IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 3, June, 2023, pp. 703-709
Journal homepage: http://iieta.org/journals/isi

Performance Evaluation of a Multi Organizations Secure Internet of Vehicles Based on Hyperledger Fabric Blockchain Platform

Zahra Jafar[1*], Ali H. Hamad[2]

[1] Commission for Computers and Informatics, Informatics Institute for Postgraduate Studies, Baghdad 10001, Iraq
[2] Department of Information and Communication Engineering, University of Baghdad, Baghdad 10071, Iraq

Corresponding Author Email: zozaalshemary20@gmail.com

https://doi.org/10.18280/isi.280320

Received: 5 February 2023
Accepted: 2 April 2023

Keywords:
IoV, blockchain technology, Hyperledger fabric platform, Hyperledger caliper, multi organizations

ABSTRACT

The Internet of Vehicles, a new paradigm, is being incorporated into vehicular networks (IoV). IoV should enable heterogeneous access technologies for vehicle-to-environment communication. Security, privacy, cooperation, and the development of trust in-vehicle networks need to be considered for it to become a reality. Popular distributed ledger technology like blockchain might help with these issues. In this research, data transfer security has been achieved using a permission Hyperledger fabric. Two scenarios involving one organization and two organization models have been examined. The performance assessment in terms of throughput and average latency has been proposed for both cases. The results show that as the number of vehicles increases, the throughput drops and increases average delay. Also, the results show that in the two-organization model, the throughput is decreased slightly compared to one organization, while the latency is almost the same in both models.

1. INTRODUCTION

The rapid expansion of multimedia applications and advancements in human-machine interface technologies have led to increased global connectivity. This development in connectivity techniques has spurred the growth of Vehicular Ad-hoc Networks (VANET) towards the Internet of Vehicles (IoV). In an ideal IoV network, vehicles are connected through material objects embedded with numerous intelligent sensors, with internet-connected devices generating and exchanging vast amounts of data to improve human services [1].

In IoV, traditional methods based on trusted third parties (TTP) face multiple challenges due to their susceptibility to single points of failure. As everyone using a computer system has the potential to be malicious, attacks are possible [2]. In the Internet of Automobiles, vehicles communicate via safety beacon messages (SBMs), which provide crucial information such as name, location, and speed. Malicious nodes can obtain user privacy information by gathering and mining SBMs. The traditional Intelligent Transportation System (ITS) introduces a third-party certifying body, the Certificate Authority (CA), to verify users' identification. However, these third-party CAs are not always entirely reliable [3]. Relying on the TTP, the conventional strategy lacks adaptability for enabling various new applications. Therefore, it is critical to develop an approach that swiftly constructs a reliable system for each member. These complex, multidisciplinary issues have hindered the development of ITS. The emergence of blockchain technology offers a new opportunity to overcome the bottleneck in centralized ITS [4, 5].

Blockchain is composed of a series of blocks connected by their hash values. Transactions made by users in a P2P network are recorded in a public ledger within the blockchain network. Asymmetric cryptography is employed to decrypt messages encrypted by a corresponding public key, with users typically having a private key for decryption and a public key for sharing with others [6]. A user first broadcasts a transaction to its peers after signing it with their private key. Upon receiving it, peers verify the signed transaction and broadcast it across the network. Distributed consensus is achieved by mutually validating the transaction among all parties involved. A miner then adds the verified transaction to a timestamped block, which is subsequently broadcast back into the network. Once validated and hash-matched with the preceding block on the chain, the broadcast block is attached to the blockchain, containing the transaction. Blockchains can be either private (permissioned) or public (permissionless), depending on data management and application types. Both categories are decentralized and protect the ledger from incompetent or malicious users, but they differ primarily in the implementation of the consensus mechanism, ledger maintenance, and permission to join the P2P network [7].

Hyperledger Fabric, an open-source, private, permissioned distributed ledger technology platform, operates under the Linux operating system. Its modular architecture uses plug-and-play components to easily build a wide range of applications, ensuring security, privacy, confidentiality, scalability, and efficiency [8].

Blockchain offers numerous benefits, but it also faces significant challenges in terms of security, scalability, power consumption, and performance [9]. Researchers are actively working to address these issues and adapt blockchain for various applications [10, 11]. Understanding its dependence on different parameters is the first step in resolving performance problems.

In this work, we propose a blockchain-based IoV solution to tackle these challenges and evaluate the performance of the Hyperledger Fabric platform by examining metrics such as

throughput, average latency, and scalability adjustments, including block size and the number of organizations. The main contributions of this paper are as follows:

i. Two scenarios involving one and two organizations are examined, with the network models considered being the infrastructure layer and the vehicles layer.

ii. Comprehensive experiments using Caliper Fabric are conducted to assess the effectiveness of the proposed method.

The remainder of this paper is organized as follows: Section 2 presents a review of relevant works in the performance assessment of blockchain platforms. Section 3 introduces the Hyperledger Fabric platform. The proposed secure IoV system architecture is suggested in Section 4. Section 5 provides a detailed conclusion.

