Blockchain Based Privacy and Security Across Cloud in Electric Vehicle Application for Sustainable Development in Industry, Innovation and Infrastructure

S. Brilly Sangeetha [1*] & Krishna Prasad K. [2]
[1] Post Doctoral Research Fellow, Institute of Computer Science & Information Science, Srinivas University, Karnataka, India,
OrcidID: 0000-0002-0989-3277; E-mail ID: brillyvino82@gmail.com
[2] Associate Professor, Institute of Computer Science & Information Science, Srinivas University, Karnataka, India,
OrcidID: 0000-0001-5282-9038; E-mail ID: krihnaprasadkcci@srinivasuniversity.edu.in

Area/Section: Computer Science.
Type of the Paper: Experimental Research.
Type of Review: Peer Reviewed as per |C|O|P|E| guidance.
Indexed in: OpenAIRE.
DOI: https://doi.org/10.5281/zenodo.7178293
Google Scholar Citation: IJMTS

How to Cite this Paper:
Brilly Sangeetha, S., & Krishna Prasad, K., (2022). Blockchain Based Privacy and Security Across Cloud in Electric Vehicle Application for Sustainable Development in Industry, Innovation and Infrastructure. *International Journal of Management, Technology, and Social Sciences (IJMTS), 7*(2), 347-358. DOI: https://doi.org/10.5281/zenodo.7178293

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.

CrossRef DOI: https://doi.org/10.47992/IJMTS.2581.6012.0225

Received on: 17/08/2022
Published on: 10/10/2022

Blockchain Based Privacy and Security Across Cloud in Electric Vehicle Application for Sustainable Development in Industry, Innovation and Infrastructure

S. Brilly Sangeetha [1*]& Krishna Prasad K. [2]
[1] Post Doctoral Research Fellow, Institute of Computer Science & Information Science, Srinivas University, Karnataka, India,
OrcidID: 0000-0002-0989-3277; E-mail ID: brillyvino82@gmail.com
[2] Associate Professor, Institute of Computer Science & Information Science, Srinivas University, Karnataka, India,
OrcidID: 0000-0001-5282-9038; E-mail ID: krihnaprasadkcci@srinivasuniversity.edu.in

ABSTRACT

Purpose: *In this paper we utilise electric vehicle-based cloud edge (EVCE) computing, it is possible to integrate vehicle contexts in a seamless manner. With the increasing use of electric vehicles (EVs) in V2X, this is likely to become a trend. When it comes to information and energy exchanges, a hybrid cloud/edge computing system with EVs as a potential resource infrastructure presents considerable security challenges. In order to find context-aware vehicular applications, the viewpoints of information and energy interactions are taken into consideration. The use of distributed consensus has resulted in the creation of blockchain-inspired energy and data coins, which use the frequency of data contributions and the amount of energy contributions to demonstrate the proof of work for each coin. When it comes to protecting vehicle interactions, the industry, innovation, and infrastructure sectors of Envision2030 are confronted with a number of different security alternatives.*
Design/Methodology/Approach: *The EVCE computing for mobile cloud architecture to the electric vehicle acting as the edges across the network. The unutilised energy resources, and communication and computational resources of EVs are pooled together and used for other purposes. Mobile cloudlets for electric vehicles are created using VANETs and other interconnected services that gets connected together. When EVs are parked for extended periods of time in different locations, they form a cooperative network of services. Incorporating flexible connected EVs into traditional cloud infrastructures enables contact with remote service providers, local area networks (LANs), as well as other organisations, while operating in the cloud computing mode.*
Findings/Result: *The primary purpose of a blockchain application is to maintain a record of all of the transactions that have been made by the various members of the network. After the submitted transactions have been confirmed and arranged, a block is formed, and the outcomes of the transactions are put on the blockchain as transaction results.*
Originality/Value: *When it comes to transactions, HLF three-stage revolutionary design, dubbed execute-order-validate, is reliant on the preceding steps of the transaction to function properly. Because the actual throughput is close to 100%, a 100 TPS transmit rate is achievable and sustainable*
Paper Type: *Experimental Research*
Keywords: Blockchain, Electric Vehicle Application, Cloud Computing, Sustainable Development

1 . INTRODUCTION :

Using an appealing network architecture known as electric vehicle cloud and edge computing, which connects disparate vehicular settings seamlessly in order to pool scattered electric cars (EVs) into a single pool of resources and use the vehicles for locally flexible use, a network architecture known as electric vehicle cloud and edge computing is being developed [1]. Because of the sensitive data they

handle and the complex context in which they operate, cargo apps raise significant security problems [2]. With the introduction of self-driving automobiles, distributed vehicular resources are becoming more and more appealing to businesses [3]. EVs are a critical component of connected services because of the energy, connectivity, and computation resources they supply, among other things. When EVs are not in use, their idle resources can be pooled together to form a mobile resource pool that can be used for collaborative tasks. By spreading and aggregating EVs throughout their activity cycles, it is feasible to build an ecosystem of EVs, roadside units (RSUs), sensors, and local aggregators (LAGs) [4].

The combination of edge and cloud computing, which have the following three characteristics, will be increasingly used in vehicular applications in the future. Due to the fact that both legal entities and attackers have equal access to the system, the EVCE presents significant security challenges in comparison to traditional systems [5]. For example, an EV can supply distributed resources such as dynamic traffic information and idle electricity. An attacker could receive omnidirectional communication through the use of wireless channels and open interfaces [6]. Blockchain is hence regarded as a viable solution that possesses two essential characteristics that can help to alleviate security problems. In this case, participants in block transactions that are carried out through the use of consensus procedures [7].

