Journal of The Korea Institute of Information Security & Cryptology
VOL.31, NO.5, Oct. 2021

ISSN 1598-3986(Print)
ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.5.889

분산형 접근 방식을 적용한 차량 인터넷에서 신뢰할수 있는 데이터 관리를 위한 인센티브 메커니즘 설계*

무함마드 필다우스,[1†] 이 경 현 [2‡]
[1]부경대학교 인공지능융합학과 (대학원생), [2]부경대학교 IT융합응용공학과 (교수)

An Incentive Mechanism Design for Trusted Data Management on Internet of Vehicle with Decentralized Approach*

Muhammad Firdaus,[1†] Kyung-Hyune Rhee[2‡]
[1]Dept. of Artificial Intelligence Convergence, Pukyong National University (Graduate student),
[2]Dept. of IT Convergence and Application Engineering, Pukyong National University (Professor)

요 약

본 논문은 블록체인 기술에서 탈중앙화된 시스템 접근 방식을 활용하여 차량 인터넷(IoV)에서 신뢰할 수 있는 데이터 공유 체계를 제안한다. 스마트 계약에 기초한 인센티브 메커니즘을 채택하여, 차량은 올바른 교통 정보 메시지를 정직하게 공유함으로써 시스템으로부터 특정한 보상을 받게 된다. 이후 차량은 평판 등급을 생성하여 수신되는 모든 정보 메세지를 검증함으로서 메시지에 대한 신뢰성을 유지한다. 한편 네트워크 성능을 분석하기 위해 이산 이벤트 시뮬레이터를 사용하여 IoT 네트워크를 시뮬레이션하였고, 인센티브 모델은 분산형 접근 방식의 이더리움 스마트 계약을 활용하여 설계하였다.

ABSTRACT

This paper proposes a reliable data sharing scheme on the internet of vehicles (IoV) by utilizing blockchain technology for constructing a decentralized system approach. In our model, to maintain the credibility of the information messages sent by the vehicles to the system, we propose a reputation rating mechanism, in which neighboring vehicles validate every received information message. Furthermore, we incorporate an incentive mechanism based on smart contracts, so that vehicles will get certain rewards from the system when they share correct traffic information messages. We simulated the IoV network using a discrete event simulator to analyze network performance, whereas the incentive model is designed by leveraging the smart contract available in the Ethereum platform.

Keywords: Blockchain, incentive mechanism, smart contract, IoV

I. Introduction

The concept of internet of vehicles (IoV) is supposed to form an essential component of the intelligent transportation system (ITS) in realizing the future of

Received(05. 24. 2021), Modified(07. 27. 2021), Accepted(07. 27. 2021)

* 본 연구는 과학기술정보통신부 및 정보통신기획평가원의 대학ICT연구센터육성지원사업의 연구결과로 수행되었음(IITP-2021-2020-0-01797) 일부는 2021년도 정부(교육부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(No. 2021R1I1A304659011)

* 본 논문은 2021년도 한국정보보호학회, 영남지부 학술대회에 발표한 우수논문을 개선 및 확장한 것임.

† 주저자, mfirdaus@pukyong.ac.kr

‡ 교신저자, khrhee@pknu.ac.kr (Corresponding author)

smart cities. IoV is designed to improve traffic safety, reduce road accidents, and conceive an efficient transportation system [1]. It enables vehicles to be longer cognizant of traffic situations by sharing road-related information messages with nearby vehicles, such as safety alerts, accident information, and traffic jams at specific times and locations.

Despite the above advantages, the traditional IoV framework, which is based on a centralized approach, has trouble addressing critical challenges associated with user data protection and privacy. In this context, where data management is centralized on a central server, the Single Point of Failure (SPoF) issues may cause the risk of user information being possibly exposed [2]. As a result, IoV network members could be reluctant to share data containing sensitive information, for instance, driving preferences, vehicle numbers, and user identities.

Furthermore, the risk of self-centered inclination may discourage participants' desire to work together in maintaining the IoV system. The problem shifts even worse when the malicious vehicle exists and conducts various adversarial activities, such as gathering the user's private information that endangers privacy protection for their profit and providing incorrect information messages to jeopardize traffic safety in the IoV network system.