2. RELATED WORK

Various frameworks and tools have been implemented by numerous organizations with different objectives to develop and deploy blockchain networks that accommodate diverse requirements and scenarios. George et al. [12] proposed a novel blockchain-based decentralized authentication approach for Vehicular Ad-hoc Networks (VANET), implemented the approach using Hyperledger Fabric, and compared its performance to the traditional Public Key Infrastructure (PKI)-based method for VANET authentication. Zhang et al. [13] suggested a privacy-preserving authentication scheme for VANETs based on a consortium blockchain, developing a prototype on the Hyperledger Fabric platform. The scheme represents the legitimacy of a vehicle or a roadside device by their transaction capacity on the blockchain, rather than a certificate or cryptographic key. Gao et al. [14] proposed a multi-channel blockchain scheme, adopting the well-known permissioned blockchain platform Hyperledger Fabric. The system first defines multiple blockchain channels and then selects the best channel based on vehicle density and application requirements for transaction throughput and latency. Chulerttiyawong and Jamalipour [15] employed a permissioned consortium blockchain system with Hyperledger Fabric to enhance security and privacy in VANETs. They proposed a vehicular blockchain system to provide secure vehicle-to-everything (V2X) communications, leveraging the consensus mechanism and smart contracts in Fabric.

Gao et al. [16] provided a comprehensive performance evaluation of Hyperledger Fabric by analyzing the impact of different parameters such as network size, block size, and payload size. They presented a set of guidelines for designing an efficient blockchain network based on the findings of their experiments. Gaba et al. [17] conducted an in-depth analysis of blockchain block size, considering various attributes of block elements and their types. They also calculated the overall size of the block based on these attributes and employed VANETs as a case study to demonstrate the application of blockchain in this context. The Hyperledger Fabric platform was used to implement the VANET application.

These studies demonstrate the potential of blockchain technologies, particularly Hyperledger Fabric, in enhancing the security, privacy, and trust in IoV applications. However, there is still a need for a systematic and comprehensive analysis of the performance of Hyperledger Fabric in an IoV setting, taking into account various network parameters and their impact on the system's efficiency. Our work contributes to this end by proposing a blockchain-based IoV solution and conducting an extensive performance evaluation of the Hyperledger Fabric platform under different scenarios and configurations.

3. HYPERLEDGER FABRIC PLATFORM

The Hyperledger fabric network is made up of various parts linked together in a peer to peer way, including peers, orderers, certificate authorities, channel and organization [17]. Hyperledger Fabric, being a permissioned platform, enables confidentiality through its channel architecture. Basically, participants on a Fabric network can establish a “channel” between the subset of participants that should be granted visibility to a particular set of transactions. Thus, only those nodes that participate in a channel have access to the smart contract (chaincode) and data transacted, preserving the privacy and confidentiality of both. Peers are two types: peer commitment and peer endorsement, and they can communicate with one another utilizing the gossip data distribution protocol. Peers will make up each organization's membership. A single channel may have any number of peers from several organizations. The company offers a client application in addition to one for peers. Smart contracts are present in peer nodes along with their copy of the ledger. A network channel's usage of a chain token deployed on peers is created from a collection of smart contracts, which are software programs that specify the rules between various organizations. The ledger, which is made up of a global state and a whole blockchain, is employed to capture important real-world data related to the application. The Hyperledger fabric ledger's current state is represented by Global State. The transactional history leading to the present state is contained in the complete blockchain. Certificate Authorities generate the certificates that represent identities for each entity in the fabric network. the MSP manages, validate these identities, authenticates clients who want to join the network based on list of permissioned identities that exist in it. Orderer nodes order all network transactions by proposing new blocks and seeking agreement. An ordering service collects orders where the Hyperledger fabric platform offers three ordering services, which are: (Solo, Kafka, and Raft) [18].

The block consists of transactions in a blockchain and is connected to other blocks. Each block contains a collection of transactions. Figure 1 illustrates the hyper ledger transaction flow when the entity requests to join Hyperledger fabric network, the Certificate Authorities generate the identities to this entity, then when entity request a transaction, the MSP validate identities if within list of permissioned identities, then it legal, and the entire transaction flow is made up of the following three phases: simulate, order-validate, and commit. A transaction proposal is created by the client (vehicle) to query or write data to the blockchain network.

The transaction proposal is being sent by the client application to numerous endorsing peers (RSU) associated with the same channel. The endorsing peers simulate the transaction. The endorsing peers (RSU) validate the transactions and query the ledger to determine the ledger's current status using the smart contract. After endorsement, the endorsing peers (Road Side Uinte RSU) send the signed endorsement result back to the client (vehicle). The client application gathers all responses and sends them to the Orderer Service Node (OSN), which uses the consensus to determine

the ordering of the transaction. The new block is broadcast to all endorsing peers and committing peers of the same channel. Now that the new block has been broadcast to all endorsing peers and committing peers of the same channel, all peers will verify this. Now that all peers have validated the new block, the transactions are in the ledger [19].

