Blockchain-based Message Dissemination in VANET

Rakesh Shrestha, Rojeena Bajracharya and Seung Yeob Nam*
Department of Information and Communication Engineering
Yeungnam University
Gyeongsangbuk-do, Korea
rakez_shre@ynu.ac.kr, rojeena@ynu.ac.kr, synam@ynu.ac.kr

Abstract— **With the evolution of vehicle technology, VANET plays an important role in saving life and property of the drivers by disseminating critical event information. However, the traditional VANET faces several security issues. We propose a new type of blockchain to resolve critical message dissemination issues in VANET. We create a local blockchain for real world event messages exchanged between the vehicles within the scope of the countries. In this paper, we discuss a blockchain suitable for VANET. We present a public blockchain that stores the node trustworthiness and message trustworthiness in a distributed ledger that is appropriate for secure message dissemination.**

Keywords—blockchain, VANET, message trustworthiness, node trustworthiness

I. Introduction

In recent decades, there has been a persistent increase in the number of smart and autonomous vehicles. In Vehicular Ad-Hoc Network (VANET), lives and property of the driver depend on communication between vehicles and infrastructure. The main goal of vehicular technology is to disseminate life-threatening event information such as traffic jam, accident reports in a short time and accurately. However, it is still a challenge to disseminate critical event information to a targeted area under dynamic vehicular environment and in the presence of dishonest vehicles. The existing VANET encounters many security issues. Due to fake and untrustworthy information generated by malicious vehicles, the dangerous messages cannot be disseminated in accurate time. As a result, it leads to collateral damage to neighboring vehicles and the drivers. The main objective of this paper is to deliver secure and trustworthy event messages by applying blockchain technology in VANETs. The blockchain has recently gained attention and has a great potential in diverse fields. We use blockchain to resolve the critical information dissemination issue in VANETs. Blockchain (BC) is an emerging decentralized and distributed computing paradigm that underpins the bitcoin cryptocurrency [1], which provides privacy and security in p2p networks. In case of VANET, the blockchain can be used as a ground truth of information for vehicles because any vehicle can access the history of event information in the public blockchain.

We propose a scheme to determine the node trustworthiness and message trustworthiness in VANET and then store them in public blockchain, which acts as a ground truth for other vehicles. A simple adoption of existing blockchain is not directly applicable for VANET scenarios, so we will use event messages as transactions in VANET unlike using cryptocurrency as transactions in bitcoin. Therefore, we introduce a new type of blockchain suitable for the VANET. We believe that BC can resolve the main issues faced by current VANET and provide security for critical information dissemination. The new blocks are built based on the event messages similar to transactions in bitcoin and hashes of each block are linked together in a sequential manner to make a blockchain. Recently, there has been a lot of interest in blockchain technology and many researchers investigate the ways in which blockchain can be used in geospatial systems. In case of bitcoin, the newly minted block is shared among all the nodes globally. However, in case of VANET, there is no need to share the blocks beyond the scope of the country. For instance, Japan and Korea are geographically separated from each other and they are not connected by roads. So, the traffic and accident information of Japan is not useful for the vehicles in Korea. Hence, it is more suitable to maintain a separate blockchain regarding vehicle node trust level and message trustworthiness in each country based on geographical location.

We will deal with a local blockchain that are independent of the chains for different countries to improve the scalability and timeliness of message dissemination in VANET. In this paper, we consider a public blockchain that independently manages and stores all the node trustworthiness and message trustworthiness in a given country.

The remaining paper is structured as follows. Section II explains the background of blockchain technology. Section III explains the proposed new type of blockchain. Section IV discusses the implementation of proposed blockchain for secure message dissemination in VANET and Section V provides the conclusion of the paper.

