2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) | 978-1-7281-9866-8/20/$31.00 ©2020 IEEE | DOI: 10.1109/MASS50613.2020.00013

A Trustworthy Blockchain based framework for Impregnable IoV in Edge Computing

Pralay Kumar Lahiri
Computer Science and Engineering
Kalyani Government Engineering College
Kalyani, India
pralaykr.lahiri15@gmail.com

Debashis Das
Computer Science and Engineering
University of Kalyani
Kalyani, India
debashis2124@gmail.com

Wathiq Mansoor
Electrical Engineering Department
University of Dubai
Dubai, UAE
wmansoor@ud.ac.ae

Sourav Banerjee
Computer Science and Engineering
Kalyani Government Engineering College
Kalyani, India
mr.sourav.banerjee@ieee.org

Pushpita Chatterjee
Computer Science & Engineering
Old Dominion University
VA, USA
pushpita.c@ieee.org

***Abstract*— The concept behind the Internet of Things (IoT) is taking everything and connecting to the internet so that all devices would be able to send and receive data online. Internet of Vehicles (IoV) is a key component of smart city which is an outcome of IoT. Nowadays the concept of IoT has plaid an important role in our daily life in different sectors like healthcare, agriculture, smart home, wearable, green computing, smart city applications, etc. The emerging IoV is facing a lack of rigor in data processing, limitation of anonymity, privacy, scalability, security challenges. Due to vulnerability IoV devices must face malicious hackers. Nowadays with the help of blockchain (BC) technology energy system become more intelligent, eco-friendly, transparent, energy efficient. This paper highlights two major challenges i.e. scalability and security issues. The flavor of edge computing (EC) considered here to deal with the scalability issue. A BC is a public, shared database that records transactions between two parties that confirms owners through cryptography. After a transaction is validated and cryptographically verified generates "block" on the BC and transactions are ordered chronologically and cannot be altered. Implementing BC and smart contracts technologies will bring security features for IoV. It plays a role to implement the rules and policies to govern the IoV information and transactions and keep them into the BC to secure the data and for future uses.**

Keywords*— *Internet of Things (IoT), Blockchain (BC),Internet of Vehicles (IoV), Edge computing (EC), Scalability, Green Computing

I. INTRODUCTION

Internet of Vehicles (IoV), part of Internet of Things (IoT) plays important roles to develop business models in digital economy. One of the purposes of IoV is to unfurl hazard information like accidental events, status of road with accuracy. Circulating critical messages to the region is the most challenging task as there could present malicious vehicle attacks. As malicious vehicle messages could affect the actual message to get circulated. As a result, the drivers and vehicles at the targeted area suffer through collateral damage. The norms of decentralized historical immutable messages are in the spotlight to the industries to apply it to their businesses. The properties of blockchain technology have been used in many business areas, such as banking, logistics, pharmaceutical industry, smart contract and most importantly IoV edge computing. There is already a trend of token-based blockchain that provides all shipment details of one company product. Several researchers have identified [1,2,3] that in digital revolution BC technology has emerged as an effective technology and has potentiality for energy efficiency and environment friendly. Here provided a discussion about similar kind implementation on IoV. Hence, it is important to identify the existing researches specifically related to the application of blockchain on IoV and edge computing. To identify the previous research that has already been conducted on blockchain and IoV, it is important to map out relevant works. Here the focus is on existing literature concerning the use of blockchain on IoV. In IoT or IoV data, location are in focus of researchers due to privacy leakage of information. It do not have the ability to encrypt or decrypt data. In case of EC location data could be in malicious attacks as IoV is unable to provide security.

There could be many research papers conducted on blockchain on IoV, one of the most recent papers of blockchain and IoV by Shrestha et al., [4]. In this study, the author shed some light on how edge computing can be implemented with the help of blockchain. Here IoV has been chosen as a field where made the research.

Edge computing (EC) [5] is come up with solutions for the scalability issue of IoT by providing more computing, networking, storage and also edge intelligence. The most applicable use of IoV in sense of IoT is for emergency response, video surveillance, speech recognition, etc.