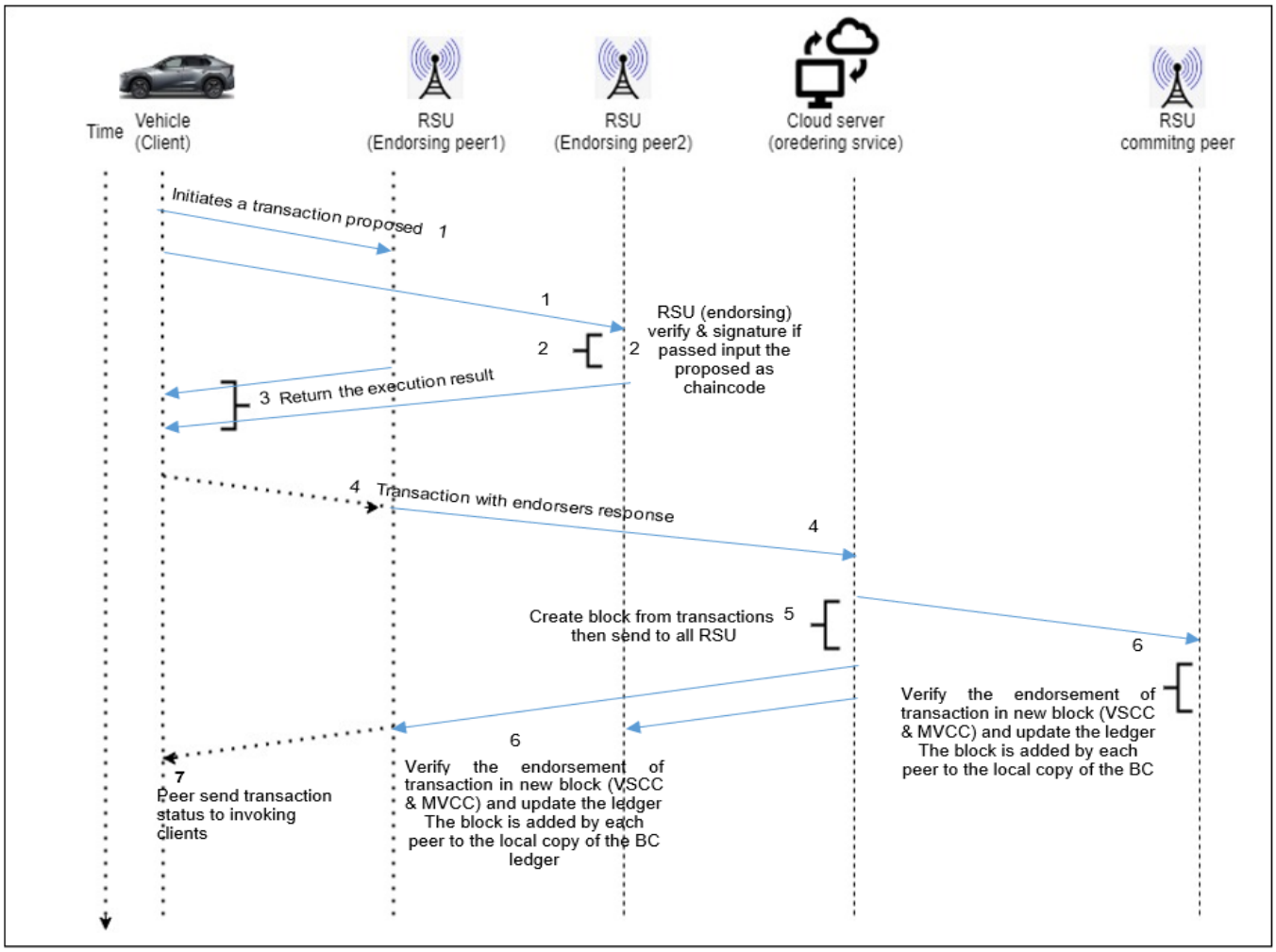


Figure 1. Hyperledger fabric transaction flow

4. PROPOSED IoV SYSTEM DESIGN

An example blockchain network built on Hyperledger fabric is suggested for performance testing blockchain-based IoV. The client nodes (vehicles) in the network deliver transactions to the client application servers. By using the software development kit (SDK) of the Hyperledger fabric, a client can communicate with all networks. Orderer service node, channel, and RSU as peers (endorser and committer) grouped into organizations represent fabric network participants. Each organization has a membership service provider (MSP), which provides a list of identity members along with the necessary rights to the certificate authority (CA) that represents identities (key pairs).

Figure 2 shows the architecture of the suggested system design. Hyperledger Caliper, a benchmarking tool, is used to analyze the performance of this network. The blockchain network is managed by Caliper; it also generates HTML reports detailing the effectiveness of the network.

The Caliper fabric provides many performance metrics, such as throughput, average latency, and resource utilization, such as memory and CPU usage.

There have been two proposed scenarios: one organization and two organizations (one peer and one endorser peer per each organization), with throughput and average latency being the two parameters to be tracked.

Throughput is the rate at which all network nodes commit legitimate transactions within a defined period of time. Transactions per second are utilized in throughput (tps). Latency is the time it takes for a transaction to complete, be recorded in the ledger, and become accessible to the general public across the network [20]. The block size and vehicle count, therefore, affect the IoV performance metrics on the blockchain.