II. Related Work

A blockchain is a distributed and decentralized public database of all transactions or digital events that have been executed or shared between participating nodes. Each event in the public database is validated by agreement of a large number of the nodes in the blockchain network. The popularity of the blockchain is due to its advantages. The advantages of blockchain includes decentralization, anonymity, chronological order of data, distributed security, transparency, immutability and suitability for trustless environments [2]. There are mainly two types of blockchains i.e. public and private blockchains. The public blockchain is an open blockchain where anyone can join and interact with the blockchain without permission from a central authority. While private blockchain is based on access control. It allows administrators to control the participants on the network and controls who can join, view and can write to the blockchain. In addition to this, the administrator can create a consensus group as a result the private blockchain can converge to centralization. However, the public blockchain is purely a decentralized blockchain that does not have a single point of failure problem and is able to withstand malicious attacks. In public blockchain, once the full node connects to peers, it first tries to construct a complete blockchain. A full node is a node

978-1-5386-6227-4/18/$31.00 ©2018 IEEE

that stores and maintains all the history of blockchain transactions, can begin transactions directly and independently and authoritatively verify any transactions in the network. Every node in the BC network knows the genesis block's hash. The genesis block is the first block in the blockchain, which is the common origin of all the blocks and contains the information that is commonly known to all the nodes. The block consists of cryptographic hash of records, with each block containing information of the previous block hash forming a chain of data creating the blockchain as shown in Fig. 1. The blockchain begins with a genesis block on top of which are stacked the successor blocks. The structure of the each block has a block header that consists of previous block's hash, nonce, timestamp as well as the Merkle hash. The block body contains lists of transactions and some additional data depending on the requirement of the blockchain. For immutability, the transactions should be hashed using a Merkle hash and this hash needs to be included in the block header. The Merkle hash is derived from the Merkle algorithm [3], which is a cryptographic algorithm that hashes all the transactions of the block.

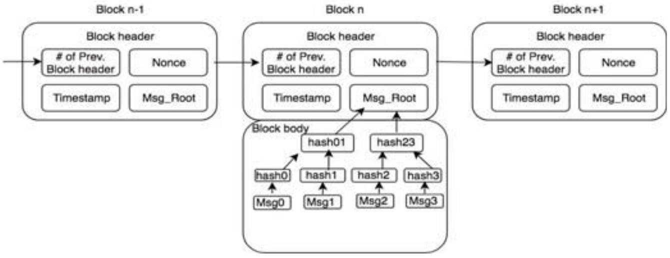

Fig. 1. The structure of block in a blockchain [1]

Every node in the network builds a trusted blockchain based on the genesis block that acts as secure root. The genesis block does not have previous block's hash. If a node is new then it only knows the genesis block and it will have to download all the blocks starting from the genesis block to synchronize with the blockchain network and is constantly updated as new blocks are found [4]. The chaining of blocks is performed by appending previous block's hash to the current block, then the current block's hash to the following block in a sequential manner [1], [4] as shown in Fig. 1. Then, it is shared with other nodes in a distributed peer-to-peer networks in a secure way without the need for a central authority. The sequential hashes of blocks ensures sequential order of transactions. Then, previous transactions cannot be modified without modifying their blocks and all subsequent blocks. The BC is verified by consensus of anonymous nodes in generation of blocks. The BC is considered secure if the aggregated computational power of the malicious nodes is not larger than the computational power of the honest nodes [1], [5]. In case of bitcoin, the Proof of work (PoW) concept makes sure that the miner is not manipulating the network to make fake blocks. A PoW is a mathematical puzzle that is very hard to solve and easy to verify that protects the blockchain from the double spending attack.

In VANET, some of the previous works related to secure event message dissemination are based on voting [6] [7]. Most voting approaches attempt to solve the node security issues by asking the opinions of other nodes to determine the trustworthiness of the node. However, this type of approaches have issues of whether the nodes providing the feedback can be trusted. In our approach, we assume all information are kept in a distributed database based on blockchain technology. On the other hand, a limited work has been done in vehicular networks using blockchain. The authors in [8] used a basic blockchain concept to simplify the distributed key management in heterogeneous vehicular networks. The authors in [9] combined VANET and Ethereum's blockchain-based application concepts, which enabled transparent, self-managed and decentralized system. They used Ethereum's smart contract system to run any type of application on an Ethereum blockchain. However, our proposed work applies a different blockchain for secure message dissemination in vehicular networks. In [10], the authors proposed a block chain technology in automotive security by using an overlay network. The authors use overlay networks in the blockchain by using additional nodes called overlay block managers. The overlay network nodes are clustered using cluster heads, and these cluster heads are accountable for handling the blockchain and operating its main functions. However, the introduction of additional overlay node might cause high latency and might be the center point of failure if the cluster head is compromised.