When it comes to the blockchain, cryptographic methods are employed to establish trust between two or more parties, which is exactly what is happening. Collaboration in large quantity is driven by data ambiguity and self-interests is hence considered as a minor consideration in this context. When the appropriate messages are authenticated by a majority of participants (adding new block in a ledger, and the previous block is removed) [8]. Because of its unique data format, it has improved robustness against a single point of failure, as well as data traceability, which helps to prevent tampering attempts [9]. Security improvements have been proposed and implemented, including blockchain key management [10], multi-signature [11], and secured network architecture [12]. Information and energy transactions are discussed in this article as a means of improving the security of information and energy transactions. In this paper session 2 presents the related works, session 3 briefs the objective, session 4 describes the methodology,session 5 gives the results and discussions, and session 6 conclusion.

2. RELATED WORKS :

This section provides an overview of the history of Bitcoin, as well as its characteristics and how it might be used as a form of identification. This section also looks at the blockchains that have been approved.

Bitcoin :

Early work by Satoshi Nakamoto on the world first cryptocurrency, Bitcoin [13], addressed the concept of employing anonymous internet users to communicate with one another in order to establish a decentralised payments in electronic system. Encryption-enabled computing nodes or networks that collaborate and execute transactions with the help of cryptography are referred to as a block or a network.

According to the Bitcoin system, each user is assigned a digital wallet, which serves as a repository for both their public and private keys, as well as any bitcoins they may have [14, 15]. The wallet can be accessed by the user by entering his or her private key. The information contained in a user public key pertains to the user Bitcoin address or wallet. The public address of each party must be known by both parties before any form of transaction can take place between them. The entire quantity of coins exchanged, as well as the particular address where the coins were swapped, are logged in each transaction.

Permissioned Blockchain :

It is possible for certificate authority organisations all over the world to join the blockchain network because blockchain technology allows for distributed nodes. Certificates are issued by this authority, and they are validated through the use of a consensus mechanism. Consensus certificates are kept on the blockchain [16], which is a distributed ledger technology.

These certificates have been approved by the CA. Despite this, ensuring anonymity while all members are on the blockchain is challenging to achieve in practise. Because the certificate contains a genuine name, maintaining anonymity becomes difficult. When the certificate holder submits the certificate to the website or service provider, the true identity of the certificate holder is exposed.

In order to operate, PAPKI proposes using a Registration Blockchain (RBC) and a User and Certificate Blockchain (UCB), both of which are permissioned blockchain-based (CBC). The responsibility of RBC is to encrypt a user identifying information, followed by the responsibility of preserving that information once it has been decoded. The Certificate Blockchain node is in charge of certifying and authenticating people, as well as reserving anonymous digital certificates and digitally certified data.

Table 1: Comparative Study

Study	Limitations
Predictive Modelling	Overfitting is a big problem
Unsupervised technique	Low imbalance rates.
Supervised Machine Learning	Not feasible solution
Unsupervised Machine Learning	Poor processing on large amount of data
Ensemble Machine Learning	Weaker Predictive Power
Deep Learning	skewed statistics

Source: Author

3. OBJECTIVE :

The study aims at developing EVCE computing in the mobile cloud at the network edge to control the electric vehicle. Mainly focussing on the security issues in hybrid cloud/edge computing systems with EVs.

4. METHODOLOGY :

In this section, we present the EVCE computing for mobile cloud architecture to the electric vehicle acting as the edges across the network, as represented in Fig 1. The first technique is known as edge computing, and it is described in more detail below.

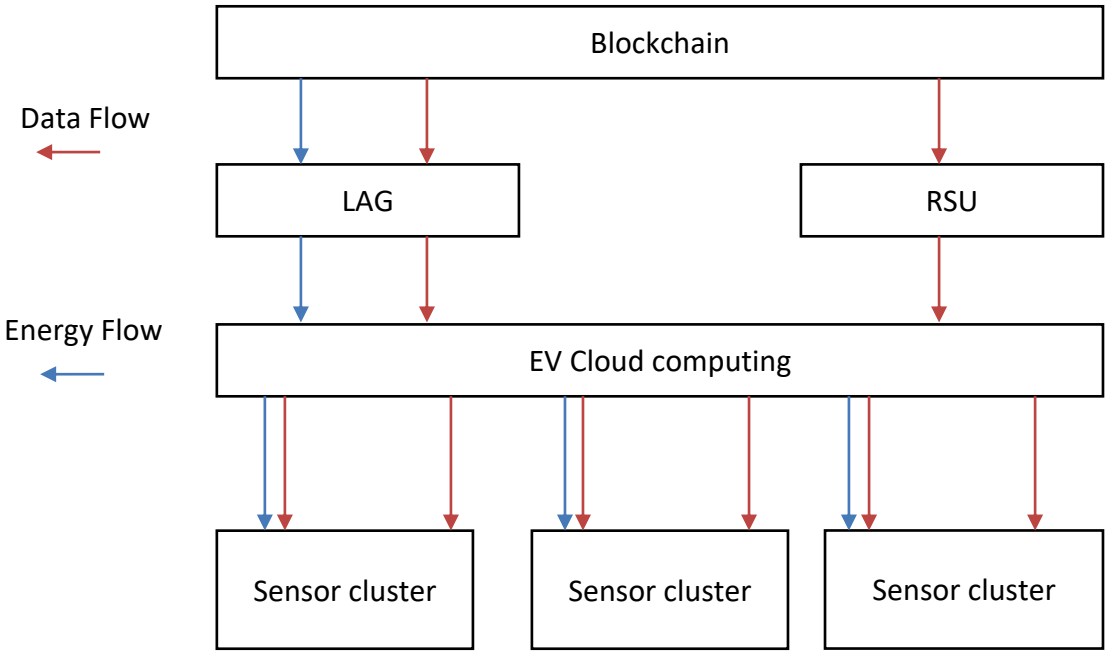

Fig. 1: Architecture of EV in Cloud

Source: Author

The unutilised energy resources, and communication and computational resources of EVs are pooled together and used for other purposes. Mobile cloudlets for electric vehicles are created using VANETs