Each scenario has varied scale of vehicles, number of transactions and block size to measure the impacts of scaling the organization. one organization provides high throughput and low latency than two organizations, but it could suffer from failure, while in two organizations scenario, this could act as a redundancy. For each scenario performed Five rounds with increase in the number of vehicles (25, 50, 75, 100, 125, 150, 175) and block size (10, 50, 100, 150, and 200 Bytes). Each round contains 100 transactions at a preset transmission rate (50, 100, 150, 200, and 250 tps) with a block timeout of 2 seconds. The transactions are produced by an application that enables several client nodes to send transactions concurrently and in parallel. Table 1 shows the basic configuration settings.

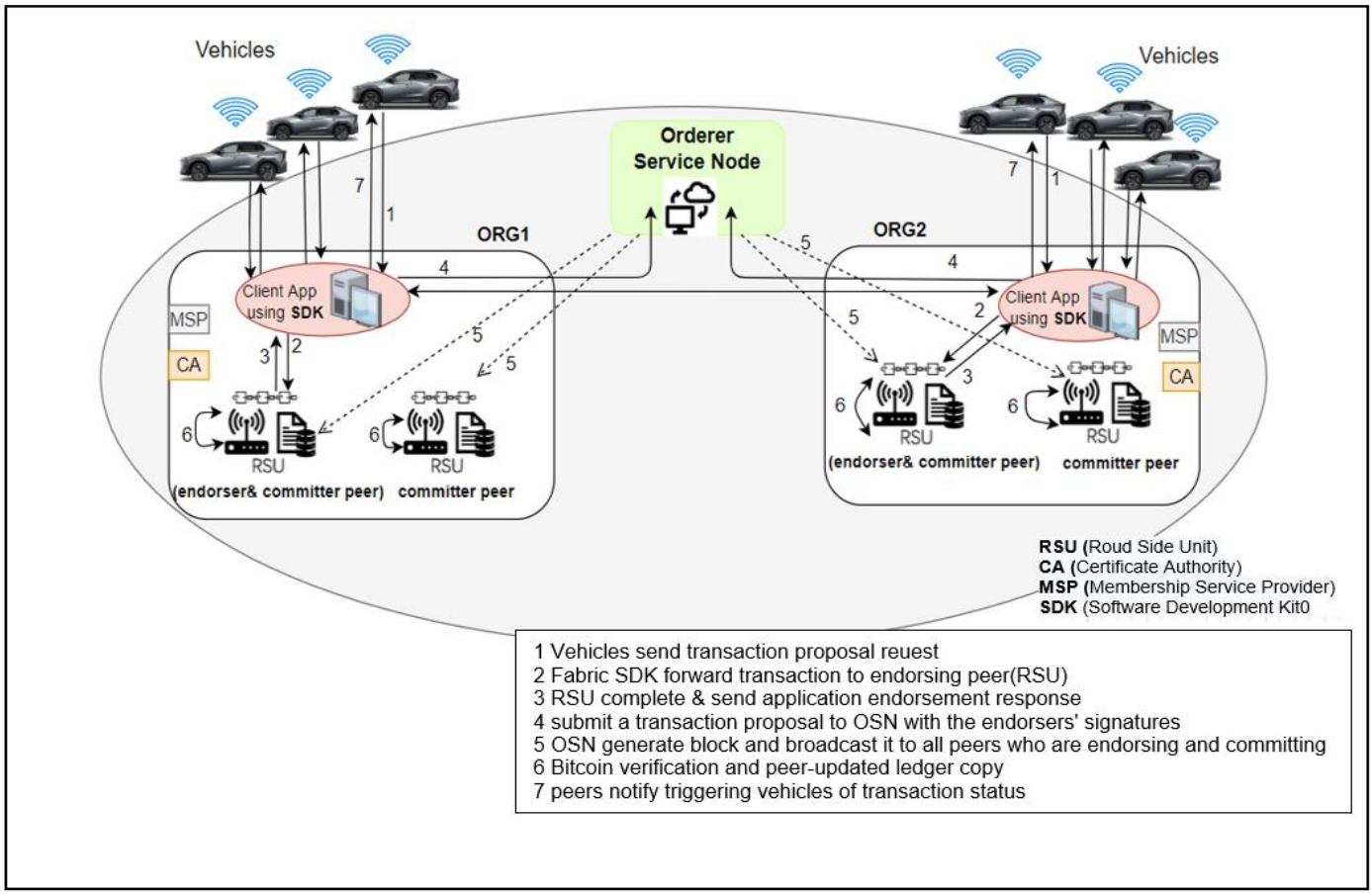


Figure 2. The Hyperledger fabric network is the base for the proposed IoV system's architecture

Table 1. Basic configuration parameters

Parameter	Configuration
7 Groups of vehicles	7 groups
Transactions	100 transactions per round
No. vehicles	(25,50,75,100,125,150,175)
Send rate	(50,100,150,200,250) tps
Block size	(10,100,300) transactions per block
Block timeout	2 sec

