) to give a relevant contribution with long term participation for system reliability and sustainability. Incentive mechanism provides rewards to the vehicles that contribute to the data sharing process to form the trusted data management system in IoV.

Blockchains have recently received increasing attention as a promising technology for providing distributed and secure solutions. They are open databases that guarantee data security by enabling anonymous and trustworthy transactions on an immutably distributed ledger without the help of a central intermediary [4]. Each transaction is recorded with a timestamp to be validated by the consensus mechanism before it is stored on a blockchain network. Moreover, by leveraging its smart contracts, blockchains have been utilized to form fairness incentives by providing a decentralized approach to overcome the risks of any single point of failure on a centralized incentive approach. Therefore, a decentralized incentive might effectively encourage user participation and contributions, creating a secure framework for users to share their data to improve system reliability and sustainability.

3. The Framework of IoV-Blockchain

This section explains our proposed model, blockchain-based secure and trusted data sharing management in IoV networks. Inspired by [5], our architecture model relies on consortium blockchain, as shown in Figure 1. In our scenario, vehicles represent the user network that communicates with other vehicles and RSUs, using V2V and V2I communication to improve traffic safety and efficiency. The sending vehicle (V_m) equipped with OBUs and their sensing devices automatically collect road-related messages (M_i) to the system, while the neighboring vehicle

(V_n) evaluate the message M_i by uploading the message credibility rating (R_i) to nearby RSU.

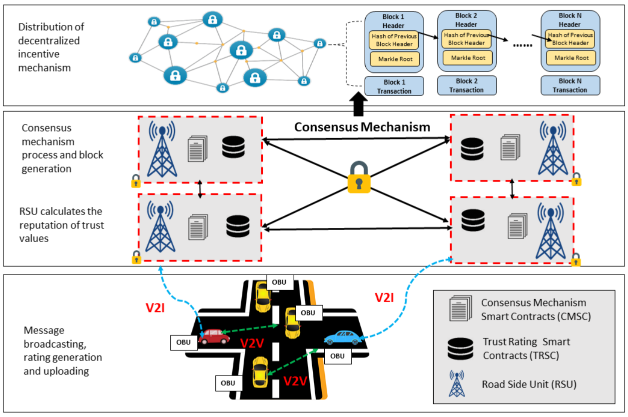

Figure 1. The framework of IoV–blockchain

Then, RSU as the roadside infrastructure and traffic handler, aggregate M_i based on R_i using the trust rating smart contract (TRSC) to generate the trust value rating of M_i (Tr_{M_i}). After that, Tr_{M_i} will be validated in the consensus mechanism smart contract (CMSC) using consensus mechanism. Here, only authorized RSUs are eligible to be the nodes participants in the consensus mechanism with more extensive storage and computation capability compared to the OBUs. Once the consensus process is finished, a new block is uploaded to the blockchain network. Thus, the distributed RSUs automatically obtain the log and authentication of block. V_m and V_n, which correctly provide the road-related message and assess the message credibility, respectively, will obtain the proportional incentive.

4. Simulation and Results

Using the OSMWebWizard package provided in the simulation of urban mobility (SUMO), we modeled a highway traffic scenario to prototype and evaluate IoV networks' efficiency. Here, a discrete-event network simulator is used to verify the result, analyzing a trace file for vehicle mobility and message credibility. We use an optimized link-state routing protocol (OLSR) as one of the protocol standards in the wireless access for the vehicular environments (WAVE). In this scenario, there are 26 vehicles in the user network layer.

