Trust Bit: Reward-based Intelligent Vehicle Commination using Blockchain Paper

Madhusudan Singh
Yonsei Institute of Convergence Technology
Yonsei University
Songdo, South Korea

Shiho Kim
School of Integrated Technology
Yonsei University
Seoul, South Korea

***Abstract*—The Intelligent vehicle is experiencing revolutionary growth in research and industry, but it still suffers from a lot of security vulnerabilities. Traditional security methods are incapable of providing secure IV, mainly in terms of communication. In IV communication, major issues are trust and data accuracy of received and broadcasted reliable data in the communication channel. Blockchain technology works for the cryptocurrency, Bitcoin which has been recently used to build trust and reliability in peer-to-peer networks with similar topologies to IV Communication world. IV to IV, communicate in a decentralized manner within communication networks. In this paper, we have proposed, Trust Bit (TB) for IV communication among IVs using Blockchain technology. Our proposed trust bit provides surety for each IVs broadcasted data, to be secure and reliable in every particular networks. Our Trust Bit is a symbol of trustworthiness of vehicles behavior, and vehicles legal and illegal action. Our proposal also includes a reward system, which can exchange some TB among IVs, during successful communication. For the data management of this trust bit, we have used blockchain technology in the vehicular cloud, which can store all Trust bit details and can be accessed by IV anywhere and anytime. Our proposal provides secure and reliable information. We evaluate our proposal with the help of IV communication on intersection use case which analyzes a variety of trustworthiness between IVs during communication.**

***Index Terms*— Blockchain Technology, Intelligent Vehicles, Communication, Security,**

I. Introduction

VANET is the encapsulation of Vehicle-to-Vehicle (V- to-V) and Vehicle-to-Infrastructure (V-to-I), which is used to provide a notification of any safety critical incident and hazard to the drivers. This information was gathered by the feedback of the nearby vehicles. This system was prone to security attacks by marking incorrect feedback and result in more congestion and severe hazard. The latest convergence of ITS and VANET lead to the innovation of intelligent vehicular networks for better safety, security and ubiquitous computing environment. To handle the vehicle communication and computing expertise, envisioned societal impact, government, agencies and vehicle manufacturers have produced international associations devoted exclusively to VANETs [1].

In the connected vehicle, data security and privacy are the most significant issues. These issues are not new issues as they were also big issues during RFID, Bluetooth technologies adoption. However, the Connected Vehicle technologies are more secure, but a risk of attacks will reach new levels of interoperability, and the autonomous decision-making will begin to embed complexity, security loopholes and potential "black swan" events [2]. In IV, the main issue is trustable and reliable information exchange between the vehicles.

In IV communication network, security is a very crucial issue during communication. These types of networks require trust and privacy. To build up this trust, we have proposed a Trust Bit element, which can help to build the trust and transmit the reliable data between IV communications. Trust bit is a unique crypto number, which is attached to message format, which is, transmitted during the communication time. The fully decentralized body stored on vehicular cloud networks manages the trust bit, which can be accessed anywhere and anytime. This trust bit mechanism is based on Blockchain technology, which is enabled to create the decentralized crypto unique ID, self-executing digital contracts and details of IV that can be controlled by over the vehicular Cloud (Internet). It provides a new governance system with more user-friendly or consensus and autonomous which can operate over a network of IV without human intervention.

Previously some of the researchers combined automotive and blockchain technology but most of them considered applications, services and smart contracts based applications. However, our proposal of blockchain technology with vehicular networks concentrate on secure and fast communication between intelligent vehicles. Here intelligent vehicles mean internet enabled self-driving cars [3].

Our contribution. We have proposed unique crypto ID, Trust Bit developed by blockchain technology. Our proposal explains the management of Trust Bit within the vehicular cloud. 3) We elicited the benefits of Trust Bit and evaluated our proposal with IV communication use case.