and other interconnected services that get connected together. When EVs are parked for extended periods of time in different locations, they form a cooperative network of services. Incorporating flexible connected EVs into traditional cloud infrastructures enables contact with remote service providers, local area networks (LANs), as well as other organisations while operating in the cloud computing mode.

(1) VANET Interactions with Blockchain:

In order for the Internet of Vehicular Energy to function, energy interactions, and network of information must be established.

Vehicular Information Interactions:

The establishment of wireless links via EVs with a large number of sensors to provide distributed perception and cooperative processing for tasks such as traffic monitoring and identification of road environment. The sensor data is collected by electric vehicles in order to meet a variety of functional requirements. There is a significant amount of vehicle data saved on the EVs for short periods of time, but only a small amount is transmitted to the entities.

EVs serve as distributed nodes that collect data for optimal delivery of services like traffic inquiry, driving assistance, and entertainment sharing, among others. Resources in EVs can be re-allocated to fit the demands of individual users. This is achievable. Information is exchanged most frequently in this environment through V2I and V2V connections, which are the most common types of connections. EVs communicate with a LAG as well as other permanent infrastructure, such as parking lots that serve as information servers, when they use V2G technology to exchange data between them.

Vehicular Energy Interactions:

A vehicle (EV) performs changing and discharging actions in the roles of energy demand, storage, and supply while communicating with another vehicle (V2G). In addition to serving as a conduit between the grid and the electric vehicles it collects, a LAG contributes to the consolidation of dispersed energy resources.

EVs have the ability to exchange energy with a LAG through the use of their own batteries, which allows them to save on fuel. With the arrival and departure of EVs from a specific place, a flexible and large energy resources are designed. The resource size changes over time as EVs arrive and depart from the location. An EV that travels over several area networks relies on distributed energy support to complete its life cycle.

(2) Blockchain Workflow:

Detailed discussions of each of these concepts will be provided in the following paragraphs.

Revoke Digital Certificate:

Anonymous certificates may be misused in a number of ways, including violation of the terms and conditions of usage, abuse, certificate expiration, and leakage of the main key. The following is the procedure to be followed when cancelling anonymous certificates:

- That person request goes to a CBC node, and it is that node that gets and processes the request.
- When CBC receives a user request, it employs the tracing function of an anonymous certificate to determine the legality of the signature and then delivers the results to the request partner nodes.
- Once all nodes have received a request for a certificate application, the RBC runs a search using the user public key as a reference, and the search results are returned to the user. From Figure 1, the exchange of data between blockchain and cloud takes place in the form of public and private keys.
- The user identity is validated after a match is made, and at that time they are routed to the companion nodes.
- The results of the companion nodes are collected, and it is up to the CBC nodes to determine the final results of the overall verification procedure. It is possible that the overall outcome will be positive if the number of nodes that passed the verification process exceeds two-thirds of the total number of nodes.
- The end user should be able to view the results of the execution process.

Tracking Digital Certificates:

Service providers may occasionally request that CBC retain track of or make a note of a certain anonymous certificate in order to provide an additional degree of protection. Having this functionality

comes in handy in the event that an anonymous certificate is discovered to be bogus. For the purpose of obtaining an anonymous certificate, this is the typical approach.

- An Anonymous Certificate generated by the blockchain can be used by users to register with or verify with a service provider after they have obtained the certificate.
- If a violation of anonymous certificates is discovered, the service provider notifies all partner nodes of the user request to have the certificate revoked.
- The CBC nodes all review the anonymous certificate, and the results are broadcast to the rest of the network to ensure that it is valid.
- Consensus nodes on the Certified Blockchain vote in accordance with a predetermined procedure. Validation is carried out if the number of nodes that have been revoked exceeds two-thirds of the total nodes.

(3) Operation of Smart Contracts :

In this paper, we present a fundamental investigative smart contract architecture, which is founded on the concept of life-cycles. Previous studies are taken into consideration when developing this paradigm. The importance of raising public knowledge of the ongoing development of Blockchain technology in order to promote its adoption. In order to compare and categorise blockchain-based systems, we can use a taxonomy to do so. This allows us to enhance our architecture in order to gain better results from Blockchain-based systems. Further dividing blockchain architecture into application and fabric layer, and then created a detailed metaphysical substructure that was further divided into two tiers, the application and fabric layers. It is proposed that a six-layered structure be used for the proposed research substructure.

Ethereum:

A smart contract, which is a transaction-based state machine, is presently the most extensively used platform for constructing smart contracts, with Ethereum being the most popular. As time passes, the state changes gradationally, and the transactions that contribute to the final state are carried out one at a time.