This paper utilizes a decentralized approach of blockchain technology to tackle the drawback of a conventional data management system in IoV. We also leverage smart contracts to facilitate data sharing transactions among involved vehicles and form an appropriate incentive mechanism. The system enforces every vehicle to provide and share the correct message by allowing the nearby vehicles to validate every information message received by generating a reputation rating. Hence, vehicles will get certain rewards from the system if they honestly share correct traffic information messages. The rewards are obtained based on the vehicle's contribution; the more they share the correct message, the more they get the rewards. As a result, this incentive motivates vehicles to sustain data sharing activities correctly to form a trusted data management system in the IoV network.

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.

II. Background

2.1 Traditional Data Management System in Vehicular Networks

Vehicles and roadside units (RSUs) are the main nodes in the data sharing process in vehicular networks (VNs) environments. They communicate with each other by forming vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication. These two types of communications refer to dedicated short-range communication (DSRC) standards that facilitate single or multi-hop communication among VNs entities [3]. Vehicles have simple communication and computation capabilities supported by on-board units

(OBUs), consisting of various sensing devices. RSUs are stationed along the road, providing wireless communications from roadside infrastructure to vehicles and acting intermediaries between vehicles and a central server.

The data sharing process starts while vehicles automatically identify traffic-related events using their sensing devices and broadcast that information message to the network. All involved entities in the same coverage area of VNs receive the broadcasted information message from the vehicle sender. Then, RSUs manage data sharing transactions among vehicles and periodically store all transactions in the centralized server as a permanent data center. However, a centralized server still faces privacy and security risks, potentially revealing and stealing users′ sensitive data without considering approval from the user itself. In this regard, service providers might trade user data that arbitrarily use it for their benefit. Moreover, the attackers can easily manipulate the broadcasted data from the vehicle sender by utilizing an insecure wireless communication ecosystem. Further, SPoF problem will still occur in a centralized server, where a single failure possibly influences the whole system operation. Therefore, the future VNs must consider those centralized server shortcomings to facilitate a trusted data management system.

2.2 Conventional Incentive Mechanism

A voluntary-based data sharing process might cause vehicles′ poor enthusiasm because the system does not give appropriate compensation or benefits for the involved vehicles [4]. Moreover, they may likewise be uninterested in sharing their data due to the nature of self-centered inclination. Therefore, the incentive mechanism motivates vehicles as data owners to positively support the process of data sharing transactions in the VNs system. Thus, vehicles will get certain rewards from the system if they honestly share the correct traffic information messages.

The current incentive mechanism, for instance, reputation-based incentive [5] and monetary-based incentive [6], enables a trusted third party (TTP) and vehicles (members) to form simple transactions with a centralized approach. Here, TTP gives incentives to involved members in the data sharing transaction as well as keeps the whole data transaction in the centralized database server. In this sense, TTP controls the incentive scheme and the entire system orchestration with the absolute authority as a service provider. However, due to the risk SPoF and untrusted environment (including untrusted vehicles), VNs members could be reluctant to share data containing sensitive information, such as, driving preferences, vehicle numbers, and user identities. Therefore, privacy and security issues must be considered for the future VNs incentive mechanism in maintaining system reliability and sustainability with the long-term participation of the members.

2.3 Decentralized Trusted Data Management System

Since Nakamoto introduced Bitcoin in 2009 [7], leveraging blockchain technology for achieving secure and decentralized solutions has lately been gaining significant attention both from academia or industries. On the other hand, blockchain itself is an open database that guarantees data security by supporting trustworthy and anonymous transactions without requiring any intermediaries and its transaction recorded on the distributed and immutable ledger [8]. Here, all transactions are marked with a timestamp, and then a certain consensus mechanism validates and stores the verified transaction on the distributed database network. Hence, the system allows all involved participants in the blockchain network to obtain an updated ledger automatically. Moreover, blockchain-based smart contracts can be used to develop a fair incentive scheme with a decentralized approach to overcome the risks of a centralized incentive approach. Therefore, it could be one solution to effectively boost user contribution and participation to maintain the system safety and efficiency in a secure and trusted framework.