Organization. Section II describes the intelligent vehicle, vehicular cloud networks and their security issues. Section III introduces Blockchain technology; section IV describes our proposed mechanism for intelligent vehicles Communication, section V evaluate the proposed mechanism use case; section VI discuss future works of blockchain technology in intelligent vehicles, and concluding remarks are mentioned in section VII.

II. Background Study

This section is categorized into four sections. Section one, describes intelligent vehicular communication, section two talk about vehicular cloud computing (VCC), and discusses security challenges in IV communication. And fourth section discussed about basic of blockchain technology and blockchain application on intelligent vehicles.

A. Intelligent vehicle communication

Connected Vehicles communicate with and within vehicles and in three ways such as In-vehicles communication, a vehicle to infrastructure (anything) and vehicle-to-vehicle. Connected Vehicle-based automotive technology has advanced network connectivity in vehicles. The industry has already started manufacturing these advanced vehicles. These vehicles have cyber-physical features. These type of vehicles collects data from physical environments and cyber systems (Connected Vehicle), make the decision and execute on such decisions within the physical environment. Some examples of such systems are Advanced Driver Assistant Systems (ADAS), Advanced Fleet Management, Smart Transportations, Autonomous driving, etc. This type of research needs built-in security and architectural design to protect emerging threats. The goal of automotive security is to provide a completely secured environment for an automotive system for different operating environments [4]. Fig 1 shown the vehicular communication with the vehicular cloud.

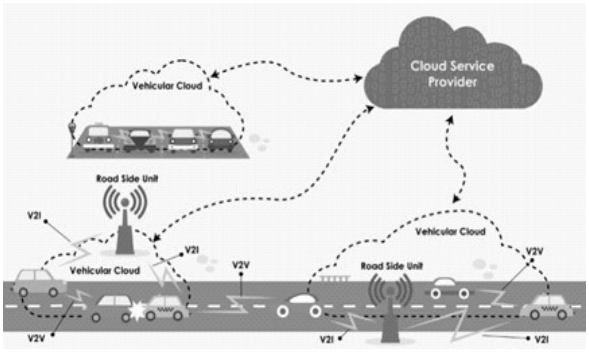

Fig. 1. Vehicle communication (V2V, V2I) and Vehicular cloud [6]

B. Vehicular cloud Networks

Similar to VANETs, there are two types of VCs. The first type is called Infrastructure-based VC, where drivers will be able to access services through network communications involving the roadside infrastructure. In the second type called the Autonomous VC (AVC) [5].

VCs provide services at three levels, i.e., application, platform, and infrastructure. Service providers use the levels differently based on what and how the services are offered. The fundamental level is called Infrastructure as a Service (IaaS), where infrastructure such as computing, storage, sensing, communicating devices, and software are created as VMs (Virtual Machines). The next level is Platform as a Service (PaaS), where components and services (such as http, ftp, and email server) are provided.

Moreover, configured as a service. The top level is called Software as a Service (SaaS), where applications are provided in a "pay-as-you- go" fashion.

VCs provide a cost-efficient way to offer comprehensive services. For example, a cheaper vehicle with network access can access a VM with strong computation, communication, sensing capability, and large storage. Many applications such as traffic news, road conditions, or intelligent navigation systems can be provided by a VM.

C. Security Challenges of IV

The security mechanism is a hard problem for seamless communication among networks.

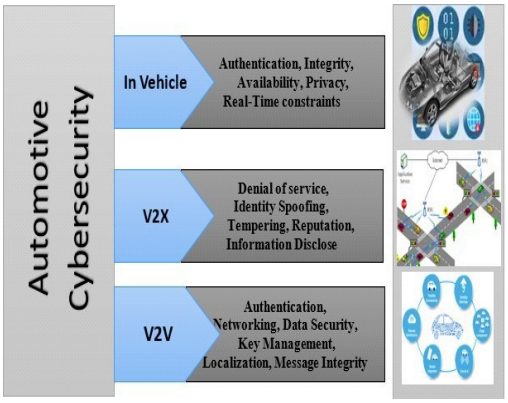

Fig. 2. Security issues in Intelligent Vehicles

Until the time, many researchers have proposed multiple security mechanisms for IV communication but almost all of them primarily working on static security on requirements engineering, but in this article, we are discussing dynamic security features or adaptive requirements. We have illustrated the possible security issues in fig.3.