III. Blockchain Scheme in VANET

We propose a new type of blockchain to solve the issues related to trustworthy message dissemination in VANET. The approach is new as we use the concept of immutable distributed public database for secure message dissemination in VANET, where any node can access the information. In addition, it can be maintained independently by each country. In recent years, this has become feasible due to the introduction of blockchain. However, the nature of our problem is different from the bitcoin blockchain as we are dealing with event messages rather than the cryptocurrency transactions.

The event information such as traffic jams, road accidents, and environmental hazards are relevant to a particular geographical location. This local information is not of much interest to other regions or countries. All the vehicles can know their positions by using location certificate based on proof of location (PoL) [12]. There are millions of vehicles in the world so if each country manages blockchain independently then there will be a lesser amount of scalability issues.

A. Assumptions

We assume Vehicle to Vehicle (V2V) and Vehicle to Everything (V2X) communications [11] and vehicles can connect to the internet efficiently. Our assumption is that all the vehicles have required equipment like On Board Units (OBUs), sensors, and GPS. We assume that the number of legitimate Road Side Units (RSUs) is greater than the malicious RSUs. The RSUs are usually fixed entities. We assume that a legitimate RSU creates a genesis block to start the blockchain based on the local events. We assume that the vehicles have high computing power and a high trust level are considered as full node vehicles that can participate in the mining process while other nodes are normal nodes that helps in message verification and forwarding. We assume that the critical event messages are disseminated within a region of interest (RoI) in a specific geographical location. We assume that the critical messages are not encrypted so that those messages can be available to any nearby vehicles. We assume the number of required message to confirm the event is fifteen so that the message is considered correct.

B. Proposed Blockchain in VANET

We propose a new type of blockchain because simple adoption of existing blockchain is not suitable for our scenario. The conventional blockchain deals with cryptocurrency while our blockchain deals with event messages without using any crypto coins. Our BC is appropriate for trustworthiness of safety messages in VANET that relates to a real world. The BC stores and manages the history of event messages along with the trust level of the vehicles in a distributed, immutable, and reliable manner. In each country, there will be a single unique blockchain and that is managed and maintained independently for recording vehicle information.

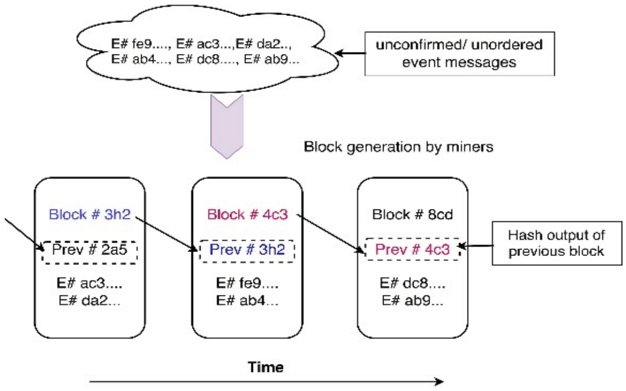
E# fe9...., E# ac3...,E# da2..,
E# ab4..., E# dc8...., E# ab9...
unconfirmed/ unordered event messages
Block generation by miners
Block # 3h2
Prev # 2a5
E# ac3....
E# da2...
Block # 4c3
Prev # 3h2
E# fe9....
E# ab4...
Block # 8cd
Prev # 4c3
E# dc8....
E# ab9...
Hash output of previous block
Time

Fig. 2. The generation of blockchain from unconfirmed event messages

In VANET, all the vehicles broadcast their positions through beacon messages. We use location certificate, which is a digital proof that a vehicle is located at a specific place at a particular time [12]. All the vehicles location need to have a location certificate to prove their position at a given time. A location certificate is provided by a legitimate RSU. The RSU issues a location certificate to the requesting vehicle using its own public and private key pair. This location certificate acts as a proof of location (PoL) for the vehicles that helps to identify the event messages in a given geographical area.