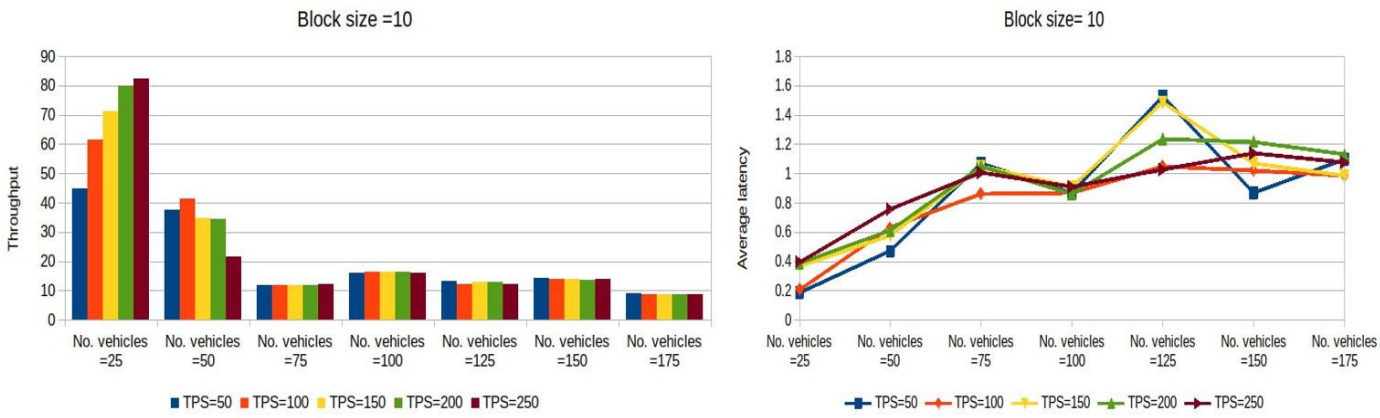
5. ONE ORGANIZATION SCENARIO

Performance analysis of various block sizes in this scenario, transaction send rates, and the number of vehicles has been tested.

Figure 3 (a) shows the block size 10. When there are 25 vehicles, the transaction throughput increases. When tps is 250, the maximum measured throughput is around (79.8), and then throughput starts to decrease. While the average latency is decreased to (0.19) when the number of vehicles is 25, tps is 50. While the highest latency (1.49).

Figure 3 (b) shows the block size 100, the highest throughput (96.1) when the number of vehicles is 25 and tps 250. The average latency is decreased to (0.48) when the number of vehicles is 25 and the tps is 200. While the highest latency (2.05).

Figure 3 (c) shows the block size 300, the highest throughput (45.7) when the number of vehicles is 25 and tps 150. And average latency is decreased to (1.1) when the number of vehicles is 25 and tps is 50. While the highest latency (2.1).



(a)