VC security system are very probable to attacks by attackers because it have multiple service data and those data are requested by multiple users with high mobility. The VC infrastructure attackers have equally distributed the same environment as their valid users, even though attackers and users are different machines. Attacker vehicles are attacks different places equally due to its physically moving features. It is hard to detect the correct location of attackers. Attacker's main targets are brake confidentiality, such as identities of other users, valuable data and documents stored on the VC, and the location of vehicles.

We have mentioned major security issues in VC, which are as follows [6]:

- Message authentication: Whether received message comes from valid vehicles.
- Message Integrity: Whether valuable data and documents stored on the VC, executable code, and result on the VC are unhampered.
- Access Control: Whether Message sender and receiver both are legal and authorized entity to communicate with each other.

- Message Confidentiality: Whether confidential data such as identities of other users, valuable data and documents stored on the VC, and the location of the VMs, where the target's services are executing are secured.
- Privacy: Whether during communication, intelligent vehicles share their secure private information with any illegal entities.
- Liability Identification: Whether members of communication process are liable to believe each members' message during the communication process.

Whether all member vehicles identify their legal communication authority.

D. Blockchain Technology

Blockchain technology is distributed, open ledger, saved by each node in the network, which is self-maintained and updated by every node. It provides the peer-to-peer network with the interference of the third party. The blockchain integrity is based on strong cryptography that validates and chains together, blocks on transactions, making it nearly impossible to tamper with any individual transaction without being detected. Fig 3 shows blockchain basic features. Blockchain technology especially includes 4 basic things, a) Shared ledger, b) Cryptography, c) Signed blocks of transactions, and d) digital signatures [6].

a) Shared ledger: It establishes a single transaction detail due to which third party necessity is finished. It is very beneficial for autonomous agents, process and organizations which imply smart contract technology .

b) Cryptography: It binds the data with the very strong crypto mechanism, which is not easy to track or tampered by unauthorized users.

c) Consensus: This preserves the sequences of transactions and allows fine-grained access control at the level of a transaction.

d) Digital signatures: It is verified possession of the private key, and verify whether message sender is a valid user or not. It also detects the message integrity.

Existing work on blockchain technology in Intelligent Vehicles [7]:

The researchers have combined Ethereum' blockchain based smart contracts system with vehicle ad-hoc network. They have proposed two applications, first mandatory application such as traffic regulation, vehicle tax, vehicle insurance and optional application of vehicles, which provides information and updates on traffic jams and weather forecasts [.

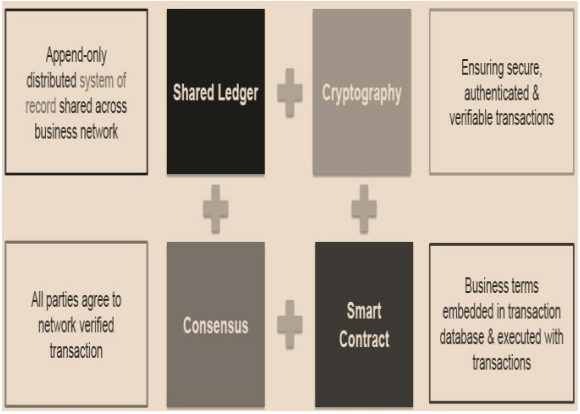

Fig. 3. Blockchain basic features [16]

Yong yuan, et.al [8] has proposed the blockchain technology for ITS for establishment of secured, trusted and decentralized autonomous ecosystem and proposed a seven-layer conceptual model for the blockchain.