Generally speaking, these final states are considered the most official versions of Ethereum. In contrast to the UTXO model of Bitcoin, Ethereum introduces the concept of accounts. Personal accounts and corporate accounts are the two types of accounts. Contract accounts (also known as contract accounts) are accounts that are contracted with a third party and Executive Orders.

Private keys take precedence over the contract code in favour of the latter, which does not necessitate the use of any associated code in order to function. An EOA is necessary before a transaction may be initiated. Transactions can include both ether and binary data, depending on the protocol (payloads). Activation of the contract account and execution of the corresponding code in the local EVM are both performed when the receiver account is a contract account. Miners verify transactions by publishing them to the Blockchain network, which serves as a validation system.

Hyperledger Fabric:

The Hyperledger Fabric project, which is hosted by the Linux Foundation, is an implementation of the Blockchain framework. However, companies and organisations that are tied to specific businesses can join through a membership service provider. However, anyone can join Ethereum and Bitcoin because they were made available to the public. Organizations that contribute to and assist in the growth of the network are those that are permitted to join the Hyperledger fabric. Peers host chain ledgers and codes, which are used to track transactions. Additionally, when chain code is invoked, there is a state transition (transaction). The ledger is updated, created, or deleted when a set of value pairs with assert keys is generated as a result of a transaction.

Security Requirements and Distributed Consensus:

In addition, security requirements such as the CIA trinity, authentication, authorization, and accounting should be addressed and addressed properly. Protecting personal information (such as a user charge status, location, and identity) falls under this category. Because of the routing limitations in wireless networks, the identity impersonation, data manipulation, and privacy violations are all more difficult to perpetrate in EVCE computing.

Hence, traceability is used for referring to the data provenance in the context of associating blockchains with EVsservices. Traceability is used to identify the data lineage trace. It is vital to follow the courses taken by data and energy as they go from one location to another during interactions. Because

participants have the same rights to participate as attackers and legal entities, it is possible that interactional data will be abused or manipulated.

For the purposes of this definition, the term transparency refers to the capacity of one entity (for example, an EV) to know exactly where and when another entity (for example, a LAG) obtains the relevant data. In the software-defined security paradigm, scrambling algorithms should be used to confuse secret data in order to prevent it from being interpreted by irrelevant entities (e.g., zero-trust model). In EVCE, there are a number of security problems to be aware of.

Because EVs establish information interactions in addition to the sharing of computation resources, achieving data access control and traceability while dynamically participating in EV cloud computing is a difficulty. Since EVs develop energy interactions based on the sharing of energy resources, it is challenging to transmit the energy aggregated while respecting the privacy of individual identities.

There are a number of instances in which dispersed data is used to compute results for a particular purpose. When capturing sequences, keep in mind the significance of spatial and temporal features. It is recommended that each piece of data be marked with a lineage tag in order to better identify its sources. EVs have dynamic positions when it comes to location identification, but RSUs and LAGs are deemed to have static locations when it comes to determining the location associations between the interacting elements, respectively.

(4) Distributed Consensus:

When using EVCE computing, all users work together to jointly validate blocks, which is similar to the blockchain features. The blockchain must first achieve a distributed consensus among all participants in order for transaction data to be added in the distributed ledger. When it comes to consensus algorithms, the two most prevalent ones to utilise are PoW and PoS, both of which have their own set of advantages and downsides. With the PoW being fully reliant on processing capacity, participants compete to gain correct data writing while knowing that they have a poor chance of success. When playing at the point of sale, the total stakes of each account are used to determine which one is chosen. A new cryptocurrency for vehicles, known as data and energy coins, is available in this country. Vehicle data is stored on a consortium blockchain, and distributed consensus mechanisms are formed as a result of interactions between information and energy systems. The vehicle records areencrypted and arranged in the form of blocks in accordance with predetermined distributed consensus procedures, and LAGs and RSUs will each audit and offload the data it in chronological order to a blockchain for verification, based on predefined distributed consensus methods.

Contribution of PoE:

An energy coin is handed to each person who uses power in exchange for proof of the electric vehicles contribution to the nation's energy supply. The LAGs that have been approved follow a consensus method, and smart metres measure the amount of energy that has been discharged. It will be possible to earn energy coins for electric vehicles that urge other electric vehicles to take part in the discharging process by giving the most energy during a specified time frame.

Only EVs are permitted to utilise the data and energy tokens, which are legal tender and can be freely traded. Because of their fundamental functions of data distribution, the sensors will not be able to gather data coins during information exchanges. Because of a shortage of spare power, no energy coins are exchanged between sensors and RSUs during the course of these exchanges, resulting in a loss of data. These two criteria are used to identify who is represented in a majority decision-making process when a majority vote is required.

There are developed data and energy currencies that can be used to give resources to the vehicles in the system, and these coins have already been established. Each time an EV makes a contribution to collaborative intelligence, it will receive data coins in exchange for its efforts. It will be given greater access to the resource pool more quickly, and the data it creates will be given greater credibility as a foundation for decision-making. When an EV returns an additional kilowatt-hour to the grid or another entity, it earns more energy coins and is given a higher priority for the utilisation of energy.

(5) Security Solutions:

RSU and LAG, as well as numerous sensors, are all components of EVCE computing, as are moving electric vehicles (EVm), discharging electric vehicles (EVd), and charging electric vehicles (EVc). Data

and energy coins are taken into consideration when EVs interact with one another; anonymous data transmission and aggregated energy transmission are both feasible.