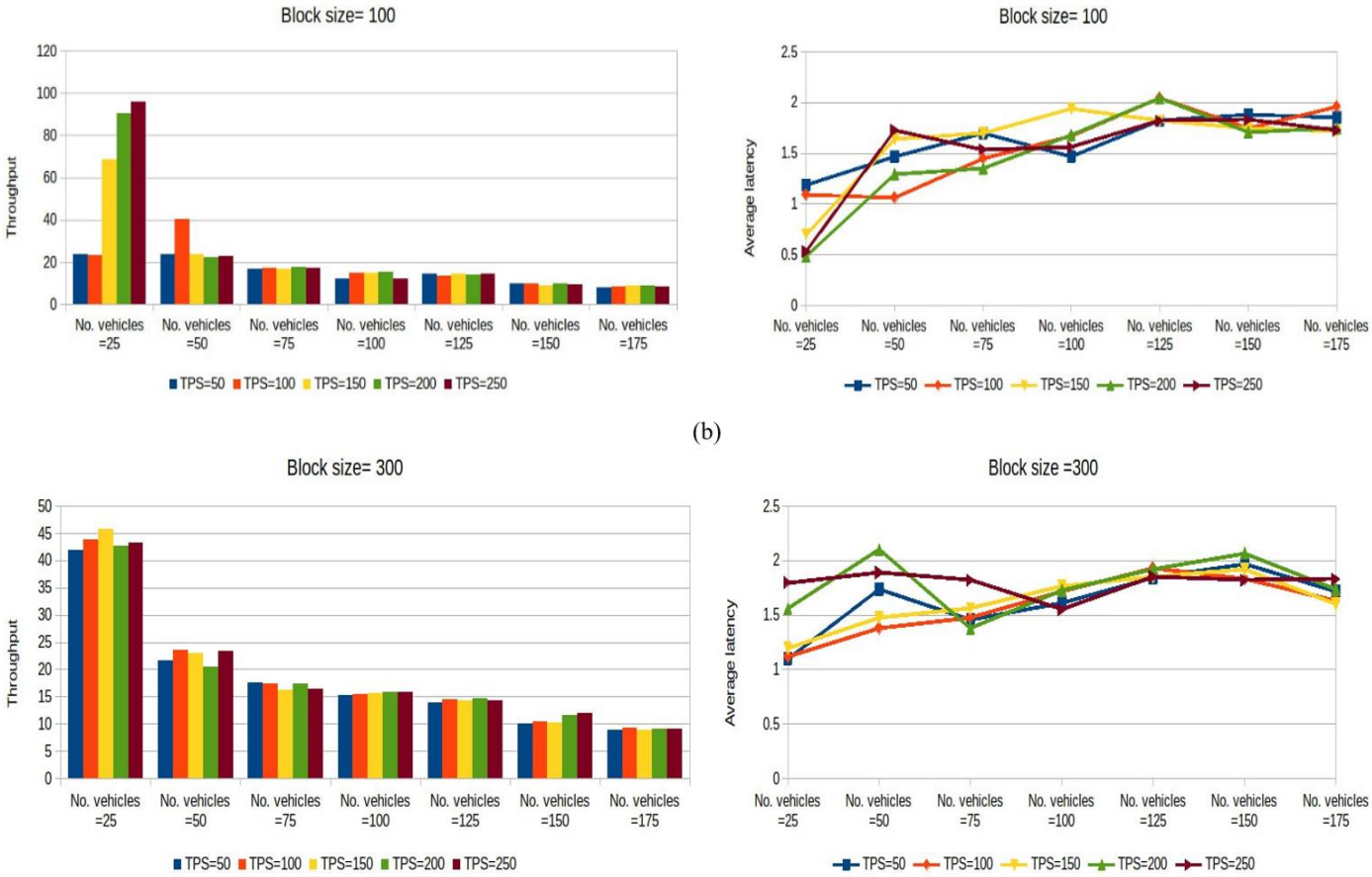


Figure 3. Throughput and latency performance for one organization

6. TWO ORGANIZATION SCENARIO

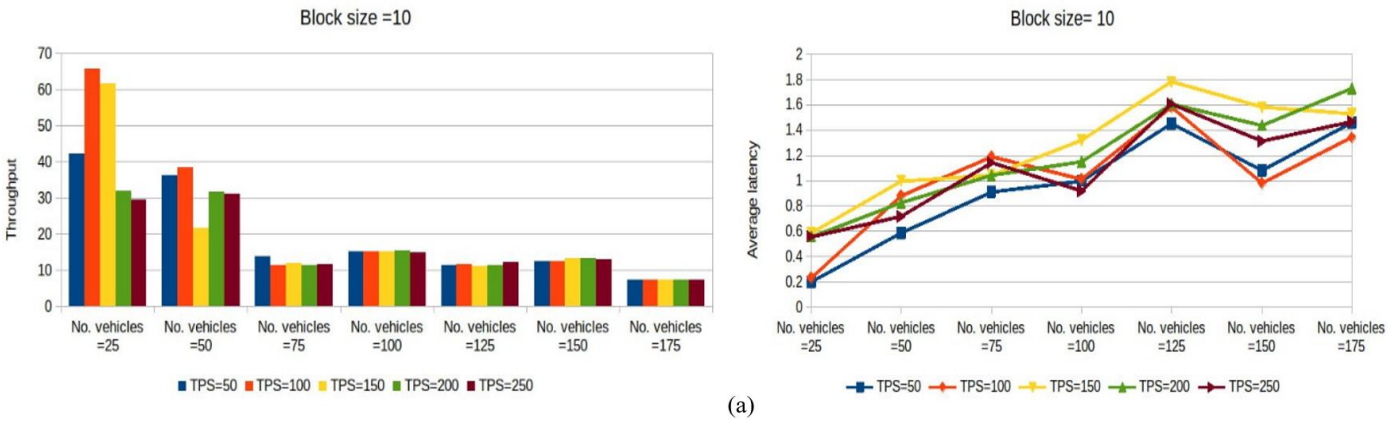
Performance assessment of variable block size, transaction send rate, and vehicle count has been conducted in this scenario. Figure 4 (a) shows the block size 10. The transaction throughput is increased when the number of vehicles is 25; the highest throughput obtained was about (65.7) when the tps is 100, then throughput starts to decrease. While average latency is reduced to (0.2) when the number of vehicles is 25, tps is 50. While the highest latency (is 1.78).

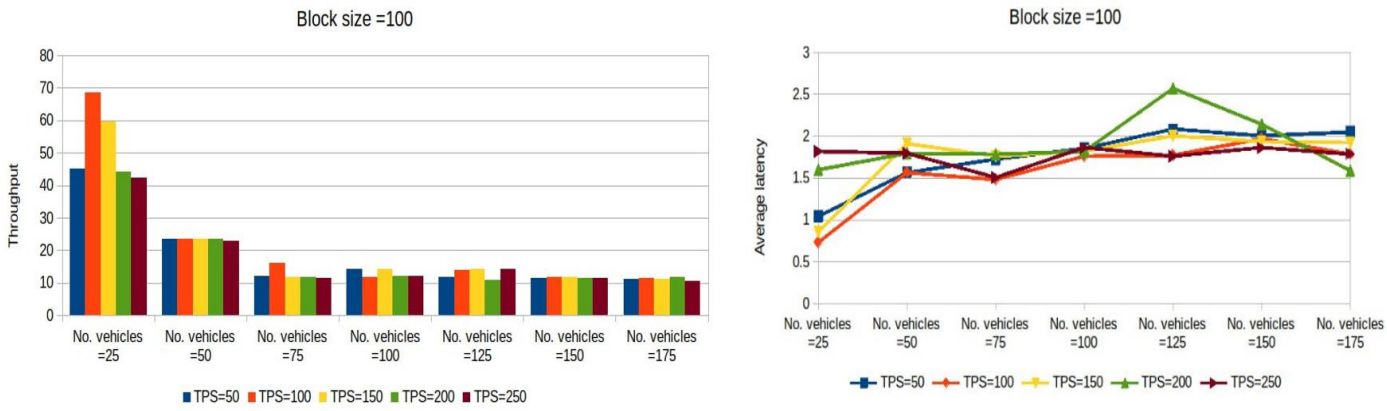
Figure 4 (b) shows the block size 100, the highest throughput (68.7) when the number of vehicles is 25 and tps 100.