Benjaminet.al [9], have also proposed the blockchain technology for vehicular ad-hoc network (VANET). They have combined Ethereum' blockchain based smart contracts system with vehicle ad-hoc network. They have proposed combination of two applications, mandatory applications (traffic regulation, vehicle tax, vehicle insurance) and optional applications (applications which provides information and updates on traffic jams and weather forecasts) of vehicles. They have tried to connect the blockchain with VANET services. Blockchain can use multiple other functionalities such as communication between vehicles, provide security, provide peer-to-peer communication without disclosing personal information etc. Ali dorri et.al. [10] have proposed the blockchain technology mechanism without disclosing any private information of vehicles user to provide and update the wireless remote software and other emerging vehicles services. Sean Rowen et.al. [11] have described the blockchain technology for securing intelligent vehicles communication through the visible light and acoustic side channels. They have verified their proposed mechanism through a new session cryptographic key, leveraging both side-channels and blockchain public key infrastructure.

III. Proposed Blockchain Technology based Vehicular Communication

In this section, we have proposed blockchain based vehicular communication. Our proposed mechanism has three basics things, A) wireless (internet) connected device, B) Vehicular Cloud Computing (VCC) and C) blockchain technology (BT).

A. Wireless (Internet) Connected device

It is an internet enabled a device which can be organize, communicate and can manage VANET as well as the service provider. Such as Smartphone, PDA, Intelligent Vehicles, etc.

B. Vehicular Cloud Computing

VCC is a hybrid technology that has a remarkable impact on traffic management and road safety by instantly using vehicle resources, such as computing, data storage, and internet decision-making.

C. Blockchain technology

Blockchain consists of a technically unlimited number of blocks which are chained together cryptographically in chronological order. In this, each block consists of transactions, which are the actual data to be stored in the chain. In figure 4 explain basic architecture of proposed blockchain intelligent vehicle communication.

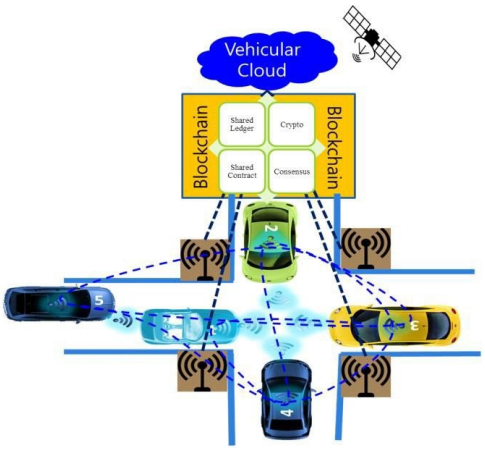

Fig. 4. Proposed blockchain Intelligent Vehicle Communication

In fig.5, we have shown our proposed blockchain based intelligent vehicle communication network architecture. In this architecture, blockchain is enabled between the application layers and perceptual layer.

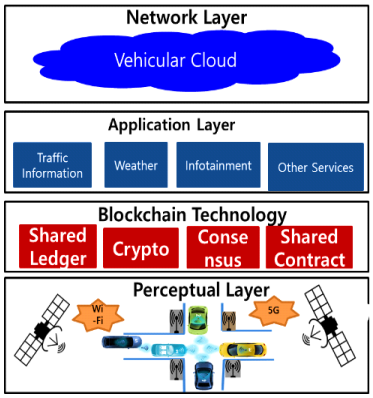

Fig. 5. Proposed Intelligent Vehicle Communication Network

In our proposed method, we have proposed a bit trust crypto unique ID that is issued by vehicle seller/authorized dealers. This Bit trust is developed by blockchain crypto mechanism and is similar to bitcoin. This bit trust will be issued to every intelligent vehicle. During communication, the vehicle will provide trust bit to build trust in the communication networks. Vehicular networks that have already blockchain-enabled service/user's data providers manage a Trust Bit. Trust t is encrypted unique number, which is a unique issued to every particular IV and is called the Bit Trust ID.