Traditional security solutions are not capable to make IoV secure enough for the market. Blockchain, merged with smart contracts [6] produce a secure environment and include other activities like event-data, transaction details, difficulty level of the message, validity information of the transaction and distributed features of transactions. Xiong et al. [7], has contributed a small work on decentralized IoT and edge computing system. EC is a highly virtualized platform where end-users perform computing and data storage operations Blockchain technology plays role to establish connection between IoT/IoV devices and nodes [8].This paper has

2155-6814/20/$31.00 ©2020 IEEE
DOI 10.1109/MASS50613.2020.00013

introduced a blockchain framework that can be helpful to store messages and effectively validate trustworthiness. The key contribution of our paper can be summarized as below:

- Here proposed blockchain treats messages as transactions and validate it's trustfulness by using geographical location certificate and IoT implementation.
- Improved the scalability of the blockchain by using EC based on geographical locations.

The rest of the paper is organized as follows: Sect. 2 describes the different related work corresponding to blockchain framework, IoV and edge computing. Section 3 describes the proposed work including the detailed algorithm and flowcharts. Section 4 describes the experimental results of proposed algorithm. Finally, Sect. 5 has the conclusion and discussion of future scope of the proposed work.

II. RELATED WORKS

In this section, briefly explain BC concept, characteristics, and related applications on previous work which has been used in this paper. It also describes the benefits of BC against privacy and efficient use of resources in a decentralized system like IoV. Satoshi Nakamoto proposed the concept of BC as digital cryptocurrency. Due to consensus mechanism like PoW (Proof of Work), data or information are immutable in BC. Once data are stored in block, it cannot be altered. If it is altered then all hashes of previous blocks will be invalid the particular block be discarded from the chain.

BC is a decentralized system so each and every nodes separately have their own record of the BC as shown in Fig.1. A block should have minimal parts like previous block hash, nonce as numeric value, transactional hash vales in merkle root, timestamp to store time at transaction occurred. Transaction in formations to store message or other data storage as represented in Fig.1. To validate and link to previous blocks the header information of each block used.

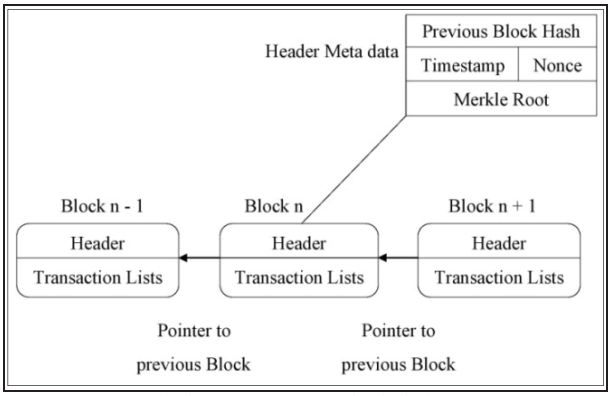

Fig.1. A typical structure of a Blockchain

In case of durability and attack resistance, as BC acts at decentralized system, it increases its ability to survive malicious attack and destroy or manipulate user information. It benefits users from scams.

In BC mining is a process which implement cryptographic puzzle like PoW to validate blocks created inside. By using nonce it generates unique hash value of usually 256 bit long for each block which make the system extremely hard to break. Overall process of mining is represented in Fig. 2. A consensus is used to achieve necessary agreement on a node to the network. In case of decentralized blockchain system shared storage system should be efficient, secure and real time. So that each and every transaction in the system become trustful and participated nodes accepts consensus mechanism.

Proof of Location (PoL):

It works on a device's geolocation that provides messages to other devices without having to trust the sender as it rely on location certificate. Geolocation devices are good enough for location detection of a vehicle, but unable to provide reliability of the vehicle, whether it is accurate or not. PoL works on independent nodes on a network system to verify secure location.

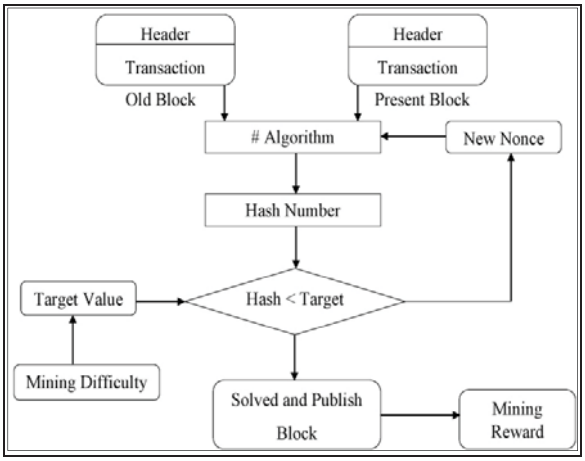

Fig.2. Mining process

Federated Byzantine Agreement (FBA):

Here consensus, nodes have a window to choose trustable persons in decentralized system. It is a public BC where each node can join at any time and get verified whenever needed. Quorum slices technique is used in FBA which denotes required number of nodes to satisfy the agreement. A decision by consensus among the validator could be applied on fresh block that permanently hold inside the local BC. FBA could detect misbehaving nodes in the network. Here consensus can be faster and efficient.