Information Driven:

EVscan thus act as a network operators in order of establishment of V2V communication. There are numerous EVs in the vicinity, and each of them communicates with the others in order to complete cooperative responsibilities. The use of data coins to provide anonymity authentication and access control for data interchange and sharing among these moving electric vehicles should be studied.

Moving EVs tends to execute the key agreement and distribution and produces the session keys can be produced through the use of symmetric encryption in moving EVs. Routing via shortest path and key mode of multi-path type are two techniques that can be utilised to achieve group key agreement. Following that, the RSU and moving EVs initiate conversations by posing access obstacles and responding to them. In this scenario, where moving EVs collaborate to exchange data, it is conceivable to broadcast signed data to other EVs using homomorphic encryption and safe multi-party computing.

When multiple EVs are in motion, it has a direct impact on the distribution of resources among them because of the encrypted data currency. Using spatio-temporal features and conditional proxy re-encryption, data sharing and data concealment concerns amongst different enterprise virtualization (EV) systems can be handled.

Energy-Driven:

The LAG facilitates the creation of an aggregated energy resource pool by the use of several discharging electric vehicles, which act as virtual power plants in the process. During transmission, the energy from these discharging EVs should be aggregated in order to protect their privacy.

In order to begin a session, pseudo-random numbers generated by EVd1, EVd2, EVdj are delivered to the LAG by the EVd servers. As soon as the two entities begin communicating, the LAG receives the aggregated identities for the EVs and uses them for mutual authentication. It is possible to transmit data totally anonymously using ECDSA-based signatures.

When it comes to charging, electric vehicles have a wide range of alternatives. The energy that an EV generates when not in use is returned to the grid, which is then used to aggregate distributed energy sources (DERs). During energy exchanges, energy is viewed as a non-differential resource, which means it has no value. Energy pools are produced when a group of EVs that are all charging at the same time share their resources. The MHT can be used to protect sensitive information from being disclosed to the wrong people. This data structure does not contain all of the data fields since it is necessary to verify a large data structure in an efficient and secure manner.

5. RESULTS AND DISCUSSIONS :

The primary purpose of a blockchain application is to maintain a record of all of the transactions that have been made by the various members of the network [17-27]. After the submitted transactions have been confirmed and arranged, a block is formed, and the outcomes of the transactions are put on the blockchain as transaction results.

When it comes to measuring the performance of blockchain applications, the Hyperledger Performance and Scale Working Group recommends the following metrics:

- **Transaction Throughput**: It is defined as the total transactions committed by the blockchain in a certain period of time that is measured in seconds, on a given blockchain.
- **Transaction Latency**: The total time it takes for the blockchain to record a transaction is referred to as Transaction Latency. After much consideration, it was found that this system could be used to measure the latency and throughput of the proposed model.

It was the aim of the study to demonstrate the framework's effectiveness by comparing its findings to parameters that had previously been reported. Throughout the study, the Hyperledger Caliper was used to make it easier for the administrator to customize his or her blockchain configuration.

Specifically, latency is defined as the length of time it takes for CHs to check for a new block in the network under the proposed paradigm. It is vital to note that the size of a block has an impact on both network and node latency. The latency of a node is estimated as the amount of time it takes the system for reaching the consensus once it first detects a new block validation algorithm. Open, transfer, and query were some of the transactions that were employed in the system analysis. Findings were reported for both Hyperledger Fabric and Ethereum, in addition to Hyperledger Fabric.

On the basis of three different transaction types, the results of the HLF simulation for latency and throughput are presented in Figure 2 and Figure 3. Generally speaking, a multi-layer approach lowers latency. In this system, new blocks are only vetted by a subset of nodes (i.e., CHs) before they are accepted.

Latency and throughput are equally as critical as security and privacy when it comes to choosing an IoT blockchain platform, and they are closely related. For a more in-depth examination of SUT behaviour, multiple rounds of benchmarks were conducted at varying transaction sending rates. To determine transaction latency, a series of experiments were carried out, and the findings are depicted in Figure 4 to Figure 5.

However, as the transmission rate approached 100 TPS, the minimum latency increased to less than 1 s. The maximum latency, on the other hand, grew to more than 100 TPS. When the transaction sending rate is changed, it has an impact on throughput, as illustrated in Diagram 12. Sending transactions at speeds of up to 110 transactions per second has no major impact on the throughput. The maximum acceptable transmitting rate for the SUT was 110 TPS, and as a result, a significant reduction in throughput.