III. The Framework of IoV-Blockchain

This paper proposes a trusted data sharing management system by empowering blockchain technology in IoV networks with a decentralized approach. Refers to [9], our proposed model consists of three planes, i.e., vehicle network plane, blockchain edge plane, and blockchain network plane. Figure 1 illustrates the detailed architecture of our proposed model. The vehicle network plane provides communication among vehicles in data sharing transaction related to traffic conditions using V2V communication standard. This plane also manages vehicle registration, broadcasts the traffic information message, and evaluates the message correctness by generating a reputation rating [10]. The blockchain edge plane comprises distributed RSUs that perform as the traffic managers to handle the covered vehicle in a particular radius range using V2I standard communication. This plane plays a crucial responsibility to validate the entire data sharing transaction process in the system.

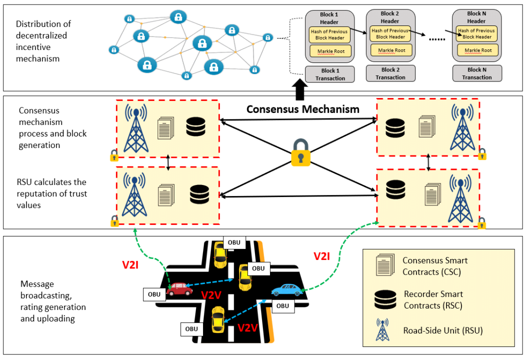

Distribution of decentralized incentive mechanism
Block 1 Header
Hash of Previous Block Header
Markle Root
Block 1 Transaction
Block 2 Header
Hash of Previous Block Header
Markle Root
Block 2 Transaction
....
Block N Header
Hash of Previous Block Header
Markle Root
Block N Transaction
Consensus mechanism process and block generation
Consensus Mechanism
RSU calculates the reputation of trust values
Message broadcasting, rating generation and uploading
V2I
V2I
OBU
OBU
OBU
OBU
OBU
V2V
V2V
Consensus Smart Contracts (CSC)
Recorder Smart Contracts (RSC)
Road-Side Unit (RSU)

Fig. 1. The framework of IoV-blockchain.

The blockchain network plane provides a decentralized incentive mechanism to motivate the participants to share their data in order to maintain the system's sustainability. Table 1 summarizes the notation used in this paper. The detailed

Table 1. Notation summary.

Symbol	Description
V_S	The sending vehicles
V_N	The neighboring vehicles
M_{V_S}	The traffic information messages
N_{V_N}	The message reputation rating
$T_{M_{V_S}}$	The trust value rating of M_{V_S}
RSC	The recorder smart contract
CSC	The consensus smart contract
$C_{M_{V_S}}$	The credibility of M_{V_S}
δ_i	The new block that already authenticated
Γ_{V_S}	The reward obtained by V_S
Γ_{V_N}	The reward obtained by V_N

model is explained as follows.

There are two types of vehicles in our scenario, i.e., the sending vehicles (V_S) and the neighboring vehicles (V_N). By using V2V and V2I communication standard, vehicles can communicate to improve traffic safety and efficiency with RSUs in the blockchain edge plane and other vehicles in the vehicle network plane. Before entering the IoV networks, all vehicles must be registered to TTP to be legitimate vehicles in access the system's service [11]. V_S automatically collect traffic information messages (M_{V_S}) using OBUs and broadcast it to the system, whereas V_N evaluates the credibility of the message ($C_{M_{V_s}}$) by the following calculation method.

$$C_{M_{V_s}} = \beta + M_{V_S} - \gamma . d \tag{1}$$

where M_{V_S} contains the specific time and location of the occurred event, $M_{V_S} = (Msg \| location \| time)$. We consider β and γ as two predefined values that control the lower bound and rate of $C_{M_{V_s}}$ refers to the distance (d) between V_S and M_{V_S}. Hence, regarding the scope of the message credibility, the main factor is the distance. The closer the distance of the vehicle from the center of information (or the location of where the event happens), the more it is considered credible. The credible messages generate a positive rating (+1); otherwise, a negative rating (-1).