Each transaction mining generates new block (B_n)as shown in Fig. 1 consists of previous block hash (B_{n-1}), nonce value (N) and hash of all transaction or messages (M_n). The mining nodes search for a nonce value such as

$H(H(M_n) \parallel H(B_{n-1}) \parallel N)$ less than difficulty level (D).

$$H(H(M_n) \parallel H(B_{n-1}) \parallel N) \le D \quad (23)$$

Biwen Chen et al,[12] has described in his paper that Pseudo-random permutation Function undistinguishable from a random. Let's assume mapping

F: $\{0,1\}^N \times \{0,1\}^\beta \rightarrow \{0,1\}^N$. Here β is a security parameter. It is a pseudo-random permutation if

Given any $G \leftarrow \{0,1\}^\beta$, the mapping F is bisection from $\{0,1\}^N to \{0,1\}^N$.

For any probabilistic polynomial-time adversary

$PA, |\Pr[PA^{F_G}(1^N) = 1] - \Pr[PA^f(1^N) = 1]| < \varepsilon,$

$where G \leftarrow \{0,1\}^\beta$, if is a random permutation on L-bit strings and ε is negligible.

Given any $G \leftarrow \{0,1\}^\beta$ and $x \leftarrow \{0,1\}^N$, computing $F_G(x)$, there exists an efficient algorithm to compute $F_G(x)$. Besides, the inverse permutation

$F^{-1} : \{0,1\}^N \times \{0,1\}^\beta \rightarrow \{0,1\}^N$ is the inverse of pseudo-random permutation function F: If $F_G(x) = y$, then $F_G^{-1}(y) = x$. Both the DES and AES are the classical instances of pseudo-random permutation function.

Jianli Pan et al. [8] has proposed a framework based on BC and smart contracts. Here they describe a different approach and framework to merge blockchain and edge computing named EdgeChain. The EdgeChain position is in between edge cloud platforms and various IoT/ IoV applications those who belong to a shared system as shown in Fig.3. EdgeChain is capable to run on various cloud platforms. EdgeChain behaves like a permission blockchain. Smart contracts are also implemented. It controls the number of connected devices connected to the edge cloud resource pool.

In [4] authors have proposed that Mobile Edge Computing (MEC) that helps to generate block event among miners which could help to lower the propagation delay. MEC could serve cloud edge communication at every edge of VANET node [9] [10].

VANET acts a vital role in saving life and property of the passengers by unfurls emergency information. It holds different types of communications like Vehicle-to-Infrastructure (V2I) and Vehicle-to-Vehicle (V2V) communication. That message needs to be circulated real time with accuracy. If it fails to circulate within conditions, may causes collateral damage. Trust a vehicle and its message is one of the highlighted issues in VANET.

Lin et al.in [11] described a framework of secure BC of user authentication. It combines Event Authentication Code and signatures. Malik et al., proposed a blockchain based intrusion detection systems for internet of things-based applications. Castellanos et al.in [12] discussed that BC has the capability to implement green certificates for authentication that helps to remove third party administration process and reduce transactional costs.