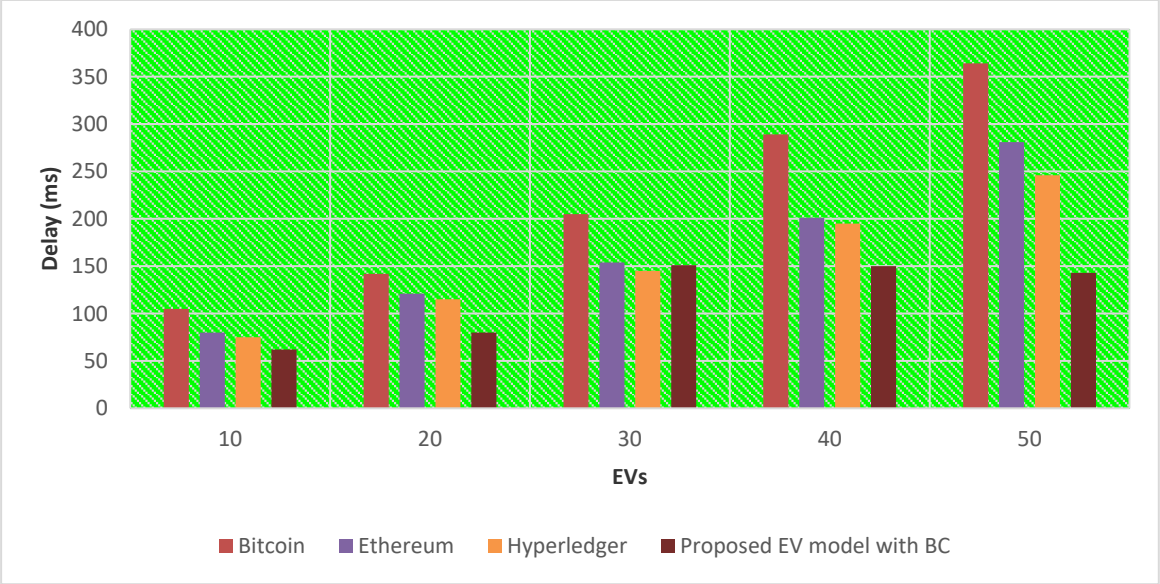

Fig. 2: Transaction Latency

Source: Author

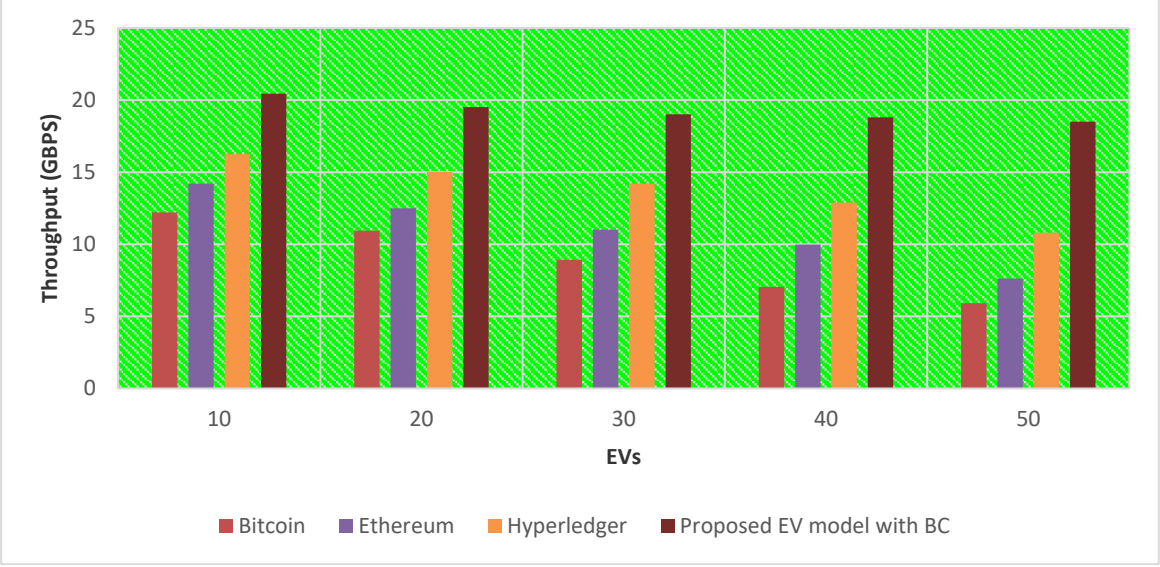

Fig. 3: Transaction Throughput

Source: Author

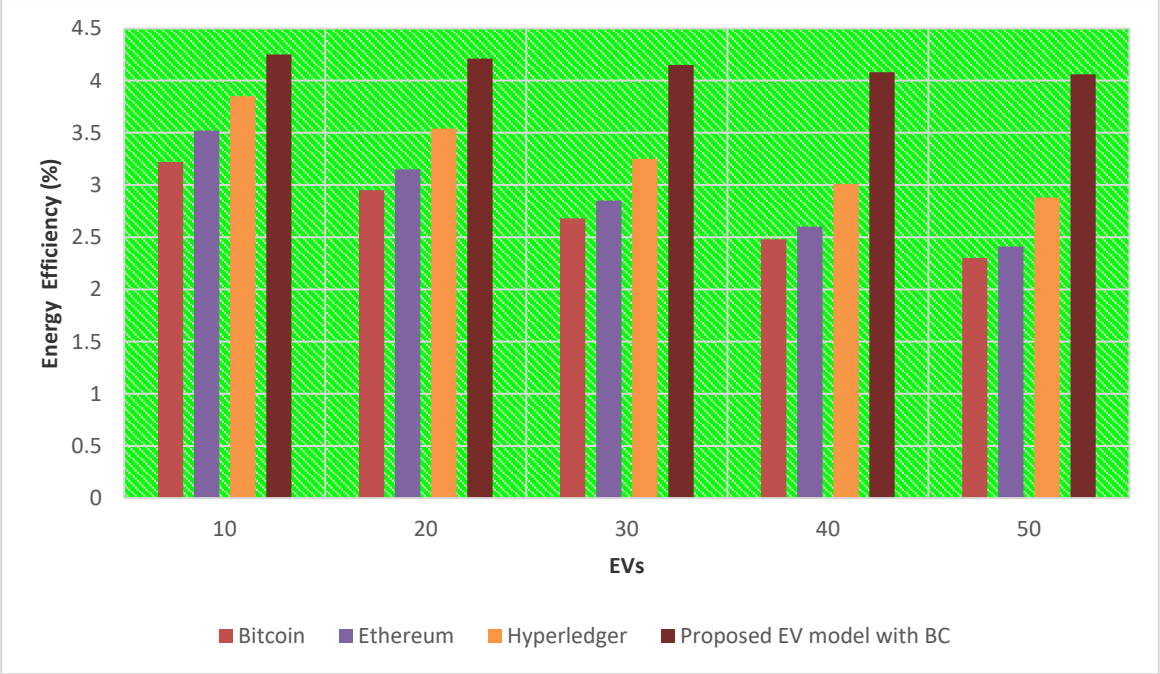

Fig. 4: Energy Efficiency

Source: Author

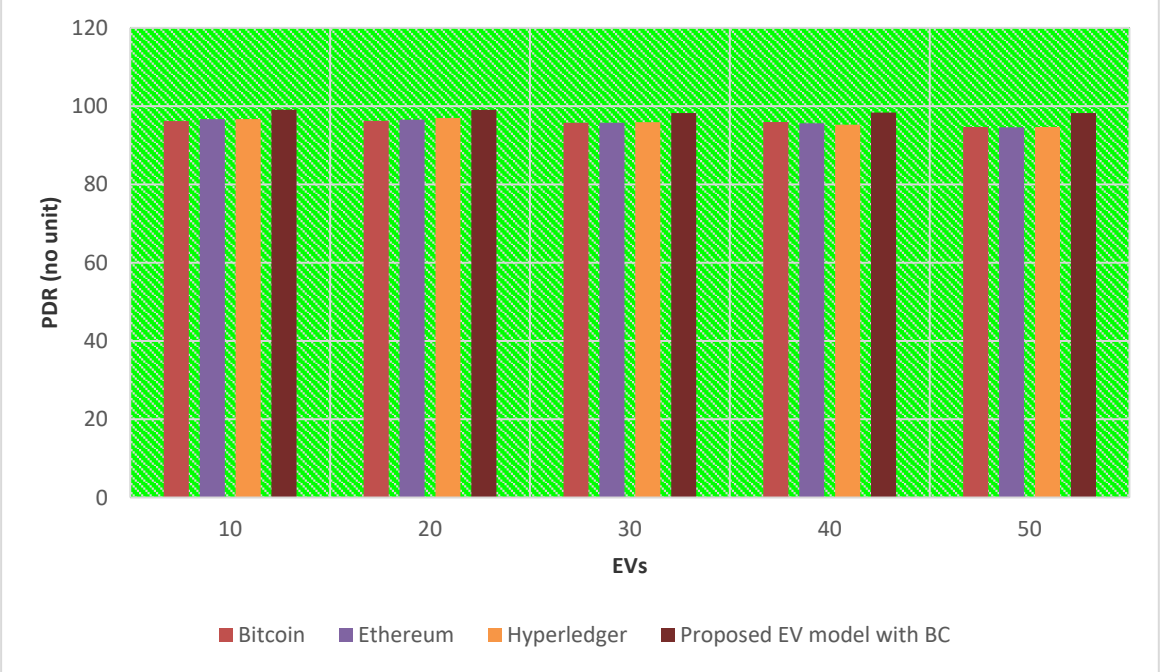

Fig. 5: Packet Delivery Ratio

Source: Author

Thus, it is seen that this network protocol acts as an efficient model in improving the data traversal across the cloud for the electrical vehicles.

6. CONCLUSIONS :

In this paper, a single client generated all of the transactions in the blockchain network under consideration. When it comes to transactions, HLF three-stage revolutionary design, dubbed execute-order-validate, is reliant on the preceding steps of the transaction to function properly. Because the actual throughput is close to 100%, a 100 TPS transmit rate is achievable and sustainable. Increasing the send rate to 100 and 200 TPS, on the other hand, only results in a small reduction in throughput. In future, the study can be improved by reducing the commercial payment fraud, which can reduce the possibility of fraudulent attack behaviour in the network.