Then, V_N uploads the result of message reputation rating (N_{V_N}) to the nearby RSU, which has the role as an edge-node infrastructure and traffic handler in the IoV environment. Subsequently, RSU aggregates the result using the recorder smart contract (RSC) to generate the trust value rating of M_{V_S} ($T_{M_{V_s}}$) by considering N_{V_N}. It is worth noting that $T_{M_{V_s}}$ is calculated based on the majority rule, assuming that malicious vehicles cannot control most of the vehicles in the network. Then, $T_{M_{V_s}}$ will be validated in the consensus smart contract (CSC) using the pre-agreed consensus mechanism. Here, a consensus mechanism is a set of rules that should ensure the agreement of the participating node is achieved to generate a new block, along with guarantees that all transactions are trustworthy in the blockchain system. Therefore, this paper considers the joint proof of stake (PoS) and practical byzantine fault tolerance (PBFT) algorithm that offer several advantages for our proposed model, including its efficiency, maturity, and consistency. PoS allows RSU with the more total value of $T_{M_{V_s}}$ to be a leader in PBFT algorithm. Further, PBFT algorithm permits the presence of anomalous nodes (f), where $f = (n-1)/3$, among the number of nodes (n) without harming the consensus result [12].

In our scenario, RSUs are considered the node participants who are eligible with more extensive capability on computation and storage to perform the consensus mechanism than OBUs. Once the consensus process has been completed, a new block (δ_i) is uploaded to the blockchain network plane. The structure of transaction block can be seen in Figure 2.

Consequently, the new block that

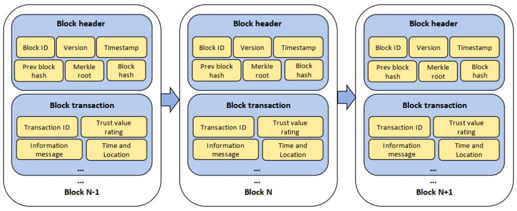


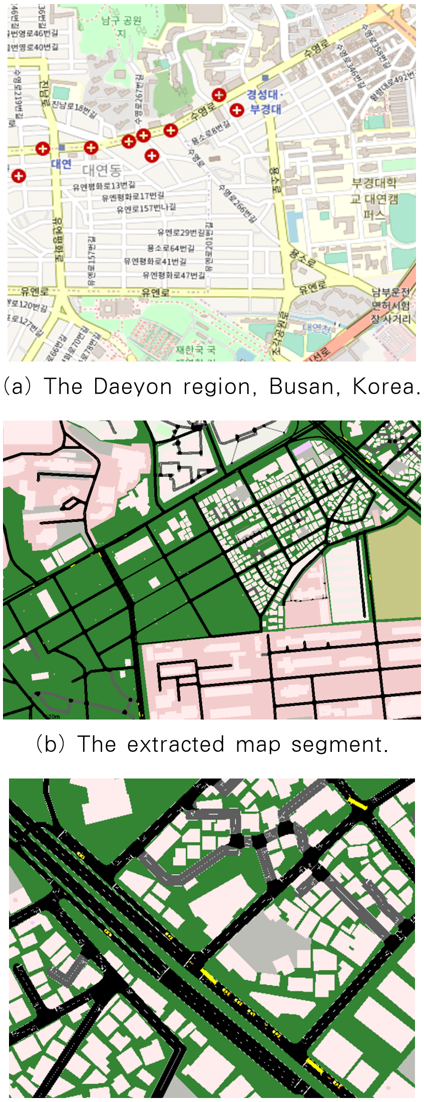
Fig. 2. The structure of transaction block [13].

already authenticated will automatically be updated to the distributed RSUs in the IoV network system. Thus, V_S and V_N will obtain an appropriate incentive as the reward (Γ_{V_i}) due to correctly providing the traffic information message and evaluate the message correctness, respectively. In addition, we also consider the punishment scheme to provide fairness and prevent several attacks from malicious vehicles. Hence, all vehicle participants that behave maliciously, e.g., V_S broadcasts fake information or V_N generates a dishonest rating, will be penalized by obtaining a low reputation from the system. Consequently, the malicious V_S cannot participate in data sharing or broadcasts M_{V_S}, whereas malicious V_N cannot generate reputation rating anymore through the network.