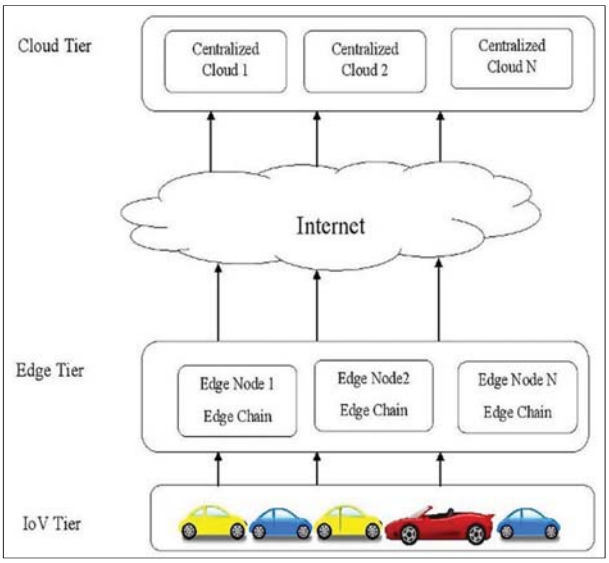

Fig 3: Edge Chain Example Scenario

III. METHODOLOGY

A different model of blockchain has been proposed to overcome the issue of event authentication. Proof of Location (PoL) is used to generate location certificate for all the vehicles. It has been assumed, vehicles can communicate efficiently to edges through internet. The local events create genesis blocks by the help of RSUs to start the BC. The vehicle has more computing power and high trust level can participate in mining.

Road Side Unit (RSU): The RSUs are used within communication range for vehicle to edge communication and by generating location certificate to the vehicle to give authentication.

Vehicles: In VANET BC system, vehicles are the main elements. After event information are generated it mines new blocks and by verifying it, stores the messages in the BC.

Blocks: A block is made of a header, body of block, previous and current block hash value, special number named as nonce, difficulty of the target, transaction timestamp, and Merkle root.

Location Certificate: It produce a certificate of a vehicle at a particular time based on its location to verify whether it actually present at that event location or not with the help of RSU as a validator.

All the vehicles location needs to maintain PoL to get location certificate at provided timestamp. A location certificate generated by a reasonable RSU called as PoL. It has drawbacks on scalability. Here events are local, i.e. message-events are limited within a geographical area. In BC, the new block is shared globally. As it is focused on emergency event message, in that case, EC help to speed up and frequent block generation

in mining. Here EC server works on PoW for providing a solution to the miner when it requests for edge services. Then the miner node circulates the PoW solution to the network. It also uses the IoT Proxy to make legacy devices interactive with the framework. Device registration is done here for legacy and non-legacy. However, for non-legacy nodes, it has access to BC to create an account. Followed by the IoT Proxy module it has Smart Contracts and its Interface, blockchain server, application interface, and edge resource-provisioning modules. In the last module, the process for the requested task and if the data is not available in the edge server it will coordinate with the neighbor edge server to get the required resources. Here is a brief explanation of the proposed model and algorithm. Here Legacy Device is those vehicles who don't have any account present in the system and non-legacy device are those vehicles which have an active account. Proxy helps legacy vehicles to create a new account. In blockchain server mining and blocks have been produced to create blockchain as a transaction or data storage system. The next edge resource is present as cloud resources where data from local servers are served to the edges in the same format.

Algorithm 1 Algorithm for message passing to the edge server

Input: Initiating message
1: Connect to multiple number of IoV devices
of different locations and make a set of it.
Set of IoV devices is represented as
$VN^{ZN} = \{VN^{ZN_x}(n_1).....VN^{ZN_x}(n_j)\}.VN$
Here VN is the virtual machine to whom IoV tries to connect,
ZN represents location of IoV devices,
ZN_x represent the IoV device of the particular location
where x is the IoV device number and
$n(n_1, n_2, ..., n_x)$ represent number of IoV devices
connected to the particular location.
2: for $(x = 1\ to\ n)$
3: if $(VN^{ZN_x}(n_x) =$ Legacy IoV Device $)$ then
4: Register it by using IoV Proxy
5: call for Smart Contract
6: end if
7: if $(VN^{ZN_x}(n_x) =$ Non-Legacy IoV Device $)$ then
8: call for Smart Contract
9: end if
10: end for
11: Inside Smart Contract Encapsulation is done.
12: ZN_x start Mining
13: Mining Winner broadcasts the Block.
14: for (All VN)
15: Implementing different VN
16: then each Edge and corresponding chains get updated.
17: end for
18: return ZN_x