REFERENCES :

[1] Su, Z., Wang, Y., Xu, Q., Fei, M., Tian, Y. C., & Zhang, N. (2018). A secure charging scheme for electric vehicles with smart communities in energy blockchain. *IEEE Internet of Things Journal*, *6*(3), 4601-4613. Google Scholar↗

[2] Liu, H., Zhang, Y., & Yang, T. (2018). Blockchain-enabled security in electric vehicles cloud and edge computing. *IEEE Network*, *32*(3), 78-83. Google Scholar↗

[3] Kim, M., Park, K., Yu, S., Lee, J., Park, Y., Lee, S. W., & Chung, B. (2019). A secure charging system for electric vehicles based on blockchain. *Sensors*, *19*(13), 3028; 1-22. Google Scholar↗

[4] Sadiq, A., Javed, M. U., Khalid, R., Almogren, A., Shafiq, M., & Javaid, N. (2020). Blockchain based data and energy trading in internet of electric vehicles. *IEEE Access*, *9*(1), 7000-7020. Google Scholar↗

[5] Sun, G., Dai, M., Zhang, F., Yu, H., Du, X., & Guizani, M. (2020). Blockchain-enhanced high-confidence energy sharing in internet of electric vehicles. *IEEE Internet of Things Journal*, *7*(9), 7868-7882. Google Scholar↗