IV. Simulation and Results

We designed our proposed model into three simulations setting that dissimilar from one another, i.e., implementing IoV network, *RSC*, and *CSC*. Inspired by [13], we simulated the prototyped traffic scenario using the simulation of urban mobility (SUMO), supported by the provided package OSMWebWizard. Figure 3 shows the traffic scenario simulation of the Daeyon region, Busan, Korea. In order to evaluate IoV network performance in this scenario, we used the NS3 network simulator by analyzing and verifying the resulted mobility and trace file.

We consider implementing *CSC* using Hyperledger Sawtooth that represents our consensus smart contract. Hyperledger Sawtooth is a new member of the Hyperledger family. Here, Docker containers are utilized to manage blockchain application interface, smart



(a) The Daeyon region, Busan, Korea.

(b) The extracted map segment.

(c) Traffic in map segment (zoomed)

Fig. 3. Simulation scenario map.

contracts, and RSUs, representing Sawtooth REST servers, transaction processors, and validators, respectively.

We also prototyped RSC as an appropriate incentive mechanism using Ethereum smart contract, implemented by the Ganache CLI-Truffle-Suite interface. All numerical results were conducted on Oracle VM Virtual Box that installed Ubuntu 16.04, executed on computer Core(TM) i5-4690 CPU Intel(R), 16.00 GB RAM 3.50 GHz. An optimized link-state routing protocol (OLSR) is used to form an IoV network in this scenario. This protocol is one of the protocol standards that provide better performance in wireless access for vehicular environments (WAVE) [14]. Table 2 describes the detailed setting of simulation parameters, where there are the total of 26 vehicles with ten vehicles acts to be the neighboring vehicles V_N.

Using V2V communication, V_S broadcasts M_{V_S} to the IoV system. In contrast, V_N placed 50 meters apart and permitted to assess the message correctness by generating N_{V_N} to the nearby blockchain edge plane (i.e., RSUs). In terms of IoV network performance, we consider packet delivery ratio (PDR) as an essential parameter to be analyzed [15]. Figure 4 shows the trust value rating of M_{V_S} aggregated by RSC based on the uploaded N_{V_N} of the total 10 V_N in the various distance range. As the results, the highest value is obtained on the lowest distance (i.e. 50 meters) between M_{V_S} and the occurred event with 0.943 of $T_{M_{V_S}}$. Contrary, the lowest value is obtained on the highest distance (i.e. within the range of 350-500 meters) between M_{V_S} and the occurred event with 0.7096 of $T_{M_{V_S}}$. Therefore, these results show that the closer the distance of the vehicle from the center of information (or the location of where the event happens), the more it is considered credible.

Table 2. Simulation parameters of IoV-Blockchain

Parameter	Value
Number of vehicle	26
Number of V_N	10
The type of routing protocol	OLSR
MAC type	IEEE 802.11p
WAVE ITS band	5,9 GHz
Transmission rate	2.048 Kbps
Data rate	6 Mbps
Fading model	Nakagami fading
Propagation loss model	Two-ray ground
packet interval	100 ms
Power transmission	20 dBm
Channel bandwidth	10 MHz
Simulation time	100 s

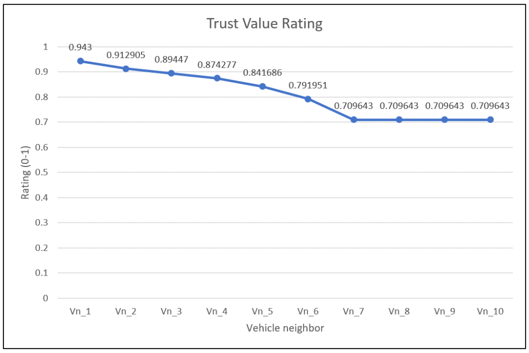


Fig. 4. Trust value rating aggregation of M_{V_S}

In addition, we consider message reception errors caused by overlapping between vehicle's authentication requests in the broadcast channel that influence the vehicular network's performance, e.g., increases delay authentication and decreases the total average of throughput. Figure 5 shows the result of vehicle