There are scalability and timeliness issues in existing blockchains, which may not be appropriate for real time VANET applications. In our scheme, all the events are local, i.e. event messages are confined to the vehicles within a particular geographical area. In conventional blockchain, the newly minted block is broadcasted globally. However, in our scheme, VANET messages need not go beyond the border of a country. As the traffic and accident information of one country is irrelevant to vehicles that are located in another country. Hence, the new concept of blockchain that different from conventional blockchain is needed. In each independent blockchain, all the miners mine the new block based on the event messages and sends the newly minted block to the local blockchain network. The blockchain acts as a global ground-truth for the node trustworthiness within the country. In other words, any vehicle can query the vehicle trust level at any time in the blockchain. The new blocks are generated by aggregating the list of unconfirmed event messages from the message pool. The hashes of each block are chained together in sequential order to build a blockchain as shown in Fig. 2. After generation, the new blocks are broadcast and all the vehicles in the network will verify and update their blockchain.

1) *Proof of Locaiton (PoL):*

A location certificate based on proof of location (PoL) is used to provide a proof about the location of a vehicle at a given time [12]. Each vehicle requires PoL to verify that the vehicle is located in a location near the event spot. In addition, the PoL is used as a location proof in an event message that assist in the blockchain. The RSU acts as a validator to provide the location certificate to the vehicles within its communication range. We consider that the vehicles and RSUs have their own public and private key pairs. The requesting vehicle sends an initiation message with its public key (K_{vpub}) to the RSU and then, the RSU sends a random session id (S_{id}) to the vehicle. The vehicle sends back the signed session id (*sign* (S_{id})) to the RSU. The RSU verifies the authenticity of the signature of (*sign* (S_{id})) with vehicle's public key (K_{vpub}) and checks the elapsed time between the session id exchange. If the time difference between sending and receiving session id is less than a few milliseconds, the RSU publishes a location certificate (C_L) including location, time and vehicle's public key (K_{vpub}) that is signed by the RSU's private key (K_{Rpr}) as shown in Fig. 3. The GPS can not be used because it can be easily spoofed [13]. The PoL is secure as the vehicles can not create a fake location certificate without the valid signature of the RSU. However, using only PoL does not guarantee the

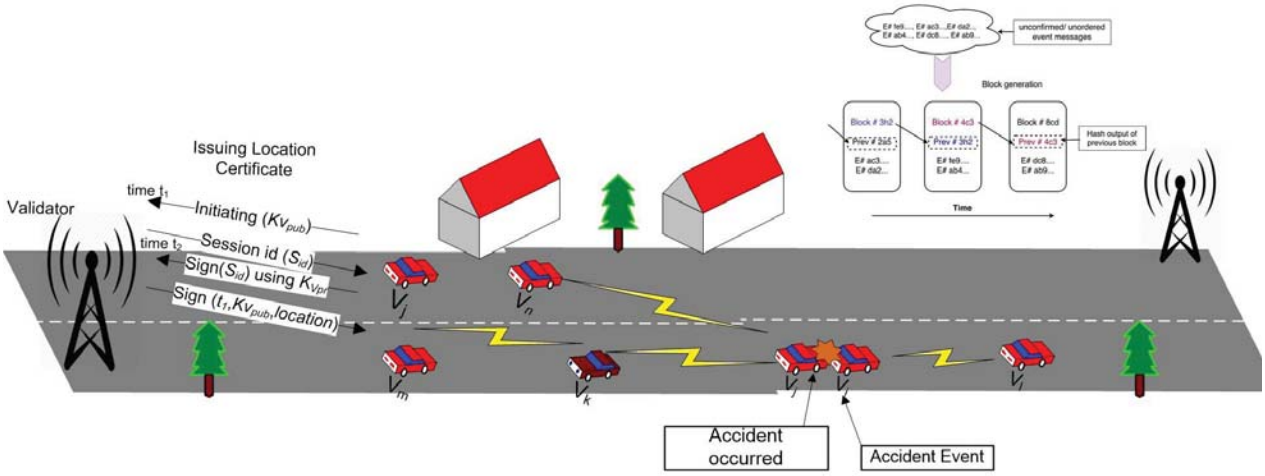

Fig.3. Blockchain scheme for secure message dissemination

message trustworthiness, we need blockchain mechanism to make the message more trustworthy.