Every IV has its own Bit Trust ID that can be generated by authorized authority. Bit Trust will earned by calculating some computation in the group communication. Greater the bit trust available for any single IV, higher will be its respect and honor. With the help of Bit Trust, we can get the complete history of vehicles (such as accident history, condition of IV, crime history, etc.). Fig. 6 has shown the Trust Bit access points for the vehicles.

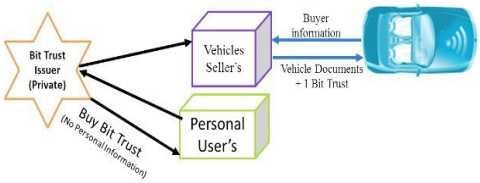

Fig. 6. Bit trust access method

The blockchain message encryption and decryption process is based on following three steps. In this figure 7 has explained the complete process.

a) Key generation: First, each IV must need to generate their private and public key. IVs must exchange their public key with the other IVs in the network and private key must be kept with itself. The private key is generated with the help of the public key.

b) Massage encryption with digital signature: Second, each vehicle shall digitally signed the message. Due to digitally signed message, receiver easily finds that the message is not tampered, and message sender is a valid member of the network.

c) Message verification and decryption: Receiver after receiving message, identify the sender by verifying the digitally signed encrypted message. After verification receiver will decrypt the message with the public key of sender.

A. Example Setting of IV networks

For example, five intelligent vehicles have Bit Trust IV- 1, IV-2, IV-3, IV-4, & IV-5, respectively. Message is broadcasted from IV-1 to IV-5. Figure 8 has an example of IV

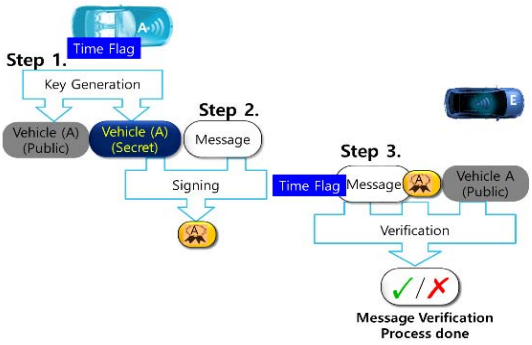

Fig. 7. Message process between two IV

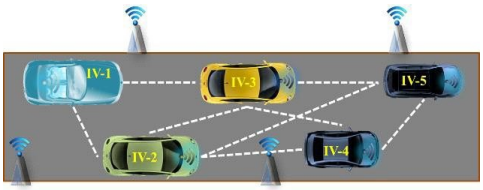

Fig. 8. Intelligent Vehicular networks

Each vehicle broadcasts the message in the networks. The blockchain maintains the table with information of "who communicates with whom". It doesn't require personal information of any IV. It needs only bit trust of IV.

TABLE I. COMMUNICATION INFORMATION ON BLOCKCHAIN

Intelligent Vehicles	Communicated Vehicles
IV-1 (Public)	IV-2, IV-3, IV-4, IV-5
IV-2 (Public)	IV-3, IV-4, IV-5, IV-1
IV-3 (Public)	IV-4, IV-5, IV-1, IV-2
IV-4 (Public)	IV-5, IV-1, IV-2, IV-3
IV-5 (Public)	IV-1, IV-2, IV-3, IV-4

Each IV broadcast the message in networks and the complete message framework looks like in figure 9 show the complete message format of IV

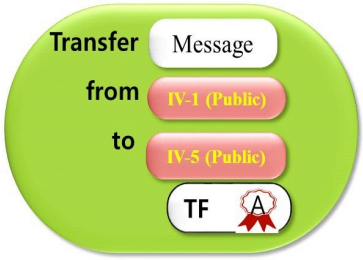

Fig. 9. Message Framework example

Where IV-1 and IV-5 are Bit Trust of intelligent vehicles 1 and 5 respectively. TF is time flag of message broadcasted from intelligent vehicles.