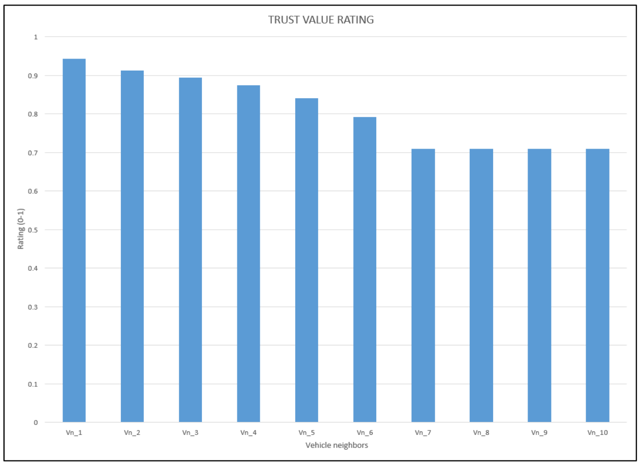

Figure 2. Trust value rating aggregation

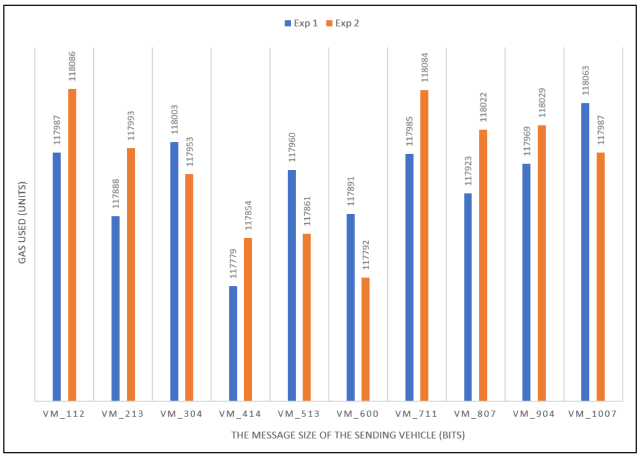

Figure 3. The information on gas usage by RSU

However, only 10 vehicles are proposed to be neighboring vehicles V_n and placed 50 meters apart from the occurred event. Once V_m broadcasts the road-related message M_i via V2V communication, V_n is allowed to evaluate the message credibility by generating the message rating to RSU. Figure 2 shows the trust value rating aggregation based on message credibility assessment over 10 V_n on various separations. The V_{n1} obtains the highest value of the message's credibility due to the nearest distance with M_i. Contrary, the V_{n10} obtains the lowest value of the message's credibility due to the fartest distance with M_i.

To support an adequate incentive for the information provider V_m, we implement Ethereum smart contracts as a decentralized and tamper-proof incentive mechanism. We utilize a smart contract feature in the Ethereum platform through Ganache Truffle (v.2.4.0) graphical user interface (GUI). Figure 3 illustrates the information on gas usage by RSU in distributing Ether for the contributed vehicles. Even though Figure 3 shows the amount of gas usage is significant from one another, the amount of gas difference between transactions is relatively the same by using units notion. Smart contracts store the address information of the requester and provider, while Ethereum network only stores arbitrary values of related information.

5. Conclusions

We have introduced a consortium blockchain and smart contracts to achieve a decentralized trust data management system in IoV. In this paper, smart contracts are exploited to accomplish efficiency, reliability, and secure data storage and sharing. Here, two smart contracts, TRSC and CMSC, are deployed on distributed RSUs to gather the trust value rating and conduct the consensus mechanism. Moreover, this framework permits vehicles to validate the credibility of messages from their neighboring vehicles by generating a reputation rating. Additionally, we utilize an incentive mechanism to motivate and propel the vehicle to contribute and sincerely share their data to obtain certain rewards from the system.

Acknowledgement

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2018R1D1A1B07048944) and partially was supported by the Republic of Korea's MSIT (Ministry of Science and ICT), under the High-Potential Individuals Global Training Program) (2020-0-01596) supervised by the IITP (Institute of Information and Communications Technology Planning & Evaluation).

[References]

[1] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE Internet of Things Journal, 6(2), 1495-1505.

[2] Kenney, J. B. (2011). Dedicated short-range communications (DSRC) standards in the United States. Proceedings of the IEEE, 99(7), 1162-1182.

[3] Xu, C., Wang, Y., Zhou, Z., Gu, B., Frascolla, V., & Mumtaz, S. (2018, December). A low-latency and massive-connectivity vehicular fog computing framework for 5G. In 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE.

[4] Firdaus, M., & Rhee, K. H. (2020). Empowering Blockchain For Secure Data Storing in Industrial IoT. In Proceedings of the Korea Information Processing Society Conference (pp. 231-234). Korea Information Processing Society.

[5] Firdaus, M., & Rhee, K. H. (2021). On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks. Applied Sciences, 11(1), 414.