And average latency is decreased to (0.73) when the number of vehicles is 25, tps is 100. While the highest latency (is 2.57).

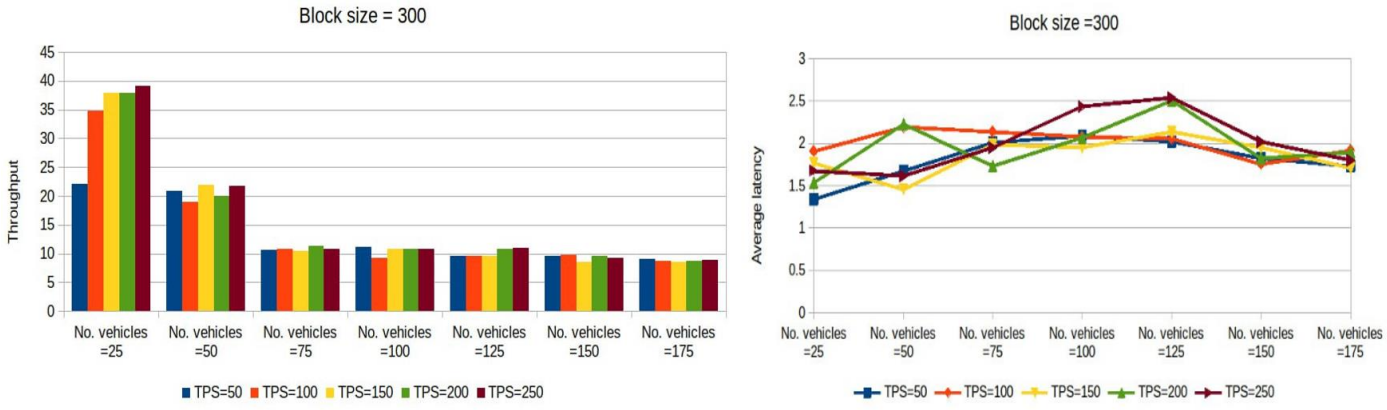
Figure 4 (c) shows the block size 300, the highest throughput (39.1) when the number of vehicles is 25 and tps 250. And average latency is decreased to (1.34) when the number of vehicles is 25, tps is 50. While the highest latency (is 2.54).

According to the findings, throughput fell and latency rose when block sizes were raised to more above 100 transactions per block. When employing a smaller block size, such as 10 transactions per block and a limited number of cars, better performance and latency were found at low send rates, like 100 tps; thus, raising the block size reduced the performance.





(b)



(c)

Figure 4. Throughput and latency performance for two organizations

7. CONCLUSION

This article examines the impact of the secure IoV workload on the throughput, scalability, and latency of the Hyperledger fabric blockchain platform. Different transaction transmits rates (tps), block sizes, and organization counts were used to simulate various scenarios. The hardware setup, smart contract complexity, and smart contract activities all affect how the blockchain network functions. Consequently, the following findings were drawn in further detail:

1 In one organization, the throughput result is higher than in two organizations; that is, the high result read 96.1, while the two organizations read 68.7. but we prefer a scenario of two because if the network stops in one organization, another organization can complete it.
2 Each block can note the number of vehicle impact to throughput and that throughput decrease when the number of vehicles is increased.
3 Latency increases when increased the number of vehicles. And latency varies when the block's size increases, but most are increased.
4 In one organization, when the block size is 10, the high throughput reads 82.3. Then in block size 100, the throughput increased to 96.1; when block size 300, the throughput is 45.7.
5 In two organizations, when the block size is 10 highest throughputs read 65.7. In block size 100, the highest throughput read 68.7, while in block size 300, the highest throughput is 39.1.
6 Therefore from 5, 6, we can summary the best block size is 100 in one organization and two organizations.
7 The result shows that an increased block size and number of vehicles have impact on the blockchain network's performance, the large block size give better results, while increasing number of vehicles shows high latency and low throughput.
8 As compared with our work [13], investigates the impact of different block sizes from 10 to 60 in steps of 10, a remarkable increase in throughput can be observed with the block size growing from 10 to 40, but the trend is terminated thereafter, which reveals that throughput cannot continuously benefit from the increase of block size.
9 In IoV security, the traditional way used identity-based encryption or authentication vehicle with the CA, but these ways depend on a trusted third party and centralized system. While blockchain is decentralized system, so if one point fails the system can continue and blockchain contain of set of blocks connected each other by their hash values, therefor the malicious nodes need add or change all blocks, and the Hyperledger network based on CA to provide identity and MSP node to validate identities. Hyperledger used consensus algorithms, to reach consensus, which requires a node to validate a batch of transactions and add them as a new block to the blockchain.

ACKNOWLEDGMENT

The IIPS institute and the University of Baghdad have developed this work.