[6] Javed, M. U., Javaid, N., Aldegheishem, A., Alrajeh, N., Tahir, M., & Ramzan, M. (2020). Scheduling charging of electric vehicles in a secured manner by emphasizing cost minimization using blockchain technology and IPFS. *Sustainability*, *12*(12), 5151. Google Scholar↗

[7] Xu, S., Chen, X., & He, Y. (2021). EVchain: an anonymous blockchain-based system for charging-connected electric vehicles. *Tsinghua Science and Technology*, *26*(6), 845-856. Google Scholar↗

[8] Knirsch, F., Unterweger, A., & Engel, D. (2018). Privacy-preserving blockchain-based electric vehicle charging with dynamic tariff decisions. *Computer Science-Research and Development*, *33*(1), 71-79. Google Scholar↗

[9] Asfia, U., Kamuni, V., Sheikh, A., Wagh, S., & Patel, D. (2019, June). Energy trading of electric vehicles using blockchain and smart contracts. In *2019 18th European Control Conference (ECC)*, 3958-3963. IEEE. Google Scholar↗

[10] Gabay, D., Akkaya, K., & Cebe, M. (2020). Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Transactions on Vehicular Technology*, *69*(6), 5760-5772. Google Scholar↗

[11] Li, H., Han, D., & Tang, M. (2020). A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. *IEEE Systems Journal*, *15*(3), 3189-3200. Google Scholar↗

[12] Firoozjaei, M. D., Ghorbani, A., Kim, H., & Song, J. (2019, August). EV Chain: A blockchain-based credit sharing in electric vehicles charging. In *2019 17th International Conference on Privacy, Security and Trust (PST)*, 1-5. IEEE. Google Scholar↗

[13] Samuel, O., Javaid, N., Shehzad, F., Iftikhar, M. S., Iftikhar, M. Z., Farooq, H., & Ramzan, M. (2019, November). Electric vehicles privacy preserving using blockchain in smart community. In *International Conference on Broadband and Wireless Computing, Communication and Applications*, 67-80. Springer, Cham. Google Scholar↗

[14] Yahaya, A. S., Javaid, N., Khalid, R., Imran, M., & Naseer, N. (2020, June). A blockchain based privacy-preserving system for electric vehicles through local communication. In *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, 1-6. IEEE. Google Scholar↗

[15] Li, Y., & Hu, B. (2020). A consortium blockchain-enabled secure and privacy-preserving optimized charging and discharging trading scheme for electric vehicles. *IEEE Transactions on Industrial Informatics*, *17*(3), 1968-1977. Google Scholar↗

[16] Baza, M., Sherif, A., Mahmoud, M. M., Bakiras, S., Alasmary, W., Abdallah, M., & Lin, X. (2021). Privacy-preserving blockchain-based energy trading schemes for electric vehicles. *IEEE Transactions on Vehicular Technology*, *70*(9), 9369-9384. Google Scholar↗

[17] Bhuvana, R. (2020). Blockchain as a Disruptive Technology in Healthcare and Financial Services-A Review based Analysis on Current Implementations. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(1), 142-155. Google Scholar↗

[18] Bhuvana, R., & Aithal, P. S. (2020). Blockchain based service: A case study on IBM Blockchain Services & Hyperledger Fabric. *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, *4*(1), 94-102. Google Scholar↗

[19] Aithal, P. S. (2020). Blockchain Technology: A Driving Force in Smart Cities Development. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 237-252. Google Scholar↗

[20] Bhuvana, R., & Aithal, P. S. (2020). RBI Distributed Ledger Technology and Blockchain-A Future of Decentralized India. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *5*(1), 227-237. Google Scholar↗

[21] Aithal, P. S., Aithal, A., & Dias, E. (2021). Blockchain Technology-Current Status and Future Research Opportunities in Various Areas of Healthcare Industry. *International Journal of Health Sciences and Pharmacy (IJHSP)*, *5*(1), 130-150. Google Scholar↗

[22] Rangi, P. K., & Aithal, P. S. (2020). A Study on Blockchain Technology as a Dominant Feature to Mitigate Reputational Risk for Indian Academic Institutions and Universities. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 275-284. Google Scholar↗

[23] Aithal, P. S., & Dias, E. (2022). Innovations in the Healthcare Industry Using Blockchain Technology: Concept, Application Areas, and Research Agendas. *Prospects of Blockchain Technology for Accelerating Scientific Advancement in Healthcare*, Chapter 3, 48-83. IGI Global, DOI: 10.4018/978-1-7998-9606-7.ch003, Google Scholar↗

[24] Manoj, K. S., & Aithal, P. S. (2020). Blockchain Cyber Security Vulnerabilities and Potential Countermeasures. *International Journal of Innovative Technology and Exploring Engineering*, *9*(5), 1516-1522. Google Scholar↗

[25] Bhuvana, R., Madhushree, L., & Aithal, P. S. (2020). Comparative Study on RFID based Tracking and Blockchain based Tracking of Material Transactions. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *4*(2), 22-30. Google Scholar↗

[26] Paul, P., Aithal, P. S., & Saavedra, R. (2021). Blockchain Technology and its Types—A Short Review. *International Journal of Applied Science and Engineering (IJASE)*, *9*(2), 189-200. Google Scholar↗

[27] Paul, P. K., Aithal, P. S., Bhuimali, A., Tiwary, K. S., Saavedra, R., & Ghosh, S. (2021). Emergence of Blockchain Technologies in Digital Healthcare— A Short Review. *International Journal of Information Science and Computing*, *8*(2), 59-67. Google Scholar↗

******