IV. Implementation of Blockchain for Secure Message Dessimination in VANET

The proposed blockchain scheme for secure message dissemination is shown in Fig. 4. All the vehicles in the network download and update the blockchain. In our scheme, the blockchain acts as a distributed public ledger, which stores all the history of vehicles' trust level in the blockchain along with event message. The vehicle that encounters an event such as accidents will broadcast the event message with several parameters to neighbor vehicles in the blockchain networks. When other vehicles receive a new event message, they first verify whether it is inside the same area based on the location certificate embedded in the event message. The vehicles consider the event message, if it belongs to the same area. Then, the neighbor vehicles check other parameters of the event messages. Every vehicle independently checks each event message before propagating it further in order to prevent spamming, denial-of-service, or other nuisance attacks against the system.

Whenever there are events, nearby vehicular nodes will broadcast an event message M_i. The neighbor vehicles will collect the information from the broadcasting vehicles. The event message contains all the associated information such as type of event, Pseudo ID, event ID, trust level, timestamp, PoL, etc. as given in Table I. The vehicles receiving the event message first check the trust-level of the sender vehicle from the blockchain and then verify the event messages. They check each event message based on the evidences regarding sender vehicle's trust level, event location, event ID, driving direction, PoL, speed, timestamp etc., and stores it in the local memory pool if message is considered to be trustworthy. Otherwise, the message is discarded. The event message is broadcast on the local blockchain network, and each vehicle in the network validates the event messages. The mining vehicle collects different event messages from an unconfirmed event message pool and verifies if the parameters of the accepted messages are valid.

TABLE I. Event message format

Message Header	
PID	Pseudo ID
Pub address:	Public key
Event ID	1
Event Type	Types of event
TimeStamp	Event timestamp
Location	Event location
Trust Leve (TL)	m/(m+n)
Direction	Driving direction
PoL	Location certificate (CL)

The mining vehicle uses message verification policies to know the message trustworthiness as follows:

- Check sender vehicle's previous trust level from the main blockchain
- Check the PoL based on location certificate
- Check if it is the first hand information.
- Check the timestamp

If the received event messages are valid and trustworthy based on the verification policy, then the trust level will be updated. The trust level is defined as the fraction of the true events messages '*m*' sent by vehicle V_i to the total event messages '*m+n*', i.e. *TL=m/(m+n)*, where '*n*' is the number of false event messages. The trust level vary over time depending upon the true or false messages. The trust level of the vehicle increases as the true message increases. The mining vehicles will calculate the updated trust level of the sender vehicle and sends the this trust level in blockchain after the new block is added in the local chain as follows:

$$\text{TL}= \frac{m}{m+n} \begin{cases} \text{If message is true then, m = m + 1} \\ \text{If message is false then, n = n + 1} \end{cases} \quad (1)$$

where *m* is true and *n* is false message counter.

Each mining vehicle will create a new block B_i as shown in Fig. 1. The block header consists of previous block hash (B_{i-1}), nonce value *N* and hash of all the unordered event messages M_i. The mining vehicles try to find a nonce such that the hash of$(H(M_i)\,||H(B_{i-1})||\,N)$ is less than the difficulty target. The difficulty target is adjusted periodically to the current computation power of the vehicle nodes such that the new blocks are created continuously at a regular interval. The miner vehicle is said to have PoW done when it solves a difficulty puzzle by finding a nonce value as a solution to meet the network 'difficulty target'. After finding the nonce, it broadcasts B_i to the blockchain network. The other vehicles receive the new block and independently verifies if the event messages are correct based on the verification policies. This guarantees that only legitimate blocks are broadcasted on the network. The independent validation also guarantees that mining vehicles who behave in an honest way get their blocks integrated in the blockchain, thus earning the reward. The mining vehicles who behave in a dishonest way get their blocks rejected. As a result, they not only lose the reward, but also waste the energy to compute a PoW solution. If the new block information is correct, then the vehicles accept it and begin to mine new blocks on top of it. The existence of the event message in the blockchain is a kind of confirmation that the event message is trustworthy.