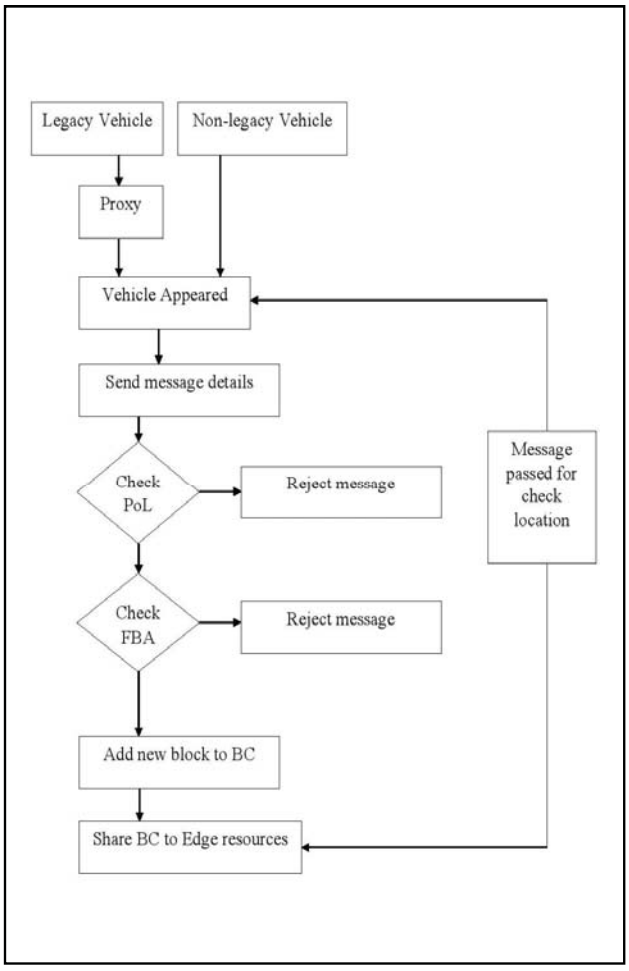

Fig.4. Proposed Blockchain workflow

The work process of the proposed work is as below. At first, there are two different kinds of devices are present as legacy and another is a non-legacy device. If there any new vehicle comes to communicate to the system, it falls under the legacy device and it needs to get registered by using the proxy to communicate with the first stage of smart contract that is PoL which fall into Algorithm from step 2 to step 2.5. But for the non-legacy vehicle as its account is already created so it can directly apply PoL as the first stage of smart contract to validate the location certificate of the message passing vehicle. Each vehicle send message in form of block as explained in Section 2. Once the block gets passed the PoL consensus mechanism goes to the next step otherwise message get rejected and stop mining for the block and will not go further steps.

Next, it passes to the blockchain server and here it goes through another consensus as FBA and store the activity logs according to the transaction has been done. It makes data more secure that makes very difficult for any malicious attack. If block do not match the consensus as FBA, it will be rejected and stop mining for the particular block and returns to the initial stage. To implement EC here a decentralized edge resource has been proposed which is maintained as location or region wise. Where VN_x is responsible for a particular virtual machine where x represents different locations.

Any non-legacy vehicle able to retrieve information related to any location. Once it passed into BC server after FBA consensus checking, BC server add the new block to the local blockchain which contain all the relative information and location of the vehicle. Lastly BC is shared to the edge resources so that it could be processed easily from other devices. Any vehicle that get registered could directly access the location status through location parameter. The edge service is provided to fit the alternative specifications of requests.

IV. Observation and Discussion

To develop the edge server here Windows 10 operating system has been used with Go-ethereum [11] to run the blockchain framework. Along with those as a development language Solidity and Truffle used for deployment tool and Node.js has been used to create the interface for interactions between IoV and blockchain.

After the IoV devices get registered the transactions have broadcasted to all the other device connected to the system then new transactions have formed as blocks, verified through mining. Here the average CPU (Central Processing Unit) utilization was 45% along with memory utilization was 22% during mining and in case of idle situation CPU utilization was 6% along with memory utilization was 12% . During mining utilization is higher due to commit new blocks and make the transactions in the decentralized system.

As here blockchain is implemented on a distributed system, each and every registered devices have to be synchronized. In our system after the local system made the transaction it then get updated to the edge server to maintain the synchronization so that other device could access it and improve the scalability. In our system average block size is 675.08 bytes. In 25 blocks minimum block size is 661 bytes and maximum block size is 690 bytes. As the proposed system is distributed in nature, it makes the system robust and durable. Each system holds its local data and shared data on edge server. Also as it is a distributed system so connected IoV devices also have a copy of local data. If any of the system goes down then it has multiple backups to recover it from local and edge server both. Moreover in every ten minute BC checks transaction blocks. It requires very high computation range to make changes in side any block that ensures security.