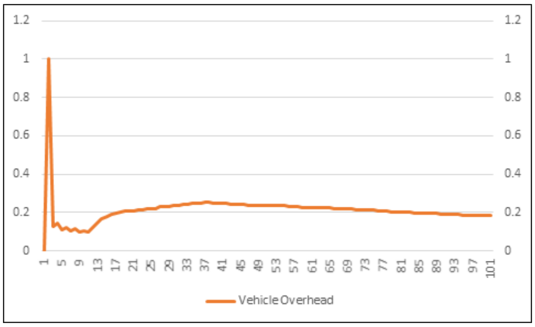


Fig. 5. The result of vehicle overhead

overhead in 100s simulation time. As pointed in the figure, we can see that after 17 s of simulation time, the overhead is nearly stable within the range of 0.2 to 0.25, and it even lightly reduces over time. In terms of vehicle overhead, the lower value indicates better performance of the system and vice versa. Our proposed protocol is relatively efficient based on the above results since it does not acquire a high overhead.

After $T_{M_{V_s}}$ is collected in RSC, then RSUs utilize CSC to perform the consensus mechanism by generating and storing the new block into distributed ledger blockchain network. We run multiple tests by changing batch size up to 100 tx/block to evaluate the effect of batch size on throughput. Here, batch size refers to the number of transactions involved in every block. As shown in Figure 6, the result shows that the throughput reaches 543 tx/sec at the total batch size of 100~tx/block. In this sense, the throughput is growing linearly across various batch sizes.

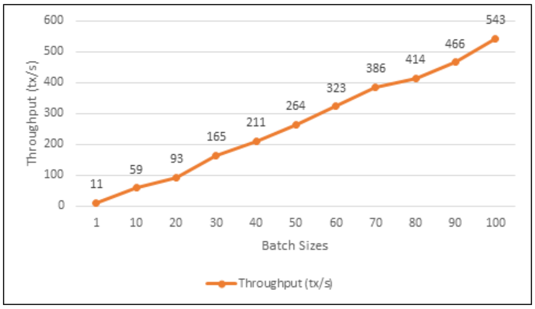
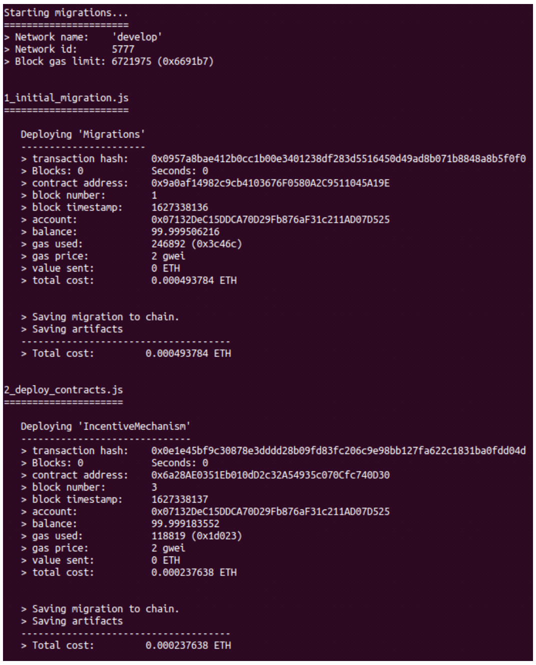