a) Consensus Protocols: Broadcasted message will validated only after verification of more than 50% of the network members. This process is called consensus.

b) Random hash functions: Blockchain, uses random hash (RH) function for cryptography,

$$RH : TextFile \rightarrow \{0,....,2^k - 1\}$$

Where all outputs are chosen uniformly and randomly and are independent of each other.

c) Process: In practice, we hope that SHA256 behaves "like a random Oracle. It means

$$SHA : TextFile \rightarrow \{0,....,2^{256} - 1\}$$

d) Calculation of blockchain data cryptography: If attackers made all computing, devices on the world would compute SH256. It will takes

$$to\ find\ x_1 \neq x_2 \; 1.10^9\ years" \quad such\ that \quad SHA256(x_1) = SHA256(x_2)$$

Where x_1 and x_2 is text files. Therefore, we can say that our proposal will provide decentralized secure communication among reliable IVs. It provides the database of each vehicle updated with road records, makes easy for data distribution, and defined the participation criteria based on services.

All vehicles communication data will be managed on a vehicular cloud with the trust bit ID. If in future, IV owners want to sell or change, his IV then anyone can access his data from beginning to till date.

IV. USE CASE EVALUATION OF BLOCKCHAIN BASED IV COMMUNICATION

We have evaluated our proposed method with the help of use case. We have randomly chosen intersection use case example for our proposal explanation.

A. IV communication on Intersection scenario

For example, 4 IV (IV-1, IV-2, IV-3, IV-4) comes together on an intersection and almost on the same time. In this condition, how our proposed system will help to overcome this situation.

Before coming to the intersection, each IV shall broadcast its status on the network, for example, it will broadcast a message that it want to cross the intersection. Every intelligent vehicle (IV) will receive the broadcasted message in the network. They will first verify the trust bit D from VC, and then they will calculate the receiving time of a message from others. The vehicle which calculates the first time of message it has again broadcast the first coming vehicles Bit Trustothers vehicles will also calculate and verify the first comes Bit trust and give the fast way to go first.

For example in table 2. We have shown the bit trust ID of each vehicle and their message broadcast time, and receiving time from others.

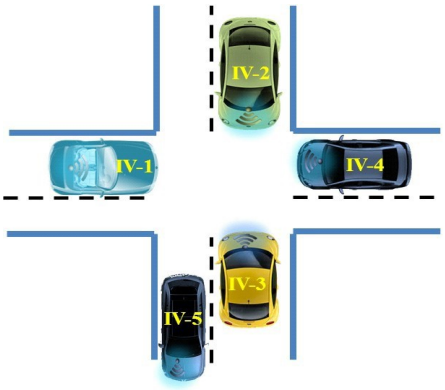

Fig. 10. Intersection scenario for IV communication

According to below table, IV-1 comes first on the Intersection region. So IV-3 which has calculated first will broadcast the message that IV-1 will move first based on first come first served and will also propose move sequences for other vehicles. Such as IV-1then next IV-2, then next IV-3 and last IV-4. Other IV (IV-1, IV-2, and IV-4) will calculate the time and agree with given schedule by IV-3. Now IV-1 will get reward as some bit trust with its own trust Bit ID. All this information will be stored on the vehicular cloud with their bit trust ID.

Note: our proposed mechanism use case is for general vehicles and not specified for Special vehicles such as ambulance, police, and VIP's vehicles, etc.

In evaluated use case, our vehicles are intelligent machine so they have enough computational power to calculate time, internet connected and self-driving vehicles.