The new block is stored in the blockchain permanently based on the consensus decision among the miner vehicles. The PoW consensus mechanism is used to prevent malicious vehicles from invalidating the database. As the size of the network increases, the blockchain becomes increasingly difficult to compromise by the attackers using double spending attacks [14]. The information in the new block can still be publicly verified; thus the public nature of the blockchain allows all participants to verify the correctness of the event messages. If any subsequent vehicles at the event spot need to know about the event information, they need to check the blockchain to verify the correctness about the event messages and act accordingly. Therefore, we can keep track of all the vehicles' recent trustworthiness.

Sometimes, two or more mining vehicles mine a new block at the same time and instantly broadcast to their immediate neighbors who begin propagating the new blocks across the networks. The blocks might arrive at different vehicles at different times, causing the vehicles to have different blockchain perspectives. As a result, blockchain forks occur. In order to solve forks, the mining vehicles should select the blockchain with the longest chain of blocks that represent the most PoW done.

Hence, the public nature of the blockchain and independent validation of each new block by all the vehicles on the network ensures distributed and secure database. The

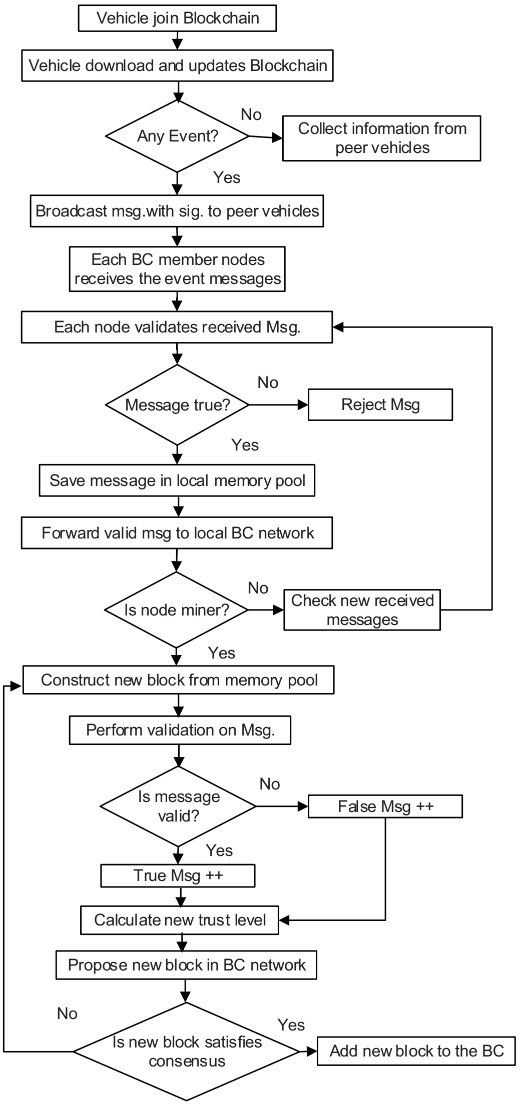
Vehicle join Blockchain
Vehicle download and updates Blockchain
Any Event?
No
Collect information from peer vehicles
Yes
Broadcast msg.with sig. to peer vehicles
Each BC member nodes receives the event messages
Each node validates received Msg.
Message true?
No
Reject Msg
Yes
Save message in local memory pool
Forward valid msg to local BC network
Is node miner?
No
Check new received messages
Yes
Construct new block from memory pool
Perform validation on Msg.
Is message valid?
No
False Msg ++
Yes
True Msg ++
Calculate new trust level
Propose new block in BC network
No
Is new block satisfies consensus
Yes
Add new block to the BC

Fig. 4. Proposed blockchain in VANET

blockchain stores the history of all the trust levels of the vehicles with corresponding event messages. Thus, we can keep track of all the vehicles recent trustworthiness. Each block based on hash of its previous block and hence manipulating and forging a block is very hard and needs a significant computation power to change the successor blocks. The malicious vehicles cannot insert fake blocks into the distributed blockchain without being noticed by other peer vehicles. As the network size grows, the blockchain becomes more difficult to compromise by the malicious vehicles. So, the event information can be disseminated securely using the new type of blockchain. In addition, the insurance company for insurance settlement can use the history of vehicle information from blockchain and the traffic police can use it as a forensic to solve the hit and run as well as traffic accident disputes.