Fig. 6. Batch size vs throughput

Since Hyperledger Sawtooth supports an alliance with Ethereum platform [16], we develop a decentralized and tamper-proof incentive mechanism for the traffic information provider V_S based on Ethereum smart contract. We utilized Ganache Truffle (v.2.4.0) graphical user interface (GUI) as a smart contract feature in the Ethereum platform with gas limit setting was 6721975. Figure 7 shows the illustration of truffle migration function in our case. As shown in the figure, we can see that the initial migration need 246892 units gas with the total cost 0.000493784 Ether. On the other hand, 118819 units gas is used to deploy incentive mechanism contract, with total cost 0.000237638 Ether.


```
Starting migrations...
======================
> Network name:    'develop'
> Network id:      5777
> Block gas limit: 6721975 (0x6691b7)


1_initial_migration.js
======================

   Deploying 'Migrations'
   ----------------------
   > transaction hash:    0x0957a8bae412b0cc1b00e3401238df283d5516450d49ad8b071b8848a8b5f0f0
   > Blocks: 0            Seconds: 0
   > contract address:    0x9a0af14982c9cb4103676F0580A2C9511045A19E
   > block number:        1
   > block timestamp:     1627338136
   > account:             0x07132DeC15DDCA70D29Fb876aF31c211AD07D525
   > balance:             99.999506216
   > gas used:            246892 (0x3c46c)
   > gas price:           2 gwei
   > value sent:          0 ETH
   > total cost:          0.000493784 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:         0.000493784 ETH


2_deploy_contracts.js
=====================

   Deploying 'IncentiveMechanism'
   ------------------------------
   > transaction hash:    0x0e1e45bf9c30878e3dddd28b09fd83fc206c9e98bb127fa622c1831ba0fdd04d
   > Blocks: 0            Seconds: 0
   > contract address:    0x6a28AE0351Eb010dD2c32A54935c070Cfc740D30
   > block number:        3
   > block timestamp:     1627338137
   > account:             0x07132DeC15DDCA70D29Fb876aF31c211AD07D525
   > balance:             99.999183552
   > gas used:            118819 (0x1d023)
   > gas price:           2 gwei
   > value sent:          0 ETH
   > total cost:          0.000237638 ETH


   > Saving migration to chain.
   > Saving artifacts
   -------------------------------------
   > Total cost:         0.000237638 ETH
```

Fig. 7. Initial migration and deploying a contract

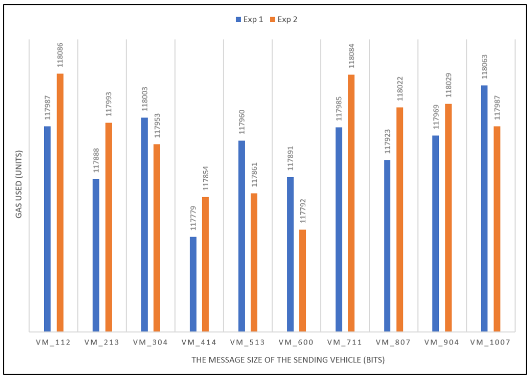


Fig. 8. The information on gas usage by RSU

After a new block is stored in the blockchain network, the system distributes Ether as a reward to the vehicles proportionally based on their recorded contribution in RSC. Figure 8 shows the information of Ether distribution and the total gas usage for the contributed V_S in data sharing transaction. Here, we conducted two experiments (Exp. 1 and Exp 2) to analyze the total number of gas usage units as the distributed rewards representation. As a result, the average gas usage to distribute incentive to V_S was 117944 units in Exp. 1 and 117966 units in Exp.2 based on the message size contribution recorded by RSC. The minimum gas usage in Exp.1 was 117772 units with 414 and 117792 units in Exp.2. Meanwhile, the maximum gas usage in Exp.1 was 118063 units and 118086 units in Exp.2.

V. Conclusion and Future Work

We have presented the model of blockchain-based trusted data management for IoV networks. Here, we use the blockchain and smart contracts to perform efficiency, reliability and enhance security and privacy in the data sharing transaction. RSC and CSC are two smart contracts deployed on distributed RSUs to gather the trust value rating and conduct the consensus mechanism. Moreover, this model allows vehicles to generate the message reputation rating after assessing the correctness of the received messages from their neighboring vehicles. In order to motivate vehicles to contribute to the data sharing transaction positively, we develop an appropriate incentive mechanism with a decentralized approach. Thus, vehicles will be interested in sharing their data to maintain safety and efficiency in IoV networks. Lastly, further studies are still required to apply the real-time mechanism by combining edge computing and artificial intelligence technology in the future IoV system.

References

[1] Yang, Zhe, et al, "Blockchain-based decentralized trust management in vehicular networks," IEEE Internet of Things Journal, 6(2), 1495-1505. 2018.