TABLE II. IV MESSAGE BROADCAST WITH BIT TRUST AND TIME

Bit Trust ID	Message transmission Time (Sec.)	Receiver Bit Trust ID	Receiver Time: Sec	Reward
IV-1	1.00	IV-2	1.01	
		IV-3	1.03	
		IV-1->IV-5	1.06	
		IV-4	1.07	
IV-2	1.01	IV-1	1.00	
		IV-3	1.03	
		IV-1->IV-5	1.06	
		IV-4,	1.07	
IV-3	1.03	IV-1	1.00	IV-1->IV-3 0.5 bit trust
		IV-2	1.01	
		IV-1->IV-5	1.06	
		IV-4	1.07	
IV-4	1.07	IV-2	1.01	
		IV-3	1.03	
		IV-1->IV-5	1.06	
		IV-4	1.07	
IV-5	1.06	IV-1	1.00	
		IV-1->IV-3	1.03	
		IV-1->IV-5	1.06	
		IV-1->IV-4	1.07	

V. CONCLUSION

In this paper, we have presented a reward based intelligent vehicle communication based on blockchain technology and unlike previous researchers who have proposed blockchain technology for specific services. In our proposal, blockchain is used to remove centralize authority for the communication between IV. We have proposed crypto Bit Trust that will help to improve the privacy of IV. Trust bit provide fast and secure communication between IVs. It also helps to detect the history of IV. IV communication data will be stored for as long as the user wants it on VC. With the help of VC IV communication history and his reputation is available ubiquitously anywhere and anytime.

Future work, we will simulate our proposed mechanism in multiple use case scenario. Due to lack of time we have evaluate our proposed method with most common issue of IV Communication that is intersection communication. We will explain some more use cases during workshop presentation.

ACKNOWLEDGMENT

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the "ICT Consilience Creative Program" (IITP-R0346-16- 1008) supervised by the IITP (Institute for Information & communications Technology Promotion)

REFERENCES

1. D. Singh, M. Singh, I. Singh and H. J. Lee, "Secure and reliable cloud networks for smart transportation services," 2015 17th International Conference on Advanced Communication Technology (ICACT), Seoul, 2 015, pp. 358-362.
2. G. Yan and S. Olariu, "A probabilistic analysis of link duration in vehicular adhoc networks," IEEE Transaction Intelligent. Transportation Syst., vol. 12, no. 4, pp. 1227–1236, Dec. 2011.
3. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE I NFOCOM, San Diego, CA, 2010, pp. 1–9.
4. S. Olariu, M. Eltoweissy, and M. Younis, "Toward autonomous vehicu lar clouds," ICST Trans. Mobile Communication Computers., vol. 11, no. 7–9, pp. 1–11, Jul.–Sep. 2011.
5. M. Singh, D. Singh, and A. Jara, "Secure cloud networks for connected & automated vehicles," 2015 International Conference on Connected Vehicles and Expo (ICCVE), Shenzhen, 2015, pp. 330 -335.
6. Satoshi Nakomoto, Bitcoin: A Peer-to-Peer Electronic Cash System,BITCOIN.ORG 3 (2009), https://bitcoin.org/bitcoin.pdf.Satoshi Nakomoto, Bitcoin: A Peer-to-Peer Electronic Cash System, BITCOIN.ORG 3 (2009).
7. Madhusudan Singh, Shiho Kim, "Blockchain based Intelligent Vehicle Data Sharing Framework", arXiv preprint, arXiv: 1708.09721, 01 Sept. 2017.
8. Yong Yuan, and Fei-Yue Wang, "Towards Blockchain-based Intelligent Transportation Systems", 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Windsor Oceanico Hotel, Rio de Janerio, Brazil, Nov.1-4, 2016.
9. Benjamin Leiding, Parisa Memarmoshrefi, and Dieter Hogrefe. 2016. Self-managed and blockchain-based vehicular ad-hoc networks. In Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct (UbiComp '16). ACM, New York, NY, USA, 137-140.
10. Ali Dorri, Marco Steger, Salil S. Kanhere, and Raja Jurdak, "Blockchain: A distributed solution to automotive security and privacy", eprint arXiv:1704.00073, March, 2017
11. Sean Rowan, Michael Clear, Meriel Huggard and Ciaran Mc Goldrick, "Securing vehicle to vehicle data sharing using blockchain through visible light and acoustic side-channels", eprint arXiv:1704.02553, April,2017