To elaborate on the importance, effectiveness and global impact here some different points have been taken as below. Here, BC has made the message system not only secure but also efficient in processing. Comparing with other IoT system it always suffers from scalability and security issues. Implementation of BC with EC technology makes the resource available to every node whenever and wherever it needs. So, besides a secure system, it resolves the scalability. The proposed system not restricted for IoV storage purpose or message events but also in many other applications like healthcare system, cloud document storage, secure social message passing system, bank information system, defense sectors, etc. as it works on EC by using BC technology. In all above cases it works on different sectors but the proposing system could be same. The proposed work mainly focused on two sections, one is security and another is scalability. By following the proposed workflow it eliminates the security issues faced by IoT or IoV devices and as here EC has been applied, so it also covers the scalability issues by providing cloud resources that hold the same cryptographic data or transactions as present in BC. So any non-legacy or legacy devices or vehicles which were previously connected or not connected to the BC could fetch transactions.

It helps to share feedback on the current geolocation if it is accidental, heavy traffic, fastest route, blocked rout, etc. Moreover, this system has the range to spread an emergency message based on location whenever there any accidental or emergency event occurred.

As the paper is describing a message storage system, so it could be effective in case of making a social message sharing system for emergency cases where it provides a trustless framework that does not depends on any user authentication. Rather than this, it could help to build a resource storing system for the banking industry and make it more secure and efficient for transaction storage and passing. So this paper provides the window to other researchers for other application-based research works on similar storage and a transaction-based system where scalability is needed.

The methodology proposed and discussed here has followed scientific correlation and explanation on providing security and scalability on EC by implementing BC technologies [2]. There could be much work proposed on the security issues on the IoV system. But here the paper proposed a workflow that correlates Edge Computing and IoV by using BC. That eliminates security issues of an IoT system and eliminates the performance by improving scalability with the help of EC implementation.

V. CONCLUSION AND FUTURE SCOPE

In the proposed scheme, blockchain technology could maintain the trustfulness of messages. Here BC could independently work within a region to store and distribute message trustworthiness in distributed ledger. VANET and EC has been integrated with BC to edge resources to store behavior of each IoV devices. The PoL consensus mechanism has been adopted here. Here, consensus of mining block has been established to create new block. The combination of FBA and PoL consensus along with EC technology makes a hybrid consensus to improves the scalability, reduces block generation time, make system robust and secure vehicular network. Furthermore, this work is specifically designed for the upcoming smart city component as it aims to achieve the flavor of energy optimization as well as bio-friendly environment.

REFERENCES

[1] A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.

[2] Chen, L. Wu, H. Wang, L. Zhou and D. He, "A Blockchain-Based Searchable Public-Key Encryption With Forward and Backward Privacy for Cloud-Assisted Vehicular Social Networks," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5813-5825, June 2020, doi: 10.1109/TVT.2019.29593

[3] A. A. Malik, D. K. Tosh and U. Ghosh, "Non-Intrusive Deployment of Blockchain in Establishing Cyber-Infrastructure for Smart City," 2019 16th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON), Boston, MA, USA, 2019, pp. 1-6, doi: 10.1109/SAHCN.2019.8824921.

[4] R. Shrestha, R. Bajracharya, A. P. Shrestha, S. Y. Nam, "A new type of blockchain for secure message exchange in VANET", Digital Communications and Networks, 2019.

[5] J. Pan and J. McElhannon, "Future Edge Cloud and Edge Computing for Internet of Things Applications," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 439-449, Feb. 2018.

[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016.

[7] Z. Xiong, Y. Zhang, D. Niyato, P. Wang and Z. Han, "When Mobile Blockchain Meets Edge Computing," in IEEE Communications Magazine, vol. 56, no. 8, pp. 33-39, August 2018.

[8] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4719-4732, June 2019.

[9] R. Shrestha, R. Bajracharya, S. Y. Nam, "Challenges of Future VANET and Cloud-Based Approaches". Wireless Communications and Mobile Computing, pp.1-15, 2018.

[10] Velasquez, K., Abreu, D.P., Assis, M. et al. "Fog orchestration for the Internet of Everything: state-of-the-art and research challenges," J Internet Serv Appl 9, 14,2018.

[11] G. Wood, "Ethereum: A secure decentralised generalised transactionledger," Ethereum Project Yellow Paper 151 (2014): 1-32.

[12] Castellanos, J.A.F.; Coll-Mayor, D.; Notholt, J.A. Cryptocurrency as guarantees of origin: Simulating a green certificate market with the Ethereum Blockchain. In Proceedings of the IEEE International Conference on Smart Energy Grid Enegineering, Oshawa, ON, Canada, 14–17 August 2017.