REFERENCES

[1] Ning, Z., Hu, X., Chen, Z., Zhou, M., Hu, B., Cheng, J., Obaidat, M.S. (2017). A cooperative quality-aware service access system for social Internet of vehicles. IEEE Internet of Things Journal, 5(4): 2506-2517. https://doi.org/10.1109/JIOT.2017.2764259

[2] Liu, X., Huang, H., Xiao, F., Ma, Z. (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. IEEE Internet of Things Journal, 7(5): 4101-4112. https://doi.org/10.1109/JIOT.2019.2957421

[3] Jabbarpour, M.R., SeyedFarshi, S., Sookhak, M., Zomaya, A.Y. (2020). Proposing a secure self-fining vehicle using blockchain and vehicular edge computing. IEEE Consumer Electronics Magazine, 11(2): 28-35. https://doi.org/10.1109/MCE.2020.3038029

[4] Wu, M., Wang, K., Cai, X., Guo, S., Guo, M., Rong, C. (2019). A comprehensive survey of blockchain: From theory to IoT applications and beyond. IEEE Internet of Things Journal, 6(5): 8114-8154. https://doi.org/10.1109/JIOT.2019.2922538

[5] Xiong, Z., Zhang, Y., Niyato, D., Wang, P., Han, Z. (2018). When mobile blockchain meets edge computing. IEEE Communications Magazine, 56(8): 33-39. https://doi.org/10.1109/MCOM.2018.1701095

[6] Bhutta, M.N.M., Khwaja, A.A., Nadeem, A., Ahmad, H. F., Khan, M.K., Hanif, M.A., Song, H., Alshamari, M., Cao, Y. (2021). A survey on blockchain technology: Evolution, architecture and security. IEEE Access, 9: 61048-61073. https://doi.org/10.1109/ACCESS.2021.3072849

[7] Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., Janicke, H. (2018). Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet of Things Journal, 6(2): 2188-2204. https://doi.org/10.1109/JIOT.2018.2882794

[8] Saeed, S.H., Hadi, S.M., Hamad, A.H. (2022). Performance evaluation of e-voting based on hyperledger fabric blockchain platform. Revue d'Intelligence Artificielle, 36(4): 581-587. https://doi.org/10.18280/ria.360410

[9] Knirsch, F., Unterweger, A., Engel, D. (2019). Implementing a blockchain from scratch: Why, how, and what we learned. EURASIP Journal on Information Security, 2019: 1-14. https://doi.org/10.1186/s13635-019-0085-3

[10] Zhang, R., Xue, R., Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys (CSUR), 52(3): 1-34. https://doi.org/10.1145/3316481

[11] Bernabe, J.B., Canovas, J.L., Hernandez-Ramos, J.L., Moreno, R.T., Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. IEEE Access, 7: 164908-164940. https://doi.org/10.1109/ACCESS.2019.2950872

[12] George, S.A., Jaekel, A., Saini, I. (2020). Secure identity management framework for vehicular ad-hoc network using blockchain. In 2020 IEEE Symposium on Computers and Communications (ISCC), pp. 1-6. https://doi.org/10.1109/ISCC50000.2020.9219736

[13] Zhang, Y., Tong, F., Xu, Y., Tao, J., Cheng, G. (2020). A privacy-preserving authentication scheme for VANETs based on consortium blockchain. In 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), pp. 1-6. https://doi.org/10.1109/VTC2020-Fall49728.2020.9348497

[14] Gao, L., Wu, C., Yoshinaga, T., Chen, X., Ji, Y. (2021). Multi-channel blockchain scheme for internet of vehicles. IEEE Open Journal of the Computer Society, 2: 192-203. https://doi.org/10.1109/OJCS.2021.3070714

[15] Chulerttiyawong, D., Jamalipour, A. (2021). A blockchain assisted vehicular pseudonym issuance and management system for conditional privacy enhancement. IEEE Access, 9: 127305-127319. https://doi.org/10.1109/ACCESS.2021.3112013

[16] Gao, L., Wu, C., Du, Z., Yoshinaga, T., Zhong, L., Liu, F., Ji, Y. (2022). Toward efficient blockchain for the internet of vehicles with hierarchical blockchain resource scheduling. Electronics, 11(5): 832. https://doi.org/10.3390/electronics11050832

[17] Gaba, P., Raw, R.S., Mohammed, M.A., Nedoma, J., Martinek, R. (2022). Impact of block data components on the performance of blockchain-based VANET implemented on hyperledger fabric. IEEE Access, 10: 71003-71018. https://doi.org/10.1109/ACCESS.2022.3188296

[18] The Linux Foundation Project. Available Online: https://www.hyperledger.org/, accessed on May 27, 2022.

[19] Sey, C., Lei, H., Qian, W., Li, X., Fiasam, L.D., Kodjiku, S.L., Adjei-Mensah, I., Agyemang, I.O. (2022). VBlock: A blockchain-based tamper-proofing data protection model for Internet of vehicle networks. Sensors, 22(20): 8083. https://doi.org/10.3390/s22208083

[20] Hyperledger white paper working group. (2018). Hyperledger Blockchain Performance Metrics. San Francisco, CA, USA: Linux Foundation, pp. 1-17. Retrieved from https://hyperledger.org/.