V. Conclusion

Our proposed scheme can effectively handle the trustworthiness of event messages in a reliable way by using blockchain technology. We introduced a new type of blockchain that can be independently managed within a country, which stores the node trustworthiness and message trustworthiness in the distributed ledger for secure message dissemination in VANET. In our scheme, we deal with event messages as transactions instead of cryptocurrency. A consensus of all the mining vehicles in the blockchain network can be established to generate a new block that can be used as a ground truth for the next block. As a future work, we will provide detailed analysis of the new type of blockchain and show how our scheme can deal with critical event message dissemination in real time with low delay in VANET environment. We will also partition the geographical map of the country into several zones or regions based on cities, province and states based on the density of the vehicles in a country, and each zone will manage and maintain independent blockchains.

Acknowledgment

This research was supported in part by Basic Science Research Program through National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (2013R1A1A2012006, 2015R1D1A1A01058595). This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-R2718-16-0035) supervised by the IITP (Institute for Information & communications Technology Promotion).

List of Acronyms

Acronyms	
VANET	Vehicular Ad-hoc Networks
BC	Blockchain
PoW	Proof of Work
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
PoL	Proof of Location
OBU	On Board Unit
RSU	Road Side Unit
RoI	Region of Interest
PID	Pseudo ID
TL	Trust Level

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," pp. 1-9, 2016.

[2] Z. Zheng, S. Xie, H. N. Dai and H. WANG, "Blockchain challenges and opportunities: a survey," International Journal of Web and Grid Services, pp. 1-24, 2006.

[3] Ralph C. Merkle. “A digital signature based on a conventional encryption function,” in proceedings of CRYPTO’87, Springer , pp 369-378, Santa Barbara,CA, USA, August 16-20, 1997..

[4] A. M. Antonopoulos, Mastering Bitcoin: Unlocking digital crypto-currencies, O'Reilly Media, Inc., 2014.

[5] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Transactions on Dependable and Secure Computing, vol. 99, 2016.

[6] B. Ostermaier, F. Dotzer, M. Strassberger, “Enhancing the security of local dangerwarnings in VANETs - A Simulative Analysis of Voting Schemes”, The 2nd International Conference on Availability, Reliability and Security, Vienna, pp 422 – 431, 2007.

[7] J. Petit, and Z. Mammeri, “Dynamic consensus for secured vehicular ad hoc networks”, IEEE 7th International Conference on Wireless and Mobile Computing, Networking and Communications, pp 1 – 8, 2011.

[8] A. Lei, C. Ogah and et al., "A secure key management scheme for heterogeneous secure vehicular communication systems," ZTE Communications, pp. 1-11, 2016.

[9] B. Leiding, P. Memarmosherfi and D. Hogrefe, "Self-managed and blockchain-based vehicular ad-hoc networks," in Proc. of ACM International Joint Conference on Pervasive and Ubiquitous Computing, pp. 137-140, Heidelberg, Germany, September 12-16, 2016.

[10] A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," in IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, December 2017.

[11] Chen, Shanzhi et al. “Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G.” IEEE Communications Standards Magazine*,* pp. 70-76, 2017.

[12] T. Dasu, Y. Kanza, and D. Srivastava, “Unchain your blockchain”, in Proc. of Foundations and Applications of Blockchain (FAB), Los Angeles, California, March 9, 2018.

[13] N. O. Tippenhauer, C. Popper, K. B. Rasmussen, and S. Capkun, “On the requirements for successful gps spoofing attacks”, in proceedings of the 18th ACM conference on Computer and communications security, pp 75, ACM 2011.

[14] Ghassan O. Karame, Elli Androulaki, Marc Roeschlin, Arthur Gervais, and Srdjan Čapkun. “Misbehavior in Bitcoin: A Study of Double-Spending and Accountability” , ACM Trans. Inf. Syst. Secur. 18, 1, Article 2 (May 2015), pp 32, 2015 .