[2] Atzori, Marcella, "Blockchain Technology and Decentralized Governance: Is the State Still Necessary?," Available online: https://ssrn.com/abstract=2709713. (Accessed: 6 May 2021).

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

[4] Xu, Chen, et al, "A low-latency and massive-connectivity vehicular fog computing framework for 5G," 2018 IEEE Globecom Workshops (GC Wkshps) (pp. 1-6). IEEE. Dec. 2018.

[5] Jurca, Radu, and Boi Faltings, "An incentive compatible reputation mechanism," EEE International Conference

on E-Commerce, 2003. CEC 2003. (pp. 285-292). IEEE. June. 2003.

〔6〕 Peng, Dan, Fan Wu, and Guihai Chen, ″Pay as how well you do: A quality based incentive mechanism for crowdsensing,″ Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing (pp. 177-186). June. 2015.

〔7〕 Nakamoto, S, ″Bitcoin: A Peer-to-Peer Electronic Cash System,″ Available online: https://bitcoin.org/bitcoin.pdf. (Accessed on 19 December 2020).

〔8〕 Rahmadika, Sandi, et al, ″Blockchain-Enabled 5G Edge Networks and Beyond: An Intelligent Cross-Silo Federated Learning Approach,″ Security and Communication Networks. 2021.

〔9〕 Firdaus, Muhammad, and Kyung-Hyune Rhee, ″On Blockchain-Enhanced Secure Data Storage and Sharing in Vehicular Edge Computing Networks,″ Applied Sciences, 11(1), 414. 2021.

〔10〕 Li, Lun, et al, ″Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles,″ IEEE Transactions on Intelligent Transportation Systems, 19(7), 2204-2220. 2018.

〔11〕 Kang, Jiawen, et al, ″Blockchain for secure and efficient data sharing in vehicular edge computing and networks,″ IEEE Internet of Things Journal, 6(3), 4660-4670. 2018.

〔12〕 Castro, Miguel, and Barbara Liskov, ″Practical Byzantine fault tolerance and proactive recovery,″ ACM Transactions on Computer Systems (TOCS), 20(4), 398-461. 2002.

〔13〕 Firdaus, Muhammad, Sandi Rahmadika, and Kyung-Hyune Rhee, ″Decentralized trusted data sharing management on internet of vehicle edge computing (IoVEC) networks using consortium blockchain,″ Sensors, 21(7), 2410. 2021.

〔14〕 Jaiswal, Raj K., and C. D. Jaidhar, ″An applicability of aodv and olsr protocols on ieee 802.11 p for city road in vanet,″ Internet of Things, Smart Spaces, and Next Generation Networks and Systems (pp. 286-298). Springer, Cham. 2015.

〔15〕 Gao, Jianbin, et al, ″A blockchain-SDN- enabled Internet of vehicles environment for fog computing and 5G networks,″ IEEE Internet of Things Journal, 7(5), 4278-4291. 2019.

〔16〕 Olson, K., et al, ″Sawtooth: An introduction. The Linux Foundation,″ San Francisco, CA, USA. 2018.

〈저자소개〉

무함마드 필다우스 (Muhammad Firdaus) 학생회원
2013년 9월: Electrical Engineering, Politeknik Negeri Bandung
2016년 4월: Telecommunication Engineering, Politeknik Elektronika Negeri Surabaya, Indonesia
2019년 4월: Electrical Engineering, Institut Teknologi Bandung, Indonesia
2019년 9월~현재: Ph.D student in the Laboratory of Information Security and Internet Application, Pukyong National University, Republic of Korea
〈관심분야〉 Blockchain Security, Information Security, Wireless Communication Security, Edge Intelligence

이 경 현 (Kyung-Hyune Rhee) 종신회원
1982년 2월: 경북대학교 수학교육과 졸업
1985년 2월: 한국과학기술원 응용수학과 석사
1992년 8월: 한국과학기술원 수학과 박사
1985년 2월~1993년 2월: 한국전자통신연구원 연구원, 선임연구원
1993년 3월~현재: 부경대학 IT융합응용공학과 교수
〈관심분야〉 정보보호, 암호이론, 암호 프로토콜, 블록체인 기술